Administrator's Guide

AudioCodes One Voice Operations Center (OVOC)

Device Manager Pro

Version 8.4

audiocodes

Notice

Date Published: June-23-2024

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

Stay in the Loop with AudioCodes

Related Documentation

Document Name
400HD Series IP Phone User Manuals
400HD Series IP Phone with Microsoft Skype for Business User Manuals
400HD Series IP Phones Administrator's Manual

Document Name
400HD Series IP Phone with Microsoft Skype for Business Administrator's Manual
400HD Series IP Phone Quick Guides
400HD Series IP Phone with Microsoft Skype for Business Quick Guides
400HD Series IP Phone for Microsoft Teams User and Administrator Manuals
Device Manager for Third-Party Vendor Products Administrator's Manual
Device Manager Deployment Guide
Device Manager Agent Installation and Configuration Guide
One Voice Operations Center IOM Manual
One Voice Operations Center User's Manual

Document Revision Record

LTRT	Description
91097	Initial release for 7.8. Set as VIP. Network Topology page. Poly phones provisioned to sites. System Settings and tabs. Rearranged GUI.
91098	7.8.1000. Endpoints Groups. Configuring DHCP Option 160 - tenant and group. Filtering by group in Manage Multiple Devices. Zero Touch: URL to associate device w Tenant and Group.
91188	8.0.1000 New look and feel. Devices Status page: Enhanced Show Info feature. Teams phones and devices: RXV80, C435HD, C448HD, C470HD. Tenant / Site Configuration: provision devices using the 'Configuration Set' parameter and the corresponding 'Configuration Key' and 'Configuration Value' parameters auto-populated after selecting a device model. Parameters in configuration file commented to indicate template source.
91189	Polycom>Poly. EPOS. Poly CCX 500/600. RXV100 (MTR). 'Show Info' page includes detailed info reported by Teams devices (Status/Configuration). New 'Collect logs' link in 'Show Info' page; capability to collect logs on native Teams phones.
91190	EPOS. RXV100 (MTR). RXV90. DST.
91221	[8.0.3000 Fix 1] Microsoft SIP Gateway

LTRT	Description
91222	[8.0.3000 Fix 2] Finalization of Microsoft SIP Gateway. RX Bundles.
91223	[8.2.1000 Fix 1] RX-PAD MTR Controller. Peripherals (RX15, RXVcam10). Desktop|PC. AppSuite. SN status parameter. Bulk Android APK update. Renovated. Replaced screenshots. RXV100 status | version info | Windows version.
91225	Document restructured. Fix to section 'Converting Skype for Business Phones to Teams SIP Gateway'.
91226	MAC prefix. Device Manager FQDN. 'Set Defaults' in ZT Templates Mapping. RX-PANEL. RXV200. RX40. MAC Address of MTR with which RX-PAD is Paired. RXV81 connected as a USB peripheral. RXVCam10 Content Camera peripheral device. Devices Status page displays 'bundle' image. DM displays MAC address of MTR with which RX-PAD is paired.
91227	8.2.2000 > 8.2.3000.
91228	8.4. 'Screen capture' feature. 'Up Time' feature. All screenshots replaced. Texts adjusted. Restore a single Native Teams device to its default settings. SIP Gateway. C436HD. Reason for last reboot. RXV81 USB Peripheral. Configuring an MTRA Bundle.

Table of Contents

1 Introduction

AudioCodes' Device Manager gives enterprise IT managers | network admins full control of their IP phones, meeting rooms and other devices throughout their lifecycle. Admins benefit from a powerful and easy-to-use tool for everyday tasks such as configuration, monitoring and troubleshooting to increase efficiency and ensure user satisfaction. This is especially true in the era of hybrid working where employee users are likely to be working from home, with meeting rooms in the office.

Device Manager enables admins to provide a reliable desktop phone service within their enterprises. With the ability to deploy and monitor AudioCodes IP phones, meeting rooms, and EPOS and Jabra headsets and speakers, the management interface enables admins to rapidly identify problems and efficiently fix them. This proactive approach ensures quality assurance and employee satisfaction, increased productivity and reduced IT expenses.

- When Device Manager is deployed in a cloud environment, it's strongly recommended to implement VPN communication between OVOC (Device Manager) server and endpoints for security reasons.
- When Device Manager is deployed in an internal network or in a private cloud environment as shown in this document, no additional definitions are required. Deployment of this (on-premises) Device Manager flavor should be restricted to either an internal network or a private cloud environment.

Commissioning and Provisioning

- Device discovery and auto-registration
- Automatic device zero-touch provisioning
- Network topology planning and design
- Large scale efficient deployment
- Support remote management of devices behind NAT (remote workers)

Streamline Day-to-Day Operations

- Increase efficiency using centralized real-time monitoring dashboard and maps
- Mass configuration and software updates for all devices or specific tenants / sites / groups
- Improve availability with accurate and correlated alarm indications

Quality Assurance and Analytics

- Identify and mitigate voice quality issues before they become service affecting using real-time network view and quality alerts
- Troubleshoot quality issues and drill down for simple and effective root cause analysis

- Pattern detection and network planning via advanced reporting tools

About this Document

This guide shows admins how to enable automatic provisioning (Zero Touch provisioning) of devices in an enterprise network from a single central point.

- See the *Device Manager Deployment Guide* for the critical steps to take to *deploy* devices in a network.
- For information about third-party vendor devices (e.g., EPOS, Jabra and Poly), see here.

2 Starting up | Logging in

After installation, start the Device Manager Pro and log in. Before logging in, you need to run OVOC.

- To access the Device Manager Pro without running OVOC, point your web browser to https://<OVOC_IP_Address>/ipp and then in the login screen that opens, log in. If the browser is pointed to HTTP, it will be redirected to HTTPS.
- Device Manager Pro is a secured web client that runs on any standard web browser supporting HTML5: Internet Explorer v11 and later, Chrome or Firefox.

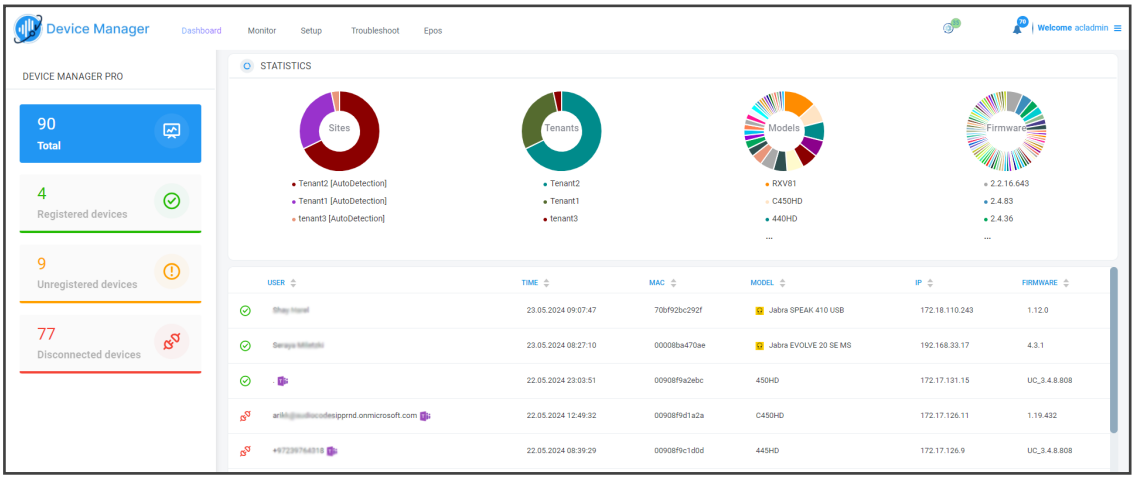
For information on installing and operating OVOC, see the *OVOC Server IOM Manual* and the *OVOC User's Manual*.

➢ To log in to the Device Manager Pro via OVOC:

1. In the OVOC's Network page, click the **Endpoints** tab and from the dropdown select **Configurations**.

The 'Username' and 'Password' used to log in to the Device Manager Pro are the same as those used to log in to OVOC.

2. Enter your Username and Password (default = **acladmin** and **pass_1234**) and click **Sign In**; the application is launched and the Monitor Dashboard is displayed.



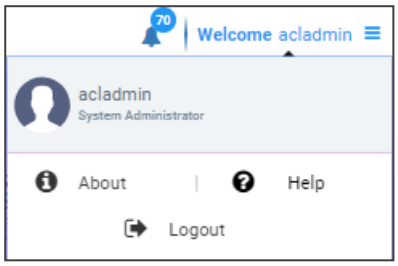
- See under here for detailed information about monitoring devices.
- The following topics show how to provision phones using Zero Touch.

Viewing the About Screen

The About screen enables admin to access info about Device Manager as well as to log out of the app from whatever page they're in. The screen is aligned with the About screen in OVOC.

➢ **To view the About screen:**

- In any page in Device Manager, click the uppermost right menu icon.

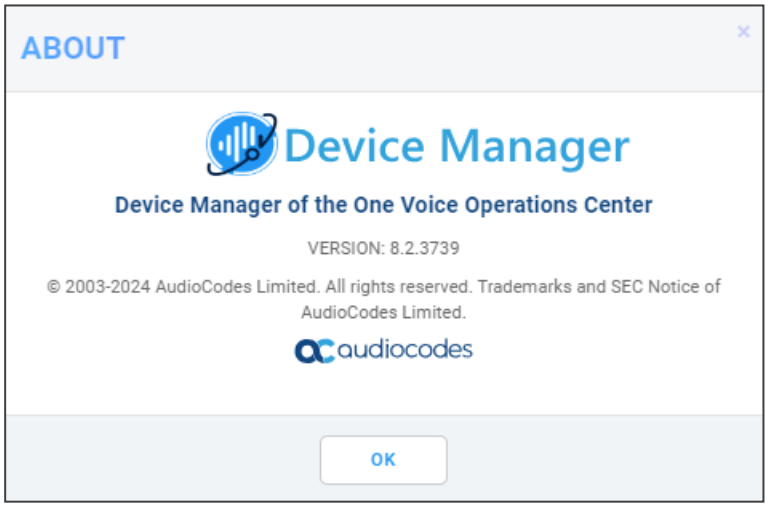


➢ **To log out:**

- Click the **Logout** option.

➢ **To view version information:**

- Click the **About** option.



3 Provisioning

Provisioning covers:

- Using the Zero Touch Setup Wizard to Provision Devices - see here
- Provisioning Devices without the Zero Touch Setup Wizard - see here
- Provisioning Android-based Teams Devices - see here

Zero Touch Provisioning

AudioCodes' IP phones can be automatically provisioned when they are plugged in to the enterprise's network if Zero Touch provisioning has been implemented.

Applies to all phones.

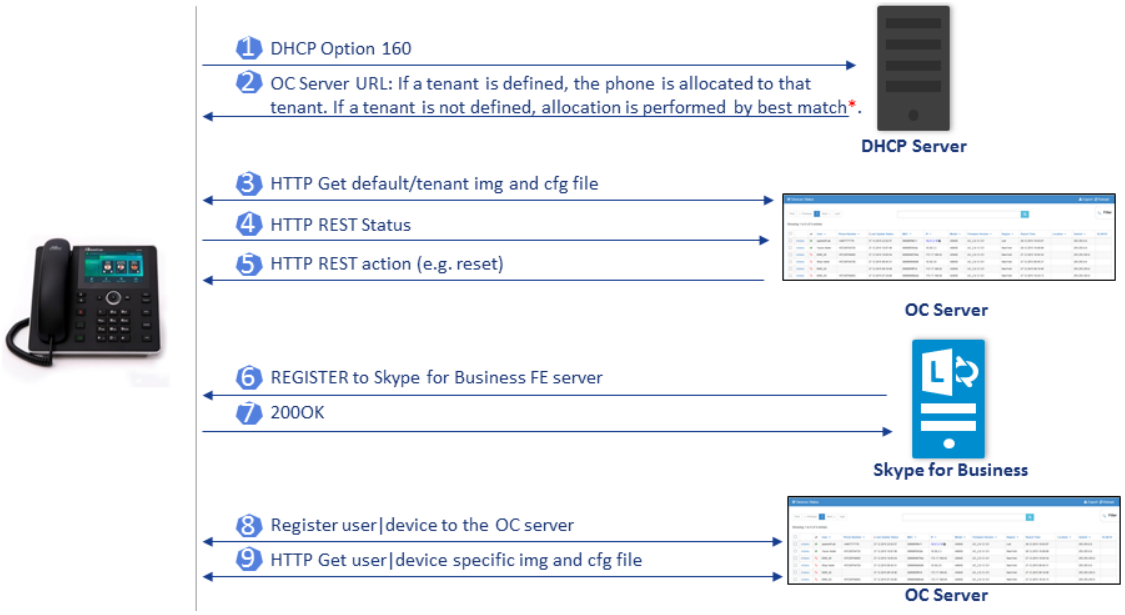
➢ **To implement Zero Touch provisioning:**

1. Build your network topology of tenants and sites using OVOC (see the *One Voice Operations Center User's Manual* for more information).
2. Start up and log in.
3. Choose the Zero Touch provisioning method. Either:
   - Configure the DHCP server to provision the phone with an IP address that is in the tenant/site range. Configure the phone to receive the IP address or subnet mask of the tenant/site.
   - Use DHCP Option 160.
4. Choose the default template for each tenant and device model.

Devices that reside behind a NAT and whose IP addresses are internal can be managed by OVOC via SBC HTTP proxy. For more information, see here.

Zero Touch Provisioning Process - Skype for Business Phone

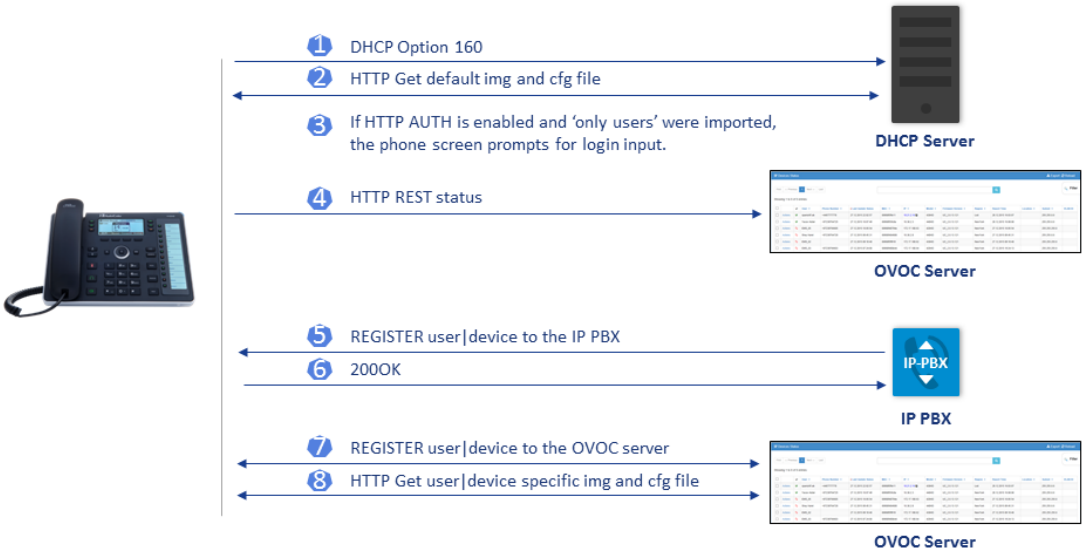
The figure below illustrates the 1-9 step provisioning process for AudioCodes' IP phones for Skype for Business when the Zero Touch feature is implemented.



*If the admin doesn't define a tenant in the URL in DHCP Option 160, the phone is allocated a tenant/site according to *best match*, that is, according to either tenant Subnet Mask or site Subnet Mask configured in OVOC. See the *OVOC User's Manual* for more information.

Zero Touch Provisioning – non Skype for Business Phone

The figure below illustrates the 1-8 step provisioning process for AudioCodes' non Skype for Business phones when the Zero Touch feature is implemented.



Using the Zero Touch Setup Wizard to Provision Devices

When plugged in to the enterprise network, phones can automatically be provisioned through the Zero Touch feature.

- Zero Touch determines which *template* the phone will be allocated.

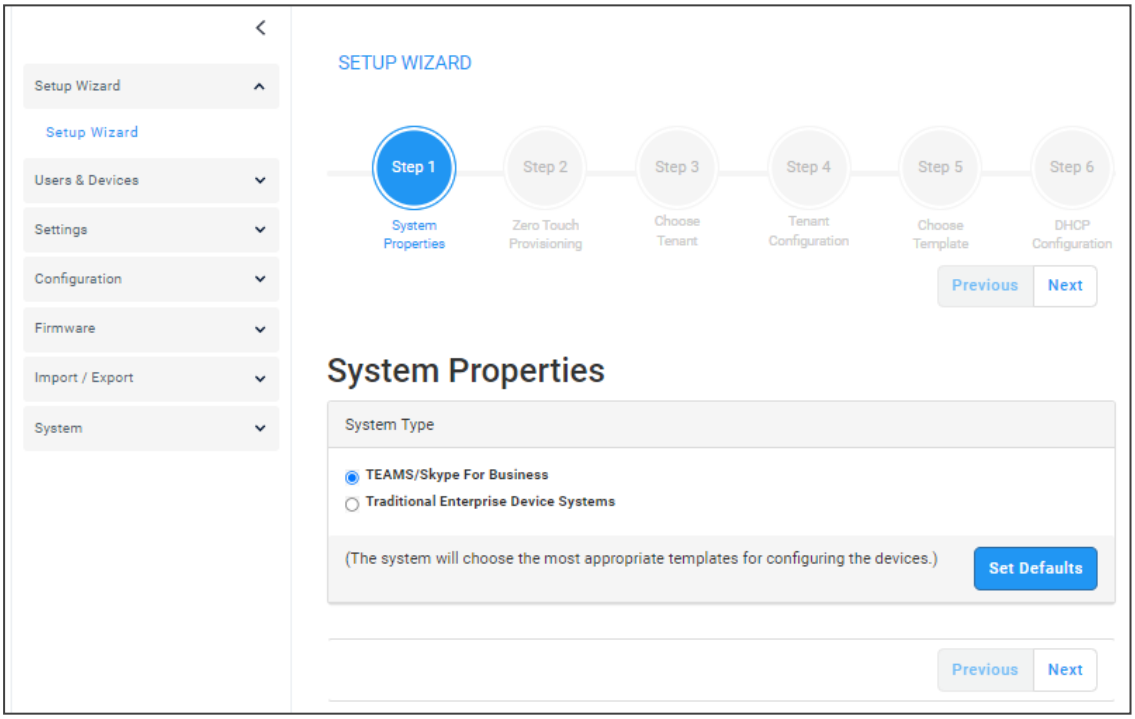
- The template is allocated *per phone model* and *per phone tenant*.
- The template determines which *firmware file* and *configuration file* the phone will be allocated.

Zero Touch provisioning *accelerates uptime* by enabling multiple users and phones to automatically be provisioned and added to the Manager.

You can use the Setup Wizard feature to *set up* Zero Touch provisioning. The Wizard simplifies deployment of phones in the enterprise for admins. The Wizard's functions were already implemented in versions of Device Manager Pro earlier than Version 7.4, only now they're centralized in a single location for a friendlier deployment experience. Here are the steps to follow to provision phones using the Wizard.

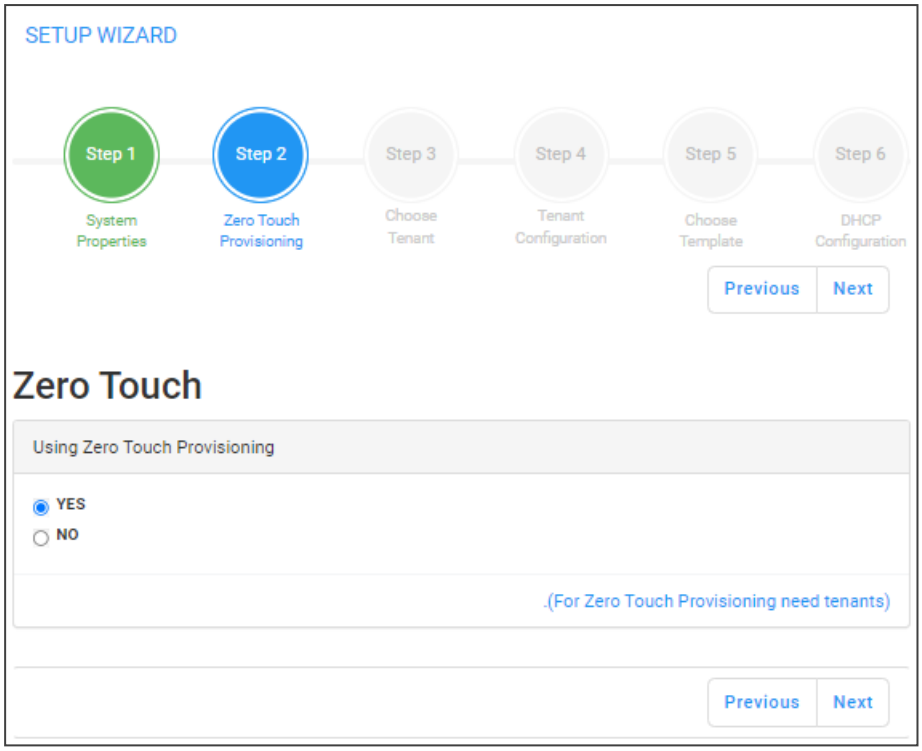
➢ To provision phones using the Zero Touch Setup Wizard:

1. In the main screen, click the 'Setup' menu and then click the **Setup Wizard** option.

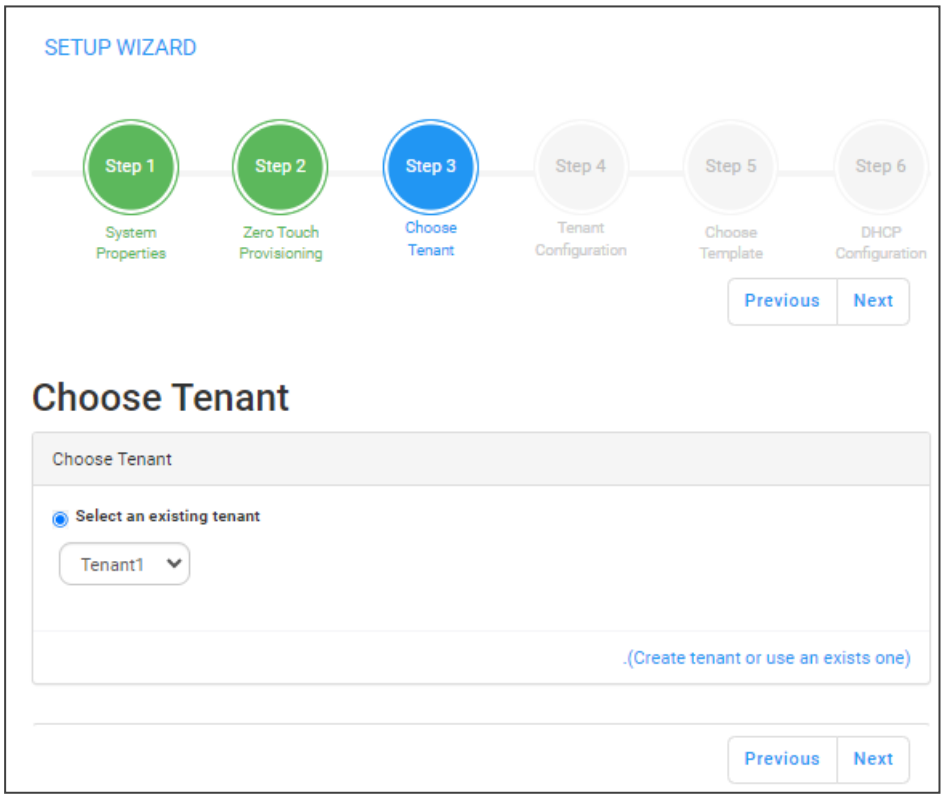


2. Select **Skype for Business** if it isn't selected already, and then click **Next**.

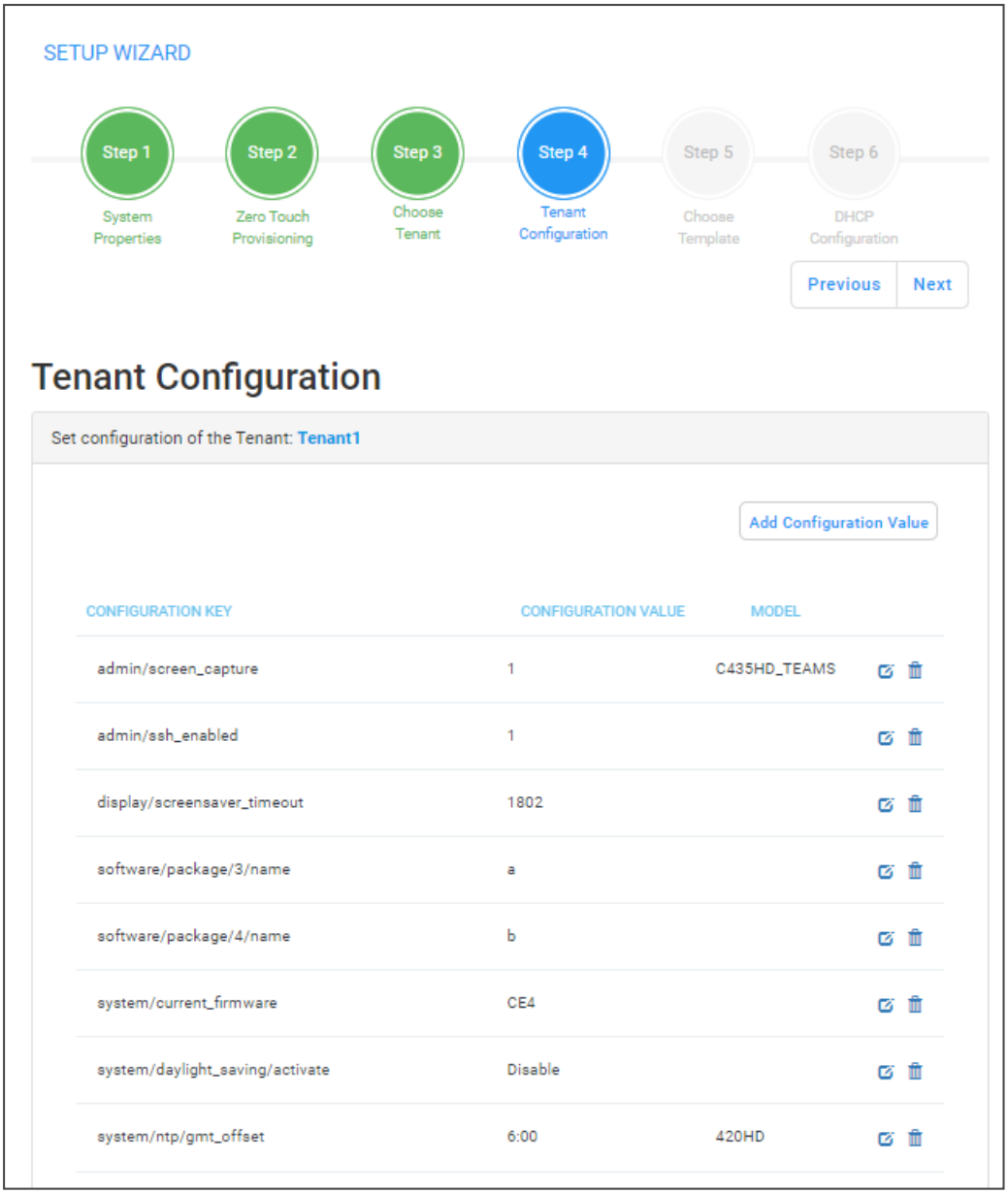
The Setup Wizard will be closed if you intend to use other PBXs besides Skype for Business. The Setup Wizard is intended exclusively for Skype for Business.



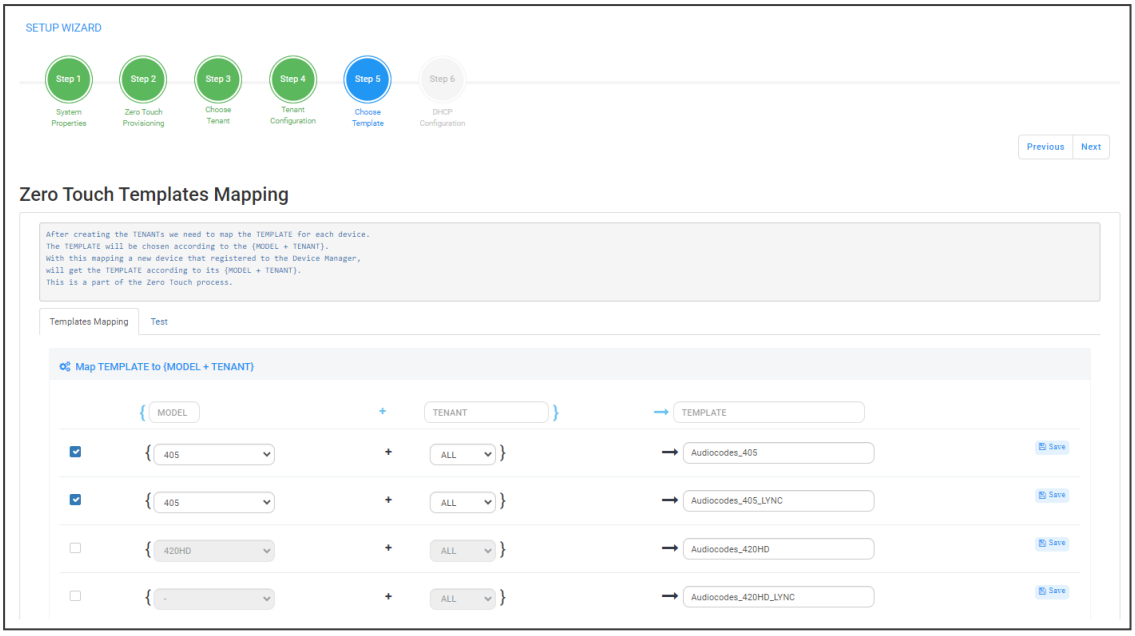
3. Select **Yes** and then click **Next**.



4. Choose an existing tenant from the dropdown and click **Next**. If a tenant doesn't already exist, click **Next** and configure one. This is to be able to create a specific configuration for the tenant and configure the URL in DHCP Option 160 so devices will use this tenant. If there's no specific tenant configuration to configure, click **Next**.



5. Click **Next** (not shown in the previous figure).

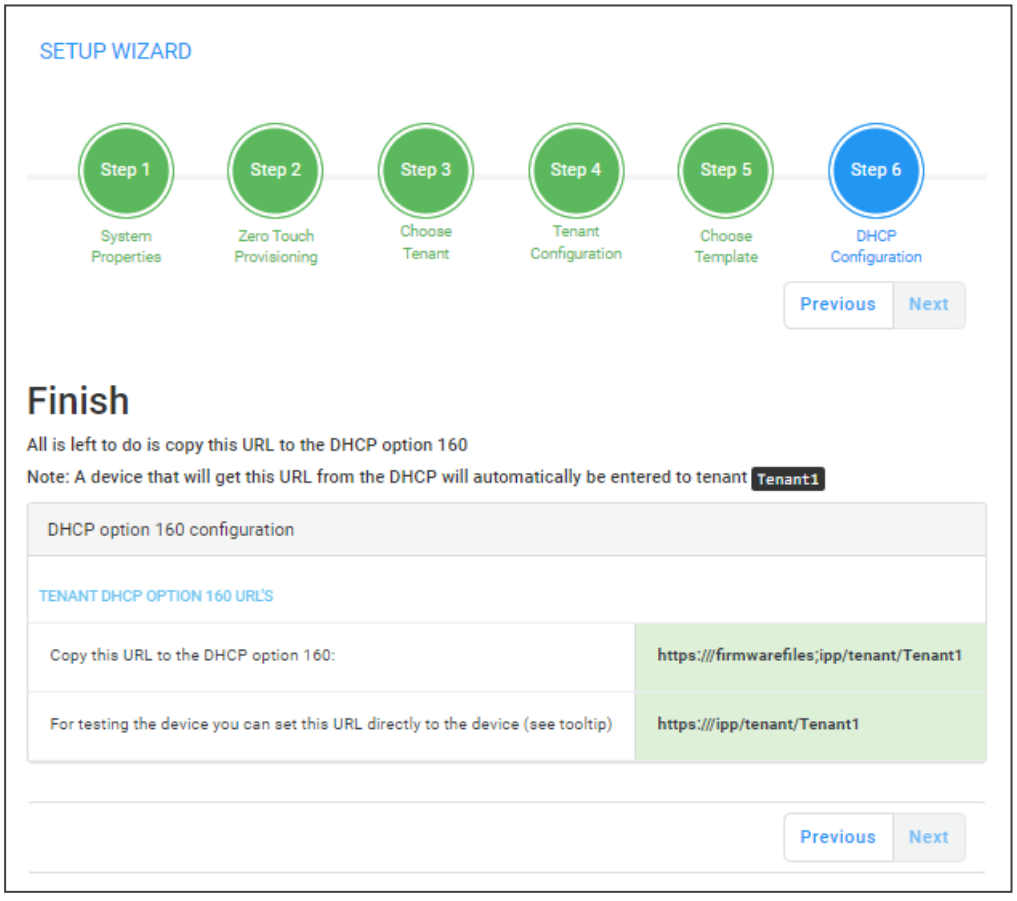


6. Associate a template according to the MODEL and TENANT. The page displays a mapping table in which you need to map {MODEL + TENANT} to TEMPLATE.

   a. Select 'IsDefault'; from this point on, the template chosen will be used.

   b. From the 'Phone' dropdown, select the model.

   c. From the 'Tenant' dropdown, select the tenant and then click **Next**.



7. Define the URL in DHCP Option 160.

Signing in to a Phone into which Another User is Signed

Applies only if the Zero Touch provisioning method was used.

If user B signs in to a phone that user A is signed in to, user A's phone is deleted from the Manage Users page and the newly signed-in phone is added to User A.

The Devices Status page is updated with the newly signed-in phone.

Provisioning Devices without the Zero Touch Setup Wizard

You can set up zero touch provisioning in the Manager without using the Setup Wizard. When plugged in to the enterprise network, phones will then automatically be provisioned.

- Zero Touch determines with which *template* the phone will be provisioned.
- The template is provisioned *per phone model* and *per phone tenant*.
- The template determines with which *firmware file* (img) and *configuration file* (cfg) the phone will be provisioned.

Zero Touch accelerates uptime by enabling multiple users and phones to automatically be provisioned and added to the Manager.

Before Implementing Zero Touch

Before implementing Zero Touch, you need to prepare the network.

This applies to:

- the admin whose OVOC is installed on-prem (in the enterprise's LAN)
- the system integrator of the Service Provider whose OVOC is installed in the cloud (WAN)

➢ **To prepare the network for Zero Touch provisioning:**

1. Prepare a template per tenant (see here).
2. Upload the firmware .img file to the server (see here).
3. Configure the DHCP server's Option 160 to allocate the phone to the tenant/site URL (see here).

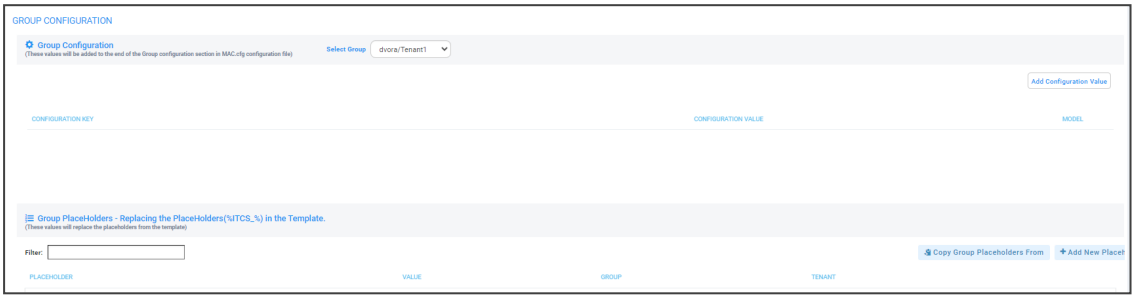
Configuring an Endpoints Group

After adding a group to OVOC as shown in the *OVOC User's Manual*, you can add an endpoint - or multiple endpoints - to that group as shown here under the action **Change Group**, and then you can configure the endpoints in the group as shown below. The feature benefits a customer

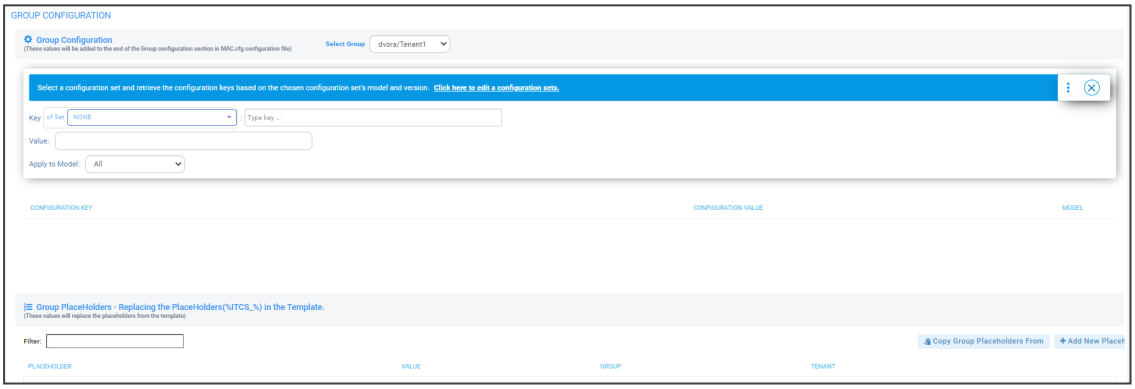
who wants for example 10 of 500 phones in a site in their enterprise organized in a group for a software upgrade to apply exclusively to the 10 phones in that group. In contrast to sites, groups are *logical* entities but configuration of both are identical; both are per tenant.

➢ To configure an endpoints group:

1. Open the Group Configuration page (**Setup** > **Configuration** > **Group Configuration**).

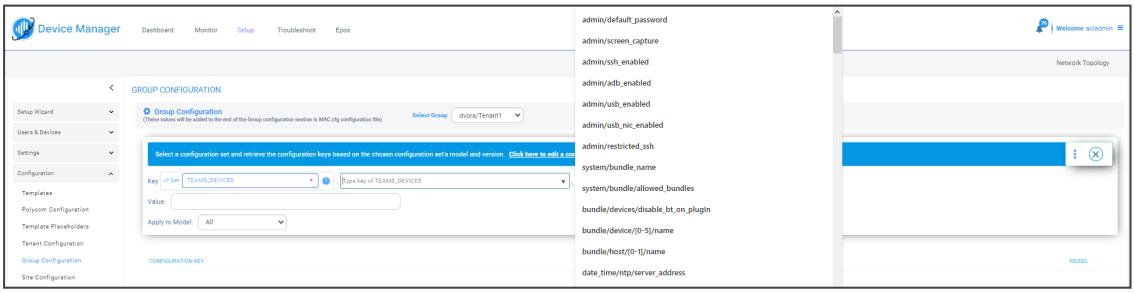


2. Click the **Add Configuration Value** button.

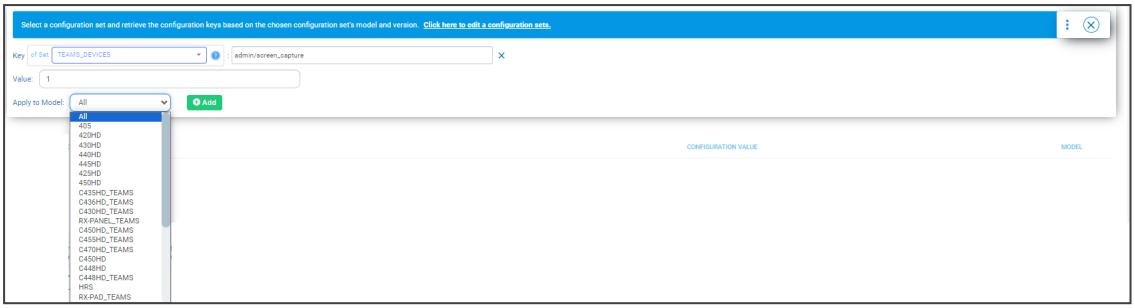


3. From the 'Select Group' drop-down, choose the group (added to OVOC) under which you want to organize endpoints.

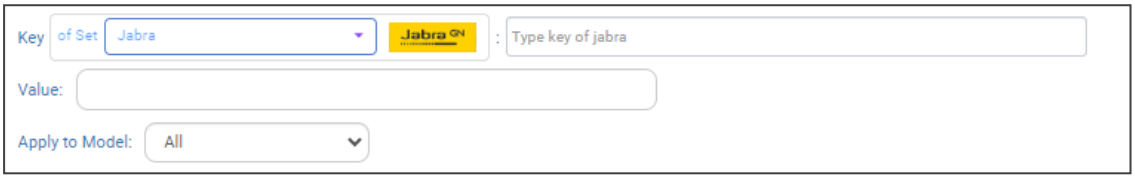
4. From the 'Type Key' drop-down, select a parameter to configure for the endpoints group.



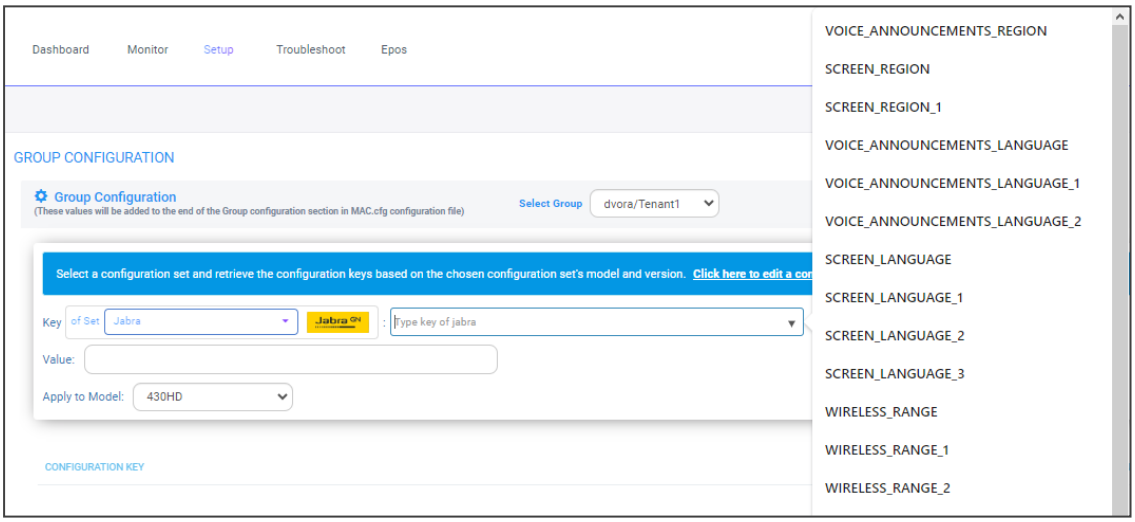
5. Provision the parameter with a value and then click **Add**.



6. (Optionally) Configure Jabra endpoints group parameters the same way only select **Jabra**.



7. From the 'Type key of Jabra' drop-down, select a Jabra parameter to configure for the Jabra endpoints group.



8. Provision the parameter with a value and then click **Add**.

Preparing a Template for a Tenant/Model

You need to prepare a template per tenant / type (phone model) in the deployment. The template informs the server how to generate the .cfg configuration file when the phones are plugged in to the network. When the phones are plugged in, the .cfg configuration file is downloaded to them from the server.

User-configured Speed Dials and Programmable Keys are saved in the device's cfg file and backed up on the server. After the user configures them (see the device's *User's Manual* for details), the phone automatically updates the cfg file on the server. They're downloaded to the phone after:

- they're deleted or some other 'crisis' occurs
- the phone is restored to factory defaults
- the user starts working with a new device
- the user deploys another device at their workstation
- the user's phone is upgraded

This saves the user from having to configure Speed Dials and Programmable Keys from the beginning. The user only needs to configure them once, initially.

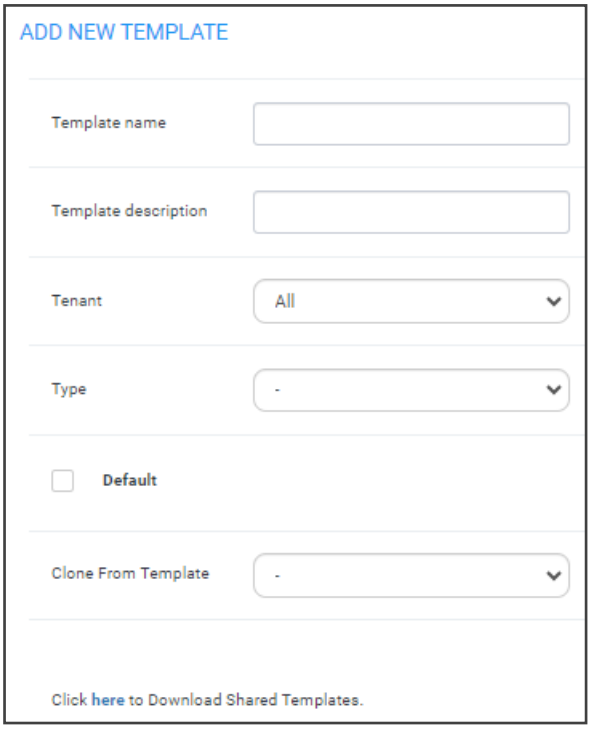
If there is no cfg file on the server, the server gets the data from the phone.

➢ To prepare a template for a tenant / phone model:

1. Open the 'Add new template' screen (**Setup** > **Configuration** > **Templates**).

For information on third-party vendor products, see the *Device Manager for Third-Party Vendor Products Administrator's Manual*.

2. Click the **Add New Template** button.



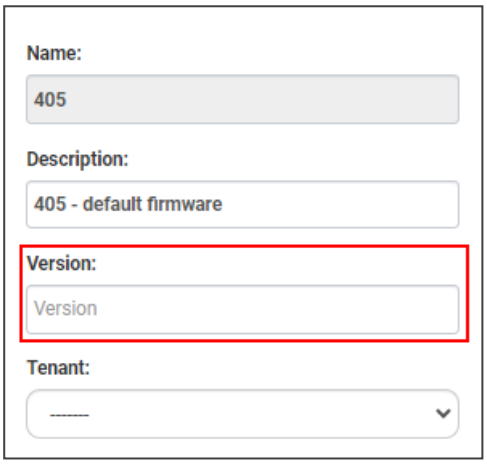
3. Enter a name for the template. Make the name intuitive. Include tenant *and* model aspects in it.
4. Provide a description of the template to enhance intuitive maintenance.
5. From the 'Tenant' dropdown list, select the tenant.
6. From the 'Type' dropdown list, select the phone model.
7. Select the **Default Tenant** option for the template to be the default for this tenant. More than one phone type can be in a tenant. All can have a common template. But only one template can be configured for a tenant. If a second template is configured for the tenant, it overrides the first. After a template is added, it's displayed as shown above in the Devices Configuration Template page (**Setup** > **Configuration** > **Templates**). When a phone is then connected to the network, if the phone is of this type and located in this tenant, it will automatically be provisioned via the DHCP server from the OVOC provisioning server (Zero Touch).
8. From the 'Clone From Template' dropdown list, select a template to clone from. If the template is for phones in a tenant that are Microsoft Skype for Business phones, choose a Skype for Business template.
9. Do this for all tenants and types (phone models) in the network.
10. If necessary, click the **here** link in 'Click **here** to Download Shared Templates'; your browser opens displaying AudioCodes' share file in which all templates are located, for example, the templates used with Genesys.

Receiving a File from AudioCodes and Uploading it to the OVOC Provisioning Server

After obtaining a device file from AudioCodes (for example, the device's .img firmware file, .cfg configuration file, certificate file, etc.), admin can upload it to the OVOC provisioning server. The Device Firmware Files page then displays the file.

The device's *default firmware file* is indicated in the page as follows:

When clicking the **Edit** button next to the device's default firmware file, observe that the 'Version' field cannot be edited, another indication of a default file.

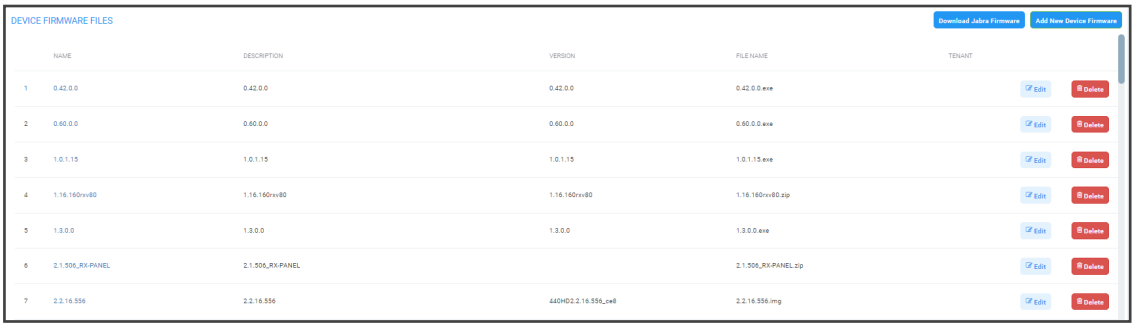


When 405 phones (in this example) are connected to the network, they will *all automatically be provisioned* with the default firmware file from the OVOC provisioning server.

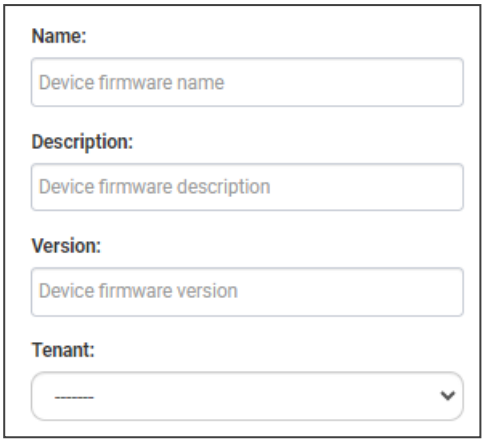
When admin uploads a new file to the OVOC provisioning server as shown in the procedure below, a new line is added (not the -default firmware line) to the Device Firmware Files page and only that device associated with the new file will be updated. ONLY WHEN PERFORMING AN UPGRADE FIRMWARE FILE ACTION FOR A DEVICE, ADMIN CAN SELECT A FIRMWARE FILE TO UPGRADE WHICH IS NOT NECESSARILY THE DEFAULT FILE.

➢ To upload a new file to the OVOC provisioning server after receiving it from AudioCodes:

1. Open the Device Firmware Files page (**Setup** > **Firmware** > **Firmware Files**).



2. Click the **Add New Device Firmware** button.



3. In the 'Name' field, enter the name of the file you received from AudioCodes.
4. In the 'Description' field, enter a description of the file to facilitate file management.
5. In the 'Version' field, enter the version of the file.
6. From the 'Tenant' drop-down, select the Tenant under whom the device is deployed.
7. Click the **Continue & Upload** button (not shown in the preceding figure).

8. Click the **Upload Firmware File** button.

9. Browse to the file and click **Submit**; the file is uploaded to the OVOC provisioning server and a new line is added to the Device Firmware Files page reflecting the new file.

   [Another option of obtaining | uploading newly released firmware files is in the Latest Versions page (**Setup** > **Firmware** > **Latest Firmware Versions**) as shown here]

Configuring DHCP Option 160 with a Tenant URL

You need to point DHCP Option 160 to a tenant URL so that the phones will be automatically provisioned with their .img firmware file and cfg configuration file when they're plugged in to the network for the first time (Zero Touch provisioning).

Either of the following two methods can be used to implement Zero Touch:

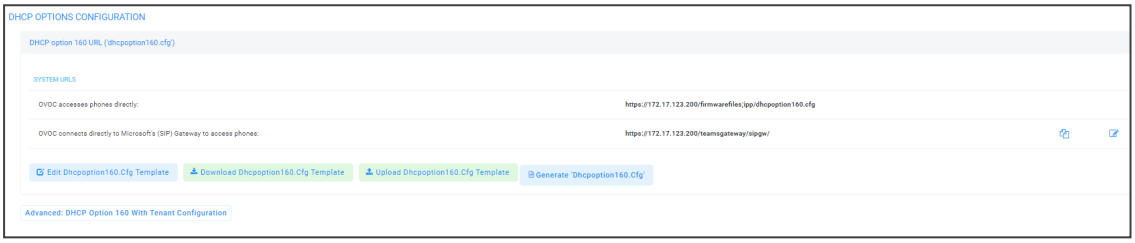
- Configure the DHCP server to provision the phone with an IP address that is in the tenant/site range. Configure the phone to receive the IP address or subnet mask of the tenant/site.
- Use DHCP Option 160

Device Manager supports backward compatibility so you can point DHCP Option 160 to a region URL. See the *Administrator's Manual* v7.2 and earlier.

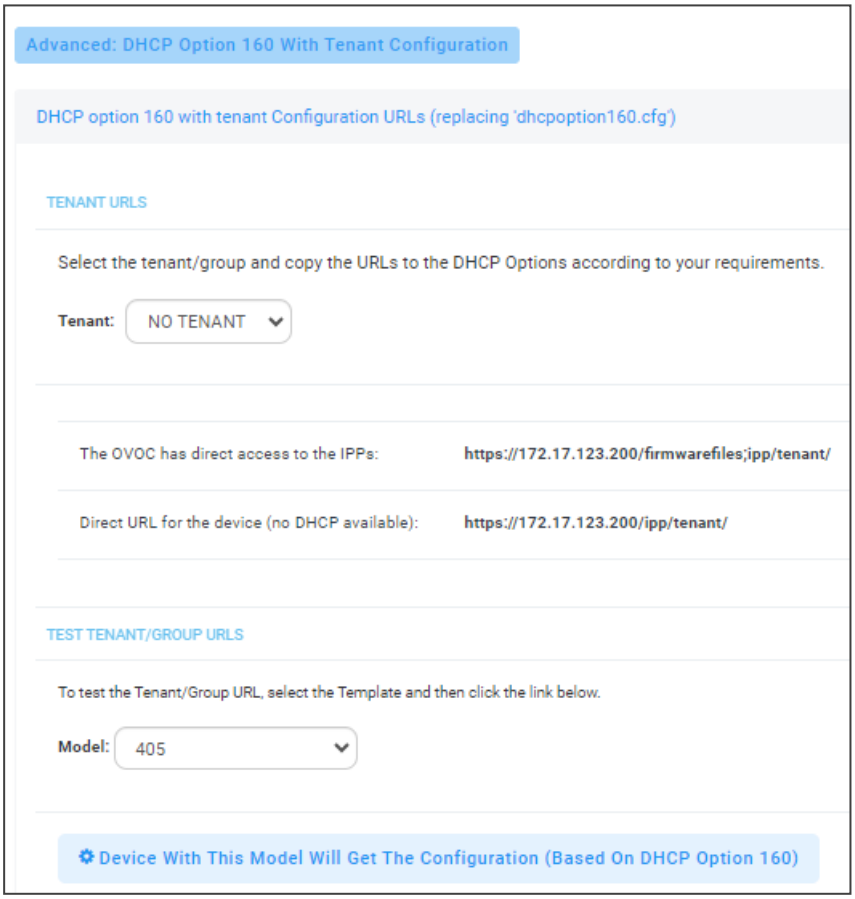
Later, when the (Skype for Business) phones are signed in, phones and users are automatically added to Device Manager which loads their specific .cfg files to them.

➢ To point DHCP Option 160 to a tenant URL:

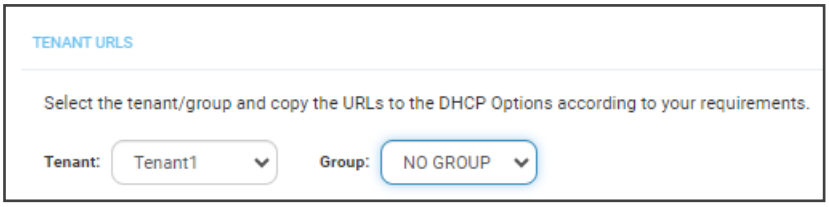
1. Open the DHCP Options Configuration page (**Setup** > **Settings** > **DHCP Options Configuration**).



2. Click the **Advanced: DHCP option 160 with Tenant Configuration** link located lowermost in the page.



3. Under the Tenant URLs section, select from the 'Tenant' dropdown a tenant with which to associate a new device.
4. From the 'Group' dropdown list, select a group with which to associate a new device.



You can configure the device's tenant URLs to retrieve files either directly from the OVOC server or via an SBC HTTP proxy. Using an SBC HTTP proxy server is useful for customers whose OVOC is installed in the cloud, or when phones are located behind a NAT.

5. Choose either:

   - **The OVOC has direct access to the phones**. The DHCP server will connect the phones directly to the OVOC server IP address.
     - Copy (Ctrl+C) the following URL and paste it into DHCP Option 160 in the enterprise's DHCP server: **HTTP://<OVOC_IP_Address>/firmwarefiles;ipp/tenant/<tenant selected in Step 1>/group/<group selected in step 1>**
   - **The OVOC access the IPP's through the SBC HTTP proxy**. The DHCP server directs the phones firstly to an SBC HTTP proxy server, which then redirects to the OVOC server.
     - If the phones communicate with an SBC HTTP proxy rather than directly with the OVOC server, copy (Ctrl+C) the following URL into DHCP Option 160 in the enterprise's DHCP server: **http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/tenant/Tenant**
   - **Direct URL for the IPP (No DHCP Available)** – typically used for debugging purposes when no DHCP is available.

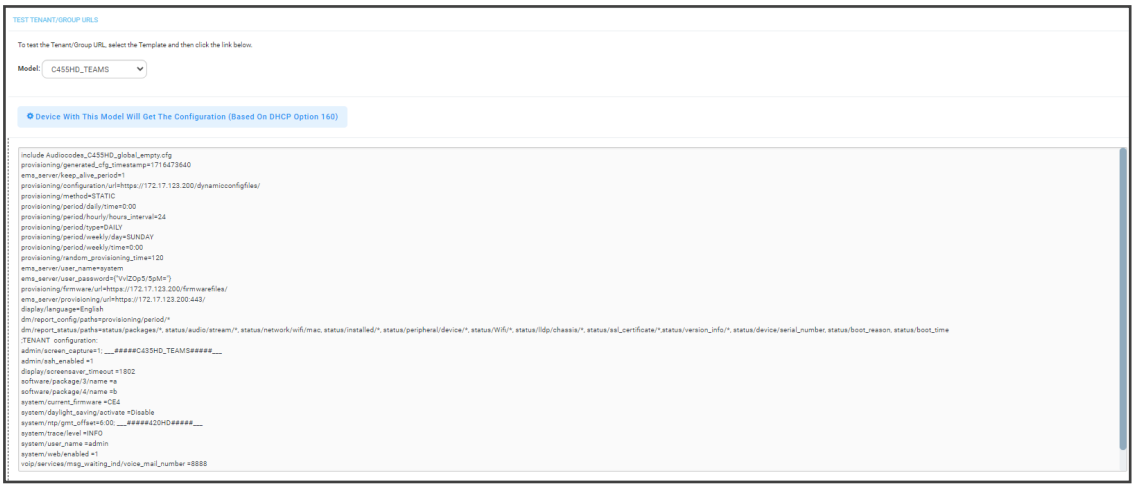
- Configure DHCP Option 160 to point to the OVOC provisioning server's URL if the phones are not behind a NAT. DHCP Option 66/67 can also be used.
- If the phones reside behind a NAT and an SBC HTTP proxy is available, configure DHCP Option 160 to point to the SBC HTTP proxy; phone-OVOC communications will then be via the SBC HTTP proxy rather than direct.

6. After copying the tenant URL (Ctrl+C) and pasting it into the enterprise's DHCP server's DHCP Option 160, select the phone model from the 'IPP Model' dropdown and then click the button **IPP with this model will get from the DHCP**; an output of the configuration file that you have configured to provision is displayed. Verify it before committing to provision multiple phones.

When a deployment covers multiple tenants, the tenants definition can be in two main hierarchies:

- DHCP server
- Subnet

For Zero Touch provisioning to function, tenant granularity must correspond with the number of DHCP servers/subnets already located within the enterprise network.



Comments in the configuration file's notation indicate a parameter's template source.

```
system/daylight_saving/start_date/day=26
system/daylight_saving/start_date/day_of_week=0
system/daylight_saving/start_date/hour=
system/daylight_saving/start_date/minute=
system/daylight_saving/start_date/month=3
;TENANT t122 configuration
system/daylight_saving/start_date/week=1
;NO GROUP group1 [t122] configuration
;SITE AutoDetection [AutoDetection] configuration:
system/hw_type = 3
system/user_name = admin
;NO USER jhon@audiocodes.com configuration
```

Template source can be:

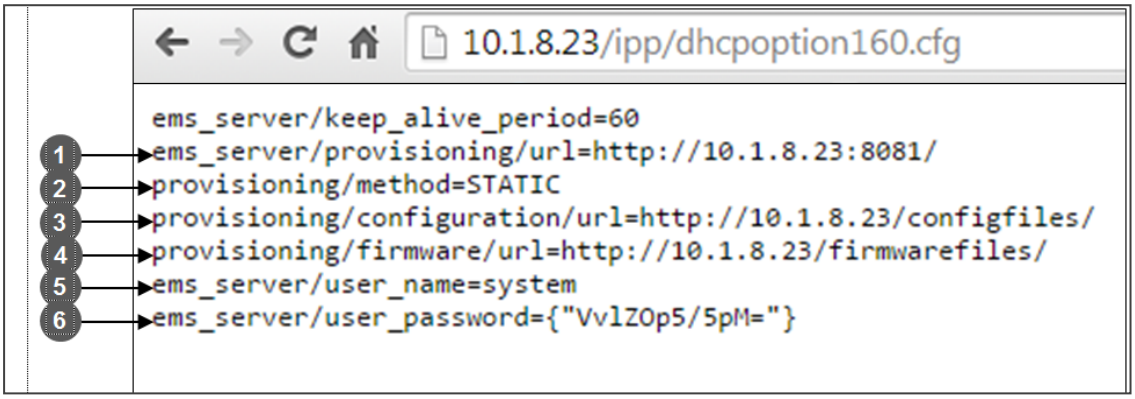
- Device Specific
- Tenant Level
- Group Level
- Site Level
- User Level

Zero Touch is supported for phones with sign-in capabilities only.

Configuring DHCP Option 160 with System URL

- This configuration is applicable when Zero Touch is not used to provision the phones.
- The instructions below therefore describe a provisioning method that is not the choice method.

The figure below shows the file **dhcpoption160.cfg** located on the server.



Legend	Description
1	Points to the URL of the OVOC provisioning server.
2	STATIC provisioning method, so the cfg and img files are automatically pulled from the OVOC provisioning server rather than from the DHCP server.
3	Location of the cfg file, pulled by the phones when they're plugged into the network, on the OVOC provisioning server.
4	Location of the img file, pulled by the phones when they're plugged into the network, on the OVOC provisioning server.
5	Name of the 'system user', necessary for basic REST API authentication when the phones are plugged in to the network for the first time.
6	(Encrypted) Password of the 'system user', necessary for basic REST API authentication when the phones are plugged in to the network for the first time.

- The **dhcpoption160.cfg** file is created when logging in for the first time to Device Manager
- The file is an internal OVOC file and cannot be manually modified.

After installation, the first, second and third lines in the file are automatically updated.

Synchronizing Device Manager with OVOC Provisioning Server, Uploading File to Device Manager

The 'Latest Versions' page in Device Manager enables admin to obtain the latest device firmware files from AudioCodes' firmware repository located in the cloud, before upgrading the devices in the 'Devices Status' page. [Note that this can also be performed in the Show Info page as shown here]. The 'Latest Versions' page enables admin to 'sync' Device Manager with the repository in the cloud before performing the device upgrade.

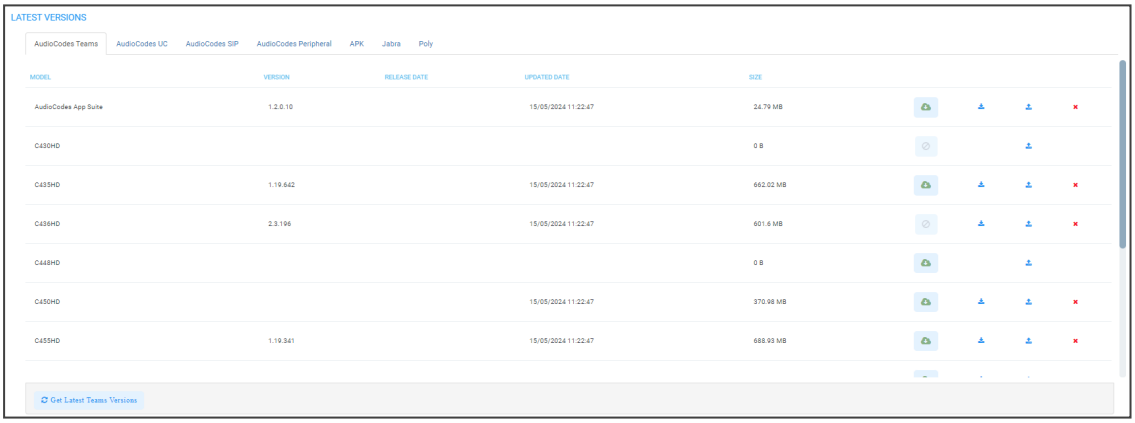
➢ **To sync Device Manager with cloud (if the page displays a newer|different version icon):**

1. Open the 'Latest Firmware Versions' page:
   - See how many (if any) devices in the network require a firmware upgrade by locating icon 

in the Dashboard page. If there are, click the icon. The icon shown here indicates there are 26. The Latest Versions page shown below opens.

     -OR-

   - Navigate to the page (**Setup** > **Firmware** > **Latest Firmware Versions**).



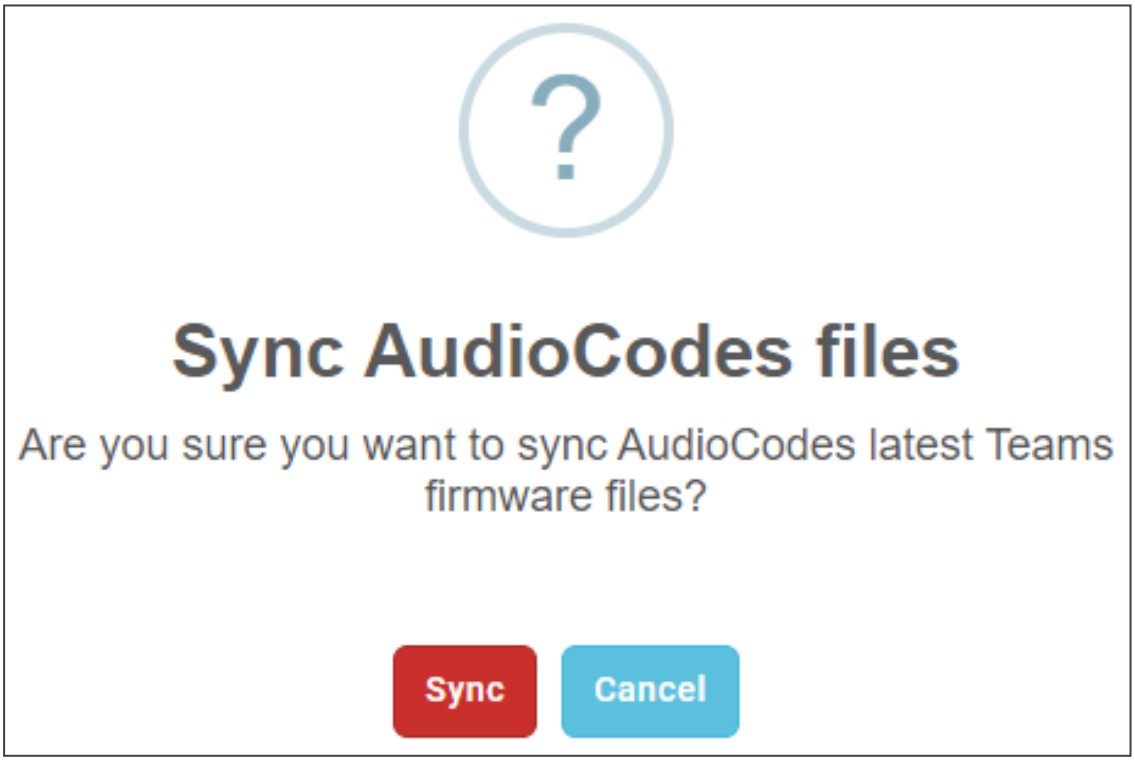
2. Click a tab to filter the page by product. By default, the page under the leftmost tab opens first. The tabs are from L-R:
   - **AudioCodes Teams** displays Teams devices such as the Teams IP phones and Microsoft Teams Rooms.
   - **AudioCodes UC** displays for example the IP phones for Skype for Business and the HRS devices for Skype for Business.
   - **AudioCodes SIP** displays generic SIP devices such as the generic SIP IP phones and generic SIP HRS devices.
   - **AudioCodes Peripheral** displays peripheral devices such as the RX15 Speakerphone, RXVCam10 Personal Webcam and RXVCam50 Video Camera.
   - **APK** displays Android Package Kits such as the Microsoft Teams APK for all Native Teams Deskphones and the Microsoft Teams Room APK for Android. APK is the file format for applications used on the Android operating system.
   - **Jabra** displays Jabra devices.

- **Polycom** displays supported Polycom devices.

3. Click the button located lowermost left in the page under each tab.
   - **Get latest Teams firmware (Sync)**. Updates the firmware versions on all Teams devices whose versions are old.
   - **Get latest Skype for Business firmware (Sync)**. Updates the firmware versions on all Skype for Business devices whose versions are old.
   - **Get latest Generic SIP firmware (Sync)**. Updates the firmware versions on all generic SIP devices whose versions are old.
   - **Get latest Peripherals version**. Updates the versions of peripheral devices software files.
   - **Get latest APK version**. Updates the versions of APK software files.
   - **Get latest Jabra firmware**. Updates the versions of all Jabra devices firmware files.
   - **Get latest Polycom firmware**. Updates the versions of all Polycom devices firmware.

Few deployments, if any, feature Skype for Business phones *and* generic SIP phones, so when performing a sync, do it for either one or the other, never for both.

4. In the prompt shown in the figure below that is then displayed, click **Sync**; the firmware on *all* Teams devices synchronized.



5. In the page under each tab, view the following icons *adjacent* to each device. The actions here are *per that device*.

Click to sync Device Manager with latest firmware version on the cloud; it will reach the device only after clicking **Generate Configuration**.

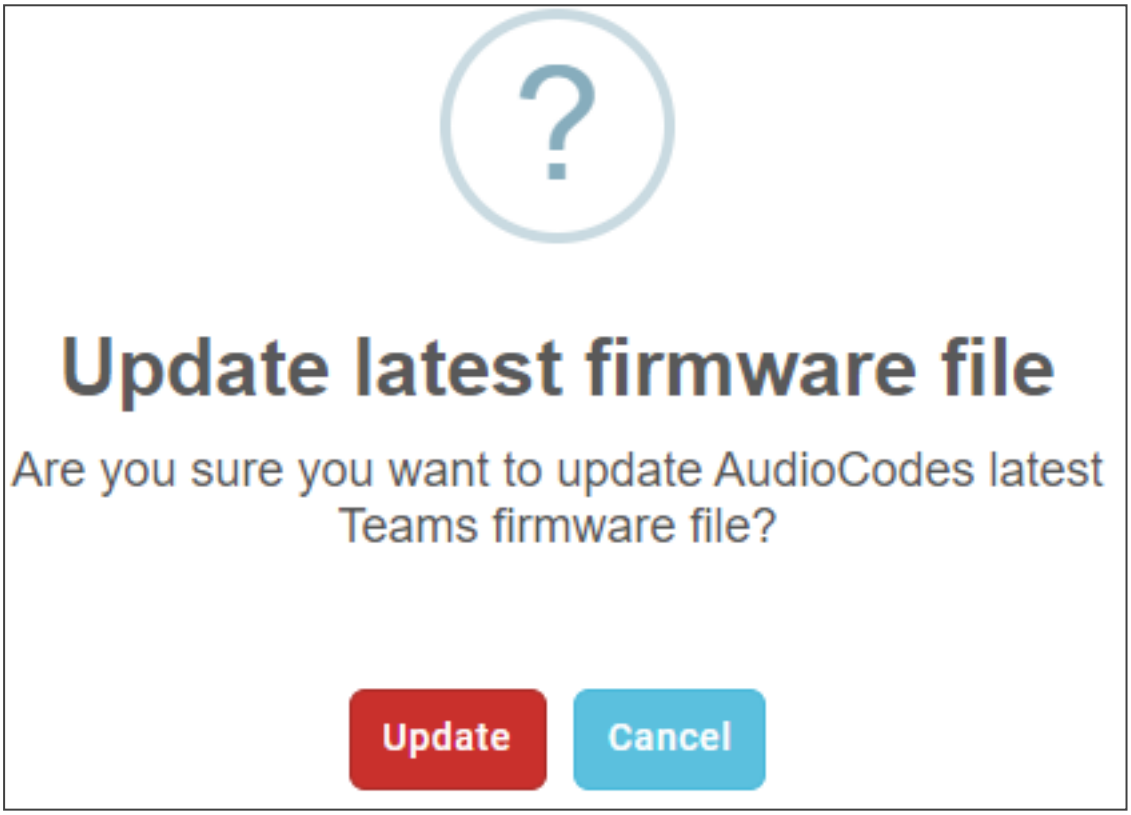
Click to download a newer firmware version from the cloud to Device Manager.

The device is disconnected.

Click to upload firmware from the pc / laptop to Device Manager.

Click to download the device's current firmware to the pc / laptop.

6. In the prompt shown below displayed after clicking , click **Update**; the firmware of the specific Teams device is updated.



7. Open the 'Devices Status' page (**Monitor** > **Dashboard** > **Devices Status**) and from the 'Actions' button adjacent to a phone, select **Update Firmware**; the phone will use the firmware file listed in the 'Latest Versions' page.

See also Checking Devices Status on page 81.

Editing the SBC HTTP Proxy

Admin can opt to edit the initial DHCP Option 160 cfg file. Choose the **HTTP Proxy Configuration** button if your phones are communicating with an SBC HTTP proxy, which is required when the phones are behind a NAT.

➢ **To configure the SBC HTTP proxy:**

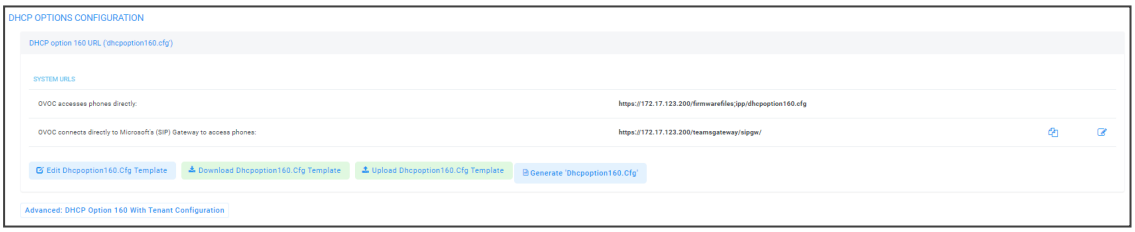
1. Open the System Settings page (**Setup** > **Settings** > **System Settings**), click the **More** tab and then the **SBC Proxy Configuration** button.

2. Click the **Edit template** button; the Edit DHCP Option screen shown previously opens. Edit as described previously here.
3. Click **Save**.

Provisioning Android-based Teams Devices

Device Manager manages Android-based Teams devices in a similar way to UC-type phones. Teams devices' configuration parameters are in the same format as UC phones. A .cfg configuration file is defined for each device. Device Manager version 7.8.2000 and later supports Android-based Teams devices.

Zero Touch Provisioning is supported in a non-tenant aware manner; each local DHCP Option 160 must be configured with a fully-specified URL pointing to **dhcpoption160.cfg** as shown here:



This URL is displayed in the Device Manager page under **Setup** > **Settings** > **DHCP Options Configuration**. After devices are added to Device Manager, they're allocated to tenants by selecting **Change Tenant** in the 'Actions' menu. Unless already used, it's recommended to leave the default tenant as a 'lobby' for the new devices. The above URL can also be configured in AudioCodes' Redirect Server. Android-based Teams devices currently support:

- Provisioning of configuration
- Provisioning of firmware
- Switching to UC / Teams
- Monitoring (based on periodic Keep-Alive messages sent from devices)
- Resetting the device

The Device Manager's 'internal' functions (which don't involve devices) are:

- Change tenant
- Change template
- Show info

- Generate Configuration
- Delete device status
- Nickname

The **Check Status** option is irrelevant for Android-based Teams devices therefore it's omitted from the 'Actions' menu.

- Changing a device's configuration using Device Manager is the same for Android-based Teams devices as for UC devices.
- To commit a change made at the template/tenant/site/group/user level, perform **Generate Configuration**. The change can be validated in the device's .cfg file. The Android-based endpoint pulls the updated configuration when the next periodic provisioning cycle occurs.

Configuring a Periodic Provisioning Cycle

Admins can configure how often periodic provisioning cycles will occur, to suit enterprise management preference.

➢ **To configure how often periodic provisioning cycles will occur:**

- Use the following table as reference.

Parameter	Description
provisioning/period/type	Defines the frequency of the periodic provisioning cycle. Valid values are: ■ HOURLY ■ DAILY (default) ■ WEEKLY ■ POWERUP ■ EVERY5MIN ■ EVERY15MIN Each value type is accompanied by additional parameters (see Supported Parameters on the next page) that further defines the selected frequency.

Configuring TimeZone and Daylight Savings

Admins can configure TimeZone and Daylight Savings to suit enterprise requirements.

➢ **To configure TimeZone and Daylight Savings:**

- Use the following table as reference.

Parameter	Description
date_time/-timezone	Defines the Timezone. Valid values are: ■ +00:00 ■ +01:00 ■ +02:00 ■ Etc.
date_time/time_dst	[Boolean parameter]. Configuring **ENABLED** adds one hour to the configured time. Valid values are: ■ 1 ■ 0

For example, to configure Central European Summer Time (CEST) you can either configure:

date_time/timezone=**+01:00**

date_time/time_dst=**1**

-OR-

date_time/timezone=**+02:00**

date_time/time_dst=**0**

Managing Devices with HTTPS

Android-based Teams devices support an HTTPS connection.

➢ **To establish an HTTPS connection:**

- The server certificate must be signed by a well-known Certificate Authority

  -OR-

- A root/intermediate CA certificate must be loaded to the device's trust store either via 802.1x or configuration parameter '/security/ca_certificate/[0-4]/uri'

➢ **To maintain backward compatibility with devices previously running UC versions:**

- Configure parameter '/security/SSLCertificateErrorsMode' to **Ignore**

Supported Parameters

Listed here are the configuration file parameters currently supported by Android-based Teams devices. They're in AudioCodes' UC version format. The parameters are comprised of Microsoft configuration profile settings and AudioCodes' device-specific parameters.

- general/silent_mode = 0 (default)/1

- general/power_saving = 0 (default)/1
- phone_lock/enabled = 0 (default)/1
- phone_lock/timeout = 900 (default) (in units of seconds)
- phone_lock/lock_pin = 123456
- display/language = English (default)
- display/screensaver_enabled = 0/1
- display/screensaver_timeout = 1800 (seconds)
- display/backlight = 80 (0-100)
- display/high_contrast = 0 (default) /1
- date_time/timezone = +02:00
- date_time/time_dst = 0 (default) /1
- date_time/time_format = 12 (default) / 24
- network/dhcp_enabled = 0/1
- network/ip_address =
- network/subnet_mask =
- network/default_gateway =
- network/primary_dns =
- network/pecondary_dns =
- network/pc_port = 0/1
- office_hours/start = 08:00
- office_hours/end = 17:00
- logging/enabled = 0/1
- logging/levels = VERBOSE, DEBUG, INFO, WARN, ERROR, ASSERT, SILENT
- admin/default_password = 1234
- admin/ssh_enabled=0/1 (default)
- security/SSLCertificateErrorsMode = IGNORE, NOTIFICATION, DISALLOW (default)
- security/ca_certificate/[0-4]/uri – uri to download costumer’s root-ca
- provisioning/period/daily/time
- provisioning/period/hourly/hours_interval
- provisioning/period/type = HOURLY, DAILY (default), WEEKLY, POWERUP, EVERY5MIN, EVERY15MIN
- provisioning/period/weekly/day

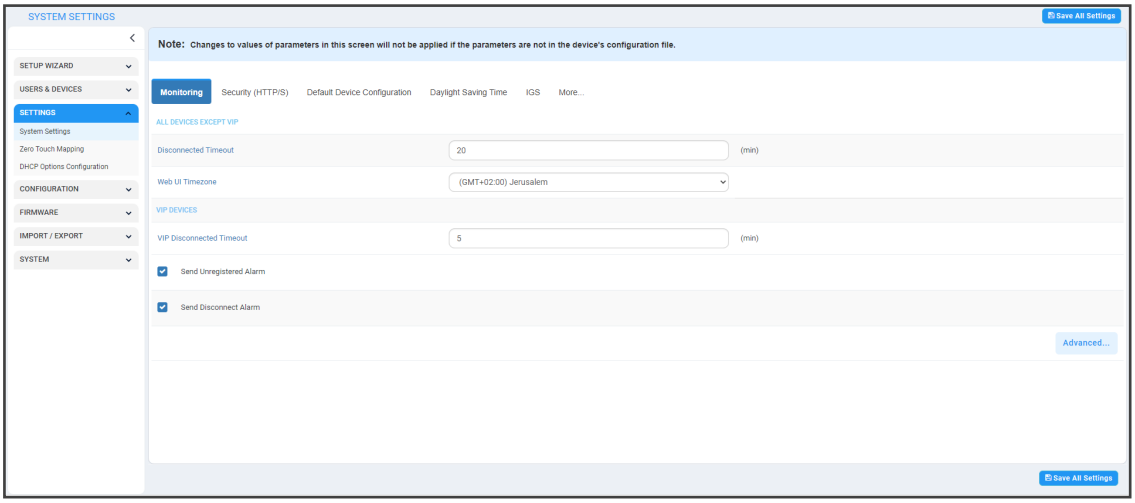
- provisioning/period/weekly/time
- provisioning/random_provisioning_time

4 Configuring System Settings

The System Settings page enables admins to configure devices according to enterprise requirements. Settings under some tabs also include placeholders so that when you generate a template, the settings values will be applied to the template. Default placeholder values can be viewed in the Default Placeholders Values page.

➢ To configure system settings:

1. Open the System Settings page (**Setup** > **Settings** > **System Settings**).



2. Use the table below as reference; tabs in the page are (L-R): **Monitoring**, **Security (HTTP/S)**, **Default Device Configuration**, **Daylight Saving Time**, **IGS** and **More**...

- The **IGS** tab applies only to enterprises whose environments are non Skype for Business. All other tabs in the screen apply to both Skype for Business and non Skype for Business environments.
- Teams devices function flawlessly behind a NAT in all scenarios; ignore the **IGS** tab if you're using Teams devices.
- Enable **IGS** if
  - ✓ you're using non-Teams devices; if using the 405HD phone, you may require a firmware upgrade
  - ✓ devices are located behind a NAT or Device Manager is unable to establish communication with them
- 420HD, 430HD and 440HD phones are incompatible when behind a NAT.

Tab | Parameter	Description
Monitoring	
Disconnected Timeout	Determines how long, in minutes, a device's status will be indicated as 'Disconnected' if not reported otherwise. Default: 20 minutes. The

Tab | Parameter	Description
	phone reports its status to the server every hour. If it does not report its status before 'Disconnect Timeout' lapses, i.e., if the parameter is left at its default and two hours pass without a status report, the status will change from **Registered** to **Disconnected** and the device's 'Status' column in the Devices Status screen will be red-coded.
Send KEEP-ALIVE Every	[Only displayed after clicking **Advanced**] Determines how often, in minutes, a KEEP-ALIVE message is sent from the device.
VIP Disconnected Timeout	Determines how long, in minutes, a VIP device's status will be indicated as 'Disconnected' if not reported otherwise. An alarm can be sent to admin if the timeout is exceeded. Default: 5 minutes. A VIP device is typically a Common Area Phone (CAP) located in the lobby of an enterprise, or a conference phone located in an enterprise's meeting rooms. It's important for a VIP device to be connected, hence the default timeout of 5 minutes compared to the default of 20 minutes for a non VIP device.
VIP Send KEEP-ALIVE Every	[Only displayed after clicking **Advanced**] Determines how often, in minutes, a KEEP-ALIVE message is sent from the VIP device.
Send Unregistered alarm	Select this option for an alarm to be sent when VIP device status changes to 'Unregistered'.
Send Disconnect Alarm	Select this option for an alarm to be sent when VIP device status changes to 'Disconnected'. It's important for a VIP device to be connected, hence the default Disconnected Timeout of 5 minutes compared to the default of 20 minutes for a non VIP device.
Security (HTTP/S)	
Secure (HTTPS) communication from Device Manager to the Devices	Sends secured (HTTPS) requests from the Device Manager server to the phone. If the option is selected, communications and REST actions such as Restart, Send Message, etc., will be carried out over HTTPS. Not relevant when using an SBC proxy (see Editing the SBC HTTP Proxy on page 24).
Secure (HTTPS) communication from the Devices to the Device Manager	Sends secured (HTTPS) requests from the phone to the Device Manager server. If the option is selected, communications and REST updates such as keep-alive, alarms and statuses between phone and server will be carried out over HTTPS. Also used for loading firmware and configuration files, and when there is an SBC proxy (see Editing

Tab | Parameter	Description
	the SBC HTTP Proxy on page 24).
Devices Status: Open Device Web Administrator using HTTPS	The browser immediately opens the device's Web interface, over HTTPS, without prompting that there is a problem with the website's security certificate and that it is not recommended to continue to the website.
Only allow devices added by the administrator into OVOC	Select this option to allow into OVOC only those phones that were added by admin. ■ Phones that were not added by admin will be blocked by OVOC. ■ If a device's Mac Address is not listed in the 'Manage Users & Devices' page, it will be blocked by OVOC. The OVOC must be restarted for the parameter to take effect.
Default Device Configuration	
Server FQDN	[Recommended] Points phones to the OVOC server using the server's name rather than its IP address. If phones are pointed to the OVOC server's IP address, then if the server is moved due to organizational changes within the enterprise, all phones are disconnected from it. Pointing using the server's name prevents this, making organizational changes easier.
Devices Language	From the dropdown select the language you want displayed in the phones' screens: **English** (default), **French**, **German**, **Hebrew**, **Italian**, **Polish**, **Portuguese**, **Russian**, **Spanish** or **Ukraine**.
NTP Server IP Address	Enter the IP address of the Network Time Protocol (NTP) server from which the phones can get the time.
Voice Mail Number	Enter the number of the enterprise's exchange. Configuration depends on the enterprise environment, specifically, on which exchange the enterprise has. If the enterprise has a Skype for Business environment, ignore this parameter. Default=1000.
Require SRTP in the Phone Configuration File	Select this option for *Secure* RTP. Real-time Transport Protocol (RTP) is the standard packet format for delivering voice over IP.
Daylight Saving Time	
Active	Determines whether the phone automatically detects the Daylight Saving Time for the selected Time Zone.

Tab | Parameter	Description
	■ Disable ■ Enable (default)
Date Format	Configures the date format. Valid values are: ■ FIXED. Date is specified as: Month, Day of month. ■ Day of Week. Date is specified as Month, Week of month, Day of week.
Start Time	Defines precisely when to start the daylight saving offset. ■ month - defines the specific month in the year ■ week – defines the specific week in the month (first – fourth) ■ day - defines the specific day in the week ■ hour - defines the specific hour in the day ■ minute - defines the specific minute after the hour Configures the precise moment the phone will start daylight savings with a specific offset.
End Time	Defines precisely when to end the daylight saving offset. ■ month - defines the specific month in the year ■ week – defines the specific week in the month (first – fourth) ■ day - defines the specific day in the week ■ hour - defines the specific hour in the day ■ minute - defines the specific minute after the hour Configures the precise moment the phone will end daylight savings with a specific offset.
Offset	The offset value for the daylight saving. Range: 0 to 180.
Generic SIP	
Redundant Mode	From the dropdown select **No Redundant** (default) or **Primary/Backup**. Enables admin to set the primary PBX / Skype for Business server to which the phone registers and the fallback option if the server is unavailable. Primary/Backup, or 'outbound proxy', is a feature that enables the phone to operate with a primary or backup PBX/Skype for Business server. If the primary falls, the other backs it up.

Tab | Parameter	Description
Primary	Enter the primary PBX/Skype for Business server's IP address, i.e., the outbound proxy's IP address.
HTTP AUTH Provisioning no password	If set to **Enabled**, only the extension number will be used for provisioning HTTP authentication. The default HTTP AUTH password will be **1234**. In DHCP option 160 and on the templates, the setting 'provisioning/configuration/http_auth/password' must be configured to **1234** to activate the feature.

3. Click the **More...** tab and if necessary, in the 'Accept Extensions' field, define file extensions you'll require which aren't already defined and then click **Save**.
   - For information about the **LDAP Configuration** button, see Configuring the LDAP Directory below
   - For information about the **SBC Proxy Configuration** button, see here.Editing the SBC HTTP Proxy on page 24
   - For information about the **Default Placeholders Values** button, see Viewing Default Placeholders Values on page 114
4. Click **Save All Settings**.

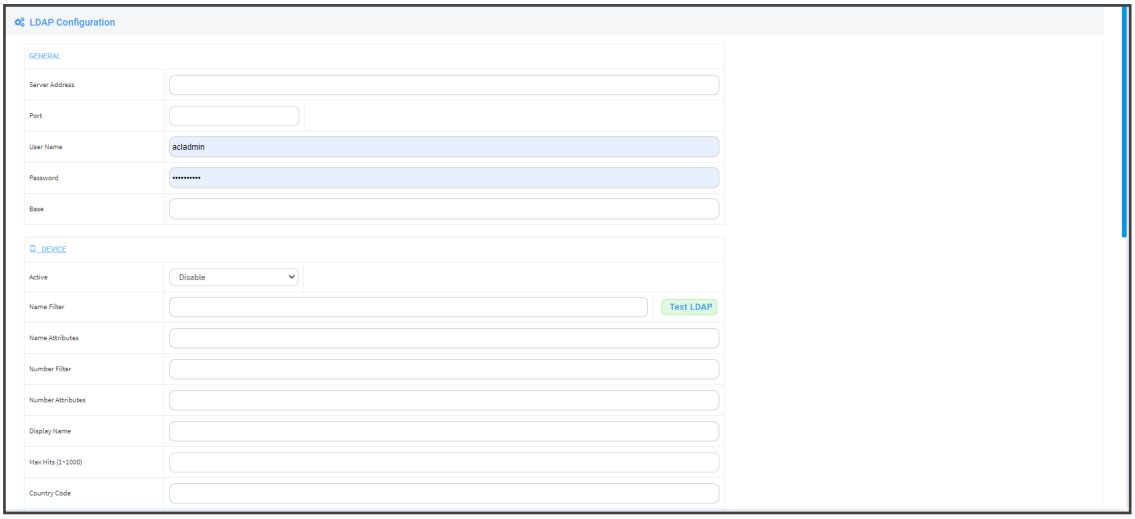
Configuring the LDAP Directory

This section is inapplicable if you're operating in a Microsoft Skype for Business environment because Skype for Business uses its own Active Directory server.

Device Manager enables admin to configure the enterprise's LDAP directory.

➢ **To access the LDAP directory:**

1. Open the System Settings page (**Setup** > **Settings** > **System Settings**).
2. Click **More...** and then click the **LDAP Configuration** button that is then displayed.



3. From the 'Active' parameter dropdown, select **Enable**.
4. Configure the parameters using the table below as reference.

Table 4-1: LDAP Configuration

Parameter	Description
Server address	Enter the IP address, or URL, of the LDAP server.
Port	Enter the LDAP service port.
User Name	Enter the user name used for the LDAP search request.
Password	Enter the password of the search requester.
Base	Enter the access point on the LDAP tree.
Active	From the dropdown, select **Disable** LDAP (default) or **Enable** LDAP. If **Enable** is selected, the parameters below are displayed.
Name Filter	Specify your search pattern for name look ups. For example, when you type in the *(&(telephoneNumber=*)(sn=%))* field, the search result includes all LDAP records which have the 'telephoneNumber' field set, and the '(“sn”-->surname)' field starting with the entered prefix. When you type in the *(|(cn=%)(sn=%))* field, the search result includes all LDAP records which have the '(“cn”-->CommonName)' OR the '(“sn”-->Surname)' field starting with the entered prefix. When you type in the *(!(cn=%))* field, the search result includes all LDAP records which “do not” have the 'cn' field starting with the entered prefix.
Name Attributes	Specifies the LDAP name attributes setting, which can be used to specify the “name” attributes of each record which is returned in the LDAP search

Parameter	Description
	results. When you type in the following field, for example, *cn sn displayName*", this requires you to specify 'cn-->commonName'. This is the Full name of the user, sn-->Surname, last name or family name and "displayName" fields for each LDAP record.
Number Filter	Specifies your search pattern for number look ups. When you type in the following field, for example, *(|(telephoneNumber=%)(Mobile=%)(ipPhone=%))*, the search result is all LDAP records which have the "telephoneNumber" OR "Mobile" OR "ipPhone"field match the number being searched. When you type in the *(&(telephoneNumber=%)(sn=*))* field, the search result is all LDAP records which have the 'sn' field set and the "telephoneNumber" match the number being searched.
Number Attributes	Specifies the LDAP number attributes setting, which can be used to specify the "number" attributes of each record which is returned in the LDAP search results. When you type in the following field, for example, *Mobile telephoneNumber ipPhone*, you must specify 'Mobile', 'telephoneNumber' and 'ipPhone' fields for each LDAP record.
Display Name	Specifies the format in which the "name, e.g. "Mike Black" of each returned search result is displayed on the IPPHONE. When you type in the following field, for example, %sn, %givenName, the displayed result returned should be "Black, Mike".
Max Hits (1~1000)	Specifies the maximum number of entries expected to be sent by the LDAP server (this parameter is sent to the LDAP server).
Country Code	Defines the country code prefix added for number search.
Area Code	Defines the area code prefix added for number search.
Sort Result	Sorts the search result by display name on the client side.
Search Timeout	The timeout value (in seconds) for LDAP search (sent to the LDAP server).
Call Lookup	Defines the user name used for the LDAP search request.

5. Click **Save**.

Adding Users & Devices in Generic SIP Environments

Admins can import

- users *and* devices -or-
- only users

If admin imports users *and* devices, the association between users and devices was made before Version 7.6

- using the device's MAC address
- through user name and password
- via an imported CSV file
- before deployment

➢ **To add users *and* devices with a version earlier than Version 7.6 of Device Manager:**

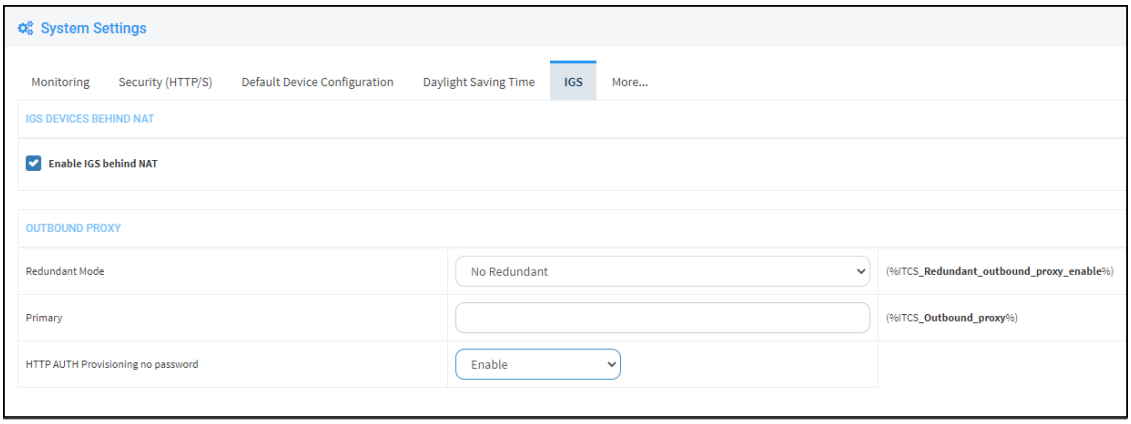
- After plugging the phones into the network, log in to Device Manager and then (best practice):
  - Export the automatically created 'System User' to a zip file (see here)
  - Unzip the zip file, open the csv file and add users and devices in the same format (see here)
  - Import the csv file with users and devices back into Device Manager (see here)

➢ **To add *only* users:**

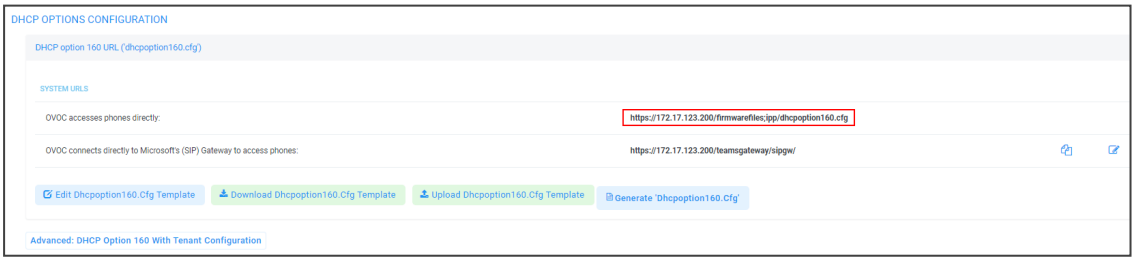
- Applies only to Version 7.6 and later
- The association is manually made after deployment, using the **Approve** button in the Devices Status page
- When the phone is connected to the network for the first time, the user is prompted to enter their username/password; it's matched with that on Device Manager. After the match, Device Manager associates the device with the user. Usernames/ passwords are then uploaded to the Manager through the import CSV *without using MAC address*. After authentication, the Manager downloads the cfg file to the phone.

1. After installing Device Manager, add the HTTP authentication configuration properties to the initial configuration file (taken from DHCP Options 160) and to the templates.
2. Select an authentication mode. Two possibilities are available:
   - With username/password
   - Without password; only username or extension

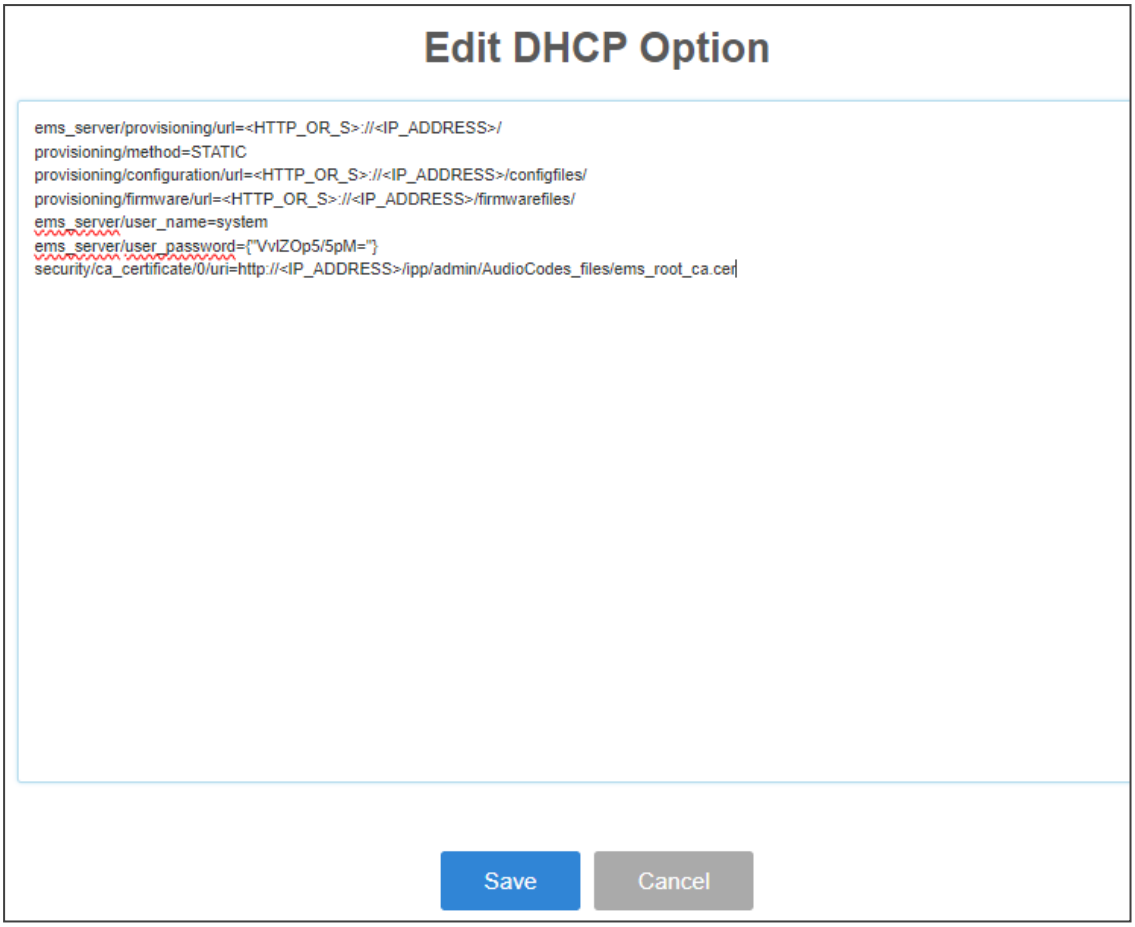
- The default authentication mode is username/password
- The Login screen then enables the user to authenticate with username only, excluding password
- If you want the user to use 'password only' for authentication, enable the 'no password' option as shown in the next figure



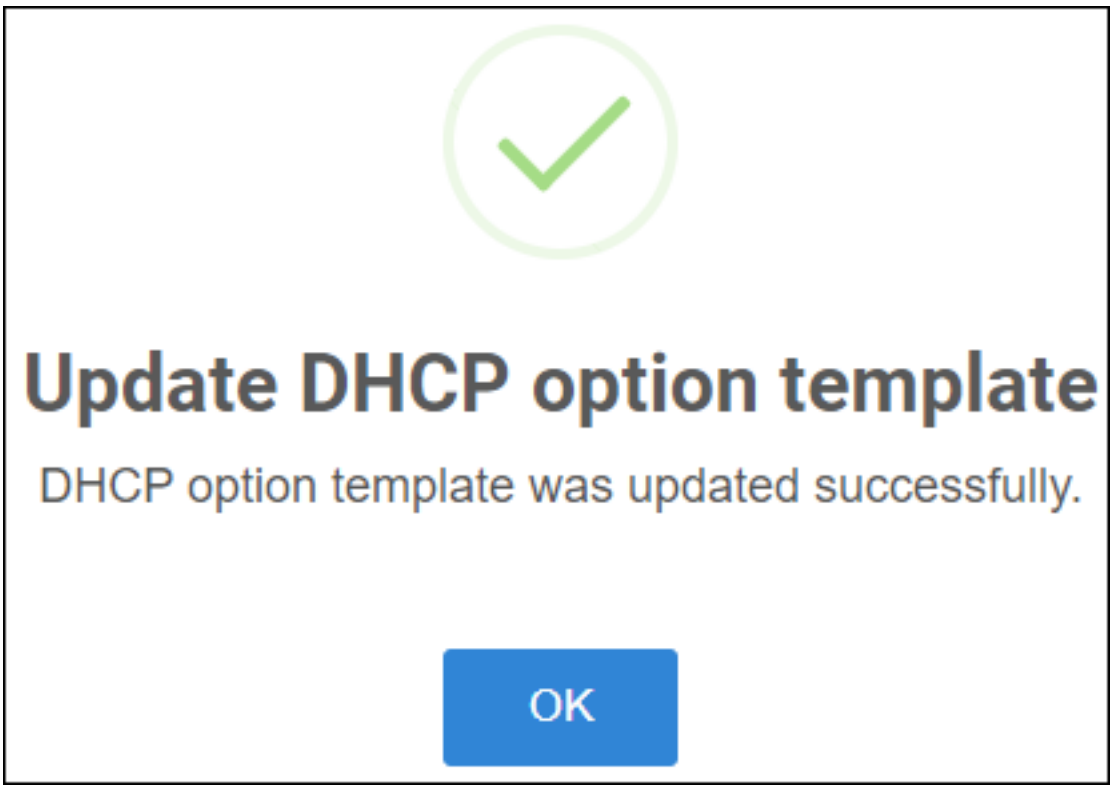
3. Configure DHCP Options for HTTP Authentication. To prompt the user for username and password, add the following HTTP authentication parameters to the DHCP Option 160 cfg file:
   - provisioning/configuration/http_auth/password=
   - provisioning/configuration/http_auth/ui_interaction_enabled=1
   - provisioning/configuration/http_auth/user_name=
4. Update the parameter 'provisioning/configuration/url'
   - provisioning/configuration/url=<HTTP_OR_S>://<IP_ADDRESS>/ipp/admin/httpauth/auth_prov.php
5. Open the DHCP Option Configuration page (**Setup** > **Settings** > **DHCP Options Configuration**)



6. Click **Edit Dhcpoption160.cfg template**:



7. Edit and click **Save**; you're prompted:



8. Click **OK**.

If you want password to be excluded from HTTP user authentication, configure parameter 'provisioning/configuration/http_auth/password' to **1234**. Users will then not have to enter a password when performing authentication.

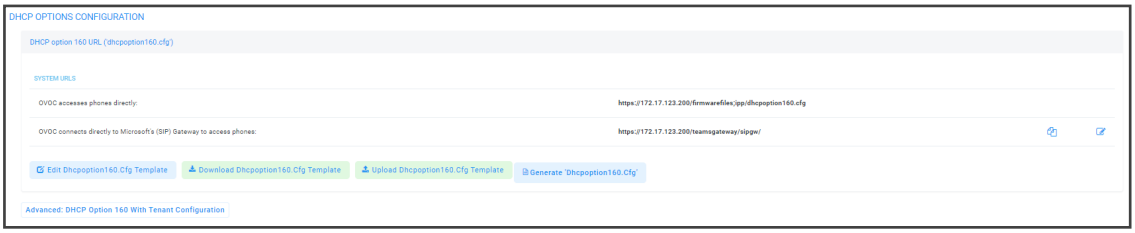
9. Configure each template to operate with HTTP authentication. Open each template you want to operate with HTTP authentication and add the following values to each:
   - provisioning/configuration/http_auth/password=%ITCS_Line1AuthPassword%
   - provisioning/configuration/http_auth/ui_interaction_enabled=1
   - provisioning/configuration/http_auth/user_name=%ITCS_Line1AuthName%
10. Update the parameter 'provisioning/configuration/url':
    - provisioning/configuration/url=%ITCS_HTTP_OR_S%://%ITCS_HTTP_PROXY_IP%:%ITCS_HTTP_PROXY_PORT%/ipp/admin/httpauth/auth_prov.php
11. Close the Directory 'configfiles'. For security reasons, it's preferable to close the 'configfiles' web directory as from now on all cfg files will be downloaded from the new location **http:<SERVER_IP_ADDRESS>/ipprest/lync_auto_prov.php** rather than from **http:<SERVER_IP_ADDRESS>/configfiles/MAC.cfg**

Editing the DHCP Option 160 cfg File

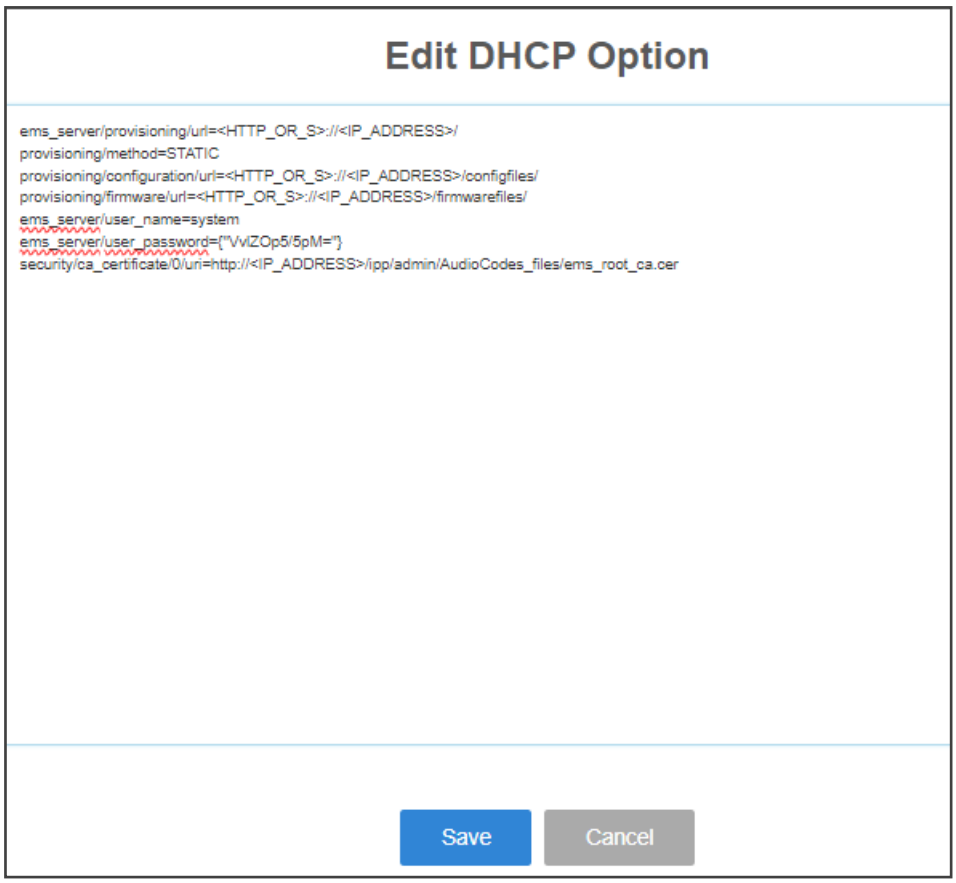
Admin can opt to edit the initial DHCP Options 160 cfg file. Choose the **DHCP Option Configuration** button if your phones are communicating with a DHCP server. A DHCP server is mandatory if the phones are behind a NAT, or when communicating with an SBC HTTP proxy.

➢ To edit the DHCP Option 160 cfg File:

1. Open the DHCP Options Configuration page (**Setup** > **Settings** > **DHCP Options Configuration**).



2. Click the **Edit cfg Template** button.



3. Edit the DHCP option using the table below as reference.

Parameter	Description
Keep alive period	You can configure how often the phones generate a keep-alive trap towards Device Manager. Default: Every 60 minutes. It's advisable to configure a period that does not exceed an hour. The management system may incorrectly determine that the phone is disconnected if a period of more than an hour is configured.
Provisioning URL	Defines the URL (including IP address and port) of the provisioning server (OVOC server).
Provisioning Method	Defines the provisioning method, i.e., STATIC or Dynamic (DHCP). Do not change this setting. The setting must remain STATIC. If not, the phone will continuously perform restarts.
Provisioning Configuration URL	Defines the URL of the location of the configuration files (including IP address and port) in the provisioning server (OVOC server).
Provisioning Firmware URL	Defines the URL of the location of the firmware files (including IP address and port) in the provisioning server (OVOC server).

Parameter	Description
User Name	Defines the user name for the REST API. Default: **System**. Later, each phone receives its own unique user name.
User Password	Encrypted. Defines the user password for the REST API. Default: **System**. Later, each phone receives its own unique user password.

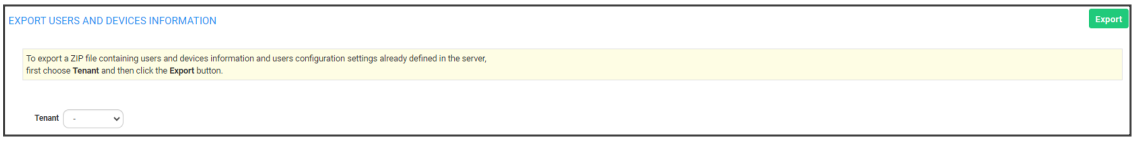
You can always restore these settings to their defaults if necessary by clicking the **Restore to default** button in the DHCP Option Configuration dialog but it's advisable to leave these settings unchanged. The button is displayed only after the DHCP Option is changed.

Exporting 'System User' to zip File

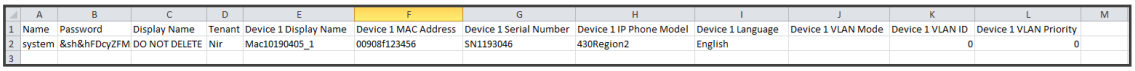
Admin can export the 'system user' that is automatically created after logging in to Device Manager, to a zip file.

➢ **To export the 'system user' to a zip file:**

1. Open the Export Users and Devices Information page (**Setup** > **Import/Export** > **Export Users and Devices**).



2. From the 'Tenant' drop-down, select the tenant and then click **Export**; the 'users' WinZIP file is downloaded to the downloads folder on the PC.
3. Double-click the file; the unzipped file opens displaying a csv file and cfg files.
4. Right-click the csv file, select **Open With** and then **Microsoft Excel**:



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	Password	Display Name	Tenant	Device 1 Display Name	Device 1 MAC Address	Device 1 Serial Number	Device 1 IP Phone Model	Device 1 Language	Device 1 VLAN Mode	Device 1 VLAN ID	Device 1 VLAN Priority	
2	system	&sh&hFDcyZFM	DO NOT DELETE	Nir	Mac10190405_1	00908f123456	SN1193046	430Region2	English		0	0	
3													

Excel displays information related to 'system user'.

Adding Users and Devices Information to the csv File

You need to add to the csv file the information related to all the users and devices in your enterprise's network.

To facilitate this task, you can export a csv from your enterprise PBX and then edit it to conform to the 'system user' csv row shown in the figure above and the columns shown in the table below.

Name	Password	Display Name	Tenant	Display Name	Serial	MAC Address	Phone Model	Language	VLAN Mode	VLAN ID	VLAN Priority

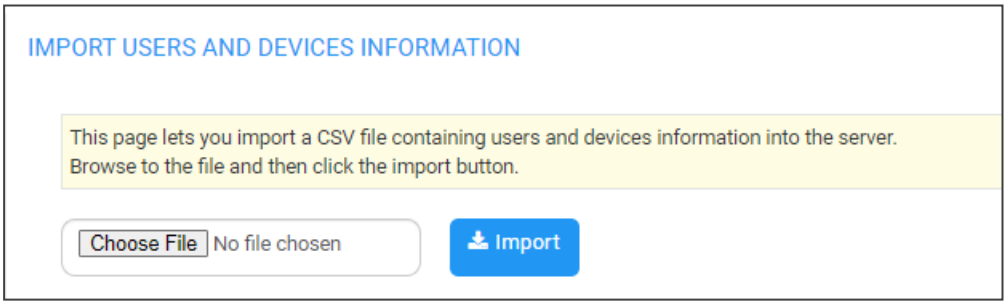
Up to 30000 users and devices can be defined in the csv file. After defining users and devices, save the csv file on your desktop from where you can import it into Device Manager.

Importing the csv File

After adding to the csv file the information related to all the users and devices in your enterprise's network, import the new csv file into Device Manager.

➢ **To import the new csv file into Device Manager:**

1. Open the Import Users & Devices Information page (**Setup** > **Import/Export**).



2. Click **Import** and then navigate to and select the csv file which you created and saved on your desktop previously; the file is imported into Device Manager.
3. Open the Manage Users page (**Setup** > **Users & Devices**) and make sure all enterprise users you imported are displayed.

Approving Users

Approving users is unnecessary
- when using the Zero Touch provisioning method
- when importing a csv file containing devices (as well as users)

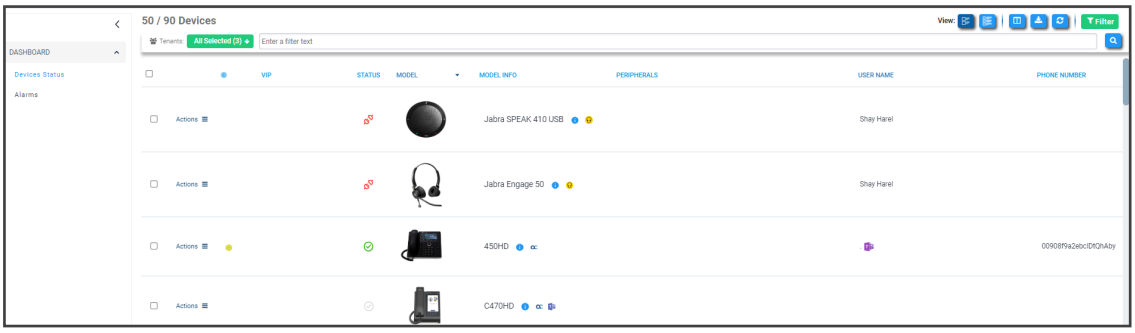
If you're *not* using the Zero Touch provisioning method or importing a csv file, then you need to approve users after plugging the phones into the network.

SIP Environment

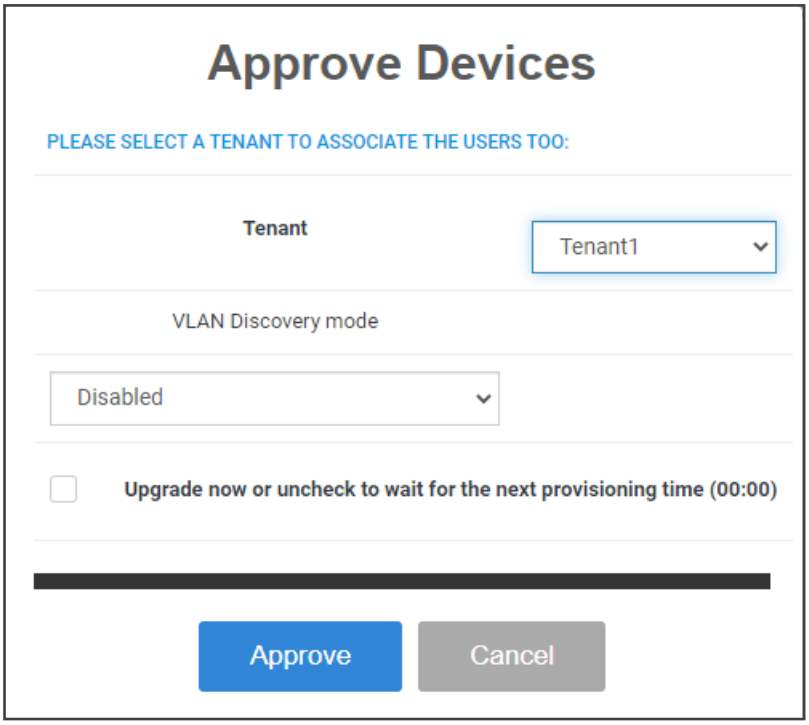
After plugging SIP phones in, they report to Device Manager which does not display user name in the UI until sign-in is performed or, until users are approved in the UI.

➢ **To approve users in a SIP environment:**

1. Open the Devices Status page (**Monitor** > **Dashboard** > **Devices Status**).



2. Optionally click the 'Export the devices to CSV file' icon; a csv file is generated; a download option is displayed. The same information on the page, e.g., Serial Number, which enables admin to efficiently manage devices stocktaking, is displayed in Excel format.
3. Click **Actions** to select (depending on device and model) Show Info, Open Web Admin, Check Status, Reset Device, Generate Configuration, Change Group, Delete Devices Status, Update Configuration, Change Tenant, Update Firmware, Nickname, Set as VIP.
4. Click the **Approve** button (only displayed if the System URL is configured for the DHCP Option because OVOC will then not know the tenant in which the device is located; if the Tenant URL is configured for the DHCP Option, the **Approve** button will not be displayed).
5. View information displayed in the page's columns next to each managed device: User Name, Phone Number, MAC Address, IP, Model, Firmware, Last Update Status, Report Time, Location, Subnet, VLAN ID
6. [Optionally] Use the **Search** option to display specific information in the page and exclude unwanted information from the page.
7. [Optionally] Click the **Filter** button to display specific information in the page and exclude unwanted information from the page.
8. Select the upper left checkbox; the **Selected Rows Actions** menu is displayed and all devices listed are selected.
9. Click the **Approve Devices** button; you're prompted to approve the selected device/s.



10. In the prompt, select the tenant and then click **Approve**; all selected users are approved; all phones restart; the cfg file is automatically uploaded to the phones from the OVOC provisioning server, which the DHCP server points them to.
11. From the 'VLAN Discovery mode' dropdown, select either:
    - **NONE**
    - **Disabled**
    - **Manual Configuration** [of the LAN; static configuration of VLAN ID and priority]
    - **Automatic - CDP** [automatic configuration of the VLAN - VLAN discovery mechanism based on Cisco Discovery Protocol]
    - **Automatic - LLDP** [automatic configuration of VLAN - VLAN discovery mechanism based on LLDP]
    - **Automatic - CDP_LLDP** [automatic configuration of VLAN (default) - VLAN discovery mechanism based on LLDP and Cisco Discovery Protocol. LLDP protocol is with higher priority].

Non-SIP Environment

Unlike SIP devices, the admin in a non-SIP environment needs to log in users phones. Admin can do this by importing a csv | zip file with the phones properties, or by approving the phones users one at a time.

- In contact centers, where multiple users may use a particular phone, a 'user' is sometimes made the equivalent of the Direct Inward Dialing (DID) number associated with the phone.
- After plugging in phones, the phones report to Device Manager, which does not display user names whose MAC address are unknown.

➢ **To approve users:**

1. Open the Devices Status page (**Monitor** > **Dashboard**); the non-SIP devices screen is identical to the SIP devices screen.
2. Click **Approve** next to the user; the Approve Device dialog opens – the non-SIP devices screen is identical to the SIP devices screen.
3. Enter the User Name and the Display Name, and then click **Approve**; the user name is displayed in Device Manager and the user is approved.

   The User Name and Password will function as the SIP user name and password.

- This procedure only applies when connecting phones for the first time. After first-time connection, the cfg file - containing user name and password - is automatically uploaded to the phones from the OVOC provisioning server, which the DHCP server points them to.
- In some non-SIP environments, for example, in Genesys contact centers, Password is not specified.

Converting Skype for Business | SIP Phones to Microsoft SIP Gateway

AudioCodes recommends that customers who have deployed legacy devices, migrate to SIP Gateway via Device Manager.

Microsoft SIP Gateway lets your organization use AudioCodes SIP phones with Microsoft Teams.

Compatible AudioCodes phones are:

- AudioCodes' Skype for Business IP phones with standard SIP firmware
- AudioCodes' SIP phones

The conversion preserves enterprises' investments in legacy phones. The conversion enables SIP phone users to sign-in to Teams with corporate credentials and make and receive calls.

- See here for information on how to plan for the Microsoft SIP Gateway.
- See here for information on how to configure the Microsoft SIP Gateway.

The conversion applies to the following phones:

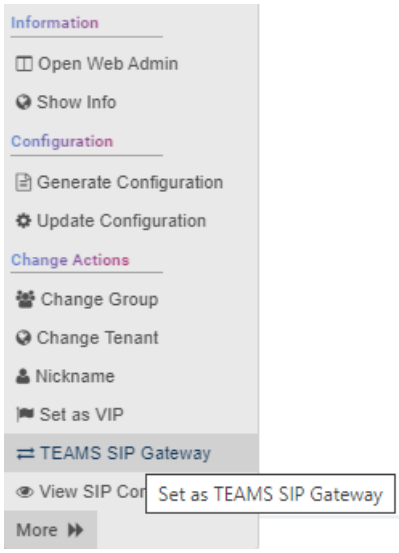
- 405HD (in Skype for Business or Generic SIP mode)
- 445HD (in Skype for Business or Generic SIP mode)
- 450HD (in Skype for Business or Generic SIP mode)
- C448HD in Teams mode (should be converted to Generic SIP mode before applying these instructions)
- C450HD in Teams mode (should be converted to Generic SIP mode before applying these instructions)

- AudioCodes recommends using the latter two phones as SIP Gateway rather than as Native Teams phones.
- See also here for maintenance period and migration options with C450HD | C448HD Native Teams phones.

After adding Microsoft's SIP Gateway to an enterprise's IP telephony network, users can connect these non Teams-certified AudioCodes phone models to the Microsoft telephony environment and reuse / re-purpose them with the Microsoft Teams cloud telephony service.

➢ **To convert an AudioCodes phone to SIP Gateway:**

1. Define the SIP Gateway URL as shown here for SIP Gateway↔Device Manager connectivity.
2. In the Monitor page, click the **Actions** link adjacent to the phone to convert and then in the menu that opens click **More...**



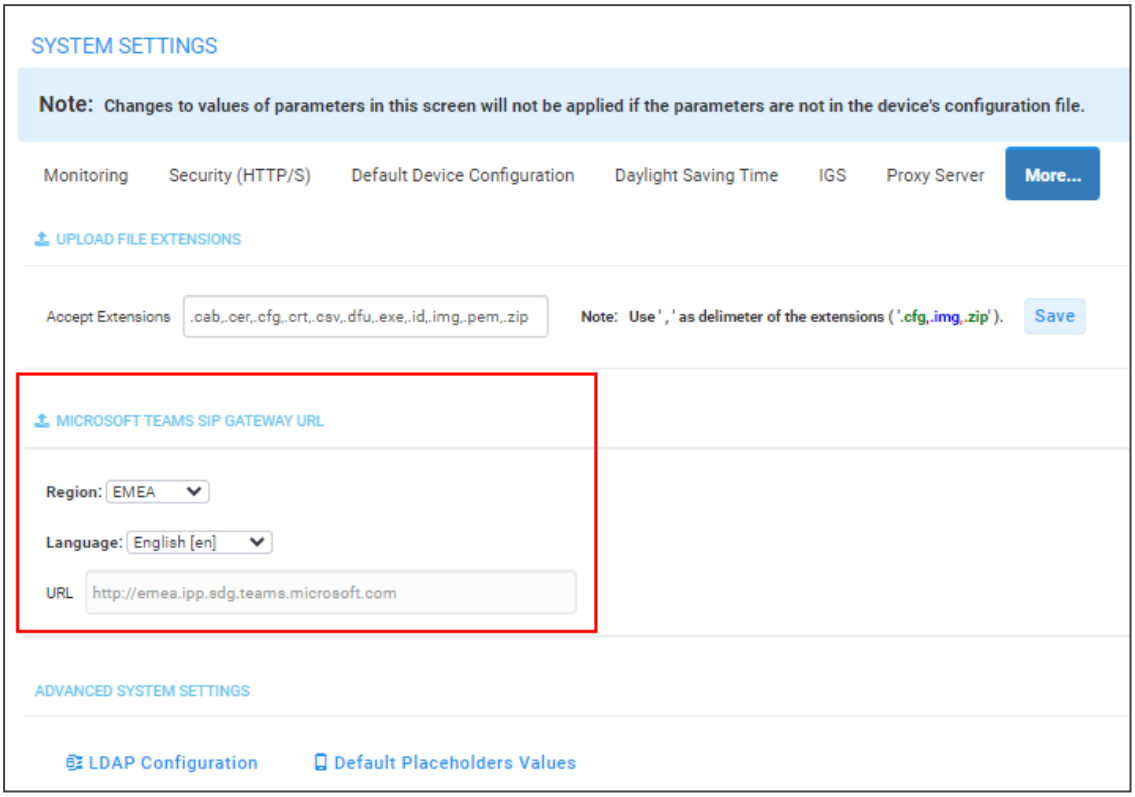
3. Select the **TEAMS SIP Gateway** option.

Configuring Microsoft SIP Gateway URL

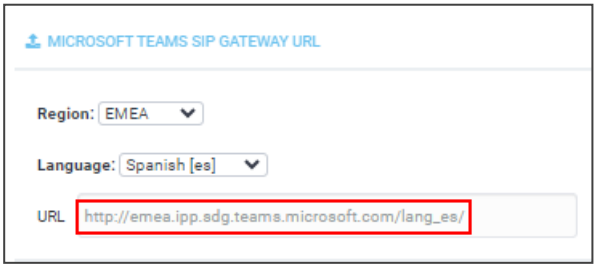
Admin must configure the Microsoft SIP Gateway URL for SIP Gateway ↔ Device Manager connectivity.

➢ To configure the URL:

1. In Device Manager, open the System Settings page (**Setup** > **Settings** > **System Settings**) and then click the **More...** tab.



2. Under the 'Microsoft Teams SIP Gateway URL' section shown in the figure, select the 'Region' from the drop-down. Select either:
   - EMEA - the Microsoft SIP Gateway's URL **http://emea.ipp.sdg.teams.microsoft.com** is automatically displayed accordingly (read-only)
   - Americas - the Microsoft SIP Gateway's URL **http://noam.ipp.sdg.teams.microsoft.com** is automatically displayed accordingly (read-only)
   - APAC - the Microsoft SIP Gateway's URL **http://apac.ipp.sdg.teams.microsoft.com** is automatically displayed accordingly (read-only)
3. Select the 'Language' from the drop-down; the URL is automatically adjusted accordingly. For example:



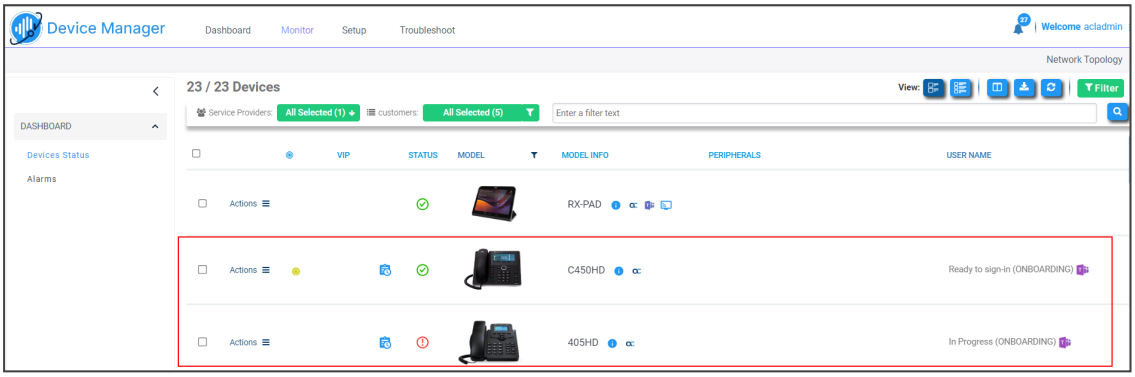
4. Click the **Save all Settings** button (not shown in the preceding figure).

Monitoring the Microsoft SIP Gateway

After converting an AudioCodes SIP phone to Microsoft SIP Gateway, admin can monitor the SIP Gateway.

➢ To monitor AudioCodes SIP phones converted to Microsoft SIP Gateway:

1. In Device Manager, open the Devices Status page (**Monitor** > **Devices Status**).



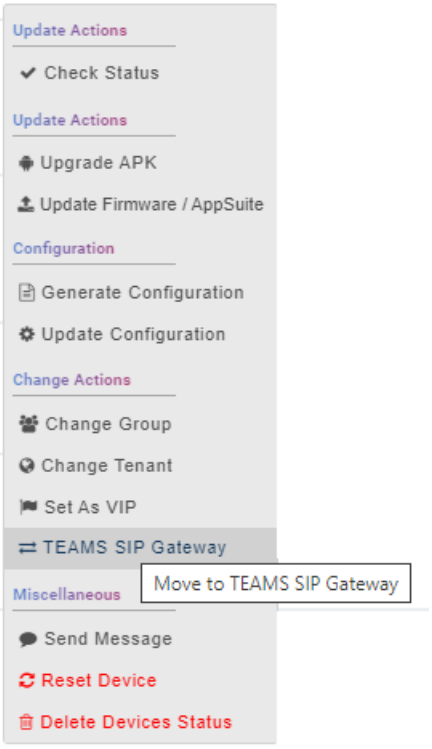
2. View the SIP Gateway icon displayed adjacent to the device under the 'User Name' column.
3. View the phone's status:
   - Onboarding (under the 'User Name' column indicates waiting for the user to sign in)
   - Registered (under the 'Status' column indicates sign-in was performed)

Converting AudioCodes SIP Phones to Microsoft SIP Gateway

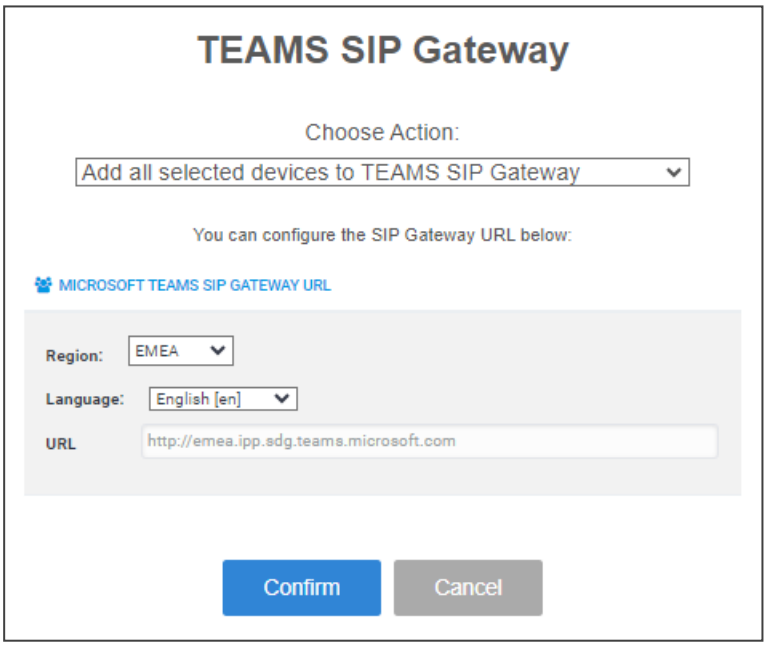
➢ To convert to Microsoft SIP Gateway:

1. Open the Devices Status page (**Monitor** > **Dashboard** > **Devices Status**).
2. Select the phones to convert using the check boxes on the left side of the page.

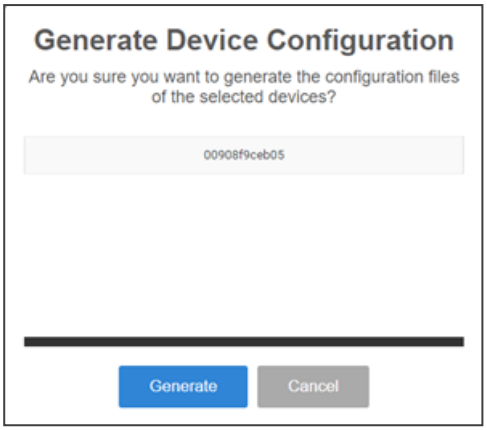
3. Click the **Selected Rows Action** link.



4. Select the **TEAMS SIP Gateway** option.



5. Select **Add all selected devices to TEAMS SIP Gateway** and then click **Confirm**.
6. Repeat step **2**.
7. Select the **Generate Configuration** option.



8. Click **Generate**.

9. From the 'Update devices now' drop-down menu, select **YES** and then click **Generate**.
10. Make sure the relevant phones are displayed as SIP Gateway:

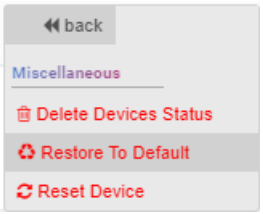
11. The phone reboots and switches to SIP Gateway. The process includes rebooting from Android to Linux and updating the configuration from SIP Gateway.

Restoring to Default

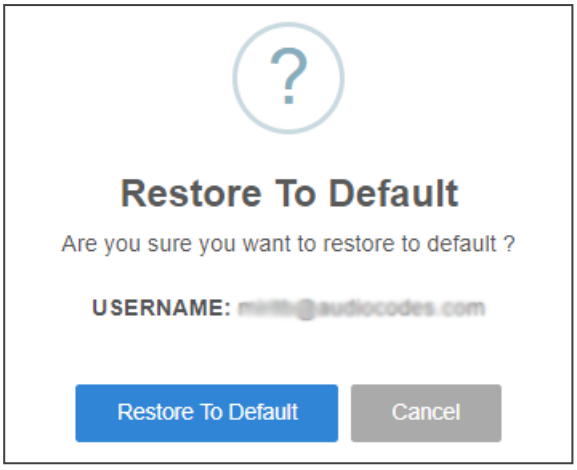
Device Manager enables admin to restore a single Native Teams device to its default settings. The feature does not enable admin to restore multiple devices to default settings (bulk).

➢ To restore a device to default:

1. In the Devices Status page (**Monitor** > **Devices Status**), click the **Actions** menu next to the device and then click **More**.



2. Select the **Restore to Default** option.



3. Click **Restore to Default**; the action might take a few minutes to complete.

5 Monitoring and Maintenance

Network admins can use Device Manager to monitor and maintain devices deployed in the network.

Monitoring & Maintaining Meeting Rooms

Device Manager supports monitoring and maintaining AudioCodes Meeting Rooms and their peripheral devices:

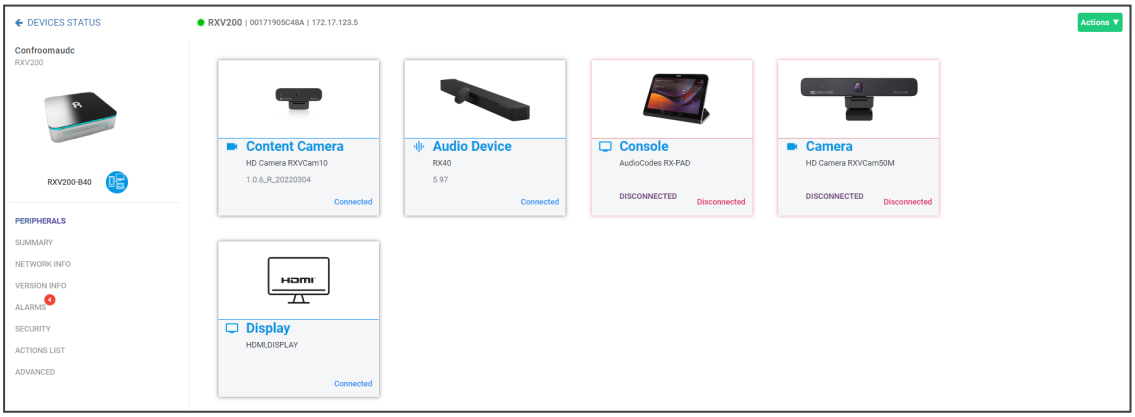
- **RXV81** Meeting Room (Android-based, Microsoft-certified). See here.
- **RXV200** Meeting Room (Android-based, Microsoft-certified). See here.
- **RX-PAD** Meeting Room Controller. See here.
- **RXV100** Meeting Room (Windows-based). See here.
- **RXV80** Meeting Room. See here.
- **RX-PANEL** Meeting Room Scheduler. See here.
- **Desktop | PC** Meeting Room. See here.

Upgrading Meeting Room Firmware

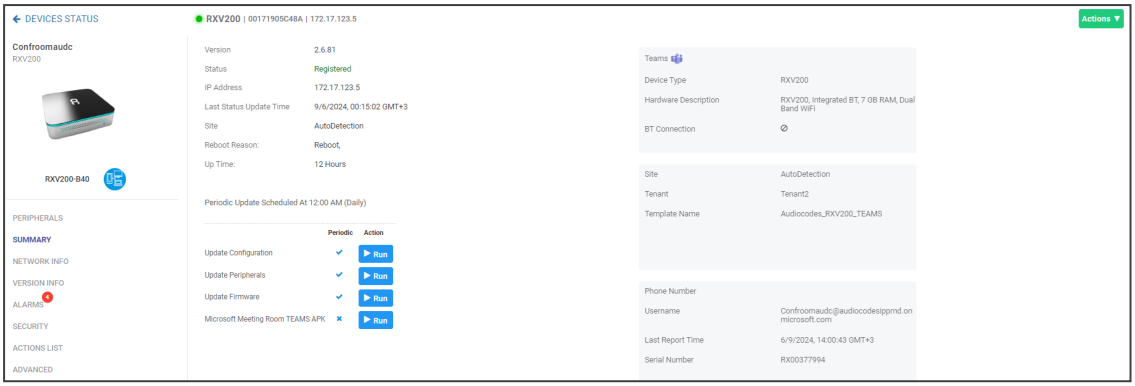
The Show Info page in Device Manager enables admins to upgrade Meeting Room firmware.

➢ **To upgrade Meeting Room firmware:**

1. Open the Device Info page (**Monitor** > **Dashboard** > **Devices Status** > click **i** adjacent to the device).



2. Click the **Summary** tab.



3. Click the **Run** button adjacent to

   - **Update Configuration** to update the device's cfg file
   - **Update Peripherals** to update the device's peripherals
   - **Update Firmware** to update the device's firmware img file
   - **Microsoft Meeting Room Teams APK** (to update the Android Package Kit on Android-based Teams devices - phones as well as Meeting Rooms)
   - **Update AudioCodes AppSuite** (applies only to Windows-based Meeting Room devices, e.g., RXV100)

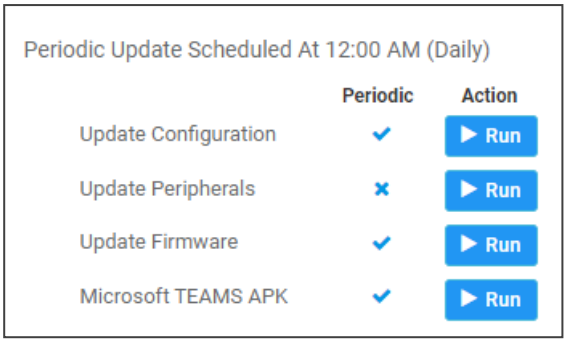
- **Update Peripherals** is only supported when the device is connected by USB and not by Bluetooth.
- **Microsoft Teams APK** is supported from version 1.17 and later.
- **Windows-based devices and Windows are interdependent**. The device checks for a new version for the Windows OS and for the device, and updates both. In the App Suite / Device Manager client, the update schedule is configured.

4. Under the **Version Info** tab, verify the device's Teams | Windows versions.

The tab for RXV100 displays:

- Status
- Version info
- Windows version

5. Enable / disable automatic upgrade of the Teams application. Allow the device to run the update *without* Device Manager involvement OR allow Device Manager to control the schedule of updating all elements.



6. If you select allowing Device Manager to be responsible for the device firmware update, two options are available:

   - **Periodic** (similar to Device Manager client)

     Configure 'Periodic' using the following provisioning parameters:

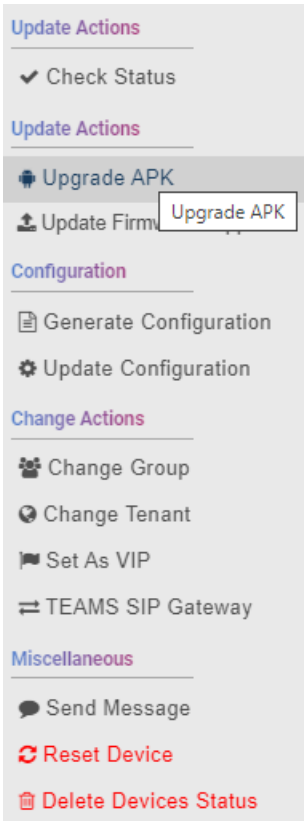
     - provisioning/period/type=DAILY (default value)
     - provisioning/period/daily/time=0:00

   - **Trigger an upgrade** (via an explicit command called 3rd party update per script) of the Teams App of the device according to the repository of the latest version (same as the other products).

Device Manager supports bulk Android APK update.

➢ **To perform bulk Android APK update:**

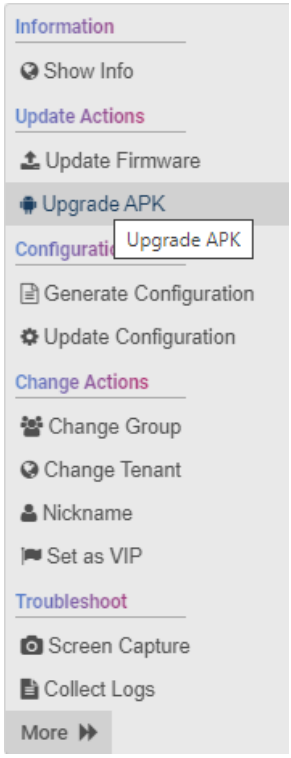
1. In the Devices Status page, select multiple Android-based devices and then click the activated **Selected Rows Actions** links:



2. From the menu that pops up shown in the preceding figure, select **Upgrade APK**.

➢ To update Android APK on a single device:

1. In the Devices Status page, click the **Actions** menu adjacent to the device:



2. From the menu that pops up shown in the preceding figure, select **Upgrade APK**.

➢ **To run Android APK on a single device:**

1. In the Devices Status page, click the **Actions** menu adjacent to the device and then from the popup menu, select the **Show Info** option.
2. Click the **Summary** tab and then click **Run** adjacent to 'Microsoft TEAMS APK'.

Upgrading Meeting Room Bundle Peripherals

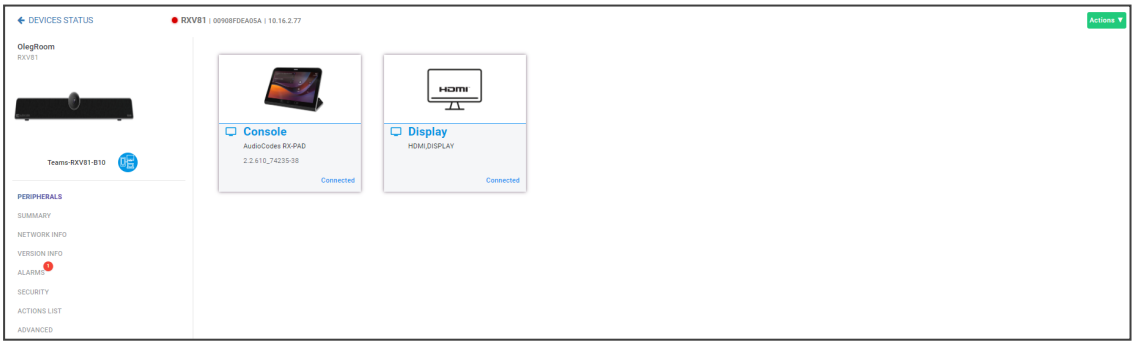
Device Manager enables admin to upgrade Meeting Room bundle peripherals to the latest version similarly to other devices. AudioCodes holds the repository of the latest GA versions of all bundle peripherals in the cloud, in the Latest Firmware page, which holds the repository of the latest GA version *per peripheral*.

Device Manager enables upgrading (for example):

- RXVCam50-M and RXVCam50-L connected to RXV100
- RX-15 connected to RXV80
- RXV40 connected to RXV100 or RXV200

➢ **To upgrade to the latest version:**

1. In the 'Latest Versions' page, sync with the latest GA versions held in AudioCodes' repository for each peripheral (see here for more information) in the same way as with other devices.
2. Open the Show Info page (in the Devices Status page, click the **i** icon adjacent to the device - OR - click the **Actions** link and select **Show Info** from the pop-up menu).



3. View the Meeting Room and its peripherals. The preceding figure shows the RXV81 Meeting Room and peripherals.
4. Under the **Summary** tab, click the **Run** button adjacent to
   - **Update Configuration**
   - **Update Peripherals**
   - **Update Firmware**
   - **Microsoft Meeting Room Teams APK**

- The peripheral upgrade is only supported when the device is connected by USB and not by Bluetooth.
- Upgrade of Microsoft Teams APK for Teams devices is supported from version 1.17 and later.

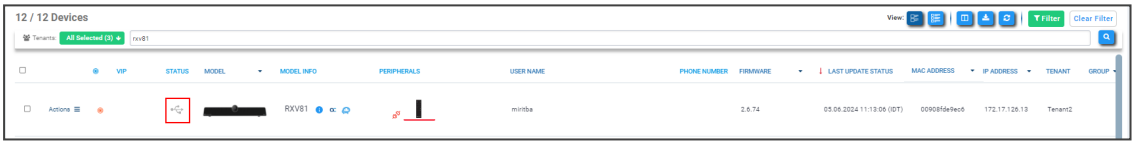
RXV81 MTR on Android

Admin can monitor and maintain the RXV81 Microsoft Teams Room on Android in their networks.

To get started with the RXV81, see the *RXV81 MTR Deployment Guide* available from AudioCodes.

➢ To monitor and maintain the RXV81:

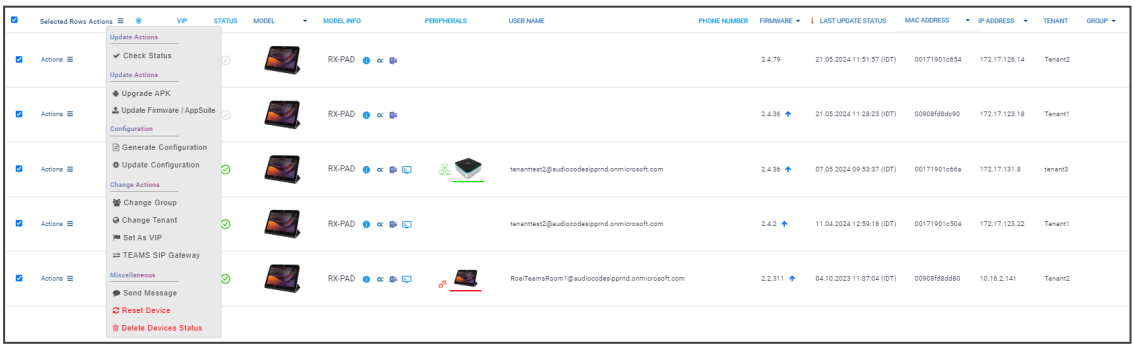
1. Open the Devices Status page (**Monitor** > **Dashboard** > **Devices Status**) and optionally reduce clutter by searching for RXV81.



2. Point your mouse at the Teams icon in the row of the device and determine the device version from the tool tip that pops up.

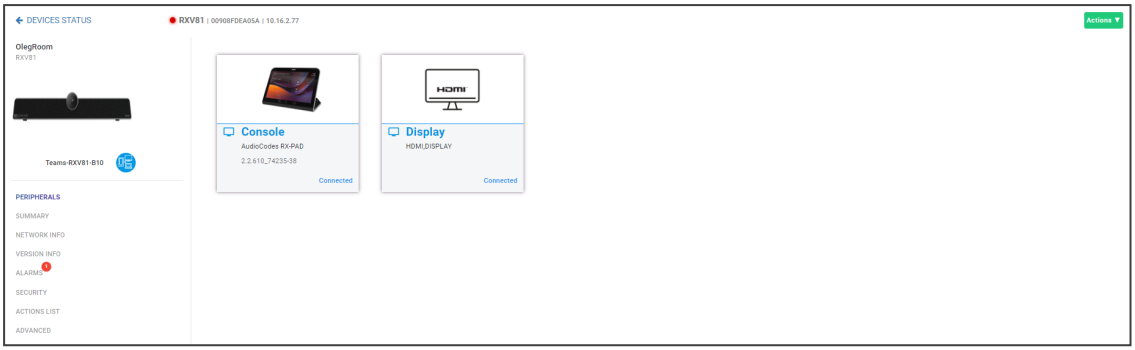
3. Point your mouse at the **i** (information) icon in the row of the device and from the tool tip that pops up determine if the device features Bluetooth, RAM size and Wi-Fi.

4. Click the Actions ≡ button adjacent to the device to manage -OR- select *multiple* devices and then click the activated Selected Rows Actions ≡ button.

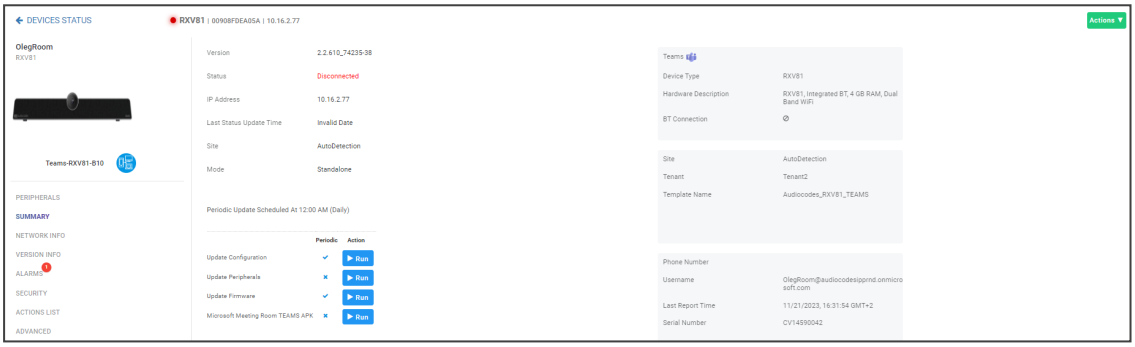


5. From the popup menu, select the management action you require; the procedures are the same as for the other managed devices described in this document.

6. Select **Show Info** or click the **i** (information) icon adjacent to the listed device.



7. Click the **Summary** tab.



8. View a summary of device-related information.

9. Click the **Network Info** tab.

10. Click the **Version Info** tab; information related to the version is displayed.

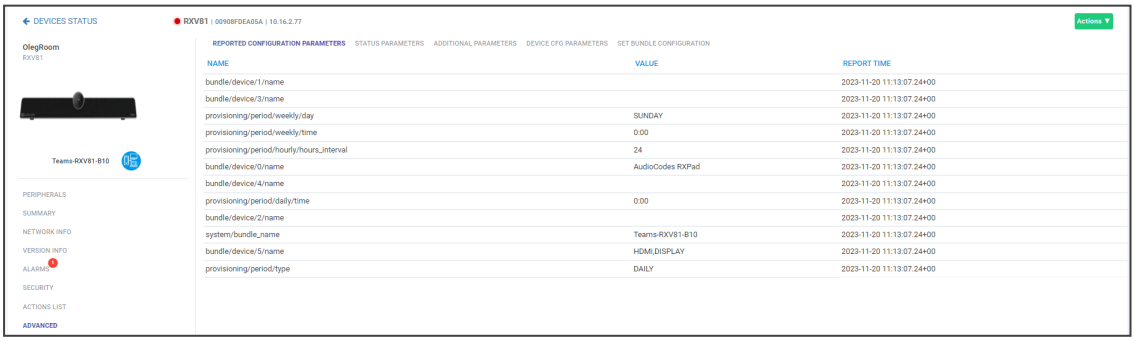
11. If an alarm is active on the device, view the indication adjacent to the **Alarms** tab as shown in the figure below.

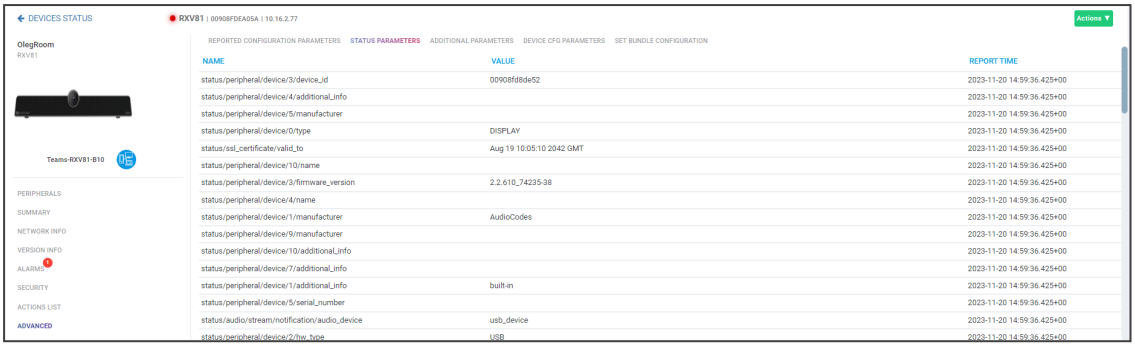
12. Click the **Security** tab.

13. View certificate status information related to the device. In the preceding figure, the reporting device is an Android device. Certificate status information includes ‘Issued by’, 'Issued to' and ‘Validity’.

14. View under the **Advanced** tab information about the device's parameters:

- Reported Configuration Parameters (see below)
- Status Parameters (see below)
- Additional Parameters
- Device CFG Parameters
- Change Bundle Configuration (see below) (for more information about available bundles, see the *RXV81 User's and Administrator's Manual*)





The following bundles are available for RXV81:

Name of Bundle	Details
TEAMS-RXV81-B15	■ Huddle Rooms | Small and Medium Meeting Rooms ■ 5-8 participants ■ RXV81 + RX-PAD Meeting Room Controller + RX15 Speaker
TEAMS-RXV81-B10	■ Huddle Rooms | Small and Medium Meeting Rooms ■ 5-8 participants ■ RXV81 + RX-PAD Meeting Room Controller
TEAMS-RXV81	■ Executive Offices | Huddle Rooms ■ RXV81 + Bluetooth Remote Controller

Admin can only change devices *with an existing bundle* via Device Manager.

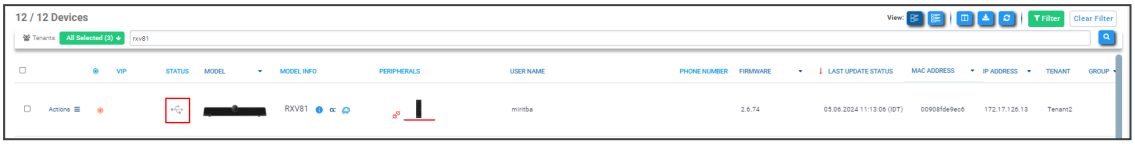
RXV81 USB Peripheral

Admin can monitor and maintain the RXV81 USB Peripheral in their networks.

To get started with the RXV81 USB Peripheral, see the *RXV81 USB Peripheral Quick Guide* available from AudioCodes.

➢ To monitor and maintain the RXV81 USB Peripheral:

1. Open the Devices Status page (**Monitor** > **Dashboard** > **Devices Status**) and optionally reduce clutter by searching for RXV81.



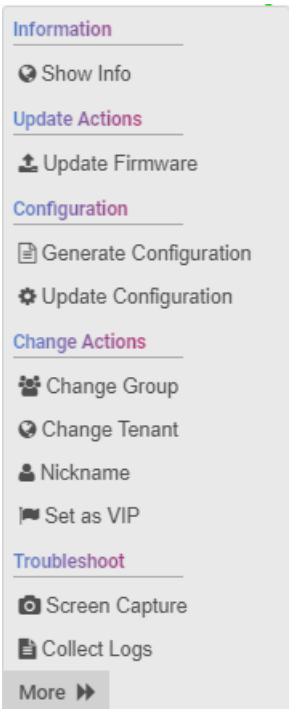
2. If in the 'Status' column you view:

   - a grayed (inactive) icon as shown in the preceding figure, it indicates that the RXV81 is disconnected from the PC and is operating as an RXV81 MTR (/license/MTRfA/enable = 1).
   - green (active) icon as shown in the figure below, it indicates that the USB is plugged in to the PC (/status/usb_device_mode/plugged = 1) and the RXV81 is operating as an RXV81 USB Peripheral.
   - Point your mouse at the green (active) icon shown in the figure below to make sure from the tool tip that pops up that RXV81 USB Peripheral is plugged in to the PC.

The 'Status' column displays this icon in a red color when RXV81 USB Peripheral is disconnected from Device Manager.

3. Point your mouse at the **i** (information) icon in the row of the device and from the tool tip that pops up determine if the device features Bluetooth, RAM size and Wi-Fi.

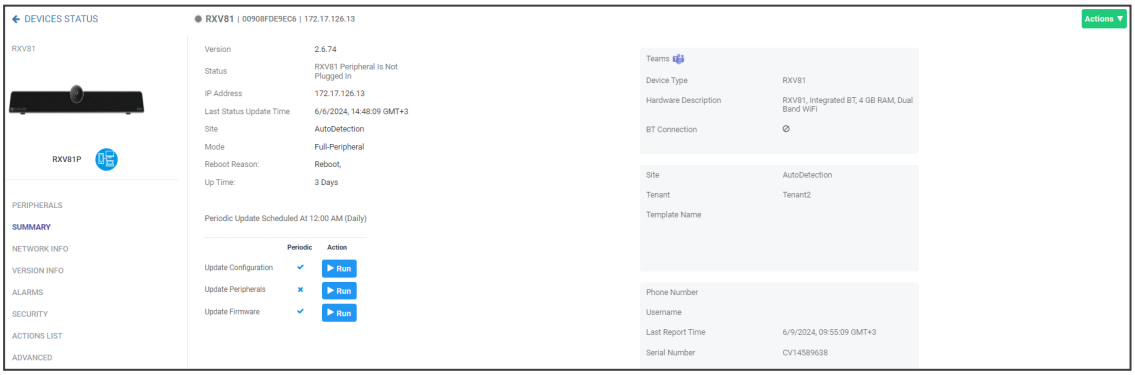
4. Click the Actions ☰ button adjacent to the device to manage -OR- select *multiple* devices and then click the activated Selected Rows Actions ☰ button.



5. From the popup menu, select the management action you require; the procedures are the same as for the other managed devices described in this document.

6. Select **Show Info** or click the **i** (information) icon adjacent to the listed device.

7. Click the **Summary** tab.



8. View a summary of device-related information.

9. Click the **Network Info** tab.

10. Click the **Version Info** tab; information related to the version is displayed.

11. If an alarm is active on the device, view the indication adjacent to the **Alarms** tab.

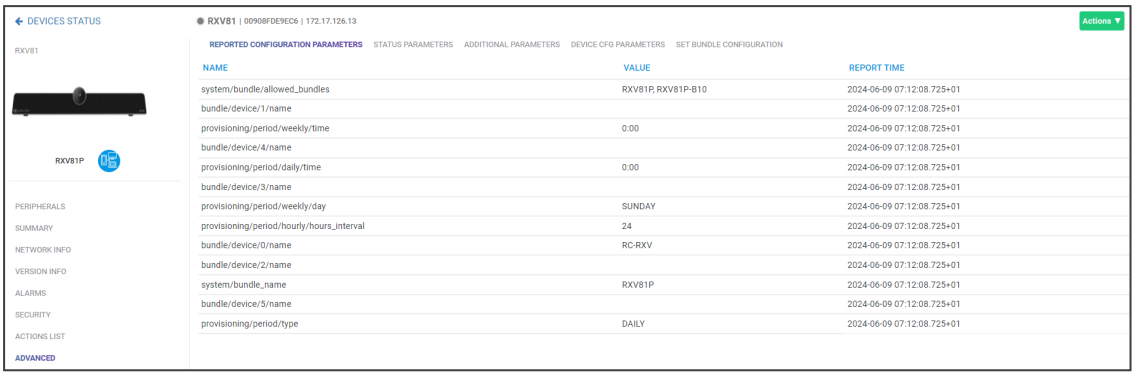
12. Click the **Security** tab.

13. View certificate status information related to the device. In the preceding figure, the reporting device is an Android device. Certificate status information includes ‘Issued by’, 'Issued to' and ‘Validity’.

14. View under the **Advanced** tab information about the device's parameters:

- Reported Configuration Parameters (see below)
- Status Parameters
- Additional Parameters
- Device CFG Parameters

- Set Bundle Configuration (see below) (for more information about available bundles, see the *RXV81 USB Peripheral User's and Administrator's Manual*)



RXV200 MTR on Android Compute

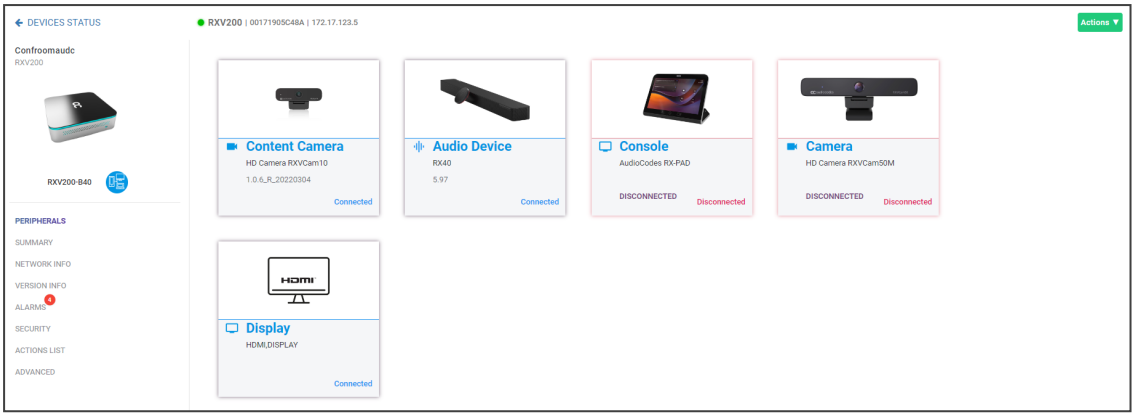
Admins can monitor and maintain the RXV200 Microsoft Teams Room Compute in their networks. For more information about RXV200, see AudioCodes' website here.

> To get started with RXV200, see the quick guide available here.

➢ To monitor and maintain RXV200:

1. Open the Monitor page (**Monitor** > **Dashboard** > **Devices Status**) and optionally enter a filter for RXV200.

2. Click the device icon or click **Actions** > **Show Info**.



3. Adjacent to 'Update Configuration' shown in the preceding figure, click **Run** to update the device with the latest .cfg file.
4. Adjacent to 'Update Peripherals' shown in the preceding figure, click **Run** to update the device's peripherals with the latest software .
5. Adjacent to 'Update Firmware' shown in the preceding figure, click **Run** to update the device with the latest .img file. If there is no latest software to update, you'll be prompted to go to the Latest Versions page to download it (**Setup** > **Firmware** > **Latest Firmware Versions**).
6. Adjacent to 'MSFT Teams Room APK For RX-Panel' shown in the preceding figure, click **Run** to update the device with the latest APK file (Android Package Kit file format).
7. View under the **Advanced** tab information about the device's parameters:
   - Reported Configuration Parameters
   - Status Parameters (see below)
   - Additional Parameters
   - Device CFG Parameters
   - Change Bundle Configuration (see below) (see the *RXV200 User's and Administrator's Manual* for more information about available bundles).

Admin can only change devices *with an existing bundle* via Device Manager.

The following bundles are available for RXV200:

Name of Bundle	Details
Teams-RXV200-B05	■ RXV200 + RX-PAD
Teams-RXV200-B20	■ RXV200 + RX-PAD + RXVCam50M + RX15 speaker
TEAMS-RXV200-B40	■ RXV200 + RX-PAD + RXVCam50M + RX40 audio bar

RX-PAD Meeting Room Controller

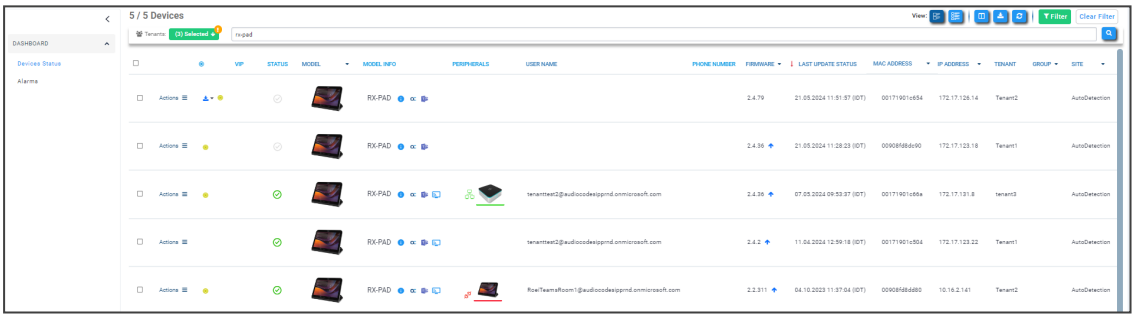
Device Manager supports AudioCodes' RX-PAD Microsoft Teams Room (MTR) Controller. RX-PAD is an Android-based MTR controller running the Teams App and compute. For more information about RX-PAD, see AudioCodes' website here.

> For a comprehensive guide on how to get started with RX-PAD, see the *RXV81 User's and Administrator's Manual* available from AudioCodes.

RX-PAD is an Android device that is managed independently after connecting it to OVOC with the Teams APK. After RX-PAD is paired with RXV81, Device Manager displays it as a peripheral device.

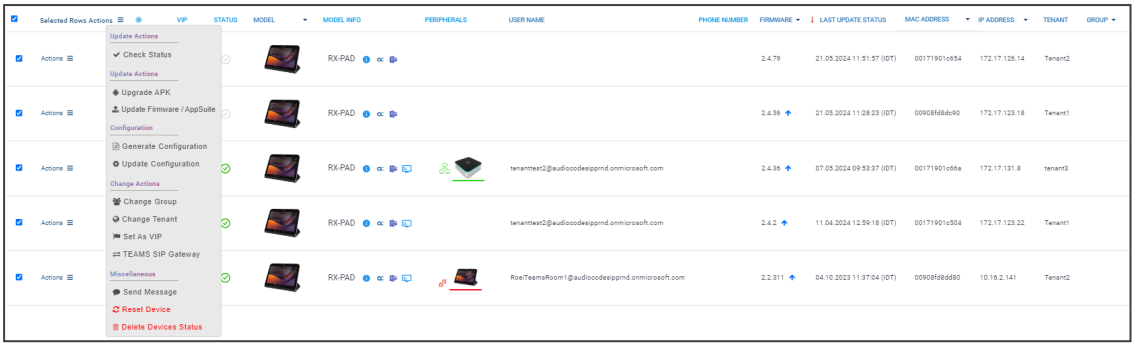
➢ To manage RX-PAD:

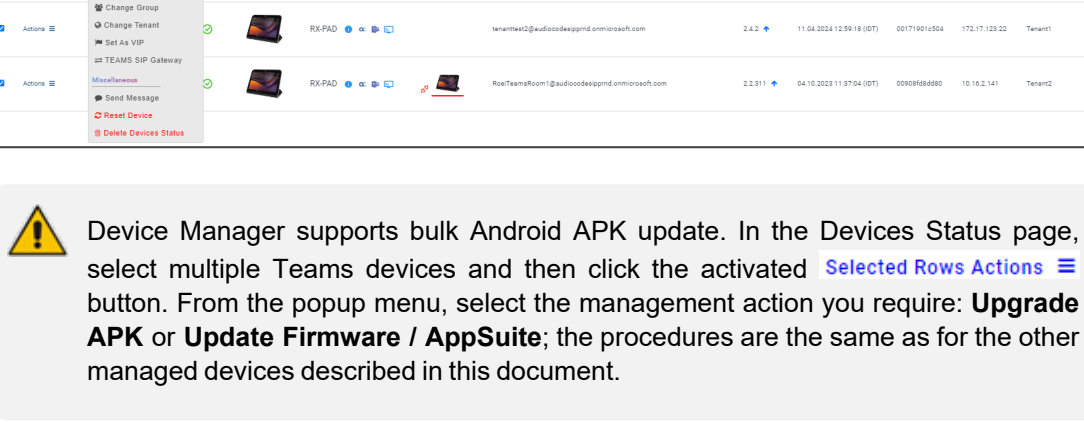
1. Open the Devices Status page (**Monitor** > **Dashboard** > **Devices Status**) and optionally reduce clutter by searching for RX-PAD.



> RXV81 does not upgrade RX-PAD as a peripheral. Device Manager's 'Latest Firmware Versions' repository contains RX-PAD Teams firmware that admin can load to the device.

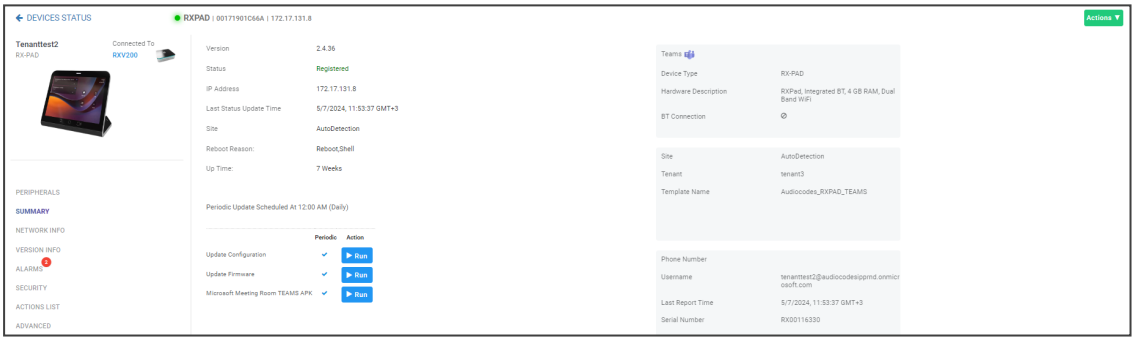
2. Point your mouse at the Teams icon in the row of the device and determine the device version from the tool tip that pops up. Alternatively, right-scroll to the 'Firmware' column to view the device's firmware version.
3. Point your mouse at the **i** (information) icon in the row of the device and from the tool tip that pops up determine if the device features Bluetooth, RAM size and Wi-Fi.
4. Click the Actions ≡ button adjacent to the device -OR- select *multiple* devices and then click the activated Selected Rows Actions ≡ button.





Device Manager supports bulk Android APK update. In the Devices Status page, select multiple Teams devices and then click the activated Selected Rows Actions button. From the popup menu, select the management action you require: **Upgrade APK** or **Update Firmware / AppSuite**; the procedures are the same as for the other managed devices described in this document.

5. Click the **i** (information) icon adjacent to the listed device, or select the **Show info** option from the menu displayed in the preceding figure.

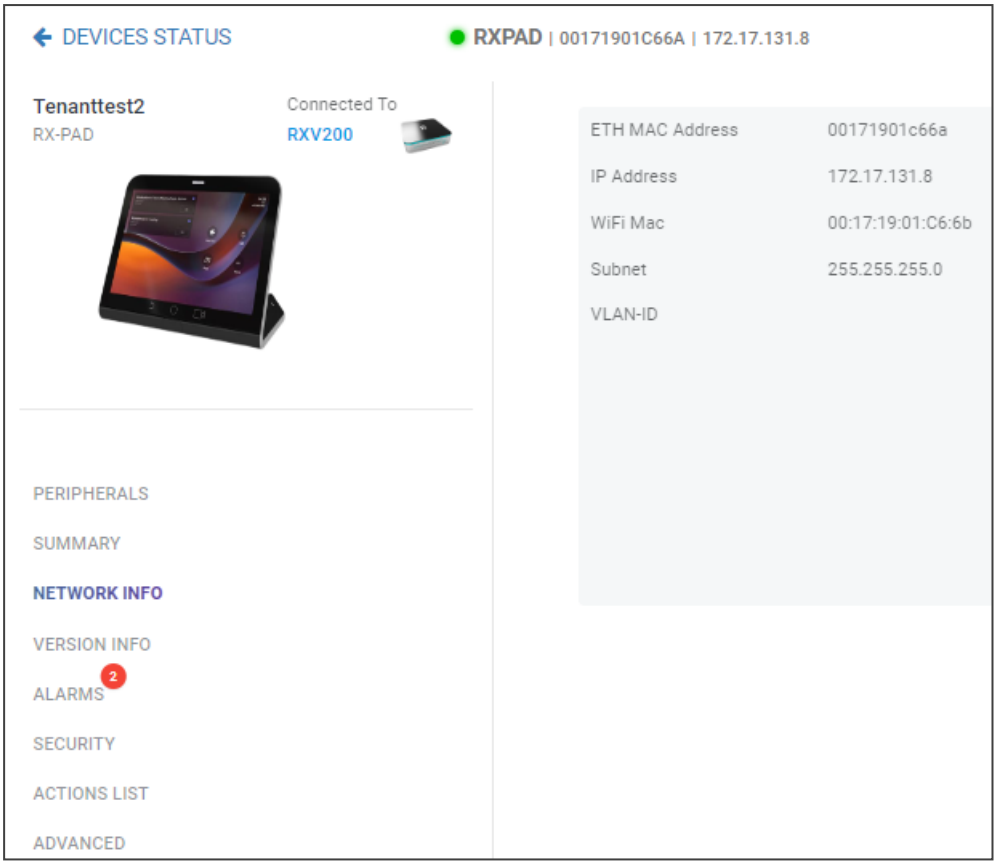


6. In the *upper pane* of the page shown in the preceding figure, view the device's version, status, IP address, Last Status Update Time and Site.

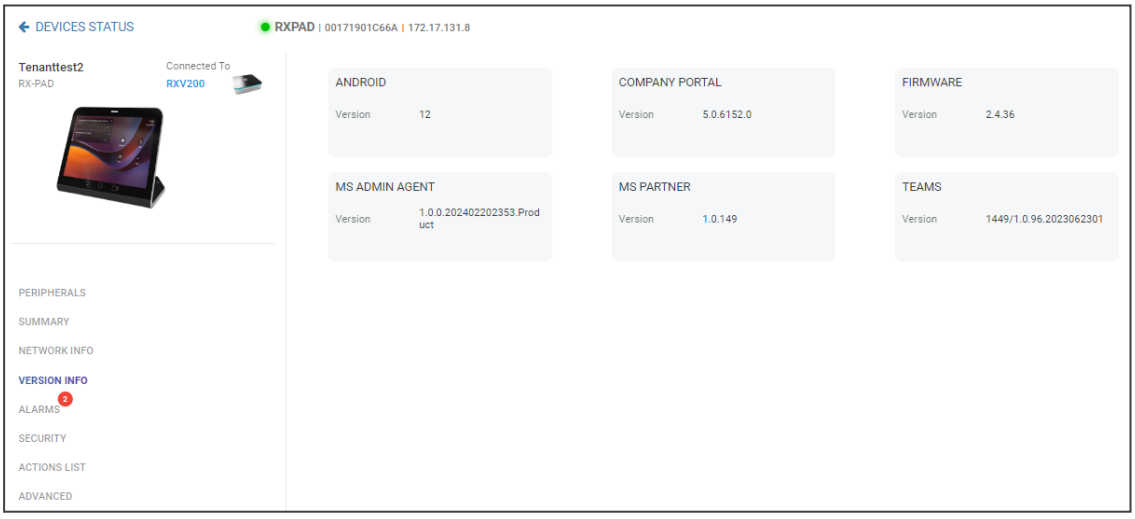
   In the *lower pane*, view information such as Tenant, Template Name and Serial Number.

   On the right side of the page, optionally use the links to update configuration, update firmware, update Microsoft Teams APK, collect logs, and / or restart.

7. Click the **Network Info** tab.



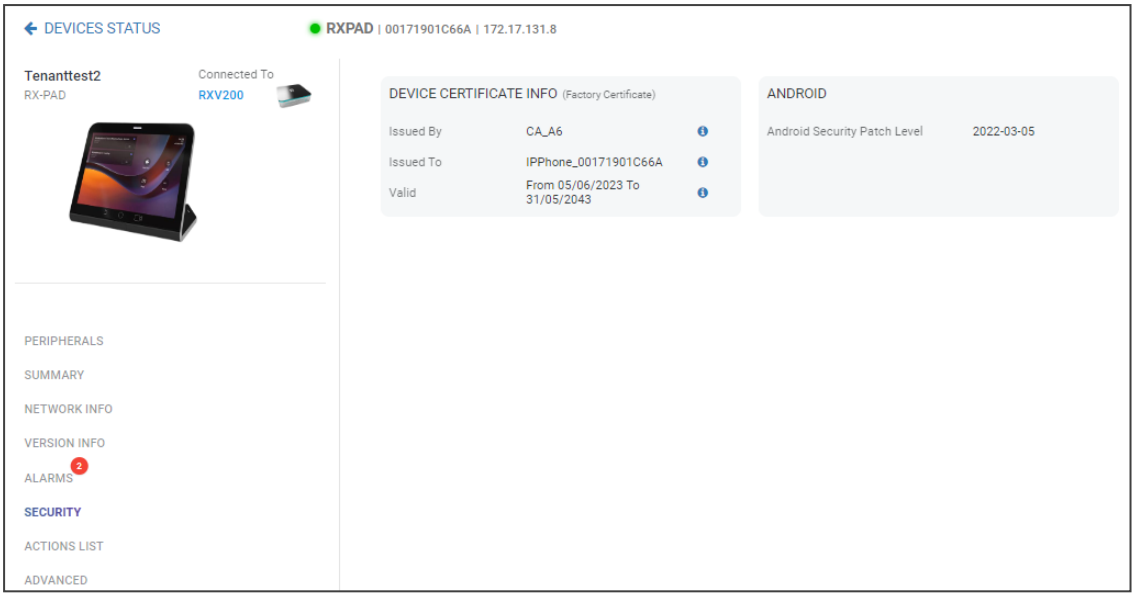
8. Click the **Version Info** tab; version information is displayed.



9. If a new alarm is active on the device, view the indication adjacent to the **Alarms** tab as shown in the preceding figure.

> A 'Teams Pairing Required' alarm is raised when RX-PAD is signed in but is not paired at the Teams level to its MTR (AudioCodes RXV81 or AudioCodes RXV200, for example).

10. Click the **Security** tab.



11. View certificate status information related to the device. In the preceding figure, the reporting device is an Android device. Certificate status information includes ‘Issued by’, 'Issued to' and ‘Validity’.

12. View under the **Advanced** tab information about the device's parameters:

    - Reported Configuration Parameters (see figure below)
    - Status Parameters (see figure below)
    - There are no Additional Parameters
    - There are no Device CFG Parameters

RXV100 MTR for Windows

Administrators can monitor and maintain the AudioCodes RXV100 Meeting Room in their networks using Device Manager. For more information about the RXV100, see here.

To *deploy* the RXV100 Meeting Room, see the *Device Manager for RXV100 Deployment Guide*.

➢ **To connect the RXV100 to Device Manager, use:**

- DHCP Option 160 -OR-
- AudioCodes Redirect Server if DHCP Option 160 is unsuccessful -OR-
- Static Provisioning URL if the former two methods are unsuccessful

For detailed information, see the *Device Manager for RXV100 Deployment Guide*.

RXV80 Standalone Video Collaboration Bar

Administrators can monitor and maintain the RXV80 Standalone Video Collaboration Bar deployed in their networks using Device Manager.

➢ **To monitor and maintain the RXV80:**

- The monitoring and maintenance procedures on the RXV80 are identical in principal to those on the RXV81. See here for more information.
- See also the *RXV80 Standalone Video Collaboration Bar User's and Administrator's Manual.*
- See also the *RXV80 Standalone Video Collaboration Bar Deployment Guide*.

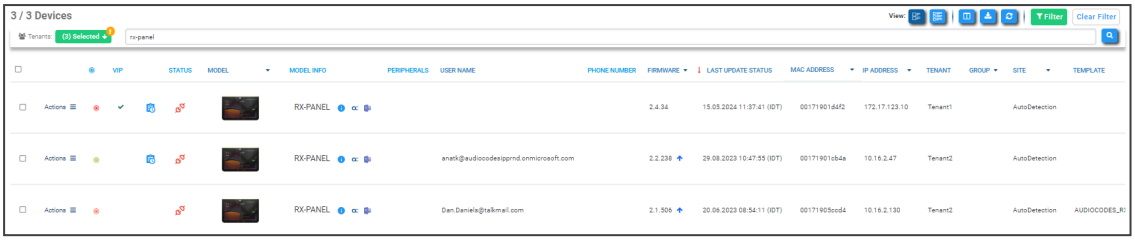
RX-PANEL Meeting Room Scheduler

Admins can monitor and maintain RX-PANEL Meeting Room Scheduler in their networks. For more information about RX-PANEL, see AudioCodes' website here.

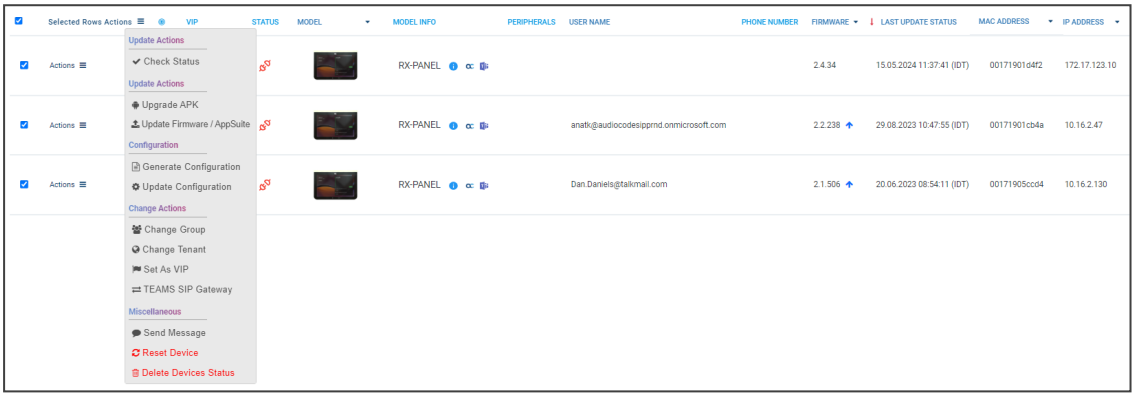
To get started with RX-PANEL, see the *RX-PANEL Quick Guide* available here.

➢ **To monitor and maintain RX-PANEL:**

1. Open the Monitor page (**Monitor** > **Dashboard** > **Devices Status**) and optionally enter a filter text for RX-PANEL.

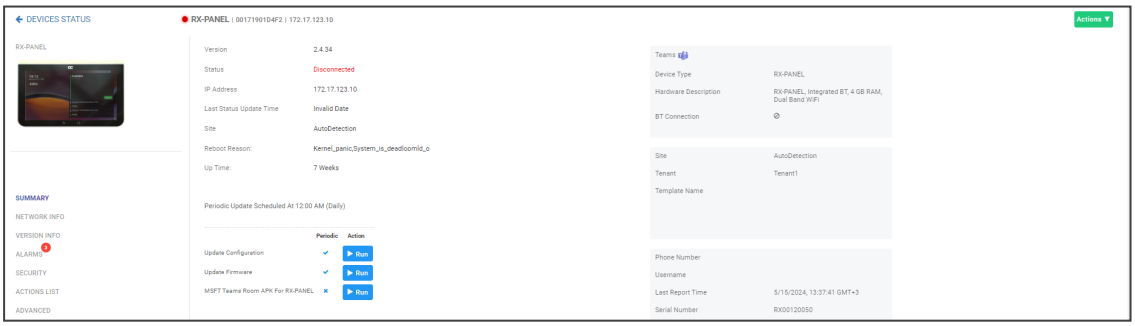


2. Click the Actions ☰ button adjacent to the device -OR- select *multiple* devices and then click the activated Selected Rows Actions ☰ button.



Device Manager supports bulk Android APK update. In the Devices Status page, select multiple Teams devices and then click the activated Selected Rows Actions ☰ button. From the popup menu, select the management action you require: **Upgrade APK** or **Update Firmware**; the procedures are the same as for the other managed devices described in this document.

3. Click the device icon or click **Actions** > **Show Info**.



4. Adjacent to 'Update Configuration' shown in the preceding figure, click **Run** to update the device with the latest .cfg file.

5. Adjacent to 'Update Firmware' shown in the preceding figure, click **Run** to update the device with the latest .img file. If there is no latest firmware to update, you'll be prompted to go to the Latest Versions page to download it (**Setup** > **Firmware** > **Latest Firmware Versions**).

6. Adjacent to 'MSFT Teams Room APK For RX-Panel' shown in the preceding figure, click **Run** to update the device with the latest APK file (Android Package Kit file format).

7. In the *upper pane* of the page shown in the preceding figure, view the device's version, status, IP address, Last Status Update Time and Site.

   In the *lower pane*, view information such as Tenant, Template Name and Serial Number.

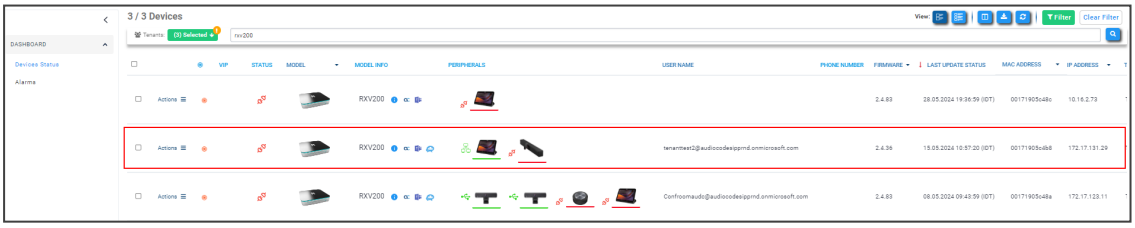
   On the right side of the page, optionally use the links to update configuration, update firmware, update Microsoft Teams APK, collect logs, and / or restart.

RX40 Audio Bar

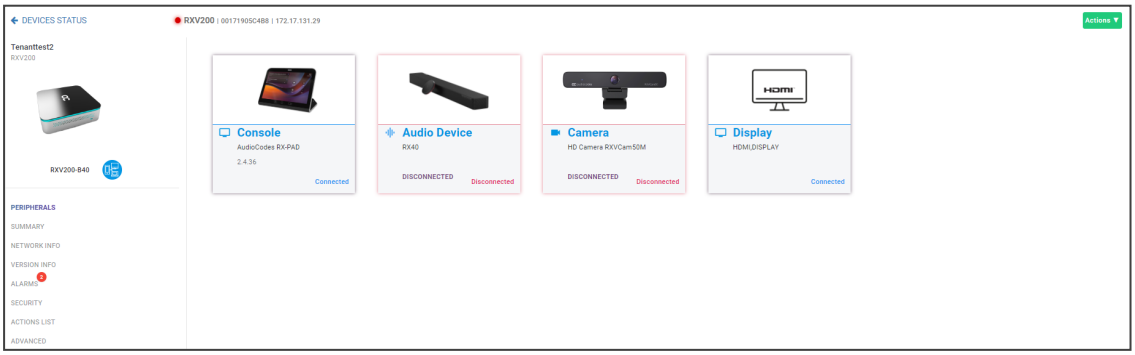
Admins can monitor and maintain the RX40 Audio Bar in their networks using Device Manager. RX-40 is a peripheral that is bundled either with RXV100 Windows MTR or RXV200 Android MTR. For more information about RX40, see AudioCodes website here. The figure below shows the RX40 with its two full duplex satellite microphones.

➢ **To monitor and maintain RX-40:**

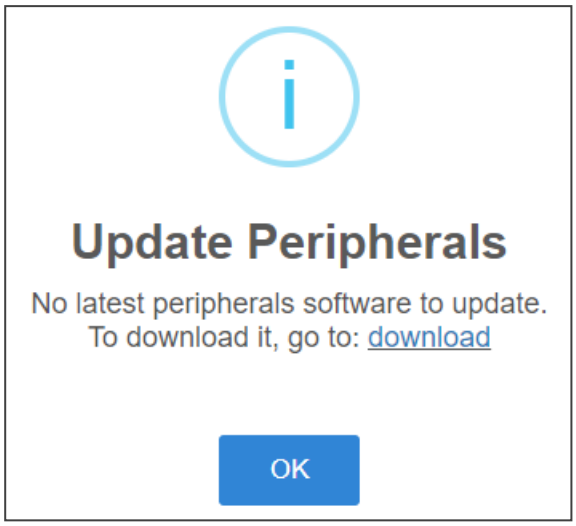
1. Open the Devices Status page (**Monitor** > **Dashboard** > **Devices Status**) and search for either the RXV100 Windows MTR or the RXV200 Android MTR.



2. View the RX40; the figure above shows RX-40 bundled with RXV200.
3. Click the RXV200 image icon or click **Actions** > **Show Info**.



4. Adjacent to 'Update Peripherals' shown in the preceding figure, click **Run**. If there is no latest peripherals software to update, you'll be prompted to go to the Latest Versions page to download it (**Setup** > **Firmware** > **Latest Firmware Versions**).



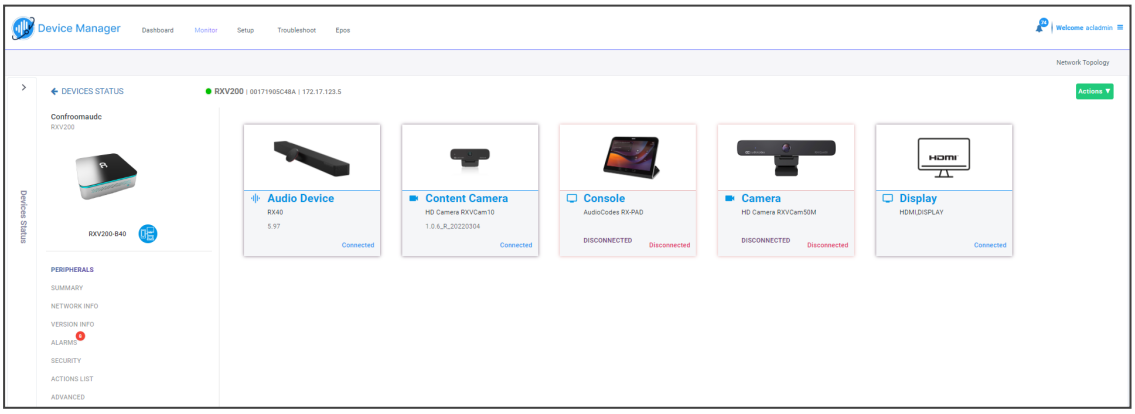
RXVCam10 Content Camera

Admins can monitor and maintain the RXVCam10 Content Camera in their networks using Device Manager.

➢ To monitor and maintain RXVCam10:

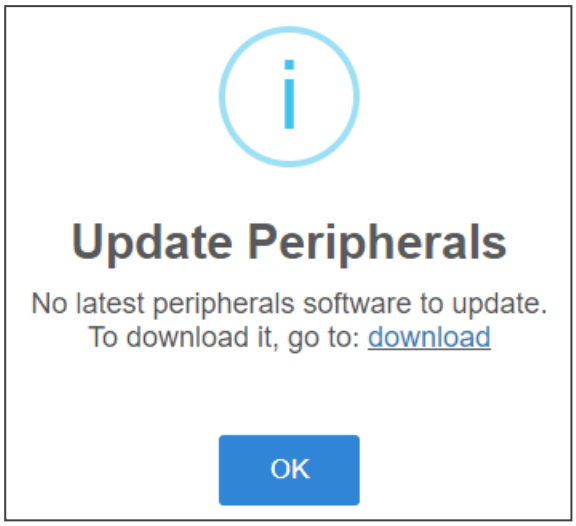
1. Open the Devices Status page (**Monitor** > **Dashboard** > **Devices Status**) and search for RXV200 (i.e., the device with which it is bundled).

2. View RXV200 displayed in the Monitor page and its peripheral, RXVCam10.
3. Click its icon or click **Actions** > **Show Info**.



4. Under the **Peripherals** tab, view RXVCam10 status ('Connected' in the figure above).

5. Under the **Summary** tab, adjacent to 'Update Peripherals', click **Run**. If there is no latest peripherals software to update, you'll be prompted to go to the Latest Versions page to download it (**Setup** > **Firmware** > **Latest Firmware Versions**).



Desktop | PC Meeting Room

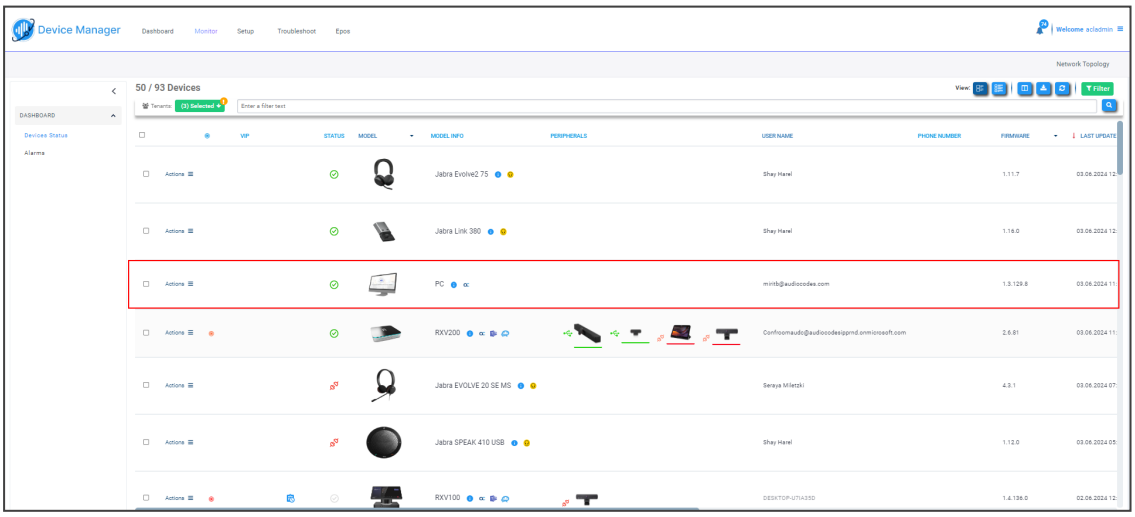
Device Manager enables admins to manage PC Meeting Room peripherals (for example):

- RX15 Speakerphone
- RXVcam10 Personal Webcam

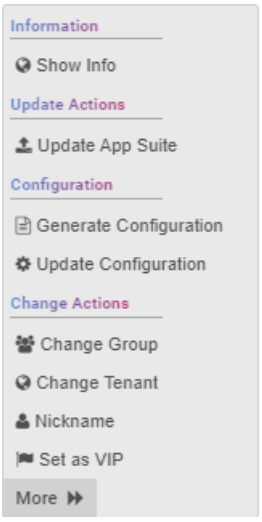
AudioCodes' AppSuite must be installed on the PC for firmware upgrade functionality.

➢ To upgrade the firmware:

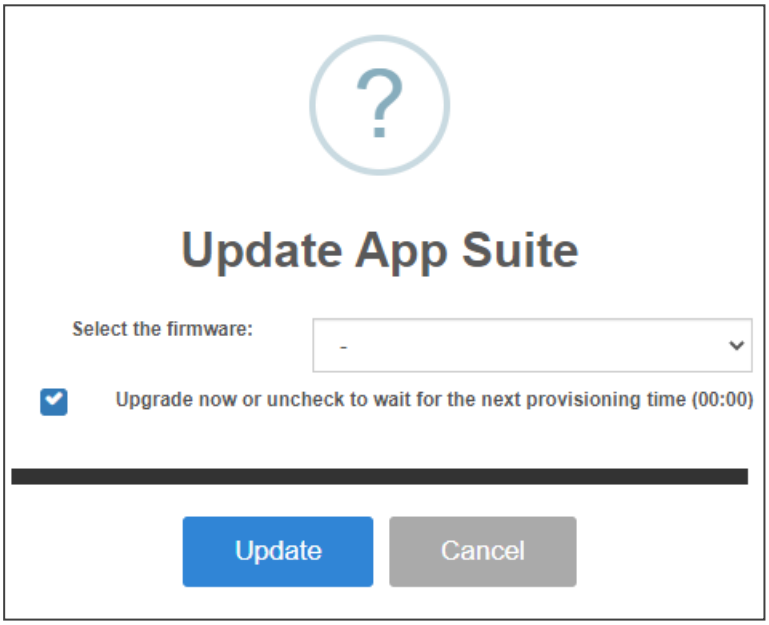
1. Open the Devices Status page (**Monitor** > **Devices Status**).



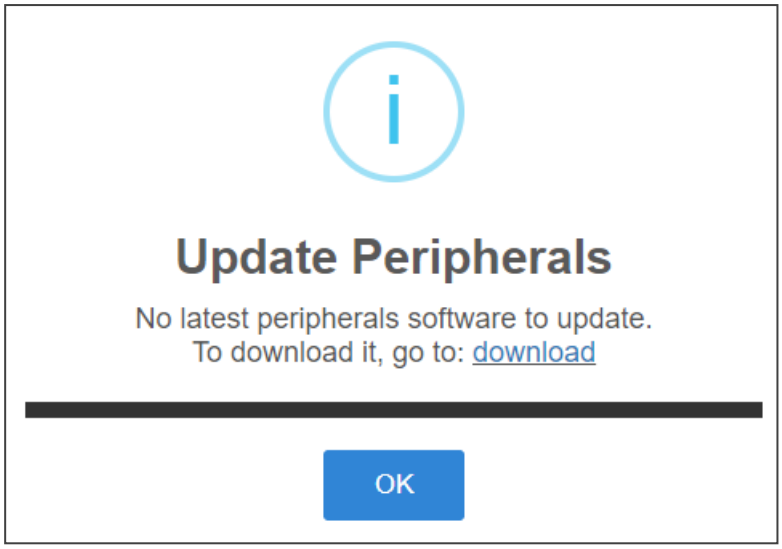
2. Click the **Actions** link adjacent to the PC to upgrade and from the menu that pops up, select **Upgrade Firmware/AppSuite**.



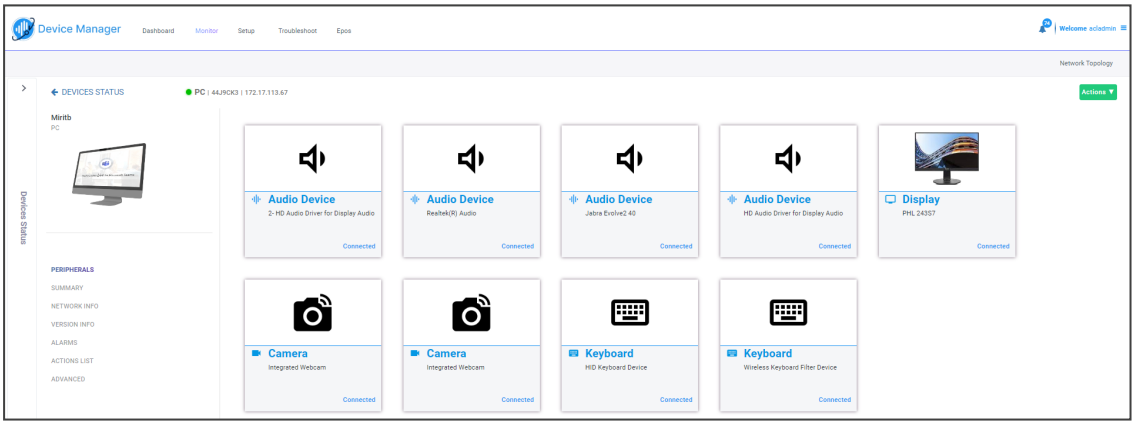
- Select **Update AppSuite** to update the app on the PC.



- Select **Update Peripherals** to update RX15 Speakerphone and RXVcam10 Personal Webcam.



3. Optionally, schedule periodic updates; select the **Show Info** option in the popup menu and then in the uppermost right corner of the Device Info page shown in the next figure, configure the periodic update and / or **Run** action.



Monitoring the Network from the Dashboard

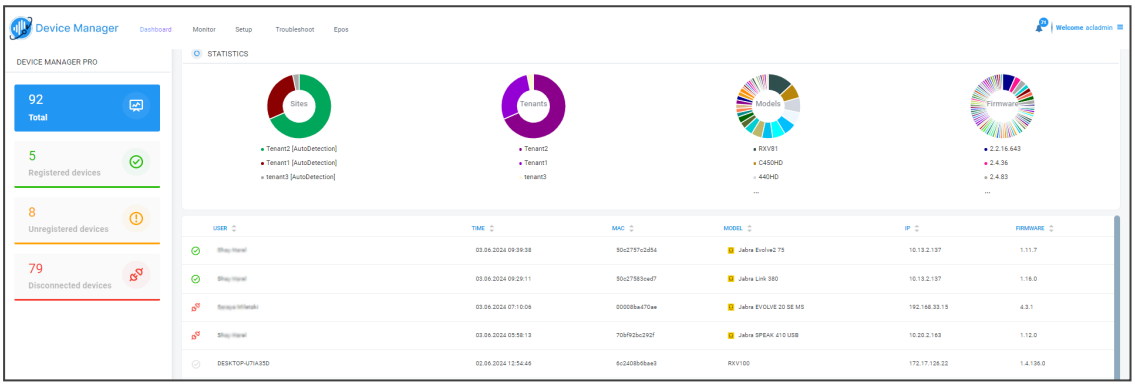
The Dashboard page lets you quickly identify

- which phones' firmware needs to be updated
  - Whenever AudioCodes adds an updated firmware version to the cloud, it's displayed here
  - All devices displayed can be synchronized with the latest firmware versions via the cloud
  - See also here for information about synchronizing per device via the 'Latest Versions' page
- which phones in the network are registered
- which phones in the network are non-registered
- # of registered and non-registered phones (in terms of SIP registration)

- % of registered phones
- MAC and IP address of each phone
- the time the information was reported
- the firmware version

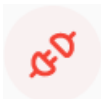
➢ To open the Dashboard page:

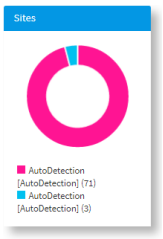
- The page opens by default (under the **Dashboard** menu) after starting the Device Manager application.



- If a Skype for Business IP phone is signed out (offline, or not registered), you'll view an icon of a gray tick inside a gray circle, and the 'User' column will be blank. It will be counted as a Non Registered Device.
- Point your mouse over the icon to view the 'offline' tooltip.
- If the phone is not registered, you'll view a red triangle enclosing an exclamation mark.
- View the status thumbnails. Use this table as reference.

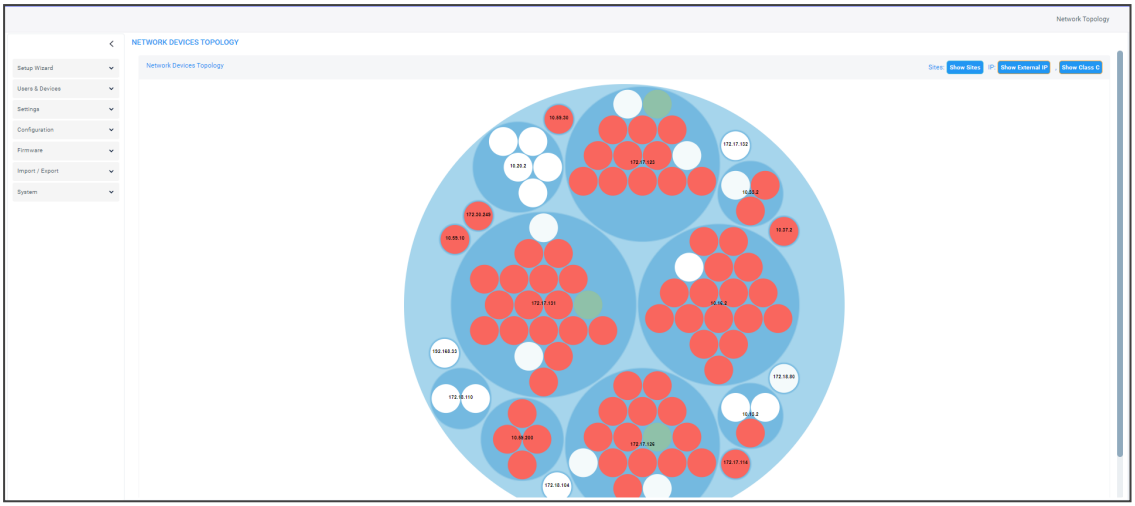
Table 5-1: Dashboard – Status Thumbnails

Status Thumbnail	Description
	Indicates the number of registered devices. Click **MORE DETAILS...** to quickly access the Devices Status page.
	Indicates the number of unregistered devices. Click **MORE DETAILS...** to quickly access the Devices Status page.
	Indicates the number of disconnected devices. Click **MORE DETAILS...** to quickly access the Devices Status page.

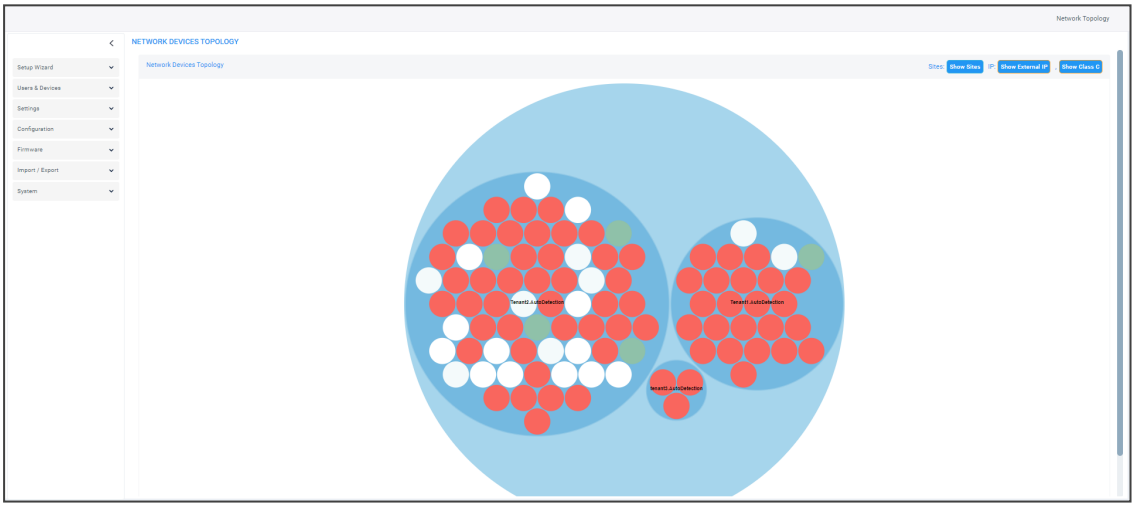
Status Thumbnail	Description
	Indicates the number of devices running the version stated above it. Click **MORE DETAILS...** to quickly access the Devices Status page.
	Pie chart showing the number of *devices per tenant* that are registered. Hover over a segment of the pie to view the tenant's name and the number of devices registered under it. Click a segment of the pie to open the Devices Status page displaying that tenant and the devices registered under it.
	Pie chart showing the number of *devices per site* that are registered. Click a segment of the pie to open the Devices Status page.
	Pie chart showing how many *phones of each model* are registered. Click a segment of the pie to open the Devices Status page.
	Pie chart showing how many *phones of each firmware version* are registered. Click a segment of the pie to open the Devices Status page.

Viewing Network Topology

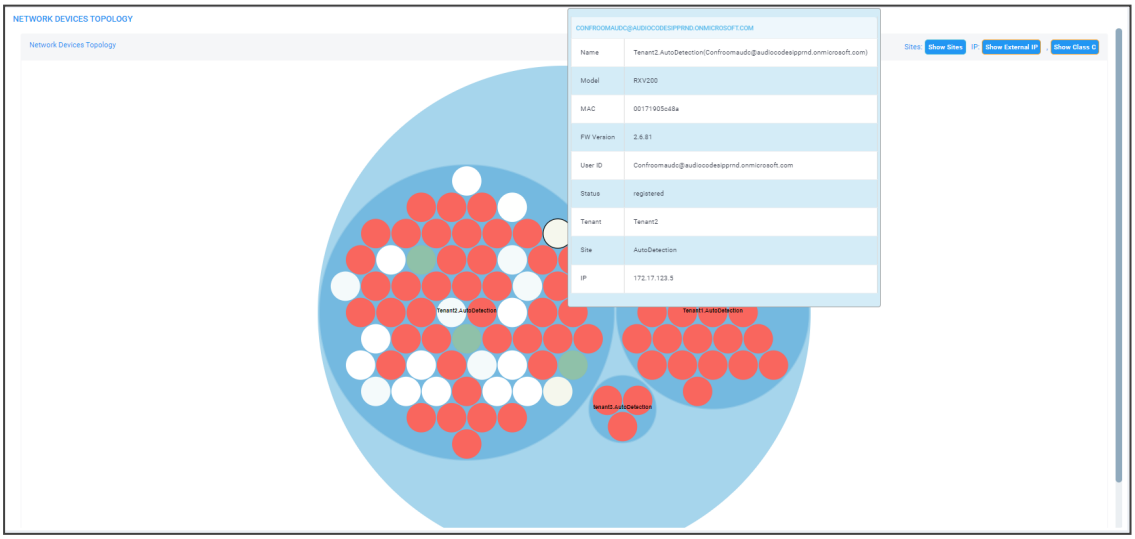
Located in the uppermost right corner of most Device Manager pages, the **Network Topology** link enables admins to view devices in their IP telephony networks according to sites, internal or external IP address, or IP address class.



In the Network Devices Topology page that opens, click the **Show Sites** button to display the Network Devices Topology page *according to sites*.



The preceding figure shows multiple sites in a single-tenant network. The page enables admins to determine at a glance which sites are causing traffic overload (for example). Admin can point their mouse at a device to view information on that device displayed in a tool tip.



Click the **Show Internal IP** | **Show LAN IP** button to display devices in the page according to *internal IP address* or *LAN IP address*. Each device in the network has an *internal* IP address - the IP address of the device located *within the enterprise network*. Some devices also use a LAN IP address - the IP address of a router via which calls transit (for example). The button displays devices according to the administrator's choice.

Click the **Show Class B** or **Show Class C** button. Every IP address in quad-dotted notation comprises four 'classes'. This button enables displaying devices according to IP addresses of Class B or Class C.

- **Show Class B** shows the first *two* classes, for example, 10.10
- **Show Class C** shows the first *three* classes, for example, 10.10.10.

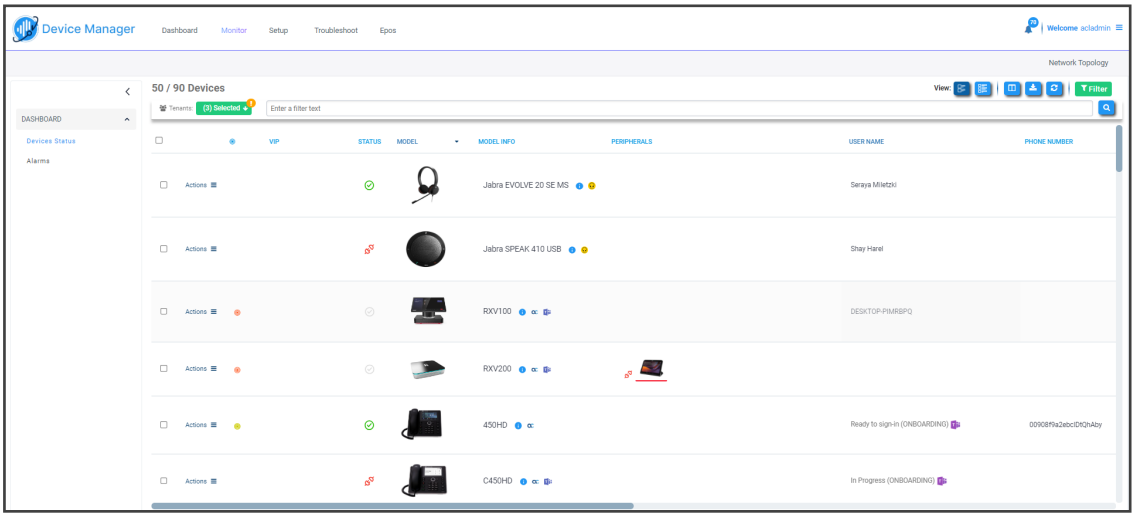
A higher number of devices will be displayed if **Show Class B** is selected than if **Show Class C** is selected since more devices' IP addresses begin with 10.10 than with 10.10.10.

Checking Devices Status

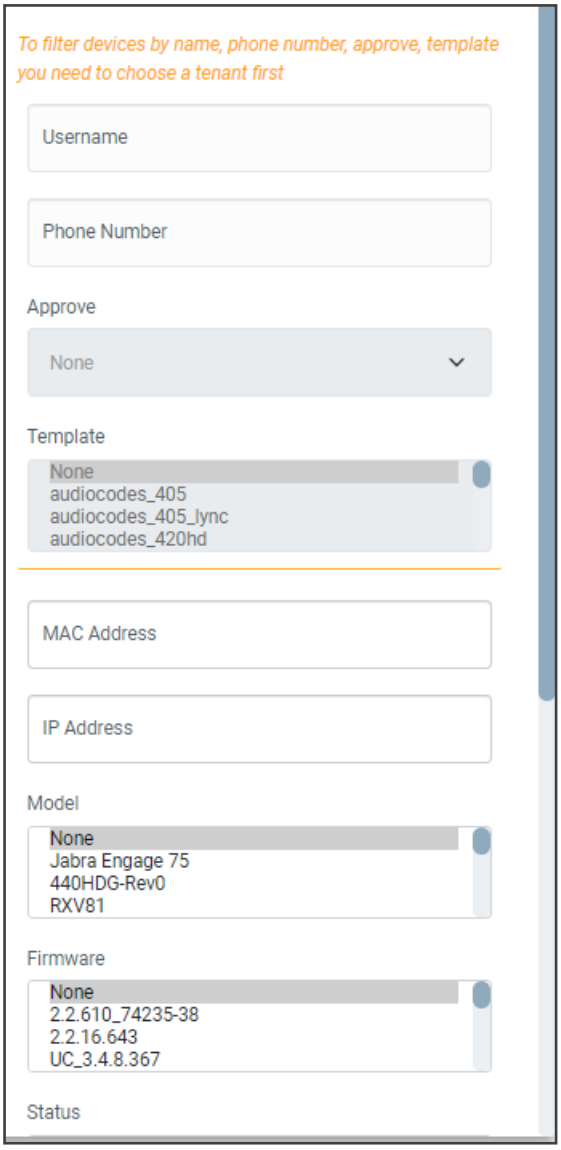
The Devices Status page enables admin to check a device's status, for example, to determine whether a device is connected or not, as well as to perform actions on an individual device or on multiple selected devices.

➢ To check a device's status:

1. Open the Devices Status page (**Monitor** > **Dashboard** > **Devices Status**).



2. [Optionally] Click **Filter**; the filter lets you view specific information in the page, preventing information that is irrelevant to you from cluttering the page.



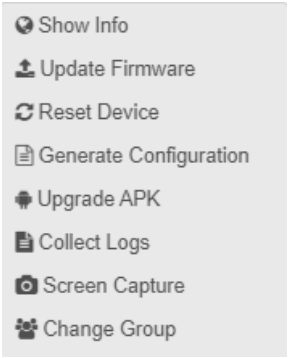
3. [Optionally] Filter per user, phone #, MAC, IP address, model, version, status (registered, offline or disconnected), approved or approval pending, users with multiple devices, VIP Devices, tenant, site, group, template or maximum devices shown in the page.
4. View in column 'USB Headset Type' if a headset is connected to a phone's USB port; in addition, column 'IPP Model' displays the USB icon.
5. View in column 'HRS Speaker Model' the Huddle Room Solution model (457 or 458) if an HRS is connected; in addition, you can view in column 'HRS Speaker FW' the speaker firmware version.
6. Non-Skype for Business phones are displayed differently to Skype for Business phones.
   - The format of 'User Agent' for non-Skype for Business phones is for example **AUDC-IPPhone/2.0.4.30 (430HD; 00908F4867AF)** while the format for Skype for Business phones is **AUDC-IPPhone-430HD_UC_2.0.7.70/1.0.0000.0**
   - Only Skype for Business phones are displayed under the 'Location' column; non-Skype for Business phones are not displayed under the 'Location' column.

7. View in the column 'Model Info' the entries **Spectralink 8440, Poly Trio 8800**, **Poly VVX**, **Poly CCX 500/600**, etc. if these models are connected; they can be monitored, configured and templates can be mapped.

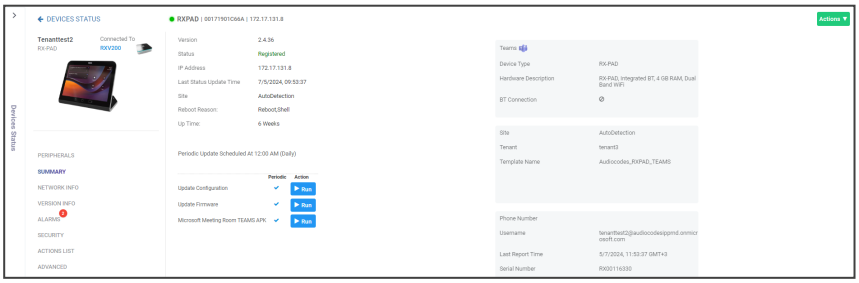
   You can also view in the 'Model Info' column an **i** icon. Point your mouse over it to display the device's vital hardware specifications:

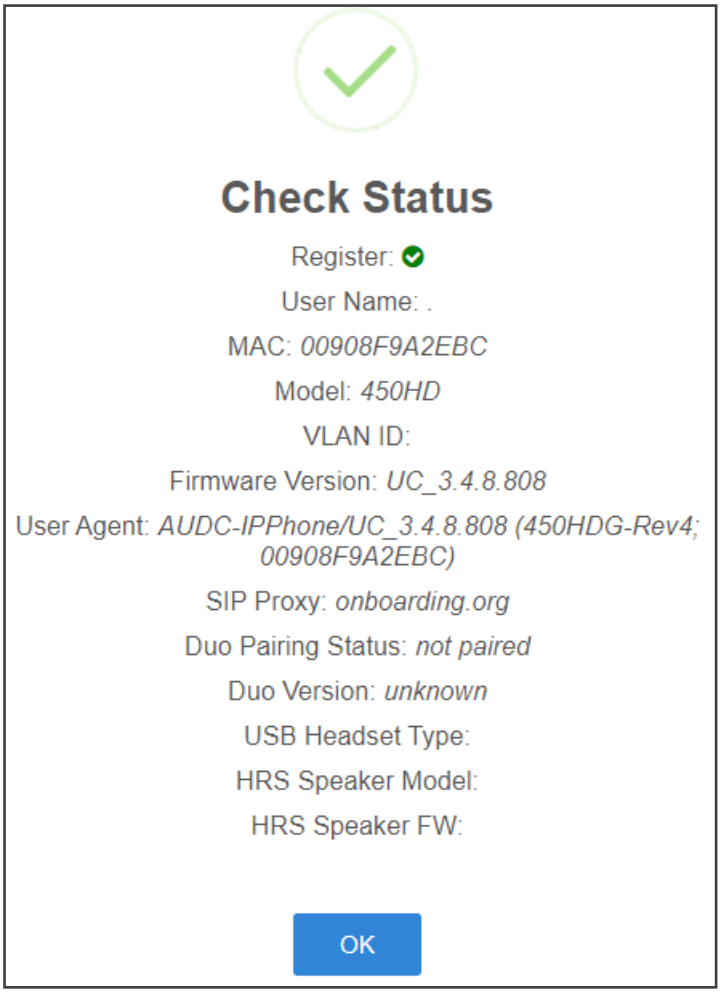
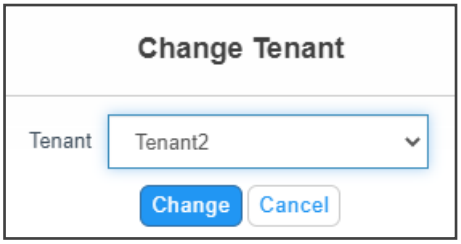
8. [Optionally] Click the **Export the devices to CSV file** button to export all entries in the page - or a selected list of entries - to a csv file. This facilitates inventory management; it lets you easily obtain a list of phone MAC addresses or serial numbers, for example. After generating a csv file, a download option is displayed in the lower-left corner. You can save the csv file or open it directly in Excel which displays the same information as that on the page.

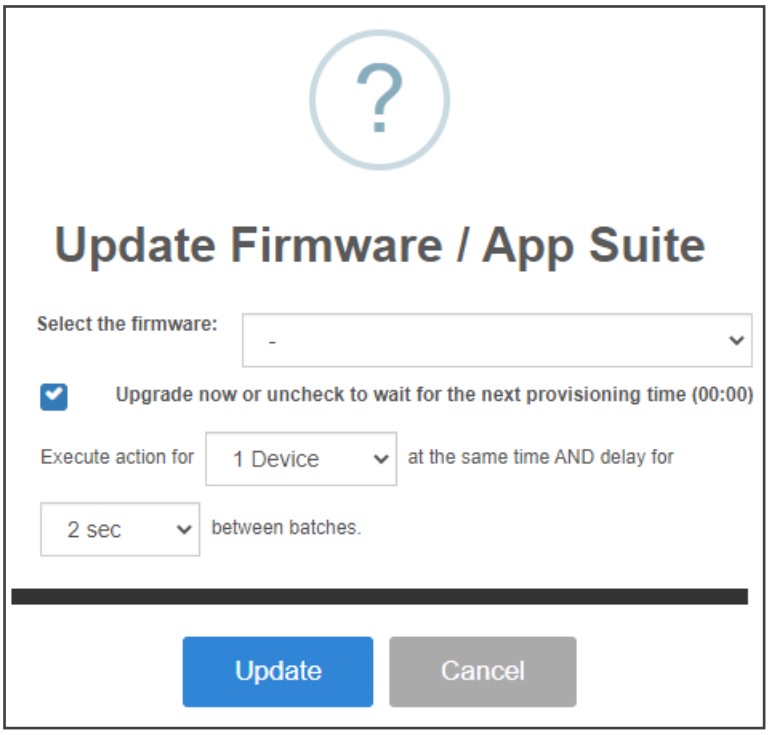
9. [Optionally] Click **Actions** adjacent to a device.

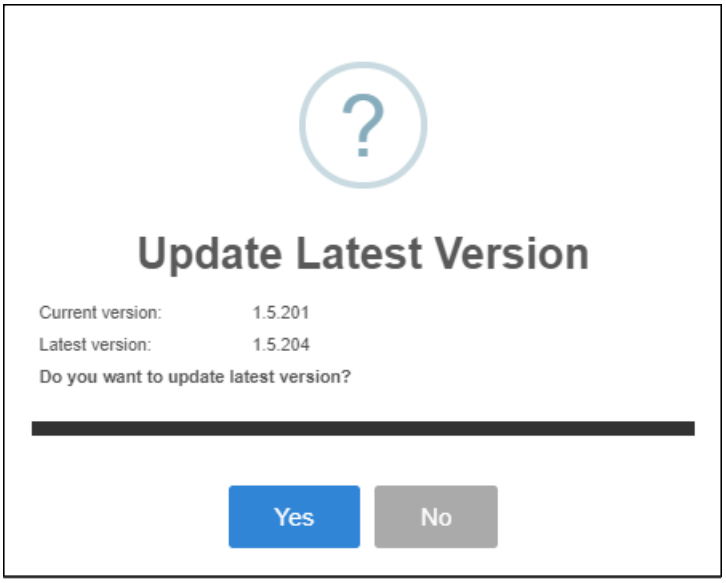
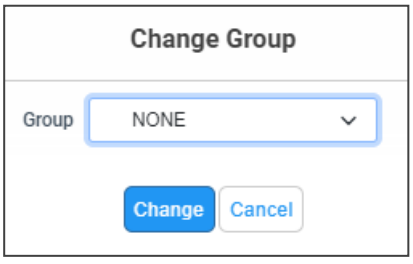


- The Actions menu changes from device to device
- The preceding figure shows the Actions menu for RXV200 MTR

Action	Description
Show Info	Displays all the information about the device needed by admin. The page differs from device to device. The following figure shows RX-PAD Room Controller.  All information about the device is available under the left tabs

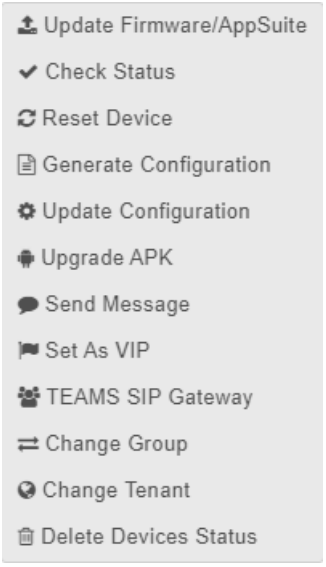
Action	Description
	Peripherals, **Summary**, **Network Info**, **Version Info**, **Alarms**, **Security**, **Actions List** and **Advanced**. These tabs differ from device to device.
Collect Logs	Enables admin to get logs without needing to go to the phone. See Collecting Logs on page 125 for more information.
Check Status	[Only applies to UC phones] Select the 'Check Status' option and after confirming your request, view the following screen (for example): 
Change Tenant	Select the 'Change Tenant' option.  From the dropdown, select the tenant, and then click **Change**.

Action	Description
Update Firmware	You can update firmware per device, or for multiple selected devices.  The figure above shows the screen that opens after selecting *multiple* devices. The screen for a *single* device is *identical* but *without* the option to execute the action in batches. From the dropdown, select the firmware file, and then click **Update**; the firmware file is updated. You can simultaneously update the device's configuration file. If you select *multiple* devices and then click the **Selected Rows Actions** link in the title bar to choose 'Update Software' from the drop-down, the screen (as shown in the figure above) will include the option to ■ update firmware simultaneously for a batch of devices, each batch containing 5 | 10 | 20 | 30 | 50 | 100 devices ■ configure a 0 second | 2 second | 5 second | 10 second | 30 second | 2 minute | 5 minute delay between batches Note that if the ↑ icon is displayed in the 'Firmware' column adjacent to a listed device in the Devices Status page, it indicates that that device's firmware is not the latest firmware available; you can click the icon to upload the device's latest firmware.

Action	Description
	
Open Web Admin	Opens the Web interface (see the device's *Administrator's Manual*). By default, the Web interface opens in HTTPS.
Nickname	Enables you to provide a nickname for the enterprise employee to facilitate more effective user and phone management.
Reset Phone	Sends a reset command to the selected device/s. Note that some phone models wait for the user to finish an active call, while others may perform an immediate restart.
Generate Configuration	Generates the device's configuration file according to its tenant, site and template. The user configuration will also be generated in case it will be needed.
Change Group	Enables you to add an endpoint to an endpoints group or to change endpoints groups. Endpoints groups are added in OVOC (see the *OVOC User's Manual* for more information). The feature benefits the customer who wants (for example) 10 of 500 phones in a site in the enterprise organized in a group for a software upgrade to apply exclusively to those 10 phones. The groups are across sites, within a specific tenant. After clicking the **Actions** menu option, this prompt is displayed: 

Action	Description
	■ From the 'Group' drop-down, select the group and click **Change**. ■ Configure an endpoints group in the Group Configuration page as shown here.
Update configuration	Sends a command to the phone to check whether there is a new configuration file to upload and updates the phone after a configurable 'Delay Time' (Default = 2 seconds).
Send Message	Lets you send a message to the screen/s of the selected device/s. Enter the message in the 'Text' field. You can configure for how long the message will be displayed in the screen/s.
Set as VIP	Enables admins to configure the phone as a VIP phone; VIP phones feature a different disconnect time interval and support disconnect / unregistered alarms. A phone configured as a VIP phone is typically a Common Area Phone (CAP) located in the lobby of an enterprise, or a conference phone located in an enterprise's meeting rooms. It's important that it be continuously connected hence the different disconnect time interval and the disconnect / unregistered alarms.
Delete Devices Status	Deletes the devices from the Devices Status table.
Switch to UC	Applies to the two flavors of the C450HD phone: Microscope Teams Native and Microscope Teams Compatible. Select this option to switch the C450HD phone from the one flavor to the other.
Telnet	Enables admin to send Telnet (CLI) debug commands to the phone for debugging purposes. Important: For this feature to function, Telnet must be enabled on the device. You can enable Telnet from the Web interface's Telnet page (**Management** > **Remote Management** > **Telnet**).

10. [Optionally] Select multiple rows and then click the activated **Selected Rows Actions** link. The following menu is displayed when multiple Android devices are selected.



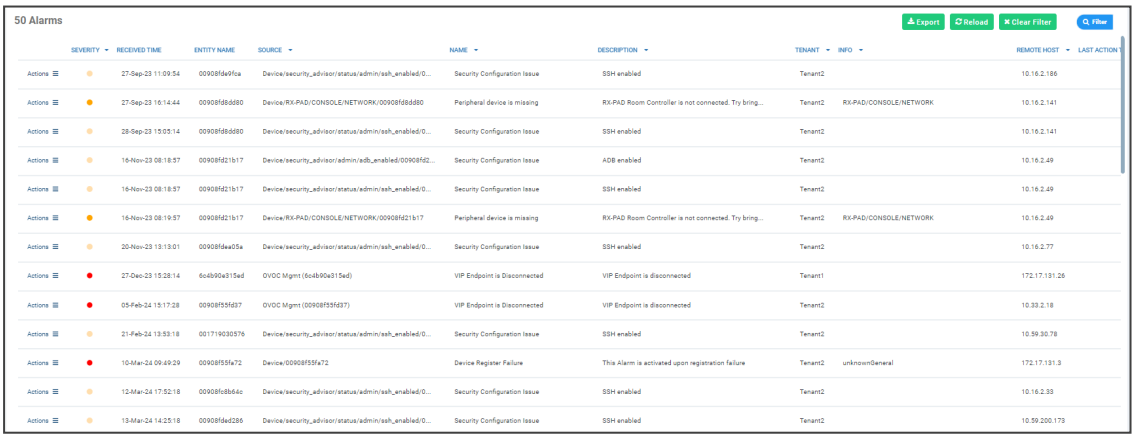
See the table above for descriptions. Any action you choose will apply to all selected rows. For example, select rows, click the **Selected Rows Actions** link, and then select the **Update Firmware** option; all selected devices will be updated with the firmware file you select.

Monitoring Alarms

Admin can monitor alarms and correct failures before users encounter them, maintaining high productivity and business without interruption.

➢ To monitor alarms:

1. Open the Alarms page (**Monitor** > **Dashboard** > **Alarms**).



> Devices send alarms via the REST protocol. They're forwarded by the AudioCodes Live Cloud platform as mail, SNMP traps, etc.

2. View in the page:
   - each device alarm in the network
   - a description of each alarm

- MAC address of the device (source)
- alarm severity
- Remote Host IP
- last action time
- date and time of receipt of the alarm

Device Manager LC displays active alarms, not historical alarms.

Red indicates a severity level of Critical

Orange indicates a severity level of Major

After an alarm is cleared, it disappears from the Alarms page.

Searching for Alarms

You can search for alarms in the Alarms page. The 'Search' field enables the functionality. You can search by

- alarm name
- a device's MAC address
- a device's IP address

Performing a Delete Action on an Alarm

You can perform a delete action on alarms in the Alarms page. Click the **Actions** link next to the alarm to delete and from the popup menu select **Delete Alarm**.

Maintaining Users

The Manage Users page lets you maintain users. You can

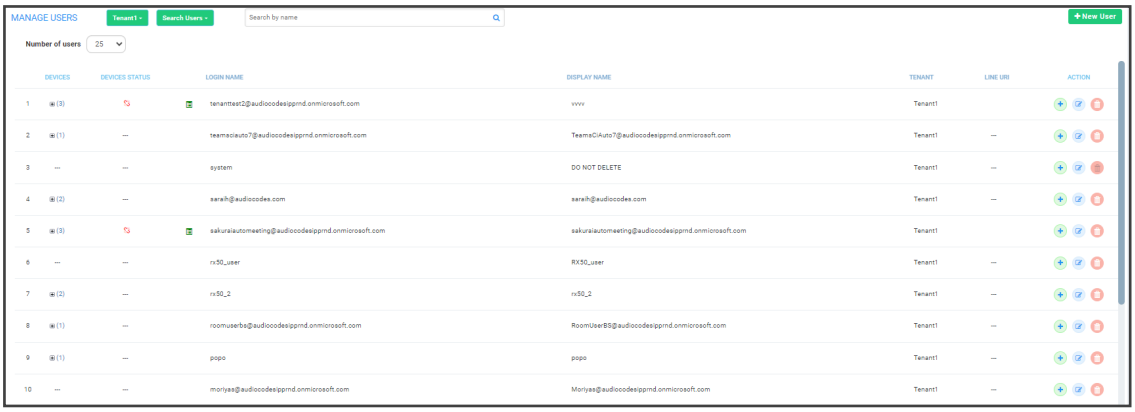
- search for a user/device
- add a user
- add a device to a user
- edit user/device
- view device status
- delete a user/device
- search for a device by tenant
- search for a device by name

Searching for Users | Devices

You can search for a user in the Manage Users page.

➢ To search for a user:

1. Open the Manage Users page (**Setup** > **Users & Devices** > **Manage Users**).



2. From the 'Tenant' drop-down, select a tenant in which to search. This narrows the search.
3. From the 'Search Users' drop-down, select **Search Users** (default) or **Search Users and Devices**.
4. [If you select **Search Users**] In the 'Search by name' field, enter the name of the user you're trying to locate.
5. [If you select **Search Users and Devices**] In the 'Search by name and device' field, enter the name of the user you're trying to locate or the MAC address of the device you're trying to locate.
6. From the 'Number of users' drop-down, select the number of users you want displayed per page. The default is 25.

Adding a User

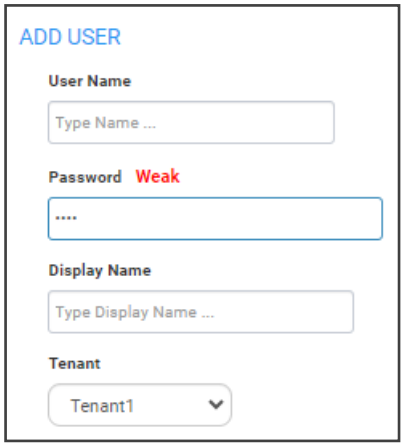
You can add a user to Device Manager. Before adding phones, you need to add users.

➢ To add a user to Device Manager:

1. Open the Manage Users page (**Setup** > **Users & Devices** > **Manage Users**) and from the **Select Tenant** drop-down, choose the tenant.

> Tenant(s) must first be defined in OVOC. See the *One Voice Operations Center User's Manual* for more information.

2. Click the **+New User** button located in the uppermost right corner of the page.



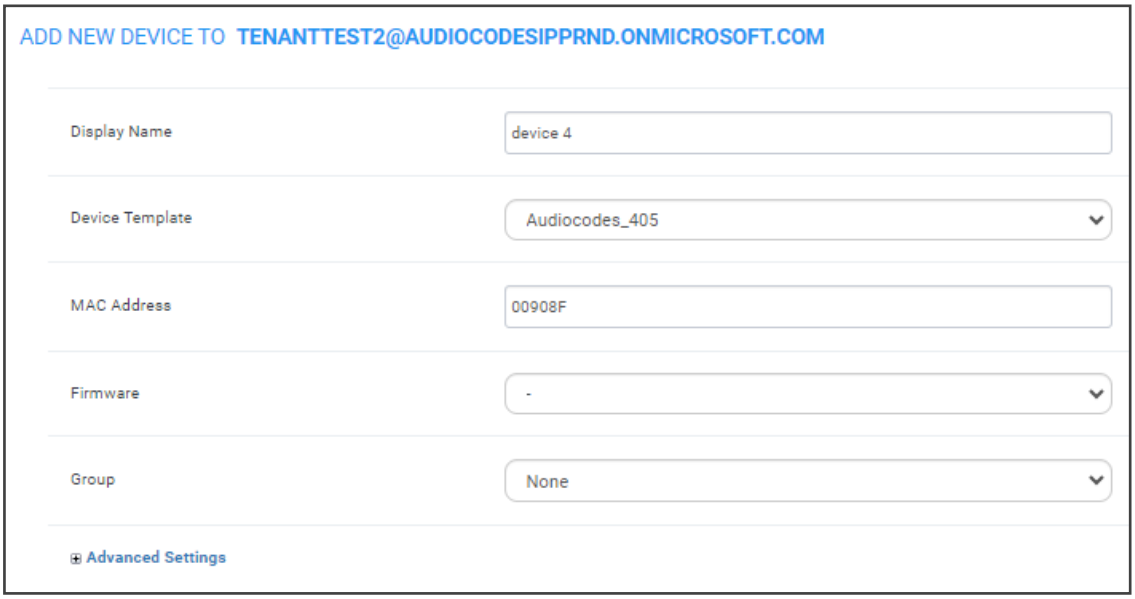
3. Define a name and (strong) password for the user.
4. Define the 'Display Name' and select a tenant from the ' Tenant' dropdown.
5. Click **Submit**; you're returned to the Manage Users page. Locate the added user.

Adding a Phone

You can manually add a single phone to the server.

➢ **To add a phone:**

1. In the Manage Users page (**Setup** > **Users & Devices** > **Manage Users**), click **+** under the **Actions** column in the row of the listed added user.



2. Enter the 'Display Name', i.e., the device's name to be displayed in Device Manager.
3. From the 'Device Template' dropdown, select a template.
4. Enter the 'MAC Address'. MAC prefix format example: **mac": "00171905c48a**

- AudioCodes MAC addresses' prefixes can be one of the following:
  - ✓ "00908F" -or-
  - ✓ "001719"
- Prior to Version 8.2.3000, AudioCodes had only "00908F"
- From Version 8.2.3000 and later, AudioCodes has "00908F" as well as "001719".
- Each vendor has its own MAC prefixes.

5. From the 'Firmware' dropdown, select the firmware relevant to the phone.
6. [Optional] Expand **+Advanced Settings**.
   - From the 'Devices Language' dropdown, select the language you want the phone interface to display.
   - From the 'VLAN Discovery mode' dropdown, select Manual / CDP / LLDP / CDP_LLDP. See here for more information.
7. Click **Submit** and then click **Back** to see the added device in the Manage Users page under the Devices column (click **+**).

Editing a User

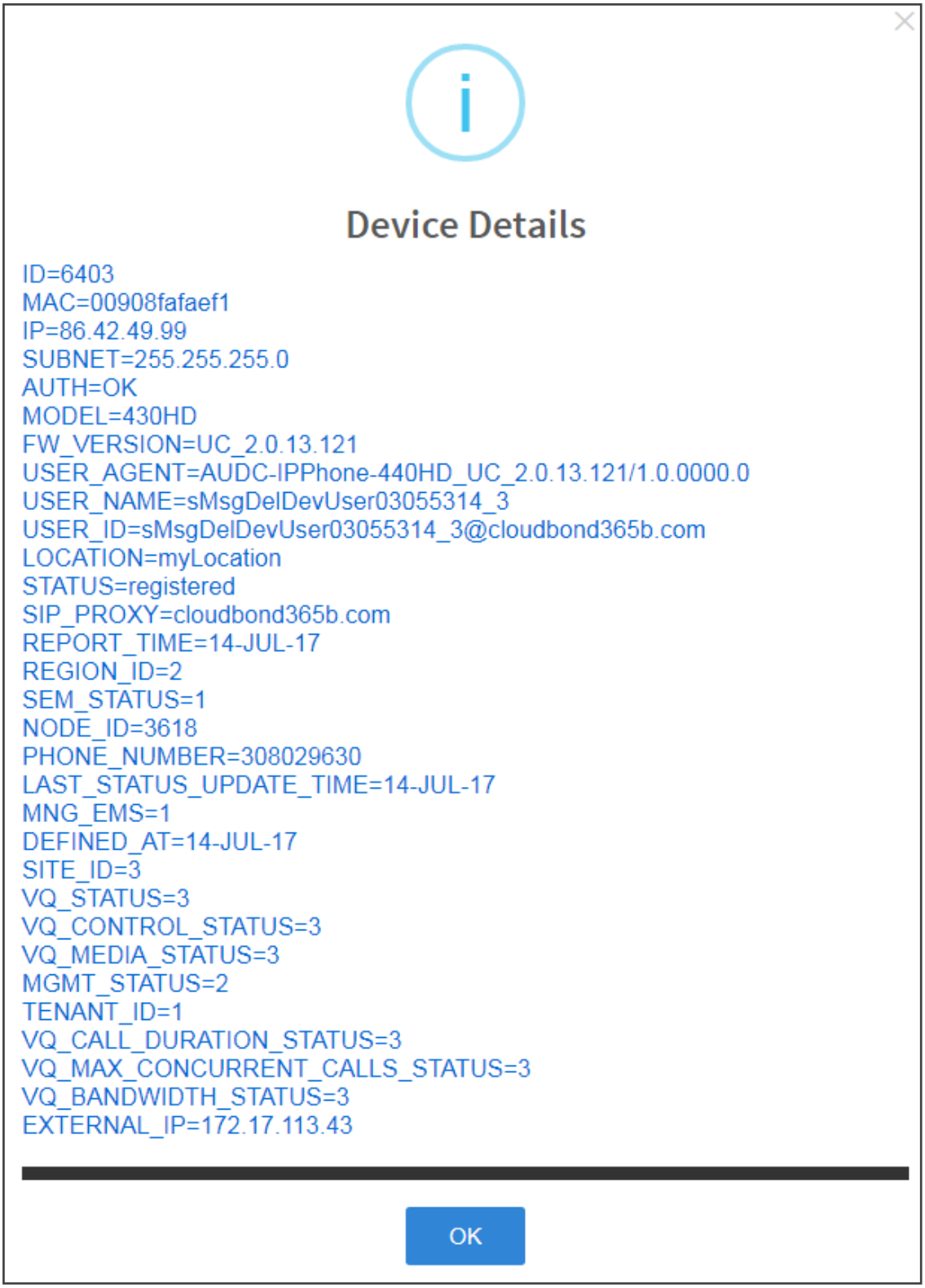
You can edit a user if (for example) they relocate to another tenant or if they are given another phone.

➢ **To edit a user:**

1. Click the **Edit** button in the row adjacent to the user; the Edit User screen opens.
2. Edit the same fields as when adding the device.

Viewing Device Status

You can quickly assess a device's status from the Manage Users page by clicking the icon in the ' Status' column.



Deleting a User

You can delete a user if, for example, they leave the company.

➢ **To delete a user:**

- Click the **Delete** button in the row adjacent to the user; the user and device are removed.

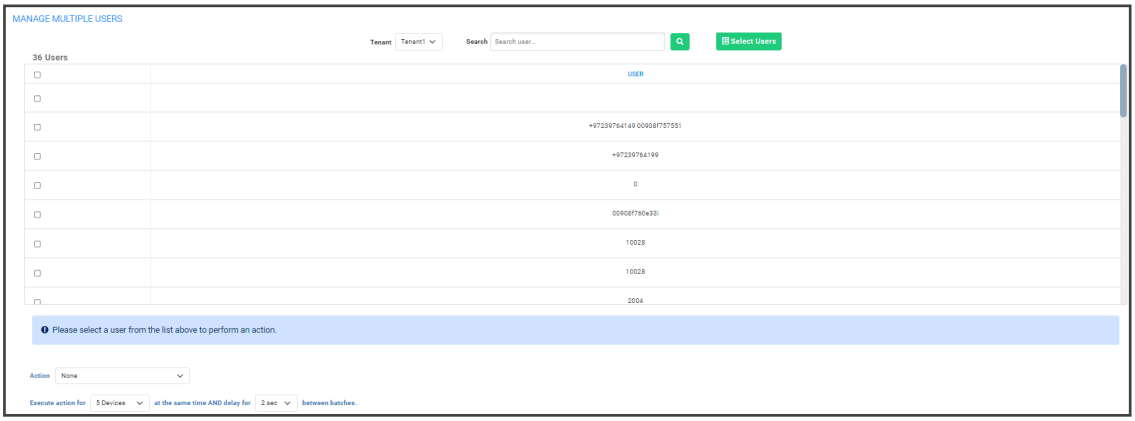
Managing Multiple Users

The Manage Multiple Users page enables you to perform an action on a single user or on multiple users simultaneously:

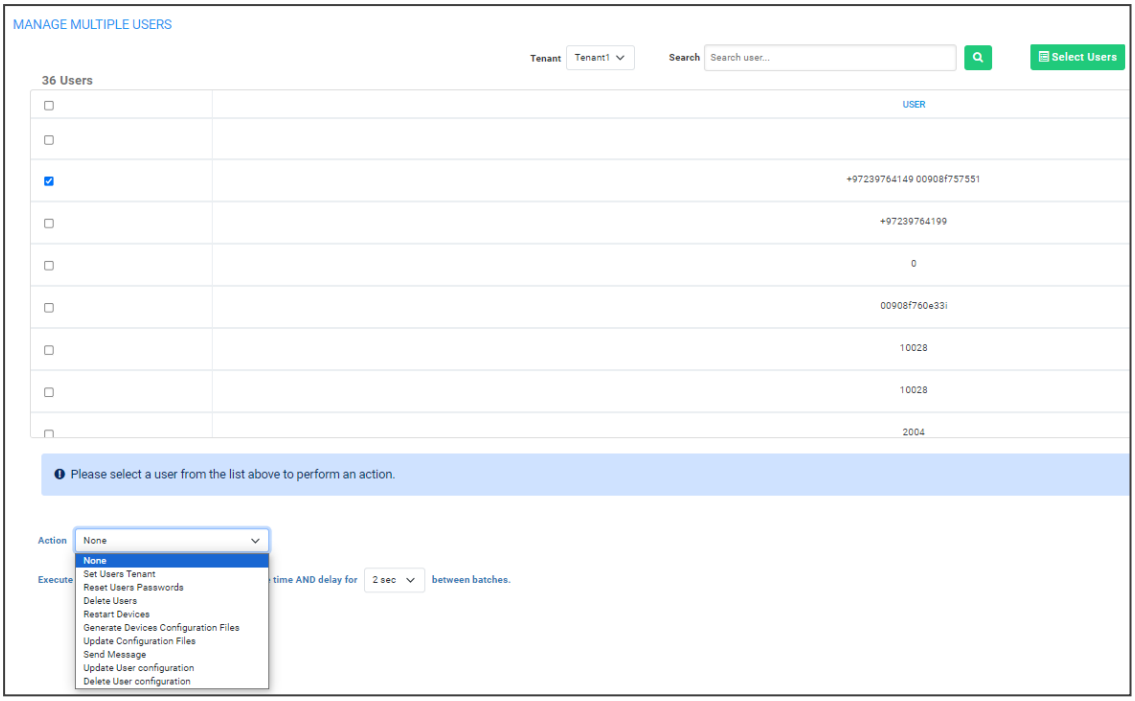
- set users tenant
- reset users passwords
- delete users
- restart devices
- generate devices configuration files
- update configuration files
- send a message to multiple phones
- update user configuration
- delete user configuration

➢ **To manage multiple users:**

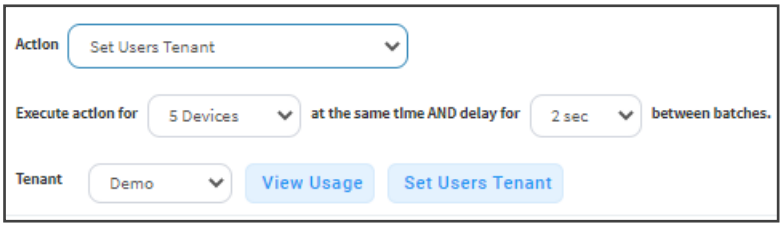
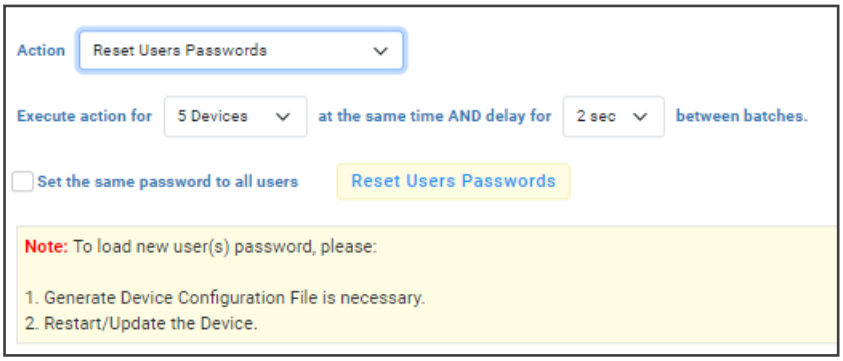
1. Open the Manage Multiple Users page (**Setup** > **Users & Devices** > **Manage Multiple Users**).

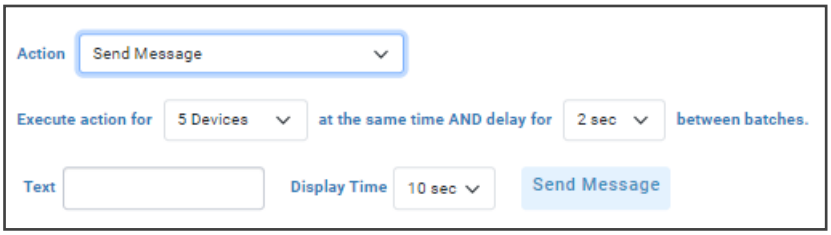


2. From the 'Tenant' drop-down, select the tenant under which the user is located, to narrow the search.
3. Search for the user | select multiple user(s) on whom to perform an action.
4. From the **Action** dropdown, select the action.



5. Use the table below as reference.

Action	Description
Set Users Tenant	 Click the **Set Users Tenant** button and in the confirmation prompt click **OK**; the tenant for the users selected is set.
Reset Users Passwords	 Resets user(s) passwords. A random password is generated for each user. To generate a single password for *all* selected users, select the **Set the same password to all users** option. To load the new user(s) passwords: ■ Perform action **Generate Devices Configuration Files** (see

Action	Description
	■ Perform action **Restart Devices** (see description below)
Delete Users	Deletes users and applies a configurable 'Delay Time' (Default = 2 seconds) after each delete is performed.
Restart Devices	Restarts devices. A reset command is sent to all selected devices. The commands are sent in batches; each batch contains 5 devices with a delay of 2 minutes between each batch. From the dropdown, choose the type of restart: ■ Graceful (default) ■ Force ■ Scheduled Before restarting, some models wait for the user to finish an active call. Other models restart immediately.
Generate Devices Configuration Files	Generates new configuration files. Updates each device with the newly generated configuration files after a configurable 'Delay Time' (default = 2 seconds) - if you select the **Updating Devices and restarting Devices after generating files** option. You can generate a private configuration file per user group, device group, or specific tenants.
Update Configuration Files	Updates each device after a configurable 'Delay Time' (default = 2 seconds).
Send Message	Enables you send a message to the screens of all user devices selected. Enter the message in the 'Text' field. You can configure the length of time the message will be displayed in the screens. Phones beep to alert users when messages come in. 
Update User Configuration	 Configures the values that will be added to the *mac.cfg* file for the selected users. Note that you can copy from one user to multiple users.

Action	Description
Delete User Configuration	Deletes the user configuration for the selected users.

The page also enables you to

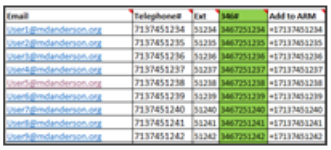
- filter per tenant before selecting users on whom to perform an action
- configure performing the action on a batch of 1 | 5 | 10 | 20 | 30 | 50 | 100 devices simultaneously
- configure a 0 second | 2 second | 5 second | 10 second | 30 second | 2 minute | 5 minute delay between batches

Applying a Configuration to a List of Users

A configuration can be applied to a *list of users* to move (for example) those users from one VoiceMail platform(Microsoft Exchange, for example) to another third-party VoiceMail platform (for example, Mutare Voice).

➢ **To move a select group of users from one VoiceMail platform to another (for example):**

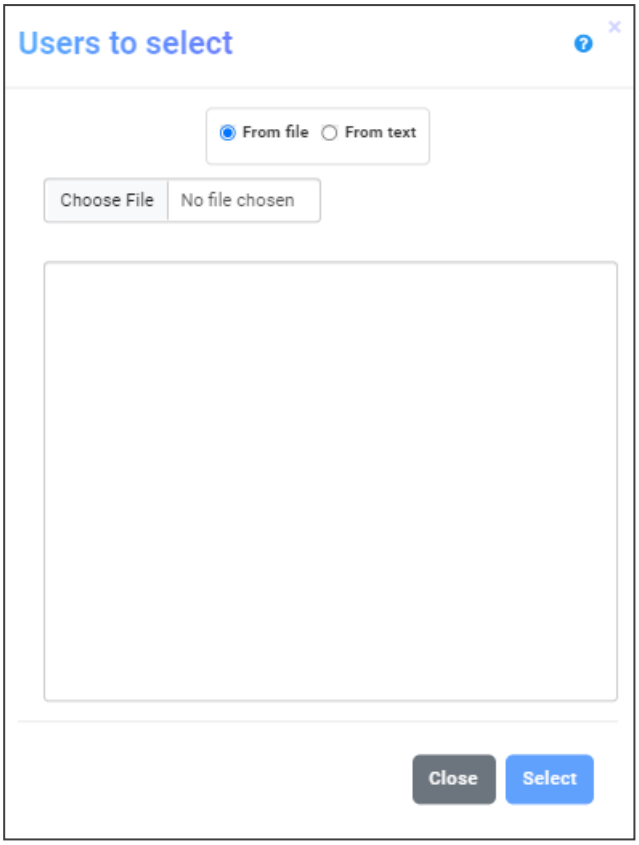
1. Obtain the list of names of those users who are to be moved (input list / raw data) as a txt or xls file.



2. In Excel, filter the file, i.e., remove all columns except the 'Users' column.

- The user is their email address in the enterprise.
- The configuration file will be applied only to phones belonging to *these* users.

3. Open the Manage Multiple Users page (**Setup** > **Users & Devices** > **Manage Multiple Users**) and then click the **Selected Users** button.



4. Import the input list / raw data into Device Manager:
   - Select the **From file** option (default) and then click the activated **Choose File** button and navigate to the txt or xls file containing the input list (the raw data) of the users to be moved, which you created in the first two steps of this procedure -OR-
   - Select the **From text** option and then copy-paste the contents of the txt or xls file containing the input list (the raw data) of the users to be moved, into the pane located below the option.
5. Click the **Select** button.

- The same user can have multiple devices.
- The configuration file is static data; it's the same for all devices.
- When moving users to a new VoiceMail platform as shown in the example here, the VoiceMail button on the phones associated with these users must also be updated (with the new VoiceMail platform); the change must take place within the same time frame as the move of the users to the new VoiceMail platform.

Maintaining Multiple Devices

The Manage Multiple Devices page lets you perform a single operation on all or on many user devices. The page lets you

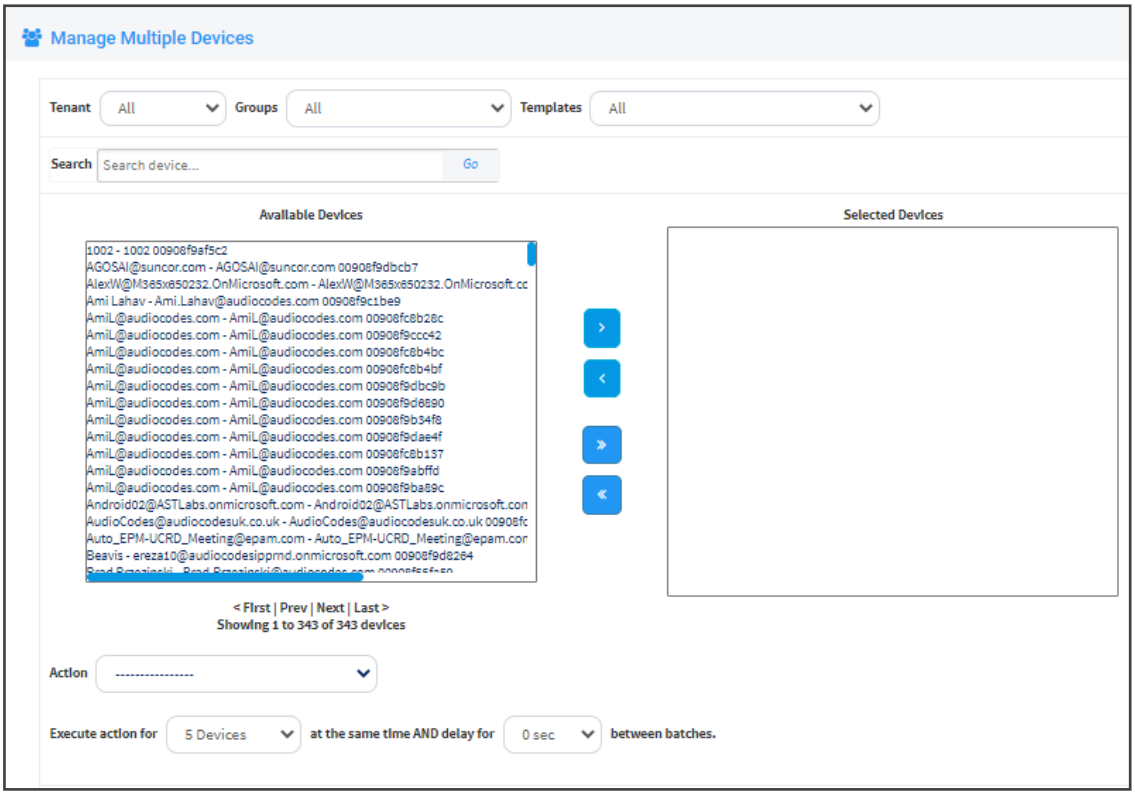
- delete multiple devices
- change devices type

- change language
- restart multiple devices
- generate devices configuration files
- update configuration files
- send a message to multiple phones

> These operations can also be performed on an endpoints group or on all endpoints groups; from the 'Groups' drop-down in the Manage Multiple Devices page shown in the figure below, select a single endpoints group, or **All**. For more information about *adding an endpoint to a group*, see under Checking Devices Status on page 81. For more information about *configuring an endpoints group*, see Configuring an Endpoints Group on page 11.

➢ To manage multiple devices:

1. Open the Manage Multiple Devices page (**Setup** > **Users & Devices** > **Manage Multiple Devices**):



2. You can filter devices per tenant, before selecting those to perform an action on.
3. You can enter a string in the 'Search' field and then click **Go** to search for devices.
4. In the Available Devices pane, select a device on which to perform an action and then click **>** to add it to the Selected Devices pane -or- select multiple devices on which to perform an action and then click **>>** to add them to the Selected Devices pane.

5. In the Selected Devices pane, select a single device and then click < to remove it, or select multiple Selected Devices and then click **<<** to remove them.
6. From the **Action** dropdown, select an action. Use the table below as reference.

Action	Description
Delete Devices	Deletes selected devices from the server applying a configurable 'Delay Time' (default = 2 seconds) in the process.
Change Template	This action will update the device template in the database. To finish the action, you need to: 1. Generate the device's Configuration File 2. Restart/Update the phone.
Change Language	Changes the phone language. Select the language from the **Language** dropdown and click **Change**. To view the usage of a language, click **View Usage**. To load a new language: 1. Generate the device's configuration file. 2. Restart/update the phone.
Restart Devices	Restarts online devices. Before restarting, some models wait for the user to finish an active call while others may perform an immediate restart. From the dropdown, choose the type of restart: ■ Graceful (default) ■ Force ■ Scheduled
Generate Devices Configuration Files	Generates new configuration files. Updates each phone with the newly generated configuration files after a configurable 'Delay Time' (default = 2 seconds) - if you selected the **Updating Devices and restarting Devices after generating files** option (by default it is selected).
Update Configuration File	Updates each phone after a configurable 'Delay Time' (default = 2 seconds).
Send Message	Lets you send a message to the screens of all user phones selected. Enter the message in the 'Text' field. You can configure the length of time the message will be displayed in the screen. Phones beep to alert users when messages come in.
Change	Lets you upload a different .img firmware file to the phone.

Action	Description
Firmware	
Change VLAN Discovery Mode	Used to change the virtual phone network's mode of operation. See here for the options descriptions [Manual/CDP/LLDP/CDP_LLDP]

➢ **To update all existing configuration files according to the new template:**

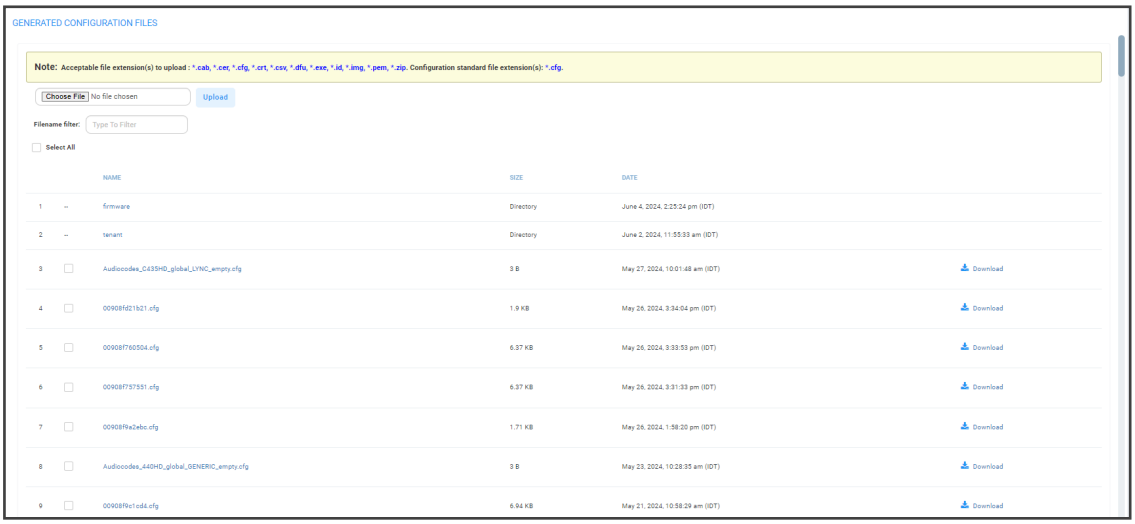
- After selecting devices, select from the 'Action' dropdown the **Generate Devices Configuration Files** option in the Manage Multiple Devices page.

Managing Configuration Files

You can manage devices' configuration files. All cfg files are created and located on the OVOC server. You can view and manage storage, and upload and delete files from storage. To avoid network congestion, a delay feature enables an interval between each installation.

➢ **To manage devices' configuration files:**

- Open the Manage Configuration Files page (**Setup** > **Configuration** > **Generated Config Files**).



The page enables admins to:

- Filter the .cfg configuration files listed by name
- Browse to a location on your PC and upload a .cfg configuration file
- Select and delete any or all of the .cfg configuration files listed
- Open any of the .cfg configuration files listed in an editor
- Save any of the .cfg configuration files listed
- Download any of the .cfg configuration files listed

- View all configuration files currently located on the server (global configuration files, company directory configuration files, and IP phone configuration files and third-party vendor product configuration files)

Viewing Your License

Usage of OVOC server platform processes is managed by a license that controls the time period validity for the use of the platform.

The License page displays the license's properties, including the number of days remaining until it expires.

➢ To view your license's properties:

1. Open the License Properties page (**Setup** > **System** > **License**).

2. Use the table below as reference.

Action	Description
Status	Indicates the license's status (Enable or Disable). If enabled and the configured time expires, connection to the OVOC server platform is denied. When it expires, Device Manager is rendered non-usable. Contact your AudioCodes partner if the license expires.
Expiration Date	Displays **DD:MM:YY**.

Action	Description
Days Left	The number of days remaining until your license expires. Minus indicates your license has expired. Contact your AudioCodes partner if the license expires.
Number of devices	The total number of devices deployed in your enterprise network.

If a license expires, communications with all servers will be suspended; users will not be able to log in, and it will not be possible to add new phones.

The time zone is determined by the OVOC server's Date & Time menu settings. If an expiration date is not configured, the 'Expiration Date' field displays **Unlimited**.

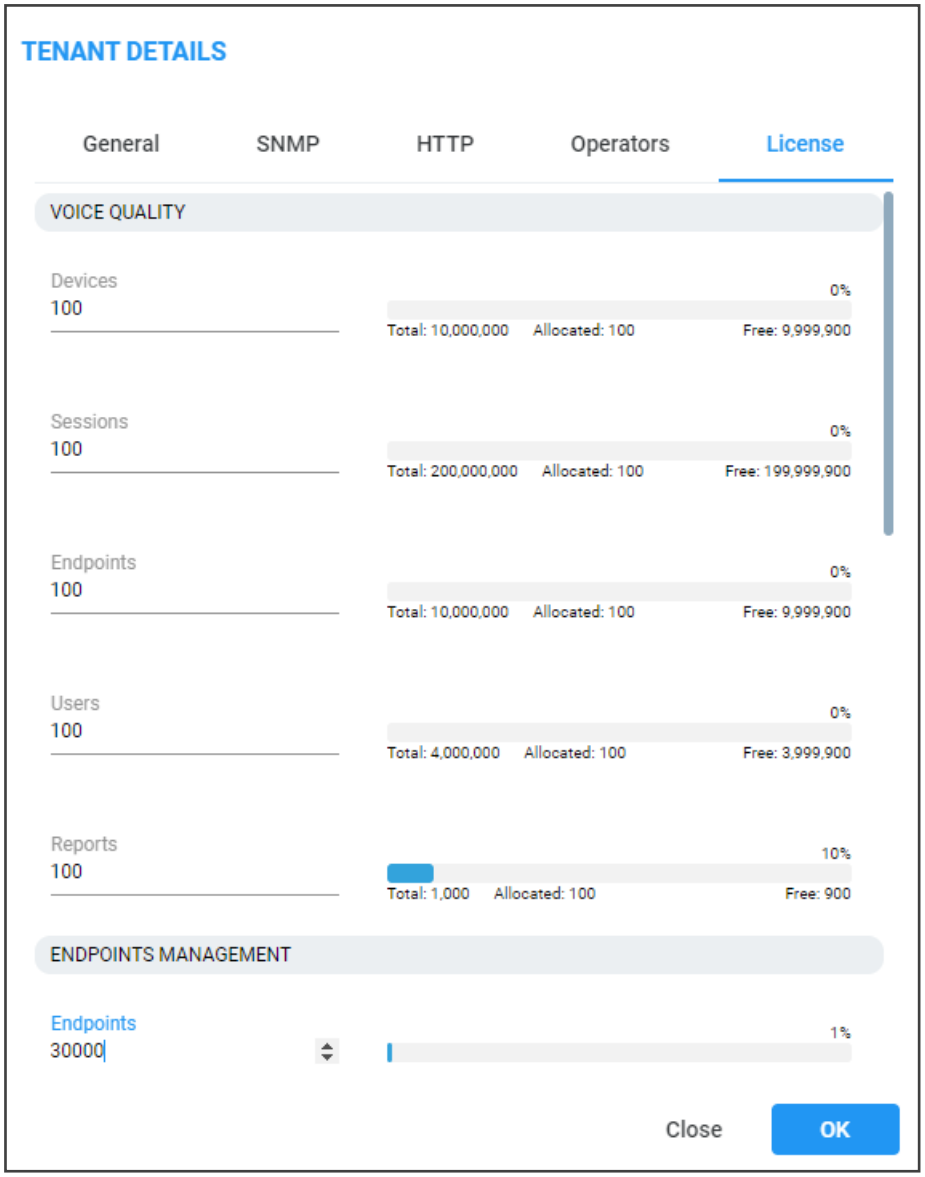
- As the license's expiration date approaches, warning alarms are issued:
  - ✓ A Major alarm is sent when 80% of the period defined in the currently running device's license is consumed
  - ✓ A Critical alarm is sent when 100% of the period defined in the currently running device's license is consumed
- When the maximum number of devices reporting to OVOC is exceeded, the OVOC server blocks them and sends an alert that is displayed in the Home page.

Licensing Endpoints

Admin can license endpoints using OVOC (see also the *One Voice Operations Center User's Manual*).

➢ **To license endpoints:**

1. When editing a tenant, click the **License** tab in the OVOC's Tenant Details screen and then scroll down to the 'Endpoints Management' section.



2. In the Endpoints field, enter the number of endpoints the Device Manager application supports for this tenant (30000 maximum), and then click **OK**.

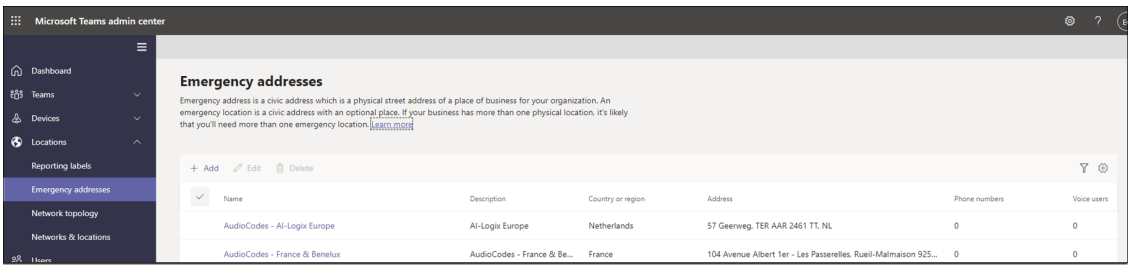
Enabling Calls to Emergency Numbers

The documentation here shows how to enable users to make emergency calls to emergency numbers (E911) from Skype for Business IP phones. It'll help you get started with configuring the infrastructure elements and call routing needed for making dynamic emergency calls.

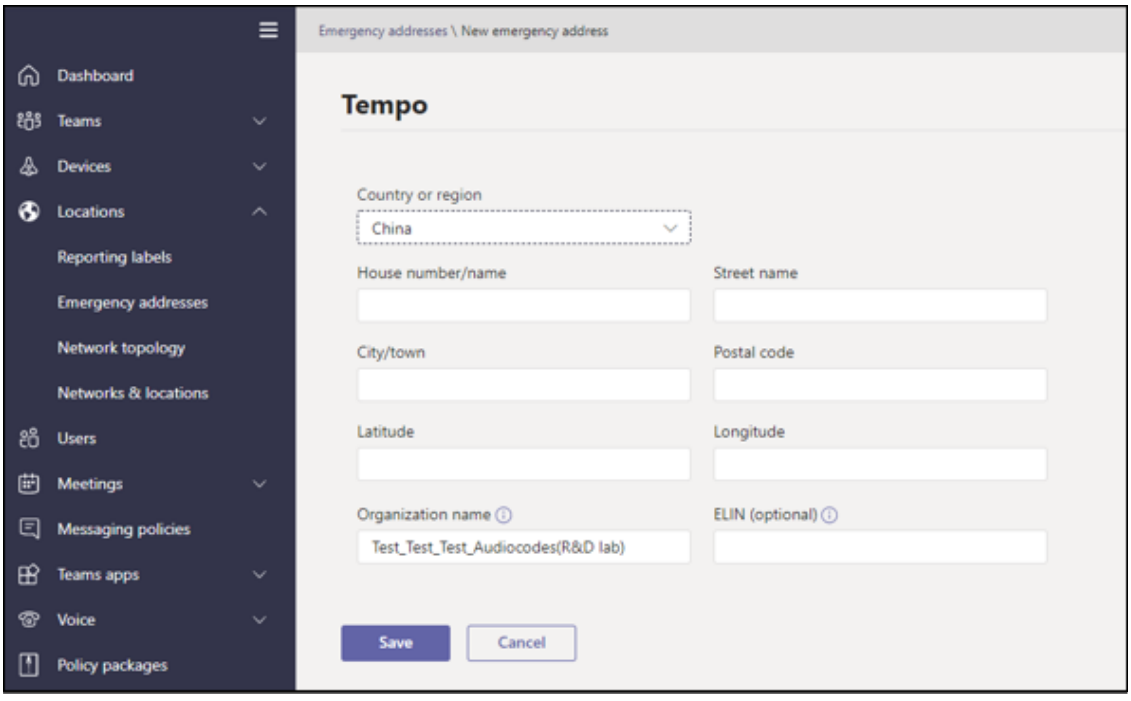
- 'Dynamic' means the Teams client gets the emergency address/location based on the network location it is at and transmits it directly to the Public Safety Answering Point (PSAP), bypassing the Emergency Call Relay Center (ECRC).
- Based on the network topology that the tenant administrator defines, the Teams client provides network connectivity information in a request to the Teams Location Information Service (LIS). If there's a match, the Teams LIS returns a location to the client. This location data is transmitted back to the client. See here for more on configuring dynamic emergency calling.
- 'Infrastructure elements' refers to information about the physical address of the building in which the devices are located and the network elements and their locations within it.

➢ To configure emergency locations in Microsoft Teams admin center:

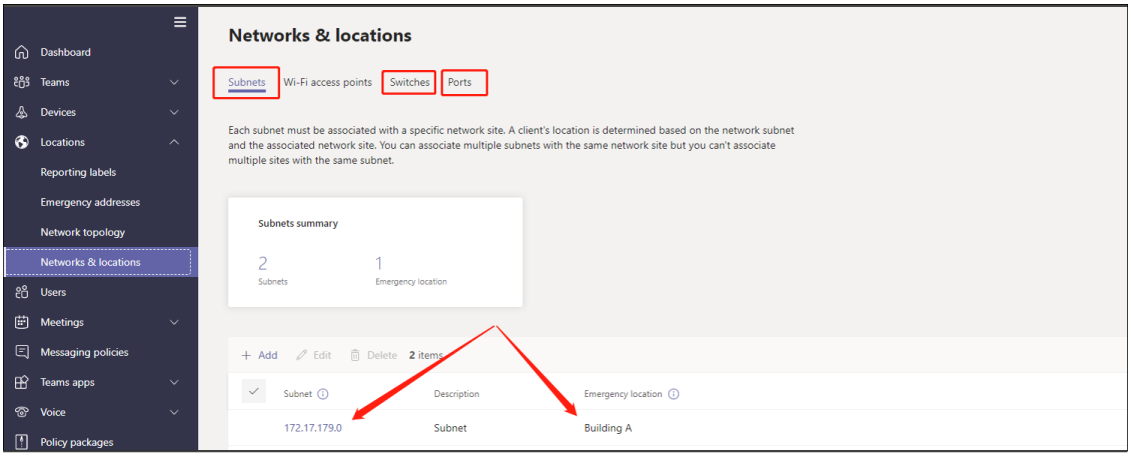
1. In the Microsoft Teams admin center, open the 'Emergency addresses' page.



2. Add addresses using the preceding and next figure as reference.



3. Click **Save** and then open the 'Networks & locations' page.



4. Assign an emergency address to the network site using the preceding figure as reference.

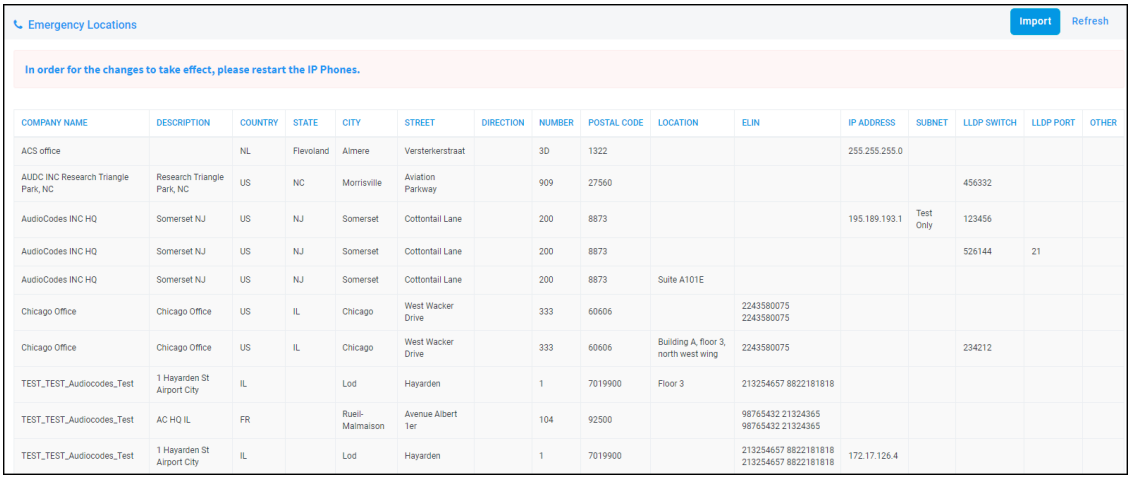
> After configuring the emergency locations in the Microsoft Teams admin center, you can import them into Device Manager.

➢ To import emergency locations into Device Manager:

1. After configuring emergency locations in Microsoft Teams admin center, open the Emergency Locations page in Device Manager (**Setup** > **System** > **Emergency Locations**).
2. Click the **Import** button; a script exports the emergency locations from the Microsoft Teams admin center into OVOC from where they're imported into Device Manager.
3. Navigate to the folder in which the CSV file is saved.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	CompanyName	Descriptic	Country	State	City	Street	Direction	Number	Postal_Code	Location	ELIN	IP_address	Subnet	LLDP_Switch	LLDP_port	
2	UCS	PDX	US	MI	Springfiel	North Bay		5987	48346	Bldg-A-Floor-1	+17208101900 +17	10.3.100.0				
3	UCS	PDX	US	MI	Springfiel	North Bay		5987	48346	Bldg-B	+17208101900 +17	10.4.100.0				
4	UCS	PDX	US	MI	Springfiel	North Bay		5987	48346	Bldg-A-Floor-2	+17208101900 +17	10.3.200.0				
5	UCS	PDX	US	MI	Springfiel	North Bay		5987	48346		+17208101900 +17	10.2.1.0				
6	UCS	PDX	US	MI	Springfiel	North Bay		5987	48346		+17208101900 +17	10.4.1.0				
7	UC Solutions	Boulder	US	CO	Longmont	Gooseberry Drive		635	80503		+17208101100 +17	10.2.100.0				
8	UC Solutions	Boulder	US	CO	Longmont	Gooseberry Drive		635	80503		+17208101100 +17	10.2.200.0				
9	UC Solutions	Boulder	US	CO	Longmont	Gooseberry Drive		635	80503		+17208101100 +17	10.2.1.128				
10	UC Solutions	Boulder	US	CO	Longmont	Gooseberry Drive		635	80503		+17208101100 +17	10.4.1.128				
11	UCS	UCS	US	NY	Huntingto	Bay Drive West		15	11743							
12																
13																

After the CSV file is imported, the locations are displayed in Device Manager's Emergency Locations table. Device Manager adds the values from the CSV without any manipulation except for removing leading / trailing white spaces.



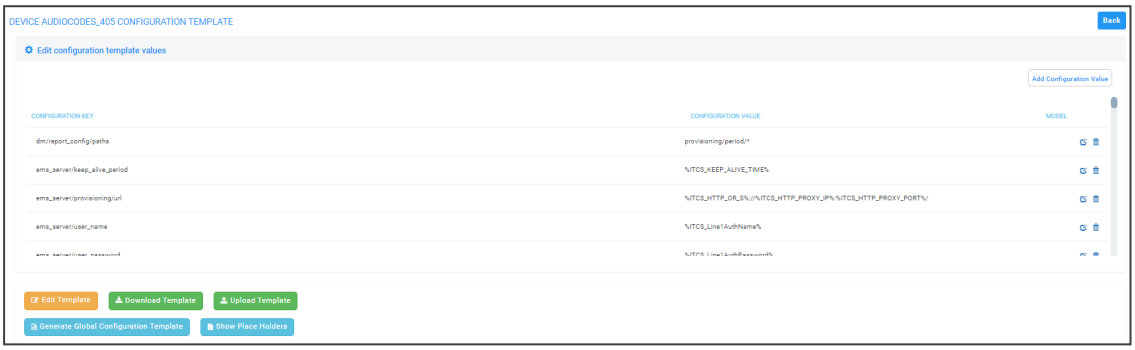
COMPANY NAME	DESCRIPTION	COUNTRY	STATE	CITY	STREET	DIRECTION	NUMBER	POSTAL CODE	LOCATION	ELIN	IP ADDRESS	SUBNET	LLDP SWITCH	LLDP PORT	OTHER
ACS office		NL	Flevoland	Almere	Versterkerstraat		3D	1322			255.255.255.0				
AUDC INC Research Triangle Park, NC	Research Triangle Park, NC	US	NC	Morrisville	Aviation Parkway		909	27560					456332		
AudioCodes INC HQ	Somerset NJ	US	NJ	Somerset	Cottontail Lane		200	8873			195.189.193.1	Test Only	123456		
AudioCodes INC HQ	Somerset NJ	US	NJ	Somerset	Cottontail Lane		200	8873					526144	21	
AudioCodes INC HQ	Somerset NJ	US	NJ	Somerset	Cottontail Lane		200	8873	Suite A101E						
Chicago Office	Chicago Office	US	IL	Chicago	West Wacker Drive		333	60606		2243580075 2243580075					
Chicago Office	Chicago Office	US	IL	Chicago	West Wacker Drive		333	60606	Building A, floor 3, north west wing	2243580075			234212		
TEST_TEST_Audiocodes_Test	1 Hayarden St Airport City	IL		Lod	Hayarden		1	7019900	Floor 3	213254657 8822181818					
TEST_TEST_Audiocodes_Test	AC HQ IL	FR		Rueil-Malmaison	Avenue Albert 1er		104	92500		98765432 21324365 98765432 21324365					
TEST_TEST_Audiocodes_Test	1 Hayarden St Airport City	IL		Lod	Hayarden		1	7019900		213254657 8822181818 213254657 8822181818	172.17.126.4				

4. View the following columns in the newly created Emergency Locations table:
   - Company Name - the name of the company in which the devices are deployed
   - Description - a description of the company in which the devices are deployed
   - Country - the name of the country in which the company is located
   - State - the name of the state in which the company is located
   - City - the name of the city in which the company is located
   - Street - the name of the street in which the company is located
   - Direction
   - Number - the street number of the company
   - Postal Code - the postal code of the company
   - Location - the company's department in which the devices are deployed
   - ELIN - Emergency Location Identification Number. A 10-digit DID number that can be obtained from the local exchange carrier (LEC). Provide it to the public safety answering point (PSAP) for 911 calls.
   - IP address - the device's IP address in the network
   - Subnet - the subnet in which the device is deployed
   - LLDP Switch - Link Layer Discovery Protocol switch. Devices use this link layer protocol to advertize their identity, capabilities and neighbors in a LAN based on IEEE 802.
   - LLDP port - Link Layer Discovery Protocol port.
   - OTHER

Make sure two rows (or more) in the Emergency Locations table do not contain same combination of:

- LLDP Switch Chassis number + LLDP port
- LLDP Switch Chassis number + EMPTY LLDP port
- IP address

5. After importing the CSV file, edit the configuration template in the Configuration Template page (**Setup** > **Configuration** > **Templates**).



6. Configure the following (refer to the preceding figure):
   - Set the parameter 'Configuration Key' to **dm/report_status/paths**
   - Set the parameter 'Configuration Value' to

     dm/report_status/paths=status/network/lan/*,
     status/diagnostics/lldp/chassis/chassisId,
     status/diagnostics/lldp/chassis/portId

- Configuration of these two parameters is mandatory for the feature to function.
- The configuration can be performed at either the device level, Tenant level, Group level or Site level.

Managing Templates

The sections below describe aspects of template management:

- Selecting a Template
- Editing a Configuration Template
- About the Template File
  - Restoring a Template to the Default
  - Downloading a Template
  - Uploading an Edited Template
  - Generating an Edited Template
  - Defining Template Placeholders

Selecting a Template

Templates are available per

- tenant
- phone model

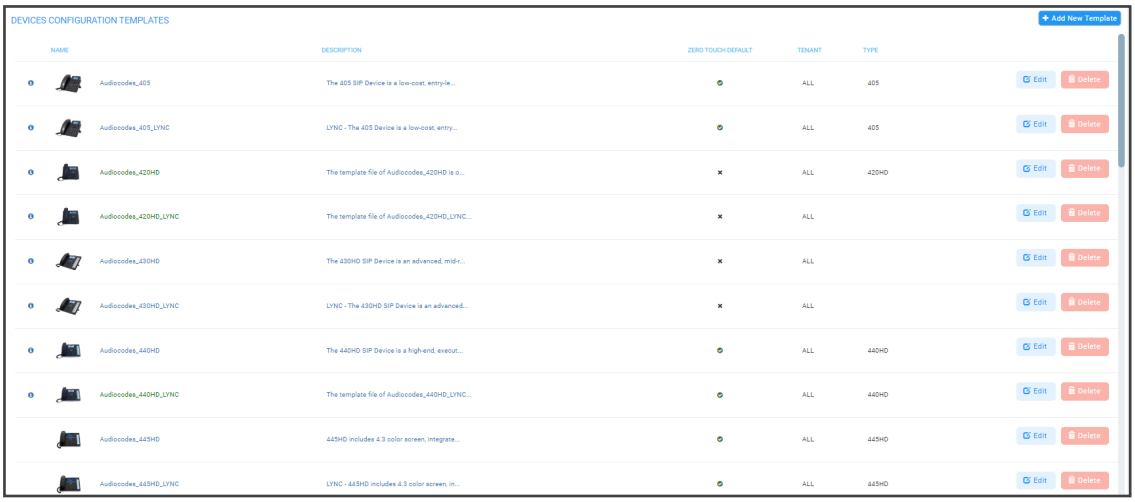
Depending on the tenant, model and the server in the enterprise, select a template for:

- AudioCodes 405
- AudioCodes 420HD
- AudioCodes 430HD
- AudioCodes 440HD
- AudioCodes 450HD
- AudioCodes 420HD Skype for Business
- AudioCodes 430HD Skype for Business
- AudioCodes 440HD Skype for Business
- AudioCodes 450HD Skype for Business
- AudioCodes C435HD Teams
- AudioCodes C436HD Teams
- AudioCodes C448HD Teams
- AudioCodes C450HD Teams
- AudioCodes C455HD Teams
- AudioCodes C470HD Teams
- AudioCodes RXV80 Standalone Video Collaboration Bar for Teams
- AudioCodes RXV81 Meeting Room Solution for Microsoft Teams
- AudioCodes RXV100 Meeting Room Solution for Microsoft Teams
- Jabra
- Poly Trio 8800
- Poly VVX
- Poly CCX 500/600
- Spectralink 8440

For information on third-party vendor products, see the *Device Manager for Third-Party Vendor Products Administrator's Manual*.

➢ To select a template:

- Open the Devices Configuration Templates page (**Setup** > **Configuration** > **Templates**):



- Click ⓘ for more information about the phone whose template is displayed.
- Click **Edit** to modify a template.

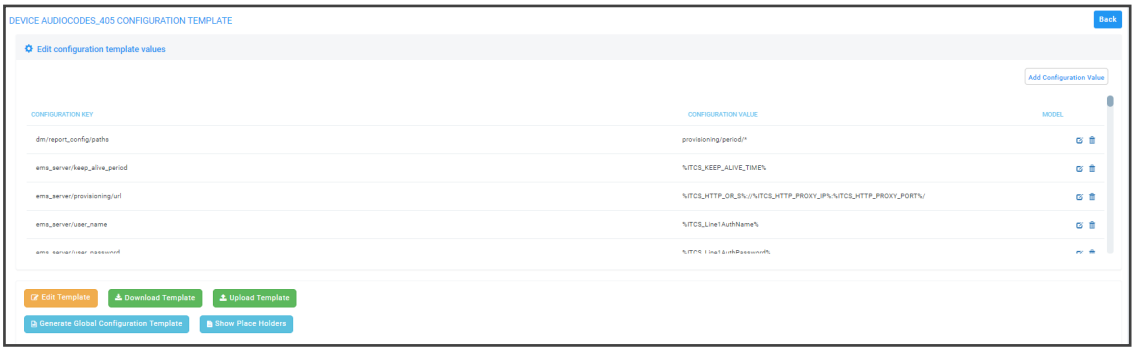
Editing a Configuration Template

Admins can edit a device's template but typically it's unnecessary to do so.

> For information on third-party vendor products, see the *Device Manager for Third-Party Vendor Products Administrator's Manual*.

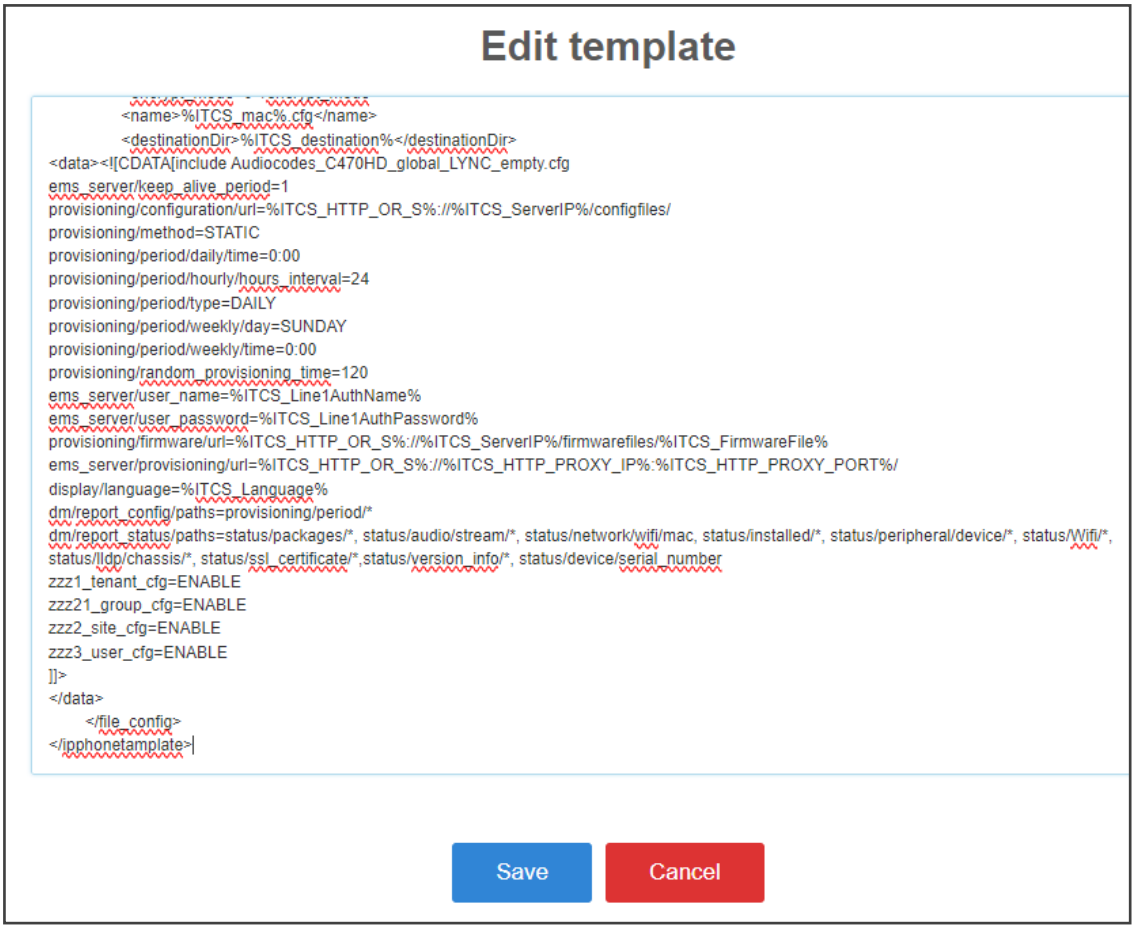
➢ To edit a template:

1. In the Devices Configuration Templates page (**Setup** > **Configuration** > **Templates**), click the link of the device or its **Edit** icon.



   When a new device of model x and tenant y will be connected for the first time to the network, it will use this template.

2. Click the **Edit Template** button; the template opens in an integral editor:



3. Edit the template and then click **Save**; in the Devices Configuration Templates page, the name of an edited template is displayed in green.

- If a device model's template is modified in any way, the Serial Number status parameter **status/device/serial_number** must be added to the template.

- SN status reporting is supported by the following models:
  - ✓ UC phones
  - ✓ Teams phones
  - ✓ Windows / Android based Meeting Room devices
  - ✓ Desktop / PC

See the device's *User's & Administrator's Manual* for parameter descriptions.

About the Template File

The template is an xml file. It defines how a device's configuration file will be generated. The template shows two sections.

- The upper section defines the *global* parameters that will be in the *global* configuration file
- The lower section defines the *private user* parameters that will be in the *device* configuration file

See also:

- Restoring a Template to the Default
- Downloading a Template
- Uploading an Edited Template
- Generating an Edited Template
- Defining Template Placeholders

Restoring a Template to the Default

You can restore a template to the factory default at any time.

➢ **To restore a template to the default:**

- Click the **Restore to default** button (displayed only if a change was made); the template and its description are displayed.

Downloading a Template

You can download a template, for example, in order to edit it in a PC-based editor.

➢ **To download a template:**

- Click the **Download configuration template** button and save the *xml* file in a folder on your PC.

Uploading an Edited Template

You can upload a template, for example, after editing it in a PC-based editor.

➢ **To upload an edited template:**

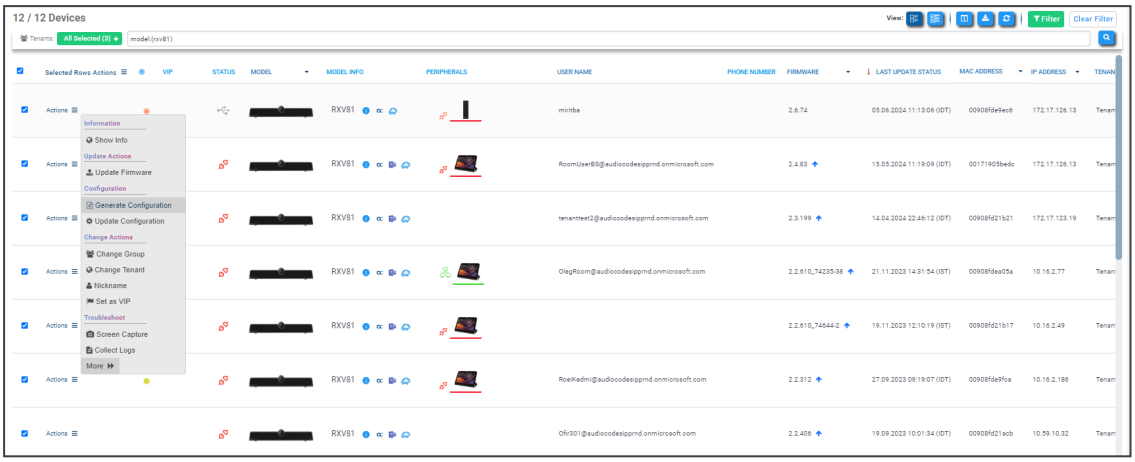
- Click the **Upload template** button and browse to the *xml* template file on your PC. The file will be the new template for the phone model.

Generating an Edited Template

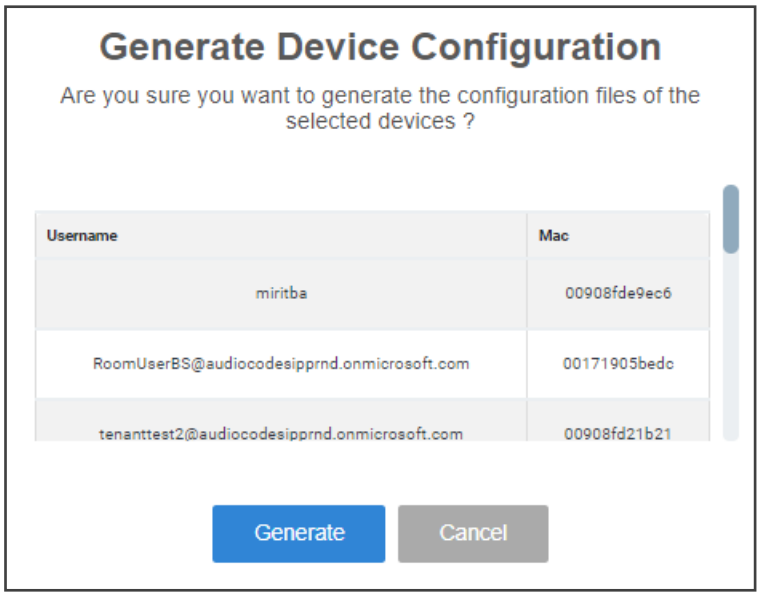
After editing a template, generate the cfg files for the users/devices with whom/which the template is associated.

➢ To generate an edited template:

1. Open the Monitor page and filter the devices for which to generate an edited template.



2. Select all and then from the **Selected Rows Actions** menu, select the **Generate Configuration** option.



3. Make sure the users | devices are correct and then click the **Generate** button.

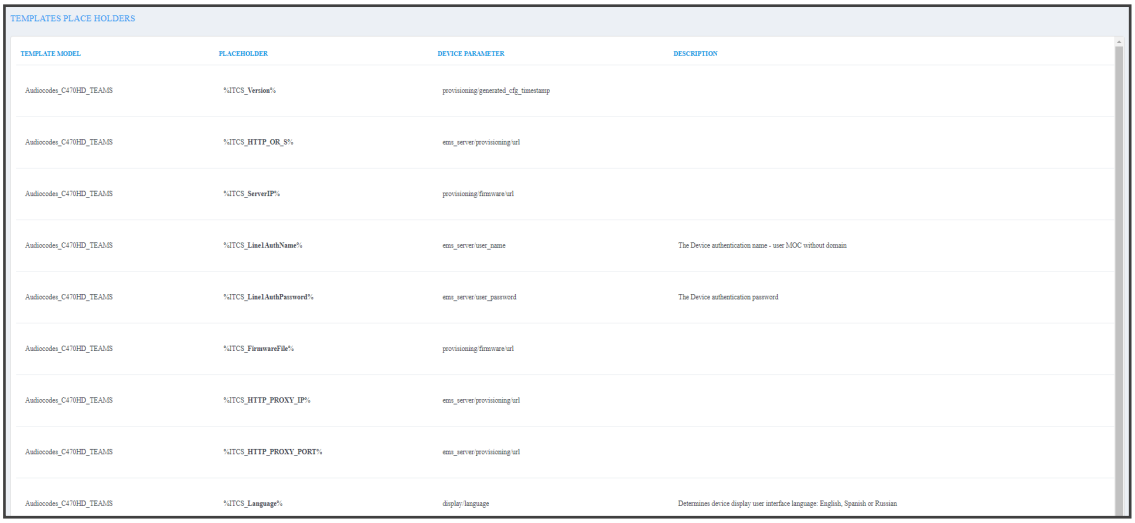
Defining Template Placeholders

Templates include *placeholders* whose values you can define. After defining values, the placeholders are automatically resolved when you generate the template. For example, placeholder **%ITCS_ TimeZoneLocation%** is replaced with local time. Placeholders can be defined per tenant, model, etc. The cfg file includes default values and overwritten values according to configured placeholders. If no placeholder is configured, the cfg file will include only default values.

➢ To show placeholders:

1. In the Device Configuration Templates page (**Setup** > **Configuration** > **Templates**), click the **Edit** button in the same row as the device model.

2. Click the **Show Placeholders** button.



The figure above shows placeholders currently defined in the xml Configuration Template file for the C470HD Teams phone. There are four kinds of placeholders: (1) System (2) Template (3) Tenant (4) Devices.

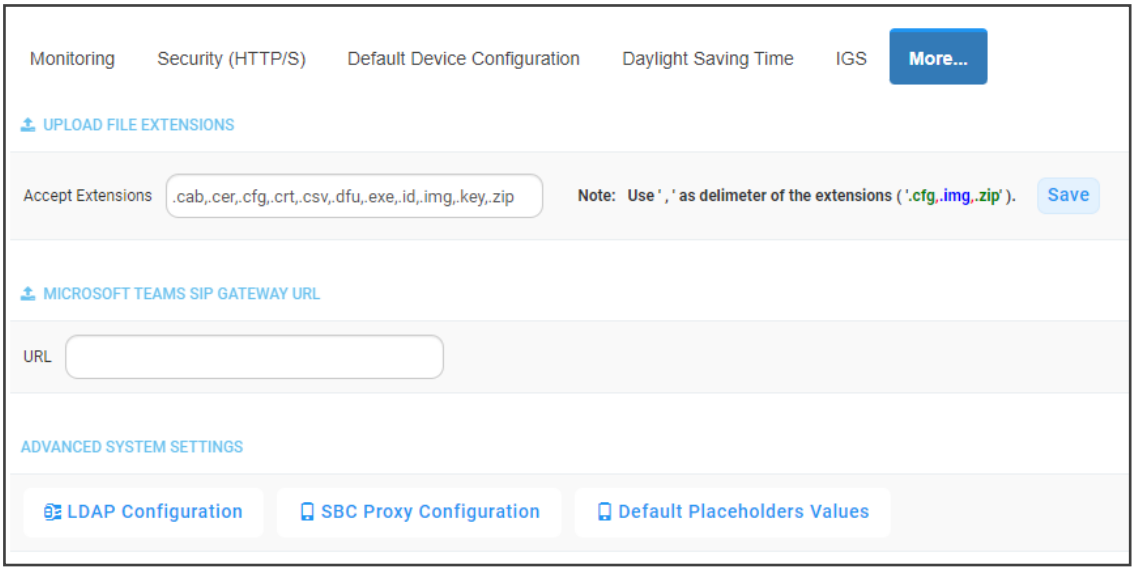
- To add/edit/delete a template placeholder, see Adding a New Template Placeholder on page 116 and Adding a New Template Placeholder on page 116
- To add/edit/delete a tenant placeholder, see Adding a New Tenant Placeholder on page 118 and Editing a Configuration Template on page 110.
- To add/edit/delete a device placeholder, see Devices Placeholders on page 121 and Changing a Device Placeholder Value on page 121

Viewing Default Placeholders Values

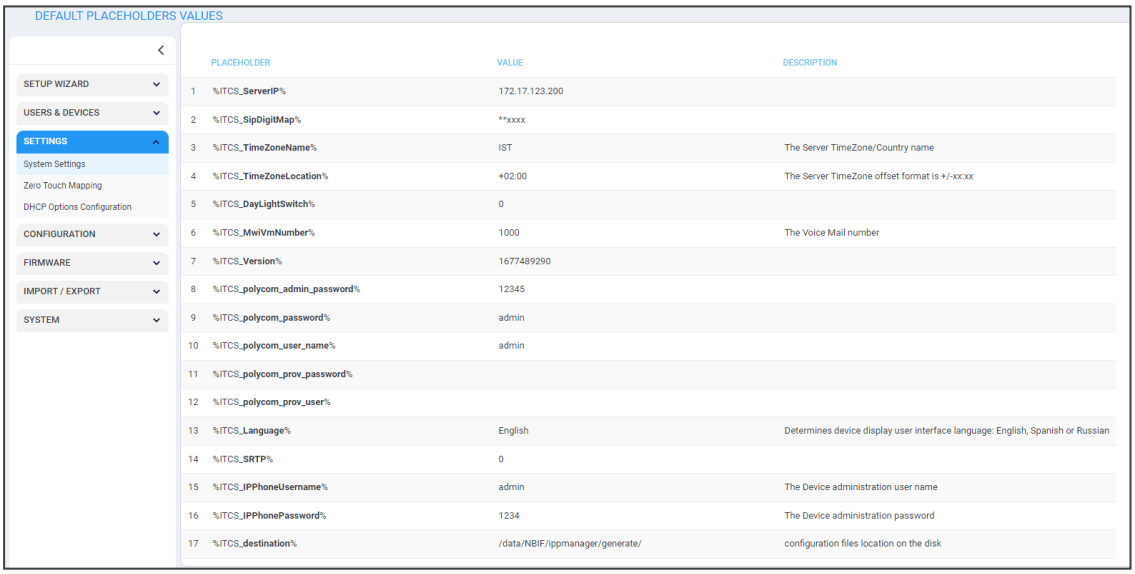
Before defining values for placeholders, you can view the default placeholders values.

➢ **To view default placeholders values:**

1. Open the Default Placeholders Values page (**Setup** > **Settings** > **System Settings** and then click the **More...** option).



2. Click the **Default Placeholders Values** button.



Template Placeholders

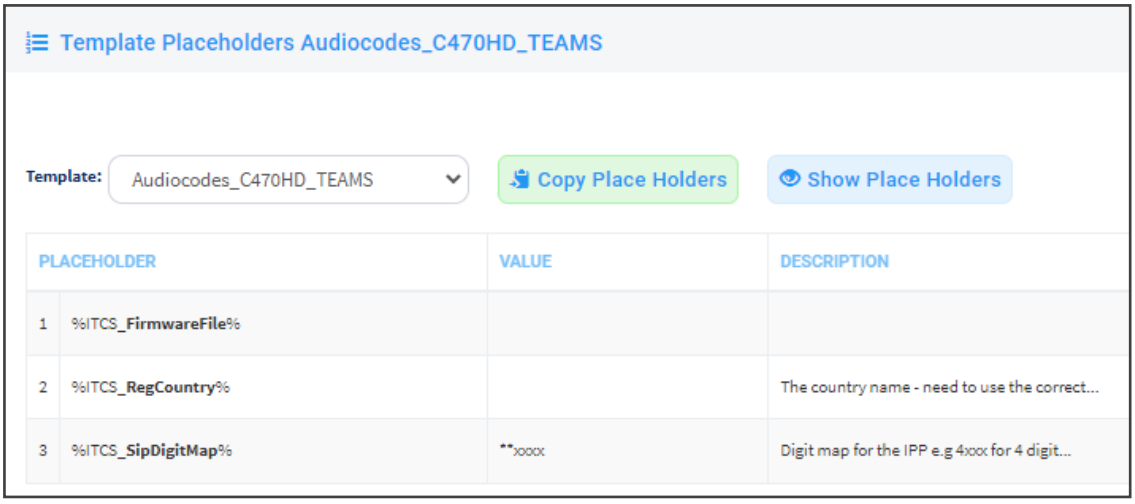
You can edit the values defined for an existing template placeholder and/or you can add a new template placeholder.

Editing Template Placeholders

You can edit the values for existing template placeholders.

➢ **To edit values for existing template placeholders:**

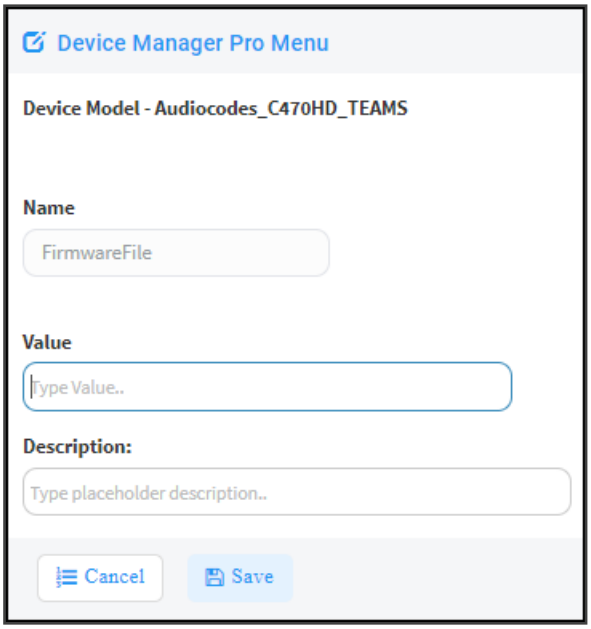
■ Open the Template Placeholders page (**Setup** > **Configuration** > **Template Placeholders**):



The page shows the placeholders and their values defined for a template.

➢ To edit a value of an existing template placeholder:

1. Click the adjacent **Edit** button.



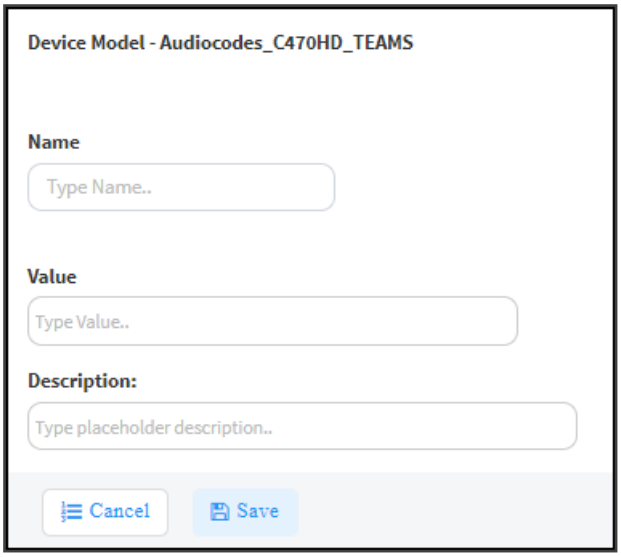
2. In the 'Name' field, you can edit the name of the placeholder.
3. In the 'Value' field, you can edit the value of the placeholder.
4. In the 'Description' field, you can edit the placeholder description.
5. Click **Save**; the edited placeholder is added to the table.

Adding a New Template Placeholder

You can add a new template placeholder. A new placeholder can be added and assigned with a new value.

➢ **To add a new template placeholder:**

1. Open the Template Placeholders page (**Setup** > **Configuration** > **Template Placeholders**):
2. From the **Template** dropdown, select the template , e.g., Audiocodes_C470HD_TEAMS.
3. Click the **Set Value to Place Holder** button located in the upper right corner of the screen.



4. In the 'Name' field, enter the name of the new placeholder.
5. In the 'Value' field, enter the value of the new placeholder.
6. In the 'Description' field, enter a short description for the new placeholder.
7. Click **Save**; the new placeholder is added to the table.

Tenant Placeholders

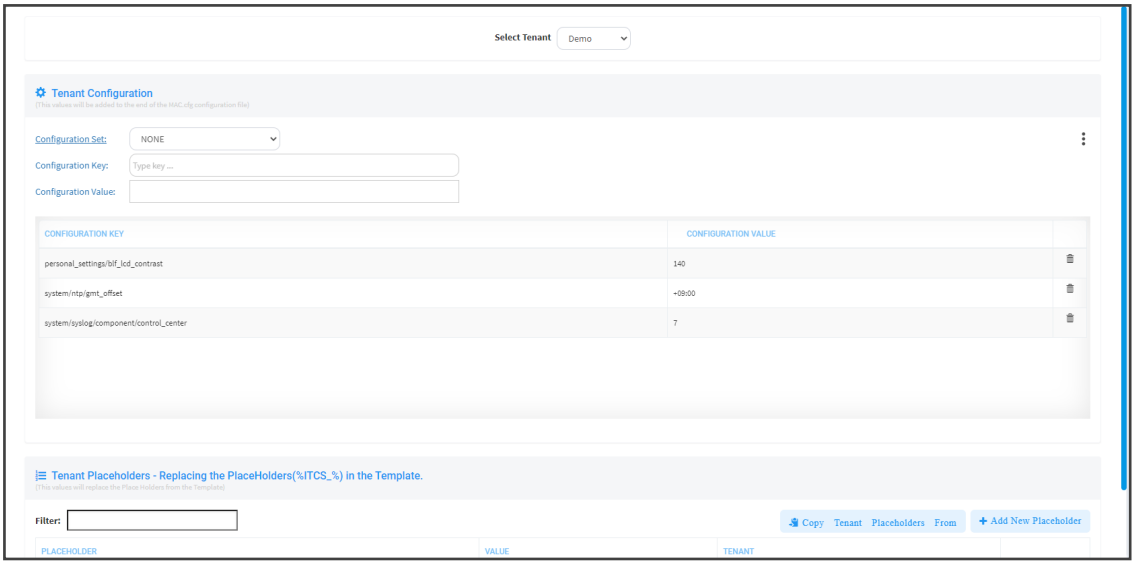
You can edit values for existing tenant placeholders and/or add new tenant placeholders.

Editing Tenant Placeholders

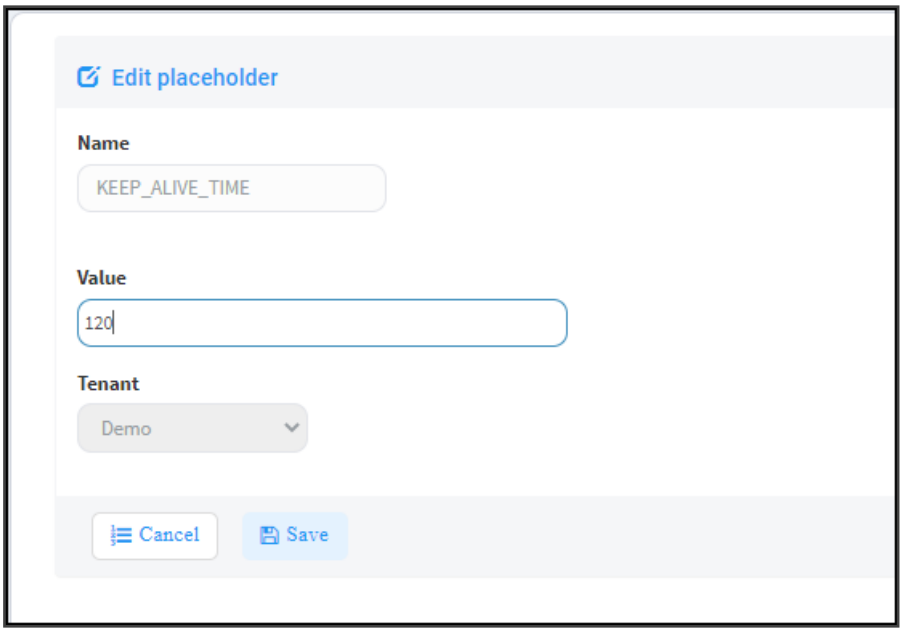
You can edit the values for existing tenant placeholders.

➢ **To edit values for existing tenant placeholders:**

1. Open the Tenant Configuration page (**Setup** > **Configuration** > **Tenant Configuration**):



2. Under the Tenant Placeholders section, select the placeholder and then click the **Edit** button.



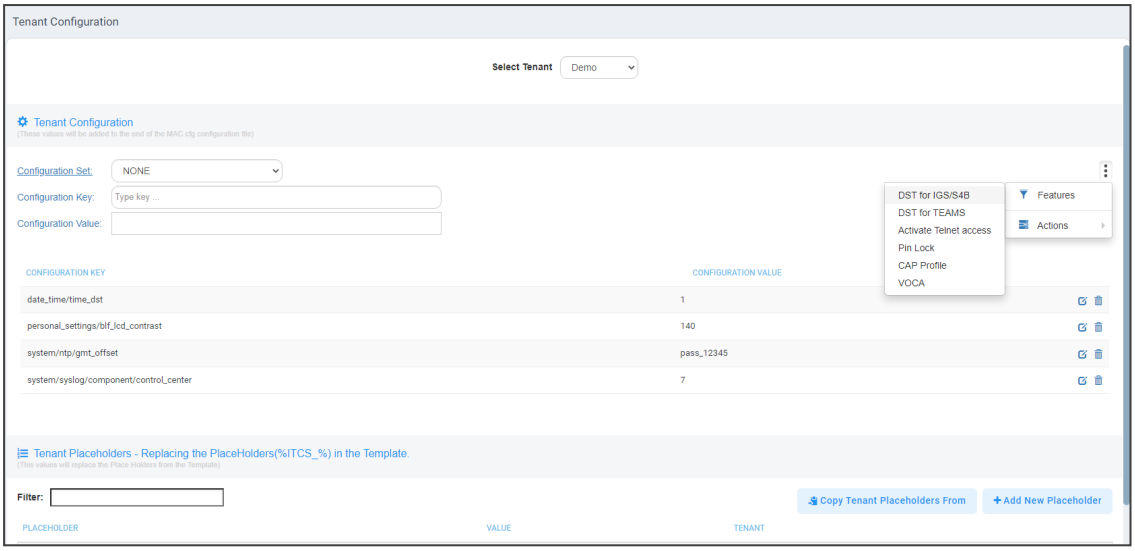
3. In the 'Name' field, you can edit the name of the placeholder.
4. In the 'Value' field, you can edit the value of the placeholder.
5. From the 'Tenant' dropdown, you can select another tenant.
6. Click **Save**; the edited placeholder is added to the table.

Adding a New Tenant Placeholder

You can add a new tenant placeholder.

➢ **To add a new tenant placeholder:**

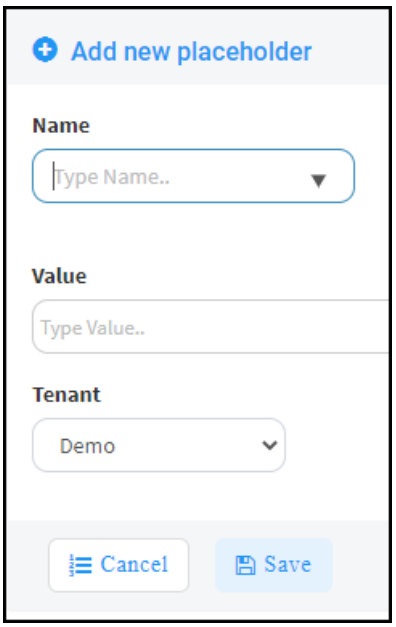
1. Open the Tenant Configuration page (**Setup** > **Configuration** > **Tenant Configuration**).



2. Under Tenant Configuration, provision devices using the 'Configuration Set' parameter and the corresponding 'Configuration Key' and 'Configuration Value' parameters that are auto-populated after selecting a device model.

   - On the right side of the page, click the vertical ellipsis ⋮ and from the menu that pops up shown in the preceding figure, select **DST for IGS/SFB** or **DST for Teams** and then select **AUTO**, **ENABLE** or **DISABLE**. This menu provides a quick and friendly way to configure Daylight Saving Time (DST) for Generic SIP / Skype for Business phones and for Native Teams phones.

3. Under the lowermost Tenant Placeholders section of the page, click the **+Add New Placeholder** button.



4. In the 'Name' field, enter / select the name of the new placeholder.
5. In the 'Value' field, enter the value of the new placeholder.
6. From the 'Tenant' dropdown, select a new tenant.

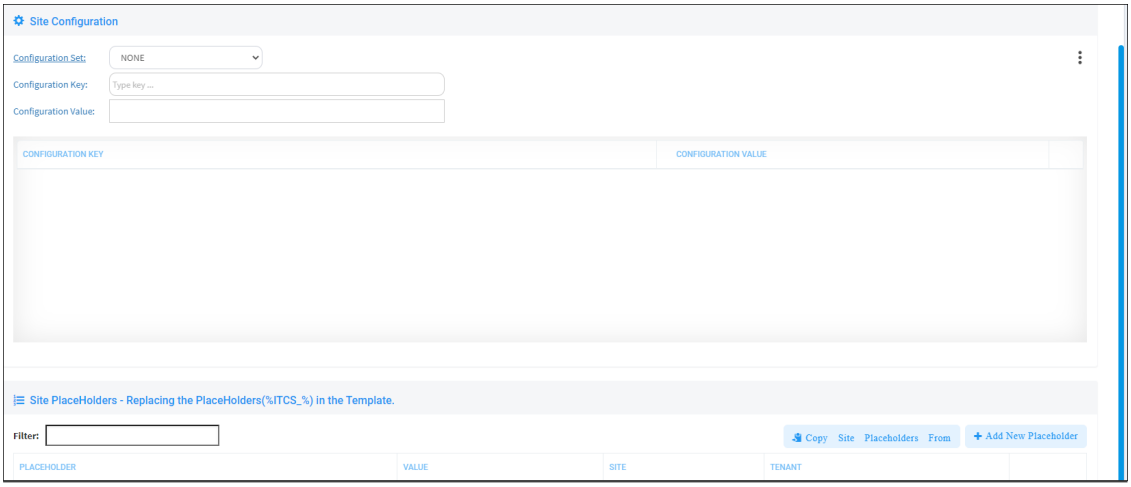
7. Click **Save**; the new placeholder is added to the table.

Adding a New Site Placeholder

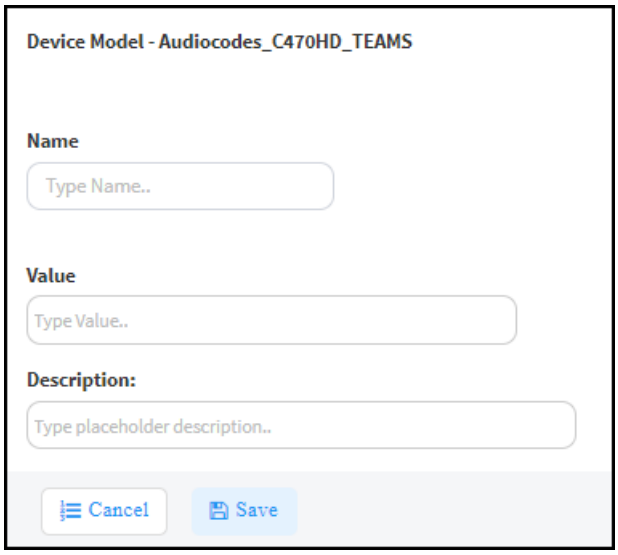
You can add a new site placeholder.

➢ **To add a new site placeholder:**

1. Open the Site Configuration page (**Setup** > **Configuration** > **Site Configuration**).



2. Under Site Configuration, provision devices using the 'Configuration Set' parameter and the corresponding 'Configuration Key' and 'Configuration Value' parameters that are auto-populated after selecting a device model.
3. Under the Site Placeholders section of the page, click the **+Add new placeholder** button.



4. From the 'Name' field drop-down, select the name of the new placeholder.
5. In the 'Value' field, enter the value of the new placeholder.
6. From the 'Site' drop-down, select a site to which the phone will automatically be provisioned.

Prior to version 7.8, Poly phones could only be provisioned to 'AutoDetection' by default. As of version 7.8, the 'Site' drop-down enables selecting a site to which Poly phones will also be automatically provisioned.

7. Click **Save**; the new placeholder is added to the table.

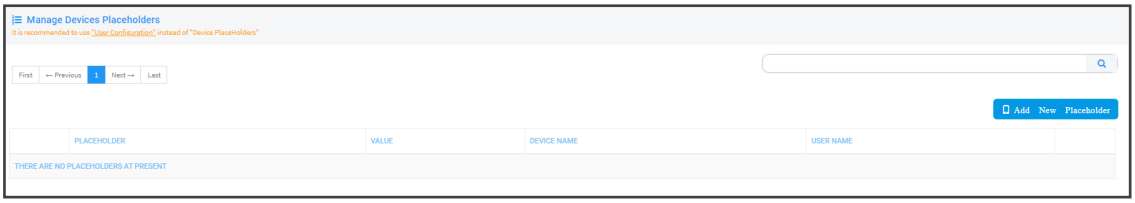
Devices Placeholders

You can change placeholders values for specific phones, for example, you can change placeholders values for the enterprise CEO's phone. You can also edit a device's placeholders values.

Changing a Device Placeholder Value

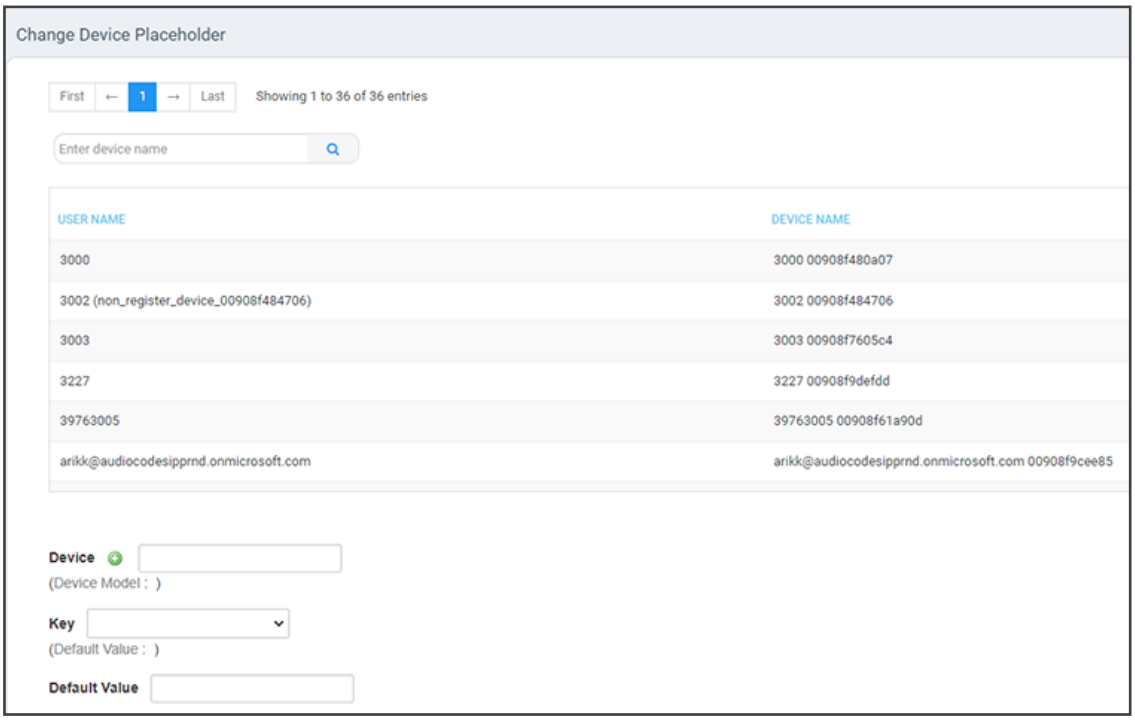
➢ **To change a device placeholder value:**

1. Open the Manage Devices Placeholders page (**Setup** > **Configuration** > **Devices Placeholders**):



Use the 'Filter' field to quickly find a specific device if many are listed. You can search for a device by its name or by its extension

2. Select the device whose placeholder value you want to change and click **Edit**.



3. Make sure the correct device is selected; the read-only 'Device' field is filled.
4. From the **Key** dropdown, choose the phone configuration key.
5. Enter the device's default value in the 'Default Value' field, and then click **Save**; the edited device placeholder is added to the table.

The new default value is not automatically generated in the device's configuration file. To generate it, choose the relevant device and then click the **Generate Configuration** link.

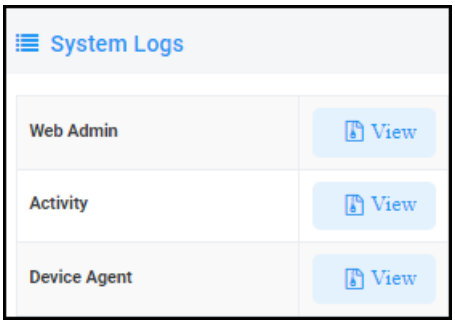
6 Troubleshooting

You can display system diagnostics to help troubleshoot problems and determine cause. System diagnostics comprise:

- Logged activities performed in the Web interface
  - Last logged activities
  - Archived activities
- Logged activities performed in the Device Manager Pro
  - Last logged activities
  - Archived activities

➢ **To display system diagnostics:**

1. Open the System Logs page (**Troubleshoot** > **System Diagnostics**).

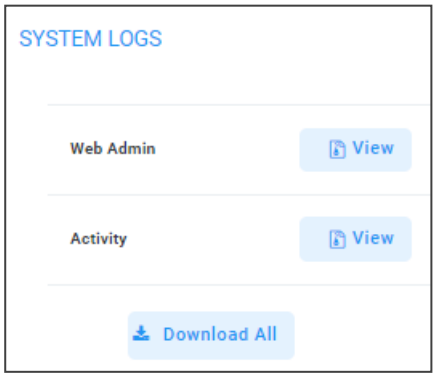


Displaying Archived Activities Performed in the Web Interface

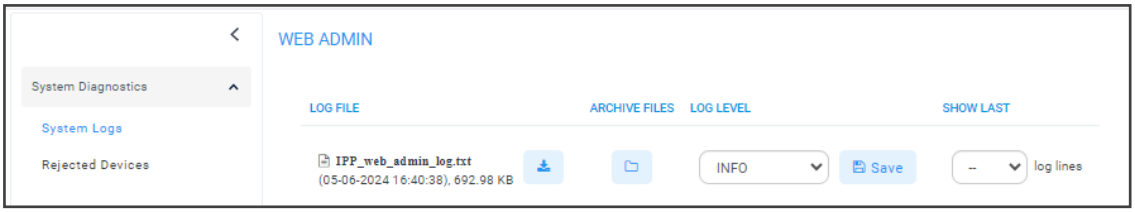
Admin can view the logged activities that were performed in the Web interface.

➢ **To display archived activities performed in the Web interface:**

1. Open the System Logs page (**Troubleshoot** > **System Diagnostics** > **System Logs**).



2. Next to **Web Admin**, click **View**.



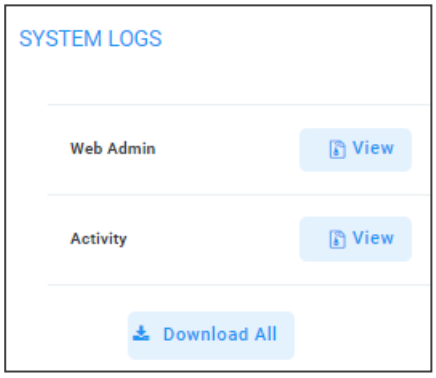
3. [Optionally] Before you download the Web admin log file, select the log level (Error, Warning, Info, Debugging or Verbose) and the number of last log lines to be shown.
4. Click the download icon to download the log file; the file is downloaded to the PC.

Displaying Logged Activities Performed in Device Manager

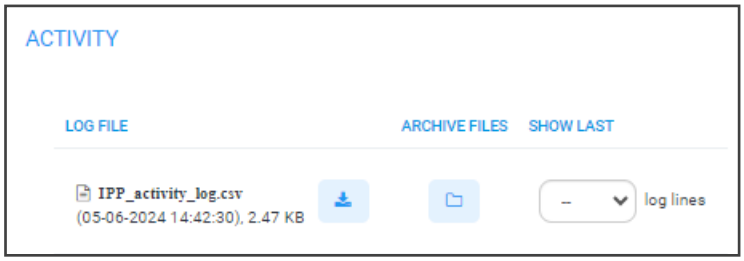
Admin can view the logged activities that were performed in Device Manager.

➢ **To display the logged activities in the Device Manager:**

1. Open the System Logs page (**Troubleshoot** > **System Diagnostics** > **System Logs**).



2. Next to **Activity**, click **View**.



3. From the 'Show last log lines' dropdown select 10, 20, 30, 40, 50 or 100 and then click the download icon to download the log file; the file is downloaded to the PC.

	A	B	C	D	E	F	G	H
1								
2								
3								
4	Login Name	Time	Host	Action	Object	Result	Data	Desc
5		added at: 2024-06-05 07:07:10	REMOTE_ADDR: 172.17.113.67	LOGIN	PASSWORD	OK	SSO - acladmin	content: Correct current password: *****.
6	acladmin	added at: 2024-06-05 07:07:10	REMOTE_ADDR: 172.17.113.67	LOGIN	ADMIN	OK	acladmin	content: Success login user name=acladmin
7		added at: 2024-06-05 07:07:27	REMOTE_ADDR: 172.17.113.13	LOGIN	PASSWORD	OK	SSO - acladmin	content: Correct current password: *****.
8	acladmin	added at: 2024-06-05 07:07:27	REMOTE_ADDR: 172.17.113.13	LOGIN	ADMIN	OK	acladmin	content: Success login user name=acladmin
9		added at: 2024-06-05 07:22:36	REMOTE_ADDR: 172.17.126.20	LOGIN	PASSWORD	OK	acladmin	content: Correct current password: *****.
10	acladmin	added at: 2024-06-05 07:22:36	REMOTE_ADDR: 172.17.126.20	LOGIN	ADMIN	OK	acladmin	content: Success login user name=acladmin
11		added at: 2024-06-05 08:03:16	REMOTE_ADDR: 172.17.113.13	LOGIN	PASSWORD	OK	SSO - acladmin	content: Correct current password: *****.
12	acladmin	added at: 2024-06-05 08:03:16	REMOTE_ADDR: 172.17.113.13	LOGIN	ADMIN	OK	acladmin	content: Success login user name=acladmin
13		added at: 2024-06-05 08:31:48	REMOTE_ADDR: 10.11.2.153	LOGIN	PASSWORD	OK	SSO - acladmin	content: Correct current password: *****.
14	acladmin	added at: 2024-06-05 08:31:48	REMOTE_ADDR: 10.11.2.153	LOGIN	ADMIN	OK	acladmin	content: Success login user name=acladmin
15		added at: 2024-06-05 09:05:27	REMOTE_ADDR: 172.18.111.164	LOGIN	PASSWORD	OK	acladmin	content: Correct current password: *****.
16	acladmin	added at: 2024-06-05 09:05:27	REMOTE_ADDR: 172.18.111.164	LOGIN	ADMIN	OK	acladmin	content: Success login user name=acladmin
17		added at: 2024-06-05 09:12:34	REMOTE_ADDR: 172.18.111.182	LOGIN	PASSWORD	OK	SSO - acladmin	content: Correct current password: *****.
18	acladmin	added at: 2024-06-05 09:12:34	REMOTE_ADDR: 172.18.111.182	LOGIN	ADMIN	OK	acladmin	content: Success login user name=acladmin
19		added at: 2024-06-05 10:33:24	REMOTE_ADDR: 172.18.111.182	LOGIN	PASSWORD	OK	SSO - acladmin	content: Correct current password: *****.
20	acladmin	added at: 2024-06-05 10:33:24	REMOTE_ADDR: 172.18.111.182	LOGIN	ADMIN	OK	acladmin	content: Success login user name=acladmin
21		added at: 2024-06-05 11:42:30	REMOTE_ADDR: 172.17.126.20	LOGIN	PASSWORD	OK	acladmin	content: Correct current password: *****.
22	acladmin	added at: 2024-06-05 11:42:30	REMOTE_ADDR: 172.17.126.20	LOGIN	ADMIN	OK	acladmin	content: Success login user name=a

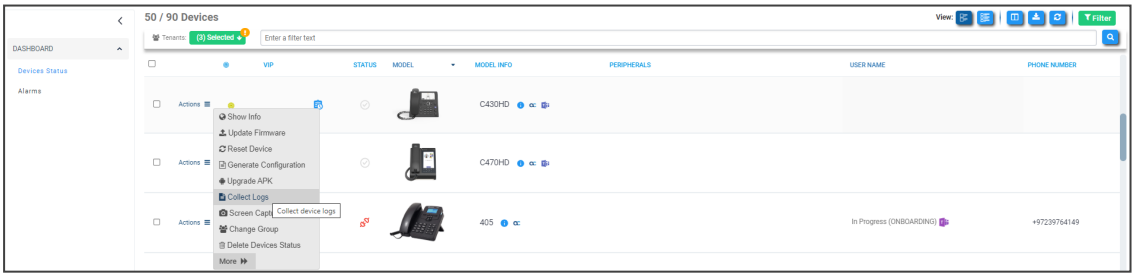
Collecting Logs

Device Manager enables admin to collect logs from AudioCodes devices for debugging purposes without needing to go to the device.

> For detailed information about the logs that are collected, see the device's *User's and Administrator's Manuals* available on AudioCodes' website.

➢ To collect logs:

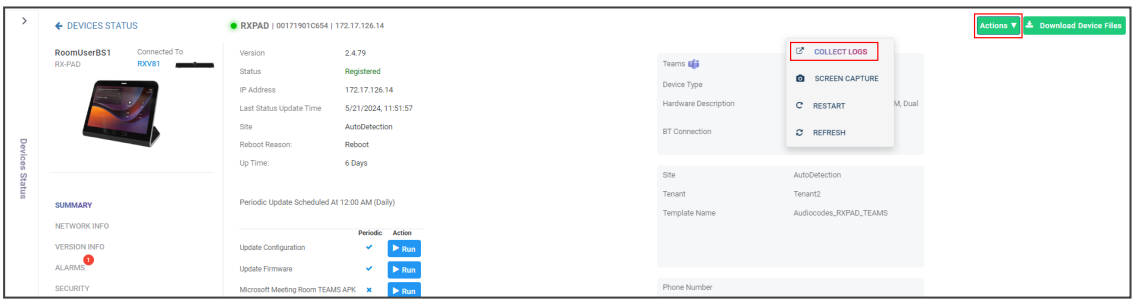
1. In the Devices Status page (**Dashboard** > **Monitor** > **Devices Status**), click **Actions** adjacent to the device from which you want to get logs and then select the **Collect Logs** option from the popup menu.



2. View the notification 'Please wait for the device to upload the log files'.

- This action might take a few minutes depending on the number and the size of the logs. If a device is unavailable or if the action time is extended, a relevant icon and notification is displayed for that device, for example: 'Collect Logs: waiting for the Device'. It might be displayed for some time.
- Log files collected via Device Manager are uploaded in the format of a .zip file. The following zipped file is provided: *bugreport-00908f9d6888-TEAMS_1.14.455-2021-12-15-11-14-06.zip*
  After unzipping the .zip file, the log files become available to admin. The zipped file includes the following log files:
  - ✓ blog files (media logs): app_process32.msrtc-0-3054496316.blog and Skylib-0-3692023773.blog
  - ✓ SessionID_For_Company_Portal_Logs.txt [this is the CP SSDI, not the logs; the logs are sent to the server]
    Logs collected via Microsoft's Teams admin center are included in the bugreport so collection of logs via Device Manager is similar to the collection of logs via Microsoft's TAC. Logs from the TAC include logcat, dumpsys, ANRs, Client Log, Call Policies File, Call Log Info File, Sky lib Log Files, Media Log Files and CP.
    Other logs collected are:
  - ✓ AudioCodes' configuration is packed into the bugreport
  - ✓ DSP logs

3. [Alternatively] Select the **Show Info** option -OR- click the device image. Make sure of the device's identity and then from the **Actions** menu, select the **Collect Logs** option.



4. After the logs are collected, the Devices Status page displays

5. Click the icon to download the logs.

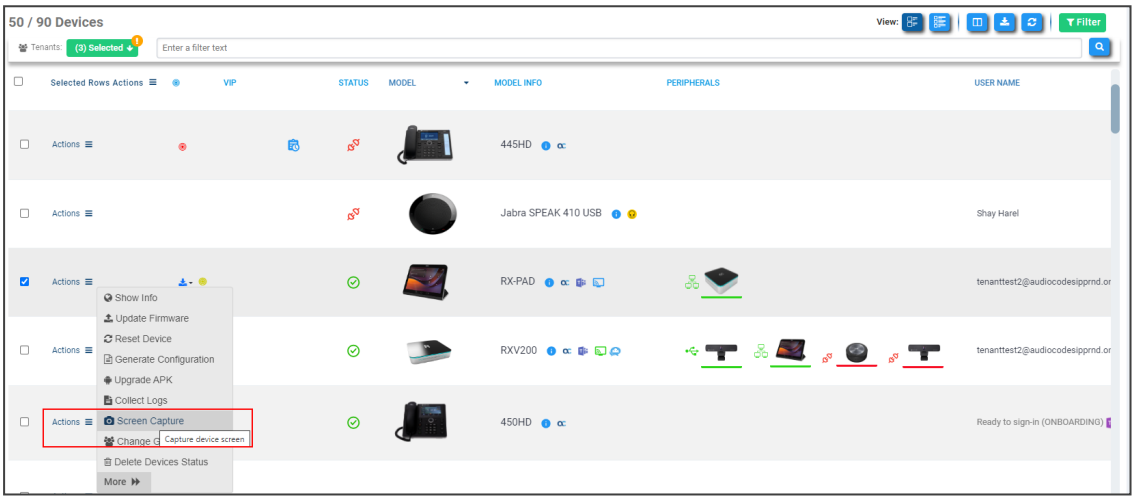
Capturing a Screen to Send to FAE

Device Manager enables admin to capture a device screen in order for admin to more effectively collaborate with FAEs and debug | troubleshoot issues. The feature enables capturing the device's main screen as well as the device's Expansion Module (sidecar) in the case of phone models with a sidecar. The feature triggers a screen capture into a jpg file on the device.

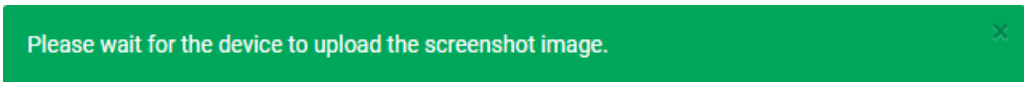
The feature complies with customer requests for AudioCodes Android Device Utility features and capabilities to be available from Device Manager because customer IT security regulations prohibit installation of unofficial third-party applications on employee PCs. See also the *Android Device Utility User's Manual* available here.

➢ To capture a screen:

1. In Device Manager, open the Devices Status page (**Monitor** > **Devices Status**).
2. Select a Tenant from the **Tenants** drop-down and then click .
3. Click Actions ≡ in the same row as the device whose screen you want to capture.



4. From the menu that pops up, select **Screen Capture**; the following notification is briefly displayed.

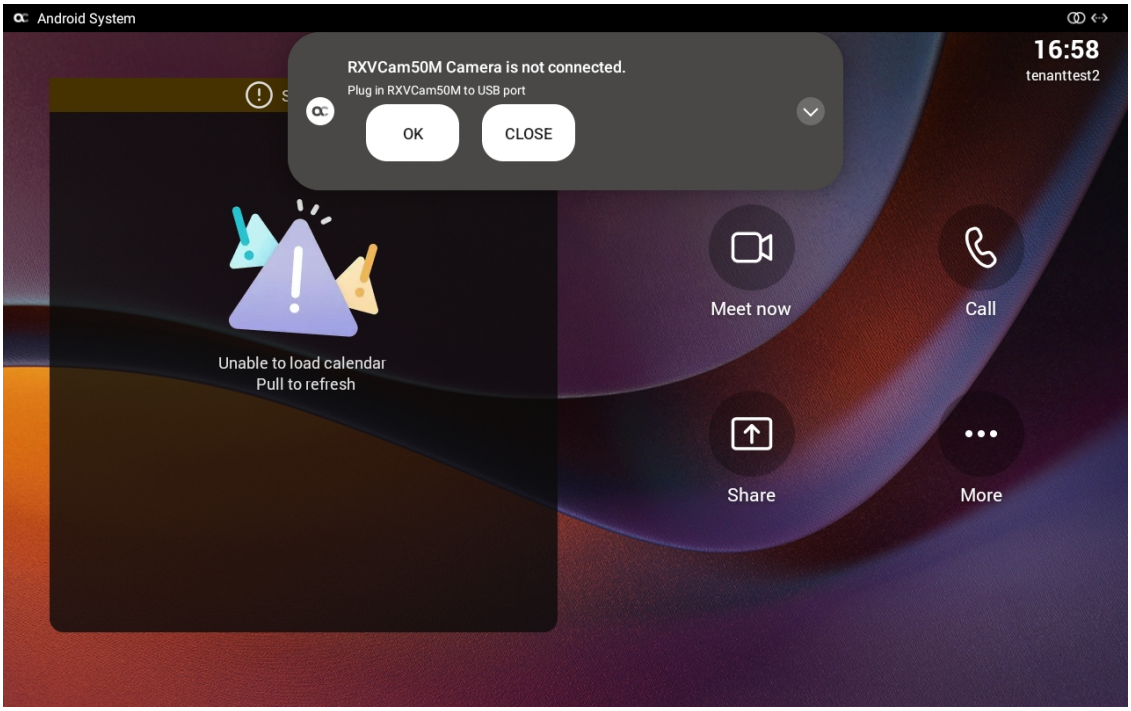


5. View in the Devices Status page the download icon displayed in the same row as the device whose screen you captured.

6. Click the download icon.

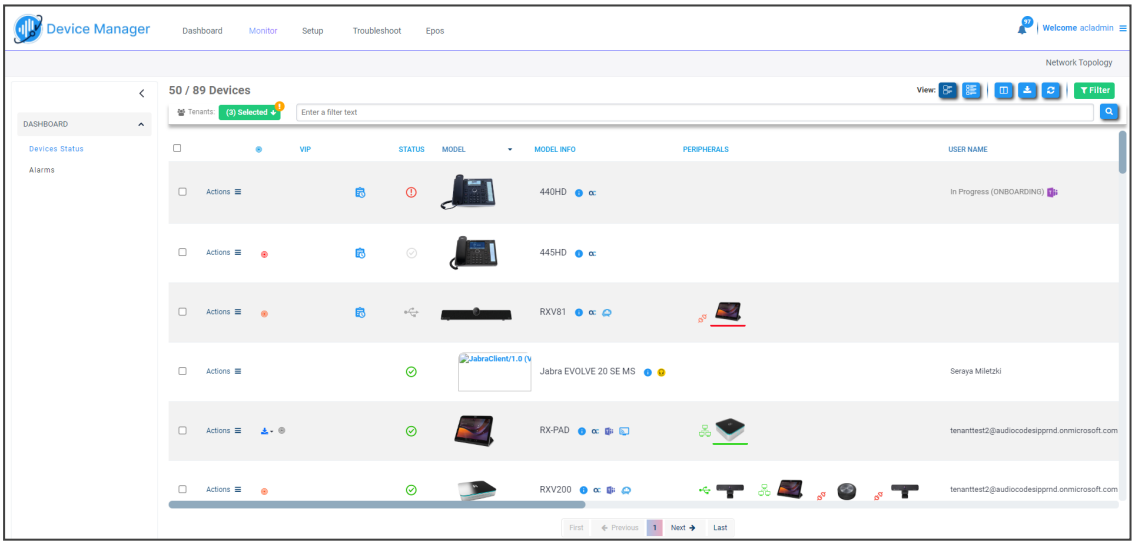
- The tooltip displayed lists *multiple* files in *chronological* order.
- The tooltip may also list *debug log files*.

7. Click the tooltip; a downloaded indication appears in the upper right corner of the page.
8. Select the jpg image file you require; the screen capture opens in an image editor.



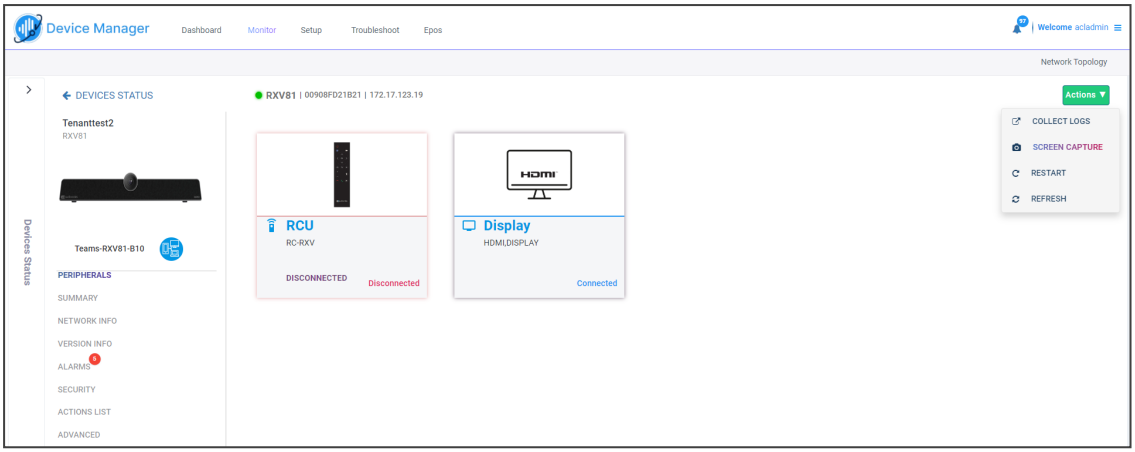
➢ To alternatively capture a screen:

1. In Device Manager, open the Devices Status page (**Monitor** > **Devices Status**).

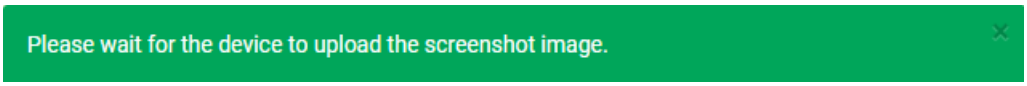


2. Select a Tenant from the **Tenants** drop-down and then click  .

3. Click the image of the device whose screen you want to capture (or click **Actions** in the same row as the device and then select **Show Info** from the menu that pops up).

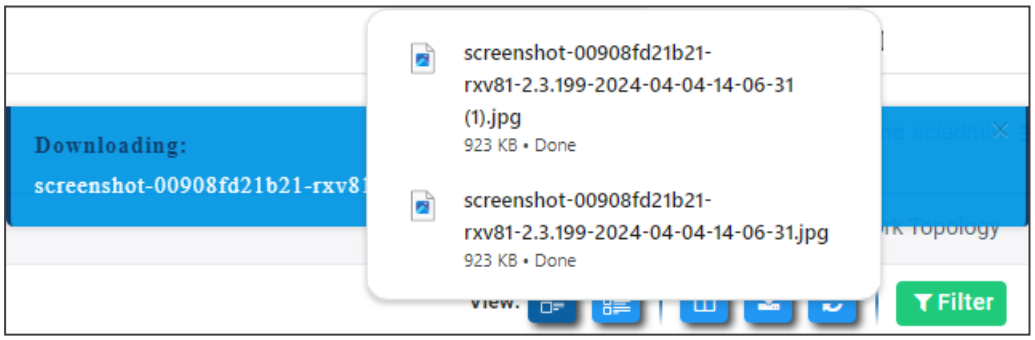


4. From the **Actions** drop-down, select **Screen Capture**.

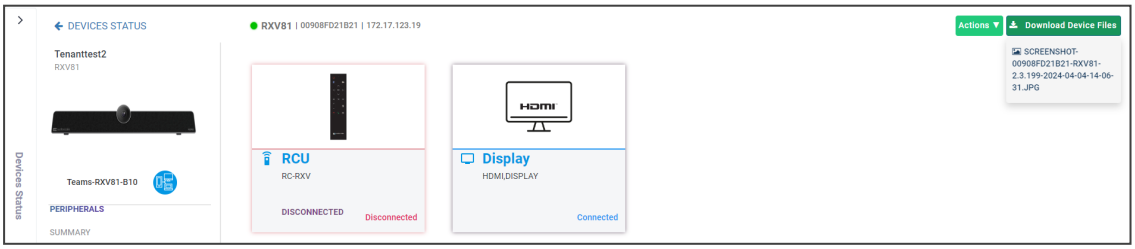


5. View in the Devices Status page the download icon displayed in the same row as the device whose screen you captured.

6. Click the icon or the tooltip; a downloaded indication appears in the upper right corner of the page.



7. Click the image of the device whose screen you captured or click **Actions** and select **Show Info**.



8. View the **Download Device Files** button now displayed in the uppermost right corner. Click it and download the file.

9. Send the file as an attachment to your FAE to more effectively debug | troubleshoot the issue.

7 Configuring Third-Party Vendor Devices

For detailed information about configuring third-party vendor devices, see also the *Device Manager for Third-Party Vendor Products Administrator's Manual*.

Performing Poly Configuration

Poly Trio devices, Poly VVX devices and Poly CCX 500/600 devices can be *automatically provisioned with templates per model* from AudioCodes' provisioning server.

The feature is an AudioCodes proprietary feature configured from the 'Poly Configuration' page in Device Manager (**Setup** > **Configuration** > **Poly Configuration**).

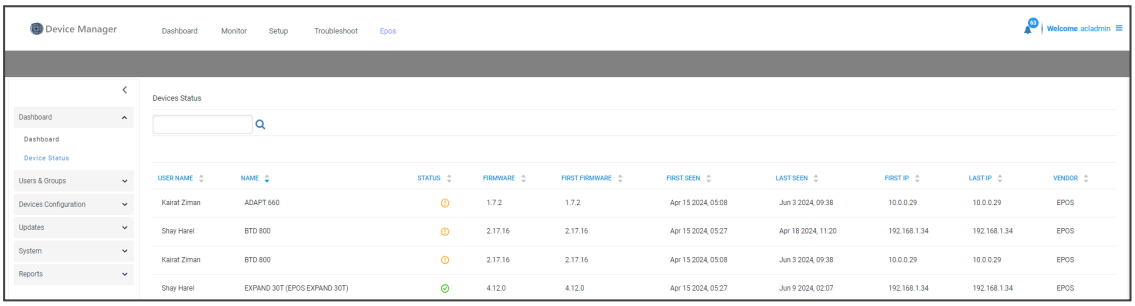
For more information, see the *Device Manager for Third-Party Vendor Products Administrator's Manual* available from AudioCodes.

Performing EPOS Configuration

Device Manager enables admin to manage and monitor EPOS (Sennheiser) headset devices (beta version). EPOS have a cloud-based EPOS Manager. AudioCodes' Device Manager reflects the EPOS Manager.

➢ To configure EPOS device settings:

- From any page in Device Manager, click the **EPOS** menu.



For detailed information about configuring EPOS device settings, see the:

- *EPOS Manager Admin Manual* available here
- *Device Manager for Third-Party Vendor Products Administrator's Manual*

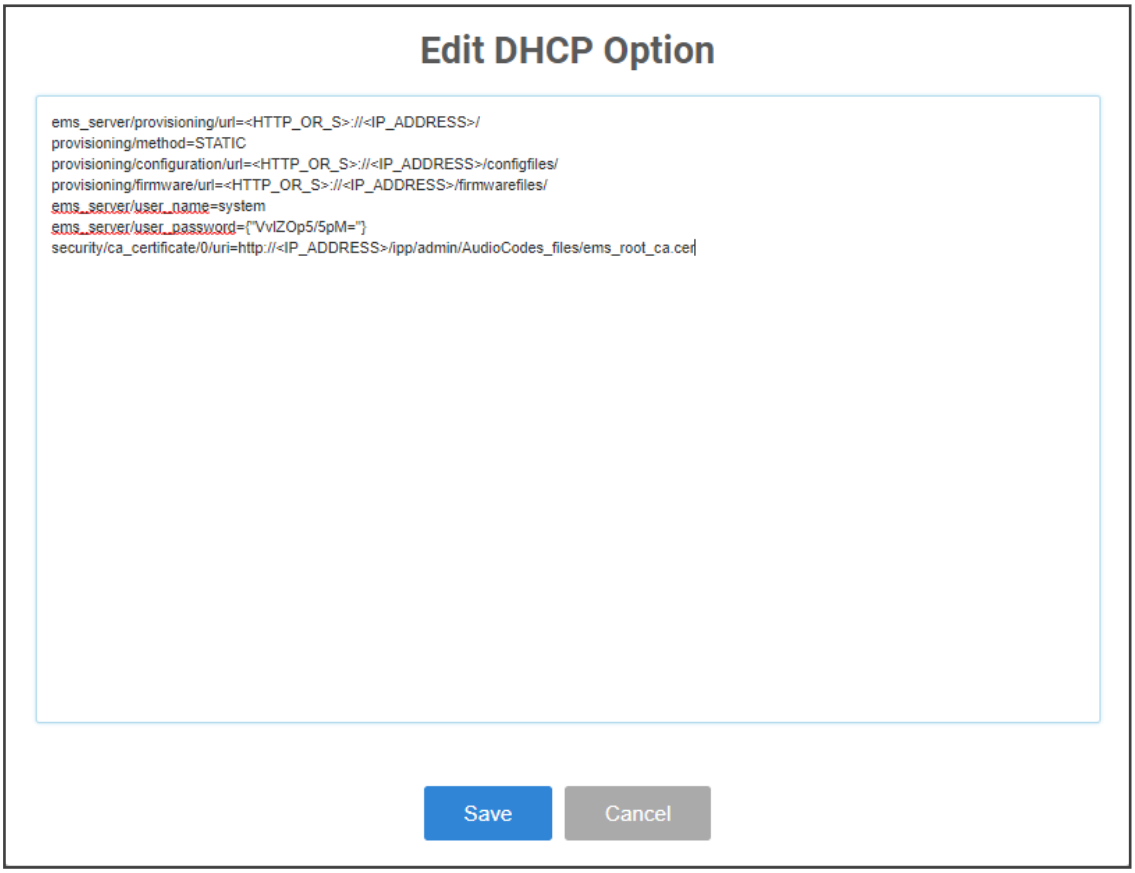
Configuring Phones to Operate in an OVR Deployment

You can configure phones to operate in an OVR (One Voice Resiliency) deployment. See the *One Voice Resiliency Configuration Note* for a detailed description of OVR.

➢ To configure phones to operate in an OVR deployment:

1. Open the DHCP Options Configuration page (**Setup** > **Settings** > **DHCP Options Configuration**).

2. Click the **Edit dhcpoption160.cfg template** button.



3. Customize dhcpoption160.cfg. Add the following lines:

```
outbound_proxy_address=<SBC IP address>
lync/sign_in/fixed_outbound_proxy_port=<SBC listening port>
lync/sign_in/use_hosting_outbound_proxy=1
```

4. Click **Save**; the phones are configured to operate in an OVR environment.

After configuring phones to operate in an OVR environment, configure their template with the same settings.

This page is intentionally left blank.

International Headquarters

6 Ofra Haza Street

Naimi Park

Or Yehuda, 6032303, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-91227