

# Device Manager

Version 8.0.3000



## Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: January-05-2022

## WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

## 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
<a href="#">Device Manager for Third-Party Vendor Products Administrator's Manual</a>
<a href="#">Device Manager Administrator's Manual</a>
<a href="#">One Voice Operations Center IOM Manual</a>

Document Name
<a href="#">One Voice Operations Center User's Manual</a>
<a href="#">IP Phones Users Manuals</a>
<a href="#">Room Experience (RX) Suite</a>

## Document Revision Record

LTRT	Description
91210	Initial release

---

## Table of Contents

---

<b>1</b>	<b>Introduction</b>	<b>1</b>
	About Device Manager	1
	About this Guide	1
	Prerequisites	1
<b>2</b>	<b>Deploying the Devices</b>	<b>3</b>
	Device Manager Discovery	3
	Configure DHCP Option 160	3
	Redirect Server	4
	Static Provisioning URL	4
	Templates Mapping	4
	Connect the Devices	5
	OVOC Bandwidth Considerations	6
<b>3</b>	<b>Best Practices   Recommendations</b>	<b>7</b>
	Define a Network Topology	7
	Check OVOC SSL Certificate Validity	8
	Change the Admin Password	11
	Update Firmware in a Pilot Site First	13

# 1 Introduction

AudioCodes' Device Manager is a component of AudioCodes' One Voice Operations Center (OVOC) that enables network administrators to manage AudioCodes devices such as IP phones, Room Experience (RX) devices and other peripherals in their IP telephony networks.

Up to 4000 Teams phones, devices and peripherals across globally distributed corporations can be provisioned and maintained using the Device Manager.

The Device Manager client, which network administrators can use to connect to the server, can be any standard web browser supporting HTML5: Microsoft's Edge, Internet Explorer version 11 and later, Chrome (recommended) or Firefox.

## About Device Manager

For more information about the Device Manager, see AudioCodes' website [here](#).

## About this Guide

This *Deployment Guide* shows network administrators how to deploy devices in their networks using the Device Manager.

- The guide focuses on the *critical steps* administrators must take to deploy devices.
- For *non-critical* procedures, administrators are referred to the *Device Manager Administrator's Manual*.

This guide exclusively covers deployment of *Teams devices*. Best practices and recommendations are also included.

## Prerequisites

Before deployment, make sure:

- OVOC is installed and the license is valid, including endpoints licenses
- OVOC FQDN is set up in your DNS server
- OVOC SSL certificate
  - Make sure the OVOC certificate is signed by a well-known CA (Certificate Authority). Make sure:
    - ◆ The certificate common name (CN) or subject alternative name (SAN) matches the OVOC FQDN.
    - ◆ The certificate expiration is valid.
  - Using the customer organization's CA:
    - Staging CA - the device should download the enterprise CA from the OVOC via HTTP in a trusted environment.

- i. Upload CAs to the OVOC [In the 'Generated Configuration Files' page of the Device Manager (**Setup > Configuration > Generated Config Files**)]
- ii. Set the DHCP Options 160 URL to use HTTP.
- iii. Add the following lines to the 'Edit DHCP Option' screen [accessed from the link **Edit DHCPoption160.cfg Template** in the DHCP Options Configuration page of the Device Manager (**Setup > Settings > DHCP Options Configuration**)]:

```
security/ca_certificate/0/uri=http://<OVOC_FQDN>/configfiles/<CA1_filename>  
security/ca_certificate/1/uri=http://<OVOC_FQDN>/configfiles/<CA2_filename>
```



If the OVOC is installed in an on-premises trusted environment, the customer can use the HTTP option, in which case there is no need for SSL certificate and/or FQDN). See also [Check OVOC SSL Certificate Validity](#) on page 8.

## 2 Deploying the Devices

Perform the following operations to deploy devices:

- Disable or configure C band (see [OVOC Bandwidth Considerations](#) on page 6)
- Configure DHCP Option 160 (see [Configure DHCP Option 160](#) below)
  - If DHCP Option 160 is unsuccessful, use the AudioCodes Redirect Server provisioning method (see [Redirect Server](#) on the next page)
  - If DHCP Option 160 and the Redirect Server methods are unsuccessful, use the Static Provisioning URL provisioning method (see [Static Provisioning URL](#) on the next page)
- Map device model to tenant for template allocation (see [Templates Mapping](#) on the next page)
- Connect the devices (see [Connect the Devices](#) on page 5)

### Device Manager Discovery

Devices in the network 'discover' the Device Manager using the following methods:

- DHCP Option 160 (recommended) (see [Configure DHCP Option 160](#) below)
- Redirect Server (see [Redirect Server](#) on the next page)
- Static Provisioning URL (see [Static Provisioning URL](#) on the next page)

### Configure DHCP Option 160

Start deploying IP phones in your enterprise's network by configuring DHCP Server Option 160 with a tenant URL (mandatory). Pointing the DHCP Server to a tenant URL enables the phones to automatically be provisioned with their .img firmware file and .cfg configuration file after they're plugged in to the network (as described in [Connect the Devices](#) on page 5). When the phones are later signed in, they're automatically added to the Device Manager which loads their specific .cfg files to them.



Before configuring DHCP Option 160, take OVOC bandwidth considerations into account, as explained in [OVOC Bandwidth Considerations](#) on page 6.

#### ➤ To configure DHCP Option 160 with a tenant URL:

1. In the Device Manager, open the DHCP Options Configuration page (**Setup > Settings > DHCP Options Configuration**).

**Figure 2-1: DHCP Options Configuration**

- Under section SYSTEM URLS, copy the URL adjacent to 'OVOC accesses phones directly' to DHCP server Option 160:

**http://10.3.180.44/firmwarefiles;ipp/dhcption160.cfg**



- DHCP Option 66/67 can also be used, instead of DHCP Option 160.
- For the *tenant-specific* provisioning URL, click the **Advanced: DHCP Option 160 With Tenant Configuration** link located lowermost in the page (see the *Device Manager Administrator's Manual* for more information).

## Redirect Server

The provisioning URL and device MAC address can alternatively be configured in AudioCodes' Redirect Server.

## Static Provisioning URL

If the DHCP Option 160 provisioning method or the AudioCodes Redirect Server provisioning method is unsuccessful, *manually* enter the provisioning URL from the device using the command line:

```
provisioning/method=STATIC
provisioning/configuration/url=Provisioning URL
```

## Templates Mapping

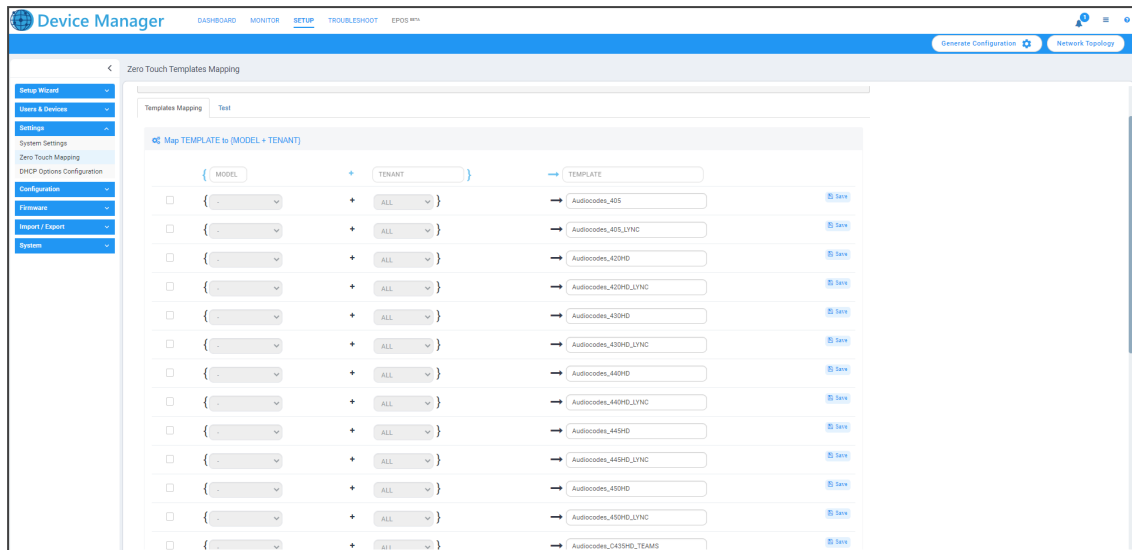
After defining tenants in the OVOC (see [Define a Network Topology](#) on page 7), map each device model in your network to a tenant for template allocation. After mapping, each device registered to the Device Manager will get its template according to {MODEL + TENANT}.

### ➤ To map each device's template:

- Open the Templates Mapping page (**Setup > Settings > Zero Touch Mapping**).



Figure 2-2: Templates Mapping



2. Deselect irrelevant device models that are not deployed in your enterprise's network and select relevant device models that are deployed in your network.
3. Choose the template according to {MODEL + TENANT}. Next to each selected model, select a tenant from the dropdown; a template associated with your selection is displayed.

Example:



The templates are part of the Device Manager's database and are supplied with the Device Manager. Though the Device Manager provides every device model with a ready-to-use template, each can be edited if necessary (**Setup > Configuration > Templates**). See the *Device Manager Administrator's Manual* for more information.

4. After selecting to each device model and tenant, click **Save**.

## Connect the Devices

After configuring DHCP Option 160 as shown in [Configure DHCP Option 160](#) on page 3 and mapping each device model to a tenant as shown in [Templates Mapping](#) on the previous page, connect the devices to power and to the IP network. The devices will then get their IP addresses from the DHCP Server and their configuration template will be allocated.

After connecting the devices, sign in to them (see the device's *Quick Guide* or *User's and Administrator's Manual* for more information if necessary); the Device Manager will then display the devices in the Monitor page.

Figure 2-3: Monitor Page

Actions	VIP	BTOE	USER NAME	PHONE NUMBER	MODEL	FIRMWARE	LAST UPDATE STATUS	MAC ADDRESS	IP ADDRESS	TENANT
Actions			noame@audiocodes.com		C47HD	TEAMS_1_16.123	10.11.2021 13:54:21	009086b27f	10.0.0.5 / 5.22.135.209	IL
Actions			Dvora Azarov	+9729764816	44SHD	UC_3_4.6.576	10.11.2021 13:23:23	00908f9c1c99	172.17.131.16 / 37.142.12.66	IL
Actions			szqa11@audiocodesppnd.onmicrosoft.com		C47HD	TEAMS_1_16.116	10.11.2021 13:19:24	009086b48e	192.168.3.105 / 58.251.26.2	IL
Actions			TeamsAuto@audiocodesppnd.onmicrosoft.com		C43SHD	TEAMS_1_15.102_DORv1	10.11.2021 12:10:54	009086c082f	10.59.2.218 / 195.189.193.1	IL
Actions			DavidR@audiocodes.com		C45HD	TEAMS_1_14.449	10.11.2021 13:02:09	009086b1107	192.168.0.29 / 86.245.221.186	IL
Actions			Teamspphone4@SESPartnerEngTest.onmicrosoft.com		C43SHD	TEAMS_1_12.33	10.11.2021 12:47:59	009086d68b	192.168.1.4 / 103.153.105.70	IL
Actions			SakuraAutoMeeting@audiocodesppnd.onmicrosoft.com		RVX100	DWC_1.0	10.11.2021 12:37:29	6C4B90E315ED	172.17.131.26 / 37.142.12.66	IL
Actions			teamsdeviceauto14@3P.onmicrosoft.com		RVX80	TEAMS_1_13.360	10.11.2021 12:33:15	06D4610022d	10.50.10.152 / 14.141.117.86	IL
Actions			szqa19@audiocodesppnd.onmicrosoft.com		C47HD	TEAMS_1_14.455	10.11.2021 12:08:07	009086b49d	172.17.179.73 / 58.251.26.2	IL
Actions			Shay Harel		Jabra Evolve 75	2.4.0	10.11.2021 12:01:03	745C4B5E9C66	10.33.2.127 / 195.189.193.1	IL
Actions			david@audiocodes.com		C45HD	TEAMS_1_8.288	10.11.2021 11:54:46	009086af5a0	192.168.1.111 / 49.248.99.11	IL
Actions			Herbert@audiocodesppnd.onmicrosoft.com		C45HD	TEAMS_1_16.139	10.11.2021 11:37:23	0090869d88a	10.16.2.141 / 195.189.193.1	IL
Actions			Shay Harel		C43SHD	TEAMS_1_14.454	10.11.2021 11:30:44	009086c084d	10.16.2.188 / 195.189.193.1	IL
Actions			Shay Harel		Jabra Link 370	1.21.0	10.11.2021 11:29:32	745C4B6A501E	10.33.2.127 / 195.189.193.1	IL
Actions			Shay Harel		C43SHD	TEAMS_1_14.454	10.11.2021 11:21:02	009086c0861	10.0.0.5 / 188.120.142.179	IL
Actions			gal@audiocodes.com		C43SHD	TEAMS_1_12.54	10.11.2021 10:43:08	0090869db0de	10.59.30.17 / 195.189.193.1	IL

## OVOC Bandwidth Considerations



Network administrators must take OVOC bandwidth considerations into account when deploying devices. Periodic updates of firmware files in deployments with large numbers of phones may consume excessive OVOC bandwidth. Moreover, customers whose deployments include phones mixed and integrated with SBC devices must additionally account for anticipated SBC CAPS (Calls per Second) when calculating bandwidth.

Note therefore that:

- Customers who have deployed *only phones* are recommended to *disable C band entirely*.
- Customers whose deployment includes phones mixed and integrated with SBC devices should configure C band to simultaneously manage phone firmware file updates as well as SBC CAPS. For more information, contact AudioCodes Technical Support.

## 3 Best Practices | Recommendations

Network administrators should follow these best practices and recommendations:

- Define a Network Topology (see [Define a Network Topology](#) below)
- Check the validity of the OVOC | Device Manager server's SSL certificate (see [Check OVOC SSL Certificate Validity](#) on the next page)
- Change the Admin password of all devices in a Site (see Change the Admin Password of all Devices in a Site)
- Update firmware in a pilot Site first (see [Update Firmware in a Pilot Site First](#) on page 13)

### Define a Network Topology

When adding devices to a network, best practice is to define a Network Topology in which to add your devices, i.e., define tenants, regions, sites and groups. AudioCodes recommends implementing this practice to ensure correct provisioning.



AudioCodes' OVOC is used to define a Network Topology. For more information, see the *OVOC User's Manual*.

Configure Network Topology based on your organization's requirements and then link to each topology configuration level. Topology configuration levels are shown below.

- **Template:** Each template represents a *device model* (C470HD, RXV100, etc.). Use a different template per each device model. See also [Templates Mapping](#) on page 4.



If the same model features both Teams *and* Generic SIP (such as the C450HD phone), use a *different template for each flavor*.

- **Tenant**
  - In a multi-tenant deployment, a tenant represents a real tenant.
  - In a non multi-tenant deployment, a tenant is just a group of devices grouped together.
  - You can add a tenant to DHCP Option 160 provisioning URL (see also [Configure DHCP Option 160](#) on page 3 in the second note).
- **Site:** Only configure a Site for a network-related configuration like VLAN. Configure it in the Site Configuration page in the Device Manager (**Setup > Configuration > Site Configuration**). See the *Device Manager Administrator's Manual* for more information.
- **Group:** Configure an Endpoints Group for a *logical* group of users like 'Management' or 'Demo'. See the *OVOC User's Manual* for more information (since Endpoints Groups are configured in the OVOC).

- Manually associate devices with a group in the 'Group Configuration' page of the Device Manager (**Setup > Configuration > Group Configuration**).
- Optionally make it Zero Touch by adding the Group to the DHCP Option 160 provisioning URL.

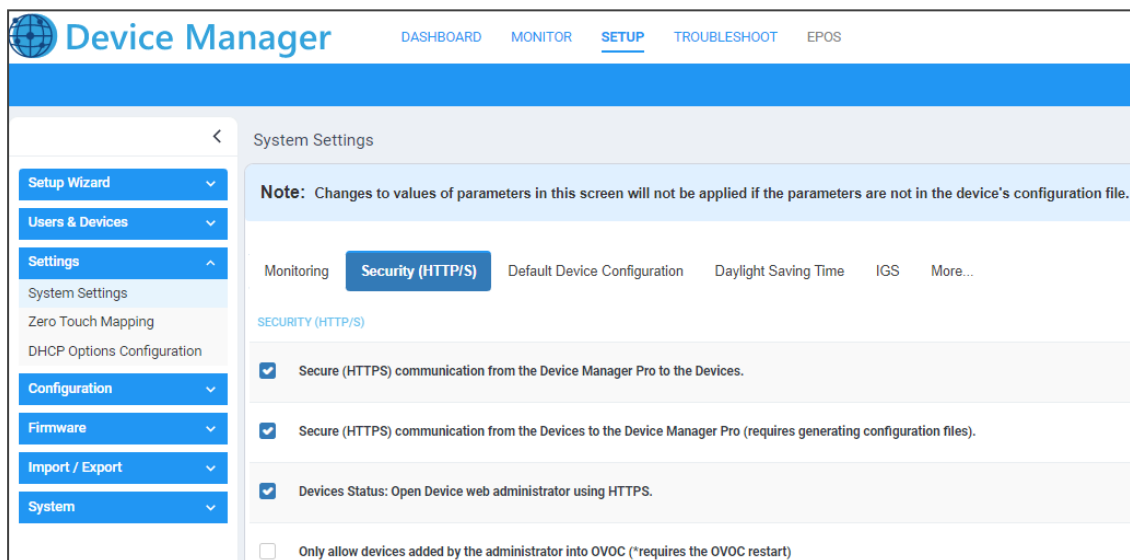
## Check OVOC SSL Certificate Validity

Best practice is to check the validity of the OVOC server's SSL certificate. AudioCodes recommends implementing this practice to avoid deployment problems that may occur if the certificate is invalid.

### ➤ To check the validity of the certificate:

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

**Figure 3-1: System Settings - Security (HTTP/S) tab**



2. Determine from the page whether you're operating with HTTP or HTTPS.
  - If you're operating with HTTP (in the page you'll observe that **Secure (HTTPS)** will be *unchecked*), *certificate validity is a non issue* but note however that HTTP should only be used in a trusted network.
  - If you operating with HTTPS (in the page you'll observe **Secure (HTTPS)** will be *checked*), *certificate validity is a critically important issue*.
    - ◆ Make sure the OVOC | Device Manager SSL certificate is signed by a well-known CA (Certificate Authority) for the HTTPS connection to be established with AudioCodes' Android-based Teams devices.
    - ◆ You can view a list of well-known CAs [here](#).

- ◆ Alternatively, a root-ca certificate / intermediate CA certificate can be loaded to the device's trust store via 802.1x or configuration file parameter `'/security/ca_certificate/[0-4]/uri'`.



AudioCodes' Android-based Native Teams devices are shipped with a unique certificate which is signed by AudioCodes Root CA. Network administrators can install a third-party certificate on AudioCodes' Teams devices in the customer's trusted environment. Follow these guidelines when replacing the existing trusted CA:

- The device certificate URL will only be valid if no SCEP server URL is present
- Use the following two parameters to set the device certificate in the device's configuration file:
  - ✓ `security/device_certificate_url=http://<server-ip>/device.crt`
  - ✓ `security/device_private_key_url=http://<server-ip>/device.key`

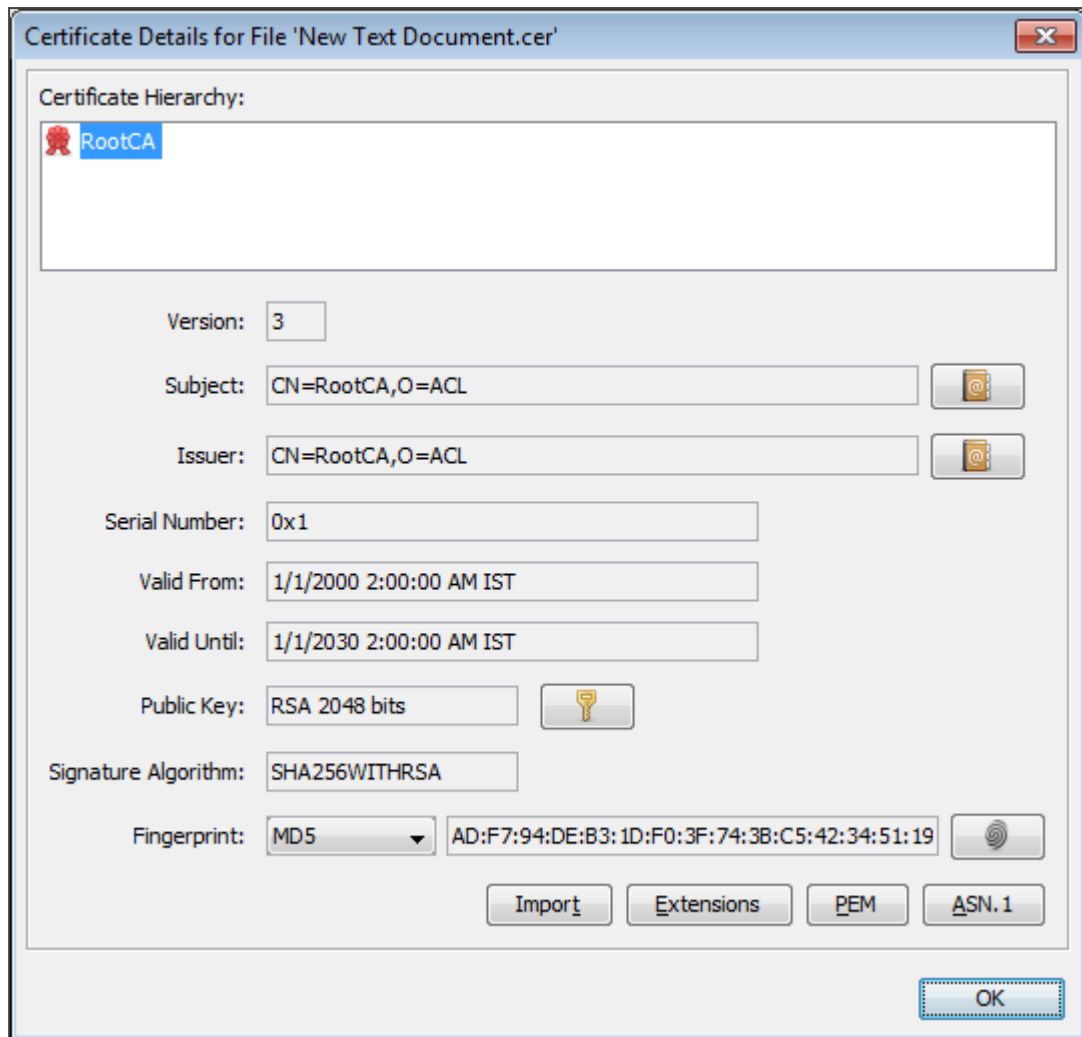
3. Make sure that:

- The certificate common name (CN) or subject alternative name (SAN) matches the Device Manager's FQDN.
- The certificate expiration is valid.



Signing the certificate with AudioCodes' CA will apply when AudioCodes signs for customers. Customers must then generate a Certificate Signing Request (CSR) and a license request, and send it to AudioCodes.

AudioCodes' Android-based Native Teams devices validate the Device Manager's identity using this well-known Root CA. The figure below shows the Root CA with which AudioCodes ships its devices. For the initial connection, the Device Manager accesses devices using this Root CA. Once a successful secured connection has been established between the device and the Device Manager, the network administrator can replace the Root CA on the Device Manager and on the phone and re-establish the connection leveraging any Private Root CA.



-----BEGIN CERTIFICATE-----

MIIDMTCCAhmGAWIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKEwNBQ0wx

DzANBgNVBAMTBiJvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBa

MB8xDDAKBgNVBAoTAF0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqhkiG9w0B

AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEEZbfZL0a

EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKkIKsGsvGWmSRNULV01CW+TX2VJN73+hh

V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4lg9kfd/ma9Czl5koESLlw/inLj/r+rD96

```
mUcPEIWkKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKK
S
EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhIhFL29nMfnaFATSS3rgGaFISvl1ZS

esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMB
gNV

HRMEBTADAQH/MB0GA1UdDgQWBBDQXySn9hz15IDraZ+iXddZGReB+zBHB
gNVHSME

QDA+gBQDXySn9hz15IDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQU
NMMQ8w

DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywo
mmWWJnH3

JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDFK
kxMp

0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXAYAJ6XgvTfN2BtyZk9Ma8WG+H1hNv
vTZY

QLbWsjQdu4eFniEufeYDke1jQ6800LwMIFlc59hMQCeJTEnRx4HdJbJV86k1gBU
E

A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwwLpEP22nYwvB28dq3JetlQ
Kwu
XC4gwl/o8K2wo3pySLU9Y/vanxXCr0/en5I3RDz1YpYWmQwHA8jJlu8rxdhr+VNQ
Zv6R/Ys=
-----END CERTIFICATE-----
```

## Change the Admin Password

Best practice is to change the Admin password **every three or six months**. AudioCodes recommends implementing this practice to guarantee that only the network administrator will be able to gain access to the Device Manager to perform management operations.



Typically, one Admin Password is defined for all the devices in the enterprise network.

### ➤ To change the Admin Password:

1. Use the Teams IP Phone Utility, available from AudioCodes, to obtain the password.

Figure 3-2: Teams IP Phone Utility - PWD

Teams IP-Phone Utility V1.0.21

Teams Operations

Single-Operations

Teams IP-Phone Address: 10.22.13.106 SSH Connect SSH Disconnect

Username: admin

PWD: 1234

Model: C450HD

Firmware file (\*.zip) Browse Submit

Command: Send

Multi-Operations

Firmware Folder (\*.zip) Browse

Certs Folder (\*.crt, \*.pem) Browse

Phones IP list (\*.txt) Browse

Bulk Upgrade

Total Number of IPPs: Firmware Version:

Current Uploaded IP Address Total Upgraded IPPs:

Submit

Switch to Teams Switch to Skype Factory Default Sign-Out Admin Agent Restart Download Certs Convert BW BW info IPP Version

Get Version Tcpdump Get Diagnostics Get Bugreport Start Syslog Stop Syslog Screen Capture Screen Record Call Logs Start DSP Record Stop DSP Record

PC IP Address:

Syslog UDP port: 514

DSP Record port: 50000

PC folder: Browse

Connected to: 10.22.13.106

2. In the Device Manager, open the Tenant Configuration page (**Setup > Configuration > Tenant Configuration**).

Figure 3-3: Tenant Configuration - Configuration Key

Device AudioCodes\_C450HD\_TEAMS Configuration Template

Edit configuration template values

Configuration Set: C450HD\_TEAMS\_NATIVE

Configuration Key: admin/default\_password

Configuration Value: Type text. Add

CONFIGURATION KEY	CONFIGURATION VALUE
audio/dtch/handset(in_background_noise_suppression	1
ems_server/keep_alive_period	1
ems_server/provisioning/url	%TCS_HTTP_OR_S%/%TCS_HTTP_PROXY_IP%/%TCS_HTTP_PROXY_PORT%/
ems_server/user_name	%TCS_Line1AuthName%
ems_server/user_password	%TCS_Line1AuthPassword%
personal_settings/language	%TCS_Language%

Actions

Edit Template Download Template Upload Template

Generate Global Configuration Template Show Place Holders Restore To Default

3. From the 'Configuration Key' dropdown, select **admin/default\_password** as shown in the preceding figure.
4. Open the Device Configuration Templates page (**Setup > Configuration > Templates**).



**Figure 3-4: Device Configuration Templates**

Devices Configuration Templates						+ Add New Template
	AudioCodes_C450HD_LYNC	LYNC - The 450HD IP Phone is a high-end, e...	x	ALL		<a href="#">Edit</a> <a href="#">Delete</a>
	AudioCodes_C435HD_TEAMS	C435HD template configuration	x	ALL		<a href="#">Edit</a> <a href="#">Delete</a>
	AudioCodes_C448HD_LYNC	The template file of AudioCodes_C448HD_LYN...	x	ALL		<a href="#">Edit</a> <a href="#">Delete</a>
	AudioCodes_C448HD_TEAMS	The template file of AudioCodes_C448HD_TEA...	o	ALL	C448HD_TEAMS	<a href="#">Edit</a> <a href="#">Delete</a>
	AudioCodes_C450HD_LYNC	The template file of AudioCodes_C450HD_LYN...	o	ALL	C450HD	<a href="#">Edit</a> <a href="#">Delete</a>
	AudioCodes_C450HD_TEAMS	The template file of AudioCodes_C450HD_TEA...	o	ALL	C450HD_TEAMS	<a href="#">Edit</a> <a href="#">Delete</a>

5. Click the **Edit** button adjacent to the model (for example, **AudioCodes C450HD Teams**).

**Figure 3-5: Edit Template**

### Edit template

```

<profile>user</profile>
<encrypt_mode>0</encrypt_mode>
<name>%ITCS_mac%.cfg</name>
<destinationDir>%ITCS_destination%</destinationDir>
<data><![CDATA[include AudioCodes_C450HD_global_TEAMS_empty.cfg
ems_server/keep_alive_period=1
provisioning/configuration/url=%ITCS_HTTP_OR_S%://%ITCS_ServerIP%/configfiles/
provisioning/method=STATIC
provisioning/period/daily/time=0:00
provisioning/period/hourly/hours_interval=24
provisioning/period/type=DAILY
provisioning/period/weekly/day=SUNDAY
provisioning/period/weekly/time=0:00
provisioning/random_provisioning_time=120
provisioning/redirect_server_url=https://redirect.audiocodes.com
ems_server/user_name=%ITCS_Line1AuthName%
ems_server/user_password=%ITCS_Line1AuthPassword%
provisioning/firmware/url=%ITCS_HTTP_OR_S%://%ITCS_ServerIP%/firmwarefiles/%ITCS_FirmwareFile%
ems_server/provisioning/url=%ITCS_HTTP_OR_S%://%ITCS_HTTP_PROXY_IP%:%ITCS_HTTP_PROXY_PORT%/
personal_settings/language=%ITCS_Language%
audio/drc/handset/in_background_noise_suppression=1
zzz1_tenant_cfg=ENABLE
zzz21_group_cfg=ENABLE
zzz2_site_cfg=ENABLE
zzz3_user_cfg=ENABLE
]]>
</data>
</file_config>
</iphonestemplate>
                
```

Save
Cancel

6. Add the password in the 'Edit template' screen as a .cfg configuration file value (the Admin Password is changed manually in the .cfg configuration file) and click **Save**. You've successfully changed the Admin password.

## Update Firmware in a Pilot Site First

Best practice is to first update firmware in a pilot site. AudioCodes recommends implementing this practice as a 'safety-first' precaution.

**This page is intentionally left blank.**

### **International Headquarters**

1 Hayarden Street,  
Airport City  
Lod 7019900, Israel  
Tel: +972-3-976-4000  
Fax: +972-3-976-4040

### **AudioCodes Inc.**

200 Cottontail Lane  
Suite A101E  
Somerset NJ 08873  
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>

©2022 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-91210

