Deployment Guide

*AudioCodes One Voice Operations Center (OVOC)*

# Device Manager

Version 8.2

audiocodes

# 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: May-11-2023

## 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 |
|---|
| Device Manager for Third-Party Vendor Products Administrator's Manual |
| Device Manager Administrator's Manual |
| One Voice Operations Center IOM Manual |

| Document Name |
| --- |
| One Voice Operations Center User's Manual |
| IP Phones Users Manuals |
| Room Experience (RX) Suite |

## Document Revision Record

| LTRT | Description |
| --- | --- |
| 91210 | Initial release |
| 91210 | Aligned with 8.2 |

# Table of Contents

# 1 Introduction

AudioCodes' Device Manager is a component of AudioCodes' One Voice Operations Center (OVOC) that enables network administrators to manage AudioCodes devices such IP phones, Meeting Room 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: Chrome (recommended), Microsoft Edge 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:

1. Disable or configure C band (see Disabling / Configuring C Band below)
2. Configure DHCP Option 160 for Device Manager discovery (recommended) (see Configure DHCP Option 160 below)
   - If DHCP Option 160 is unavailable, use the AudioCodes Redirect Server provisioning method (see Redirect Server on the next page)
3. Map device model to tenant for template allocation (see Templates Mapping on the next page)
4. Connect the devices (see Connect the Devices on page 5)

## Disabling / Configuring C Band

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*. For more information, contact AudioCodes Technical Support.
- Customers whose deployment includes phones *and* 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.

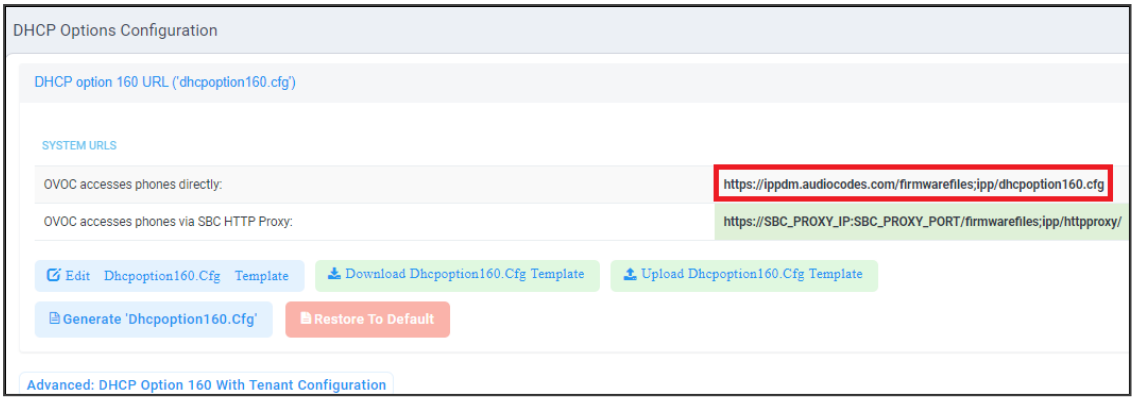
## Configure DHCP Option 160

Start deploying devices 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 devices 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).

Before configuring DHCP Option 160, take OVOC bandwidth considerations into account, as explained in Disabling / Configuring C Band above.

➢ **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**).




2. Under section SYSTEM URLS, copy the URL adjacent to **OVOC accesses phones directly** indicated in the preceding figure, to DHCP Server Option 160.

- DHCP Option 66/67 can also be used, instead of DHCP Option 160.
- For a *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

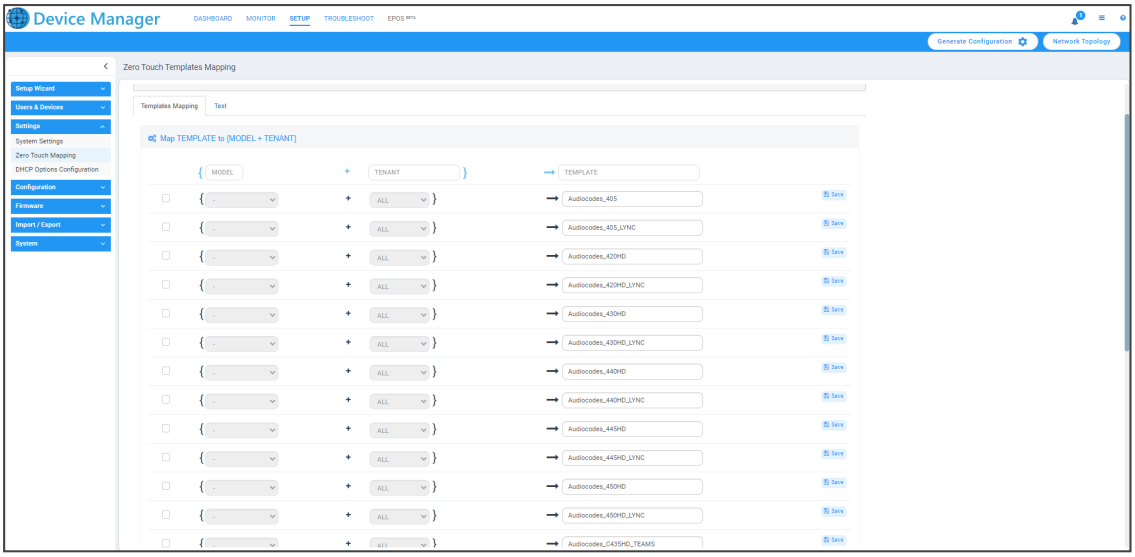
The provisioning URL and device MAC address can alternatively be configured in AudioCodes' Redirect Server. For more information, see AudioCodes *Redirect Service Web Interface User's Manual* available here.

## 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:

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




2. Deselect irrelevant device models that are not deployed in your enterprise's network and select relevant 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:

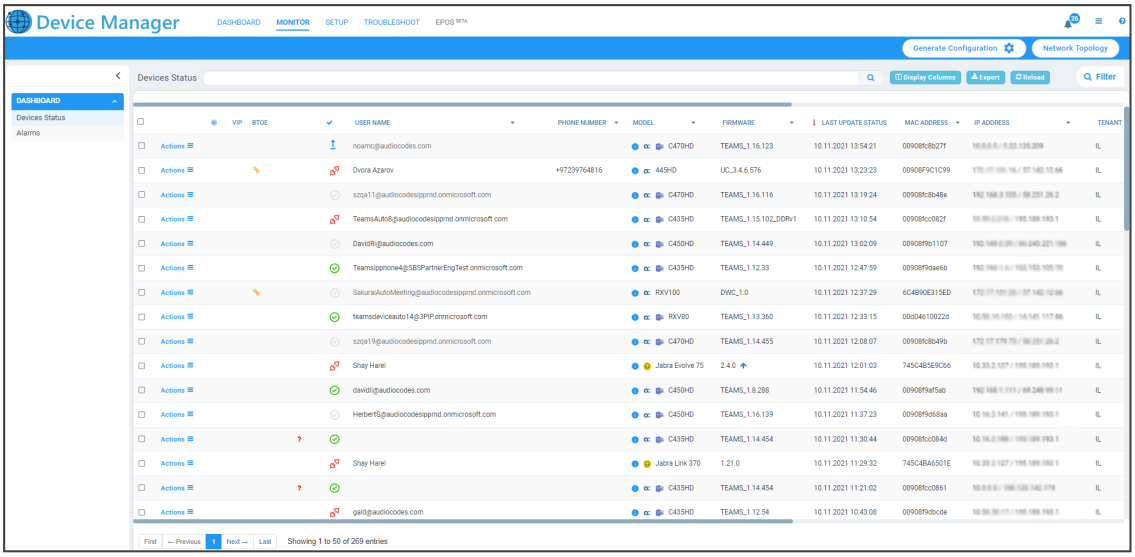

> The templates are part of the Device Manager's database and are supplied with the Device Manager. Though the Device Manager provides every device model with a ready-to-use template, each can be edited if necessary (**Setup** > **Configuration** > **Templates**). See the *Device Manager Administrator's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

4. After selecting 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, the Device Manager displays them in the Monitor page.




After signing in (see the device's *Quick Guide* or *User's and Administrator's Manual* for more information if necessary), the user name is displayed in the Monitor page.

# 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 12)

## 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).

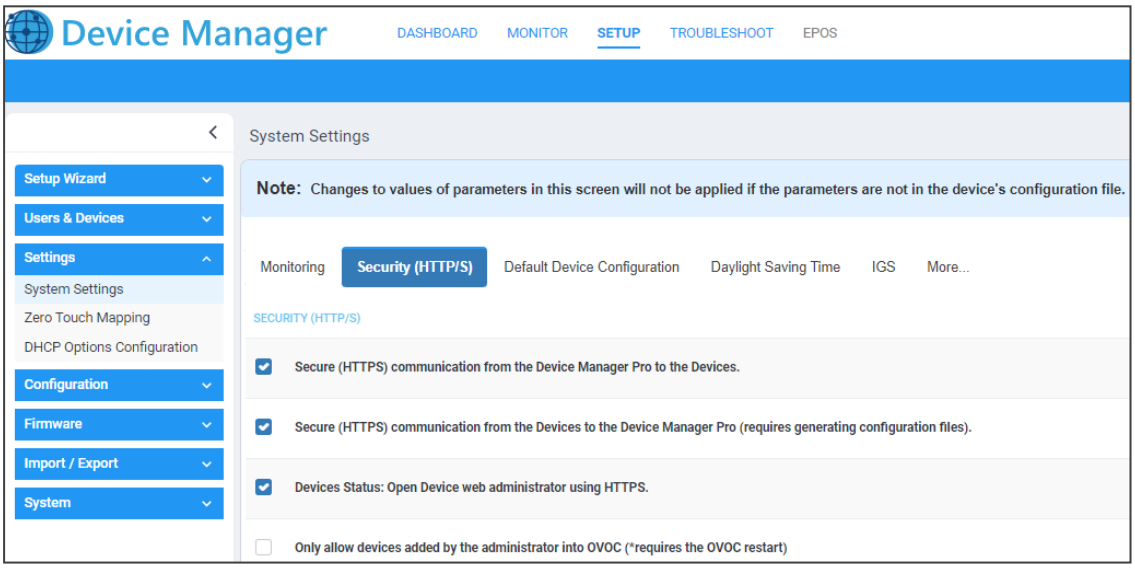
- Manually associate devices with a group in the 'Group Configuration' page of the Device Manager (**Setup** > **Configuration** > **Group Configuration**).
- Optionally make it Zero Touch by adding the Group to the DHCP Option 160 provisioning URL.

## 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.




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're 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:

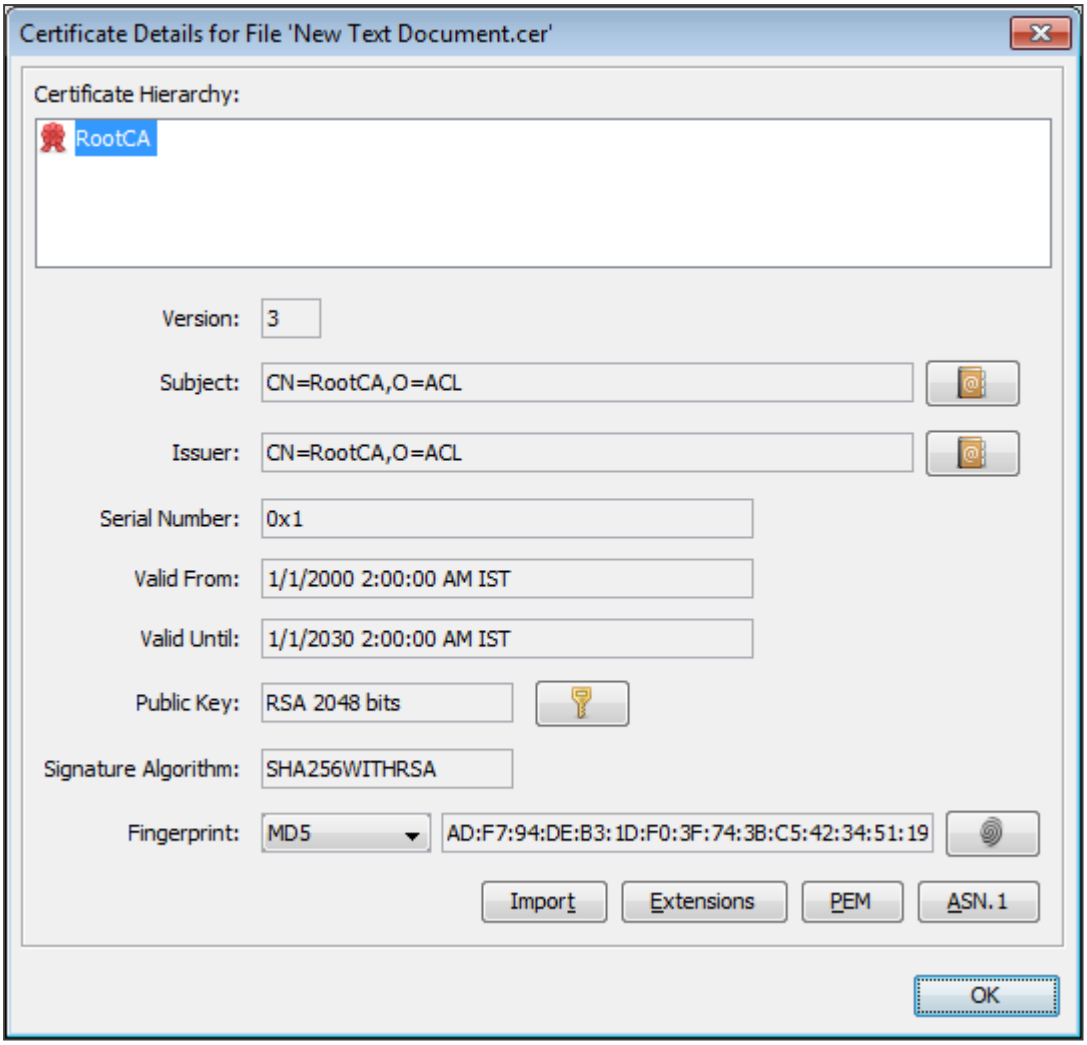
- The device certificate URL will only be valid if no SCEP server URL is present
- Use the following two parameters to set the device certificate in the device's configuration file:
  - ✓ security/device_certificate_url=http://<server-ip>/device.crt
  - ✓ security/device_private_key_url=http://<server-ip>/device.key

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-----

MIIDMTCCAhmgAwIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKE
wNBQ0wx

DzANBgNVBAMTBlJvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMD
EwMDAwMDBa

MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqh
kiG9w0B

AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEYz
bfZL0a

EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKklKsGsvGWmSRNULV01CW+TX2VJN7
3+hh
V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4Ig9kfd/ma9Czl5koESLlw/inLj/r+rD96

mUcPElWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKK
s
EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhlhFL29nMfnaFATSS3rgGaFlSvl1ZS

esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwlDAQABo3gwdjAMB
gNV

HRMEBTADAQH/MB0GA1UdDgQWBBQDXySn9hz15lDraZ+iXddZGReB+zBHB
gNVHSME

QDA+gBQDXySn9hz15lDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQU
NMMQ8w

DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywo
mmWWJnH3

JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDFK
kxMp

0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXYAJ6XgvTfN2BtyZk9Ma8WG+H1hNv
vTZY

QLbWsjQdu4eFniEufeYDke1jQ6800LwMlFlc59hMQCeJTenRx4HdJbJV86k1gBU
E

A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwvLpEP22nYwvB28dq3JetlQ
Kwu
XC4gwl/o8K2wo3pySLU9Y/vanxXCr0/en5l3RDz1YpYWmQwHA8jJlu8rxdhr+VNQ
Zv6R/Ys=
-----END CERTIFICATE----

## Change the Admin Password

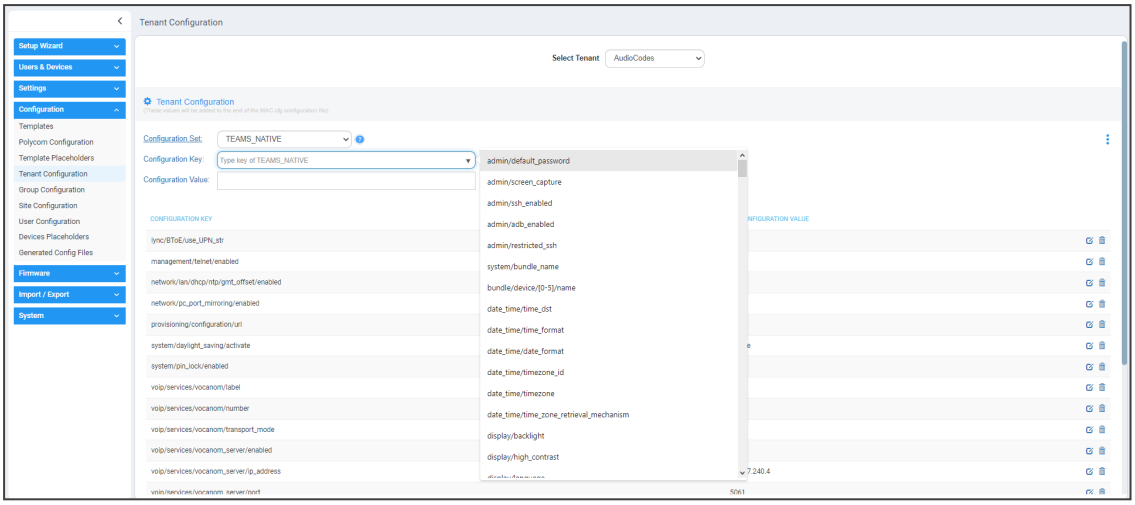
Best practice is to change the Admin password **every three or six months**. AudioCodes recommends implementing this practice to guarantee that only the network administrator will be able to gain access to devices to perform management operations.

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

➢ **To change the Admin Password:**

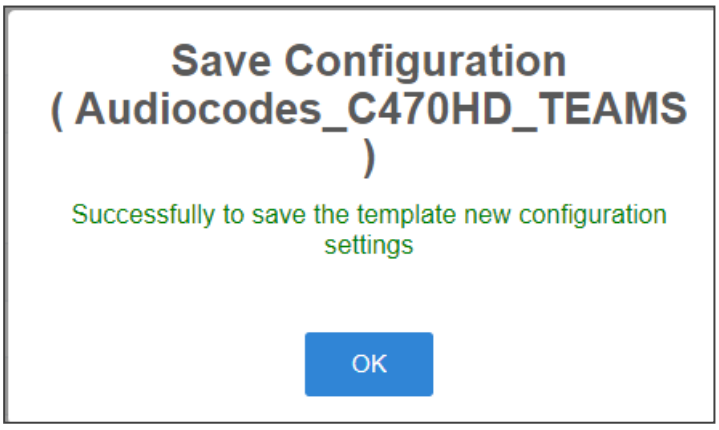
1. In the Device Manager, open either the Templates page, Tenant Configuration page, Group Configuration page or Site Configuration page (**Setup** > **Configuration**), depending on the

range of phones whose Admin Password you want to change.




The example above shows the Tenant Configuration page (**Setup** > **Configuration** > **Tenant Configuration**). Use the instructions here as reference for the Templates page, Group Configuration page and Site Configuration page.

2. Make sure field 'Configuration Set' is configured per the device model in the deployments whose Admin Password you want to change.
3. From the 'Configuration Key' dropdown, select **admin/default_password** as shown in the preceding figure.
4. In the 'Configuration Value' field, enter the Admin Password to change to.
5. Click the **+ Add** button that is then displayed.




6. Click **OK**.

## 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.**

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

©2023 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, and AudioCodes Room Experience 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-91211