Using Avaya Device Enrollment Services to Manage Endpoints

Issue 22
December 2021

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the software (“Third Party Terms”). The Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document describes how to use the Device Enrollment Services web portal to manage endpoints or devices. This document is primarily intended for external audiences. It focuses on service provider, reseller, and customer tasks. It does not provide detailed descriptions of tasks performed by Avaya support personnel.

The Device Enrollment Services server is installed and maintained by Avaya. Therefore, this information is not described in this document.

Related links

Device Enrollment Services account types on page 9

Change history

This section describes the major changes in this document.

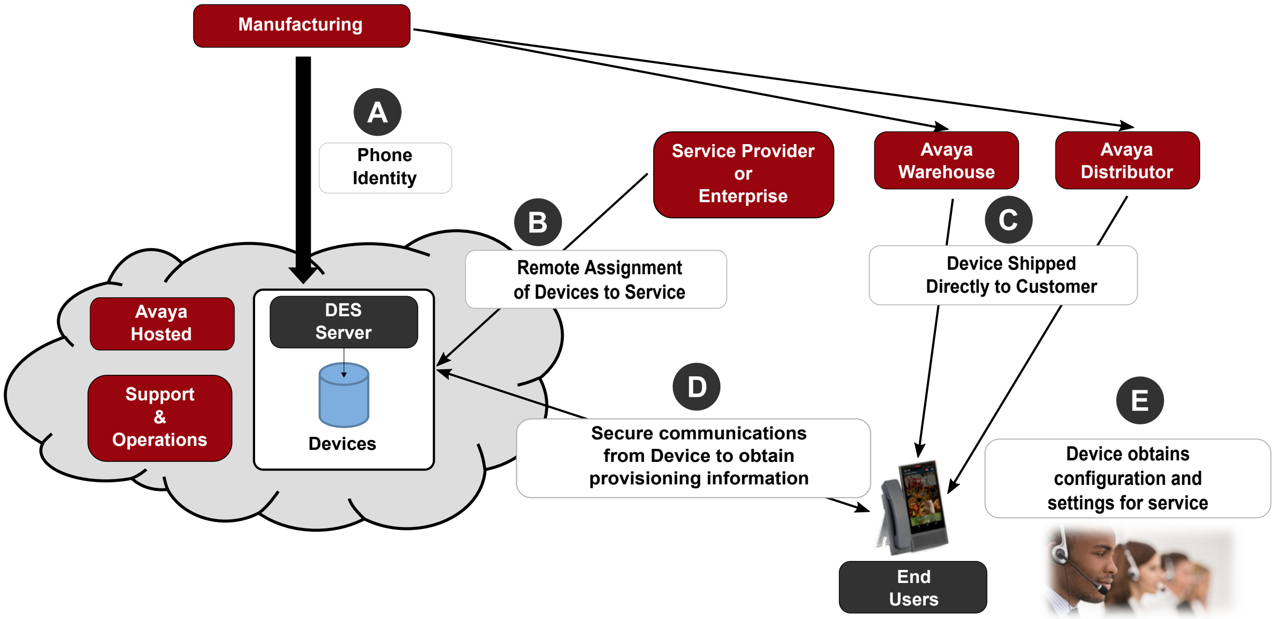
Issue	Date	Summary of changes
Release 3.1.23, Issue 22	December 31st, 2021	• Updated Claiming, activating, associating, disassociating, or releasing devices in bulk on page 54. • Added Viewing Avaya Cloud Office (ACO) product ID on page 67.
Release 3.1.22, Issue 21	December 3rd, 2021	Navigation enhancements
Release 3.1.21, Issue 20	November 2021	Updated Supported devices and features on page 75.

Chapter 2: Device Enrollment Services overview

Device Enrollment Services provides a mechanism for Avaya endpoints to be securely authenticated and redirected to the file server. By simplifying and automating the discovery of the provisioning server, Device Enrollment Services reduces the costs involved in deploying an out-of-the-box device.

Use the Device Enrollment Services web portal to set up and manage devices, profiles, and other settings. The device manufacturer starts the process by entering device details, such as certificate information, MAC addresses, and serial numbers. The details are imported to the Device Enrollment Services server through a file, which enables the device to authenticate with Device Enrollment Services.

The service provider or enterprise administrator can then log in to Device Enrollment Services to configure customer information and provisioning settings. When the end user, or administrator, connects their device to the network, the device establishes a secure connection to Device Enrollment Services. Device Enrollment Services provides the device with information the file server address and optionally new firmware and configuration data.


Manufacturing
A
Phone Identity
Service Provider or Enterprise
Avaya Warehouse
Avaya Distributor
B
Remote Assignment of Devices to Service
C
Device Shipped Directly to Customer
Avaya Hosted
DES Server
Devices
Support & Operations
D
Secure communications from Device to obtain provisioning information
E
Device obtains configuration and settings for service
End Users

What's New

Release 3.1.23 key features:

- Introduction of Avaya Cloud Office™ (ACO) product ID field for ACO supported devices

Release 3.1.22 key features:

- Navigation enhancements to view account details on the Manage Devices page
- Navigation enhancements to view corresponding profiles on the **By Profile** and **Firmware Management** > **Site** pages
- Performance improvement for the Manage Devices page

Release 3.1.21 key features:

- Device Enrollment Services now supports Avaya CU360
- Database Migration and Platform upgrade for Service Scalability

Note:

To view new features or updates introduced in this version, navigate to the menu with your username at the top right of the screen and click **What's new?**.

Device Enrollment Services account types

An account represents a customer or a company involved in the device enrollment process. The basic account types for Device Enrollment Services are:

- Service provider
- Reseller
- Customer

Service provider account

This account is for the company that provides communication services and supplies equipment to resellers or customers. A service provider administrator can:

- Create reseller accounts.
- Create customer accounts.
- Add customer sites and profiles.
- Enable or disable reseller and customer accounts.
- Perform site management and generate enrollment codes.
- Activate or deactivate devices.
- Claim or release devices.

Reseller account

This account is for the company that supplies communication equipment to customers. A reseller administrator has almost the same privileges as a service provider. A reseller can:

- Create, enable, and disable customer accounts.
- Add customer sites and profiles.
- Perform site management and generate enrollment codes.
- Activate or deactivate devices.
- Claim or release devices.

A reseller administrator cannot create a reseller account.

Customer account

This account represents customer sites where devices are enrolled. A customer can:

- Edit their own account.
- Add customer sites and profiles.
- Perform site management and generate enrollment codes for their own customer sites.
- Associate devices with their own profiles and sites.
- Activate or deactivate devices.
- Claim or release devices.

Device provisioning work flow

The following table lists the tasks you perform to enable device enrollment in the Device Enrollment Services web portal:

Task	Role you need to perform this task	Related section
Log in to Device Enrollment Services.	All users	Logging in to the Device Enrollment Services web portal on page 13.
Create a profile.	Service provider, reseller, or customer	Adding a profile on page 27.
Create a customer account and customer site and associate it with the appropriate profile.	Service provider, reseller, or customer	Adding a customer account on page 31.
Import devices.	Manufacturer	Importing devices on page 53.

Table continues…

Task	Role you need to perform this task	Related section
Enroll devices with or without an enrollment code. Enrollment without an enrollment code is called zero-touch provisioning. For enrollment with an enrollment code, you can use an 8-digit or 12-digit enrollment code. If the device user enters the wrong enrollment code more than three times, then the device will be deactivated. You must reactivate the device before it can be enrolled. For zero-touch provisioning, you must: 1. Claim devices 2. Associate the devices with a customer site. 3. Activate the devices for enrollment.	Service provider, reseller, or customer	To use an enrollment code, see Enrollment codes on page 43. For zero-touch provisioning, see: 1. Claiming a device on page 57. 2. Associating a device with a customer site on page 58. 3. Activating or deactivating a device on page 59. To manage devices in bulk, see Claiming, activating, associating, disassociating, or releasing devices in bulk on page 54.

For information about how devices interact with Device Enrollment Services, see the following documents:

- For Avaya Vantage™: “Avaya Vantage™ deployment through Device Enrollment Services” in *Installing and Administering Avaya Vantage™ in an Avaya Aura® or IP Office Environment* and *Installing and Administering Avaya Vantage™ in an Open SIP Environment*.
- For the Avaya J100 Series IP Phones: The sections under “Phone installation” in *Installing and Administering Avaya J100 Series IP Phones*.

Chapter 3: Accessing the Device Enrollment Services web portal

Signing up for a Device Enrollment Services account

About this task

You can request a service provider, reseller, or customer account if you do not have one. When a service provider or reseller creates a customer account, you cannot log in to Device Enrollment Services with that account. You must sign up for a new customer account to log in to Device Enrollment Services. If you have an existing account and sign up for a new one, there is no link between your existing account and the new one.

After you submit the request, an Avaya administrator reviews the information provided and accepts or declines the request. You receive a confirmation email when the administrator accepts your request.

Procedure

1. On a web browser, navigate to https://des.avaya.com to access the Device Enrollment Services web portal Login page.
2. **(Optional)** In the top right corner of the screen, select your preferred language from the list.
3. Click **Click here to request access**.

   The Device Enrollment Services displays the Sign Up for your Devices Enrollment Services Account page.
4. In the Company Information section, from the **My Relationship with Avaya** field, click the appropriate account.

   You can request a service provider, reseller, or customer account.
5. Do one of the following:
   - If you request a service provider or reseller account, in the **BP Link ID** field, enter the Avaya Business Partner ID for the account.
   - If you request a customer account, in the **SAP Sold to Number/ Functional Location (FL)** field, enter the numeric ID for the account.
6. In the **Company Name** field, enter the name of the company.

7. In the Contact Information section, do the following:
    a. Enter your first and last name, business phone number, and business email address.

       The business email address that you provide here is used as your login name.

    b. From **User Locale**, select your preferred language for the Device Enrollment Services web portal.
8. In the Company Address section, enter the address of the company.
9. Select the **I accept Avaya's Terms and Conditions** check box.
10. Click **Request Access**.

Related links

Device Enrollment Services account types on page 9

Logging in to the Device Enrollment Services web portal

About this task

Log in to the Device Enrollment Services web portal to access the functionality enabled for your account type.

Use the latest version of any of the following browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari

Procedure

1. In your browser, navigate to https://des.avaya.com to access the Device Enrollment Services web portal Login page.
2. **(Optional)** In the top right corner of the screen, select your preferred language for the Device Enrollment Services web portal from the list.
3. Do one of the following to log in:
    - Enter your account credentials in the **Username** and **Password** fields, and click **Log in**.

      If you forget your password, see Resetting your password on page 14.

    - If your user identity certificate is imported in the browser, select the certificate when prompted, click **OK**, and click **Continue**.

      For successful authentication, the common name in the certificate must match your login name.

Next steps

If two-factor authentication is enabled for your account, enter a code before accessing Device Enrollment Services. For more information, see Using two-factor authentication to access Device Enrollment Services on page 14.

Resetting your password

Procedure

1. On the Device Enrollment Services login page, click **Forgot Password**.
2. Enter the user name, and click **Submit**.
3. Check your inbox for a Reset password email.
4. Click the URL provided in the email.

   The link expires in 5 minutes.
5. Enter a new password.
6. Type the new password again to confirm it.
7. Click **Submit**.

Using two-factor authentication to access Device Enrollment Services

About this task

Two-factor authentication adds a layer of security to your account by using One Time Password (OTP) as a second factor. Two-factor authentication is an optional feature, which is disabled by default.

When two-factor authentication is enabled, after your first login, you are prompted to set up the mobile authenticator to activate your account. On future logins, you must enter the OTP code to access Device Enrollment Services. A mobile device is required only for OTP authentication. You must use a computer to access the Device Enrollment Services interface.

Procedure

1. To set up the mobile authenticator to activate your account, install one of the following applications on your mobile device:
   - Free OTP
   - Google Authenticator
   - Authy
2. Open the application and scan the barcode.

Steps 1 and 2 are one-time tasks.

3. Enter the code displayed on the mobile application.

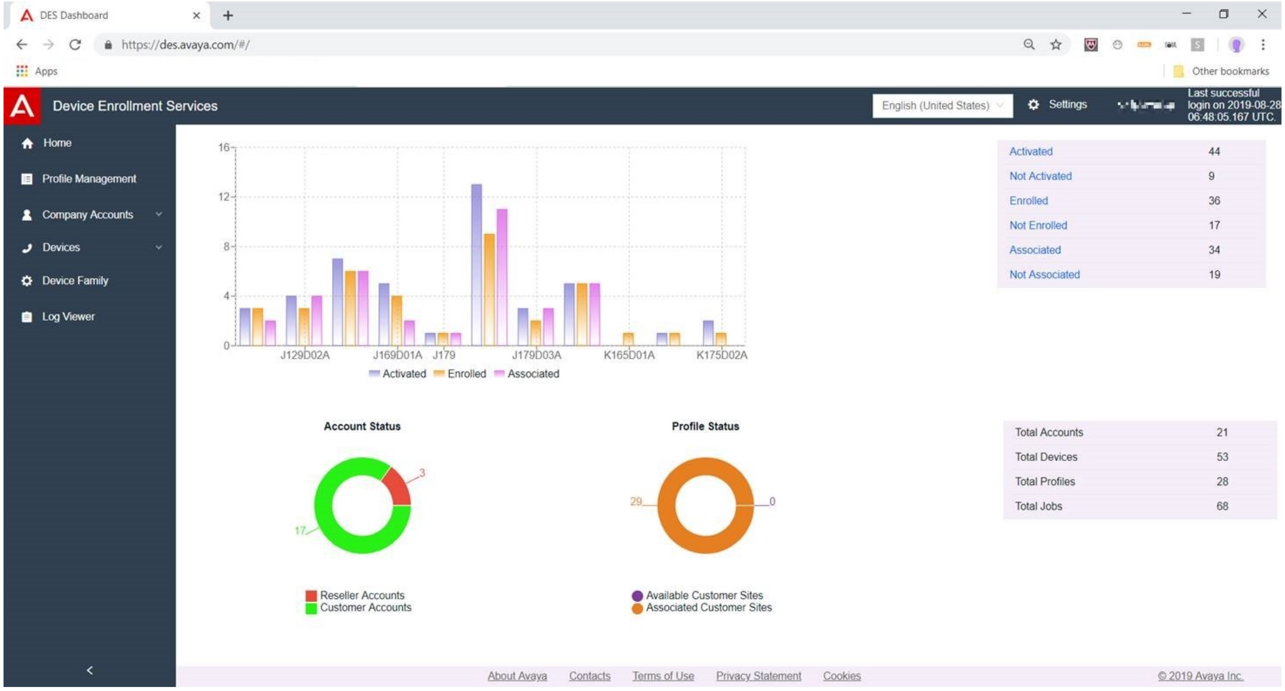
   Perform this step after every login to access Device Enrollment Services.

4. Click **Submit**.

Device Enrollment Services dashboard navigation

When you log in to Device Enrollment Services, you can see the default dashboard, which contains statistics about accounts, devices, profiles, and imported files. The number of available charts on the dashboard depends on the account type. You can click **Home** on the top bar to access the dashboard.

The following is an example of the dashboard for a service provider account:



Last successful login on 2019-08-28 06:48:05.167 UTC.

Activated	44
Not Activated	9
Enrolled	36
Not Enrolled	17
Associated	34
Not Associated	19

Total Accounts	21
Total Devices	53
Total Profiles	28
Total Jobs	68

Logging out of the Device Enrollment Services web portal

About this task

Log out of the Device Enrollment Services web portal to finish your session and prevent unauthorized access to the system.

Procedure

1. Navigate to the menu with your user name at the top right of the screen.
2. From the list of options, click **Logout**.

Chapter 4: General settings

This chapter describes how to:

- Access general information and help
- Manage settings

Viewing version information

Procedure

1. On the Device Enrollment Services web portal, navigate to the menu with your user name at the top right-hand side of the screen.
2. Click **About** to see the current Device Enrollment Services version.

Accessing help information

About this task

The Device Enrollment Services web administration portal provides easy access to the online help version of this document. The document opens in a new tab.

Procedure

On the Device Enrollment Services web administration portal, do one of the following to access help information:

a. Click the blue **Help** link, which is available on most screens.

   This link redirects you to the appropriate section in the document, so you can quickly find the information you need.

b. From the menu with your user name at the top right-hand side of the screen, click **Help**.

   You can use this option if a direct **Help** link is not available on the screen. You can then navigate to the appropriate section in the document.

Changing the online help language

Procedure

1. On the Avaya Documentation Portal, in the top right corner of the screen, click 🌐 .
2. Select one of the following supported languages:
   - English
   - French
   - Italian
   - German
   - Russian
   - Simplified Chinese
   - Japanese
   - Korean
   - Spanish
   - Brazilian-Portuguese

Managing email notification settings

Procedure

1. On the Device Enrollment Services web portal, click **Settings** > **Email Notification Settings**.
2. Enable or disable email notifications using the On/Off switch next to each setting.

   By default, all notification settings are enabled. You can disable a notification setting by setting the switch to **Off**.
3. Click **Submit** to save your changes.

Email notification descriptions

The following table describes the email notification settings in the Device Enrollment Services web administration portal:

Setting	Purpose of the email notification
Enrollment Code Usage	To inform the company and user administrator when a device user has entered an enrollment code.
Provision Changes	To indicate when the provisioning URL has been modified.
Claiming Device	To provide information about a claimed device.
Associating Device	To indicate when a device has been associated with an account or a customer site.
Device Enrollment Failure	To inform the company administrator that device enrollment failed. The reason for the failure is also included in the email.
User Password Reset	To inform a user that their password has been changed.
Account Linking	To inform the service provider and reseller when accounts are linked.

Device lockout settings

The Avaya administrator can configure device lockout settings. If the device user enters a wrong enrollment code multiple times, the device is locked based on the Device lockout attempt count configuration. The Avaya administrator can configure the following settings in **Settings** > **Device Lockout Settings**:

- **Device Lockout Time**: The amount of time in minutes that the device is locked.
- **Enrollment Code Invalid Attempts**: The number of times that the device user can enter wrong enrollment codes before they are locked out.

You cannot edit these settings. They are available in read-only format.

If a device is locked out, the device can be manually activated, or the user must wait until the lockout time has elapsed.

Related links

Enrollment codes on page 43

Chapter 5: Device Enrollment Services as a provisioning server

When adding a profile, you can use Device Enrollment Services as a provisioning server. To do this, enter `https://des.avaya.com` in the **Provisioning URL** field. From **Server Type**, select **DES**.

If you use Device Enrollment Services as the provisioning server, upload a basic device configuration zip file when creating a customer account. The zip file can use `.xml`, `.png`, `.jpg`, `.jpeg`, `.gif`, `.bmp`, `.mp3`, `.wav`, `.ogg`, `.pkcs12`, `.p12`, `.pfx`, and `.txt` files. For example, the zip file can include the `46xxsettings.txt` file and upgrade files, such as `J100Supgrade.xml` and `K1xxSupgrade.xml`. It can optionally also include the certificates from the TRUSTCERTS parameter in the `46xxsettings.txt` file. The settings and upgrade file names are case-sensitive.

Related links

Upgrade files for Avaya J100 Series IP Phones and Avaya Vantage on page 21
Adding a profile on page 27
Adding a customer account on page 31

Settings file template for Avaya J100 Series IP Phones and Avaya Vantage™

The filename must be `46xxsettings.txt` for Device Enrollment Services to work as a provisioning server.

The following is an extract from the `46xxsettings.txt` file for the Avaya J100 Series IP Phones:

```
SET ADMIN_PASSWORD 13579
SET SIP_CONTROLLER_LIST "135.12.345.670:5061;transport=tls"
SET TIMEZONE "America/New_York"
SET TRUSTCERTS "prod-sip-ca.crt"
SET SIPDOMAIN "avaya.com"
```

The following is an extract from the `46xxsettings.txt` file for Avaya Vantage™:

```
SET ADMIN_PASSWORD 13579
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"
SET SIP_CONTROLLER_LIST "135.12.345.670:5061;transport=tls"
SET TIMEZONE "America/New_York"
SET TRUSTCERTS "prod-sip-ca.crt"
SET SIPDOMAIN "avaya.com"
```

To update the parameters, see the following links:

- For Avaya J100 Series IP Phones: https://support.avaya.com/downloads/download-details.action?contentId=C201773928555860_8&productId=P1661.
- For Avaya Vantage™: https://support.avaya.com/downloads/download-details.action?contentId=C201773928555860_8&productId=P1644.

Upgrade files for Avaya J100 Series IP Phones and Avaya Vantage™

The following is an extract from the J100Supgrade file for the Avaya J100 Series IP Phones:

```
IF $MODEL4 SEQ J129 GOTO J129_SW
IF $MODEL4 SEQ J139 GOTO J139_SW
IF $MODEL4 SEQ J169 GOTO J169_SW
IF $MODEL4 SEQ J179 GOTO J179_SW

GOTO GETSET

# J129_SW
GOTO GETSET

# J139_SW
GOTO GETSET

# J169_SW
GOTO GETSET

# J179_SW
GOTO GETSET

# GETSET
GET 46xxsettings.txt
```

The following is an extract from the K1xxSupgrade file for Avaya Vantage™:

```
IF $MODEL4 SEQ K155 GOTO K155SW
IF $MODEL4 SEQ K165 GOTO K175SW
IF $MODEL4 SEQ K175 GOTO K175SW
GOTO GETSET

# K155SW
GOTO GETSET

# K175SW
GOTO GETSET

# GETSET
GET 46xxsettings.txt
```

Related links

Device Enrollment Services as a provisioning server on page 20

Chapter 6: Firmware management

As a customer, you can turn off the firmware upgrade for a specific device model, upgrade a device to its latest firmware version, or select any firmware version from the previous five firmware versions for a device model.

Updating the firmware version for a device model

About this task

You can manage the firmware version of the claimed devices. This enables the control over which firmware gets downloaded, and when it gets downloaded, to particular devices. Firmware can be managed on an company account basis. Unclaimed devices are automatically upgraded to the latest firmware version when they contact Device Enrollment Services.

Note:

If you are using Device Enrollment Services as a provisioning server, you can always use the **Firmware Management** feature. If you are redirecting the device to a different file server other than Device Enrollment Services, then the **Firmware Management** feature applies only when the pre-claimed device connects to Device Enrollment Services for the first time.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. Do one of the following:
   - Add a new customer account, enter the basic and site details.
   - To update an account, select the customer account from the list and click **Edit**.
3. On the Site tab, click **Firmware Settings**.

   Note:

   The **Upload Settings** option is enabled only when you add https://des.avaya.com as a provisioning server.
4. On the Firmware Settings tab, click ✎ for the device model of which you want to update the firmware version.

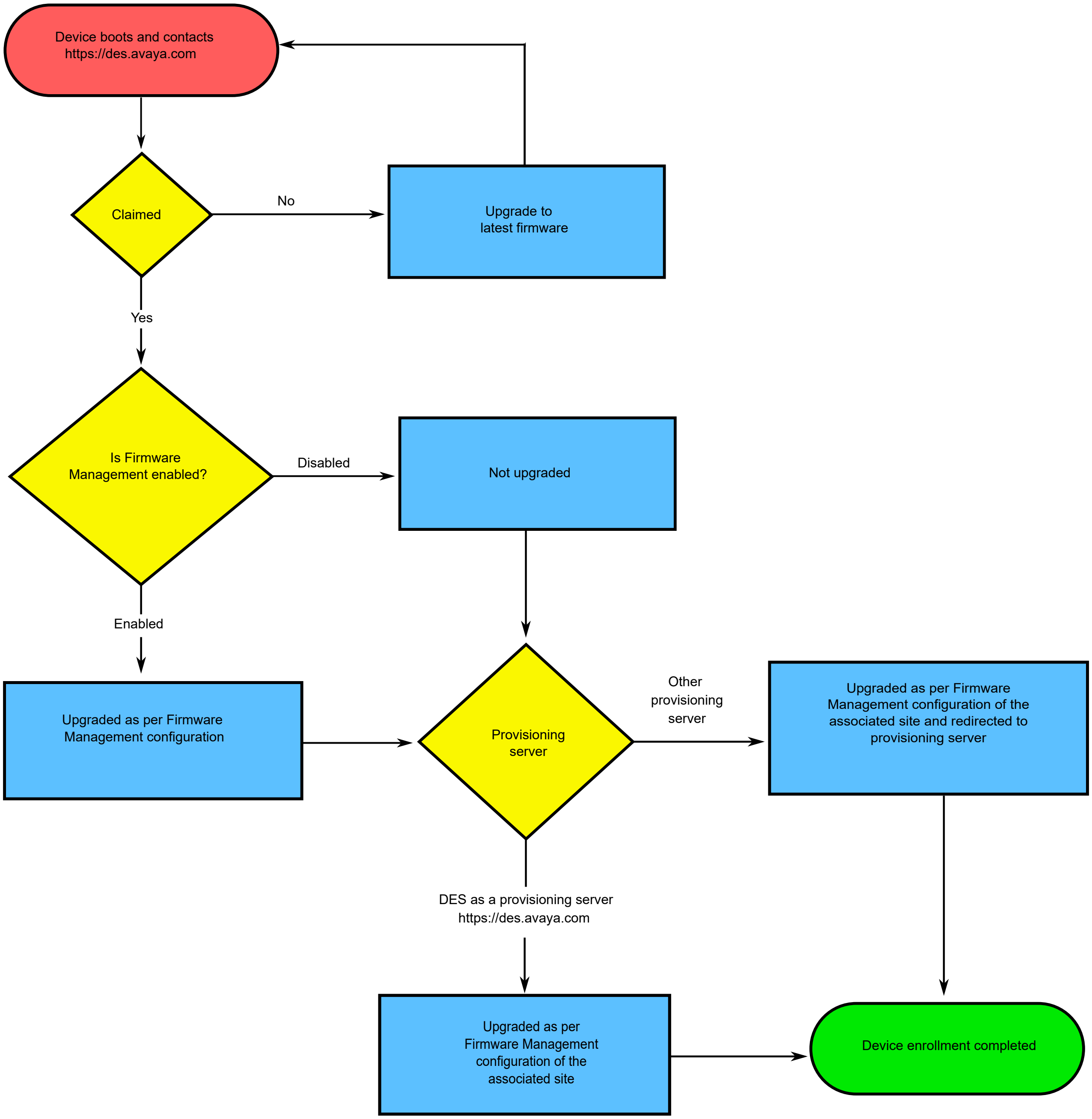
5. In the **Firmware Version** field, select one of the following options:
    - Same as account (Default)
    - Latest
    - Off
    - From the releases of the device model

    Note:

    By default, the most recent ten releases of the device model are available. Avaya Administrators control the number of releases for each device model.

6. Click ✓ to save the changes.

Device Enrollment Services as a Firmware Manager flowchart


Device boots and contacts https://des.avaya.com
Claimed
No
Upgrade to latest firmware
Yes
Is Firmware Management enabled?
Disabled
Not upgraded
Enabled
Upgraded as per Firmware Management configuration
Provisioning server
Other provisioning server
Upgraded as per Firmware Management configuration of the associated site and redirected to provisioning server
DES as a provisioning server https://des.avaya.com
Upgraded as per Firmware Management configuration of the associated site
Device enrollment completed

Chapter 7: Profile management

A profile is associated with one or more customer sites and contains a link to the provisioning server. Service providers, resellers, and customers can perform profile management tasks.

Provisioning server setup

A provisioning server is required for storing device configuration files. The provisioning server can use an HTTP or HTTPS protocol.

Provisioning server certificate guidelines

If you use your provisioning server with the HTTPS protocol and a private certificate authority, upload the root certificate of that certificate authority. If you use a public certificate authority, there is no need to upload a root certificate. You can upload the certificate from the **Profile Management** section. The certificate is used to establish a secure connection between the device and the provisioning server.

❗ **Important:**

Device Enrollment Services recommends to use an explicit FQDN in the certificate because some devices might not accept a certificate containing FQDNs with wildcards. For example, *.domain.com.

Non-secure provisioning URL

New Avaya Vantage™ and Avaya J100 Series IP Phones permit an HTTP connection, which is not secure. Here no certificate is required. Examples of the provisioning URL with HTTP are `http://192.168.10.87` or `http://provisioning.avaya.com` if DNS is available.

Avaya certification generation

A Public Key Infrastructure (PKI) identify certificate is used to establish a secure connection between the device and the provisioning server. The certificate is required when the provisioning server uses a secure HTTPS connection with mutual authentication. The device receives the certificate from Device Enrollment Services.

When you enable Avaya certificate generation, the device gets the identity certificate from the Avaya Devices Root Certification Authority (CA). If Avaya CA generates the identity certificate, you can configure a secure connection between the device and the provisioning server. After the identity certificate is generated, the device uses the new identity certificate. The link to the Avaya CA is https://des.avaya.com/downloads/DeviceEnrollmentServiceRootCA.pem.

For general information about enabling mutual authentication, see the following links:

- For Windows: https://blogs.msdn.microsoft.com/asiatech/2014/02/12/how-to-configure-iis-client-certificate-mapping-authentication-for-iis7/
- For XAMPP or Apache: https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html#allclients

Related links

Provisioning URL formats on page 26

Adding a customer account on page 31

Enabling or disabling Avaya certificate generation

About this task

Certificate generation is disabled by default.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Profile Management**.
2. Select the required profile.
3. In the Avaya certificate generation column, do one of the following:
    - To enable Avaya certificate generation, move the switch to the right.
    - To disable Avaya certificate generation, move the switch to the left.

Provisioning URL formats

The following provisioning URL types can be used for profile configuration:

Type	Example
https://<FQDN>	https://utilityserver.avaya.com
https://<FQDN>:<Port>	https://utilityserver.avaya.com:443
https://<FQDN>/<sub-directory>	https://utilityserver.avaya.com/firmware
https://<FQDN>:<Port>/<sub-directory>	https://utilityserver.avaya.com:443/firmware
http://<FQDN>	http://utilityserver.avaya.com
http://<FQDN>:<Port>	http://utilityserver.avaya.com:8080
http://<FQDN>/<sub-directory>	http://utilityserver.avaya.com/firmware
http://<FQDN>:<Port>/<sub-directory>	http://utilityserver.avaya.com:8080/firmware
https://<HOST IP address>	https://10.10.10.10

Table continues…

Type	Example
https://<HOST IP address>:<Port>	https://10.10.10.10:443
https://<HOST IP address>/<sub-directory>	https://10.10.10.10/firmware
https://<HOST IP address>:<Port>/<sub-directory>	https://10.10.10.10:443/firmware
http://<HOST IP address>	http://10.10.10.10
http://<HOST IP address>:<Port>	http://10.10.10.10:
http://<HOST IP address>/<sub-directory>	http://10.10.10.10/firmware
http://<HOST IP address>:<Port>/<sub-directory>	http://10.10.10.10:8080/firmware
http://<FQDN>/<Device_Family>/$MODEL4	http://utilityserver.avaya.com/J100/$MODEL4
http://<FQDN>/<Device_Family>/$MODEL4/$MACADDR	http://utilityserver.avaya.com/J100/$MODEL4/$MACADDR
http://<FQDN>/<Device_Family>/$MODEL4/$SERIALNO	http://utilityserver.avaya.com/J100/$MODEL4/$SERIALNO
https://<Username>:<Password>@<FQDN>	https://admin:t0pSecret@utilityserver.avaya.com
https://<Username>:<Password>@<FQDN>/Directory	https://admin:t0pSecret@utilityserver.avaya.com/Directory

Adding a profile

About this task

A profile is required for device configuration during the enrollment process. It defines a provisioning file server URL, internal certificate, and phone group. Profiles provide a common place to configure provisioning for multiple customer sites.

The profile settings are not applied to already enrolled devices.

Before you begin

- Ensure the provisioning server is functional and contains the appropriate configuration files.
- If you use your provisioning server with the HTTPS protocol and a private certificate authority, upload the root certificate of that certificate authority. If you use a public certificate authority, there is no need to upload a root certificate.

Procedure

1. Click **Profile Management**.
2. Click **Add**.
3. Complete the **Profile Name** field.
4. Click **Add**.
5. In the **Server Type** field, select one of the following:
    - **DES** if the provisioning URL points to `https://des.avaya.com`.

- **HTTP(S)** in all other scenarios.

6. In the **Provisioning URL** field, enter the complete URL with the path to the directory where the settings file of the device is located.

   If you set the provisioning URL to `https://des.avaya.com`, upload a settings file with basic device configuration information when creating a customer account.

7. **(Optional)** To generate the identity certificate, move the **Avaya certificate generation** switch to the right.

   If the provisioning server is configured for mutual authentication, you can trigger the device to install an identity certificate from Device Enrollment Services. Download and install the root certificate on your provisioning server.

8. **(Optional)** To download the root certificate, click **Avaya Devices Root CA**.
9. If you use a private Certificate Authority, in the **Root CA Certificate** field, click **Select File** and upload the root CA certificate.
10. Enter the device or phone group number in the **Phone Group (0 – 999)** field.

    The phone group number is used to distinguish sets of parameters in the configuration file. For example, if the configuration file contains settings for phone groups 16 and 17, and you enter `17` in this field, the settings for group 17 are applied to the enrolled devices. The default value for this field is 0.

11. In the Action column, click ✓ to save your changes.
12. **(Optional)** To add multiple provisioning URLs to the profile, click **Add** and repeat the above steps, starting from step 3.
13. Click **Submit** to add the profile.

Related links

Provisioning server certificate guidelines on page 25
Provisioning URL formats on page 26
Adding a customer account on page 31
Avaya certification generation on page 25
Associating a device with a customer site on page 58

Updating a profile

About this task

If you change a profile, devices use the updated configuration during the enrollment process.

Procedure

1. Click **Profile Management**.

2. Select the required profile.
3. Click **Edit**.
4. Select the required provisioning URL.
5. In the Action column, click ✎.
6. Update the profile settings as required and click ✓.
7. Click **Submit**.

Removing a profile

About this task

Remove a profile if it is no longer used for device enrollment. If there is no profile associated with a customer site, you cannot complete device enrollment.

Procedure

1. Click **Profile Management**.
2. Select the required profile.
3. Click **Delete**.
4. Click **OK** to confirm.

Chapter 8: Company accounts

Company account management

The **Account Management** menu contains options for creating, updating, enabling, and disabling different account types.

Related links

Firmware management on page 22

Adding a reseller account

About this task

A reseller supplies communication equipment to customers. A reseller administrator can:

- Create customer accounts.
- Add customer sites and profiles.
- Perform site management and generate enrollment codes.
- Activate or deactivate devices.
- Claim or release devices.

Service providers can create a reseller account. However, only Avaya personnel can create a service provider account. This document is not intended for Avaya personnel, and therefore, it does not describe how to create service provider accounts.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. Click **Add**.
3. In the Basic Information section, do the following:
    a. In the **Account Type** field, click **Reseller**.
    b. In the **Account Name** field, type an appropriate account name.
    c. Provide the contact's first and last name, business phone number, and business email address.
    d. **(Optional)** In the **BP Link ID** field, enter the Avaya Business Partner ID for the account.

You can link a reseller account with your service provider account using the BP link ID.

4. In the Company Address section, enter the company address.
5. **(Optional)** In the Services section, enable **Two Factor Authentication** by moving the switch to the right.

   Two Factor Authentication adds a layer of security to your account. For more information, see Using two-factor authentication to access Device Enrollment Services on page 14.
6. Click **Submit**.

Next steps

Add the account administrator for the reseller account. When you add an account administrator, you can create a temporary password for the account.

Related links

Adding an account administrator on page 40

Sending an account linking request on page 49

Adding a customer account

About this task

A customer account is used to associate devices with customer sites. Required profiles for device configuration are also associated with customer sites. Service providers and resellers can create a customer account.

Before you begin

Add a profile from the **Profile Management** menu.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. Click **Add**.
3. On the Basic Details tab, go to the Basic Information section and do the following:
   a. In the **Account Type** field, click **Customer**.
   b. In the **Account Name** field, type an appropriate account name.
   c. Provide the contact first and last name, business phone number, and business email address.
   d. **(Optional)** In the **SAP Sold to Number/Functional Location (FL)** field, enter the numeric ID for the account.
4. In the Company Address section, enter the company address.

5. Click **Submit**.
6. On the Site tab, click **Add** and do the following:
    a. In the **Site** field, enter the site location name.
    b. In **Profile**, do one of the following:
        - Click **Add Profile** to create and associate a new profile with the site.
        - Click a profile to associate with the site.

          The list displays the profiles that you add in the Profile Management tab.

    c. **(Optional)** To use a 12-digit enrollment code, enter your 4-digit PIN in the **PID (0000 – 9999)** field.
    d. If the provisioning URL is set to `https://des.avaya.com`, upload a zip file with the basic device configuration.

       Note:

       The **Firmware Settings** option is enabled after the site is created.

    e. In the Action column, click ✓.
    f. **(Optional)** Click **Firmware Settings** to upgrade the device firmware version.
    g. **(Optional)** Click ✎ for the device model of which you want to update the firmware version, and in the **Firmware Version** field, select one of the following options:
        - Same as default
        - Latest
        - Off
        - From the five releases of the device model
7. **(Optional)** On the Firmware Management tab, do the following:
    a. Click ✎ for the device model of which you want to update the firmware version.
    b. In the **Firmware Version** field, select one of the following options:
    - Latest (Default)
    - Off
    - From the five releases of the device model

    Note:

    By default, the **Firmware Upgrade** switch is on, and the latest firmware version is selected for all devices. In the **Model** column, the **All** option upgrades all device models of that device type to the selected firmware version.

8. Click ✓ to save the changes.

Related links

Device Enrollment Services as a provisioning server on page 20

Adding a profile on page 27
Enabling or disabling device firmware upgrades on page 38
12–digit provisioning enrollment code on page 46

Associating multiple sites with a profile from the Account Management section

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. From the list, click the customer account for which you want to associate multiple sites with a profile.
3. On the Site tab, from the list, select multiple sites that you want to associate with a profile.

   The Site tab is only available for customer accounts. It is not available for service provider or reseller accounts.
4. Click **Bulk Profile Association**.
5. In the **Provisioning details** field, select the profile and provisioning server.
6. In the **Basic Provisioning Settings File** field, click **Select File** and upload the zip file with a basic device configuration.
7. Click **Submit**.

Enabling or disabling an account

About this task

When you add a customer account, it is automatically enabled. When enabled, the account becomes available for login, but it is not automatically associated with any profiles or devices.

When you disable an account, the account administrator cannot log in to Device Enrollment Services anymore. Profiles and devices are dissociated from the account.

Service providers and resellers can enable or disable an account.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. In the Company Account Management list, select the required account.
3. Click **More Actions**.
4. Click one of the following:
   - **Enable Account** to unlock the account.
   - **Disable Account** to lock the account.

Updating an account

About this task

You can update an account's settings. The fields available for editing depend on the account type. You cannot change the account type, but you can change the account name.

You can also upload a root CA certificate for the account. The root certificate identifies the user certificate, which is used for logging in to the Device Enrollment Services web portal. When the certificate is generated by a public Certificate Authority (CA), you do not need a client root certificate. The common name in the certificate must match the login name of the user. For a list of public CAs, see List of public CAs on page 34.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. Select the required account from the list.
3. Click **Edit**.
4. Update the required fields.

   The account type cannot be changed.
5. **(Optional)** In the **Client root CA** field:
   - If the root certificate is not uploaded, click **Select File** and upload the certificate.
   - If the root certificate is uploaded, click ⤓ to download and view the certificate file.
6. Click **Submit** to save your changes.

List of public CAs

If the user certificate, which is used to log in to Device Enrollment Services, is generated by one of the following public CAs, then you do not need to upload a client root certificate when adding and updating an account.

Certificate name	Issued by	Type
Actalis Authentication Root CA	Actalis Authentication Root CA	RSA
AffirmTrust Commercial	AffirmTrust Commercial	RSA
AffirmTrust Premium	AffirmTrust Premium	RSA
AffirmTrust Premium ECC	AffirmTrust Premium ECC	ECDSA
ANF Global Root CA	ANF Global Root CA	RSA
ApplicationCA2 Root	ApplicationCA2 Root	RSA
Atos TrustedRoot 2011	Atos TrustedRoot 2011	RSA
Autoridad de Certificacion Raiz del Estado Venezolano	Autoridad de Certificacion Raiz del Estado Venezolano	RSA

Table continues…

Certificate name	Issued by	Type
Buypass Class 2 Root CA	Buypass Class 2 Root CA	RSA
Buypass Class 3 Root CA	Buypass Class 3 Root CA	RSA
CA Disig Root R2	CA Disig Root R2	RSA
Certinomis - Root CA	Certinomis - Root CA	RSA
Certum Trusted Network CA 2	Certum Trusted Network CA 2	RSA
CFCA EV ROOT	CFCA EV ROOT	RSA
COMODO ECC Certification Authority	COMODO ECC Certification Authority	ECDSA
COMODO RSA Certification Authority	COMODO RSA Certification Authority	RSA
ComSign Global Root CA	ComSign Global Root CA	RSA
DigiCert Assured ID Root G2	DigiCert Assured ID Root G2	RSA
DigiCert Assured ID Root G3	DigiCert Assured ID Root G3	ECDSA
DigiCert Global Root G2	DigiCert Global Root G2	RSA
DigiCert Global Root G3	DigiCert Global Root G3	ECDSA
DigiCert Trusted Root G4	DigiCert Trusted Root G4	RSA
D-TRUST Root Class 3 CA 2 2009	D-TRUST Root Class 3 CA 2 2009	RSA
D-TRUST Root Class 3 CA 2 EV 2009	D-TRUST Root Class 3 CA 2 EV 2009	RSA
Entrust Root Certification Authority - EC1	Entrust Root Certification Authority - EC1	ECDSA
Entrust Root Certification Authority - G2	Entrust Root Certification Authority - G2	RSA
Federal Common Policy CA	Federal Common Policy CA	RSA
GeoTrust Primary Certification Authority - G2	GeoTrust Primary Certification Authority - G2	ECDSA
GeoTrust Primary Certification Authority - G3	GeoTrust Primary Certification Authority - G3	RSA
GlobalSign	GlobalSign	ECDSA or RSA
Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	RSA
Government Root Certification Authority	Government Root Certification Authority	RSA
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root CA 1	RSA
IdenTrust Public Sector Root CA 1	IdenTrust Public Sector Root CA 1	RSA
ISRG Root X1	ISRG Root X1	RSA

Table continues…

Certificate name	Issued by	Type
Izenpe.com	Izenpe.com	RSA
Microsec e-Szigno Root CA 2009	Microsec e-Szigno Root CA 2009	RSA
NetLock Arany (Class Gold) Főtanúsítvány	NetLock Arany (Class Gold) Főtanúsítvány	RSA
OISTE WISeKey Global Root GB CA	OISTE WISeKey Global Root GB CA	RSA
QuoVadis Root CA 1, 2, or 3 G3	QuoVadis Root CA 1, 2, or 3 G3	RSA
Security Communication RootCA2	Security Communication RootCA2	RSA
Staat der Nederlanden Root CA - G3	Staat der Nederlanden Root CA - G3	RSA
Starfield Root Certificate Authority - G2	Starfield Root Certificate Authority - G2	RSA
Starfield Services Root Certificate Authority - G2	Starfield Services Root Certificate Authority - G2	RSA
StartCom Certification Authority	StartCom Certification Authority	RSA
StartCom Certification Authority G2	StartCom Certification Authority G2	RSA
Swisscom Root CA 2	Swisscom Root CA 2	RSA
Swisscom Root EV CA 2	Swisscom Root EV CA 2	RSA
SwissSign Gold Root CA - G3	SwissSign Gold Root CA - G3	RSA
SwissSign Platinum Root CA - G3	SwissSign Platinum Root CA - G3	RSA
SwissSign Silver Root CA - G3	SwissSign Silver Root CA - G3	RSA
Symantec Class 1 Public Primary Certification Authority - G4	Symantec Class 1 Public Primary Certification Authority - G4	ECDSA
Symantec Class 1 Public Primary Certification Authority - G6	Symantec Class 1 Public Primary Certification Authority - G6	RSA
Symantec Class 2 Public Primary Certification Authority - G4	Symantec Class 2 Public Primary Certification Authority - G4	ECDSA
Symantec Class 2 Public Primary Certification Authority - G6	Symantec Class 2 Public Primary Certification Authority - G6	RSA
Symantec Class 3 Public Primary Certification Authority - G4	Symantec Class 3 Public Primary Certification Authority - G4	ECDSA
Symantec Class 3 Public Primary Certification Authority - G6	Symantec Class 3 Public Primary Certification Authority - G6	RSA
thawte Primary Root CA - G2	thawte Primary Root CA - G2	ECDSA
thawte Primary Root CA - G3	thawte Primary Root CA - G3	RSA
TRUST2408 OCES Primary CA	TRUST2408 OCES Primary CA	RSA

Table continues…

Certificate name	Issued by	Type
T-TeleSec GlobalRoot Class 2 or 3	T-TeleSec GlobalRoot Class 2 or 3	RSA
TWCA Global Root CA	TWCA Global Root CA	RSA
USERTrust ECC Certification Authority	USERTrust ECC Certification Authority	ECDSA
USERTrust RSA Certification Authority	USERTrust RSA Certification Authority	RSA
VeriSign Class 3 Public Primary Certification Authority - G4	VeriSign Class 3 Public Primary Certification Authority - G4	ECDSA
VeriSign Universal Root Certification Authority	VeriSign Universal Root Certification Authority	RSA

Related links

Adding a reseller account on page 30

Deleting an account

About this task

As a service provider or reseller, you can delete an account if it is not required anymore. Devices associated with this account are associated with the account they belonged to before the association with the deleted account.

Note:

Accounts that the administrator of the deleted account created are also deleted.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. Select the required account from the list.
3. Click **Delete**.
4. Click **OK**.

Viewing account hierarchy

About this task

Use this procedure to view a list of accounts. The accounts are displayed in a hierarchical order. You can expand an account category, such as Reseller, to see the accounts created under that category. You can also edit account details.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. Click **Open Account Hierarchy**.
3. On the left of the screen, click the forward arrow (▸) to expand an account category and view the sub-accounts under it.

   For example, if you expand Reseller, Device Enrollment Services displays a list of reseller accounts.
4. Click an account to update the account details.
5. Click **Close Account Hierarchy** to close the account hierarchy area.

Related links

Updating an account on page 34

Enabling or disabling device firmware upgrades

About this task

If a device that is not claimed uses an enrollment code, the device is upgraded to the upgradeable firmware version shown in the **Device Family** menu. If a device is claimed, the Device Enrollment Services verifies the account firmware upgrade setting. By default, the firmware upgrade setting is disabled for customer accounts. You can enable automatic firmware upgrades for claimed devices when the firmware version is older than the version required for device enrollment. After the device is upgraded, device enrollment becomes possible.

The firmware version configured in the settings file on your provisioning server must be the same as or higher than the version configured in Device Enrollment Services.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. In the Company Account Management list, select the required customer account.
3. Click **More Actions**.
4. Click one of the following:
   - **Enable Firmware Upgrade**.
   - **Disable Firmware Upgrade**.

Related links

Viewing firmware versions on page 63

Supported devices and features on page 75

Enabling two-factor authentication

About this task

Two-factor authentication adds an additional layer of security to your account by using OTP as a second factor. If two-factor authentication is enabled at the company level, all administrative users in that company are required to enter OTP after performing the initial login procedure. If two-factor authentication is disabled at the company level, you can enable this option for specific accounts. Two-factor authentication is disabled by default.

Service providers can enable two-factor authentication for the reseller accounts under them.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. In the Company Account Management list, select the account.
3. Click **More Actions**.
4. Click **Enable two factor authentication**.

Related links

Using two-factor authentication to access Device Enrollment Services on page 14

Requesting Application Programming Interface (API) access

About this task

Application Programming Interface (API) is set of definitions and protocols for building and integrating application software. Device Enrollment Services APIs can be integrated with other applications. If you do not have access to the API, you can request for the access to the administrator. For more information on APIs, see https://des.avaya.com/apidocs/.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. Select the required account from the list.
3. Click **Edit**.
4. In the Services section, click **Request**.

Management of administrative users

In the **User Management** menu, you can add, update, or delete administrators for your account. As a service provider, you can also manage administrators of the reseller accounts you have created.

Adding an account administrator

About this task

After adding a reseller or customer account, you must add an administrator for that account.

As an account administrator, you can perform operations with claimed devices and manage other administrators for your account. As a service provider administrator, you can also manage reseller and customer accounts. A reseller administrator can manage customer accounts.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **User Management**.
2. Click **Add**.
3. In **Account Name**, select the required account.
4. Enter the first name and last name of the account administrator.
5. In **Email ID**, enter an email address.
6. In **Login Name**, enter a user name for the account administrator to log in to Device Enrollment Services.
7. In **Password** and **Confirm Password**, enter a temporary login password.

   After logging in to Device Enrollment Services for the first time, the new account administrator will be prompted to change their password.
8. From **User Locale**, select the preferred language.

   The Device Enrollment Services web portal for the selected account is displayed in this language.
9. Click **Submit**.

Result

After you add the account administrator, they will receive an email with credentials for logging into Device Enrollment Services.

Related links

Adding a reseller account on page 30

Updating an account administrator

About this task

You can edit your administrators to update their personal information or reset their password.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **User Management**.
2. Select the required user account from the list.
3. Click **Edit**.
4. **(Optional)** Update the first name, last name, email, login name, and password as required.

   When you are updating user details, you cannot change the account name.
5. **(Optional)** From **User Locale**, change the preferred language if required.
6. Click **Submit**.

Deleting an account administrator

About this task

You can delete an account administrator to disable their access to the Device Enrollment Services web portal.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **User Management**.
2. Select the required account administrator from the list.
3. Click **Delete**.
4. Click **OK**.

Site management

You can do the following from the **Site Management** menu:

- Go to **By Profile** to manage the profiles associated with customer accounts.
- Go to **By EC** to generate and manage enrollment codes if you want to enroll devices using an enrollment code.
- Go to **Bulk Administration** to view the status and details of the uploaded basic configuration file for multiple customer sites.

Related links

Importing devices on page 53

Searching for an account

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Site Management**, and click one of the following:
   - **By Profile**
   - **By EC**
2. On the right side of the screen, click ▼.

   Search fields are displayed under most columns.
3. To search for an account, enter key words in one or more of the **Search** fields.

Related links

By EC search options on page 42
By Profile search options on page 42

By EC search options

The following table describes the **Search** fields on By EC screen:

Search options	Function
Account Name	In the **Search** field, type the account name.
Site	In the **Search** field, type the site location. For example, London.
Enrollment Code	In the **Search** field, type the 8-digit or 12-digit numeric enrollment code. This enrollment code is randomly generated.
Expired	In the **Search** field, select one of the following options: • **Yes**: To view accounts with an expired enrollment code. • **No**: To view accounts with an active enrollment code.
Created By	In the **Search** field, type the name of the account administrator.

Related links

Enrollment codes on page 43

By Profile search options

The following table describes the **Search** fields on By Profile screen:

Search options	Function
Account Name	In the **Search** field, type the account name.

Table continues…

Search options	Function
Site	In the **Search** field, type the site location. For example, London.
Profile	In the **Search** field, type the profile name to search.
PEC	In the **Search** field, type the 12-digit provisioning enrollment code that contains the 8-digit account ID and a 4 digit PIN.
Created By	In the **Search** field, type the name of the account administrator.

Related links

Enrollment codes on page 43

Setting the profile associated with an account

About this task

You can select a different profile from the available options. The information displayed for the profile includes the profile name, associated provisioning URL, and phone group.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Site Management** > **By Profile**.
2. From the list, find the account you want to update.
3. In the Action column, click ✎.
4. Select another profile option from the list.

   The profile options displayed depend on what you configure in **Profile Management**.
5. In the Action column, ✓.

Related links

Adding a profile on page 27

Enrollment codes

After a device is imported, you can enroll it with or without an enrollment code. After you generate an enrollment code, the device user enters it on their device. Then the device is automatically activated, claimed, and associated with the customer site.

You can generate the following two types of enrollment codes:

- 8-digit or 12-digit numeric enrollment code: The numbers in this enrollment code are generated randomly. This enrollment code can also have an expiry date. Use an 8-digit or 12-digit numeric enrollment code for additional security.
- 12-digit provisioning enrollment code: This enrollment code contains 8-digit account ID of the customer and a 4-digit PIN. You can create a PIN of your choice. This enrollment code does not expire and is easy to remember.

Related links

Device lockout settings on page 19

8-digit or 12-digit numeric enrollment code

Generating an 8–digit or 12-digit numeric enrollment code

About this task

The numbers in an 8-digit or 12-digit numeric enrollment code are random, and this type of enrollment code can have an expiry date. An 8-digit or 12-digit numeric enrollment code is more secure than a 12-digit provisioning enrollment code.

Before you begin

Ensure that a profile is associated with the site for which you are creating the enrollment code.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Site Management** > **By EC**.
2. Select a site from the list.
3. To change the associated profile and phone group, in the Action column, do the following:
   a. Click ✎.
   b. Update the required fields.
   c. **(Optional)** If the profile contains multiple provisioning URLs, in the **Provisioning URL** list, select the appropriate provisioning URL.
   d. Click ✓ to apply the changes.
4. Click **Generate**.

   The Numeric Enrollment Code Setting dialog box is displayed. The **Name** field is populated automatically.
5. In the **NEC Length** field, select from two numeric enrollment code length options:
   - 8 Digits
   - 12 Digits
6. In the **Total Devices To Be Enrolled** field, enter the number of devices to be configured using the code.

   When you reach the total, no more devices can be enrolled using this enrollment code.
7. In the **Expiry Type** field, select one of the following:
   - **Hour(s) (1–72)**
   - **Day(s) (1–90)**
   - **Week(s) (1–12)**
   - **Month(s) (1–3)**

- **Never Expire**

8. In the **Expiry Time Limit** field, enter a number.

   For example, if you enter `2` and you select **Week(s) (1–12)** in the previous step, then the expiry time for the enrollment code is set to 2 weeks. The maximum expiry limit is 3 months.

   This step is not applicable if you select **Never Expire** in the previous step.

9. Click **Submit**.

Result

Devices can now be configured using the generated enrollment code.

Related links

Regenerating an 8-digit or 12-digit numeric enrollment code on page 45

Updating the 8-digit or 12-digit numeric enrollment code settings for a site

About this task

You can update settings for an 8-digit or 12-digit numeric enrollment code, such as the total number of devices to be enrolled and the expiry time limit for the enrollment code.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Site Management** > **By EC**.
2. Select a site from the list.
3. Click **Update**.
4. Update the settings as required.

   In the **Number of Enrolled Devices** field, you can see the number of devices enrolled with the current enrollment code.

5. Click **Submit** to save your changes.

Regenerating an 8-digit or 12-digit numeric enrollment code

About this task

If an 8-digit or 12-digit numeric enrollment code expires, you can regenerate it with the same settings. In this case, a new code is generated, and the expiration period starts from the regeneration time. If an enrollment code is regenerated, the enrolled device count is not reset.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Site Management** > **By EC**.
2. Select a site from the list.
3. Click **Regenerate**.

   The **Regenerate Numeric Enrollment Code** dialog box is displayed.

4. In the **Regenerate Numeric Enrollment Code** dialog box, select from two numeric enrollment code length options:
    - 8 Digits
    - 12 Digits
5. Click **Submit**.

12–digit provisioning enrollment code

You can generate a 12–digit provisioning enrollment code from two sections:

- Site Management
- Account Management

A 12–digit provisioning enrollment code consists of:

- The 8–digit account ID. You can view account IDs from the Account Management screen.
- A 4-digit PIN, which you create.

This type of enrollment code does not expire.

Generating a 12–digit provisioning enrollment code from the Site Management section

About this task

You can set up a 12-digit provisioning enrollment code for a profile from Site Management.

Before you begin

- Add a profile.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Site Management** > **By Profile**.
2. From the list, find the account you want to update.
3. In the Action column, click ✎.
4. Select a profile from the list.
5. In the **PID (0000 – 9999)** field, enter your 4-digit PIN.
6. In the Action column, click ✓.

Result

The enrollment code is applied to the new profile that you selected.

Related links

[Adding a customer account](#) on page 31
[Setting the profile associated with an account](#) on page 43

Generating a 12–digit provisioning enrollment code from the Account Management screen

About this task

You can set up a 12–digit provisioning enrollment code while adding or editing a customer account from the Account Management screen.

Before you begin

- Add a profile.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. Do one of the following:
   - To add a new customer account, click **Add**.
   - To edit an account, select the account and then click **Edit**.
3. On the Basic Details tab, go to the Basic Information section and do the following:
   a. In the **Account Type** field, click **Customer**.
   b. Update the required fields.
4. On the Site tab, click **Add** and do the following:
   a. In the **Site** field, enter the name of the site location.
   b. In **Profile**, select a profile for which you want to generate the enrollment code.

      The list displays the profiles that you added in the Profile Management tab.
   c. In the **PID (0000 – 9999)** field, enter your 4-digit PIN.
   d. In the Action column, click ✓.
5. Click **Submit**.

Result

The enrollment code is applied to the new profile that you selected.

Related links

Adding a customer account on page 31

Bulk profile association

You can upload a single zip file with basic device configuration for multiple customer sites. You can associate multiple customer sites with a profile from the following two sections:

- **Account Management**
- **Site Management**

Note:

You can upload basic configuration zip files if you use Device Enrollment Services as the provisioning server.

Associating multiple sites with a profile from the Account Management section

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. From the list, click the customer account for which you want to associate multiple sites with a profile.
3. On the Site tab, from the list, select multiple sites that you want to associate with a profile.

   The Site tab is only available for customer accounts. It is not available for service provider or reseller accounts.
4. Click **Bulk Profile Association**.
5. In the **Provisioning details** field, select the profile and provisioning server.
6. In the **Basic Provisioning Settings File** field, click **Select File** and upload the zip file with a basic device configuration.
7. Click **Submit**.

Associating multiple sites with a profile from the Site Management section

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Site Management** > **By Profile**.
2. From the list, select multiple sites that you want to associate with a profile.
3. Click **Bulk Profile Association**.
4. In the **Provisioning details** field, select the profile and provisioning server.
5. In the **Basic Provisioning Settings File** field, click **Select File** and upload the zip file with a basic device configuration.
6. Click **Submit**.

Viewing site details

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Site Management** > **Bulk Administration**.

   The Site Bulk Administration page displays a list of all jobs. The row for each job provides basic job details and the job status.
2. To view additional details for a specific job, click on the job name.

Site Bulk Administration search options

The following table describes the **Search** fields on the Site Bulk Administration screen:

Search options	Function
Name	In the **Search** field, type the name of the job.
Status	In the **Search** field, select one of the following options: • **COMPLETE**: To view completed jobs. • **FAIL**: To view failed jobs. • **IN PROGRESS**: To view jobs in progress.
Start Time	In the **Search** field, type the start time and date of the task performed.
End Time	In the **Search** field, type the end time and date of the task performed.
Created By	In the **Search** field, type the name of the account administrator..

Account linking

Sending an account linking request

About this task

As a service provider, you can send an account linking request to a reseller. Linking enables you to transfer the ownership of claimed devices to a reseller account.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Account Management**.
2. Click **Link Reseller**.
3. In the **BP Link ID** field, enter the Avaya Business Partner ID for the reseller.
4. Click **Submit**.

Related links

Adding a reseller account on page 30

Approving linking requests

About this task

As a reseller, you can approve or reject linking requests that you receive from service providers who want to transfer device ownership to you.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Company Accounts** > **Linking Requests**.
2. Select the service provider account that you want to link with your reseller account.
3. To approve the linking request, click **Approve Linking**.
4. Click **OK**.

Chapter 9: Label management

You can create labels to help you categorize devices. For example, you can use a label to categorize Avaya Vantage™ devices for a specific customer site. You can then associate the labels you created to one or more devices. You can also select labels while performing a bulk action. When you no longer need a label, you can delete it.

Creating a new label

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Label Management**.
2. Click **Add**.
3. Complete the following fields:
    - **Label Name**
    - **Description**
4. Click **Submit**.

Next steps

Associate labels to devices.

Associating a device with a label

About this task

Use this procedure to associate labels to a small number of devices. If you want to select labels for a bulk action, see Claiming, activating, associating, disassociating, or releasing devices in bulk on page 54.

Before you begin

Create labels.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.

2. From the table, select one or more devices.
3. Click **More Actions**.
4. Click **Associate Devices to Labels**.
5. Select a label.

   You can select multiple labels for a device.
6. Click **Submit**.

Related links

Claiming, activating, associating, disassociating, or releasing devices in bulk on page 54
Creating a new label on page 51

Dissociating labels from a device

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.
2. From the table, select one or more devices.
3. Click **More Actions**.
4. Click **Dissociate Labels**.
5. In the **Select Labels** list, select one or more labels.
6. Click **Submit**.

Deleting a label

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Label Management**.
2. Select one or more labels from the list.
3. Click **Delete Labels**.
4. Click **OK**.

Chapter 10: Device management

Before you can enroll a device, it must be imported to Device Enrollment Services. The manufacturer imports devices in bulk using a JSON, CSV, or ZIP file. These devices are approved by the Avaya administrator.

To enroll an imported device, you can:

- Generate an enrollment code. After successful enrollment, the device is automatically activated, claimed to your account, and associated with the customer site. For more information, see Site management on page 41.
- Manually perform device management operations, including claiming devices, associating them with a customer site, and activating them. The devices are enrolled without an enrollment code.

Importing devices

About this task

As a manufacturer, you can import devices. After the devices are imported, they are added to Device Enrollment Services. Imported devices must be approved by the Avaya administrator to be available for further management.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Bulk Administration**.
2. Click **New Job**.
3. Type a name in the **Bulk Operation Name** field.
4. In **Select Bulk Action**, select **Import**.

   Manufacturers can import devices.
5. **(Optional)** Click **Download Template** to download a template for the file type that you selected in the previous step.
6. In **Select File Type**, select the type of file you are importing.
7. Click **Browse** to upload the file that contains information about the devices to be imported.
8. Click **Submit**.

Related links

Label management on page 51

Claiming, activating, associating, disassociating, or releasing devices in bulk

About this task

You can:

- Claim devices in bulk.
- Associate or disassociate multiple devices with a customer site.
- Activate or deactivate devices in bulk.
- Release the ownership of multiple devices in bulk. This action returns the ownership of the devices to the parent account.
- Synchronize one or more devices to customer's account on Ring Central system in bulk. This action claims, activates, associates, and synchronizes devices with the Ring Central system in a single step. The synchronization operation applies only to Avaya Cloud Offer accounts. If the Avaya Cloud Office™ (ACO) product ID data is provided in the input file, Device Enrollment Services ignores the data.

You can perform one or more bulk management operations at a time. Device Enrollment Services presents a series of options together. For example, if you select **Claim**, you can also select **Associate** or **Activate** simultaneously.

You must manually claim, associate, and activate devices if you want to perform enrollment without an enrollment code.

Before you begin

- Ensure that the devices are imported by a manufacturer and approved by the Avaya administrator.
- Before using labels to categorize devices, you must create labels by navigating to **Devices** > **Label Management**. For more information, see Creating a new label on page 51.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Bulk Administration**.
2. Click **New Job**.
3. Type a name in **Bulk Operation Name**.
4. In **Select Bulk Action**, select one or more options from the following groups:
    - If you select **Claim**, you can also select **Associate** or **Activate**.
    - If you select **Disassociate**, you can also select **Associate** or **Release**.

- If you select **Associate**, you can also select **Activate**.
- If you select **Activate**, **Deactivate**, **Sync**, or **Release**, no other options are available.

The available options vary depending on your role.

5. If you select **Associate**, enter the account name in the **Account Name** field.
6. **(Optional)** Move the **Use Device Labels** switch to the right to enable device labels.

   This switch is not available if you select **Claim**. In this case, you can select the appropriate labels as described in the next step.
7. **(Optional)** From **Associate with labels** or **Select Labels**, select the appropriate labels.

   Associate with labels is displayed if you selected **Claim**. **Select Labels** is displayed for all other actions.
8. **(Optional)** Click **Download Template** to download a template for the selected file type.
9. If you are not using labels, select the type of file to import in **Select File Type**.
10. Click **Browse** to upload the file containing device information.
11. Click **Submit**.

Related links

Importing devices on page 53

Label management on page 51

Viewing job details

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Bulk Administration**.

   The Bulk Administration page displays a list of all added jobs. The row for each job provides basic job details and the job status.
2. To view additional details for a specific job, click on the job name.

Device Job Details search options

The following table describes the **Search** fields on the Device Job Details screen:

Search options	Function
MAC Address	In the **Search** field, type the MAC address of the device.

Table continues…

Search options	Function
Job Status	In the **Search** field, type the status of the job. For example, if you want to view failed jobs, enter **FAIL**. Device Enrollment Services displays a list of all failed jobs.
Serial Number	In the **Search** field, type the serial number of the device.
Reseller Order ID	In the **Search** field, type the name of the customer.
Avaya Order ID	In the **Search** field, type the number of the Avaya order.
Shipment Carrier	In the **Search** field, type the name of the shipment carrier. For example, if you want to view shipments carried by DHL, type `DHL`. Device Enrollment Services displays the list of all shipments carried by DHL.
Carrier Tracking ID	In the **Search** field, type the carrier tracking number.
Product ID	In the **Search** field, type the product ID of the device.
Model Number	In the **Search** field, type the model number of the device.
Manufacturing Date And Time	In the **Search** field, type the manufacturing date or time. Device Enrollment Services searches for devices that match this date or time.
Is Active	In the **Search** field, select one of the following options: • **Yes**: To view active devices. • **No**: To view inactive devices.

Exporting job details

About this task

You can export information about added jobs, including the MAC address, job status, serial number, product ID, model number, manufacturing date and time, status, reseller order ID, Avaya order ID, shipment carrier, and carrier tracking ID.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Bulk Administration**.
2. Click ⤓.
3. Select one of the following file type you want to export:
   - **JSON**
   - **CSV**
4. Click **Submit**.

   Device Enrollment Services downloads the job details.

Management operations for a small number of devices

Use the following sections to manage a single device or a few devices. You must manually claim, associate, and activate devices if you want to perform enrollment without an enrollment code.

Claiming a device

About this task

If you claim a device, you get ownership of it and can associate it with a customer site.

Before you begin

Obtain the device MAC address, serial number, or both.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Claim Device**.
2. Enter the device MAC address, serial number, or both.
3. Click **Claim**.

Next steps

The claimed device can now be associated with a customer site. A service provider can also choose to associate the device with a reseller account.

Related links

Associating a device with a reseller account on page 57
Associating a device with a customer site on page 58
Releasing a device on page 59
Activating or deactivating a device on page 59

Associating a device with a reseller account

About this task

As a service provider, you can transfer the ownership of claimed devices to a reseller account.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.
2. From the table, select one or more devices.
3. Click **Associate**.
4. Select a reseller account.
5. Click **Submit**.

Next steps

After devices are associated with a reseller account, the reseller administrator can associate them with a customer site or perform other device management tasks.

Associating a device with a customer site

About this task

You can associate claimed devices with a customer site to enable enrollment without an enrollment code.

Before you begin

Associate a profile with the customer site. The profile configuration must contain the correct provisioning URL and phone group.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.
2. From the table, select one or more devices.
3. Click **Associate**.
4. Select an account and a customer site.
5. Click **Submit**.

Next steps

Activate devices for enrollment.

Related links

Adding a profile on page 27
Claiming a device on page 57
Activating or deactivating a device on page 59

Disassociating a device

About this task

You can disassociate a device from a child account and the ownership of the device is returned to your account.

Note:

After you disassociate a device, Device Enrollment Services deletes information, such as reseller order ID, Avaya order ID, shipment carrier, and carrier tracking ID.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.

2. From the table, select one or more devices.
3. Click **Disassociate**.
4. Click **OK** to confirm.

Activating or deactivating a device

About this task

You must activate a device in the following situations:

- To enable automatic enrollment without an enrollment code.
- When an enrollment code is used, but the device user enters the code incorrectly more than three times. In this case, the device cannot be enrolled until it is re-activated.

An activated or deactivated device, which is not associated with an account, can be enrolled with an enrollment code.

Before you begin

- Claim the required devices.
- To automatically enroll a device without an enrollment code, you must associate the device with a customer site before you activate it.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.
2. From the table, select one or more devices.
3. To activate the selected devices, click **Activate**.
4. To deactivate the selected devices, click **Deactivate**.

   If a device is not activated, it can only be enrolled with an enrollment code.

Related links

Associating a device with a customer site on page 58
Claiming a device on page 57

Releasing a device

About this task

You can release claimed devices to return the ownership to the parent account.

Note:

After you release a device, Device Enrollment Services deletes information, such as reseller order ID, Avaya order ID, shipment carrier, and carrier tracking ID.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.
2. From the table, select one or more devices.
3. Click **Release**.

Related links

Claiming a device on page 57

Viewing additional columns

About this task

By default, some columns are displayed on the Manage Devices page. You can view more columns from the settings options.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.
2. Click ⚙.
3. Click **Columns**.
4. Check the required columns from the following:
   - **Product ID**
   - **Thumbprint**
   - **Hardware**
   - **Carrier Tracking ID**
   - **Reseller Order ID**
   - Avaya **Order ID**
   - **Shipment Carrier**
   - **Is Synced**

   Device Enrollment Services displays the selected columns on the Manage Devices page.

Exporting device details

About this task

You can export information about claimed devices. The device details that are exported include the MAC address, serial number, product, model number, hardware, thumbprint, and manufacturing date and time.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.
2. From the table, select one or more devices.
3. Click **Export**.
4. In **Select File Type**, select the type of file you want to export.

   You can download the device details in JSON or CSV format.
5. Click **Submit**.

   The Export Devices page displays the exported devices.
6. Click ⤓ to download the device details onto your computer.

Selecting all devices for bulk operations

About this task

You can perform one or more bulk management operations at a time on all devices in your account.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.
2. Click **Select All nnnn Items** (where nnnn is the number of devices in your account).
3. Select the appropriate action you want to perform on all selected devices.

Searching for device information

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.
2. Click **Options**.
3. Select **Advanced Search**.
4. Select the search category from the list.

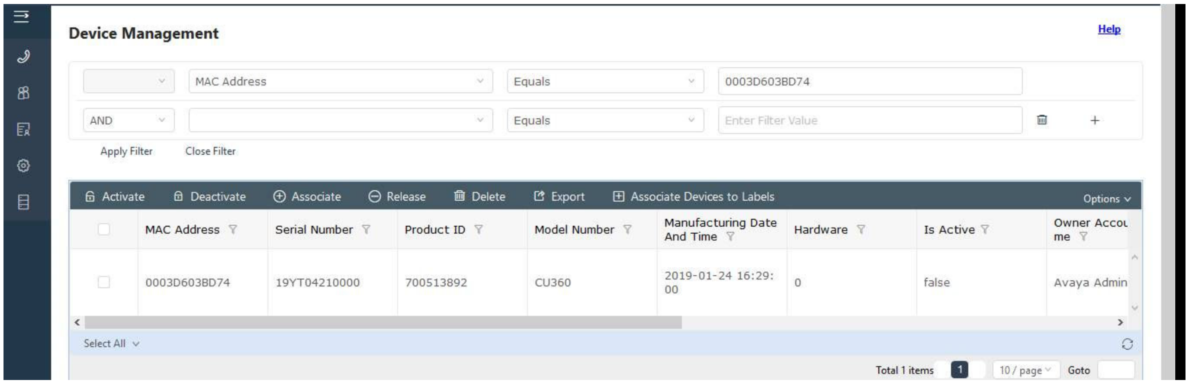
   Examples of options you can select include the following:

   - **MAC Address**
   - **Serial Number**
   - **Product ID**
   - **Model Number**

5. Select one of the following options:
   - **Equals**
   - **Not Equals**
   - **Starts With**
   - **Ends With**
   - **Contains**
6. Enter a search value or keyword.

   The following are examples of how Device Enrollment Services searches based on the specified search settings:

   - If the previous fields were set to **MAC Address** and **Equals**, enter the MAC address that you want to search for.
   - If the previous fields were set to **MAC Address** and **Not Equals** and you enter `15` in this field, then Device Enrollment Services searches for devices without 15 in the MAC address.
7. **(Optional)** To add another search option, do the following:
   a. Click +.
   b. Select **AND** or **OR** from the list.
   c. Repeat steps 4 to 6 to define the search criteria for the new line.



	MAC Address	Equals	0003D603BD74
AND		Equals	Enter Filter Value

	MAC Address	Serial Number	Product ID	Model Number	Manufacturing Date And Time	Hardware	Is Active	Owner Account Name
□	0003D603BD74	19YT04210000	700513892	CU360	2019-01-24 16:29:00	0	false	Avaya Admin

8. **(Optional)** To delete a search condition, click 🗑.

   This button is available if there is more than one search condition.
9. When you are ready to perform the search, click **Apply Filter**.

Chapter 11: Firmware versions and logs

Viewing firmware versions

About this task

Devices must have the correct firmware version installed for enrollment. By default, if a device is not claimed, Device Enrollment Services upgrades it to the minimum required version. If a device is claimed, automatic upgrades are disabled for customer accounts by default. To enable firmware upgrades, see Enabling or disabling device firmware upgrades on page 38.

Note:

Some phone versions, such as version 1.5 of the Avaya J100 Series IP Phones, do not support automatic firmware upgrades. You must manually upgrade the Avaya J100 Series IP Phones to version 2.0 and reset to the factory default settings.

Procedure

1. On the Device Enrollment Services web portal, click **Device Family**.
2. In the device list, locate the device model.

   The Upgradable Firmware Version column displays the latest supported firmware version for device enrollment. The Supported Firmware Version column displays the minimum supported firmware version.

   The Avaya administrator can update the minimum firmware version. Other account administrators can only view firmware settings.

Viewing logs

About this task

You can view logs for the operations performed on your account.

Procedure

1. To view logs, on the Device Enrollment Services web portal, click **Log Viewer**.
2. On the right side of the screen, click ▼.

   Search fields are displayed under all columns.

3. Use one or more **Search** fields to search for logs.

   For more information about using the **Search** fields, see Log Viewer search options on page 64.

Log Viewer search options

The following table describes the **Search** fields on the Log Viewer screen:

Search options	Function
Time Stamp	In the **Search** field, type a date or time. Device Enrollment Services searches for logs that match this date or time.
Account Name	In the **Search** field, you can type your account name to view logs for your account.
Process Name	In the **Search** field, select a log type. For example, if you select **ENROLLMENT**, Device Enrollment Services displays the MAC address and certificate information of the device. The following is an example of the certificate information that might be displayed: `CN=MACaddress,OU=Devices SV,O=Avaya India Private Limited,L=Pune,ST=MH,C=IN`
Client Host	In the **Search** field, type the remote IP address used to connect to Device Enrollment Services.
Action	In the **Search** field, select an action to view all logs related to that action. For example, if you select **ENROLLMENT**, Device Enrollment Services displays all logs related to the device enrollment.
Status	In the **Search** field, select one of the following status options: • **SUCCESS**: To view logs for successful operations. • **FAIL**: To view logs for failed operations.
Message	In the **Search** field, type key words from the message. The following is an example of a message: `LoginId: exampleid, ObjectType: com.avaya.des.jpa.DesAccount, Details: {accountId: 200, accountName: TestTest, desProfiles: [], desCustomerSites: [], desAccountUsers: [], desAccountType: {id: 5, accountType: Customer} }`

Chapter 12: Avaya Cloud Office™ by RingCentral device management

Device Enrollment Services enables Avaya distributors to upload device information to the Avaya Cloud Office™ (ACO) system using the **Sync** operation.

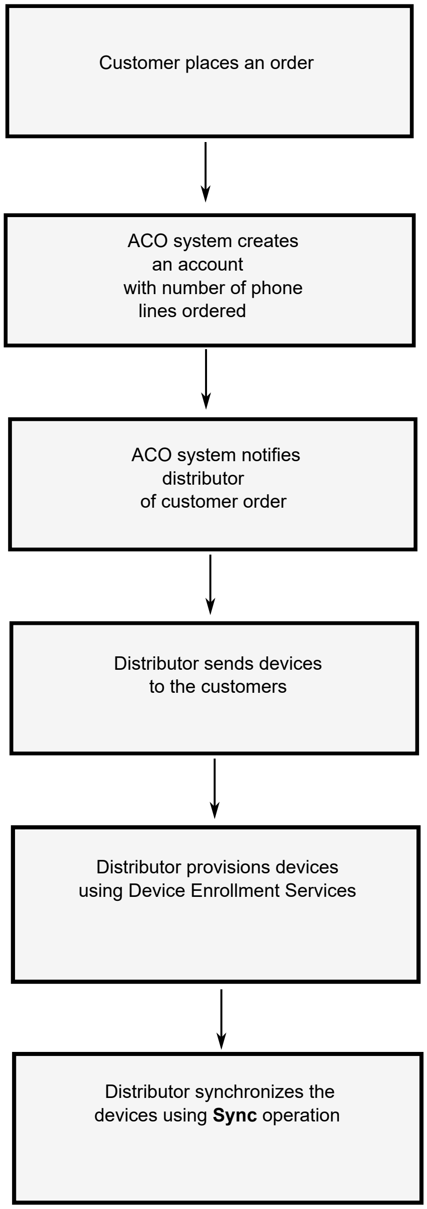
Avaya Cloud Office™ synchronization operation overview

Device Enrollment Services checks for the Avaya Cloud Office™ (ACO) supported phone models in the Device Enrollment Services inventory. It claims, associates, activates, and synchronizes supported ACO phone models with the ACO system.

The following list of devices currently support the **Sync** operation with ACO:

- Avaya J139 IP Phone
- Avaya J159 IP Phone
- Avaya J169/J179 IP Phone
- Avaya Conference Phone B199

ACO synchronization operation



Customer places an order

ACO system creates an account with number of phone lines ordered

ACO system notifies distributor of customer order

Distributor sends devices to the customers

Distributor provisions devices using Device Enrollment Services

Distributor synchronizes the devices using **Sync** operation

Synchronizing ACO supported devices with the ACO system

About this task

Device Enrollment Services claims, associates, activates, and synchronizes the supported ACO phone models with the ACO system.

Before you begin

Obtain the following device details:

- MAC address, serial number, or both
- Reseller order ID, which is also called the RingCentral customer account number

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Bulk Administration**.
2. Click **New Job**.
3. Type a name in **Bulk Operation Name**.
4. In **Select Bulk Action**, select **Sync**.
5. **(Optional)** Move the **Use Device Labels** switch to the right to enable device labels.
6. **(Optional)** From **Select Labels**, select the appropriate labels.
7. **(Optional)** Click **Download Template** to download a template for the selected file type.
8. If you are not using labels, select the type of file to import in **Select File Type**.
9. Click **Browse** to upload the file containing device information.
10. Click **Submit**.

Viewing Avaya Cloud Office™ (ACO) product ID

About this task

The devices in the Ring Central system have different product IDs. You can view the Avaya Cloud Office™ (ACO) product ID on the Manage Devices screen for the ACO supported device models. Device Enrollment Services synchronizes the supported phones. You can also see the ACO product ID when you export and download the device details in JSON or CSV format.

Procedure

1. On the Device Enrollment Services web portal, navigate to **Devices** > **Manage Devices**.
2. Click ⚙.
3. Click **Columns**.

4. Check the **ACO Product ID** option.

   Device Enrollment Services displays the **ACO Product ID** column on the Manage Devices screen.

Chapter 13: Switching accounts

As a service provider, you can switch to any of your reseller accounts and perform all tasks in that account. You must send a request to the Avaya administrator in order to receive access to this functionality. After you submit the request, an Avaya administrator can accept or decline the request. You and all of your resellers receive a confirmation email when the administrator accepts your request. If the Avaya administrator declines your request, you receive an email with the reason for declining the request.

Sending a switch account request to an Avaya administrator

About this task

As a service provider, you can send an account switching request to an Avaya administrator. Switching enables you to navigate to any reseller account you create.

Procedure

1. On the Device Enrollment Services web portal, click **Switch Account**.
2. Click **Request Access**.
3. Click **OK** to confirm.

Switching to a reseller account

About this task

Once the Avaya administrator approves your request, you can view all data related to that reseller account. You can switch to any reseller account in your own hierarchy and perform any required tasks as a service provider.

Procedure

1. On the Device Enrollment Services web portal, click **Switch Account**.
2. From the list of accounts, click **Switch** to navigate to that account.

Device Enrollment Services navigates you to a reseller account. In the top right corner, you can view a notification after you switch to a reseller account.

3. Click **Exit from Reseller Account** to navigate back to your service provider account.

Chapter 14: Resources

Documentation

Device Enrollment Services currently supports Avaya Vantage™ and Avaya J100 Series IP Phones. You can find this Device Enrollment Services document and the related documents listed in the following table at http://support.avaya.com and http://documentation.avaya.com.

Document	Use this document to:	Audience
Installing and Administering Avaya J100 Series IP Phones	Install, configure, and maintain Avaya J100 Series IP Phones, including the J129, J139, J169, and J179 phone models.	Implementation personnel and administrators
Installing and Administering Avaya Vantage™ in an Avaya Aura® or IP Office Environment	Install, configure, and maintain Avaya Vantage™ in an Avaya Aura® or IP Office environment.	Implementation personnel and administrators
Installing and Administering Avaya Vantage™ in an Open SIP Environment	Install, configure, and maintain Avaya Vantage™ in an Open SIP environment.	Implementation personnel and administrators

Other reference documents

The following table lists other reference documents, which are available at http://support.avaya.com. These documents are primarily intended for internal implementation personnel or people who need general information about ports and security.

Note:

You might need to log in to the Support site to access some of these reference documents.

Document	Link
Avaya Device Enrollment Services Port Matrix	https://downloads.avaya.com/css/P8/documents/101056581
Installation Guide for Device Enrollment Services	https://downloads.avaya.com/css/P8/documents/101056289
Data Privacy Controls Addendum for Device Enrollment Services	https://downloads.avaya.com/css/P8/documents/101057536

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in**Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** (🌐) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
- Add topics from various documents to a collection.
- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon (👁).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Appendix A: Supported devices and features

The following tables lists the enrollment features and specifies the minimum supported device release for each feature. Device Enrollment Services currently supports following devices:

- Avaya J100 Series IP Phones
- Avaya Vantage™
- B199
- Avaya CU360

Related links

Enabling or disabling device firmware upgrades on page 38

Avaya J100 Series IP Phones

The following table lists enrollment features and specifies the minimum supported device release for Avaya J100 Series IP Phones:

Device enrollment features	J129	J139	J159	J169 and J179	J189
Provisioning URLs	2.0	3.0	4.0.3	2.0	4.0.5
Re-provisioning devices	2.0	3.0	4.0.3	2.0	4.0.5
HTTPS provisioning URL	2.0	3.0	4.0.3	2.0	4.0.5
Firmware upgrade	3.0	3.0	4.0.3	3.0	4.0.5
HTTP provisioning URL	3.0	3.0	4.0.3	3.0	4.0.5
Provisioning URL with IP address	3.0	3.0	4.0.3	3.0	4.0.5

Table continues…

Device enrollment features	J129	J139	J159	J169 and J179	J189
Certificate with provisioning URL	2.0	3.0	4.0.3	2.0	4.0.5
8–digit numeric enrollment code	3.0	3.0	4.0.3	3.0	4.0.5
12-digit numeric enrollment code	3.0	3.0	4.0.3	3.0	4.0.5
Re-trigger after firmware upgrade	3.0	3.0	4.0.3	3.0	4.0.5
Device group ID	3.0	3.0	4.0.3	3.0	4.0.5
Avaya issued certificates	4.0.1	4.0.1	4.0.3	4.0.1	4.0.5
Provisioning enrollment code	4.0.4	4.0.4	4.0.4	4.0.4	4.0.5
Firmware manager tool	4.0.6.0	4.0.6.0	4.0.6.0	4.0.6.0	4.0.6.0
Avaya Cloud Office™ support	4.0.6.1.9	4.0.6.1.9	4.0.6.1.9	4.0.6.1.9	4.0.6.1.9
Device Enrollment Services as Provisioning Server	2.0	2.0	2.0	2.0	2.0

Avaya Vantage™ phones

The following table lists enrollment features and specifies the minimum supported device release for Avaya Vantage™:

Device enrollment features	Avaya Vantage™ K155	Avaya Vantage™ K165 and K175	Avaya Vantage™ HW-3 K155 and K175
Provisioning URLs	2.0	1.1	3.0
Re-provisioning devices	2.0	1.1	3.0
HTTPS provisioning URL	2.0	1.1	3.0
Firmware upgrade	2.0	1.1	3.0
HTTP provisioning URL	2.0	1.1 (Service pack 1)	3.0
Provisioning URL with IP address	N/A	N/A	N/A
Certificate with provisioning URL	2.0	2.0	3.0

Table continues…

Device enrollment features	Avaya Vantage™ K155	Avaya Vantage™ K165 and K175	Avaya Vantage™ HW-3 K155 and K175
8–digit numeric enrollment code	2.0	2.0	3.0
12-digit numeric enrollment code	2.0	2.0	3.0
Re-trigger after firmware upgrade	2.0	2.0	3.0
Device group ID	2.0	2.0	3.0
Avaya issued certificates	2.1	2.1	3.0
Provisioning enrollment code	N/A	N/A	N/A
Firmware manager tool	2.0.5	2.0.5	3.0
Avaya Cloud Office™ support	N/A	N/A	3.0
Device Enrollment Services as Provisioning Server	2.0	1.1	3.0

Other devices

The following table lists enrollment features and specifies the minimum supported device release for B199 and Avaya CU360 (Model number- 700513892, 700513893, and 700513894):

Device enrollment features	B199	CU360
Provisioning URLs	1.0.1	11.3.0.40
Re-provisioning devices	1.0.1	11.3.0.40
HTTPS provisioning URL	1.0.1	11.3.0.40
Firmware upgrade	N/A	N/A
HTTP provisioning URL	1.0.1	11.3.0.40
Provisioning URL with IP address	1.0.1	11.3.0.40
Certificate with provisioning URL	1.0.1	11.3.0.40
8–digit numeric enrollment code	1.0.1	11.3.0.40
12-digit numeric enrollment code	N/A	11.3.0.40
Re-trigger after firmware upgrade	1.0.1	N/A
Device group ID	N/A	11.3.0.40
Avaya issued certificates	1.0.1	11.3.0.40
Provisioning enrollment code	N/A	11.3.0.40
Firmware manager tool	1.0.3.0	N/A

Table continues…

Device enrollment features	B199	CU360
Avaya Cloud Office™ support	1.0.1.0.9	N/A
Device Enrollment Services as Provisioning Server	N/A	11.3.0.40

Device enrollment feature descriptions

The following table provides a description of the device enrollment features:

Feature	Description
Provisioning URLs	The provisioning URL provides the path to the directory where the device settings file is located. All successfully enrolled devices are redirected to the provisioning URL.
Re-provisioning devices	The device administrator can use the **Settings** menu on the device to perform Device Enrollment Services discovery.
HTTPS provisioning URL	The device can read or parse an HTTPS-based provisioning URL. A certificate is required to provide a secure connection for non-public FQDNs on provisioning servers that use the secure HTTPS protocol. For more information, see Provisioning server setup on page 25.
Firmware upgrade	Devices support redirection to the firmware upgrade URL if the software version for the device is not the latest version.
HTTP provisioning URL	The device can read or parse an HTTP-based provisioning URL.
Provisioning URL with IP address	The provisioning URL can use an IP address. Devices can read or parse a provisioning URL based on an IP address.
Certificate with provisioning URL	During the device enrollment process, the device provisions the root CA certificate sent by Device Enrollment Services.
8–digit or 12-digit numeric enrollment codes	If the device is not claimed, associated with a customer site, and activated on Device Enrollment Services, then it prompts for a numeric enrollment code. For more information, see Generating an 8–digit or 12-digit numeric enrollment code on page 44.
Re-trigger provisioning after firmware upgrade	After the firmware is upgraded, the device performs Device Enrollment Services discovery again.
Device group ID	During enrollment, the device configuration is based on the phone group number defined in the profile on Device Enrollment Services.
Avaya issued certificates	A Public Key Infrastructure (PKI) identify certificate is used to establish a secure connection between the device and the management server. The phone receives the certificate from Device Enrollment Services.

Table continues…

Feature	Description
Provisioning enrollment code	A 12-digit provisioning enrollment code contains the 8-digit account ID and a 4 digit PIN that you create. For more information, see 12–digit provisioning enrollment code on page 46.
Firmware manager tool	A customer can turn off the firmware upgrade for a specific device model, upgrade a device to its latest firmware version, or select any firmware version from the previous firmware versions.
Avaya Cloud Office™ support	Supported Avaya Cloud Office™ phone models device information can be uploaded and synchronized with the ACO system.
Device Enrollment Services as Provisioning Server	The device can read or parse Device Enrollment Services as an HTTPS-based provisioning URL to redirect and obtain settings files only from Device Enrollment Services server.

Index