Avaya one-X™ Mobile Administration and Maintenance Guide
Notice
While reasonable efforts were made to ensure that the information in this
document was complete and accurate at the time of printing, Avaya Inc. can
assume no liability for any errors. Changes and corrections to the information
in this document may be incorporated in future releases.

For full support information, please see the complete document,
Avaya Support Notices for Software Documentation, document number
03-600758.
To locate this document on our Web site, simply go to http://
www.avaya.com/support and search for the document number in the
search box.

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to
the original published version of this documentation unless such modifications,
additions, or deletions were performed by Avaya. Customer and/or End User
agree 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 the Customer or End User.

Link disclaimer
Avaya Inc. is not responsible for the contents or reliability of any linked Web
sites referenced elsewhere within this documentation, and Avaya does not
necessarily endorse the products, services, or information described or offered
within them. We cannot guarantee that these links will work all of the time and
we have no control over the availability of the linked pages.

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to your sales
agreement to establish the terms of the limited warranty. In addition, Avaya’s
standard warranty language, as well as information regarding support for this
product, while under warranty, is available through the following Web site:
http://www.avaya.com/support.

Copyright
Except where expressly stated otherwise, the Product is protected by copyright
and other laws respecting proprietary rights. Unauthorized reproduction,
transfer, and/or use can be a criminal, as well as a civil, offense under the
applicable law.
Cisco is a registered trademark of Cisco Systems, Inc.

Avaya support
Avaya provides a telephone number for you to use to report problems or to ask
questions about your product. The support telephone number
is 1-800-242-2121 in the United States. For additional support telephone
numbers, see the Avaya Web site: http://www.avaya.com/support.
## Contents

### Chapter 1: Overview
- About this Guide .................................................. 7
- Conventions ......................................................... 7
- Acronyms and Definitions ........................................ 8
- Support .............................................................. 8
- About the Avaya one-X Mobile Server ......................... 9
- Key Features and Benefits ....................................... 9

### Chapter 2: Getting Started
- Status Screen ........................................................ 13
- Configuring the Avaya one-X Mobile Server Setup Page .... 13
  - Server Setup ...................................................... 14
  - SMTP Settings .................................................. 14
  - Split Server Configuration ................................... 15

### Chapter 3: Avaya Setup
- Create a Provisioning Profile .................................. 17
- Create a CTI Profile ............................................... 20
  - Copy a Profile ................................................. 20
  - Create a New Profile ........................................... 23
- Create a Voicemail Profile ....................................... 26
  - Configure the Microsoft Active Directory Server ....... 27
  - Configure the Exchange Administrative User Setting. ... 28
  - Configure Modular Messaging with MSS ................. 30
- Create a Corporate Directory Profile .......................... 31
- Create a Class of Service ......................................... 34
- Configure CTI Ports ............................................... 38
- Create VDNs ........................................................ 40
- Administer Users .................................................. 42
  - Import Users .................................................... 42
  - Manage Unlicensed Users ..................................... 43
    - License Selected Users ....................................... 44
  - Manage Licensed Users ........................................ 44
    - Change Class of Service ..................................... 45
    - Reprovision Selected Users ................................. 46
    - Unlicense Selected Users .................................... 46
    - Delete Selected Users ....................................... 46
# Contents

View User Details .................................................. 47
Lost or Stolen Mobile Phone ..................................... 47
No Longer an Employee ........................................... 48
Unlock one-X Mobile Account ................................... 48

Chapter 4: Serviceability .......................................... 49
View Control Center ............................................... 49
View Route Points .................................................. 50
View Trace Components ......................................... 50
View Component Info ............................................. 51

Chapter 5: Licenses .................................................. 53
View License Information ......................................... 53

Chapter 6: Dial Plan Settings ..................................... 55
Configure Dial Plans ............................................... 55

Chapter 7: Carrier Offset .......................................... 57
Set Carrier Offset Settings ....................................... 57

Chapter 8: Cisco Setup ............................................. 59
Configure Cisco CallManager Settings ......................... 59
Create a Provisioning Profile .................................... 63
Copy a Profile ..................................................... 65
Create a Voicemail Profile ....................................... 66
Copy a Profile ..................................................... 70
Edit a Profile ...................................................... 71
Create a Corporate Directory Profile ......................... 71
Copy a Profile ..................................................... 74
Edit a Profile ...................................................... 74
Create a Class of Service ........................................ 75
Create CTI Ports .................................................... 79
Import Route Points ............................................... 82
Manage Route Points ............................................. 83
Administer Users ................................................... 84
Import Users ......................................................... 84
Manage Unlicensed Users ........................................ 85
Change Class of Service .......................................... 85
License Selected Users ............................................ 86
Contents

Manage Licensed Users .................................................. 87
  Change Class of Service ............................................ 87
  Reprovision Selected Users ...................................... 88
  Unlicense Selected Users ......................................... 88
  Delete Users .......................................................... 89
View User Details ....................................................... 89
  Lost or Stolen Mobile Phone ...................................... 90
  No Longer an Employee ............................................ 90
  Unlock one-X Mobile Account .................................... 90
Chapter 1: Overview

About this Guide

The Avaya one-X™ Mobile Administration and Maintenance Guide provides instructions for administering, configuring, and maintaining the Avaya one-X™ Mobile Server. It describes the tasks which must be completed using the Administrative Interface.

This guide is written for network and IT administrators who are responsible for administering, configuring, and maintaining the Avaya one-X Mobile Server. It requires knowledge of Avaya Communication Manager, Avaya Modular Messaging, Application Enablement Services, Cisco® CallManager, and Messaging applications.

Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong> font</td>
<td>Keywords and names of text fields are in boldface font.</td>
</tr>
<tr>
<td><em>Italic</em> font</td>
<td>Values that the administrator must enter into text fields are in italic font.</td>
</tr>
<tr>
<td><strong>Courier Font</strong></td>
<td>Text which must be entered into a terminal session is in courier font.</td>
</tr>
<tr>
<td><strong>Menu</strong> Font</td>
<td>Menu Items are in Bold Font</td>
</tr>
</tbody>
</table>
Acronyms and Definitions

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Application Enablement Services</td>
</tr>
<tr>
<td>AXL</td>
<td>AVVID XML Layer</td>
</tr>
<tr>
<td>CCM</td>
<td>Cisco CallManager</td>
</tr>
<tr>
<td>CM</td>
<td>Communication Manager</td>
</tr>
<tr>
<td>CMC</td>
<td>Client Matter Code</td>
</tr>
<tr>
<td>COS</td>
<td>Class of Service</td>
</tr>
<tr>
<td>CSS</td>
<td>Calling Search Space</td>
</tr>
<tr>
<td>EC500</td>
<td>Extension to Cellular</td>
</tr>
<tr>
<td>FAC (Avaya)</td>
<td>Feature Access Code</td>
</tr>
<tr>
<td>FAC (Cisco)</td>
<td>Forced Authorization Code</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol</td>
</tr>
<tr>
<td>JTAPI</td>
<td>Java Telephony Application Programming Interface</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MAPI</td>
<td>Messaging Application Programming Interface</td>
</tr>
<tr>
<td>MSS</td>
<td>Message Storage Server</td>
</tr>
<tr>
<td>SAC</td>
<td>Send All Calls</td>
</tr>
<tr>
<td>SAFE</td>
<td>EC500 Self Administration Feature</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
</tbody>
</table>

Support

For support, contact Avaya Support at 1-800-242-2121. There are also help tips on the right side of each page.
About the Avaya one-X Mobile Server

The Avaya one-X Mobile Server is the server platform which supports the Avaya one-X Mobile Client and serves as the mobile gateway to enterprise services.

The Avaya one-X Mobile Server extends enterprise telephony, data, and messaging capabilities to J2ME, Palm, and Blackberry mobile clients.

The Avaya one-X Mobile Server administrative interface enables configuration of settings for all network entities with which it will interact. It is also used to configure settings for users of the services provided by the Avaya one-X Mobile Server. Before configuring these settings, it is vital that the environment be configured appropriately. See the Avaya one-X™ Mobile Integration Guide, document number 18-602153, for more information.

Key Features and Benefits

The Avaya one-X Mobile Server key features include the following:

- Control of delivery of inbound calls to multiple locations of the user’s choice. This includes call routing based on VIP screening, scheduling, and GPS location.
- Visual view and playing of new and saved voicemails on the Avaya one-X Mobile handset or web client. This includes caller ID, length of message, and time/date of messages.
- View of Corporate Directories from the Avaya one-X Mobile handset or web client.
- The Avaya one-X Mobile Server is used to remotely place outbound calls via the Avaya one-X Mobile telephony system to execute the callback feature on the Avaya one-X Mobile handset or web client.
- Remote view of call logs on the Avaya one-X Mobile handset or web client.
Chapter 2: Getting Started

To begin working with the Avaya one-X Mobile administrative interface, follow these steps:

1. Obtain the Avaya one-X Mobile license file.

2. Open the WebLM page in the browser and install the license file. Perform this procedure on the single, combined home/edge from the server’s Avaya Services port, usually eth1.

An SES home/edge server requires these licenses:

- Home proxy license
- Edge proxy license
- Home seat licenses

These three licenses are accommodated in one file. Terminology differs between the Master Administration Interface License screen and the WebLM > Licensed Products > IMPRESS screen. See the table below.

The WebLM server is installed in one location only, on an edge or combined home/edge server.

License Terminology

<table>
<thead>
<tr>
<th>Administrative Web Interface</th>
<th>Web LM Screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Proxy</td>
<td>Edge Proxy License (EDGE_proxy)</td>
</tr>
<tr>
<td>Basic Proxy</td>
<td>Home Proxy License (BASIC_proxy)</td>
</tr>
<tr>
<td>Home Seats</td>
<td>Home Seat Licenses (HOME_seats)</td>
</tr>
</tbody>
</table>

Follow these steps to obtain licenses for the Avaya SES system:

1. To obtain the correct MAC address, go to a command line and type `get-mac-address` for eth0, the customer LAN connection. Note that it may have changed since you checked the server BIOS information. Alternatively, you can do the following:
   a. Enable and log in to WebLM using steps 5 through 8 below.
   b. Select Server Properties. The contents of the Primary Host ID field is the eth0 MAC address of the server.

2. Use your established RFA web procedures for obtaining licenses for Avaya servers.
   a. Use the MAC address you obtained in step 1.
   b. Go to the RFA web site at http://rfa.avaya.com and download the license file to where you can upload later on, typically to a location on a laptop used by services personnel.
Chapter 2: Getting Started

Note: To obtain RFA licenses needed to install the entire SES solution, you must have required manager approval for three product families: CM, SES, and Softclients.

3. Log in to SES and select the link to the Maintenance Web Interface.

4. From the list of available Security screens, select the link to view the WebLM Software screen.

5. If WebLM is not already enabled, select Enable WebLM.

6. From the list of available Security screens, select the link to view the WebLM License Administration screen.

7. Select Access WebLM. The system displays the WebLM application screen.

Note: The disable pop-ups option will need to be disabled if the WebLM browser screen does not launch.

8. From the WebLM screen, select License Administration and then enter the WebLM default administrative password.

9. After your initial login to WebLM, the system prompts you to change the password. When you do, WebLM logs you out and expects you to log back in with your new password.

10. Select Install license.

11. Select Browse and navigate to the location where you saved the license file in step 2, and then select Install. The proxy server will renew acquired licenses every 5 minutes. Initially, however, it has not acquired any licenses (since none were installed) so the proxy server will attempt to acquire licenses every 60 seconds. After it has acquired all licenses, it will renew them every 5 minutes.

12. Import the SSL certificates.

13. Proceed with the Avaya one-X Mobile Server Administrative Interface.

To access the Avaya one-X Mobile Server administrative user interface, first install the Avaya one-X Mobile Server Software. See the Avaya one-X™ Mobile Installation Guide, document number 18-602135, for instructions on how to install the software.

The Avaya one-X Mobile Server administration user interface is available at the following address: http(s):/<server ip or name>/Admin.

Microsoft Windows credentials are required to log in to the Avaya one-X Mobile Server Administrative Web site. This includes credentials for the local host of the Avaya one-X Mobile Server or for the domain for the Avaya one-X Mobile Server.
Status Screen

The status screen is displayed by default when navigating to the Avaya one-X Mobile Server administrative interface.

![Status Screen](image)

Various administrative tasks can be accessed by clicking tabs on this screen. If the Avaya one-X Mobile Server is being configured for the first time, click the **Server Setup** tab.

Configuring the Avaya one-X Mobile Server Setup Page

The Server Setup section of the administrative interface enables the configuration of the server’s authentication credentials.

Click on the **Server Setup** tab to open the Avaya one-X Mobile Server Setup page.
Chapter 2: Getting Started

Server Setup

The Server Setup page enables configuration of administrative information related to the various servers that the Avaya one-X Mobile Server communicates with. As shown in the Server Setup screen below, there are two tabs in the Server Setup view—the SMTP Settings tab and the Split Server Configuration tab.

SMTP Settings

The SMTP Settings section enables configuration of the SMTP server. The Avaya one-X Mobile server uses the SMTP server to send notifications of new voicemail.

To configure SMTP settings:

1. Enter the SMTP Username. This username will be used to login to the SMTP server.
2. Enter the SMTP Password. Asterisks will be entered in the field. Enter the IP address or hostname of the SMTP server. For example: 192.168.20.6 (Enter the SMTP Username and Password only if the server requires authentication.)

   Note: If Exchange is being used, the SMTP username must be in the following format: domain name/username.

3. Enter the SMTP port. Typically 25 is the default port for SMTP.
4. Enter the sender’s email. This email address is the address that the end user will see as the sender of messages sent to various web clients. Use a descriptive name such as notifier@example.com.
5. Enter the Avaya one-X Mobile Server administrator’s email address. This is the email address of the administrator that will be setting up and managing the system.

When certain events occur, the Avaya one-X Mobile Server can send an email to notify the IT administrator. An example of this is when an account is locked out due to exceeding the allowed number of login retries.

6. To save the SMTP changes, click the **Save Changes** button.

7. To discard any changes and revert to the previous settings, click the **Clear Changes** button.

See the *Avaya one-X™ Mobile Installation Guide*, document number 18-602135, for more information if using a split server configuration. The Avaya one-X Mobile server will need to know the IP addresses of external servers for security purposes. This will prevent connections from non-approved servers.

### Split Server Configuration

The Split Server Configuration settings can be configured only if a split server setup was chosen at the time of installation.

#### To configure the split server settings:

1. Enter the **Server IP addresses** as appropriate.

   **Note:**
   The *Internal Server IP Address* field is pre-populated with the loopback IP address 127.0.0.1

2. Click **Add Trusted Server** to add approved servers.

3. Add an external server that has the address of the internal server as it appears to the external server (not the loopback address).
Chapter 3: Avaya Setup

This chapter describes how to set up the Avaya one-X Mobile server for systems that use Avaya Communication Manager. If your system uses only Cisco CallManager, see Chapter 8: Cisco Setup on page 59.

Perform the Avaya Setup tasks in the following order:

1. Setup Profiles:
   a. Create a Provisioning Profile.
   b. Create a CTI Profile.
   c. Create a Voicemail Profile.
   d. Create a Corporate Directory Profile (a through d can be completed in any order).
   e. Create a Class of Service.

2. Configure CTI Resources:
   a. Configure CTI Ports.
   b. Create VDNs.

3. Administer Users:
   a. Import Users.
   b. Manage Unlicensed Users.
   c. Manage Licenses Users.

Create a Provisioning Profile

The Provisioning Profile must be completed before any further steps are taken. The Provisioning Profile task imports the users from the Active Directory and is used for two purposes:

- To indicate the source of user accounts that will be imported into the Avaya one-X Mobile database.
- To indicate the source for user account authentication.

Avaya one-X Mobile is capable of using LDAP v3 directories for the Provisioning Profile.
To create a new Provisioning Profile:

1. Select **Avaya Setup > Setup Profiles > Provisioning Profile**.

2. Click **New Provisioning Profile**.

3. In the **Profile Name** field, enter the name of the new profile.
4. In the **Description** field, enter a description of the profile.

5. In the **LDAP User DN** field, enter the LDAP user DN (for example, cn=administrator, ou=users, dc=example, dc=com). This is the user that will be used to search the directory for Avaya one-X Mobile users.
6. In the **LDAP Hostname** field, enter the LDAP hostname.
7. In the **LDAP Port Number** field, enter the LDAP port. The default value for Microsoft Active Directory is 389.
8. In the LDAP Password field, enter the password for this user. Asterisks appear in the field for security purposes.

9. In the LDAP Base DN field, enter the search base DN (for example, ou=users, dc=example, dc=com.)

Depending on the Directory setup, it may be necessary to fill out the advanced settings for LDAP attributes. The LDAP Attributes section allows for parameterization of the required fields as different directory implementations may use different attribute names to store the information required by the Avaya one-X Mobile Server.

Upon installation, Avaya one-X Mobile defaults many of these LDAP attributes to commonly used Microsoft Active Directory attribute names. These LDAP attributes may need to be changed depending on the implementation of the Directory.

10. In the Extension field, enter the attribute name used to hold the extension. If the extension is not housed in the directory, it may be derived as part of the import process.

11. In the 10 Digit Phone Number field, enter the attribute name for phone number.

12. In the Handle or UserID field, enter the attribute name user ID.

13. In the First Name field, enter the name user’s first name.

14. In the Last Name field, enter the attribute name for the user’s last name.

15. In the Email field, enter the attribute name for the user’s email address.

16. In the Department field, enter the attribute name for the user’s department.

17. Click Save to save the Provisioning Profile settings.

**Note:**
If an entry was not configured correctly, an error message appears. Red text indicates the section(s) that contain errors.
Create a CTI Profile

The CTI Profile is necessary to create a link to the AES to manage inbound and outbound calls for the Avaya one-X Mobile users.

**Note:**
Before setting up the CTI Profile, make sure that the AES integration steps have been completed. Refer to the *Avaya one-X™ Mobile Integration Guide*, document number 18-602153, for instructions on configuration of AES for Avaya one-X Mobile.

To create a new CTI Profile, you can:

- copy an existing CTI profile
- create a new CTI profile

Procedures for both methods are provided in this section.

---

Copy a Profile

To create a new CTI profile by copying an existing CTI profile:

1. Select **Avaya Setup > Setup Profiles > CTI Profile**.
2. Click **Copy Profile** next the profile to be copied.

The New CTI Profile screen appears as shown below.

3. In the **CTI Profile Name** field, rename the profile.

4. Change information in the other fields as appropriate.

5. Click **Save**.
Chapter 3: Avaya Setup

6. Click **Next**.

A status screen appears as shown below. Processing may take a few minutes.

After processing is complete, the New CTI Profile screen appears as shown below. The profile reflects the new profile information.
Create a New Profile

There are two steps involved in creating a new CTI Profile. You must:

1. Configure TSAPI and get TSAPI links
2. Create the CTI Profile using the selected TSAPI link

To create a new CTI profile:

1. Select **Avaya Setup > Setup Profiles > CTI Profile**.

2. Click **New CTI Profile**.

The New CTI Profile screen appears as shown below.

3. In the **CTI Profile Name** field, enter the name for this profile.
4. In the **Description** field, enter a description of this profile.
5. In the **AES Hostname** field, enter the hostname of the Application Enablement Services. Use the Avaya site’s Administration tool for more information. Make sure the hostname entered is resolvable from the Avaya one-X Mobile Server.
6. In the **JTAPI Port** field, enter the JTAPI port number. The default value for the JTAPI port is 450.

7. Click **Next**.

A message appears indicating the system is working, and the process may take a few minutes.

![Image](Please wait...Configuring Trapi Pro and getting Trapi Link. This may take a few minutes)

**Note:**

The Avaya one-X Mobile Server should be able to see the domain where AES is available, or AES is visible. If DNS is not setup for the AES server, then a hosts file entry should be made for the AES hostname entered in the AES hostname field.

After processing, the New CTI Profile screen appears.

<table>
<thead>
<tr>
<th>States</th>
<th>Server Setup</th>
<th>Avaya Setup</th>
<th>Cisco Setup</th>
<th>Serviceability</th>
<th>Licenses</th>
<th>Dial Plan Settings</th>
<th>Carrier Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI Resources</td>
<td>Setup Profiles</td>
<td>Users</td>
<td>CTI Profile</td>
<td>Voicemail Profile</td>
<td>Corporate Directory Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class of Service</td>
<td>Provisioning Profile</td>
<td>CTI Profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CTI Profile Name:**
- **Name:** Copy_of_TR_DEFAULT
- **Description:** Test
- **AES Hostname:** 140.147.220.124
- **JTAPI Port:** 450
- **Rank:** AVRT/AVRT/HOSTNAME/AES1
- **TLink Username:** Avaya
- **TLink Password:** SWITCH
- **Switch Name:** Avaya
- **DMCC Username:** Avaya
- **DMCC Password:** SWITCH

8. In the **TLinks** field, choose the link to be used from the drop down menu. This should match with the TLink that was created in the AES configuration. See “Chapter 4, Configure AES” in the *Avaya one-X™ Mobile Integration Guide*, document number 18-602153, for more information.

9. In the **JTAPI Username** field, enter the JTAPI username that was created in the AES configuration. See “Chapter 4, Configure AES” in the *Avaya one-X™ Mobile Integration Guide*, document number 18-602153, for more information.
10. In the **JTAPI Password** field, enter the JTAPI password that was created in the AES configuration. See “Chapter 4, Configure AES” in the *Avaya one-X™ Mobile Integration Guide*, document number 18-602153, for more information.

11. In the **Switch Name** field, enter the name of the switch as it is known in the AES configuration.

12. In the **DMCC Username** field, enter the DMCC username that was created in the AES configuration. See “Chapter 4, Configure AES” in the *Avaya one-X™ Mobile Integration Guide*, document number 18-602153, for more information.

13. In the **DMCC Password** field, enter the DMCC password that was created in the AES configuration. See “Chapter 4, Configure AES” in the *Avaya one-X™ Mobile Integration Guide*, document number 18-602153, for more information.

14. In the **Communication Manager Login** field, enter the login used to make changes in the Avaya Communication Manager.

15. In the **Communication Manager Password** field, enter the password for the Avaya Communication Manager login.

16. In the **Communication Manager Hostname** field, enter the Avaya Communication Manager hostname.

In the following section, **Switch Feature Access Codes**, you must collect the FACs from the switch and enter them into the Avaya one-X Mobile Server on this page. The server needs these FACs to perform call control actions on behalf of the user.

<table>
<thead>
<tr>
<th>Communication Manager Login</th>
<th>Password</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>cell</td>
<td>**********</td>
<td>148.147.22.124</td>
</tr>
</tbody>
</table>

17. In the **EC500 Enable FAC** field, enter the FAC to enable EC500. This FAC turns EC500 on.

18. In the **EC500 Disable FAC** field, enter the FAC to disable EC500. This FAC turns EC500 off.

19. In the **EC500 SAFE FAC** field, enter the EC500 SAFE FAC. This FAC changes the destination of the EC500 mobile phone.

20. In the **SAC enable FAC** field, enter the FAC to enable SAC. This FAC enables Send All Calls (SAC).
21. In the **SAC disable FAC** field, enter the FAC to disable SAC. This FAC disables Send All Calls (SAC).

---

### Create a Voicemail Profile

Although the Voicemail Profile types are different for Avaya and Cisco setups, a Voicemail Profile created under the Avaya setup can be used in a Cisco Class of Service, and a Voicemail Profile created under the Cisco setup can be used in an Avaya Class of Service.

**Note:**
Steps for Voicemail setup are the same for Cisco and Avaya.

There are two types of Voicemail Profiles:

- **Modular Messaging with MSS (Default for Avaya)** — the settings displayed under this type of profile are MSS Administrative user settings and LDAP Settings. Microsoft Active Directory Server and Exchange Administrative user settings are not displayed for this type of voicemail profile.

- **Modular Messaging with Exchange** — the settings displayed under this type of profile are Microsoft Active Directory Server and Exchange Administrative user settings. MSS Administrative User settings and LDAP Settings are not displayed for this type of voicemail profile.

To create a new Voicemail Profile:

1. Select **Avaya Setup > Setup Profiles > Voicemail Profile**.
2. **Click New Voicemail Profile.**

The New Voicemail Profile screen appears.

3. In the **Profile Name** field, enter a profile name.

4. In the **Profile Type** drop-down menu, select the profile type.

   If you select **Modular Messaging with Exchange Integration**, the Microsoft Active Directory Server and Exchange Administrative User Settings are displayed. These are further described in the next two sections. If you select Modular Messaging with MSS, see [Configure Modular Messaging with MSS](#) on page 30.

5. In the **Voicemail Platform Hostname** field, enter the hostname of the voicemail platform.

6. In the **IMAP Port** field, enter the IMAP port. In the previous field, if you selected Modular Messaging with MSS, the IMAP Port should be a secure port. For the Modular Messaging with Exchange Integration profile type, the IMAP port is often 993.

### Configure the Microsoft Active Directory Server

The Avaya one-X Mobile Server must be a member of a domain that is trusted by the Microsoft Exchange Server(s) where Avaya Modular Messaging deposits voicemail.

The **Microsoft Active Directory Settings** section enables the configuration of the location and authentication credentials of the Active Directory associated with the Microsoft Exchange Server. Access to Active Directory is required by the Avaya one-x Mobile Server for the following tasks:

- To accurately map received voice messages with the person that left the message.
Chapter 3: Avaya Setup

- To retrieve configuration information such as the hostname of the Microsoft Exchange Server for a particular user.
- To retrieve the Microsoft Exchange Alias of a particular user.

<table>
<thead>
<tr>
<th>Microsoft Active Directory Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory IP Address</td>
</tr>
<tr>
<td>Active Directory Port Number</td>
</tr>
<tr>
<td>Administrator User DN</td>
</tr>
<tr>
<td>Administrator Password</td>
</tr>
<tr>
<td>User Base DN</td>
</tr>
</tbody>
</table>

1. In the **Active Directory IP Address** field, enter the Active Directory IP address or hostname.
2. In the **Active Directory Port Number**, enter the Active Directory LDAP port number. In Active Directory deployments, port 389 is the default LDAP port.
3. In the **Administrator User DN** field, enter the Active Directory administrator user DN (for example, `cn=administrator, cn=users, dc=example, dc=com`).
4. In the **Administrator Password** field, enter the Active Directory administrator password. Asterisks appear for security purposes when the password is entered.
5. In the **User Base DN** field, enter the Active Directory user base DN (for example, `cn=users, dc=example, dc=com`). This should be the base DN where all users of Modular Messaging are stored.

**Configure the Exchange Administrative User Setting**

The **Microsoft Exchange Setup** section enables the configuration of the location and authentication credentials of the Exchange Server. Access to Exchange is required by the Avaya one-X Mobile Server to provide Visual Voicemail functionality. Authentication credentials of the Exchange administrator must be entered so that the Avaya one-X Mobile Server can access voicemail for any user.

**Create a Domain User**

The domain user is used by the Avaya one-X Mobile Application Suite to access voice messages from user mail boxes.

To create a domain user:

1. In the **Active Directory Users and Computer**, create a domain user account in the domain where the Microsoft Exchange server resides.

**Note:**

If multiple Exchange Servers are being used, perform the following tasks on each Exchange Server used by the Avaya one-X Mobile Application Suite.
2. In the **Exchange System Manager**, assign the permissions to domain user:
   a. Navigate to the **Mailbox Store** of the Exchange Server.
   b. Right click **Mailbox Store** and select **Properties**.
   c. Select the **Security** tab.
   d. Click the **Add** button and add the domain user.
   e. Assign the following permissions:
      - Read
      - Execute
      - Delete
      - Read permission
      - Change permission
      - List contents
      - Read properties
      - Write properties
      - List object
      - Open mail send queue
      - Receive As
      - Send As

   Once these permissions have been applied to the domain user, stop and restart the Microsoft Exchange System Attendant service, Microsoft Exchange MTA Stacks service, and Microsoft Exchange Information Store service. Optionally, wait for the update period to pass (usually around 24 hours). The permissions assigned to the domain user read into the Microsoft Exchange Applications.

   **Exchange Administrative User Setting**

<table>
<thead>
<tr>
<th>Exchange Username</th>
<th>Exchange Password</th>
</tr>
</thead>
</table>

   Identify the Exchange Administrative User used for Visual Voicemail to access end user messages. Ideally, this user should be a member of the domain administrators group. Additionally, the user must have permissions to log on as a service locally on the Avaya one-X Mobile Server.

3. In the **Exchange Username** field, enter the Exchange Administrative User name. Example: mydomain/administrator. Note that the domain name must be included here for Visual Voicemail to work correctly. This account should be an account that is a member of domain administrators and the Log on as Service permission.
4. In the Exchange Password field, enter the Exchange Administrative User password. Asterisks appear for security purposes when the password is entered.

5. Click Save to save the changes.

Configure Modular Messaging with MSS

If you selected Modular Messaging with MSS in the Profile Type field when you created a Voicemail Profile, the MSS Administrative User Settings and MSS LDAP Settings are required.

1. In the Profile Name field, enter a profile name.

2. In the Profile Type drop-down box, select Modular Messaging with MSS.

3. In the Voicemail Platform Hostname field, enter the hostname of the voicemail platform.

4. In the IMAP Port field, enter the IMAP port. The IMAP port should be a plain-text port. Often, the IMAP port for Modular Messaging with Exchange Integration is 143.

5. In the Administrative Username field, enter the username.
6. In the **Administrative Password** field, enter the password.
   
   The **Administrative Username** and **Password** information should be set up in the Trusted Servers section on the MSS Admin page.

   MSS LDAP Settings
   
   | LDAP User DN       |   |
   | LDAP Hostname      |   |
   | LDAP Port Number   | 389 |
   | LDAP Password      |   |
   | LDAP Base DN       |   |

7. In the **LDAP User DN** field, enter the LDAP user DN (for example, cn=administrator, ou=users, dc=example, dc=com).

8. In the **LDAP Hostname** field, enter the LDAP hostname.

9. In the **LDAP Port Number** field, enter the LDAP port number. The default value for Microsoft Active Directory is 389.

10. In the **LDAP Password** field, enter the LDAP password.

11. In the **LDAP Base DN** field, enter the search base DN (for example, ou=users, dc=example, dc=com.)

   Voicemail Mailbox Settings
   
   | Voicemail Mailbox ID Source |   |
   |                             |   |

12. In the **Voicemail Mailbox ID Source** drop-down box, select the source for the voicemail mailbox ID.

13. Click **Save** to save the Voicemail Profile settings.

   **Note:**
   If an entry was not configured correctly, an error message appears. Red text indicates the section(s) that contain errors.

---

### Create a Corporate Directory Profile

In order to provide the Avaya one-X Mobile client Corporate Directory Lookup feature, the Avaya one-X Mobile Server must integrate with a directory source such as Avaya one-X Mobile Server or Active Directory. This integration is known as a Corporate Directory Profile and may later be applied to a Class of Service which can be applied to a user group.
To create a Corporate Directory Profile:

1. Select **Avaya Setup > Setup Profiles > Corporate Directory Profile**.

2. Click **New Corporate Directory Profile**.
   The New Corporate Directory Profile screen appears.

3. In the **Profile Name** field, choose a unique profile name which will identify this profile.

   **Note:**
   This is the name that is used when specifying a corporate directory profile for a Class of Service.

4. In the **Description** field, enter a description of this profile.

5. In the **LDAP User DN** field, enter the LDAP user DN (for example, `cn=Administrator, ou=users, dc=example, dc=com`).

6. In the **LDAP Hostname** field, enter the LDAP hostname.
7. In the **LDAP Port Number** field, enter the LDAP port number. The default value for Microsoft Active Directory is 389.

8. In the **LDAP Password** field, enter the LDAP password.

9. In the **Corporate Directory Search Base DN** field, enter the corporate directory search base DN (for example, ou=users, dc=example, dc=com). This is the default value for the Avaya one-X Mobile Server.

10. Click **Show Advanced Settings** to view the LDAP Attributes section.

11. In the **Extension** field, enter the attribute name used to hold the extension. If the extension is not housed in the directory, it may be derived as part of the import process.

12. In the **10 Digit Phone Number** field, enter the attribute name for phone number.

13. In the **Handle or UserID** field, enter the attribute name user ID. This should be capitalized and will be the same as what was entered in the LDAP Attributes section of the **Provisioning Profile** tab in the **Setup Profile** section.

14. In the **First Name** field, enter the attribute name for the user’s first name.

15. In the **Last Name** field, enter the attribute name for the user’s last name.

16. In the **Email** field, enter the attribute name for the user’s email address.

17. In the **Department** field, enter the attribute name for the user’s department address.

18. Click **Save** to save the Corporate Directory Profile settings.

**Note:**
If an entry was not configured correctly, an error message appears. Red text indicates the section(s) that contain errors.
Create a Class of Service

After completing the profiles, a Class of Service is required. Class of Service is a representation of ways in which an Avaya one-X Mobile user will interact with the system. Class of Service settings include profiles (as described earlier in this chapter) as well as non-aggregated settings.

Note:
A valid Provisioning Profile is required to create a Class of Service. An error message appears if there is an attempt to create a Class of Service using an invalid Provisioning Profile.

To create a new Class of Service:

1. Select **Avaya Setup > Setup Profiles > Class of Service**.

2. Click **New Class of Service**.

   The New Class of Service Profile section appears.

3. In the **Class of Service Name** field, enter the name for this Class of Service.

4. In the **Description** field, enter a description of this Class of Service.
5. In the **Provisioning Profile** drop-down box, select the appropriate profile.
6. In the **Voicemail Profile** drop-down box, select the appropriate profile.
7. In the **Corporate Directory Profile** drop-down box, select the appropriate profile.
8. In the **CTI Profile** drop-down box, select the appropriate profile.

![Security Section]

9. In the **Security** section, do the following:
   a. Click the checkbox to **Allow voicemail to be stored on the mobile device**.
   b. Click the checkbox to **Require login each time one-X Mobile is launched on mobile device**, if required.
   c. Set the **Maximum number of attempts before user is locked out** (default is 5).
   d. Set the **Time period for which a user is locked out in minutes** (default is 90).

![Dial Plan Settings Section]

10. In the **Dial Plan Settings** section, do the following:
    a. Set the **Maximum number of phones to Send Calls to**.
    b. Set the **PSTN Prefix** (which is the number necessary to dial to reach an outside line).
    c. Click the checkbox to **Require DTMF during callback via PBX**, if required.
    d. Click the checkbox to **Allow International Dialing**, if required.
    e. Click the checkbox to **Translate 10-digit numbers to extensions**, if required.
Chapter 3: Avaya Setup

Note:
For Avaya Setup, the minimum and maximum number of phones to send calls to is 2 and 5 respectively.

11. In the Mobile Client Settings section, do the following:
   a. Click the checkbox to Require client software upgrades, if required.
   b. Set the Number of days to warn users before making updates mandatory.
   c. Select the RIM Blackberry Connection Settings from the drop-down box.

12. In the Server section, do the following:
   a. Enter the End user website server URL.
   b. If this is a secure server, click the checkbox to set this as is a secure server.
13. To view the LDAP Attribute Source Profiles, click **Show Advanced Settings**.

In the **LDAP Attribute Source Profiles** section, there is an opportunity to fine tune the Avaya one-X Mobile Server to use different directory sources for different data fields collected from directories. In some enterprise deployments, one directory may contain some information such as first name, last name; while another may contain information such as the 10-digit phone number.

The Avaya one-X Mobile Server can map from one directory to another; where the sources are the Corporate Directory Profile and the Provisioning Profile. The Provisioning Profile will always be used for authentication and the Corporate Directory Profile may be used for name resolution. In all cases, the **Handle or UserID** must be the key between the two directory sources. That is, if mapping is done, the UserID in one directory must match that of the other directory.

Use the drop-down boxes to tell the Avaya one-X Mobile Server from what directory to source the different attributes.

<table>
<thead>
<tr>
<th>LDAP Attribute Source Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Handle or UserID</strong></td>
</tr>
<tr>
<td><strong>10 Digit Phone Number</strong></td>
</tr>
<tr>
<td><strong>First Name</strong></td>
</tr>
<tr>
<td><strong>Last Name</strong></td>
</tr>
<tr>
<td><strong>Email</strong></td>
</tr>
<tr>
<td><strong>Department</strong></td>
</tr>
<tr>
<td><strong>Determine Extension from</strong></td>
</tr>
<tr>
<td><strong>LDAP Extension Source</strong></td>
</tr>
</tbody>
</table>

14. In the **Handle or UserID** drop-down box, select the appropriate profile.
15. In the **10 Digit Phone Number** drop-down box, select the appropriate profile.
16. In the **First Name** drop-down box, select the appropriate profile.
17. In the **Last Name** drop-down box, select the appropriate profile.
18. In the **Email** drop-down box, select the appropriate profile.
19. In the **Department** drop-down box, select the appropriate profile.
20. In the **Determine Extension from** drop-down box, select the appropriate source.

**Note:**
For the **Determine Extension from** drop-down box, extensions for users can be determined either directly from the LDAP attribute or manually from the 10-digit phone number. Manual determination can be done in one of two ways:

- automatically – determined automatically using dial plan rules
- algorithmically – by entering the number of leading digits to strip from the 10-digit phone number and/or adding prefixed after the digits have been stripped.
21. In the **LDAP Extension Source** drop-down box, select the appropriate profile.

---

**Configure CTI Ports**

CTI Ports are used to make outbound calls from the switch. An example of when this would be used is when a user has their Simulring feature enabled. A CTI Port would be used to make a call to the mobile phone so both the desk phone and the mobile phone would ring. The Avaya one-X Mobile Server can automatically create CTI Ports for use by the application.

The Avaya one-X Mobile database provides the option to create database entries for CTI Ports/VDNs for CTI Ports that already exist. This allows creation of CTI Ports/VDNs in the database if they already exist.

To view CTI Port information, select **Avaya Setup > CTI Resources > CTI Ports**.
To make CTI Ports available to the Avaya one-X Mobile Server, click **Create New Directory Range**.

1. In the **Directory Number Range** fields, enter the directory number range of the CTI Ports to be added. Choose a range of numbers which do not conflict with any other stations or directory numbers in Avaya Communication Manager.

2. In the **Class of Service** drop-down box, select the Avaya one-X Mobile Class of Service which was created in the Class of Service section. This Class of Service should have a properly configured CTI Profile.

3. In the **Switch Class of Restriction** field, enter a Class of Restriction for the CTI Ports. It may be helpful to use a special one so they can be administered as a group.

4. In the **Switch Class of Service** field, enter a Switch Class of Service that is preconfigured on Avaya Communication Manager. For Avaya one-X Mobile to work properly, **console permissions** must be set to `y` in the Class of Service table.

5. If ports already exist on the switch that will be used, enter all the information relating to those ports in the appropriate fields, then click the checkbox next to **Create CTI Ports in one-X Mobile database only**.

   **Note:**
   
   If the checkbox remains unchecked before clicking **Save**, new CTI ports will be created in the next step.

6. Click **Save** to save the CTI Ports you have created.

   A message appears notifying you that the ports are being created. After the process is complete, it is recommended that you test the ports to ensure they were created correctly. This will ensure that all calls are routed successfully.
Create VDNs

Vector Directory Numbers (VDNs) are used to collect Dual Tone Multi Frequency (DTMF) tones to ensure that a network voicemail platform does not answer a callback and then connect the callback destination party to the voicemail platform. To avoid this situation, a tone is collected to ensure that a human being answers the first leg of the callback. As part of this, VDNs are used to play a prompt to the user when they answer the first leg of a callback call. For example, if a user wishes to place a callback to their mobile phone, they will hear a message, stating to press a digit or tone to complete the call. Once Avaya one X Mobile detects the DTMF entry by the user, the second leg of the callback is placed. If the caller does not press the appropriate key, the server will not initiate the second leg of the callback. This prevents the second leg of the callback from being placed if mobile phone connectivity is lost before the call is completed.

The Avaya one-X Mobile platform must have knowledge of provisioned VDNs to function. VDNs can be created from the Avaya one-X Mobile administration interface and from Avaya Communication Manager. They can also simply be uploaded if they already exist.

To view VDN information, select **Avaya Setup > CTI Resources > VDNs**.
To make VDNs available to the Avaya one-X Mobile Server, click **Create New Directory Range**.

Note: If the VDNs already exist on the switch and you do not want to create new VDNs, click the checkbox for **Create VDNs in one-X Mobile database only**. This will create VDNs only in the Avaya one-X Mobile Server database.

Some important information about triplets:

- How many triplets you create depends on how many callbacks you expect at your busy hour, since it is a busy hour calculation. One triplet is needed to service a callback. They are returned to the pool after use.
- If you run out of VDN triplets, the call is placed, but no DTMF tone is collected. The second leg of the call is immediately placed.

For each triplet, follow these steps:

1. In the **Virtual Directory Number Range** field, enter the directory number range of the VDNs and CTI Ports to be added. Choose a range of numbers which do not conflict with any other stations or directory numbers in Avaya Communication Manager.

   Note: This range must be a multiple of 3 to accommodate two VDNs and a CTI Port triplet. You will receive an error if your range is not valid.

2. In the **CTI Profile** drop-down box, select the Avaya one-X Mobile CTI Profile which was created in the CTI Profile section.

3. In the **Switch Class of Service**. The Switch Class of Service should be one that is preconfigured on Avaya Communication Manager. For Avaya one-X Mobile to work properly, **console permissions** must be set to **y** in the Class of Server table.
4. In the **Class of Restriction** field, enter a Class of Restriction for the CTI Ports. It may be helpful to use a special one so they can be administered as a group.

5. In the **TN** field, enter a tenant number. A **TN** is a tenant partition number and identifies the partition for the phone you are administering. The default value for this field is 1.

6. Click the checkbox for **Create VDNs in one-X Mobile database only** if existing VDNs will be used. If the checkbox remains unchecked before clicking **Save**, new VDNs will be created in the next step.

7. Click **Save** to create the VDNs in the switch and Avaya one-X Mobile platform.

8. Before proceeding, make sure all required triplets were created.

9. See the **Avaya one-X™ Mobile Integration Guide**, document number 18-602153, for instructions on how to configure the VDNs that have been created.

---

**Administer Users**

This section describes how to provision users for whom the Avaya one-X Mobile Server services will be available. This section describes how to:

- Import Users
- Manage Unlicensed Users
- Manage Licensed Users

---

**Import Users**

To import users:

1. Select **Avaya Setup > Users > Import Users**.
2. In the **Class of Service** drop-down box, select the appropriate Class of Service.

3. In the **Filter** field, enter the filter. Valid filters are similar to those entered directly in LDAP.
   - To import a single user, use `sAMAccountName=<pbxusername>`. For example, to import a single user enter `sAMAccountName=edge8`.
   - To import several users, use wildcards `cn=*, objectclass=user`. For example, to import several users, enter `cn=edge*, cn=*, mail=*mydom.com`.

   **Note:**
   The screen does not refresh itself during a user import.

4. Click **Import Users**.

---

**Manage Unlicensed Users**

To view all imported user accounts that are not yet licensed:

1. Select **Avaya Setup > Users > Unlicensed User Management**.

2. To search for specific users, enter text in the **Search** field.

3. To search for all users, leave the **Search** text box blank and press **Enter** or click **Show All**, if it is available.

4. To navigate to a particular section of users when a large number of results are returned, use the **Sort by** drop-down box.
License Selected Users

To license a user, click the checkbox next to that user’s name and click **License Selected Users**.

This will license the user in the Avaya one-X Mobile Server database and decrement the number of licenses available for assignment.

A message appears letting you know that it is importing users in a background process. Licensing users can take some time depending on the size of the user base. When users are licensed, the Avaya one-X Mobile Server works in the background to retrieve required provisioning information for the user. When complete, you will be able to locate the new users in the **Licensed User Management** tab.

Manage Licensed Users

To view all imported user accounts that are licensed:

1. Select **Avaya Setup > Users > Licensed User Management**.

2. To search for a user, in the **Search** field enter the user’s last name, first name, extension, Class of Service, or department.

3. To change the page displayed, in the **Show** drop-down box, select the appropriate page.

4. To change the way the information is sorted on the page, in the **Sort by** drop-down box, make the appropriate selection.
To manage licensed users, the following features are available:

- Change Class of Service
- Reprovision Selected Users
- Unlicense Selected Users
- Delete Selected Users

**Change Class of Service**

To change the Class of Service for a user or group of users:

1. On the **Licensed User Management** screen, click the checkbox next to each user for whom you want to change the Class of Service.

2. In the **Class of Service** drop-down box, select the new class of service.

3. Click **Yes**.
Reprovision Selected Users

To reprovision users or a group of users:

1. On the Licensed User Management screen, click the checkbox next to each user or user group that you want to reprovision.

2. Click Reprovision Selected Users.

   The Avaya one-X Mobile Server retrieves the new user information and updates the Avaya one-X Mobile Server database.

Unlicense Selected Users

Unlicensed users are not able to log in to their Avaya one-X Mobile account from either the Avaya one-X Mobile Web site or their mobile device.

To unlicense a user:

1. On the Licensed User Management screen, click the checkbox next to the user you want to unlicense.

2. Click Unlicense Selected Users.

   This will increment the number of licenses available for assignment.

**Important:**

When you remove a license from a user, remember to move the user back into a Partition which is not managed by the Avaya one-X Mobile Server. This will prevent the Avaya one-X Mobile Server from managing the call.

Delete Selected Users

Deleting a user will delete all the call logs and any other data associated with that user in the Avaya one-X Mobile database. The user will not be able to login to their Avaya one-X Mobile account from either the Avaya one-X Mobile Web site or their mobile device.
To delete a user:

1. On the **Licensed User Management** screen, click the checkbox next to the user(s) you want to delete.

2. Click **Delete Selected Users**.

This will decrement the number of used licenses and remove the user from the Avaya one-X Mobile Server database. It will **not** remove the user from the LDAP directory.

---

**View User Details**

Click on **Details** next to any user on the **Licensed User Management** or **Unlicensed User Management** screens to display more information about that user.

- From the User Details screen you can:
  - Reprovision a user
  - Delete a user
  - Take action on a user’s account if the user has lost their mobile phone.
  - Take action on a user’s account if the user is no longer an employee.
  - Unlock a locked user account.

**Lost or Stolen Mobile Phone**

If a user’s mobile phone has been lost or stolen, click on **Lost or Stolen Mobile** on the User Details screen. This screen will provide instructions for further steps you should take. This may include resetting the user’s password and loss of local data on their mobile phone.
No Longer an Employee

If a user is no longer an employee, click on No Longer an Employee on the User Details screen. This screen will provide further instructions depending on whether the user account needs to be retained or completely removed from the Avaya one-X Mobile Database.

Unlock one-X Mobile Account

A user account may get locked out by the Avaya one-X Mobile Server if the user enters an incorrect login too many times. This will prevent a user from logging into the Avaya one-X Mobile application on both their mobile phone and the Avaya one-X Mobile Web site. A user account that is locked will automatically be unlocked after the lockout time (as set in the Class of Service for the user) has expired.

If a user account needs to be unlocked before the lockout time expires, click on Unlock one-X Mobile Account on the User Details screen. This will unlock the user account, and access to the Avaya one-X Mobile Web site and the Avaya one-X Mobile application on their mobile phone will be allowed.

Note:
This does not unlock a user’s voicemail mailbox.
Chapter 4: Serviceability

The Serviceability section of the Avaya one-X Mobile Administrative Interface allows monitoring and management of services, and provides information about Avaya one-X Mobile Server components and allows fine tuning of these components.

View Control Center

To view the Control Center, select Serviceability > Control Center.

Control Center allows you to stop, start, and monitor services controlled by the Avaya one-X Mobile Server. All components show whether they are installed or not.
View Route Points

To view Route Points, select Serviceability > Route Points.

Route Points lists the status of Route Points used in the Cisco Setup.

View Trace Components

To view Trace Components, select Serviceability > Trace Components.

Trace Components allow you to manipulate the data stored in logs. The default setting on each field on this page is to debug. This provides the most information and will also allow you to troubleshoot more thoroughly.
View Component Info

To view Component Info, select Serviceability > Component Info.

Component Info provides information about various components such as version numbers and last known status.
Chapter 5: Licenses

The Licenses section of the Avaya one-X Mobile Administrative Interface displays the most current information about licenses being used, licenses available, and licenses acquired.

View License Information

To view License Information, select Licenses > License Information.

You must enter the hostname of the WebLM server in the WebLM Hostname URL field in order to get accurate information about licenses.

There are 3 Application Modes in which WebLM will operate:

1. Grace — allows users to be licensed for a trial period of 30 days. The number of grace days remaining will be displayed on the License Information page if the server is in Grace mode.

2. Normal — indicates that WebLM is functioning normally.

3. Restricted — indicates the Grace period has expired and users cannot log in to their accounts.
Chapter 6: Dial Plan Settings

The Dial Plan Settings section of the Avaya one-X Mobile Administrative Interface shows how the dial plans are configured. Dial Plan settings tell the Avaya one-X Mobile Server how to send calls. For Avaya Setup, this is based on the Class of Service. For Cisco Setup, this is based on the Calling Search Base.

Configure Dial Plans

To view Dial Plans, select **Dial Plan Settings > Dial Plans**.

![Dial Plan Settings](image)

The default setting is to dial 1 plus ten numbers, but additional rules can be configured.
For example, if an enterprise has phone numbers set up as seven digits to take advantage of toll savings, the dial plan can be configured to dial seven digits instead of ten.
Chapter 7: Carrier Offset

The Carrier Offset section of the Avaya one-X Mobile Administrative Interface allows you to control the amount of time between when a call reaches the carrier network and is answered by the carrier’s voicemail system. This allows the Avaya one-X Mobile Server to redirect a call that was answered by carrier voicemail to the Cisco Unity Voicemail.

For example, if a user has their call handling settings set to To Mobile, a CTI port makes an outbound call to the mobile phone. If the call is answered in less than the carrier offset seconds, the call is diverted to Cisco Unity Voicemail.

Set Carrier Offset Settings

To set the Carrier Offset Settings for a particular carrier:

1. Select Carrier Offset > Carrier Offset Settings.

   ![Carrier Offset Settings](image)

   Note: The Carrier Offset Setting is set on a per-wireless carrier basis because some networks are much faster than others.

2. In the appropriate carrier field, enter the offset in milliseconds. A value of 100 milliseconds means that if a call to a mobile phone is answered in less than 100 milliseconds, the Avaya one-X Mobile Server will redirect the incoming call into Cisco Unity Voicemail.

3. Click the Update Settings button.
Chapter 8: Cisco Setup

This chapter describes how to set up the Avaya one-X Mobile Server for systems that use Cisco CallManager.

Perform the Cisco setup tasks in the following order:

1. Configure Cisco CallManager settings.
2. Set up Profiles:
   a. Create a Provisioning Profile.
   b. Create a Voicemail Profile.
   c. Create a Corporate Directory Profile.
   d. Create a Class of Service.
3. Create CTI Ports.
4. Set up Route Points:
   a. Import Route Points.
   b. Manage Route Points.
5. Administer Users:
   a. Import Users.
   b. Manage Unlicensed Users.
   c. Manage Licenses Users.

Configure Cisco CallManager Settings

Cisco CallManager Settings enables you to configure the Avaya one-X Mobile Server with the location and administrative information related to the various servers with which the Avaya one-X Mobile Server communicates.

The Cisco CallManager Settings that must be configured are:

- **AXL Settings** — enables the Avaya one-X Mobile Server to communicate with the Cisco AXL interface on the CallManager. This is required to provision other user functions on the Avaya one-X Mobile Server.
Chapter 8: Cisco Setup

- **LDAP Settings** — enables configuration of the location of the Cisco CallManager LDAP directory. The Avaya one-X Mobile Server requires access to the LDAP server to enable end user logins and corporate directory searches.

- **JTAPI Settings** — enables the configuration of the Cisco CallManager JTAPI authentication credentials. JTAPI is the protocol used by the Avaya one-X Mobile Server to communicate with Cisco CallManager for call handling services.

To configure Cisco CallManager Settings:

1. Select **Cisco Setup > Cisco CallManager Settings**.

2. In the **AXL Hostname** field, enter the Cisco AXL hostname. This should be the IP address of a published Cisco CallManager (for example, 192.168.98.6).

3. In the **AXL Port** field, enter the Cisco AXL port number (for example, 80). This port is the port on which Cisco AXL services run. By default this is set to port 80 during Cisco CallManager installation.

4. In the **AXL Username** field, enter the Cisco AXL username. This is the username used to access AXL (for example, administrator).
5. In the **AXL Password** field, enter the Cisco AXL password. Asterisks appear in the field for security purposes.

The Cisco CallManager LDAP structure has two main trees which it needs to access. The first is the User Base Distinguished Name (DN) and the second is the Cisco Configuration Base DN. All Cisco CallManager users are stored under the User Base DN. Specific profile information about users is stored under the Cisco Configuration Base DN. When the Avaya one-X Mobile Server performs corporate directory lookups or logins, the search is initiated from the User Base DN. The common name (CN) for Cisco CallManager users contains pointers to the Cisco Configuration Base DN where all the CallManager specific information is kept.

Cisco CallManager hosts its own LDAP DC Directory. If you have integrated Cisco CallManager LDAP with Active Directory, then the fields in the LDAP Settings section should point to Active Directory instead of Cisco CallManager LDAP.

6. In the **LDAP User DN** field, enter the LDAP user DN (for example, `cn=Directory Manager, o=cisco.com`). If you have not integrated Active Directory with Cisco CallManager, then this User DN is the default that was created when you installed Cisco CallManager. The default name for the Directory Manager account is **Directory Manager**.

7. In the **LDAP Hostname** field, enter the LDAP host IP address (for example, 193.148.88.5). If Active Directory has been integrated, then this will be the IP address of Active Directory; otherwise, it should be the IP address of Cisco CallManager.

8. In the **LDAP Port Number** field, enter the number of the LDAP port. The default value for Cisco CallManager DC Directory LDAP is 8404. If Active Directory and Cisco CallManager have been integrated, then the default value for Active Directory is 389.

9. In the **LDAP Password** field, enter the LDAP Password. Asterisks appear in the field for security purposes.

10. In the **Cisco Configuration Base DN** field, enter the Cisco Configuration Base DN (for example, `ou=CCN, o=cisco.com`). The value given in the example is the default set when Cisco CallManager is installed. If Active Directory has been integrated, then this value was set during the integration of Active Directory and Cisco CallManager.
11. In the **Cisco Base DN** field, enter the Cisco User Base DN (for example, ou=Users, o=cisco.com). The example is the default set when Cisco CallManager is installed. If Active Directory has been integrated, then this value was set during the integration of Active Directory and Cisco CallManager.

![JTAPI Settings](image)

12. In the **CallManager Cluster Node IP Addresses** field, enter the Cisco CallManager IP addresses or hostnames.

⚠️ **Important:**

If you have a clustered environment, be sure to enter a comma-separated list which includes each node in the cluster.

13. In the **JTAPI Username** field, enter the JTAPI username you created (for example, jtapiuser).

14. In the **JTAPI Password** field, enter the JTAPI password for the JTAPI user. Asterisks appear in the field for security purposes.

15. If you have taken steps to integrate Cisco CallManager LDAP with Microsoft Active Directory, click the checkbox for **Cisco CallManager is integrated with Microsoft Active Directory**.

16. Click **Save Changes**.

17. To check for JTapi updates, click **Check for JTapi Updates**. Be sure to click this link when the Cisco CallManager version has been updated to keep the Avaya one-X Mobile server application in sync with Cisco CallManager.
Create a Provisioning Profile

The Provisioning Profile task imports the users from the Active Directory and is used for two purposes:

- To indicate the source of user accounts that will be imported into the Avaya one-X Mobile database.
- To indicate the source for user account authentication.

Avaya one-X Mobile is capable of using LDAP v3 directories for the Provisioning Profile.

To create a new Provisioning Profile:

1. Select **Cisco Setup > Setup Profiles > Provisioning Profile**.
2. Click **New Provisioning Profile**.

![Cisco Setup Interface](image)

3. In the **Profile Name** field, enter the name of the new profile.
4. In the **Description** field, enter a description of the profile.
5. In the **LDAP User DN** field, enter the LDAP user DN (for example, cn=administrator, ou=users, dc=example, dc=com). This is the user that will be used to search the directory for Avaya one-X Mobile users.
6. In the **LDAP Hostname** field, enter the LDAP hostname.
7. In the **LDAP Port Number** field, enter the LDAP port. The default value for Microsoft Active Directory is 389.
8. In the **LDAP Password** field, enter the password for this user. Asterisks appear in the field for security purposes.
9. In the **LDAP Base DN** field, enter the search base DN (for example, ou=users, dc=example, dc=com).
10. To view LDAP Attributes fields, click **Show Advanced Settings**.

11. In the **Extension** field, enter the attribute name used to hold the extension. If the extension is not housed in the directory, it may be derived as part of the import process.

12. In the **10 Digit Phone Number** field, enter the attribute name for phone number.

13. In the **Handle or UserID** field, enter the attribute name user ID. This should be capitalized and will be the same as what was entered in the LDAP Attributes section of the Provisioning Profile tab in the Setup Profile section.

14. In the **First Name** field, enter the name user’s first name.

15. In the **Last Name** field, enter the attribute name for the user’s last name.

16. In the **Email** field, enter the attribute name for the user’s email address.

17. In the **Department** field, enter the attribute name for the user’s department.

18. Click **Save** to save the Provisioning Profile settings.

**Note:**
If an entry was not configured correctly, an error message appears. Red text indicates the section(s) that contain errors.

---

**Copy a Profile**

You can create a new Provisioning Profile by copying an existing profile, and changing the desired settings.

To create a new Provisioning Profile by copying an existing Provisioning Profile:

1. Select **Cisco Setup > Setup Profiles > Provisioning Profile**.

2. Click **Copy Profile** next to the profile to be copied.

   The **New Provisioning Profile** screen appears.

3. In the **Profile Name** field, rename the profile.
4. Change information in the other fields as appropriate.
5. Click Save.

Create a Voicemail Profile

In order to provide the Cisco CallConnect client Visual Voicemail feature, the Avaya one-X Mobile Server must integrate with Unity or Unity Connections. This integration is known as a Voicemail Profile and may later be applied to a Class of Service which can be applied to a user group.

Depending on your network configuration, either follow the instructions for Configuring a Unity Voicemail Profile or the instructions for Configuring a Unity Connections Voicemail Profile.

To create a new Voicemail Profile:

1. Select Cisco Setup > Setup Profiles > Voicemail Profile.
2. Click **New Voicemail Profile**.

3. In the **Profile Name** field, enter a profile name. Note that this is the name that is used when specifying a voicemail profile for a Class of Service.

4. In the **Profile Type** drop-down menu, select **Unity**.

5. In the **Voicemail Pilot Number** field, enter the Voicemail pilot number. Note that this will only be used if the Avaya one-X Mobile Server is unable to provision the pilot number directly via the AXL interface.

6. In the **Active Directory IP Address** field, enter the Active Directory IP address or hostname (for example, 192.168.20.7).

The Avaya one-X Mobile Server must be a member of a domain that is trusted by the Microsoft Exchange server(s) where Cisco Unity deposits voicemail.

The **Microsoft Active Directory Server** section enables the configuration of the location and authentication credentials of the Active Directory associated with the Microsoft Exchange Server. Access to Active Directory is required by the Avaya one-X Mobile Server for the following tasks:

- To accurately map received voice messages with the person that left the message.
- To retrieve configuration information such as the hostname of the Microsoft Exchange Server for a particular user.
- To retrieve the Microsoft Exchange Alias of a particular user.
Chapter 8: Cisco Setup

7. In the **Active Directory Port Number**, enter the Active Directory LDAP port number. In Active Directory deployments, port 389 is the default LDAP port.

8. In the **Administrator User DN** field, enter the Active Directory administrator user DN (for example, `cn=administrator, cn=users, dc=example, dc=com`).

9. In the **Administrator Password** field, enter the Active Directory administrator password. Asterisks appear for security purposes when the password is entered.

10. In the **User Base DN** field, enter the Active Directory user base DN (for example, `cn=users, dc=example, dc=com`). This should be the base DN where all users of Cisco Unity are stored.

![Exchange Administrative User Setting](image)

The **Exchange Administrative User Setting** section enables the configuration of the location and authentication credentials of the Exchange Server. Access to Exchange is required by the Avaya one-X Mobile Server to provide Visual Voicemail functionality. You must enter the authentication credentials of the Exchange administrator so that the Avaya one-X Mobile Server can access voicemail for any user.

Identify the Exchange Administrative User you wish to use for Visual Voicemail to access end user messages. Ideally, this user should be a member of the Domain Administrators group. Additionally, the user must have permissions to Log on as a Service locally on the Avaya one-X Mobile Server.

Perform the following steps to make sure the user has permissions to log on locally:

a. Go to **Start > Run** on the Avaya one-X Mobile Server.

b. In the **Open** field, enter `secpol.msc`.

c. Double click **Local Policies**.

d. Click on **User Rights Assignment**.

e. On the right panel double click **Log on as Service**.

f. Click the **Add** button.

g. In the **Look in:** drop-down box, choose the domain of the administrative user.

h. In the **Name** list box, locate the administrative user.

i. Double-click on the user name. This should add the user to the bottom section of the dialog box.

j. Click **OK**. You should see the user name and the domain name in the **Local Setting** column.
k. Close the **Local Security Settings** window.

Perform the following steps to validate that the designated Exchange Administrative User has sufficient permissions to manage the end user mailbox:

l. Go to the Domain controller for the specified domain that the Administrative user is a member of.

m. Go to **Start > Programs > Administrative Tools > Active Directory Users and Computers** to bring up the Management Console.

n. Click on **View > Advanced Features**.

o. Expand the tree control for the specified domain of the Administrative user.

p. Click on **Users**.

q. Locate the user in the right-hand pane.

r. Right click on the designated user and click on **Properties**.

s. Locate the group in which the user is a member.

t. In the **Permissions** frame, check all the listed permissions as **allow** except **Full Control**. **Full Control** should have neither **allow** nor **deny** checked.

u. Click **Apply** if changes were required.

v. Click **OK** to exit the property page.

w. Exit out of the Management Console.

11. In the **Exchange Username** field, enter the Exchange Administrative username (for example, mydomain/administrator). Note that the domain name must be included here for Visual Voicemail to work correctly. This account should be an account that is a member of Domain Administrators and the Log on as Service permission.

12. In the **Exchange Password** field, enter the Exchange Administrative user password. Asterisks appear in the field for security purposes.

13. Setup the Win32 Service Logon Rights:

   a. Go to **Start > Control Panel > Administrative Tools**.

   b. Double-click on the Services control panel element.

   c. Locate the **Edge MapiMgr Service** in the list.

   d. Open the properties of the service.

   e. Click on the **LogOn** Tab.

   f. Click on the **This Account** radio button.

   g. Enter the fully qualified username and password.

   h. Click **OK** and start the service.
14. Click **Save** to save the Voicemail Profile settings.

**Note:**

If your settings are configured correctly, a **Test Successful** message appears following each setup area.

If an entry was not configured correctly, an error message appears. Red text indicates the section(s) that contain errors. Sections which tested correctly will have green text indicating that the test for that section was successful.

---

### Copy a Profile

You can create a new Voicemail Profile by copying an existing profile, and changing the desired settings.

To create a new Voicemail Profile by copying an existing Voicemail Profile:

1. Select **Cisco Setup > Setup Profiles > Voicemail Profile**.

2. Click **Copy Profile** next to the profile to be copied.

   The **New Voicemail Profile** screen appears.

3. In the **Profile Name** field, rename the profile.

4. Change information in the other fields as appropriate.

5. Click **Save**.
Create a Corporate Directory Profile

In order to provide the Cisco CallConnect client Corporate Directory Lookup feature, the Avaya one-X Mobile Server must integrate with a Directory Source such as Cisco CallManager or Active Directory. This integration is known as a Corporate Directory Profile and may later be applied to a Class of Service which can be applied to a user group.

Depending on your network configuration either follow the instructions for Configuring an LDAP Corporate Directory Profile or if you are using Cisco CallManager 5.0 follow the instructions for Configuring an AXL Corporate Directory Profile.

To create a Corporate Directory Profile:

1. Select **Avaya Setup > Setup Profiles > Corporate Directory Profile**.

---

### Edit a Profile

To edit a Voicemail Profile:

1. Select **Cisco Setup > Setup Profiles > Voicemail Profile**.
2. Click **Edit Profile** next to the profile you want to edit.
3. Edit the appropriate fields.
4. Click **Save**.
2. Click **New Corporate Directory Profile**.

3. In the **Profile Name** field, choose a unique profile name which will identify this profile.

   **Note:**
   This is the name that is used when specifying a corporate directory profile for a Class of Service.

4. In the **Description** field, enter a description of this profile.

5. In the Profile Type drop-down menu, select **LDAP**.

6. In the **LDAP User DN** field, enter the LDAP user DN (for example, cn=Directory Manager, o=cisco.com, dc=example, dc=com).

7. In the **LDAP Hostname** field, enter the LDAP hostname.

8. In the **LDAP Port Number** field, enter the LDAP port number. The default value for Cisco CallManager DC Directory LDAP is 8404. If you are pointing the corporate directory search to Active Directory the default value for Active Directory is 389.

9. In the **LDAP Password** field, enter the LDAP password.
10. In the **Corporate Directory Search Base DN** field, enter the corporate directory search base DN (for example, ou=users, o=cisco.com). This is the default value for Cisco CallManager. The Avaya one-X Mobile Server will pull users under this root when searching the corporate directory.

11. Click **Show Advanced Settings** to view the LDAP Attributes section.

12. In the **Extension** field, enter the attribute name used to hold the extension. If the extension is not housed in the directory, it may be derived as part of the import process.

13. In the **10 Digit Phone Number** field, enter the attribute name for phone number.

14. In the **Handle or UserID** field, enter the attribute name user ID. This should be capitalized and will be the same as what was entered in the LDAP Attributes section of the **Provisioning Profile** tab in the **Setup Profile** section.

15. In the **First Name** field, enter the attribute name for the user’s first name.

16. In the **Last Name** field, enter the attribute name for the user’s last name.

17. In the **Email** field, enter the attribute name for the user’s email address.

18. In the **Department** field, enter the attribute name for the user’s department address.

19. Click **Save** to save the Corporate Directory Profile settings.
Copy a Profile

You can create a new Corporate Directory Profile by copying an existing profile, and changing the desired settings.

To create a new Corporate Directory Profile by copying an existing Corporate Directory Profile:


2. Click Copy Profile next to the profile to be copied.

   The New Corporate Directory Profile screen appears.

3. In the Profile Name field, rename the profile.

4. Change information in the other fields as appropriate.

5. Click Save.

Edit a Profile

To edit a Corporate Directory Profile:


2. Click Edit Profile next to the profile you want to edit.

3. Edit the appropriate fields.

4. Click Save.
Create a Class of Service

After completing the profiles, a Class of Service is required. Class of Service is a representation of ways in which an Avaya one-X Mobile user will interact with the system. Class of Service settings include profiles (as described earlier in this chapter) as well as non-aggregated settings.

**Note:**

A valid Provisioning Profile is required to create a Class of Service. An error message appears if there is an attempt to create a Class of Service using an invalid Provisioning Profile.

To create a new Class of Service:

1. Select **Cisco Setup > Setup Profiles > Class of Service**.
2. Click **New Class of Service**.

   The New Class of Service Profile section appears.

3. **Class of Service Name** field, enter the name for this class of service.
4. In the **Description** field, enter a description of this class of service.
5. In the **Provisioning Profile** drop-down box, select the appropriate profile.
6. In the **Voicemail Profile** drop-down box, select the appropriate profile.
7. In the **Corporate Directory Profile** drop-down box, select the appropriate profile.

8. In the **Security** section, do the following:
   a. Click the checkbox to **Allow voicemail to be stored on the mobile device**.
   b. Click the checkbox to **Require login each time one-X Mobile is launched on mobile device**, if required.
   c. Set the **Maximum number of attempts before user is locked out** (default is 5).
   d. Set the **Time period for which a user is locked out in minutes** (default is 90).
9. Click the checkbox to require the Cisco CallManager PIN reset upon reprovisioning.

<table>
<thead>
<tr>
<th>Dial Plan Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of phones to Send Calls to</td>
</tr>
<tr>
<td>PSTN Prefix</td>
</tr>
<tr>
<td>☑ Allow International dialing</td>
</tr>
<tr>
<td>☑ Translate 10-digit numbers to extensions</td>
</tr>
</tbody>
</table>

10. In the Dial Plan Settings section, do the following:
   a. Set the Maximum number of phones to Send Calls to.
   b. Set the PSTN Prefix (which is the number necessary to dial to reach an outside line).
   c. Click the checkbox to Allow International Dialing, if required.
   d. Click the checkbox to Translate 10-digit numbers to extensions, if required.

<table>
<thead>
<tr>
<th>Mobile Client Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Require client software upgrades</td>
</tr>
<tr>
<td>Number of days to warn users before making updates mandatory</td>
</tr>
<tr>
<td>RIM Blackberry Connection Settings</td>
</tr>
</tbody>
</table>

11. In the Mobile Client Settings section, do the following:
   a. Click the checkbox to Require client software upgrades, if required.
   b. Set the Number of days to warn users before making updates mandatory.
   c. Select the RIM Blackberry Connection Settings from the drop-down box.

<table>
<thead>
<tr>
<th>Forced Authorization Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ This organization uses Forced Authorization Codes (FACs)</td>
</tr>
</tbody>
</table>

12. Click the checkbox for This organization uses Forced Authorization Codes (FACs), if applicable.
Chapter 8: Cisco Setup

13. In the CMC Usage drop-down box, select the appropriate item.

![Server settings](image1)

14. In the **Server** section, do the following:
   a. Enter the **End user website server URL**.
   b. If this is a secure server, click the checkbox to set this as is a secure server.

15. To view the LDAP Attribute Source Profiles, click **Show Advanced Settings**.

   In the **LDAP Attribute Source Profiles** section, there is an opportunity to fine tune the Avaya one-X Mobile Server to use different directory sources for different data fields collected from directories. In some enterprise deployments, one directory may contain some information such as first name, last name; while another may contain information such as the 10-digit phone number.

   The Avaya one-X Mobile Server can map from one directory to another; where the sources are the Corporate Directory Profile and the Provisioning Profile. The Provisioning Profile will always be used for authentication and the Corporate Directory Profile may be used for name resolution. In all cases, the **Handle or UserID** must be the key between the two directory sources. That is, if mapping is done, the UserID in one directory must match that of the other directory.

   Use the drop-down boxes to tell the Avaya one-X Mobile Server from what directory to source the different attributes.

![LDAP Attribute Source Profiles](image2)

16. In the **Handle or UserID** drop-down box, select the appropriate profile.

17. In the **10 Digit Phone Number** drop-down box, select the appropriate profile.

18. In the **First Name** drop-down box, select the appropriate profile.
19. In the **Last Name** drop-down box, select the appropriate profile.
20. In the **Email** drop-down box, select the appropriate profile.
21. In the **Department** drop-down box, select the appropriate profile.
22. In the **Determine Extension from** drop-down box, select the appropriate source.

**Note:**
For the **Determine Extension from** drop-down box, extensions for users can be determined either directly from the LDAP attribute or manually from the 10-digit phone number. Manual determination can be done in one of two ways:
- automatically – determined automatically using dial plan rules
- algorithmically – by entering the number of leading digits to strip from the 10-digit phone number and/or adding prefixed after the digits have been stripped

23. In the **LDAP Extension Source** drop-down box, select the appropriate profile.

---

### Create CTI Ports

Different types of call handling settings require different CTI Ports usage schemes. The following table illustrates the number of CTI Ports used for a particular call handling setting.

<table>
<thead>
<tr>
<th>Call Handling Setting</th>
<th>CTI Ports Used Per Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Voicemail</td>
<td>0</td>
</tr>
<tr>
<td>Ring office</td>
<td>0</td>
</tr>
<tr>
<td>Ring office and PSTN phone</td>
<td>1</td>
</tr>
<tr>
<td>Ring PSTN phone</td>
<td>2</td>
</tr>
<tr>
<td>Ring two other PSTN phones</td>
<td>3</td>
</tr>
<tr>
<td>Ring three other PSTN phones</td>
<td>4</td>
</tr>
<tr>
<td>Ring four other PSTN phones</td>
<td>5</td>
</tr>
<tr>
<td>Ring five other PSTN phones</td>
<td>6</td>
</tr>
<tr>
<td>Ring four PSTN and office</td>
<td>5</td>
</tr>
<tr>
<td>Ring other office phone</td>
<td>2</td>
</tr>
</tbody>
</table>
Chapter 8: Cisco Setup

The Avaya one-X Server uses a pool of CTI Ports to make outbound calls. You should decide what scenarios from the above tables are the most commonly used and base the number of CTI ports you need to create on your expected user base usage patterns. Once you determine this, a busy hour calculation can help to determine the number of CTI Ports you need to create to support your enterprise.

For example, if you expect to support 30 simultaneous incoming calls for 30 managed users, you should create a minimum of 30 CTI Ports and a maximum of 90 depending on the expected user usage patterns. If most users are set to Office with Simulring on, then a number closer to 30 would be sufficient. If most users choose to ring their mobile phone and one other PSTN phone, then a number closer to 90 would be more appropriate.

⚠️ Important:
If the Avaya one-X Mobile Server runs out of CTI Ports, all subsequent calls will be routed directly to the desk as in the Office setting.

To create CTI Ports:

1. Select **Cisco Setup > CTI Resources > CTI Ports**.
2. Click **Create New Directory Range**.

   This screen allows you to specify the parameters for automated creation of CTI Ports for use by the Avaya one-X Mobile Server.

3. In the **Directory Number Ranges** fields, enter the range of CTI Ports to be added. Choose a range of numbers which does not conflict with any Route Patterns or Translation Patterns in the Cisco CallManager. Not doing so will lead to Interdigit timeouts.

4. In the **Partition** drop-down box, select a partition for the CTI Ports which has the following attributes:
   - It can be dialed from the Calling Search Space of the Transfer Route Point you created.
   - It can be dialed by the Calling Search Space of the managed phones.

5. In the **Calling Search Space** drop-down box, select the Cisco CallManager Calling Search Space associated with the partition. The Calling Search Space for the CTI Ports should have the following attributes:
   - It should include at the top of the Calling Search Space, the partition you created for the Interceptor CTI Route Point.
   - It should include a partition which has access to the Route Pattern which routes calls to the PSTN. Typically, this is a 9 @ Route Pattern.
   - It should include the partition that contains the Transfer Route Point.

1. In the **Device Pool** drop-down box, identify the Device Pool associated with the CTI Ports.
2. Click **Create CTI Ports**.
Import Route Points

Before proceeding with the Import Route Points task, be sure the following tasks have been performed:

- At least one Transfer CTI Route Point and one or more Interceptor Route Points have been configured within Cisco CallManager. These tasks should have been performed prior to configuring the Avaya one-X Mobile Server. If they have not, you must perform them before proceeding.
- You must configure the Cisco CallManager Settings in order for the correct information to appear in the Import Route Points screen. If the Cisco CallManager Settings have not yet been configured, you must do so before proceeding. See Configure Cisco CallManager Settings on page 59 for more information.

To import route points:

1. Select Cisco Setup > Setup RoutePoints > Import RoutePoints.

   ![Import Route Points Screen]

   The Import Route Points screen provides a list of all CTI Route Points configured within Cisco CallManager.

2. Click the checkbox for the CTI Route Point(s) on the list that you established as the Interceptor Route Points and Transfer Route Points in “Creating CTI Route Points for Intercepting Calls” in the Avaya one-X Mobile Integration Guide, document number 18-602153. Interceptor Route Points are used to intercept calls for users and apply the call handling settings of the user to the call.

3. Click Add to one-X Server Database to save the settings in the Avaya one-X Mobile Server.
Manage Route Points

Once Route Points are imported, you can edit a Transfer CTI Route Point or Interceptor Route Point. You can also delete them from the Avaya one-X Mobile Server database.

1. Select Cisco Setup > Setup Route Points > Manage Route Points.

2. In the Default Transfer Route Point drop-down box, choose a route point. This is the route point that will be used as the Transfer Route Point in the event that there is no Transfer Route Point to match the particular CSS of a given user.

3. For each imported route point, denote the Route Point Type as either a Transfer Route Point (used to change CID and manage calling permissions) or Interceptor Route Point (used to intercept incoming calls).

⚠️ Important:
In order for call handling services to work correctly, you must specify at least one Transfer Route Point and at least one Interceptor Route Point.
Chapter 8: Cisco Setup

Administer Users

This section describes how to provision users for whom the Avaya one-X Mobile Server services will be available. This section describes how to:

- Import Users
- Manage Unlicensed Users
- Manage Licensed Users

Import Users

To import users:

1. Select Cisco Setup > Users > Import Users.

The first time you navigate to the Import Users page, the list of users will be empty (as shown above).

2. Click Import Users to import the users from the CallManager LDAP (or Active Directory if the integration has been performed) into the Avaya one-X Mobile Server database.

Note:

For very large user populations, this can take some time.

Users which appear in the Manage Users list are retrieved from the Cisco CallManager LDAP Directory (or Active Directory, if the integration has been performed). To search for all users use “cn=*”.

When a large number of results are returned, you can use the alphabetical bar to navigate to a particular section of users beginning with that letter. The sort attribute is whatever attribute you are currently sorting on (that is, First, Last, Extension, or Department).
Manage Unlicensed Users

To view all imported user accounts that are not yet licensed:

1. Select **Cisco Setup > Users > Unlicensed User Management**.

2. To search for specific users, enter text in the **Search** field.

3. To search for all users, leave the **Search** text box blank and press **Enter** or click **Show All**, if it is available.

4. To navigate to a particular section of users when a large number of results are returned, use the **Sort by** drop-down box.

Change Class of Service

Once users have been imported, they are all configured with the **Default** Class of Service. To change the Class of Service of a user group:

1. On the Unlicensed User Management screen, click the checkbox for the users for whom you want to change the Class of Service.

2. Click **Change Class of Service**.

3. In the **Choose a Class of Service** drop-down box, choose a Class of Service.

4. Click **Save**.

The new Class of Service will be applied to all the selected users.
Chapter 8: Cisco Setup

License Selected Users

To license a user, click the checkbox next to that user’s name and click License Selected Users.

This will license the user in the Avaya one-X Mobile Server database and decrement the number of licenses available for assignment.

A message appears letting you know that it is importing users in a background process. Licensing users can take some time depending on the size of your user base. When users are licensed, the Avaya one-X Mobile Server works in the background to retrieve required provisioning information for the user. When complete, you will be able to locate the new users in the Licensed User Management tab.

⚠️ Important:

The Avaya one-X Mobile Server associates a user’s device with the JTAPI user specified in the Setup screen. If you are licensing more than 1500 users, you must do this through the Cisco CallManager Administration User Interface as there are limitations on the size of AXL queries. Follow the same procedure as provided in section 6.3, “Associating the JTAPI User with the Interceptor Route Points,” of the Cisco CallManager Integration Guide. The only difference is that you will be associating the remaining CallConnect user devices with the JTAPI user instead of the CTI Route Points.
Manage Licensed Users

To view all imported user accounts that are licensed:

1. Select **Cisco Setup > Users > Licensed User Management**.

2. To search for a user, in the **Search** field enter the user’s last name, first name, extension, Class of Service, or department.

3. To change the page displayed, in the **Show** drop-down box, select the appropriate page.

4. To change the way the information is sorted on the page, in the **Sort by** drop-down box, make the appropriate selection.

To manage licensed users, the following features are available:

- Change Class of Service
- Reprovision Selected Users
- Unlicense Selected Users
- Delete Selected Users

**Change Class of Service**

To change the Class of Service for a user or group of users:

1. On the **Licensed User Management** screen, click the checkbox next to each user for whom you want to change the Class of Service.
2. Click **Change Class of Service**.

3. In the **Class of Service** drop-down box, select the new class of service.

4. Click **Yes**.

**Reprovision Selected Users**

You may need to reprovision users when:
- You are changing Voicemail Pilot numbers and it affects these users.
- You are changing Microsoft Exchange Server hostnames or IP addresses and it affects these users.
- You are changing Microsoft Exchange Server aliases used by Cisco Unity.

To reprovision users or a group of users:

1. On the **Licensed User Management** screen, click the checkbox next to each user or user group that you want to reprovision.

2. Click **Reprovision Selected Users**.

   The Avaya one-X Mobile Server retrieves the new user information and updates the Avaya one-X Mobile Server database.

**Unlicense Selected Users**

Unlicensed users are not able to log in to their Avaya one-X Mobile account from either the Avaya one-X Mobile Web site or their mobile device.

To unlicense a user:

1. On the **Licensed User Management** screen, click the checkbox next to the user you want to unlicense.
2. Click **Unlicense Selected Users**.
   This will increment the number of licenses available for assignment.

⚠️ **Important:**
When you remove a license from a user, remember to move the user back into a Partition which is not managed by the Avaya one-X Mobile Server. This will prevent the Avaya one-X Mobile Server from managing the call.

### Delete Users

Deleting a user will delete all the call logs and any other data associated with that user in the Avaya one-X Mobile database. The user will not be able to login to their Avaya one-X Mobile account from either the Avaya one-X Mobile Web site or their mobile device.

To delete a user:

1. On the **Licensed User Management** screen, click the checkbox next to the user(s) you want to delete.
2. Click **Delete Selected Users**.
   This will decrement the number of used licenses and remove the user from the Avaya one-X Mobile Server database. It will **not** remove the user from the LDAP directory.

### View User Details

Click on **Details** next to any user on the **Licensed User Management** or **Unlicensed User Management** screens to display more information about that user.

![User Details](image)
Chapter 8: Cisco Setup

From the User Details screen you can:

- Reprovision a user
- Delete a user
- Take action on a user’s account if the user has lost their mobile phone
- Take action on a user’s account if the user is no longer an employee
- Unlock a locked user account

**Lost or Stolen Mobile Phone**

If a user’s mobile phone has been lost or stolen, click on **Lost or Stolen Mobile** on the User Details screen. This screen will provide instructions for further steps you should take. This may include resetting the user’s password and loss of local data on their mobile phone.

**No Longer an Employee**

If a user is no longer an employee, click on **No Longer an Employee** on the User Details screen. This screen will provide further instructions depending on whether the user account needs to be retained or completely removed from the Avaya one-X Mobile Database.

**Unlock one-X Mobile Account**

A user account may get locked out by the Avaya one-X Mobile Server if the user enters an incorrect login too many times. This will prevent a user from logging into the Avaya one-X Mobile application on both their mobile phone and the Avaya one-X Mobile Web site. A user account that is locked will automatically be unlocked after the lockout time (as set in the Class of Service for the user) has expired.

If a user account needs to be unlocked before the lockout time expires, click on **Unlock one-X Mobile Account** on the User Details screen. This will unlock the user account, and access to the Avaya one-X Mobile Web site and the Avaya one-X Mobile application on their mobile phone will be allowed.

**Note:**

This does not unlock a user’s voicemail mailbox.