Avaya one-X™ Mobile Integration Guide

18-602153
Issue 1
November 2007

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.

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: Introduction

The *Avaya one-X™ Mobile Integration Guide* provides the procedures required to properly integrate the Avaya one-X Mobile server with existing equipment in a corporate IP voice network.

This document explains how to configure the equipment that the Avaya one-X Mobile Server integrates with. To provision the server itself, refer to the:

- *Avaya one-X™ Mobile Installation Guide*, document number 18-602135
- *Avaya one-X™ Mobile Administration and Maintenance Guide*, document number 18-602144

Audience

This book is written for the people who are installing the Avaya one-X Mobile Server into a corporate IP voice network. You need administrator or root permissions to accomplish most (or all) of the tasks in this book.

Acronyms Used

Acronym	Definition
ACM	Avaya Communication Manager
AES	Application Enablement Services
EC500	Extension to Cellular
SAT	Site Administration Tool

What you need to know

To successfully integrate the Avaya one-X Mobile Server into your network, you need to know:

- the details of your IP network
- how to configure your call management switch (either Avaya Communication Manager or Cisco CallManager)
- how to configure Avaya AES
- how to configure your messaging platform.

Related Documents

You can find Avaya documents on the Avaya support web site: http://support.avaya.com

Avaya one-X Mobile Documentation

This book is part of a set of documents about Avaya one-X Mobile. The rest of the documents in the set are listed below.

Title	Document Number
Avaya one-X™ Mobile Site Survey	18-602143
Avaya one-X™ Mobile Pre-Installation Checklist	18-602133
Avaya one-X™ Mobile Getting Started	18-602134
Avaya one-X™ Mobile Installation Guide	18-602135
Avaya one-X™ Mobile System Acceptance/Signoff	18-602433
Avaya one-X™ Mobile Integration Guide	18-602153
Avaya one-X™ Mobile Administration and Maintenance Guide	18-602144
Avaya one-X™ Mobile User Guide for J2ME	18-602147
Avaya one-X™ Mobile User Guide for RIM Blackberry	18-602148
	1 of 2

Title	Document Number
Avaya one-X™ Mobile User Guide for Palm Treo	18-602149
Avaya one-X™ Mobile Web User Guide	18-602150
	2 of 2

Other Product Documentation

The documents listed below may help in completing the tasks in this book

Title	Document Number
Avaya Communication Manager Documentation	
Avaya Application Enablement Services Documentation	
Avaya MultiVantage® Application Enablement Services TR/87 Implementation Guide	02-601893

Avaya MultiVantage® Application Enablement Services TR/87 Implementation Guide, document number 02-601893, especially the Dial Plan section (Chapter 2). http://support.avaya.com/elmodocs2/AES/4.0/02_601893_1_1.pdf

You should also refer to the manuals for other vendor's equipment that may be installed in your network.

Chapter 2: Overview

This section briefly describes Avaya one-X Mobile and how it is used in your network. More detailed information regarding how to install the Avaya one-X Mobile Server in your network can be found in the *Avaya one-X Mobile Installation Guide*, document number 18-602135.

Avaya one-X Mobile Overview

Avaya one-X Mobile is software and hardware that offers enterprise voice, messaging, voicemail, and corporate directory integration on mobile devices (cell phones and PDAs). Avaya one-X Mobile allows the corporate voice network to be invisibly and seamlessly extended to employees' mobile phones. Features include:

- Managing call routing of corporate PBX extensions directly to other locations, such as a mobile phone.
- Routing calls based on an individual caller using special routing rules (for example, allow a spouse to reach an employee's mobile phone, while all other calls redirect to voicemail).
- Access and receive corporate voice mail.
- View and manage personal phone book and corporate directory.
- Administration portal for administering and provisioning users.
- Web interface for user configuration and changing settings.

Implementation Overview

When installing Avaya one-X Mobile, you can locate the Avaya one-X Mobile server in several areas of your network:

- Inside the network (behind the firewall)
- Outside the firewall, in the network DMZ
- Inside the network, using a reverse proxy server in the DMZ
- Placing multiple Avaya one-X Mobile Servers, one behind the network firewall, and others in the DMZ.

Supported Equipment

The table below lists the equipment that may be in your network. It is unlikely that you would have equipment from different vendors performing the same function in your network.

Function	Avaya Equipment	Cisco Equipment	Other Vendor's Equipment
Call Management	Communication Manager	CallManager	
Voicemail	Modular Messaging	Unity (via MS Exchange)	MS Exchange Server
IP Phones	Supported Avaya IP Phones	Cisco IP Phones	
Corporate Directory	CM	AXL	Active Directory
MS Exchange			
Other	Application Enablement Services (AES)		

Integration Task Overview

This section describes the integration tasks for a network containing Avaya equipment, in the order these tasks should be performed. Detailed descriptions of how to perform these tasks are provided in subsequent sections.

For integration with Cisco equipment, see Appendix B.

Before You Begin

You should have the equipment and software listed in the following sections installed on your network before performing any integration with Avaya one-X Mobile.

You should also have all the relevant documentation for this equipment on hand for reference.

The following equipment and software should be installed:

- Avaya AES server
  - SE Linux must be disabled
  - AES license must be installed
- Avaya Communication Manager (version 3.1) installed in the network
- Modular Messaging (optional)

Integration Task Flow

To integrate Avaya one-X Mobile, perform these tasks in the following order:

1. Configure Avaya Communication Manager
   a. Validate the Licensed Features
   b. Configure CTI Links on Avaya Communication Manager
   c. Configure IP Services
   d. Configure EC500
   e. Configure SAT Access
   f. Configure VDNs
2. Configure AES
   a. Validate Licensing
   b. Create a JTAPI user
   c. Create a DMCC User
   d. Network Configuration of AES
   e. Configure Switch Connections in AES
   f. Enable Unrestricted Access
   g. Configure TSAPI
   h. Create TSAPI Links
   i. Validate TSAPI Links
   j. jTR87 Configuration
   k. SMS Configuration
3. Configure Voicemail Platforms
   a. Configure Modular Messaging 3.1 with MSS
   b. Configure Modular Messaging 3.0 with MSS

c. Configure Modular Messaging 3.1 with Exchange

Chapter 3: Configure Avaya Communication Manager

Avaya one-X Mobile uses Avaya Communication Manager to:

- Route inbound calls to match the call handling settings selected by the user in Avaya one-X Mobile.
- Place calls on behalf of the user while they are away from the office.
- Monitor inbound and outbound call activity by the user so it can be displayed in a call log for access by Avaya one-X Mobile.

The configuration includes setup of CTI links, IP Services, and EC500. The following sections describe the required steps in detail.

Validate Licensed Features

It is important to validate the licensed features on Avaya Communication Manager before attempting to configure.

Validate the following licenses exist:

- FEAT_ADJLK
- FEAT_BSCVEC
- FEAT_PRTVEC
- FEA_RCNAA_CFF
- REGISTRATION IP_API_A*
- FEAT_EC500
- FEAT_XCOV_ADMIN
- VALUE_OPT_EC500

It is necessary to use the Site Administration Tool (SAT) to perform the following validations:

1. Perform a display **system-parameters special-applications** command.
2. Select the fourth tab.
3. Look for the feature named **(SA8481) – Replace Calling Party Number with ASAI ANI.**
4. Ensure that this is set to **y**.

Contact your Avaya Business Partner if you do not have the proper features licensed.

Configure CTI Links in Avaya Communication Manager

In preparation for this section, a number from the dial plan is required. Complete the following commands in the SAT to configure a CTI Link in Avaya Communication Manager:

1. Enter the command **`add cti-link <n>`** where **n** is the CTI Link number. If you need to identify a free CTI link, perform the command **`list cti-link`** to identify a free number.
2. Adding the CTI Link will bring up two tabs. On the first tab, change the **Extension** to an unused extension in the dial plan.
3. Change the Type to **ADJ-IP**.
4. Give the link a **Name.**
5. Change the Class of Restriction to one that allows the type of dialing you allow your users from their desks. This can be changed depending on company requirements.
6. On tab 2, the default configuration is to set all flags to **n**.
7. Press **F3** to save.
8. To validate, enter **`list cti-link`**. Validate that the CTI Link you created is in the list.

Configure IP Services

IP Services must be configured to link the switch to an AES switch connection. The following commands must be performed in the SAT.

1. Enter the command **`change ip-services.`**
2. On the first tab, for the **Service Type**, select **AESVCS** from the drop-down box.
3. Set **Enabled** to **y**.
4. Enter the **Local Node**.
5. Set the **Local Port** to 8765.
6. Go to tab 3.
7. Enter a Server ID for the AES being used.

Note:
The Server ID must match the hostname found in the /etc/hosts file on the AES server.

8. Enter a password and set **Enabled** to **y**.

Note:
The password is required when configuring the AES later.

Configure EC500

The Extension to Cellular feature is used as part of Avaya one-X Mobile. It is necessary to configure EC500 for all Avaya one-X Mobile users before provisioning them for the product.

This guide provides a very cursory introduction to configuring EC500. Complete documentation on EC500 is found in *Feature Description and Implementation for Avaya Communication Manager.*

Configure Feature Access Codes

Feature Access Codes (FACs) are used to effect features of the EC500 product during Avaya one-X Mobile call flows. It may be helpful to note them down as they will be required for administration of the Avaya one-X Mobile Server.

To setup the required FACs using the SAT:

1. Enter the command **`change feature-access-codes`**.
2. Enter FACs on page 2 (if they do not already exist) for the following:
   a. EC500 Self Administration _____
   b. Enhanced EC500 Activation_____
   c. Enhanced EC500 Deactivation _____
3. Enter FACs on page 3 (if they do not already exist) for the following:
   a. Send All Calls Activation _____
   b. Send All Calls Deactivation _____
4. Press **Enter** or **F3** to save.

Create a Configuration Set

The following steps are necessary to allow EC500 to detect cellular voicemail correctly.

1. Enter **`change xmobile configuration-set <n>`** where **n** is a new configuration set if one is not predefined.

2. Press **Enter**.
3. Give the configuration set a name to identify which mobile carrier it is associated with.
4. Change the Cellular Voicemail Detection as required. This information is typically published by cellular carriers. Typically a number of no less than 2 seconds is adequate. A large number here will make it difficult for users to accept calls in good networks.
5. Press **Enter** or **F3** to save.

Configure EC500 for Avaya one-X Mobile Users

EC500 must be configured for all Avaya one-X Mobile users. For *each* Avaya one-X Mobile user, perform the following:

1. Enter the command **`change off-pbx-telephone station-mapping <station extension>`**.
2. Press **Enter.**
3. In tab 1, enter the station extension of the user.
4. Enter the application as **EC500**.
5. Leave the **Dial Prefix** empty.
6. Leave the **Phone Number** empty if the mobile number is not known. The Avaya one-X Mobile Server will provision this automatically when the user logs in to setup their account for the first time.
7. Set Trunk selection as **ars.**
8. Enter the configuration set configured in Create a Configuration Set on page 17.
9. Press **Enter** or **F3** to save.

Note:

For situations involving a bridged appearance, it may be helpful to set the **Bridged Calls** setting on tab 2 to **none** when the primary owner of the device does not want bridged call appearances to extend to their mobile phone.

For situations when the same mobile phone is used in an enterprise, it may be helpful to set the **Mapping Mode** to **termination** on page 2.

Since Avaya one-X Mobile uses EC500 in it's call flows, it is recommended that EC500 buttons be removed from stations used by Avaya one-X Mobile.

Configure SAT Access

The Avaya one-X Mobile Server requires SAT access in order to provision CTI resources such as CTI Ports and VDNs. For Avaya Communication Manager, SSH port 5022 and Telnet port 5023 need to be enabled.

Perform the following steps to allow access:

1. Log on to the Avaya Communication Manager web page.
2. Go to **Maintenance**.
3. Go to **Security/Server Access**.
4. Make sure SAT (SSH 5022) is enabled for both **Service State** and **Corporate LAN Firewall**.
5. Make sure SAT (Telnet 5023) is enabled for both **Service State** and **Corporate LAN Firewall**.

Configure DTMF Functionality

Avaya one-X Mobile uses VDNs to collect DTMF digits to confirm answer by a user rather than a cellular voicemail provider. The application manages a pool of VDN triplets. Each triplet consists of two VDNs and one CTI Port.

The first VDN has a vector program attached to it that does the following:

1. Waits for one second
2. Collects a digit after playing an announcement
3. Routes to the Second VDN

The second VDN is monitored by the application and is used to retrieve the actual digit entered. The second VDN is attached to a vector that waits for 0 seconds and then routes to the CTI Port. The CTI Port is used to keep the call up.

To configure DTMF functionality for Avaya one-X Mobile:

1. Create announcements.
2. Configure VDNs and Vectors.
3. Create directory ranges for the VDNs created in step 2.

Create Announcements

In this step, create an announcement that is similar to this one:

"Please press 5 to connect your call"

<pause 5 seconds>

"Please press 5 to connect your call"

<pause 5 seconds>

"Please press 5 to connect your call"

Note:
Use a phone with Class of Service permissions to perform this task.

For instructions about how to create and record announcements using Avaya Communication Manager, refer to the Avaya Communication Manager Online Help or the *Administrator's Guide for Avaya Communication Manager Software* for more information.

Ensure that the CM is configured so that the

- Announcement Queue field is set to **Y**
- System-Parameters Customer Options - Call Center Features - Vectoring (ANI/II-Digits Routing) is set to **Y**
- DTMF licenses are installed

Configure Vectors and VDNs

You need to create a vector directory number (VDN) triplet. A VDN triplet consists of two VDNs and one CTI port. The VDN triplet is used to provide DTMF acceptance on a callback. This avoids the call getting sent to cellular voicemail. DTMF gives positive acknowledgement that a human answered the phone. VDN triplets are created using the Avaya one-X Mobile Administration **Avaya Setup > CTI Resources > VDNs** screen. See the *Avaya one-X™ Mobile Administration and Maintenance Guide*, document number 18-602144, for more information.

Determine Triplet Quantity

One triplet is needed to service a callback. They are managed in a pool. The number of VDN triplets is determined by the quantity of callbacks expected during your busy hour. If you run out of VDN triplets, the call is placed, but no DMTF information is collected. The second leg of the call is placed immediately.

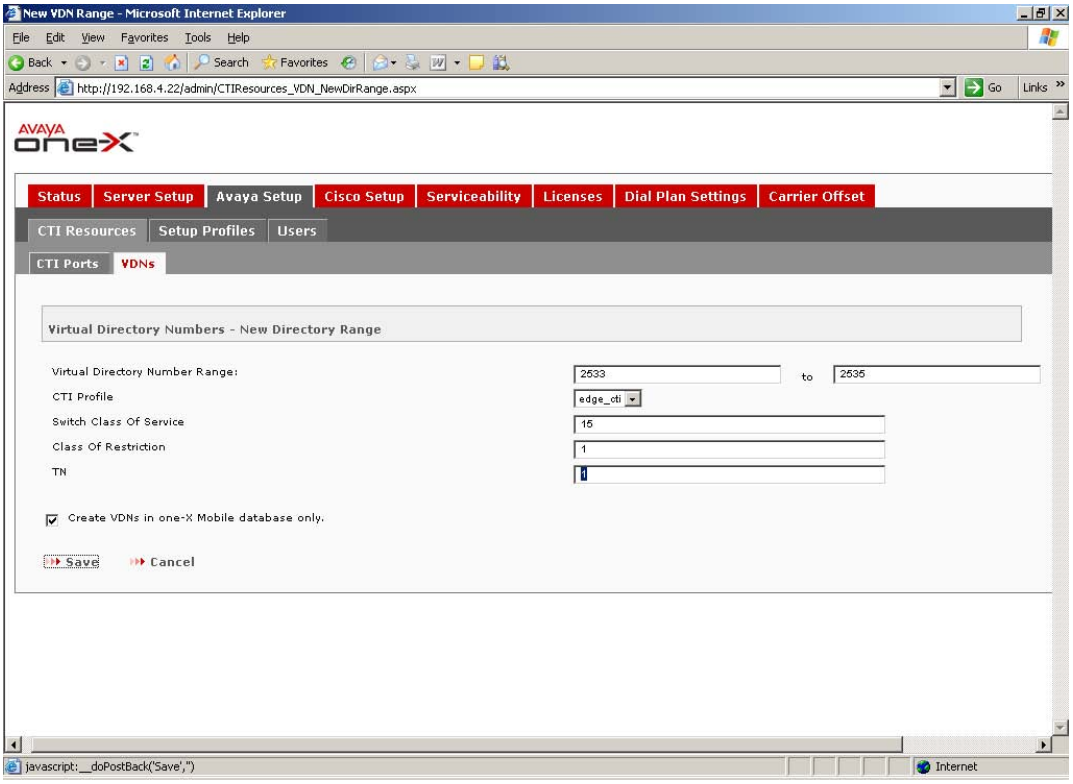
Configure VDN Triplets

After the VDNs are created, provision the switch. For each triplet:

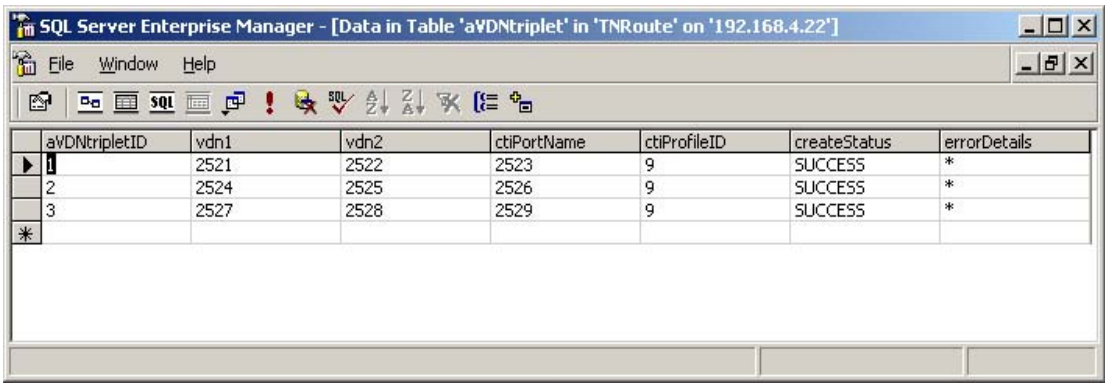
1. Create a vector number for the first VDN.
2. Assign that vector number to the first VDN
3. Enter **`change vector x`** on the command line.
4. Change the steps of the vector to be:
   a. Wait 1 second
   b. Collect 1 digit after announcement *1234* (where 1234 is an announcement created by the administrator which says something like “please press any key to connect your call”)
   c. Route-to VDN2
5. Create a vector number for the second VDN.
6. Assign that vector number to the first VDN.
7. Enter **`change vector y`**.
8. Change the steps of the second vector to be:
   a. Wait 0 seconds
   b. Route-to CTIPort (the one that is part of the triplet).

Create Directory Ranges for VDNs

This is performed using the Avaya one-X Mobile Server Administration web interface. VDN triplets must be populated in the local Avaya one-X Mobile database.



1. Open the database table **aVDNtriplet** in the **TNRoute** database.
2. Change the value of **errorDetails** (did not create) to *(asterisk) for all rows.



aVDNtripletID	vdn1	vdn2	ctiPortName	ctiProfileID	createStatus	errorDetails
1	2521	2522	2523	9	SUCCESS	*
2	2524	2525	2526	9	SUCCESS	*
3	2527	2528	2529	9	SUCCESS	*

Chapter 4: Configure Application Enablement Services

The Avaya one-X Mobile Server uses Application Enablement Services (AES) to communicate with Avaya Communication Manager via JTAPI.

Note:
This guide provides a cursory set of steps for configuring AES. Refer to the complete AES documentation for installation instructions.

The following sections outline the steps to configure AES to interact with the Avaya one-X Mobile Server.

Validate Licensing

Validate that the proper licensing is available on the AES:

1. Go to the AES URL **http://<AESHOST>/WebLM**
2. Enter the credentials.
3. Validate that the following licenses exist:
   - VALUE_CVLAN_VERSION
   - VALUE_AEC_CONNECTIONS
   - VALUE_TSAPI_VERSION
   - VALUE_AEC_VERSION
   - VALUE_NOTES
   - VALUE_TSAPI_USERS

Create a JTAPI User

In the User Administration portion of the AES, it is necessary to create a user that the Avaya one-X Mobile Server can use to communicate with the AES. Perform the following steps:

1. Login to AES **User Management**.

Note:
This is a separate login from CTI OAM.

2. Navigate to **User Management > Add User**.
3. Create a new User ID.
4. Fill in the required fields.
5. Set the CT User field to **yes**.
6. Click **Apply**.
7. If desired, note the User and Password in Appendix A: Administrator's Worksheet on page 37 for future reference.

Create a DMCC User

In the User Administration portion of the AES, it is necessary to create a user that the Avaya one-X Mobile Server can use to communicate with DMCC. Perform the following steps:

1. Login to AES **`User Management`**

Note:
This is a separate login from CTI OAM.

2. Navigate to **User Management > Add User**.
3. Create a new User ID.
4. Fill in the required fields.
5. Set the CT User field to **yes**.
6. Click **Apply**.
7. If desired, note the User and Password in Appendix A: Administrator's Worksheet on page 37 for future reference.

Network Configuration of AES

Inside the CTI OAM Administration, perform the following steps:

1. Login to AES CTI OAM.

Note:
This is a non-root Linux user login.

2. Go to the **Administration > Network Configuration > Local IP** page.

3. Ensure all the interfaces are set to the correct network interfaces. Otherwise, the Avaya one-X Mobile Server will not be able to contact the AES.

Configure Switch Connections in AES

Perform these steps to configure switch connections in AES:

1. Navigate to **Administration > Switch Connections**.
2. Click **Add Connection**.
3. Set the **Switch Connection Type** to **CTI/Call Information** in the drop-down box.
4. Set the **Switch Password** to what you configured in the switch in Configuring IP Services in Chapter 3.
5. Click **Apply**.
6. The newly created connection should show in the list of connections.
7. Click on **Edit CLAN IPs**.
8. Enter the IP Address of the Avaya Communication Manager you configured and click on **Add Name or IP**.
9. Save the changes.

Enable Unrestricted Access

This configuration must be done in the CTI OAM.

1. Navigate to **Administration > Security Database > CTI Users > List All Users**.
2. Select the user you created in Create a JTAPI User on page 23 and click **Edit**.
3. Make sure that **Unrestricted Access** is enabled. The default is for it to be disabled.

TSAPI Configuration

This configuration must be done in the CTI OAM.

1. Navigate to **Administration > TSAPI Configuration**.
2. Ensure that **Enable SDB** is checked.

3. Apply the changes.

Create TSAPI Links

This configuration must be done in the CTI OAM.

1. Navigate to **Administration > CTI Link Admin > TSAPI Links**.
2. Click the **Add Link** button.
3. For the link drop-down box, select a link number for AES.
4. For the switch connection drop-down box, select the name of the switch that you configured in Configure Switch Connections in AES on page 25.
5. For the **Switch CTI Link Number**, set the CTI Link Number to the cti-link you configured in Configure CTI Links in Avaya Communication Manager on page 16.
6. Click **Apply Changes**.

Validate TSAPI Links

This configuration must be done in the CTI OAM.

1. Navigate to **Administration > Security Database**.
2. Click on **Tlinks**.
3. You should see the following Tlink:
   AVAYA#<switch connection Name>#CSTA#<Hostname>

Validate the ASAI Link

Perform these steps to validate the ASAI Link:

1. Navigate to **Utilities > ASAI Test**.
2. Select the TSAPI link you configured in Validate TSAPI Links on page 26.
3. Click **Test**.
4. If the test is successful, text should display **Heartbeat with switch for TSAPI link 01 was successful**.

TSAPI Test

Perform these steps to test the TSAPI Link:

1. Navigate to **Utilities > TSAPI Test**.
2. Select the Tlink created in Create TSAPI Links on page 26.
3. Enter the JTAPI User created in Create a JTAPI User on page 23.
4. Enter the JTAPI User password.
5. Enter an extension in the **from** field.
6. Enter an extension in the **to** field.
7. Click the **Dial** button.
8. If the test is successful, the phone should dial from one extension to the other.

TR-87 Configuration

The TR-87 configuration on AES must be performed to administer dial plan information so that that Avaya one-X Mobile Server can access it.

This document provides a cursory description of TR-87 configuration. For full details, refer to http://support.avaya.com/elmodocs2/AES/4.0/02_601893_1_1.pdf

Configure the DMCC Port

Perform these steps to configure the DMCC port:

1. Navigate to **Administration > Network Configuration > Ports**.
2. Make sure the unencrypted port 4721 is enabled in the **DMCC Server Ports** section.
3. Do not enable the TR/87 port.

Create Dial Plan Rules for the Switch

Dial plan rules must be configured in AES so that Avaya one-X Mobile can determine if numbers are on-switch or off-switch.

1. Navigate to **Administration > TR87 Configuration > Dial Plan > Switch Administration**.

2. Click on **Detail** for the switch you are administering.
3. In the **From TelURI** section, enter conversion rules for the switch that map from E.164 numbers to extensions that are on-switch.

Refer to the full AES documentation for notes on how to administer the dial plan and order the conversion rules.

SMS Configuration

The Avaya one-X Mobile Server needs to access the SMS interface in order to administer the product.

Perform the following steps on the AES:

1. Log in to AES as *root*.
2. Edit **syslog.conf** using the following command:

   `vi /etc/syslog.conf`
3. Add the following line to the end of the file:

   `local1.*   /var/log/ossicm.log`
4. Save and exit.
5. Search for any **syslogd** processes that may be running:

   `ps -ef | grep syslogd`
6. Terminate any **syslogd** processes found in the previous step:

   `kill -SIGHUP <syslogd-PID>`
   if this command does not work, use
   `kill-9`
7. Edit **saw.ini**:

   `vi /opt/mvap/web/sms/saw.ini`
8. Add the switches **-T -V** to **Proxy options**. The resulting line appears:

   `ProxyOptions=-n -T -V`
9. Set CMPort to 5023:

   `CMPort=5023`
10. Save and exit.
11. Search for any ossi processes that may be running:

    `ps -ef | grep ossi`

12. Terminate any ossi processes found in the previous step:

    `kill <ossicm-PID>`

    A reboot is not necessary for this step.

Install the occsim Binary Patch

You need to install this patch *only* if the Avaya Communication Manager version is not 4.x. If Avaya Communication Manager is a version other than 4.x, perform the steps below.

AES 3.X

For AES 3.x, verify the telnet option is turned on.

1. Open **/opt/mvap/web/sms/saw.ini**.
2. Under **ACP**, check to see if **ProxyOption=-T** and **CMPort= 5023**.
3. If the settings are not as described in step 2, edit the file.

AES 4.0 and AES 4.0.x

For AES 4.0 and AES 4.0.x, follow these steps:

1. Download the AES 4.1 rpm file from **http://www.avaya.com/support**.
2. Save to any directory.
3. Run **`swversion`** to see what the **Offer Type** is:
   a. If the offer type is **SWONLY**, run **`su root`**.
   b. If the offer type **TURNKEY**, run **`su sroot`**.
4. Run **`ps -ef | grep ossi`**.
5. Run **`kill <pid>`**.
6. Back up **/opt/mvap/web/sms/saw.ini**.
7. Run **`rpm -U --force mvap-sms-4.0.651-1.noarch.rpm`**.

If the commands do not run properly and you need to restore the **saw.ini** file, follow these steps:

1. Run **`swversion`** to see what the **Offer Type** is:
   a. If the offer type is **SWONLY**, run **`su root`**.
   b. If the offer type **TURNKEY**, run **`su sroot`**.
2. Run **`rpm -e mvap-sms`**.
3. For **SWONLY**, run **`rpm -ivh /var/disk/rpms/mvap-sms-4.<release>.rpm`**.

4. For **TURNKEY**, run **`rpm -ivh /var/disk/software/MVAP/rpms/mvap-sms-4.<release>.rpm`**
5. Run **`ps -ef | grep ossi`**.
6. Run **`kill <pid>`**.
7. Restore the old **saw.ini** file to **/opt/mvap/web/sms/saw.ini**.

Chapter 5: Configure Integration with Modular Messaging

This section describes how to prepare Modular Messaging for integration with the Avaya one-X Mobile Server.

Configure Modular Messaging 3.1 with MSS

This section describes how to configure Modular Messaging 3.1 with MSS.

Perform the following steps to configure the trusted server in the Modular Messaging Administration:

1. Log onto the MSS webpage.
2. Click **TrustedServer Management**.
3. Click the **Add a New Trusted Server** button.
4. Type in the superuser in the **Trusted Server Name** field.

   Note:
   This name is needed in the Avaya one-X Mobile Server configuration. Add it to the worksheet in Appendix A: Administrator's Worksheet on page 37.
5. Type in the superuser's password in the **Password** and **Confirm Password** fields.

   Note:
   This name is needed in the Avaya one-X Mobile Server configuration. Add it to the worksheet in Appendix A: Administrator's Worksheet on page 37.
6. Type in the IP address of the Edge server in the **IP Address** field.
7. Set **Service Name** to edge.
8. Set **Connection Security** to **No encryption required**.
9. Click **Save**.

Configure Modular Messaging 3.0 with MSS

This section describes how to configure Modular Messaging 3.0 with MSS.

Configure the Trusted Server

Perform the following steps to configure the trusted server in the Modular Messaging Administration:

1. Log onto the MSS web page.
2. Click **Global Administrator** (for MM 3.0 only).
3. Click **TrustedServer Management**.
4. Click the **Add a New Trusted Server** button.
5. Type in the superuser in the **Trusted Server Name** field.

   Note:
   This name is needed in the Avaya one-X Mobile Server configuration. Add it to the worksheet in Appendix A: Administrator's Worksheet on page 37.
6. Type in the superuser's password in the **Password** and **Confirm Password** fields.

   Note:
   This name is needed in the Avaya one-X Mobile Server configuration. Add it to the worksheet in Appendix A: Administrator's Worksheet on page 37.
7. Type in the IP address of the Edge server in the **IP Address** field.
8. Set **Service Name** to **edge**.
9. Set **Connection Security** to **No encryption required**.
10. Click **Save**.

Enable Superuser Mode

If Modular Messaging 3.0 is used, the Superuser mode needs to be manually turned on in the MSS.

To turn on the Superuser mode on MSS:

1. Log in to the MSS using SSH.
2. Provide the **tsc** password.
3. At the command prompt, type **sroot**.

4. Provide the **sroot** password.
5. Edit the file /VM/config/config_params:

   vi /VM/config/config_params
6. Change the line that read as follows:

   default 'IMAP4: Trusted Servers May Login As Superusers' = 0

   into this:

   default 'IMAP4: Trusted Servers May Login As Superusers' = 1
7. If the line is not in the file, then the system is either not as R3.0 or does not have service pack 1.
8. Save the file.
9. Restart VM.
10. Stop VM:

    /VM/bin/stop_vm
11. Wait 10 minutes.
12. Start VM:

    /VM/bin/start-vm
13. Leave the root session:

    exit
14. Leave the **tsc** session:

    exit

Configure Modular Messaging with Exchange

This section explains the credential set that is necessary to integrate Avaya one-X Mobile with Modular Messaging Exchange message store. Access to Exchange is required by the Avaya one-X Mobile Server to provide Visual Voicemail functionality.

Perform the steps in this section on a Domain Controller.

Configure the Exchange Administrative User

You need to configure 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.

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

Access to Exchange is required by the Avaya one-X Mobile Server to provide the Avaya one-X Mobile Visual Voicemail functionality. The Domain User is used by Avaya one-X Mobile Application Suite to access voice messages from user mail boxes for this purpose.

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 down to the **Mailbox Store** of the Exchange Server.
   b. Right click on it and select **Properties**.
   c. Select the **Security** tab.
   d. Click the **Add** button and add the Domain User.
   e. Assign the following permissions to it:
      - 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.

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 (for example: Example/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 changes.

Validate Exchange Administrative User Permissions

Perform this procedure for both Avaya MMS and Cisco Unity voicemail installations.

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

1. Go to the Domain controller for the specified domain that the Administrative user is a member of.
2. Go to **Start > Programs > Administrative Tools > Active Directory Users and Computers** to bring up the Management Console.
3. Click **View > Advanced Features**.
4. Expand the tree control for the specified domain of the Administrative user.

5. Click on **Users**.
6. Locate the user in the right-hand pane.
7. Right click on the designated user and click on **Properties**.
8. Locate the group in which the user is a member.
9. In the **Permissions** frame, check all the listed permissions as **allow** except **Full Control**. **Full Control** should have neither **allow** nor **deny** checked.
10. Click **Apply** if changes were required.
11. Click **OK** to exit the property page.
12. Exit out of the Management Console.

Appendix A: Administrator's Worksheet

This worksheet is designed to help keep track of the configuration information required in the Avaya one-X Mobile Server Administration.

Information from Avaya Communication Manager

AES Password _____

AES Server Name _____

EC500 Self Administration FAC_____

Enhanced EC500 Activation FAC _____

Enhanced EC500 Deactivation FAC _____

Send All Calls Activation FAC _____

Send All Calls Deactivation FAC _____

Information from Application Enablement Services (AES)

JTAPI User _____

JTAPI Password _____

DMCC User _____

DMCC Password _____

Appendix B: Integration with Cisco CallManager

This document describes the configuration steps necessary to prepare Cisco CallManager for integration with the Avaya one-X Mobile Server.

Cisco CallManager must be configured to route calls to the Avaya one-X Mobile Server where the Avaya one-X Mobile Server can make routing decisions based on the user's settings.

Summary of Tasks

The following tasks must be completed to integrate Cisco CallManager and the Avaya one-X Mobile Server:

- Prepare Partitions and Calling Search Spaces for the integration.
- Create a JTAPI user.
- Create CTI route points.
- Configure phones for the integration.
- Configure Cisco CallManager to correctly pass caller ID.

Cisco CallManager Versions

This appendix covers Cisco CallManager versions 4.1X through 5.0X.

CTI Devices used by Avaya one-X Mobile Server to Intercept Calls

In order for the Avaya one-X Mobile Server to intercept and route calls, Cisco CallManager CTI objects must be used.

CTI Route Points

CTI Route Points are virtual devices inside the Cisco CallManager. Route Points may be used to redirect calls before they ring to the IP phone. CTI applications may register CTI Route Points in order to intercept calls before routing them to the IP phone.

The Avaya one-X Mobile Server uses CTI Route Points to intercept calls destined for a set of extensions specified by the directory number of the Route Point. The Avaya one-X Mobile Server application examines the preferences of the user before routing the call.

CTI Ports

CTI Ports are used by the Avaya one-X Mobile Server to make outbound calls to destinations specified by users. This includes mobile phones or other PSTN phones.

A CTI port is a virtual phone. It can be configured just like a physical IP phone device.

Partitions and Calling Search Space Background

The Avaya one-X Mobile Server uses partitions and Calling Search Spaces to intercept incoming calls to Cisco CallManager.

Calling Search Spaces and Partition Explanation

When a call comes in to Cisco CallManager, Cisco CallManager has to make a decision on how that call should be routed. Calling Search Spaces and Partitions help determine to what device a call is routed to and whether or not a device has permission to dial another device.

For additional background on Calling Search Spaces and Partitions, see the Cisco CallManager document *Partitions and Calling Search Spaces*.

Partition

The frequently used analogy of a partition is that of a phone book. A Cisco CallManager directory number (DN) has a partition attribute. The partition is simply a name given to a set of numbers. Using the analogy, a partition named “TraverseFremont” would contain all the directory numbers which are in the Traverse Fremont location.

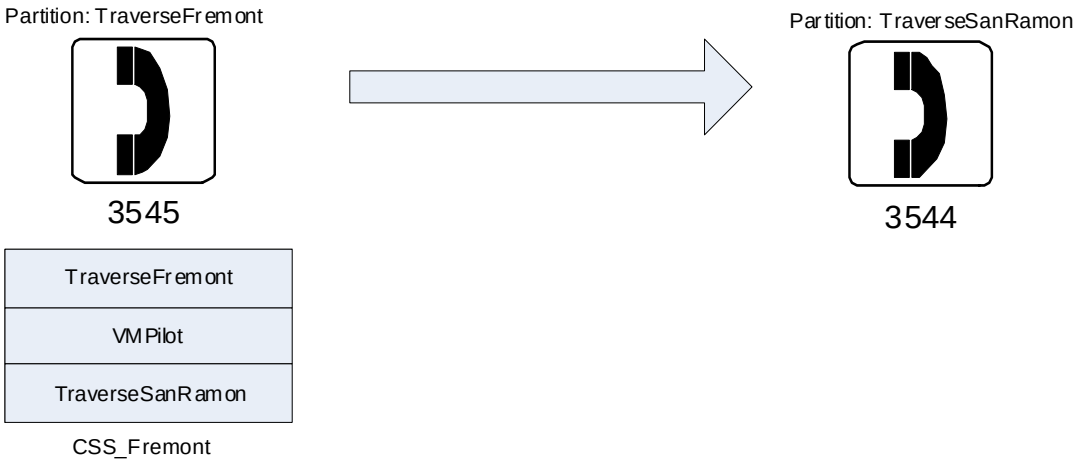
Calling Search Space

A Calling Search Space (CSS) is an attribute held by both a Cisco CallManager device and the directory number(s) associated with that device. The Calling Search Space attribute determines what partitions a device or directory number is allowed to dial. Using the phone book analogy, the Calling Search Space is similar to a list of phone books. The device or directory number may dial anyone in the list of phone books.

When a call is made, Cisco CallManager looks for potential matches for the digits dialed within the Calling Search Space of that device. One important concept to note for the Avaya one-X Mobile Server is that CallManager looks for exact matches first.

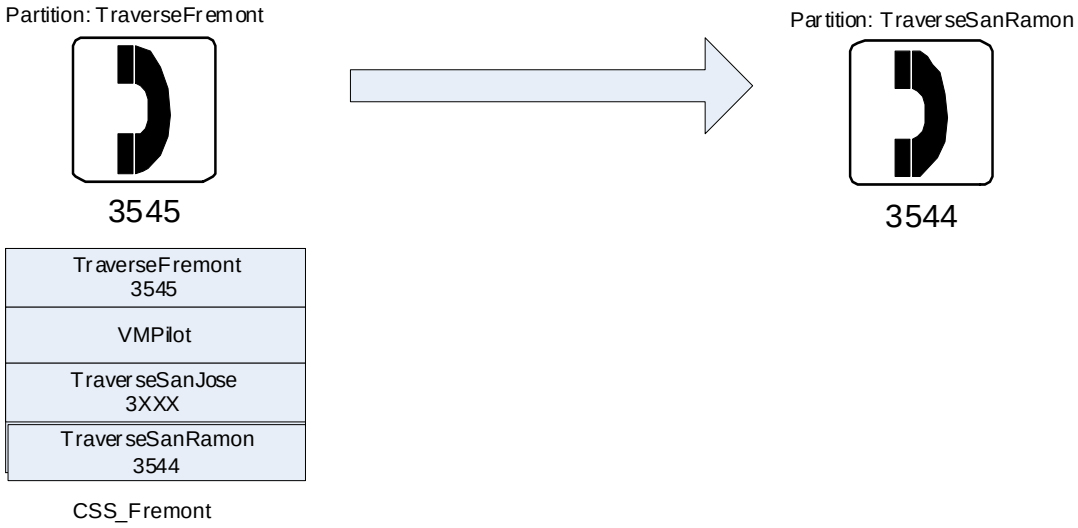
Example 1: Calling Search Space

In the following example, extension 3545 is making a call to extension 3544. Extension 3545 has the Calling Search Space CSS_Fremont and the directory number 3545 is in partition “TraverseFremont”. When 3545 dials 3544, CallManager looks for an exact match first in the Calling Search Space. In this case, it finds a match for 3544 in the “TraverseSanRamon” partition and routes the call to 3544.



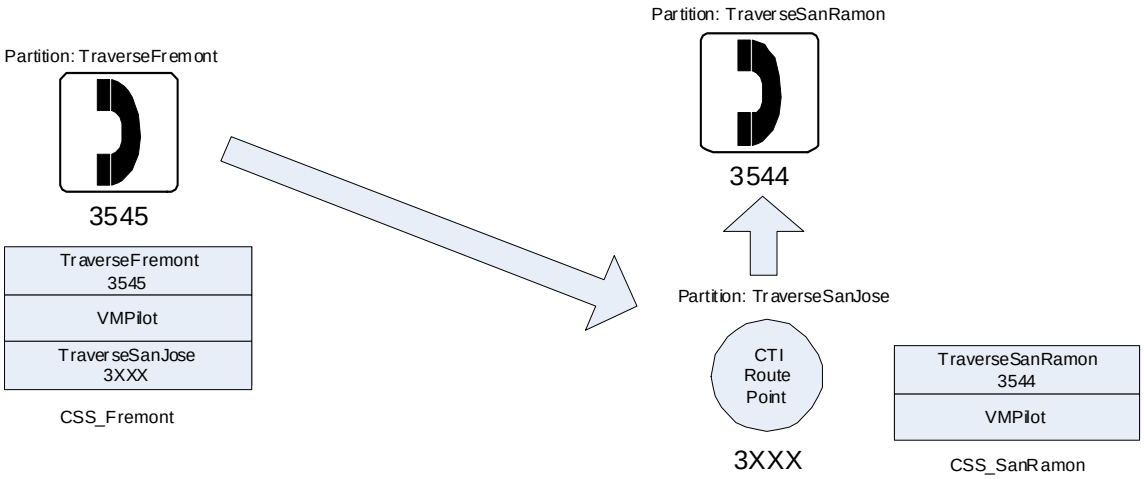
Example 2: Exact Match Takes Precedence

In the following example 3545 is dialing 3544 again. This time, there is a device with a directory number 3XXX in partition “TraverseSanJose”. When evaluating the potential matches, Cisco CallManager first looks for an exact match. It finds an exact match in the TraverseSanRamon partition and routes the call to that device. During evaluation, it found a potential match in partition “TraverseSanJose” for the wildcard directory number 3XXX, it kept evaluating to make sure there was no exact match in the remaining partitions. Once an exact match is found, the call is routed to that device and evaluation is stopped.



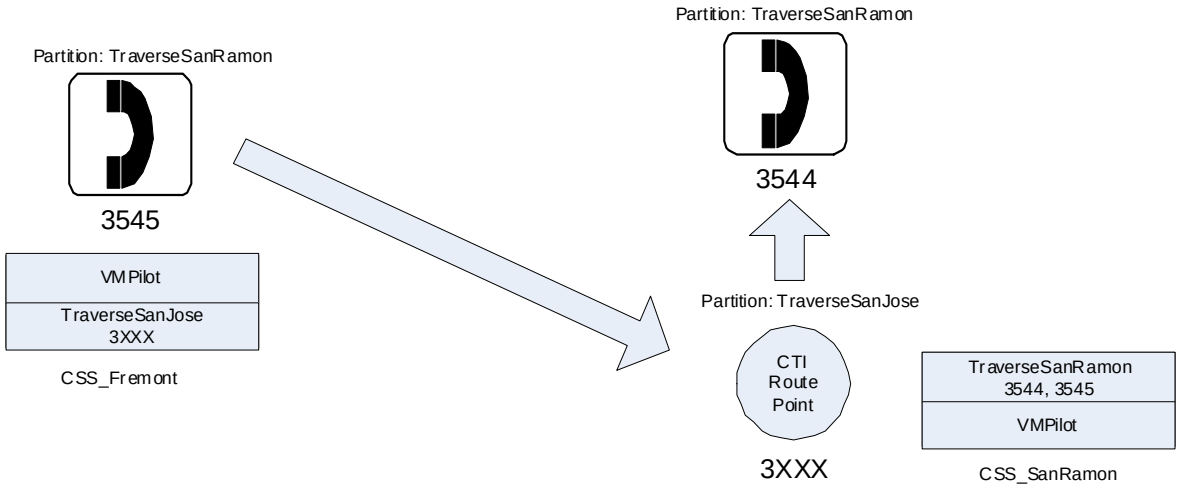
Example 3: Pattern Match

In this example, 3545 dials 3544. The partition TraverseSanRamon is not in the CSS_Fremont Calling Search Space and CallManager finds no exact match. It finds a wildcard match 3XXX in the TraverseSanJose partition and routes the call to that CTI Route Point device with directory number 3XXX. Upon receiving the call, the route point redirects the call to 3544. Cisco CallManager searches the CSS of the route point (CSS_SanRamon) and finds an exact match in the first partition, TraverseSanRamon and routes the call to 3544.



Example 4: Two Managed Phones in Same Partition

In this example, 3545 dials 3544. The partition TraverseSanRamon is not in the CSS_Fremont Calling Search Space and CallManager finds no exact match. It finds a wildcard match 3XXX in the TraverseSanJose partition and routes the call to that CTI Route Point device with directory number 3XXX. Upon receiving the call, the route point redirects the call to 3544. CallManager searches the CSS of the route point (CSS_SanRamon) and finds an exact match in the first partition, TraverseSanRamon and routes the call to 3544.



Prepare CallManager Calling Search Spaces and Partitions for the Avaya one-X Mobile Server

Add a Partition for Avaya one-X Mobile Server Managed Phones

Calls for Avaya one-X Mobile users are intercepted by the Interceptor CTI Route Points and then redirected to the IP phone based on user preferences. In order for the Interceptor CTI Route Point to redirect the call to the IP phone, the phone needs to be in a partition which is dialable from the Interceptor Route Point. Moreover, the phones which are managed by the Avaya one-X Mobile Server should be in a separate partition.

To create a partition for phones managed by the Avaya one-X Mobile Server, perform the following steps in the Cisco CallManager Administration User Interface:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Click on the **Route Plan** menu.	1. Click on the **Call Routing** menu.
2. Click on the **Class of Control** submenu.	2. Click on the **Class of Control** submenu.
3. Click on the **Partition** submenu.	3. Select the **Partition** item.
4. Click the **Add a New Partition** hyperlink.	4. Click the **Add New** button.
5. Enter the name of the Managed Phones partition you want to create, followed by the description. Example: “TraverseManaged, Avaya one-X Mobile Server Managed Phones”	5. Enter the name of the Managed Phones partition you want to create, followed by the description. Example: “TraverseManaged, Avaya one-X Mobile Server Managed Phones”
6. Click the **Insert** button.	6. Click the **Save** button.
7. A popup dialog box should confirm the success of adding the partition. Click **OK**. This will navigate back to the **Find and List Partitions** page.	7. Confirm in the **Find and List Partitions** that the newly added partition exists in the list.
8. Confirm in the **Find and List Partitions** that the newly added partition exists in the list.	

Create a Partition for Interceptor CTI Route Points

In order to intercept calls, the Interceptor CTI Route Points must be in a separate partition. To create a partition for the Interceptor CTI Route Points perform the following steps in the Cisco CallManager Administration User Interface:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Click on the **Route Plan** menu.	1. Click on the **Call Routing** menu.
2. Click on the **Class of Control** submenu.	2. Click on the **Class of Control** submenu.
	1 of 2

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
3. Click on the **Partition** submenu.	3. Select the **Partition** item.
4. Click the **Add a New Partition** hyperlink.	4. Click the **Add New** button.
5. Enter the name of the Managed Phones partition you want to create, followed by the description. Example: "TraverseManaged, Avaya one-X Mobile Server Managed Phones"	5. Enter the name of the Managed Phones partition you want to create, followed by the description. Example: "TraverseManaged, Avaya one-X Mobile Server Managed Phones"
6. Click the **Insert** button.	6. Click the **Save** button.
7. A popup dialog box should confirm the success of adding the partition. Click **OK**. This will navigate back to the **Find and List Partitions** page.	7. Confirm in the **Find and List Partitions** that the newly added partition exists in the list.
8. Confirm in the **Find and List Partitions** that the newly added partition exists in the list.	
	2 of 2

Create a Calling Search Space for Interceptor CTI Route Points

Interceptor CTI Route Points will need their own Calling Search Space. Perform the following steps in the Cisco CallManager Administration User Interface to create a Calling Search Space:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Click on the **Route Plan** menu.	1. Click on the **Call Routing** menu
2. Click on the **Class of Control** submenu.	2. Click on the **Class of Control** submenu.
3. Click on the **Calling Search Space** submenu.	3. Select the **Calling Search Space** item.
4. Click the **Add a New Calling Search Space** hyperlink.	4. Click the **Add New** button.
5. Enter a Calling Search Space Name: Example: "CSS_RoutePoint"	5. Enter a Calling Search Space Name: Example: "CSS_RoutePoint"
	1 of 2

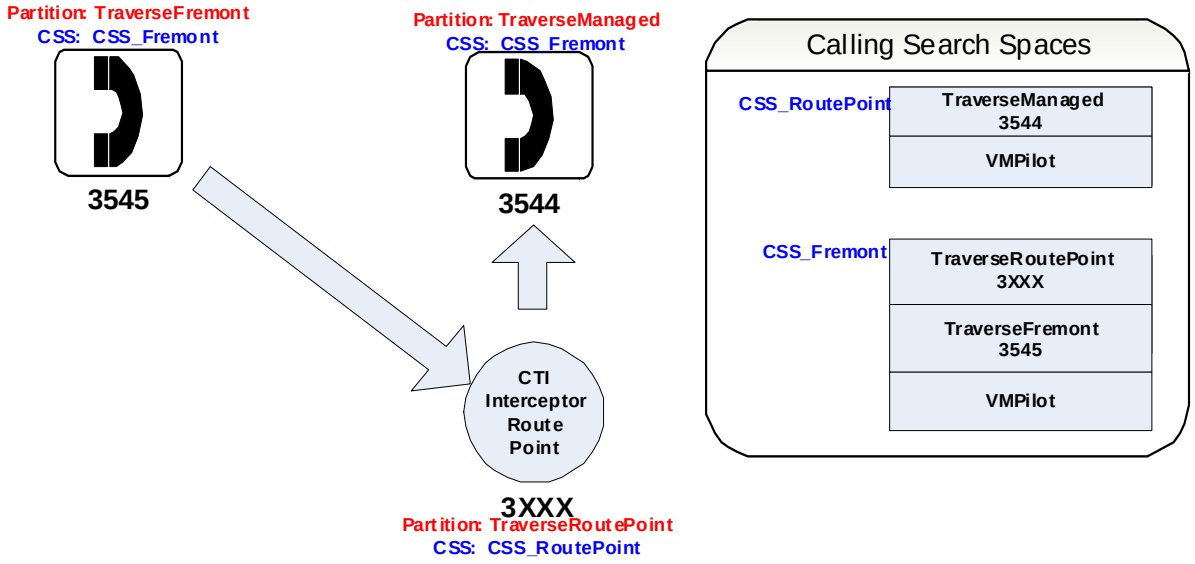
Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
6. If desired, enter a description: Example: “Calling Search Space for Interceptor Route Points.”	6. If desired, enter a description: Example: “Calling Search Space for Interceptor Route Points.”
7. From the **Available Partitions** list box, include the managed phones partition created in Add a Partition for Avaya one-X Mobile Server Managed Phones on page 44. This will allow the Interceptor Route Point to route calls directly to the managed phones.	7. From the **Available Partitions** list box, include the managed phones partition created in Add a Partition for Avaya one-X Mobile Server Managed Phones on page 44. This will allow the Interceptor Route Point to route calls directly to the managed phones.
8. From the **Available Partitions** list box, include the managed phones partition created in Add a Partition for Avaya one-X Mobile Server Managed Phones on page 44. This will allow the Interceptor Route Point to route calls directly to the managed phones.	8. From the **Available Partitions** list box, include the managed phones partition created in Add a Partition for Avaya one-X Mobile Server Managed Phones on page 44. This will allow the Interceptor Route Point to route calls directly to the managed phones.
9. Include any partitions required to reach Voicemail pilot numbers.	9. Include any partitions required to reach Voicemail pilot numbers.
10. Do **not** include the Route Point Partition in this Calling Search Space. Doing so may cause a routing loop.	10. Do **not** include the Route Point Partition in this Calling Search Space. Doing so may cause a routing loop.
11. Click on the **Insert** button.	11. Click on the **Save** button.
12. Click on the **Back to Find/List Calling Search Spaces** hyperlink to validate the new Calling Search Space was added to the list.	12. Click on the **Back to Find/List Calling Search Spaces** hyperlink to validate the new Calling Search Space was added to the list.
	2 of 2

Include the Route Point Partition in other Calling Search Spaces

After creating the Route Point Partition, you need to place it at the top of all other Calling Search Spaces ***except*** the Calling Search Space you created for the Interceptor Route Points in the Create a Partition for Interceptor CTI Route Points on page 45. This will make sure that all calls destined for managed numbers go through the Avaya one-X Mobile Server and have proper call handling settings applied. If you include the Route Point Partition in the Calling Search Space of the Interceptor Route Point, it may cause a routing loop.

Calling Search Space Example with Route Point Partition

The following example shows how the Interceptor Route Point works with Calling Search Spaces.



1. Extension 3545 in Calling Search Space CSS_Fremont dials extension 3544 in partition TraverseManaged.
2. CSS_Fremont does not contain an exact match for 3544. However, it does contain a pattern match in the TraverseRoutePoint Partition which contains 3XXX.
3. Cisco CallManager routes the call to the Route Point (controlled by the Avaya one-X Mobile Server) first.
4. The Avaya one-X Mobile Server examines the signaling and current call handling settings for the user at extension 3544 and decides to route the call to the desk.
5. The Interceptor Route Point 3XXX has a Calling Search Space “CSS_RoutePoint” which includes the TraverseManaged Partition. The TraverseManaged Partition contains 3544 and the call is routed to the desk.

Modify Other Calling Search Spaces to Include the Route Point Partition

For each Calling Search Space ***except*** the Calling Search Space created for the Interceptor Route Points, perform the following steps in the Cisco CallManager Administration User Interface:

Cisco CallManager 4.1X through 4.2X	**Cisco CallManager 5.0X**
1. Click on the **Route Plan** menu.	1. Click on the **Call Routing** menu
2. Click on the **Class of Control** submenu.	2. Click on the **Class of Control** submenu.
3. Click on the **Calling Search Space** submenu.	3. Select the **Calling Search Space** item.
4. Search for the Calling Search Space you want to modify using the **Find** button.	4. Search for the Calling Search Space you want to modify using the **Find** button.
5. From the **Available Partitions** list box, select the Route Point Partition created in the section Create a Partition for Interceptor CTI Route Points on page 45.	5. From the **Available Partitions** list box, select the Route Point Partition created in the section Create a Partition for Interceptor CTI Route Points on page 45.
6. Hit the down arrow to include it in the **Selected Partitions** list box.	6. Hit the down arrow to include it in the **Selected Partitions** list box.
7. Use the Up and Down arrows to the right of the **Selected Partitions** list box to move the Route Point Partition to the top of the Calling Search Space.	7. Use the Up and Down arrows to the right of the **Selected Partitions** list box to move the Route Point Partition to the top of the Calling Search Space.
8. Press the **Update** button.	8. Press the **Save** button.
9. Click on the **Back to Find/List Calling Search Spaces** hyperlink to modify additional Calling Search Spaces.	

Modify the MWI and Voicemail Ports Calling Search Space

Make sure that the Calling Search Spaces used for MWI and Voicemail ports include the Managed Partition(s) that you created in the section Add a Partition for Avaya one-X Mobile Server Managed Phones on page 44. Also ensure that the Route Point Partition is ***not*** included in these Calling Search Spaces. MWI will not work properly if the Route Point Partition is included in these Calling Search Spaces.

Create the JTAPI user

In order to route calls the JTAPI application on the Avaya one-X Mobile Server requires all CTI objects used by the application to be associated with a given JTAPI user.

Perform the following steps in the Cisco CallManager Administration User Interface to create a JTAPI user for use by the Avaya one-X Mobile Server:

Cisco CallManager 4.1X through 4.2X	**Cisco CallManager 5.0X**
1. Click on the **User** menu.	1. Click on the **User Management** menu.
2. Click on the **Add New User** submenu.	2. Click on the **Application User** submenu.
3. Enter a first name. Example: “traverse.”	3. Click on the **Add New** button.
4. Enter a last name. Example: “jtapi.”	4. Enter a user ID. Example: “tvjtapi”
5. Enter a user ID. Example: “tvjtapi”	5. Enter a password.
6. Enter a password.	6. Confirm the password.
7. Confirm the password.	7. In the **Groups** box, make sure the permissions “Standard CTI Allow Calling Number Modification” and “Standard CTI Enabled” are present.
8. Enter a PIN.	8. In the **Roles** list box, make sure the permissions “Standard CTI Allow Calling Number Modification” and “Standard CTI Enabled” are present.
9. Confirm the PIN.	9. Click the **Save** button.
	1 of 2

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
10. Check the **Enable CTI Application Use** checkbox.	
11. Check the **Call Park Retrieval Allowed** checkbox.	
12. Check the **Enable Calling Party Number Modification** checkbox.	
13. Click the **Insert** button.	
14. A status in red should read **Status: Insert Completed**.	
	2 of 2

You will be asked for the JTAPI username and password in the Avaya one-X Mobile Server Administration web site.

Create CTI Route Points for Intercepting Calls

Interceptor CTI Route Points are created in the Cisco CallManager Administration Website. If desired, multiple Interceptor Route Points can be created and registered with the Avaya one-X Mobile Server.

Understanding Patterns in Directory Numbers

Before Creating Route Points, it is important to understand how Route Points use pattern matching in Directory Numbers.

The Avaya one-X Mobile Server will intercept all calls that match the given pattern in the Directory Number field. For example, to make the Avaya one-X Mobile Server intercept all calls to the range of Directory Numbers 3000 to 3999, the Directory Number on the Route Point should be set to 3XXX.

The following characters are valid entries in the Directory Number field:
“[^ 0 1 2 3 4 5 6 7 8 9 -] + ? ! X * # +”.

Examples:

Directory Number Pattern	Matches Directory Numbers
3XXX	3000 to 3999
35XX	3500 to 3599
352[0-3]	3520, 3521, 3522, 3523

See "Wildcards and Special Characters in Route Patterns in Hunt Pilots" in the *Cisco CallManager System Guide* for a thorough explanation of each type.

Create an Interceptor Route Point

The Avaya one-X Mobile Server can utilize multiple Interceptor Route Points. It is not necessary to limit Interceptor Route Points to one. To create an Interceptor Route Point, perform the following steps in the Cisco CallManager Administration User Interface:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Click on the **Device** menu.	1. Click on the **Device** menu.
2. Click on the **CTI Route Point** submenu.	2. Click on the **CTI Route Point** submenu.
3. Click on the **Add a New CTI Route Point** hyperlink.	3. Click on the **Add New** button.
4. Enter a Device Name. Example: “MS_IntRP”	4. Enter a Device Name. Example: “MS_IntRP”
5. If desired, enter a description: Example: “Avaya one-X Mobile Server Interceptor Route Point”	5. If desired, enter a description: Example: “Avaya one-X Mobile Server Interceptor Route Point”
6. Select the appropriate Device Pool from the drop-down menu.	6. Select the appropriate Device Pool from the drop-down menu.
7. Select the Calling Search Space created in Create a Calling Search Space for Interceptor CTI Route Points on page 46.	7. Select the Calling Search Space created in Create a Calling Search Space for Interceptor CTI Route Points on page 46.
8. Click the **Insert** button.	8. Select the Location.
	1 of 3

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
9. When prompted to Add a Directory Number to the CTI Route Point, press the **OK** button.	9. Click the **Save** button.
10. In the **Directory Number** text box, enter the directory number for the route point. When entering the directory number for an Interceptor Route Point, patterns and wild cards may be used. For example, to make the Avaya one-X Mobile Server intercept all calls in the range 3000 to 3999, enter the directory number as 3XXX.	10. Click on the **Add a new DN** hyperlink on the bottom of the page.
11. In the **Partition** drop-down menu, select the partition created in Create a Partition for Interceptor CTI Route Points on page 45.	11. In the **Directory Number** text box, enter the directory number for the route point. When entering the directory number for an Interceptor Route Point, patterns and wild cards may be used. For example, to make the Avaya one-X Mobile Server intercept all calls in the range 3000 to 3999, enter the directory number as 3XXX.
12. Leave the **Voice Mail Profile** set to “<None>”.	12. In the **Route Partition** drop-down menu, select the partition created in Create a Partition for Interceptor CTI Route Points on page 45.
13. In the Calling Search Space drop-down, select the Calling Search space created in Create a Calling Search Space for Interceptor CTI Route Points on page 46.	13. Leave the **Voice Mail Profile** set to “<None>”.
	2 of 3

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
14. In the **Forward No Answer Internal, Forward No Answer External, Forward Unregistered Internal (CCM 4.2 only), and Forward Unregistered External (CCM 4.2 only)** fields, enter the Directory Number entered in step 10. Set the Calling Search Space drop-down to the same value entered in step 13. **Important:** this will ensure that calls are routed to the IP phone if the Avaya one-X Mobile Server is unavailable.	14. In the Calling Search Space drop-down, select the Calling Search space created in Create a Calling Search Space for Interceptor CTI Route Points on page 46.
15. Click the **Add** button to add the directory number.	15. In the **Forward No Answer Internal** and **Forward No Answer External** fields, enter the directory number entered in step 11. Set the Calling Search Space drop-down to the same value in step 14. **Important:** this will ensure that calls are routed to the IP phone if the Avaya one-X Mobile Server is unavailable.
	16. Click the **Save** button to add the directory number.
	3 of 3

Associate the JTAPI User with the Interceptor Route Points

After creating the Interceptor Route Points, you need to associate the Interceptor Route Points with the JTAPI user you created in Create the JTAPI user on page 50. To associate the Interceptor Route Points with the JTAPI user, perform the following steps in the Cisco CallManager Administration User Interface for each Interceptor Route Point you created:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Click on the **User** menu in Cisco CallManager.	1. Click on the **User Management** menu.
2. Click on the **Global Directory** menu.	2. Click on the **Application User** submenu.
	1 of 2

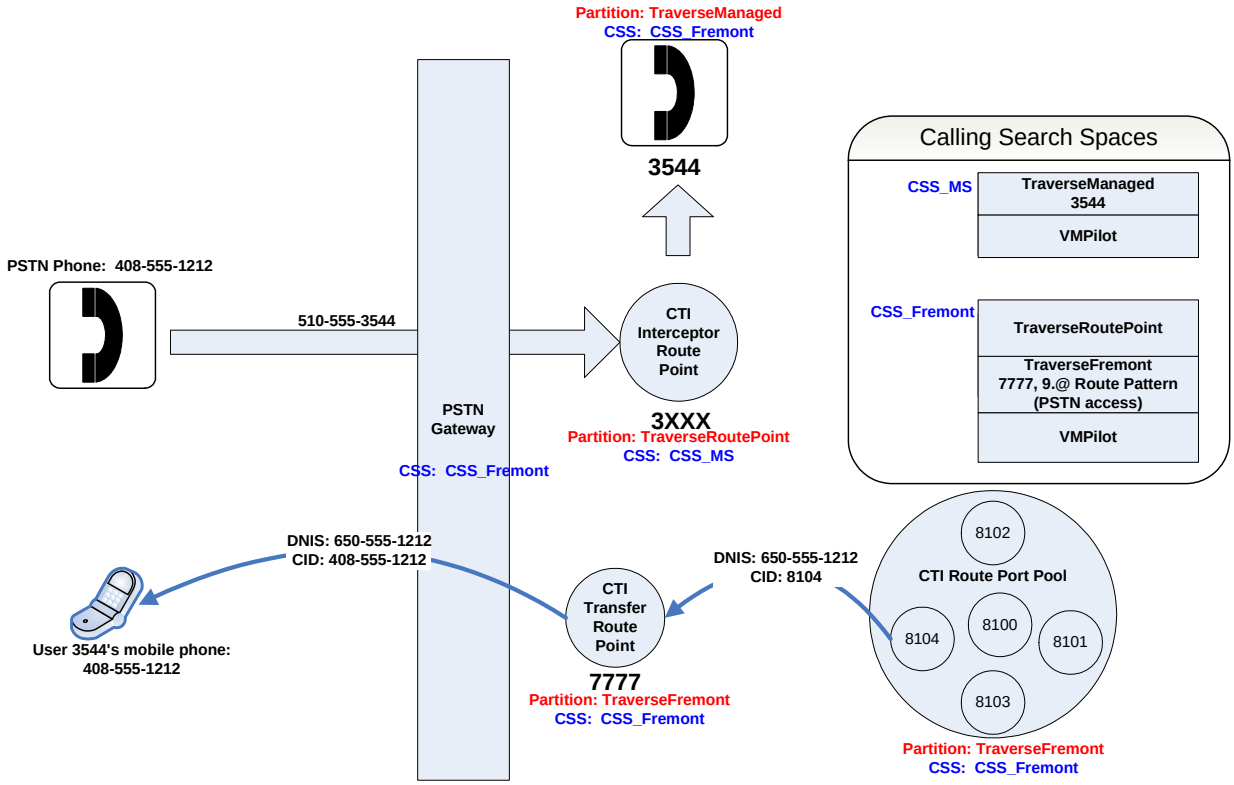
Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
3. In the **User Search** text box, enter the name of the JTAPI user you created in Create the JTAPI user on page 50.	3. In the **User Search** text box, enter the name of the JTAPI user you created in Create the JTAPI user on page 50.
4. Press the **Search** Button.	4. Press the **Find** Button.
5. Click the hyperlink of the JTAPI user you created.	5. Click the hyperlink of the JTAPI user you created.
6. In the **Application Profiles** section on the left-hand side, click on the **Device Association** hyperlink.	6. In the **Device Information > Available Devices** section of the page, select the Interceptor CTI Route Point you created in Create an Interceptor Route Point on page 52.
7. On the **Device Association** page, search for the device name of the Interceptor CTI Route Point you created in Create an Interceptor Route Point on page 52.	7. Select the CTI Route Point in the **Available Devices** section and press the down arrow to move it into the **Controlled Devices** list box.
8. Check the checkbox of the **CTI Interceptor Route Point**.	8. Repeat the process for other Interceptor Route Points you created.
9. Press the **Update Selected** button to associate the device.	9. Press the **Save** button to update the user.
10. Repeat the process for other Interceptor Route Points you created.	
	2 of 2

Transfer Route Points

The Avaya one-X Mobile Server uses CTI Route Points to preserve caller ID on outbound calls to mobile phones and other PSTN phones. This is called a Transfer Route Point. When a call is made to a mobile phone, it actually routes through a Transfer Route Point. The Transfer Route Point preserves the caller ID so that the mobile phone can see the caller ID of the calling party.

How the Avaya one-X Mobile Server uses Transfer Route Points

The following diagram illustrates how the Avaya one-X Mobile Server uses a Transfer Route Point.



1. A PSTN phone 408-555-1212 makes a call to a Cisco CallManager and Avaya one-X Mobile Server user at 510-555-3544.
2. The call goes through the PSTN gateway and routes to the CTI Interceptor Route Point as the gateway has Calling Search Space for inbound calls set to “CSS_Fremont” and the Interceptor Route Point is in the “TraverseRoutePoint” partition that is at the top of the “CSS_Fremont” Calling Search Space.
3. The Interceptor Route Point then routes the call to the desk at 3544. This works because the Route Point is in CSS_MS which has the “TraverseManaged” partition at the top of its CSS. 3544 is in “TraverseManaged”, so the Avaya one-X Mobile Server routes the incoming call to the desk.

4. Simultaneously, the Avaya one-X Mobile Server needs to ring the user at 3544's mobile phone. The Avaya one-X Mobile Server initiates an outbound call from a CTI port from the CTI Port Pool to the Transfer Route Point at 7777. Note that the Calling Search Space of the CTI Ports is "CSS_Fremont" which includes the "TraverseFremont" partition at the top. The Transfer Route Point is in the "TraverseFremont" partition, so the call routes to the Transfer Route Point at 7777. The Transfer Route Point changes the calling party number to the calling party that originally called 510-555-3544; 408-555-1212 and simply let's the call pass through, only changing the signaling.
5. The Transfer Route Point has Calling Search Space "CSS_Fremont" and therefore has "TraverseFremont" (which has the 9.@ Route Pattern and PSTN access) and is able to complete the call to the mobile phone.
6. The mobile phone caller sees the call as originating from 408-555-1212.

Choose Directory Numbers for the Transfer Route Point

It is important to select an appropriate Directory Number for a Transfer Route Point to make sure calls route in a timely fashion.

Allowed Characters Transfer Route Point Directory Numbers

Use no special characters in the Directory Number for the Transfer Route Point. The Transfer Route Point must have specific Directory Number consisting of digits 0-9 only.

Interdigit Timeout Issues with Pattern Matching

The Directory Number entered must not conflict or match with any other route patterns, translation patterns, etc. This will cause a significant delay in calls made to the PSTN.

Example: Matching Route Pattern

For example, if there is a route pattern called "9.@", do not create a Transfer Route Point Directory Number of 9345. The route pattern will cause a match in calls made to the PSTN. This will cause the Cisco CallManager to wait for the interdigit timeout before routing the call and will result in significant delay.

Example: Matching Directory Number

If a device with the Directory Number "5432" exists in the Cisco CallManager, a Transfer Route Point with the Directory Number "543" will invoke the interdigit timeout before routing the call. Choose a Directory Number with more digits than any longer matching Directory Number.

Route Plan Report

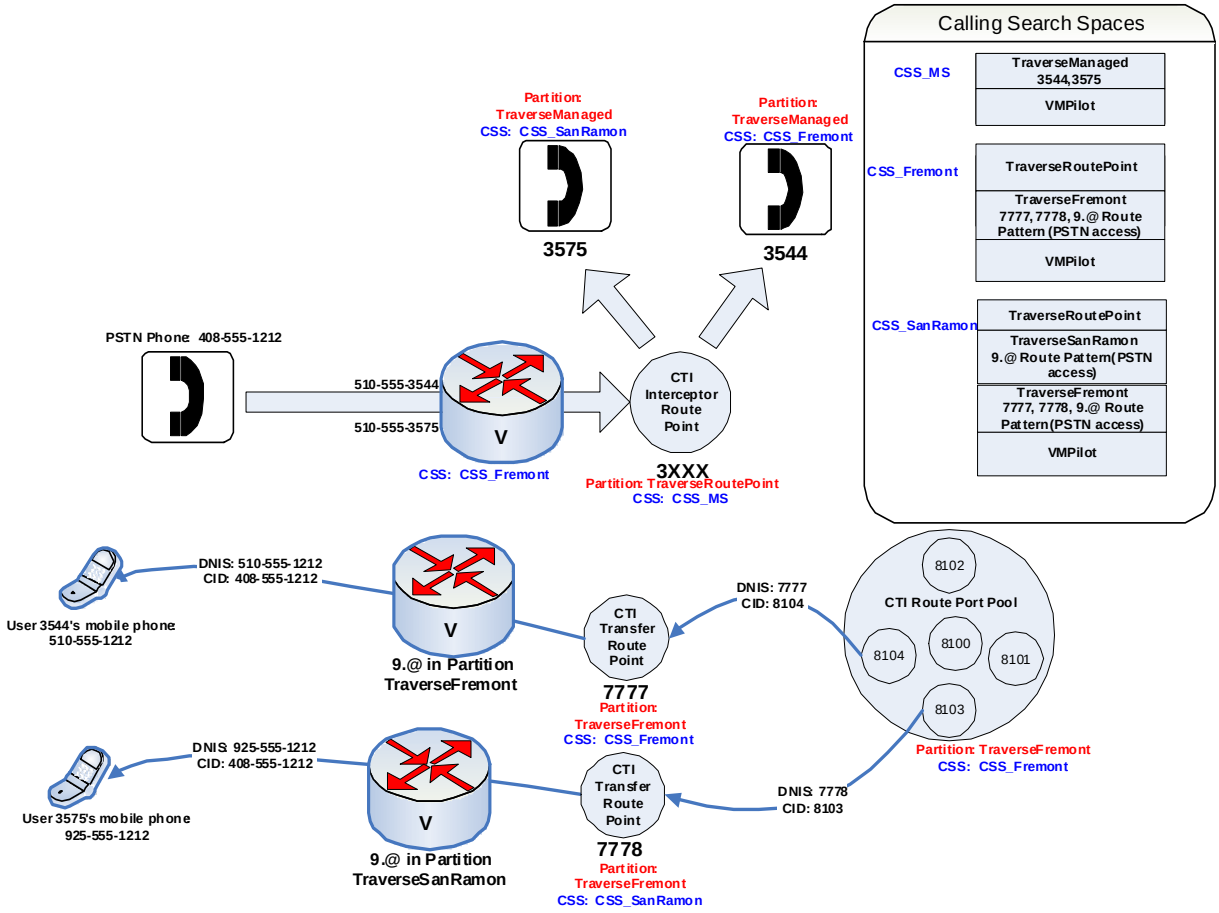
Before selecting the Directory Number, check the “Route Plan Report” in Cisco CallManager Administration to determine if undesirable potential matches exist for the Transfer Route Point Directory Number chosen.

The Route Plan Report is accessible under the “Route Plan” menu and the Route Plan Report menu item.

Use Multiple Transfer Route Points to Preserve Users Calling Search Spaces

In general, one Transfer Route Point is necessary for each Calling Search Space that managed users use. For example, if users with CSS_Fremont and CSS_SanRamon are managed by the Avaya one-X Mobile Server, a Transfer Route Point should be created for each CSS. This will preserve the Calling Search Space of the user. For example, if the user is in CSS_Fremont, you would need to create a Transfer Route Point with the Calling Search Space CSS_Fremont to be used to route calls outbound to the PSTN for users with that Calling Search Space.

The Avaya one-X Mobile Server automatically determines the Calling Search Space for each user and selects a Transfer Route Point with the appropriate Calling Search Space in order to preserve the user's dialing rules. The following diagram illustrates how the Avaya one-X Mobile Server uses multiple Transfer Route Points to preserve the Calling Search Space of the user.



In the diagram, incoming calls are directed from a PSTN phone with CID 408-555-1212 to two different phones. The device with the Directory Number 3575 is in CSS_SanRamon and the device with Directory Number 3544 is in CSS_Fremont. Both use different outbound gateways.

When a request to redirect the incoming calls to the user's mobile phone is made, CTI ports from the pool make the outbound calls. They first make calls to Transfer Route Points. They direct the call to the Transfer Route Point that has the same Calling Search Space as the called user (in this case 3544 and 3575). The user with DN 3544 has Calling Search Space CSS_Fremont on their device. Their outbound call is initiated through a Transfer Route Point which has the same Calling Search Space as the called user: CSS_Fremont is the matching Calling Search Space so Transfer Route Point 7777 is used. This routes the call out of the Fremont Gateway.

The call to the user at 3575 is routed through the Transfer Route Point 7778 as 3575 has the Calling Search Space CSS_SanRamon on their Directory Number. The call is then routed through the San Ramon Gateway, thus preserving the called users dialing rules.

The Avaya one-X Mobile Server also has the ability to select a default Transfer Route Point for outbound calls. Selection of the default Transfer Route Point is discussed in the *Avaya one-X™ Administration and Maintenance Guide*, document number 18-602144.

Create a Transfer Route Point

Create Transfer Route Points according to the following steps to be performed in the Cisco CallManager Administration User Interface:

Cisco CallManager 4.1X through 4.2X	**Cisco CallManager 5.0X**
1. Click on the **Device** menu.	1. Click on the **Device** menu.
2. Click on the **CTI Route Point** submenu.	2. Click on the **CTI Route Point** submenu.
3. Click on the **Add a New CTI Route Point** hyperlink.	3. Click on the **Add New** button.
4. Enter a Device Name. Example: “MS_TransferRP”	4. Enter a Device Name. Example: “MS_TransferRP”
5. If desired, enter a description: Example: “Avaya one-X Mobile Server Transfer Route Point”	5. If desired, enter a description: Example: “Avaya one-X Mobile Server Transfer Route Point”
6. Select the appropriate Device Pool from the drop-down menu.	6. Select the appropriate Device Pool from the drop-down menu.
7. Select a Calling Search Space which includes a partition that allows the PSTN to be reached. If you are creating multiple Transfer Route Points to preserve the Calling Search Spaces of users, select a Calling Search Space that maps to the specified group of users.	7. Select a Calling Search Space which includes a partition that allows the PSTN to be reached. If you are creating multiple Transfer Route Points to preserve the Calling Search Spaces of users, select a Calling Search Space that maps to the specified group of users.
8. Click the **Insert** button.	8. Select the Location.
9. When prompted to Add a Directory Number to the CTI Route Point, press the **OK** button.	9. Click the **Save** button.
	1 of 3

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
10. In the **Directory Number** text box, enter the directory number for the route point. When entering the directory number for an Interceptor Route Point, patterns and wild cards may be used. For example, to make the Avaya one-X Mobile Server intercept all calls in the range 3000 to 3999, enter the directory number as 3XXX.	10. Click on the **Add a new DN** hyperlink on the bottom of the page.
11. In the Partition drop-down menu, select the partition which can be dialed from the Calling Search Space of the managed phones. Additionally, the partition should be dialable from the Calling Search Space of the CTI ports. The Calling Search Space should be the same as in step 7.	11. In the **Directory Number** text box, enter the directory number for the route point. When entering the directory number for an Interceptor Route Point, patterns and wild cards may be used. For example, to make the Avaya one-X Mobile Server intercept all calls in the range 3000 to 3999, enter the directory number as 3XXX.
12. Leave the **Voice Mail Profile** set to “<None>”.	12. In the Partition drop-down menu, select the partition which can be dialed from the Calling Search Space of the managed phones. Additionally, the partition should be dialable from the Calling Search Space of the CTI ports. The Calling Search Space should be the same as in step 7.
13. Select a Calling Search Space which includes a partition that allows the PSTN to be reached. If you are creating multiple Transfer Route Points to preserve the Calling Search Spaces of users, select a Calling Search Space that maps to the specified group of users.	13. Leave the **Voice Mail Profile** set to “<None>”.
	2 of 3

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
14. In the **Forward No Answer Internal** and **Forward No Answer External** fields, enter the directory number entered in step 10. Set the Calling Search Space drop-down to the same value as in step 13. **Important:** this will make sure that calls are routed to the IP phone if the Avaya one-X Mobile Server is unavailable.	14. Select a Calling Search Space which includes a partition that allows the PSTN to be reached. If you are creating multiple Transfer Route Points to preserve the Calling Search Spaces of users, select a Calling Search Space that maps to the specified group of users.
15. Click the **Add** button to add the Directory Number.	15. In the **Forward No Answer Internal** and **Forward No Answer External** fields, enter the directory number entered in step 11. Set the Calling Search Space drop-down to the same value as in step 14. **Important:** this will make sure that calls are routed to the IP phone if the Avaya one-X Mobile Server is unavailable.
	16. Click the **Save** button to add the directory number.
	3 of 3

Associate Transfer Route Points with the JTAPI User

After creating Transfer Route Points, you need to associate them with the JTAPI user you created in Create the JTAPI user on page 50. To associate a Transfer Route Point with the JTAPI user, perform the following steps in the Cisco CallManager Administration User Interface for the Transfer Route Point you created:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Click on the **User** menu in Cisco CallManager.	1. Click on the **User Management** menu.
2. Click on the **Global Directory** menu item.	2. Click on the **Application User** submenu.
3. In the **User Search** text box, enter the name of the JTAPI user you created in Create the JTAPI user on page 50.	3. In the **User Search** text box, enter the name of the JTAPI user you created in Create the JTAPI user on page 50.
	1 of 2

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
4. Press the **Search** Button.	4. Press the **Find** Button.
5. Click the hyperlink of the JTAPI User you created.	5. Click the hyperlink of the JTAPI User you created.
6. In the **Application Profiles** section on the left-hand side, click on the **Device Association** hyperlink.	6. In the **Device Information|Available Devices** section of the page, select the Transfer CTI Route Points you created in Create a Transfer Route Point on page 60.
7. On the **Device Association** page Search for the device name of the Transfer CTI Route Point you created in Create a Transfer Route Point on page 60.	7. Select the CTI Route Points in the **Available Devices** section and press the down arrow to move it into the **Controlled Devices** list box.
8. Check the checkbox of the CTI Transfer Route Point.	8. Repeat the process for other Transfer Route Points you created.
9. Press the **Update Selected** button to associate the device.	9. Press the **Save** button to update the user.
	2 of 2

Create a Pool of CTI Route Ports for Outbound calls

The Avaya one-X Mobile Server uses CTI Route Ports for making outbound calls. For example, when a user has the Simulring feature enabled, an Avaya one-X Mobile Server uses a CTI Port to make an outbound call to the user's mobile phone.

Since the number of CTI Route Ports needed depends on the number of users, the Avaya one-X Mobile Server Administration user interface provides an automated way to create CTI ports in a range. See the document *Traverse Networks Mobility Server 1.5 Administration UI Guide* section 3.3 "CTI Route Ports."

Modify AXL Throttle Settings

In order to retrieve configuration settings from the Cisco AXL Database layer, make the following temporary modifications to the AXL Settings.

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Click on the **Service** menu in Cisco CallManager Administration UI.	1. Click on the **System** menu.
2. Click on the **Service Parameters** menu item.	2. Click on the **Service Parameters** submenu.
3. For each node in the cluster, do the following: a. Select the node from the **Server** drop-down menu. b. Select **Cisco Database Layer Monitor** from the **Service** drop-down menu. c. Press the **Advanced** button. d. Scroll to the bottom of the page and set the **Maximum AXL Writes Allowed per Minute** to 300. e. Press the **Update** button.	3. For each node in the cluster do the following: a. Select the node from the **Server** drop-down menu. b. Select **Cisco Database Layer Monitor** from the **Service** drop-down menu. Ensure it is set to **Active.** c. Press the **Advanced** button. d. Scroll to the bottom of the page and set the **Maximum AXL Writes Allowed per Minute** to 300. e. Press the **Save** button.
4. Repeat steps 3a to 3e for each node in the cluster.	

Note:
This configuration need only be temporarily set while licensing and provisioning of Cisco CallConnect users is taking place. After user licensing and provisioning are finished, this parameter may be set back to its previous setting.

Configure Phones for the Integration

Before the Avaya one-X Mobile Server can intercept calls, you must move IP phones into the Avaya one-X Mobile Server managed partition created in Add a Partition for Avaya one-X Mobile Server Managed Phones on page 44.

Important:
You should perform this step after configuring the Avaya one-X Mobile Server Administration UI.

To move an IP phone into an Avaya one-X Mobile Server Managed Partition, perform the following steps in the Cisco CallManager Administration User Interface:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Click on the **Device** menu.	1. Click on the **Device** menu.
2. Click on the **Phone** menu item.	2. Click on the **Phone** menu item.
3. In the **Find and List Phones** search for the phones you want to manage.	3. In the **Find and List Phones** search for the phones you want to manage.
4. Click on the phone to go to the **Phone Configuration** page.	4. Click on the phone to go to the **Phone Configuration** page.
5. Click on the Directory Number in the left-hand side of the page.	5. Click on the Directory Number hyperlink on the left-hand side of the page.
6. Change the Partition to the one you created in Add a Partition for Avaya one-X Mobile Server Managed Phones on page 44.	6. Change the Partition to the one you created in Add a Partition for Avaya one-X Mobile Server Managed Phones on page 44.
7. In the **Call Forward and Pickup Settings** section, set the **No Answer Ring Duration** to 20 seconds. This will ensure that calls to the Mobile phone will have enough time to ring before rolling to voicemail.	7. In the **Call Forward and Pickup Settings** section, set the **No Answer Ring Duration** to 20 seconds. This will ensure that calls to the Mobile phone will have enough time to ring before rolling to voicemail.
8. In the **Forwarded Call Information Display** section, check the following four boxes: a. Caller Name b. Redirected Number c. Caller Number d. Dialed Number	8. In the **Forwarded Call Information Display** section, check the following four boxes: a. Caller Name b. Redirected Number c. Caller Number d. Dialed Number
9. Press the **Update** button.	9. Check the **Allow control of device from CTI** box.
10. Press the **Reset Device** button.	10. Press the **Save** button.
	1 of 2

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
11. Press the **OK** button to reset the device.	11. Press the **Reset** button.
12. Click on the **Configure Device** hyperlink to go back to the device.	12. Repeat the process for each phone you want to manage. **Important Note**: If you have a large number of phones to move to the Managed Partition, Cisco does provide a Bulk Administration Tool (BAT) which can make the task easier. The BAT is located on the “Applications” and “Install Plugins” page.
13. Click on the **Back to Find/List Phones** hyperlink.	
14. Repeat the process for each phone you want to manage. **Important Note**: If you have a large number of phones to move to the Managed Partition, Cisco does provide a Bulk Administration Tool (BAT) which can make the task easier. The BAT is located on the “Applications” and “Install Plugins” page.	
	2 of 2

Configure Cisco CallManager to Correctly Pass Caller ID

In order for the Avaya one-X Mobile Server to deliver the correct caller ID to the mobile phone you must use ISDN for connectivity to the PSTN. There are two possible ways to ensure that caller ID is correctly passed. The first method is the preferred method and should be used when there is a mapping or correlation between internal Directory Number and external Directory Number. For example: External Directory Number 510-555-1212 maps to internal Directory Number 1212. The second method can be used if there is no correlation between internal to external Directory Numbers but is not preferred as it is more time-intensive to set up.

Method One: Preserve Caller ID via Route Pattern

The following steps should be performed on the Route Pattern which routes traffic to your PSTN gateway. Typically, this is a 9.@ route pattern or something similar.

Modify the Route Pattern

Perform the following steps in the Cisco CallManager Administration User Interface:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Go to the **Route Plan** menu.	1. Go to the **Call Routing** menu.
2. Select the **Route Pattern** menu item.	2. Select the **Route/Hunt** submenu.
3. Search for the Route Pattern that routes calls to the PSTN. Most likely, this is a “9.@” Route Pattern.	3. Select the **Route Pattern** menu item.
4. Click on the hyperlink for that Route Pattern.	4. Search for the Route Pattern that routes calls to the PSTN. Most likely, this is a “9.@” Route Pattern.
5. In the **Calling Party Transformations** section, leave unchecked the checkbox titled **Use Calling Party's External Phone Number Mask**.	5. Click on the hyperlink for that Route Pattern.
6. For the **Calling Party Transform Mask** you can set some of the wildcards to mask off the internal Directory Numbers. For example “XXXX”.	6. In the **Calling Party Transformations** section, leave unchecked the checkbox titled **Use Calling Party's External Phone Number Mask**.
7. For the **Prefix Digits (Outgoing Calls)** field enter the company wide prefix, for example 510555. This should make outbound calls go out with 510555XXXX where XXXX is the Internal Directory Number.	7. For the **Calling Party Transform Mask** you can set some of the wildcards to mask off the internal Directory Numbers. For example “XXXX”.
8. Set **Calling Line ID Presentation** to **Allowed**.	8. For the **Prefix Digits (Outgoing Calls)** field enter the company wide prefix, for example 510555. This should make outbound calls go out with 510555XXXX where XXXX is the Internal Directory Number.
	9. Set **Calling Line ID Presentation** to **Allowed**.

Modify the Route List Detail Configuration

Perform the following steps on the CallManager Administration Interface:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Go to the **Route Plan** menu.	1. Go to the **Call Routing** menu.
2. Select the **Route Pattern** menu item.	2. Select the **Route/Hunt** submenu.
3. Search for the Route Pattern that routes calls to the PSTN. Most likely, this is a “9.@” Route Pattern.	3. Select the **Route Pattern** menu item.
4. Click on the hyperlink for that Route Pattern.	4. Search for the Route Pattern that routes calls to the PSTN. Most likely, this is a “9.@” Route Pattern.
5. Click the **Edit** hyperlink adjacent to the **Gateway or Route List** drop-down. (Note: If the drop-down value is set to “Not Selected”, then skip the remaining steps.)	5. Click on the hyperlink for that Route Pattern.
6. On the **Route List Configuration** page, click the **Route List Details** link on the left hand side.	6. Click the **Edit** hyperlink adjacent to the **Gateway or Route List** drop-down. (Note: If the drop-down value is set to “Not Selected”, then skip the remaining steps.)
7. In the **Calling Party Transformations** section set the **User Calling Party’s External Phone Number Mask** to **Default.** Leaving the value set to **on** will not pass the CID correctly.	7. On the **Route List Configuration** page, click the **Route List Details** link on the left hand side.
	8. In the **Calling Party Transformations** section set the **User Calling Party’s External Phone Number Mask** to **Default.** Leaving the value set to **on** will not pass the CID correctly.

Method Two: Preserve Caller ID via External Phone Number Mask.

Perform the following steps to preserve caller ID via the External Phone Number Mask:

1. Set the External Phone Number Mask on every Directory Number on every phone.

2. Modify the Route Pattern for external calls.
3. Modify the H.323 Gateway settings in Cisco CallManager.

Set the External Phone Number Mask

To set the External Phone Number Mask, perform the following steps in the Cisco CallManager Administration User Interface for every phone that is managed by the Avaya one-X Mobile Server.

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Click on the **Device** menu.	1. Click on the **Device** menu.
2. Click on the **Phone** menu item.	2. Click on the **Phone** menu item.
3. In the **Find and List Phones** search for the phones you want to manage.	3. In the **Find and List Phones** search for the phones you want to manage.
4. Click on the phone to go to the **Phone Configuration** page.	4. Click on the phone to go to the **Phone Configuration** page.
5. Click on the Directory Number in the left-hand side of the page.	5. Click on the Directory Number hyperlink on the left-hand side of the page.
6. Change the **External Phone Number Mask** to the full ten-digit number sent to the PSTN.	6. Change the **External Phone Number Mask** to the full ten-digit number sent to the PSTN.
7. Press the **Update** button.	7. Press the **Save** button.
8. Press the **OK** button to reset the device.	8. Press the **Reset** button to reset the device.
9. Click on the **Configure Device** hyperlink to go back to the device.	9. Repeat the process for every phone in Cisco CallManager. **Important Note**: Fill in the External Phone Number Mask for every phone in Cisco CallManager, not just the Avaya one-X Mobile Server managed phones. Otherwise, the caller ID will not work for outbound calls from non-managed phones.
	1 of 2

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
10. Click on the **Back to Find/List Phones** hyperlink.	
11. Repeat the process for every phone in the CallManager. **Important Note**: Fill in the External Phone Number Mask for every phone in Cisco CallManager, not just the Avaya one-X Mobile Server managed phones. Otherwise, the caller ID will not work for outbound calls from non-managed phones.	
	2 of 2

Modify the Route Pattern for External Calls

You need to modify the Route Pattern for External Calls so that it does not mask off any digits. This will allow the Avaya one-X Mobile Server to pass the correct caller ID for calls originating from the PSTN. Perform the following steps in the Cisco CallManager Administration User Interface:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Go to the **Route Plan** menu.	1. Go to the **Call Routing** menu.
2. Select the **Route Pattern** menu item.	2. Select the **Route/Hunt** submenu.
3. Search for the Route Pattern that routes calls to the PSTN. Most likely, this is a “9.@” Route Pattern.	3. Select the **Route Pattern** menu item.
4. Click on the hyperlink for that Route Pattern.	4. Search for the Route Pattern that routes calls to the PSTN. Most likely, this is a “9.@” Route Pattern.
5. In the **Calling Party Transformations** section, check the checkbox titled **Use Calling Party's External Phone Number Mask**.	5. Click on the hyperlink for that Route Pattern.
6. Set the **Calling Party Transform Mask** to “XXXXXXXXXX”. These ten X’s will ensure that the entire ten digits are delivered to the mobile phone.	6. In the **Calling Party Transformations** section, check the checkbox titled **Use Calling Party's External Phone Number Mask**.
	1 of 2

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
7. Leave the **Prefix Digits (Outgoing Calls)** field blank.	7. Set the **Calling Party Transform Mask** to “XXXXXXXXXX”. These ten X’s will ensure that the entire ten digits are delivered to the mobile phone.
8. Set **Calling Line ID Presentation** to **Allowed**.	8. Leave the **Prefix Digits (Outgoing Calls)** field blank.
9. Set **Calling Name Presentation** to **Allowed**.	9. Set **Calling Line ID Presentation** to **Allowed**.
	10. Set **Calling Name Presentation** to **Allowed**.
	2 of 2

Modify the H.323 Gateway Settings in Cisco CallManager

Modify the gateway settings so the Avaya one-X Mobile Server can pass the correct ten-digit caller ID to the mobile phone (or other PSTN phone). Perform the following steps in the Cisco CallManager Administration User Interface.

Cisco CallManager 4.1X through 5.0X
1. Go to the **Device** menu.
2. Click on the **Gateway** menu item.
3. Search for the appropriate H.323 Gateway in the **Find and List Gateways** search page.
4. Click on the hyperlink for the appropriate gateway.
5. Under the **Outbound Calls** section, set the field **Calling Party Selection** to **Originator**.
6. Set the field **Calling Party Presentation** to **Allowed** or **Default**.
7. If using National ISDN, set the field **Called party IE number type unknown*** to **National**.
8. If using National ISDN, set the field **Calling party IE number type unknown*** to **National**.
9. Set the **Called Numbering Plan*** to **Cisco CallManager**.
10.Set the **Calling Numbering Plan*** to **ISDN**.
1 of 2

Cisco CallManager 4.1X through 5.0X
11.Set the **Caller ID DN** to “XXXXXXXXXX”. These ten X’s allow the Avaya one-X Mobile Server to set the caller ID to an outside PSTN caller.
12.Check the checkbox titled **Display IE Delivery**.
13.Check the checkbox titled **Redirecting Number IE Delivery – Outbound.**
2 of 2

Modify the Route List Detail Configuration

Perform the following steps on the Cisco CallManager Administration Interface:

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
1. Go to the **Route Plan** menu.	1. Go to the **Call Routing** menu.
2. Select the **Route Pattern** menu item.	2. Select the **Route/Hunt** submenu.
3. Search for the Route Pattern that routes calls to the PSTN. Most likely, this is a “9.@” Route Pattern.	3. Select the **Route Pattern** menu item.
4. Click on the hyperlink for that Route Pattern.	4. Search for the Route Pattern that routes calls to the PSTN. Most likely, this is a “9.@” Route Pattern.
5. Click the **Edit** hyperlink adjacent to the **Gateway or Route List** drop-down. (Note: If the drop-down value is set to “Not Selected”, then skip the remaining steps.)	5. Click on the hyperlink for that Route Pattern.
6. On the **Route List Configuration** page, click the **Route List Details** link on the left-hand side.	6. Click the **Edit** hyperlink adjacent to the **Gateway or Route List** drop-down. (Note: If the drop-down value is set to “Not Selected”, then skip the remaining steps.)
1 of 2	

Cisco CallManager 4.1X through 4.2X	Cisco CallManager 5.0X
7. In the **Calling Party Transformations** section set the **User Calling Party's External Phone Number Mask** to **Default.** Leaving the value set to **on** will not pass the CID correctly.	7. On the **Route List Configuration** page, click the **Route List Details** link on the left hand side.
	8. In the **Calling Party Transformations** section set the **User Calling Party's External Phone Number Mask** to **Default.** Leaving the value set to **on** will not pass the CID correctly.
	2 of 2