



Configuring SIP Connectivity Between Avaya Communications Process Manager and Cisco Unified Communications Manager via Avaya SIP Enablement Services to Provide a Solution for Avaya Communications Enabled Business Processes - Issue 0.1

Abstract

These Application Notes describe the procedures for configuring SIP connectivity between Avaya Communications Process Manager (CPM) and Cisco Unified Communications Manager (UCM) via Avaya SIP Enablement Services. Employing this configuration enables call origination/termination between endpoints registered to Cisco UCM and Avaya CPM, where the signaling is SIP and the media is Real-time Transport Protocol (RTP). This configuration integrates endpoints registered to Cisco UCM with web services for business applications offered by Avaya CPM to provide a solution for Avaya Communications Enabled Business Processes (CEBP).

1. Introduction

These Application Notes describe the procedures for configuring SIP connectivity between Avaya Communications Process Manager (CPM) and Cisco Unified Communications Manager (UCM) via Avaya SIP Enablement Services. Employing this configuration enables call origination/termination between endpoints registered to Cisco UCM and Avaya CPM, where the signaling is SIP and the media is Real-time Transport Protocol (RTP). This configuration integrates endpoints registered to Cisco UCM with web services for business applications offered by Avaya CPM to provide a solution for Avaya Communications Enabled Business Processes (CEBP).

Figure 1 illustrates the sample configuration utilized for these Application Notes.

Avaya CPM is a Service-Oriented Architecture (SOA) based platform that exposes web services to enable continuous, closed-loop communications. All Avaya CEBP communications are continuous and “closed loop”, e.g., information about actions taken by users can be communicated back to the originating system that triggers an event, affecting the business process in real-time. Once an action is set in motion, Avaya CEBP helps assure that the business process keeps moving toward resolution. Refer to [1] and [2] for required/optional hardware/software components regarding Avaya CPM deployments.

Cisco UCM provides enterprise telephony features for the IP telephones present in this sample configuration. Cisco UCM is provisioned for call origination via SIP trunking to Avaya CPM.

The following web services are offered by Avaya CPM and were used to verify SIP connectivity between Avaya CPM and Cisco UCM:

- **Advisory service** - Sends a notification that consists of a subject and message to one or more recipients. Advisories can be sent to a telephone, e-mail account or SMS account as defined by user preference settings. Recipients acknowledge receipt of an advisory by telephone or the Avaya CPM Web Portal. For this sample configuration, only telephones, registered to Cisco UCM are utilized for receiving and acknowledging this service. The originator receives notification of users who have and have not acknowledged the advisory.
- **Notify and Respond** - Sends a notification to one or more recipients and collects responses. The notification includes context information (subject, message and possible responses). Notifications can be sent to a telephone, e-mail account or SMS account as defined by user preference settings. The response is more complex than an Advisory acknowledgement in that actual response data is returned to Avaya CPM. The response data can be an answer to a multiple choice question and can include optional associated data. Recipients can respond by telephone or the Avaya CPM Web Portal. For this sample configuration, only telephones, registered to Cisco UCM are utilized for receiving and acknowledging this service.
- **Notify and Conference** - Sends a notification to one or more recipients that invite them to join a conference. Recipients can respond and join in the following ways:
 - They can respond by telephone that they wish to join and are then automatically placed in the conference

- They can respond through the Avaya CPM Web Portal and provide a callback number at which to contact them. Avaya CPM then calls them and places them in the conference.
 - They can call into Avaya CPM to join the conference.
- Find and Call - Locates users by trying multiple devices according to user contact preferences and then sets up a conference call.

For this sample configuration, Avaya CPM is comprised of a server hosting the Avaya CPM software application, Avaya SIP Enablement Services, Avaya Meeting Exchange Express Edition (Meeting Exchange) and Avaya Voice Portal. Avaya CPM offered web services to users with an account defined on Avaya CPM as well as transient users, with no account. Both users and transient users used Cisco IP Phones registered to Cisco UCM. Avaya SIP Enablement Services provides SIP proxy functionality between Avaya CPM and Cisco UCM.

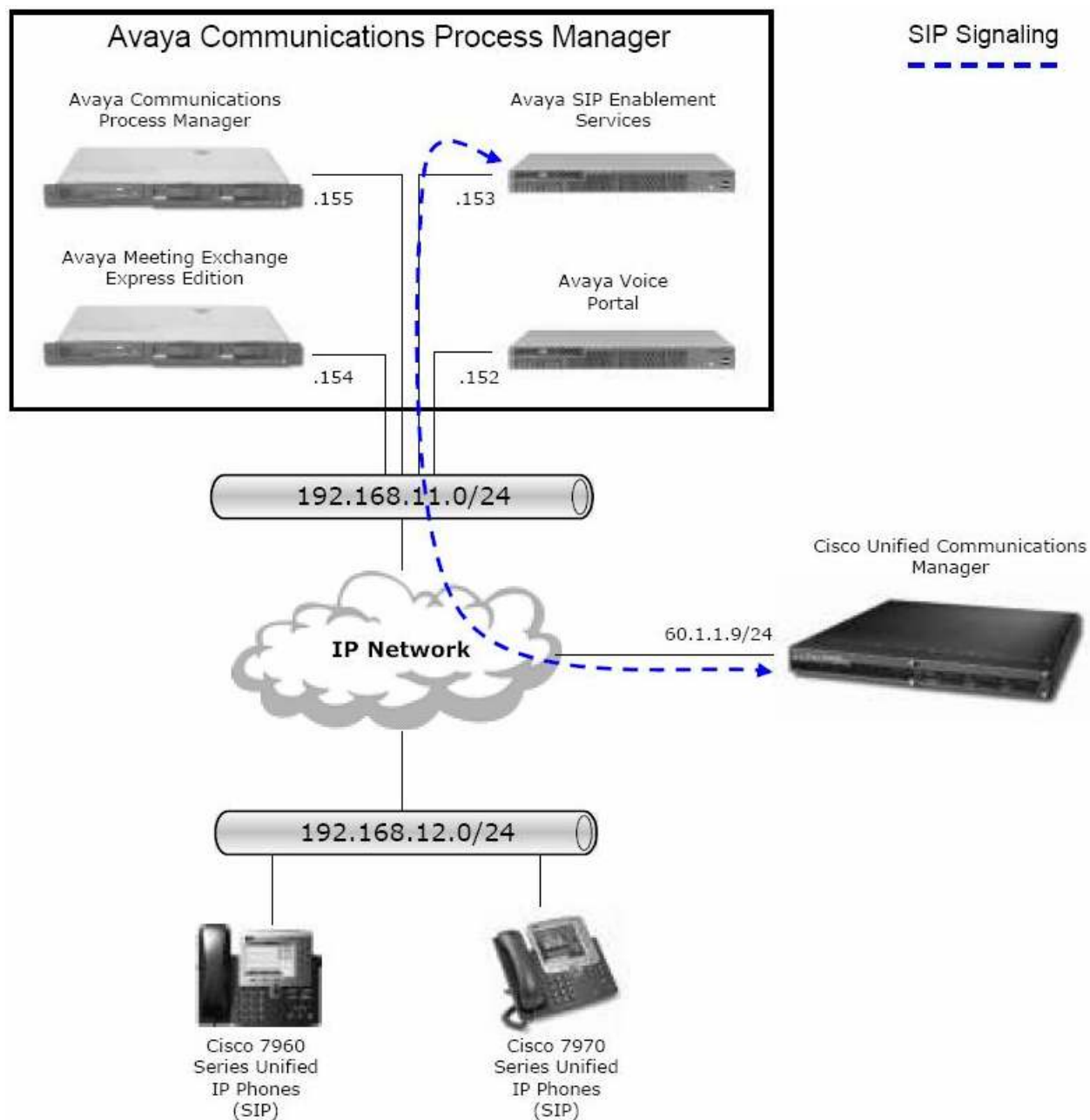


Figure 1: Sample Configuration

2. Equipment and Software Validated

The following equipment and software versions are used for this sample configuration:

Equipment	Software Version
Avaya Communications Process Manager <ul style="list-style-type: none">Avaya Communications Process ManagerAvaya SIP Enablement ServicesAvaya Meeting Exchange Express EditionAvaya Voice Portal	CPM 2.1 cpm 2.1.53 3.1-03.1.018.0 2.5.22.0 4.0.0.0.2901
Cisco Unified Communications Manager	CUCM 6.0 (6.0.1.2000-3)
Cisco 7960 Series IP Phones (SIP)	POS3-08-6-02
Cisco 7970 Series IP Phones (SIP)	SIP70.8-3-1S

Table 1: Equipment and Software Versions

3. Avaya Communications Process Manager Configuration

This section describes the configuration for enabling Avaya CPM to interoperate with Cisco UCM via Avaya SIP Enablement Services. For this sample configuration, it is assumed that Avaya CPM is provisioned to communicate with Avaya communication resources, e.g., Avaya Voice Portal, Avaya Meeting Exchange and Avaya SIP Enablement Services. Refer to [1] and [2] for additional information regarding the administration of Avaya CPM. Avaya CPM has two user interfaces:

- Web Portal - A web-based thin client that lets users manage their account, e.g., provision contact rules so their notifications are based on their preferences and availability. For this sample configuration, the Web Portal interface is used to invoke the web services as described in **Section 1** to both users and transient users. The Web Portal is accessed over a secure connection by entering **https://<Avaya CPM IP Address or Fully Qualified Domain Name (FQDN)>** into a web browser's Uniform Resource Locator (URL) bar.
- Operations Administration and Maintenance (OAM) - A web-based thin client user interface that lets a system administrator configure Avaya CPM with connectivity to Avaya communication resources. The OAM interface also provides access to system status, statistics, licenses, security certificates, logs and alarms. For this sample configuration, the OAM interface is used to provision Avaya CPM for dial-in services. The OAM interface is accessed over a secure connection by entering **https://<Avaya CPM IP Address or FQDN>/admin** into a web browser's URL bar.

***Note:** Some features described in these Application Notes require licensing. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya account representative to make the appropriate changes.*

3.1. Configure Avaya Communications Process Manager

This section describes the steps for configuring Avaya CPM to interoperate with Cisco UCM via Avaya SIP Enablement Services.

- **Steps 3.1.1 - 3.1.4** describe the provisioning of dial-in services. This enables endpoints registered to Cisco UCM to dial-in to Avaya CPM via Avaya SIP Enablement Services.
- **Step 3.1.5** describes the provisioning of call routing from Avaya CPM to endpoints registered to Cisco UCM via Avaya SIP Enablement Services. This enables the web services (see **Section 1**) delivery to endpoints registered to Cisco UCM.
- **Steps 3.1.6 - 3.1.8** describe the provisioning of a user account on Avaya CPM.

Step	Description
3.1.1	<p>From the Avaya CPM OAM interface, administer settings to notify users on Avaya CPM of a call back number to use for dial-in services as follows:</p> <ul style="list-style-type: none"> • Click System Configuration → Subsystem Settings → Notification & Response. • From the Notification and Response Configuration page, provision the Call Back Number field to define the telephone number that is specified in notifications for recipients to call into Avaya CPM. This number is included in e-mail, SMS notifications and voice mail messages. <p><i>Note: The semicolon is added to this field by Avaya CPM when this page is submitted.</i></p> <ul style="list-style-type: none"> • [Not Shown] Click Update.

AVAYA CPM Operations Administration and Maintenance

Welcome [admin] Log Out About Help

Notification and Response Configuration

* Scheduler Pool Size: 10 * Inbox Forward: ☒

* Connect Timeout: 120 Seconds

User Contact Retry

Maximum Delay: 90 Seconds * Minimum Delay: 30 Seconds

* Maximum Attempts: 3

Account

Refresh: ☐ * Refresh Rate: 3600 Seconds

LDAP Servers:

Directory

* Max Pool Size: 5 * Unused Connection Timeout: 300 Seconds

Login

* Delay: 10 Seconds * Timeout: 600 Seconds

Phone


* NDO: 1 * ID: 011

* Country Code: 1 Extension length: 4

Out Dial Code: 9 Call Back Number: 1800;

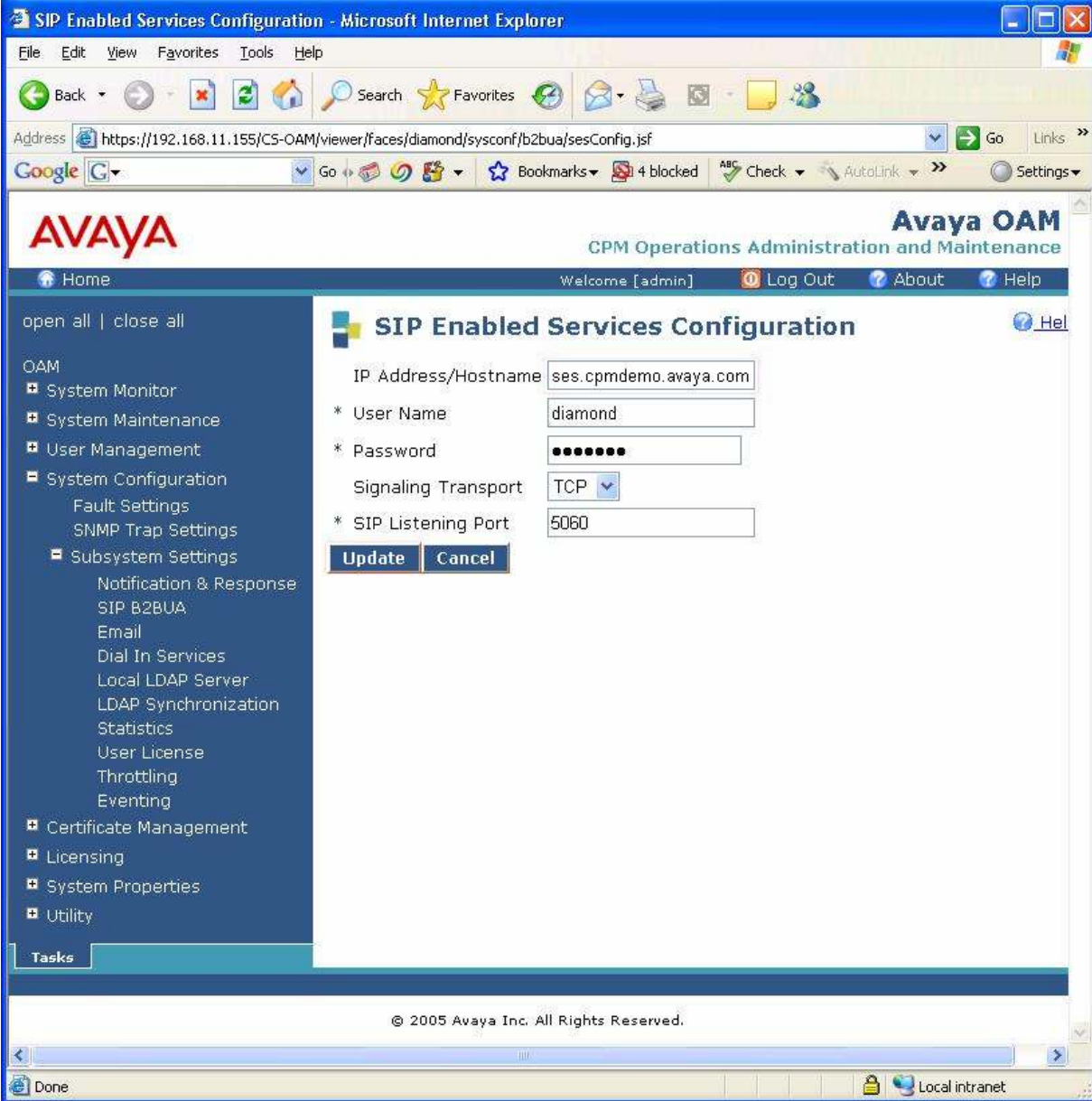
Step	Description
3.1.2	<p>From the Avaya CPM OAM interface, administer settings that enable dial-in services to Avaya CPM as follows:</p> <ul style="list-style-type: none"> Click System Configuration → Subsystem Settings → Dial In Services. From the Dial In Services page, modify or add an entry that associates the dialed telephone number with specific Avaya CPM services that users can access by calling into Avaya CPM. Modify the entry by selecting the appropriate entry and clicking Modify.

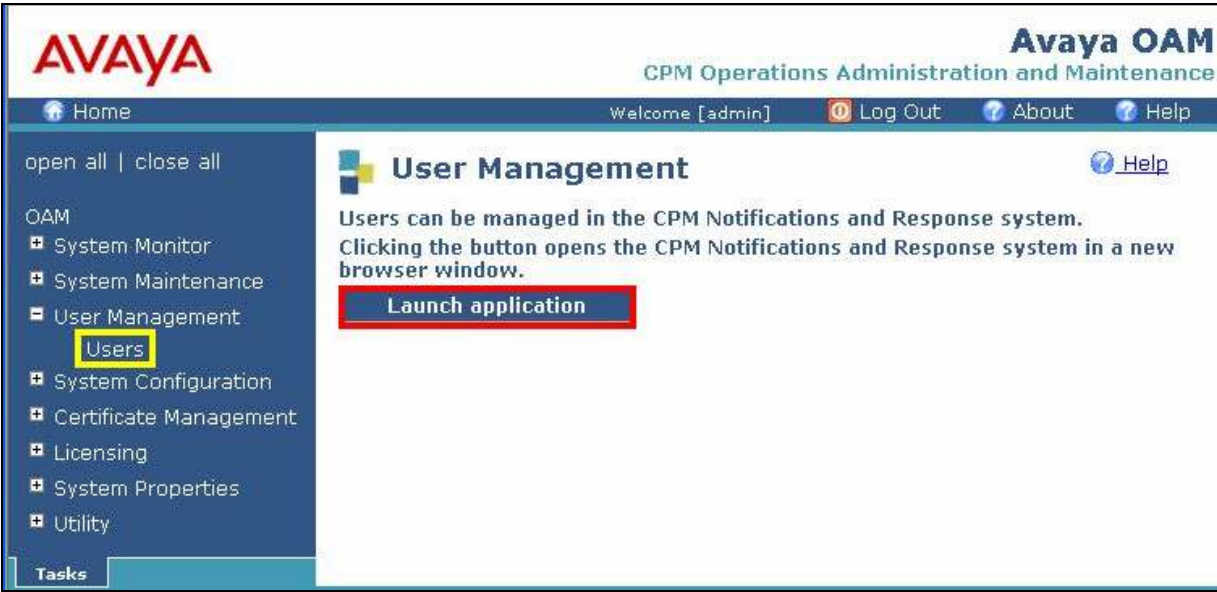


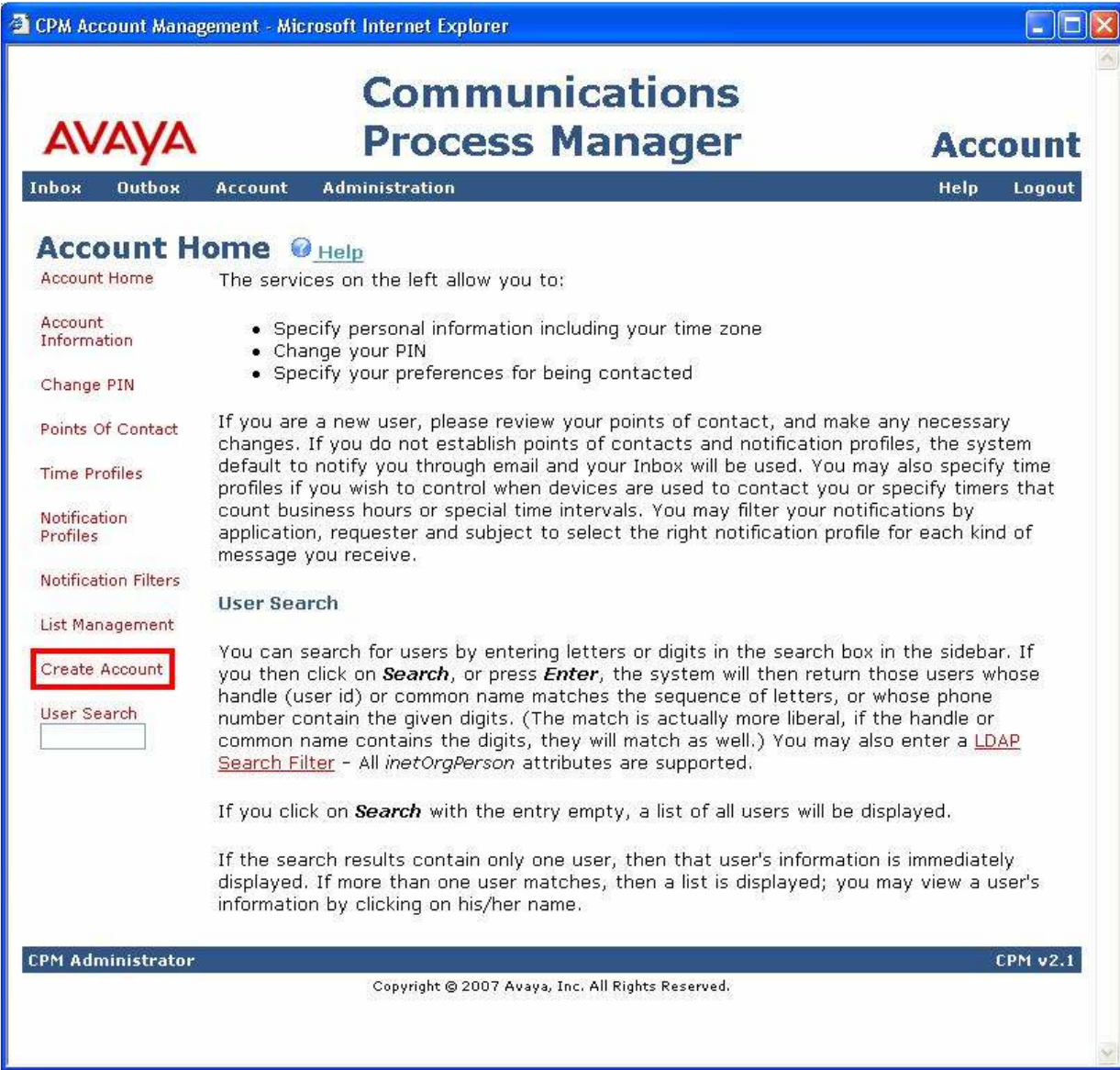
Step	Description
3.1.3	<p>From the Modify Dial In Service page, administer settings as displayed.</p> <ul style="list-style-type: none"> Enter the dialed telephone number in the Dial In Number field. Calls directed to Avaya CPM and targeted to this number will reach the b2buaOutputSender service. <i>Note: The Service Name field defines the interface to which incoming calls to Avaya CPM are routed. Do not change the default setting for this field unless a customized interface has been written and deployed for Avaya CPM. Changing this field for any other reason may cause dial-in services to stop functioning.</i> Refer to [2] for definitions regarding the remaining fields on this page. Click Update. 

Step	Description
3.1.4	<p>From the Avaya CPM OAM interface, administer settings for the SIPB2BUA as follows:</p> <ul style="list-style-type: none"> Click System Configuration → Subsystem Settings → SIPB2BUA. <ul style="list-style-type: none"> From the SIP Configurations page, provision the Third Party Callflow field to define 3pcc Call Establishment as per RFC 3725. Click Update. To provision call routing from Avaya CPM to endpoints registered to Cisco UCM via Avaya SIP Enablement Services, click SIP Enabled Services.

The screenshot displays the Avaya OAM interface for CPM Operations Administration and Maintenance. The left sidebar contains a navigation menu with the following items: Home, open all | close all, OAM, System Monitor, System Maintenance, User Management, System Configuration (expanded), Fault Settings, SNMP Trap Settings, Subsystem Settings (expanded), Notification & Response, SIP B2BUA (highlighted), Email, Dial In Services, Local LDAP Server, LDAP Synchronization, Statistics, User License, Throttling, Eventing, Certificate Management, Licensing, System Properties, and Utility. The main content area is titled 'SIP Configurations' and shows the 'SIP B2BUA Configuration' section. This section includes four configuration fields: Stack IP Address (192.168.11.155), SIP Domain (avaya.com), Third Party Callflow (Flow 1), and Limited Port Strategy (Proceed with Limited Ports). An 'Update' button is located below these fields. Below the configuration section, there is a link to 'SIP Enabled Services'.

Step	Description
3.1.5	<p>From the SIP Enabled Services Configuration page, verify Avaya CPM is provisioned for connectivity with Avaya SIP Enablement Services.</p> <p><i>Note: It is assumed that Avaya CPM is provisioned to communicate with Avaya communication resources, e.g., Avaya Voice Portal, Avaya Meeting Exchange and Avaya SIP Enablement Services. Refer to [1] and [2] for additional information regarding the administration of connectivity between Avaya CPM and Avaya communication resources.</i></p> 

Step	Description
3.1.6	<p>From the Avaya CPM OAM interface, add a user account as follows:</p> <ul style="list-style-type: none"> • Click User Management → Users. • From the User Management page, click Launch application.  <p>The screenshot shows the Avaya OAM interface. The top header includes the Avaya logo and 'Avaya OAM CPM Operations Administration and Maintenance'. The navigation bar shows 'Home', 'Welcome [admin]', 'Log Out', 'About', and 'Help'. The left sidebar contains a list of OAM functions: System Monitor, System Maintenance, User Management, Users (highlighted with a yellow box), System Configuration, Certificate Management, Licensing, System Properties, and Utility. The main content area is titled 'User Management' and contains the text: 'Users can be managed in the CPM Notifications and Response system. Clicking the button opens the CPM Notifications and Response system in a new browser window.' Below this text is a red button labeled 'Launch application' (highlighted with a red box).</p>

Step	Description
3.1.7	<p>From the Account Home page, click Create Account.</p> 

Step	Description
3.1.8a	Provision settings for a user account as displayed and scroll down. For this sample configuration, the Phone Number field corresponds to an endpoint registered to Cisco UCM.

CPM Account Management - Microsoft Internet Explorer

AVAYA **Communications Process Manager** **Account**

[Inbox](#) [Outbox](#) [Account](#) [Administration](#) [Help](#) [Logout](#)

Create Account [Help](#)

[Account Home](#) [Clear](#) [Save](#)

[Account Information](#)

[Change PIN](#)

[Points Of Contact](#)

[Time Profiles](#)

[Notification Profiles](#)

[Notification Filters](#)

[List Management](#)

[Create Account](#)

[User Search](#)

Those attributes marked with a red asterisk (*) are required and must have a value.

Roles

Administrator: ☐ Yes ☒ No

CPM User: ☒ Yes ☐ No

Attributes

***Handle:**

***ID Number:**

Display Name:

First Name:

***Last Name:**

***Common Name(s):**

Phone Number:

Mobile Phone Number:

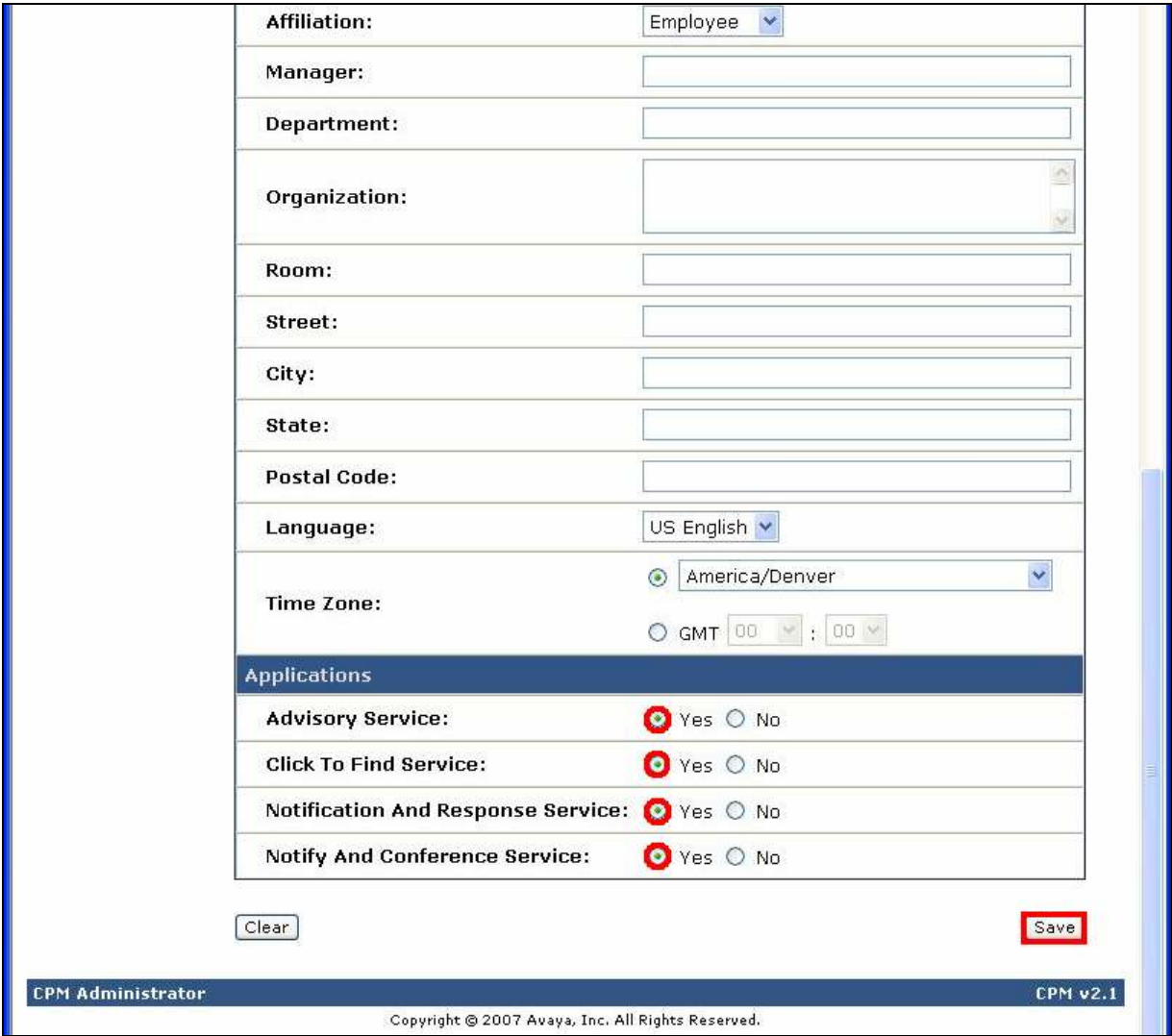
Fax Number:

Pager Number:

Electronic Mail Address:

Honorific:

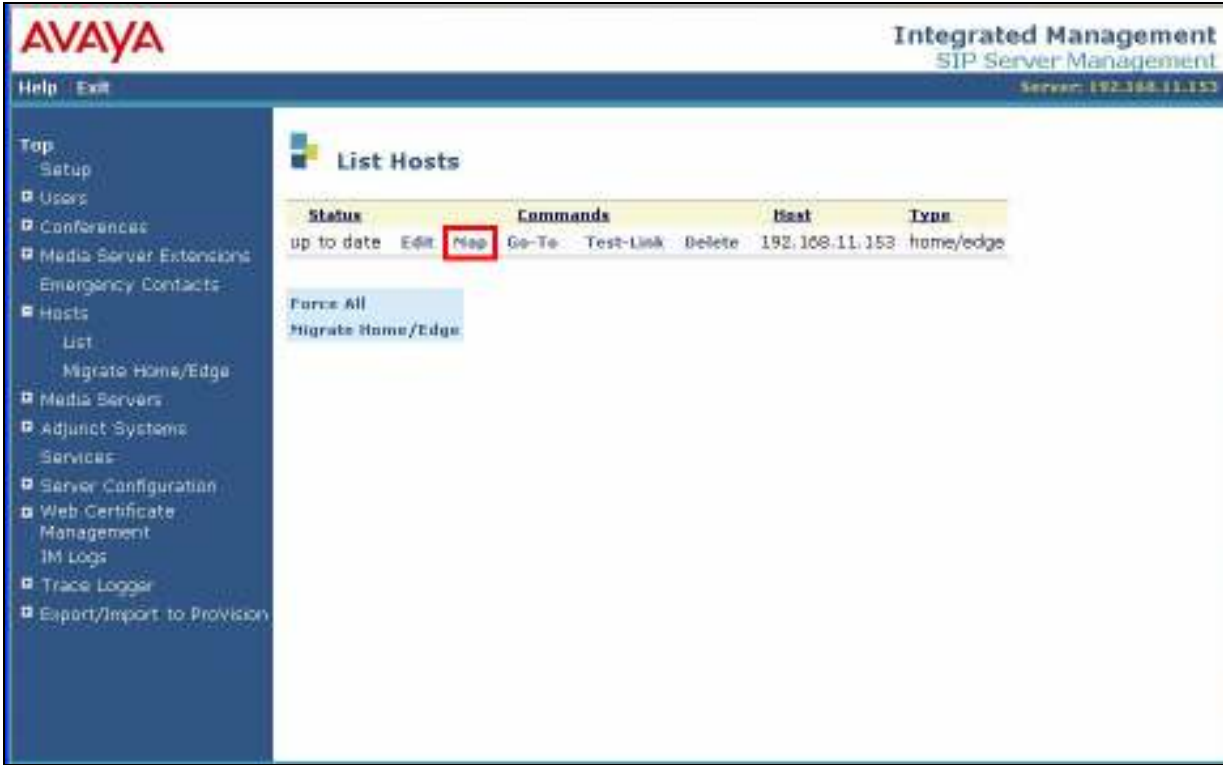
Title:


Step	Description
3.1.8b	<p>Provision settings for a user account as displayed and click Save.</p> 

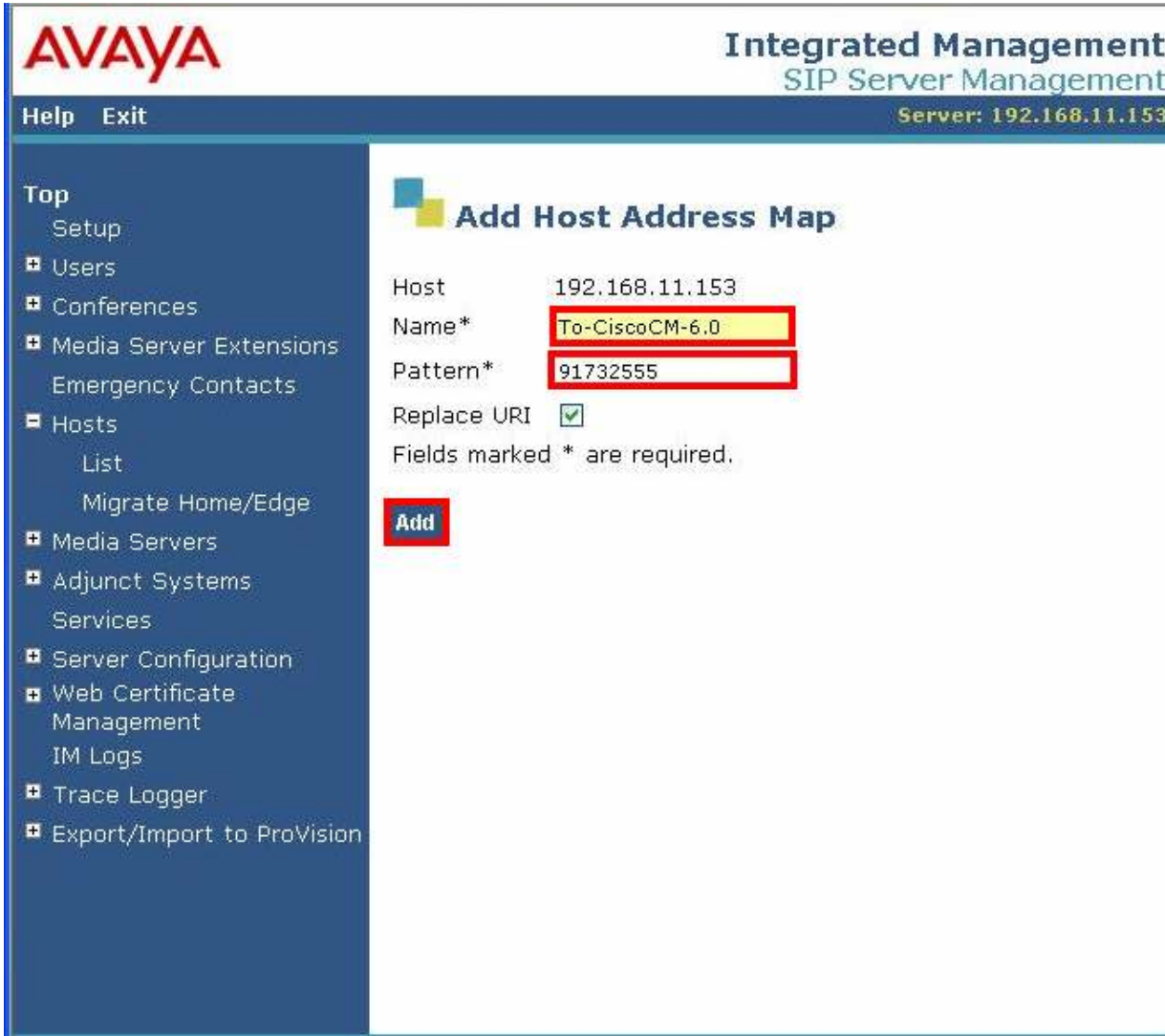
3.2. Configure Avaya SIP Enablement Services


This section describes the steps for configuring call routing between Avaya CPM and endpoints registered to Cisco UCM via Avaya SIP Enablement Services. Avaya SIP Enablement Services is administered over a secure connection by entering **https://<Avaya SIP Enablement Services IP Address or FQDN>/admin** into a web browser's URL bar.

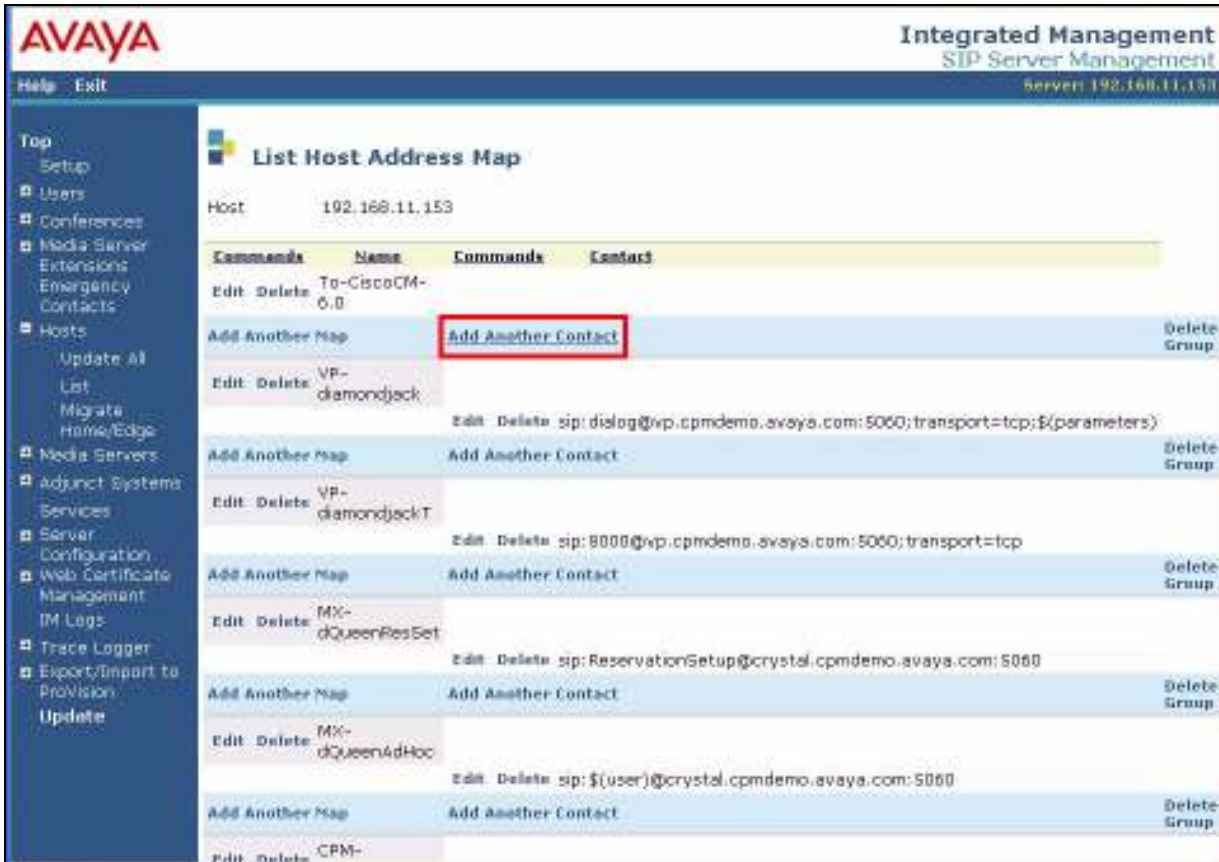
- **Steps 3.2.1 - 3.2.6** describe the provisioning of call routing from Avaya CPM to endpoints registered to Cisco UCM via Avaya SIP Enablement Services. This enables the web services (see **Section 1**) delivery to endpoints registered to Cisco UCM.
- **Steps 3.2.7 - 3.2.9** describe the provisioning of call routing from endpoints registered to Cisco UCM to Avaya CPM via Avaya SIP Enablement Services. This enables the dial-in services for endpoints registered to Cisco UCM.

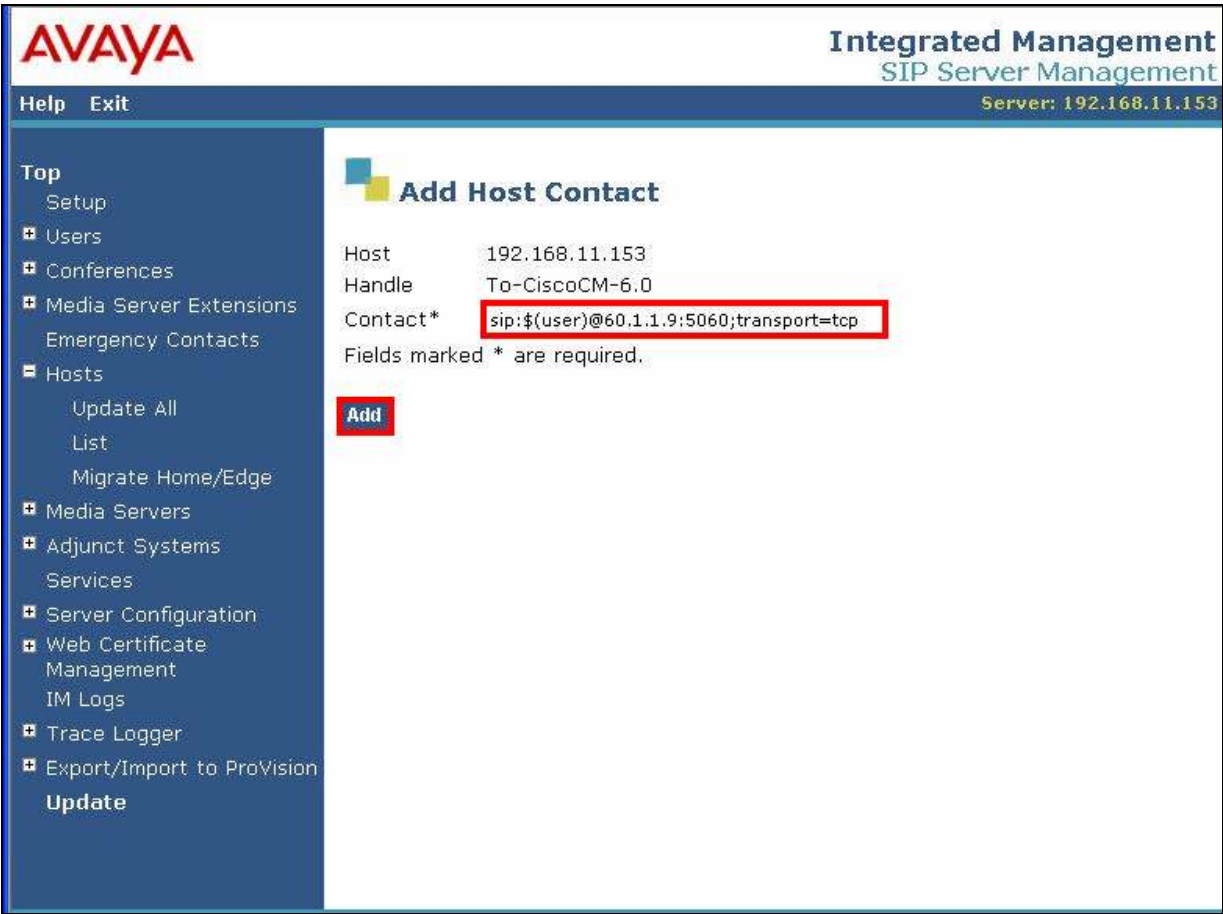
Step	Description
3.2.1	<p>To enable call routing from Avaya CPM to endpoints registered to Cisco UCM via Avaya SIP Enablement Services, add a host Map as follows. From the Administration Web Interface:</p> <ul style="list-style-type: none"> • Click Hosts → List. • From the List Hosts, click Map. 

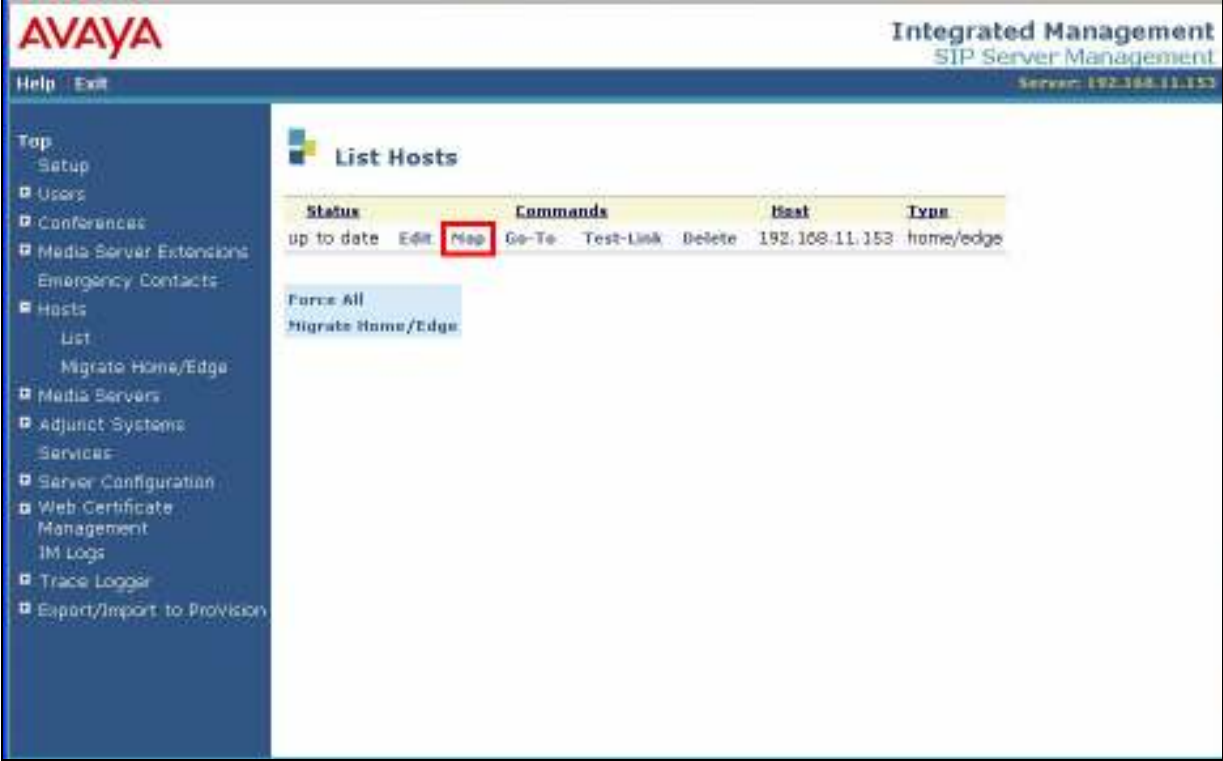
Step	Description
3.2.2	<p>From the List Host Address Map page, click Add Map In New Group.</p> 

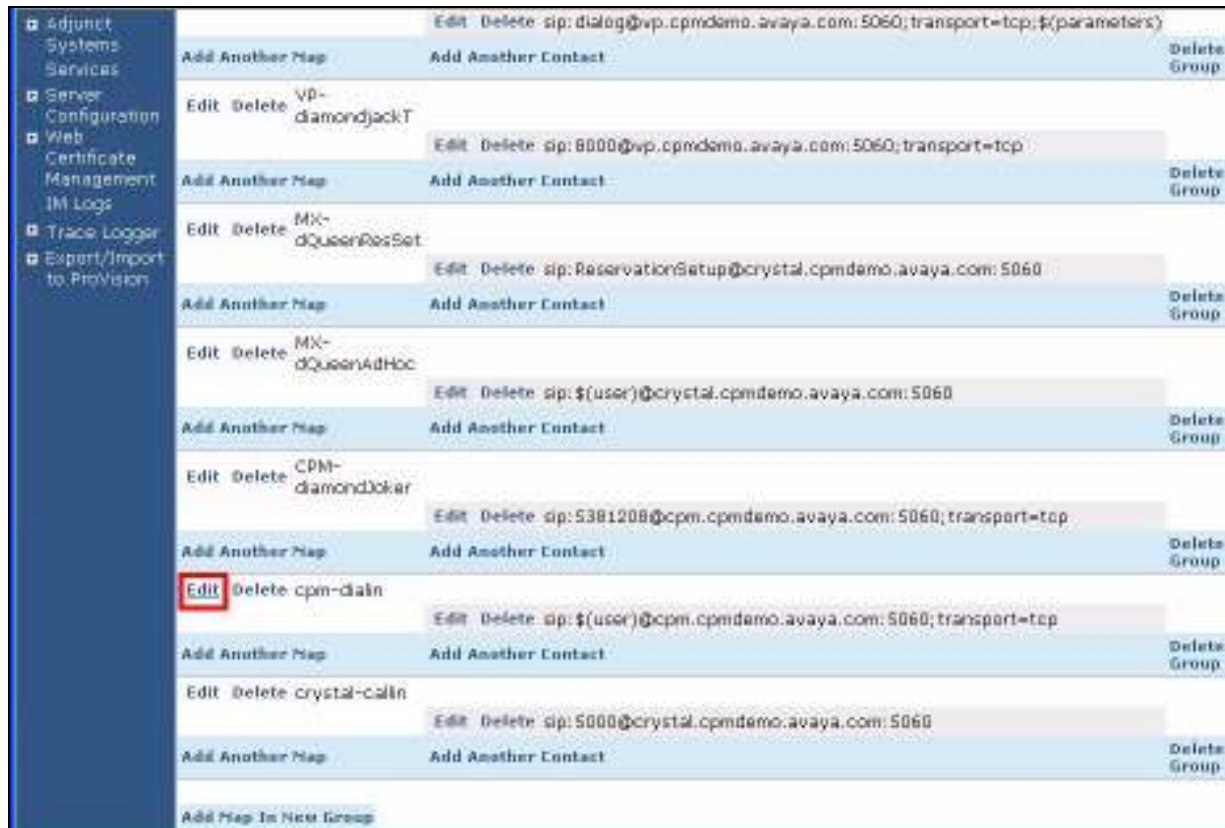
Step	Description
3.2.3	<p data-bbox="293 268 1505 342">From the Add Host Address Map page, provision as displayed. For this sample configuration, the Pattern field corresponds to endpoints registered to Cisco UCM.</p> <div data-bbox="293 373 1505 1451">  <p>The screenshot displays the 'Add Host Address Map' configuration page in the Avaya Integrated Management SIP Server Management interface. The page header includes the Avaya logo and the title 'Integrated Management SIP Server Management' with the server address '192.168.11.153'. A sidebar on the left provides navigation options such as 'Top', 'Setup', 'Users', 'Conferences', 'Media Server Extensions', 'Emergency Contacts', 'Hosts', 'List', 'Migrate Home/Edge', 'Media Servers', 'Adjunct Systems', 'Services', 'Server Configuration', 'Web Certificate Management', 'IM Logs', 'Trace Logger', and 'Export/Import to ProVision'. The main configuration area contains the following fields:</p> <ul style="list-style-type: none"> Host: 192.168.11.153 Name*: To-CiscoCM-6.0 Pattern*: 91732555 Replace URI: <input checked="" type="checkbox"/> <p>A note states 'Fields marked * are required.' and an 'Add' button is located at the bottom of the form.</p> </div>

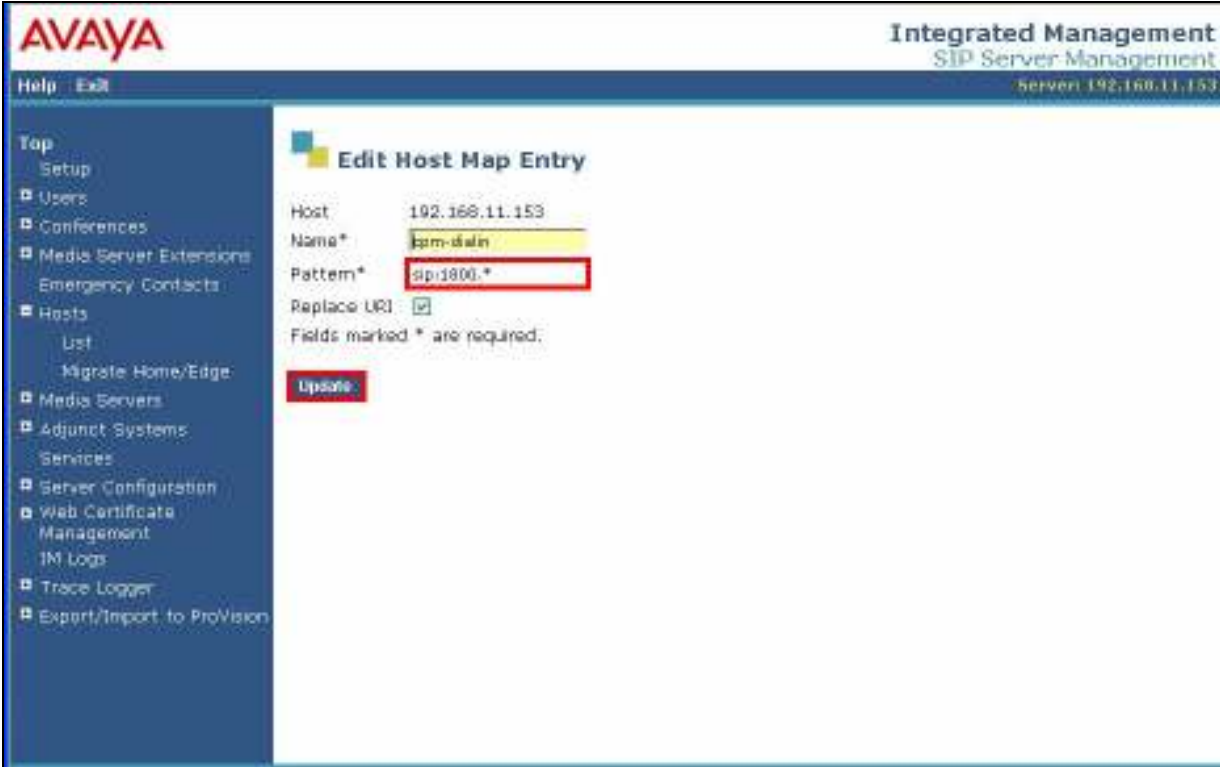
Step	Description
3.2.4	<p>Click Continue.</p>  <p>The screenshot shows the Avaya Integrated Management SIP Server Management web interface. The top header includes the Avaya logo and the title 'Integrated Management SIP Server Management' with the server address 'Server: 192.168.11.153'. A sidebar menu on the left contains various navigation options. The main content area displays a message: 'Host address map To-CiscoCM-6.0 added.' with a 'Continue' button highlighted by a red rectangle.</p>

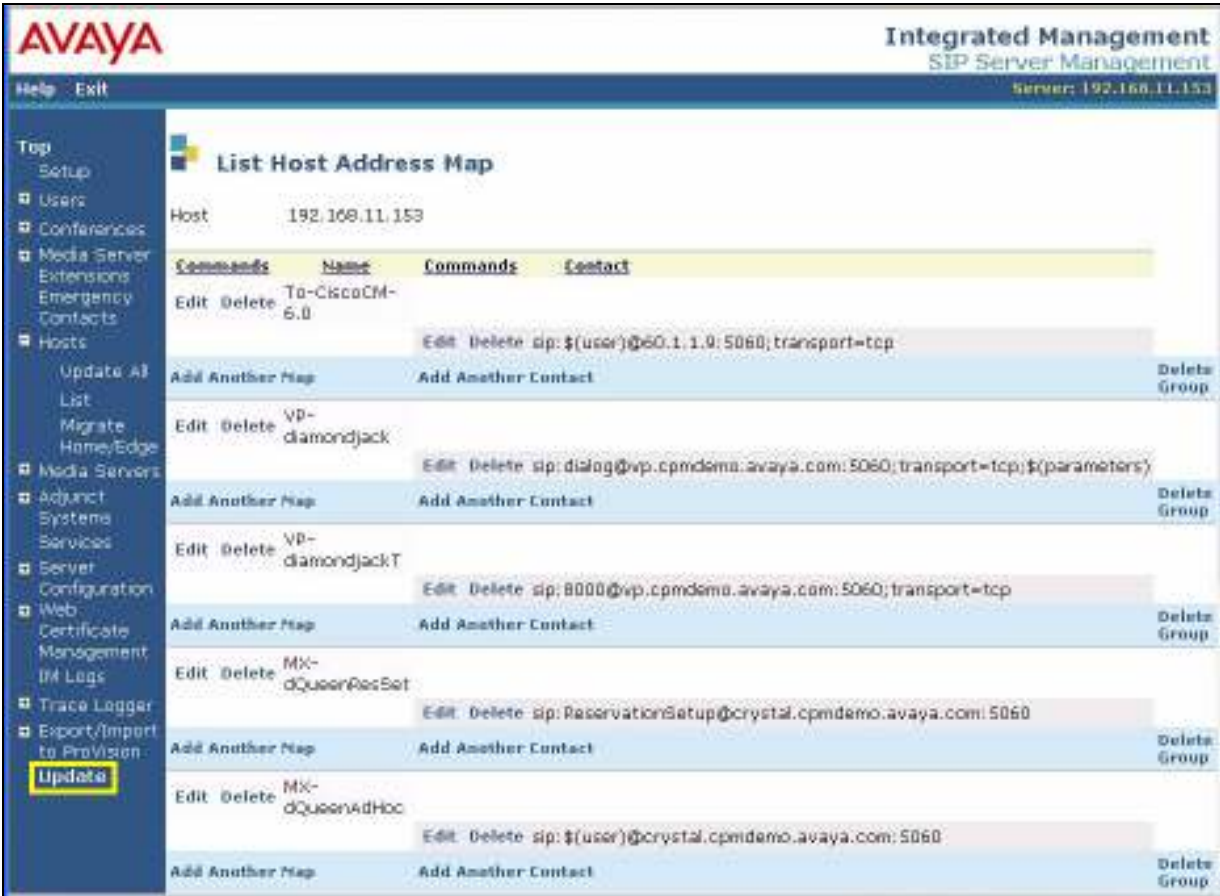
Step	Description
3.2.5	<p>From the List Host Address Map page, specify routing information for the Host Address Map defined in Step 3.2.3. Click Add Another Contact.</p>  <p>The screenshot shows the Avaya Integrated Management SIP Server Management interface. The page title is "List Host Address Map". The host is 192.168.11.153. The interface displays a table with columns: Commands, Name, Commands, and Contact. The table contains several rows of contact information, including "To-CiscoCM-6.0", "VP-diamondjack", "VP-diamondjackT", "MX-dQueenResSet", "MX-dQueenAdHoc", and "CPM-". The "Add Another Contact" button is highlighted with a red box.</p>


Step	Description
3.2.6	<p>From the Add Host Contact page, provision as displayed. The Contact field corresponds to a SIP-URI.</p> <ul style="list-style-type: none"> To enable SIP connectivity via TCP to Cisco UCM, enter sip:\$(user)@60.1.1.9:5060;transport=tcp in the Contact field. <i>Note: The hostport and transport-param are consistent with the SIP configuration for Cisco UCM defined in Step 4.1.1. Avaya SIP Enablement Services substitutes “\$(user)” with the “User” Field obtained from the originating Request-URI. To enable SIP connectivity over UDP, set the transport-param in the SIP-URI to udp.</i> Click Add. [<i>Not Shown</i>] Click Continue on the confirmation page. 

Step	Description
3.2.7	<p>To enable call routing from endpoints registered to Cisco UCM to Avaya CPM via Avaya SIP Enablement Services, add a host Map as follows. From the Administration Web Interface:</p> <ul style="list-style-type: none"> Click Hosts → List. From the List Hosts, click Map.
	

Step	Description																																										
3.2.8	<p>From the List Host Address Map page, locate the entry for used for dial-in services and click Edit.</p>  <p>The screenshot shows a web interface with a left-hand navigation menu and a main content area. The navigation menu includes options like 'Adjunct Systems Services', 'Server Configuration', 'Web', 'Certificate Management', 'IM Logs', 'Trace Logger', and 'Expert/Import to Provision'. The main content area displays a table of host address maps. Each row in the table has three columns: a set of links ('Edit', 'Delete'), a host address map name, and another set of links ('Edit', 'Delete'). The 'cpm-dialin' entry is highlighted, and its 'Edit' link is enclosed in a red rectangular box.</p> <table><tr><th>Links</th><th>Host Address Map</th><th>Links</th></tr><tr><td>Edit Delete</td><td>vp-diamondjackT</td><td>Edit Delete</td></tr><tr><td>Add Another Map</td><td>Add Another Contact</td><td>Delete Group</td></tr><tr><td>Edit Delete</td><td>MX-dQueenResSet</td><td>Edit Delete</td></tr><tr><td>Add Another Map</td><td>Add Another Contact</td><td>Delete Group</td></tr><tr><td>Edit Delete</td><td>MX-dQueenAdHoc</td><td>Edit Delete</td></tr><tr><td>Add Another Map</td><td>Add Another Contact</td><td>Delete Group</td></tr><tr><td>Edit Delete</td><td>CPM-diamondDoker</td><td>Edit Delete</td></tr><tr><td>Add Another Map</td><td>Add Another Contact</td><td>Delete Group</td></tr><tr><td>Edit Delete</td><td>cpm-dialin</td><td>Edit Delete</td></tr><tr><td>Add Another Map</td><td>Add Another Contact</td><td>Delete Group</td></tr><tr><td>Edit Delete</td><td>crystal-callin</td><td>Edit Delete</td></tr><tr><td>Add Another Map</td><td>Add Another Contact</td><td>Delete Group</td></tr><tr><td colspan="3">Add Map To Next Group</td></tr></table>	Links	Host Address Map	Links	Edit Delete	vp-diamondjackT	Edit Delete	Add Another Map	Add Another Contact	Delete Group	Edit Delete	MX-dQueenResSet	Edit Delete	Add Another Map	Add Another Contact	Delete Group	Edit Delete	MX-dQueenAdHoc	Edit Delete	Add Another Map	Add Another Contact	Delete Group	Edit Delete	CPM-diamondDoker	Edit Delete	Add Another Map	Add Another Contact	Delete Group	Edit Delete	cpm-dialin	Edit Delete	Add Another Map	Add Another Contact	Delete Group	Edit Delete	crystal-callin	Edit Delete	Add Another Map	Add Another Contact	Delete Group	Add Map To Next Group		
Links	Host Address Map	Links																																									
Edit Delete	vp-diamondjackT	Edit Delete																																									
Add Another Map	Add Another Contact	Delete Group																																									
Edit Delete	MX-dQueenResSet	Edit Delete																																									
Add Another Map	Add Another Contact	Delete Group																																									
Edit Delete	MX-dQueenAdHoc	Edit Delete																																									
Add Another Map	Add Another Contact	Delete Group																																									
Edit Delete	CPM-diamondDoker	Edit Delete																																									
Add Another Map	Add Another Contact	Delete Group																																									
Edit Delete	cpm-dialin	Edit Delete																																									
Add Another Map	Add Another Contact	Delete Group																																									
Edit Delete	crystal-callin	Edit Delete																																									
Add Another Map	Add Another Contact	Delete Group																																									
Add Map To Next Group																																											

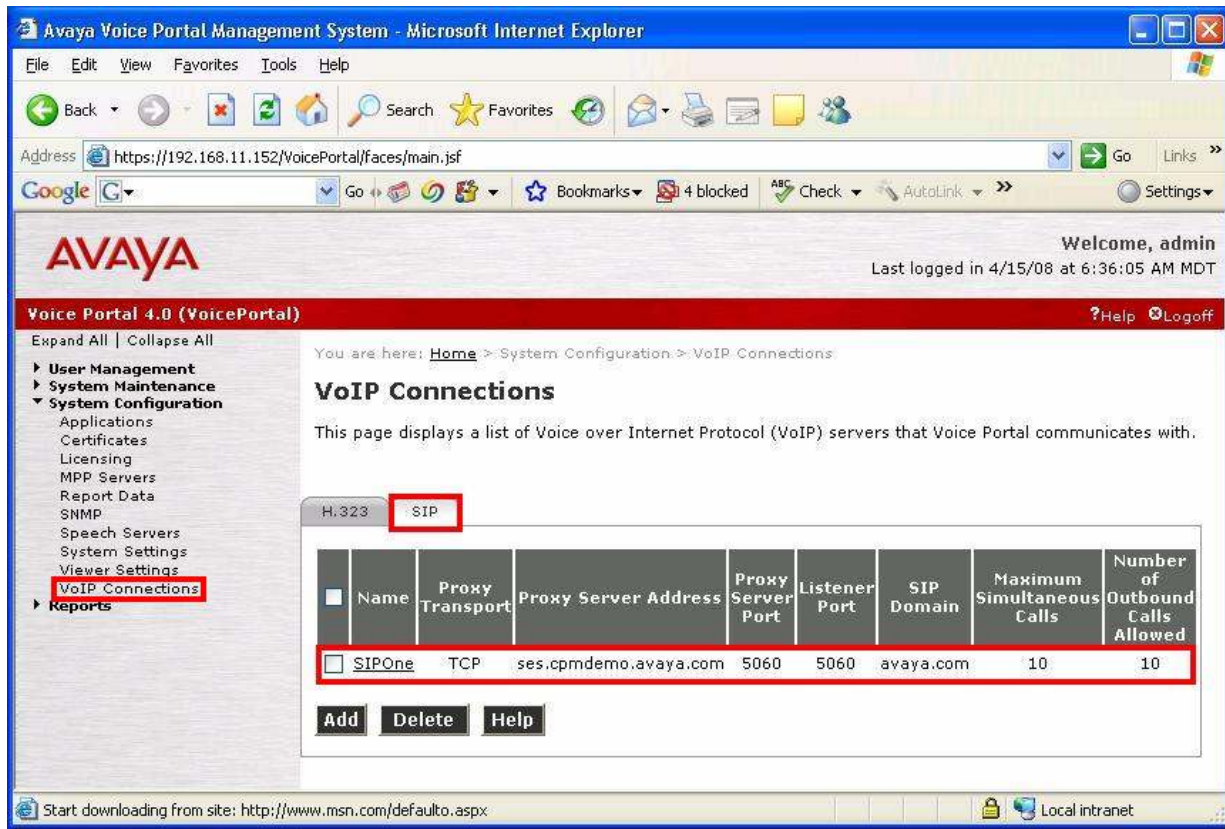
Step	Description
3.2.9	<p>From the Edit Host Map Entry page, provision as displayed. For this sample configuration, the Pattern field corresponds to the telephone number dialed from endpoints registered to Cisco UCM. This field also correlates with dial-in services provisioned on Avaya CPM in Steps 3.1.1 - 3.1.3.</p> <ul style="list-style-type: none"> • Click Update. • <i>[Not Shown] Click Continue on the confirmation page.</i> 

Step	Description
3.2.10	<p>To apply the administration in Section 3.2, click on Update on the left side of the page.</p> 

Step	Description						
3.2.11	<p>Add Cisco UCM as a trusted host on Avaya SIP Enablement Services. All SIP user agents, proxies and gateways to which calls can be routed should be administered as trusted hosts on Avaya SIP Enablement Services. This permits call setup and termination by remote parties to be handled without authentication challenges. Trusted hosts are provisioned at the Avaya SIP Enablement Services command line of the edge, or home/edge server.</p> <ul style="list-style-type: none">Log in to the Avaya SIP Enablement Services console with the appropriate credentials.Add Cisco UCM as a trusted host by entering the following command: trustedhost -a <trusted host IP address> -n <trusting SES IP address> [-c <comment text>]. <pre>SES> trustedhost -a 60.1.1.9 -n 192.168.11.153 -c Cisco_CM_6.0</pre>						
3.2.12	<p>Verify trusted host entries by entering the following command: trustedhost -L.</p> <pre>SES> trustedhost -L</pre> <p>Third party trusted hosts.</p> <table><thead><tr><th>Trusted Host</th><th>CCS Host Name</th><th>Comment</th></tr></thead><tbody><tr><td>60.1.1.9</td><td>192.168.11.153</td><td>Cisco_CM_6.0</td></tr></tbody></table>	Trusted Host	CCS Host Name	Comment	60.1.1.9	192.168.11.153	Cisco_CM_6.0
Trusted Host	CCS Host Name	Comment					
60.1.1.9	192.168.11.153	Cisco_CM_6.0					
3.2.13	<p>To apply the administration defined in Step 3.2.11, click on Update on the left side of the page on the web browser interface.</p> <div></div>						

3.3. Configure Avaya Voice Portal

This section describes the steps for configuring Avaya Voice Portal to interoperate with Avaya CPM via Avaya SIP Enablement Services. Avaya Voice Portal is administered via the Voice Portal Management System (VPMS) over a secure connection by entering **https://<Avaya Voice Portal IP Address or FQDN>/VoicePortal** into a web browser's URL bar.

Step	Description																
3.3.1	<p>From the Avaya Voice Portal VPMS interface, verify settings to enable SIP connectivity with Avaya SIP Enablement Services as follows:</p> <ul style="list-style-type: none">Click System Configuration → VoIP Connections.From the SIP tab on the VoIP Connections page, verify the configuration of the entry corresponding to Avaya SIP Enablement Services. <p><i>Note: It is assumed that Avaya CPM is provisioned to communicate with Avaya communication resources, e.g., Avaya Voice Portal, Avaya Meeting Exchange and Avaya SIP Enablement Services. Refer to [1] and [2] for additional information regarding the administration of connectivity between Avaya CPM and Avaya communication resources.</i></p>  <p>The screenshot shows the Avaya Voice Portal Management System interface in a Microsoft Internet Explorer browser. The address bar shows the URL: https://192.168.11.152/VoicePortal/faces/main.jsf. The page title is "Avaya Voice Portal Management System - Microsoft Internet Explorer". The page content includes a navigation menu on the left with "System Configuration" expanded, and "VoIP Connections" selected. The main content area shows the "VoIP Connections" page with a table of VoIP servers. The table has columns: Name, Proxy Transport, Proxy Server Address, Proxy Server Port, Listener Port, SIP Domain, Maximum Simultaneous Calls, and Number of Outbound Calls Allowed. A row is highlighted with a red border, showing the configuration for "SIPOne" with a proxy server address of "ses.cpmdemo.avaya.com" and a maximum of 10 simultaneous calls.</p> <table><tr><th>Name</th><th>Proxy Transport</th><th>Proxy Server Address</th><th>Proxy Server Port</th><th>Listener Port</th><th>SIP Domain</th><th>Maximum Simultaneous Calls</th><th>Number of Outbound Calls Allowed</th></tr><tr><td>SIPOne</td><td>TCP</td><td>ses.cpmdemo.avaya.com</td><td>5060</td><td>5060</td><td>avaya.com</td><td>10</td><td>10</td></tr></table>	Name	Proxy Transport	Proxy Server Address	Proxy Server Port	Listener Port	SIP Domain	Maximum Simultaneous Calls	Number of Outbound Calls Allowed	SIPOne	TCP	ses.cpmdemo.avaya.com	5060	5060	avaya.com	10	10
Name	Proxy Transport	Proxy Server Address	Proxy Server Port	Listener Port	SIP Domain	Maximum Simultaneous Calls	Number of Outbound Calls Allowed										
SIPOne	TCP	ses.cpmdemo.avaya.com	5060	5060	avaya.com	10	10										

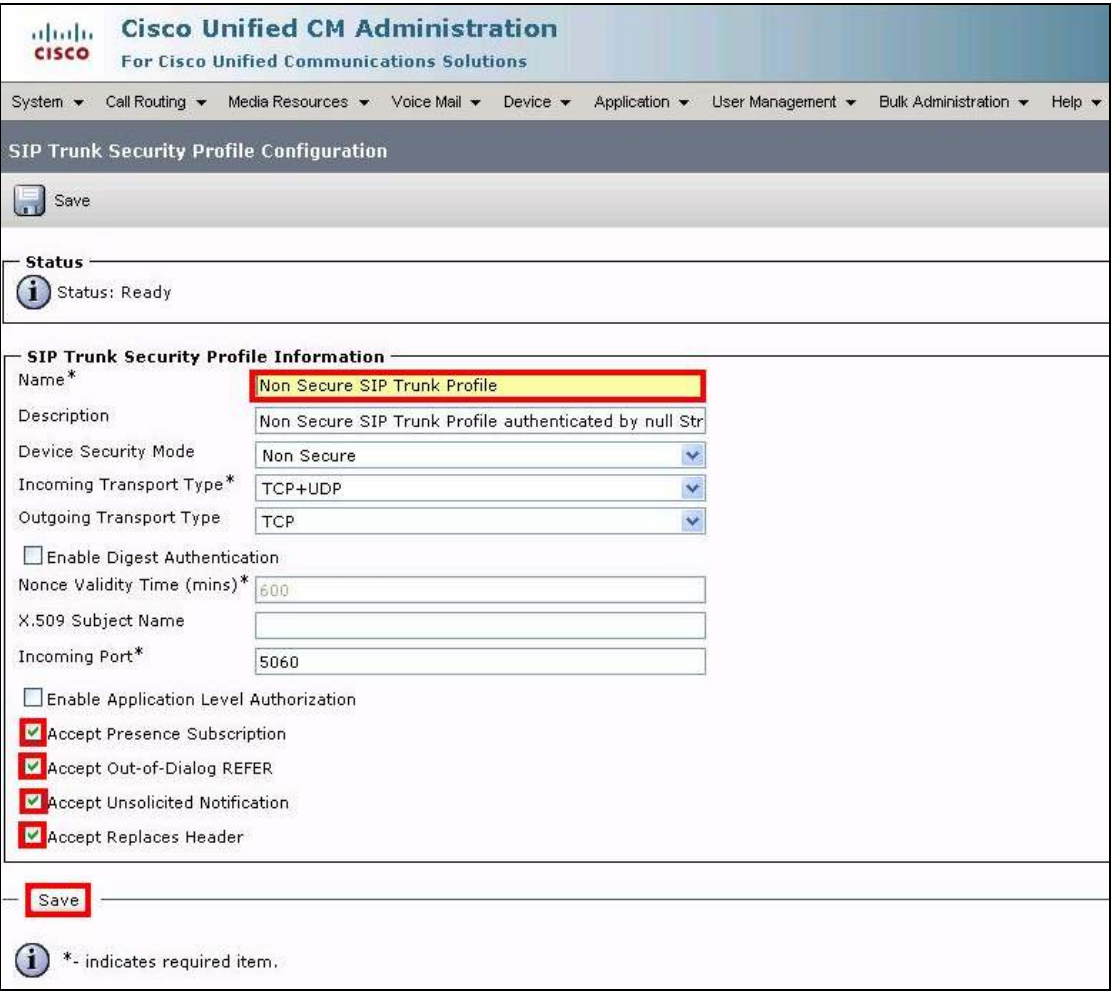
4. Cisco Unified Communications Manager Configuration


This section describes the configuration for enabling Cisco UCM to interoperate with Avaya CPM. Cisco UCM is administered and maintained using a standard web browser over a secure connection by entering **https://<Cisco UCM IP Address or FQDN>** into the web browser's URL bar. Refer to [3] for additional information regarding the administration of Cisco UCM.

- **Section 4.1** describes the provisioning of SIP connectivity utilizing TCP between Cisco UCM and Avaya CPM via Avaya SIP Enablement Services. This enables call origination/termination between endpoints registered to Cisco UCM and Avaya CPM,
- **Section 4.2** describes the provisioning of SIP connectivity utilizing TCP between Cisco UCM and Avaya Meeting Exchange. This enables Cisco UCM to properly handle the web services that utilize the SIP REFER method to access Avaya Meeting Exchange:
 - Find and Call
 - Notify and Conference


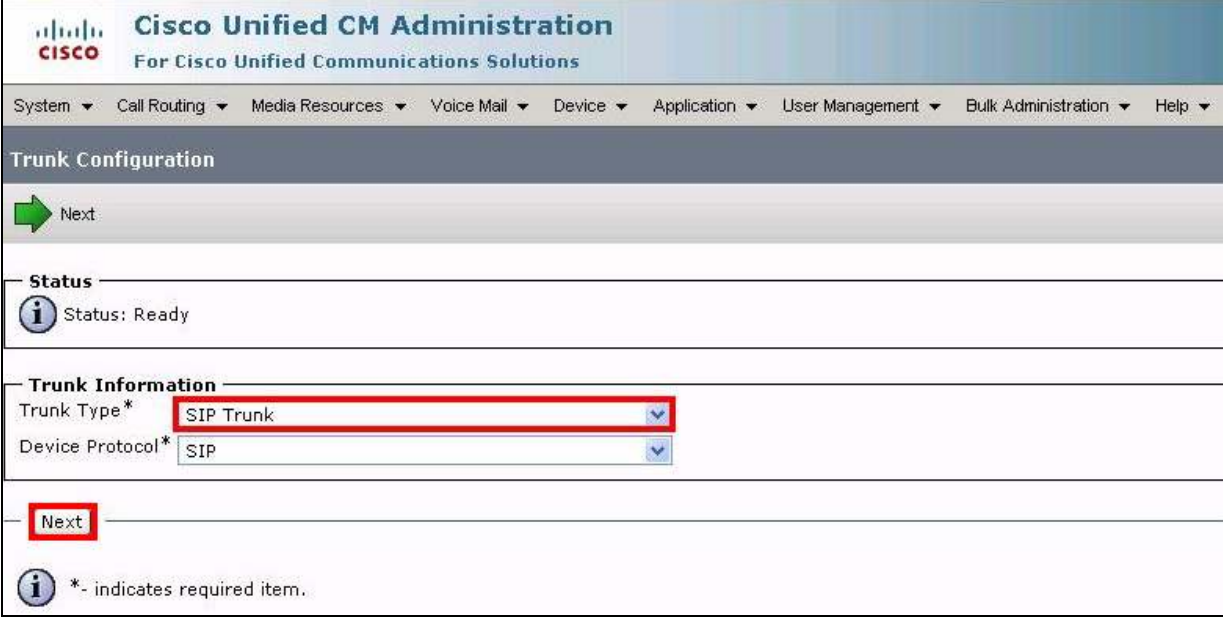
4.1. Configure Connectivity to Avaya SIP Enablement Services

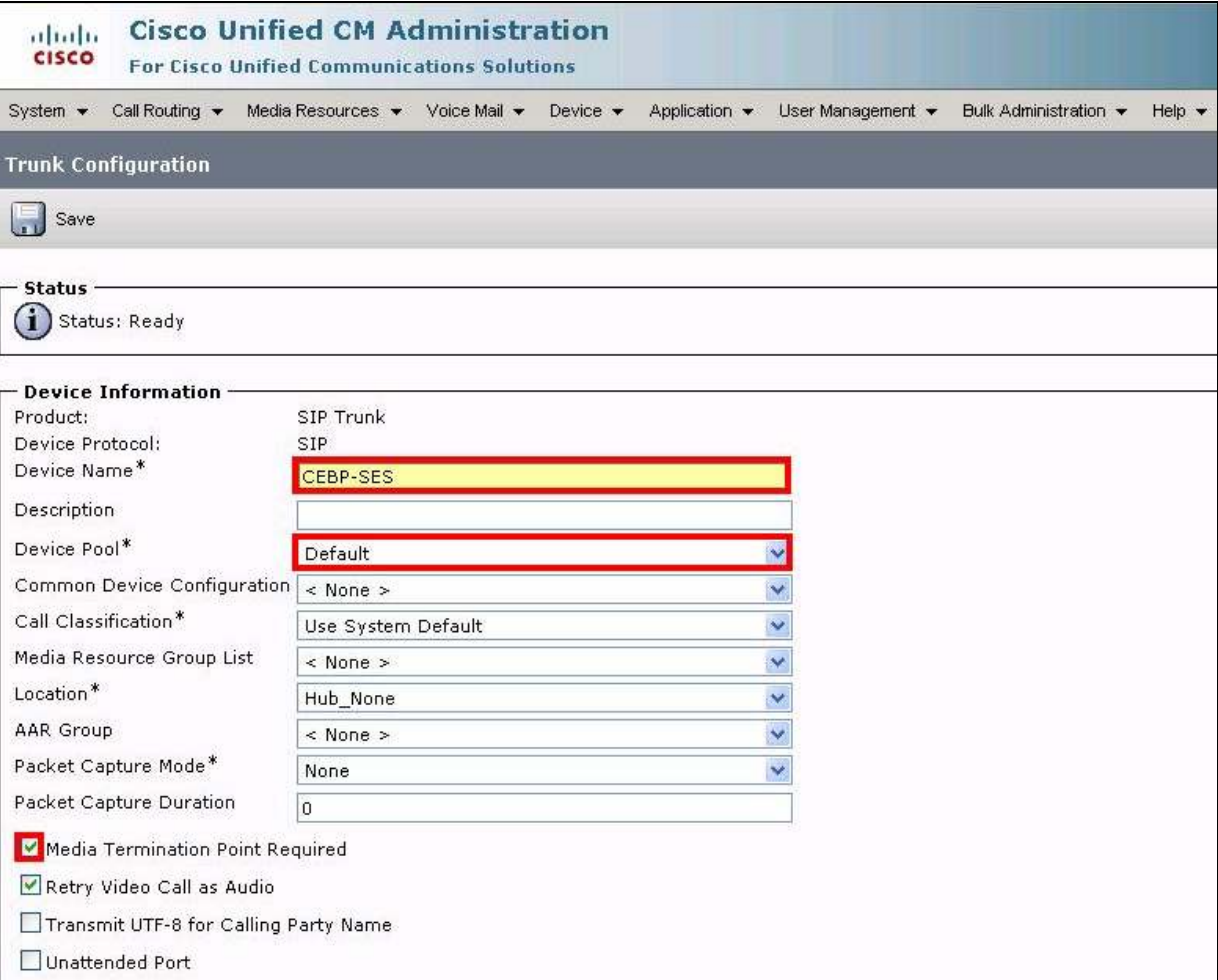
This section describes the steps for configuring SIP connectivity between Cisco UCM and Avaya CPM via Avaya SIP Enablement Services.

Step	Description
4.1.1	<p>To enable SIP connectivity with Avaya CPM via Avaya SIP Enablement Services utilizing TCP, configure a SIP Trunk Security Profile as follows:</p> <ul style="list-style-type: none">From the Cisco UCM main menu, select System → Security Profile → SIP Trunk Security Profile.[<i>Not Shown</i>] Click Add New to create a new SIP Trunk Security Profile.Provision settings as displayed and click Save. <p><i>Note:</i> To enable SIP connectivity to with Avaya CPM via Avaya SIP Enablement Services utilizing UDP, set the Outgoing Transport Type field to UDP.</p> 

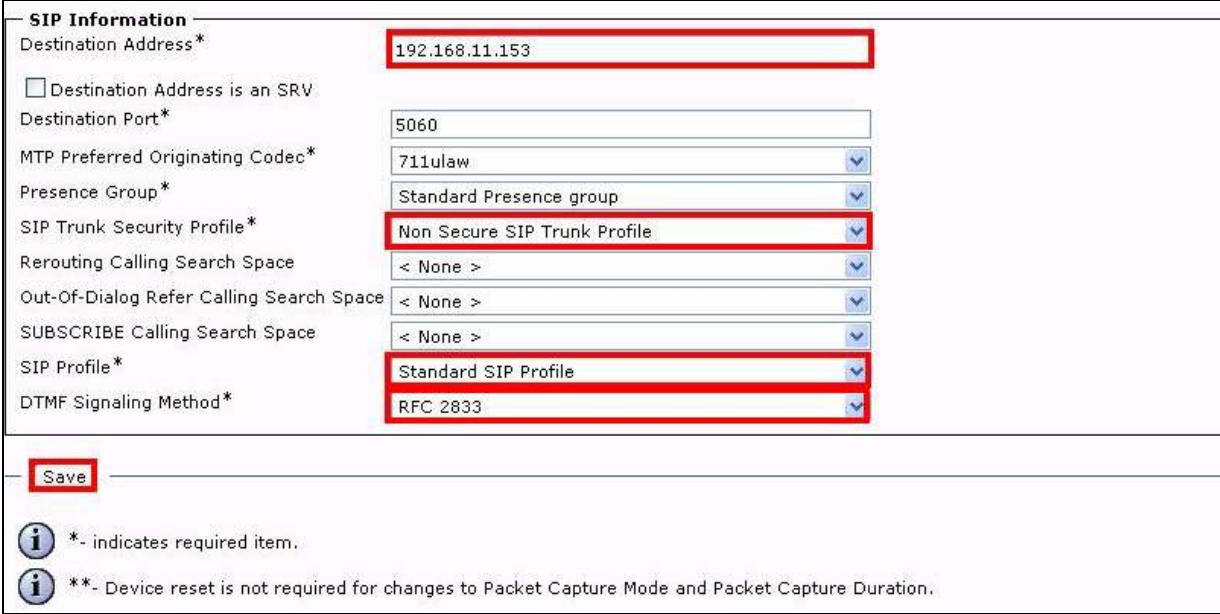


Step	Description
4.1.2a	<p>To enable SIP connectivity with Avaya CPM via Avaya SIP Enablement Services, configure a SIP Profile as follows:</p> <ul style="list-style-type: none"> From the Cisco UCM main menu, select Device → Device Settings → SIP Profile. [<i>Not Shown</i>] Click Add New to create a new SIP Profile. Provision settings under SIP Profile Information as displayed and scroll down. 

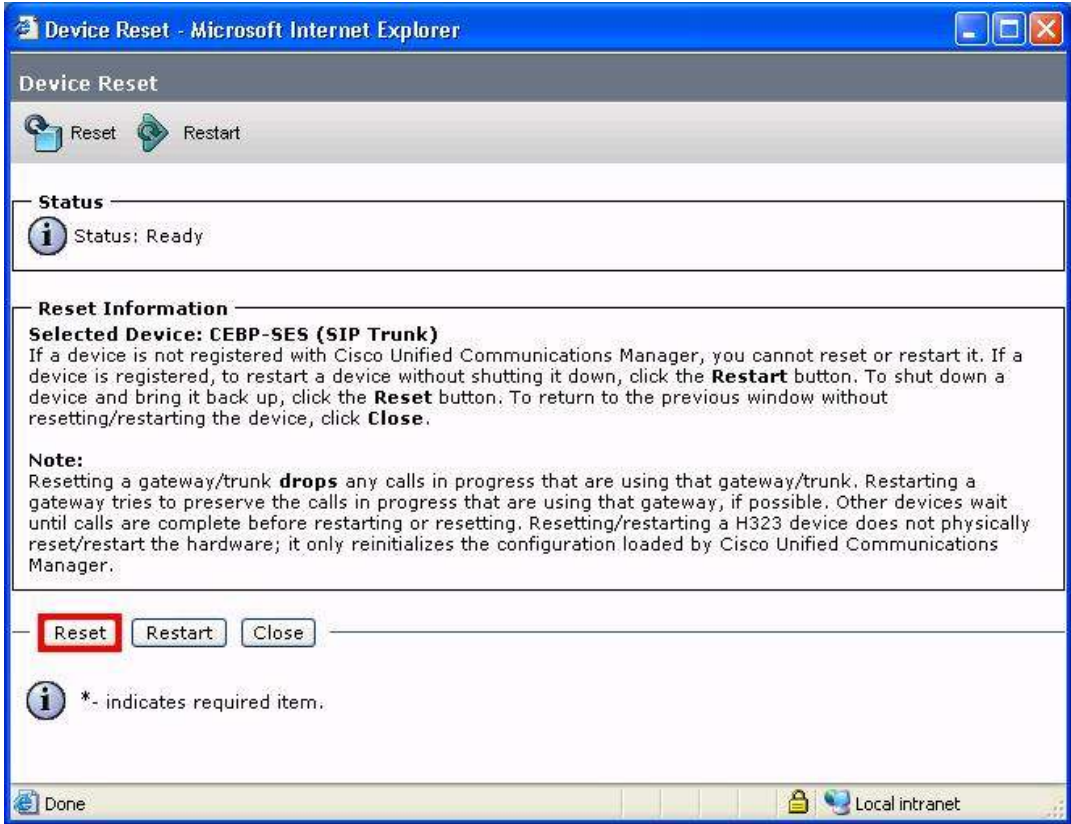
Step	Description																																																						
4.1.2b	<p>Use default settings under Parameters used in Phone as displayed and click Save.</p> <div> <p>Parameters used in Phone</p> <table> <tr><td>Timer Invite Expires (seconds)*</td><td>180</td></tr> <tr><td>Timer Register Delta (seconds)*</td><td>5</td></tr> <tr><td>Timer Register Expires (seconds)*</td><td>3600</td></tr> <tr><td>Timer T1 (msec)*</td><td>500</td></tr> <tr><td>Timer T2 (msec)*</td><td>4000</td></tr> <tr><td>Retry INVITE*</td><td>6</td></tr> <tr><td>Retry Non-INVITE*</td><td>10</td></tr> <tr><td>Start Media Port*</td><td>16384</td></tr> <tr><td>Stop Media Port*</td><td>32766</td></tr> <tr><td>Call Pickup URI*</td><td>x-cisco-serviceuri-pickup</td></tr> <tr><td>Call Pickup Group Other URI*</td><td>x-cisco-serviceuri-opickup</td></tr> <tr><td>Call Pickup Group URI*</td><td>x-cisco-serviceuri-gpickup</td></tr> <tr><td>Meet Me Service URI*</td><td>x-cisco-serviceuri-meetme</td></tr> <tr><td>User Info*</td><td>None</td></tr> <tr><td>DTMF DB Level*</td><td>Nominal</td></tr> <tr><td>Call Hold Ring Back*</td><td>Off</td></tr> <tr><td>Anonymous Call Block*</td><td>Off</td></tr> <tr><td>Caller ID Blocking*</td><td>Off</td></tr> <tr><td>Do Not Disturb Control*</td><td>User</td></tr> <tr><td>Telnet Level for 7940 and 7960*</td><td>Disabled</td></tr> <tr><td>Timer Keep Alive Expires (seconds)*</td><td>120</td></tr> <tr><td>Timer Subscribe Expires (seconds)*</td><td>120</td></tr> <tr><td>Timer Subscribe Delta (seconds)*</td><td>5</td></tr> <tr><td>Maximum Redirections*</td><td>70</td></tr> <tr><td>Off Hook To First Digit Timer (milliseconds)*</td><td>15000</td></tr> <tr><td>Call Forward URI*</td><td>x-cisco-serviceuri-cfwdall</td></tr> <tr><td>Abbreviated Dial URI*</td><td>x-cisco-serviceuri-abbrdial</td></tr> </table> <p> <input checked="" type="checkbox"/> Conference Join Enabled <input type="checkbox"/> RFC 2543 Hold <input checked="" type="checkbox"/> Semi Attended Transfer <input type="checkbox"/> Enable VAD <input type="checkbox"/> Stutter Message Waiting <input type="checkbox"/> Call Stats </p> <p>Save</p> <p> *- indicates required item.</p> </div>	Timer Invite Expires (seconds)*	180	Timer Register Delta (seconds)*	5	Timer Register Expires (seconds)*	3600	Timer T1 (msec)*	500	Timer T2 (msec)*	4000	Retry INVITE*	6	Retry Non-INVITE*	10	Start Media Port*	16384	Stop Media Port*	32766	Call Pickup URI*	x-cisco-serviceuri-pickup	Call Pickup Group Other URI*	x-cisco-serviceuri-opickup	Call Pickup Group URI*	x-cisco-serviceuri-gpickup	Meet Me Service URI*	x-cisco-serviceuri-meetme	User Info*	None	DTMF DB Level*	Nominal	Call Hold Ring Back*	Off	Anonymous Call Block*	Off	Caller ID Blocking*	Off	Do Not Disturb Control*	User	Telnet Level for 7940 and 7960*	Disabled	Timer Keep Alive Expires (seconds)*	120	Timer Subscribe Expires (seconds)*	120	Timer Subscribe Delta (seconds)*	5	Maximum Redirections*	70	Off Hook To First Digit Timer (milliseconds)*	15000	Call Forward URI*	x-cisco-serviceuri-cfwdall	Abbreviated Dial URI*	x-cisco-serviceuri-abbrdial
Timer Invite Expires (seconds)*	180																																																						
Timer Register Delta (seconds)*	5																																																						
Timer Register Expires (seconds)*	3600																																																						
Timer T1 (msec)*	500																																																						
Timer T2 (msec)*	4000																																																						
Retry INVITE*	6																																																						
Retry Non-INVITE*	10																																																						
Start Media Port*	16384																																																						
Stop Media Port*	32766																																																						
Call Pickup URI*	x-cisco-serviceuri-pickup																																																						
Call Pickup Group Other URI*	x-cisco-serviceuri-opickup																																																						
Call Pickup Group URI*	x-cisco-serviceuri-gpickup																																																						
Meet Me Service URI*	x-cisco-serviceuri-meetme																																																						
User Info*	None																																																						
DTMF DB Level*	Nominal																																																						
Call Hold Ring Back*	Off																																																						
Anonymous Call Block*	Off																																																						
Caller ID Blocking*	Off																																																						
Do Not Disturb Control*	User																																																						
Telnet Level for 7940 and 7960*	Disabled																																																						
Timer Keep Alive Expires (seconds)*	120																																																						
Timer Subscribe Expires (seconds)*	120																																																						
Timer Subscribe Delta (seconds)*	5																																																						
Maximum Redirections*	70																																																						
Off Hook To First Digit Timer (milliseconds)*	15000																																																						
Call Forward URI*	x-cisco-serviceuri-cfwdall																																																						
Abbreviated Dial URI*	x-cisco-serviceuri-abbrdial																																																						

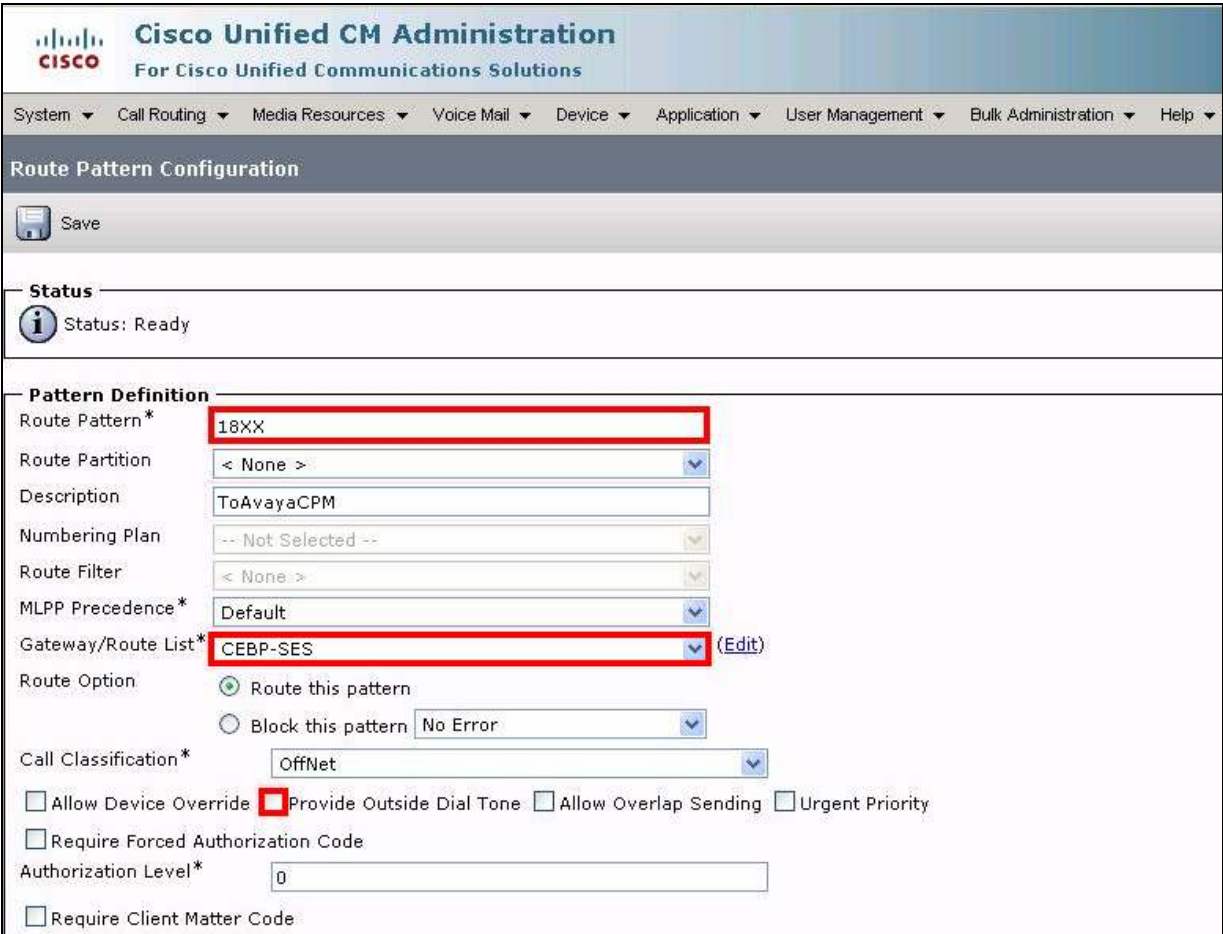
Step	Description
4.1.3	<p>To enable SIP connectivity with Avaya CPM via Avaya SIP Enablement Services, configure a SIP Trunk as follows:</p> <ul style="list-style-type: none"> From the Cisco UCM main menu, select Device → Trunk. Click Add New to create a new SIP Trunk. 
4.1.4	<p>Select SIP Trunk from the drop-down list for the Trunk Type field. Accept the default setting for the Device Protocol field and click Next.</p> 

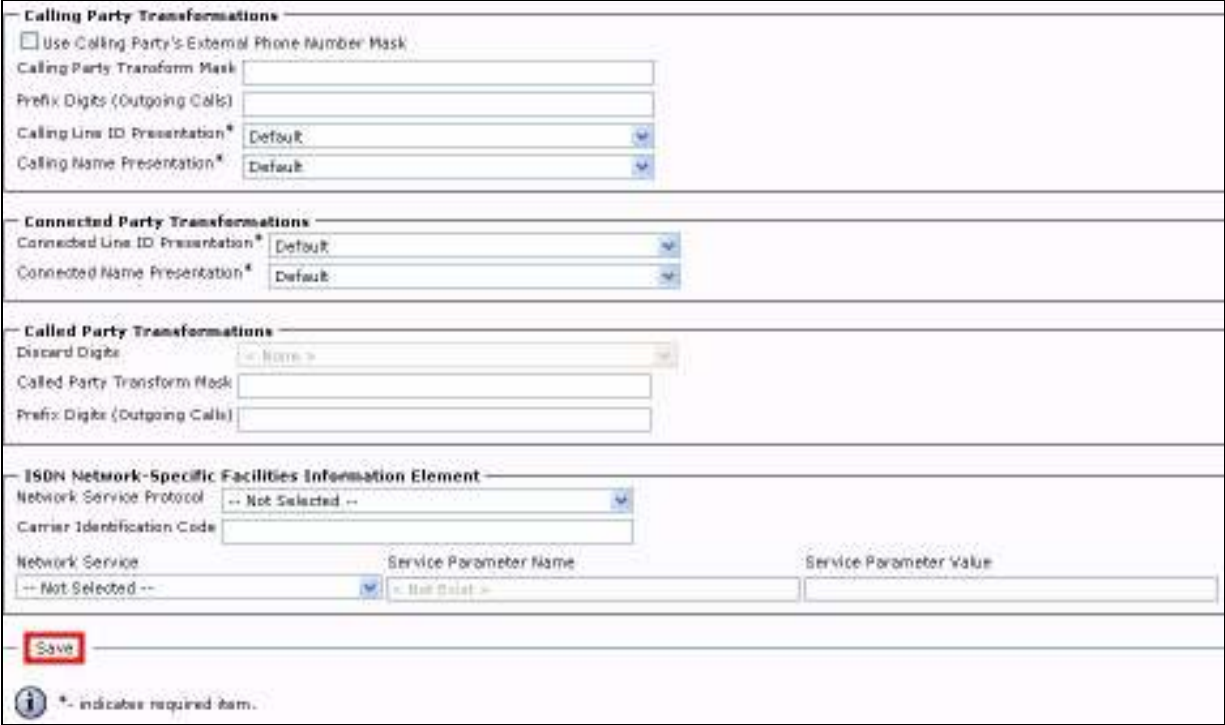
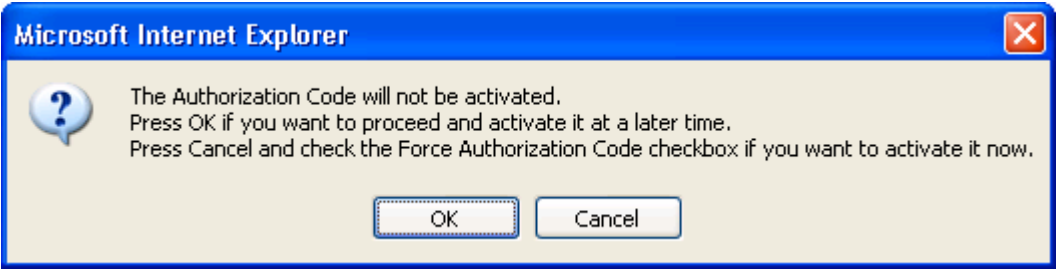
Step	Description
4.1.5a	<p>Provision settings under Device Information as displayed and scroll down. The Location field specifies the total bandwidth that is available for calls between this location and the central location, or hub. Using the default setting Hub_None specifies unlimited available bandwidth.</p> 

Step	Description
4.1.5b	<p>Use default settings as displayed and scroll down.</p> <div data-bbox="297 338 1513 1050"> <div> Multilevel Precedence and Preemption (MLPP) Information </div> <div> MLPP Domain < None > </div> <div> Call Routing Information </div> <div> Inbound Calls </div> <div> <div>Significant Digits*</div> <div>All</div> </div> <div> <div>Connected Line ID Presentation*</div> <div>Default</div> </div> <div> <div>Connected Name Presentation*</div> <div>Default</div> </div> <div> <div>Calling Search Space</div> <div>< None ></div> </div> <div> <div>AAR Calling Search Space</div> <div>< None ></div> </div> <div> <div>Prefix DN</div> <div></div> </div> <div> <input type="checkbox"/> Redirecting Diversion Header Delivery - Inbound </div> <div> Outbound Calls </div> <div> <div>Calling Party Selection*</div> <div>Originator</div> </div> <div> <div>Calling Line ID Presentation*</div> <div>Default</div> </div> <div> <div>Calling Name Presentation*</div> <div>Default</div> </div> <div> <div>Caller ID DN</div> <div></div> </div> <div> <div>Caller Name</div> <div></div> </div> <div> <input type="checkbox"/> Redirecting Diversion Header Delivery - Outbound </div> </div>

Step	Description
4.1.5c	<p>Provision settings under SIP Information as displayed.</p> <ul style="list-style-type: none"> • Enter the IP address of Avaya SIP Enablement Services in the Destination Address field. • Select the SIP Trunk Security Profile provisioned in Step 4.1.1 from the drop-down list for the SIP Trunk Security Profile field. • Select the SIP Profile provisioned in Step 4.1.2 from the drop-down list for the SIP Profile field. • Select RFC 2833 from the drop-down list for the DTMF Signaling Method field. • Click Save. 
4.1.6	<p>From the pop-up window, click OK and reset the trunk by clicking Reset,  [<i>Not Shown, located at the bottom of the SIP Trunk page</i>].</p> 

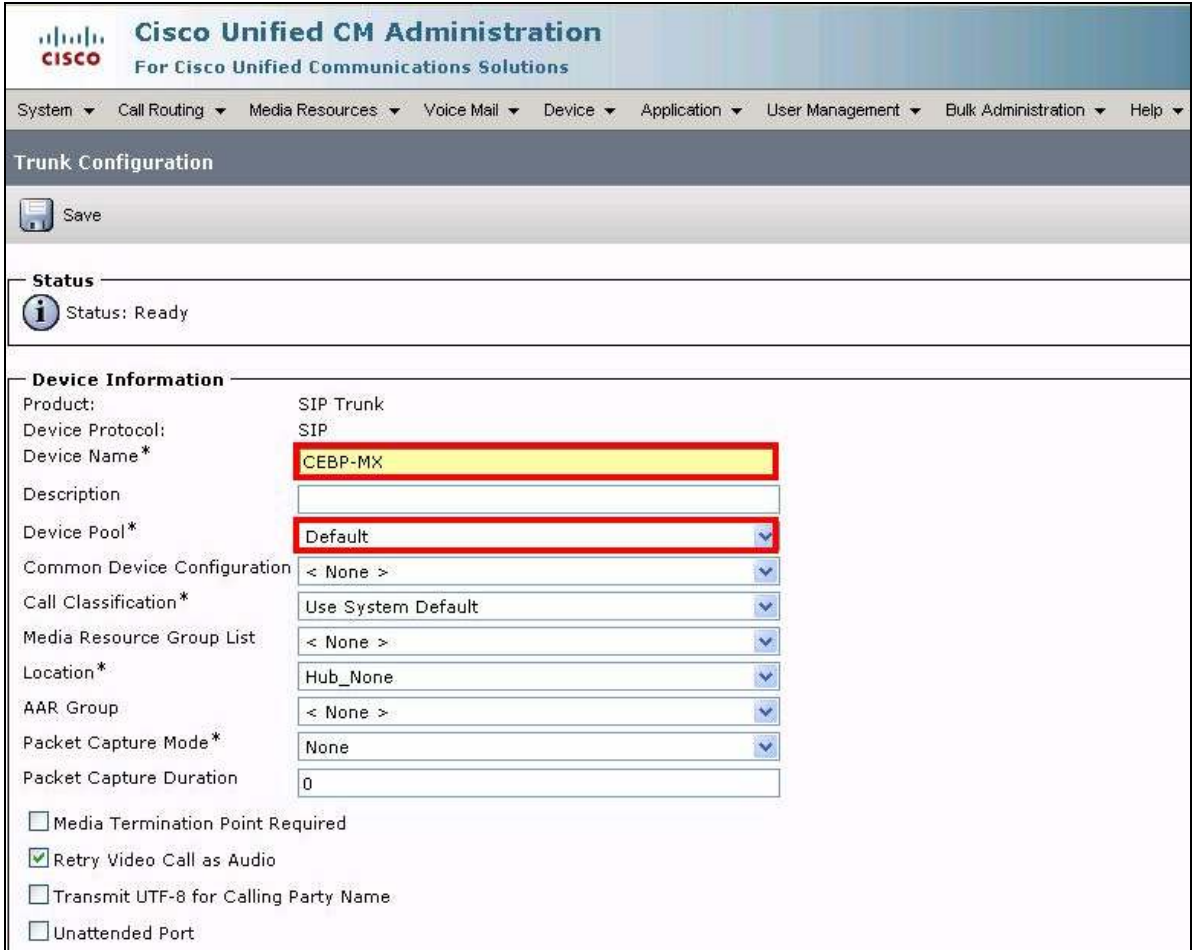
Step	Description
4.1.7	<p>From the pop-up window, click Reset.</p> 

Step	Description
4.1.8a	<p>To enable call routing from Cisco UCM to Avaya CPM utilizing the SIP trunk provisioned in the previous steps, configure a Route Pattern as follows:</p> <ul style="list-style-type: none"> From the Cisco UCM main menu, select Call Routing → Route/Hunt → Route Pattern. [<i>Not Shown</i>] Click Add New to create a new Route Pattern. Provision settings under Pattern Definition as displayed and scroll down. <ul style="list-style-type: none"> Enter a pattern in the Route Pattern field that corresponds to the Host Map provisioned on Avaya SIP Enablement Services in Step 3.2.9. Note that “X” is a wildcard and represents any digit 0 through 9. Select the SIP trunk provisioned in Steps 4.1.4 - 4.1.5 from the drop-down list for the Gateway/Route List field. Verify that the Provide Outside Dial Tone field is not selected.  <p>The screenshot displays the 'Route Pattern Configuration' page in the Cisco Unified CM Administration console. The 'Pattern Definition' section is expanded, showing the following configuration details:</p> <ul style="list-style-type: none"> Route Pattern*: 18XX Route Partition: < None > Description: ToAvayaCPM Numbering Plan: -- Not Selected -- Route Filter: < None > MLPP Precedence*: Default Gateway/Route List*: CEBP-SES (with an (Edit) link) Route Option: <input checked="" type="radio"/> Route this pattern; <input type="radio"/> Block this pattern (No Error) Call Classification*: OffNet Checkboxes: <input type="checkbox"/> Allow Device Override; <input type="checkbox"/> Provide Outside Dial Tone; <input type="checkbox"/> Allow Overlap Sending; <input type="checkbox"/> Urgent Priority <input type="checkbox"/> Require Forced Authorization Code Authorization Level*: 0 <input type="checkbox"/> Require Client Matter Code

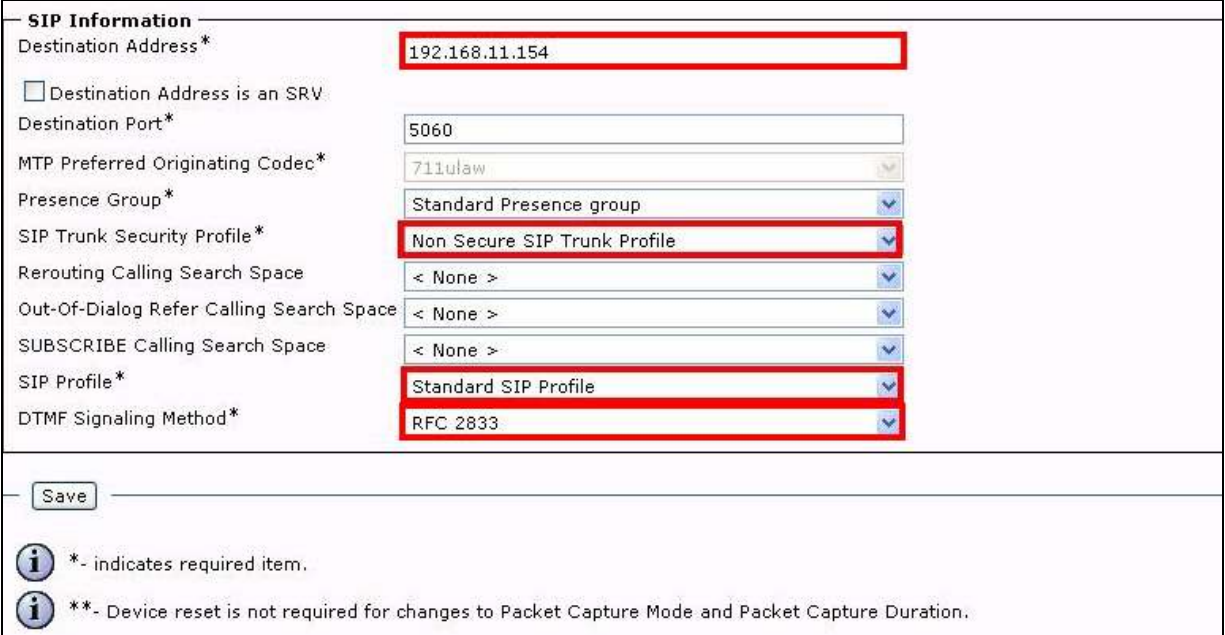
Step	Description
4.1.8b	<p>Use default settings as displayed and click Save.</p> 
4.1.9	<p>The Require Forced Authorization Code option was not enabled in Step 4.1.8, click OK.</p> 

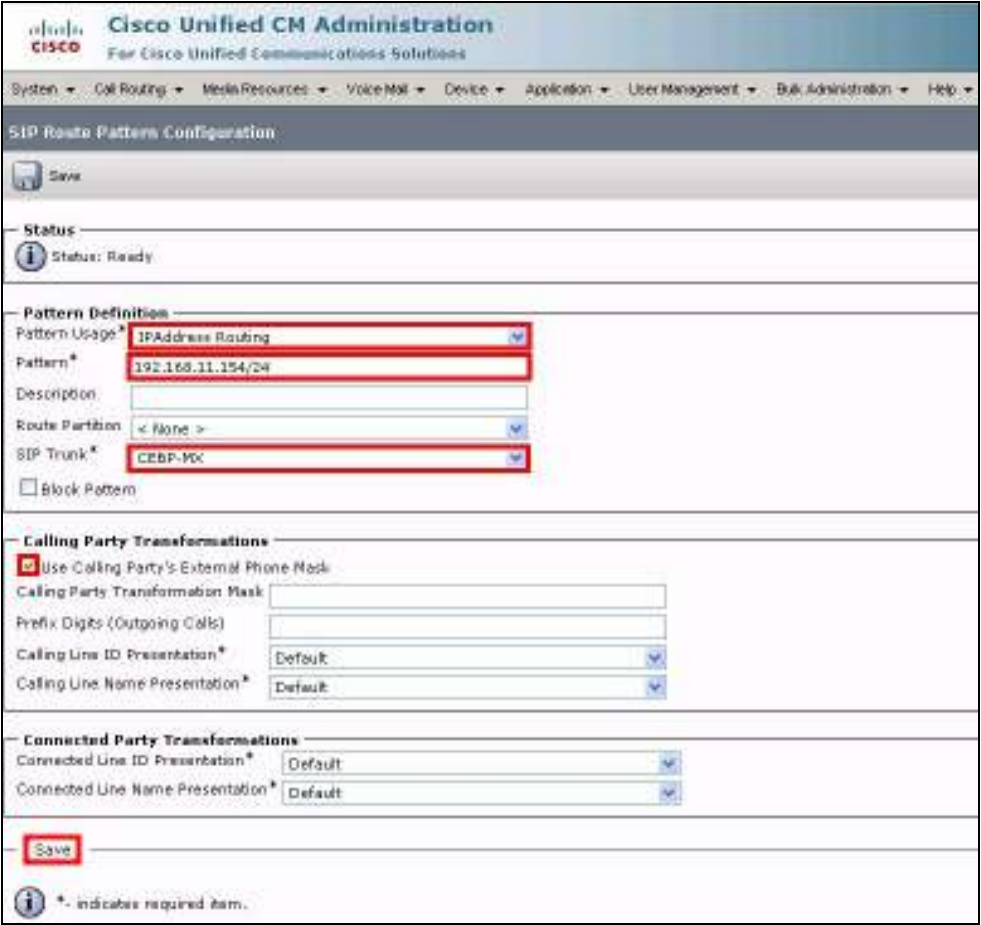
4.2. Configure Connectivity to Avaya Meeting Exchange Express Edition

This section describes the steps for configuring SIP connectivity between Cisco UCM and Avaya Meeting Exchange. This configuration enables Cisco UCM to properly handle the web services that utilize the SIP REFER method to access Avaya Meeting Exchange.

Step	Description
4.2.1	Repeat Steps 4.1.3 - 4.1.4 to add a SIP Trunk that enables SIP connectivity with Avaya Meeting Exchange.
4.2.2a	<p>Provision settings under Device Information as displayed and scroll down. The Location field specifies the total bandwidth that is available for calls between this location and the central location, or hub. Using the default setting Hub_None specifies unlimited available bandwidth.</p> 

Step	Description
4.2.2b	<p>Use default settings as displayed and scroll down.</p> <div data-bbox="297 338 1513 1060"> <div> Multilevel Precedence and Preemption (MLPP) Information </div> <div> MLPP Domain < None > </div> <div> Call Routing Information </div> <div> Inbound Calls </div> <div> <div>Significant Digits*</div> <div>All</div> </div> <div> <div>Connected Line ID Presentation*</div> <div>Default</div> </div> <div> <div>Connected Name Presentation*</div> <div>Default</div> </div> <div> <div>Calling Search Space</div> <div>< None ></div> </div> <div> <div>AAR Calling Search Space</div> <div>< None ></div> </div> <div> <div>Prefix DN</div> <div></div> </div> <div> <input type="checkbox"/> Redirecting Diversion Header Delivery - Inbound </div> <div> Outbound Calls </div> <div> <div>Calling Party Selection*</div> <div>Originator</div> </div> <div> <div>Calling Line ID Presentation*</div> <div>Default</div> </div> <div> <div>Calling Name Presentation*</div> <div>Default</div> </div> <div> <div>Caller ID DN</div> <div></div> </div> <div> <div>Caller Name</div> <div></div> </div> <div> <input type="checkbox"/> Redirecting Diversion Header Delivery - Outbound </div> </div>

Step	Description
4.2.2c	<p>Provision settings under SIP Information as displayed.</p> <ul style="list-style-type: none"> • Enter the IP address of Avaya SIP Enablement Services in the Destination Address field. • Select the SIP Trunk Security Profile provisioned in Step 4.1.1 from the drop-down list for the SIP Trunk Security Profile field. • Select the SIP Profile provisioned in Step 4.1.2 from the drop-down list for the SIP Profile field. • Select RFC 2833 from the drop-down list for the DTMF Signaling Method field. • Click Save. 
4.2.3	Repeat Steps 4.1.6 - 4.1.7 to Reset the trunk.

Step	Description
4.2.4	<p>To enable call routing from Cisco UCM to Avaya Meeting Exchange utilizing the SIP trunk provisioned in the previous steps, configure a Route Pattern as follows:</p> <ul style="list-style-type: none"> From the Cisco UCM main menu, select Call Routing → SIP Route Pattern. [<i>Not Shown</i>] Click Add New to create a new SIP Route Pattern. Provision settings under Pattern Definition as displayed. <ul style="list-style-type: none"> Select the appropriate routing choice from the drop-down list for the Pattern Usage field. Enter the IP address of Avaya Meeting Exchange in Classless Inter-Domain Routing (CIDR) notation in the Pattern field. Select the SIP trunk provisioned in Steps 4.2.1 - 4.2.2 from the drop-down list for the SIP Trunk field. To enable the full, external phone number to be used for calling line identification (CLID) on outgoing calls, select the Use Calling Party's External Phone Mask field. Click Save. 

5. Interoperability Testing

5.1. General Test Approach

The general test approach was to place calls between endpoints registered to Cisco UCM and Avaya CPM, utilizing the sample configuration displayed in **Figure 1**.

The main objectives were to verify the following:

- Web services offered by Avaya CPM to endpoints registered to Cisco UCM via Avaya SIP Enablement Services:
 - Advisory
 - Find and Call
 - Notify and Response
 - Notify and Conference
- Dial-in services from endpoints registered to Cisco UCM to Avaya CPM via Avaya SIP Enablement Services
- Record/Playback of messages from endpoints registered to Cisco UCM
- Transport methods for signaling between Avaya CPM and Cisco UCM via Avaya SIP Enablement Services:
 - SIP/TCP
 - SIP/UDP
- Transport methods for media between Avaya CPM and Cisco UCM:
 - RTP/UDP
- Codecs:
 - G711MU
- Voice quality, verified subjectively from endpoints registered to Cisco UCM
- 3pcc Call Establishment as defined by RFC 3725:
 - Flow 1
- DTMF transmission as defined by RFC 2833


5.2. Test Results

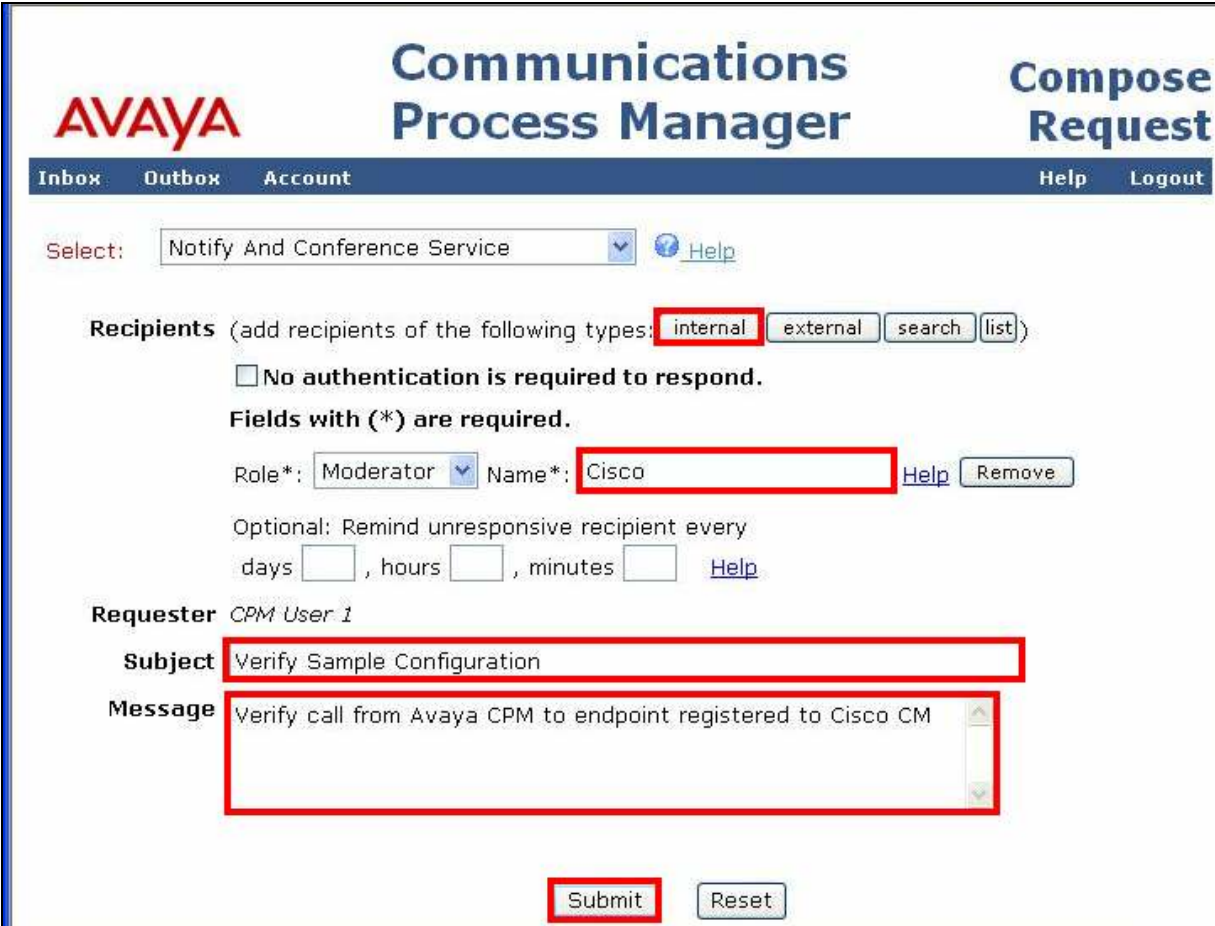
All test cases, as defined by the general test approach, passed.

6. Verification Steps

The following steps were used to verify the administrative steps presented in these Application Notes and are applicable for similar configurations in the field.

Step	Description
6.1.1	<p>Validate signaling and media connectivity for call origination from Avaya CPM to Cisco UCM. This is accomplished by verifying that the SIP trunks provisioned in Section 4 are utilized when a web service to endpoint(s) registered to Cisco UCM is initiated. To verify that both trunks are operational, a web service that utilizes the SIP REFER method is initiated as displayed.</p> <ul style="list-style-type: none">From a sample account accessed via the Avaya CPM Web Portal, click Outbox.Select Notify And Conference Service from the drop-down list for the Select field.



Step	Description
6.1.2	<p>Initiate the Notify And Conference Service to an endpoint registered to Cisco UCM. For this sample configuration the endpoint provisioned in Step 3.1.8 is selected as displayed.</p> <ul style="list-style-type: none"> • To display the Role and Name fields, click internal. • Enter the name of the endpoint provisioned in Step 3.1.8 in the Name field. • Enter descriptive test in the Subject and Message fields. • Click Submit. 

Step	Description
6.1.3	<p>Verify the following:</p> <ul style="list-style-type: none"> The endpoint selected in Step 6.1.2 rings. The account where the Notify And Conference Service was initiated is updated as displayed. <ul style="list-style-type: none"> From the sample account where the Notify And Conference Service was initiated, click Outbox. Select Pending from the drop-down list for the Select field. Verify the Notify And Conference Service is listed.

AVAYA Communications Process Manager **Outbox**

Inbox **Outbox** Account Help Logout

Select: Pending Help

You have one pending request.

	Application	Session Id	Start Date	Subject
<input type="checkbox"/> 1	Notify And Conference Service	AAAAAGDm00k=9Fk7QQ==	Tuesday 01 April 2008 , 9:46:38 am	Verify Sample Configuration

Cancel Selected Request(s)

CPM User 1 CPM v2.1

Copyright © 2007 Avaya, Inc. All Rights Reserved.

Step	Description
6.1.4	<p>Answer the call from Avaya CPM and verify the following:</p> <ul style="list-style-type: none"> The endpoint receives prompts from Avaya CPM. The endpoint can enter appropriate responses (via DTMF) to navigate through the Notify And Conference Service. <ul style="list-style-type: none"> The endpoint is placed in conference and has media connectivity with Avaya Meeting Exchange. The endpoint can terminate the call by going on-hook or by entering the appropriate response (via DTMF). Avaya CPM moves the Notify And Conference Service from Pending to Completed. <ul style="list-style-type: none"> From the sample account where the Notify And Conference Service was initiated, click Outbox. Select Completed from the drop-down list for the Select field. Verify the Notify And Conference Service is listed.

AVAYA Communications Process Manager Outbox

Inbox **Outbox** Account Help Logout

Select: **Completed** Help

You have one completed request.


<input type="checkbox"/>	Application	Session Id	Start Date	End Date	Subject
<input type="checkbox"/> 1	Notify And Conference Service	AAAAAGDm00k=9Fk7QQ==	Tuesday 01 April 2008 , 9:46:38 am	Tuesday 01 April 2008 , 9:48:43 am	Verify Sample Configuration

Delete Selected Request(s)

CPM User 1 CPM v2.1

Copyright © 2007 Avaya, Inc. All Rights Reserved.

Step	Description
6.1.5	<p>Below is a SIP call flow of the Notify And Conference Service initiated in Steps 6.1.1 - 6.1.4. This trace is intended display the provisioning presented in these Application Notes and may be used for verification purposes.</p> <ul style="list-style-type: none"> Avaya SIP Enablement Services (192.168.11.153) sends a SIP INVITE to Cisco UCM (60.1.1.9) at Time 75.016. Avaya SIP Enablement Services (192.168.11.153) sends a SIP REFER to Cisco UCM (60.1.1.9) at Time 108.483. Cisco UCM accepts the REFER at Time 108.488 and sends and INVITE to Avaya Meeting Exchange (192.168.11.154) at Time 108.555.
<p>The diagram illustrates a SIP call flow involving five IP addresses: 192.168.11.153, 60.1.1.9, 192.168.11.152, 192.168.11.154, and 192.168.12.62. The flow is divided into three distinct time periods, each with a different background color: green (75.016 to 108.504), blue (108.555 to 108.591), and cyan (108.611 to 131.681). In the green section, 192.168.11.153 sends an INVITE to 60.1.1.9, which responds with 100 Trying, 180 Ringing, and 200 OK. 192.168.11.153 then sends an ACK and two RTP packets to 60.1.1.9. In the blue section, 192.168.11.153 sends a REFER to 60.1.1.9, which responds with 202 Accepted. 60.1.1.9 then sends a NOTIFY to 192.168.11.154, which responds with 200 OK. In the cyan section, 60.1.1.9 sends an INVITE to 192.168.11.154, which responds with 100 Trying and 200 OK. 60.1.1.9 then sends a NOTIFY to 192.168.11.153, which responds with 200 OK. Finally, 60.1.1.9 sends a BYE to 192.168.11.154, which responds with 200 OK.</p>	

Step	Description
6.1.6	<p>Validate signaling and media connectivity for call origination from Cisco UCM to Avaya Meeting Exchange. This is accomplished by verifying that the SIP trunk provisioned in Section 4.1 is utilized when a call from an endpoint registered to Cisco UCM dials in to Avaya CPM. From an endpoint registered to Cisco UCM, dial 1800 to initiate dial-in services and verify the following:</p> <ul style="list-style-type: none"> • The endpoint receives prompts from Avaya CPM. • The endpoint can enter appropriate responses (via DTMF) to navigate through the dial-in service. • The call terminates automatically if there are no pending requests. <p>Below is a SIP call flow of the dial-in service. This trace is intended display the provisioning presented in these Application Notes and may be used for verification purposes.</p> <ul style="list-style-type: none"> • Cisco UCM (60.1.1.9) sends a SIP INVITE to Avaya SIP Enablement Services (192.168.11.153) at Time 10.106. • Avaya SIP Enablement Services (192.168.11.153) sends a BYE to Cisco UCM (60.1.1.9) at Time 28.977.  <pre> sequenceDiagram participant CUCM as 60.1.1.9 participant ASE as 192.168.11.153 participant AME as 192.168.11.152 Note over CUCM, ASE: 10.106 INVITE SDP (g711U telephone-event) Note over ASE, AME: 10.108 100 Trying Note over ASE, AME: 10.120 180 Ringing Note over CUCM, ASE: 10.255 200 OK SDP (g711U telephone-event) Note over CUCM, ASE: 10.258 ACK Note over ASE, AME: 10.278 RTP (g711U) Note over ASE, AME: 24.799 RTP (g711U) Note over ASE, AME: 28.977 BYE Note over CUCM, ASE: 28.983 200 OK </pre>

7. Conclusion

These Application Notes present a sample configuration comprised of Avaya Communications Process Manager (CPM) and Cisco Unified Communications Manager (UCM) via Avaya SIP Enablement Services. Employing this configuration enables call origination/termination between endpoints registered to Cisco UCM and Avaya CPM, where the signaling is SIP and the media is Real-time Transport Protocol (RTP). This configuration integrates endpoints registered to Cisco UCM with web services for business applications offered by Avaya CPM to provide a solution for Avaya Communications Enabled Business Processes (CEBP).

8. Additional References

Avaya references are available at <http://support.avaya.com>.

- [1] Communications Process Manager Installation and Configuration Guide, Issue 3, Doc ID 04-601158, December 2007.
- [2] Communications Process Manager Administration and Maintenance Guide, Issue 5, Doc ID 04-601159, December 2007.

Cisco references are available at <http://www.cisco.com>.

- [3] Cisco Unified Communications Manager Administration Guide Release 6.0(1), Document #: OL-12525-01.

©2008 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com