



## **Avaya Solution & Interoperability Test Lab**

---

# **Integrating Avaya Aura® Session Manager R6.1, Avaya Aura® Communication Manager R6.0.1, and Cisco Unified Communications Manager R7.1.5 – Issue 1.0**

## **Abstract**

These Application Notes present a sample configuration for an enterprise network that integrates Avaya Aura® Session Manager R6.1, Avaya Aura® Communication Manager R6.0.1, and Cisco Unified Communications Manager R7.1.5. Although the tested configuration also uses Session Manager to provide access to a centralized voice messaging solution using Avaya Modular Messaging, the focus of these Application Notes is interoperability between Avaya Communication Manager and Cisco Unified Communications Manager using Session Manager. Separate companion application notes focus on supporting Cisco Unified Communications Manager users with Avaya Modular Messaging via Avaya Aura® Session Manager.

The interoperability testing was conducted by the Solution and Interoperability Test Lab at the request of Session Manager Product Management.

# 1. Introduction

These Application Notes address integration of Cisco Unified Communications Manager (hereafter referred to as Cisco UCM) into an enterprise telephony network consisting of Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Although the configuration and verification testing included a centralized voice messaging solution using Avaya Modular Messaging, the focus of these Application Notes is interoperability between Avaya Communication Manager and Cisco Unified Communications Manager using Session Manager. A separate companion document [10] focuses on supporting Cisco UCM users with Avaya Modular Messaging via Session Manager.

In the test configuration shown in **Figure 1**, Cisco UCM supports the Cisco telephones, which have 5-digit extensions in the range 60xxx. Communication Manager, running on an Avaya S8300D server, is configured as an Evolution Server, controls an Avaya G430 Media Gateway, and supports all of the Avaya telephones shown, which have 5-digit extensions in the range 3xxxx. An adaptation module is defined in Session Manager for the Cisco UCM to translate the Remote-Party-ID SIP header to P-Asserted-Identity and the Diversion header to History-Info. This operation is performed so that calling and called party displays are properly supported, and Modular Messaging can properly identify Cisco subscribers during call coverage and other voice messaging operations. Using Session Manager SIP trunks, Modular Messaging supports both Avaya and Cisco telephones for voice messaging coverage. Both Communication Manager and Cisco UCM are configured to access Modular Messaging using extension 33000.

Session Manager can support flexible inter-system call routing based on dialed number, calling number and system location, and can also provide protocol adaptation to allow multi-vendor systems to interoperate. It is managed by a separate Avaya Aura® System Manager, which can manage multiple Session Managers by communicating with their management network interfaces. Modular Messaging expands the capabilities and features of messaging services. Centralized messaging enables the Modular Messaging system to provide voicemail service to subscribers at the Cisco and Avaya sites in a multi-site configuration.

These Application Notes will focus on configuration of Session Manager, Communication Manager, and Cisco UCM. Detailed administration of the endpoint telephones will not be described. As mentioned, a companion Application Notes [10] focuses on configuration of Session Manager, Modular Messaging, and Cisco UCM to support a centralized voice messaging solution using Session Manager.

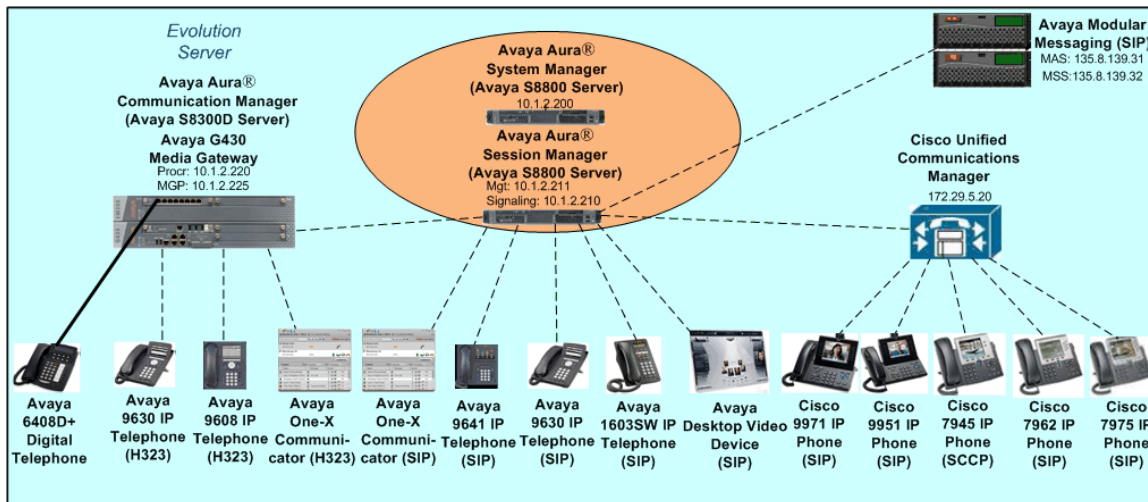


Figure 1: Sample Configuration

## 2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration:

Manufacturer	Hardware Component	Software Version
Avaya	S8300D Server with G430 Media Gateway	Avaya Aura® Communication Manager 6.0.1, Load 510.1, Patch 18599
Avaya	S8800 Server	Avaya Aura® Session Manager 6.1, Load 6.1.0.0.610012
		Avaya Aura® System Manager 6.1, Build Number 6.1.0.4.5072, Patch 6.1.4.62
Avaya	Avaya 9641 IP Telephone (SIP)	S96x1_SALBR6_0r95_V4r52B
Avaya	Avaya 9630 IP Telephone (SIP)	2.6.3
Avaya	Avaya 9630 IP Telephone (H.323)	3.101S
Avaya	Avaya 9608 IP Telephone (H323)	S9608_11_HALBR6_0_V452
Avaya	Avaya 1603 IP Telephone (SIP)	R1.0.1
Avaya	Avaya 6408D+ Digital Telephone	-
Avaya	Avaya Desktop Video Device (SIP)	SIP_A175_1_0_0_032706.tar
Avaya	Avaya one-X Communicator (H323, SIP)	SIP_A175_1_0_0_002635
Avaya	Modular Messaging Storage Server	5.2, Service Pack 5 Patch 1
Avaya	Modular Messaging Application Server	5.2, Service Pack 5 Patch 1
Cisco	Unified Communications Manager	7.1.5.31900-3
Cisco	7945 Unified IP Phone (SCCP)	SCCP45.9-0-3S
Cisco	7962 Unified IP Phone (SIP)	SIP42.9-0-3S
Cisco	7975 Unified IP Phone (SIP)	SIP75.9-0-3S
Cisco	9951 Unified IP Phone (SIP)	SIP9951.9-0-3
Cisco	9971 Unified IP Phone (SIP)	SIP9971.9-0-3

### 3. Configure Avaya Aura<sup>®</sup> Communication Manager

This section addresses the configuration of Communication Manager. All configurations in this section are performed using the System Access Terminal (SAT). These Application Notes assume that the basic configuration has already been completed. For further information on Communication Manager, see references [4-6]. The procedures include the following areas:

- Verify Avaya Aura<sup>™</sup> Communication Manager License
- Configure System Parameters Features
- Configure IP Node Names
- Configure IP Network Region and Codec set
- Configure SIP Signaling Group and Trunk Group
- Configure Route Pattern
- Configure Private Numbering
- Configure Dial Plan and AAR analysis
- Save Changes

#### 3.1. Verify Avaya Aura<sup>®</sup> Communication Manager License

Use the **display system-parameter customer options** command to compare the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

**Note:** The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

change system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES				USED
Maximum Administered H.323 Trunks:		12000		100
Maximum Concurrently Registered IP Stations:		18000		6
Maximum Administered Remote Office Trunks:		12000		0
Maximum Concurrently Registered Remote Office Stations:		18000		0
Maximum Concurrently Registered IP eCons:		414		0
Max Concur Registered Unauthenticated H.323 Stations:		100		0
Maximum Video Capable Stations:		18000		0
Maximum Video Capable IP Softphones:		18000		0
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>		<b>156</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		24000		0

### 3.2. Configure System Parameters Features

Use the **change system-parameters features** command to allow for trunk-to-trunk transfers. This feature is needed to allow for transferring an incoming/outgoing call from/to a remote switch back out to the same or different switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to **all** to enable all trunk-to-trunk transfers on a system wide basis.

**Note:** This feature poses significant security risk and must be used with caution. As an alternative, the trunk-to-trunk feature can be implemented using Class Of Restriction or Class Of Service levels.

```
change system-parameters features                                     Page 1 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS
                                Self Station Display Enabled? n
                                Trunk-to-Trunk Transfer: all
                                Automatic Callback with Called Party Queuing? y
                                Automatic Callback - No Answer Timeout Interval (rings): 3
                                Call Park Timeout Interval (minutes): 10
                                Off-Premises Tone Detect Timeout Interval (seconds): 20
                                AAR/ARS Dial Tone Required? y

                                Music (or Silence) on Transferred Trunk Calls? no
                                DID/Tie/ISDN/SIP Intercept Treatment: attd
                                Internal Auto-Answer of Attnd-Extended/Transferred Calls: transferred
                                Automatic Circuit Assurance (ACA) Enabled? n
```

### 3.3. Configure IP Node Names

Use the **change node-names ip** command to add entries for Communication Manager and Session Manager that will be used for connectivity. In the sample network, **procr** and **10.1.2.220** are automatically added as **name** and **IP Address** by Communication Manager as a result of the initial template installation on the Avaya S8300D Server. Enter **SM1** and **10.1.2.210** for the signaling interface (security module) of Session Manager.

```
change node-names ip                                               Page 1 of 2
                                IP NODE NAMES
                                Name          IP Address
                                SM1          10.1.2.210
                                procr        10.1.2.220
```

### 3.4. Configure IP Network Region and Codec Set

Use the **change ip-network-region n** command, where **n** is the network region number to configure the network region being used. In the sample network, ip-network-region 1 is used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise (see **Section 4.2**) and a descriptive **Name** for this ip-network-region. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec Set** to **1** to use ip-codec-set 1.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: Authoritative Domain: avaya.com
Name: HQ CM and SIP Phones
MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes
Codec Set: 1 Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048 IP Audio Hairpinning? y
UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

Use the **change ip-codec-set n** command, where **n** is the existing codec set number to configure the desired audio codecs. The G.722-64K codec has been included first in the list, since G.722 is supported for calls between Avaya H.323/SIP and Cisco SIP telephones, as well as between Avaya H323/SIP telephones and Cisco SCCP telephones.<sup>1</sup> G.729A was successfully tested as well.<sup>2</sup> G.729B is not supported.

```
change ip-codec-set 1                                         Page 1 of 2
                                                                IP Codec Set
Codec Set: 1
Audio Silence Frames Packet
Codec Suppression Per Pkt Size(ms)
1: G.722-64K 2 20
2: G.711MU n 2 20
3: G.729A n 2 20
```

<sup>1</sup> Direct media, and therefore G.722 is not supported for calls from Cisco SCCP telephones to Avaya H323 and SIP telephones.

<sup>2</sup> Direct media is not supported for G.729A calls from Cisco telephones to the Avaya 1603 IP Telephone (SIP).

## 3.5. Configure SIP Signaling Group and Trunk Group

### 3.5.1. SIP Signaling Group

In the sample configuration, Communication Manager is configured as an Evolution Server, supporting H.323 and digital telephones as well as providing feature server support for SIP telephones. Signaling group 60 along with trunk group 60 supports a SIP trunk to Session Manager. Use the **add signaling-group n** command, where **n** is the signaling-group number being added to the system. Set the **Group Type** to **SIP**. For Evolution Server configuration, **IMS Enabled** should be set to **n** and **Peer Detection Enabled** to **y**.<sup>3</sup> The **Peer Server** field will later be automatically populated with **SM** as a result of peer detection. For tracing purposes, **Transport Method** is set to **TCP** (note that the more secure TLS is also supported). Use the values defined in **Sections 3.3** and **3.4** for **Near-end Node Name**, **Far-End Node-Name** and **Far-End Network Region**. Since an adaptation module will be defined in Session Manager to set the domain for all incoming calls to **avaya.com** (see **Section 4.4**), this value can be put in the **Far-end Domain**, and all outgoing and incoming calls to/from Session Manager will use this single trunk. This eliminates the need for a separate trunk for incoming calls from Cisco UCM which use the IP address of Session Manager instead of the SIP domain. Setting **H.323 Station Outgoing Direct Media** and **Initial IP-IP Direct Media** to **y** will minimize the number of SIP messages used by Communication Manager in establishing calls. For example, call setup will not require RTP media to be initially connected to the CM VoIP engine, and then on answer be shuffled directly between IP endpoints. Default values can be used for the remaining fields.

```
add signaling-group 60                                     Page 1 of 1
                                                         SIGNALING GROUP

Group Number: 60                                         Group Type: sip
IMS Enabled? n                                           Transport Method: tcp
  Q-SIP? n                                              SIP Enabled LSP? n
  IP Video? n                                           Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: Others

Near-end Node Name: procr                               Far-end Node Name: SM1
Near-end Listen Port: 5061                             Far-end Listen Port: 5061
                                                         Far-end Network Region: 1

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate                   Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                             RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3                    Direct IP-IP Audio Connections? y
  Enable Layer 3 Test? n                               IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? y                 Initial IP-IP Direct Media? y
                                                         Alternate Route Timer(sec): 6
```

---

<sup>3</sup> Note that this differs from *Feature Server* configuration, where the **IMS Enabled** field is set to “y”.

### 3.5.2. SIP Trunk Group

Use the **add trunk-group n** command, where **n** is the new trunk group number being added to the system. The following screens show the settings used for trunk group 60. Navigate to **Page 1** and enter the following:

<b>Group Type</b>	<b>sip</b>
<b>TAC</b>	a dial access code (see <b>Section 3.8</b> )
<b>Service Type</b>	<b>tie</b>
<b>Signaling Group</b>	the signaling group defined in <b>Section 3.5.1</b>
<b>Number of Members</b>	a numeric value within the capacity range (see <b>Section 3.1</b> )

```
add trunk-group 60                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 60                                     Group Type: sip          CDR Reports: y
  Group Name: SM1                                     COR: 1          TN: 1          TAC: 160
    Direction: two-way          Outgoing Display? n
    Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                                     Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 60
                                                Number of Members: 100
```

Navigate to **Page 2** and enter **900** for **Preferred Minimum Session Refresh Interval (sec)**. This will eliminate session refresh interval negotiation with Cisco UCM and reduce the amount of SIP signaling messages required for call setup.

```
add trunk-group 60                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                                Redirect On OPTIM Failure: 5000
  SCCAN? n                                     Digital Loss Group: 18
  Preferred Minimum Session Refresh Interval(sec): 900
```

Navigate to **Page 3** and enter **private** for **Numbering Format**.

```
change trunk-group 60                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n          Measured: none          Maintenance Tests? y
  Numbering Format: private
                                                UII Treatment: service-provider
                                                Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```



### 3.6. Configure Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use the **change route-pattern n** command, where **n** is the route pattern number. Configure this route pattern to route calls to trunk group number **60** configured in **Section 3.5.2**. Assign the lowest **FRL** (facility restriction level) to allow all callers to use this route pattern. For **LAR** in row number (1) corresponding to the first trunk group entry, enter **next**. This will ensure that for calls (SIP INVITEs) for which Communication Manager receives no response, the shorter **Alternate Route Timer** will be used instead of the much longer **Session Establishment Timer**, minimizing the time before the caller hears reorder. See **Section 3.5.1** for these parameters.

change route-pattern 60										Page	1 of	3
Pattern Number: 60 Pattern Name: SM1												
SCCAN? n Secure SIP? n												
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted			DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits			QSIG		
											Intw	
1:	60	0				0				n	user	
2:										n	user	
3:										n	user	
4:										n	user	
5:										n	user	
6:										n	user	
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR												
0 1 2 M 4 W Request												
										Dgts Format		
										Subaddress		
1:	y	y	y	y	y	n	n	rest		next		
2:	y	y	y	y	y	n	n	rest		none		
3:	y	y	y	y	y	n	n	rest		none		
4:	y	y	y	y	y	n	n	rest		none		

### 3.7. Configure Private Numbering

Use the **change private-numbering** command to define the calling party number to be sent out through SIP trunk 60. In the sample network configuration below, all calls originating from a 5-digit extension beginning with 3 will result in a 5-digit calling number. This number will be in the SIP “From” and “P-Asserted-Identity” headers.

change private-numbering 0										Page	1 of	2
NUMBERING - PRIVATE FORMAT												
Ext	Ext	Trk		Private		Total						
Len	Code	Grp(s)		Prefix		Len						
5	2					5		Total Administered: 6				
5	3	60				5		Maximum Entries: 540				
5	4					5						
5	5					5						

### 3.8. Configure Dial Plan and AAR analysis

Configure the dial plan for dialing 5-digit extensions beginning with **6** to stations registered with Cisco UCM. Use the **change dialplan analysis** command to define **Dialed String 6** as an **ext Call Type**.

change dialplan analysis								
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	3	dac						
3	5	ext						
6	5	ext						

Use the **change aar analysis n** command where **n** is the dial string pattern to configure an entry for **Dialed String 6** to use **Route Pattern 60**. Add an entry for the Cisco UCM extensions which begin with **6**. Set **Call Type** to **unku**.

change aar analysis 6							
AAR DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 0	
Dialed String	Total Min Max		Route Pattern	Call Type	Node Num	ANI Req'd	
6	5	5	60	unku		n	

### 3.9. Save Changes

Use the **save translation** command to save all changes.

save translation	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

## 4. Configuring Avaya Aura® Session Manager

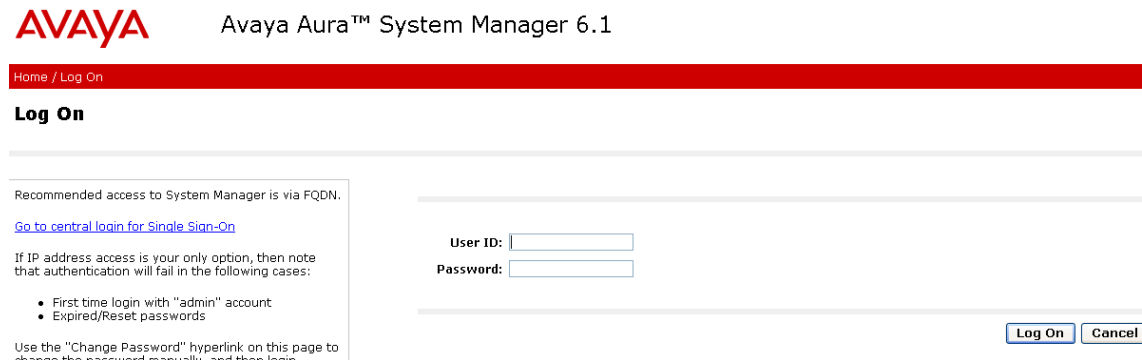
This section provides the procedures for configuring Session Manager. For further information on Session Manager, see [1-3]. The procedures include the following areas:

- Login to Avaya Aura® Session Manager
- Configure SIP domain
- Add Location
- Configure Adaptations
- Configure SIP Entities
- Configure Entity Links
- Configure Routing Policies
- Configure Dial Patterns
- Configure Session Manager
- Add Communication Manager as a Evolution Server
- Add Users for SIP Telephones

If it is desired to provide Avaya Modular Messaging support for Cisco UCM users, then see Reference [10] for configuring the appropriate items for Modular Messaging in Session Manager.

## 4.1. Log in to Avaya Aura® Session Manager

Access the Avaya Aura® System Manager using a Web Browser and entering ***http://<ip-address>/SMGR***, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials.



The login page features the Avaya logo and the title 'Avaya Aura™ System Manager 6.1'. A red header bar contains the links 'Home / Log On'. Below this, a 'Log On' section includes a message about recommended access via FQDN and a link to 'Go to central login for Single Sign-On'. It also lists cases where IP address access might fail: first-time login with 'admin' or expired passwords. A 'Change Password' link is provided. The login form has fields for 'User ID' and 'Password', and 'Log On' and 'Cancel' buttons.

AVAYA Avaya Aura™ System Manager 6.1

Home / Log On

**Log On**

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

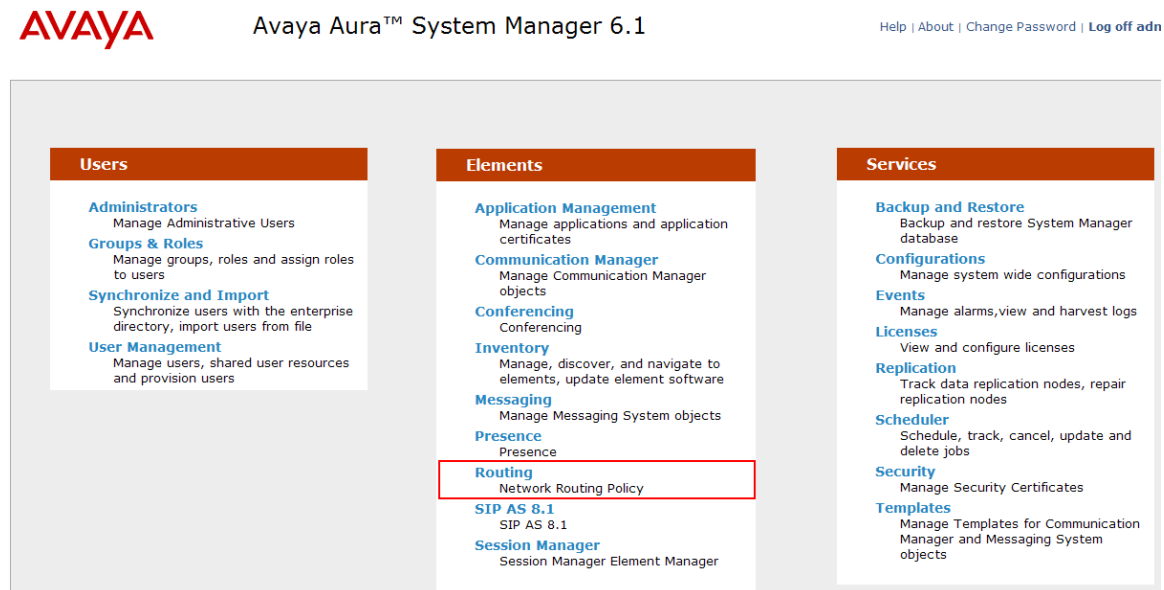
- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login

User ID:

Password:

The main menu screen will be displayed. For the configuration steps described in **Sections 4.2 – 4.8**, access the **Routing** menu shown below under the **Elements** section.



The main menu displays three sections: Users, Elements, and Services. The 'Elements' section is highlighted with a red box around the 'Routing' option, which is described as 'Network Routing Policy'. Other options in the 'Elements' section include Application Management, Communication Manager, Conferencing, Inventory, Messaging, Presence, SIP AS 8.1, and Session Manager.

AVAYA Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off **adm**

Users	Elements	Services
<b>Administrators</b> Manage Administrative Users	<b>Application Management</b> Manage applications and application certificates	<b>Backup and Restore</b> Backup and restore System Manager database
<b>Groups &amp; Roles</b> Manage groups, roles and assign roles to users	<b>Communication Manager</b> Manage Communication Manager objects	<b>Configurations</b> Manage system wide configurations
<b>Synchronize and Import</b> Synchronize users with the enterprise directory, import users from file	<b>Conferencing</b> Conferencing	<b>Events</b> Manage alarms, view and harvest logs
<b>User Management</b> Manage users, shared user resources and provision users	<b>Inventory</b> Manage, discover, and navigate to elements, update element software	<b>Licenses</b> View and configure licenses
	<b>Messaging</b> Manage Messaging System objects	<b>Replication</b> Track data replication nodes, repair replication nodes
	<b>Presence</b> Presence	<b>Scheduler</b> Schedule, track, cancel, update and delete jobs
	<b>Routing</b> Network Routing Policy	<b>Security</b> Manage Security Certificates
	<b>SIP AS 8.1</b> SIP AS 8.1	<b>Templates</b> Manage Templates for Communication Manager and Messaging System objects
	<b>Session Manager</b> Session Manager Element Manager	

## 4.2. Configure SIP Domain

Add the SIP domain, for which the communications infrastructure will be authoritative, by selecting **Routing** → **Domains** on the left panel menu and clicking the **New** button (not shown) to create a new SIP domain entry.

Complete the following options:

**Name**      The authoritative domain name (e.g., **avaya.com**)  
**Notes**      Description for the domain (optional)  
**Type**        Use the default **sip**

Click **Commit** to save changes.

AVAYA Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / Domains - Domain Management

Domain Management [Commit](#) [Cancel](#) [Help ?](#)

1 Item Refresh Filter: Enable

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	

\* Input Required [Commit](#) [Cancel](#)

**Note:** Since the sample network does not deal with any foreign domains, no additional SIP Domains entry is needed.

### 4.3. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, select **Routing** → **Locations** on the left and click on the **New** button (not shown) on the right.

Under **General**, enter:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

The remaining fields under **General** can be filled in to specify bandwidth management parameters between Session Manager and this location. These were not used in the sample configuration, and reflect default values. Note also that although not implemented in the sample configuration, routing policies can be defined based on location.

Under **Location Pattern**:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Descriptive text (optional).

The screens below show the Basking Ridge location, which includes Communication Manager and Session Manager, and the California location, which includes Cisco UCM.

**AVAYA** Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

**Routing** \* Home

**Home / Elements / Routing / Locations- Location Details**

**Location Details** [Help ?](#) [Commit](#) [Cancel](#)

**General**

\* Name: BaskingRidge HQ

Notes: CME, CS1K R5 & R7, AAC R6, CM

**Overall Managed Bandwidth**

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

**Per-Call Bandwidth Parameters**

\* Default Audio Bandwidth: 80 Kbit/sec

**Location Pattern**

[Add](#) [Remove](#)

5 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.1.2.*	SM/CM R5.2.0, R6.0, R6.1
<input type="checkbox"/>	* 10.7.7.*	CS1K R7



Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Locations - Location Details

Location Details

Commit

Cancel

Help ?

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.  
See Session Manager -> Session Manager Administration -> Global Setting

General

\* Name: California

Notes: Cisco UCM's

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

\* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add

Remove

2 Items | Refresh

Filter: Enable

IP Address Pattern	Notes
* 172.29.5.*	UCM R7.1.5

## 4.4. Configure Adaptations

Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic, and can modify other headers to permit interoperability with third party SIP products. Three adaptation modules are employed in the sample configuration:

1. To set the SIP domain of incoming calls to Communication Manager to “avaya.com”, so that a single SIP trunk can be configured in Communication Manager for inbound and outbound calls. See **Section 3.5.1**.
2. An adaptation module designed specifically for interoperating with Cisco Unified Communications Manager products has been developed and is installed with Session Manager. In the sample configuration, it is used for incoming calls from Cisco UCM. This is required to convert the Diversion header, supported by Cisco UCM, to the standard History-Info header used by Modular Messaging and the Remote-Party-ID to P-Asserted-Identity.
3. Multi-site Modular Messaging represents its subscribers using 11 digit telephone numbers. **DigitConversionAdapter** is used in Session Manager to convert between the 5 and 11 digit formats when routing between Modular Messaging and either Communication Manager or Cisco UCM.

The third adaptation is covered in [10], which addresses Modular Messaging configuration. The first two will be covered here.

To add the adaptation module, select **Routing → Adaptations** on the left and click on the **New** button (not shown) on the right. Under **General**, fill in:

- **Name** An informative name for the adaptation (e.g., **CM-ES Inbound, Cisco-UCM7**)
- **Adaptation Module** The adaptation module name (**DigitConversionAdapter, CiscoAdapter**)
- **Module Parameter** (see the individual screens below)

The following screen shows the adaptation module added for Communication Manager. The parameter **odstd=avaya.com** specifies that the domain in the SIP Request-URI and NOTIFY/message-summary body of messages sent by Session Manager to that SIP Entity will be overridden with “avaya.com”. The parameter **osrcd=avaya.com** specifies that the domain in the P-Asserted-Identity header and the calling part of the History-Info header of messages sent by Session Manager will be overridden with “avaya.com”. Since no digit conversions are required, the remaining fields can be left at their defaults.



[Routing](#) X [Home](#)

[Home / Elements / Routing / Adaptations - Adaptation Details](#)

- Routing
- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

[Help ?](#)  
[Commit](#) [Cancel](#)

### Adaptation Details

**General**

\* Adaptation name:

Module name:

Module parameters:

Egress URI Parameters:

Notes:

**Digit Conversion for Incoming Calls to SM**

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
■							

**Digit Conversion for Outgoing Calls from SM**

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
■							

The following screen shows the adaptation module added for Cisco UCM. Specification of **avaya.com** for the **Module parameter** is equivalent to **odstd=avaya.com** as defined above.

[Routing](#) X [Home](#)

[Home / Elements / Routing / Adaptations - Adaptation Details](#)

- Routing
- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

[Help ?](#)  
[Commit](#) [Cancel](#)

### Adaptation Details

**General**

\* Adaptation name:

Module name:

Module parameters:

Egress URI Parameters:

Notes:

**Digit Conversion for Incoming Calls to SM**

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
■							

**Digit Conversion for Outgoing Calls from SM**

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
■							

## 4.5. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by a SIP Trunk. Select **Routing** → **SIP Entities** on the left panel menu and then click on the **New** button (not shown). Enter the following for each SIP Entity:

Under **General**:

**Name** An informative name (e.g., **SM1**)  
**FQDN or IP Address** IP address of the signaling interface on the Session Manager (Security Module), the **procr** interface for Communication Manager, or Cisco UCM.  
**Type** **Session Manager**, **CM**, or **Other** for Cisco UCM  
**Time Zone** Time zone for this location

For SIP Entities of **Type** “Session Manager”, under **Port**, click **Add**, and then edit the fields in the resulting new row:

**Port** Port number on which the system listens for SIP requests  
**Protocol** Transport protocol to be used to receive SIP requests  
**Default Domain** The domain (e.g., **avaya.com**)

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition. The following screen shows the SIP Entity for Session Manager.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". The main content area is titled "SIP Entity Details" and is divided into two sections: "General" and "SIP Link Monitoring".

**General Section:**

- Name:** SM1
- FQDN or IP Address:** 10.1.2.210
- Type:** Session Manager (dropdown)
- Notes:** (empty text box)
- Location:** BaskingRidge HQ (dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** America/New\_York (dropdown)
- Credential name:** (empty text box)

**SIP Link Monitoring Section:**

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)

**Entity Links Section:**

A warning message states: "Entity Links can be modified after SIP Entity is committed." Below this, there is an "Add" button and a "Remove" button. A table shows the current entity link configuration:

Port	Protocol	Default Domain	Notes
5060	TCP	avaya.com	

The following screen shows the SIP Entity for Communication Manager. Note specification of the **Adaptation** module defined in **Section 4.4**.

**AVAYA** Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin

Routing X Home

Home / Elements / Routing / SIP Entities - SIP Entity Details Help ?

SIP Entity Details Commit Cancel

General

\* Name: CM-ES R6.0.1

\* FQDN or IP Address: 10.1.2.220

Type: CM

Notes: CM R6.0.1 ES

Adaptation: CM-ES Inbound

Location: BaskingRidge HQ

Time Zone: America/New\_York

Override Port & Transport with DNS SRV: ☐

\* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the SIP Entity for Cisco UCM. Note specification of the **Adaptation** module defined in **Section 4.4**.

**AVAYA** Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin

Routing X Home

Home / Elements / Routing / SIP Entities - SIP Entity Details Help ?

SIP Entity Details Commit Cancel

General

\* Name: Cisco-UCM7

\* FQDN or IP Address: 172.29.5.20

Type: Other

Notes:

Adaptation: Cisco-UCM7

Location:

Time Zone: America/Los\_Angeles

Override Port & Transport with DNS SRV: ☐

\* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

## 4.6. Configure Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. To add an Entity Link, select **Routing** → **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

<b>Name</b>	An informative name
<b>SIP Entity 1</b>	Select the Session Manager Entity created in the previous section
<b>Port</b>	Port number to which the other system sends its SIP requests
<b>SIP Entity 2</b>	The other SIP Entity for this link, created in the previous section
<b>Port</b>	Port number to which the other system expects to receive SIP requests
<b>Trusted</b>	Verify that this box is checked
<b>Protocol</b>	Transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screens show the Entity Links used in the sample network for Communication Manager and Cisco UCM.

**AVAYA** Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

**Entity Links** [Help ?](#) [Commit](#) [Cancel](#)

1 Item [Refresh](#) Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CM-ES R6.0.1	* SM1	TCP	* 5060	* CM-ES R6.0.1	* 5060	<input checked="" type="checkbox"/>	

\* Input Required [Commit](#) [Cancel](#)

**AVAYA** Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

**Entity Links** [Help ?](#) [Commit](#) [Cancel](#)

1 Item [Refresh](#) Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* Cisco-UCM7	* SM1	TCP	* 5060	* Cisco-UCM7	* 5060	<input checked="" type="checkbox"/>	

\* Input Required [Commit](#) [Cancel](#)

## 4.7. Configure Routing Policies

Create routing policies to direct how calls will be routed to a system. Two routing policies must be added, one for Communication Manager and one for Cisco UCM. To add a routing policy, select **Routing** → **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

Under **General:**

Enter an informative **Name**

Under **SIP Entity as Destination:**

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

Under **Time of Day:**

Click **Add**, and then select a time range, or use the default range **24/7**

The following screen shows the **Routing Policy Details** for Communication Manager.

The screenshot displays the Avaya Aura™ System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the product name, and links for Help, About, Change Password, and Log off admin. The left sidebar shows a menu with options like Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes a breadcrumb trail: Home / Elements / Routing / Routing Policies - Routing Policy Details. There are 'Commit' and 'Cancel' buttons, along with a 'Help ?' link. The 'General' tab is active, showing a 'Name' field with the value 'To CM-ES R6.0.1', a 'Disabled' checkbox, and a 'Notes' field. The 'SIP Entity as Destination' section has a 'Select' button. Below this is a table with columns: Name, FQDN or IP Address, Type, and Notes. The table contains one entry: 'CM-ES R6.0.1', '10.1.2.220', 'CM', and 'CM R6.0.1 ES'. The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows a table with 1 item, a 'Refresh' button, and a 'Filter: Enable' option. The table has columns for Ranking, Name, and days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun), along with Start Time, End Time, and Notes. The single entry shows a ranking of 0, a name of 24/7, and is checked for all days of the week, with a start time of 00:00 and an end time of 23:59. The notes for this entry are 'Time Range 24/7'. At the bottom of the table, there is a 'Select' dropdown with options 'All' and 'None'.

Name	FQDN or IP Address	Type	Notes
CM-ES R6.0.1	10.1.2.220	CM	CM R6.0.1 ES

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

The following screen shows the **Routing Policy Details** for Cisco UCM.

Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Home /Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details

Commit Cancel

General

\* Name: To Cisco UCM7 (60xxx)

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Cisco-UCM7	172.29.5.20	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

## 4.8. Configure Dial Patterns

A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample configuration, 5-digit extensions beginning with 3 are supported by Communication Manager, and 5-digit extensions beginning with 60 reside on Cisco UCM. To add a dial pattern, select **Routing → Dial Patterns** on the left panel menu and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under **General**:

**Pattern** Dialed number or prefix  
**Min** Minimum length of dialed number  
**Max** Maximum length of dialed number  
**SIP Domain** Select **-ALL-**

Under **Originating Locations and Routing Policies**:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save each dial pattern. The following screens show the resulting two dial pattern definitions.

[Routing](#) x [Home](#)

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home /Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

Commit

Cancel

Help ?

General

\* Pattern:

3

\* Min:

5

\* Max:

5

Emergency Call:

☐

SIP Domain:

-ALL-

Notes:

Extension range for CM-ES R6.0.1

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	<a href="#">To CM-ES R6.0.1</a>	0	<input type="checkbox"/>	CM-ES R6.0.1	

Select : All, None

[Routing](#) x [Home](#)

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home /Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

Commit

Cancel

Help ?

General

\* Pattern:

60

\* Min:

5

\* Max:

5

Emergency Call:

☐

SIP Domain:

-ALL-

Notes:

Cisco UCM7

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	<a href="#">To Cisco UCM7 (60xxx)</a>	0	<input type="checkbox"/>	Cisco-UCM7	

Select : All, None

## 4.9. Configure Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Navigate to **Session Manager** → **Session Manager Administration** under the **Elements** section of the **Home** menu . Then on the right, under **Session Manager Instances**, click **New** (not shown) and fill in the fields as described below:

### Under **General**:

<b>SIP Entity Name</b>	Select the name of the SIP Entity added for Session Manager, here <b>SM1</b>
<b>Description</b>	Descriptive comment (optional)
<b>Management Access Point Host Name/IP</b>	Enter the IP address of the Session Manager management interface

### Under **Security Module**:

<b>SIP Entity IP Address</b>	Will be automatically filled in based on the selected <b>SIP Entity Name</b> .
<b>Network Mask</b>	Enter the network mask corresponding to the IP address of Session Manager
<b>Default Gateway:</b>	Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager. The following screen shows the resulting Session Manager.

**AVAYA** Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Session Manager](#) × [Routing](#) × [Home](#)

Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration [Help ?](#)

### View Session Manager

[Return](#)

[General](#) ▾

General | [Security Module](#) | [NIC Bonding](#) | [Monitoring](#) | [CDR](#) | [Personal Profile Manager \(PPM\)](#) - [Connection Settings](#) | [Event Server](#) | [Expand All](#) | [Collapse All](#)

<b>SIP Entity Name</b>	SM1
<b>Description</b>	R6.1 SM
<b>Management Access Point Host Name/IP</b>	10.1.2.211
<b>Direct Routing to Endpoints</b>	Enable

[Security Module](#) ▾

<b>SIP Entity IP Address</b>	10.1.2.210
<b>Network Mask</b>	255.255.255.0
<b>Default Gateway</b>	10.1.2.1
<b>Call Control PHB</b>	46
<b>QOS Priority</b>	6
<b>Speed &amp; Duplex</b>	Auto
<b>VLAN ID</b>	



## 4.10. Add Avaya Aura™ Communication Manager as an Evolution Server


In order for Communication Manager to provide configuration and Evolution Server support to telephones, Communication Manager must be added as an application in Session Manager. This comprises a two step procedure. First, an access login must be configured on Communication Manager for the purpose of data synchronization with System Manager. Then the Application Element for that Communication Manager can be added via System Manager.

### 4.10.1. Create a Login on the Communication Manager Server

Use a web browser to access the Communication Manager maintenance web interface, and navigate to **Security → Administrator Accounts** on the left menu. Select **Add Login** and **Privileged Administrator**, as shown below. Click on **Submit**.

The screenshot displays the Avaya Aura Communication Manager maintenance web interface. The top navigation bar is red with links for Help, Log Off, Administration, and Upgrade. The left sidebar contains a tree view of maintenance tasks, with 'Security' expanded and 'Administrator Accounts' selected. The main content area is titled 'Administrator Accounts' and includes a description: 'The Administrator Accounts web pages allow you to add, delete, and modify administrator accounts.' Below this, the 'Select Action:' section offers several options: 'Add Login' (selected), 'Privileged Administrator' (selected), 'Unprivileged Administrator', 'SAT Access Only', 'Web Access Only', 'Modem Access Only', 'CDR Access Only', 'CM Messaging Access Only', 'Business Partner Login (dadmin)', 'Business Partner Craft Login', and 'Custom Login'. At the bottom, there are three rows of actions: 'Change Login' with a 'Select Login' dropdown, 'Remove Login' with a 'Select Login' dropdown, and 'Lock/Unlock Login' with a 'Select Login' dropdown. Below these is an 'Add Group' option with a 'Select Group' dropdown, and a 'Remove Group' option with a 'Select Group' dropdown. The 'Submit' and 'Help' buttons are at the bottom right.

On the next screen, enter a **Login name** and a password in the **Enter password or key** and **Re-enter password or key** fields, and click **Submit**.



Help Log Off Administration Upgrade

Administration / Server (Maintenance)

Netstat

Server

- Status Summary
- Process Status
- Shutdown Server
- Server Date/Time
- Software Version

Server Configuration

- Server Role
- Network Configuration
- Static Routes
- Display Configuration

Server Upgrades

- Manage Updates

IPSI Firmware Upgrades

- IPSI Version
- Download IPSI Firmware
- Download Status
- Activate IPSI Upgrade
- Activation Status

Data Backup/Restore

- Backup Now
- Backup History
- Schedule Backup
- Backup Logs
- View/Restore Data
- Restore History

Security

- Administrator Accounts**
- Login Account Policy
- Login Reports
- Server Access
- Syslog Server
- Authentication File
- Firewall
- Install Root Certificate
- Trusted Certificates
- Server/Application Certificates
- Certificate Alarms

### Administrator Accounts -- Add Login: Privileged Ad

This page allows you to add a login that is a member of the **SUSERS** gr

Login name:

Primary group:

Additional groups (profile):

Linux shell:

Home directory:

Lock this account: ☐

Date after which account is disabled-blank to ignore (YYYY-MM-DD):

Select type of authentication:

- ☒ Password
- ☐ ASG: enter key
- ☐ ASG: Auto-generate key

Enter password or key:

Re-enter password or key:

Force password/key change on next login:

- ☐ Yes
- ☒ No

## 4.10.2. Create an Application Element on System Manager

Return to System Manager and select **Inventory** → **Manage Elements** under the **Elements** section of the **Home** menu. Click on **New** (not shown). On the initial **Application** page select **CM** for the **Type**.

Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Inventory \* Home

Home /Elements / Inventory / Manage Elements- New Entities Instance

Help ?

**New Entities Instance**

Commit Cancel

Application \*

Application

\* Type

Select Type

Select Type

AES

Application

CM

Conferencing 6.0

JP Office

Media Gateway

Messaging

PS 6.0

PS 6.1

Session Manager

TPS

\*Required

Commit Cancel

Enter the following fields and use defaults for the remaining fields on the resulting **Application** tab:

**Name** A descriptive name

**Node** Enter the IP address for Communication Manager SAT access

Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Inventory \* Home

Home /Elements / Inventory / Manage Elements- New CM Instance

Help ?

**New CM Instance**

Commit Cancel

Application \*

Attributes \*

Application

\* Name

CM-ES R6.0.1

\* Type

CM

Reset

Description

\* Node

10.1.2.220

Access Point

Port

\*Required

Commit Cancel

Select the **Attributes** tab and enter the following:

<b>Login</b>	Login created in <b>Section 4.10.1</b>
<b>Password</b>	Password created in the previous section
<b>Confirm Password</b>	Password created in the previous section

Click on **Commit** to save.

Inventory ▾ Home /Elements / Inventory / Manage Elements- New CM Instance Help ?

**New CM Instance** Commit Cancel

Application \* **Attributes \***

SNMP Attributes ▾

\* Version ☒ None ☐ V1 ☐ V3

Attributes ▾

\* Login

Password

Confirm Password

Is SSH Connection ☒

\* Port

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled ☐

ASG Key

Confirm ASG Key

Location

### 4.10.3. Create an Application

Select **Session Manager** → **Application Configuration** → **Applications** under the **Elements** section of the **Home** menu. Click on **New** (not shown). Enter following fields and use defaults for the remaining fields and click on **Commit** to save.

**Name** A descriptive name  
**SIP Entity** Select the CM SIP Entity defined in **Section 4.5**  
**CM System for SIP Entity** Select the CM application element added in the previous section

The screenshot shows the Avaya Aura™ System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". Below the navigation bar, there are tabs for "Session Manager" and "Home". The left sidebar contains a tree view with categories like "Session Manager", "Dashboard", "Session Manager Administration", "Communication Profile Editor", "Network Configuration", "Device and Location Configuration", "Application Configuration", "Applications", "Application Sequences", "Implicit Users", "NRS Proxy Users", "System Status", and "System Tools". The main content area is titled "Application Editor" and contains the following fields:

- Name**: Text input field with value "CM-ES R6.0.1".
- SIP Entity**: Dropdown menu with value "CM-ES R6.0.1".
- CM System for SIP Entity**: Dropdown menu with value "CM-ES R6.0.1" and a "Refresh" button. A link "View/Add CM Systems" is also present.
- Description**: Text input field.
- Application Attributes (optional)**: A table with two columns: "Name" and "Value". It contains two rows: "Application Handle" and "URI Parameters", each with an associated text input field.

At the bottom of the form, there is a legend indicating that an asterisk (\*) denotes a required field. "Commit" and "Cancel" buttons are located at the top right and bottom right of the form area.

#### 4.10.4. Create an Application Sequence

Select **Session Manager** → **Application Configuration** → **Application Sequences** under the **Elements** section of the **Home** menu. Click on **New** (not shown). Enter a descriptive **Name**. Click on the + sign next to the appropriate **Available Applications** and they will move up to the **Applications in this Sequence** section. Click on **Commit** to save.

**AVAYA**Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager ×Home

Home / Elements / Session Manager / Application Configuration / Application Sequences- Application Sequences

Help ?

**Application Sequence Editor**

CommitCancel

Application Sequence

\*NameCM-ES R6.0.1

Description

Applications in this Sequence

Move FirstMove LastRemove

1 Item

	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		CM-ES R6.0.1	CM-ES R6.0.1	<input checked="" type="checkbox"/>	

Select : All, None

Available Applications

1 Item RefreshFilter: Enable

	Name	SIP Entity	Description
<input checked="" type="checkbox"/>	CM-ES R6.0.1	CM-ES R6.0.1	

#### 4.10.5. Synchronize Avaya Aura™ Communication Manager Data

Select **Inventory** → **Synchronization** → **Communication System** under the **Elements** section of the **Home** menu. Select the appropriate **Element Name**. Select **Initialize data for selected devices**. Then click on **Now**. This may take some time.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar has a menu with 'Inventory' selected. The main content area shows the path 'Home / Elements / Inventory / Synchronization / Communication System - Synchronize CM Data and Configure Options'. The title is 'Synchronize CM Data and Configure Options'. Below the title, there's a section 'Synchronize CM Data/Launch Element Cut Through' with a dropdown menu. A table lists the synchronization data for 'CM-ES R6.0.1'. The table has columns: Element Name, FQDN/IP Address, Last Sync Time, Last Translation Time, Sync Type, Sync Status, Location, and Software Version. The row for 'CM-ES R6.0.1' is highlighted. Below the table, there are radio buttons for 'Initialize data for selected devices', 'Incremental Sync data for selected devices', and 'Save Translations for selected devices'. The 'Now' button is highlighted.

Item	Refresh	Show	ALL	Filter: Enable				
<input checked="" type="checkbox"/>	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version
<input checked="" type="checkbox"/>	CM-ES R6.0.1	10.1.2.220	December 22, 2010 11:00:35 PM -05:00	12:55 am THU DEC 23, 2010	Incremental	Completed		R016x.00.1.510.1

Select : All, None

☒ Initialize data for selected devices  
☐ Incremental Sync data for selected devices  
☐ Save Translations for selected devices

**Now** Schedule Cancel Launch Element Cut Through

Use the menus on the left under **Scheduler** under the **Services** section of the **Home** menu to determine when the task is complete.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar has a menu with 'Scheduler' selected. The main content area shows the path 'Home / Services / Scheduler / Pending Jobs - Pending Jobs'. The title is 'Pending Jobs'. Below the title, there's a section 'Job List' with buttons for 'View', 'Edit', 'Delete', and 'More Actions'. A table lists the pending jobs. The table has columns: Job Type, Job Name, Job Status, State, Frequency, Scheduled By, and Element. The row for 'CSM\_CMSSynch\_INIT\_CM-ES R6.0.1\_1293132411753' is highlighted. Below the table, there are radio buttons for 'All', 'None', and 'Selected'.

Job Type	Job Name	Job Status	State	Frequency	Scheduled By	Element
<input type="checkbox"/>	PurgeJobStatus	PENDING EXECUTION	Enabled	Weekly	admin	
<input type="checkbox"/>	LogPurgeRule	PENDING EXECUTION	Enabled	Daily	admin	
<input type="checkbox"/>	ClrdAlarmPurgeRule	PENDING EXECUTION	Enabled	Daily	admin	
<input type="checkbox"/>	SoftDelRTSPurgeRule	PENDING EXECUTION	Enabled	Daily	admin	
<input checked="" type="checkbox"/>	CSM_CMSSynch_INIT_CM-ES R6.0.1_1293132411753	RUNNING	Enabled	Once	admin	CM-ES R6.0.1
<input type="checkbox"/>	CSM_CMSSynch_INCR_CM-ES R6.0.1_1289243227389	PENDING EXECUTION	Enabled	Hourly	admin	CM-ES R6.0.1
<input type="checkbox"/>	CSM_Iptcmobject_CleanupBackedupAnnc	PENDING EXECUTION	Enabled	Hourly	admin	CSM
<input type="checkbox"/>	CSM_Iptcmobject_MAINTENANCE_1289242761579	PENDING EXECUTION	Enabled	Daily	admin	CSM
<input type="checkbox"/>	sys_ConfRefreshConfig	PENDING EXECUTION	Enabled	Minutes	admin	

Select : All, None

## 4.11. Add Users for SIP Telephones

SIP telephone users must be added to Session Manager. **User Management** → **Manage Users** under the **Users** section of the **Home** menu.. Then click on **New** (not shown).

Under the **Identity** tab enter:

<b>Last Name</b>	The user's last name
<b>First Name</b>	The user's first name
<b>Login Name</b>	The desired phone extension number@domain.com where domain was defined in <b>Section 4.2</b>
<b>Password</b>	Password for user to log into System Manager (SMGR)
<b>Localized Display Name</b>	The name to be used as calling party
<b>Endpoint Display Name</b>	The name to be used as calling party
<b>Honorific</b>	Enter the appropriate information
<b>Language Preference</b>	Enter the appropriate information
<b>Time Zone</b>	Enter the appropriate information

Home /Users / User Management / Manage Users- New User Profile

**New User Profile** [Commit] [Cancel] [Help ?]

**Identity** \* Communication Profile \* Membership Contacts

Identity

\* Last Name: User

\* First Name: Avaya

Middle Name:

Description:

\* Login Name: 30050@avaya.com

\* Authentication Type: Basic

\* Password: 12345678

\* Confirm Password: 12345678

Localized Display Name: Avaya User

Endpoint Display Name: Avaya User

Honorific: Mr.

Language Preference: English

Time Zone: (-5:0)Eastern Time (US & Canada)



Select the **Communication Profile** tab.  
Under **Communication Profile** enter:

**Communication Profile Password**  
**Confirm Password**

Password to be entered by the user when logging into the phone.

Then click on **New** under **Communication Address** and enter the following and use defaults for the remaining fields:

**Type** Select **Avaya SIP**  
**Fully Qualified Address** Enter the extension number  
**@** Select the domain defined in **Section 4.2**

Click on **Add**.

Manage Users  
Public Contacts  
Shared Addresses  
System Presence ACLs

**New User Profile** Commit Cancel Help ?

Identity \* **Communication Profile \*** Membership Contacts

Communication Profile ▾

Communication Profile Password:

Confirm Password:

New Delete Done Cancel

Name
Primary

Select : None

\* Name:

Default : ☒

Communication Address ▾

New Edit Delete

Type	Handle	Domain
No Records found		

Type:

\* Fully Qualified Address:  @

Add Cancel

Navigate to **Session Manager Profile** and click on the checkbox to expand the section. Select the appropriate Session Manager server for **Primary Session Manager**. For **Origination Application Sequence** and **Termination Application Sequence** select the application sequence created in **Section 4.10.4**. Select the location defined in **Section 4.3** for **Home Location**. Navigate to **Endpoint Profile** and click on the checkbox to expand the section. Enter the following fields and use defaults for the remaining fields. Click on **Commit** to save (not shown).<sup>4</sup>

**System** Select the CM Entity  
**Profile Type** Select **Endpoint**  
**Extension** Enter a desired extension number  
**Template** Select a telephone type template  
**Port** Select **IP**  
**Voice Mail Number** Enter the voice messaging access number

☒ Session Manager Profile ▾

\* Primary Session Manager

SM1 ▾

Primary	Secondary	Maximum
11	0	11

Secondary Session Manager

(None) ▾

Primary	Secondary	Maximum

Origination Application Sequence

CM-ES R6.0.1 ▾

Termination Application Sequence

CM-ES R6.0.1 ▾

Survivability Server

(None) ▾

\* Home Location

BaskingRidge HQ ▾

\* System

CM-ES R6.0.1 ▾

\* Profile Type

Endpoint ▾

Use Existing Endpoints

☐

\* Extension

30050

Endpoint Editor

\* Template

DEFAULT\_9630SIP\_CM\_6\_0 ▾

Set Type

9630SIP

Security Code

\* Port

IP

Voice Mail Number

33000

Delete Endpoint on Unassign of Endpoint

☐

<sup>4</sup> Note that when **Use Existing Endpoints** is not checked, Session Manager will automatically create station and off-pbx station-mapping forms in Communication Manager. This section should not be completed until the data synchronization task created in **Section 4.10.5** has completed.

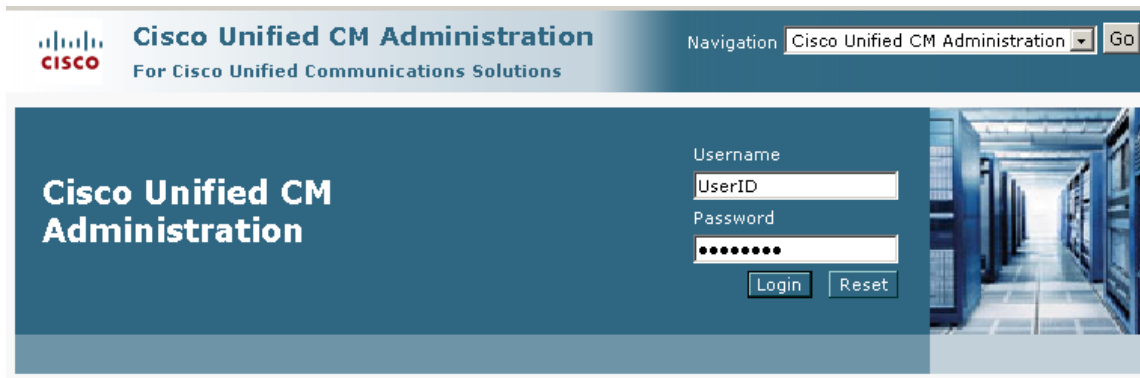
## 5. Configure Cisco UCM

This section provides the procedures for configuring Cisco UCM. These Application Notes assumed that the basic configuration needed to support Cisco IP telephones has been completed. For further information on Cisco UCM, see references [7-9]. The procedures include the following areas:

- Log in to Cisco UCM
- Configure SIP Domain
- Configure SIP Trunk Security Profile
- Configure SIP Trunk
- Configure Route Pattern
- Configure Audio Codecs
- Configure Music on Hold
- Configure Voicemail Pilot
- Configure Voicemail Profile
- Configure a Telephone

### 5.1. Log in to Cisco UCM

Open Cisco Unified CM Administration by entering the IP address of the Cisco UCM into the Web Browser address field, and log in using an appropriate **Username** and **Password**.



## 5.2. Administer SIP Domain

Select **System** → **Enterprise Parameters**. Scroll down to the heading **Clusterwide Domain Configuration**. Ensure that the **Organization Top Level Domain** matches the SIP domain configured in Session Manager and Communication Manager. Recall that “avaya.com” has been used throughout the sample configuration.

The screenshot displays the Cisco Unified CM Administration interface. At the top, the Cisco logo and 'Cisco Unified CM Administration' title are visible. Below the title bar, a navigation menu includes 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', and 'Bulk Administration'. The main heading is 'Enterprise Parameters Configuration'. Below this, there are icons for 'Save', 'Set to Default', 'Reset', and 'Apply Config'. The first parameter shown is 'IPCC Express Installed' with a value of 'false'. The 'Clusterwide Domain Configuration' section is highlighted with a red box and contains two parameters: 'Organization Top Level Domain' with the value 'avaya.com', and 'Cluster Fully Qualified Domain Name' which is empty. Below this is the 'Denial-of-Service Protection' section, which includes 'Denial-of-Service Protection' set to 'True'.

Clusterwide Domain Configuration	
Organization Top Level Domain	avaya.com
Cluster Fully Qualified Domain Name	

Denial-of-Service Protection	
Denial-of-Service Protection *	True

### 5.3. Administer SIP Trunk Security Profile

Select **System** → **Security Profile** → **SIP Trunk Security Profile** from the top menu then click **Add New** to add a new SIP Trunk Security Profile.






The screenshot shows the Cisco Unified CM Administration web interface in Microsoft Internet Explorer. The address bar displays the URL: `https://172.29.5.20/ccmadmin/sipTrunkSecurityProfileFindList.do?<%=reqParams%>&recCnt=4&colCnt=3`. The page title is "Find and List SIP Trunk Security Profiles". Below the title bar, there are navigation tabs: System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area has a sub-header "Find and List SIP Trunk Security Profiles" and a toolbar with buttons: Add New, Select All, Clear All, and Delete Selected. Below this, a status box indicates "1 records found". The main table displays the following data:

SIP Trunk Security Profile (1 - 1 of 1)	
Name	Description
<a href="#">Non Secure SIP Trunk Profile</a>	Non Secure SIP Trunk Profile authenticated by null String

At the bottom of the table, there is a row of buttons: Add New, Select All, Clear All, and Delete Selected. The "Add New" button is circled in red.


The following is a screen capture of the **SIP Trunk Security Profile Configuration** used in the sample network. Configure the highlighted areas, noting that to allow MWI (Message Waiting Indicator) messages to be accepted by Cisco UCM from Modular Messaging, the SIP Trunk provisioned towards Session Manager needs to be able to **Accept Unsolicited Notification**. Click **Save** to commit the changes.

**SIP Trunk Security Profile Configuration**

 Save  Delete  Copy  Reset  Add New

---

**Status**

 Status: Ready

---

**SIP Trunk Security Profile Information**

Name\*

Avaya

Description

SIP connection to Avaya

Device Security Mode

Non Secure

Incoming Transport Type\*

TCP+UDP

Outgoing Transport Type

TCP

☐ Enable Digest Authentication

Nonce Validity Time (mins)\*

600

X.509 Subject Name

Incoming Port\*

5060

☐ Enable Application Level Authorization

☒ Accept Presence Subscription

☒ Accept Out-of-Dialog REFER

☒ Accept Unsolicited Notification

☒ Accept Replaces Header

☐ Transmit Security Status

Save

Delete

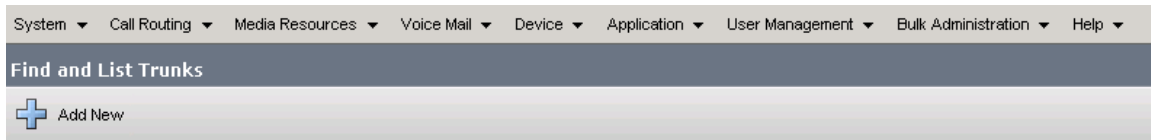
Copy

Reset

Add New

## 5.4. Administer SIP Trunk

Add a new SIP trunk by selecting **Device** → **Trunk** from the top menu then click **Add New** to begin adding a new SIP trunk.



Select “SIP Trunk” as the **Trunk Type** and the **Device Protocol** field will automatically be changed to “SIP”. Click **Next** to continue.

This screenshot shows the 'Trunk Configuration' page in the Cisco Unified CM Administration interface. The page has a header with the Cisco logo and the title 'Cisco Unified CM Administration For Cisco Unified Communications Solutions'. Below the header is a navigation bar with links for System, Call Routing, Media Resources, Voice Mail, Device, and Application. The main content area is titled 'Trunk Configuration' and features a green arrow pointing right with the text 'Next'. Below this is a 'Status' section with an information icon and the text 'Status: Ready'. The 'Trunk Information' section contains two dropdown menus: 'Trunk Type\*' set to 'SIP Trunk' and 'Device Protocol\*' set to 'SIP'. At the bottom of the form is a 'Next' button. A footnote at the bottom left states: '\*- indicates required item.'

Enter the appropriate information for the SIP Trunk in each section. The following screens show the configuration used in the sample network. The important fields to configure are listed before each screen

**Device Name**

An informative name

**Description**

Any note for this trunk

**Media Resource Group List**

Select from the list (see **Section 5.7**)

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help

**Trunk Configuration**

Save Delete Reset Apply Config Add New

**Status**  
Status: Ready

**Device Information**

Product: SIP Trunk  
Device Protocol: SIP  
Device Name\*: SM61  
Description: Session Manager 6.1  
Device Pool\*: Default  
Common Device Configuration: < None >  
Call Classification\*: Use System Default  
Media Resource Group List: MoH  
Location\*: Hub\_None  
AAR Group: < None >  
Packet Capture Mode\*: None  
Packet Capture Duration: 0  
☐ Media Termination Point Required  
☒ Retry Video Call as Audio  
☐ Transmit UTF-8 for Calling Party Name  
☐ Unattended Port  
☐ SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security.  
Use Trusted Relay Point\*: Default



Under **Call Routing Information**:

**Remote-Party-Id**      Checked to send  
**Asserted-Identity**      Checked to send caller information

Cisco UCM must be configured to populate the Diversion header with the appropriate reason code when a call is forwarded to voice mail. Ensure that **Redirecting Diversion Header Delivery - Outbound** is selected under **Outbound Calls** section, as shown below.

Call Routing Information	
<input checked="" type="checkbox"/> Remote-Party-Id	
<input checked="" type="checkbox"/> Asserted-Identity	
Asserted-Type*	Default
SIP Privacy*	Default
Inbound Calls	
Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	
<input type="checkbox"/> Redirecting Diversion Header Delivery - Inbound	
Outbound Calls	
Called Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Called Party Transformation CSS	
Calling Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Calling Party Transformation CSS	
Calling Party Selection*	Originator
Calling Line ID Presentation*	Default
Calling Name Presentation*	Default
Caller ID DN	
Caller Name	
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Outbound	

Navigate to the **SIP Information** section and enter following:

**Destination Address** IP address of the Session Manager signaling interface  
**Destination Port** Destination port number use for SIP communication  
**SIP Trunk Security Profile** Profile configured in **Section 5.3**  
**DTMF Signaling Method** Default **No Preference** (will result in RFC2833)

Click **Save** to complete.

SIP Information	
Destination Address	10.1.2.210
Destination Address IPv6	
<input type="checkbox"/> Destination Address is an SRV	
Destination Port*	5060
MTP Preferred Originating Codec*	711ulaw
Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Avaya
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
DTMF Signaling Method*	No Preference

## 5.5. Administer Route Pattern

To configure a route pattern, a Route Group must be defined that includes the SIP trunk, and a Route List must be defined that references the Route Group. Then the Route Pattern will select the Route List for the configured dial pattern.

Add a Route Group by selecting **Call Routing** → **Route/Hunt** → **Route Group** and click **Add New**. Enter a **Route Group Name**, and under **Find Devices to Add to Route Group** select the SIP trunk previously created, and click on **Add to Route Group**. The screen below shows the result of doing this, with the SIP trunk name (“SM61”) appearing under **Current Route Group Members** in the **Selected Devices** window. Click **Save** to save the configuration.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

**Route Group Configuration**

Save Delete Add New

**Route Group Information**

Route Group Name\* SM61-RteGrp

Distribution Algorithm\* Circular ▾

**Route Group Member Information**

**Find Devices to Add to Route Group**

Device Name contains Find

Available Devices\*\*

Avaya_G430
SIP2MASmwi
SM2-SIP-TLS
<b>SM61</b>
To_IPOffice

Port(s) None Available ▾

Add to Route Group


**Current Route Group Members**

Selected Devices\*\*\* SM61 (All Ports) ▼

Removed Devices\*\*\*\*







Reverse Order of Selected Devices

Next, add a Route List by selecting **Call Routing → Route/Hunt → Route List**, then click **Add New**. Enter a **Name**, an optional **Description**, select **Default** for **Cisco Unified Communications Manager Group**, and click on **Add Route Group**.


**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk A

**Route List Configuration**

 Save  Delete  Copy  Reset  Apply Config  Add New

**Status**

 Status: Ready

**Route List Information**

☒ Device is trusted

Name *	SMR6.1-RtLst
Description	Session Manager R6.1
Cisco Unified Communications Manager Group *	Default ▾

☒ Enable this Route List (change effective on Save; no reset required)

**Route List Member Information**

Selected Groups\*\*

▼▲

**Add Route Group**

Removed Groups\*\*\*

On the screen that follows (below), select the Route Group Previously created, leaving the remaining fields as their default values. Click on **Save**, and then on **OK** in the subsequent dialogue box.

The screenshot displays the Cisco Unified CM Administration web interface. At the top, the navigation bar includes links for System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled "Route List Detail Configuration". A "Save" button is visible on the left. A "Status" section shows "Status: Ready". A "Route List Member Information" section is highlighted with a red box, showing "Route Group\*" set to "SM61-RteGrp -[NON-QSIG]". Below this, the "Calling Party Transformations" section contains fields for "Use Calling Party's External Phone Number Mask\*" (Default), "Calling Party Transform Mask", "Prefix Digits (Outgoing Calls)", "Calling Party Number Type\*" (Cisco CallManager), and "Calling Party Numbering Plan\*" (Cisco CallManager). The "Called Party Transformations" section contains fields for "Discard Digits" (< None >), "Called Party Transform Mask", "Prefix Digits (Outgoing Calls)", "Called Party Number Type\*" (Cisco CallManager), and "Called Party Numbering Plan\*" (Cisco CallManager). A "Microsoft Internet Explorer" dialog box is overlaid on the form, stating: "The settings for this Route List member are about to be saved. You must reset the Route List for changes to take effect. Click OK to return to the current Route List, or Cancel to stay on the Route List Detail page." The dialog box has "OK" and "Cancel" buttons.

The screen returns to the Route List definition, with the selected Route List Group shown in the **Selected Groups** window under **Route List Member Information**. Click **Reset**.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Ad

**Route List Configuration**

Save Delete Copy **Reset** Apply Config Add New

**Status**  
Status: Ready

**Route List Information**

☒ Device is trusted  
Name\* SMR6.1-RtLst  
Description Session Manager R6.1  
Cisco Unified Communications Manager Group\* Default ▾  
☒ Enable this Route List (change effective on Save; no reset required)

**Route List Member Information**

Selected Groups\*\* SM61-RteGrp

▼ ▲ Add Route Group

Removed Groups\*\*\*

Select **Call Routing** → **Route/Hunt** → **Route Pattern** then click **Add New** to add a new route pattern for extension range 3xxxx which includes the Modular Messaging access number 33000, as well as calls to telephones registered to Avaya Session Manager and Communication Manager. Calls to Cisco UCM telephones that are redirected to voice mail will be routed to Modular Messaging using extension 33000.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾

**Find and List Route Patterns**

+ Add New

The following screen shows the route pattern used in the sample network. The route pattern **3xxxx** will cause all 5 digit calls beginning with 3 to be routed using the **Gateway/Route List** choice of “SM6.1-RtLst” that was just defined. Parameters on this screen other than those indicated below can be left at their default values. Click **Save** to complete the form.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

**Route Pattern Configuration**

Save Delete Copy Add New

**Status**  
Status: Ready

**Pattern Definition**

Route Pattern\* 3XXXX

Route Partition < None >

Description To CM R6.0.1 stations

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence\* Default

Resource Priority Namespace Network Domain < None >

Gateway/Route List\* SMR6.1-RtLst (Edit)

Route Option  
☒ Route this pattern  
☐ Block this pattern No Error

Call Classification\* OffNet

☐ Allow Device Override ☒ Provide Outside Dial Tone ☐ Allow Overlap Sending ☐ Urgent Priority

☐ Require Forced Authorization Code

Authorization Level\* 0

☐ Require Client Matter Code

## 5.6. Configure Audio Codecs

Select **System** → **Region** from the top menu and select the **default** profile. Under **Modify Relationship to other Regions**, select **Default** under **Regions** and **G.722** under **Audio Codec**. This will select the G.722 codec as first choice. If the endpoints involved in a particular call do not support this high fidelity codec, then G.711 will be used.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | interop | About

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

**Region Configuration** Related Links: [Back To Find/List](#)

Save X Delete Reset Add New

**Status**  
Update successful  
Click on the Reset button to have the changes take effect.

**Region Information**  
Name: Default

**Region Relationships**

Region	Audio Codec	Video Call Bandwidth	Link Loss Type
Default	G.711	384	Use System Default

NOTE: Regions(s) not displayed Use System Default Use System Default Use System Default

**Modify Relationship to other Regions**

Regions	Audio Codec	Video Call Bandwidth	Link Loss Type
Default JamesMMTest	G.722	<input checked="" type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input type="text"/> kbps	Keep Current Setting

Save Delete Reset Add New

Click **Save** to save configuration.



## 5.7. Configure Music on Hold

Several steps are required to configure music on hold for calls from Avaya users. Select **Media Resources** → **Media Resource Group** from the top menu, and click **Add New**. In the screen that follows, under **Media Resource Group Information**, enter a **Name** and optional **Description**. Under **Devices for this Group**, select a music-on-hold server in the **Available Media Resources** box and click ▼ to move it to the **Selected Media Resources** box. The screen below was taken after clicking ▼. Click **Save**.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk

**Media Resource Group Configuration**

Save Delete Copy Add New

**Status**  
 Status: Ready

**Media Resource Group Status**  
Media Resource Group: MoH\_Fred (used by 28 devices)

**Media Resource Group Information**

Name\*   
Description

**Devices for this Group**

Available Media Resources\*\*

Selected Media Resources\*

☐ Use Multicast for MOH Audio (If at least one multicast MOH resource is available)

Save Delete Copy Add New

Select **Media Resources** → **Media Resource Group List** from the top menu, and click **Add New**. In the screen that follows, under **Media Resource Group List Information**, enter a **Name**. Under **Media Resource Groups for this List**, select a media resource group in the **Available Media Resource Groups** box and click ▼ to move it to the **Selected Media Resource Groups** box. The screen below was taken after clicking ▼. Click **Save**.

The screenshot shows the Cisco Unified CM Administration web interface. The top navigation bar includes links for System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, and Bulk. The main title is "Cisco Unified CM Administration For Cisco Unified Communications Solutions". Below the navigation bar is a section titled "Media Resource Group List Configuration". This section contains several tabs: Save, Delete, Copy, and Add New. The "Status" section shows "Status: Ready". The "Media Resource Group List Status" section shows "Media Resource Group List: MoH (used by 28 devices)". The "Media Resource Group List Information" section has a "Name\*" field with the value "MoH". The "Media Resource Groups for this List" section shows two boxes: "Available Media Resource Groups" and "Selected Media Resource Groups". The "Selected Media Resource Groups" box contains the value "MoH". A red box highlights the "MoH" text in the "Selected Media Resource Groups" box, and a red box highlights the downward arrow button between the two boxes. At the bottom of the page are buttons for Save, Delete, Copy, and Add New.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk ▾

**Media Resource Group List Configuration**

Save Delete Copy Add New

**Status**  
Status: Ready

**Media Resource Group List Status**  
Media Resource Group List: MoH (used by 28 devices)

**Media Resource Group List Information**  
Name\* MoH

**Media Resource Groups for this List**  
Available Media Resource Groups  
Selected Media Resource Groups MoH

Save Delete Copy Add New

Finally, to provide music on hold on held calls and ringback on transferred calls to Avaya callers into Cisco UCM, select **System** → **Service Parameters** from the top menu. On the screen that follows, select the Cisco UCM from **Server**, and **Cisco CallManager (Active)** from **Service**.



**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bu ▾

**Service Parameter Configuration**

Save Set to Default Advanced

**Status**  
Status: Ready

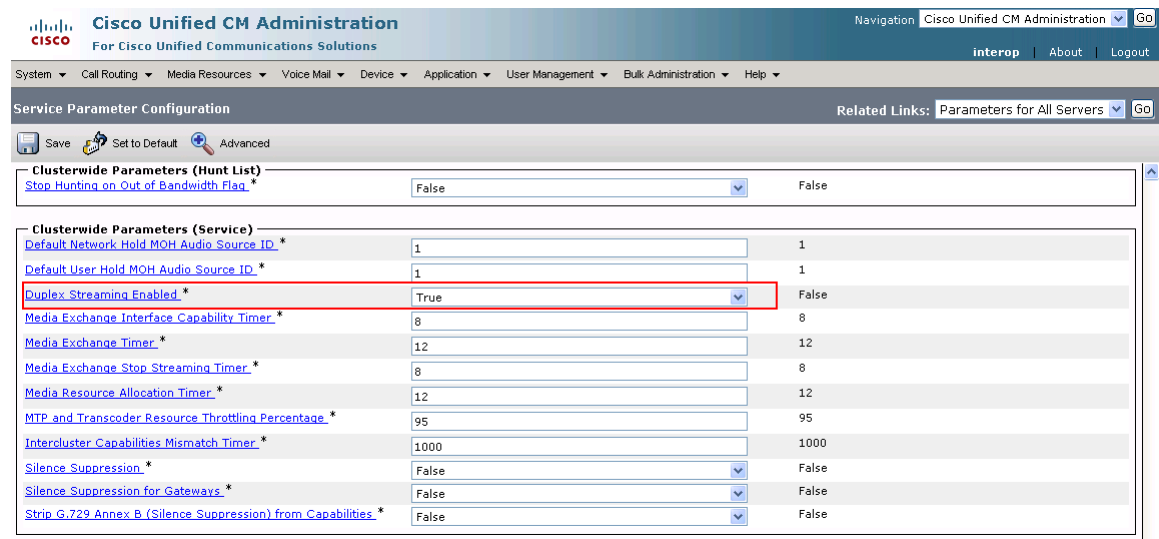
**Select Server and Service**

Server\* cucm7 (Active) ▾

Service\* Cisco CallManager (Active) ▾

All parameters apply only to the current server except parameters that are in the Clusterwide group(s).

On the following screen, scroll down to **Clusterwide Parameters (Service)**, and Select **True** for **Duplex Streaming Enabled**. Click **Save**.



**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration ▾ Go

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

**Service Parameter Configuration** Related Links: Parameters for All Servers ▾ Go

Save Set to Default Advanced

**Clusterwide Parameters (Hunt List)**

Stop Hunting on Out of Bandwidth Flag \* False ▾ False

**Clusterwide Parameters (Service)**

Default Network Hold MOH Audio Source ID *	1	1
Default User Hold MOH Audio Source ID *	1	1
Duplex Streaming Enabled *	True ▾	False
Media Exchange Interface Capability Timer *	8	8
Media Exchange Timer *	12	12
Media Exchange Stop Streaming Timer *	8	8
Media Resource Allocation Timer *	12	12
MTP and Transcoder Resource Throttling Percentage *	95	95
Intercluster Capabilities Mismatch Timer *	1000	1000
Silence Suppression *	False ▾	False
Silence Suppression for Gateways *	False ▾	False
Strip G.729 Annex B (Silence Suppression) from Capabilities *	False ▾	False

## 5.8. Configure Voice Mail Pilot

Configure voice mail coverage for telephone users. Select **Voice Mail → Voice Mail Pilot** from the top menu then click **Add New** to add a new Voicemail Pilot. Enter the **Voice Mail Pilot Number** (“33000”, the Modular Messaging access number in the sample configuration), a **Description** and check the box next to **Make this the default Voice Mail Pilot for the system**. Click **Save** to save configuration. See [10] for details on configuring Modular Messaging support for Cisco UCM via Session Manager.

The screenshot shows the Cisco Unified CM Administration web interface. At the top, the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions" are visible. Below this is a navigation bar with tabs: System, Call Routing, Media Resources, Voice Mail, Device, and Application. The "Voice Mail" tab is selected, and the "Voice Mail Pilot Configuration" page is displayed. The page has a header bar with "Save", "Delete", and "Add New" buttons. The main content area is divided into two sections. The first section, titled "Status", shows an information icon and the text "Status: Ready". The second section, titled "Voice Mail Pilot Information", contains three input fields: "Voice Mail Pilot Number" with the value "33000", "Calling Search Space" with a dropdown menu showing "< None >", and "Description" with the value "MM via ASM R6". Below these fields is a checkbox labeled "Make this the default Voice Mail Pilot for the system", which is checked. At the bottom of the page, there are three buttons: "Save", "Delete", and "Add New".

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application

**Voice Mail Pilot Configuration**

Save Delete Add New

**Status**

Status: Ready

**Voice Mail Pilot Information**

Voice Mail Pilot Number

Calling Search Space

Description

☒ Make this the default Voice Mail Pilot for the system

## 5.9. Configure Voice Mail Profile

Select **Voice Mail** → **Voice Mail Profile** from the top menu then click **Add New** to add a new Voicemail Profile. Enter **Voice Mail Profile Name** and select the **Voice Mail Pilot** from the drop down list as defined in **Section 5.8**. Click **Save** to save the configuration.

The screenshot shows the Cisco Unified CM Administration web interface. At the top, the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions" are visible. Below this is a navigation bar with tabs: System, Call Routing, Media Resources, Voice Mail, Device, and Application. The "Voice Mail" tab is selected, and the "Voice Mail Profile Configuration" page is displayed. The page has a header bar with icons for Save, Delete, Copy, Reset, and Add New. The main content area is divided into sections. The "Status" section shows an information icon and the text "Status: Ready". The "Voice Mail Profile Information" section contains several fields: "Voice Mail Profile" is set to "ASM\_R6 (used by 3 devices)"; "Voice Mail Profile Name\*" is a text field containing "ASM\_R6"; "Description" is an empty text field; "Voice Mail Pilot\*\*" is a dropdown menu showing "33000/< None >"; and "Voice Mail Box Mask" is an empty text field. Below these fields is a checkbox labeled "Make this the default Voice Mail Profile for the System". At the bottom of the page, there is a row of buttons: Save, Delete, Copy, Reset, and Add New.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾

**Voice Mail Profile Configuration**

Save Delete Copy Reset Add New

— **Status** —

Status: Ready

— **Voice Mail Profile Information** —

Voice Mail Profile ASM\_R6 (used by 3 devices)

Voice Mail Profile Name\* ASM\_R6

Description

Voice Mail Pilot\*\* 33000/< None >

Voice Mail Box Mask

☐ Make this the default Voice Mail Profile for the System

— —

## 5.10. Configure a Telephone

Select **Device** → **Phone** then click on the telephone to be configured. The following screen shows the display after a telephone has been selected. Under **Device Information**, select the **Media Resource Group List** created in **Section 5.7**. Click on the line for the telephone as highlighted in the screen below.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | interop | About | Logout

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Phone Configuration | Related Links: Back To Find/List

Save | Delete | Copy | Reset | Add New

**Status**  
Status: Ready

**Association Information**

	Modify Button Items
1	Line [1] - 60015 (no partition)
2	Line [2] - Add a new DN
3	Add a new SD
4	Add a new SD
5	Add a new SD
6	Add a new SD
7	Add a new SD
8	Add a new SD
----- Unassigned Associated Items -----	
9	Add a new SD
10	Add a new BLF Directed Call Park
11	Do Not Disturb

**Phone Type**  
Product Type: Cisco 7975  
Device Protocol: SIP

**Device Information**

Registered with Cisco Unified Communications Manager cucm7

IP Address: 172.29.5.162

MAC Address\*: 001D45E95E7A

Description: 7975 R7

Device Pool\*: Default [View Details](#)

Common Device Configuration: < None > [View Details](#)

Phone Button Template\*: Standard 7975 SIP

Softkey Template: < None >

Common Phone Profile\*: Standard Common Phone Profile

Calling Search Space: < None >

AAR Calling Search Space: < None >

Media Resource Group List: MoH

The following screen shows the display after the line has been selected. Enter information for **Directory Number**, **Description**, **Alerting Name** and **ASCII Alerting Name**.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Admin

Directory Number Configuration

Save | Delete | Reset | Add New

**Status**  
Status: Ready

**Directory Number Information**

Directory Number\*: 60015

Route Partition: < None >

Description: 7975 SIP R7

Alerting Name: 7975 R7

ASCII Alerting Name: 7975 R7

☒ Allow Control of Device from CTI

Associated Devices: SEP001D45E95E7A

[Edit Device](#) [Edit Line Appearance](#)

Dissociate Devices:

Navigate to **Directory Number Settings** and select the **Voice Mail Profile** created in **Section 5.9**.

Directory Number Settings	
Voice Mail Profile	ASM_R6 (Choose <None> to use system default)
Calling Search Space	< None >
Presence Group*	Standard Presence group
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Auto Answer*	Auto Answer Off

Navigate to **Call Forward and Call Pickup Settings**. Check all the call forward related parameters as shown below.

Call Forward and Call Pickup Settings			
	Voice Mail	Destination	Calling Search Space
Calling Search Space Activation Policy			Use System Default
Forward All	<input type="checkbox"/> or		< None >
Secondary Calling Search Space for Forward All			< None >
Forward Busy Internal	<input checked="" type="checkbox"/> or		< None >
Forward Busy External	<input checked="" type="checkbox"/> or		< None >
Forward No Answer Internal	<input checked="" type="checkbox"/> or		< None >
Forward No Answer External	<input checked="" type="checkbox"/> or		< None >
Forward No Coverage Internal	<input checked="" type="checkbox"/> or		< None >
Forward No Coverage External	<input checked="" type="checkbox"/> or		< None >
Forward on CTI Failure	<input checked="" type="checkbox"/> or		< None >
Forward Unregistered Internal	<input checked="" type="checkbox"/> or		< None >
Forward Unregistered External	<input checked="" type="checkbox"/> or		< None >
No Answer Ring Duration (seconds)			
Call Pickup Group		< None >	

Navigate to the **Line 1 on Device** section and enter information for **Display (Internal Caller ID)** and **ASCII Display (Internal Caller ID)**. This will be displayed on the called party phone on all outgoing calls.

Line 1 on Device SEP001D45E95E7A	
Display (Internal Caller ID)	7975 R7
Display text for a line appearance is intended for displaying text such as a name instead of a number for internal calls. If you specify a number, the person receiving a call may not see the proper identity of the caller.	
ASCII Display (Internal Caller ID)	7975 R7
Line Text Label	
ASCII Line Text Label	
External Phone Number Mask	
Visual Message Waiting Indicator Policy*	Use System Policy
Audible Message Waiting Indicator Policy*	Off
Ring Setting (Phone Idle)*	Use System Default
Ring Setting (Phone Active)	Use System Default
Applies to this line when any line on the phone has a call in progress.	
Call Pickup Group Audio Alert Setting(Phone Idle)	Use System Default
Call Pickup Group Audio Alert Setting(Phone Active)	Use System Default
Recording Option*	Call Recording Disabled
Recording Profile	< None >
Monitoring Calling Search Space	< None >

Check all boxes in **Forwarded Call Information Display on Device** section. Click **Save** to complete.

**Forwarded Call Information Display on Device SEP001D45E95E7A**

☒ Caller Name

☒ Caller Number

☒ Redirected Number

☒ Dialed Number

**Users Associated with Line**

Associate End Users

Save

Delete

Reset

Add New

Repeat steps in this section for all phones that will use Modular Messaging for voice messaging services.



## 6. Verification Steps

This section provides the tests that can be performed on Communication Manager, Session Manager, and Cisco UCM to verify their proper configuration.

### 6.1. Verify Avaya Aura® Communication Manager

Verify the status of the SIP trunk to Session Manager. Use the **status signaling-group n** command, where **n** is the signaling group number. Verify that the **Group State** is **in-service**.

```
status signaling-group 60
                        STATUS SIGNALING GROUP

      Group ID: 60
      Group Type: sip

      Group State: in-service
```

Verify the status of the trunk group by using the **status trunk n** command, where **n** is the trunk group number. Verify that all trunks are in the **in-service/idle** state as shown below.

```
status trunk 60

                        TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                        Busy

0060/001 T00199   in-service/idle    no
0060/002 T00200   in-service/idle    no
0060/003 T00201   in-service/idle    no
0060/004 T00202   in-service/idle    no
0060/005 T00203   in-service/idle    no
0060/006 T00204   in-service/idle    no
0060/007 T00205   in-service/idle    no
0060/008 T00206   in-service/idle    no
0060/009 T00207   in-service/idle    no
0060/010 T00208   in-service/idle    no
0060/011 T00219   in-service/idle    no
0060/012 T00220   in-service/idle    no
0060/013 T00221   in-service/idle    no
0060/014 T00222   in-service/idle    no
```

## 6.2. Verify Avaya Aura® Session Manager

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** on the left panel. Verify that the SIP Entity Links for Communication Manager and Cisco UCM are up, indicating that they are all reachable for routing.

### SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

#### Entity Link Status for All Session Manager Instances

[Run Monitor](#)

1 Item | [Refresh](#)

<input type="checkbox"/>	Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
<input type="checkbox"/>	<a href="#">SM1</a>	20/35	1	0	3

Select : All, None

#### All Monitored SIP Entities

[Run Monitor](#)

32 Items | [Refresh](#) | Show [15](#) | Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	<a href="#">AACR6</a>
<input type="checkbox"/>	<a href="#">ACE</a>
<input type="checkbox"/>	<a href="#">AG2330</a>
<input type="checkbox"/>	<a href="#">AllanC-S8300-G350</a>
<input type="checkbox"/>	<a href="#">alpinemas1</a>
<input type="checkbox"/>	<a href="#">AudioCodes M1000</a>
<input type="checkbox"/>	<a href="#">AuraSBC</a>
<input type="checkbox"/>	<a href="#">BC-AuraSBC</a>
<input type="checkbox"/>	<a href="#">BR2 AudioCodes MP114</a>
<input type="checkbox"/>	<a href="#">BR2 AudioCodes MP118</a>
<input type="checkbox"/>	<a href="#">CallCenter</a>
<input type="checkbox"/>	<a href="#">CM-ES R6.0.1</a>
<input type="checkbox"/>	<a href="#">Cisco-UCM7</a>

On the above screen under **All Monitored SIP Entities**, click on the SIP Entity names for Communication Manager (**CM-ES R6.0.1**) and Cisco UCM (**Cisco-UCM7**) and verify that the **Link Status** is **Up**, as shown below:

### Avaya Aura™ System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Session Manager](#) × [Session Manager](#) × [Home](#)

[Home](#) / [Elements](#) / [Session Manager](#) / [System Status](#) / [SIP Entity Monitoring- SIP Entity Monitoring](#)

[Help ?](#)

### SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

#### All Entity Links to SIP Entity: CM-ES R6.0.1

[Summary View](#)

1 Item | [Refresh](#)

Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
<input type="checkbox"/> Show	<a href="#">SM1</a>	10.1.2.220	5060	TCP	Up	200 OK	Up

Session Manager x Session Manager x Home

Home /Elements / Session Manager / System Status / SIP Entity Monitoring- SIP Entity Monitoring

**SIP Entity, Entity Link Connection Status** [Help ?](#)

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

[All Entity Links to SIP Entity: Cisco-UCM7](#)

[Summary View](#)

1 Item | Refresh Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
<input type="checkbox"/> Show	SM1	172.29.5.20	5060	TCP	Up	200 OK	Up

Call traffic can be traced by selecting **Elements → Session Manager → System Tools → SIP Tracer Configuration** as shown below. Under **Session Manager Instances**, select the Session Manager for which tracing will be enabled. See reference [2] for details on available SIP tracing and filtering options.

Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin

Session Manager x Session Manager x Home

Home /Elements / Session Manager / System Tools / SIP Tracer Configuration- SIP Tracer Configuration

**Tracer Configuration** [Help ?](#) [Read](#) [Commit](#)

This page allows you to configure the tracer configuration properties for one or more Security Modules.

**Tracer Configuration**

Tracer Enabled: ☒

Trace All Messages: ☒

From Network to Security Module: ☒ From Security Module to Network: ☒

From Server to Security Module: ☐ From Security Module to Server: ☐

Trace Dropped Messages: ☒ Max Dropped Message Count:

Send Trace to a Remote Server: ☐

Remote Server FQDN or IP Address:  Send Trace Method:

Tunnel Port:

---

**User Filter** [New](#) [Delete](#)

	From	To	Source	Destination	Max Message Count
--	------	----	--------	-------------	-------------------

---

**Call Filter** [New](#) [Delete](#)

	From	To	Source	Destination	Max Call Count	Request URI
--	------	----	--------	-------------	----------------	-------------

---

**Session Manager Instances**

1 Item | Refresh Filter: Enable

<input checked="" type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	SM1	R6.1 SM

Select : All, None

[Read](#) [Commit](#)

Once the tracer configuration has been established, SIP message traces can be specified by selecting **Elements → Session Manager → System Tools → SIP Trace Viewer**. Set the appropriate **Filter** options for the desired trace time period (details not shown). The following screen shows an example of a trace for a call from an Avaya user to a Cisco user. Details of the INVITE can be shown under each entry by clicking on **Show** under the **Details** column. Below, the entry is already expanded, and the details can be hidden by clicking on **Hide** under the **Details** column.

Home / Elements / Session Manager / System Tools / SIP Trace Viewer- SIP Trace Viewer
Help ?

**Trace Viewer**
Commit

Filter | Trace Viewer |  
Expand All | Collapse All

Filter ▾

Trace Viewer ▾

Dialog Filter Cancel Hide dropped messages More Actions ▾
Number of retrieved records: 9755

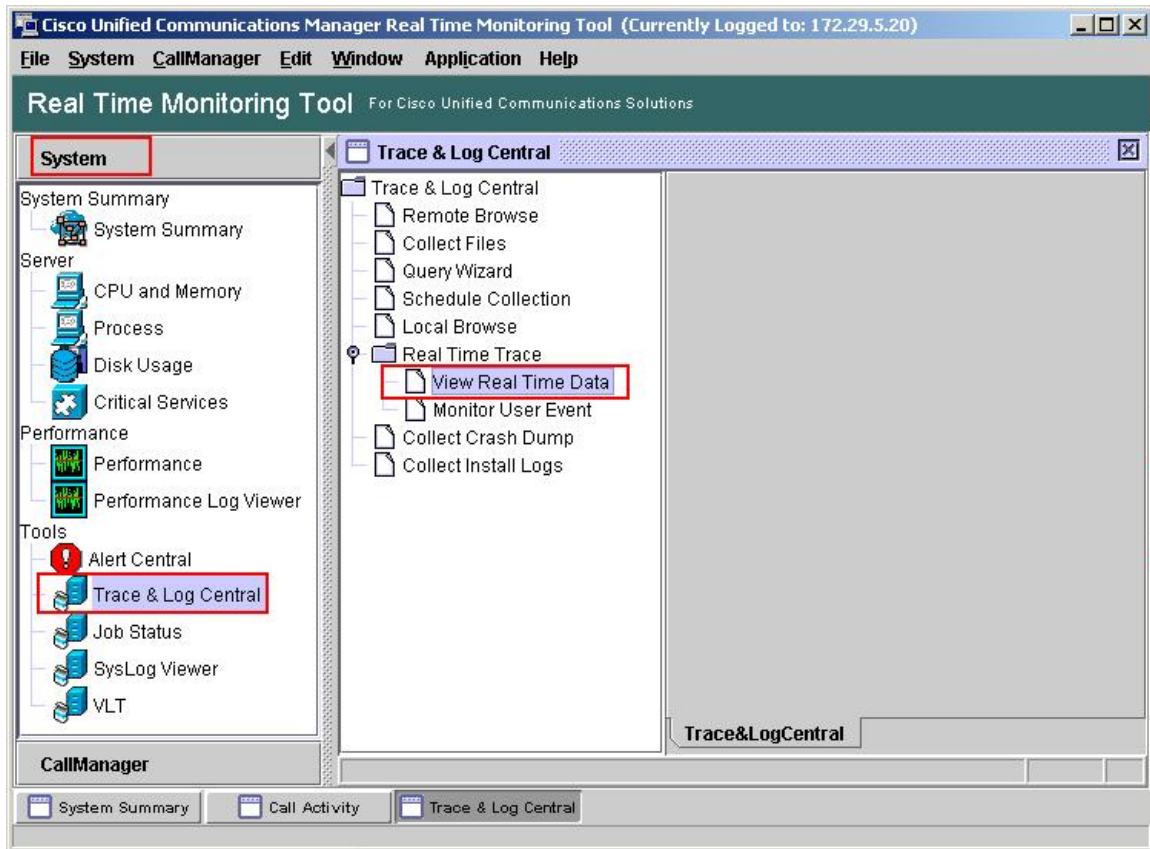
10536 Items Refresh Filter: Enable

	Details	Time	Tracing Entity	From	Action	To	Protocol	Call
<input type="radio"/>	▼ Hide	10:37:22.437	SM1	sip:36004@avaya.com	-- INVITE -->	sip:60015@avaya.com	TCP	1f9_2 2c74e

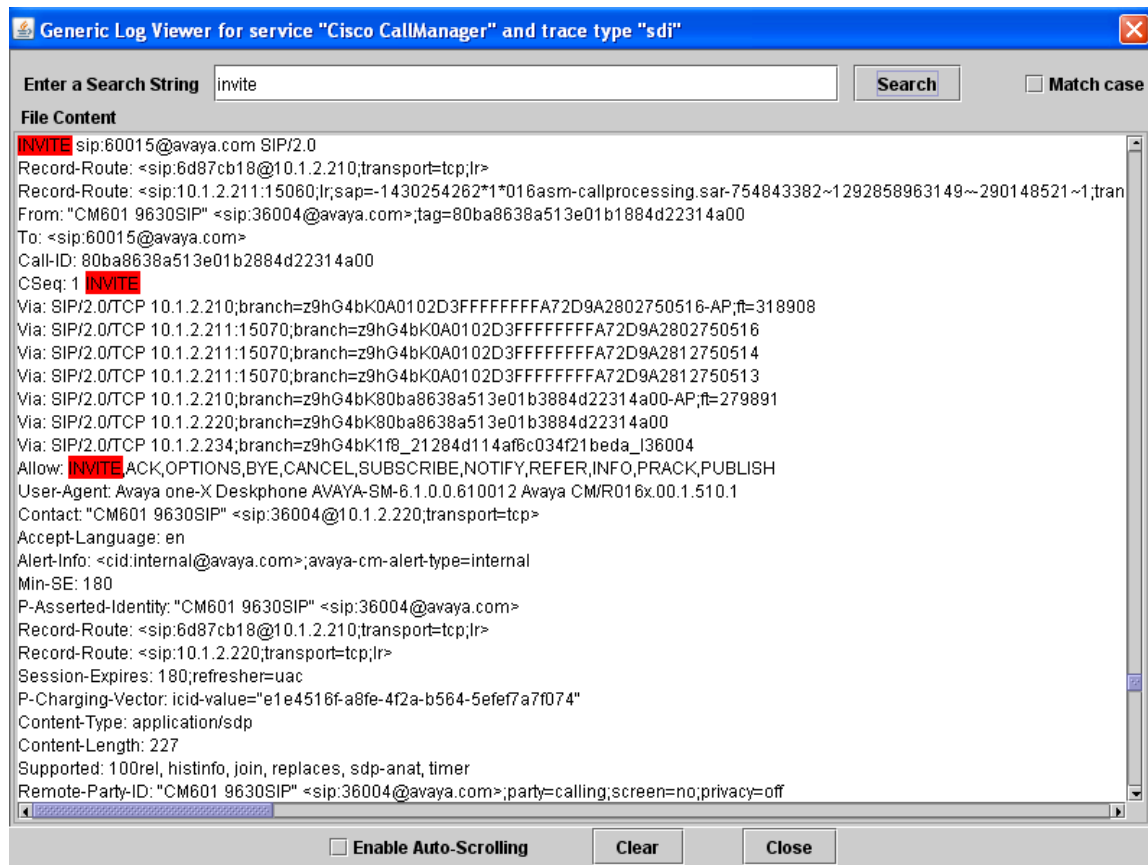
**SIP Message**  
**Dec 20 10:37:22 sm61 AasSipMgr[4281]:**  
-05:00 2010 437 1 com.avaya.asm | 2 com.avaya.asm SIPMSGT ----- 20/12/2010 10:37:22.437 --> octets: 2136, Body Length: 37  
ingress: { L10.1.2.210:5060/R10.1.2.210:57915/TCP/0x4ddbc }  
egress: [NO TARGET]  
SIPMsgContext: [NONE]  
INVITE sip:60015@avaya.com;routeinfo=0-0-0 SIP/2.0  
Record-Route: <sip:10.1.2.211:15060;lr;sap=-1430254262\*1\*016asm-callprocessing.sar-754843382~1292859442393~-290147413~1;transport=  
Record-Route: <sip:6d87cb18@10.1.2.210;transport=tcp;lr>  
From: sip:36004@avaya.com;tag=10b8a0234d0f31e14f228000\_F3600410.1.2.234  
To: sip:60015@avaya.com  
Call-ID: 1f9\_2133ffd-2c74ef254f2271df\_1@10.1.2.234  
CSeq: 508 INVITE  
Via: SIP/2.0/TCP 10.1.2.211:15070;branch=z9hG4bK0A0102D3FFFFFFFFFA72D9A2802751355  
Via: SIP/2.0/TCP 10.1.2.211:15070;branch=z9hG4bK0A0102D3FFFFFFFFFA72D9A2812751353  
Via: SIP/2.0/TCP 10.1.2.211:15070;branch=z9hG4bK0A0102D3FFFFFFFFFA72D9A2812751352  
Via: SIP/2.0/TCP 10.1.2.210;branch=z9hG4bK1fc\_2134015420995344f2271fe\_I36004-AP;ft=264169  
Via: SIP/2.0/TCP 10.1.2.234;branch=z9hG4bK1fc\_2134015420995344f2271fe\_I36004  
Content-Length: 374  
Content-Type: application/sdp

### 6.3. Verify Cisco Unified Communications Manager

The **Real Time Monitoring Tool** (RTMT) can be used to monitor events on Cisco UCM. This tool can be downloaded by selecting **Application → Plugins** from the top menu of the Cisco Unified CM Administration Web interface. For further information on this tool, see [9]. Once the Real Time Monitoring Tool plug-in is installed, real-time data can be captured by selecting **Tools → Trace & Log Central** in the left panel, and **Real Time Trace → View Real Time Data** on the right.



The following screen shows an example of a trace for a call from an Avaya user to a Cisco user. The string “invite” was entered in the top search bar.



## 6.4. Verified Scenarios

Verification scenarios for the configuration described in these Application Notes included:

- Basic calls between various telephones on Communication Manager and Cisco UCM can be made in both directions using G.711MU, G.729A and G.722, with media shuffled directly between the endpoints<sup>5</sup>, and correct calling and called name and number displays.
- Callers from the Avaya side are able to hear music on hold from Cisco UCM.
- Unanswered calls from the Avaya side to Cisco UCM are properly forwarded to voice mail (Modular Messaging in the sample configuration).
- Calling number block.
- Supplementary calling features were verified, such as performing an unattended transfer of the SIP trunk call to a local endpoint on the same PBX, and then repeating the scenario to transfer the SIP trunk call to a remote endpoint on the other PBX. The supplementary calling features verified are shown below.
  - Unattended transfer
  - Attended transfer
  - Hold/Unhold<sup>6</sup>
  - Consultation hold
  - Call forwarding
  - Conference

## 7. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager can interoperate with Cisco Unified Communications Manager using SIP trunks via Avaya Aura® Session Manager.

---

<sup>5</sup> Media shuffling and G.722 are not supported for calls from Cisco SCCP telephones to Avaya telephones.

<sup>6</sup> On calls between Cisco Unified 9951 and 9971 IP Phones and Avaya telephones, call hold at the Cisco telephone is not supported.

## 8. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>

- [1] *Avaya Aura<sup>TM</sup> Session Manager Overview*, Doc # 03-603323, Issue 2
- [2] *Administering Avaya Aura<sup>TM</sup> Session Manager*, Doc # 03-603324, Issue 2
- [3] *Maintaining and Troubleshooting Avaya Aura<sup>TM</sup> Session Manager*, Doc # 03-603325, Issue 2
- [4] *Administering Avaya Aura<sup>TM</sup> Communication Manager Server Options*, Doc # 03-603479, Issue 2, June 2010.
- [5] *SIP Support in Avaya Aura<sup>TM</sup> Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, Issue 9, May, 2009.
- [6] *Administering Avaya Aura<sup>TM</sup> Communication Manager*, Doc # 03-300509, Issue 6.0, June 2010.

Product documentation for Cisco Systems products may be found at

<http://www.cisco.com>

- [7] *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition*, Release 7.0(1), Part Number: OL-15405-01
- [8] *Cisco Unified Communications Manager Features and Services Guide for Cisco Unified Communication Manager Business Edition*, Release 7.0(1), Part Number: OL-15409-01
- [9] *Cisco Unified Real-Time Monitoring Tool Administration Guide*, Release 7.0(1), Part Number: OL-14994-01

The following Application Notes may be found at <http://support.avaya.com>

- [10] *Configuring Avaya Modular Messaging 5.2 with Cisco Unified Communications Manager 7.1.5 using Avaya Aura® Session Manager 6.1 – Issue 1.0*



---

**©2011 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](mailto:interoplabnotes@list.avaya.com)