



Configuring SIP Trunks among Avaya Aura® Session Manager R6.1, Avaya Aura® Communication Manager R6.0.1, and Cisco Unified Communications Manager R5.1.3 – 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 R5.1.3. 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.

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

Table of Contents

1. INTRODUCTION.....	4
2. EQUIPMENT AND SOFTWARE VALIDATED.....	6
3. CONFIGURE AVAYA AURA® COMMUNICATION MANAGER.....	7
3.1. VERIFY AVAYA AURA® COMMUNICATION MANAGER LICENSE.....	7
3.2. CONFIGURE SYSTEM PARAMETERS FEATURES.....	8
3.3. CONFIGURE IP NODE NAMES	8
3.4. CONFIGURE IP NETWORK REGION AND CODEC SET.....	9
3.5. CONFIGURE SIP SIGNALING GROUP AND TRUNK GROUP	10
3.5.1. SIP Signaling Group.....	10
3.5.2. SIP Trunk Group	11
3.6. CONFIGURE ROUTE PATTERN.....	12
3.7. CONFIGURE PRIVATE NUMBERING.....	13
3.8. CONFIGURE DIAL PLAN AND AAR ANALYSIS	13
3.9. SAVE CHANGES.....	13
4. CONFIGURING AVAYA AURA® SESSION MANAGER.....	14
4.1. LOG IN TO AVAYA AURA® SESSION MANAGER.....	15
4.2. CONFIGURE SIP DOMAIN	16
4.3. ADD LOCATIONS	17
4.4. CONFIGURE ADAPTATIONS	19
4.5. CONFIGURE SIP ENTITIES	21
4.6. CONFIGURE ENTITY LINKS.....	23
4.7. CONFIGURE ROUTING POLICIES	24
4.8. CONFIGURE DIAL PATTERNS.....	25
4.9. CONFIGURE SESSION MANAGER	27
4.10. ADD AVAYA AURA® COMMUNICATION MANAGER AS AN EVOLUTION SERVER	28
4.10.1. Create a Login on the Communication Manager Server.....	28
4.10.2. Create an Application Element on System Manager	30
4.10.3. Create an Application.....	32
4.10.4. Create an Application Sequence.....	33
4.10.5. Synchronize Avaya Aura® Communication Manager Data	34
4.11. ADD USERS FOR SIP TELEPHONES	35
5. CONFIGURE CISCO UCM.....	39
5.1. LOG IN TO CISCO UCM.....	39
5.2. MEDIA RESOURCES	39
5.2.1. Verify Annunciator (ANN).....	39
5.2.2. Verify Conference Bridge (CFB).....	40
5.2.3. Verify Media Termination Point (MTP)	42
5.2.4. Add Music On Hold Audio Source.....	43
5.2.5. Verify Music On Hold Server (MOH).....	44
5.2.6. Define a Media Resource Group (MRG).....	45
5.2.7. Define a Media Resource Group List (MRGL).....	47
5.3. CONFIGURE DEFAULT DEVICE POOL.....	48
5.4. CONFIGURE SYSTEM MUSIC ON HOLD SETTINGS	49
5.5. ADMINISTER SIP TRUNK SECURITY PROFILE	50
5.6. ADMINISTER SIP TRUNK	52
5.7. ADMINISTER ROUTE PATTERN	55
5.8. CONFIGURE AUDIO CODECS.....	57
5.9. CONFIGURE VOICE MAIL PILOT	58

5.10.	CONFIGURE VOICE MAIL PROFILE	59
5.11.	CONFIGURE A TELEPHONE	60
6.	VERIFICATION STEPS	64
6.1.	VERIFY AVAYA AURA [®] COMMUNICATION MANAGER	64
6.2.	VERIFY AVAYA AURA [®] SESSION MANAGER.....	65
6.3.	VERIFY CISCO UNIFIED COMMUNICATIONS MANAGER.....	69
6.4.	VERIFIED SCENARIOS	71
7.	CONCLUSION	71
8.	ADDITIONAL REFERENCES.....	74

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.

In the test configuration shown in **Figure 1**, Cisco UCM supports the Cisco telephones, which have 4-digit extensions in the range 50xx. 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 36xxx. 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. The Avaya Modular Messaging configuration is also outside of the scope of these Application Notes.

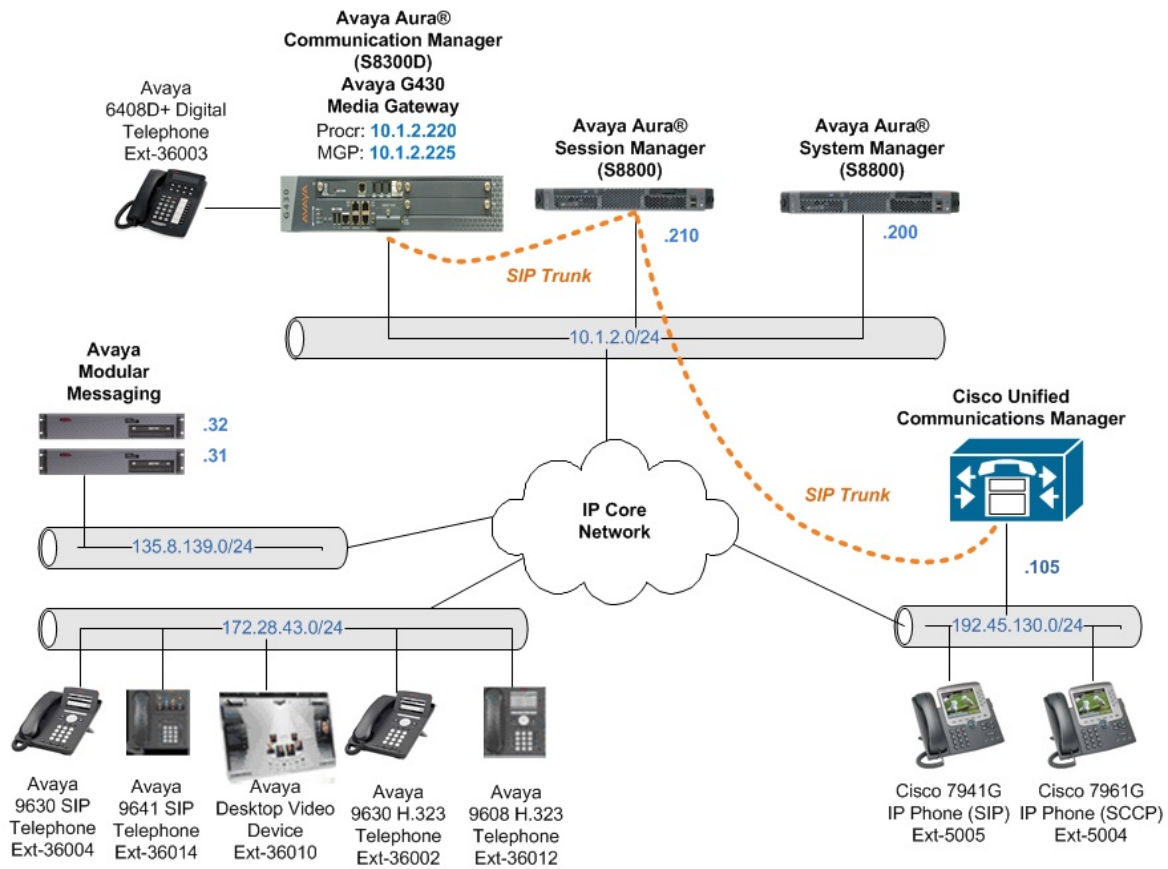


Figure 1: Sample Configuration

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 18621
Avaya	S8800 Server	Avaya Aura® Session Manager 6.1 SP0, Load 6.1.0.0.610023
		Avaya Aura® System Manager 6.1 SP0, Build Number 6.1.0.4.5072-6.1.4.62
Avaya	Avaya 9641 IP Telephone (SIP)	6.0 (S96x1_SALBR6_0r95_V4r52B)
Avaya	Avaya 9630 IP Telephone (SIP)	2.6.4
Avaya	Avaya 9630 IP Telephone (H.323)	3.101S
Avaya	Avaya 9608 IP Telephone (H323)	6.0 (S9608_11_HALBR6_0_V452)
Avaya	Avaya 6408D+ Digital Telephone	-
Avaya	Avaya Desktop Video Device (SIP)	SIP_A175_1_0_0_012849.tar
Avaya	Modular Messaging Storage Server	5.2, Service Pack 6 Patch 2
Avaya	Modular Messaging Application Server	5.2, Service Pack 6 Patch 2
Cisco	Unified Communications Manager	5.1.3.1000-12
Cisco	7941G Unified IP Phone (SIP)	SIP41.8-3-2S
Cisco	7961G Unified IP Phone (SCCP)	SCCP41.8-3-2S

3. Configure Avaya Aura® 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® 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® 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
Maximum Administered SIP Trunks:		24000	156
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. During the testing, the codec parameters for codec set 1 were varied, with successful calls using “G.711MU” and G.729. G.729B is not supported by Cisco Telephones.

```
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.729   n                2           20
2: G.711MU n                2           20
```

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**.¹ 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 uses 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 G430 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
    IP Video? n
Peer Detection Enabled? y Peer Server: Others
                                     SIP Enabled LSP? n
                                     Enforce SIPS URI for SRTP? y

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
DTMF over IP: rtp-payload
Session Establishment Timer(min): 3
    Enable Layer 3 Test? n
H.323 Station Outgoing Direct Media? y

Bypass If IP Threshold Exceeded? n
RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
    IP Audio Hairpinning? n
Initial IP-IP Direct Media? y
Alternate Route Timer(sec): 6
```

¹ 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:

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

```
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
```

The following shows Page 4 for trunk group 60. All parameters shown are at default values, with the exception of the **Telephone Event Payload Type** associated with DTMF signaling, which has been set to the value “101” to match the default Cisco Unified Communications Manager configuration. The **Always Use re-INVITE for Display Updates** parameter was set to “y” because Cisco UCM R5.1.3 did not reply to display SIP UPDATE messages from Communication Manager during testing.

Note: While the **Identity for Calling Party Display** parameter is set to the default value of “P-Asserted-Identity”, during testing it was observed that setting the parameter to “From” resolved some display issues. See **Section 7** for additional details.

change trunk-group 60	Page 4 of 21
PROTOCOL VARIATIONS Mark Users as Phone? n Prepend '+' to Calling Number? n Send Transferring Party Information? n Network Call Redirection? n Send Diversion Header? n Support Request History? y Telephone Event Payload Type: 101 Convert 180 to 183 for Early Media? n Always Use re-INVITE for Display Updates? y Identity for Calling Party Display: P-Asserted-Identity Enable Q-SIP? 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							
Dgts										Intw							
1:	60	0					0				n	user					
2:											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	

3.7. 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 Len	Ext Code	Trk Grp(s)	Private Prefix	Total 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 4-digit extensions beginning with 5 to stations registered with Cisco UCM. Use the **change dialplan analysis** command to define **Dialed String 5** as an ext Call Type.

change dialplan analysis										Page 1 of 12
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								
5	4	ext								

Use the **change aar analysis n** command where **n** is the dial string pattern to configure an entry for **Dialed String 5** to use **Route Pattern 60**. Add an entry for the Cisco UCM extensions which begin with 5. Set **Call Type** to **unku**.

change aar analysis 5								Page 1 of 2
AAR DIGIT ANALYSIS TABLE								
Location: all				Percent Full: 0				
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd		
5	4	4	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

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.

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.

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

Users

- Administrators**
Manage Administrative Users
- Groups & Roles**
Manage groups, roles and assign roles to users
- Synchronize and Import**
Synchronize users with the enterprise directory, import users from file
- User Management**
Manage users, shared user resources and provision users

Elements

- Application Management**
Manage applications and application certificates
- Communication Manager**
Manage Communication Manager objects
- Conferencing**
Conferencing
- Inventory**
Manage, discover, and navigate to elements, update element software
- Messaging**
Manage Messaging System objects
- Presence**
Presence
- Routing**
Network Routing Policy
- SIP AS 8.1**
SIP AS 8.1
- Session Manager**
Session Manager Element Manager

Services

- Backup and Restore**
Backup and restore System Manager database
- Configurations**
Manage system wide configurations
- Events**
Manage alarms, view and harvest logs
- Licenses**
View and configure licenses
- Replication**
Track data replication nodes, repair replication nodes
- Scheduler**
Schedule, track, cancel, update and delete jobs
- Security**
Manage Security Certificates
- Templates**
Manage Templates for Communication Manager and Messaging System objects

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](#)

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

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 “BaskingRidge HQ” location, which includes Communication Manager and Session Manager, and the “Westminster – CO” location, which includes Cisco UCM.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular, Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Locations - Location Details'. It includes a 'Location Details' section with a 'General' tab. The 'General' tab contains fields for 'Name' (BaskingRidge HQ) and 'Notes' (CME, CS1K R5 & R7, AAC R6, CM). Below this is the 'Overall Managed Bandwidth' section with 'Managed Bandwidth Units' set to 'Kbit/sec' and a 'Total Bandwidth' field. The 'Per-Call Bandwidth Parameters' section shows 'Default Audio Bandwidth' set to '80 Kbit/sec'. The 'Location Pattern' section has an 'Add' button and a table with 5 items. The table has columns for 'IP Address Pattern' and 'Notes'. The first two rows are highlighted with a red box: the first row has '10.1.2.*' and 'SM/CM R5.2.x, R6.0, R6.1', and the second row has '10.7.7.*' and 'CS1K R7'.

IP Address Pattern	Notes
10.1.2.*	SM/CM R5.2.x, R6.0, R6.1
10.7.7.*	CS1K R7

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

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 ?

General

* Name:

Westminster - CO

Notes:

Cisco UCM

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000 Kbit/Sec

Minimum Multimedia Bandwidth:

64 Kbit/Sec

* Default Audio Bandwidth:

80 Kbit/sec

Location Pattern

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 192.45.130.*	Cisco CallManager 5.1.3

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 Communication Manager and between 4 and 11 digit formats when routing between Modular Messaging and Cisco UCM.

The third adaptation is not covered in these Application Notes, however it was implemented during testing to address the integration with Modular Messaging. 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-UCM513**)
- **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](#) [Home](#)

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Adaptations - Adaptation Details

Adaptation Details

Commit

Cancel

Help ?

General

* Adaptation name:

CM-ES Inbound

Module name:

DigitConversionAdapter

Module parameter:

odstd=avaya.com osrcd=avaya.c

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 **192.45.130.105** for the **Module parameter** is equivalent to **odstd=192.45.130.105**.

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

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Adaptations - Adaptation Details

Adaptation Details

Commit

Cancel

Help ?

General

* Adaptation name:

Cisco-UCM513

Module name:

CiscoAdapter

Module parameter:

192.45.130.105

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

* Input Required

Commit

Cancel

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 left sidebar shows a menu with "Routing" selected, and sub-items like "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", "Regular", "Expressions", and "Defaults". The main content area is titled "SIP Entity Details" and includes a "General" tab. The configuration fields are as follows:

- Name:** SM1
- * FQDN or IP Address:** 10.1.2.210
- Type:** Session Manager (dropdown)
- Notes:** (empty text field)
- Location:** BaskingRidge HQ (dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** America/New_York (dropdown)
- Credential name:** (empty text field)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)

Below the configuration fields, there is a section for "Entity Links" with a warning: "Entity Links can be modified after SIP Entity is committed." It includes an "Add" button and a "Remove" button. At the bottom, there is a table for "Port" 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 **Home** **Elements** **Routing** **SIP Entities - SIP Entity Details**

SIP Entity Details Commit Cancel Help ?

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 **Home** **Elements** **Routing** **SIP Entities - SIP Entity Details**

SIP Entity Details Commit Cancel Help ?

General

* Name: CUCM-513

* FQDN or IP Address: 192.45.130.105

Type: Other

Notes:

Adaptation: Cisco-UCM513

Location: Westminster - CO

Time Zone: America/Denver

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.

Name	An informative name
SIP Entity 1	Select the Session Manager Entity created in the previous section
Port	Port number to which the other system sends its SIP requests
SIP Entity 2	The other SIP Entity for this link, created in the previous section
Port	Port number to which the other system expects to receive SIP requests
Trusted	Verify that this box is checked
Protocol	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 **Entity Links** Commit Cancel

Home / Elements / Routing / Entity Links - Entity Links

Entity Links Help ?

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 **Entity Links** Commit Cancel

Home / Elements / Routing / Entity Links - Entity Links

Entity Links Help ?

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* Cisco UCME 513	* SM1	TCP	* 5060	* CUCM-513	* 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 contains three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. The 'General' section has fields for Name (To CM-ES R6.0.1), Disabled (unchecked), and Notes. The 'SIP Entity as Destination' section has a 'Select' button and a table with one entry: CM-ES R6.0.1, 10.1.2.220, CM, CM R6.0.1 ES. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, a table with one entry: 24/7, and a 'Select' dropdown set to 'All'.

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 Help ? Cancel

General

* Name: To CM-ES R6.0.1

Disabled: ☐

Notes:

SIP Entity as Destination

Select

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

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

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 Policy Details

General

* Name: To Cisco UCM513 (50xx)

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CUCM-513	192.45.130.105	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
<input type="checkbox"/>	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 36 are supported by Communication Manager, and 4-digit extensions beginning with 50 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](#) [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

General

* Pattern: 36

* 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	To CM-ES R6.0.1	0	<input type="checkbox"/>	CM-ES R6.0.1	

Select : All, None

[Routing](#) [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

General

* Pattern: 50

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Dial pattern to Cisco UCM513

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	To Cisco UCM513 (50xx)	0	<input type="checkbox"/>	CUCM-513	

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**:

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

Under **Security Module**:

SIP Entity IP Address	Will be automatically filled in based on the selected SIP Entity Name .
Network Mask	Enter the network mask corresponding to the IP address of Session Manager
Default Gateway:	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](#) | [Security Module](#) | [NIC Bonding](#) | [Monitoring](#) | [CDR](#) | [Personal Profile Manager \(PPM\)](#) - [Connection Settings](#) | [Event Server](#) | [Expand All](#) | [Collapse All](#)

[General](#) ▾

SIP Entity Name	<input type="text" value="SM1"/>
Description	<input type="text" value="R6.1 SM"/>
Management Access Point Host Name/IP	<input type="text" value="10.1.2.211"/>
Direct Routing to Endpoints	<input type="text" value="Enable"/>

[Security Module](#) ▾

SIP Entity IP Address	<input type="text" value="10.1.2.210"/>
Network Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="10.1.2.1"/>
Call Control PHB	<input type="text" value="46"/>
QOS Priority	<input type="text" value="6"/>
Speed & Duplex	<input type="text" value="Auto"/>
VLAN ID	<input type="text" value=""/>

4.10. Add Avaya Aura® Communication Manager as an Evolution Server

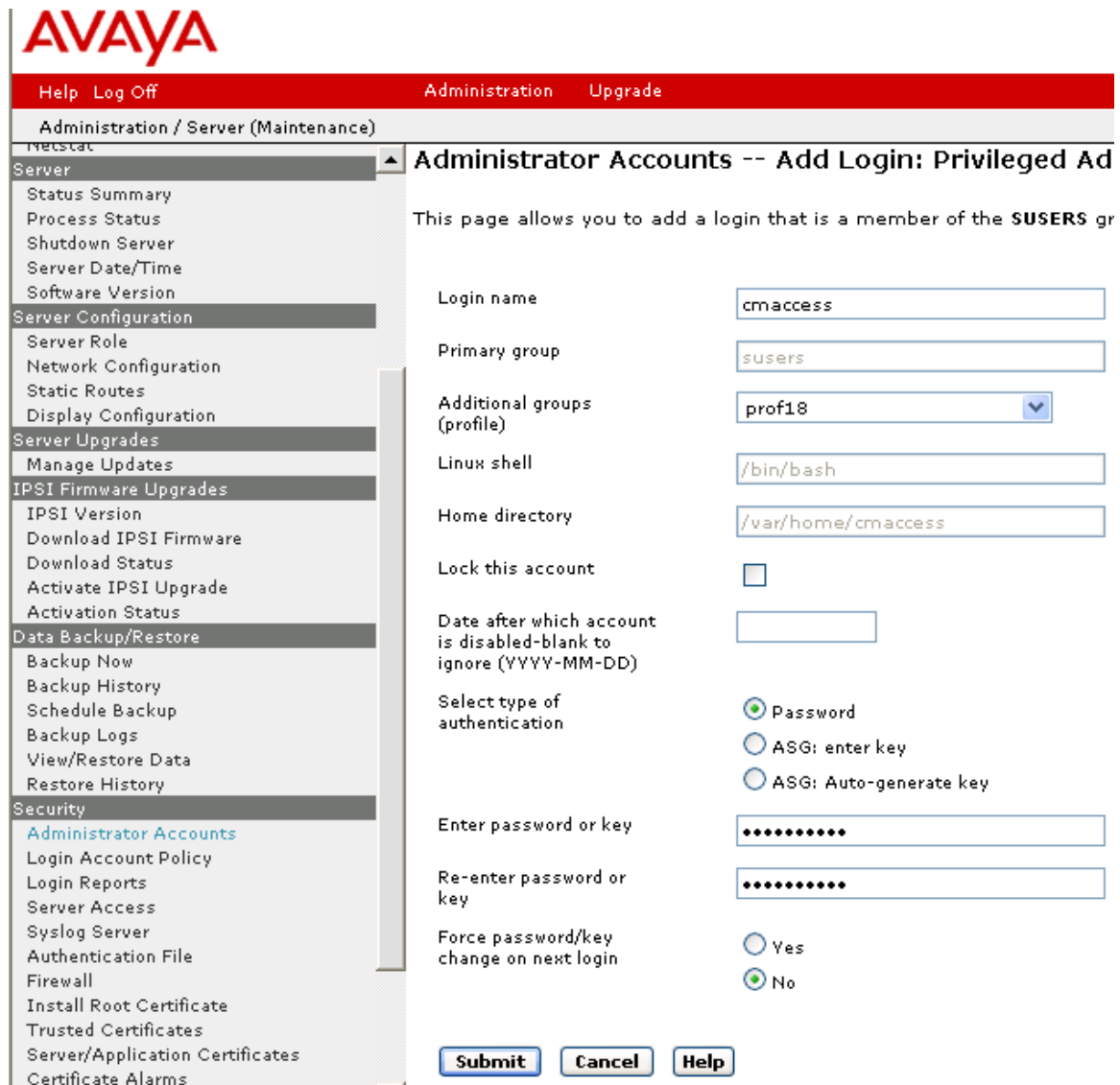
In order for Communication Manager to provide configuration and Evolution Server support to telephones, Communication Manager must be added as an application in Session Manager. This comprises a two step procedure. First, an access login must be configured on Communication Manager for the purpose of 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, or 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', 'Custom Login', 'Change Login' (with a dropdown menu), 'Remove Login' (with a dropdown menu), 'Lock/Unlock Login' (with a dropdown menu), 'Add Group', and 'Remove Group' (with a dropdown menu). At the bottom, there are 'Submit' and 'Help' buttons.

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**.



The screenshot shows the Avaya Administration web interface. The top navigation bar includes 'Help', 'Log Off', 'Administration', and 'Upgrade'. The main header is 'Administration / Server (Maintenance)'. A left-hand menu lists various system management options, with 'Administrator Accounts' selected under the 'Security' section. The main content area is titled 'Administrator Accounts -- Add Login: Privileged Ad'. Below the title, a descriptive text states: 'This page allows you to add a login that is a member of the **SUSERS** group'. The form contains several fields: 'Login name' (cmaccess), 'Primary group' (susers), 'Additional groups (profile)' (a dropdown menu showing 'prof18'), 'Linux shell' (/bin/bash), 'Home directory' (/var/home/cmaccess), 'Lock this account' (an unchecked checkbox), 'Date after which account is disabled-blank to ignore (YYYY-MM-DD)' (an empty text box), 'Select type of authentication' (radio buttons for 'Password' (selected), 'ASG: enter key', and 'ASG: Auto-generate key'), 'Enter password or key' (a masked text box), 'Re-enter password or key' (another masked text box), and 'Force password/key change on next login' (radio buttons for 'Yes' and 'No' (selected)). At the bottom of the form are three buttons: 'Submit', 'Cancel', and 'Help'.

AVAYA

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** group

Login name: cmaccess

Primary group: susers

Additional groups (profile): prof18

Linux shell: /bin/bash

Home directory: /var/home/cmaccess

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

Submit **Cancel** **Help**

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:

Login	Login created in Section 4.10.1
Password	Password created in the previous section
Confirm Password	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", "Network Configuration", "Device and Location Configuration", "Application Configuration", and "System Tools". The "Application Configuration" category is expanded, showing "Applications" as the selected option. The main content area is titled "Application Editor" and contains the following fields:

- Name**: A text input field with the value "CM-ES R6.0.1".
- SIP Entity**: A dropdown menu with the value "CM-ES R6.0.1".
- CM System for SIP Entity**: A dropdown menu with the value "CM-ES R6.0.1" and a "Refresh" button. A link "View/Add CM Systems" is also present.
- Description**: A 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. Two buttons, "Commit" and "Cancel", are located at the 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.

The screenshot shows the Avaya Aura System Manager 6.1 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 this is a breadcrumb trail: "Home / Elements / Session Manager / Application Configuration / Application Sequences- Application Sequences". A 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 Sequence Editor" and includes "Commit" and "Cancel" buttons. It features three sections: "Application Sequence" with input fields for "Name" (containing "CM-ES R6.0.1") and "Description"; "Applications in this Sequence" with "Move First", "Move Last", and "Remove" buttons, and a table with one item; and "Available Applications" with a "Refresh" button, a "Filter: Enable" option, and a table with one item. The "Applications in this Sequence" table has columns for "Sequence Order (first to last)", "Name", "SIP Entity", "Mandatory", and "Description". The "Available Applications" table has columns for "Name", "SIP Entity", and "Description".

Application Sequence Editor

Application Sequence

*Name: CM-ES R6.0.1

Description:

Applications in this Sequence

Move First Move Last Remove

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

Select : All, None

Available Applications

1 Item Refresh Filter: Enable

Name	SIP Entity	Description
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 contains a navigation menu with 'Inventory' selected. The main content area is titled 'Synchronize CM Data and Configure Options'. It displays a table with columns: Element Name, FQDN/IP Address, Last Sync Time, Last Translation Time, Sync Type, Sync Status, Location, and Software Version. The table contains one row for 'CM-ES R6.0.1'. Below the table, there are radio buttons for 'Initialize data for selected devices' (selected), 'Incremental Sync data for selected devices', and 'Save Translations for selected devices'. At the bottom, there are buttons for 'Now', 'Schedule', 'Cancel', and 'Launch Element Cut Through'.

Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version
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

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 contains a navigation menu with 'Scheduler' selected. The main content area is titled 'Pending Jobs'. It displays a table with columns: Job Type, Job Name, Job Status, State, Frequency, Scheduled By, and Element. The table contains several rows, including 'CSM_CMSSynch_INIT_CM-ES R6.0.1_1293132411753' which is highlighted in red. Below the table, there are buttons for 'View', 'Edit', 'Delete', and 'More Actions'. At the bottom, there are buttons for 'Now', 'Schedule', 'Cancel', and 'Launch Element Cut Through'.

Job Type	Job Name	Job Status	State	Frequency	Scheduled By	Element
✱	PurgeJobStatus	PENDING EXECUTION	Enabled	Weekly	admin	
✱	LogPurgeRule	PENDING EXECUTION	Enabled	Daily	admin	
✱	ClrdAlarmPurgeRule	PENDING EXECUTION	Enabled	Daily	admin	
✱	SoftDelRTSPurgeRule	PENDING EXECUTION	Enabled	Daily	admin	
ⓘ	CSM_CMSSynch_INIT_CM-ES R6.0.1_1293132411753	RUNNING	Enabled	Once	admin	CM-ES R6.0.1
ⓘ	CSM_CMSSynch_INCR_CM-ES R6.0.1_1289243227389	PENDING EXECUTION	Enabled	Hourly	admin	CM-ES R6.0.1
ⓘ	CSM_Iptcmobject_CleanupBackedupAnnc	PENDING EXECUTION	Enabled	Hourly	admin	CSM
ⓘ	CSM_Iptcmobject_MAINTENANCE_1289242761579	PENDING EXECUTION	Enabled	Daily	admin	CSM
✱	sys_ConfRefreshConfig	PENDING EXECUTION	Enabled	Minutes	admin	

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:

Last Name	The user's last name
First Name	The user's first name
Login Name	The desired phone extension number@domain.com where domain was defined in Section 4.2
Password	Password for user to log into System Manager (SMGR)
Localized Display Name	The name to be used as calling party
Endpoint Display Name	The name to be used as calling party
Honorific	Enter the appropriate information
Language Preference	Enter the appropriate information
Time Zone	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: 36010@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).²

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

² 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.

✓ Session Manager Profile ▾

* Primary Session Manager	SM1 ▾	<table border="1"><thead><tr><th>Primary</th><th>Secondary</th><th>Maximum</th></tr></thead><tbody><tr><td>11</td><td>0</td><td>11</td></tr></tbody></table>	Primary	Secondary	Maximum	11	0	11
Primary	Secondary	Maximum						
11	0	11						
Secondary Session Manager	(None) ▾	<table border="1"><thead><tr><th>Primary</th><th>Secondary</th><th>Maximum</th></tr></thead><tbody></tbody></table>	Primary	Secondary	Maximum			
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 ▾							

✓ Endpoint Profile ▾

* System	CM-ES R6.0.1 ▾	
* Profile Type	Endpoint ▾	
Use Existing Endpoints	<input type="checkbox"/>	
* Extension	36010	Endpoint Editor
* Template	DEFAULT_9640SIP_CM_6_0 ▾	
Set Type	9630SIP	
Security Code		
* Port	QIP	
Voice Mail Number	33000	
Delete Endpoint on Unassign of Endpoint	<input type="checkbox"/>	

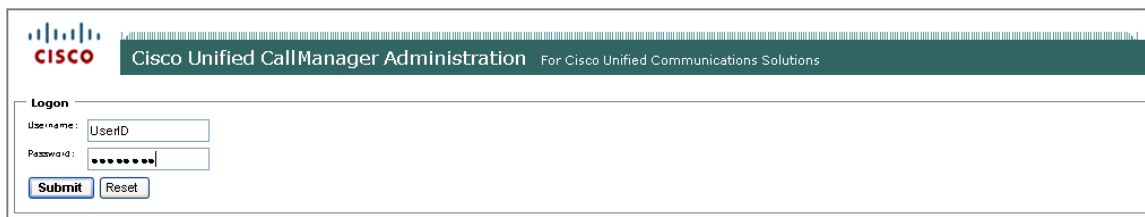
5. Configure Cisco UCM

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 Media Resources
- Configure Device Pool and System Settings
- 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. Media Resources

In order to support some of the supplementary service features like Transfer, Conferencing, Music on Hold (MOH), call Annunciation, etc., media resource groups and lists need to be configured using default software Annunciators (ANN), Conference Bridges (CFBs), Music on Hold (MOH) and Media Termination Points (MTPs). This section will verify the default installed ANN, CFB, MOH and MTP which will be used to create a new Media Resource Group (MRG) and then a Media Resource Group List (MRGL) which will be used in additional configurations of the SIP Trunk and Phone Devices.

5.2.1. Verify Annunciator (ANN)

Select **Media Resources**→**Annunciator**

- Click on **Find** to list the available annunciators.
- A default annunciator should be available and registered with the CUCM publisher listing its assigned IP address.
- Select the default ANN. (In the sample configuration below the annunciator is named ANN_2; this name may be different on other systems).
- Verify the **Device Pool** assigned is “Default.”

The screenshot shows the 'Find and List Annunciators' page in the Cisco Unified CallManager Administration interface. The page header includes the navigation bar with 'Cisco Unified CallManager Administration' and 'Logged in as: ccmadministrator'. The main content area has a 'Status' section indicating '1 records found'. Below this is a 'Search Options' section with a 'Find' button and a 'Search Within Results' checkbox. The 'Search Results' section displays a table with the following data:

Name	Description	Device Pool	Status	IP Address
ANN_2	ANN_cuc	Default	Registered with cuc	192.45.130.105

Below the table are buttons for 'Select All', 'Clear All', and 'Reset Selected', along with a 'Rows per Page' dropdown set to 50.

The screenshot shows the 'Annunciator Configuration' page in the Cisco Unified CallManager Administration interface. The page header includes the navigation bar with 'Cisco Unified CallManager Administration' and 'Logged in as: ccmadministrator'. The main content area has a 'Status' section indicating 'Status: Ready'. Below this is a 'Device Information' section with the following fields:

- Registration: Registered with Cisco Unified CallManager cuc
- IP Address: 192.45.130.105
- Server*: cuc
- Name*: ANN_2
- Description: ANN_cuc
- Device Pool*: Default
- Location*: Hub_None

At the bottom of the form are 'Save' and 'Reset' buttons. A note at the bottom left states: '* - indicates required item.'

5.2.2. Verify Conference Bridge (CFB)

Select **Media Resources**→**Conference Bridge**

- Click on **Find** to list the available conference bridges.
- A default conference bridge should be available and registered to the CUCM publisher listing its assigned IP address.
- Select the default CFB. (In the sample configuration below the conference bridge is named CFB_2; this name may be different on other systems).


- Verify the **Device Pool** assigned is “Default.”

Navigation Cisco Unified CallManager Administration Go

Cisco Unified CallManager Administration For Cisco Unified Communications Solutions Logged in as: ccmadministrator

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

Conference Bridge Configuration Related Links: Back To Find/List Go

 Status: Ready


Conference Bridge Information

Conference Bridge : CFB_2 (CFB_cuc)
 Registration Registered with Cisco Unified CallManager cuc
 IP Address 192.45.130.105

Software Conference Bridge Info

Conference Bridge Type* Cisco Conference Bridge Software
 Host Server cuc
 Conference Bridge Name* CFB_2
 Description CFB_cuc
 Device Pool* Default
 Location* Hub_None

Save Reset

 *- indicates required item.

5.2.3. Verify Media Termination Point (MTP)

Select **Media Resources**→**Media Termination Point**

- Click on **Find** to list the available MTPs.
- A default MTP should be available and registered to the CUCM publisher listing its assigned IP address.
- Select the default MTP. (In the sample configuration below the MTP is named MTP_2; this name may be different on other systems).
- Verify the **Device Pool** assigned is “Default.”

Cisco Unified CallManager Administration For Cisco Unified Communications Solutions Logged in as: ccmadministrator

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

Find and List Media Termination Points

Status: 1 records found

Search Options
Find Media Termination Point where Name ▾ begins with ▾ Find ☐ Search Within Results
(device.name begins with any)

Search Results

Name	Description	Device Pool	Status	IP Address	Copy
MTP_2	MTP_cuc	Default	Registered with cuc	192.45.130.105	Not Allowed

Add New Select All Clear All Delete Selected Reset Selected Rows per Page: 50 ▾

Cisco Unified CallManager Administration For Cisco Unified Communications Solutions Logged in as: ccmadministrator

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

Media Termination Point Configuration Related Links: Back To Find/List ▾ Go

Status: Status: Ready

Media Termination Point Information

Registration: Registered with Cisco Unified CallManager cuc
IP Address: 192.45.130.105
Media Termination Point Type*: Cisco Media Termination Point Software
Host Server*: cuc
Media Termination Point Name*: MTP_2
Description: MTP_cuc
Device Pool*: Default ▾

Save Reset

*- indicates required item.

5.2.4. Add Music On Hold Audio Source

Select **Media Resources**→**Music On Hold Audio Sources**

- Click on **Find** to list the available MOH stream numbers.
- Verify a MOH is listed and configured to use the SampleAudioSource (2 in the sample configuration); if there is no MOH defined click on **Add New** button to create one.
- Verify the following in the MOH configuration page:
 - MOH Audio Source File: SampleAudioSource
 - MOH Audio Source Name: SampleAudioSource
 - Play continuously is checked
 - Allow multicasting is checked

Click on **Save**.

The screenshot shows the Cisco Unified CallManager Administration web interface. The top navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'Media Resources' tab is selected. The page title is 'Find and List Music On Hold Server Audio Sources'. Below the title, there is a status bar indicating '2 records found'. The search options section shows a search for 'MOH Audio Stream Number' beginning with '1'. The search results table lists two entries: '1' with source name 'bob' and '2' with source name 'SampleAudioSource'. The 'Add New' button is located at the bottom left of the results area.

MOH Audio Stream Number	MOH Audio Source Name
1	bob
2	SampleAudioSource

Cisco Unified CallManager Administration For Cisco Unified Communications Solutions
 Navigation Cisco Unified CallManager Administration Go
 System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help Log Off
 Logged in as: ccmadministrator

Music On Hold Audio Source Configuration Related Links: Music On Hold Server Configuration Go

Status
 Status: Ready

Music On Hold Server Audio Source Information
 MOH Audio Stream Number* 2
 MOH Audio Source File SampleAudioSource
 MOH Audio Source Name* SampleAudioSource
☒ Play continuously (repeat)
☒ Allow Multicasting

MOH Audio Source File Status
 InputFileName: SampleAudioSource
 ErrorCode: 0
 ErrorText: Translation Complete
 DurationSeconds: 338
 DiskSpaceKB: 8092
 LowDateTime: 1130860118
 HighDateTime: 0
 OutputFileList:
 SampleAudioSource.ulaw.wav
 SampleAudioSource.alaw.wav
 SampleAudioSource.g729.wav

MOH Audio Sources
 MOH_1 :: bob
 MOH_2 :: SampleAudioSource

Save Delete Add New Upload File

*- indicates required item.
 **Music On Hold will not be available while the servers are resetting.

5.2.5. Verify Music On Hold Server (MOH)

Select **Media Resources**→**Music On Hold Server**

- Click on **Find** to list the available MOH Servers.
- A default MOH server should be available and registered to the CUCM publisher listing its assigned IP address.
- Select the default MOH server. (In the sample configuration below the MOH server is named MOH_2; this name may be different on other systems).
- Verify the **Device Pool** assigned is “Default.”

Cisco Unified CallManager Administration For Cisco Unified Communications Solutions
 Navigation Cisco Unified CallManager Administration Go
 System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help Log Off
 Logged in as: ccmadministrator

Find and List Music On Hold Servers

Status
 1 records found

Search Options
 Find Music On Hold Server where Name begins with Find Search Within Results
 (device.name begins with any) Select item or enter search text

Search Results

Music On Hold Server Name	Description	Device Pool	Status	IP Address
MOH_2	MOH_CUCMS.x	Default	Registered with cuc	192.45.130.105

Select All Clear All Reset Selected Rows per Page 50

Cisco Unified CallManager Administration For Cisco Unified Communications Solutions
 Navigation Cisco Unified CallManager Administration Go
 System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help Log Off
Music On Hold (MOH) Server Configuration Related Links: Back To Find/List Go

Status
 Status: Ready

Device Information
 Registration Registered with Cisco Unified CallManager cuc
 IP Address 192.45.130.105
 Host Server* CUC
 Music On Hold Server Name* MOH_2
 Description MOH_CUCM5.x
 Device Pool* Default
 Location* Hub_None
 Maximum Half Duplex Streams* 250
 Maximum Multicast Connections* 30
 Fixed Audio Source Device
 Run Flag* Yes

Multicast Audio Source Information
☐ Enable Multicast Audio Sources on this MOH Server
 Base Multicast IP Address* 0.0.0.0
 Base Multicast Port Number* 0 (Even numbers only)
 Increment Multicast on* ☒ Port Number ☐ IP Address

Selected Multicast Audio Sources

No.	Audio Source Name	Max Hops
1	bob	2
2	SampleAudioSource	2

Save Reset

***** - indicates required item.

5.2.6. Define a Media Resource Group (MRG)

Select **Media Resources** → **Media Resource Group** → **Add New**.

- Name: Enter “MRG_1”
- Description: Enter a brief description.

Under *Devices for this Group*:

- Select the following devices from the “Available Media Resources” window and click on the down arrow (▼) move the selected resource to the “Selected Media Resources” window:
 - ANN_2
 - CFB_2
 - MOH_2
 - MTP_2

Note: The resource names in the Available Media Resource window may be different that those listed in the sample configuration below. Please use the default names of the resources verified in the media verifications in previous steps.

Click on **Save**.

Navigation
Cisco Unified CallManager Administration
Go

Cisco Unified CallManager Administration
For Cisco Unified Communications Solutions
Logged in as: ccmadministrator

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

Media Resource Group Configuration
Related Links: Back To Find/List
Go

Status
i Status: Ready

Media Resource Group Status
Media Resource Group: MRG_1 (used by 9 devices)

Media Resource Group Information
Name* MRG_1
Description Media Resource Group 1

Devices for this Group
Available Media Resources** MTP0011936915E9

Selected Media Resources*
ANN_2 (ANN)
CFB_2 (CFB)
MOH_2 (MOH)
MTP_2 (MTP)

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

Save Delete Copy Reset Add New

i *- indicates required item.
i **Includes Annunciators (ANN), Conference Bridges (CFB), Media Termination Points (MTP), Music On Hold Servers (MOH) and Transcoders (XCODE)

5.2.7. Define a Media Resource Group List (MRGL)

Select **Media Resources**→**Media Resource Group List** → **Add New**.

- Name: Enter “MRGL_1”

Under *Media Resource Groups for this List*:

- In the “Available Media Resource Groups” window, select MRG_1 and click on the down arrow (▼) to move the selected MRG to the lower window, “Selected Media Resource Groups.”

Click on **Save**.

The screenshot displays the Cisco Unified CallManager Administration web interface. The top navigation bar includes the title "Cisco Unified CallManager Administration" and a "Navigation" dropdown menu. Below the navigation bar, a breadcrumb trail shows the path: System > Call Routing > Media Resources > Voice Mail > Device > Application > User Management > Bulk Administration > Help. The main content area is titled "Media Resource Group List Configuration". It features a "Status" section indicating "Status: Ready". Below this, the "Media Resource Group List Status" section shows "Media Resource Group List: MRGL_1 (used by 9 devices)". The "Media Resource Group List Information" section contains a "Name*" field with the value "MRGL_1". The "Media Resource Groups for this List" section is divided into two panes: "Available Media Resource Groups" and "Selected Media Resource Groups". The "Available" pane contains a list box with "MRS1". The "Selected" pane contains a list box with "MRG_1". Arrows between the panes indicate the ability to move items. At the bottom, there are buttons for "Save", "Delete", "Copy", "Reset", and "Add New". A note at the bottom left states: "i *- indicates required item."

5.3. Configure Default Device Pool

Select **System**→**Device Pool**

Click on **Find** to list the device pools and verify the “Default” device pool settings:

- Device Pool Name: Default
- Date/Time Group: CMLocal
- Media Resource Group List: MRGL_1
- Network Hold MOH Audio Source: SampleAudioSource
- User Hold Audio Source: SampleAudioSource

Click on **Save**.

The screenshot displays the Cisco Unified CallManager Administration web interface. The top navigation bar includes links for System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The user is logged in as 'ccmadministrator'. The main heading is 'Device Pool Configuration' for the 'Default' device pool, which has 9 members. The 'Device Pool Settings' section contains various configuration options, most of which are required (indicated by an asterisk). The 'Multilevel Precedence and Preemption (MLPP) Information' section is also visible. At the bottom, there are buttons for Save, Delete, Copy, Reset, and Add New, along with a note about the number of devices that will be reset upon saving.

Device Pool Settings	
Device Pool Name*	Default
Cisco Unified CallManager Group*	Default
Date/Time Group*	CMLocal
Region*	Default
Softkey Template*	Standard User
SRST Reference*	Disable
Calling Search Space for Auto-registration	< None >
Media Resource Group List	MRGL_1
Network Hold MOH Audio Source	2-SampleAudioSource
User Hold MOH Audio Source	2-SampleAudioSource
Network Locale	United States
User Locale	English, United States
Connection Monitor Duration	

Multilevel Precedence and Preemption (MLPP) Information	
MLPP Indication*	Default
MLPP Preemption*	Default
MLPP Domain	< None >

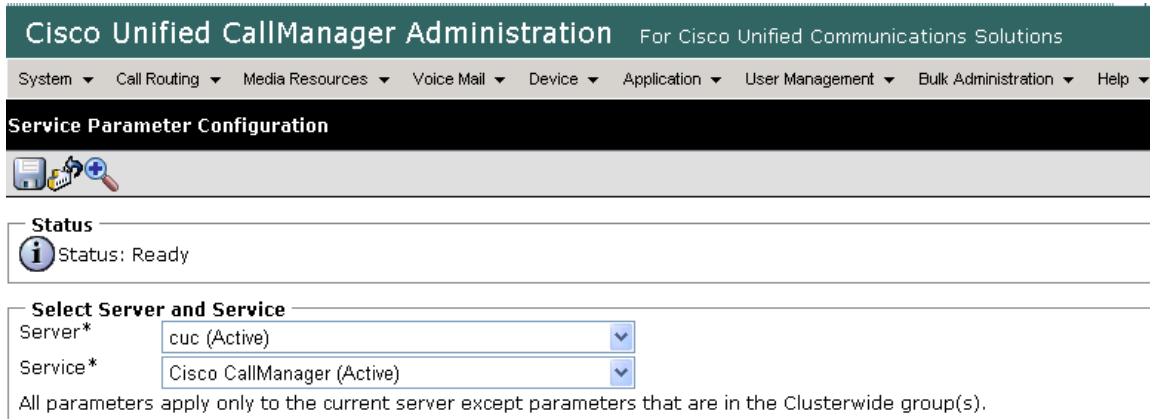
Buttons: Save, Delete, Copy, Reset, Add New

*- indicates required item.

*** Number of devices that have to be reset when this device pool is updated. To see a detailed list of these devices and other dependencies, click on Dependency Records.

5.4. Configure System Music on Hold Settings

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 Call Manager (Active)** from **Service**.



Cisco Unified CallManager Administration For Cisco Unified Communications Solutions

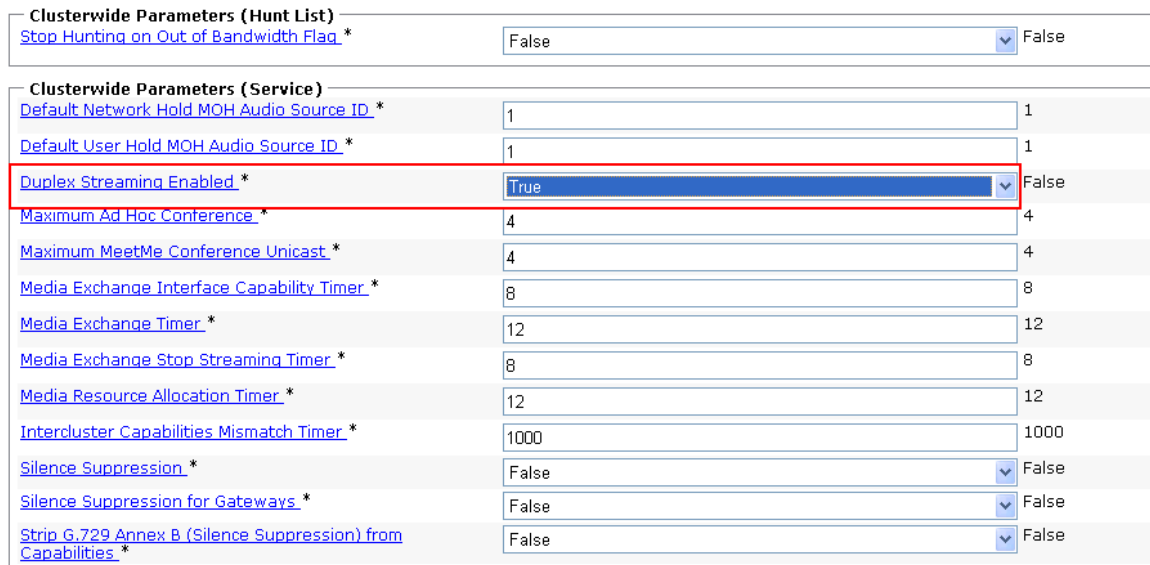
System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Service Parameter Configuration

Status
Status: Ready

Select Server and Service
Server* cuc (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**.



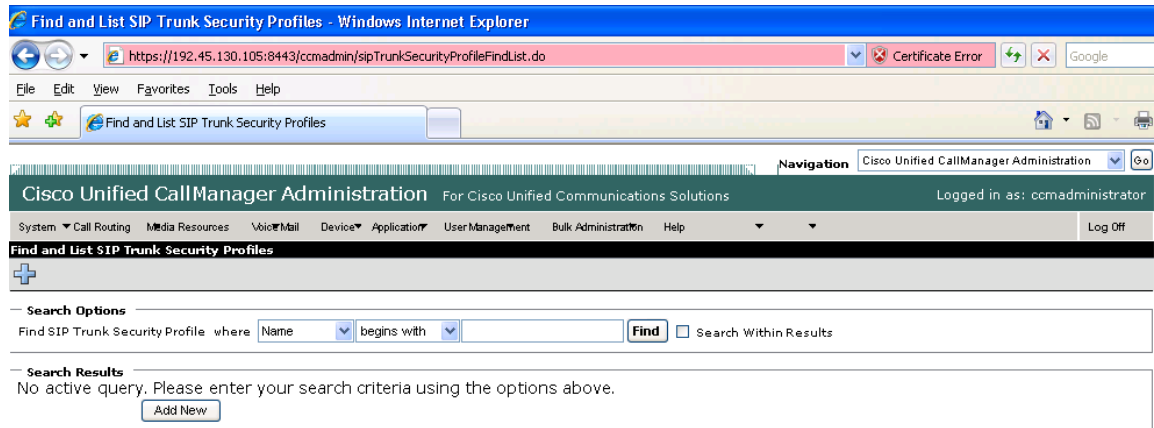
Clusterwide Parameters (Hunt List)
[Stop Hunting on Out of Bandwidth Flag](#) * False ▾ False

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
Maximum Ad Hoc Conference *	4	4
Maximum MeetMe Conference Unicast *	4	4
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
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

5.5. 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 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.

Cisco Unified CallManager Administration For Cisco Unified Communications Solutions
Navigation: Cisco Unified CallManager Administration Go
Logged in as: ccmadministrator
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help Log Off

SIP Trunk Security Profile Configuration Related Links: Back To Find/List Go

Status
Status: Ready

SIP Trunk Security Profile Information

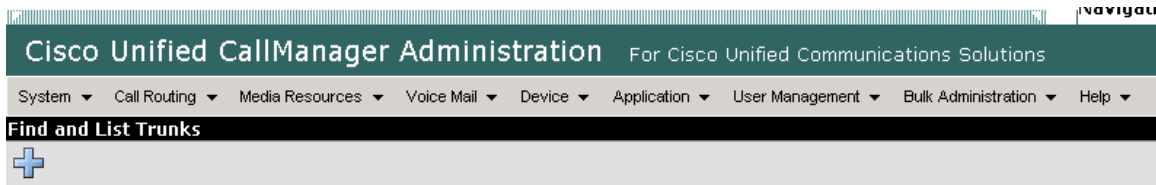
Name *	Avaya SIP Trunk
Description	SIP trunk security profile to Avaya Session Manager
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5060
<input type="checkbox"/> Enable Application Level Authorization	
<input checked="" type="checkbox"/> Accept Presence Subscription	
<input checked="" type="checkbox"/> Accept Out-of-Dialog REFER	
<input checked="" type="checkbox"/> Accept Unsolicited Notification	
<input checked="" type="checkbox"/> Accept Replaces Header	

Save Delete Copy Reset Add New

i *- indicates required item.

5.6. 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.

A screenshot of the Cisco Unified CallManager Administration web interface, specifically the 'Trunk Configuration' section. The top navigation bar is the same as the previous screenshot. Below the 'Trunk Configuration' header, there is a green arrow icon. The 'Status' section shows '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 configuration section 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 5.2.7)

Navigation

Cisco Unified CallManager Administration
For Cisco Unified Communications Solutions

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

Trunk Configuration

Status

Status: Ready

Device Information

Product:

SIP Trunk

Device Protocol:

SIP

Device Name*

SIP_Trunk_To_Avaya_BR

Description

SIP_Trunk_To_Avaya CM601_SM61_BR

Device Pool*

Default

Call Classification*

Use System Default

Media Resource Group List

MRGL_1

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

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.

Multilevel Precedence and Preemption (MLPP) Information

MLPP Domain < None >

Call Routing Information

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	

☐ Redirecting Diversion Header Delivery - Inbound

Outbound Calls

Calling Party Selection*	Originator
Calling Line ID Presentation*	Default
Calling Name Presentation*	Default
Caller ID DN	
Caller Name	

☒ 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 5.5
DTMF Signaling Method	Select RFC 2833

Click **Save** to complete.

SIP Information

Destination Address* 10.1.2.210

☐ Destination Address is an SRV

Destination Port* 5060

MTP Preferred Originating Codec* 711ulaw

Presence Group* Standard Presence group

SIP Trunk Security Profile* Avaya SIP Trunk

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* RFC 2833

5.7. Administer Route Pattern

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 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 CallManager Administration For Cisco Unified Communications Solutions

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

Find and List Route Patterns

Search Options

Find Route Patterns where Pattern ▾ begins with ▾ **Find** ☐ Search Within Results

Search Results

No active query. Please enter your search criteria using the options above.

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 “SIP_Trunk_To_Avaya_BR”, which has already been defined as the “SM61” SIP Trunk defined in **Section 5.6**. Parameters on this screen other than those indicated below can be left at their default values. Click **Save** to complete the form (not shown).

Cisco Unified CallManager Administration For Cisco Unified Communications Solutions

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

Route Pattern Configuration

Status
Status: Ready

Pattern Definition

Route Pattern* 3XXXX

Route Partition < None >

Description To Avaya CM601_SM61_BR

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence* Default

Gateway/Route List* SIP_Trunk_To_Avaya_BR (Edit) Find

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

5.8. Configure Audio Codecs

Select **System** → **Region** from the top menu and select the **default** profile. Under **Modify Relationships to other Regions**, select **Default** under **Regions**.

The screenshot shows the Cisco Unified CallManager Administration web interface. The top navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'Region Configuration' page is active, showing the 'Default' region. The 'Region Relationships' table lists the 'Default' region with 'G.711' audio codec and '384' video call bandwidth. The 'Modify Relationship to other Regions' section shows the 'Default' region selected, with 'Keep Current Setting' chosen for the audio codec and 'Use System Default' for the video call bandwidth. The page includes a 'Save' button and a footer with a note about audio codec selection.

Region	Audio Codec	Video Call Bandwidth
Default	G.711	384

Regions	Audio Codec	Video Call Bandwidth
Default	Keep Current Setting	<input checked="" type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input type="text"/> kbps

Save Delete Reset Add New

*- indicates required item.
**The Audio Codec selection determines bandwidth only. The G.711 and G.722 codecs both result in a maximum bandwidth of 64 Kbps between regions and can be used interchangeably.

Click **Save** to save configuration.

5.9. Configure Voice Mail Pilot




Configure voice mail coverage for telephone users. Select **Voicemail → Voicemail 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.

Cisco Unified CallManager Administration


For Cisco Unified Communications Solutions

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

Voice Mail Pilot Configuration



Status

 Status: Ready

Voice Mail Pilot Information

Voice Mail Pilot Number

33000

Calling Search Space

< None > ▾

Description


BR MM via SM61

☒ Make this the default Voice Mail Pilot for the system

Save

Delete

Add New

 *- indicates required item.

5.10. Configure Voice Mail Profile


Select **Voicemail** → **Voicemail 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 5.9**. Click **Save** to save the configuration.

Cisco Unified CallManager Administration


For Cisco Unified Communications Solutions

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

Voice Mail Profile Configuration



Status

 Status: Ready

Voice Mail Profile Information

Voice Mail Profile BR_SM61 (used by 2 devices)


Voice Mail Profile Name*


Description

Voice Mail Pilot**

Voice Mail Box Mask

☐ Make this the default Voice Mail Profile for the System

 *- indicates required item.

 **- The Voice Mail Pilot is comprised of the Voice Mail Pilot Number and it's corresponding Calling Search Space Name (CSS) (>).

5.11. 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 5.2**. Click on the line for the telephone as highlighted in the screen below.

The screenshot displays the Cisco Unified CallManager Administration interface. At the top, the navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'Device' menu is expanded, showing 'Phone Configuration'. The 'Status' section indicates 'Status: Ready'. The 'Association Information' section on the left lists several items, with 'Line [1] - 5005 (no partition)' highlighted. The 'Phone Type' section on the right shows 'Product Type: Cisco 7941G-GE' and 'Device Protocol: SIP'. The 'Device Information' section on the right lists various configuration parameters, with 'Media Resource Group List' highlighted and set to 'MRGL_1'.

Association Information	
1	Line [1] - 5005 (no partition)
2	Line [2] - Add a new DN
3	Unassigned Associated Items
4	Add a new SD
5	Add a new BLF SD
6	Privacy
7	None

Phone Type	
Product Type:	Cisco 7941G-GE
Device Protocol:	SIP

Device Information	
Registration	Registered with Cisco Unified CallManager cuc
IP Address	172.28.43.222
MAC Address*	0019563CBF86
Description	SEP0019563CBF86 - BR2
Device Pool*	Default
Phone Button Template*	Standard 7941G-GE SIP
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	MRGL_1
User Hold MOH Audio Source	2-SampleAudioSource
Network Hold MOH Audio Source	2-SampleAudioSource
Location*	Hub_None
User Locale	< None >
Network Locale	< None >

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 CallManager Administration
For Cisco Unified Communications Solutions

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

Directory Number Configuration
Re

Status
 Status: Ready

Directory Number Information
Directory Number* 5005
Route Partition < None >
Description Phone BR2 CUCM 5.x
Alerting Name Phone BR2 CUCM 5.x
ASCII Alerting Name Phone BR2 CUPhone BR2 CUCM 5.x
☒ Allow Control of Device from CTI
Associated Devices SEP0019563CBF86
Edit Device
Edit Line Appearance
Dissociate Devices

Navigate to **Directory Number Settings** and select the **Voice Mail Profile** created in **Section 5.10**.

Directory Number Settings
Voice Mail Profile BR_SM61 (Choose <None> to use system default)
Calling Search Space < None >
Presence Group* Standard Presence group
AAR Group < None >
User Hold MOH Audio Source 2-SampleAudioSource
Network Hold MOH Audio Source 2-SampleAudioSource
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
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 >
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 SEP0019563CBF86	
Display (Internal Caller ID)	Phone BR2
Display text for a line appearance is intended for displaying text such as a name instead of a directory 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)	Phone BR2
Line Text Label	Phone BR2 - 5005
ASCII Line Text Label	Phone BR2 - 5005
External Phone Number Mask	5XXX
Message Waiting Lamp Policy*	Use System Policy
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.	

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

— **Forwarded Call Information Display on Device SEP0019563CBF86** —

☒ Caller Name

☒ Caller Number

☒ Redirected Number

☒ Dialed Number

— —

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.

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

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"/>	SM1	19/40	1	0	3

Select : All, None

All Monitored SIP Entities

Run Monitor

37 Items | Refresh | Show 15 | Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	CM-ES R6.0.1
<input type="checkbox"/>	CM-Evolution-procr-5062
<input type="checkbox"/>	CM-Evolution-procr-5065
<input type="checkbox"/>	CM5-2-1
<input type="checkbox"/>	CM601-Evolution-procr-5064
<input type="checkbox"/>	CM601-Evolution-procr-5068
<input type="checkbox"/>	CS1000E R7.0
<input type="checkbox"/>	CS1K R5.5
<input type="checkbox"/>	CUCM-513
<input type="checkbox"/>	Denver Nortel CS1000e

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 (**CUCM-513**) and verify that the **Link Status** is **Up**, as shown below:

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	SM1	10.1.2.220	5060	TCP	Up	200 OK	Up

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: CUCM-513

Summary View

1 Item | Refresh Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	SM1	192.45.130.105	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.

Session Manager

Session Manager

Home

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

Help ?

ReadCommit

Tracer Configuration

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 Server to Security Module:☐

Trace Dropped Messages:☒

Send Trace to a Remote Server:☐

Remote Server FQDN or IP Address:

Tunnel Port:

From Security Module to Network:☒

From Security Module to Server:☐

Max Dropped Message Count:

Send Trace Method:

Syslog (unsecure UDP)

User Filter

NewDelete

<input type="checkbox"/>	From	To	Source	Destination	Max Message Count
--------------------------	------	----	--------	-------------	-------------------

Call Filter

NewDelete

<input type="checkbox"/>	From	To	Source	Destination	Max Call Count	Request URI
--------------------------	------	----	--------	-------------	----------------	-------------

Session Manager Instances

1 Item RefreshFilter: Enable

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

Select : All, None

ReadCommit

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: 3731

4 Items Found
Refresh
Filter: Disable, Apply, Clear

	Details	Time	Tracing Entity	From	Action	To	Protocol	Call ID
				< sip:36002@10.1.2.210 >	-- INVITE -->			
	Show	13:10:36.497	SM1	< sip:36002@10.1.2.210 >	-- INVITE -->	"Phone BR1" < sip:5004@192.45.130.105 >	TCP	660f3800-d5e1c899-8c0-69822dc0@192.45.130.105
	Show	13:10:36.532	SM1	< sip:36002@10.1.2.210 >	-- INVITE -->	"Phone BR1" < sip:5004@192.45.130.105 >	TCP	660f3800-d5e1c899-8c0-69822dc0@192.45.130.105
	Show	13:16:48.176	SM1	< sip:36002@10.1.2.210 >	-- INVITE -->	"Phone BR1" < sip:5004@192.45.130.105 >	TCP	43315380-d5e1ca0c-8d2-69822dc0@192.45.130.105
	Hide	13:16:48.212	SM1	< sip:36002@10.1.2.210 >	-- INVITE -->	"Phone BR1" < sip:5004@192.45.130.105 >	TCP	43315380-d5e1ca0c-8d2-69822dc0@192.45.130.105

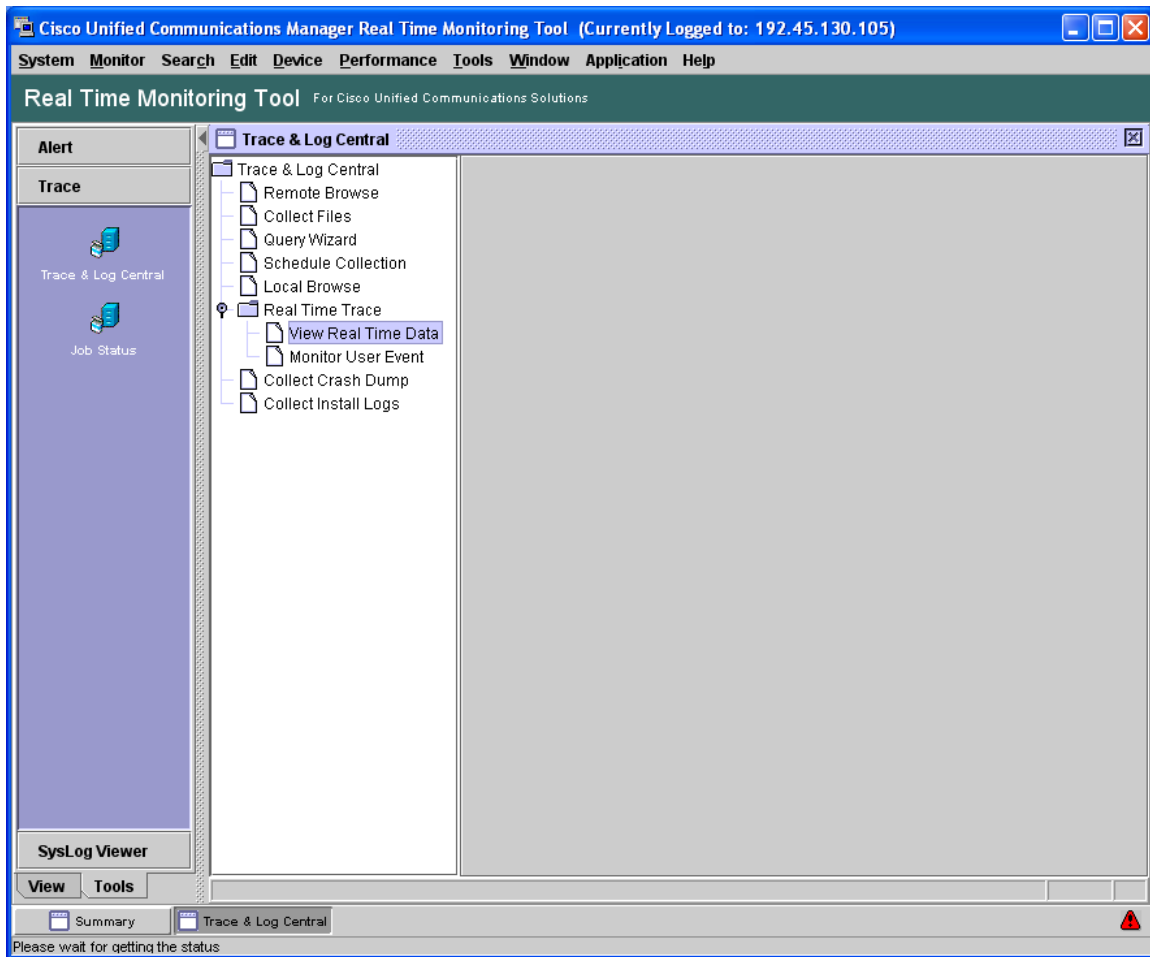
SIP Message

Feb 18 13:16:48 sm61 AasSipMgr[4576]:
-05:00 2011 212 1 com.avaya.asm | 2 com.avaya.asm SIPMSGT ----- 18/02/2011 13:16:48.212 --> octets: 1239, Body Length: 0

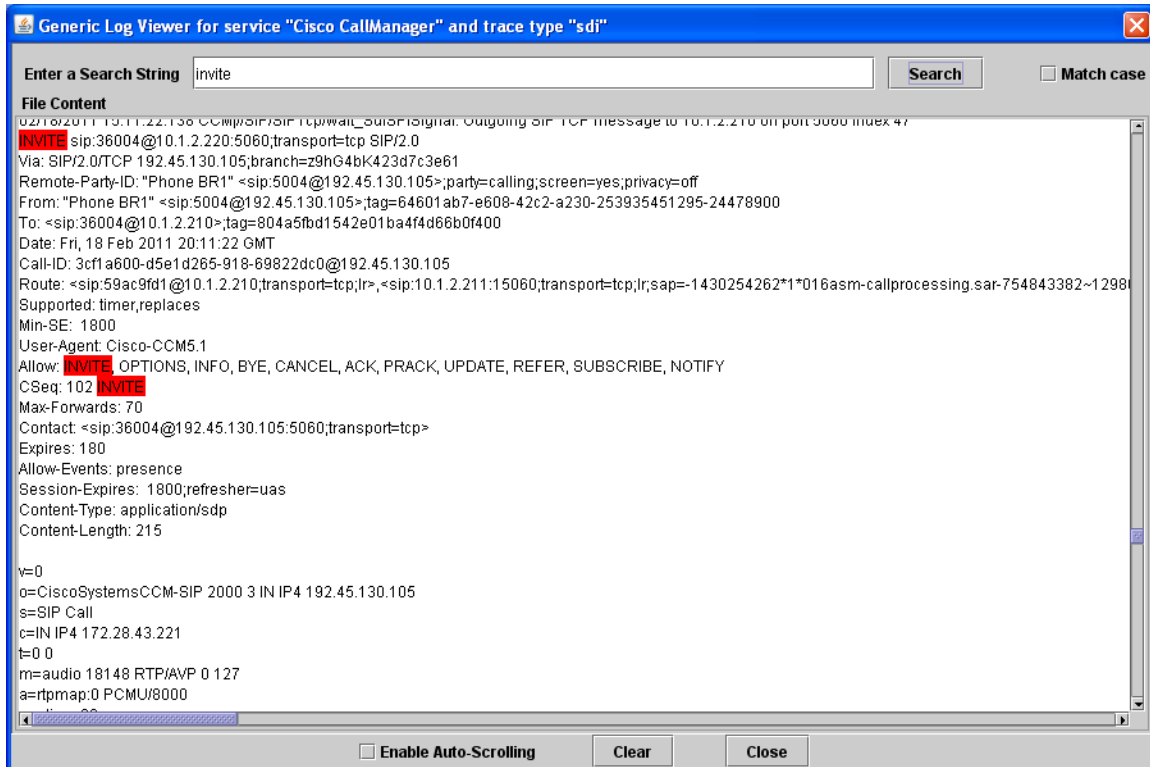
ingress: { L10.1.2.210:5060/R10.1.2.210:36520/TCP/0xc502 }
egress: [NO TARGET]
SIPMsgContext: [NONE] -----
INVITE sip:5004@192.45.130.105:5060;transport=tcp SIP/2.0
From: < sip:36002@10.1.2.210 >;tag=8034d5c11042e015e4f4d66b0f400
To: "Phone BR1" < sip:5004@192.45.130.105 >;tag=64601ab7-e608-42c2-a230-253935451295-24478892
Call-ID: 43315380-d5e1ca0c-8d2-69822dc0@192.45.130.105
CSeq: 1 INVITE
P-Av-Transport: AP;fe=10.1.2.220:10089;ne=10.1.2.210:5060;tt=TCP;th
Via: SIP/2.0/TCP 10.1.2.211:15070;branch=z9hG4bK0A0102D325D3497C0602893
Via: SIP/2.0/TCP 10.1.2.211:15070;branch=z9hG4bK0A0102D325D3497C1602891
Via: SIP/2.0/TCP 10.1.2.210;branch=z9hG4bK808e37c41042e015f4f4d66b0f400-AP;ft=13301
Via: SIP/2.0/TCP 10.1.2.220;branch=z9hG4bK808e37c41042e015f4f4d66b0f400
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH

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 a Cisco user to an Avaya 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 Avaya Aura® Communication Manager and Cisco UCM can be made in both directions with media shuffled directly between the endpoints, 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
 - Consultation hold
 - Call forwarding
 - Conference

7. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager R6.0.1 can interoperate with Cisco Unified Communications Manager R5.1.3 using SIP trunks via Avaya Aura® Session Manager R6.1.

The following is a list of interoperability items to note:

- Calls originated by Cisco SCCP telephones to Avaya H.323 or SIP telephones did not shuffle over the SIP trunk. Although shuffling did not work, the calls were successful.
- Calls (voice) originated by Cisco SCCP or SIP telephones to the Avaya Video Desktop Device did not shuffle over the SIP trunk. Although shuffling did not work, the calls were successful.
- On calls originated by Cisco SIP telephones to any Avaya telephone, when the Cisco SIP telephones attended transferred the call to another remote Avaya telephone, there was no audio after the call was transferred. Enabling the “Media Termination Point Required” field on the Cisco UCM SIP trunk (Section 5.6) resolved the problem. This issue was not observed for unattended transferred calls.

- A Cisco telephone hold/resume issue was observed when “IP video” was enabled on the Avaya Aura® Communication Manager SIP trunk. Disabling “IP Video” on the Communication Manager signaling group resolved the issue (Section 3.5.1). Alternatively, disabling shuffling on the Avaya or Cisco side also resolved the issue.
- Cisco UCM R5.1.3 did not reply to SIP UPDATE messages from Avaya Aura® Communication Manager even though it originally signals Avaya that it supports the UPDATE method in the “Allow” header (see Section 6.3 for sample INVITE from Cisco UCM). Avaya Aura® Communication Manager was configured to disable SIP UPDATES on the SIP trunk (Section 3.5.2).
- Calling and Called Party Name and Number displays may not be consistent in some cases for basic calls and calls involving transfers, conferences, and call forwarding.
 - On calls originated by Cisco SCCP telephones to Avaya H.323 or SIP telephones, upon answering the connected number on the Avaya telephones displayed the Avaya telephone number instead of the Cisco SCCP telephone number. The connected name was displayed correctly. The telephone name and number was also displayed correctly during the ringing process. This issue happened because Cisco sent Avaya an “in-dialog” re-INVITE message with the wrong number in the contact header and Session Manager built a P-Asserted-ID header based on the contents of the Contact Header. A workaround for this issue was found in Communication Manager by setting the “Identity for Calling Party Display” parameter on the SIP Trunk Group form to “From” (Section 3.5.2).
 - On held calls by Cisco SIP or SCCP telephones to Avaya H.323 or SIP telephones, the connected number on Avaya telephones displayed the Avaya telephone number after resuming the call. The same workaround documented for the first display issue above fixes this issue.
 - On calls originated by Cisco SCCP or SIP to Avaya H.323 and SIP telephones, when the Cisco telephones blind transferred the call to another local Cisco telephone, the display on the Avaya telephone still showed the original calling party name with its own telephone number. Setting the Communication Manager “Identity for Calling Party Display” parameter on the SIP Trunk Group form to “From” (Section 3.5.2) fixed the telephone number display issue; however the issue still remains that the display on the Avaya telephone remains unchanged after the transfer.
 - On calls originated by Cisco SCCP or SIP to Avaya digital telephones when the Cisco telephones transferred (attended or unattended) the call to another local Cisco telephone, the display on the Avaya telephones remained unchanged after the transfer.
 - On calls originated by Avaya SIP telephones to any Cisco telephone, when the Cisco telephone forwarded the call to another local Cisco telephone, the display on the Avaya SIP telephone shows the telephone number of the originally dialed number with the name of the forwarded-to telephone.

- On calls originated by Cisco SCCP Telephones to any Avaya telephone, when the Avaya telephone forwarded the call to another local Avaya SIP telephone, the display on the forwarded-to Avaya SIP telephone displayed its own telephone number. The name was displayed properly. Setting the Communication Manager “Identity for Calling Party Display” parameter on the SIP Trunk Group form to “From” (Section 3.5.2) fixed the issue.
- On calls originated by any Avaya telephone to any Cisco telephone, when the Cisco telephone forwarded the call to a remote Avaya telephone, the display on the calling Avaya telephone shows the telephone number of the originally dialed number with the name of the forwarded-to telephone.

8. Additional References

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

- [1] *Avaya Avaya® Session Manager Overview*, Doc # 03-603323, Issue 2
- [2] *Administering Avaya Avaya® Session Manager*, Doc # 03-603324, Issue 2
- [3] *Maintaining and Troubleshooting Avaya Avaya® Session Manager*, Doc # 03-603325, Issue 2
- [4] *Administering Avaya Aura® Communication Manager Server Options*, Doc # 03-603479, Issue 2, June 2010.
- [5] *SIP Support in Avaya Avaya® Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, Issue 9, May, 2009.
- [6] *Administering Avaya Avaya® 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 CallManager Manager Administration Guide, Release 5.1\(3\)*](#), Part Number: OL-14152-01
- [8] [*Cisco Unified CallManager Features and Services Guide, Release 5.1\(3\)*](#), Part Number: OL-14154-01
- [9] [*Cisco Unified CallManager Serviceability Administration Guide, Release 5.1\(3\)*](#), “[*Real-Time Monitoring Configuration*](#)”, “[*Trace Collection and Log Central in RTMT*](#)”

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

- [10] *Configuring Avaya Modular Messaging 5.2 with Cisco Unified Communications Manager 7.15 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