Avaya Solution & Interoperability Test Lab

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

Abstract

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

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

1. Introduction

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

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

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

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

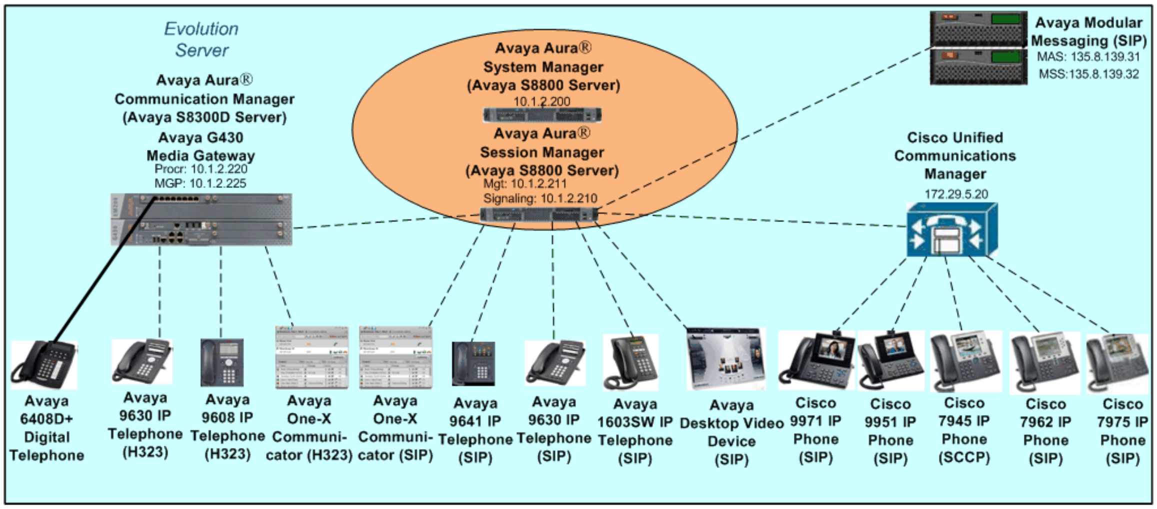


Figure 1: Sample Configuration

2. Equipment and Software Validated

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

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

3. Configure Avaya Aura® 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 Attd-Extended/Transferred Calls: transferred
                   Automatic Circuit Assurance (ACA) Enabled? n
```

3.3. Configure IP Node Names

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

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

3.4. Configure IP Network Region and Codec Set

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

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

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

```
change ip-codec-set 1                                           Page   1 of   2

                          IP Codec Set
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.722-64K                   2        20
 2: G.711MU          n          2        20
 3: G.729A           n          2        20
```

[1] Direct media, and therefore G.722 is not supported for calls from Cisco SCCP telephones to Avaya H323 and SIP telephones.
[2] Direct media is not supported for G.729A calls from Cisco telephones to the Avaya 1603 IP Telephone (SIP).

3.5. Configure SIP Signaling Group and Trunk Group

3.5.1. SIP Signaling Group

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

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

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



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

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

[3] 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
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

3.6. Configure Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use the **change route-pattern n** command, where **n** is the route pattern number. Configure this route pattern to route calls to trunk group number **60** configured in **Section 3.5.2.** Assign the lowest **FRL** (facility restriction level) to allow all callers to use this route pattern. For **LAR** in row number (1) corresponding to the first trunk group entry, enter **next**. This will ensure that for calls (SIP INVITEs) for which Communication Manager receives no response, the shorter **Alternate Route Time**r 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
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                     next
 2: y y y y y n  n            rest                                     none
 3: y y y y y n  n            rest                                     none
 4: y y y y y n  n            rest                                     none
```

3.7. Configure Private Numbering

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

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private           Total
Len Code             Grp(s)     Prefix            Len
 5  2                                             5     Total Administered: 6
 5  3                60                           5        Maximum Entries: 540
 5  4                                             5
 5  5                                             5
```

3.8. Configure Dial Plan and AAR analysis

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

```
change dialplan analysis                                       Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 2

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   1           3   dac
   3           5   ext
   6           5   ext
```

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

```
change aar analysis 6                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 0

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    6                     5    5     60       unku         n
```

3.9. Save Changes

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

```
save translation

                               SAVE TRANSLATION

           Command Completion Status                                Error Code

           Success                                                  0
```

4. Configuring Avaya Aura® Session Manager

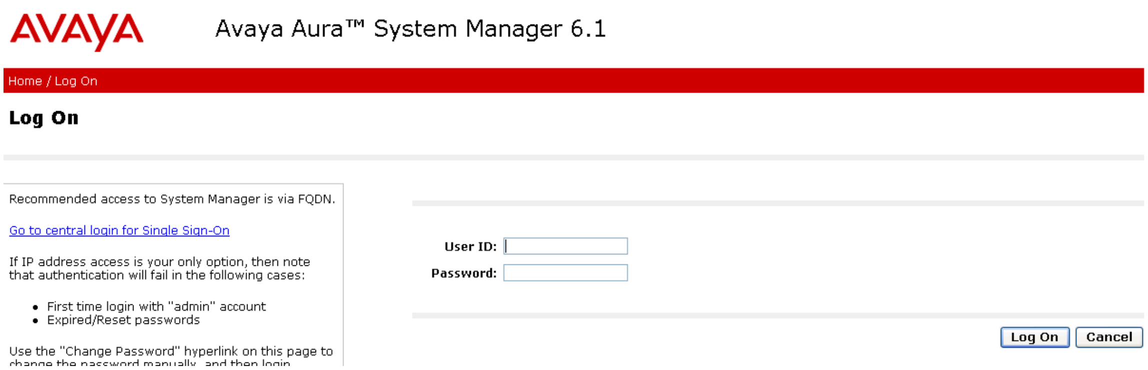
This section provides the procedures for configuring Session Manager. For further information on Session Manager, see **[1-3]**. The procedures include the following areas:

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

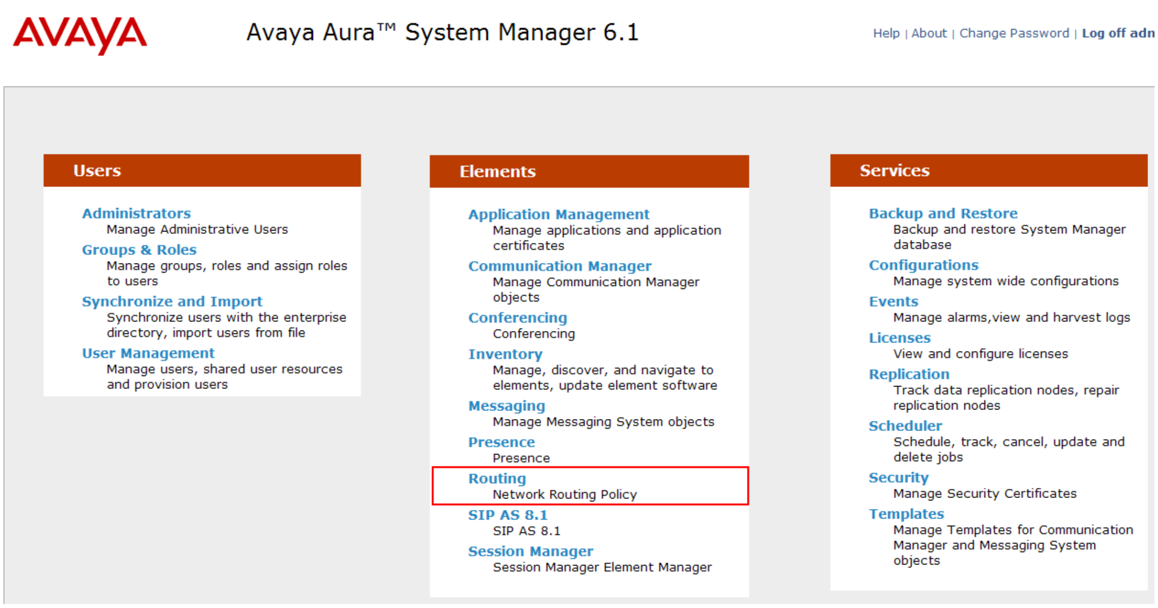
If it is desired to provide Avaya Modular Messaging support for Cisco UCM users, then see Reference **[10]** for configuring the appropriate items for Modular Messaging in Session Manager.

4.1. Log in to Avaya Aura® Session Manager

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



The 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.



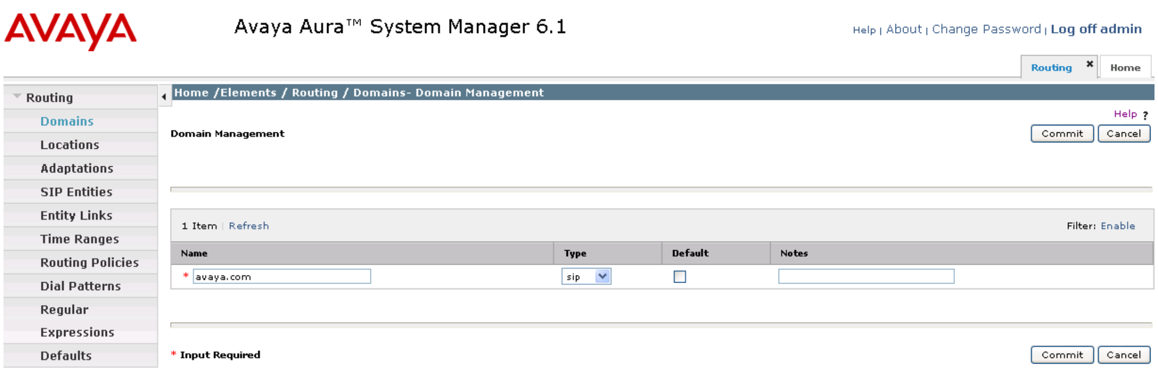
4.2. Configure SIP Domain

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.



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

4.3. Add Locations

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

Under **General**, enter:

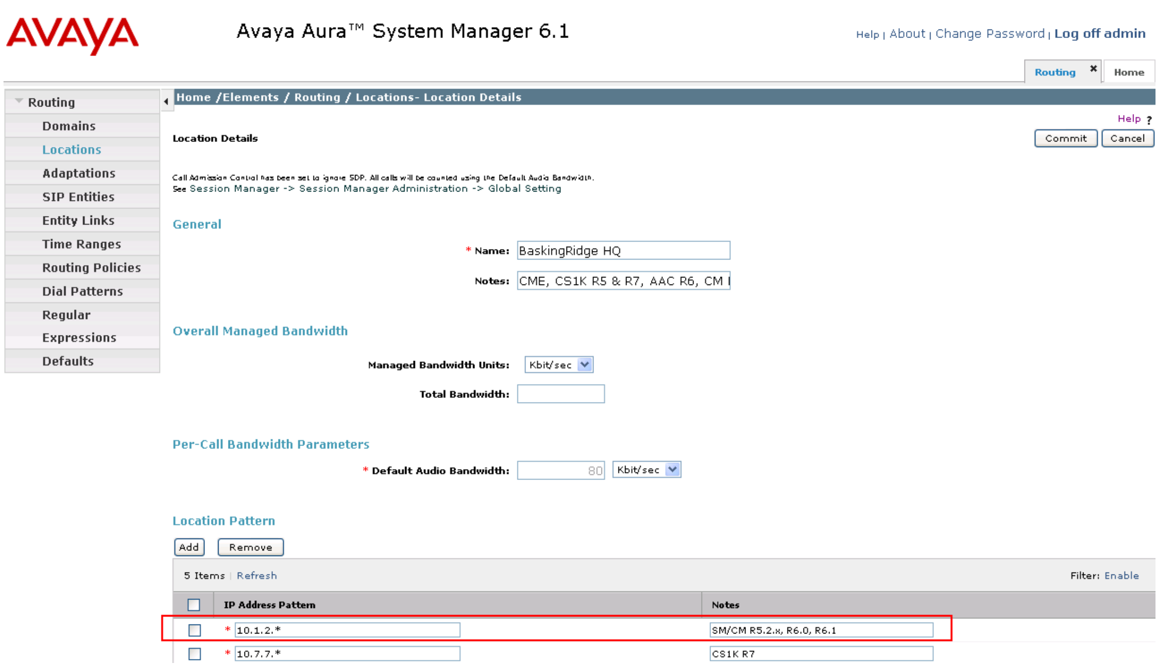
- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

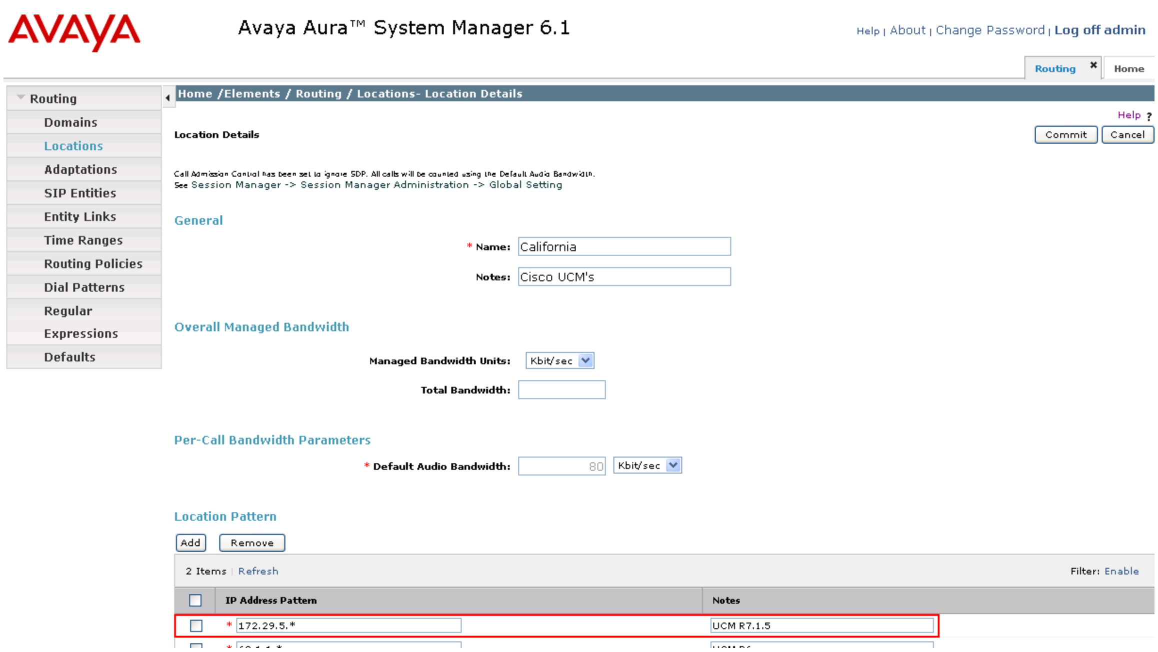
The remaining fields under **General** can be filled in to specify bandwidth management parameters between Session Manager and this location. These were not used in the sample configuration, and reflect default values. Note also that although not implemented in the sample configuration, routing policies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

Under **Location Pattern**:

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

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




AVAYA
Avaya Aura™ System Manager 6.1
Help | About | Change Password | Log off admin
Routing
Home
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home /Elements / Routing / Locations- Location Details
Help ?
Location Details
Commit
Cancel
Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting
General
* Name: California
Notes: Cisco UCM's
Overall Managed Bandwidth
Managed Bandwidth Units: Kbit/sec
Total Bandwidth:
Per-Call Bandwidth Parameters
* Default Audio Bandwidth: 80 Kbit/sec
Location Pattern
Add
Remove
2 Items | Refresh
Filter: Enable
IP Address Pattern
Notes
* 172.29.5.*
UCM R7.1.5

4.4. Configure Adaptations

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

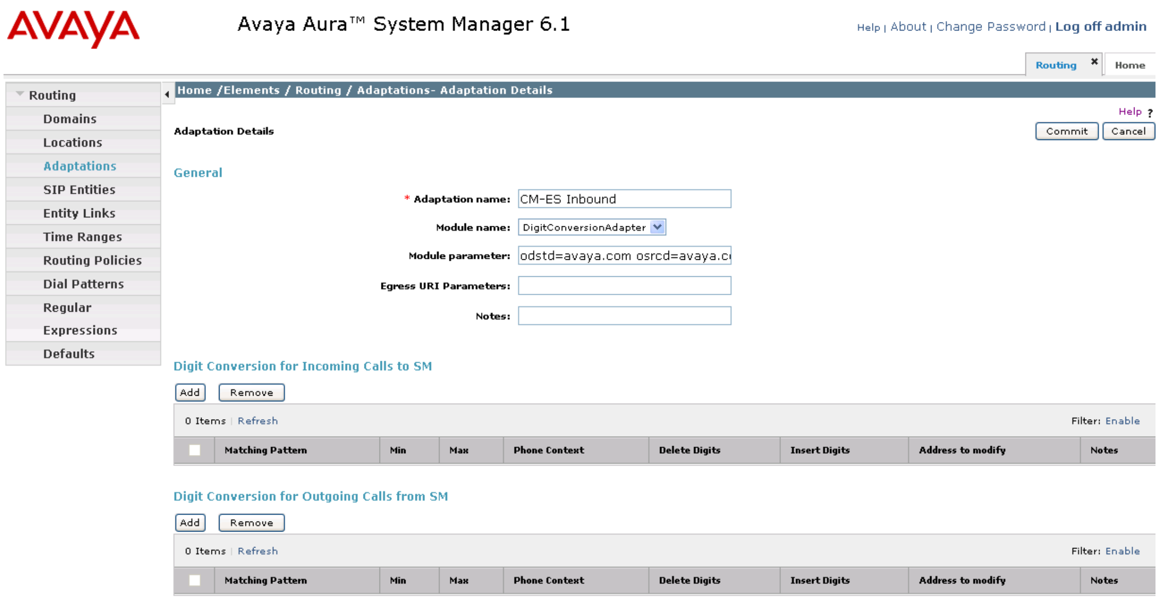
1. To set the SIP domain of incoming calls to Communication Manager to "avaya.com", so that a single SIP trunk can be configured in Communication Manager for inbound and outbound calls. See **Section 3.5.1.**
2. An adaptation module designed specifically for interoperating with Cisco Unified Communications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

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

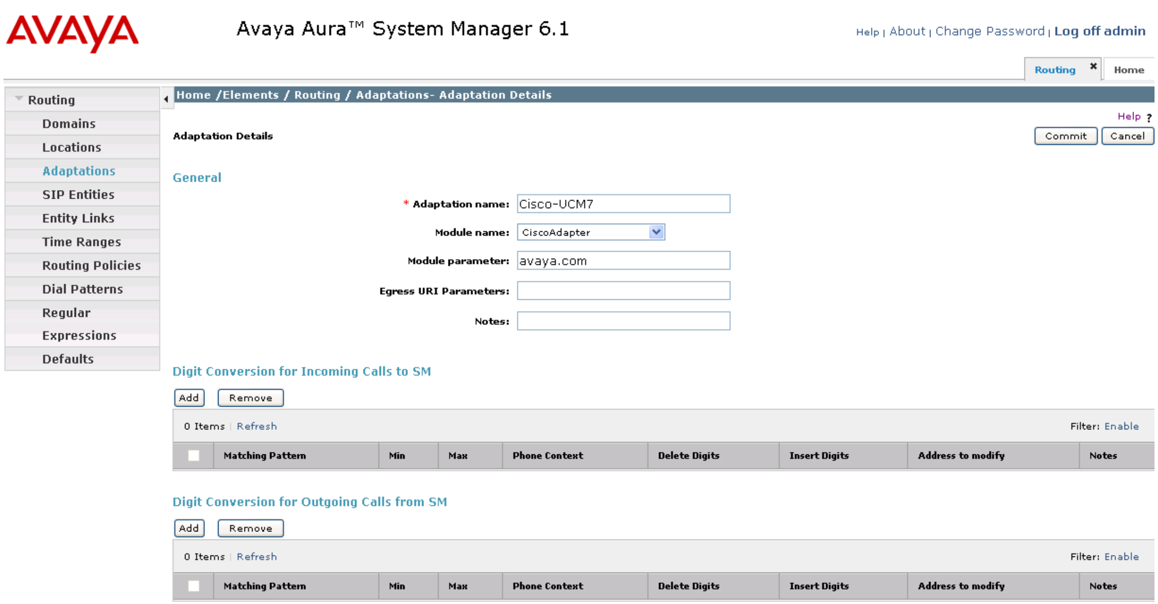
To add the adaptation module, select **Routing → Adaptations** on the left and click on the **New** button (not shown) on the right. Under **General**, fill in:

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

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



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



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:

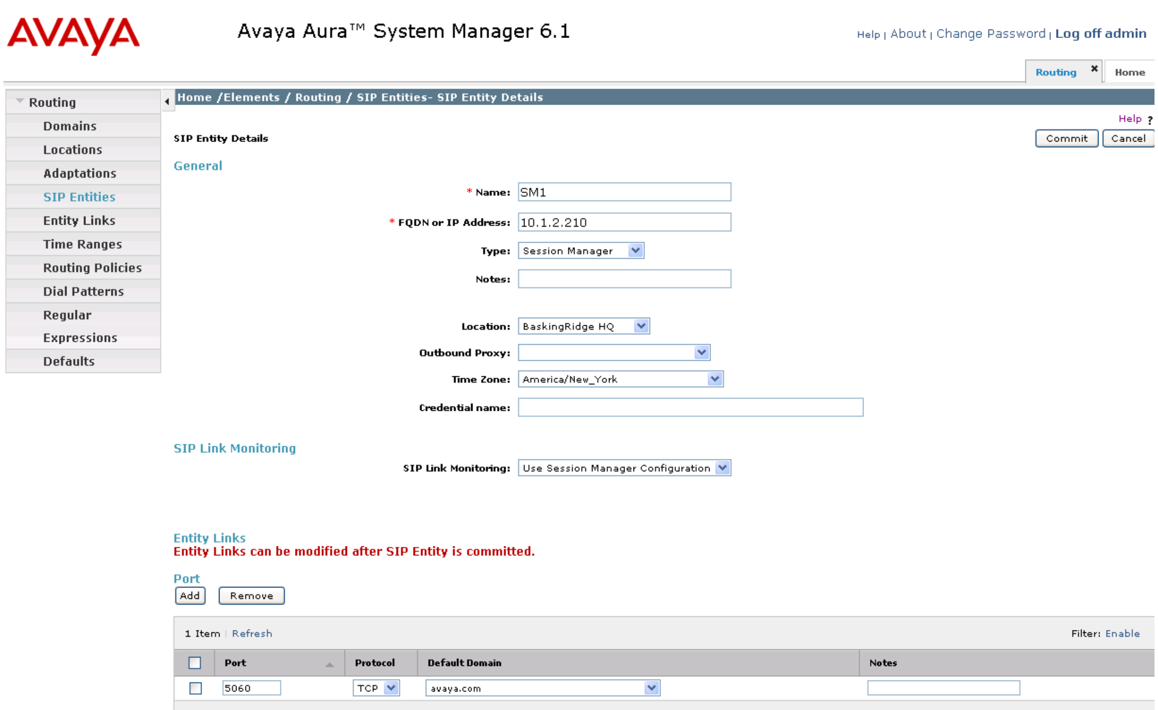
Under **General:**

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

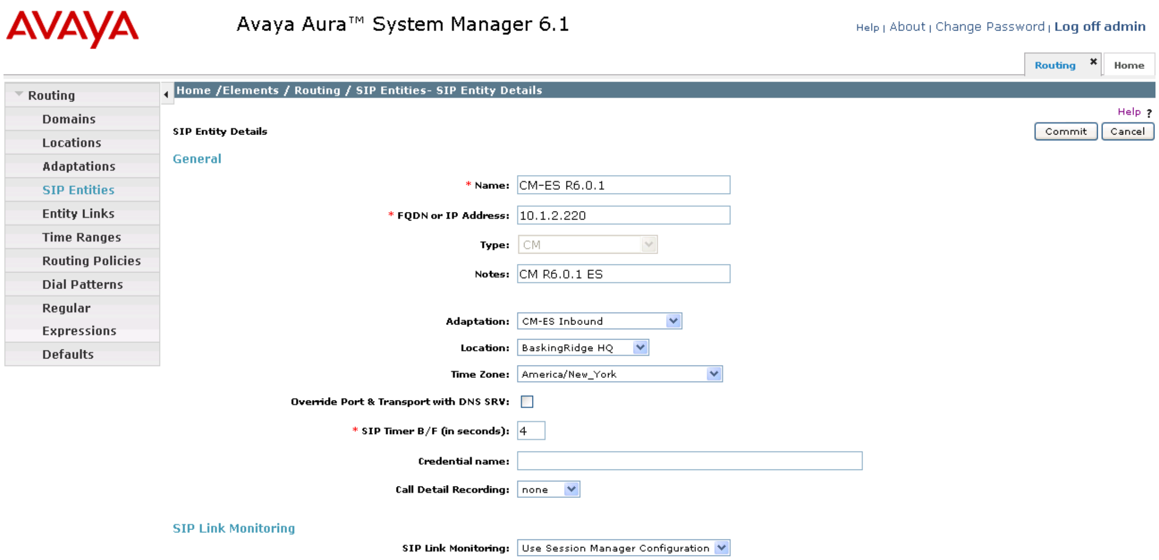
For SIP Entities of **Type** "Session Manager", under **Port**, click **Add,** and then edit the fields in the resulting new row:

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**)

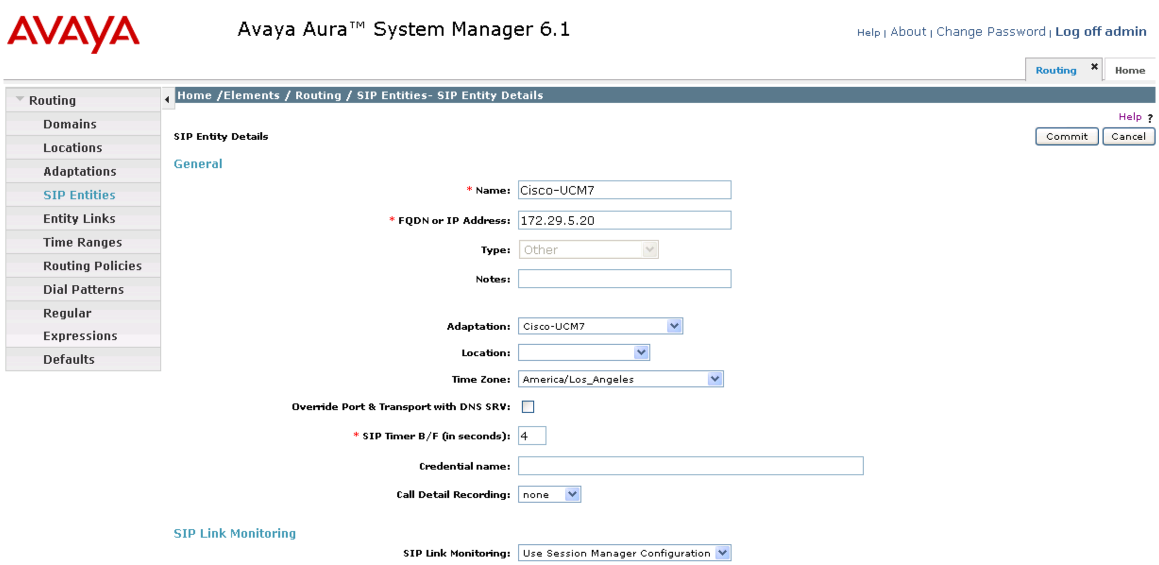
Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition. The following screen shows the SIP Entity for Session Manager.



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



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

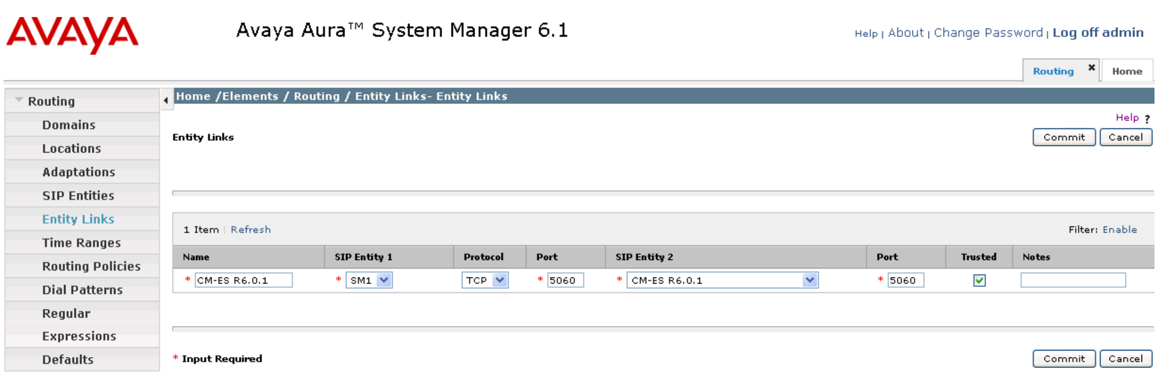


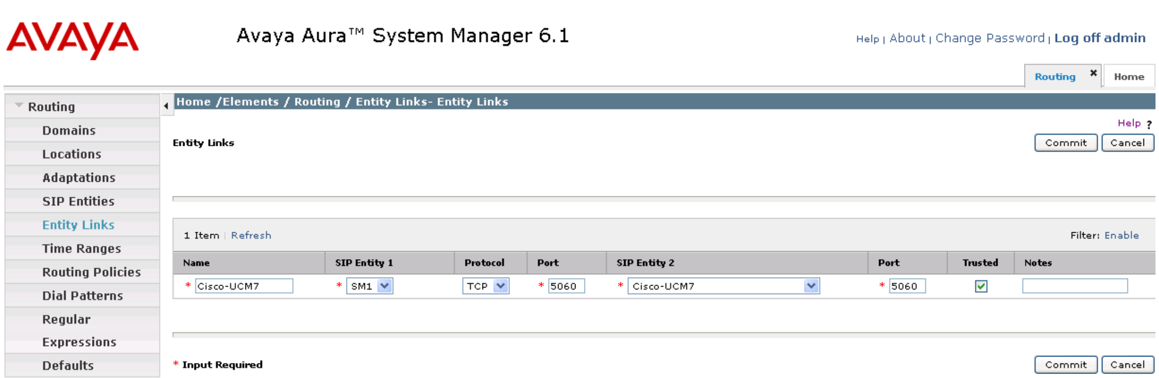
4.6. Configure Entity Links

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.





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**

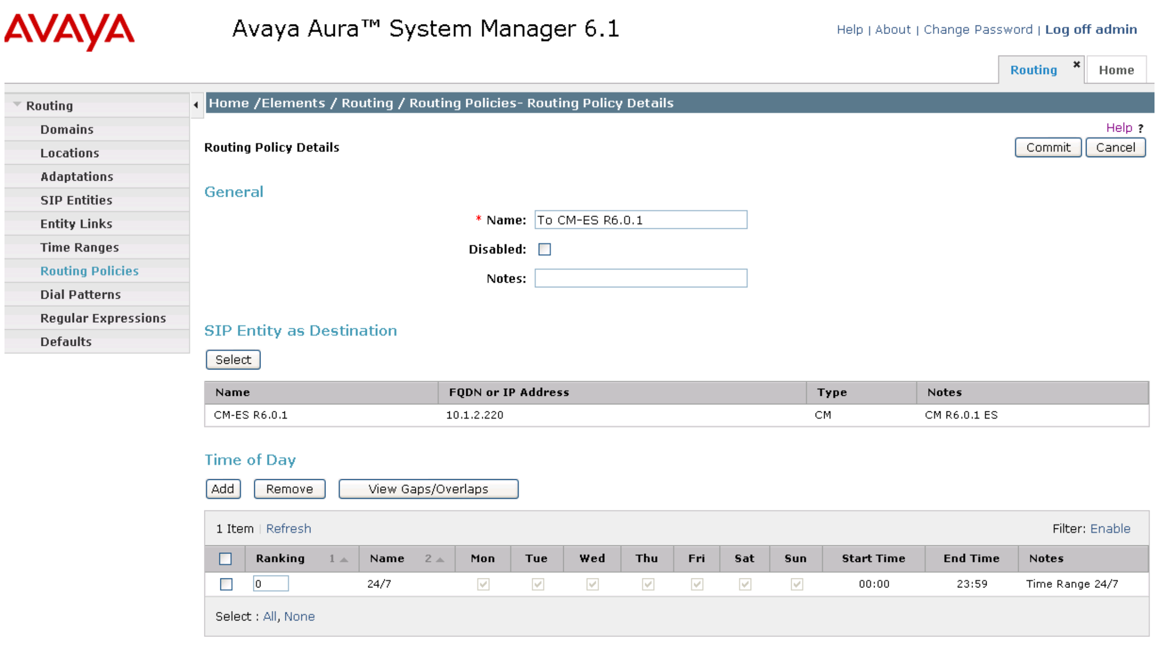
Under **SIP Entity as Destination:**

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

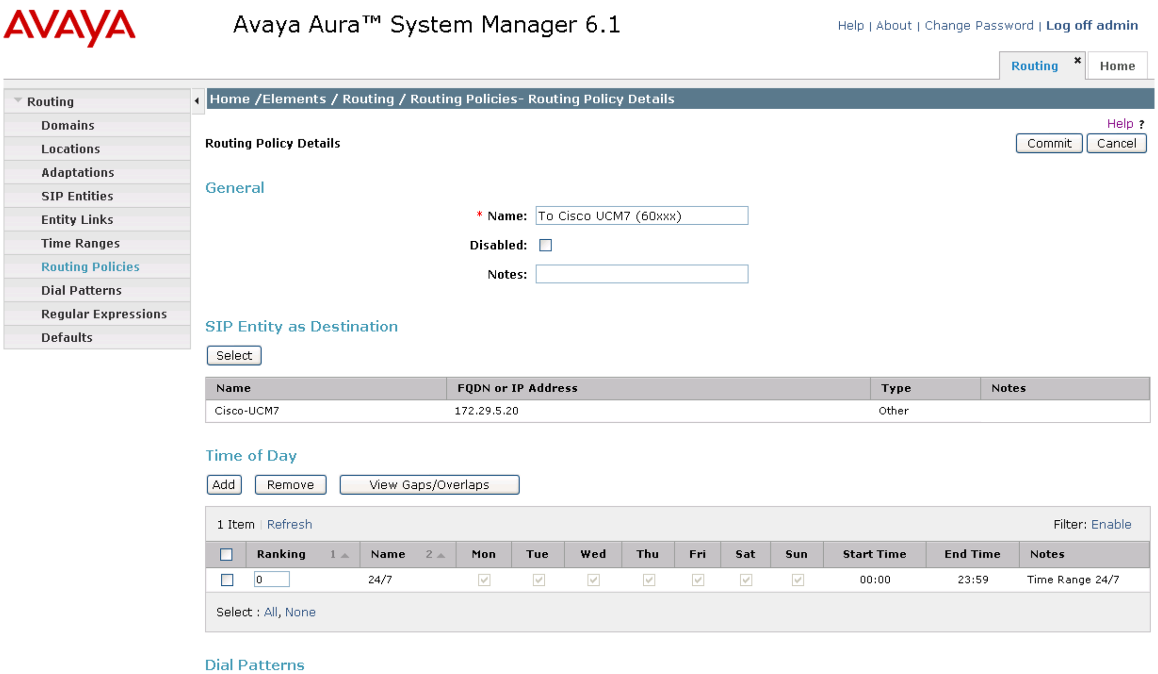
Under **Time of Day:**

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

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



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



4.8. Configure Dial Patterns

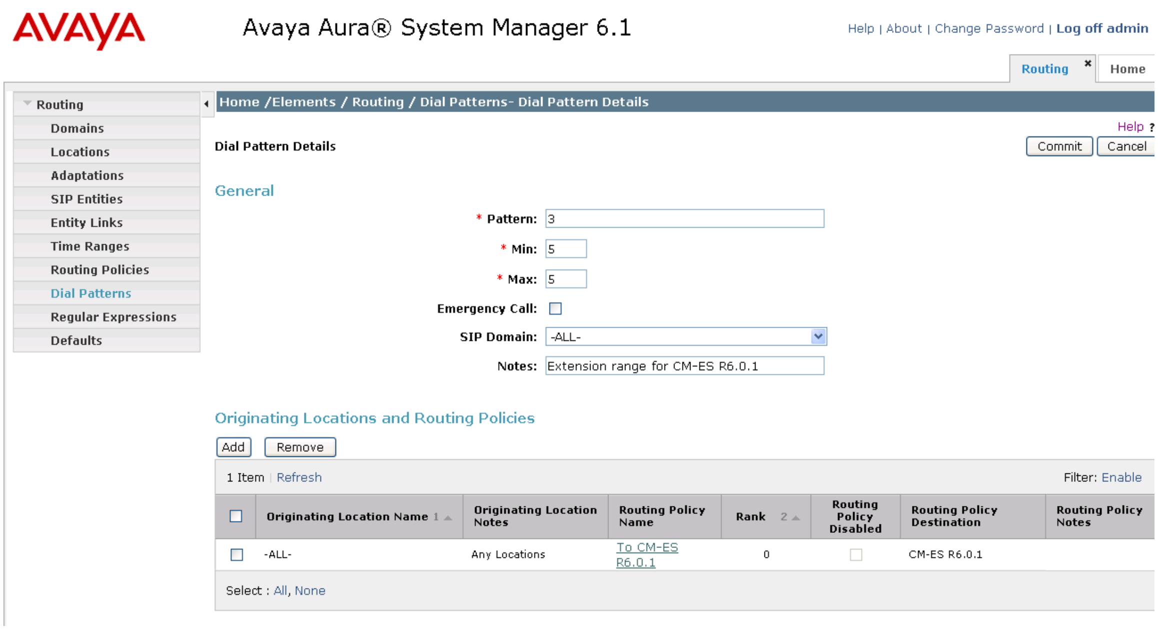
A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample configuration, 5-digit extensions beginning with 3 are supported by Communication Manager, and 5-digit extensions beginning with 60 reside on Cisco UCM. To add a dial pattern, select **Routing → Dial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

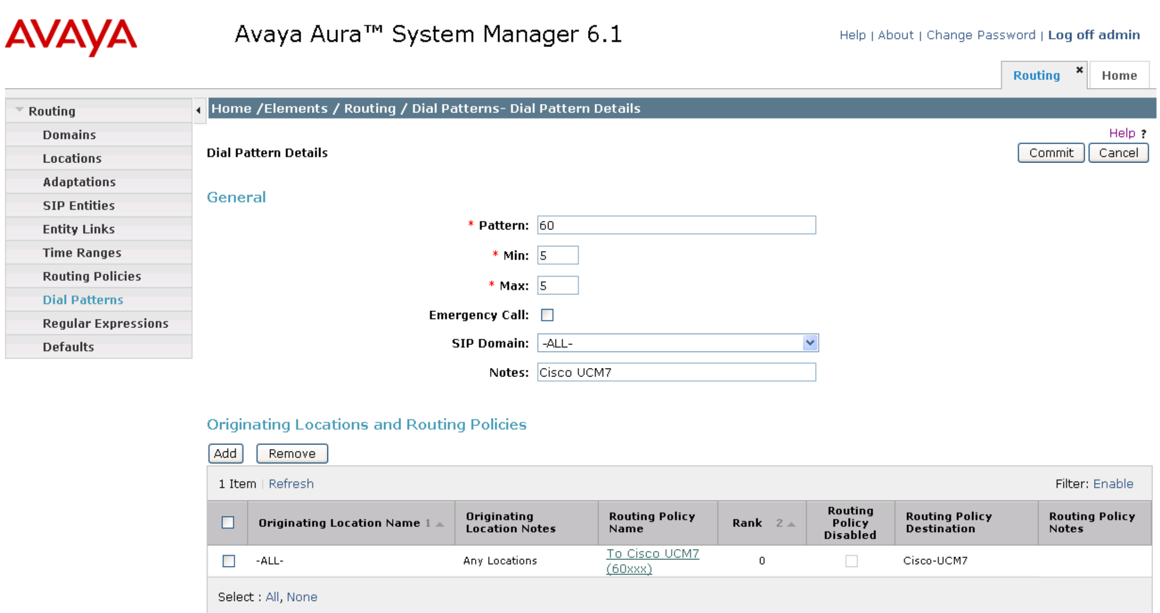
Under **General:**

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

Under **Originating Locations and Routing Policies**:
Click **Add**, and then select the appropriate location and routing policy from the list.

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


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 / Dial Patterns- Dial Pattern Details
Help ?
Dial Pattern Details
Commit
Cancel
General
* Pattern: 3
* Min: 5
* Max: 5
Emergency Call:
SIP Domain: -ALL-
Notes: Extension range for CM-ES R6.0.1
Originating Locations and Routing Policies
Add
Remove
1 Item | Refresh
Filter: Enable
Originating Location Name
Originating Location Notes
Routing Policy Name
Rank
Routing Policy Disabled
Routing Policy Destination
Routing Policy Notes
-ALL-
Any Locations
To CM-ES R6.0.1
0
CM-ES R6.0.1
Select : All, None


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 / Dial Patterns- Dial Pattern Details
Help ?
Dial Pattern Details
Commit
Cancel
General
* Pattern: 60
* Min: 5
* Max: 5
Emergency Call:
SIP Domain: -ALL-
Notes: Cisco UCM7
Originating Locations and Routing Policies
Add
Remove
1 Item | Refresh
Filter: Enable
Originating Location Name
Originating Location Notes
Routing Policy Name
Rank
Routing Policy Disabled
Routing Policy Destination
Routing Policy Notes
-ALL-
Any Locations
To Cisco UCM7 (60xxx)
0
Cisco-UCM7
Select : All, None

4.9. Configure Session Manager

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

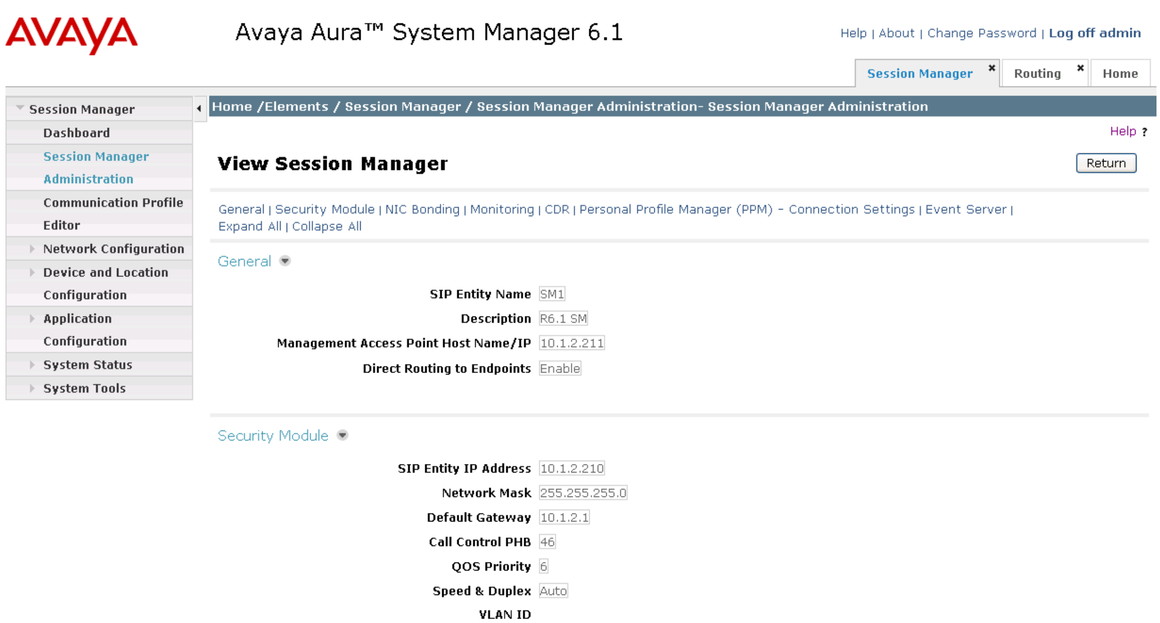
Under **General:**

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.

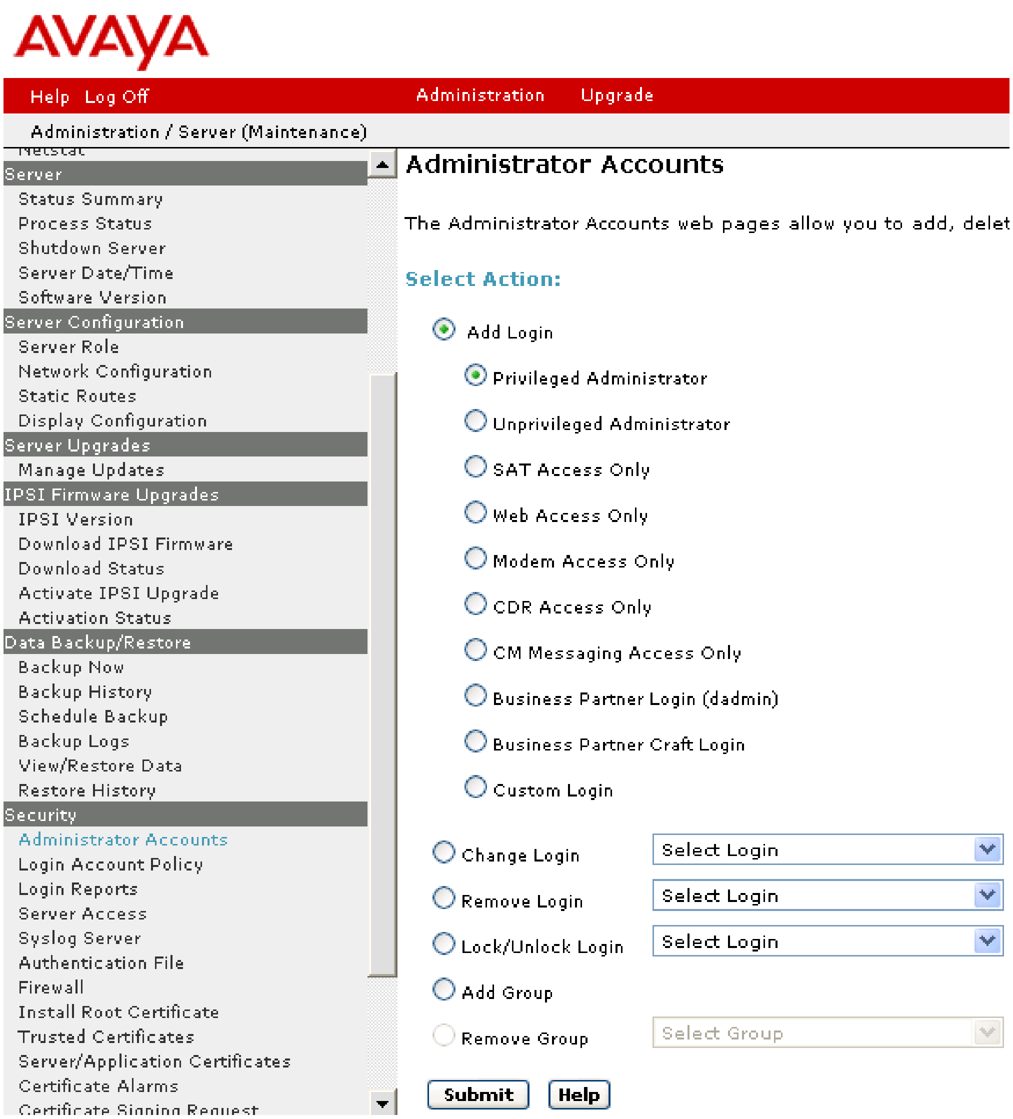


4.10. Add Avaya Aura™ Communication Manager as an Evolution Server

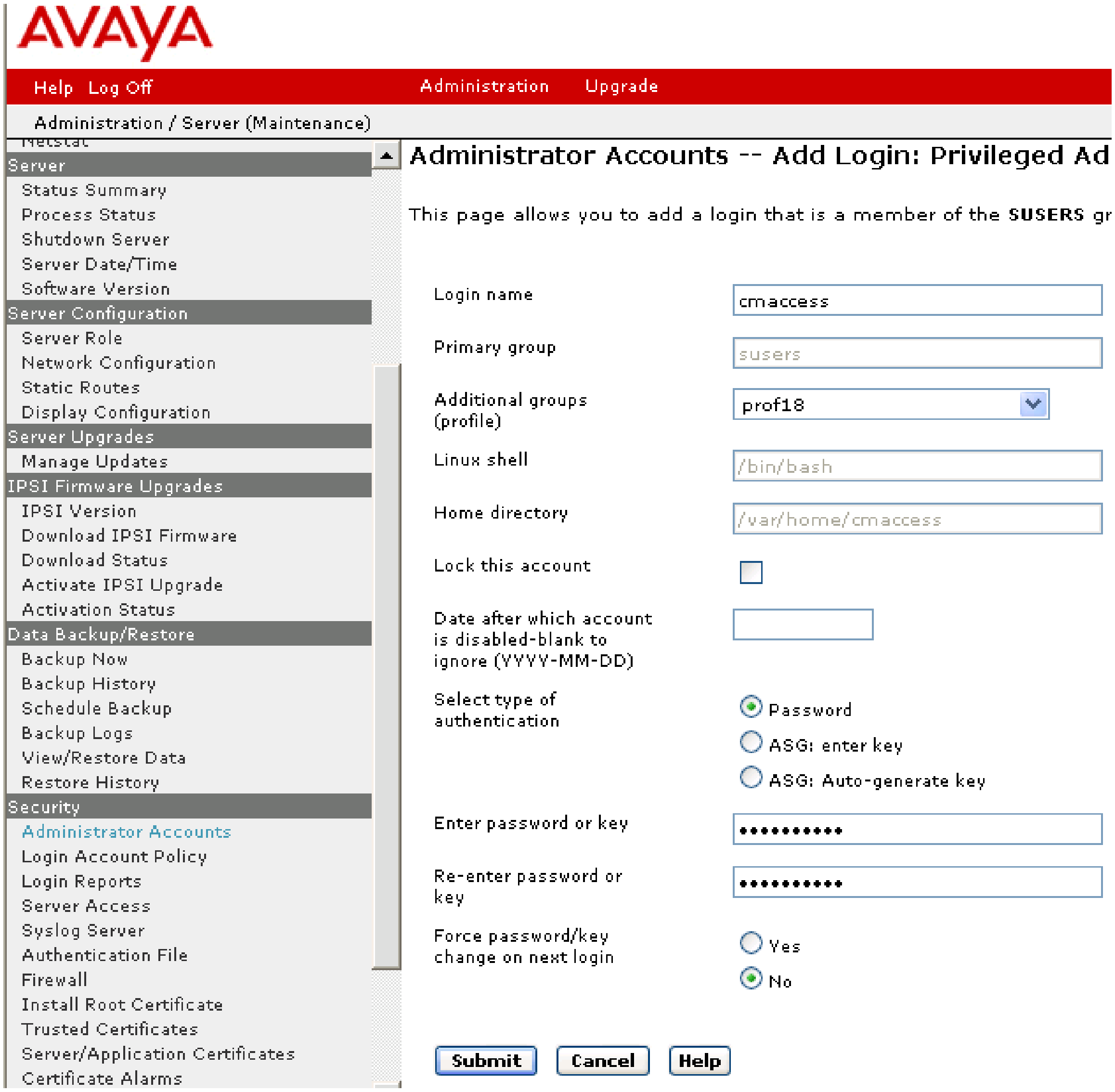
In order for Communication Manager to provide configuration and Evolution Server support to telephones, Communication Manager must be added as an application in Session Manager. This comprises a two step procedure. First, an access login must be configured on Communication Manager for the purpose of 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**.

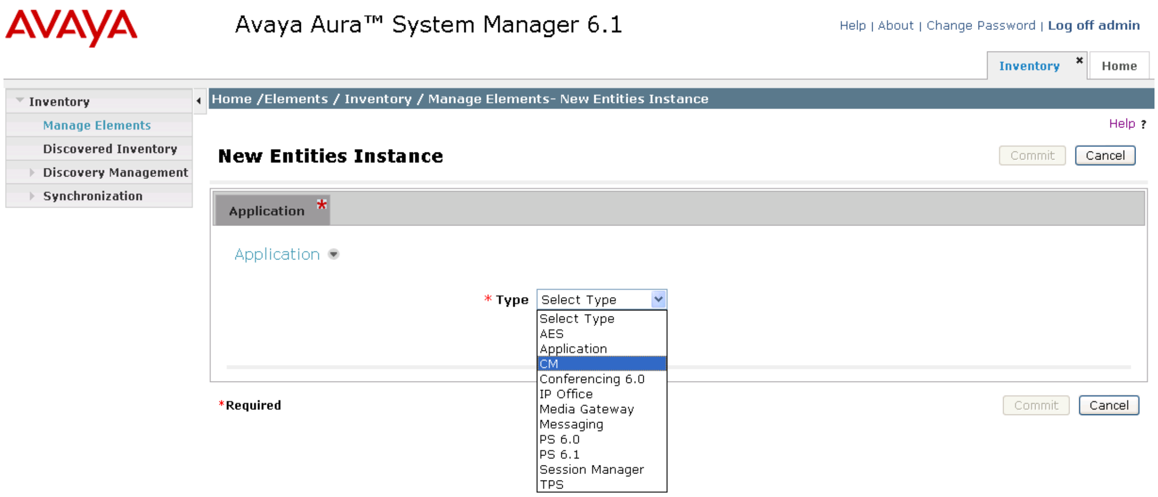


On the next screen, enter a **Login name** and a password in the **Enter password or key** and **Re-enter password or key** fields, and click **Submit**.



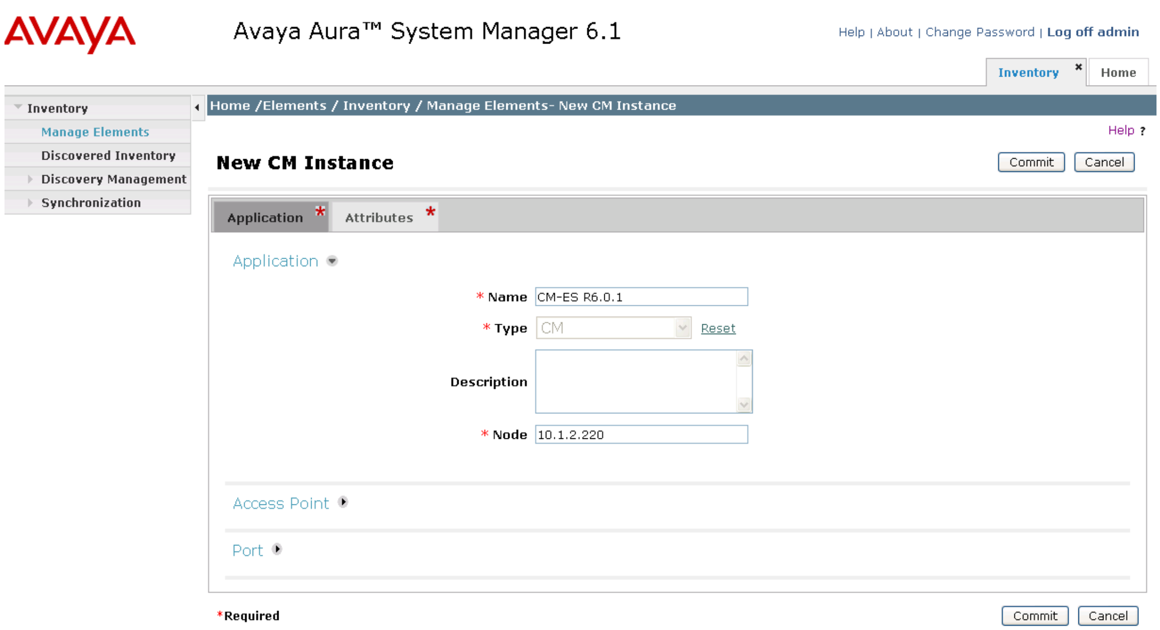
4.10.2. Create an Application Element on System Manager

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**.



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

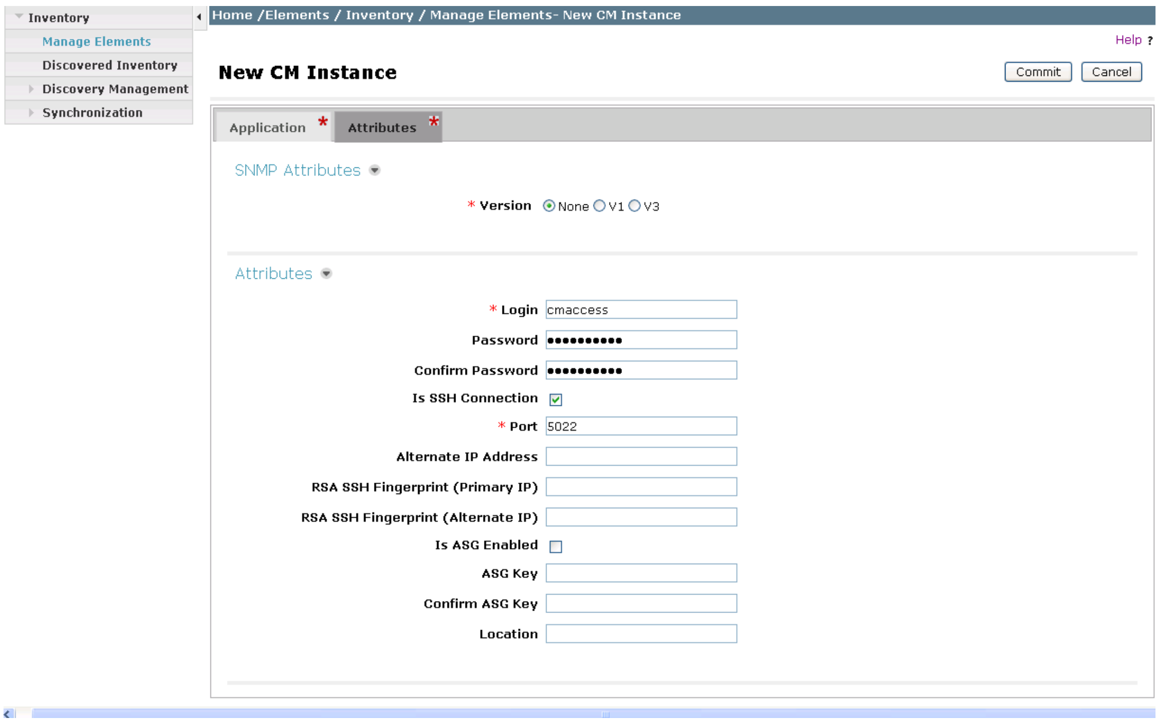
Name	A descriptive name
Node	Enter the IP address for Communication Manager SAT access



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

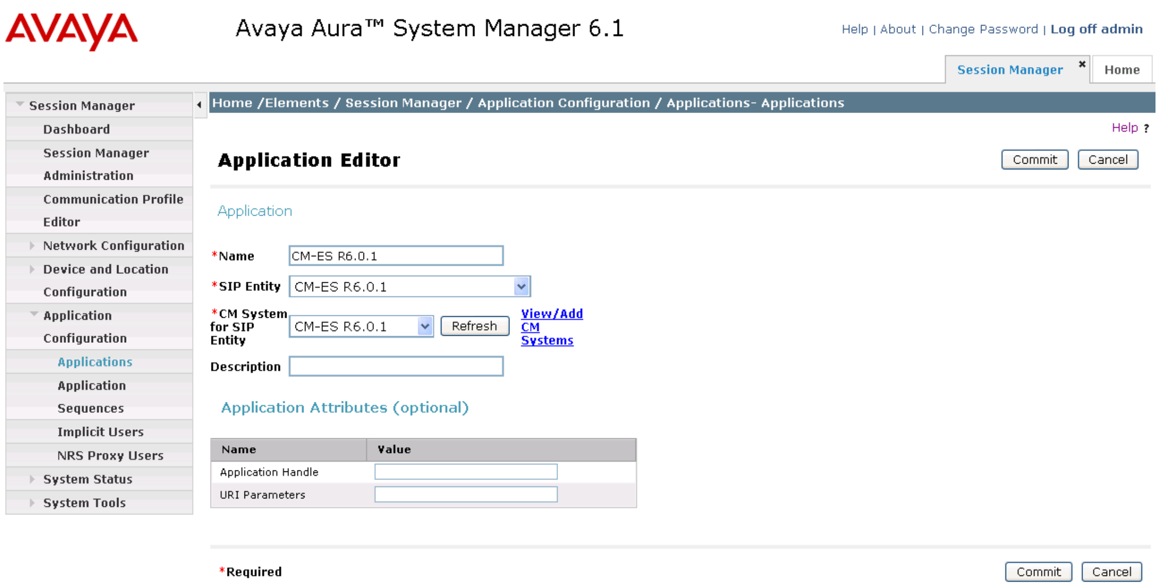
Click on **Commit** to save.



4.10.3. Create an Application

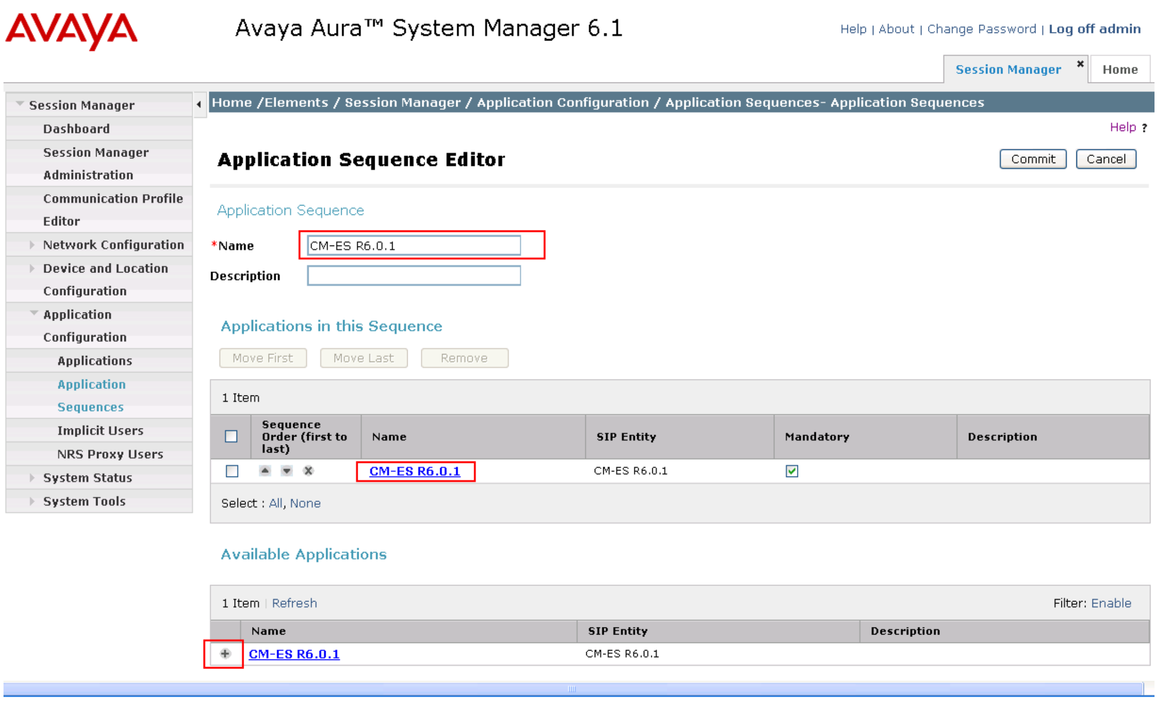
Select **Session Manager → Application Configuration → Applications** under the **Elements** section of the **Home** menu. Click on **New** (not shown). Enter following fields and use defaults for the remaining fields and click on **Commit** to save.

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



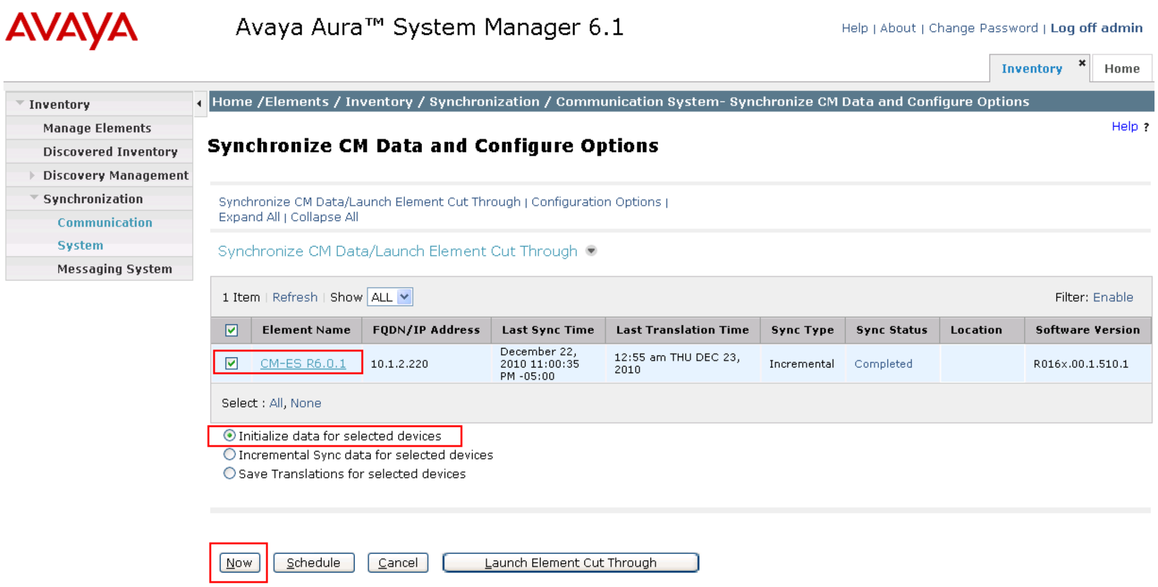
4.10.4. Create an Application Sequence

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.

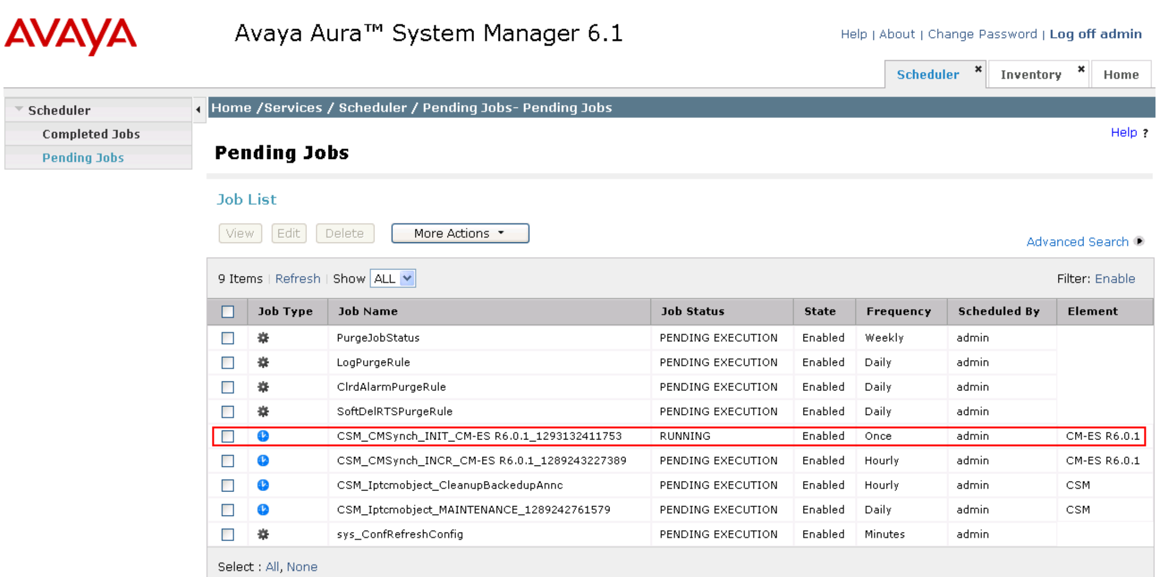


4.10.5. Synchronize Avaya Aura^{TM} Communication Manager Data

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.



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

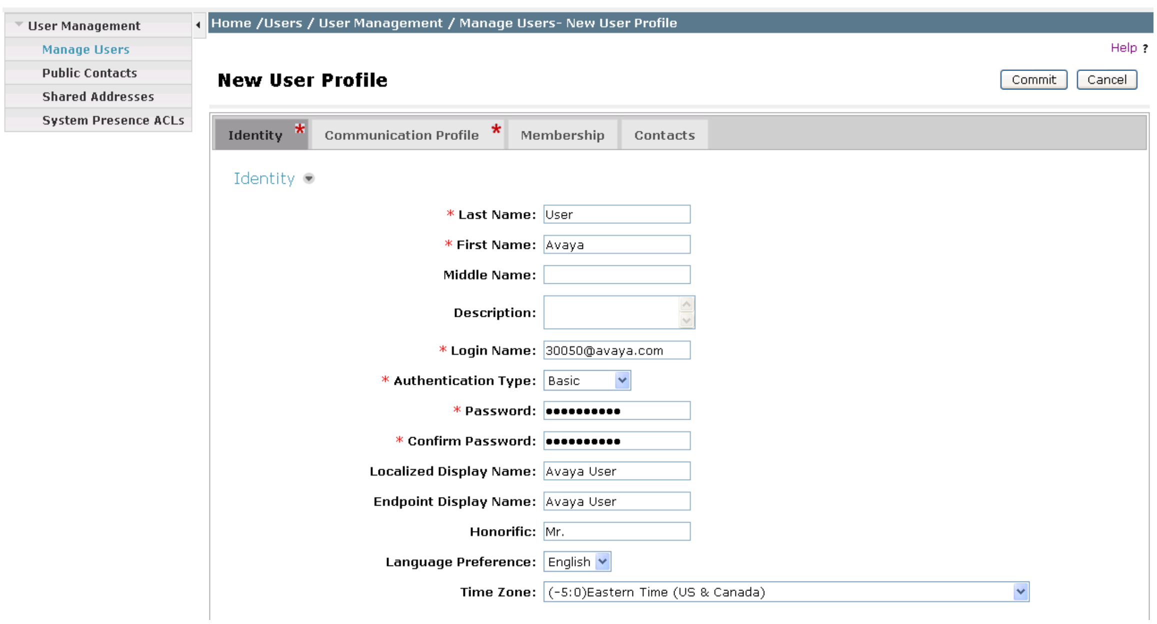


4.11. Add Users for SIP Telephones

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



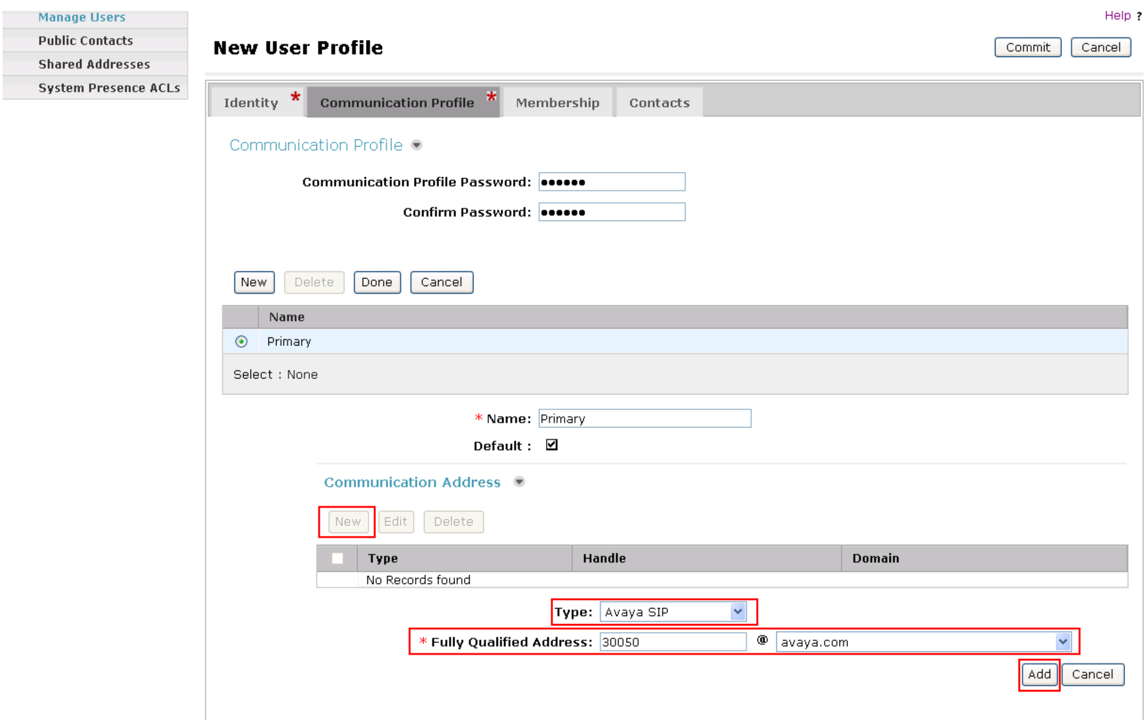
Select the **Communication Profile** tab.
Under **Communication Profile** enter:

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:

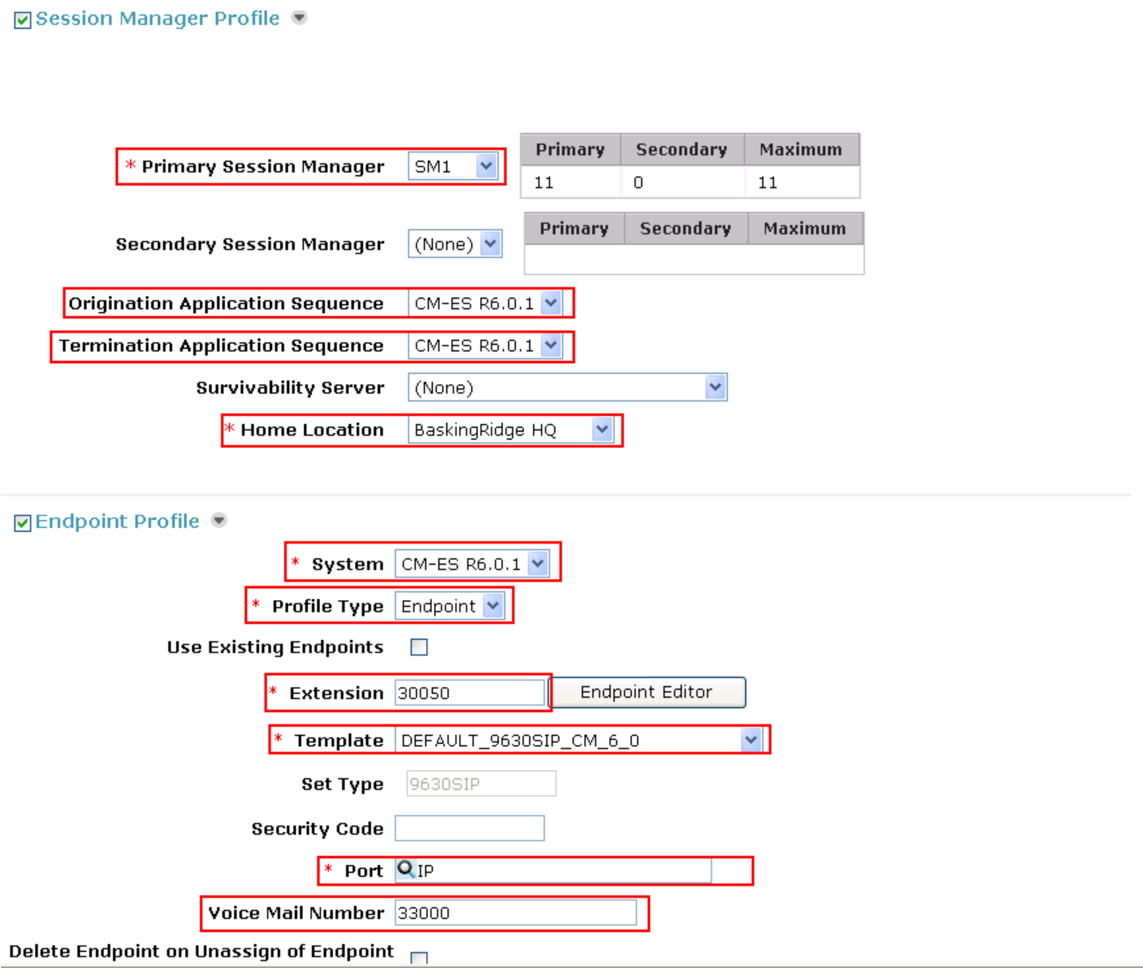
Type	Select **Avaya SIP**
Fully Qualified Address	Enter the extension number
@	Select the domain defined in **Section 4.2**

Click on **Add**.



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).[4]

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



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

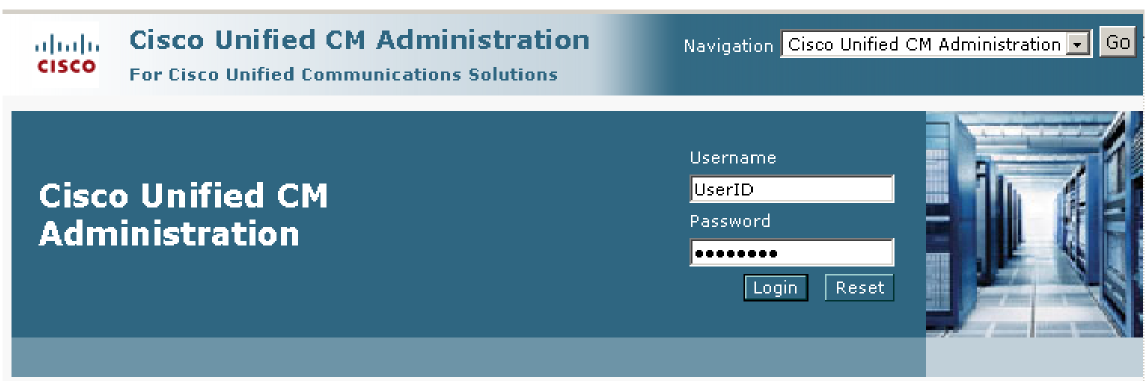
5. Configure Cisco UCM

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

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

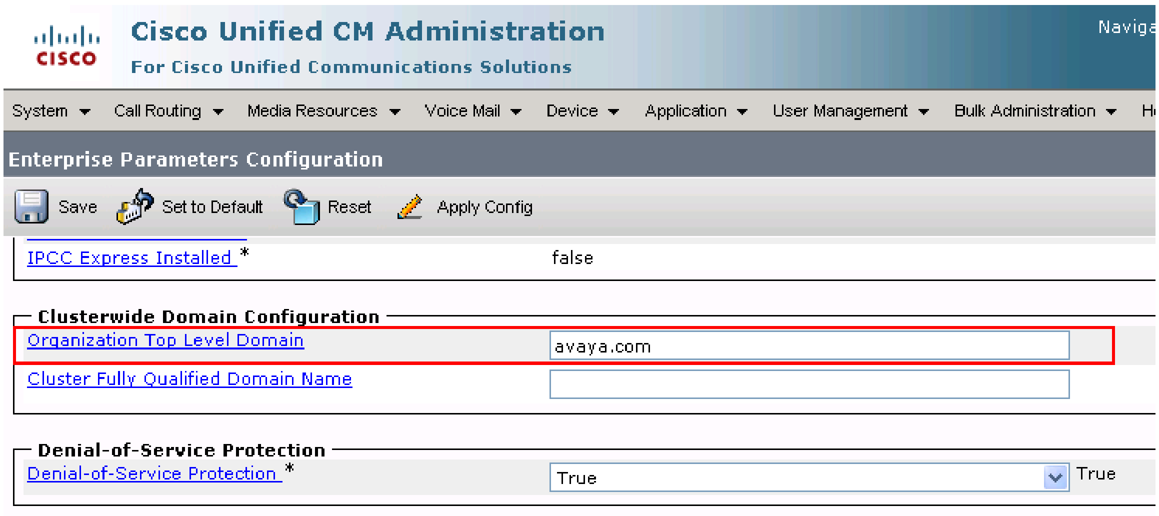
5.1. Log in to Cisco UCM

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



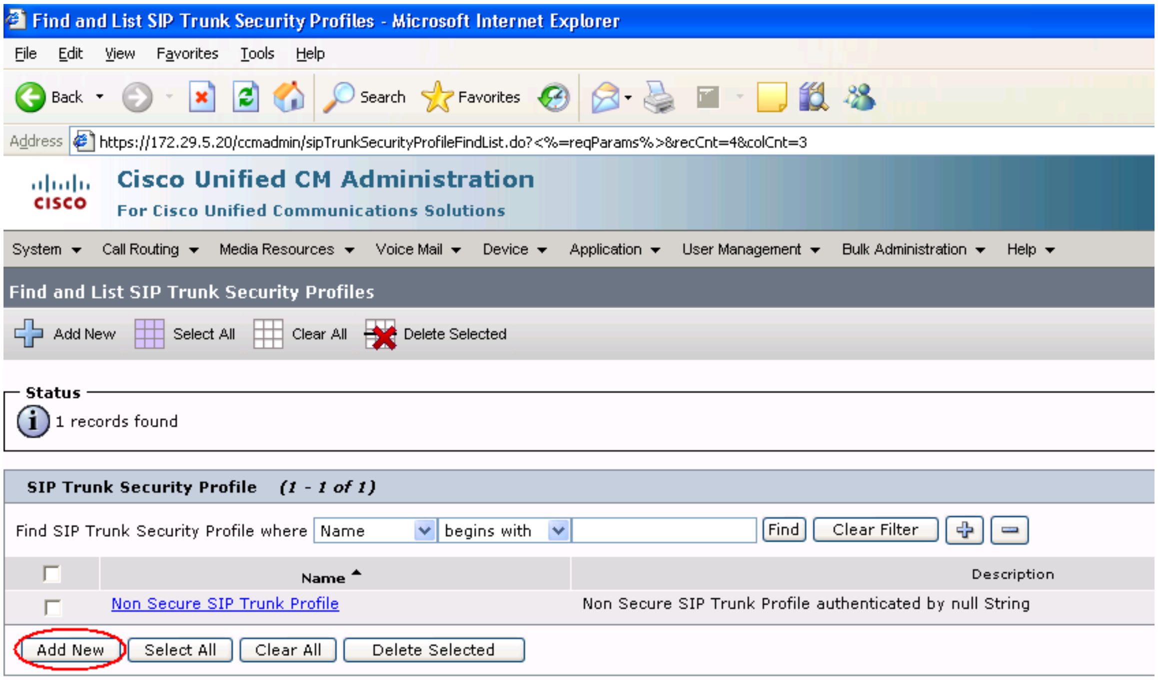
5.2. Administer SIP Domain

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

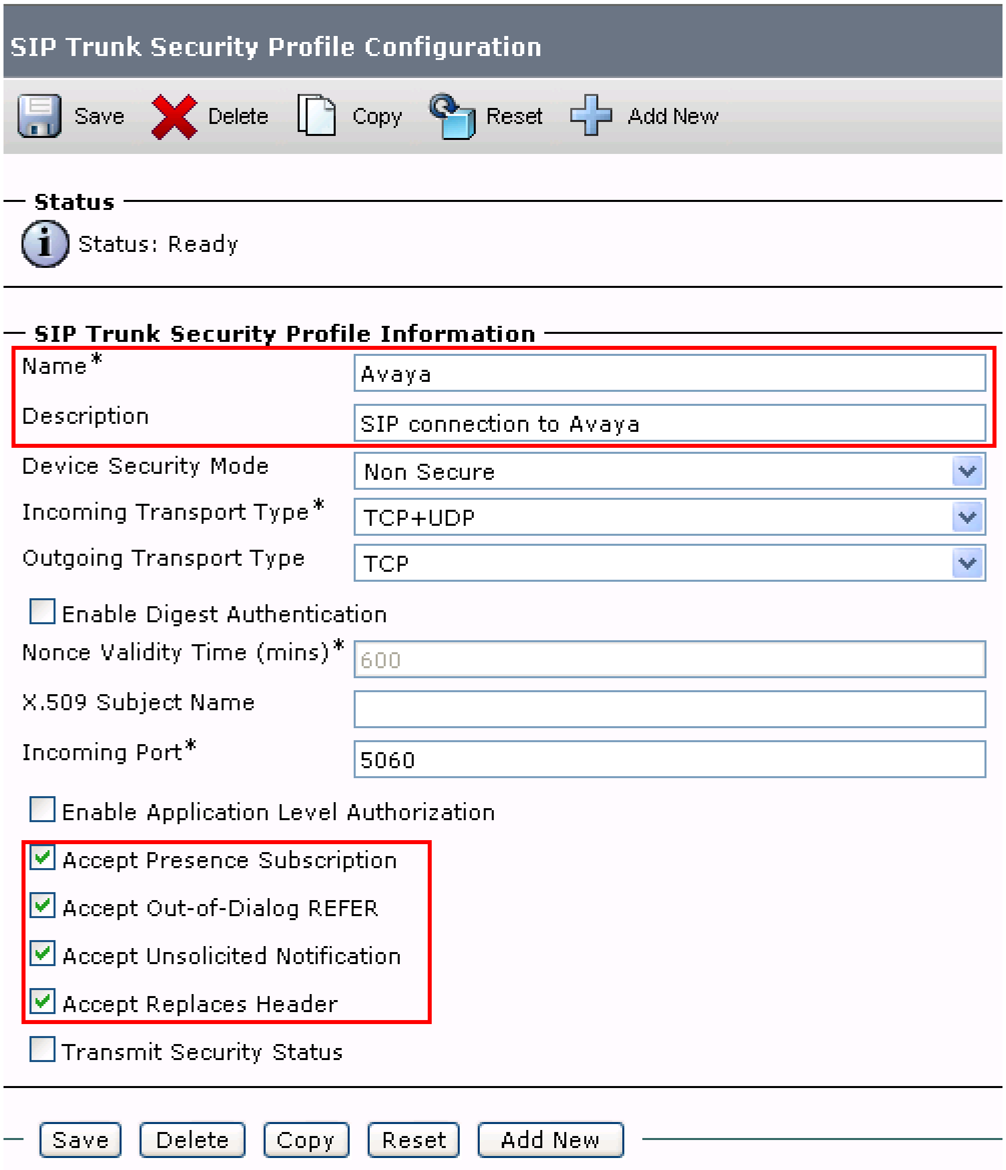


5.3. Administer SIP Trunk Security Profile

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



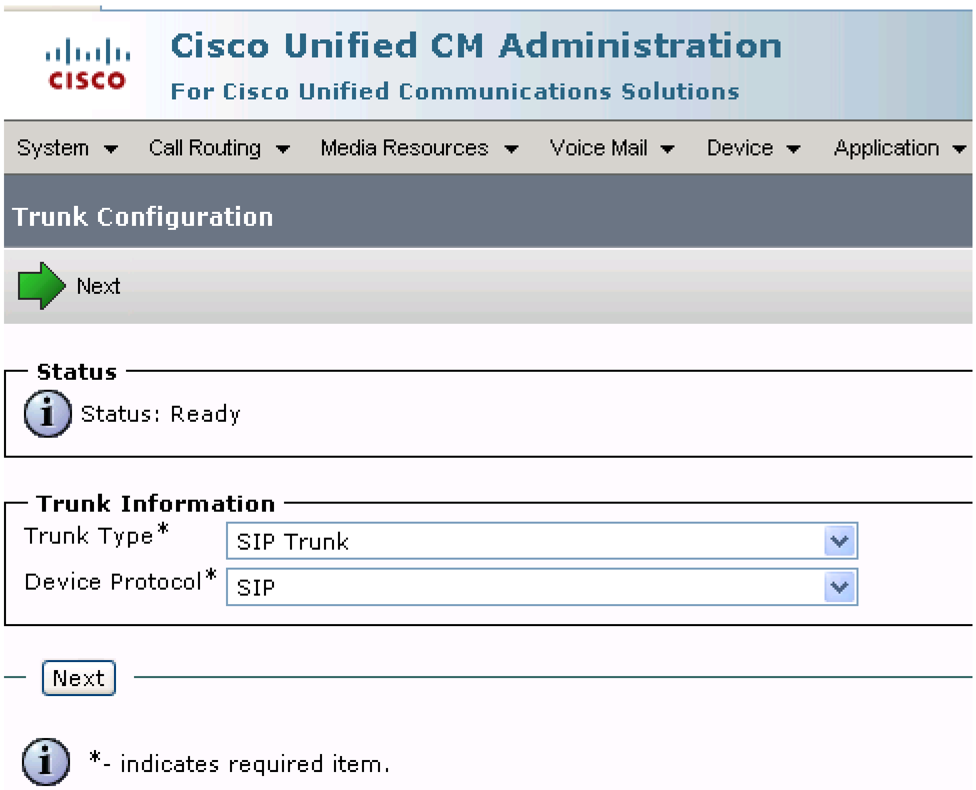
The following is a screen capture of the **SIP Trunk Security Profile Configuration** used in the sample network. Configure the highlighted areas, noting that to allow MWI (Message Waiting Indicator) messages to be accepted by Cisco UCM from Modular Messaging, the SIP Trunk provisioned towards Session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



5.4. Administer SIP Trunk

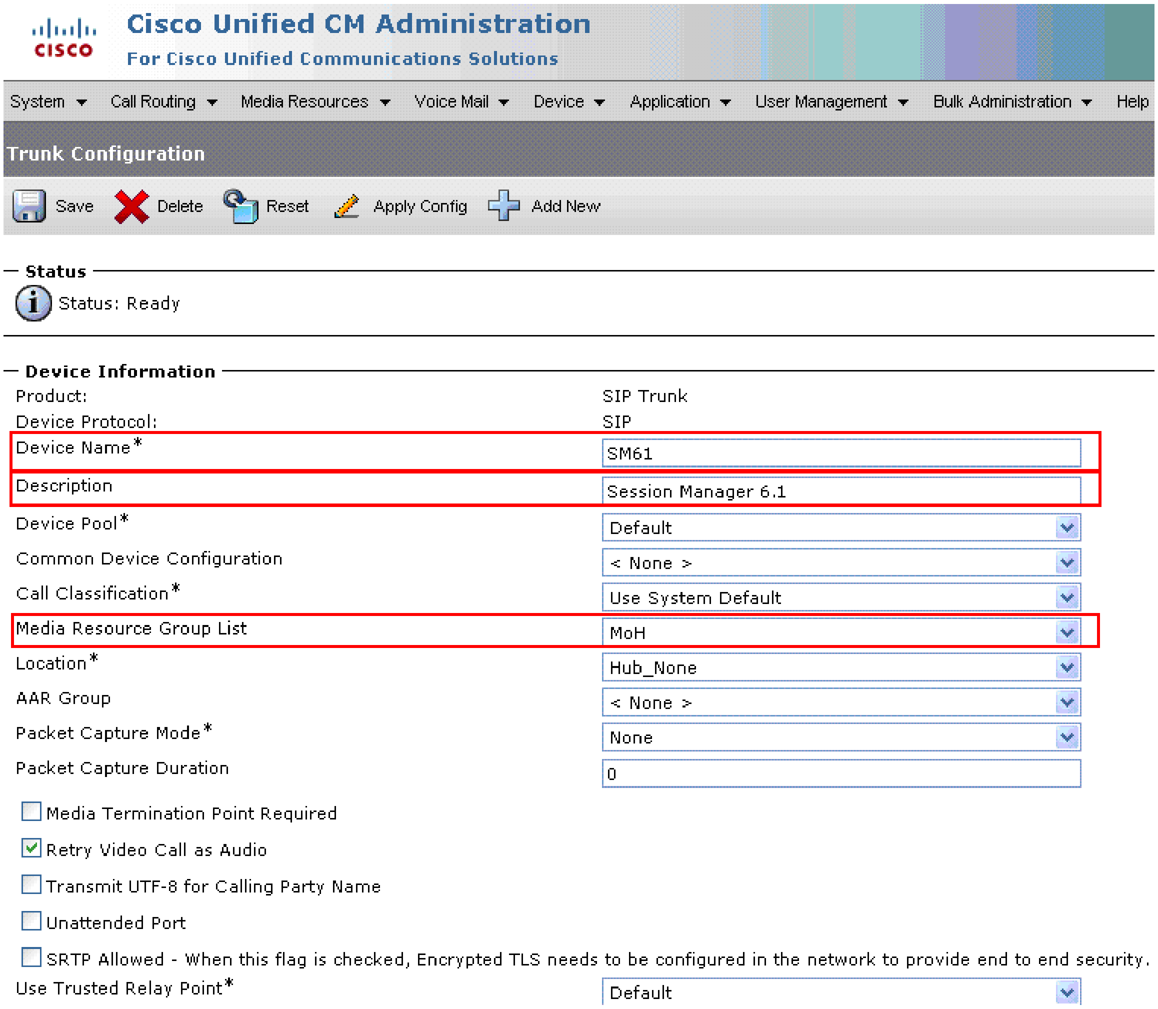
Add a new SIP trunk by selecting **Device → Trunk** from the top menu then click **Add New** to begin adding a new SIP trunk.

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



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

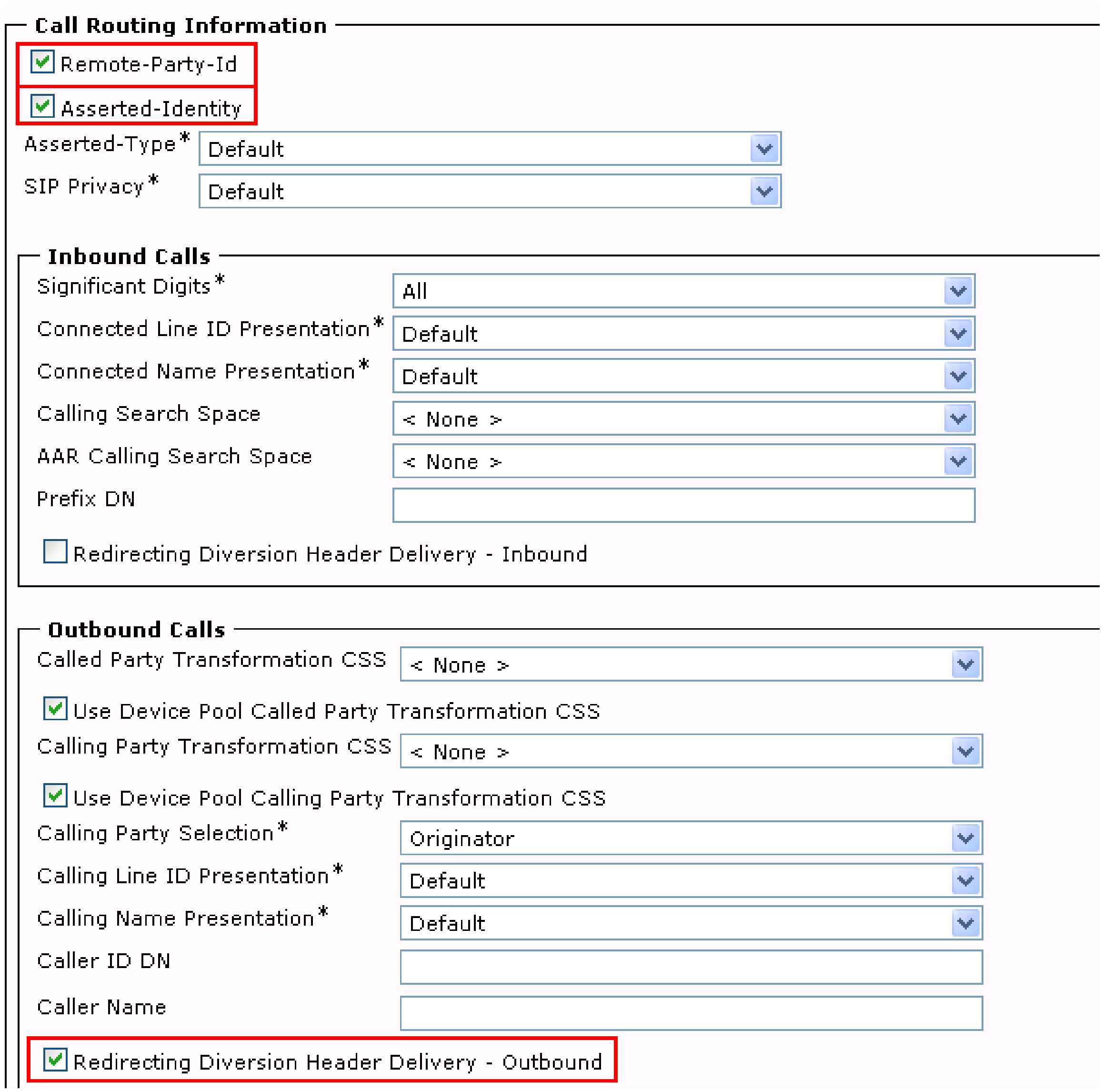
Device Name	An informative name
Description	Any note for this trunk
Media Resource Group List	Select from the list (see **Section 5.7**)



Under **Call Routing Information**:

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

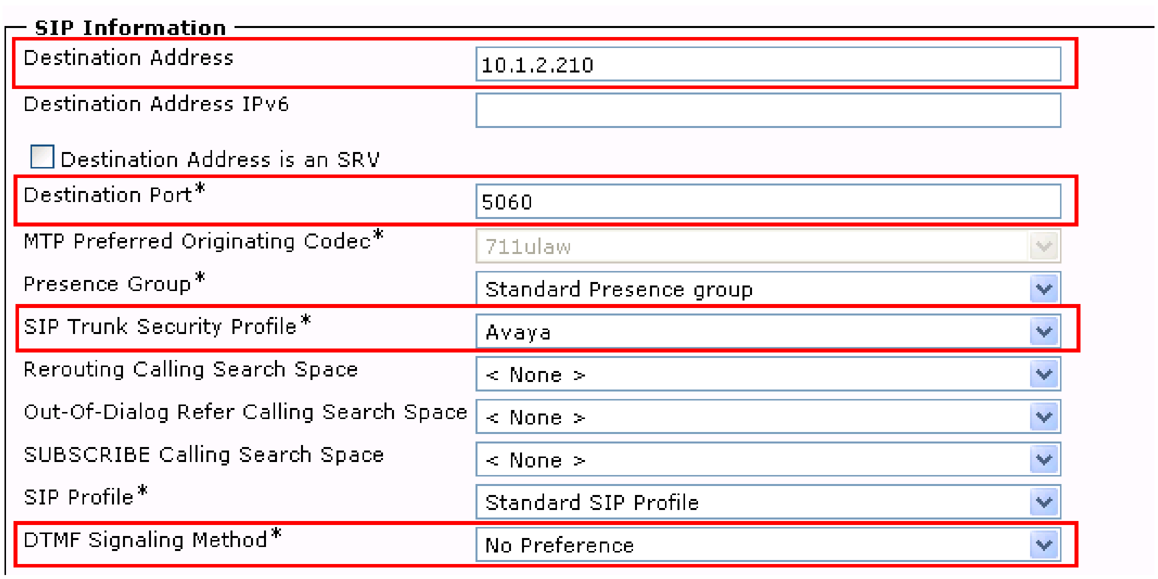
Cisco UCM must be configured to populate the Diversion header with the appropriate reason code when a call is forwarded to voice mail. Ensure that **Redirecting Diversion Header Delivery - Outbound** is selected under **Outbound Calls** section, as shown below.



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

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

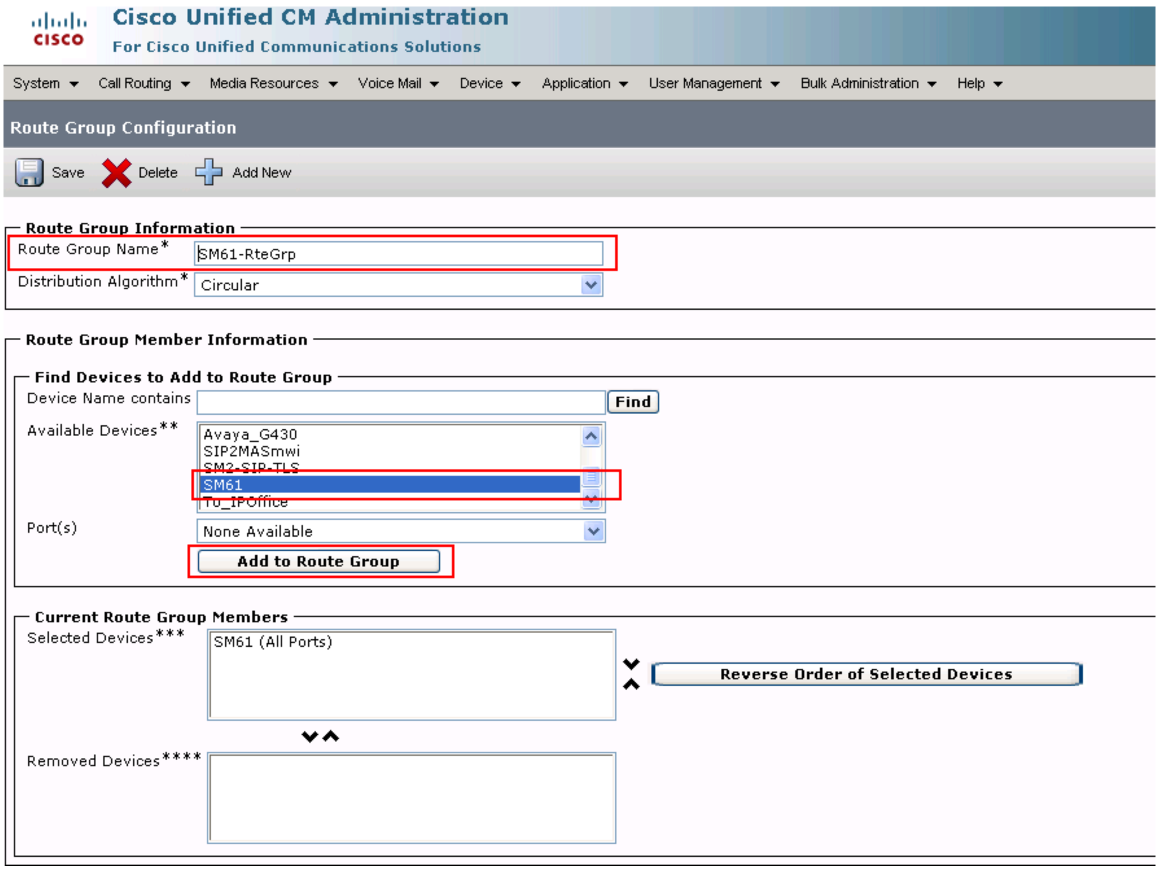
Click **Save** to complete.



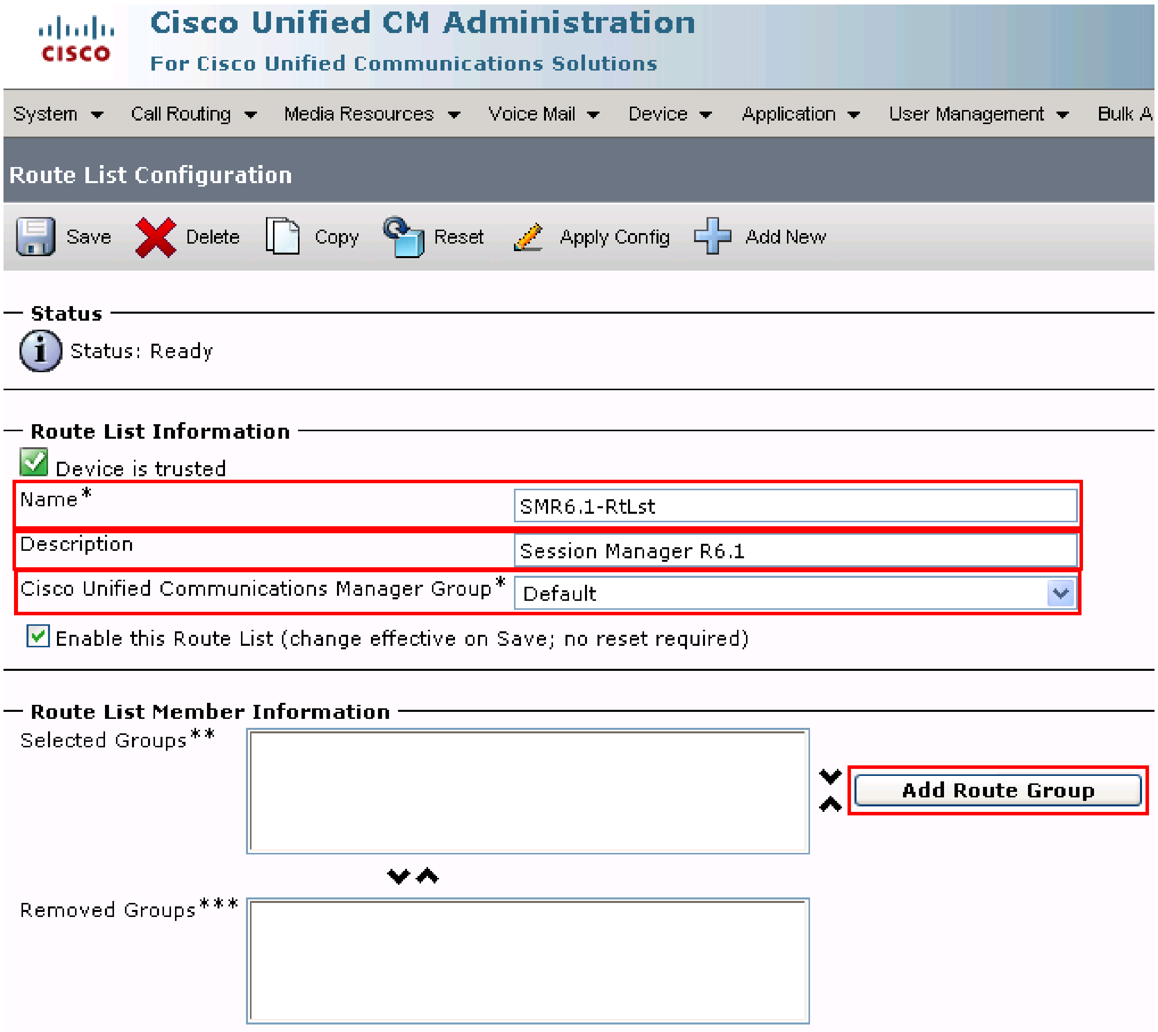
5.5. Administer Route Pattern

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

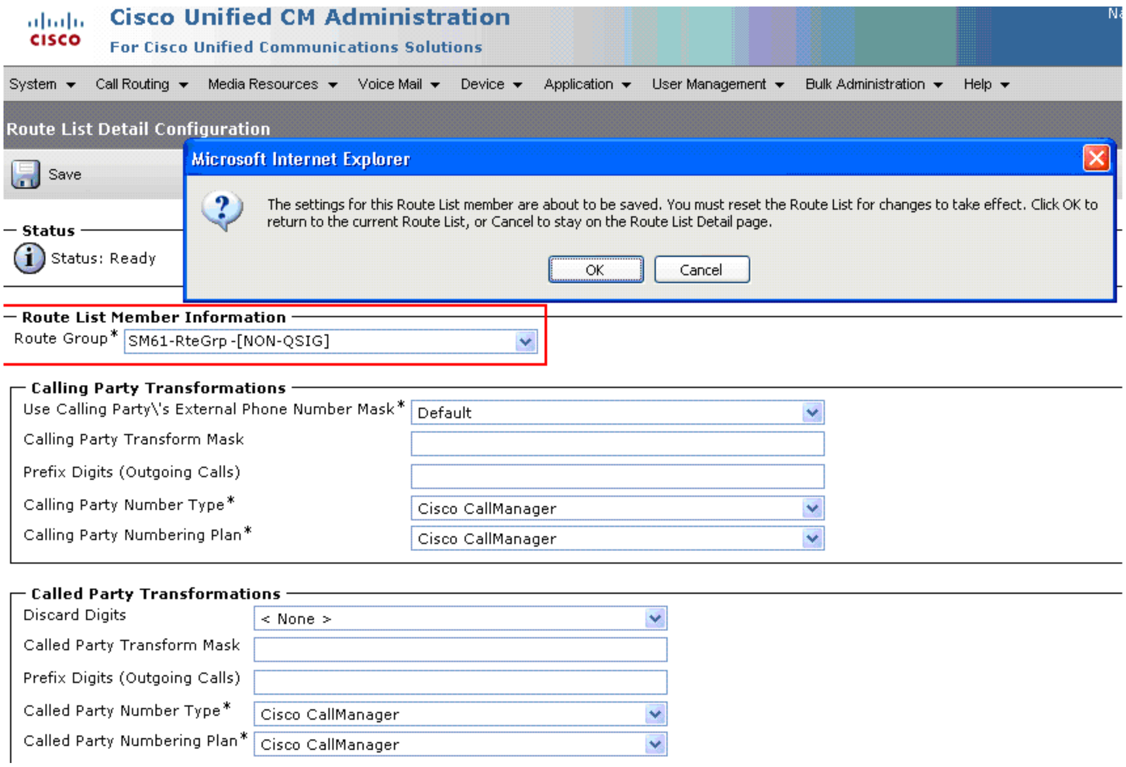
Add a Route Group by selecting **Call Routing → Route/Hunt → Route Group** and click **Add New**. Enter a **Route Group Name**, and under **Find Devices to Add to Route Group** select the SIP trunk previously created, and click on **Add to Route Group**. The screen below shows the result of doing this,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



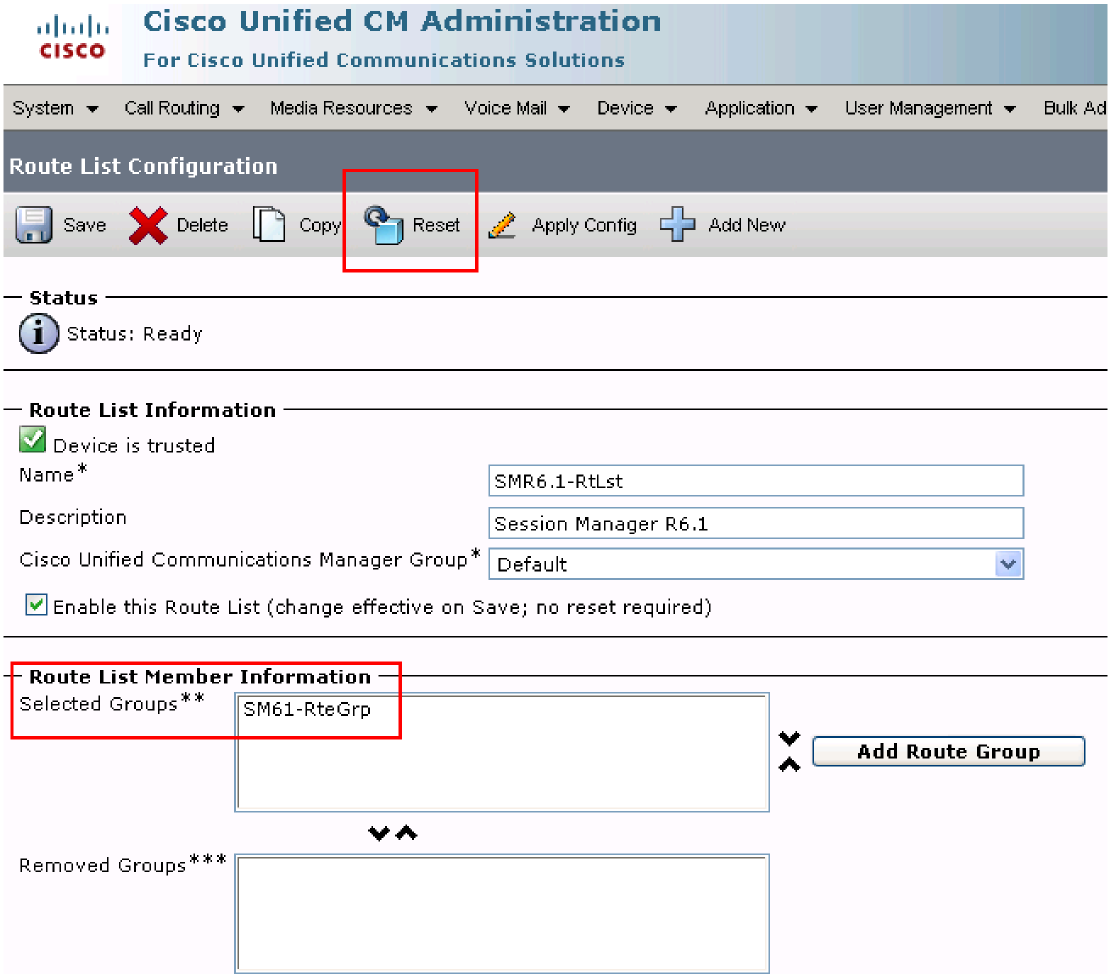
Next, add a Route List by selecting **Call Routing → Route/Hunt → Route List**, then click **Add New**. Enter a **Name**, an optional **Description**, select **Default** for **Cisco Unified Communications Manager Group**, and click on **Add Route Group**.



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

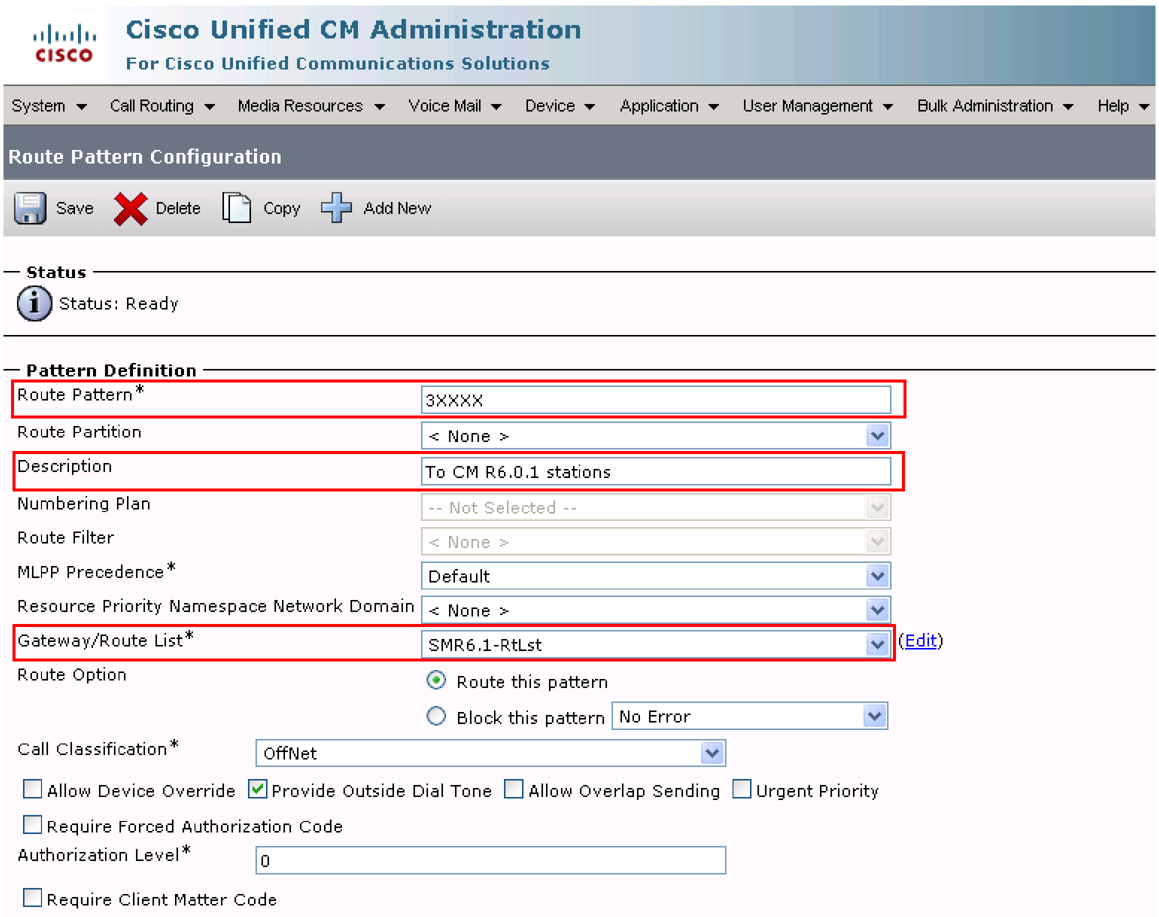


The screen returns to the Route List definition, with the selected Route List Group shown in the **Selected Groups** window under **Route List Member Information**. Click **Reset**.



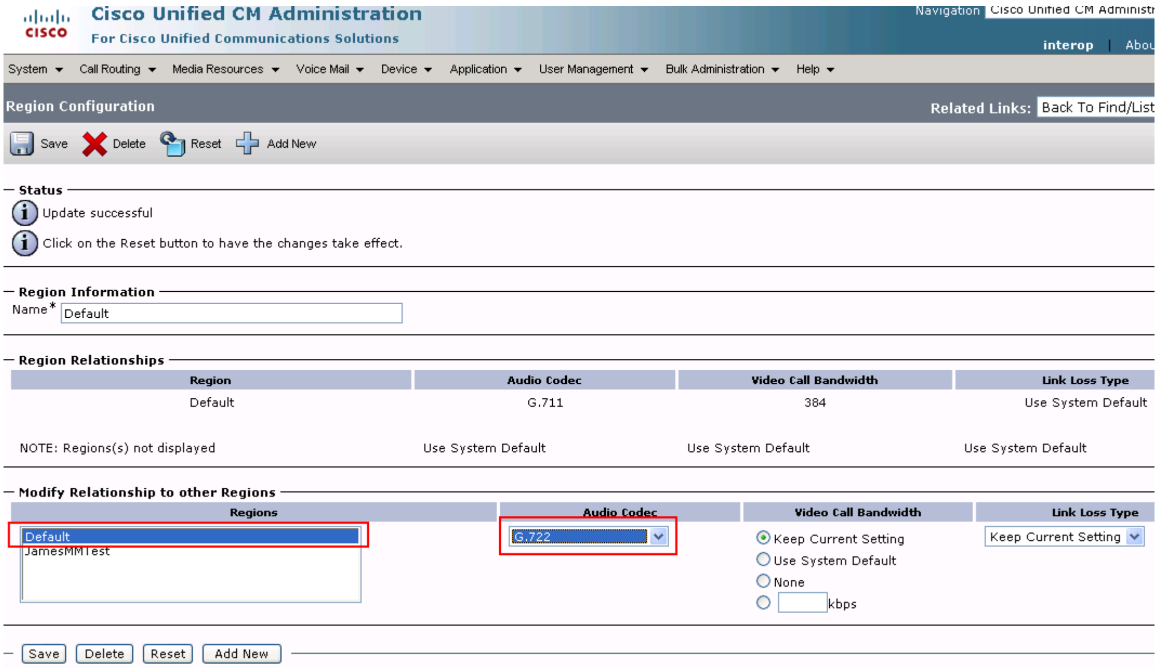
Select **Call Routing → Route/Hunt → Route Pattern** then click **Add New** to add a new route pattern for extension range 3xxxx which includes the Modular Messaging access number 33000, as well as calls to telephones registered to Avaya Session Manager and Communication Manager. Calls to Cisco UCM telephones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

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



5.6. Configure Audio Codecs

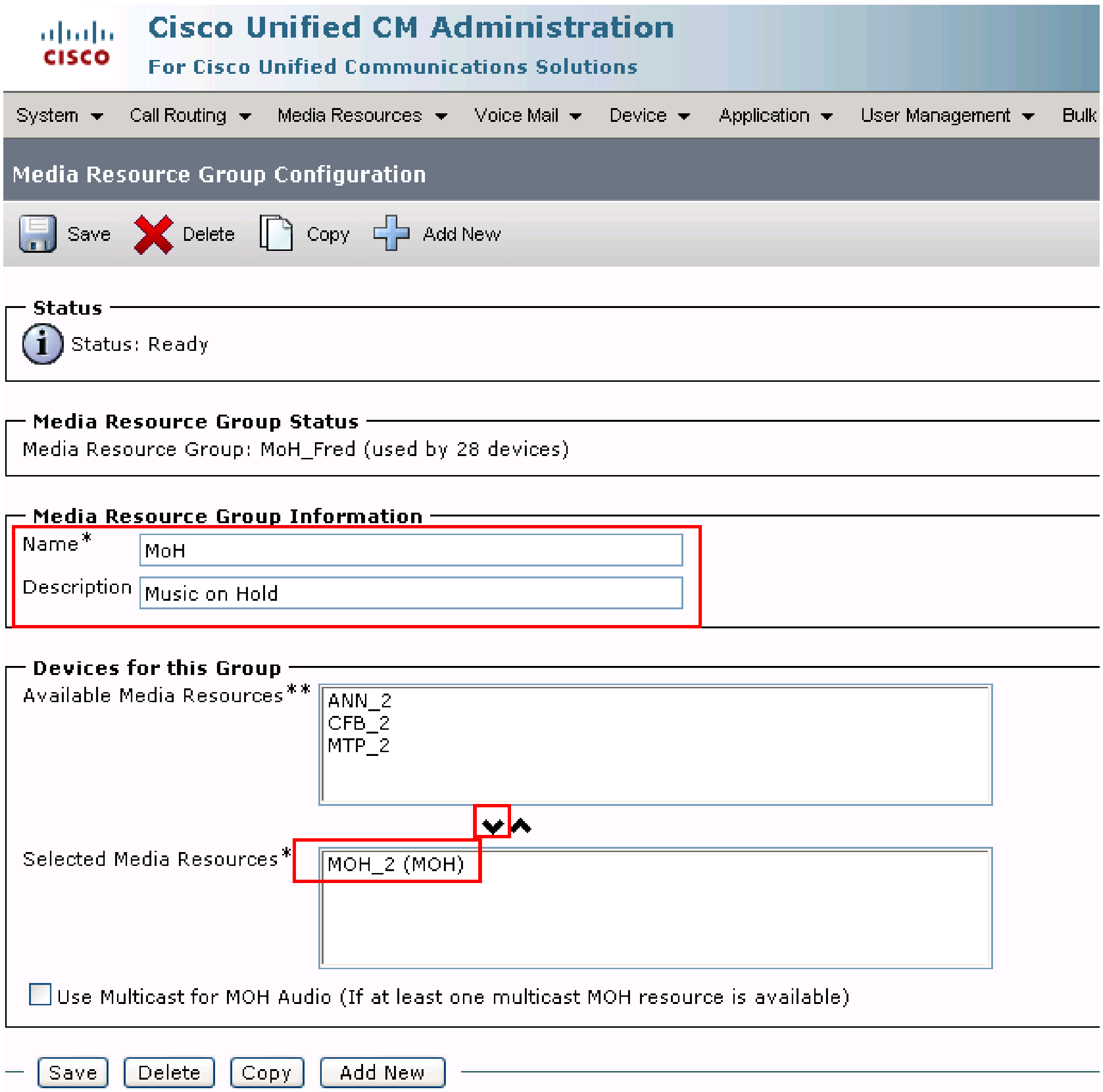
Select **System → Region** from the top menu and select the **default** profile. Under **Modify Relationship to other Regions**, select **Default** under **Regions** and **G.722** under **Audio Codec**. This will select the G.722 codec as first choice. If the endpoints involved in a particular call do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



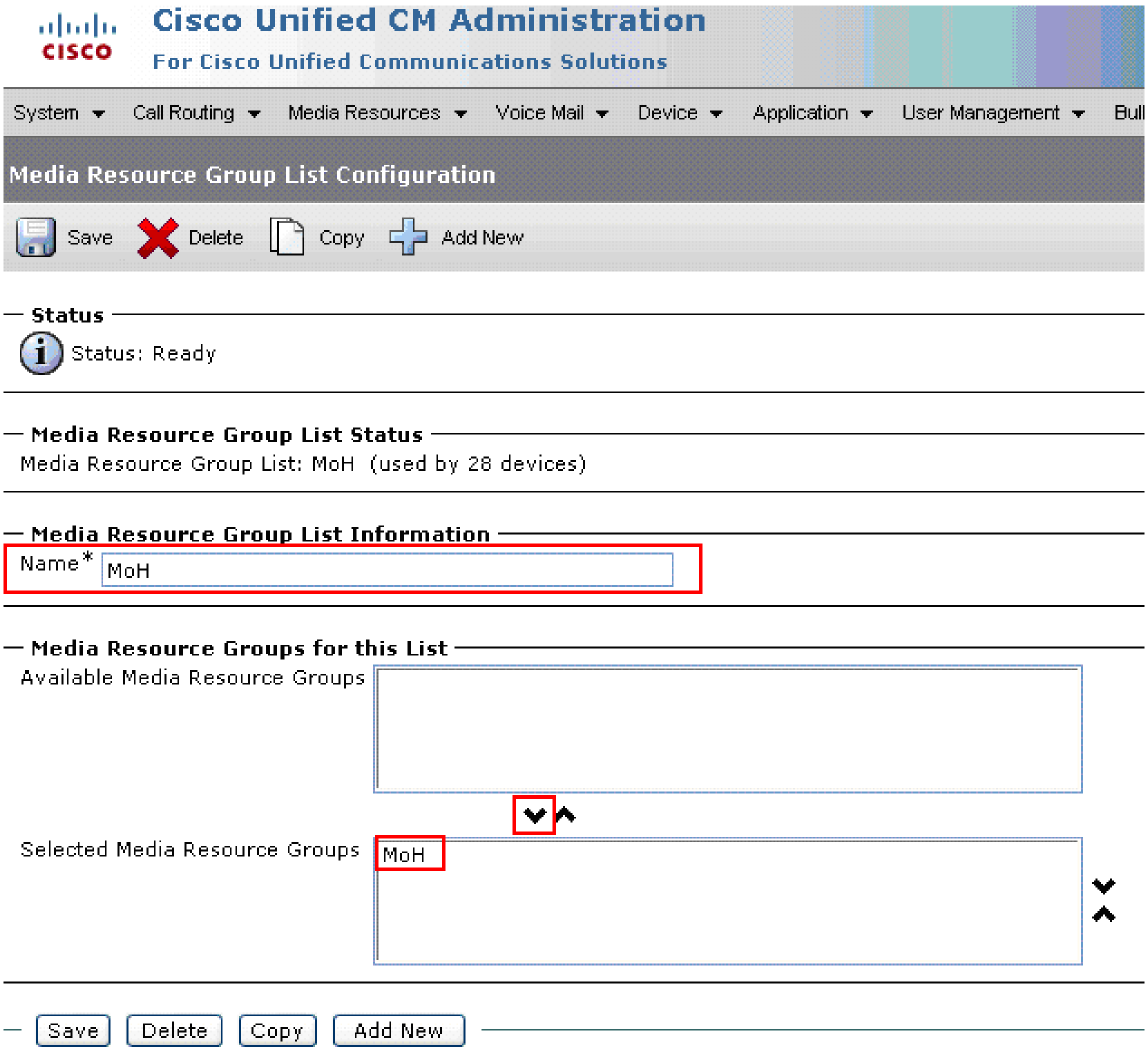
Click **Save** to save configuration.

5.7. Configure Music on Hold

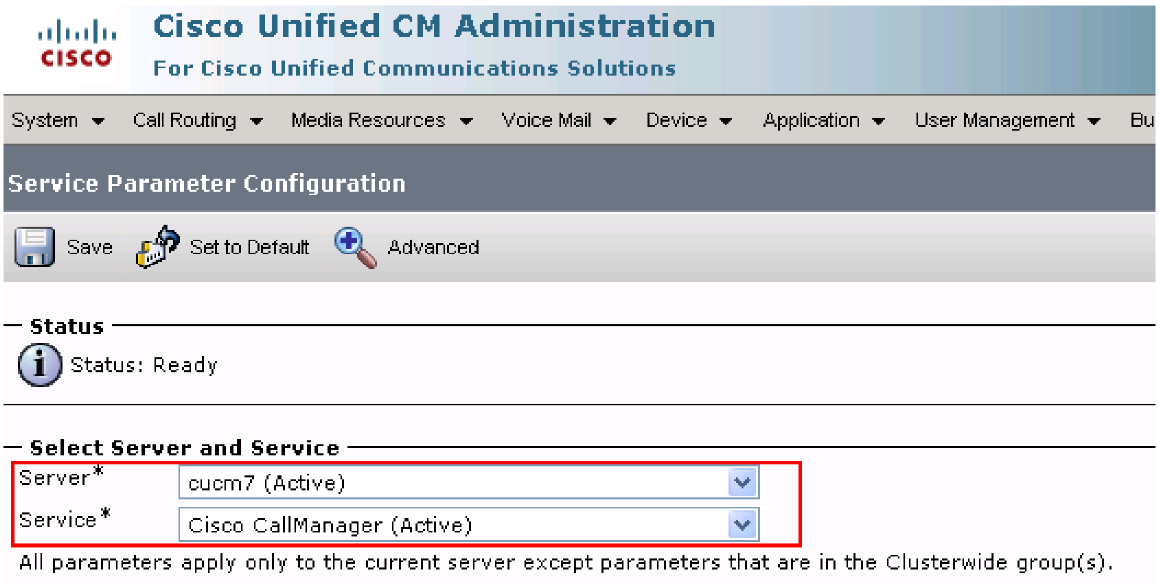
Several steps are required to configure music on hold for calls from Avaya users. Select **Media Resources → Media Resource Group** from the top menu, and click **Add New**. In the screen that follows, under **Media Resource Group Information**, enter a **Name** and optional **Description**. Under **Devices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



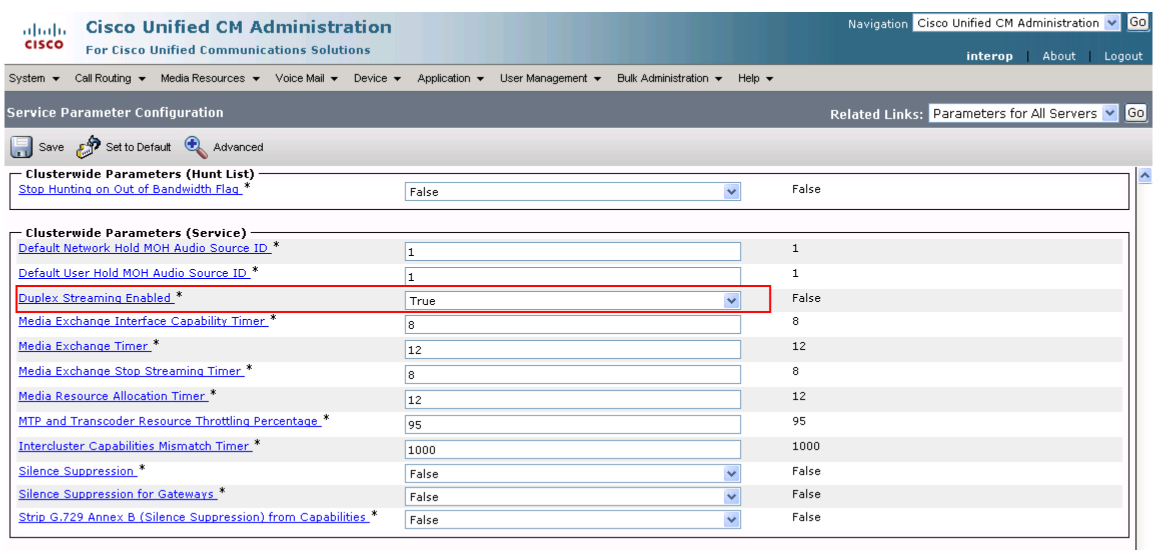
Select **Media Resources → Media Resource Group List** from the top menu, and click **Add New**. In the screen that follows, under **Media Resource Group List Information**, enter a **Name**. Under **Media Resource Groups for this List**, select a media resource group in the **Available Media Resource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



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

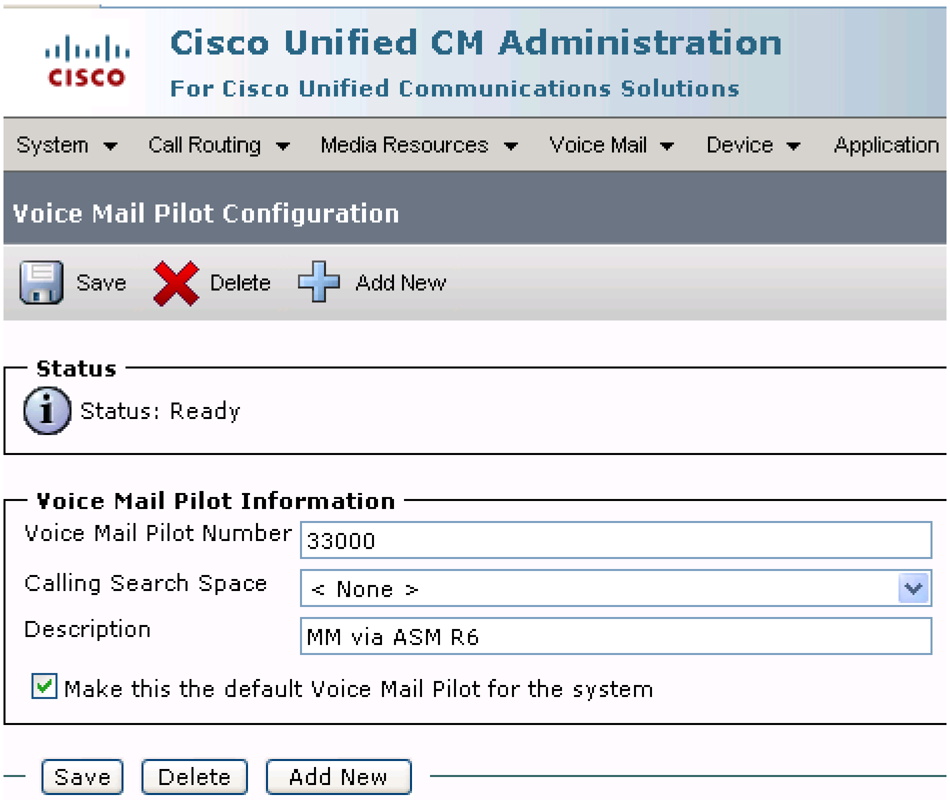


On the following screen, scroll down to **Clusterwide Parameters (Service)**, and Select **True** for **Duplex Streaming Enabled**. Click **Save**.



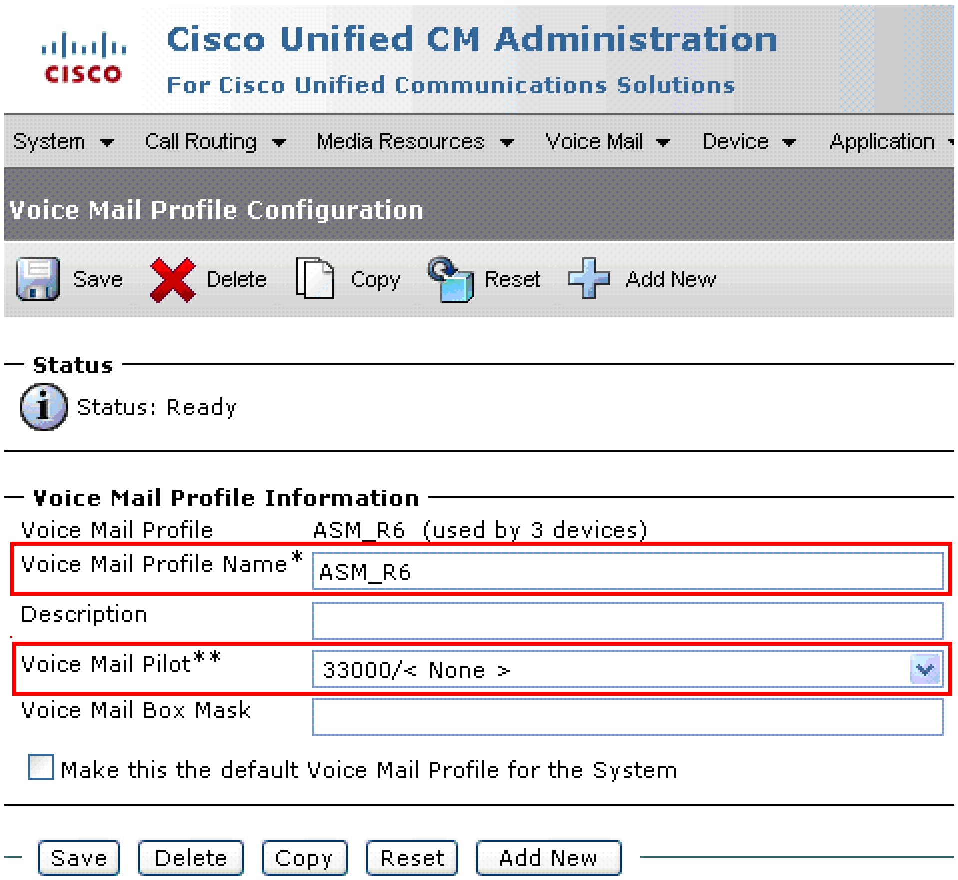
5.8. Configure Voice Mail Pilot

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



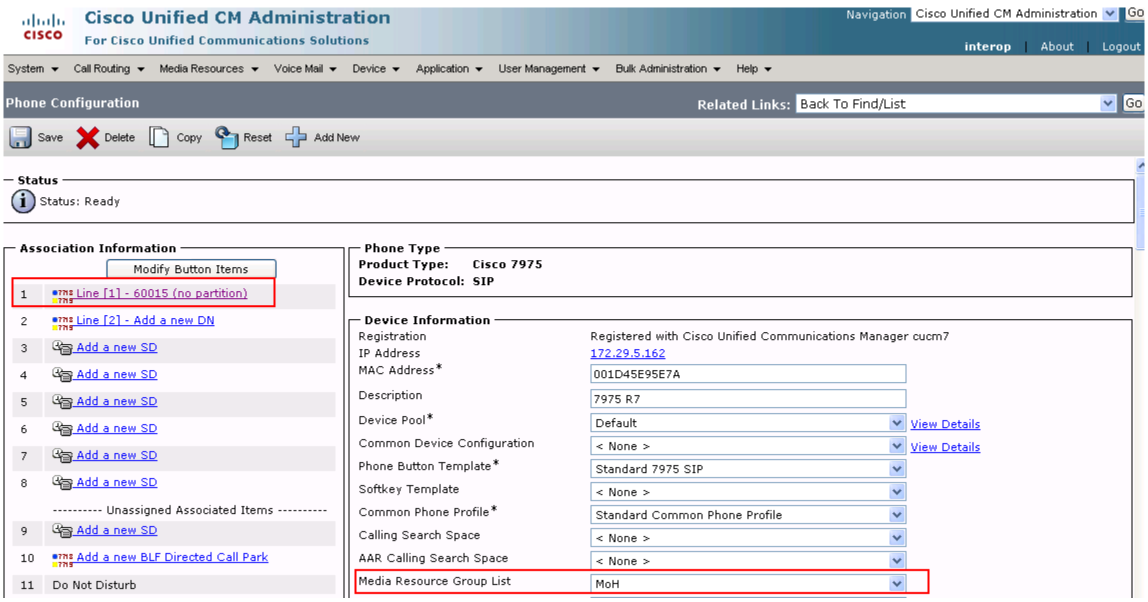
5.9. Configure Voice Mail Profile

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

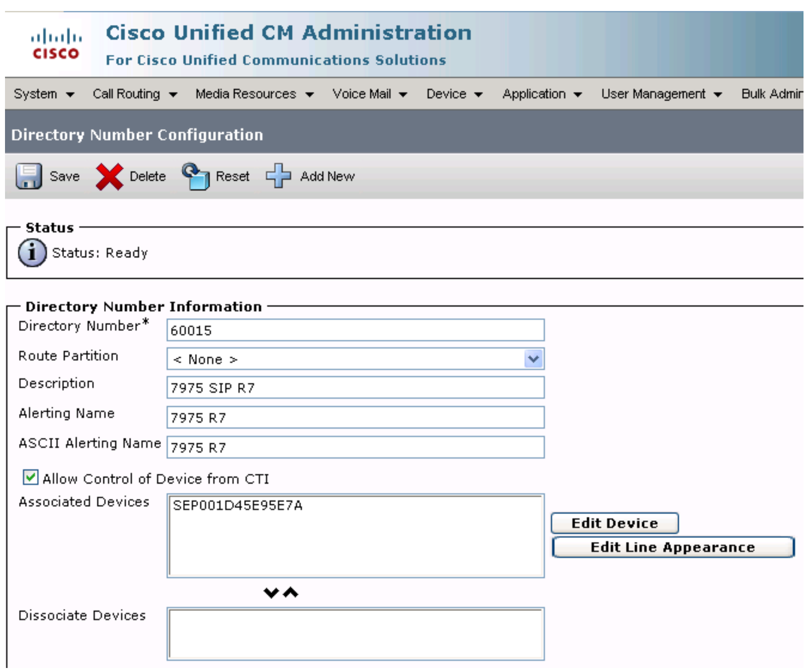


5.10. Configure a Telephone

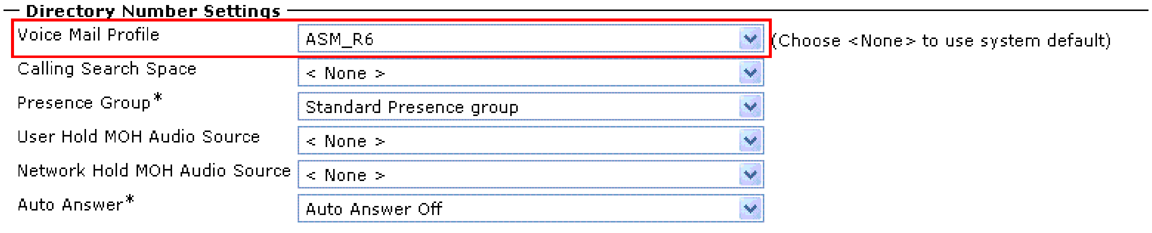
Select **Device → Phone** then click on the telephone to be configured. The following screen shows the display after a telephone has been selected. Under **Device Information**, select the **Media Resource Group List** created in **Section 5.7**. Click on the line for the telephone as highlighted in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



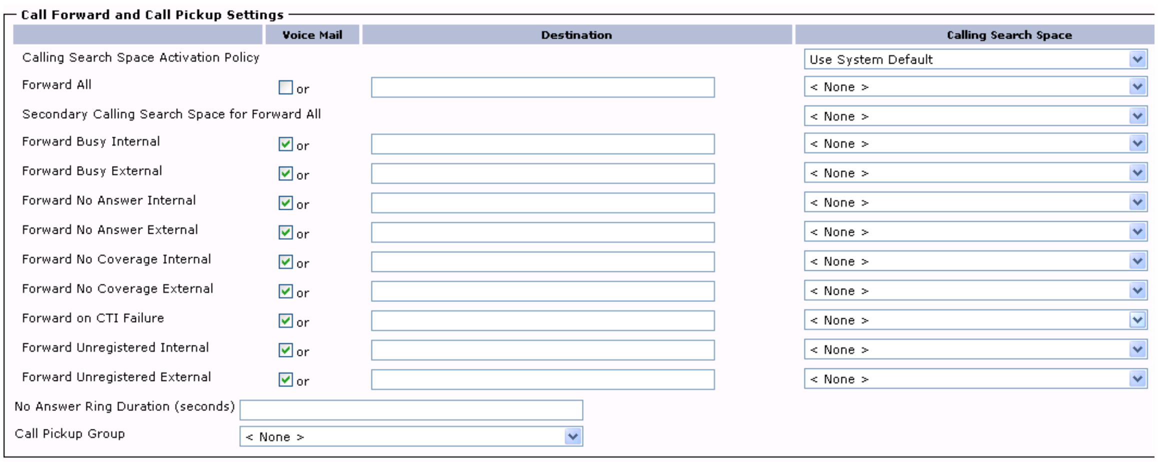
The following screen shows the display after the line has been selected. Enter information for **Directory Number**, **Description**, **Alerting Name** and **ASCII Alerting Name.**



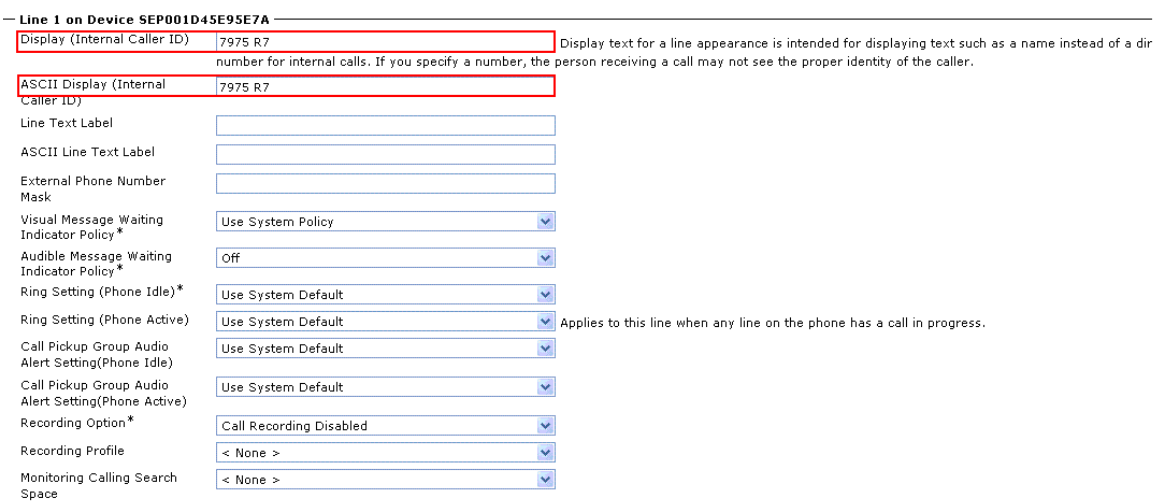
Navigate to **Directory Number Settings** and select the **Voice Mail Profile** created in **Section 5.9**.



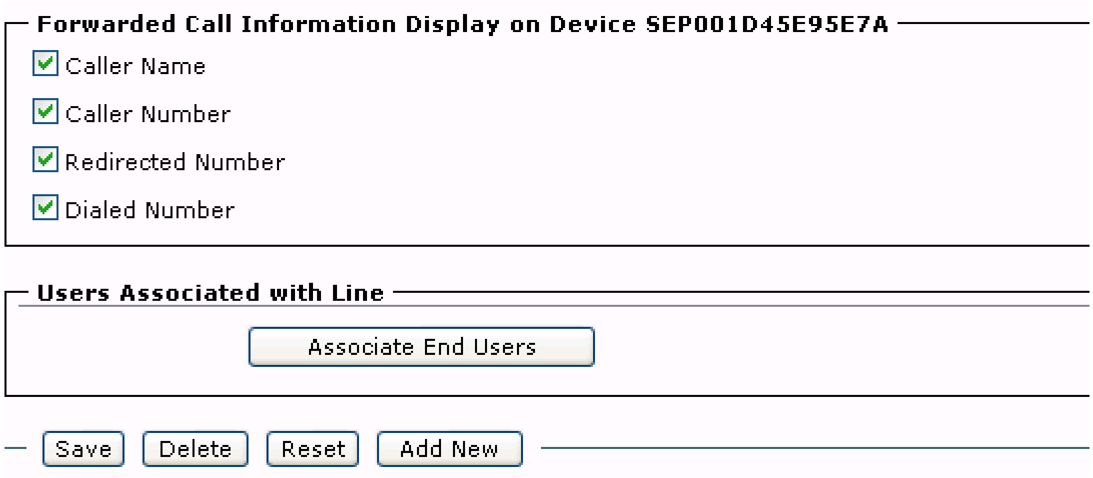
Navigate to **Call Forward and Call Pickup Settings**. Check all the call forward related parameters as shown below.



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.



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



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**.

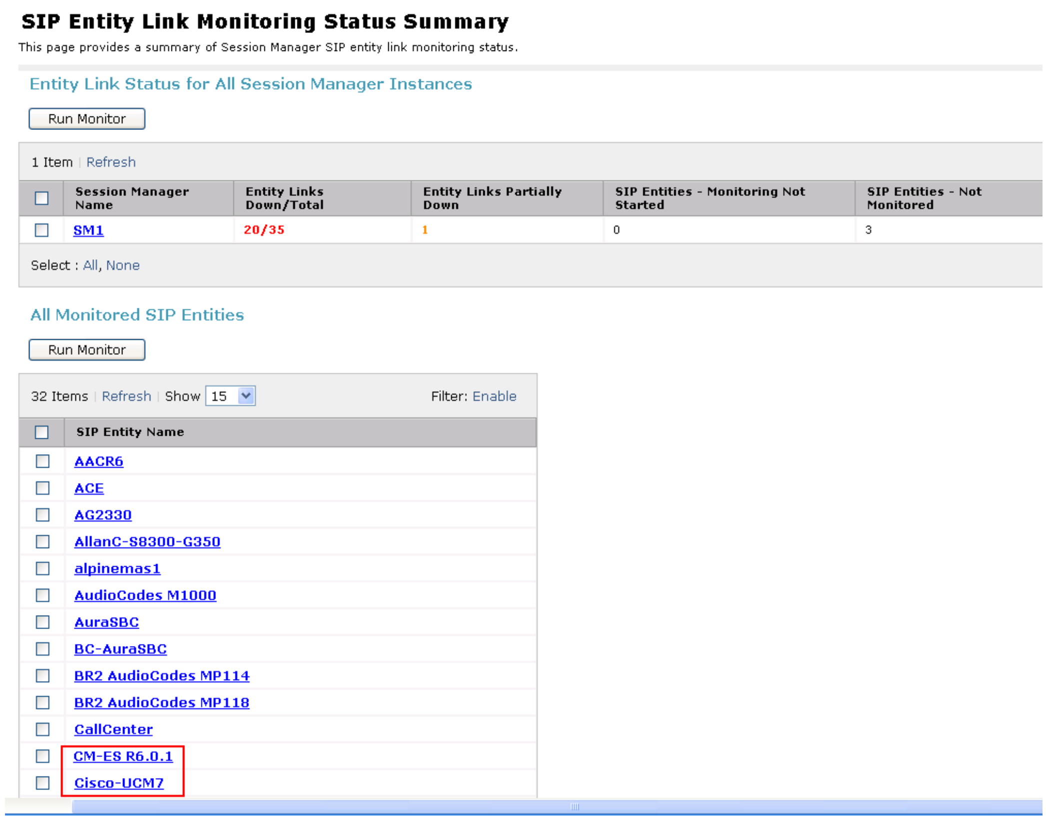
```
status signaling-group 60
                         STATUS SIGNALING GROUP

        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.

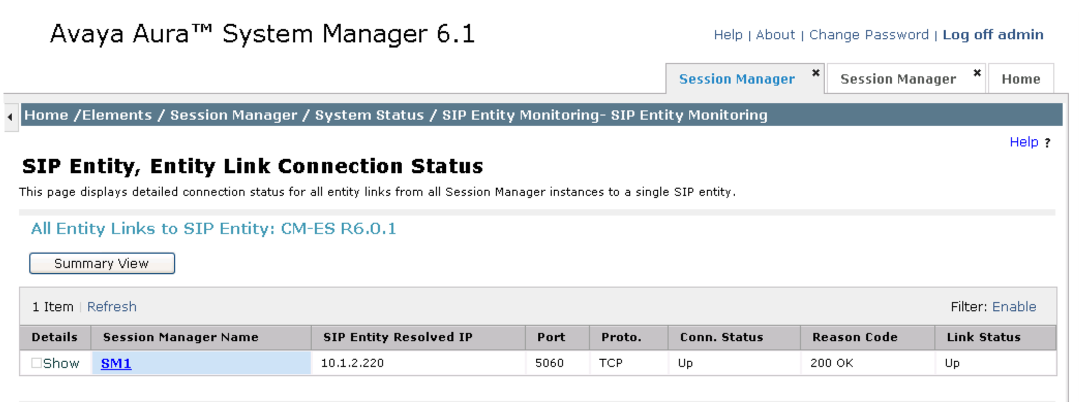
```
status trunk 60

                             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
```

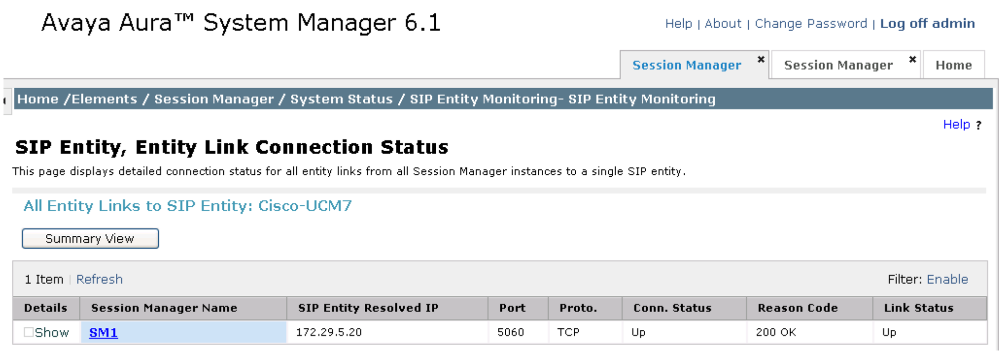
6.2. Verify Avaya Aura® Session Manager

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.

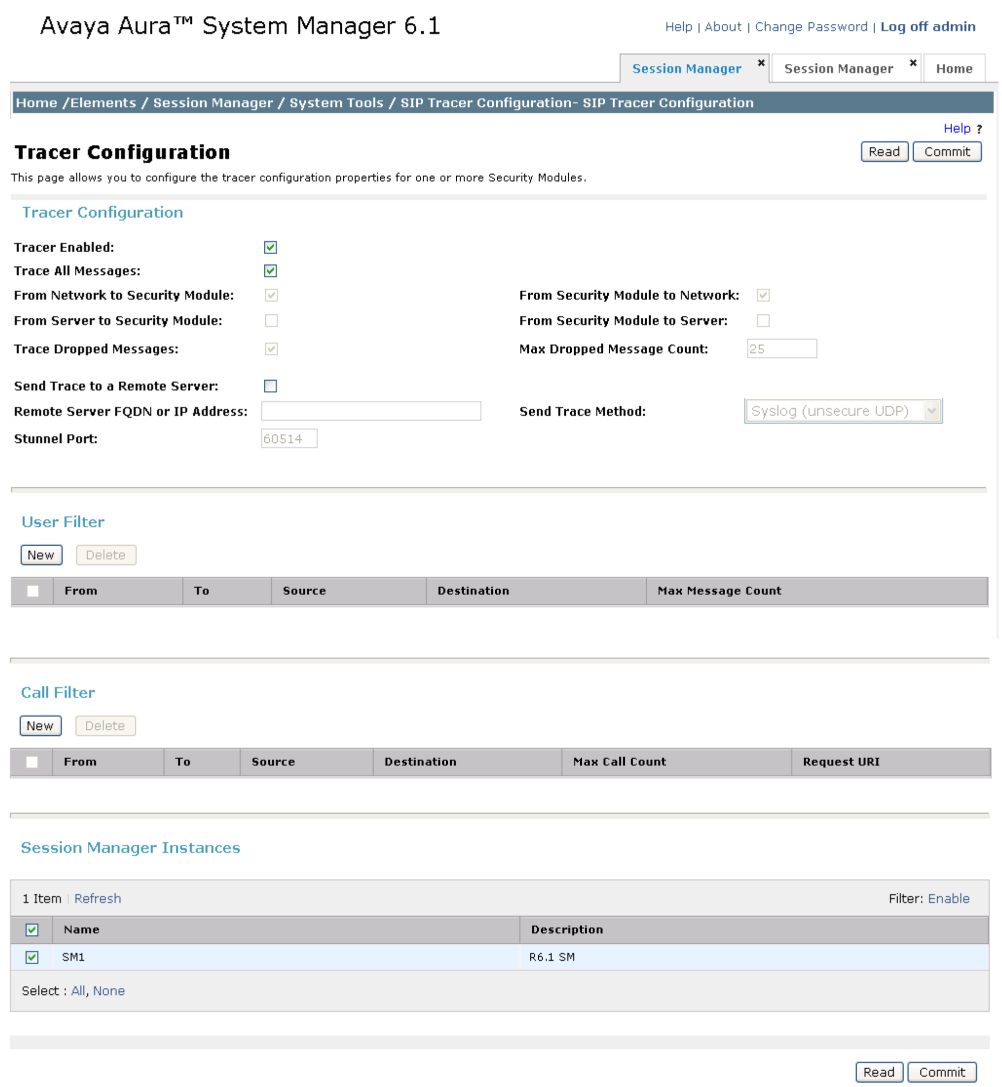


On the above screen under **All Monitored SIP Entities**, click on the SIP Entity names for Communication Manager (**CM-ES R6.0.1**) and Cisco UCM (**Cisco-UCM7**) and verify that the **Link Status** is **Up**, as shown below:

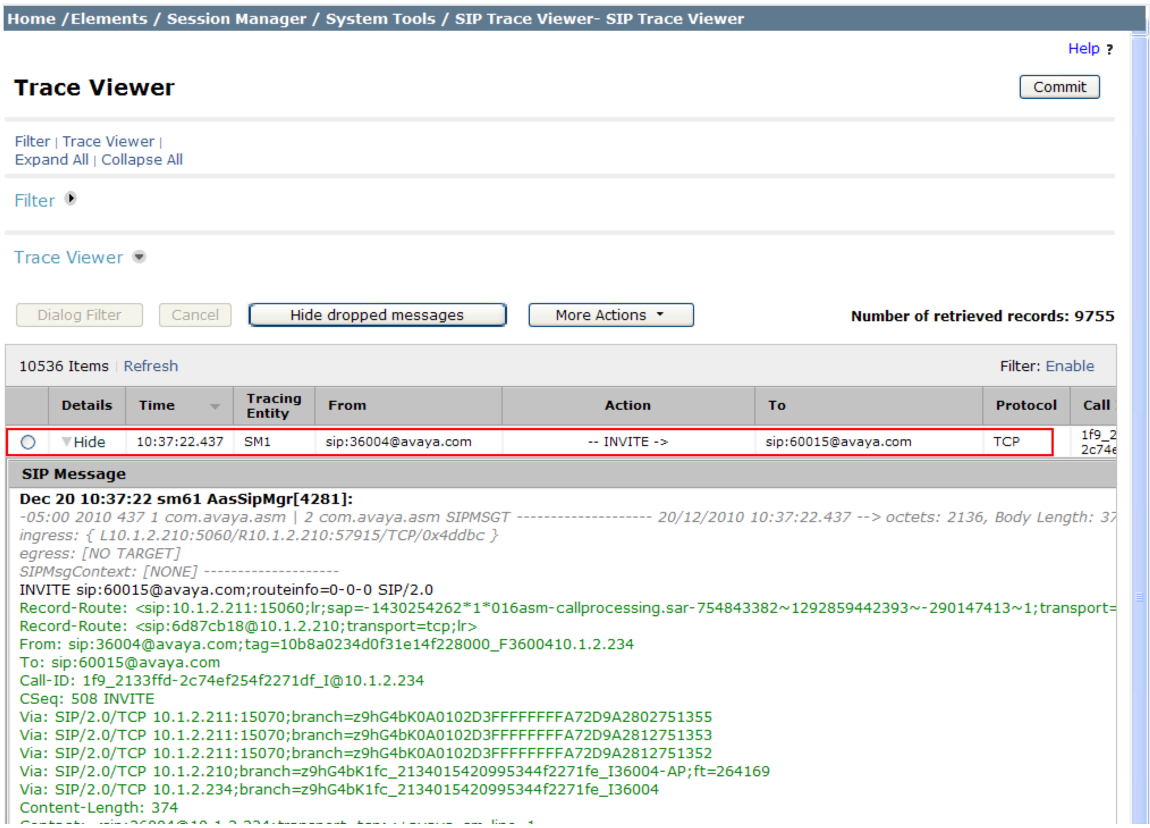




Call traffic can be traced by selecting **Elements → Session Manager → System Tools → SIP Tracer Configuration** as shown below. Under **Session Manager Instances**, select the Session Manager for which tracing will be enabled. See reference **[2]** for details on available SIP tracing and filtering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

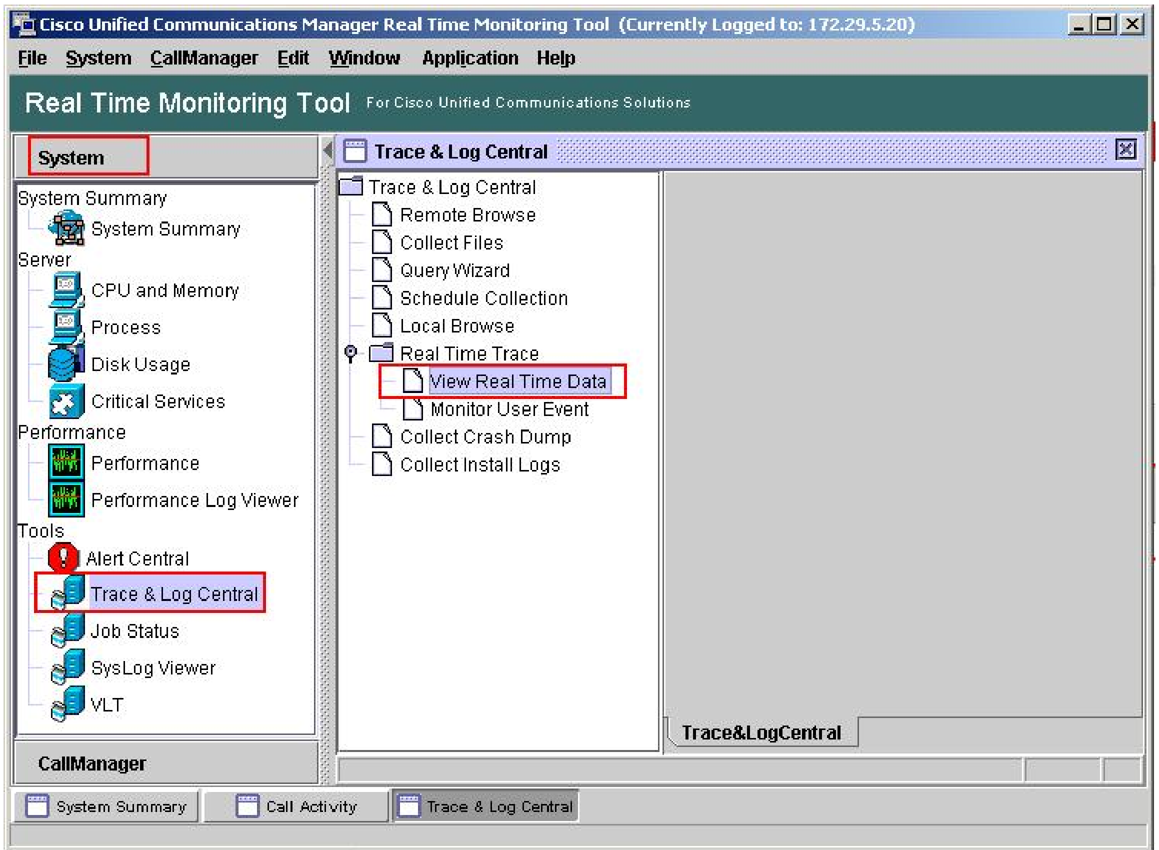


Once the tracer configuration has been established, SIP message traces can be specified by selecting **Elements → Session Manager → System Tools → SIP Trace Viewer**. Set the appropriate **Filter** options for the desired trace time period (details not shown). The following screen shows an example of 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.

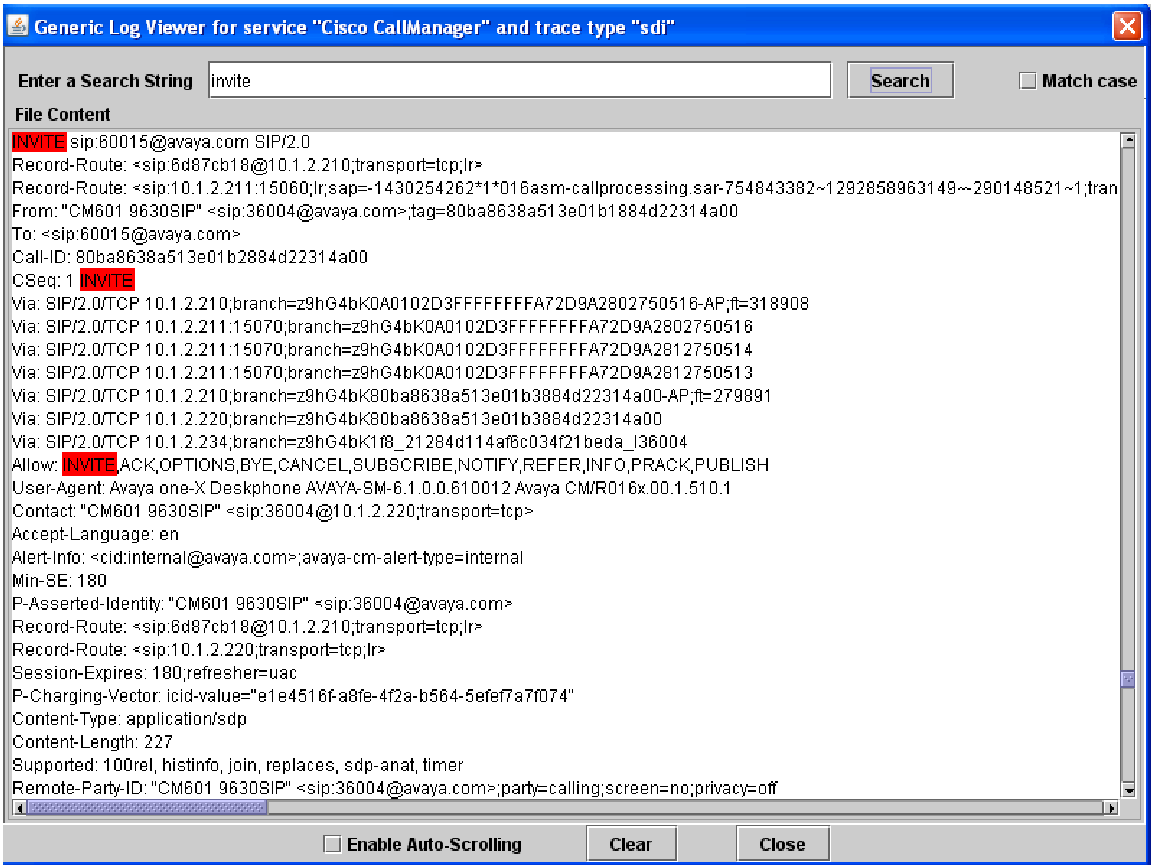


6.3. Verify Cisco Unified Communications Manager

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



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



6.4. Verified Scenarios

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

- Basic calls between various telephones on Communication Manager and Cisco UCM can be made in both directions using G.711MU, G.729A and G.722, with media shuffled directly between the endpoints[5], 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[6]
    - Consultation hold
    - Call forwarding
    - Conference

7. Conclusion

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

---

[5] Media shuffling and G.722 are not supported for calls from Cisco SCCP telephones to Avaya telephones.
[6] On calls between Cisco Unified 9951 and 9971 IP Phones and Avaya telephones, call hold at the Cisco telephone is not supported.

8. Additional References

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

[1] *Avaya Aura™ Session Manager Overview*, Doc # 03-603323, Issue 2

[2] *Administering Avaya Aura™ Session Manager*, Doc # 03-603324, Issue 2

[3] *Maintaining and Troubleshooting Avaya Aura™ 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 Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, Issue 9, May, 2009.

[6] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, Issue 6.0, June 2010.

Product documentation for Cisco Systems products may be found at http://www.cisco.com

[7] *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition*, Release 7.0(1), Part Number: OL-15405-01

[8] *Cisco Unified Communications Manager Features and Services Guide for Cisco Unified Communication Manager Business Edition*, Release 7.0(1), Part Number: OL-15409-01

[9] *Cisco Unified Real-Time Monitoring Tool Administration Guide*, Release 7.0(1), Part Number: OL-14994-01

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

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

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