Avaya Solution Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Messaging 6.1 as a Voice Messaging Solution for Avaya Aura® Communication Manager 6.0.1 Feature & Evolution Server Using SIP Trunks and Avaya Aura® Session Manager 6.1 – Issue 1.0

Abstract

These Application Notes describe a sample configuration of Avaya Aura® Messaging Release 6.1 as a voice messaging solution for Avaya Aura® Communication Manager Feature Server and Evolution Server Release 6.0.1 integrated via SIP trunks using two Avaya Aura® Session Managers in an active-active configuration as a centralizing call routing solution.

- Avaya Aura® Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and adaptations to resolve SIP protocol differences across different telephony systems.
- Avaya Aura® Communication Manager provides call features to a variety of telephony endpoints as well as private a public trunking.
- Avaya Aura® Messaging acts as a centralized voice mail system for Avaya Aura® Communication Manager.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested on this solution.

Table of Contents

1. Introduction

These Application Notes describe a sample configuration of Avaya Aura® Messaging Release 6.1 as a voice messaging solution for Avaya Aura® Communication Manager Feature Server and Evolution Server Release 6.0.1 integrated via SIP trunks using Avaya Aura® Session Manager as a centralizing call routing solution.

As shown in **Figure 1**, Communication Manager runs on the S8300D Server integrated with a G430 Gateway. Communication Manager Feature Server supports only SIP endpoints whereas Communication Manager Evolution Server supports both SIP and non-SIP endpoints (DCP, H323, analog). In the sample configuration both instances of Communication Manager are connected over SIP trunks to Avaya Aura® Session Manager Release 6.1 and use the SIP Signaling network interface on Session Manager.

Avaya Aura® Messaging consists of single Avaya S8800 server serving in both the Application and Storage roles. Avaya Aura® Messaging is also connected over SIP trunk to Session Manager. All inter-system calls are carried over these SIP trunks.

Avaya Aura® Session Manager is managed by Avaya Aura® System Manager. Avaya Aura® System Manager and Avaya Aura® Session Manager each run on an Avaya S8800 Server. For the sample configuration, two Session Manager servers were configured in an **active-active** setup to support both load-balancing and/or failure of one Session Manager.

These Application Notes will focus on the configuration and call routing needed to integrate Aura® Communication Manager with Avaya Aura® Messaging. Not all administration details or other aspects of Communication Manager and Session Manager integration will be described. For more information on these other administration actions, see the appropriate documentation listed in **Section 9.**

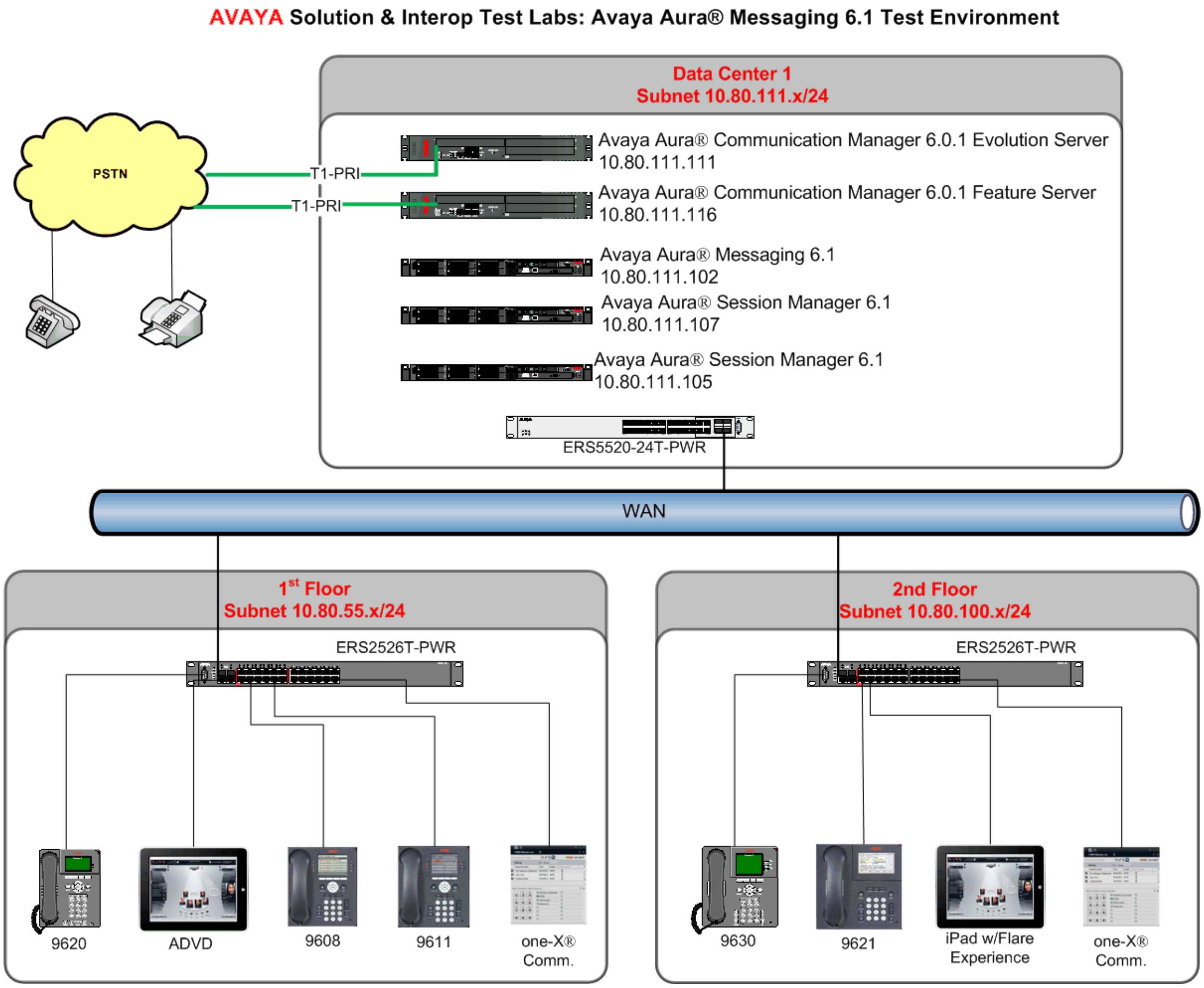


Figure 1 – Sample Configuration

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Component	Software Version
Avaya Aura® Session Manager on Avaya S8800 server	Release 6.1-115
Avaya Aura® System Manager	Release 6.1 SP4
Avaya Aura® Messaging running on single Avaya S8800 server	Release 6.1 Version: 6.1-7.0
Avaya Aura® Communication Manager Evolution & Feature Server	Release 6.0.1 Version R16x.00.1.510.1 SP4 (19100)
96XX Series IP Deskphone (SIP)	FW: SIP R2.6.4
96XX Series IP Deskphone (H323)	FW: R3.1, SP1
96X1 Series IP Deskphone (SIP)	6.0.1-2A
96X1 Series IP Deskphone (H323)	6.016T
Avaya oneX® Communicator (SIP & H.323)	Release 6.1 SP1
Avaya ADVD w/Flare Experience	1.1.0. 007001
Apple iPad-2 w/Flare Experience	iOS: 4.3.5 Flare:1.0-116

Note: The following field updates were also installed on Avaya Aura® Messaging. See http://support.avaya.com for more information on installing these field updates.

- C16013rf+aa
- MANGOset 6.1.115-1.56393
- m61115rf+ac 6.1.115-4

3. Configure Avaya Aura® Communication Manager

This section describes the administration of Communication Manager using a System Access Terminal (SAT). Alternatively, some of the station administration could be performed using the Communication System Management application on System Manager. These instructions assume the G430 Media Gateway is already configured on Communication Manager. Some administration screens have been abbreviated for clarity.

In addition, these instructions assume a SIP trunk between Communication Manager and Session Manager has already been configured as described in reference **[6]**, **Section 9.**

In this section the following administration steps will be described:
Note: Some administration screens have been abbreviated for clarity.

- Verify licensing and system capabilities
- Verify SIP trunk and signaling groups to Session Manager
- Verify ip-codec set used for calls to/from Avaya Aura® Messaging.
- Verify ip-network-region settings.
- Create a coverage-path
- Create a hunt-group
- Configure AAR routing
- Configure a station for coverage to Avaya Aura® Messaging
- Save Changes

3.1. Verify System Capabilities and Licensing

This section describes the procedures to verify the correct system capabilities and licensing have been configured. If there is insufficient capacity or a required feature is not available, contact an authorized Avaya sales representative to make the appropriate changes.

3.1.1. SIP Trunk Capacity Check

Issue the **display system-parameters customer-options** command to verify that an adequate number of SIP trunk members are licensed for the system as shown below.

```
display system-parameters customer-options                  Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                USED
                     Maximum Administered H.323 Trunks: 500   0
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 50    20
```

3.1.2. Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable trunk-to-trunk transfers. This feature is needed to be able to transfer an incoming/outgoing call from/to the remote switch back out to the same or another 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 can pose a significant security risk by increasing the risk of toll fraud and must be used with caution. To minimize the risk, a COS can be defined to allow trunk-to-trunk transfers for a specific trunk group(s). For more information regarding how to configure a Communication Manager to minimize toll fraud, see **Reference [9].**

```
change system-parameters features                               Page   1 of  18
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
```

3.2. Verify SIP Trunk and Signaling Groups

For the sample configuration, SIP trunk and signaling-group 10 and 11 were configured to communicate with Session Manager. The screen shots below show the fields and their settings which were changed from their default for the sample configuration.

- **Group Type:** sip
- **TAC:** #10 (#11 was used for trunk-group 11)
- **Group Name:** ASM1 r 6.1
- **Direction:** two-way
- **Service Type:** tie
- **Signaling Group:** 10 & 11 (not shown)
- **Number of Members:** 30

```
display trunk-group 10                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 10                   Group Type: sip          CDR Reports: y
  Group Name: ASM1 r6.1                   COR: 1        TN: 1        TAC: #10
   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: 10
                                                   Number of Members: 30
```

- **Numbering Format:** private

```
display trunk-group 10                                          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



                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

- **Telephone Event Payload Type:** Should be left blank to let Communication Manager and SIP phones negotiate the payload type for proper DTMF function.

```
display trunk-group 10                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? y
                 Network Call Redirection? n
                   Send Diversion Header? n
                 Support Request History? y
             Telephone Event Payload Type:


       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                            Enable Q-SIP? n
```

Use the command **display signaling-group x** to display the SIP signaling group properties between Communication Manager and Session manager.

- **Group Number:** 10 & 11 were used for the two signaling groups
- **Group Type:** sip
- **IMS Enabled:** Set to '**n**' for Evolution Server and '**y**' for Feature Server
- **Transport Method** Can be TCP or TLS.
- **IP Video:** Set to 'y' if there are IP video capable endpoints in use
- **Priority Video:** Set to 'y' if there are ADVD and one-X® endpoints in use
- **Peer Detection Enabled:** Set to 'y'
- **Peer Server:** Should be set to '**SM**' when the far-end is Session Manager
- **Near-end Node Name:** '**procr**' for S8300
- **Far-end Node Name:** Node-name of the Session Manager
- **Near-end Listen Port:** 5060 is typically used for TCP connection. 5061 for TLS.
- **Far-end Listen Port:** 5060 is typically used for TCP connection. 5061 for TLS**.**
- **Far-end Network Region:** '**1**' for the sample configuration
- **Far-end Domain:** Should be same domain used in Session Manager. See **Section 4.1**

```
display signaling-group 10
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                           SIP Enabled LSP? n
     IP Video? y          Priority Video? y      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                     Far-end Node Name: ASM1-6_1
 Near-end Listen Port: 5060                    Far-end Listen Port: 5060
                                            Far-end Network Region: 1
                                         Far-end Secondary Node Name:
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? y                     Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

For the sample configuration a second sip trunk and signaling-group, **11**, were administered to support the active-active Session Manager configuration. Both are administered identically to the trunk and signaling-group shown above though the Far-end Node Name uses the value of the 2nd Session Manager as shown below.

```
display signaling-group 11
                                SIGNALING GROUP

 Group Number: 11             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                          SIP Enabled LSP? n
     IP Video? y         Priority Video? y      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                     Far-end Node Name: ASM2-6_1
 Near-end Listen Port: 5060                    Far-end Listen Port: 5060
                                            Far-end Network Region: 1
                                       Far-end Secondary Node Name:
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? y                 Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

3.3. Verify IP Codec Set

Verify voice codec that will be used. Avaya endpoints support a variety of codec though Avaya Aura® Messaging Supports only G.711Mu-law and A-law. The ip-codec shown below allows IP phones to communicate directly with each other using the G.729A codec thus reducing the amount of IP bandwidth utilized but also allows them to communicate with the messaging server using G.711Mu-law.

For encrypted audio change 'none' to one of the supported encryption methods. Avaya Aura® Messaging supports the following encryption algorithms:

- srtp-aescm128-hmac80
- srtp-aescm128-hmac32

```
display 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.729A             n         2        20
 2: G.711MU            n         2        20
 3:
 4:


     Media Encryption
 1: none
 2:
```

Navigate to page 2. In order to enable IP Video with Avaya endpoints its necessary to set **Allow Direct-IP Multimeida** to '**y**'. To enable Fax over IP set **FAX** to **t.38-standard**.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia: 15360:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia: 15360:Kbits

                    Mode                 Redundancy
    FAX             t.38-standard         0
    Modem           off                   0
    TDD/TTY         US                    3
    Clear-channel   n                     0
```

3.4. Verify IP Network Region

Run the command **display ip-network-region 1** to determine the **ip-codec-set** that is chosen when this region is in use. In **Section 3.2** the far-end network region value was set to **1**, the **Procr** interface is region 1 and IP phones are in region 1, therefore calls that route over signaling-group 10 will be viewed by Communication Manager as a call that stays within ip-network-region 1.

Page 1 of the ip-network-region 1 form shown below indicates that for a call that is considered to stay within **ip-network-region 1**, **ip-codec-set 1** will be utilized. See **Section 9** for more information on administering ip-network-regions.

```
display ip-network-region 1                                        Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: SIP Trunk
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? n
   UDP Port Max: 3329
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
```

3.5. Create a Coverage Path

Configure a coverage path for the messaging subscribers. Use the command **add coverage path n** where **n** is the coverage path number to be assigned. Configure a coverage point, using value **hx** where **x** is the hunt group number defined in **Section 3.6**. In this case it is hunt-group 1 or **h1** as shown below.

```
add coverage path 1                                            Page   1 of   1
                                 COVERAGE PATH

                   Coverage Path Number: 1
     Cvg Enabled for VDN Route-To Party? y        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n               n
               Busy?             y               y
         Don't Answer?           y               y        Number of Rings: 2
                All?             n               n
 DND/SAC/Goto Cover?             y               y
   Holiday Coverage?             n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h1             Rng:    Point2:
  Point3:                        Point4:
  Point5:                        Point6:
```

3.6. Create a Hunt Group

Configure a **Hunt Group** to be used as the call coverage point for the call coverage path assigned to MAS subscribers. Use the **add hunt-group n** command where **n** is the hunt group number to be assigned. Configure a **Group Name** and **Group Extension** number to be used as the Avaya Aura® Messaging pilot name and number. Select **ucd-mia** for **Group Type.**

```
add hunt-group 1                                                 Page   1 of  60
                                  HUNT GROUP

            Group Number: 1                                ACD? n
              Group Name: Cover to Aura Msg              Queue? n
         Group Extension: 444-5002                      Vector? n
              Group Type: ucd-mia                Coverage Path:
                      TN: 1          Night Service Destination:
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display: grp-name
```

Navigate to **Page 2**. Select **sip-adjunct** for **Message Center**. **Voice Mail Number** and **Voice Mail Handle** can be the same value and need not be the same number used for **Group Extension** on Page 1. In fact these values and not the Group Extension will used in the SIP INVITE in the *To*, *From* and *PAI* headers.
Routing Digits (for example, *8) are only necessary if the number used in the **Voice Mail Number** field require a Feature Access Code (FAC) to access the SIP trunk.

```
add hunt-group 1                                            Page   2 of  60
                                   HUNT GROUP





                      Message Center: sip-adjunct

     Voice Mail Number         Voice Mail Handle          Routing Digits
                                                   (e.g., AAR/ARS Access Code)
     4445000                   4445000
```

3.7. Administer Routing for Calls to Messaging

In **Section 3.6** a Hunt Group was created to send calls that cover to messaging to extension **444-5000**. This same extension will be used by messaging subscribers to retrieve their messages. In **Section 5.1** an additional pilot number is configured to directly access the messaging Auto Attendant. That extension is **444-5001**. As these extensions overlap with the dial plan configured for extensions on Communication Manager, configure Uniform Dialing and AAR to route these calls over a SIP trunk to Session Manager and ultimately to Avaya Aura® Messaging without the need to dial a Feature Access Code (FAC).

Use the command **change uniform dial-plan 4** to create an entry in the UDP table which covers extensions 444500 & 4445001.

As shown below, any number dialed to **4445xxx** totaling 7-digits will be routed to the AAR table.

```
change uniform-dialplan 4                                      Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                               Percent Full: 0

  Matching                    Insert              Node
  Pattern        Len Del      Digits     Net Conv Num
 4445             7   0                  aar  n
 508              7   0                  ext  n
 5089110          7   0                  aar  n
 5089111          7   0                  aar  n
```

Next, use the command **change aar analysis 4** to create an entry that will route calls to these extensions to the appropriate Route Pattern. For the sample configuration, this is **route-pattern 10** (not shown) on both the Evolution and Feature Servers.

```
change aar analysis 4                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 3

          Dialed             Total     Route     Call   Node  ANI
          String           Min  Max  Pattern    Type   Num   Reqd
    4443008                7    7     10        unku         n
    4443030                7    7     10        unku         n
    4443111                7    7     10        unku         n
    4443112                7    7     10        unku         n
    4443113                7    7     10        unku         n
    4445                   7    7     10        unku         n
    508                    7    7     10        unku         n
```

Next, use the command **display route-pattern 10** to verify that SIP trunks shown in **Section 3.2** are used in the route-pattern. As previously indicated, two SIP trunk-groups, 10 & 11 were configured for redundancy. As shown below, both of these trunks are present in the route pattern. In addition, **Numbering Format** is set to **lev0-pvt** to ensure that the calling extension number can be properly displayed at the called destination. Lastly, the **LAR** field for trunk-group 10 is set to **next** to allow for use of trunk-group 11 in the event that 10 is out of service or otherwise unavailable.

```
display route-pattern 10                                        Page   1 of   3
                    Pattern Number: 10  Pattern Name: to ASM1 6.1
                             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: 10   0                                                             n   user
 2: 11   0                                                             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                               lev0-pvt  next
 2: y y y y y n  n           rest                               lev0-pvt  none
```

3.8. Administer a Station for Coverage to Messaging

Configure any and all phones that have a mailbox on the messaging server for call coverage. Use the command **change station xyz** and on **Page1** for **Coverage Path 1** use the coverage path defined in **Section 3.5** In the example below station 444-3008 was configured to cover to messaging using cover path 1.

```
change station 4443008                                          Page   1 of   6
                                     STATION

Extension: 444-3008                      Lock Messages? n             BCC: 0
     Type: 9630SIP                       Security Code: 123456         TN: 1
     Port: S00063                      Coverage Path 1: 1             COR: 1
     Name: 9608SIP-ES                  Coverage Path 2:               COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                Location:                  Time of Day Lock Table:
              Loss Group: 19
                                                 Message Lamp Ext: 444-3008

        Display Language: english                  Button Modules: 0

          Survivable COR: internal
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                                         IP Video? n
```

Navigate to page 2 and set the **MWI Served User Type** to **sip-adjunct**.

```
change station 4443008                                          Page   2 of   6
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe
          LWC Activation? y                      Coverage Msg Retrieval? y
                                                         Auto Answer: none
             CDR Privacy? n                            Data Restriction? n
                                                Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n
  Active Station Ringing: single

        H.320 Conversion? n          Per Station CPN - Send Calling Number?
                                                        EC500 State: enabled

    MWI Served User Type: sip-adjunct

                                                 Coverage After Forwarding? s

                                               Direct IP-IP Audio
Connections? y
  Emergency Location Ext: 444-3008      Always Use? n IP Audio Hairpinning? n
```

4. Configure Avaya Aura Session® Manager

This section provides the procedures for configuring Avaya Aura® Session Manager to route calls between Communication Manager and Avaya Aura® Messaging.

These instructions assume other administration activities have already been completed such as defining the SIP entities for Communication Manager and Session Manager, defining the network connection between System Manager and Session Manager, and defining the Entity Link for the SIP trunk between Communication Manager and Session Manager.

For more information on configuring a SIP Trunk between Communication Manager and Session Manager, see additional references in **Section 9**.

The following administration activities will be described:

- Define SIP Domain
- Define Location for Avaya Aura® Messaging
- Define SIP Entity corresponding to Avaya Aura® Messaging
- Define Entity Links between Avaya Aura® Messaging and both Session Managers.
- Verify Entity Links between Communication Manager and both Session Managers.
- Define Routing Policies, which control call routing between the SIP Entities.
- Define Dial Patterns, which govern to which SIP Entity a call is routed.

Note: Some administration screens have been abbreviated for clarity.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL "**http://<ip-address>/SMGR**", where **<ip-address>** is the IP address of Avaya Aura® System Manager. Login with the appropriate credentials.

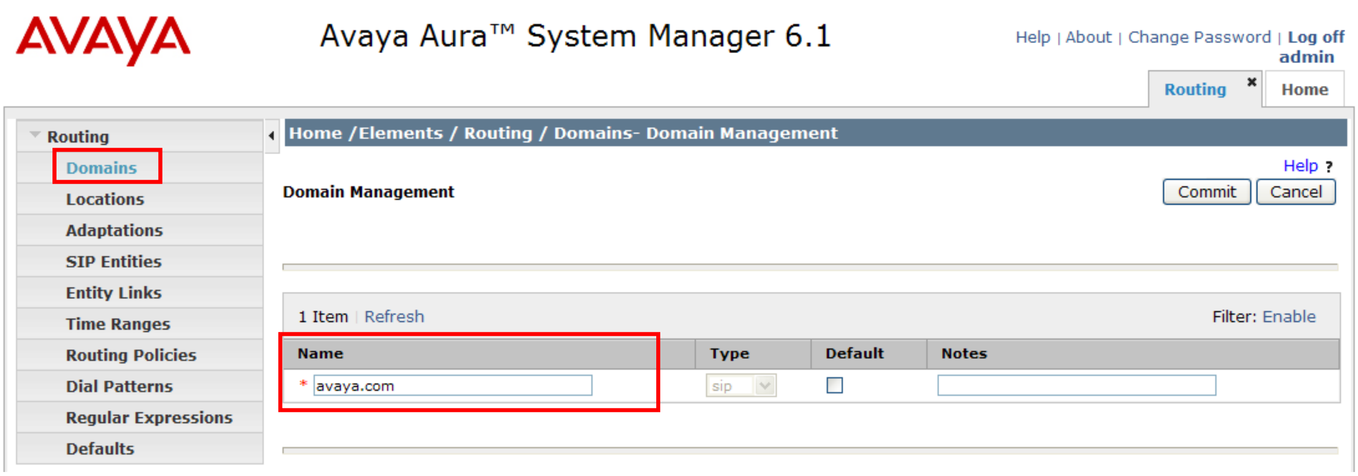
4.1. Define SIP Domain

Expand **Elements → Routing** and select **Domains** from the left navigation menu.

Click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name** Enter the Domain Name for the configuration
  In the sample configuration, "**avaya.com**" was used.
- **Type** Verify "**SIP**" is selected.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.



4.2. Define Location for Avaya Aura® Messaging

Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

Expand **Elements → Routing** and select **Locations** from the left navigational menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

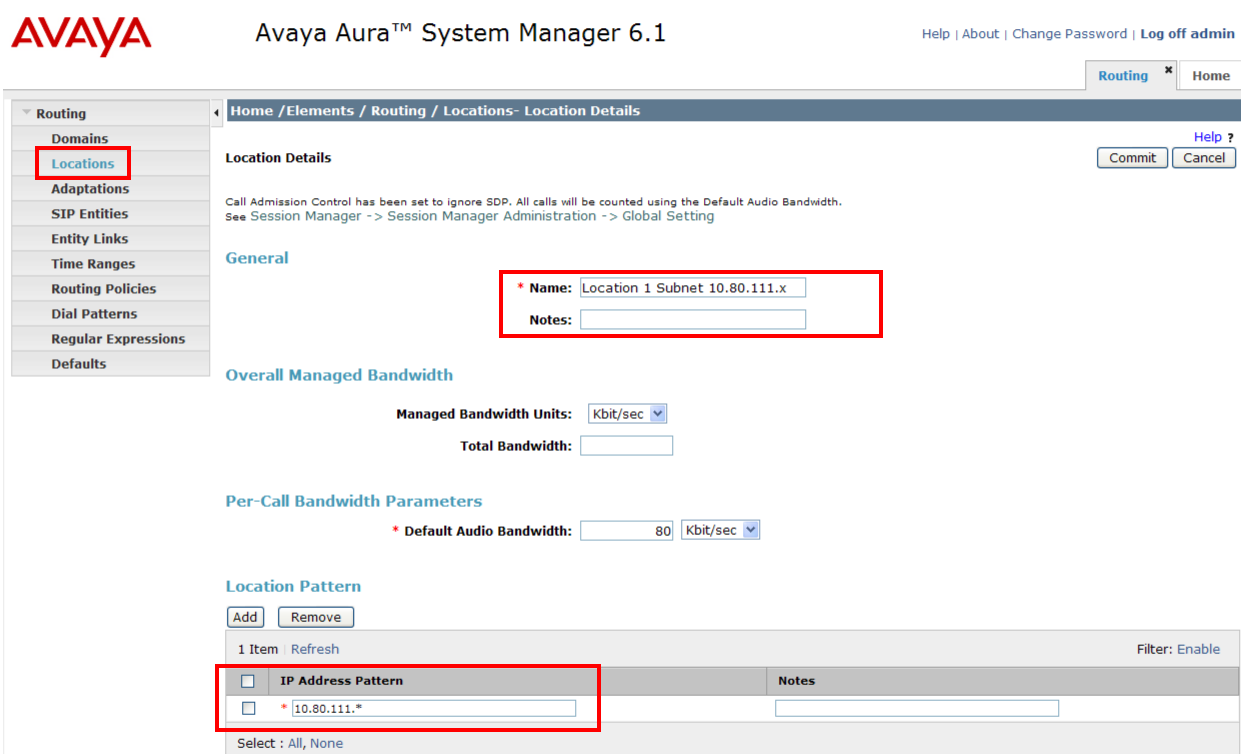
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location. For the sample configuration, "**10.80.111.***" was used.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows the Location defined for Avaya Aura® Messaging in the sample configuration.



4.3. Define SIP Entity

A SIP Entity must be added for Avaya Aura® Messaging.

Expand **Elements → Routing** and select **SIP Entities** from the left navigation menu.

Click **New** (not shown)**.** In the **General** section, enter the following values and use default values for remaining fields**.**

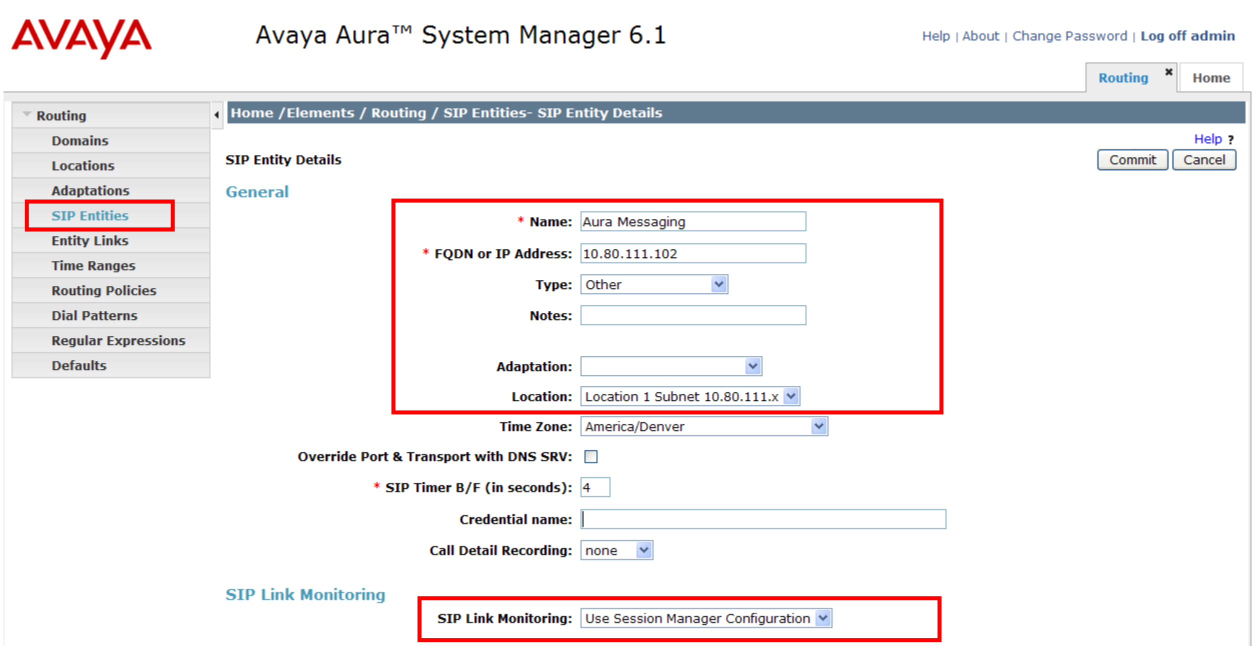
- **Name:** Enter an identifier for the SIP Entity
- **FQDN or IP Address:** Enter IP address of Avaya Aura® Messaging.
- **Type:** Select "**Other**"
- **Notes:** Enter a brief description. [Optional]
- **Location:** Select the Location defined for Avaya Aura® Messaging in **Section 4.2**

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select "**Use Session Manager Configuration**"

Click **Commit** to save the definition of the new SIP Entity.

The following screen shows the SIP Entity defined for Avaya Aura® Messaging in the sample configuration.



4.4. Define Entity Links for Avaya Aura® Messaging

The SIP trunk between Session Manager and Avaya Aura® Messaging is described by an Entity link.

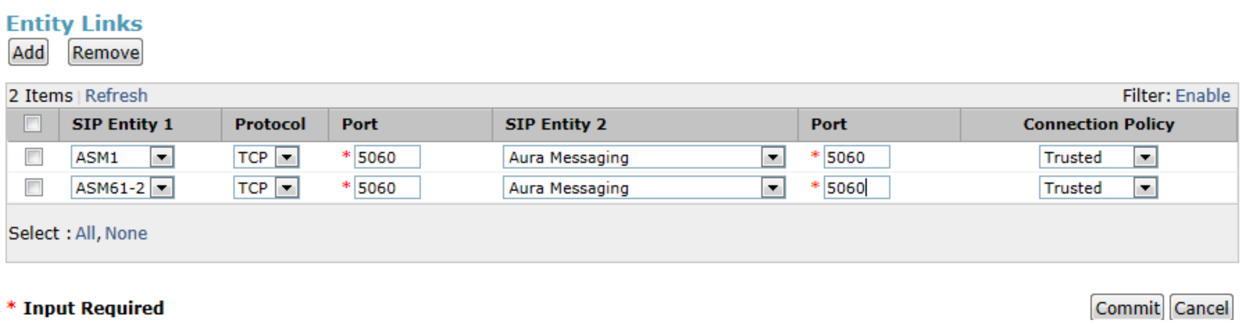
Expand **Elements → Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

- **Name** Enter an identifier for the link to each telephony system.
- **SIP Entity 1** Select SIP Entity defined for Session Manager
- **Protocol** After selecting both SIP Entities, select "**TCP"** as the required protocol.
  Note: TCP was used for the sample configuration. However, TLS would typically be used in production environments. For more information on configuring the system to use TLS, see **Reference [5]** in **Section 9.**
- **Port** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is "**5060**".
- **SIP Entity 2** Select the SIP Entity defined for Avaya Aura® Messaging in **Section 4.3**
- **Trusted** Enter
- **Notes** Enter a brief description. [Optional]

Click **Commit** to save **Entity Link** definition.

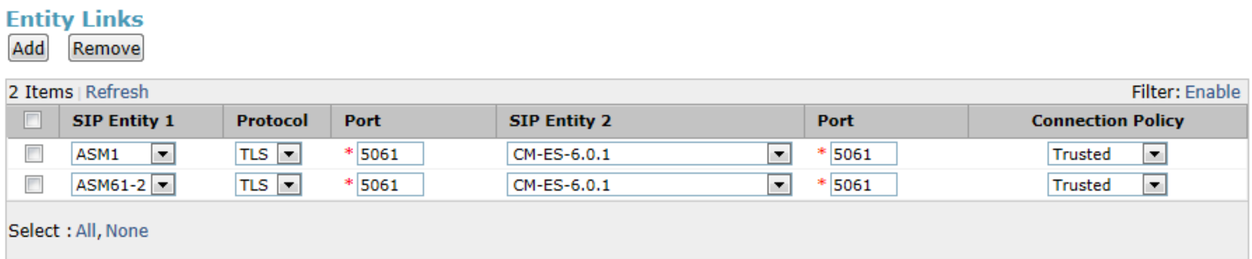
The following screen shows the entity links defined for the SIP trunk between both Session Managers and Avaya Aura® Messaging.



	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
	ASM1	TCP	* 5060	Aura Messaging	* 5060	Trusted
	ASM61-2	TCP	* 5060	Aura Messaging	* 5060	Trusted

NOTE: In order to support active-active redundant Session Managers the following Entity Links must also be defined (not shown).

- An Entity Link between the two Session Managers (not shown)
- An Entity Link between the 2nd Session Manager and the 2nd signaling-group on Communication Manager. As shown below, Communication Manager Evolution Server has entity links to both Session Manager servers.



See **Section 9** for more information on configuring Session Manager.

4.5. Define Routing Policy

Routing policies describe the conditions under which Session Manager will route calls between Communication Manager and Avaya Aura® Messaging.

To add a routing policy, expand **Elements → Routing** and select **Routing Policies.**

Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional]

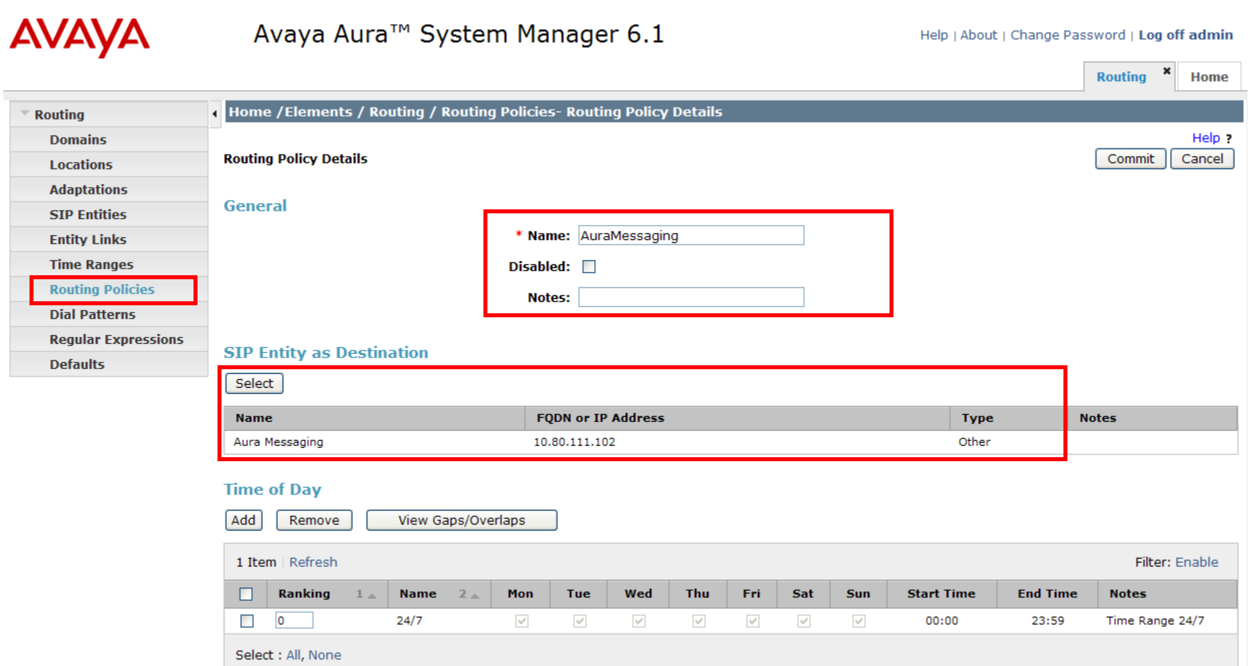
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with Avaya Aura® Messaging defined in **Section 4.3** and click **Select.**
- The selected SIP Entity displays on the **Routing Policy Details** page.

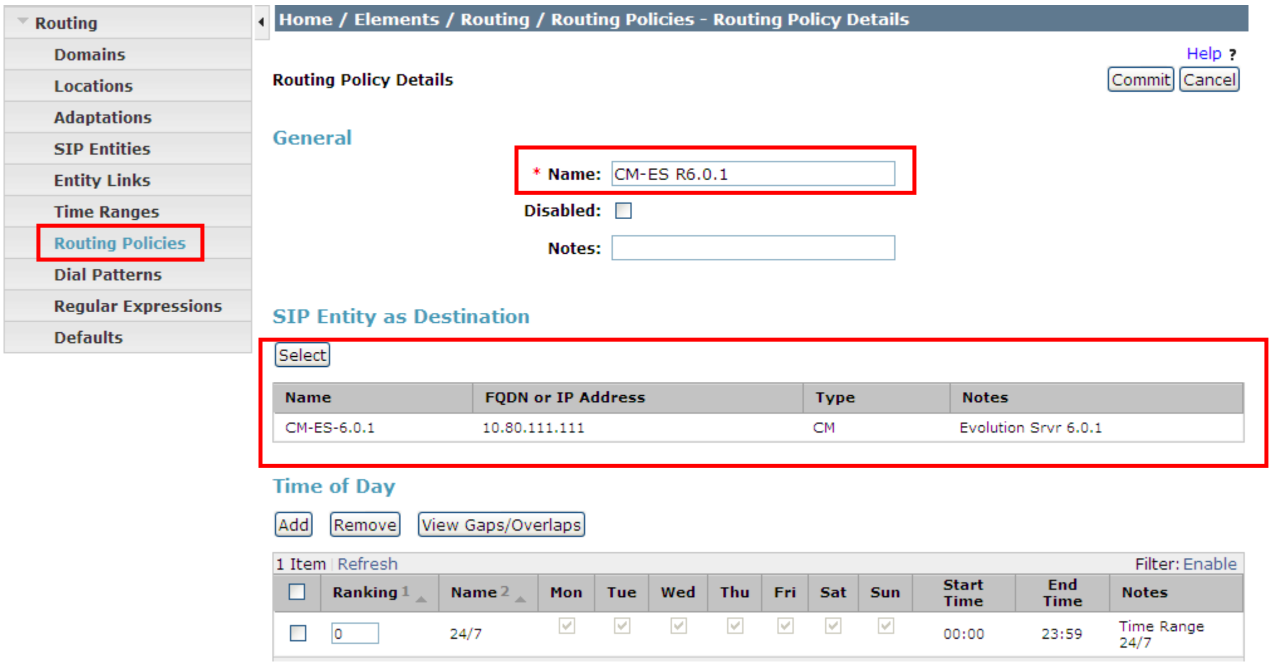
Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

Note: The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

The following screen shows the Routing Policy for Avaya Aura® Messaging.



Repeat the steps to define a Routing Policy for Communication Manager Evolution Server.



4.6. Define Dial Patterns

In the sample configuration, two dial patterns were defined for routing calls to Communication Manager Evolution Server and Avaya Aura® Messaging.

- "**444**" corresponds to non-SIP stations on Avaya Aura® Communication Manager Evolution Server
- "**44450**" corresponds to the Pilot and Auto Attendant numbers for Avaya Aura® Messaging.

- **NOTE:** No dial pattern or routing policy need to be defined to route calls to SIP endpoints which get their call features from Avaya Aura® Communication Manager. SIP endpoints, which are directly registered to Session Manager, require no additional call routing administration in Session Manager.

To define a dial pattern, expand **Elements → Routing** and select **Dial Patterns** (not shown).

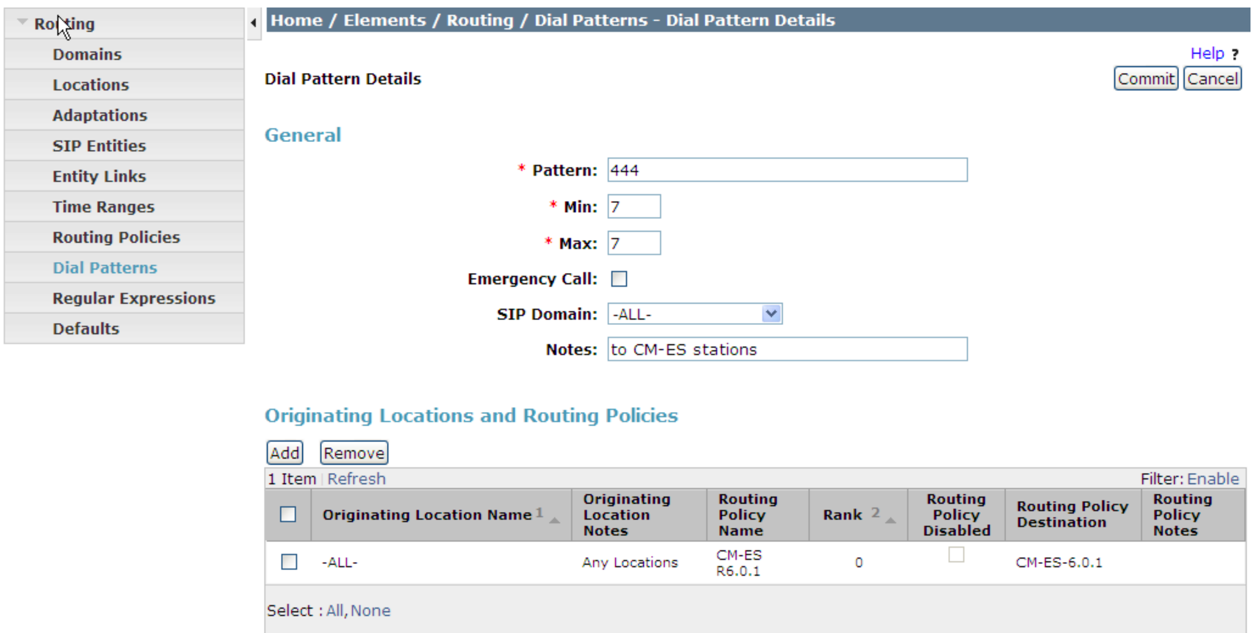
Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern
- **Min:** Enter the minimum number digits that must to be dialed.
- **Max:** Enter the maximum number digits that may be dialed.
- **SIP Domain:** Select the SIP Domain from drop-down menu or select **"All**" if Session Manager should accept incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

In the **Originating Locations and Routing Policies** section, click **Add.**
The **Originating Locations and Routing Policy List** page opens (not shown).

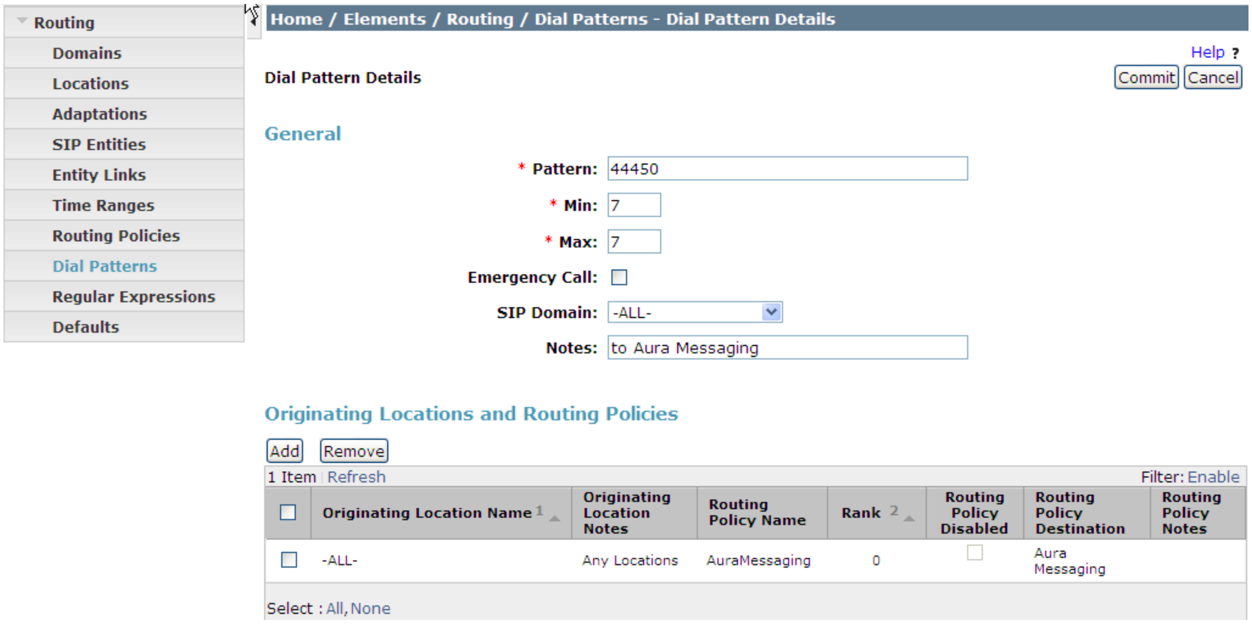
- In **Originating Locations** table, select "**ALL**"
- In **Routing Policies** table, select the Routing Policy defined Communication Manager in **Section 4.5.**
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save. The following screen shows the first Dial Pattern defined for sample configuration for calls to non-SIP stations supported by Communication Manager Evolution Server.



Repeat the steps to define a second dial pattern corresponding to the Pilot and Auto Attendant numbers for Avaya Aura® Messaging (4445000 & 4445001 respectively).

The second dial pattern defined for sample configuration is shown below:



5. Configure Avaya Aura® Messaging

This section provides the procedures for configuring Avaya Aura® Messaging to connect to Avaya Aura® Session Manager over a SIP trunk and to add Communication Manager subscribers.

These instructions assume other administration activities have already been completed such as configuring the Message Storage Server and Messaging Application Server, defining the system mailbox or configuring other system level parameters.

Note: In earlier releases of Avaya Aura® Messaging, IMAP ports were configured to support access from external clients such as Microsoft Outlook. However, in Avaya Aura® Messaging Release 6.1, configuration of IMAP ports is required for all subscribers. For more information on administering this system parameter or other aspects of administering Avaya Aura® Messaging, see **references [9]** through **[11]** in **Section 9.**

The following administration activities will be described:

- Administer Sites
- Administer Telephony Integration
- Administer Dial Rules
- Administer Class of Service to enable Message Waiting
- Administer Subscribers

Note: Some administration screens have been abbreviated for clarity.

Configuration is accomplished by accessing the browser-based System Management Interface of Avaya Aura® Messaging, using the URL "**http://<ip-address>/**", where **<ip-address>** is the IP address of Avaya Aura® Messaging. Login with the appropriate credentials.

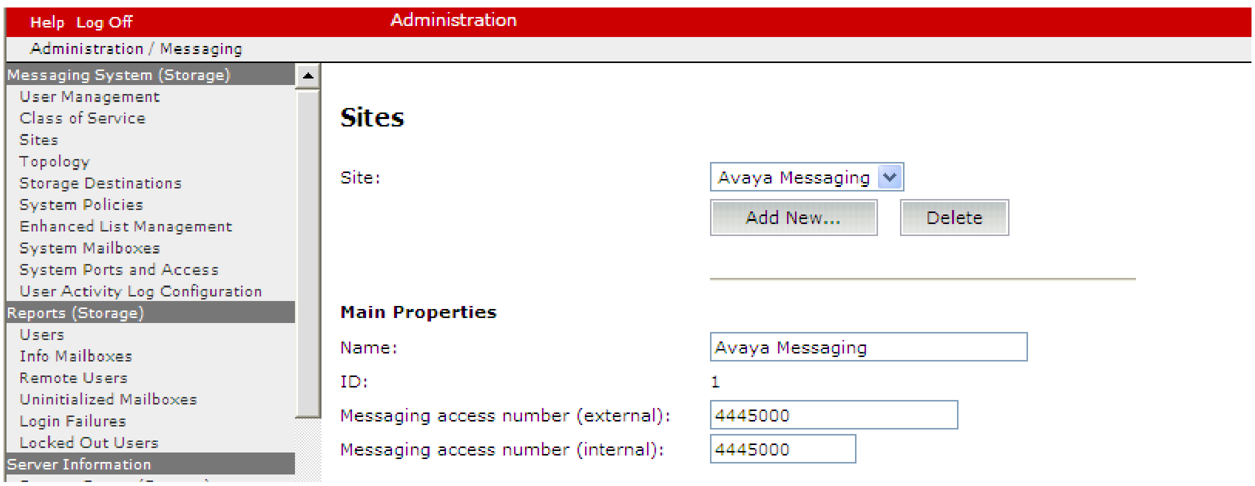
5.1. Administer Sites

A Messaging Pilot number and Auto Attendant number needs to be defined for every site. For the sample configuration, "**444-5000**" and "**444-5001**" were used.

Use **Administration → Messaging** menu and select **Sites** under **Messaging System (Storage).**

Under **Main Properties** section, enter the following values.

- **Name:** Enter descriptive name for the Site
- **Messaging access number (internal):** Enter the Pilot number for the Site
- **Messaging access number (external):** Enter the Pilot number for the Site
- **Extension Length**: Enter number of digits in station numbers
- **Mailbox Length:** Enter number of digits in mailbox number



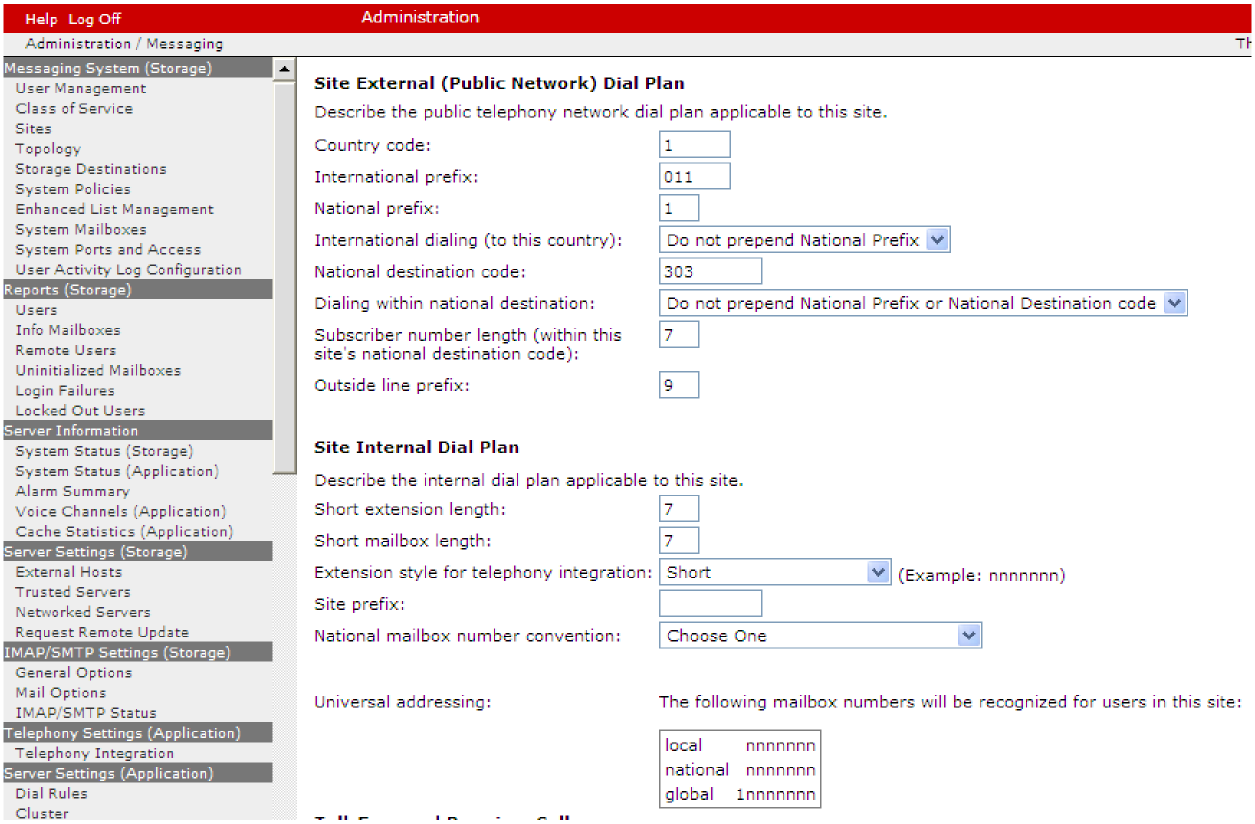
Under **Site External (Public Network) Dial Plan**, the following values were used for the sample configuration. These are typical for sites in North America.

- **Country Code:** 1 for the US
- **International Prefix:** 011
- **National Prefix:** **'1'** often used for dialing outside one's area code
- **National destination code:** **'303'** which is the local area code
- **Subscriber number length:** Subscribers were configured with 7 digit extensions which matches the length of the extension on Communication Manager.
- **Outside line prefix:** **'9'** An access code often used on PBX's for accessing an external line.

Under **Site Internal Dial Plan** the following values were used for the sample configuration.

- **Short extension length:** Enter number of digits in station numbers.
- **Short mailbox length:** Enter number of digits in mailbox number.
- **Extension Style for**

All other fields were left at their defaults. The following screenshot shows the data as entered for the sample configuration.



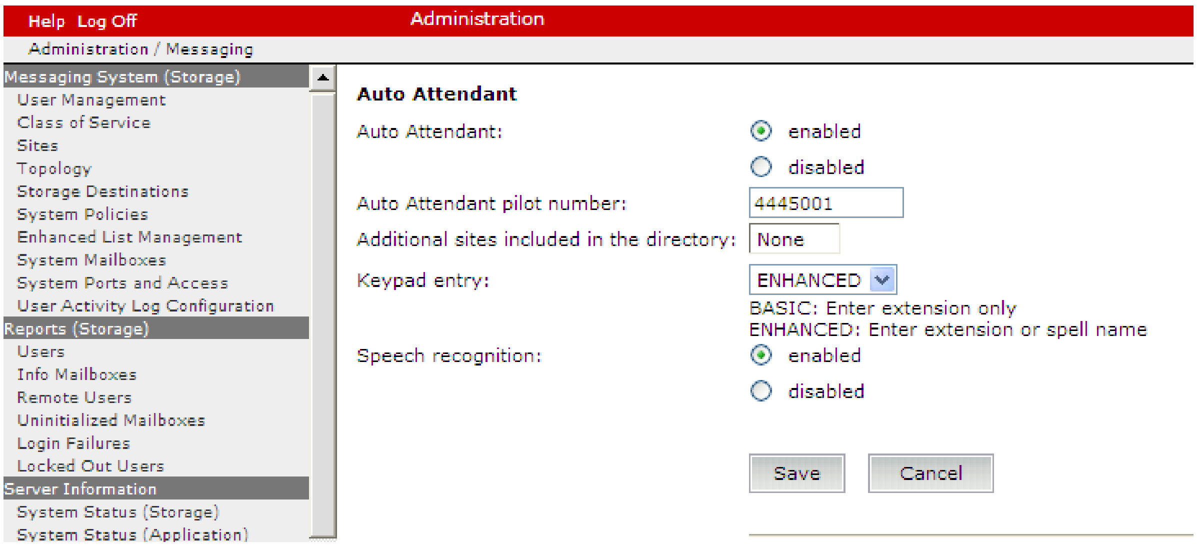
Under **Auto Attendant** section, enter the following values, using default values for other fields.

- **Auto Attendant:** Enter in **enabled** field
- **Auto Attendant pilot number:** Enter an Auto Attendant number

Under **Auto Attendant** section, enter the following values, using default values for other fields.

- **Auto Attendant:** Enter in **enabled** field
- **Auto Attendant pilot number:** Enter an Auto Attendant number

-



Click the **Save button** when complete.

5.2. Administer Telephony Integration

Use **Administration → Messaging** menu and select **Telephony Integration** under **Telephony Settings (Application)** to configure the SIP Trunk between Avaya Aura® Messaging and Session Manager.

Under **BASIC CONFIGURATION** section, enter the following value.

- **Switch Integration Type** Select "**SIP**"
- **Extension Length** Enter the extension length used on Communication Manager. "**7**" for the sample configuration.

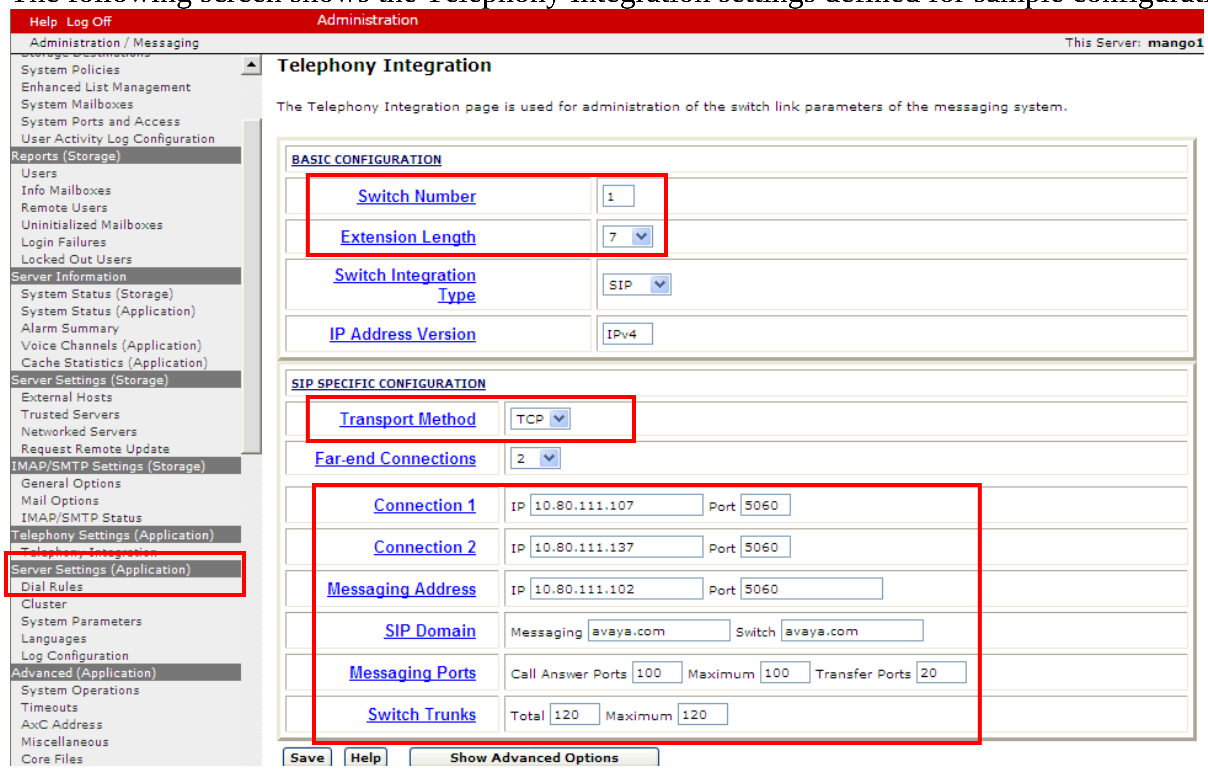
Under **SIP SPECIFIC CONFIGURATION** section, enter the following values and use default values for remaining fields.

- **Transport Method** Select "**TCP**" (TLS is also supported)
- **Far End Connections** For the sample configuration, two Session Managers were present so the value "**2**" was entered.
- **Connection 1/Port** Enter IP address and Port Number for the 1st Session Manager specified in **Section 4.4**
- **Connection 2/Port** Enter IP address and Port Number for the 2nd Session Manager.

- **Messaging Address** Enter IP address and Port Number of Avaya Aura®
- **SIP Domain** Enter domain name from **Section 4.1**

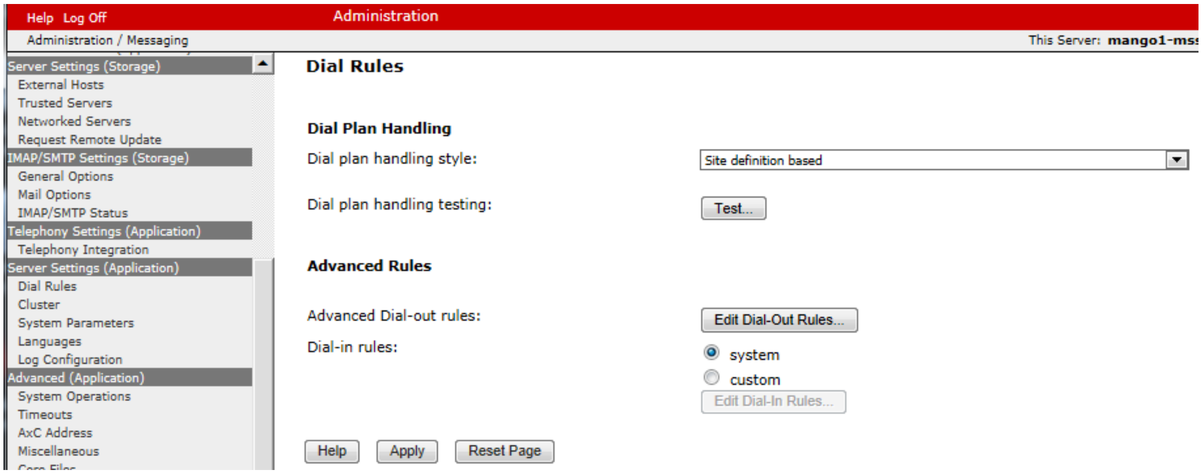
Click **Save** to save changes.

The following screen shows the Telephony Integration settings defined for sample configuration.



5.3. Configure Dial Rules

Navigate to Administration→Messaging→Server Settings (Application)→ Dial Rules to configure the dial rules. Set the **Dial plan handling style:** field to **Site definition based** as shown below.



Next select the **Edit Dial-Out Rules** button to verify the appropriate paramaters for outbound dialing from Avaya Aura® Messaging were set above. These dial rules help Avaya Aura® messaging send the correct number and combination of digits when originating a call to Communication Manager, whether the call is destined for another extension or ultimately expected to be routed to the PSTN.

For the sample configuration, 7-digit extensions were used on Communcation Manager so any time Aura Messaging originates a call to an extension it should send the 7-digit number and not attempt to insert or delete any digits.

Scroll down to the section titled **Dial-out Test Numbers**. Enter in a number in the appropriate section an select the **Test** button to see how Avaya Aura® Messaging would dial that number.

As shown below the number **7785002** is treated as an internal number and is dialed intact, whereas the test number **408-555-7086** is treated as a long-distance national number which requires a **9** prefixed as an access code.

Dial-Out Test Numbers

```
# Examples below:
# Add more phone numbers to test for your specific configuration.

# Extension (example):
2001
7785002
(212) 555-7086


# Local number (example):
555-7086
333-3030

# Long-distance number (example):
(408) 555-7086
```

Test Save

Dial-Out Test Results

Input Phone Number	→	Call Type	Output Phone Number
2001	→	INTERNAL	2001
7785002	→	INTERNAL	7785002
555-7086	→	INTERNAL	5557086
333-3030	→	INTERNAL	3333030
(408) 555-7086	→	LONGDISTANCE	914085557086

5.4. Configure Class of Service

Verify Messaging Waiting is enabled for all subscribers.

Use **Administration → Messaging** menu and select **Class of Service** under **Messaging System (Storage).** Select **"Standard"** from the **Class of Service** drop-down menu.

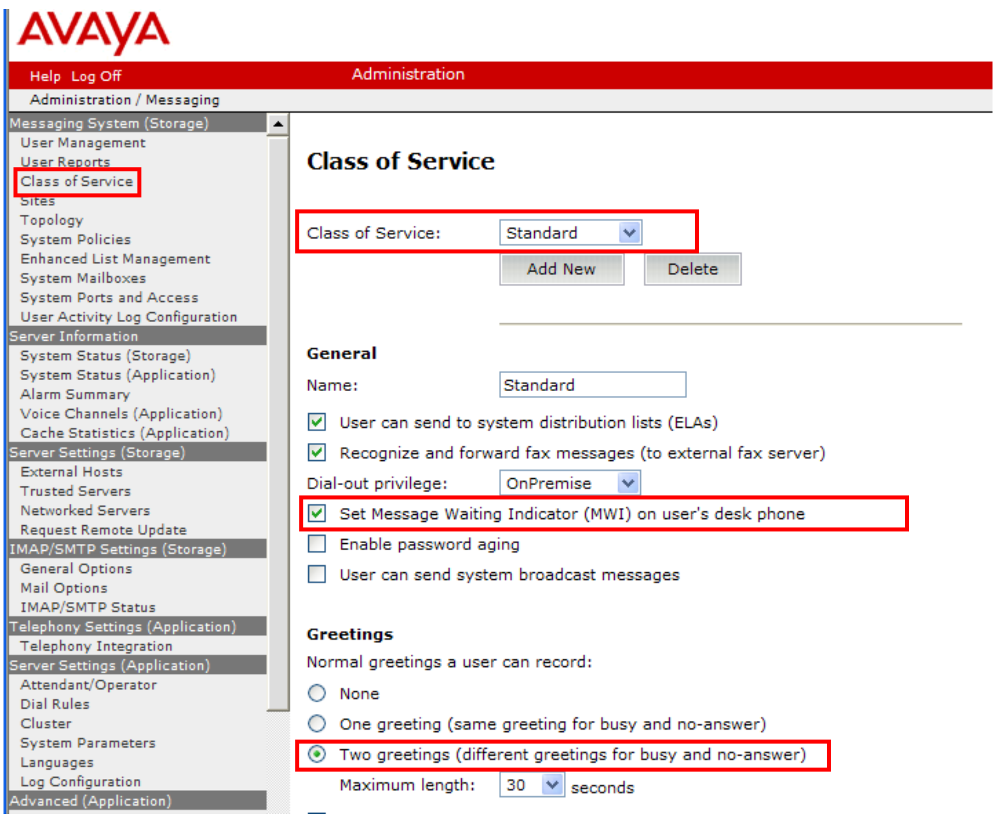
Under **General** section, enter the following value and use default values for remaining fields.

- **Set Message Waiting Indicator (MWI):** Enter

Under **Greetings** section, enter for **Two Greetings (different greetings for busy and no-answer)** field to allow subscribers to record different personal greetings for busy and no-answer scenarios.

Click **Save** (not shown) to save changes.

The following screen shows the settings defined for the "**Standard**" Class of Service in the sample configuration.



5.5. Administer Subscribers

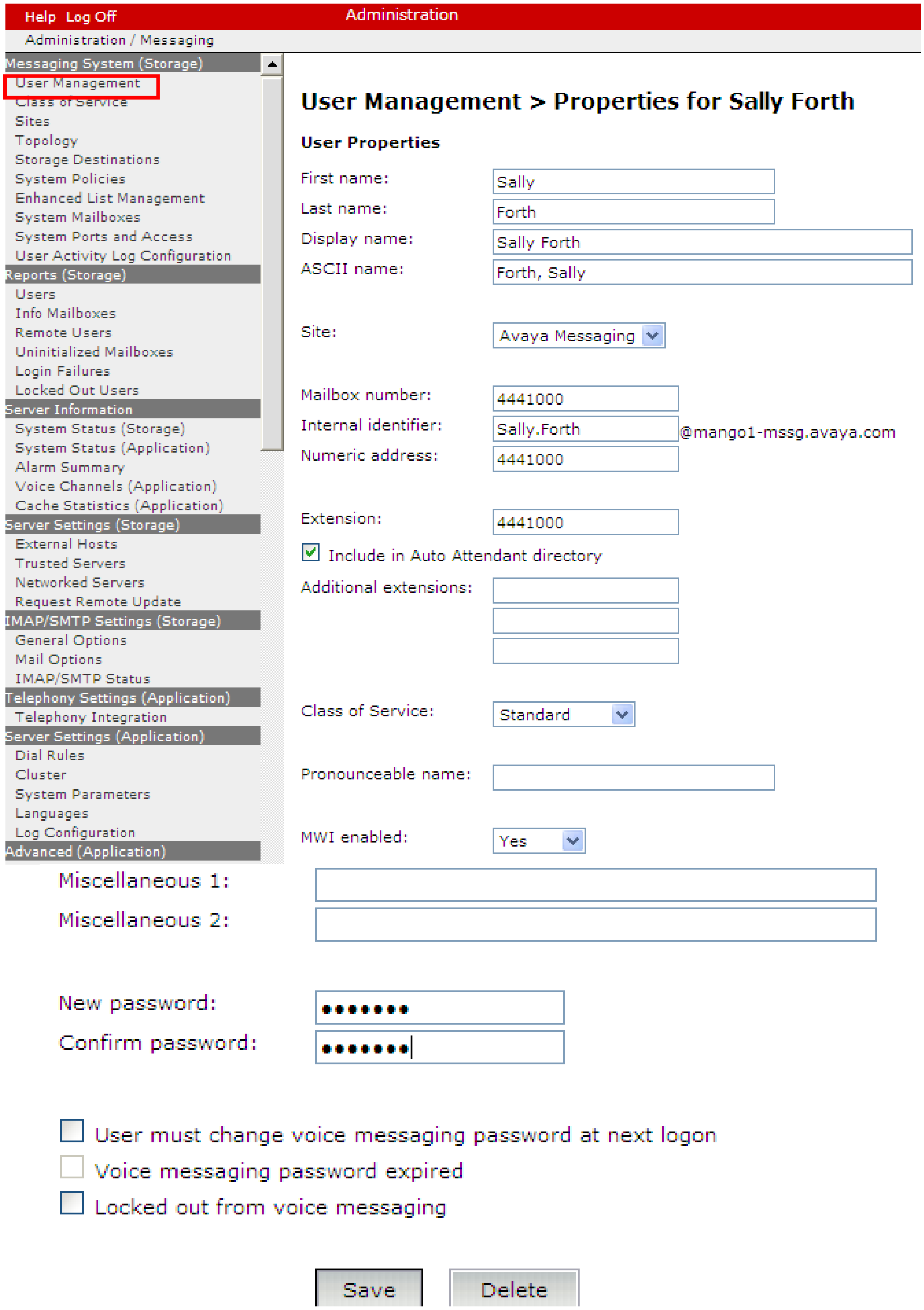
Define a subscriber mailbox for each Communication Manager station.

Use **Administration → Messaging** menu and select **User Management** under **Messaging System (Storage).** Under **Add User/Info Mailbox** section, click **Add** (not shown).

Under **User Properties**, enter the following values and use default values for remaining fields.

- **First Name:** Enter first name of the user
- **Last Name:** Enter last name of the user
- **Display Name:** Enter display name of the user
- **Mailbox Number:** Enter mailbox number corresponding to a station
- **Extension:** Enter dialed number of station
  Enter to include extension in Auto Attendant directory
- **Class of Service:** Select Class of Service defined in **Section 5.4**
- **MWI enabled:** Select "**Yes**"
- **Password:** Enter numeric password

Click **Save.** The following screen shows a new subscriber defined in sample configuration.



6. Verification Steps

6.1. Verify Avaya Aura® Communication Manager Status

Verify the status of the SIP trunk-group and signaling-group by using the **status trunk n** and **status signaling-group n** commands where **n** is the group number being investigated. Verify that all trunks are in the **in-service/idle** state as shown below.

```
status trunk 10                                                   Page   1

                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0010/001 T00001   in-service/active  no
0010/002 T00002   in-service/idle    no
0010/003 T00003   in-service/idle    no
0010/004 T00004   in-service/idle    no
0010/005 T00005   in-service/idle    no
0010/006 T00006   in-service/idle    no
0010/007 T00007   in-service/idle    no
0010/008 T00008   in-service/idle    no
0010/009 T00009   in-service/idle    no
0010/010 T00010   in-service/idle    no
0010/011 T00099   in-service/idle    no
0010/012 T00100   in-service/idle    no
0010/013 T00101   in-service/idle    no
0010/014 T00102   in-service/idle    no
```

For the signaling-group **Group state** should be **in-service** as shown below.

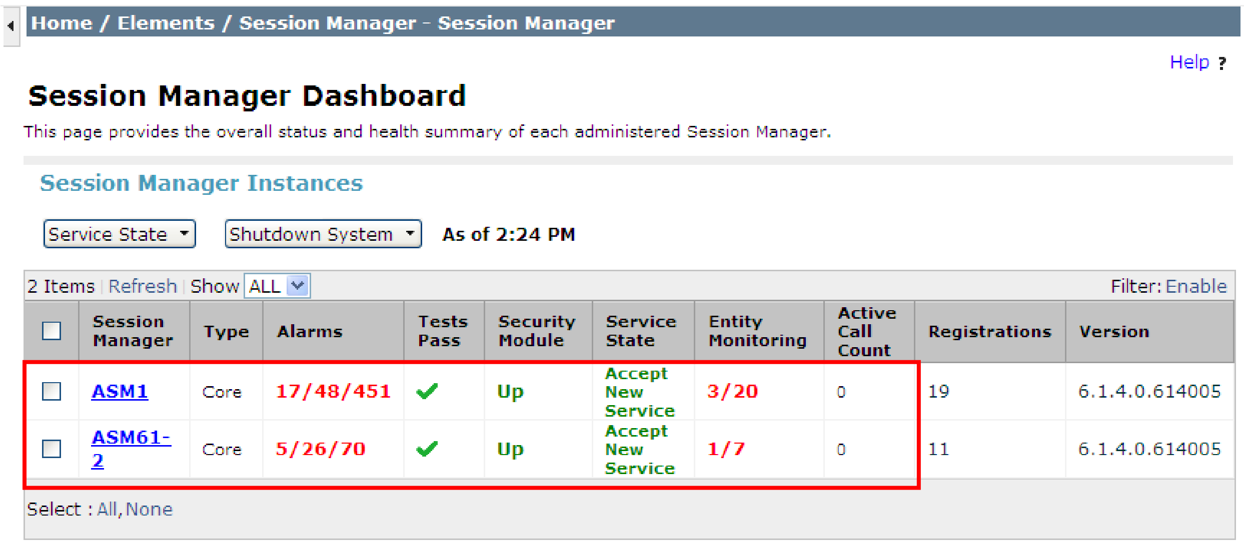
```
status signaling-group 10
                          STATUS SIGNALING GROUP

        Group ID: 10
      Group Type: sip

     Group State: in-service
```

6.2. Verify Avaya Aura® Session Manager Operational Status

Step 1: To verify Session Manager is Operational, navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager.

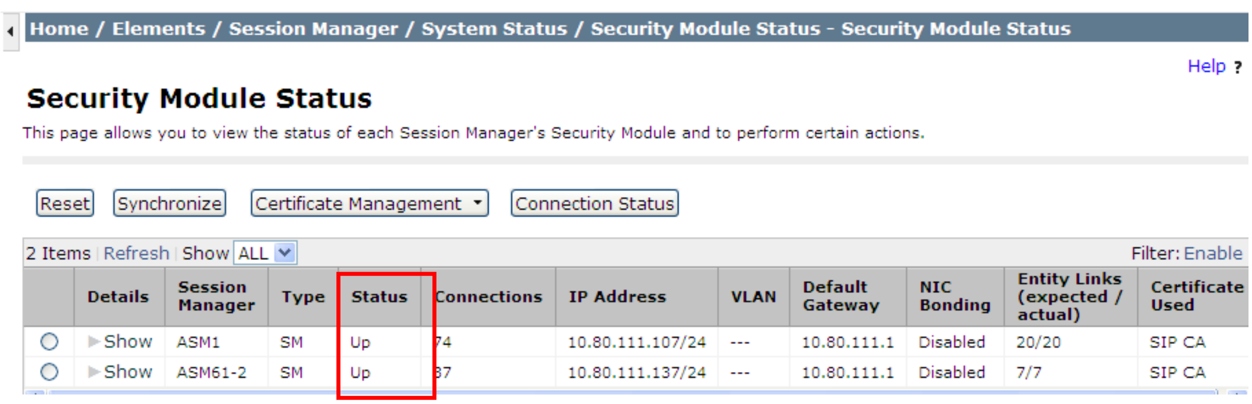
Specifically, verify the status of the following fields for both Session Managers as shown below:

- **Tests Pass** ✔
- **Security Module** Up
- **Service State** Accept New Service



Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
ASM1	Core	17/48/451	✔	Up	Accept New Service	3/20	0	19	6.1.4.0.614005
ASM61-2	Core	5/26/70	✔	Up	Accept New Service	1/7	0	11	6.1.4.0.614005

Step 2: Navigate to **Elements → Session Manager → System Status → Security Module Status** (not shown) to view more detailed information regarding the status of Security Module for Session Manager. Verify the **Status** column displays "**Up**" as shown below.

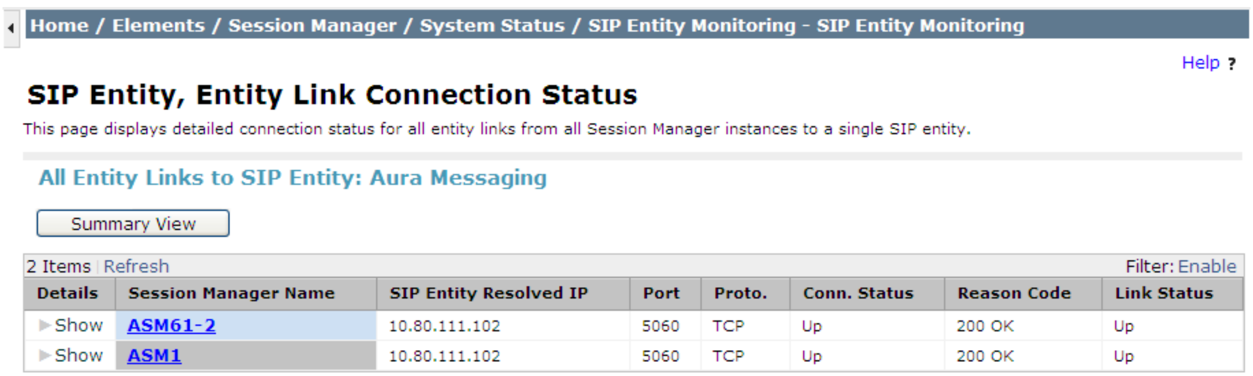


Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
Show	ASM1	SM	Up	74	10.80.111.107/24	---	10.80.111.1	Disabled	20/20	SIP CA
Show	ASM61-2	SM	Up	37	10.80.111.137/24	---	10.80.111.1	Disabled	7/7	SIP CA

Step 3: To verify the status of the SIP Entity Links between Session Manager and either Communication Manager or Avaya Aura® Messaging, navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** (not shown) to view more detailed status information of the SIP Entity Links.

Select the appropriate SIP Entity from the **Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

In the **All Entity Links to SIP Entity: Aura Messaging** table, verify the **Conn. Status** for the link is “**Up**” for both Session Managers as shown below.



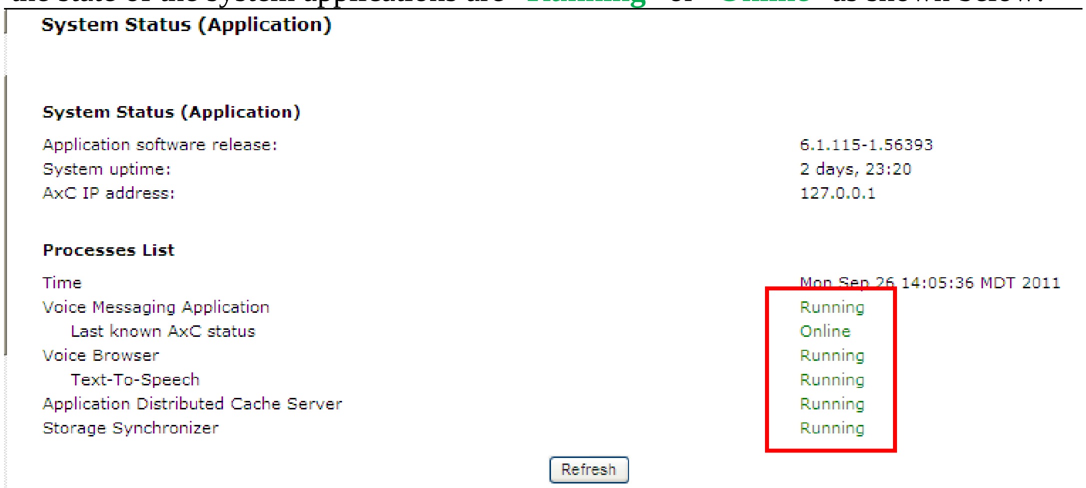
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	ASM61-2	10.80.111.102	5060	TCP	Up	200 OK	Up
▶ Show	ASM1	10.80.111.102	5060	TCP	Up	200 OK	Up

Repeat **Step 3** described above to verify the status of SIP Entity Link between Session Manager and Avaya Aura® Communication Manager.

6.3. Verify Avaya Aura® Messaging Operational Status

Step 1: To verify the overall system is operational, use **Administration → Messaging** menu and select **System Status (Application)** (not shown) under **Server Information.**

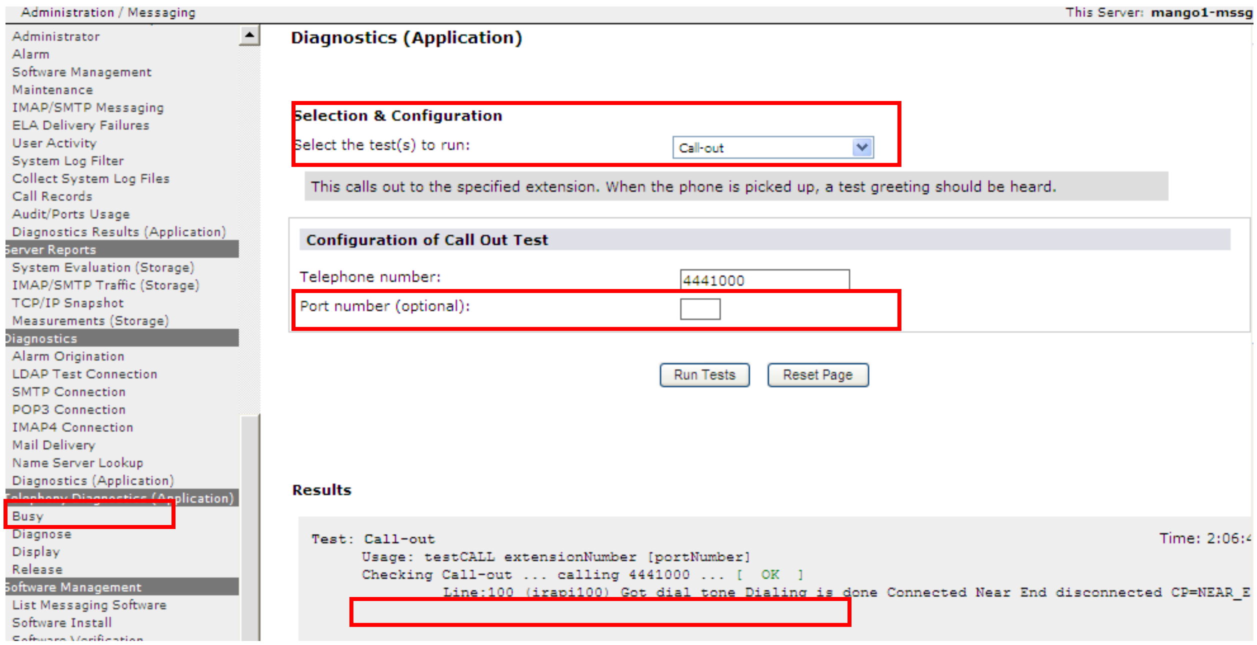
Verify the state of the system applications are "**Running**" or "**Online**" as shown below:



Step 2: To verify connectivity between Avaya Aura® Messaging and Session Manager, use **Administration → Messaging** menu and select **Diagnostics (Application)** (not shown) under **Diagnostics.**

Under **Selection & Configuration** section, select **"Call-out"** and enter an Communication Manager station number in **Telephone number** field. Click **Run Tests.**

As shown in screen below, verify result of Call-out test is "**OK**" in **Results** section.



6.4. Call Scenarios Verified

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

Basic Features:

- Use Pilot Number to access Avaya Aura® Messaging and verify Communication Manager subscribers were properly recognized and could login without entering their mailbox number.
- Verify calls between Communication Manager subscribers were forwarded to the correct Avaya Aura® Messaging mailbox in both No Answer and Busy conditions.
- Verify calls between Communication Manager subscribers were successfully forwarded to Avaya Aura® Messaging and the correct Personal Greetings were played in both No Answer and Busy conditions.
- Verify Communication Manager subscribers could leave voice mail messages for other subscribers.
- Verify Avaya Aura® Messaging sends appropriate Message Waiting Notification (MWI) messages when Communication Manager subscribers leave or retrieve messages.

Supplemental Features:

- Use Auto Attendant Number to access Avaya Aura® Messaging and verify Avaya Aura® Messaging was able to successfully transfer calling party to correct Communication Manager subscriber
- When Reach-Me was activated for a Communication Manager subscriber, verify Avaya Aura® Messaging was able to successfully call the Reach-Me destination. After subscriber accepts call, verify calling party was connected to subscriber.
- Verify Communication Manager subscribers could use Reply, Forward and Call Sender features with other Communication Manager subscribers.

- Verify Avaya Aura® Messaging sends appropriate Message Waiting Notification (MWI) messages when Communication Manager subscribers use Reply or Forward features.
- Verify Communication Manager subscribers were able to create 3-party conferences when call was forwarded or re-directed to Avaya Aura® Messaging.

Long Duration Scenarios

- Verify Communication Manager subscribers could leave long voice mail messages for other subscribers.

6.5. Issues Found

All test calls were successful. The following issues were observed during testing:

- Displays on Communication Manager stations may not be correctly updated when calls were transferred by Avaya Aura® Messaging.

7. Acronyms

DTMF	Dual Tone Multi Frequency
GUI	Graphical User Interface
FQDN	Fully Qualified Domain Name (hostname for Domain Naming Resolution)
IMAP	Internet Message Access Protocol
IP	Internet Protocol
LAN	Local Area Network
MWI	Message Waiting Indicator
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SIL	Solution Interoperability Lab
SIP	Session Initiation Protocol
SM	Avaya Aura® Session Manager
SMGR	System Manager (used to configure Session Manager)
SNMP	Simple Network Management Protocol
SRE	SIP Routing Element
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
WAN	Wide Area Network

8. Conclusion

These Application Notes describe how to configure a sample network that uses SIP trunks between Avaya Aura® Session Manager Release 6.1, Avaya Aura® Communication Manager Feature & Evolution Servers Release 6.0.1, and Avaya Aura® Messaging Release 6.1.

Interoperability testing included verification that calls from several different types of Communication Manager endpoints were successfully forwarded to Avaya Aura® Messaging in both busy and no-answer scenarios and Communication Manager subscribers could use supplemental Avaya Aura® Messaging features such as Auto Attendant and Reach-Me .

9. Additional References

This section provides references to the product documentation relevant to these Application Notes.

Avaya Aura® Session Manager

1) Avaya Aura® Session Manager Overview, Doc ID 03-603323, available at http://support.avaya.com.
2) Installing and Configuring Avaya Aura® Session Manager, available at http://support.avaya.com.
3) Avaya Aura® Session Manager Case Studies, available at http://support.avaya.com
4) Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, available at http://support.avaya.com.
5) Administering Avaya Aura® Session Manager, Doc ID -3-603324, available at http://support.avaya.com

Avaya Aura® Communication Manager

6) Configuring SIP Trunks Among Avaya Aura™ Session Manager 6.0, Avaya Aura™ Communication Manager Feature Server 6.0, Avaya one-X®Deskphone Edition for 9600 Series SIP IP Telephones, and Avaya Communication Server 1000E 6.0, available at http://support.avaya.com
7) Application Notes for Configuring Avaya Desktop Video Device to connect to Avaya Aura® Session Manager with Avaya Aura® Communication Manager as an Evolution Server Issue – Issue 1.0, available at http://support.avaya.com
8) Application Notes for configuring Avaya Desktop Video Device to connect to Avaya Aura® Session Manager with Avaya Aura® Communication Manager as a Feature Server Issue – Issue 1.0, available at http://support.avaya.com

Avaya Aura® Messaging

9) Administering Avaya Aura® Messaging, available at http://support.avaya.com
10) Using Avaya Aura® Messaging, available at http://support.avaya.com
11) Implementing Avaya Aura® Messaging, available at http://support.avaya.com

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