Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura™ Communication Manager 6.0 and Avaya Aura™ Session Manager 6.0 to Allow Interoperability between Avaya Aura™ Conferencing Standard Edition 6.0 using SIP Trunks – Issue 1.0

Abstract

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager to connect Avaya Aura™ Conferencing Standard Edition using SIP trunks.

Testing was conducted at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager to connect Avaya Aura™ Conferencing Standard Edition using SIP trunks. SIP trunks connect Avaya Aura™ Communication Manager and Avaya Aura™ Conferencing Standard Edition to Avaya Aura™ Session Manager. All inter-system calls are carried over these SIP trunks. Avaya Aura™ Session Manager is managed by Avaya Aura™ System Manager via the management network interface. Installation and configuration details can be found in references **[7]**, **[8]**, **[9]**, **[10]** and **[11]**.

Avaya Aura™ Conferencing Standard Edition is a fully integrated audio and data conferencing solution. Avaya Aura™ Conferencing Standard Edition consists of a number of components which provide booking engines, account management utilities, data sharing functionality, billing outputs, directory server integration capabilities, and audio management for all calls. In Avaya Aura™ Conferencing Standard Edition, the media server and the application server reside on a single server. Avaya Aura™ Conferencing Standard Edition is managed by either Avaya Aura™ Conferencing Manager or Avaya Aura™ System Manager, if one already exists. These Application Notes focus on TCP connectivity and alternative methods such as TLS is not covered in these Application Notes. These Application Notes do not describe how to install or license Avaya Aura™ Conferencing Standard Edition. Installation and licensing details can be found in reference **[1]**. Ensure the Avaya Aura™ Conferencing Standard Edition has the latest released patches installed, details can be found in reference **[4]**. Using Avaya Aura™ Conferencing Manager or Avaya Aura™ System Manager the IP addresses of the Conferencing virtual machines need to be specified and connections between the virtual machines need to be established, details can be found in **Chapter 3** of reference **[1]**. These Application Notes do not describe how to schedule a conference by Client Registration Server (CRS) Front End. Installation details can be found in references **[2]** and **[3]** .

The sample configuration shown in **Figure 1** was used to compliance test Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager and Avaya Aura™ Conferencing Standard Edition.

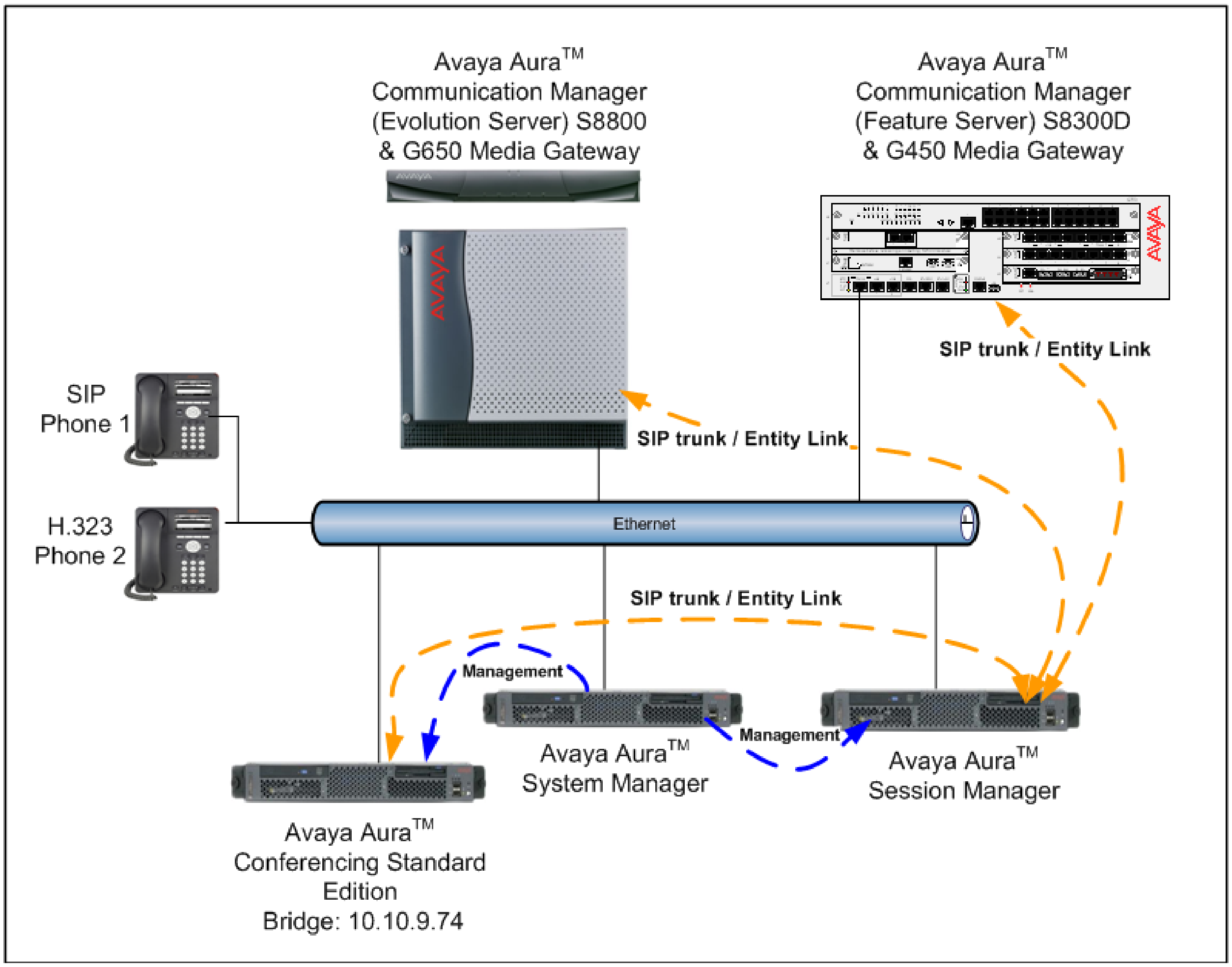


Figure 1 – Test Configuration used in these Application Notes

2. Equipment and Software Validated

The following equipment and software versions were used for the sample configuration provided in these Application Notes.

Equipment	Software
S8800 Server	Avaya Aura™ Communication Manager 6.0 SP 0 (Load 345, Patch 18246)
Avaya G650 Media Gateway - CLAN - TN799DP - MedPro - TN2602AP	 HW01 FW034 HW02 FW049
Avaya S8300D Server	Avaya Aura™ Communication Manager 6.0 SP 0 (Load 345, Patch 18246)
Avaya G450 Media Gateway	Firmware 30.11.3
IBM 3550	Avaya Aura™ Session Manager 6.0, Load 600020
IBM 3550	Avaya Aura™ System Manager 6.0, Load 600020
Avaya Aura™ Conferencing Standard Edition server, IBM 3550	Avaya Aura™ Conferencing Standard Edition Server 6.0.0.0.262 + Release Patches
Avaya 9620 IP Telephone (SIP)	2.5.5.18
Avaya 9630 IP Telephone (H.323)	3.10

Table 1: Hardware and Software Versions

The solution was tested with the GA versions of the products shown in **Table 1**. However, a pre-GA build of System Manager was used to capture screens. Therefore, screen captures shown in these Application Notes may not precisely match the final version of the product. Known differences in screens will be noted in the text accompanying the screen capture.

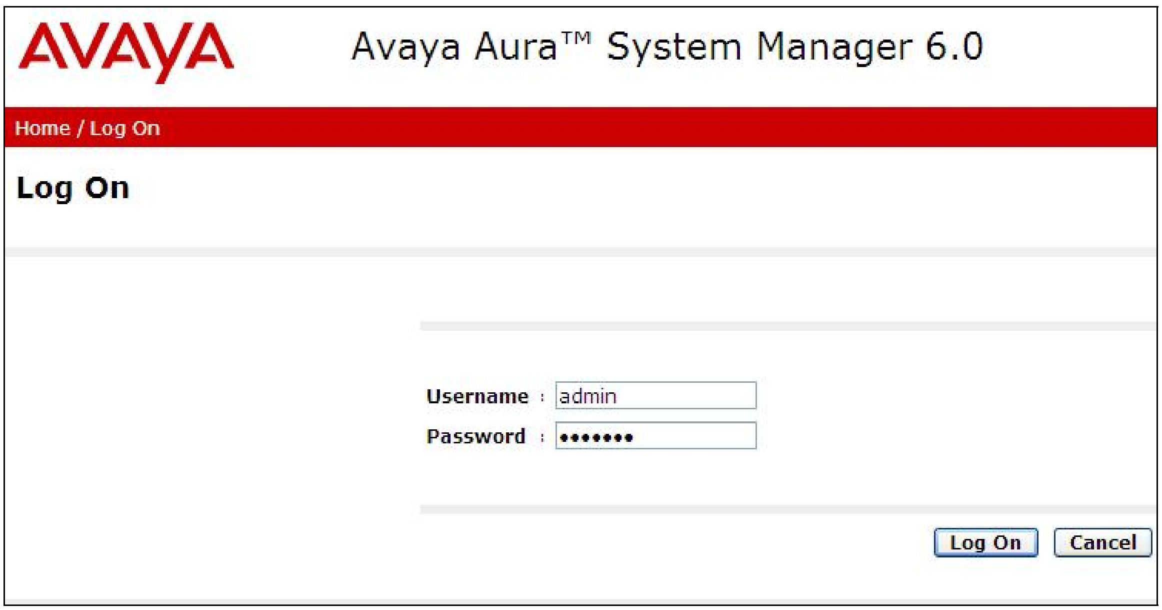
3. Configure Avaya Aura™ Conferencing Standard Edition

This section describes the procedure for configuring the Conferencing Standard Edition to interoperate with Session Manager via SIP trunking. The procedures include the following areas:

- Log in to Avaya Aura™ System Manager
- Configure SIP Connectivity
- Configure Dialout
- Map DNIS Entries

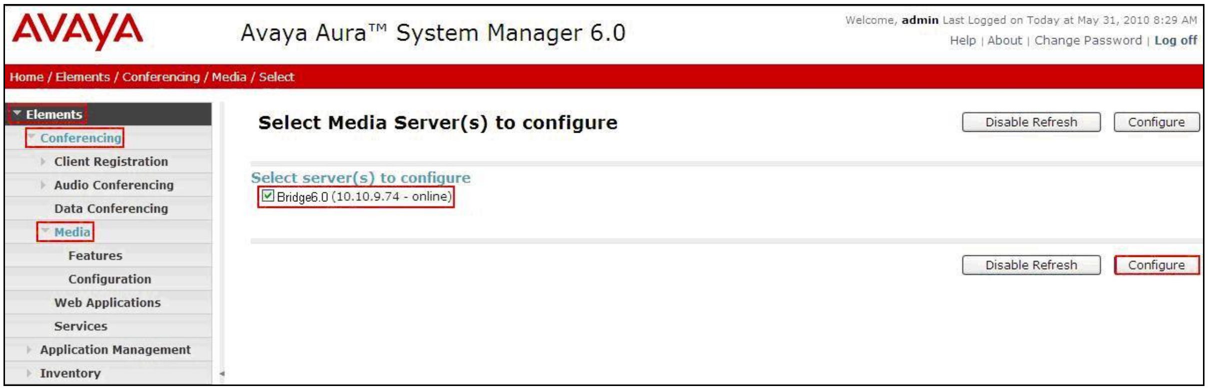
3.1. Log in to Avaya Aura™ System Manager

Access the System Manager using a Web Browser and entering ***https://<ip-address>/smgr***, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials and accept the subsequent Copyright Legal Notice.

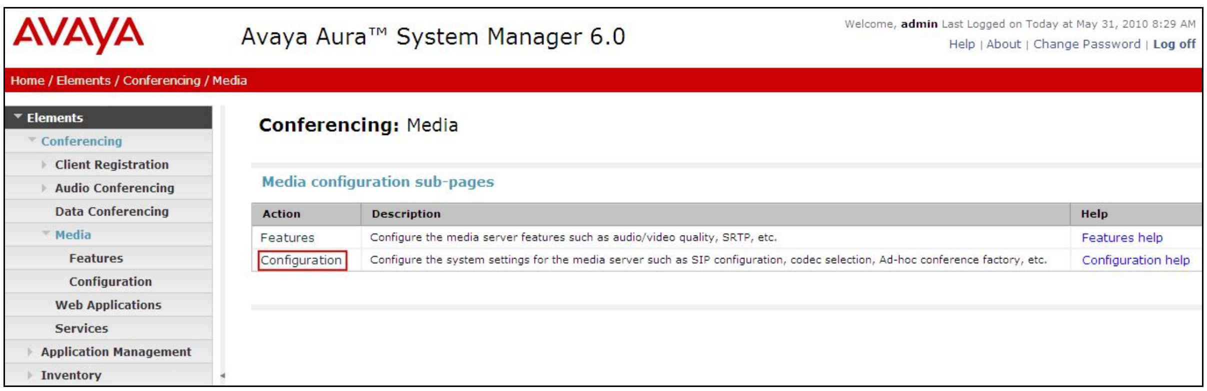


3.2. Configuring SIP Connectivity

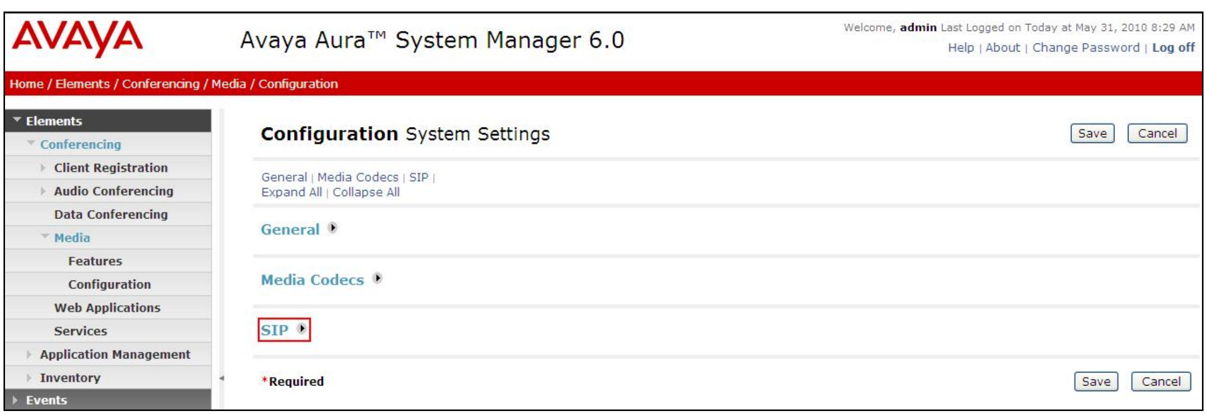
Configure settings that enable SIP connectivity between the Conferencing bridge and other devices by configuring the SIP System Settings. Select **Elements → Conferencing → Media** on the left panel menu. From the right panel menu select the media server to configure by selecting the tick box and select **Configure**.



From the right panel menu select **Configuration**.



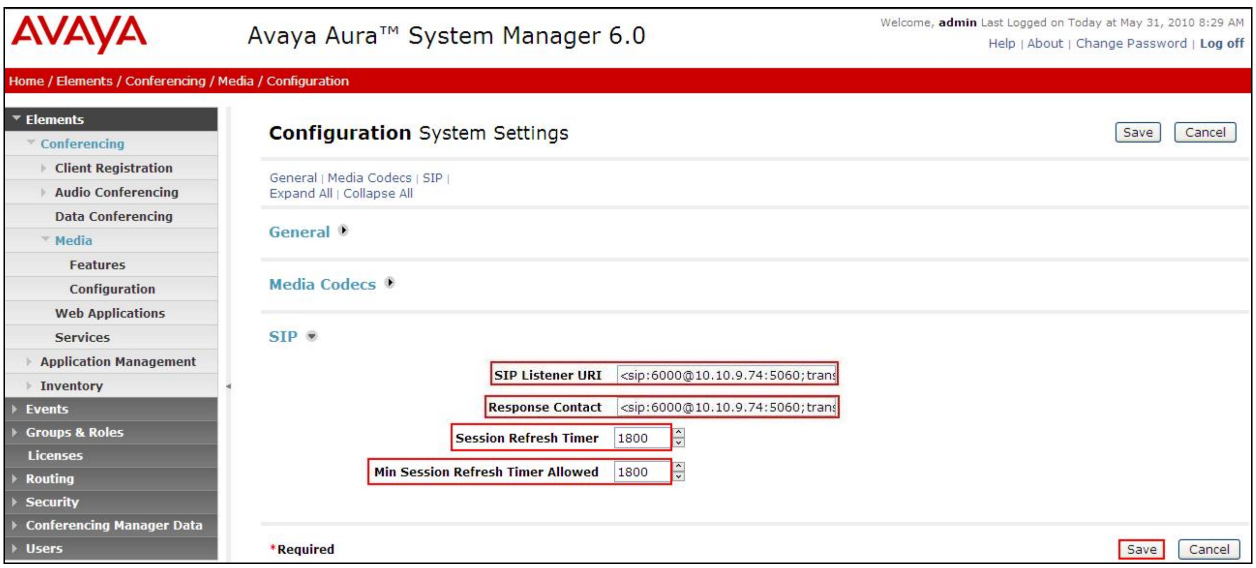
From the right panel menu select **SIP**.



From the **SIP** menu on the right panel menu verify the following options:

- **SIP Listener URI <sip:6000@10.10.9.74:5060;transport=tcp>**
  Depending on the SIP signalling protocol, TCP or UDP, configure the following line to populate the From Header Field in SIP INVITE messages:
  Note: The user field 6000, defined for this SIP URI must conform to RFC 3261. For consistency, it is selected to match the user field provisioned for the **Response Contact** entry (see below).
- **Response Contact <sip:6000@10.10.9.74:5060;transport=tcp>**
  Depending on the SIP signalling protocol, TCP or UDP, configure the following line to provide SIP Device Contact address to use for acknowledging SIP messages from the Conferencing Standard Edition:
- **Session Refresh Timer 1800**
- **Min Session Refresh Timer Allowed 1800**

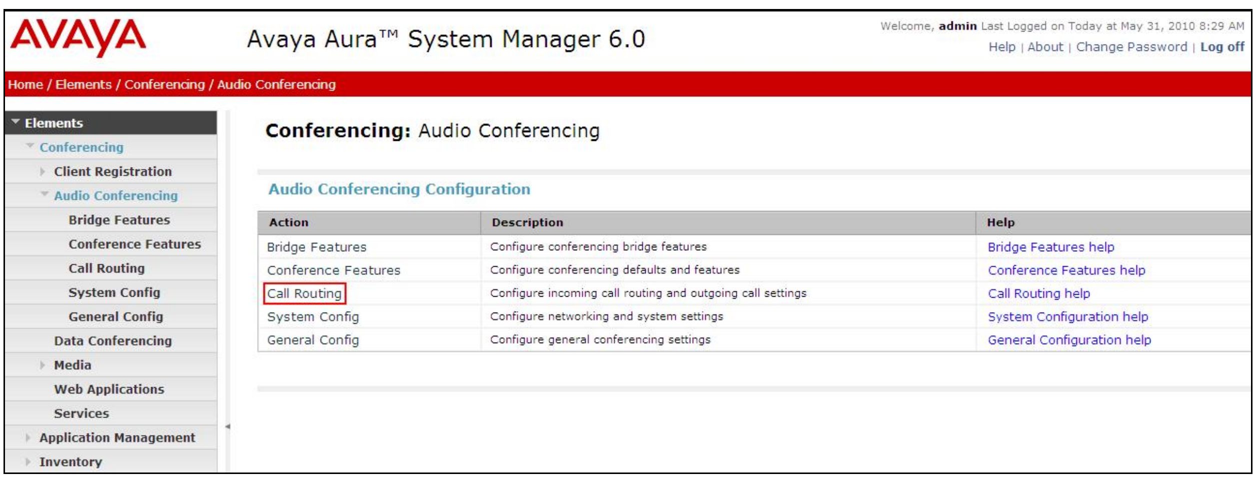
Click the **Save** button.



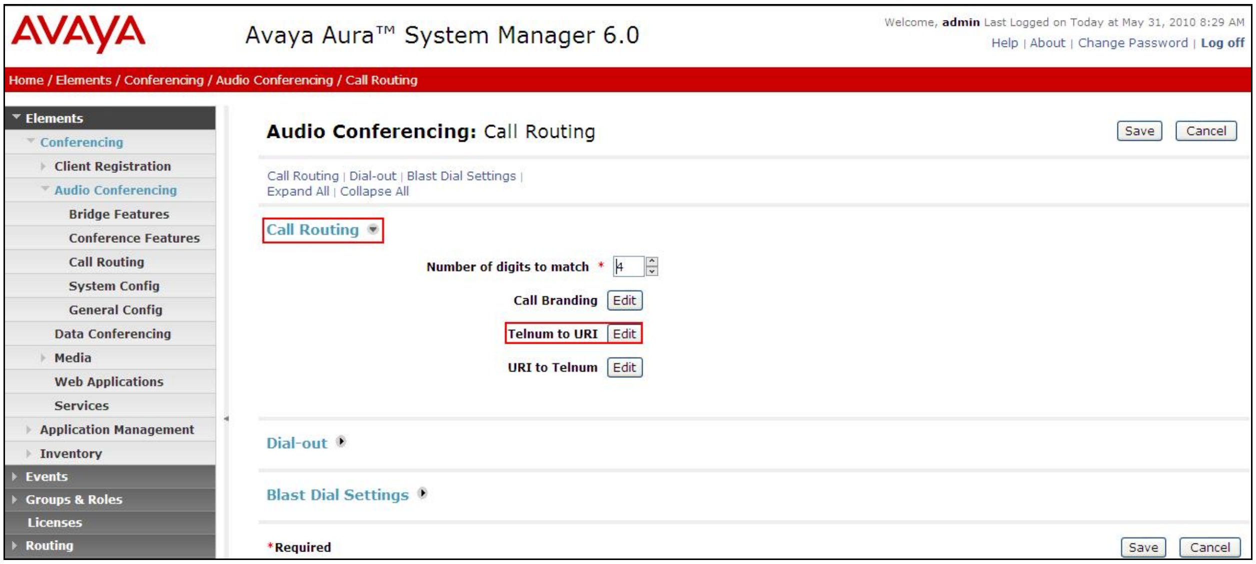
3.3. Configure Dialout

To enable Dial-Out from the Conferencing to the Session Manager, configure the **telnumToUri** by selecting **Elements → Conferencing → Audio Conferencing** on the left panel menu. From the right panel menu select the conferencing server to configure by selecting the tick box and select **Configure**.

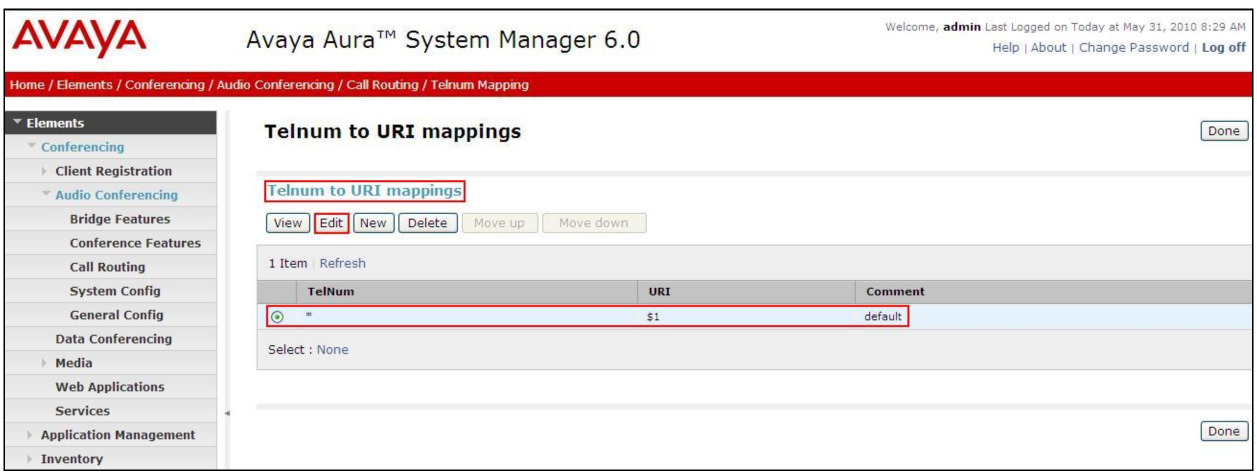
From the right panel menu select **Call Routing**.



From the **Call Routing** menu on the right panel menu select the **Edit** button for **Telnum to URI** option.



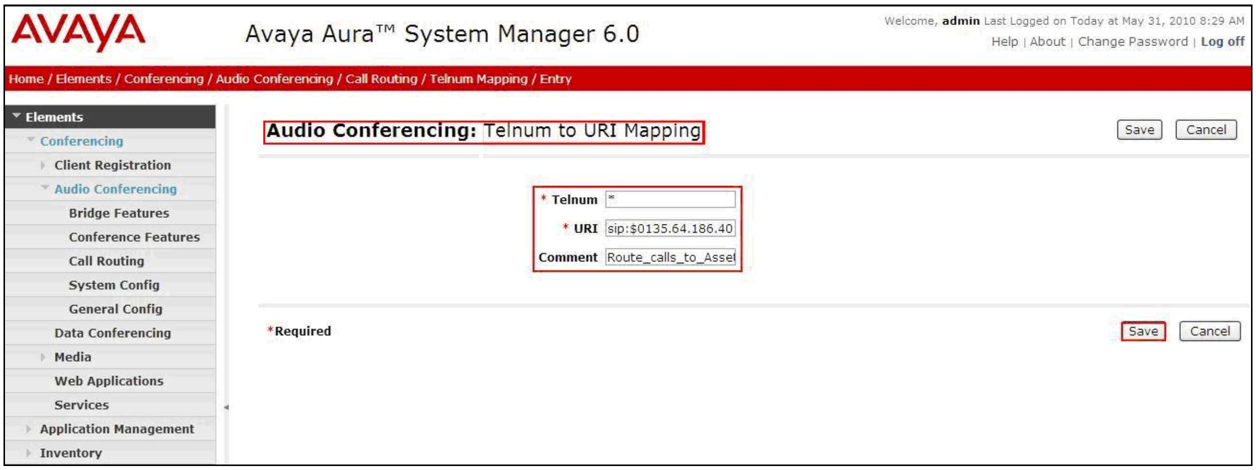
From the right panel menu select the default **Telnum to URI mappings** and select **Edit**.



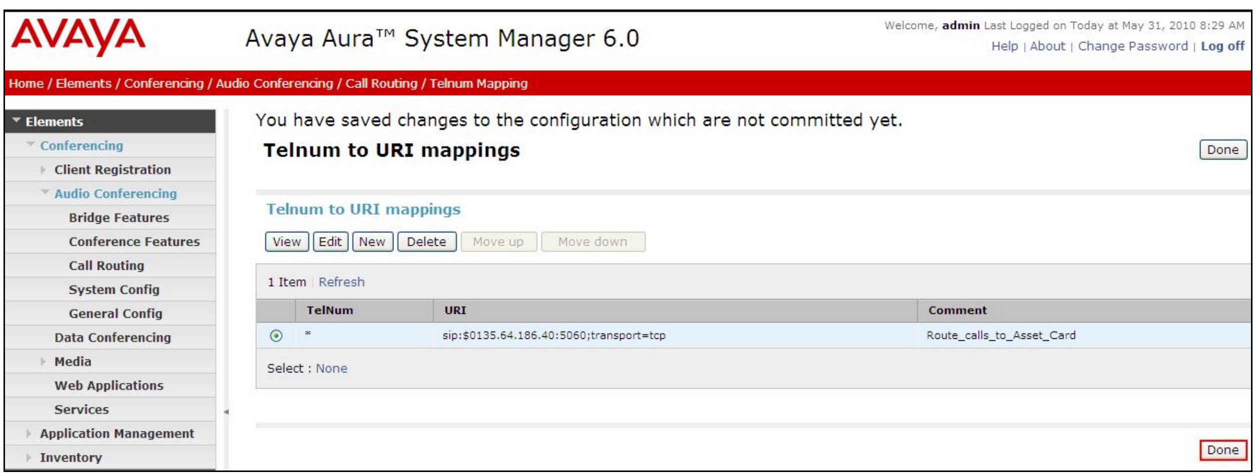
From the right panel menu complete the following options; under **Audio Conferencing: Telnum to URI Mapping**.

- **Telnum** *****
- **URI** **sip:$0@135.64.186.40:5060;transport=tcp**
  To route outbound calls from the Conferencing bridge to the Session Manager.
- **Comment** A descriptive comment

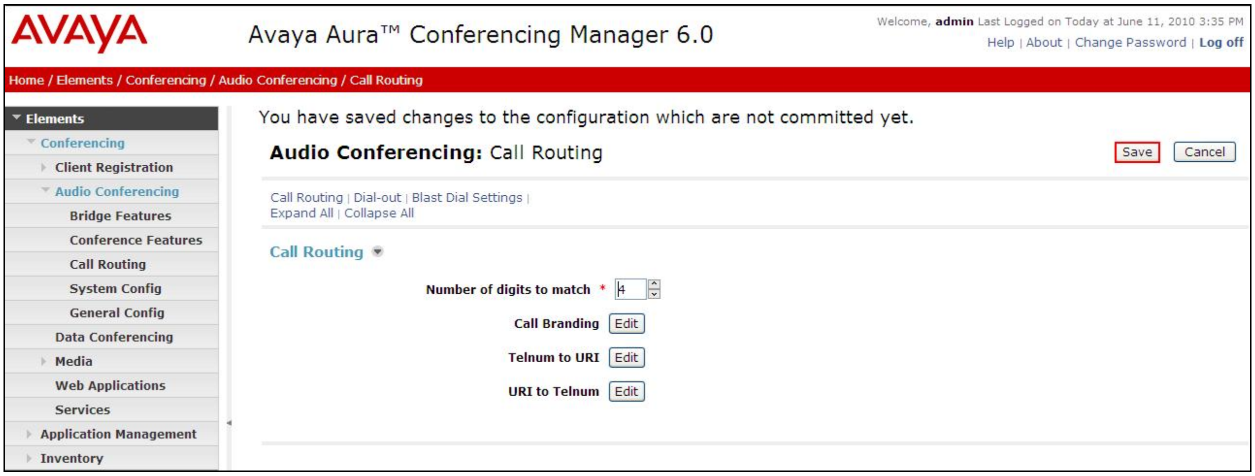
Click the **Save** button.



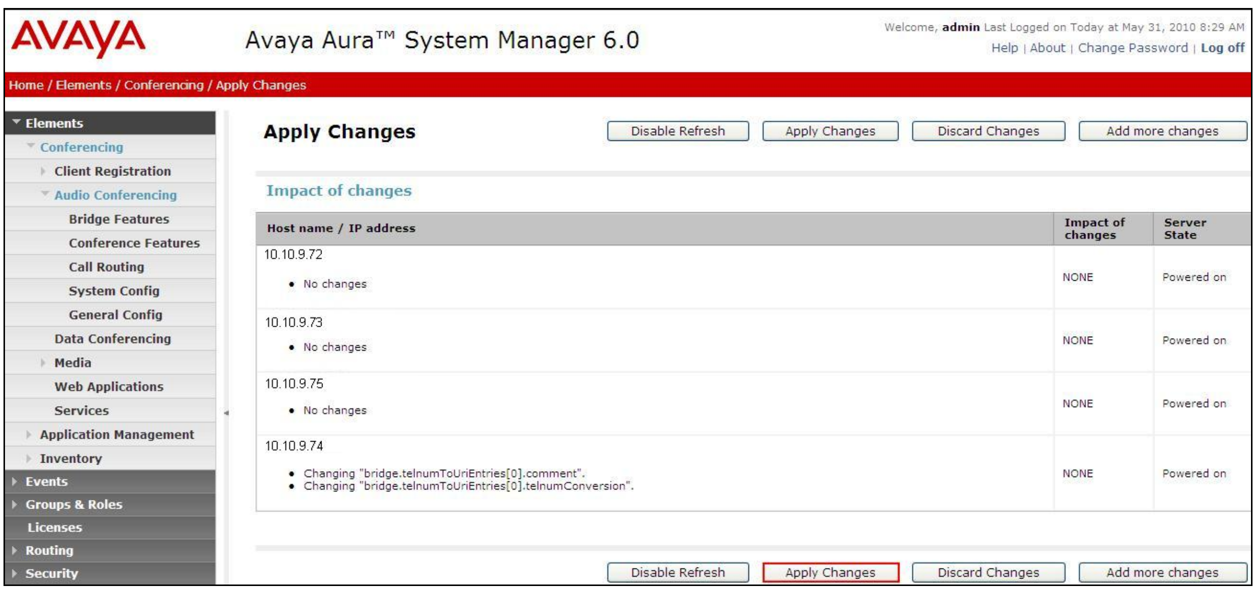
From the right panel menu select **Done**.



From the right panel menu select **Save**.



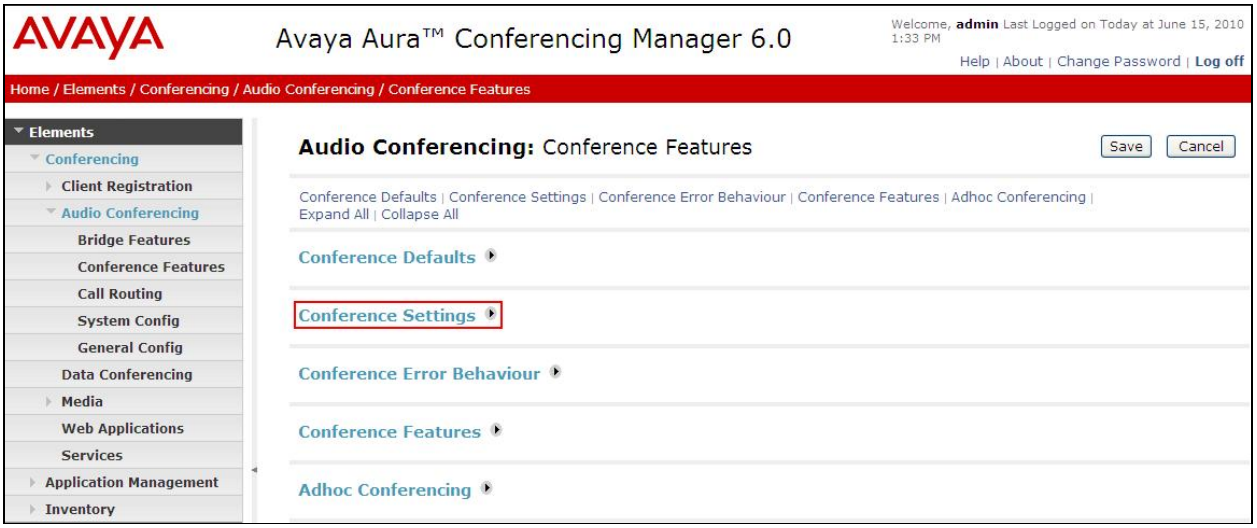
From the right panel menu select **Apply Changes**.



To enable Dial-Out from the Conferencing bridge to the Session Manager, configure the **Originator Dial Out** by selecting **Elements → Conferencing → Audio Conferencing** on the left panel menu. From the right panel menu select the conferencing server to configure by selecting the tick box and select **Configure**.

From the right panel menu select **Conference Features**.

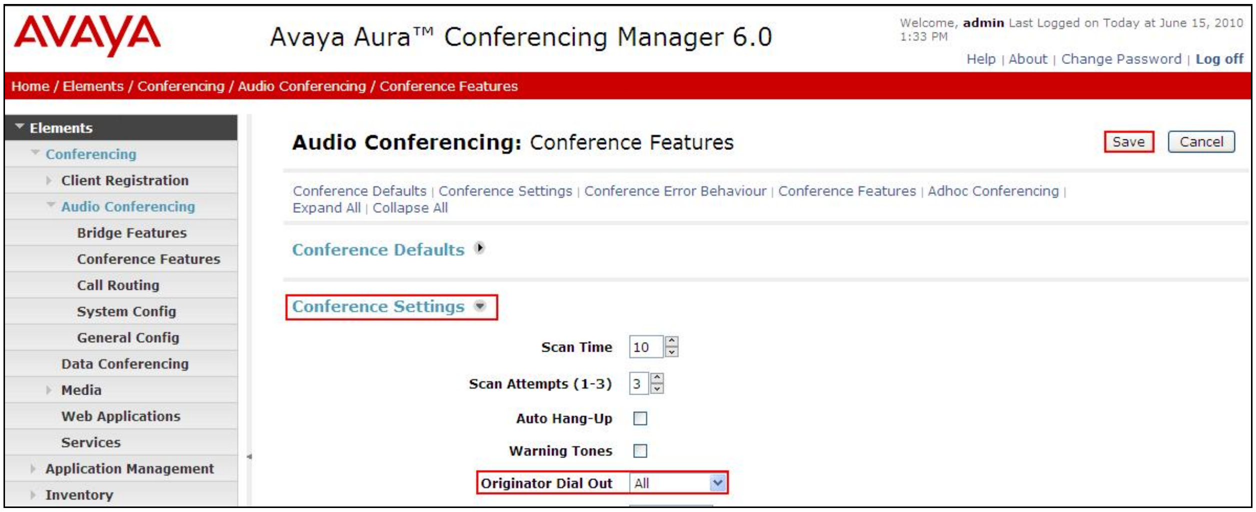
From the right panel menu select **Conference Settings**.



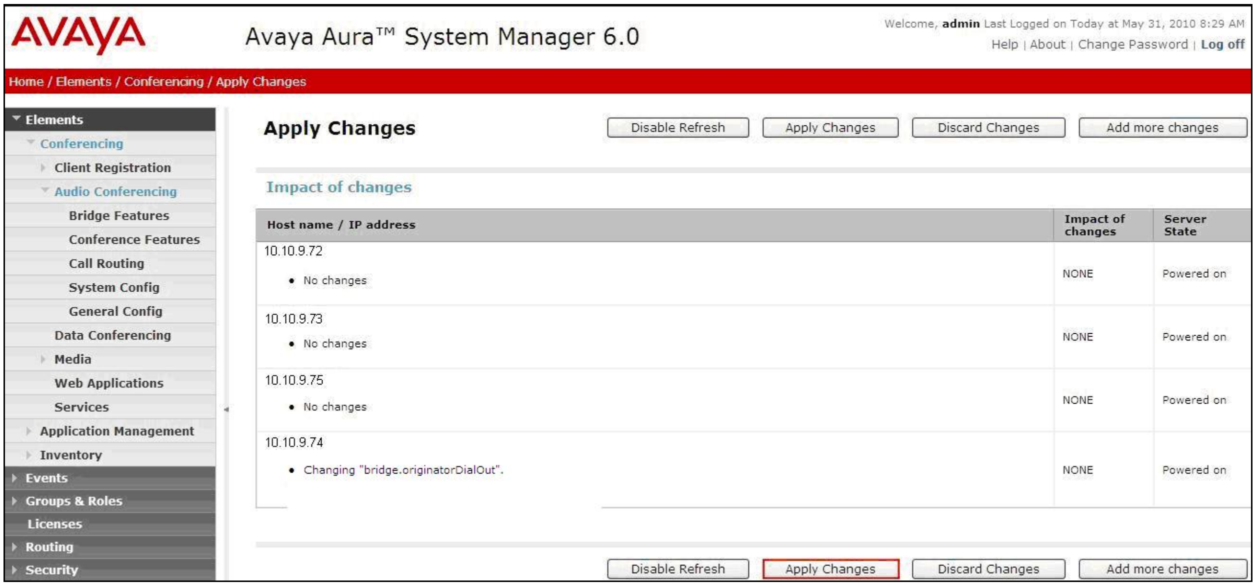
From the **Conference Settings** drop down menu on the right panel menu select the following parameter, leaving the remaining parameters at their default values.

- **Originator Dial Out** Select **All**

Click the **Save** button.



From the right panel menu select **Apply Changes**.

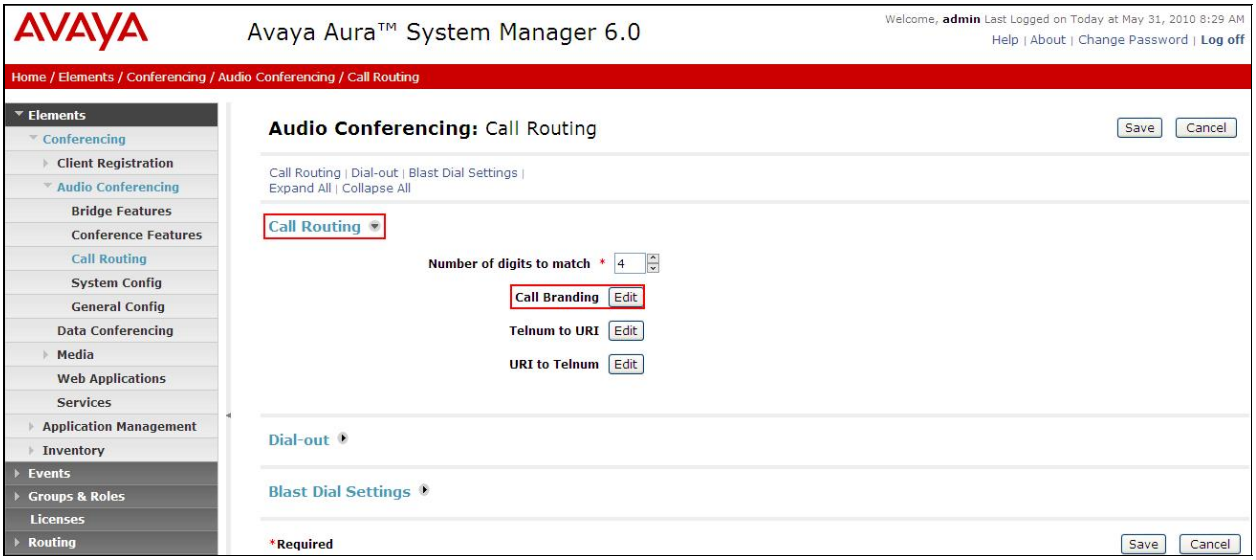


3.4. Map DNIS Entries

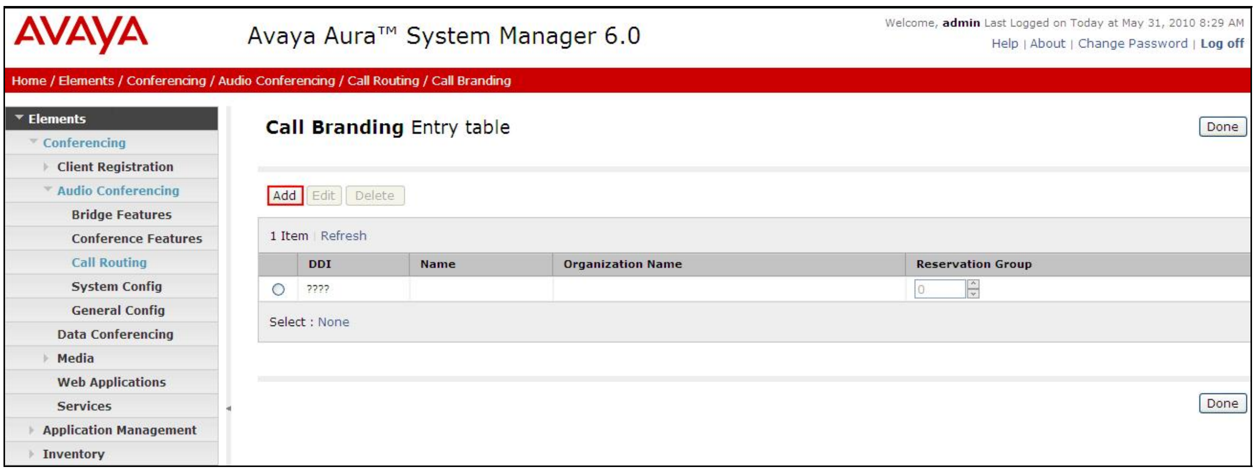
To map DNIS entries, run the Call Branding utility by selecting **Elements → Conferencing → Audio Conferencing** on the left panel menu. From the right panel menu select the conferencing server to configure by selecting the tick box and select **Configure**.

From the right panel menu select **Call Routing**.

From the **Call Routing** menu on the right pane select the **Edit** button for **Call Branding** option.



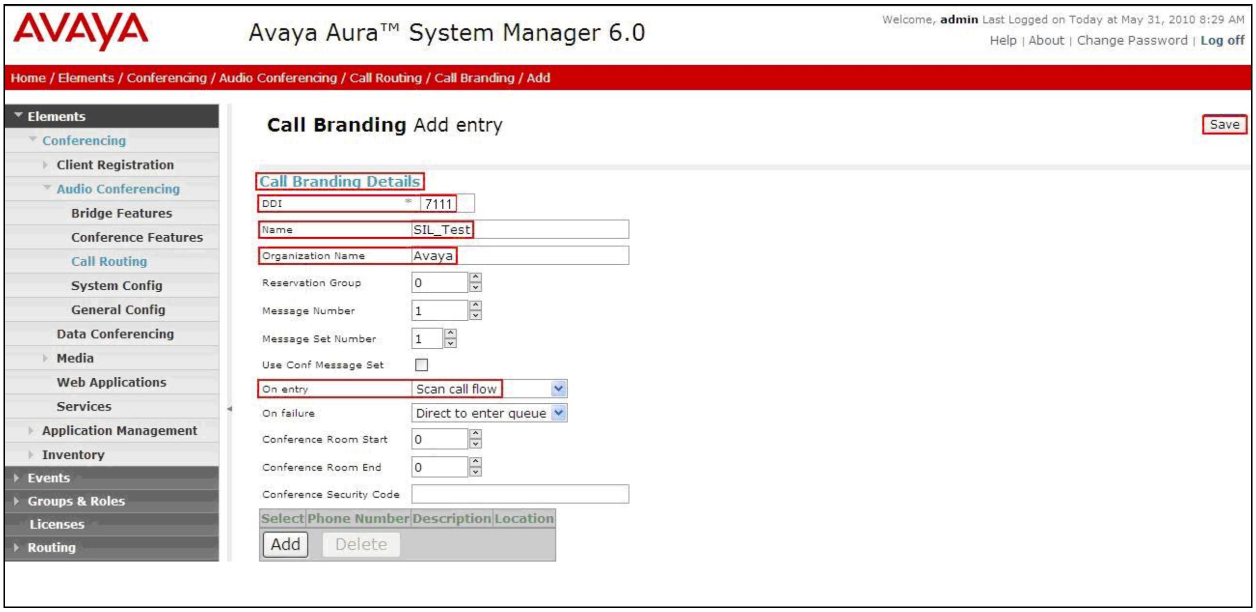
From the right panel menu select the **Add** button to create a new call branding entry.



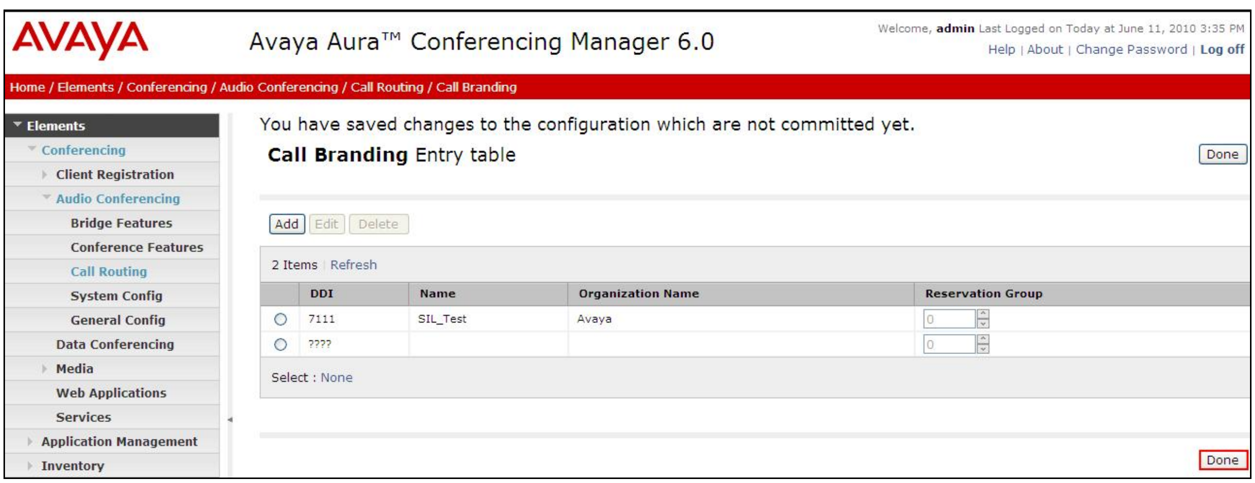
In this sample configuration for **Call Branding Details** select the following parameters, leaving the remaining parameters at their default values.
Under **Call Branding Details**

- **DDI** **7111**
- **Name** A descriptive name
- **Organization Name** A descriptive name
- **On Entry** Select **Scan call flow** from the drop down menu.

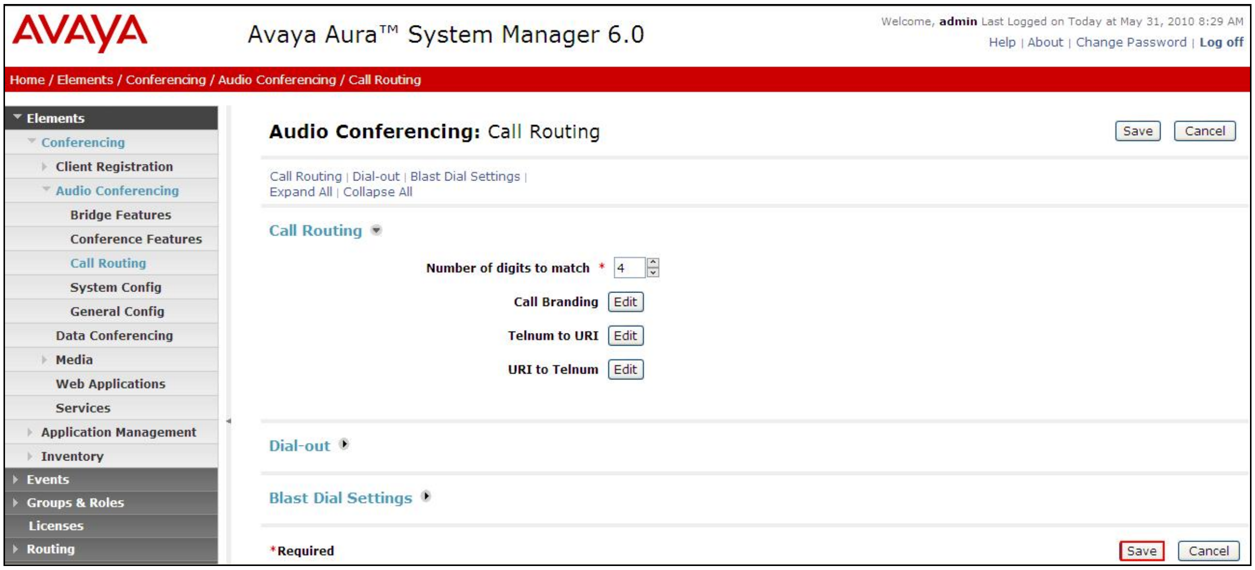
Click the **Save** button.



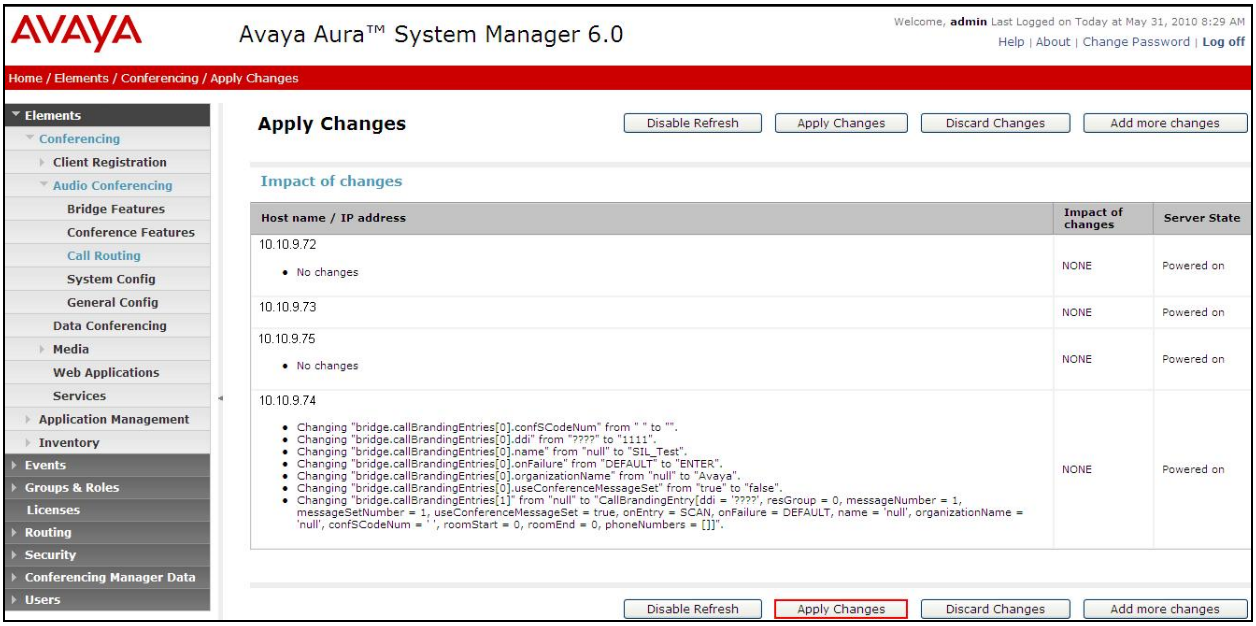
From the right panel menu select **Done**.



From the right panel menu select **Save**.



From the right panel menu select **Apply Changes**.



4. Configure Avaya Aura^{TM} Communication Manager as Evolution Server

This section describes the steps for configuring the Communication Manager as an Evolution Server. All configurations in the section are administered using the System Access Terminal (SAT). These Application Notes assume that the basic Communication Manager configuration has already been administered. The procedures include the following areas:

- Confirm Necessary Features
- Administer IP Node Names
- Administer IP Network Region
- Administer IP Codec Set
- Administer SIP Signaling Group
- Administer SIP Trunk Group
- Administer Private Numbering
- Administer Route patterns
- Administer Uniform Dialplan
- Administer AAR
- Save Translations

Throughout this section the administration of Communication Manager is performed using a System Access Terminal (SAT). The following commands are entered on the system with the appropriate administrative permissions. Some administration screens have been abbreviated for clarity. These instructions assume that the Communication Manager has been installed, configured, licensed and provided with a functional dial plan. Refer to the appropriate documentation as described in reference **[5]** for more details**.**

4.1. Confirm Necessary Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Log into the Communication Manager SAT interface and use the **display system-parameters customer-options** command to determine these values. On **Page 2** verify that the available **Maximum Administered SIP Trunks** is equal to or greater than the desired number of simultaneous SIP trunk connections.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 7
             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 1
                   Maximum Video Capable IP Softphones: 18000 1
                       Maximum Administered SIP Trunks: 24000 30
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   1
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

On **Page 4** verify the field **IP Trunks** is set to **y**.

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                                IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                          ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                            ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                   ISDN-PRI? y
              ESS Administration? y                 Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                       Malicious Call Trace? y
     External Device Alarm Admin? y                   Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                   Multifrequency Signaling? y
      Global Call Classification? y           Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y        Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y                 Multimedia IP SIP Trunking? y
                       IP Trunks? y
           IP Attendant Consoles? y
```

4.2. Administer IP Node Names

Use the **change node-names ip** command to add entries for the Communication Manager and Session Manager that will be used for connectivity. In the sample network, **clan1a3** and **135.64.186.6** are entered as **Name** and **IP Address** for the CLAN card in Communication Manager running on the Avaya S8800 Server. In addition, **SessionM1** and **135.64.186.40** are entered for Session Manager.

```
 change node-names ip
                                  IP NODE NAMES
    Name                IP Address
clan1a3               135.64.186.6
GatewaySub3           135.64.186.65
mpro1a2               135.64.186.8
mpro1b2               135.64.186.9
SessionM1             135.64.186.40
procr                 135.64.186.70
```

4.3. Administer IP Network Region

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 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. See the following section.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: silstack.com
    Name: Dublin
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
```

4.4. Administer IP Codec Sets

Use the **change ip-codec-set n** command, where **n** is the codec set specified in the **IP Network Region** form. Enter the codecs eligible to be used; the codecs defined here must be supported by the far end device.

```
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.711MU           n         2        20
 2: G.711A            n         2        20
 3:
 4:
 5:
```

4.5. Administer SIP Signaling Group

Use the **add signaling-group n** command, where **n** is the number of the SIP signaling-group to create. Set the **Group Type** field to be **sip** and **Transport Method** to **tcp**. Use the values defined in **Section 4.2** and **4.3** for **Near-end Node Name**, **Far-End Node-Name** and **Far-End Network Region**. The **Far-end Domain** is left blank so that the signaling group accepts any authoritative domain.

```
add signaling-group 120                                       Page   1 of   1
                                SIGNALING GROUP

 Group Number: 120           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: SM


   Near-end Node Name: clan1a3              Far-end Node Name: SessionM1
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 1

Far-end Domain:
                                              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? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

4.6. Administer 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 120. Set the **Group Type** field to be **sip**.

```
add trunk-group 120                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 120                  Group Type: sip           CDR Reports: y
  Group Name: TO ASM                      COR: 1        TN: 1        TAC: 120
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 120
                                                     Number of Members: 20
```

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

```
add trunk-group 120                                              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
```

4.7. Administer Private Numbering

Use the **change private-numbering** command to define the calling party number to be sent out through the SIP trunk. All calls originating from a **5**-digit extension beginning with **2** will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  2                120                         5     Total Administered: 1
                                                       Maximum Entries: 540
```

4.8. Administer Route Patterns

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 specified in **Section 4.10**. Configure this route pattern to route calls to trunk group number **120** configured in **Section 4.6**. Assign the lowest **FRL** (facility restriction level) to allow all callers to use this route pattern.

```
change route-pattern 120                                              Page   1 of   3
                    Pattern Number: 120   Pattern Name: To ASM
                             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: 120 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
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

4.9. Administer Uniform Dialplan

Use the **change uniform-dialplan n** command to administer the uniform dialplan. In this configuration extension **7111** is configured as **aar** to send calls via the aar analysis table.

```
change uniform-dialplan 7                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                   Insert               Node
  Pattern       Len Del      Digits     Net Conv Num
 7111           4   0                  aar  n
```

4.10. Administer AAR

Use the **change aar analysis n** command to specify which route pattern to use based upon the number dialed. In this example, **Route Pattern 120** is used for extension **7111**.

```
change aar analysis 7                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all           Percent Full:    1

Dialed           Total     Route    Call   Node  ANI
String          Min  Max  Pattern   Type   Num   Reqd
7111             4    4     120      aar          n
```

4.11. Save Translations

Configuration of Communication Manager is complete. Use the **save translation** command to save these changes.

5. Configure Avaya Aura^{TM} Communication Manager as Feature Server

This section describes the steps for configuring the Communication Manager as a Feature Server. All configurations in the section are administered using the System Access Terminal (SAT). These Application Notes assume that the basic Communication Manager configuration has already been administered. The procedures include the following areas:

- Administer IP Node Names
- Administer IP Network Region
- Administer IP Codec Set
- Administer SIP Signaling Group
- Administer SIP Trunk Group
- Administer Private Numbering
- Administer Route patterns
- Administer Uniform Dialplan
- Administer AAR
- Save Translations

Throughout this section the administration of Communication Manager is performed using a System Access Terminal (SAT). The following commands are entered on the system with the appropriate administrative permissions. Some administration screens have been abbreviated for clarity. These instructions assume that the Communication Manager has been installed, configured, licensed and provided with a functional dial plan. Refer to the appropriate documentation as described in reference **[5]** and **[6]** for more details**.**

5.1. Administer IP Node Names

Use the **change node-names ip** command to add entries for the Session Manager that will be used for connectivity. In addition, **SM** and **135.64.186.40** are entered for Session Manager. Also note the IP Address of the **procr** and **135.64.186.55** as this will be used to configure the SIP signaling group.

```
change node-names ip
                                  IP NODE NAMES
    Name              IP Address
SILStackAES         135.64.186.28
SM                  135.64.186.40
default             0.0.0.0
fs-acm              135.64.186.55
procr               135.64.186.55
```

5.2. Administer IP Network Region

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 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. See the following section.

```
change ip-network-region 1                                          Page   1 of  20
                               IP NETWORK REGION
 Region: 1
Location: 1       Authoritative Domain: silstack.com
    Name: To ASM
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
```

5.3. Administer IP codec sets

Use the **change ip-codec-set n** command, where **n** is the codec set specified in the IP Network Region form. Enter the codecs eligible to be used. The codecs defined here must be supported by the far end device.

```
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.711MU           n         2        20
 2: G.711A            n         2        20
 3:
 4:
 5:
```

5.4. Administer SIP Signaling Group

Use the **add signaling-group n** command, where **n** is the number of the SIP signaling-group to create. Set the **Group Type** field to be **sip** and **Transport Method** to **tcp**. Set the **IMS Enabled** field to **y**. Use the values defined in **Section 5.2** and **5.3** for **Near-end Node Name**, **Far-End Node-Name** and **Far-End Network Region**. The **Far-end Domain** is left blank so that the signaling group accepts any authoritative domain.

```
add signaling-group 150                                         Page   1 of   1
                                SIGNALING GROUP

 Group Number: 150             Group Type: sip
  IMS Enabled? y        Transport Method: tcp
        Q-SIP? n                                              SIP Enabled LSP? n
     IP Video? n
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                Far-end Node Name: SM
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 1
Far-end Domain:

                                            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? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

5.5. Administer 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 150. Set the **Group Type** field to be **sip**.

```
add trunk-group 150                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 150                   Group Type: sip          CDR Reports: y
  Group Name: To ASM SM100            COR: 1        TN: 1        TAC: 150
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 150
                                                     Number of Members: 10
```

On **Page 3** of the trunk-group form set the **Numbering Format** field to **private**.

```
add trunk-group 150                                          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

 DSN Term? n
```

5.6. Administer Private Number

Use the **change private-numbering** command to define the calling party number to be sent out through the SIP trunk. All calls originating from a **5**-digit extension beginning with **4** will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  4                150                         5     Total Administered: 1
                                                       Maximum Entries: 540
```

5.7. Administer Route Patterns

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 specified in **Section 5.8**. Configure this route pattern to route calls to trunk group number **150** configured in **Section 5.5**. Assign the lowest **FRL** (facility restriction level) to allow all callers to use this route pattern.

```
change route-pattern 150                                              Page   1 of   3
                    Pattern Number: 150   Pattern Name: FeatureCM
                             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: 150  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
 5: y y y y y n  n            rest                                            none
 6: y y y y y n  n            rest                                            none
```

5.8. Administer Uniform Dialplan

Use the **change uniform-dialplan n** command to administer the uniform dialplan. In this configuration extension **7111** is configured as **aar** to send calls via the aar analysis table.

```
change uniform-dialplan 7                                          Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                                 Percent Full: 0

  Matching                   Insert               Node
  Pattern        Len Del     Digits     Net Conv  Num
 7111            4   0                  aar  n
```

5.9. Administer AAR

Use the **change aar analysis n** command to specify which route pattern to use based upon the number dialed. In this example, **Route Pattern 150** is used for extension **7111**.

```
change aar analysis 7                                              Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all              Percent Full:    1

Dialed           Total     Route     Call   Node   ANI
String          Min  Max  Pattern    Type   Num    Reqd
7111             4    4     150       aar           n
```

5.10. Save Translations

Configuration of Communication Manager is complete. Use the **save translation** command to save these changes.

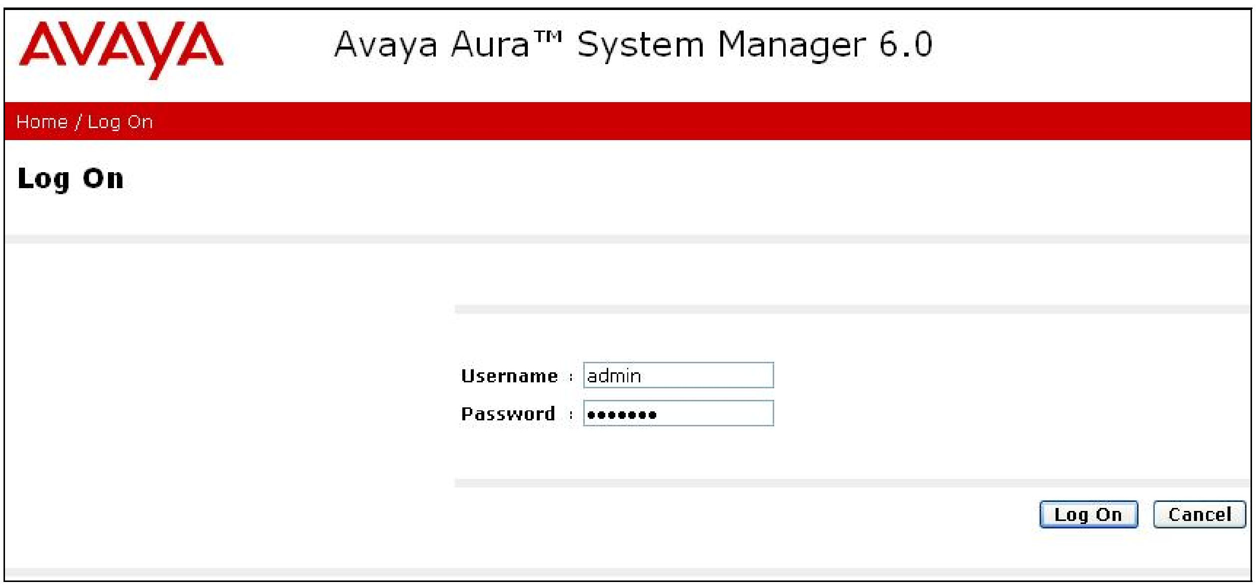
6. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured via the System Manager. The procedures include the following areas:

- Log in to Avaya Aura™ System Manager
- Administer SIP domain
- Administer SIP Entities
- Administer Entity Links
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns
- Administer Session Manager

6.1. Log in to Avaya Aura™ System 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 and accept the subsequent Copyright Legal Notice.

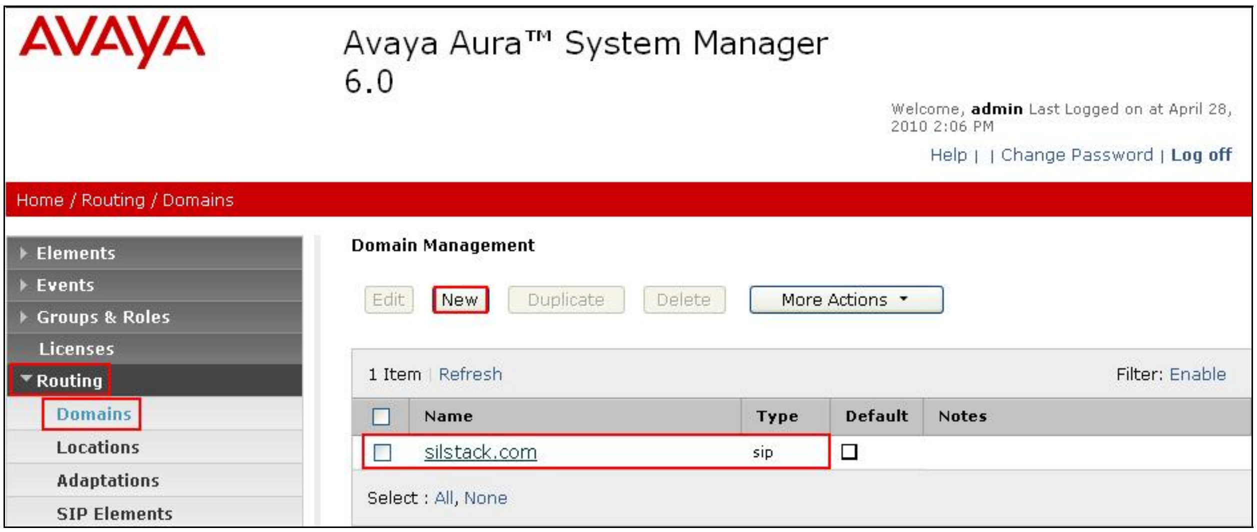


6.2. Administer Domains

Add the SIP authoritative domain for the communications infrastructure by selecting **Routing → Domains** on the left panel menu and click **New** to create a new domain entry. Select the following parameters, leaving the remaining parameters at their default values.

- **Name** The authoritative domain name (e.g., **silstack.com**)
- **Type** Select **sip**
- **Notes** Description for the domain (optional)

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



6.3. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management. Location is added to the configuration for both Communication Manager and Conferencing Standard Edition. To add a location, select **Routing → Locations** on the left panel menu and click **New** (not shown). Select the following parameters, leaving the remaining parameters at their default values.

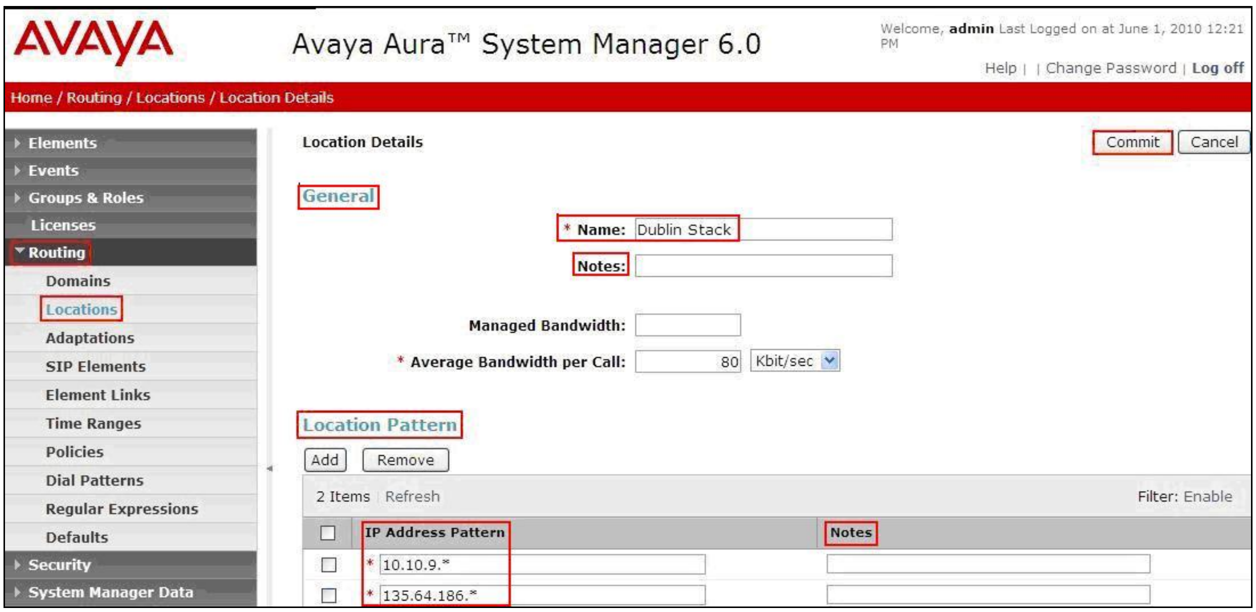
Under **General**:

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

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location
- **Notes:** Descriptive text (optional)

Click **Commit** to save changes.

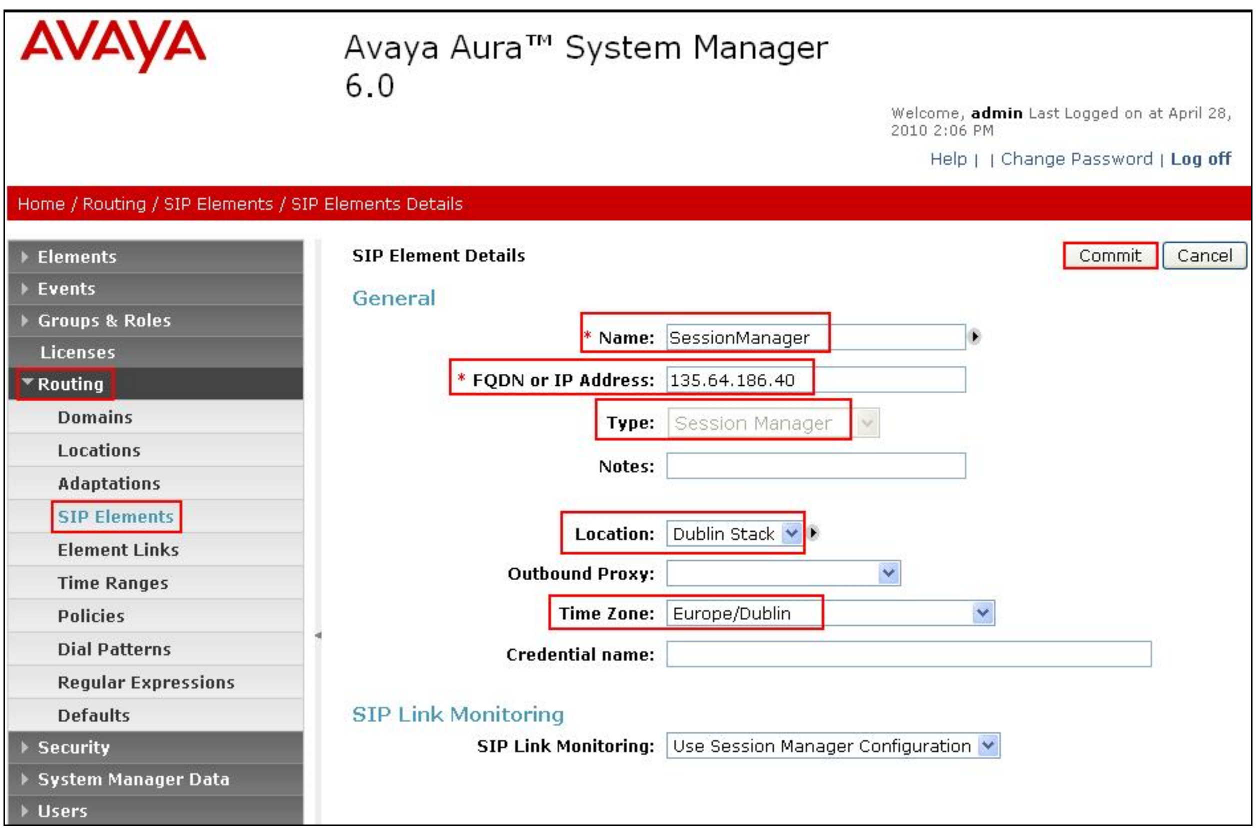


6.4. Add SIP Elements

Note that the “SIP Elements” menu option shown in the screen below was changed to “SIP Entities” in the GA release. For the purposes of these Application Notes, the terms “Element” and “Entity” are interchangeable. SIP Elements must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration a SIP Entity is added for the Session Manager, the C-LAN board in the Avaya G650 Media Gateway, the procr in the Avaya G450 Media Gateway and the Conferencing bridge. To add a SIP Element, select **Routing → SIP Element** on the left panel menu and click **New** (not shown). Select the following parameters, leaving the remaining parameters at their default values.
Under **General**:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the ASM or the signaling interface on the telephony system.
- **Type:** Select between **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for Conferencing server
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

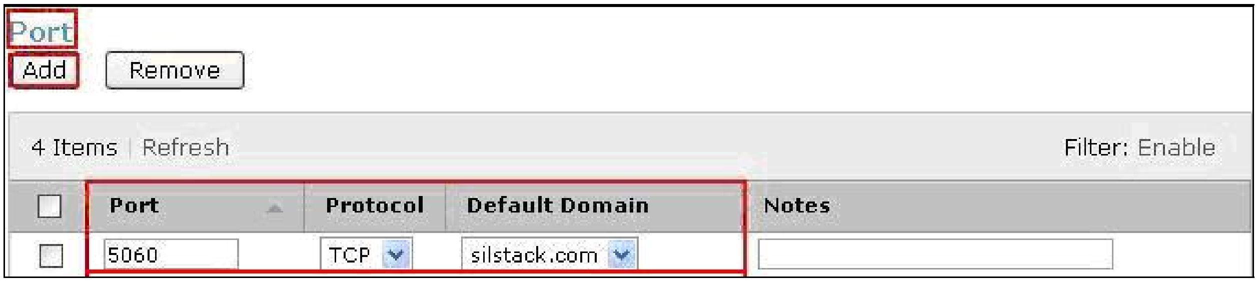
The following screen shows addition of Session Manager. The IP address used is that of the Session Manager’s SIP routing interface.



Under **Port**, click **Add**, select the following parameters, leaving the remaining parameters at their default values. Note that the adding of ports only applies when the SIP Element is a Session Manager.

- **Port** Port number on which the system listens for SIP requests.
- **Protocol** Transport protocol used to listen to SIP requests.
- **Default Domain** The domain used for the enterprise (e.g., **silstack.com**).

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

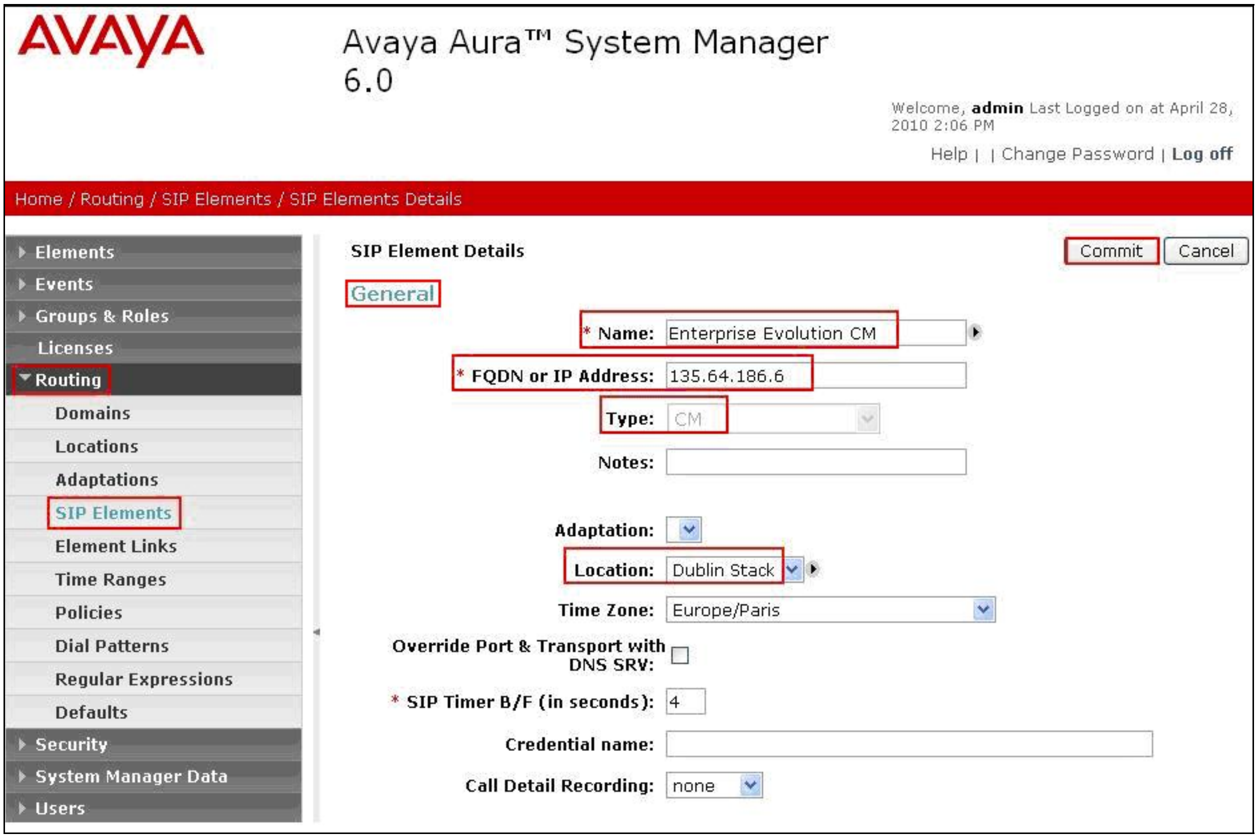


The following screen shows addition of Evolution Server. Select the following parameters, leaving the remaining parameters at their default values.

Under **General**:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the C-LAN board.
- **Type:** Select **CM**
- **Location:** Select one of the locations defined previously.

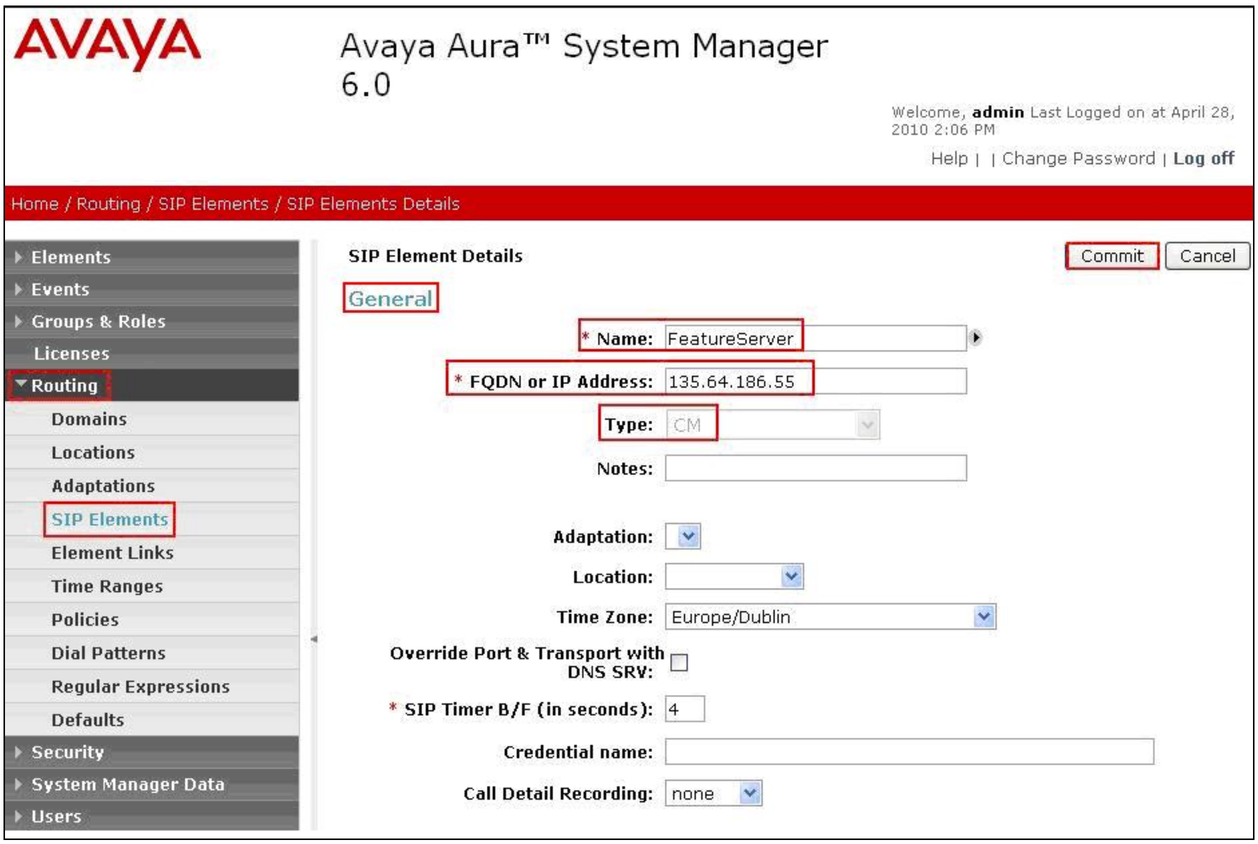
Click **Commit** to save changes.



The following screen shows addition of Feature Server. Select the following parameters, leaving the remaining parameters at their default values.
Under **General**:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the procr
- **Type:** Select **CM**
- **Location:** Select one of the locations defined previously.

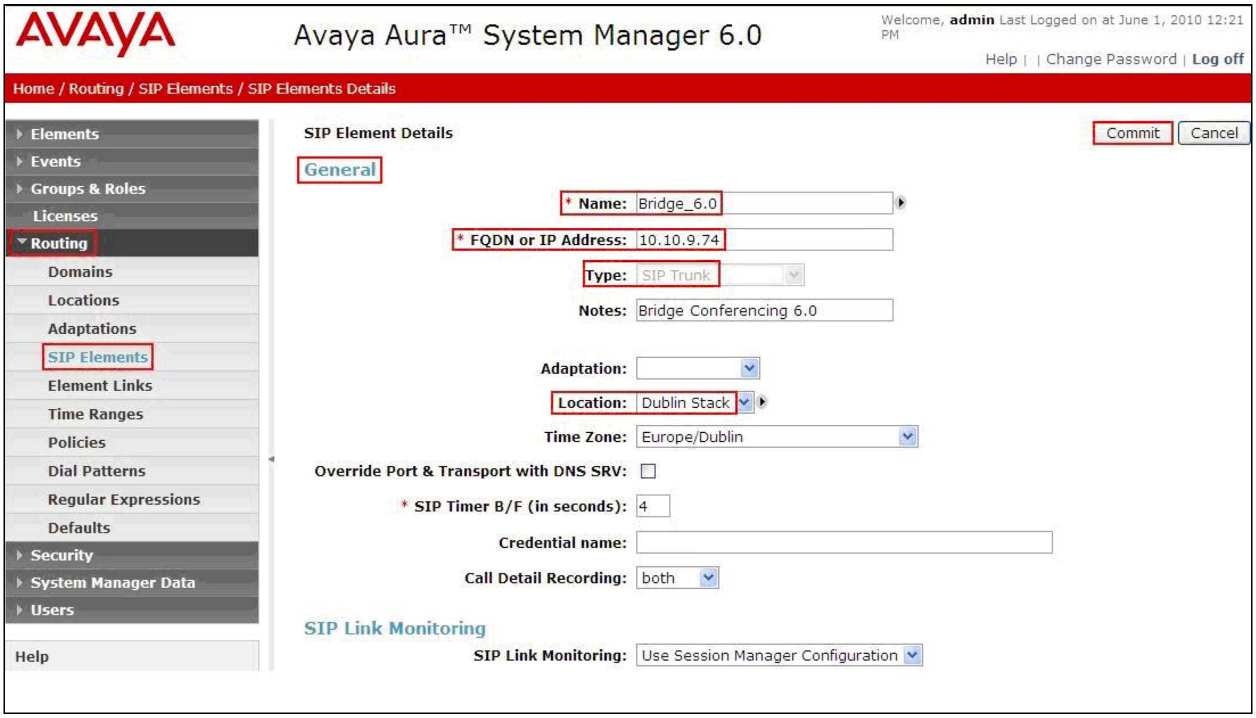
Click **Commit** to save changes.



The following screen shows addition of Conferencing Standard Edition (**Bridge_6.0**). Select the following parameters, leaving the remaining parameters at their default values.
Under **General**:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the Conferencing Bridge
- **Type:** Select **SIP Trunk**
- **Location:** Select one of the locations defined previously.

Click **Commit** to save changes.

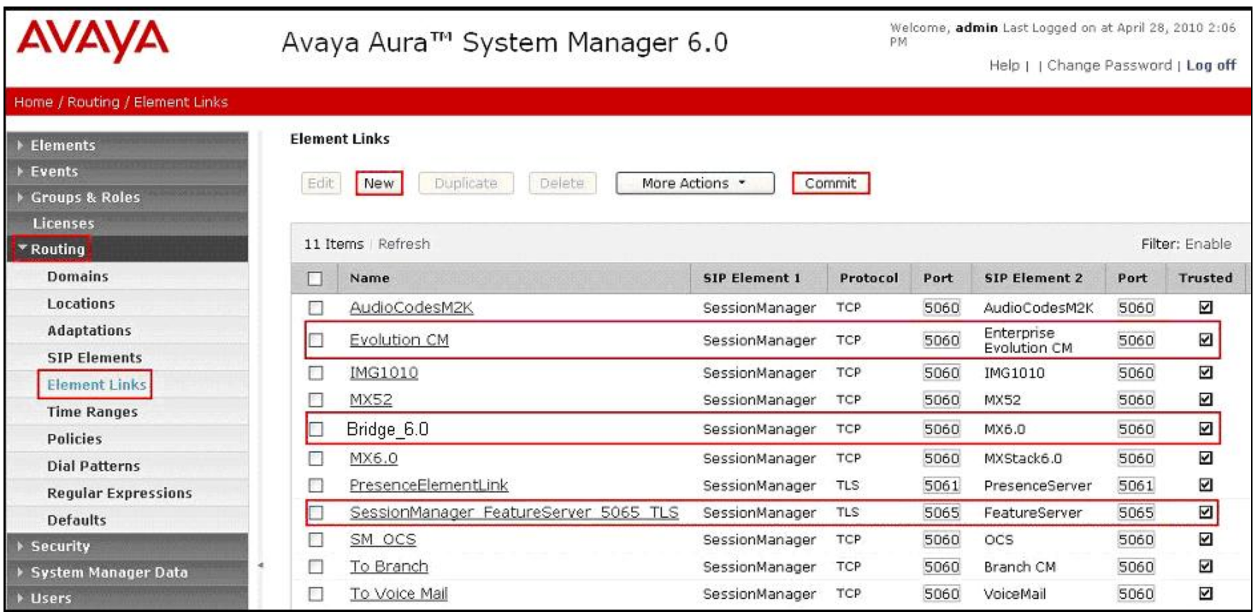


6.5. Add Element Links

A SIP trunk between a Session Manager and a telephony system is described by an Element Link. To add an Element Link, select **Routing → Element Links** on the left panel menu and click **New**. Select the following parameters in the rows that are displayed:

- **Name** An informative name
- **SIP Element 1** Select **SessionManager**
- **Protocol** Transport protocol to be used to send SIP requests
- **Port** Port number to which the other system sends its SIP requests
- **SIP Element 2** The other SIP Element for this link, created in **Section 6.4**
- **Port** Port number to which the other system expects to receive SIP requests
- **Trusted** Whether to trust the other system

Click **Commit** to save changes. The following screen shows the Element Links used in the sample network.



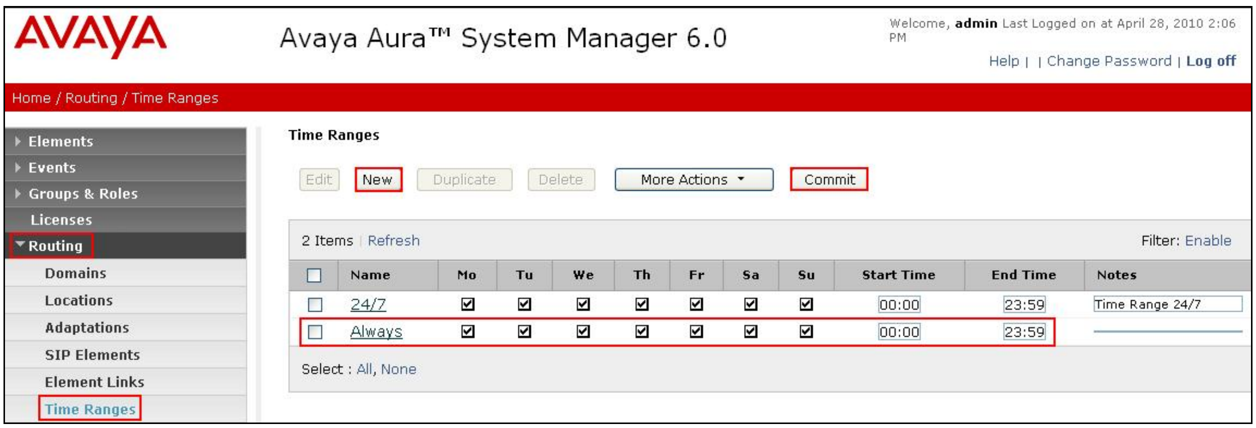
Name	SIP Element 1	Protocol	Port	SIP Element 2	Port	Trusted
AudioCodesM2K	SessionManager	TCP	5060	AudioCodesM2K	5060	☑
Evolution CM	SessionManager	TCP	5060	Enterprise Evolution CM	5060	☑
IMG1010	SessionManager	TCP	5060	IMG1010	5060	☑
MX52	SessionManager	TCP	5060	MX52	5060	☑
Bridge_6.0	SessionManager	TCP	5060	MX6.0	5060	☑
MX6.0	SessionManager	TCP	5060	MXStack6.0	5060	☑
PresenceElementLink	SessionManager	TLS	5061	PresenceServer	5061	☑
SessionManager_FeatureServer_5065_TLS	SessionManager	TLS	5065	FeatureServer	5065	☑
SM_OCS	SessionManager	TCP	5060	OCS	5060	☑
To Branch	SessionManager	TCP	5060	Branch CM	5060	☑
To Voice Mail	SessionManager	TCP	5060	VoiceMail	5060	☑

6.6. Administer Time Ranges

Before adding routing policies (see next section), time ranges must be defined during which the policies will be active. In the sample configuration, one policy was defined that would allow routing to occur at any time. To add this time range, select **Routing → Time Ranges** on the left panel menu, then click **New**. Select the following parameters, leaving the remaining parameters at their default values.

- **Name:** A descriptive name (e.g. **Always**)
- **Mo** through **Su** Check the box under each of these headings
- **Start Time** Enter **00:00**.
- **End Time** Enter **23:59**

Click **Commit** to save this time range.



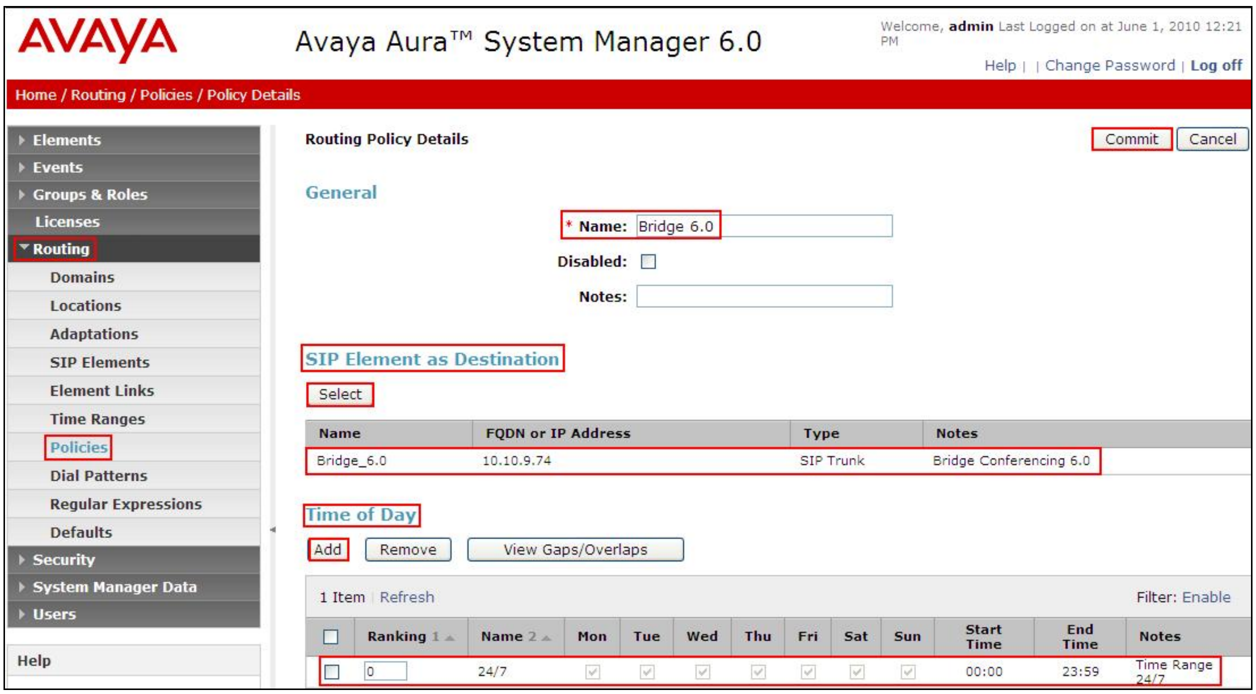
6.7. Administer Routing Policies

A routing policy must be created to direct how calls will be routed to a system. Note that the "Policies" menu option shown in the screen below was changed to "Routing Policies" in the GA release.To add a routing policy, select **Routing → Policies** on the left panel menu and then click **New** (not shown). Select the following parameters, leaving the remaining parameters at their default values.

Under **General**:

- **Name** An informative name (e.g., **Bridge 6.0)**

Under **SIP Element as Destination,** click **Select**, and then select the appropriate SIP Element to which this routing policy applies. Under **Time of Day**, click **Add**, and then select the time range configured in the previous step. Click **Commit** to save changes. The following screen shows the **Routing Policy Details** for the Conferencing server.



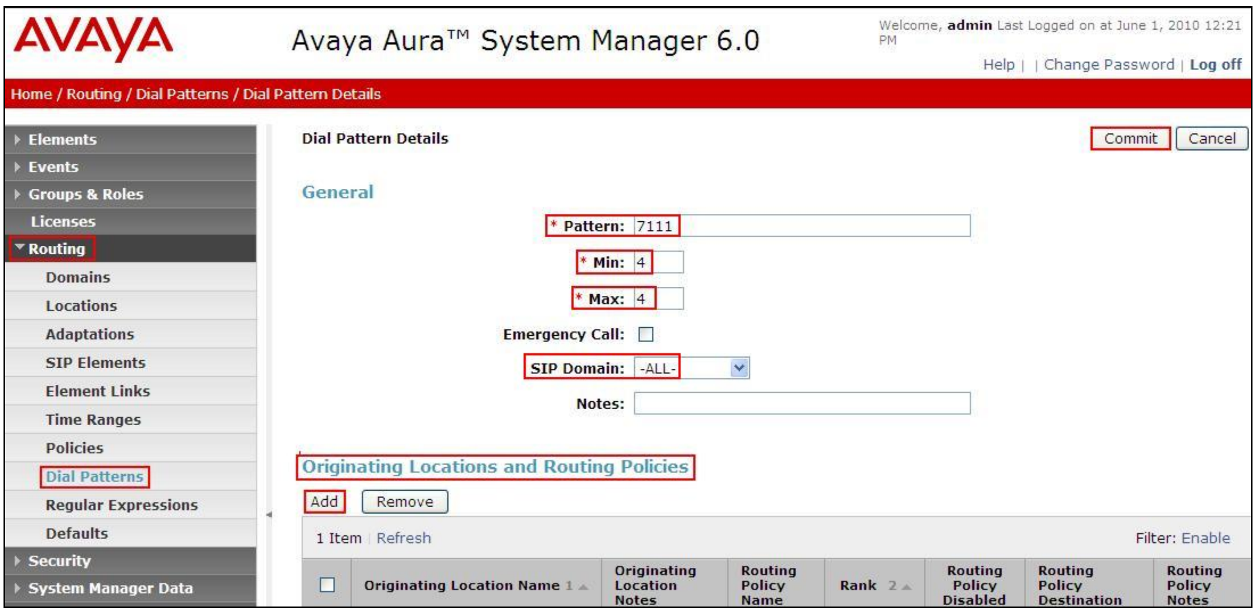
6.8. Administer Dial Patterns

A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample network, the 4-digit extension **7111** will be used as the number that resides on the Conferencing server. Select **Routing → Dial Patterns** on the left panel menu and then click **New** (not shown). Select the following parameters, leaving the remaining parameters at their default values.

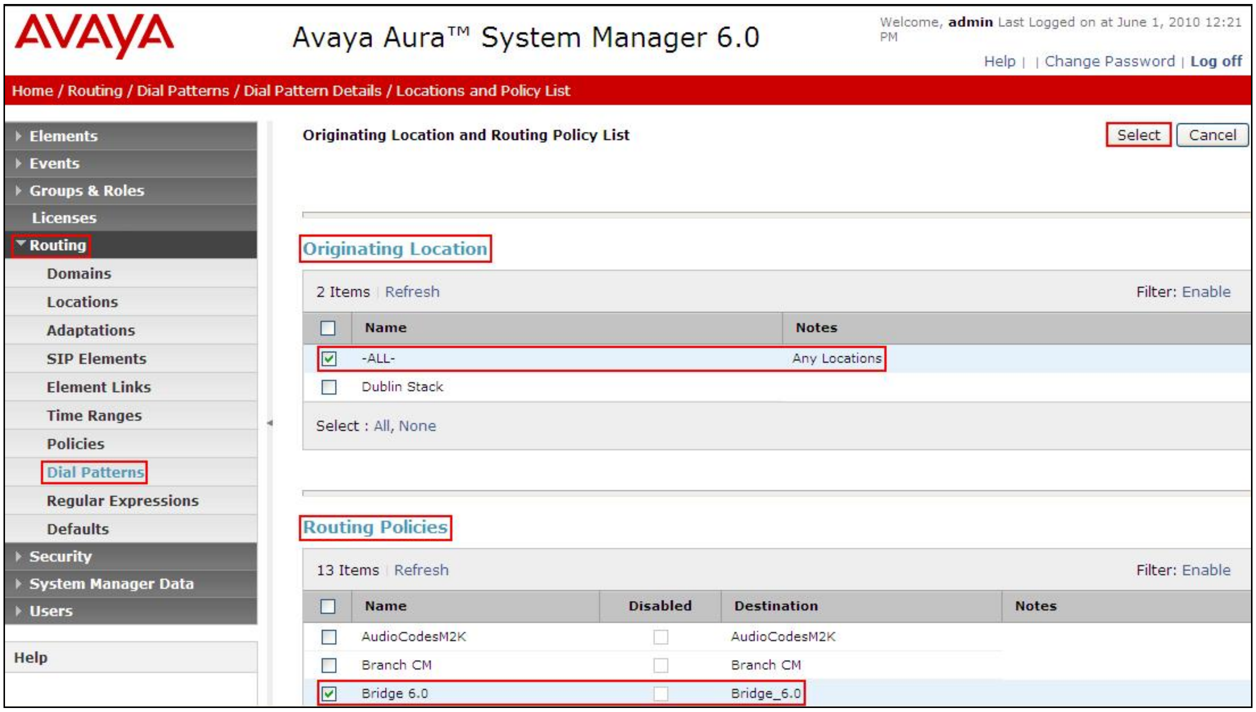
Under **General**:

- **Pattern** Dialed number or prefix i.e. **7111**
- **Min** Minimum length of the dialed number i.e. **4**
- **Max** Maximum length of the dialed number i.e. **4**
- **SIP Domain** Select **ALL**
- **Notes** Comment on purpose of dial pattern

Navigate to **Originating Locations and Routing Policies** and select **Add**.



Under **Originating Location** select all locations by checking the box next to **ALL** and under **Routing Policies** select the Routing Policy created in **Section 6.7**. Click **Select** to confirm the chosen options and return to the Dial Pattern screen (shown above). Click **Commit** to save changes shown in the previous screen.



6.9. Administer Avaya Aura™ Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Select **Elements→ Session Manager Administration** on the left panel menu. Then click **Add** (not shown) and fill in the following parameters, leaving the remaining parameters at their default values.

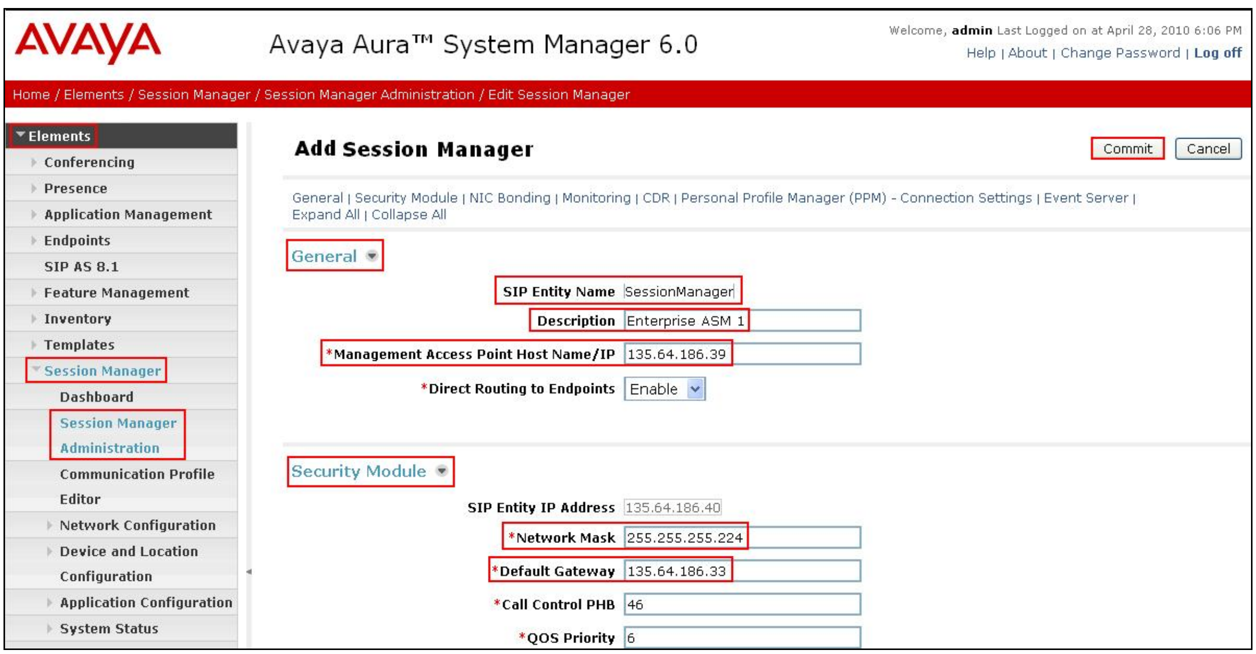
Under **General**:

- **SIP Entity Name** Select the name of the SIP Entity added for Session Manager
- **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** IP Address of Session Manager's SIP routing interface
- **Network Mask** Enter the network mask corresponding to the IP address of Session Manager's SIP routing interface.
- **Default Gateway:** Enter the IP address for the Session Manager's SIP routing interface.

Click **Commit** to add this Session Manager.



6.10. Add Avaya Aura™ Communication Manager as a Feature Server

In order for Communication Manager to provide configuration and Feature Server support to SIP phones when they register to Session Manager, Communication Manager must be added as an application.

6.10.1. Create an Application Entity

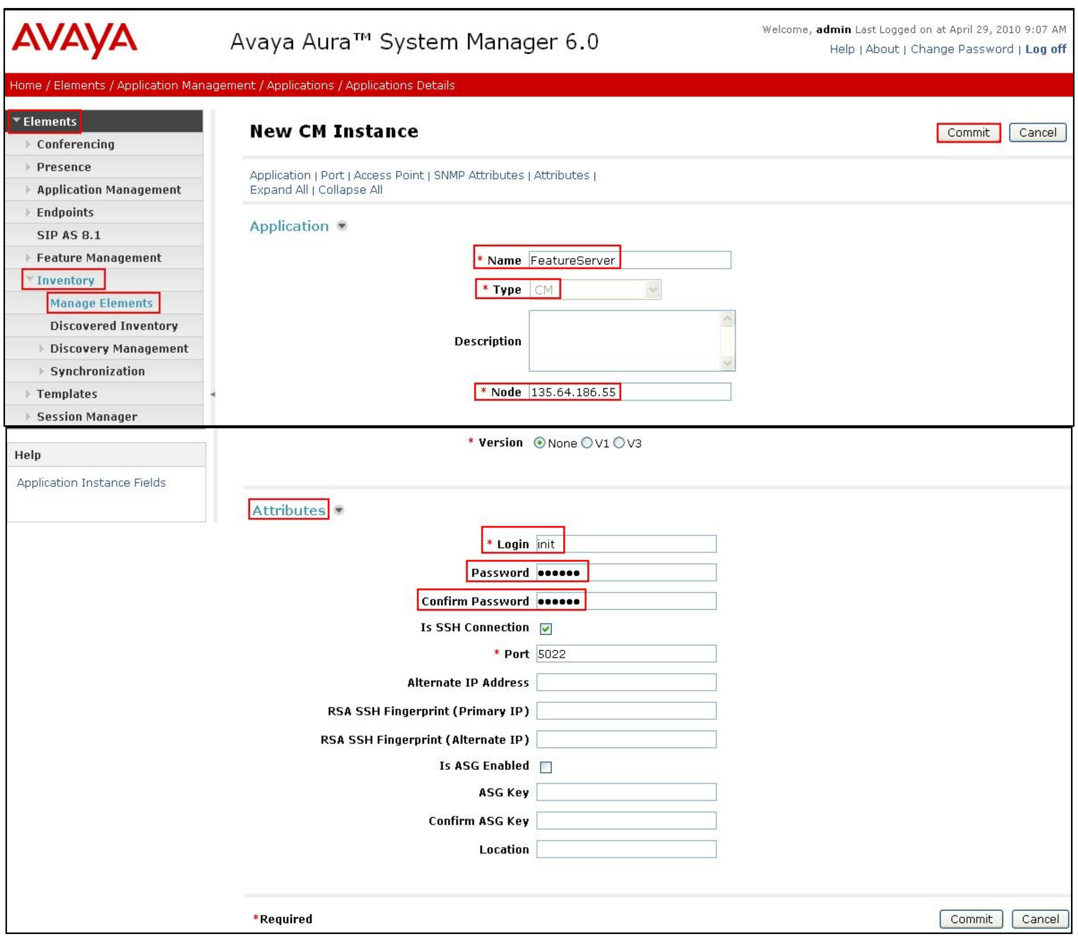
Select **Elements → Inventory → Manage Elements** on the left panel menu. Click on **New** (not shown). Select the following parameters, leaving the remaining parameters at their default values.

- **Name** A descriptive name i.e. **FeatureServer**
- **Type** Select **CM**
- **Node** Enter the IP address for CM SAT access

Navigate to the **Attributes** section and enter the following:

- **Login** Login used for SAT access
- **Password** Password used for SAT access
- **Confirm Password** Password used for SAT access

Click on **Commit** to save.

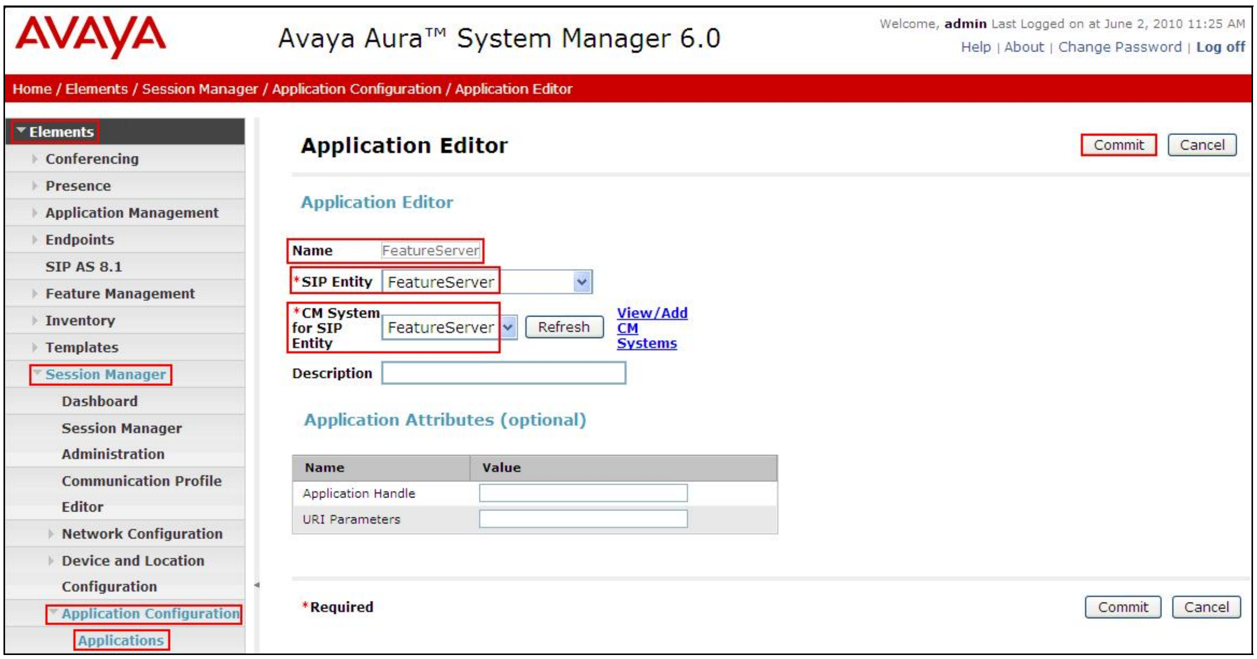


6.10.2. Create a Feature Server Application

Select **Elements → Session Manager → Application Configuration → Applications** on the left panel menu. Click on **New** (not shown). Select the following parameters, leaving the remaining parameters at their default values.

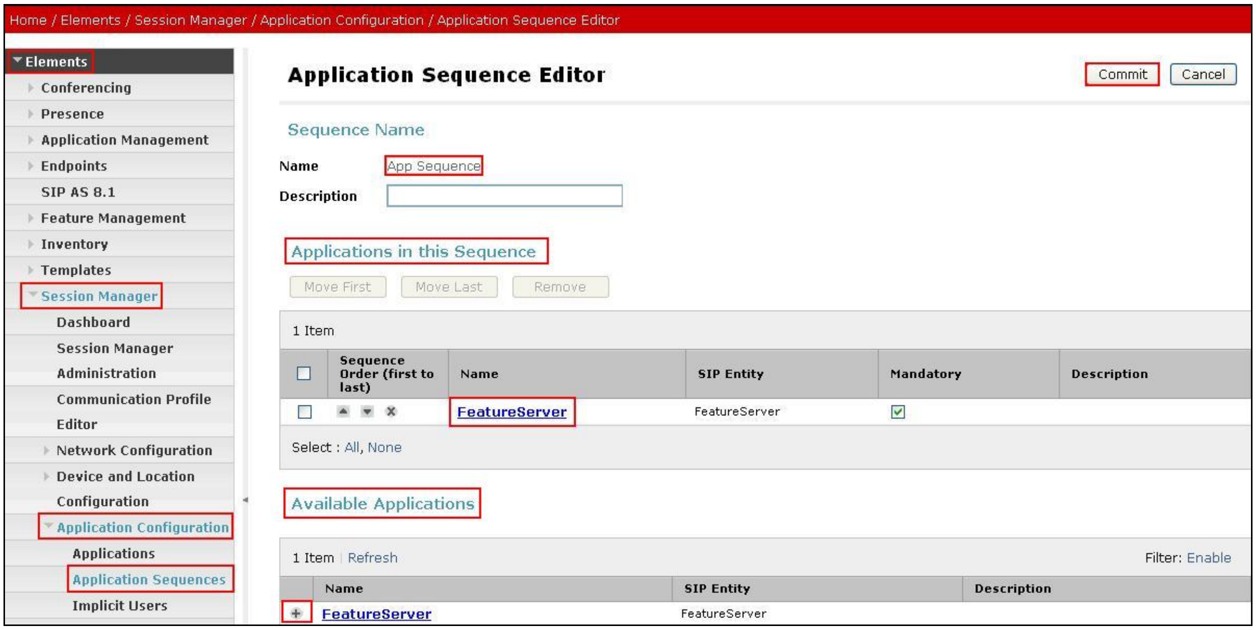
- **Name** A descriptive name
- **SIP Entity** Select the CM Application Entity defined in **Section 6.4**
- **CM System for SIP Entity** Select the CM Application Entity defined in **Section 6.10.1**

Click on **Commit** to save.



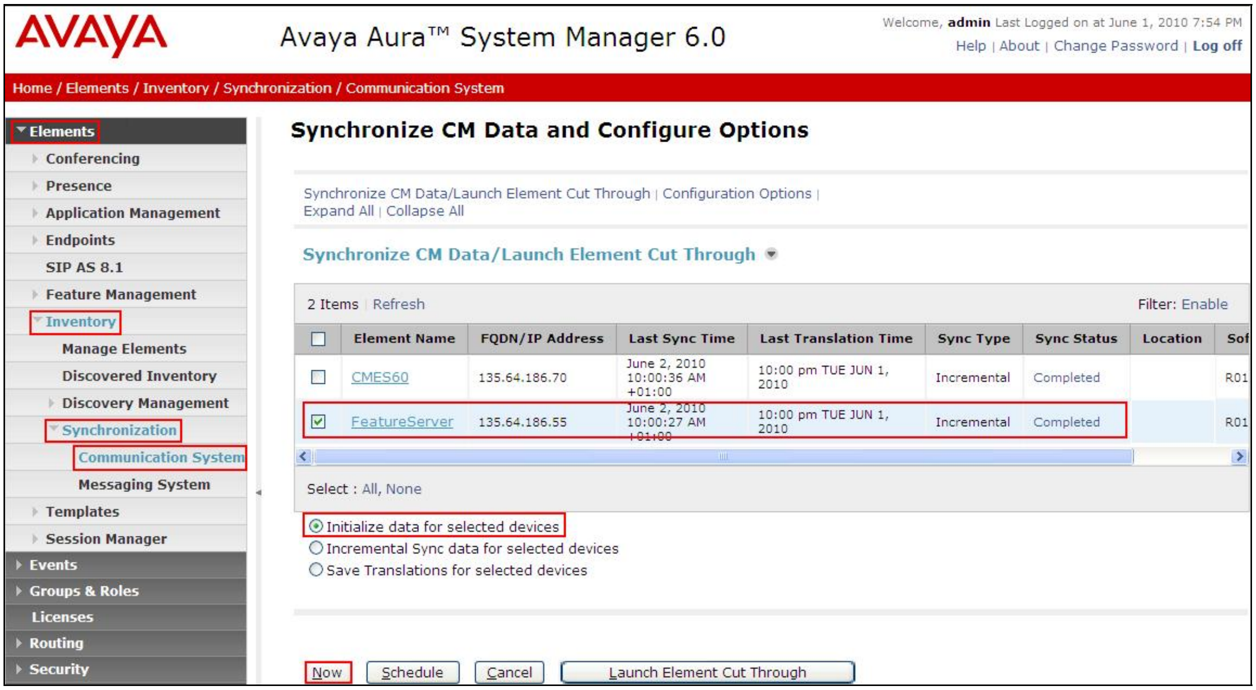
6.10.3. Create a Feature Server Application Sequence

Select **Elements → Session Manager → Application Configuration → Application Sequences** on the left panel menu. Click on **New** (not shown). Enter a descriptive name in the **Name** field. In this case the Sequence name is **App Sequence**. 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.



6.10.4. Synchronize Avaya Aura™ Communication Manager Data

Select **Elements → Inventory → Synchronization → Communication System** on the left panel menu. Select the appropriate **Element Name** from the list. Check the **Initialize data for selected devices** box. Then click on **Now**. This may take some time.

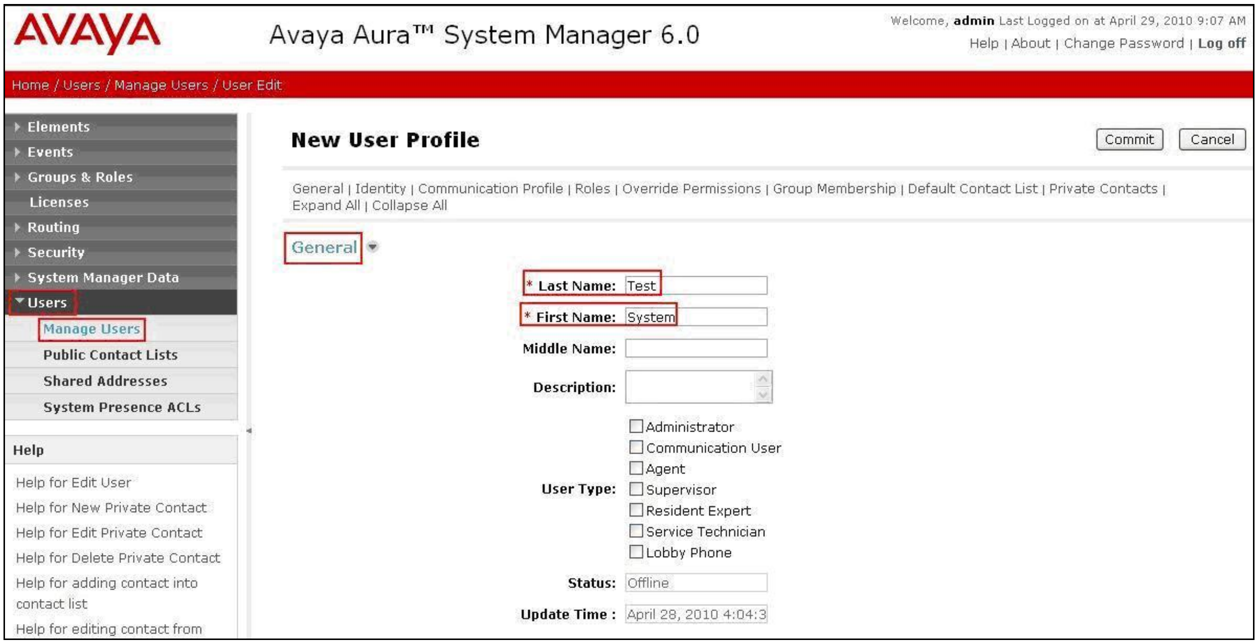


6.11. Add Users for SIP Phones

Users must be added via Session Manager and the details will be updated on the Communication Manager. Select **Users → Manage Users** on the left panel menu. Then click on **New** (not shown). Select the following parameters, leaving the remaining parameters at their default values.

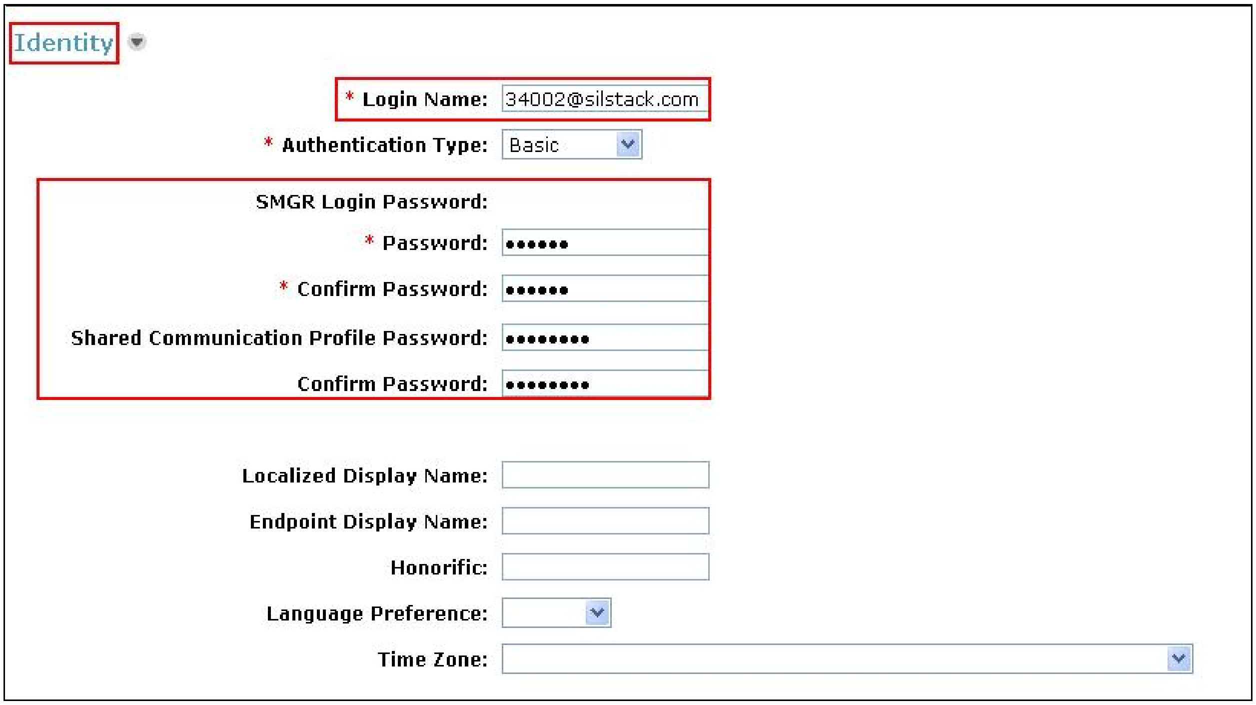
Under **General**:

- **Last Name** Any name
- **First Name** Any name



Navigate to the **Identity** section, select the following parameters, leaving the remaining parameters at their default values.

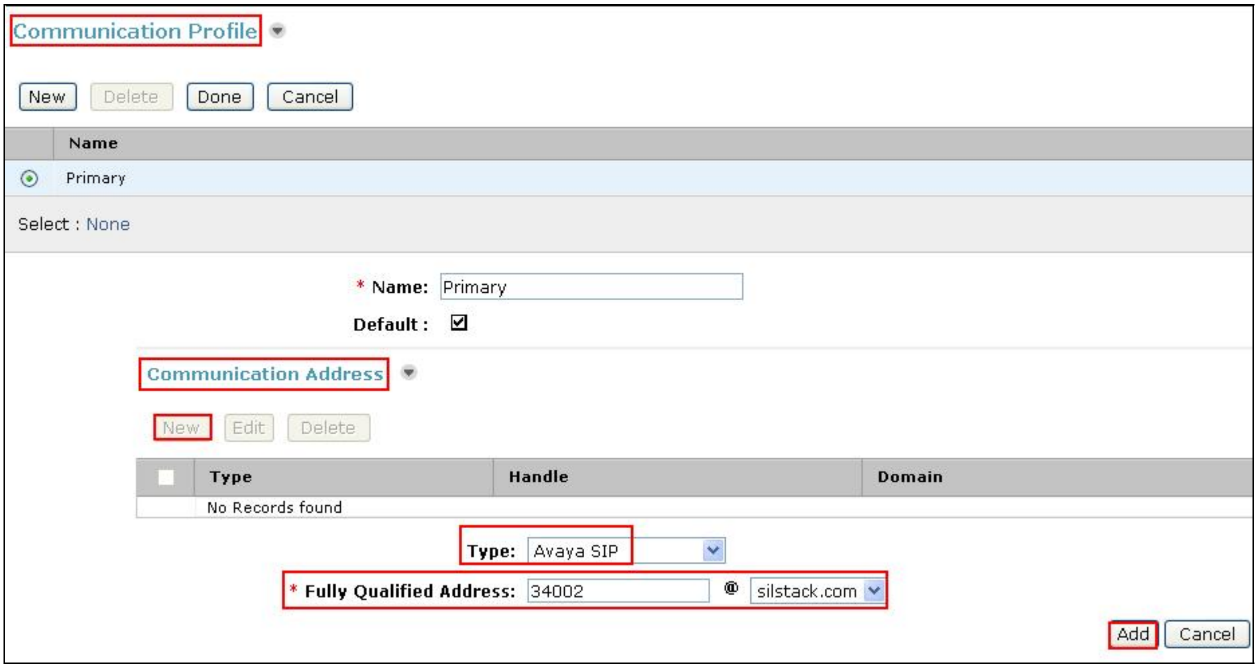
- **Login Name** The desired phone-extension-number@domain where domain was defined in **Section 6.2**
- **Password** Password for user to log into SMGR
- **Shared Communication Profile Password** Password to be entered by the user when logging into the phone



Navigate to and click on **Communication Profile** section to expand that section. Use the default values. Then click on **Communication Address** to expand that section. Click **New** and enter the following:

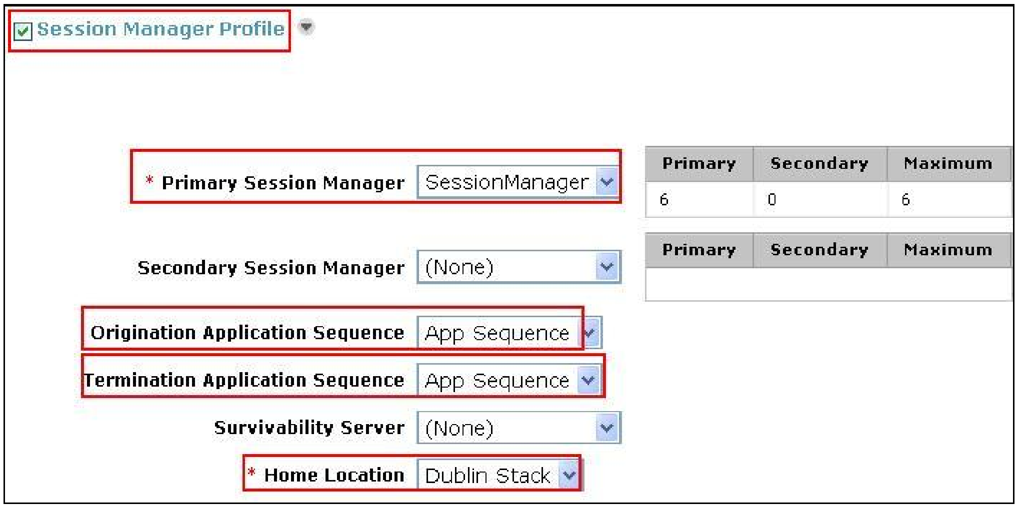
- **Type** Select **Avaya SIP** from the drop down menu.
- **Fully Qualified Address** Enter the extension-number@domain

Click on **Add**.



Navigate to and click on **Session Manager Profile** section to expand. Select the following parameters, leaving the remaining parameters at their default values.

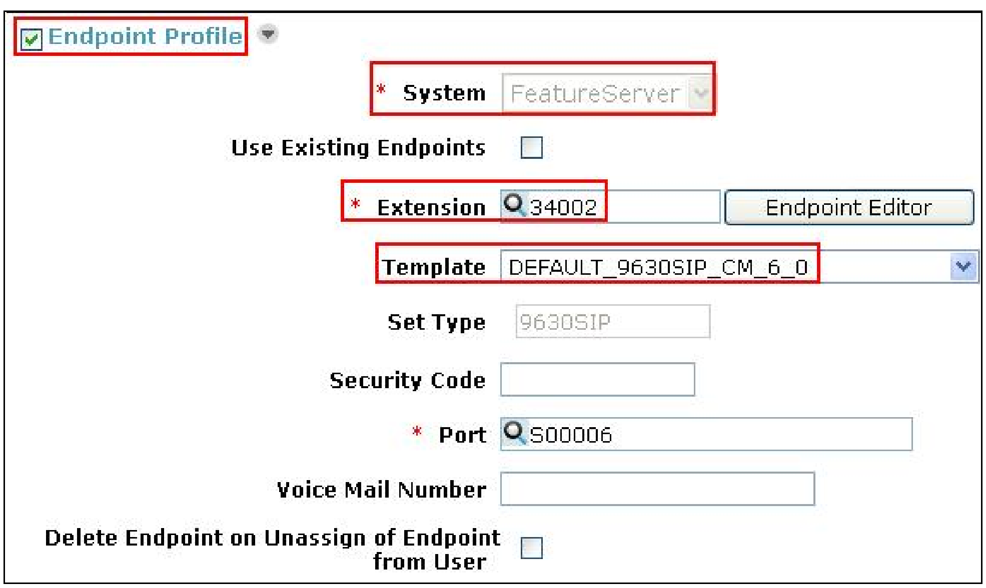
- **Primary Session Manager** Select **SessionManager**
- **Origination Application Sequence** Select **App Sequence**
- **Termination Application Sequence** Select **App Sequence**
- **Home Location** Select **Dublin Stack**



Click on **Endpoint Profile** to expand that section. Select the following parameters, leaving the remaining parameters at their default values.

- **System** Select the Application Entity created in **Section 6.10.1**
- **Extension** Enter a desired extension number
- **Template** Select a telephone type template

Click on **Commit** to save (not shown).



7. Verification Steps

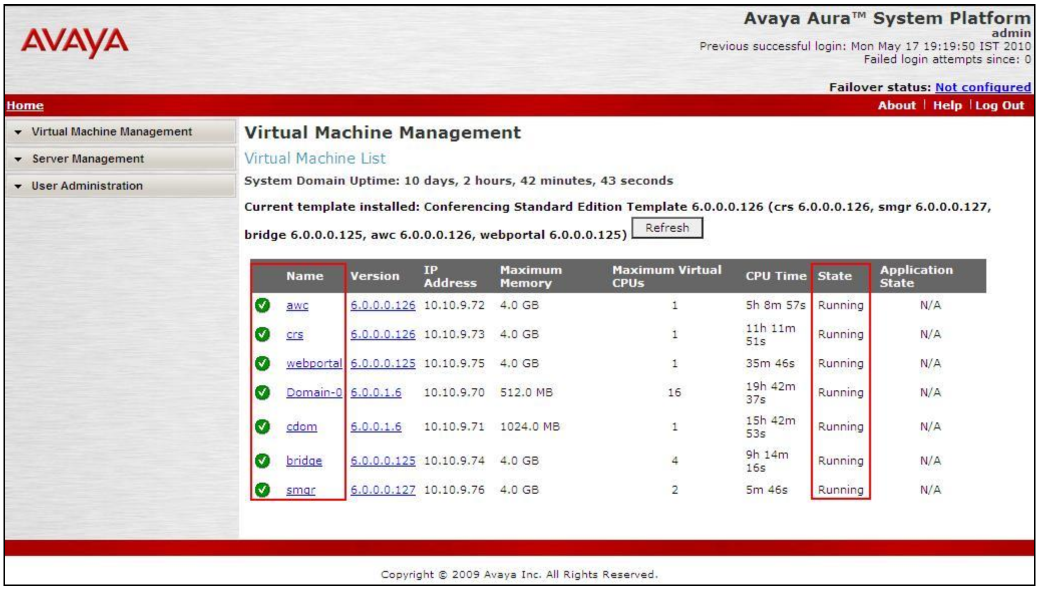
The following steps were used to verify the administrative steps presented in these Application Notes and are applicable for similar configurations in the field. The verification steps in this section validated the following:

- The Conferencing Standard Edition configuration
- Session Manager

7.1. Avaya Aura™ Conferencing Standard Edition

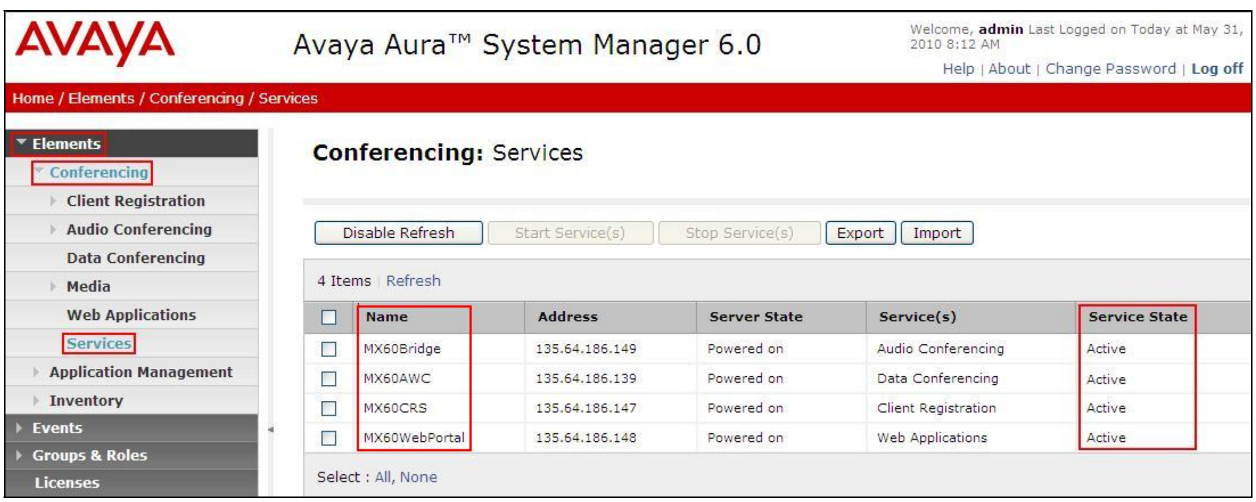
Verify all Virtual Machines are in a running state. Access the System Platform using a Web Browser and entering ***https://<ip-address>/webconsole***, where <ip-address> is the IP address of System Platform. Log in using appropriate credentials.

Verify all Virtual Machines are in a **Running State**.



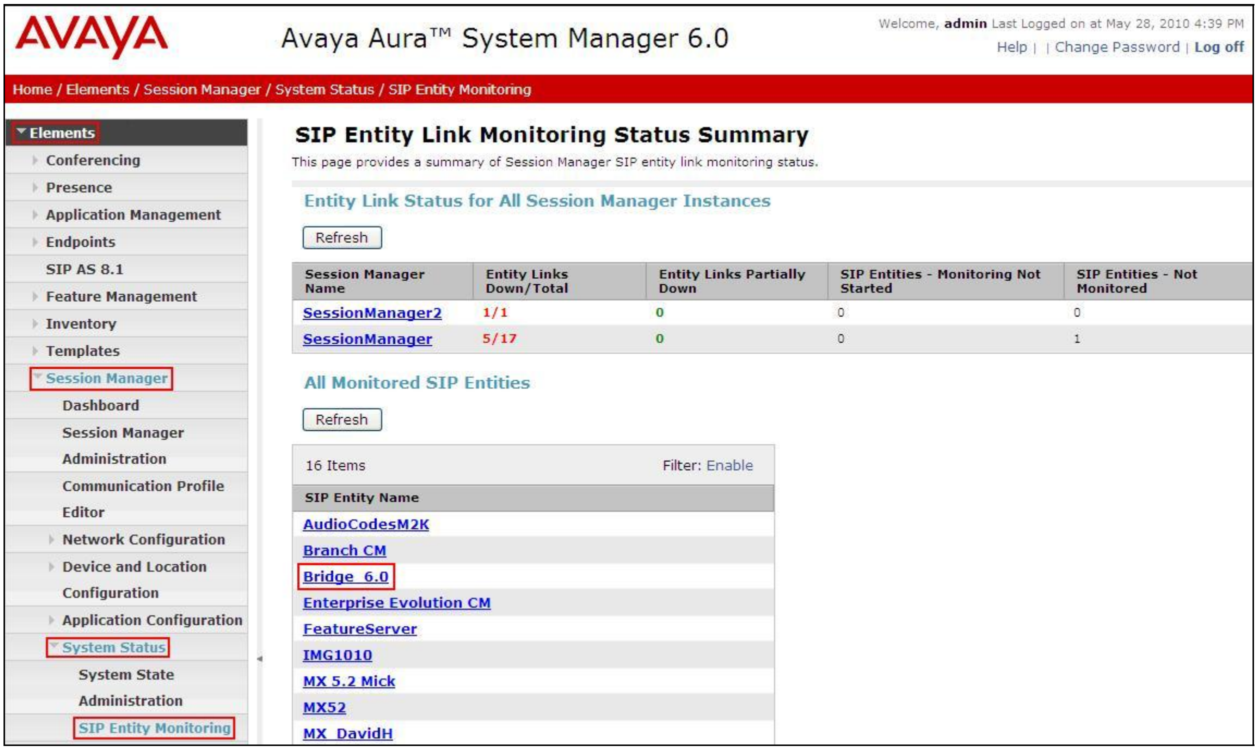
7.2. Conferencing Standard Edition Services

Check **Service State** between the Conferencing bridge and other devices by configuring the SIP System Settings. Select **Elements → Conferencing → Services** on the left panel menu. From the right panel menu ensure the **Conferencing Services** are in an **Active** Service State.

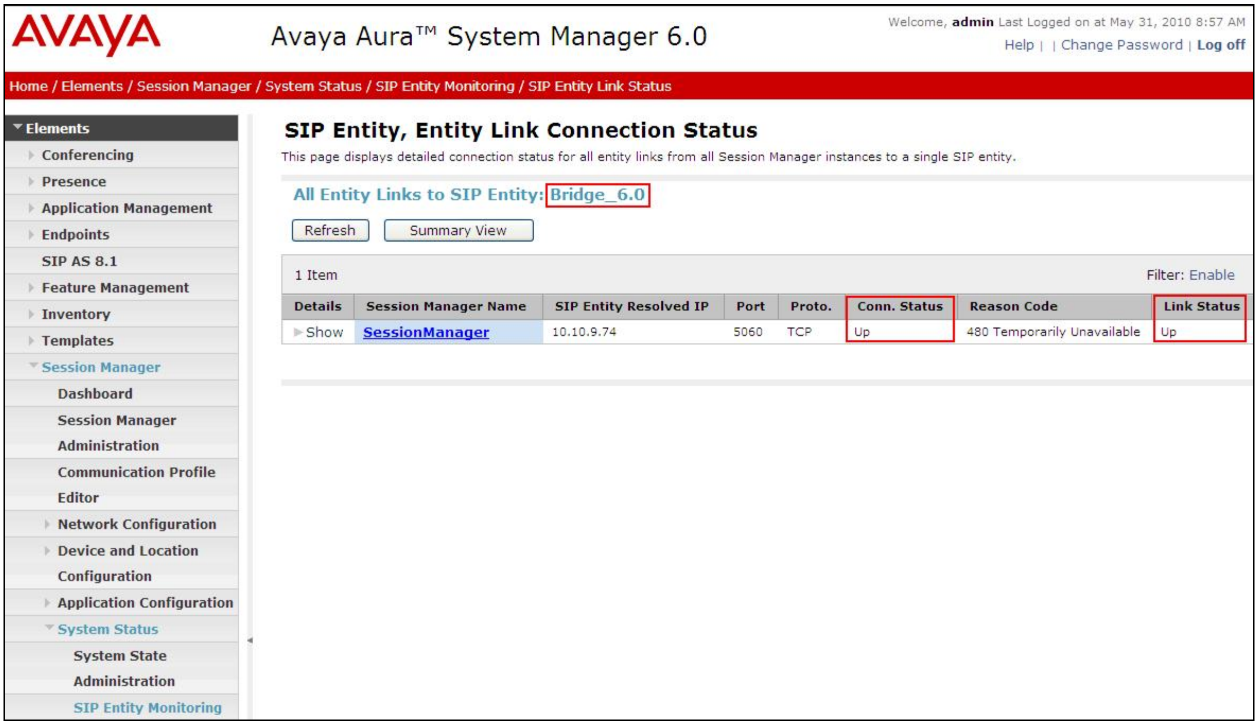


7.3. SIP Monitoring on Avaya Aura™ Session Manager

Verify that none of the links to the defined SIP entities are down, indicating that they are all reachable for call routing by selecting **Elements → Session Manager → System Status → SIP Entity Monitoring** on the left panel menu. From the right panel menu select one of the SIP Entities created in **Section 6.4**



Click on the SIP Entity Name **Bridge 6.0**, shown in the previous screen, and verify that the **Conn. Status** and **Link Status** are **Up**.



7.4. Verification Scenarios

Verify end to end signalling/media connectivity between the Communication Manager and Conferencing Standard Edition via the Session Manager, this is accomplished by:

- Placing a call from 2 end points into conference ensuring 1 of the callers is a moderator.
- Verify both callers are in the same conference and there is two way speech between the callers.
- Initiate dial out by dialing *1 xxxx on the moderator phones touch pad, where xxxx is the extension for an end point. Follow the instructions provided by the Conferencing bridge.
- After answering the call, on the moderator phone dial *2 to join the new participant into the conference.
- Verify both callers are in the same conference and there is two way speech between the callers.

8. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Conferencing Standard Edition can interoperate successfully with Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager using SIP trunks.

9. Additional References

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

Avaya Aura™ Conferencing Standard Edition 6.0

[1] *Implementing Avaya Aura™ Conferencing Standard Edition, Doc ID 04-603508, June 2010, available at http://support.avaya.com.*

[2] *Operating Avaya Aura™ Conferencing Standard Edition, Doc ID 04-603510, June 2010, available at http://support.avaya.com.*

[3] *Using Avaya Aura™ Conferencing Standard Edition, Doc ID 04-603509, June 2010, available at http://support.avaya.com.*

[4] *Avaya Aura™ Conferencing Standard Edition Release Notes, Doc ID 04-603528, June 2010, available at http://support.avaya.com.*

Avaya Aura™ Communication Manager 6.0

[5] *Administering Avaya Aura™ Communication Manager, Doc ID 03-300509, June 2010, available at http://support.avaya.com.*

[6] *Administering Avaya Aura™ Communication Manager as a Feature Server, Doc # 03-603479, Issue 1.2, Release 5.2 January 2010, available at http://support.avaya.com.*

Avaya Aura™ Session Manager 6.0

[7] *Avaya Aura™ Session Manager Overview, Doc ID 03-603323, available at http://support.avaya.com.*

[8] *Administering Avaya Aura™ Session Manager, Doc ID 03-603324 available at http://support.avaya.com.*

[9] *Installing and Upgrading Avaya Aura™ Session Manager 6.0, Doc ID 03-603324, available at http://support.avaya.com.*

[10] *Installing and Upgrading Avaya Aura™ System Manager 6.0, available at http://support.avaya.com.*

[11] *Maintaining and Troubleshooting Avaya Aura™ Session Manager 6.0, 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