Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Thrupoint Enterprise Mobility Solution with Avaya Aura® Session Manager 6.1 and Avaya Aura® Communication Manager 6.0.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Thrupoint Enterprise Mobility solution to interoperate with Avaya Aura® Session Manager 6.1 and Avaya Aura® Communication Manager 6.0.1 for SIP Users.

Thrupoint's Fixed Mobile Convergence (FMC) solution (i.e. Enterprise Mobility) delivers a converged solution by extending the enterprise PBX functionality to mobile devices. This allows end users to be accessible when out of the office as well as to leverage wireless LAN networks to improve wireless coverage, reduce costs, and provide the ability to manually move calls from the Wi-Fi network to the mobile network and vice-versa.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedures for configuring Thrupoint Enterprise Mobility solution to interoperate with Avaya Aura® Session Manager 6.1 and Avaya Aura® Communication Manager 6.0.1.

Thrupoint's Fixed Mobile Convergence (FMC) solution (i.e. Enterprise Mobility) delivers a converged solution by extending the enterprise PBX functionality to mobile devices. This allows end users to be accessible when out of the office as well as to leverage wireless LAN networks to improve wireless coverage, reduce costs, and provide the ability to manually move calls from the Wi-Fi network to the mobile network and vice-versa.

The Thrupoint FMC solution consists of two key components: the Thrupoint FMC Client and the Thrupoint FMC Server. Installed on a mobile handset, the FMC client provides user access to the same types of features and functionalities (e.g. call transfer, call hold and resume, call conference and mute) as the user's desk phone. Compliance testing focused on the Thrupoint FMC iPhone client. Additional basic functionality testing was done with the Thrupoint FMC Android client (version 1.1.7) and the Thrupoint FMC BlackBerry client (version 1.1.7); however, the Android and BlackBerry clients were not fully compliance tested.

The Thrupoint FMC Server is designed to provide locally managed mobility services that can be integrated with customers' existing PBXs. Once the server is installed on the enterprise network, Smartphone handsets behave as IP desk phones, providing a cost-effective option for adding mobile extensions without a system forklift. The server also incorporates a management server for administration of the system.

2. General Test Approach and Test Results

The general test approach was to make mobile originating and mobile terminating calls route through the Avaya telephony infrastructure. The configuration shown in **Figure 1** was used to exercise the features and functionality listed in **Section 2.1**. Compliance testing focused on the Thrupoint FMC iPhone client. Additional basic functionality testing was done with the Thrupoint FMC Android client (version 1.1.7) and the Thrupoint FMC BlackBerry client (version 1.1.7); however, the Android and BlackBerry clients were not fully compliance tested.

2.1. Interoperability Compliance Testing

All functional test cases were performed manually. Testing entailed verifying different types of Avaya system features interacting with the Thrupoint FMC solution. Tests were performed focusing on the following:

- Mobile originated calls routed through the Avaya telephony infrastructure terminating to a desk phone, mobile device, or PSTN
- Mobile terminated calls routed through the Avaya telephony infrastructure
- Manually move calls from the Wi-Fi network to the mobile network and vice-versa.
- Desktop originated calls routed to mobile devices

- DTMF digit support for voicemail and conference calls
- Call Forwarding
- Call Hold /Resume
- Transfer / Conference

2.2. Test Results

The Thrupoint FMC solution successfully completed all test cases for the features identified in **Section 2.1** with the following observations made:

- Moving a on a mobile call between the Wi-Fi network and the cellular network was a manual process within the Thrupoint client application, rather than automatic.
- Music-on-hold was not extended to the mobile phones.
- If a second call arrived at a mobile phone, the mobile phone user heard ringing for the second call; however, the display did not show the caller ID of the caller.
- The mobile phones were not integrated to display a Message Waiting Indicator (MWI)

2.3. Support

For technical support with the Thrupoint Enterprise Mobility solution, contact Thrupoint at:

- Web: http://www.thrupoint.com
- Phone: +1 646 837 5541
- Email: BMcMenamin@thrupoint.com

3. Reference Configuration

Figure 1 illustrates the reference configuration used during compliance testing.

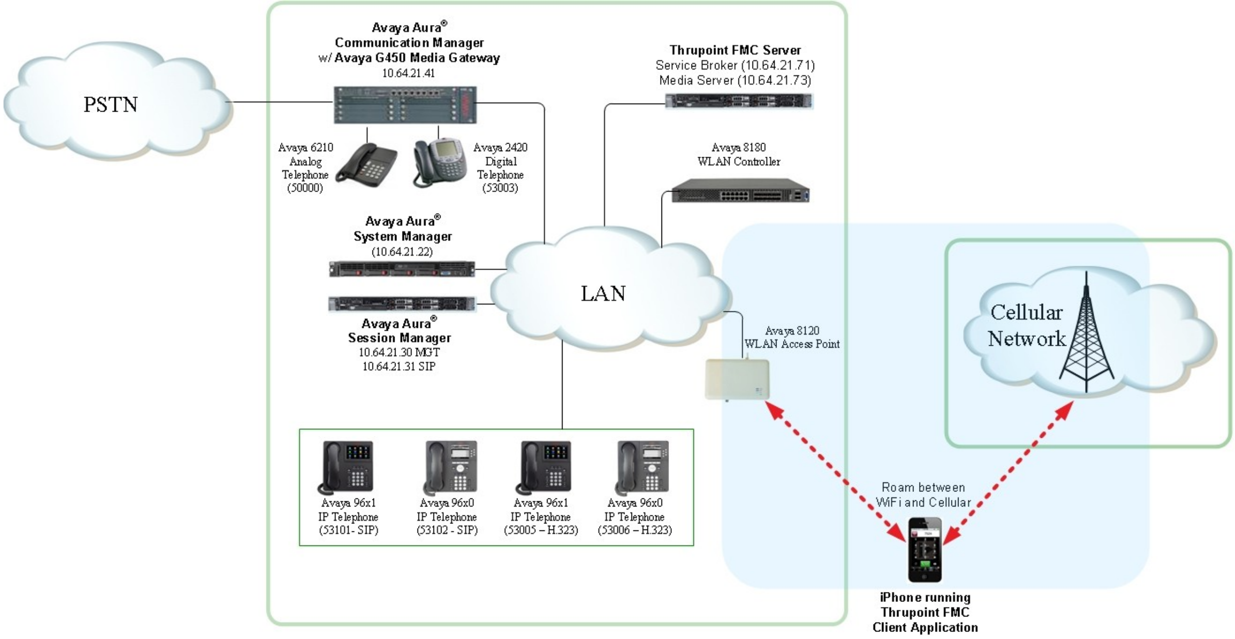


Figure 1: Thrupoint Enterprise Mobility solution in an Avaya Aura® Environment

4. Equipment and Software Validated

The following equipment and software were used for the reference configuration:

Equipment	Software
Avaya S8300D Server with a Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.0.1, R016x.00.1.510.1, Patch 19009 (Avaya Aura® System Platform: 6.0.3.0.3)
Dell™ PowerEdge™ R610 Server	Avaya Aura® System Manager: 6.1.0 (Build No. – 6.1.0.0.7345-6.1.5.106), Software Update Revision No : 6.1.6.1.1087 (Avaya Aura® System Platform: 6.0.3.0.3)
HP ProLiant DL360 G7 Server	Avaya Aura® Session Manager 6.1.2.0.612004
Avaya 96xx Series IP Deskphones	Release 3.1 Service Pack 3 (H.323) Release 2.6 Service Pack 5 (SIP)
Avaya 96x1 Series IP Deskphones	Release 6 Service Pack 5 (H.323)Release 6 Service Pack 2 (SIP)
Avaya 2400 Series Digital Telephone	Release 6
Avaya 6200 Series Analog Telephone	-
Thrupoint FMC Server • SIP A/S • UAS Manager • Service Broker • FMC • MySQL • Inbound Digit Adaptation	 • Ubiquity SIP A/S 8.3.8 Patch 1 Drop 7 • UAS Manager 1.0.1 • Service Broker 1.1.6_1 Patch Drop 8 • 1.1.7 • MySQL Cluster 7.1.8 • 1.1.6.1.11
Thrupoint FMC iPhone Client	1.1.7.1.1

5. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration shown in **Figure 1**.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

License

Use the **display system-parameters customer-options** command to verify that the Communication Manager license has proper permissions/capacity for the features illustrated in these Application Notes. If there is insufficient permissions/capacity, contact an authorized Avaya sales representative to make the appropriate changes.

On **Page 1** to ensure that the **Maximum Off-PBX Telephones – EC500** value is equal to or greater than the number of endpoints projected in the configuration.

```
display system-parameters customer-options                      Page   1 of  11
                                OPTIONAL FEATURES

     G3 Version: V16                             Software Package: Enterprise
       Location: 2                                System ID (SID): 1
       Platform: 28                               Module ID (MID): 1

                                                             USED
                                Platform Maximum Ports: 65000 340
                                      Maximum Stations: 41000 37
                              Maximum XMOBILE Stations: 41000 0
                    Maximum Off-PBX Telephones - EC500: 41000 3
                    Maximum Off-PBX Telephones -   OPS: 41000 10
                    Maximum Off-PBX Telephones - PBFMC: 41000 0
                    Maximum Off-PBX Telephones - PVFMC: 41000 0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 313   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

</td></tr>
</table>

Step	Description

Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

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

 IP PORT CAPACITIES                                                USED
                     Maximum Administered H.323 Trunks: 12000 32
           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 0
                   Maximum Video Capable IP Softphones: 18000 1
                       Maximum Administered SIP Trunks: 24000 170
   Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
    Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
    Maximum Number of Expanded Meet-me Conference Ports: 300   0

         (NOTE: You must logoff & login to effect the permission changes.)
```

On Page 4, verify **Enhanced EC500** in enabled.

```
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? y
    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
        (NOTE: You must logoff & login to effect the permission changes.)
```

Step	Description
2.	**IP network region** Use the **display ip-network-region** command to view the IP network region settings. The values shown below are the values used during compliance testing. ▪ **Authoritative Domain**: ***avaya.com*** This field was configured to match the domain name configured on Session Manager (see **Section 6**, **Step 2**). The domain will appear in the "From" header of SIP messages originating from this IP region. ▪ **Name**: Any descriptive name may be used (if desired). ▪ **Intra-region IP-IP Direct Audio**: ***no*** **Inter-region IP-IP Direct Audio**: ***no*** By default, IP-IP direct audio (media shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. The Thrupoint solution does not support media shuffling and these fields must be disabled. Shuffling can be further restricted at the trunk level on the **Signaling Group** form. ▪ **Codec Set**: ***1*** The codec set contains the list of codecs available for calls within this IP network region.

```
display ip-network-region 1                                    Page   1 of  20
                                IP NETWORK REGION
   Region: 1
 Location:          Authoritative Domain: avaya.com
     Name:
 MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
       Codec Set: 1              Inter-region IP-IP Direct Audio: no
    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
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

Codecs

IP codec set 1 was used during compliance testing. Multiple codecs can be listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The example below shows the values used during compliance testing.

<pre>
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.711MU   n   2   20
 2: G.729A   n   2   20
 3:
 4:
 5:
 6:
 7:

     Media Encryption
 1: none
 2:
 3:
</pre>

</td></tr>
</table>

Step	Description
4.	**Node Names** Use the **change node-names ip** command to create a node name for the IP address of Session Manager. Enter a descriptive name in the **Name** column and the IP address assigned to Session Manager in the **IP address** column.

```
change node-names ip                                            Page   1 of   2
                                   IP NODE NAMES
     Name              IP Address
 SM_21_31            10.64.21.31
 default             0.0.0.0
 msgserver           10.64.21.41
 procr               10.64.21.41
 procr6              ::
```

Step	Description

5. **Signaling Group**

Signaling group 1 was used for the signaling group associated with the SIP trunk group between Communication Manager and Session Manager. Signaling group 1 was configured using the parameters highlighted below.

- **Group Type**: ***sip***
- **IMS Enabled?**: ***n*** This field is set to ***n*** for a Communication Manager configured as an Evolution server. When configuring Communication Manager as a Feature Server, set this field to ***y***.
- **Transport Method: *tls***
- **Peer Detection Enabled?**: ***y***
- **Peer Server: *SM*** This field will automatically be populated when the **Peer Detection Enabled?** field is set to ***y***.
- **Near-end Node Name**: ***procr*** This node name maps to the IP address of the Avaya S8300D Server. Node names are defined using the **change node-names ip** command.
- **Near-end Listen Port**: ***5061*** The listening port for Communication Manager.
- **Far-end Node Name**: ***SM_21_31*** This node name maps to the IP address of Session Manager.
- **Fear-end Listen Port**: ***5061*** The listening port for Session Manager.
- **Far-end Network Region**: ***1*** This defines the IP network region which contains Session Manager.
- **Direct IP-IP Audio Connections**: ***n*** The Thrupoint solution does not support media shuffling and this field must be disabled.

```
display signaling-group 1
                                 SIGNALING GROUP

  Group Number: 1              Group Type: sip
   IMS Enabled? n        Transport Method: tls
         Q-SIP? n                                             SIP Enabled LSP? n
      IP Video? y          Priority Video? n        Enforce SIPS URI for SRTP? y
   Peer Detection Enabled? y  Peer Server: SM



    Near-end Node Name: procr                 Far-end Node Name: SM_21_31
  Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                         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? n
 Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
          Enable Layer 3 Test? y
                                                   Alternate Route Timer(sec): 20
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.</td><td>

Trunk Group

Trunk group 1 was used for the SIP trunk group between Communication Manager and Session Manager. Trunk group 1 was configured using the parameters highlighted below.

- **Group Type:** ***sip*** This field sets the type of the trunk group.
- **Group Name:** Any descriptive name may be used (if desired).
- **TAC:** ***101*** Enter an valid value consistent with the Communication Manager dial plan.
- **Service Type:** ***tie*** Set to tie.
- **Member Assignment Method:** ***auto*** Set to Auto.
- **Signaling Group**: ***1*** This field is set to the signaling group shown in the previous step.
- **Number of Members:** ***50*** This field represents the number of trunk group members in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.

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

 Group Number: 1                  Group Type: sip           CDR Reports: y
   Group Name: to SM_21_31               COR: 1        TN: 1        TAC: 101
    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: 1
                                                    Number of Members: 50
```

</td></tr>
</table>

Step **Description**

Trunk Group – continued

On **Page 3**:

- The **Numbering Format** field was set to ***unk-pvt***. This field specifies the format of the calling party number sent to the far-end.
- The default values may be retained for the other fields.

```
display trunk-group 1                                         Page   3 of  21
 TRUNK FEATURES
           ACA Assignment? n            Measured: none
                                                  Maintenance Tests? y



                      Numbering Format: unk-pvt
                                                 UUI Treatment: service-provider

                                                  Replace Restricted Numbers? n
                                                 Replace Unavailable Numbers? n



                                 Modify Tandem Calling Number: no





  Show ANSWERED BY on Display? y
```

7. **Private Numbering**

Private Numbering defines the calling party number to be sent to the far-end. In the example shown below, all calls originating from a ***5***-digit extension beginning with ***5*** and routed across any trunk group will be sent as a ***5*** digit calling number. The calling party number is sent to the far-end in the SIP "From" header.

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

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

Step **Description**

8. **Automatic Alternate Routing**

Automatic Alternate Routing (AAR) was used to route the EC500 calls to Session Manager for onward routing to the Thrupoint Service Broker. Use the **change aar analysis** command to create an entry in the AAR Digit Analysis Table. The example below shows dialed strings that begin with ***362*** and are ***14*** digits long use route pattern ***1*** (to Session Manager). Note that the digits **362** are only steering digits and any desired steering digits can be used. When the call reaches the Thrupoint Service Broker, the **362** digits will be stripped, and the remaining 11 digits will be used to route the call.

```
change aar analysis 362                                         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
     362                   14   14    1        aar          n
```

The example below shows dialed strings that begin with ***303*** and are ***10*** digits long use route pattern ***1*** (to Session Manager). Direct Inward Dial (DID) number 303-538-3501 was configured so that when the call came into Communication Manager from the PSTN, the call was routed to the Thrupoint Service Broker. Thrupoint's Service Broker forwards the DID into the FMC server as the access number. This call then is routed to the appropriate Mobile client and connect to the endpoint provided over the Light Weight Ubiquity Protocol (LUMP)

```
change aar analysis 303                                         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
     3035383501            10   10    1        aar          n
```

9. **Off PBX Telephone Station Mapping**

Each mobile device was associated with a station extension configured on Communication Manager. The station extension may represent a physical desk phone or may be an extension with no phone logged in to it. To associate a mobile device to each of these station extensions, an off-pbx station mapping is required as shown below. Below, mobile **Phone Number** 1-917-435-2029 is associated with Communication Manager **Station Extension** 53005 (a H.323 phone). Note the leading 362 digits in the **Phone Number** field are only used as steering digits to route the call to the Thrupoint Service broker.

```
change off-pbx-telephone station-mapping 53005                  Page   1 of   3
                   STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

  Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
  Extension                 Prefix                     Selection   Set     Mode
  53005            EC500         -     36219174352029   aar        1
```

Step	Description

```
change off-pbx-telephone station-mapping 53005                  Page   2 of   3
                   STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

  Station       Appl    Call        Mapping    Calls       Bridged       Location
  Extension     Name    Limit       Mode       Allowed     Calls
  53005         EC500    2        both         all         both
```

```
change off-pbx-telephone station-mapping 53005                  Page   3 of   3
                   STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

  Station       Appl  Share    Calls Accepted
  Extension     Name  Level    S C H I P R-COR
  53005         EC500   5
```

The example below shows mobile **Phone Number** 1-917-435-2448 is associated with Communication Manager **Station Extension** 53102 (a SIP phone). Note again that the leading 362 digits in the **Phone Number** field are only used as steering digits to route the call to the Thrupoint Service broker. The first entry below with the ***OPS* Application** is automatically created when a SIP station is created on Communication Manager.

```
change off-pbx-telephone station-mapping 53102                  Page   1 of   3
                   STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

  Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
  Extension                 Prefix                     Selection   Set     Mode
  53102            OPS          -     53102            aar        1
  53102            EC500        -     36219174352448   aar        1
```

```
change off-pbx-telephone station-mapping 53102                  Page   2 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Appl    Call        Mapping    Calls       Bridged       Location
 Extension     Name    Limit       Mode       Allowed     Calls
 53102         OPS      2        both         all         none
 53102         EC500    2        both         all         both
```

```
change off-pbx-telephone station-mapping 53102                  Page   3 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Appl  Share    Calls Accepted
 Extension     Name  Level    S C H I P R-COR
 53102         OPS
 53102         EC500   5
```

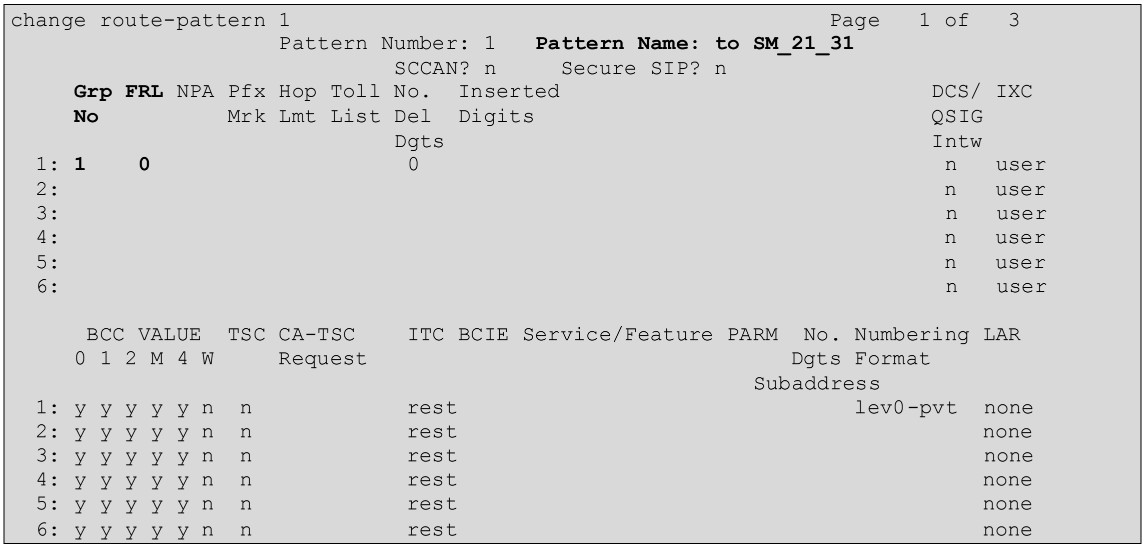
Step	Description
10.	**Automatic Route Selection** Automatic Route Selection (ARS) was used to route calls to out the PSTN trunk (the configuration of the PSTN trunk is outside the scope of these Application Notes and is therefore not shown in this document). Use the **change ars analysis** command to create an entry in the ARS Digit Analysis Table. The example below shows dialed strings that begin with ***130*** and are ***11*** digits long use route pattern ***2*** (to the PSTN trunk).

```
change ars analysis 130                                         Page   1 of   2
                            ARS DIGIT ANALYSIS TABLE
                                  Location: all           Percent Full: 1

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    130                   11   11    2         hnpa         n
```

Similarly, the example below shows dialed strings that begin with ***191*** and are ***11*** digits long use route pattern ***2*** (to the PSTN trunk).

```
change ars analysis 191                                         Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    1917                  11   11    2         hnpa         n
```

Step	Description
11.	**Route Pattern** Route pattern 1 was used to route calls to Session Manager. Route pattern 1 was configured using the parameters highlighted below. ▪ **Pattern Name**: Any descriptive name. ▪ **Grp No**: ***1*** This field is set to the trunk group number defined in **Step 6**. ▪ **FRL**: ***0*** This field sets the Facility Restriction Level of the trunk. It must be set to an appropriate level to allow authorized users to access the trunk.



```
change route-pattern 1                                           Page   1 of   3
                     Pattern Number: 1   Pattern Name: to SM_21_31
                              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: 1    0                    0                                         n   user
  2:                                                                     n   user
  3:                                                                     n   user
  4:                                                                     n   user
  5:                                                                     n   user
  6:                                                                     n   user

      BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
     0 1 2 M 4 W     Request                                 Dgts Format
                                                          Subaddress
  1: y y y y y n  n            rest                               lev0-pvt  none
  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
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as shown in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface. System Manager delivers a set of shared, secure management services and a common console across multiple products in the Avaya Aura® network, including the central administration of routing policies, and a common format for logs and alarms.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

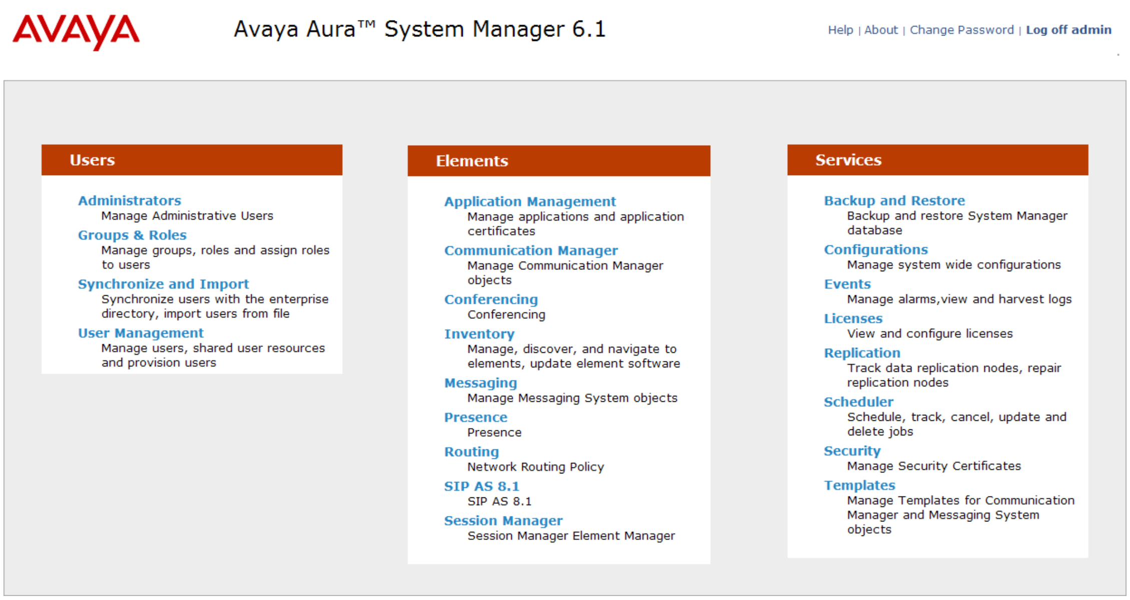
The Session Manager server provides the network interface for all inbound and outbound SIP signaling to all provisioned SIP entities. During compliance testing, the IP address assigned to the SIP signaling interface is 10.64.21.31 as specified in **Figure 1**. The Session Manager server also has a separate network interface used for connectivity to System Manager for provisioning Session Manager. The IP address assigned to the Session Manager management interface is 10.64.21.30.

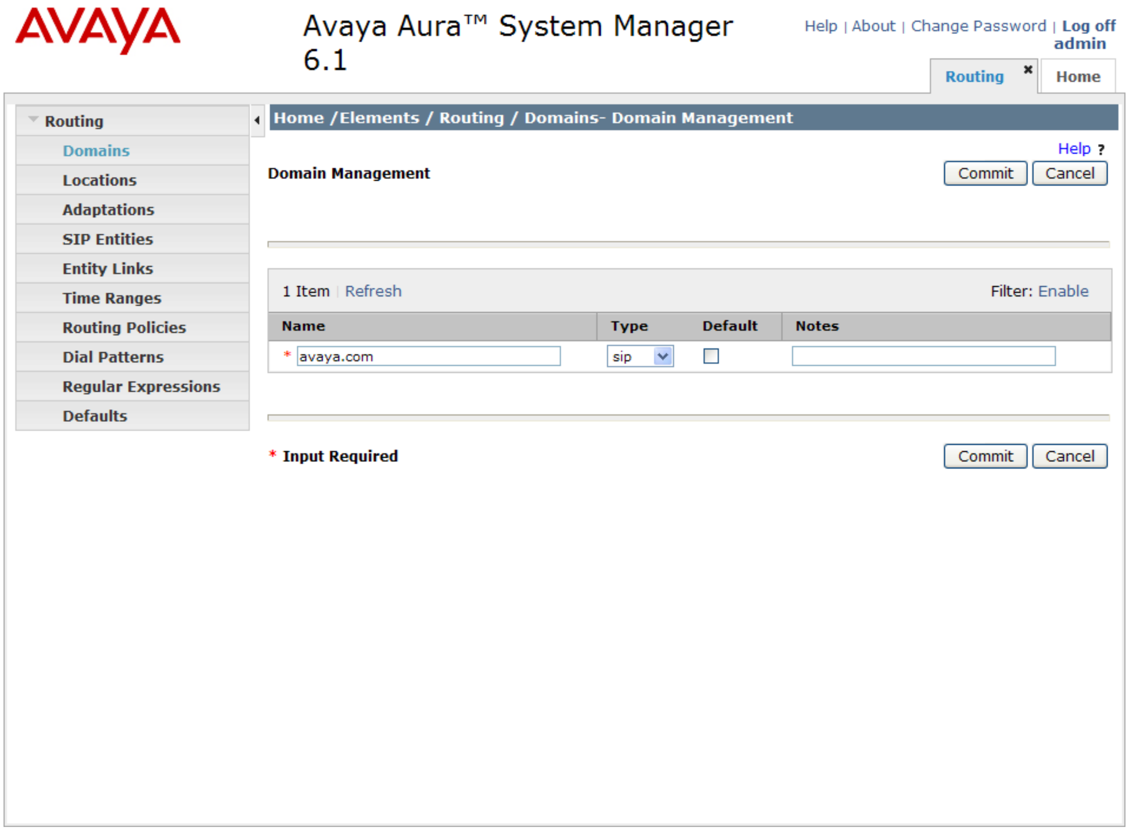
The procedures described in this section include configurations for the following:

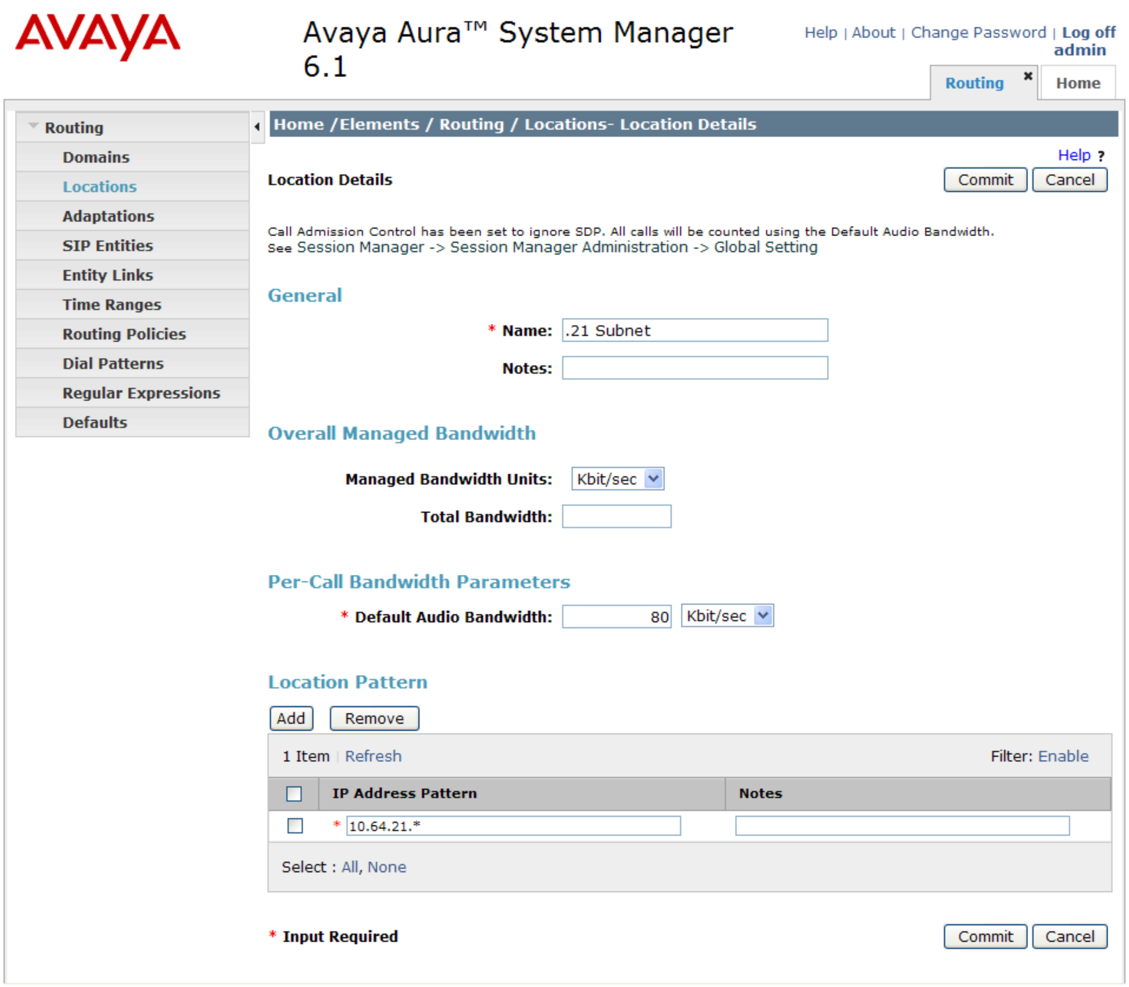
- **SIP Domains** – SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Network Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS).
- **Locations** – Locations define the physical and/or logical locations in which SIP Entities reside. Call Admission Control (CAC) / bandwidth management may be administered for each location to limit the number of calls to and from a particular Location.
- **SIP Entities** – SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- **Entity Links** – Entity Links define the SIP trunk/link parameters, e.g., ports, protocol (UDP/TCP/TLS), and trust relationship, between Session Manager instances and other SIP Entities.
- **Time Ranges** – Time Ranges specify customizable time periods, e.g., Monday through Friday from 9AM to 5:59PM, Monday through Friday 6PM to 8:59AM, all day Saturday and Sunday, etc. A Network Routing Policy may be associated with one or more Time Ranges during which the Network Routing Policy is in effect.
- **Routing Policies** – Routing Policies are used in conjunction with a Dial Patterns to specify a SIP Entity that a call should be routed to.
- **Dial Patterns** – A Dial Pattern specifies a set of criteria and a set of Network Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one of the Network Routing Policies specified in the Dial Pattern. The

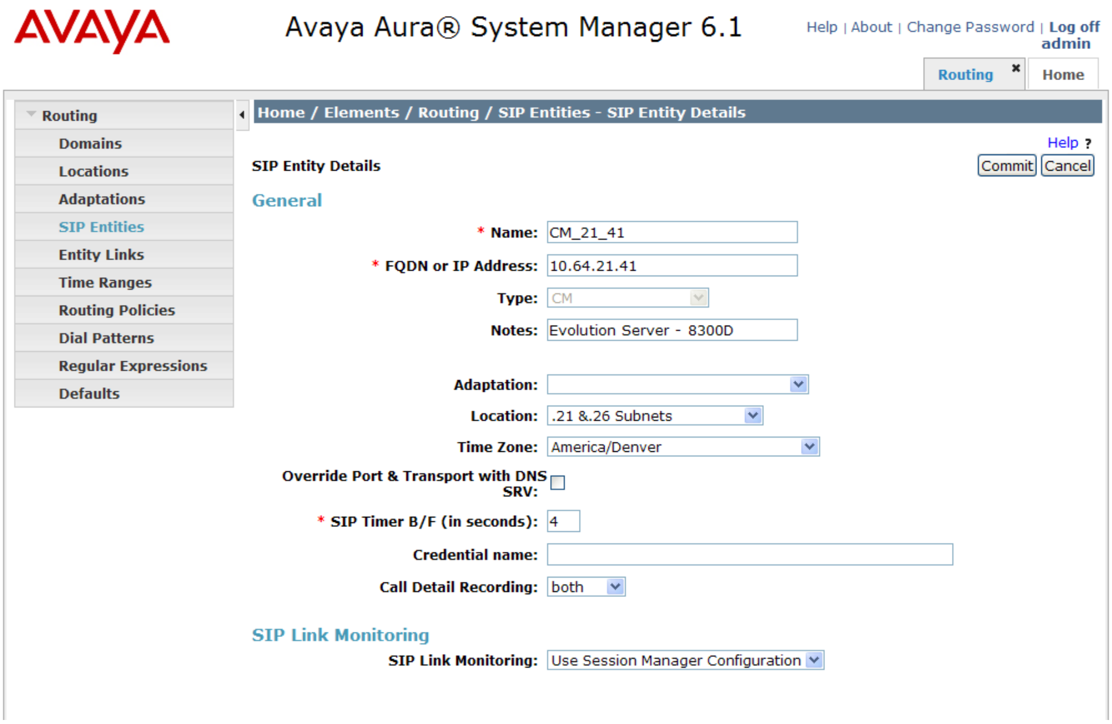
selected Network Routing Policy in turn specifies the SIP Entity to which the call is to be routed.

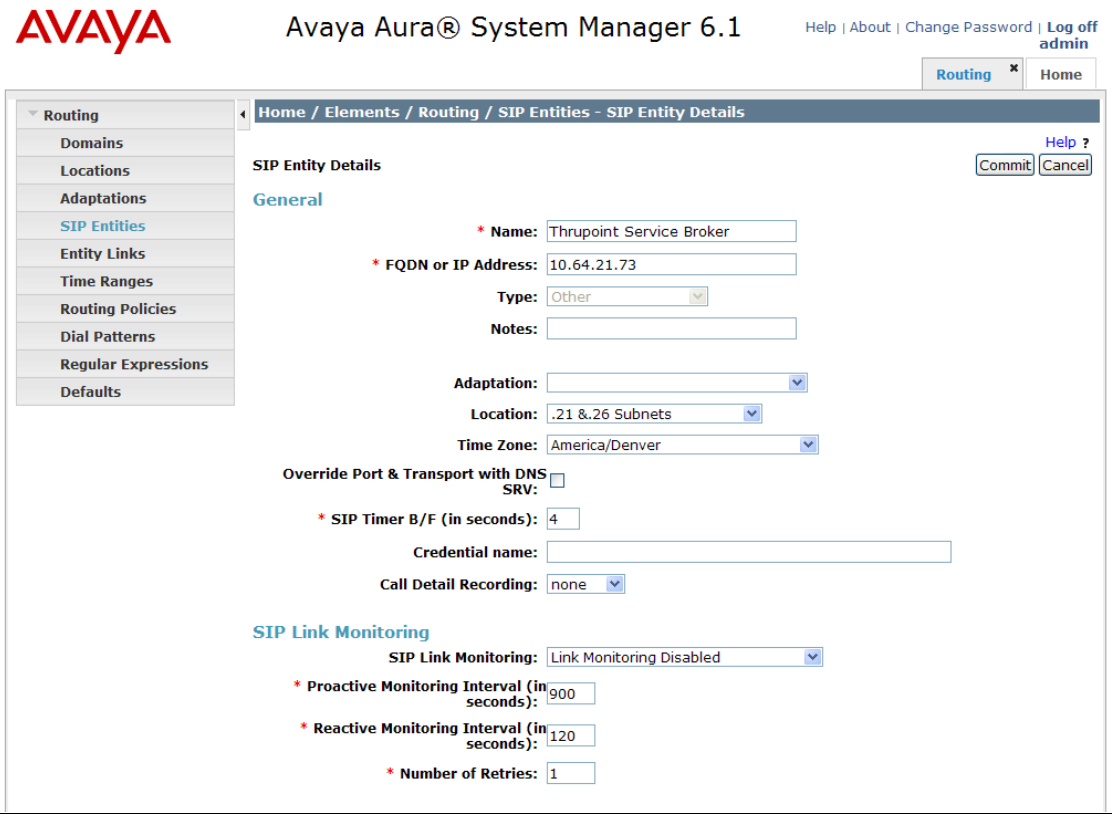
- **Applications –** Application entries are used to define and manage single applications with application attributes for inclusion into one or more application sequences.
- **Application Sequences** – An Application Sequence enables defining and managing an ordered set of applications using in call sequencing. These application sets can be associated as the origination and/or termination application sequence for a registered user's "Communication Profile" in the User Management module and enable routing every incoming, outgoing, or combined call for that user.
- **Users** – Users that register with Session Manager.

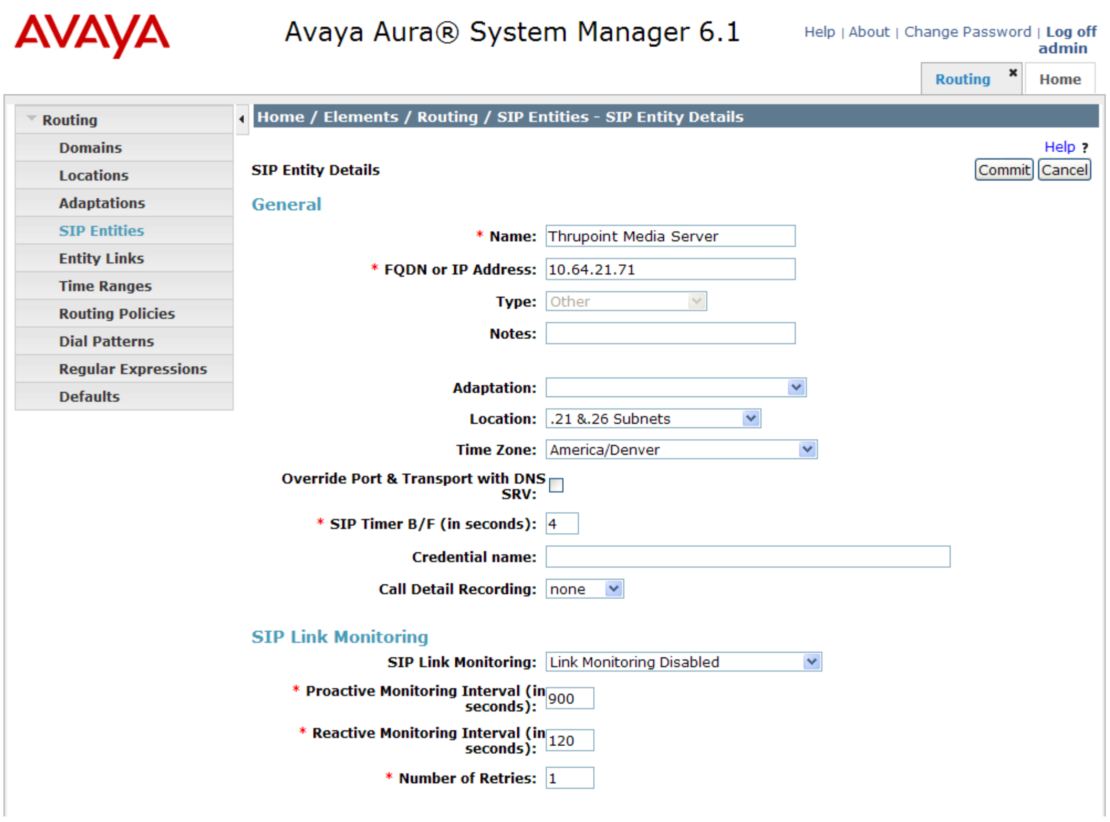
Step	Description
1.	**Login** Access the Session Manager administration web interface by entering https://<*ip-addr*>/network-login/ as the URL in an Internet browser, where <*ip-addr*> is the IP address of the System Manager server. Log in using appropriate credentials. The main page for the administrative interface is shown below.  Avaya Aura™ System Manager 6.1 Help | About | Change Password | **Log off admin** **Users** **Administrators** Manage Administrative Users **Groups & Roles** Manage groups, roles and assign roles to users **Synchronize and Import** Synchronize users with the enterprise directory, import users from file **User Management** Manage users, shared user resources and provision users **Elements** **Application Management** Manage applications and application certificates **Communication Manager** Manage Communication Manager objects **Conferencing** Conferencing **Inventory** Manage, discover, and navigate to elements, update element software **Messaging** Manage Messaging System objects **Presence** Presence **Routing** Network Routing Policy **SIP AS 8.1** SIP AS 8.1 **Session Manager** Session Manager Element Manager **Services** **Backup and Restore** Backup and restore System Manager database **Configurations** Manage system wide configurations **Events** Manage alarms,view and harvest logs **Licenses** View and configure licenses **Replication** Track data replication nodes, repair replication nodes **Scheduler** Schedule, track, cancel, update and delete jobs **Security** Manage Security Certificates **Templates** Manage Templates for Communication Manager and Messaging System objects

Step	Description
2.	**Add SIP Domain** The **Routing** menu contains all the configuration tasks listed at the beginning of this section. During compliance testing, one SIP Domain was configured. Navigate to **Routing→Domains**, and click the **New** button (not shown) to add the SIP domain with • **Name**: ***avaya.com*** (as set in **Section 8, Step 2**) • **Notes**: optional descriptive text Click **Commit** to save the configuration.  AVAYA Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin Routing Home Routing Domains Locations Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults Home /Elements / Routing / Domains- Domain Management Help ? Domain Management Commit Cancel 1 Item | Refresh Filter: Enable Name: * avaya.com Type: sip Default: □ Notes: * Input Required Commit Cancel

Step	Description
3.	**Add Location** Locations identify logical and/or physical locations where SIP entities reside. Only one Location was configured at each site for compliance testing. Navigate to **Routing→Locations** and click the **New** button (not shown) to add the Location. Under **General**: • **Name**: a descriptive name • **Notes**: optional descriptive text Under **Location Pattern**, click the **Add** button to add a new line: • **IP Address Pattern**: ***10.64.21.**** • **Notes**: optional descriptive text Click **Commit** to save the configuration.  Avaya Aura™ System Manager 6.1 Home /Elements / Routing / Locations- Location Details Location Details Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting General * Name: .21 Subnet Notes: Overall Managed Bandwidth Managed Bandwidth Units: Kbit/sec Total Bandwidth: Per-Call Bandwidth Parameters * Default Audio Bandwidth: 80 Kbit/sec Location Pattern Add Remove 1 Item | Refresh Filter: Enable □ IP Address Pattern | Notes □ * 10.64.21.* | Select : All, None * Input Required Commit Cancel

Step	Description
4.	**Add SIP Entities** A SIP Entity must be added for Session Manager (not shown) and for each SIP-based telephony system supported by it using SIP trunks. During compliance testing, a SIP Entity was added for the Session Manager itself, Communication Manager, the Thrupoint Service Broker, and the Thrupoint Media Server. Navigate to **Routing→SIP Entities**, and click the **New** button (not shown) to add a SIP Entity. The configuration details for the SIP Entity defined for the Communication Manager are as follows: Under **General**: • **Name**: a descriptive name • **FQDN or IP Address**: ***10.64.21.41*** as specified in **Figure 1**. • **Type**: select ***CM*** Default settings can be used for the remaining fields. Click **Commit** to save the SIP Entity definition. The screen below shows the SIP Entity configuration details for Communication Manager.  Home / Elements / Routing / SIP Entities - SIP Entity Details SIP Entity Details General * Name: CM_21_41 * FQDN or IP Address: 10.64.21.41 Type: CM Notes: Evolution Server - 8300D Adaptation: Location: .21 &.26 Subnets Time Zone: America/Denver Override Port & Transport with DNS SRV: □ * SIP Timer B/F (in seconds): 4 Credential name: Call Detail Recording: both SIP Link Monitoring SIP Link Monitoring: Use Session Manager Configuration

Step	Description
	Add SIP Entities (continued) – Thrupoint Service Broker The screen below shows the SIP Entity configuration details for the Thrupoint Service Broker. Note the ***Other*** selection for **Type**. Although **SIP Link Monitoring** was disabled during compliance testing, it is recommended to leave this field enabled. The default setting is ***Use Session Manager Configuration***.  AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin Routing Home Routing Domains Locations Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults Home / Elements / Routing / SIP Entities - SIP Entity Details Help ? Commit Cancel SIP Entity Details General * Name: Thrupoint Service Broker * FQDN or IP Address: 10.64.21.73 Type: Other Notes: Adaptation: Location: .21 &.26 Subnets Time Zone: America/Denver Override Port & Transport with DNS SRV: □ * SIP Timer B/F (in seconds): 4 Credential name: Call Detail Recording: none SIP Link Monitoring SIP Link Monitoring: Link Monitoring Disabled * Proactive Monitoring Interval (in seconds): 900 * Reactive Monitoring Interval (in seconds): 120 * Number of Retries: 1

Step	Description
	Add SIP Entities (continued) – Thrupoint Media Server The screen below shows the SIP Entity configuration details for the Thrupoint Media Server. Note the ***Other*** selection for **Type**. Although **SIP Link Monitoring** was disabled during compliance testing, it is recommended to leave this field enabled. The default setting is ***Use Session Manager Configuration***.  AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin Routing Home Routing Domains Locations Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults Help ? Commit Cancel Home / Elements / Routing / SIP Entities - SIP Entity Details SIP Entity Details General * Name: Thrupoint Media Server * FQDN or IP Address: 10.64.21.71 Type: Other Notes: Adaptation: Location: .21 &.26 Subnets Time Zone: America/Denver Override Port & Transport with DNS SRV: □ * SIP Timer B/F (in seconds): 4 Credential name: Call Detail Recording: none SIP Link Monitoring SIP Link Monitoring: Link Monitoring Disabled * Proactive Monitoring Interval (in seconds): 900 * Reactive Monitoring Interval (in seconds): 120 * Number of Retries: 1

Step	Description
5.	**Add Entity Links**

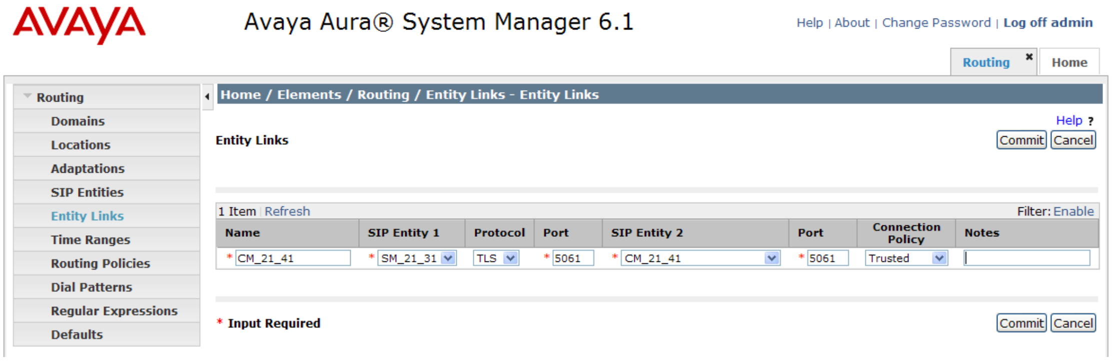
A SIP trunk between Session Manager and a telephony system is described by an Entity link. Three Entity Links were created:

- Session Manager ←→ Communication Manger
- Session Manager ←→ Thrupoint Service Broker
- Session Manager ←→ Thrupoint Media Server

Navigate to **Routing→Entity Links**, and click the **New** button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager to Communication Manager.

- **Name**: a descriptive name
- **SIP Entity 1**: select the Session Manager SIP Entity.
- **Port**: ***5061***. This is the port number to which the other system sends SIP requests.
- **SIP Entity 2**: select the Communication Manager SIP Entity.
- **Port**: ***5061***. This is the port number on which the other system receives SIP requests.
- **Trusted**: check this box
- **Protocol**: select ***TLS*** as the transport protocol.
- **Notes**: optional descriptive text

Click **Commit** to save the configuration.



Home / Elements / Routing / Entity Links - Entity Links

Entity Links

1 Item | Refresh Filter: Enable

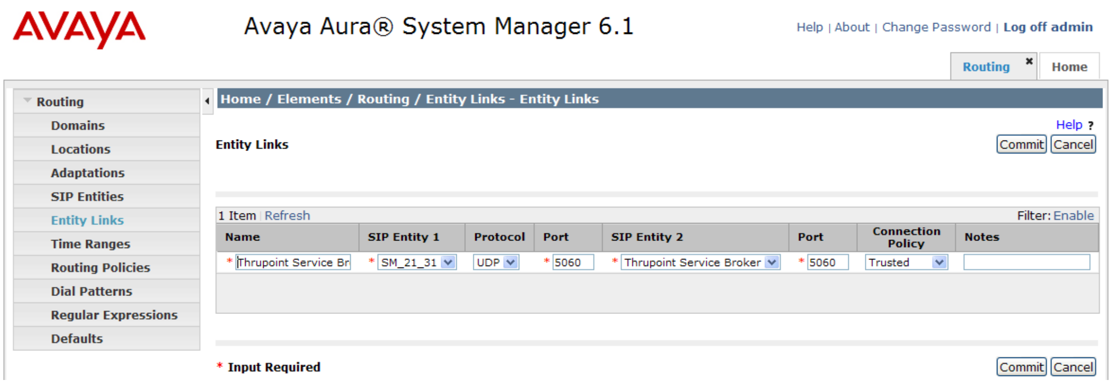
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* CM_21_41	* SM_21_31	TLS	* 5061	* CM_21_41	* 5061	Trusted	

* Input Required

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td></td><td>

Add Entity Links (continued)

The Entity Link for connecting Session Manager to the Thrupoint Service Broker was similarly defined as shown in the screen below. Only the UDP protocol was compliance tested; however, Thrupoint does support both TCP and TLS for this connection as well.



Home / Elements / Routing / Entity Links - Entity Links

Entity Links

1 Item Refresh

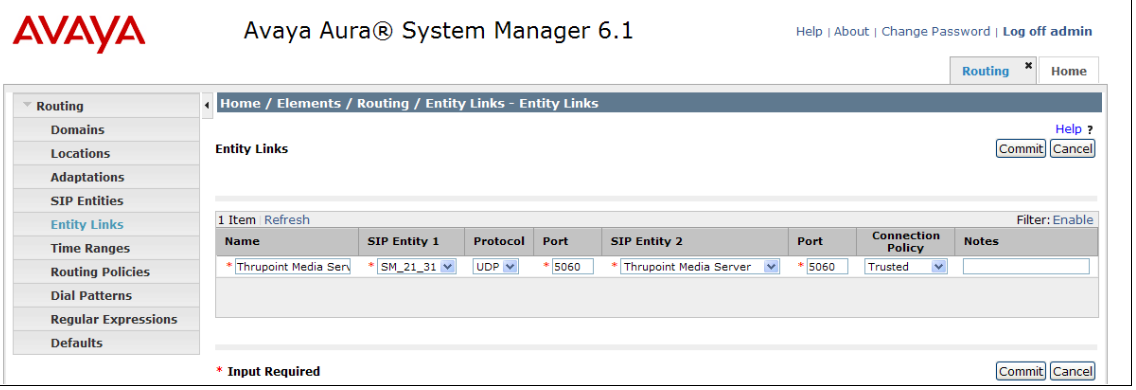
<table>
<tr><th>Name</th><th>SIP Entity 1</th><th>Protocol</th><th>Port</th><th>SIP Entity 2</th><th>Port</th><th>Connection Policy</th><th>Notes</th></tr>
<tr><td>* Thrupoint Service Br</td><td>* SM_21_31</td><td>UDP</td><td>* 5060</td><td>* Thrupoint Service Broker</td><td>* 5060</td><td>Trusted</td><td></td></tr>
</table>

* Input Required

</td></tr>
<tr><td></td><td>

Add Entity Links (continued)

The Entity Link for connecting Session Manager to the Thrupoint Media Server was similarly defined as shown in the screen below. Only the UDP protocol was compliance tested; however, Thrupoint does support both TCP and TLS for this connection as well.



Home / Elements / Routing / Entity Links - Entity Links

Entity Links

1 Item Refresh

<table>
<tr><th>Name</th><th>SIP Entity 1</th><th>Protocol</th><th>Port</th><th>SIP Entity 2</th><th>Port</th><th>Connection Policy</th><th>Notes</th></tr>
<tr><td>* Thrupoint Media Serv</td><td>* SM_21_31</td><td>UDP</td><td>* 5060</td><td>* Thrupoint Media Server</td><td>* 5060</td><td>Trusted</td><td></td></tr>
</table>

* Input Required

</td></tr>
</table>

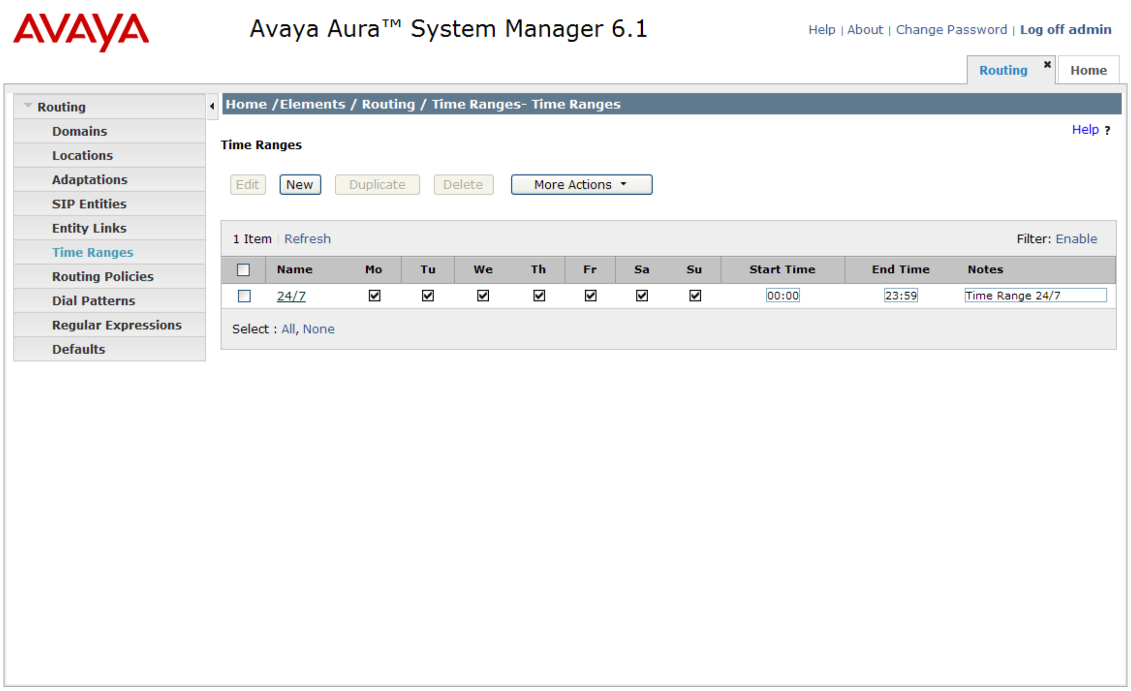
Step	Description
6.	**Add Time Ranges**

Before adding routing policies (configured in next step), time ranges must be defined during which the policies will be active. One Time Range was defined that would allow routing to occur at anytime.

Navigate to **Routing→Time Ranges**, and click the **New** button to add a new Time Range:

- **Name**: a descriptive name
- **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. The screen below shows the configured Time Range.



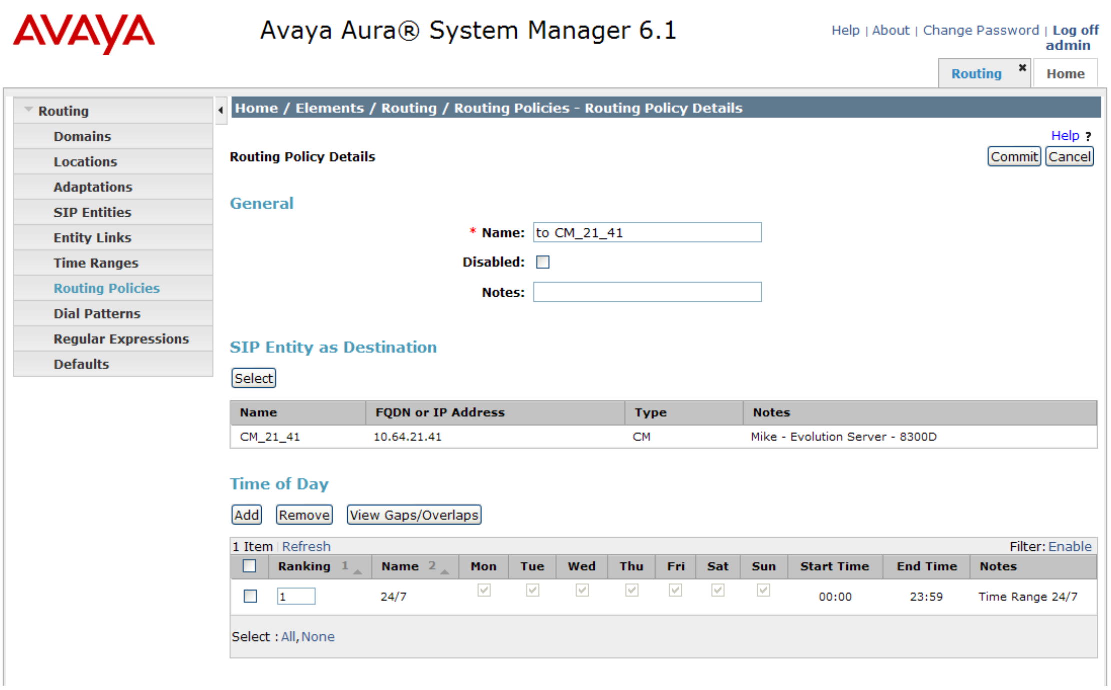
☐	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
☐	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Step	Description
7.	**Add Routing Policies** Routing policies describe the conditions under which calls will be routed to the SIP Entities connected to the Session Manager. A Routing Policy was added for routing calls to local extensions and PSTN calls to Communication Manager. Navigate to **Routing→Routing Policies**, and click the **New** button (not shown) to add a new Routing Policy. Under **General**: • **Name**: a descriptive name • **Notes**: optional descriptive text Under **SIP Entity as Destination** Click **Select** to select the appropriate SIP Entity to which the routing policy applies (not shown). Under **Time of Day** Click **Add** to select the Time Range configured in the previous step (not shown). Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

Step	Description

Add Routing Policies (continued)

The screen below shows the configuration details for the Routing Policy to route calls to Communication Manager.



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

Routing Policy Details

General

* Name: to CM_21_41

Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CM_21_41	10.64.21.41	CM	Mike - Evolution Server - 8300D

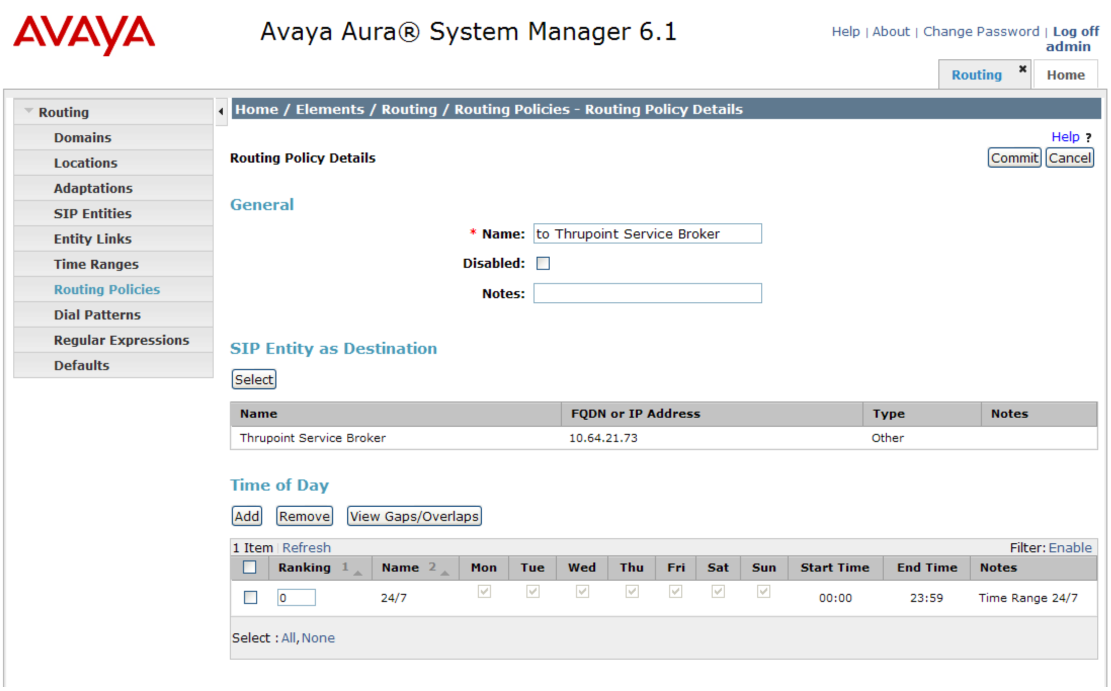
Time of Day

1 Item

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	1	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

A Routing Policy to route calls to the Thrupoint Service Broker was similarly defined as shown in the screen below.



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

Routing Policy Details

General

* Name: to Thrupoint Service Broker

Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Thrupoint Service Broker	10.64.21.73	Other	

Time of Day

1 Item

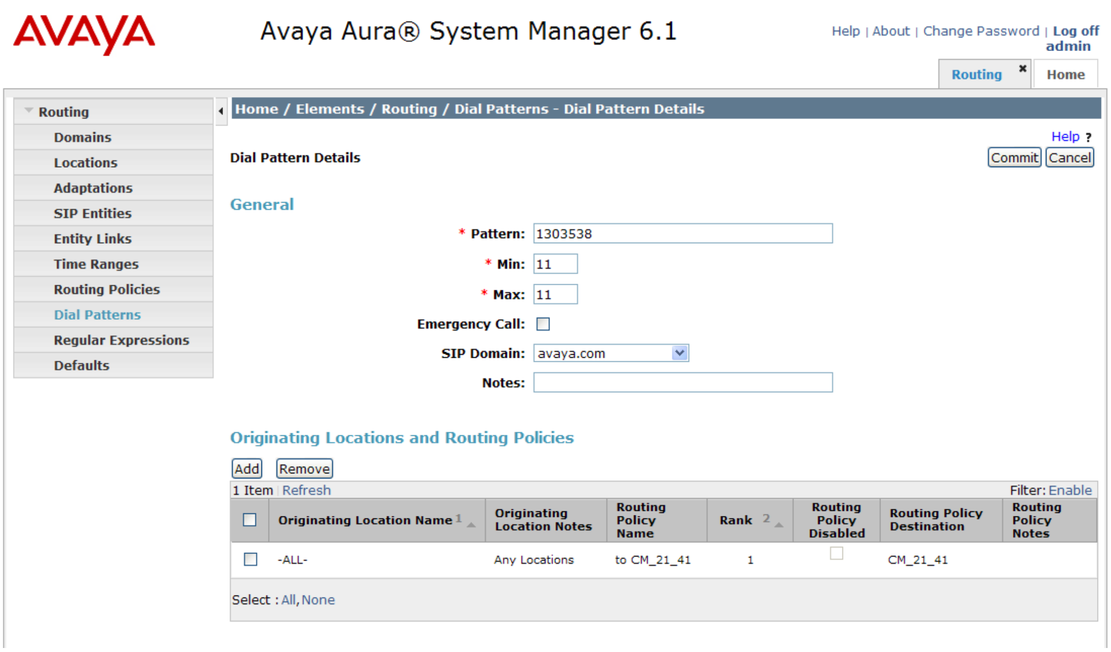
□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Step	Description
8.	**Add Dial Patterns** Dial Patterns define digit strings to be matched against dialed numbers for directing calls to the appropriate SIP Entities. 11-digit PSTN numbers beginning with "1303538" and "1917" were routed to the Communication Manager for onward routing to the PSTN. Navigate to **Routing→Dial Patterns**, click the **New** button (not shown) to add a new Dial Pattern. Under **General**: • **Pattern**: dialed number or prefix • **Min**: minimum length of dialed number • **Max**: maximum length of dialed number • **SIP Domain**: select the SIP Domain created in **Step 2** (or select **–ALL–** to be less restrictive) • **Notes**: optional descriptive text Under **Originating Locations and Routing Policies** Click **Add** to select the appropriate originating Location and Routing Policy from the list (not shown). Under **Time of Day** Click **Add** to select the time range configured in **Step 6**. Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

Add Dial Patterns (continued)

The screens below shows the configuration details for the Dialed Pattern defined for routing PSTN calls to Communication Manager.



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

Dial Pattern Details

General

* Pattern: 1303538

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: avaya.com

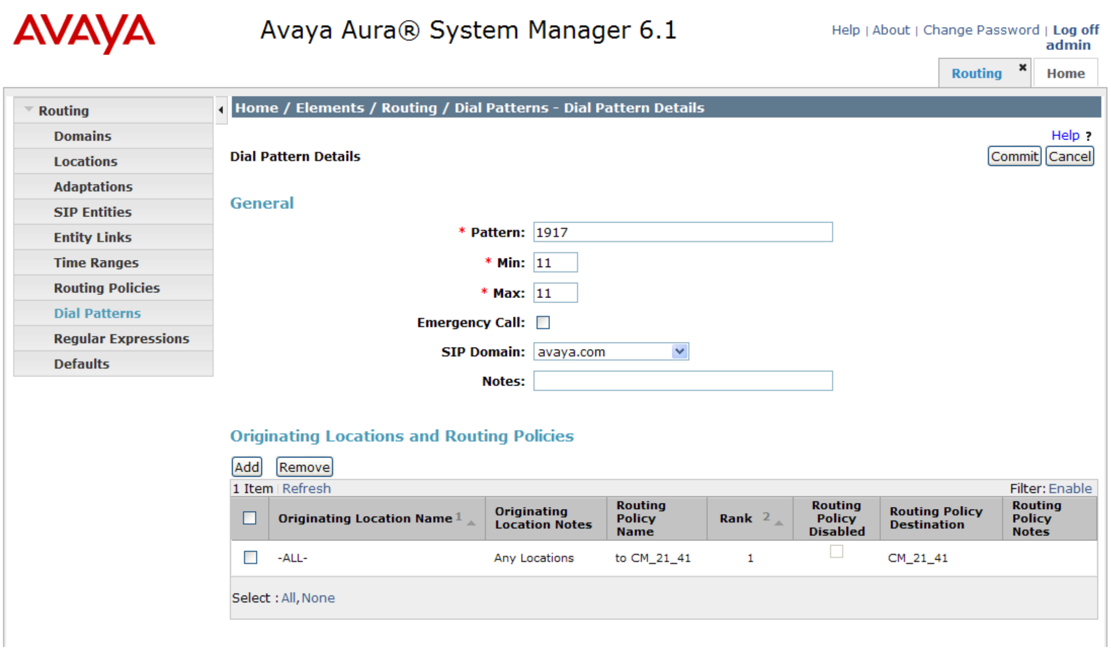
Notes:

Originating Locations and Routing Policies

1 Item | Refresh

☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-	Any Locations	to CM_21_41	1	☐	CM_21_41	

Select : All, None



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

Dial Pattern Details

General

* Pattern: 1917

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

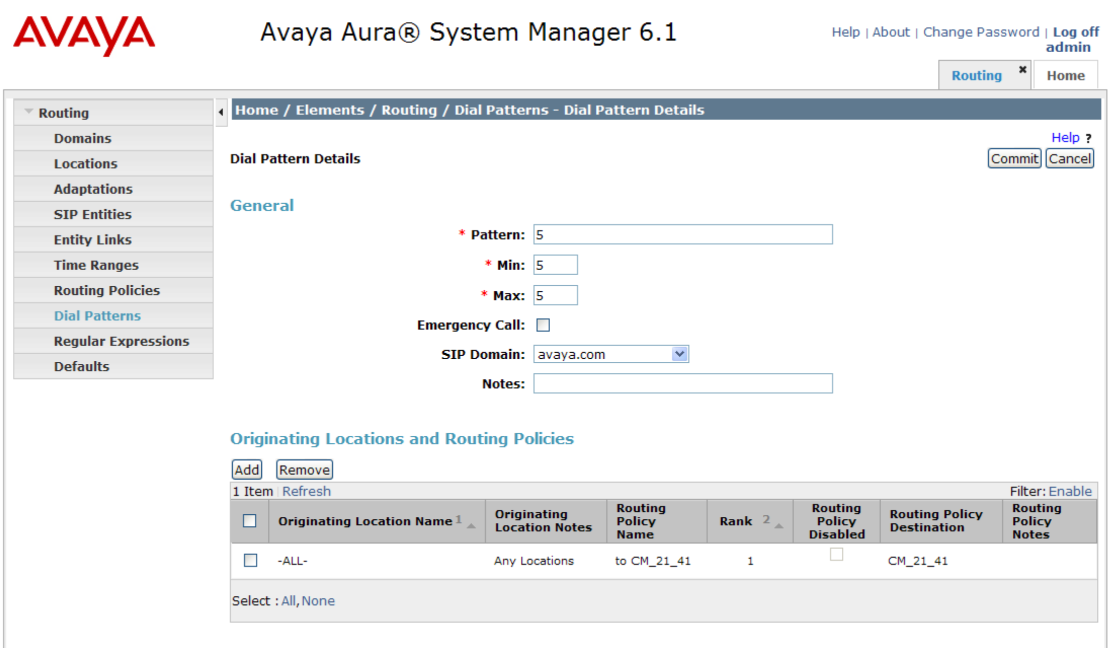
1 Item | Refresh

☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-	Any Locations	to CM_21_41	1	☐	CM_21_41	

Select : All, None

Add Dial Patterns (continued)

The screen below shows the configuration details for the Dialed Pattern defined for routing local extension (e.g. 5xxxx) calls to Communication Manager.



Dial Pattern Details

General

* Pattern:	5
* Min:	5
* Max:	5
Emergency Call:	□
SIP Domain:	avaya.com
Notes:	

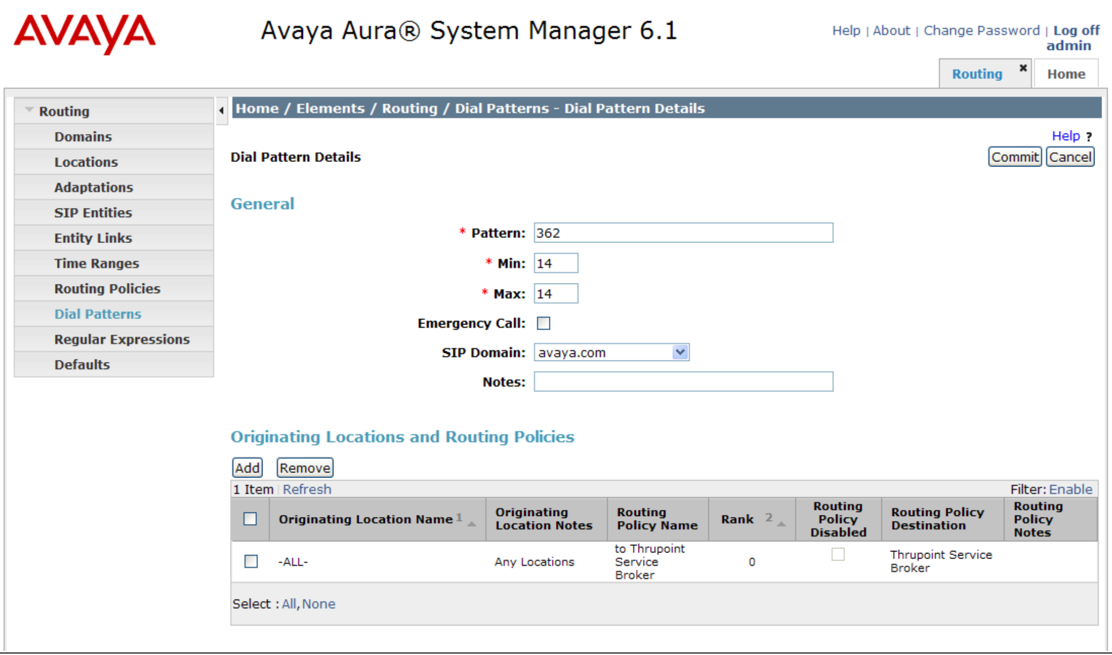
Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	to CM_21_41	1	□	CM_21_41	

Select : All, None

The screen below shows the configuration details for the Dialed Pattern defined for routing EC500 calls to the Thrupoint Service Broker. Note that the digits **362** are only steering digits and will be stripped by Thrupoint.



Dial Pattern Details

General

* Pattern:	362
* Min:	14
* Max:	14
Emergency Call:	□
SIP Domain:	avaya.com
Notes:	

Originating Locations and Routing Policies

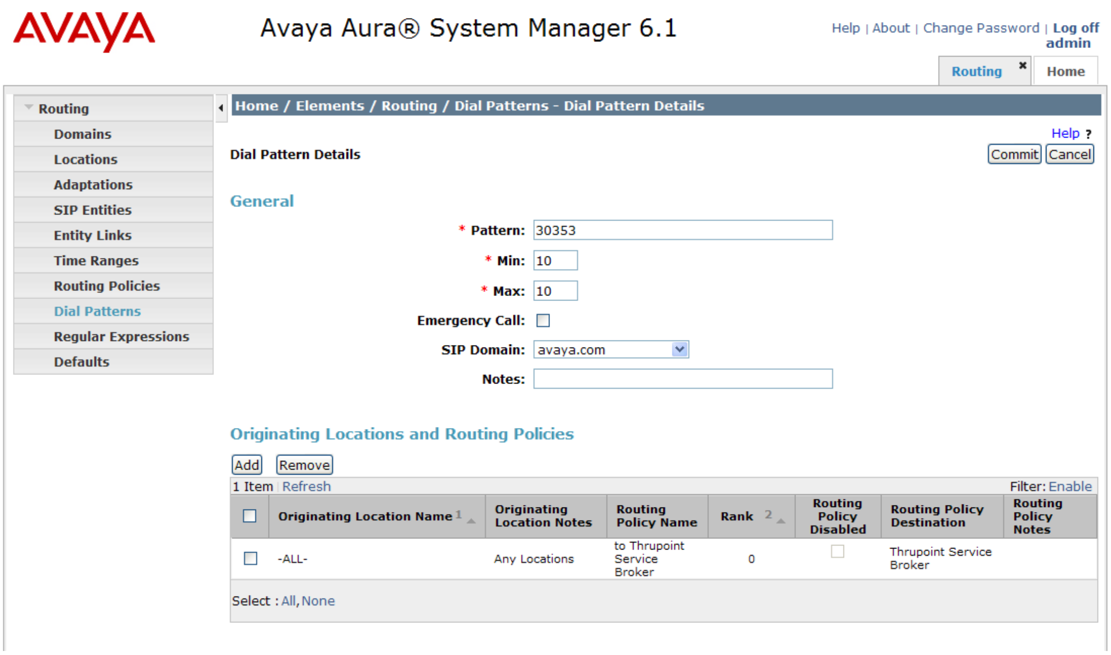
1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	to Thrupoint Service Broker	0	□	Thrupoint Service Broker	

Select : All, None

Add Dial Patterns (continued)

The screen below shows the configuration details for the Dialed Pattern defined for routing 3035383501 to the Thrupoint Service Broker. Direct Inward Dial (DID) number 303-538-3501 was configured so that when the call came into Communication Manager from the PSTN, the call was routed to the Thrupoint Service Broker. Thrupoint's Service Broker forwards the DID into the FMC server as the access number. This call then is routed to the appropriate Mobile client and connect to the endpoint provided over the Light Weight Ubiquity Protocol (LUMP)



Dial Pattern Details

General

* Pattern: 30353

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

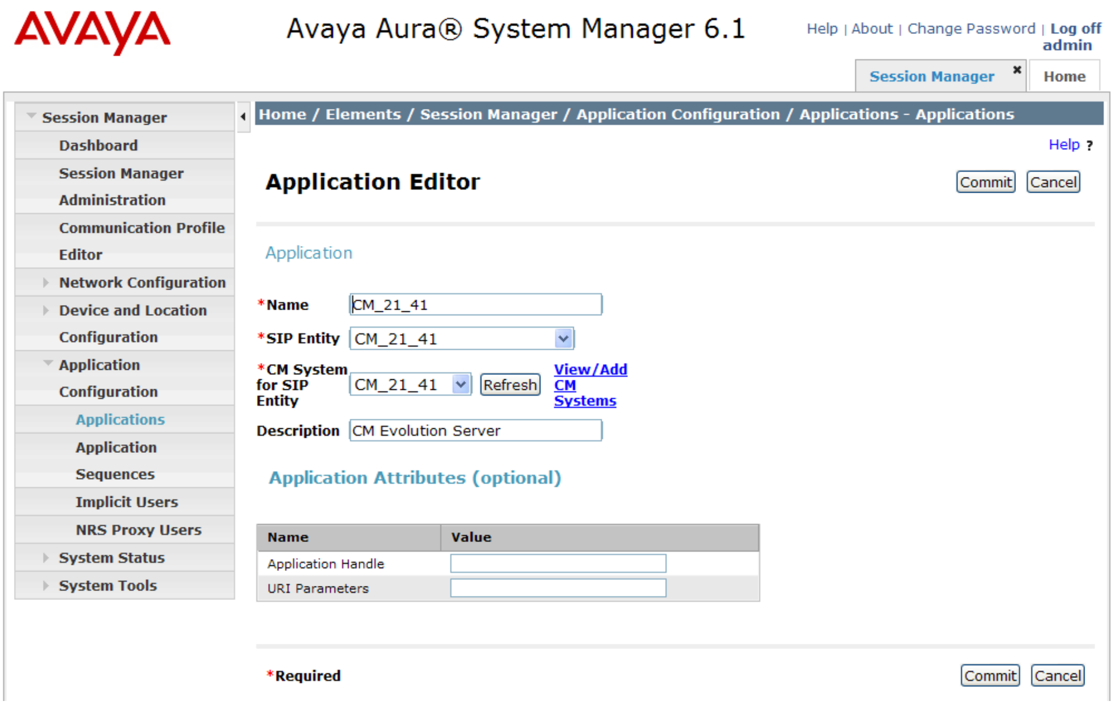
☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-	Any Locations	to Thrupoint Service Broker	0	☐	Thrupoint Service Broker	

9. **Add Application**

Application entries are used to define and manage single applications with application attributes for inclusion into one or more application sequence.

Navigate to **Session Manager →Application Configuration → Applications**, and click the **New** button to add a new Application for the Communication Manager:

- **Name**: a descriptive name
- **SIP Entity**: Select the Communication Manager SIP entity
- **CM System for SIP Entity**: Select the Communication Manager SIP Entity
- **Description**: optional descriptive text



AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
Applications
Application Sequences
Implicit Users
NRS Proxy Users
System Status
System Tools
Home / Elements / Session Manager / Application Configuration / Applications - Applications
Help ?
Commit
Cancel
Refresh
View/Add CM Systems

Application Editor

Application

*Name	CM_21_41
*SIP Entity	CM_21_41
*CM System for SIP Entity	CM_21_41
Description	CM Evolution Server

Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

*Required

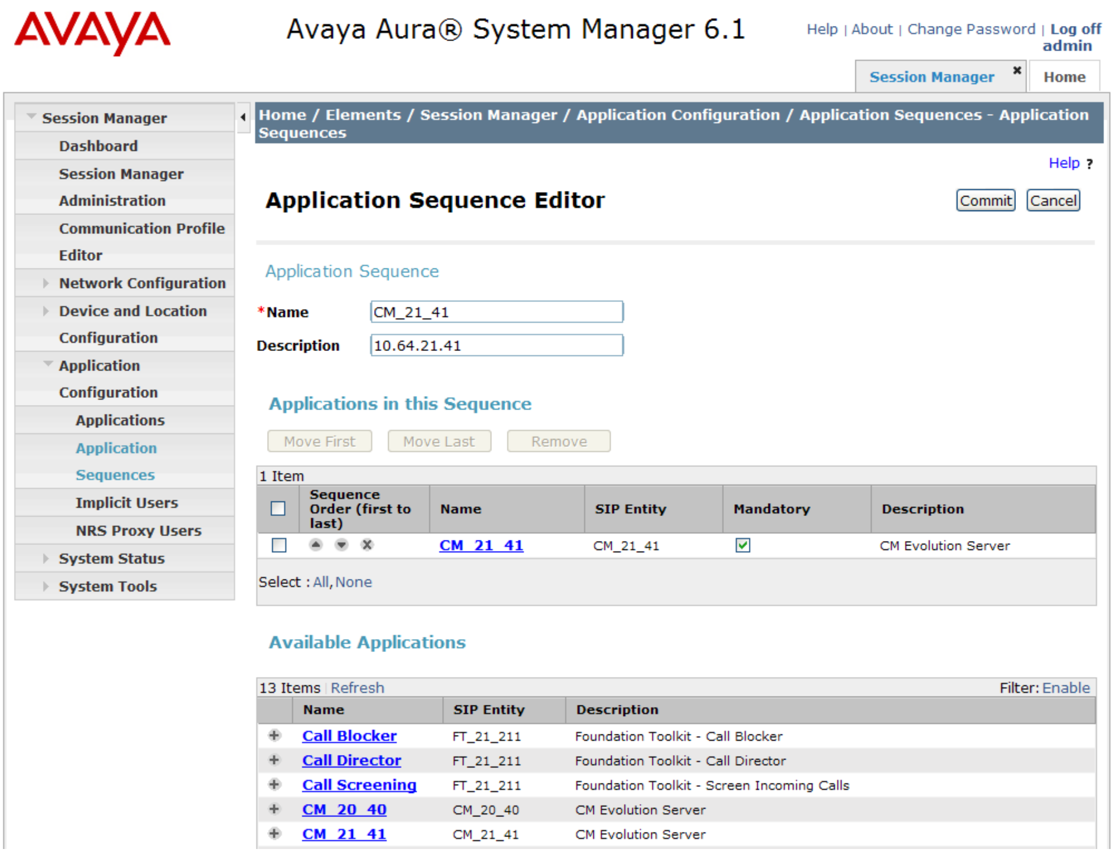
10. **Add Application Sequences**

An Application Sequence enables defining and managing an ordered set of applications using in call sequencing. These application sets can be associated as the origination and/or termination application sequence for a registered user's "Communication Profile" in the User Management module and enable routing every incoming, outgoing, or combined call for that user.

Navigate to **Session Manager** → **Application Configuration** → **Application Sequences**, and click the **New** button (not shown) to add a new Application:

- **Name**: a descriptive name
- **Description**: optional descriptive text
- Under **Available Applications**, click the "+" symbol next to the Application created in the previous step to it up to **Applications in this Sequence**. .

Click **Commit** to save the Application Sequence. The screen below shows the configured Application Sequence.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
Applications
Application Sequences
Implicit Users
NRS Proxy Users
System Status
System Tools
Home / Elements / Session Manager / Application Configuration / Application Sequences - Application Sequences
Help ?
Commit
Cancel
Move First
Move Last
Remove

Application Sequence Editor

Application Sequence

*Name	CM_21_41
Description	10.64.21.41

Applications in this Sequence

1 Item

□	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
□	▲ ▼ ✕	CM_21_41	CM_21_41	☑	CM Evolution Server

Select : All, None

Available Applications

13 Items | Refresh   Filter: Enable

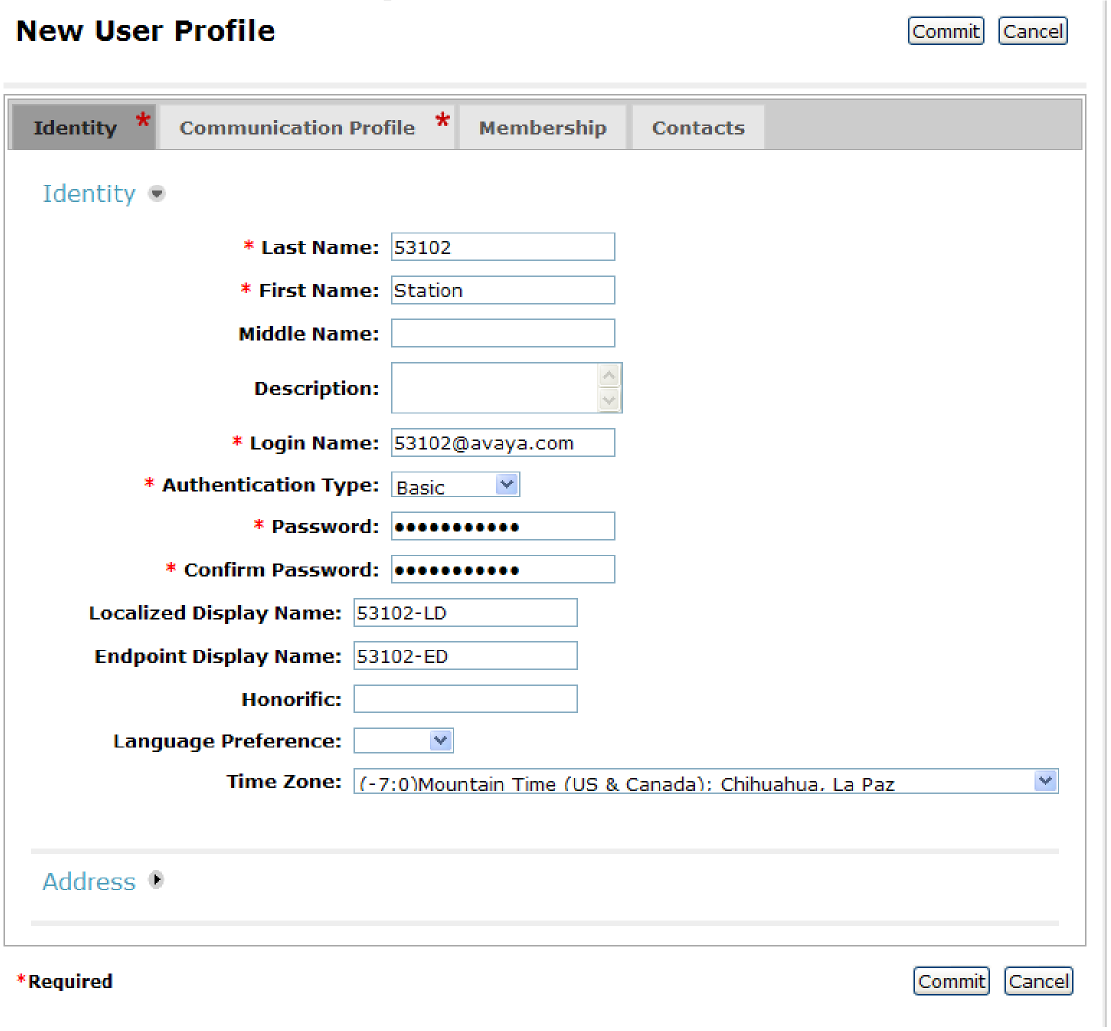
	Name	SIP Entity	Description
+	Call Blocker	FT_21_211	Foundation Toolkit - Call Blocker
+	Call Director	FT_21_211	Foundation Toolkit - Call Director
+	Call Screening	FT_21_211	Foundation Toolkit - Screen Incoming Calls
+	CM_20_40	CM_20_40	CM Evolution Server
+	CM_21_41	CM_21_41	CM Evolution Server

11. **Add Users (users that register with Session Manager)**

To add a SIP user, navigate to **User Management → Manage Users →**, and click the **New** button (not shown) to add a new User:

Under *Identity*:

- **Last**: Enter the last name of the user.
- **First**: Enter the first name of the user.
- **Login Name**: Enter a unique system login given to the user. It takes the form of username@domain (e.g. "53102@avaya.com") and it is used to create the user's primary handle.
- **Authentication Type**: Select "Basic" to have the user's login authenticated by an Avaya Authentication Server.
- **Password** and **Confirm Password**: Enter the password used to log into System Manger.
- **Localized Display Name**: Enter the localized display name of the user.
- **Endpoint Display Name**: Enter the full text name of the user represented in ASCII to support displays that cannot handle localized text.
- **Time Zone**: Select the preferred time zone of the user.



New User Profile

Identity

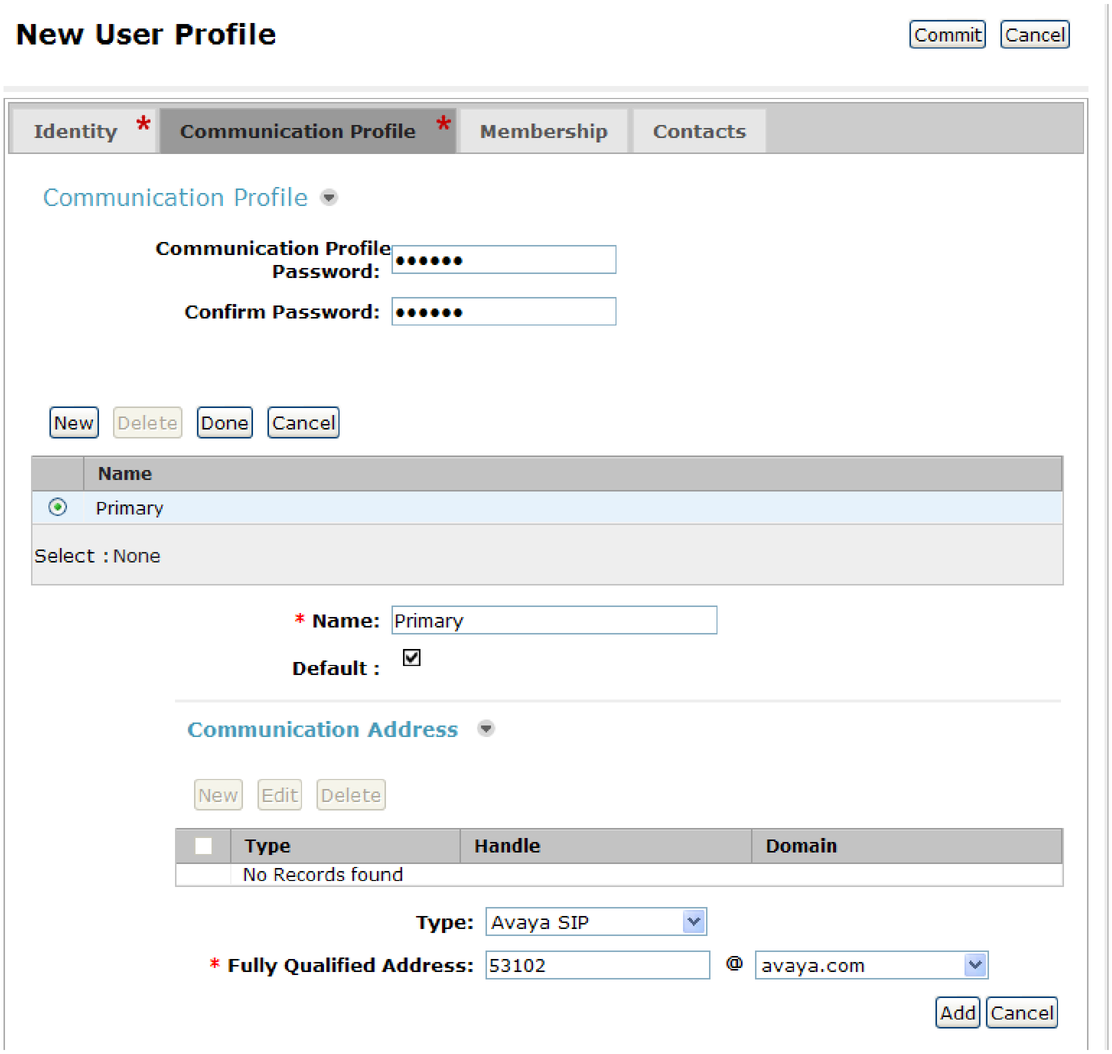
* Last Name:	53102
* First Name:	Station
Middle Name:	
Description:	
* Login Name:	53102@avaya.com
* Authentication Type:	Basic
* Password:	●●●●●●●●●●●
* Confirm Password:	●●●●●●●●●●●
Localized Display Name:	53102-LD
Endpoint Display Name:	53102-ED
Honorific:	
Language Preference:	
Time Zone:	(-7:0)Mountain Time (US & Canada); Chihuahua, La Paz

*Required

Add Users (continued – Communication Profile tab)

Under *Communication Profile*:

- **Communication Profile Password** and **Confirm Password**: Enter the user's station password/security code.
- **Type**: Select ***Avaya SIP***
- **Fully Qualified Address**: Enter the station's extension and select the appropriate domain for the user.
- Click the **Add** button.



New User Profile

Communication Profile

Communication Profile Password: ••••••

Confirm Password: ••••••

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address

□	Type	Handle	Domain
	No Records found		

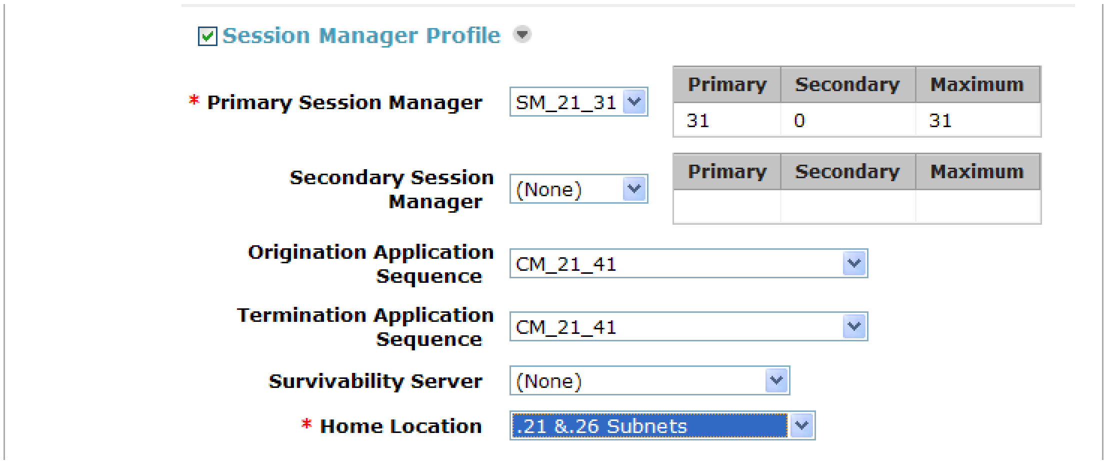
Type: Avaya SIP

* Fully Qualified Address: 53102 @ avaya.com

Add Users (continued – Communication Profile tab)

Under *Session Manager Profile*:

- **Primary Session Manager**: Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile.
- **Origination Application Sequence**: Select the Application Sequence from **Step 10** that will be invoked when calls are routed from this user.
- **Termination Application Sequence**: Select an Application Sequence that will be invoked when calls are routed to this user.
- **Home Location**: Select the Home Location of this user.



☑ Session Manager Profile

* Primary Session Manager: SM_21_31

Primary	Secondary	Maximum
31	0	31

Secondary Session Manager: (None)

Primary	Secondary	Maximum

Origination Application Sequence: CM_21_41

Termination Application Sequence: CM_21_41

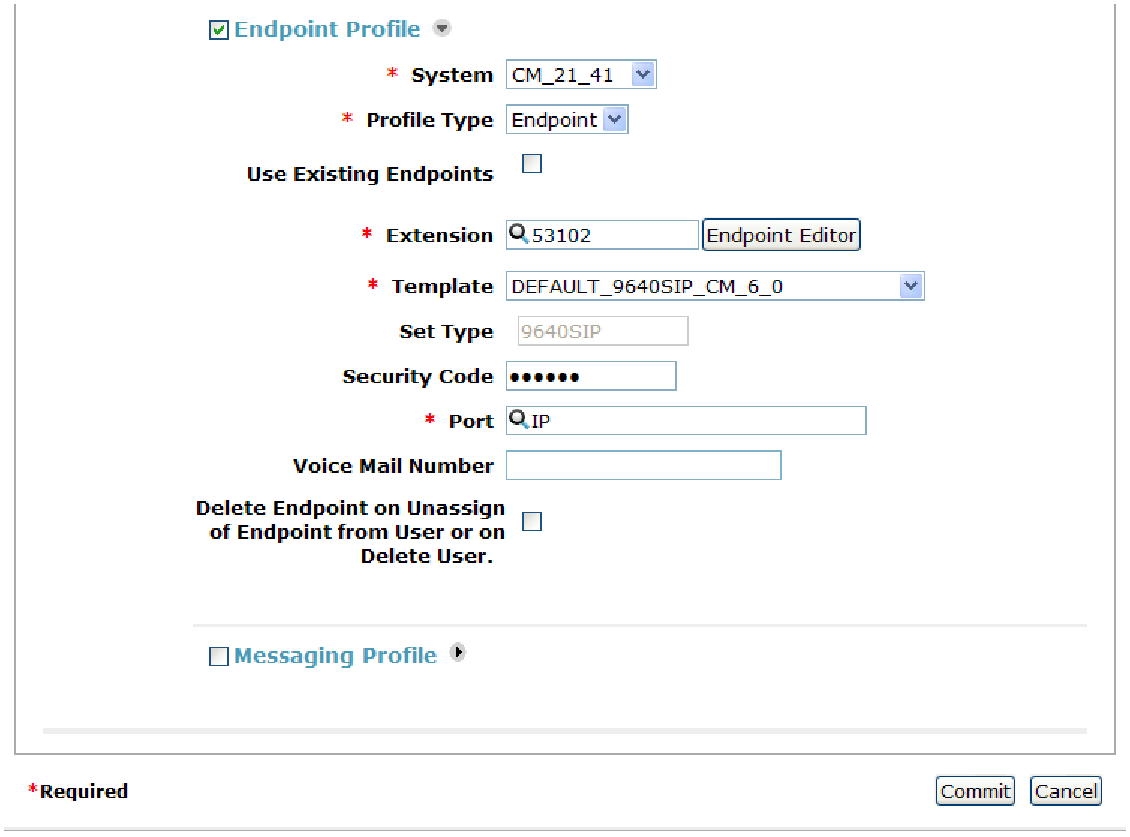
Survivability Server: (None)

* Home Location: .21 &.26 Subnets

Add Users (continued – Communication Profile tab)

Under *Endpoint Profile*:

- **System**: Select the Communication Manager system where the endpoint exists.
- **Profile Type**: Select ***Endpoint***.
- **Use Existing Endpoints:** Check this box to use an endpoint already administered in Communication Manager. Otherwise, leave the box unchecked.
- **Extension**: Enter the extension of the endpoint that you want to associate with this user.
- **Template**: Select an appropriate template for the endpoint.
- **Security Code**: Enter the security code to be used by the endpoint when registering to the Session Manager.
- **Port**: Select ***IP***.



☑ Endpoint Profile

* System CM_21_41

* Profile Type Endpoint

Use Existing Endpoints □

* Extension 53102

* Template DEFAULT_9640SIP_CM_6_0

Set Type 9640SIP

Security Code ••••••

* Port IP

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User or on Delete User. □

□ Messaging Profile

*Required

7. Configure Thrupoint Enterprise Mobility Server

This section describes the configuration of Thrupoint Enterprise Mobility Server. It assumes that the application and all required software components have been installed and properly licensed.

The tables shown below were provided by Thrupoint and represent the relevant configuration used during compliance testing. Contact Thrupoint and refer to Thrupoint's documentation for complete configuration details.

7.1. List of Location

Identifier	name
1	Avaya

7.2. List of rule-set

Name	inbound-to-domain	inbound-from-domain	outbound-to-domain	outbound-from-domain
uasm				
sb				
fmc			fmc.avaya.com	fmc.avaya.com
ms				
avaya			avaya.com	

UASM = Ubiquity Application Server Manager
SB = Service Broker
FMC = Fixed Mobile Convergence Server
MS = Media Server
Avaya = Avaya SM

7.3. List of Entity

Name	Address	Trusted	Auth-Record-Route	Rule-Set-Name
UASM	10.64.21.72	True	True	UASM
SB	10.64.21.73	True	True	SB
FMC	10.64.21.74	True	True	FMC
MS	10.64.21.71	True	True	MS
AVAYA	10.64.21.31	True	True	AVAYA

7.4. List of Routing

ID	Prefix	Domain	URL-Scheme	URL-User	URL-entity	URL-Parameters
1		avaya.com	SIP		AVAYA	
2	3035383501		SIP		FMC	

7.5. List of Digits

ID	rule-set-name	address-to-modify	direction	pattern	min-length	max-length	digits-to-delete	prepend-digits	domain
1	AVAYA	TO	INBOUND	362	1	15	3		
2	AVAYA	TO	OUTBOUND	1917	1	15	0		
3	FMC	FROM	OUTBOUND	9174	1	15	0	1	
4	AVAYA	FROM	OUTBOUND	1	1	15	0		
5	AVAYA	FROM	OUTBOUND	5	1	15	0		

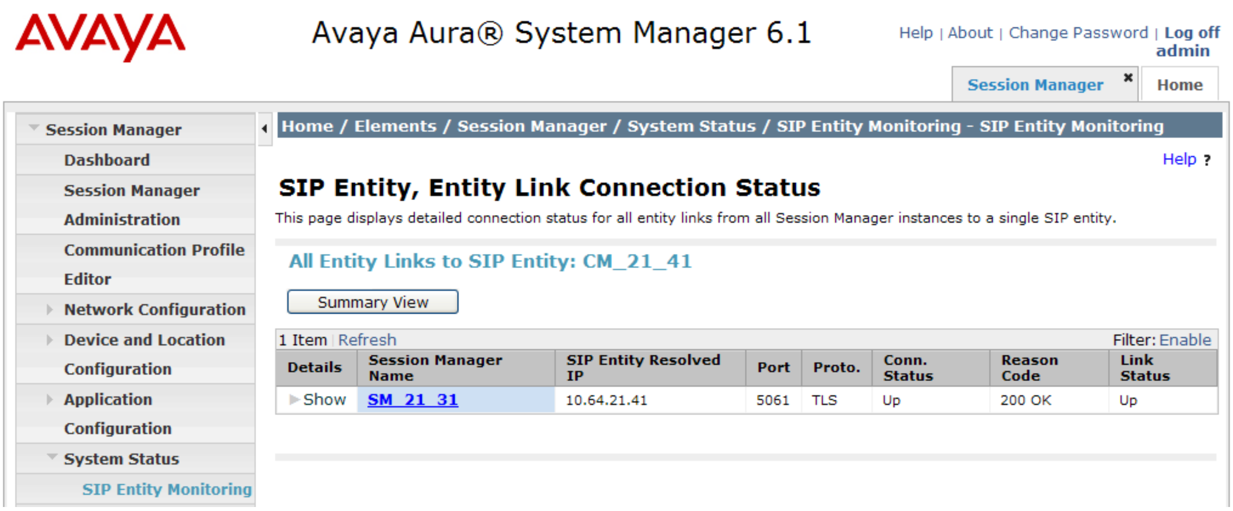
7.6. List of Adaptation

Entity	Direction	Apps
SB	outbound	OutboundDigitAdaptation
FMC	outbound	OutboundDigitAdaptation
MS	outbound	OutboundDigitAdaptation
AVAYA	outbound	OutboundDigitAdaptation
SB	inbound	InboundDigitAdaptation
FMC	inbound	InboundDigitAdaptation
MS	inbound	InboundDigitAdaptation
AVAYA	inbound	InboundDigitAdaptation

8. Verification Steps

The following steps may be used to verify the configuration:

- Using System Manager, navigate to **Session Manager→System Status→SIP Entity Monitoring**, and click on the appropriate SIP Entities to verify that the Entity Links to Communication Manager, the Thrupoint Service Broker, and the Thrupoint Media Server are up (as indicated by the **Link Status**). The Link Connection Status to Communication Manager is shown below as an example.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring
Help ?
Summary View
1 Item | Refresh
Filter: Enable

SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: CM_21_41

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▸ Show	SM_21_31	10.64.21.41	5061	TLS	Up	200 OK	Up

- From the Communication Manager SAT, use the **status signaling-group *x*** command to verify that the SIP signaling group is in-service (where ***x*** is the signaling group number associated with the trunk between Communication Manager and Session Manager).

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

- From the Communication Manager SAT, use the **status trunk-group *y*** command to verify that the SIP trunk group is in-service (where ***y*** is the trunk group number for the trunk between Communication Manager and Session Manager).

```
status trunk 1

                                TRUNK GROUP STATUS

Member    Port     Service State       Mtce Connected Ports
                                       Busy

0001/001 T00001   in-service/idle     no
0001/002 T00002   in-service/idle     no
0001/003 T00003   in-service/idle     no
0001/004 T00004   in-service/idle     no
0001/005 T00005   in-service/idle     no
0001/006 T00006   in-service/idle     no
0001/007 T00007   in-service/idle     no
0001/008 T00008   in-service/idle     no
0001/009 T00009   in-service/idle     no
0001/010 T00010   in-service/idle     no
```

- Place calls to a user's desk phone. Verify the call rings at both the desk phone and the mobile phone. Answer the call at the mobile phone. Manually move the call between the Wi-Fi and cellular networks. Verify the call and talk paths remain up.

9. Conclusion

The Thrupoint Enterprise Mobility solution passed compliance testing. These Application Notes describe the procedures required for configuring the Thrupoint Enterprise Mobility solution to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager, to support the reference configuration shown in **Figure 1**.

10. Additional References

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

[1] *Avaya Aura® Communication Manager Feature Description and Implementation*, Doc ID: 555-245-205, August 2010.
[2] *Administering Avaya Aura® Communication Manager*, Doc ID: 03-300509, August 2010.
[3] *Administering Avaya Aura® Session Manager*, Doc ID: 03-603324, May 2011.
[4] *Installing and Configuring Avaya Aura® Session Manager*, Doc ID: 03-6034723, April 2011.

Product documentation for the Thrupoint Enterprise Mobility solution may be obtained from Thrupoint. Please contact ThruPoint for access to documentation.

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.