Avaya Solution & Interoperability Test Lab

Application Notes for Polycom SoundStation IP 7000 and Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Polycom SoundStation IP 7000 which was compliance tested with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

The overall objective of the interoperability compliance testing is to verify Polycom SoundStation IP 7000 functionalities in an environment comprised of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and various Avaya H.323 and SIP IP Telephones.

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 Polycom SoundStation IP 7000 (herein refers as SoundStation IP 7000) which was compliance tested with Avaya Aura® Communication Manager and Avaya Aura® Session Manager . SoundStation IP 7000 is a SIP based IP conference phone that delivers superior performance for small to midsize conference rooms.

These Application Notes assume that Communication Manager and Session Manager are already installed and basic configuration steps have been performed. Only steps relevant to this compliance test will be described in this document.

For further details on configuration steps not covered in this document, consult **[3]**.

During the Compliance test, SoundStation IP 5000, IP 6000 and IP 7000 were simultaneously tested. Since separate Application Notes have been requested for each endpoint, these Application Notes will only mention SoundStation IP 7000.

2. General Test Approach and Test Results

The general test approach was to place calls to and from SoundStation IP 7000 and exercise basic telephone operations. The main objectives were to verify that:

- SoundStation IP 7000 successfully registers with Session Manager.
- Successfully establish calls between SoundStation IP 7000 and Avaya SIP, H.323, and digital telephones attached to Session Manager or Communication Manager.
- SoundStation IP 7000 successfully negotiates the right codec (G.711MU, G.729A and G.722-64K).
- SoundStation IP 7000 successfully holds a call.
- SoundStation IP 7000 successfully transfers a call (origination, destination, and attended).
- DTMF tone was tested and verified.
- SoundStation IP 7000 successfully establishes a three party conference call.
- SoundStation IP 7000 successfully verifies following FNE features:
  - Call Park
  - Call Pickup
  - Call Forward (Unconditional, Busy/no answer)
- Shuffling and unshuffling were tested, and verified.

For serviceability testing, failures such as cable pulls and hardware resets were applied.

2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the interoperability compliance testing was primarily on verifying call establishment on the SoundStation IP 7000. SoundStation IP 7000 operations such as inbound calls, outbound calls, hold, transfer, forward, conference, Feature Name Extension (FNE), and SoundStation IP 7000 interactions with Session Manager, Communication Manager, and Avaya SIP, H.323, and digital telephones were verified. The serviceability testing introduced failure scenarios to see if SoundStation IP 7000 can recover from failures.

2.2. Test Results

The test objectives were verified. For serviceability testing, the SoundStation IP 7000 operated properly after recovering from failures such as cable disconnects, and resets of the SoundStation IP 7000 and the Session Manager server. SoundStation IP 7000 successfully negotiated the codec that was used. The features tested and worked as expected.

Note: *Although MWI did not work, calls were be able to store in voicemail and retrieve from voice mail.*

2.3. Support

Technical documentation and software downloads for the SoundStation IP 7000 can be found at:
http://www.polycom.com/support/voice/soundstation_ip_series/soundstation_ip7000.html

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of an Avaya S8300D Server, an Avaya G450 Media Gateway, a Session Manager Server, a System Manager Server, and SoundStation IP 7000. The solution described herein is also extensible to other Avaya Media Servers and Media Gateways. Avaya S8720 Servers with an Avaya G650 Media Gateway were included in the test to provide an inter-switch scenario. For completeness, Avaya 4625 H.323 IP Telephones, Avaya 9600 Series SIP IP Telephones, Avaya 9600 Series H.323 IP Telephones, and Avaya 6400 Series Digital Telephones, are included in **Figure 1** to demonstrate calls between the SIP-based SoundStation IP 7000 and Avaya SIP, H.323, and digital telephones.

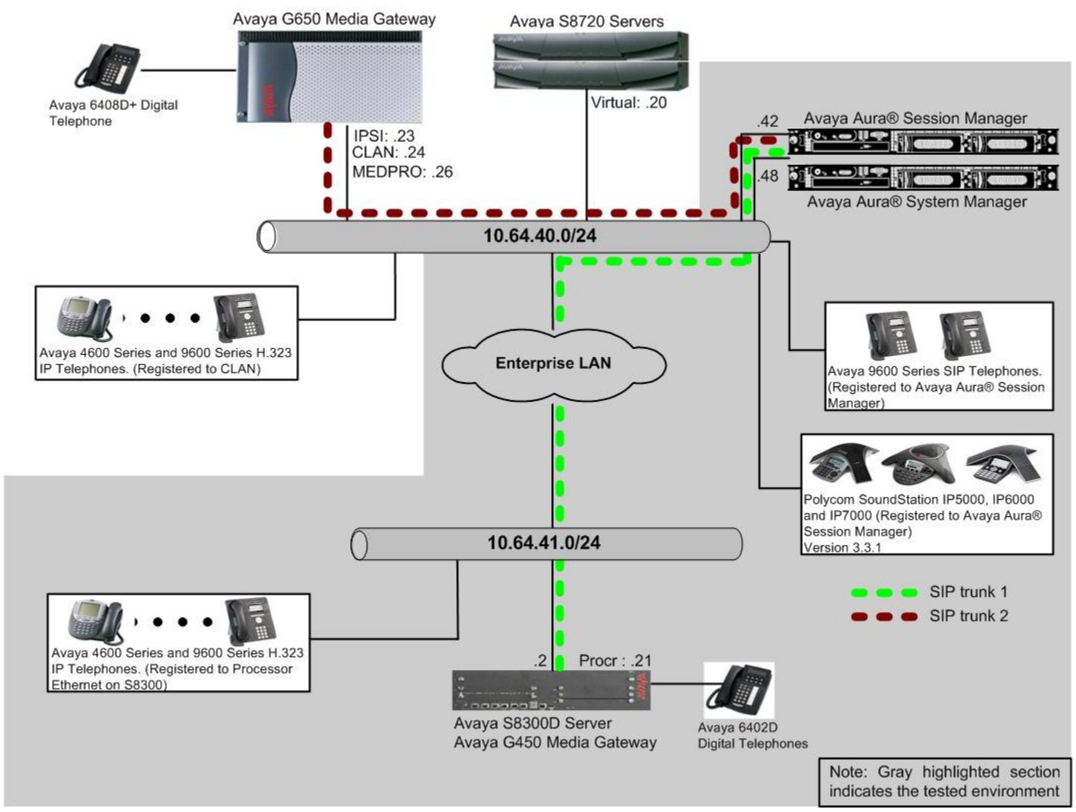


Figure 1: Test Configuration of Polycom SoundStation IP 7000

4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300D Media Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.0 (R016x.00.0.345.0) with SP 2
Avaya Aura® System Manager		6.0.6.0
Avaya Aura® Session Manager		6.0.0.0.600020
Avaya S8720 Servers with Avaya G650 Media Gateway		Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya 9600 Series SIP Telephones		
	9620 (SIP) 9630 (SIP) 9650 (SIP)	2.6.3 2.6.3 2.6.3
Avaya 4600 and 9600 Series IP Telephones		
	4625 (H.323) 9620 (H.323) 9630 (H.323) 9650 (H.323)	2.9 3.1 3.1 3.1
Avaya 6408D+ Digital Telephone		-
Polycom SoundStation IP 7000		3.3.1

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, and a SIP station. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface. SoundStation IP 7000 and other SIP telephones are configured as off-PBX telephones in Communication Manager.

5.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient Maximum Off-PBX Telephones – OPS licenses. If not, contact an authorized Avaya account representative to obtain additional licenses

```
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: 6400  211
                                      Maximum Stations: 2400  35
                              Maximum XMOBILE Stations: 2400  0
                    Maximum Off-PBX Telephones - EC500: 9600  0
                    Maximum Off-PBX Telephones -   OPS: 9600  18
                    Maximum Off-PBX Telephones - PBFMC: 9600  0
                    Maximum Off-PBX Telephones - PVFMC: 9600  0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 313   1
```

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. If not, contact an authorized Avaya account representative to obtain additional licenses.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  30
           Maximum Concurrently Registered IP Stations: 2400  5
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  110
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    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
```

5.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.3** for configuring IP network region to specify which codec sets may be used within and between network regions. During the compliance test, G.711MU, G.729A and G.722-64K were tested for verification.

```
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:
 3:
```

5.3. Configure IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and Session Manager. Enter the **change ip-network-region <n>** command, where **n** is a number between **1** and **250** inclusive, and configure the following:

- **Authoritative Domain** – Set to the appropriate domain. During the compliance test, the authoritative domain is set to **avaya.com**. This should match the SIP Domain value on Session Manager in **Section 6.1**.
- **Intra-region IP-IP Direct Audio** – Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in the same IP network region. The default value for this field is **yes**.
- **Codec Set** – Set the codec set number as provisioned in **Section 5.2**.
- **Inter-region IP-IP Direct Audio** – Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in different IP network regions. The default value for this field is **yes**.

```
change 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: 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
```

5.4. Configure IP Node Name

This section describes the steps for setting IP node name for Session Manager in Communication Manager. Enter the **change node-names ip** command, and add a node name for Session Manager and its IP address.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
SM-1                   10.64.40.42
default                0.0.0.0
msgserver-ip           10.64.41.21
msgserver-sip          10.64.41.21
procr                  10.64.41.21
procr6                 ::
```

5.5. Configure SIP Signaling

This section describes the steps for administering a signaling group in Communication Manager for communication between Communication Manager and Session Manager. Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- Group Type – Set to **sip.**
- IMS Enabled – Verify the field is set to **n**. This will set Communication Manager as Evolution Server. Setting this field to **y** will cause Communication Manager to function as a Feature Server.
- Near-end Node Name - Set to procr as displayed in **Section 5.4**.
- Far-end Node Name - Set to the Session Manager in **Section 5.4**.
- Far-end Network Region - Set to the region configured in **Section 5.3**.
- Far-end Domain - Set to **avaya.com**. This should match the SIP Domain value in **Section 6.1**.

```
add signaling-group 92                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 92             Group Type: sip
  IMS Enabled? n          Transport Method: tls
        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: procr                 Far-end Node Name: SM-1
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 30
```

5.6. Configure SIP Trunk

This section describes the steps for administering a trunk group in Communication Manager for communication between Communication Manager and Session Manager. Enter the **add trunk-group <t>** command, where **t** is an unallocated trunk group and configure the following:

- **Group Type** – Set the Group Type field to **sip**.
- **Group Name** – Enter a descriptive name.
- **TAC** (Trunk Access Code) – Set to any available trunk access code.
- **Signaling Group** – Set to the Group Number field value configured in **Section 5.5**.
- **Number of Members –** Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
add trunk-group 92                                             Page   1 of  21
                                TRUNK GROUP

Group Number: 92                   Group Type: sip          CDR Reports: y
  Group Name: No IMS SIP trk             COR: 1        TN: 1         TAC: 1092
   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: 92
                                                     Number of Members: 10
```

5.7. Configure SIP Endpoint and Off PBX Telephone Station

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication manager when users (SIP endpoints) are created in Session Manager.

5.8. Configure Avaya Feature Name Extension

The following Avaya feature name extension (FNE) set was utilized during the compliance test. Enter **change off-pbx-telephone feature-name-extensions set 1** to view the feature name extensions. The highlighted fields were tested during the compliance test.

```
change off-pbx-telephone feature-name-extensions set 1          Page   1 of   2
     EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME
                     Set Name:

        Active Appearance Select: 27051
             Automatic Call Back: 27052
      Automatic Call-Back Cancel: 27053
                Call Forward All: 27054
     Call Forward Busy/No Answer: 27055
             Call Forward Cancel: 27056
                       Call Park: 27057
           Call Park Answer Back: 27058
                    Call Pick-Up: 27059
            Calling Number Block: 27060
          Calling Number Unblock: 27061
  Conditional Call Extend Enable:
 Conditional Call Extend Disable:
             Conference Complete:
            Conference on Answer: 27062
           Directed Call Pick-Up: 27063
           Drop Last Added Party: 27064
```

6. Configure Avaya Aura® Session Manager

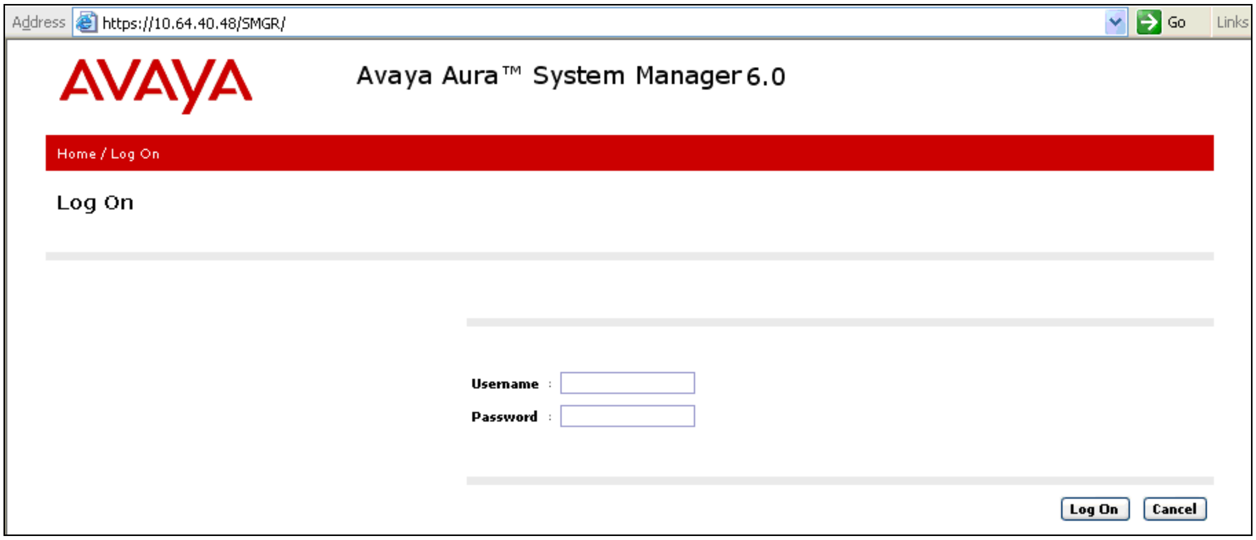
This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

This section assumes that Session Manager and System Manager have been installed, network connectivity exists between the two platforms, and the basic configuration is performed.
The following steps describe for configuring Session Manager

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element
- Applications
- Application Sequence
- User Management

6.1. Configure SIP Domain

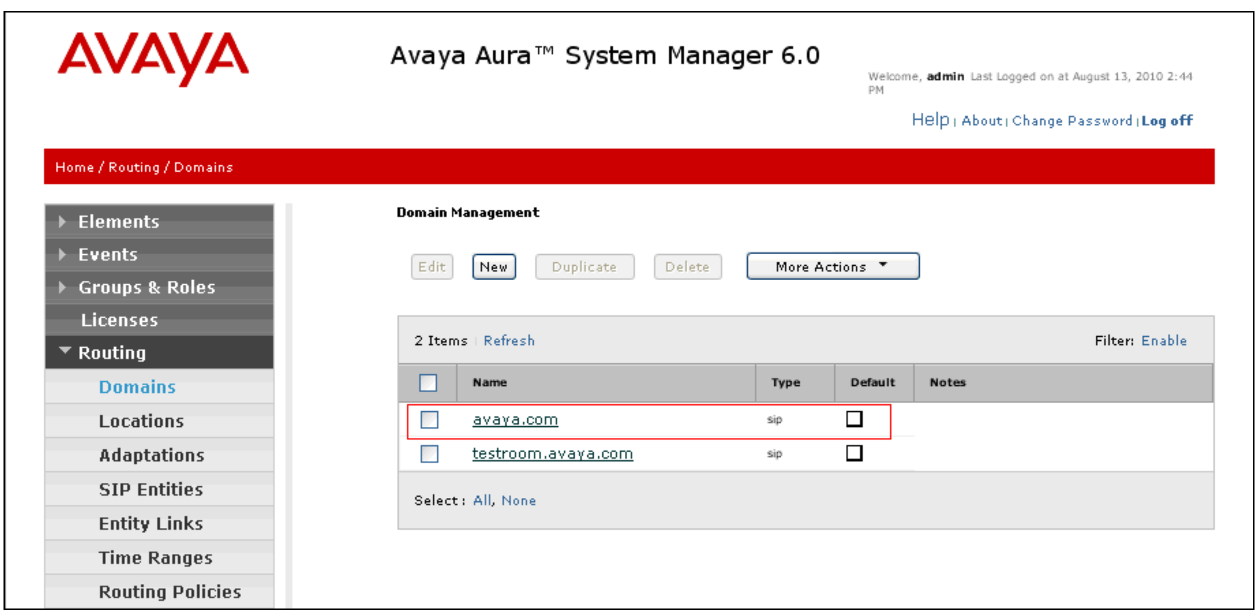
Launch a web browser, enter **https://<IP address of System Manager>/SMGR** in the URL, and log in with the appropriate credentials.



Navigate to **Routing → Domains**, and click on the **New** button to create a new SIP Domain (screen not shown). Enter the following values and use default values for remaining fields:

- **Name –** Enter the Authoritative Domain name specified in **Section 5.3**, which is **avaya.com**.
- **Type** – Select **SIP**

Click **Commit** to save. The following screen shows the Domains page used during the compliance test.



6.2. Configure Locations

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

Navigate to **Routing → Locations**, and click on the **New** button to create a new SIP Entity location (screen not shown).

General section

Enter the following values and use default values for remaining fields.

- Enter a descriptive Location name in the **Name** field (e.g. **S8300-Subnet**).
- Enter a description in the **Notes** field if desired.

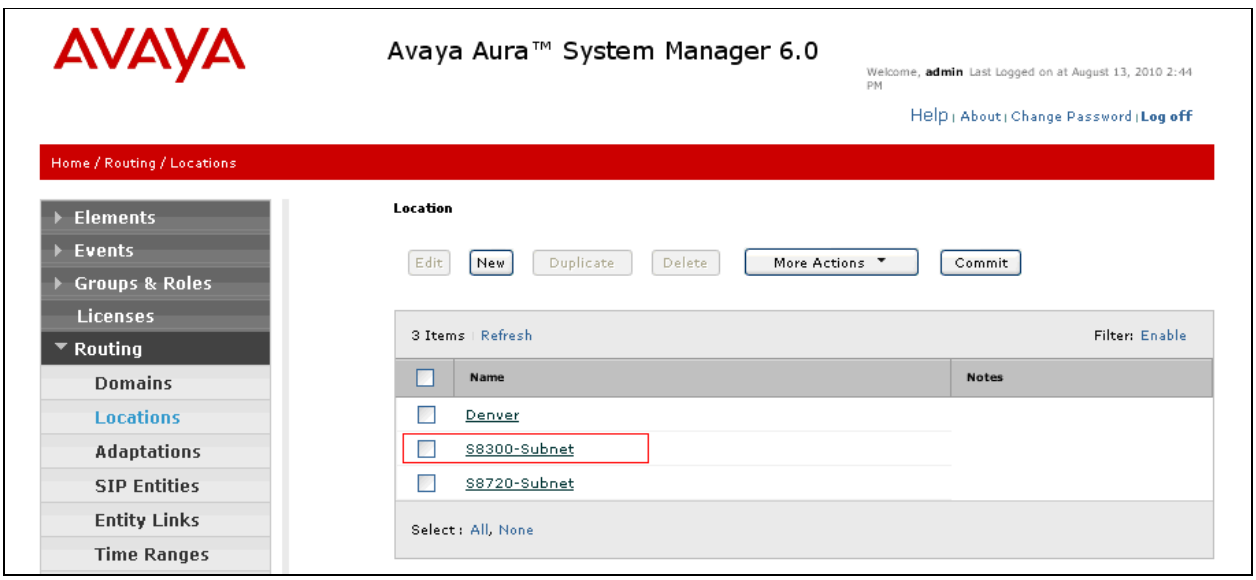
Location Pattern section

Click **Add** and enter the following values:

- Enter the IP address information for the **IP address Pattern** (e.g. **10.64.41.***)
- Enter a description in the **Notes** field if desired.

Repeat steps in the Location Pattern section if the Location has multiple IP segments. Modify the remaining values on the form, if necessary; otherwise, use all the default values. Click on the **Commit** button.

Repeat all the steps for each new Location. The following screen shows the Location page used during the compliance test.



6.3. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk provisioned to Session Manager. During the compliance test, the following SIP Entities were configured:

- Session Manager itself
- Communication Manager (Avaya S8300D Server)
- Communication Manager (Avaya S8720 Servers – not shown)

Navigate to **Routing → SIP Entities**, and click on the **New** button to create a new SIP entity (screen not shown). Provide the following information:

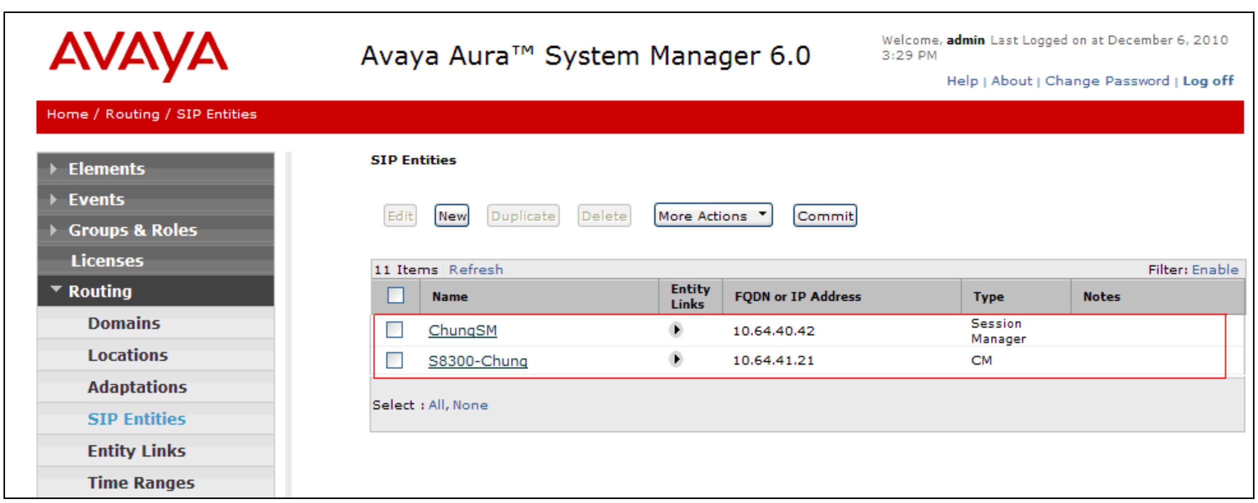
General section

Enter the following values and use default values for remaining fields.

- Enter a descriptive name in the **Name** field.
- Enter IP address for signaling interface on each Communication Manager, virtual SM-100 interface on Session Manager, or 3rd party device in the **FQDN or IP Address** field
- From the **Type** drop down menu, select a type that best matches the SIP Entity.
    - For Communication Manager, select **CM**
    - For Session Manager, select **Session Manager**
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.

Click on the **Commit** button to save each SIP entity. The following screen shows the SIP Entities page used during the compliance test.

Repeat all the steps for each new entity.



6.4. Configure Entity Links

Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

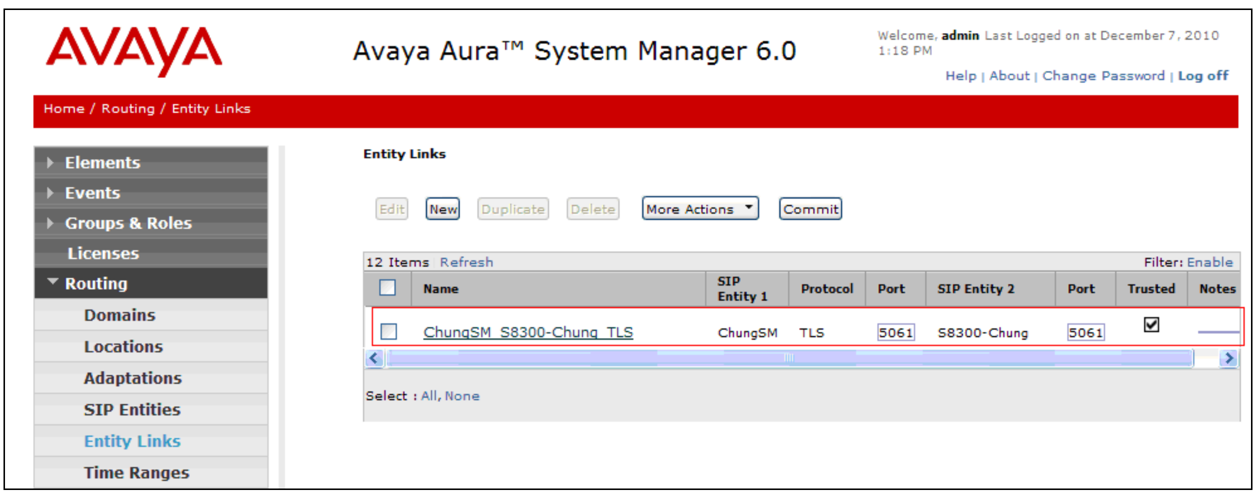
- Session Manager ⇔ Communication Manager (Avaya S8300D Server)
- Session Manager ⇔ Communication Manager (Avaya S8720 Servers – not shown)

Navigate to **Routing → Entity Links**, and click on the **New** button to create a new entity link (screen not shown). Provide the following information:

- Enter a descriptive name in the **Name** field.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 6.3** (e.g. **ChungSM**).
- In the **Protocol** drop down menu, select the protocol to be used.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
    - TLS – 5061
    - UDP or TCP – 5060
- In the **SIP Entity 2** drop down menu, select one of the two entities in the bullet list above (which were created in **Section 6.3**). In the compliance test **S8300-Chung** was selected.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- Check the **Trusted** box.
- Enter a description in the **Notes** field if desired.

Click on the **Commit** button to save each Entity Link definition. The following screen shows an Entity Links page (between Session Manager and Communication Manager) used during the compliance test.

Repeat all the steps for each new SIP Entity Link.



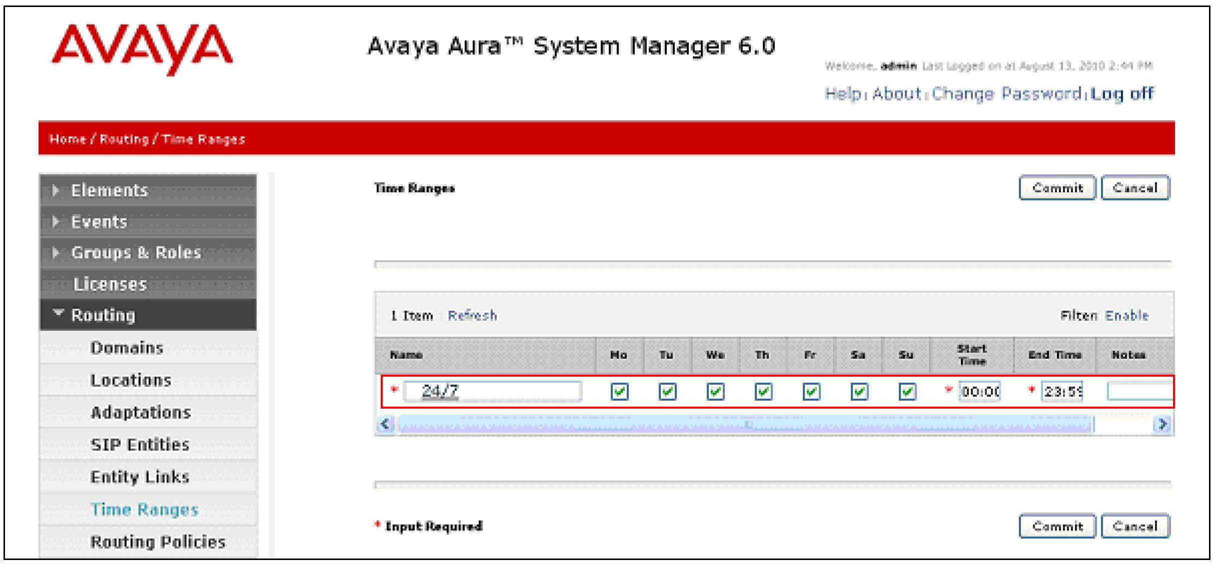
6.5. Time Ranges

The Time Ranges form allows admission control criteria to be specified for Routing Policies (**Section 6.6**). In the reference configuration, no restrictions were used.

To add a Time Range, navigate to **Routing → Time Ranges**, and click on the **New** button (not shown). Provide the following information:

- Enter a descriptive name in the **Name** field (e.g. **24/7**).
- Check each day of the week.
- In the **Start Time** field, enter **00:00**.
- In the **End Time** field, enter **23:59**.
- Enter a description in the **Notes** field if desired.

Click the **Commit** button. The following screen shows the Time Range page used during the compliance test.



6.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 6.3**) with Time of Day admission control parameters (**Section 6.5**) and Dial Patterns (**Section 6.7**). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Communication Manager.

To add a Routing Policy, navigate to **Routing → Routing Policies**, and click on the **New** button on the right (screen not shown). Provide the following information:

General section

- Enter a descriptive name in the **Name** field.
- Enter a description in the **Notes** field if desired.

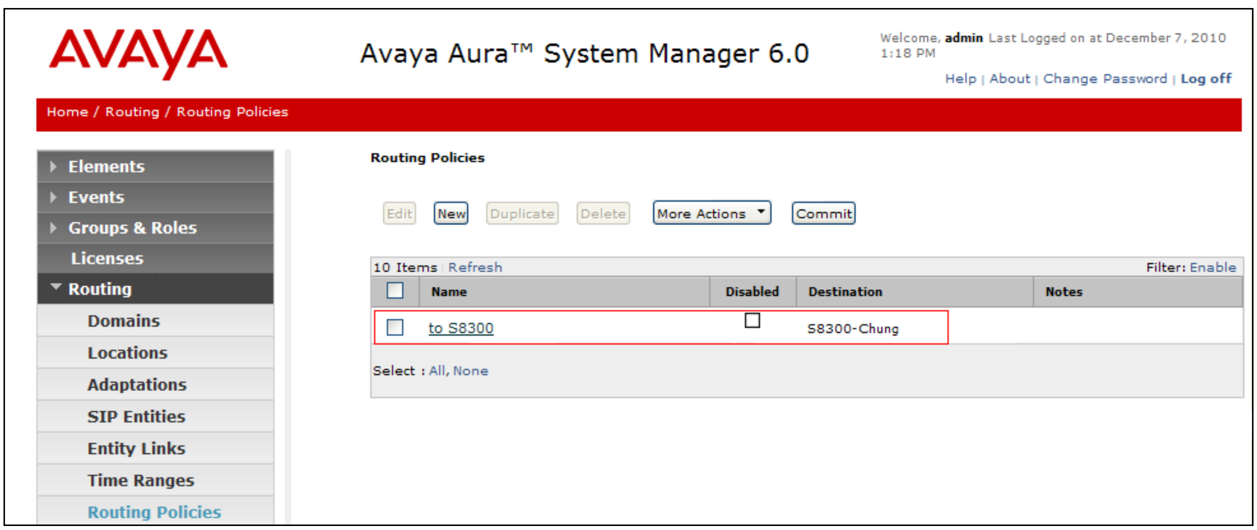
SIP Entity as Destination section

- Click the **Select** button.
- Select a SIP Entity that will be the destination for this call.
- Click the **Select** button and return to the Routing Policy Details form.

Time of Day section

- Leave default values.

Click **Commit** to save Routing Policy definition. The following screen shows the Routing Policy used for Communication Manager during the compliance test.



6.7. Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In the compliance test, the following dial patterns are defined from Session Manager.

- 7202x – SIP endpoints in Avaya S8300D Server
- 7301x – Polycom SIP endpoints in Avaya S8300D Server (not shown)
- 270xx – FNE feature in Avaya S8300D Server (not shown)

To add a Dial Pattern, select **Routing → Dial Patterns,** and click on the **New** button (not shown) on the right pane. Provide the following information:

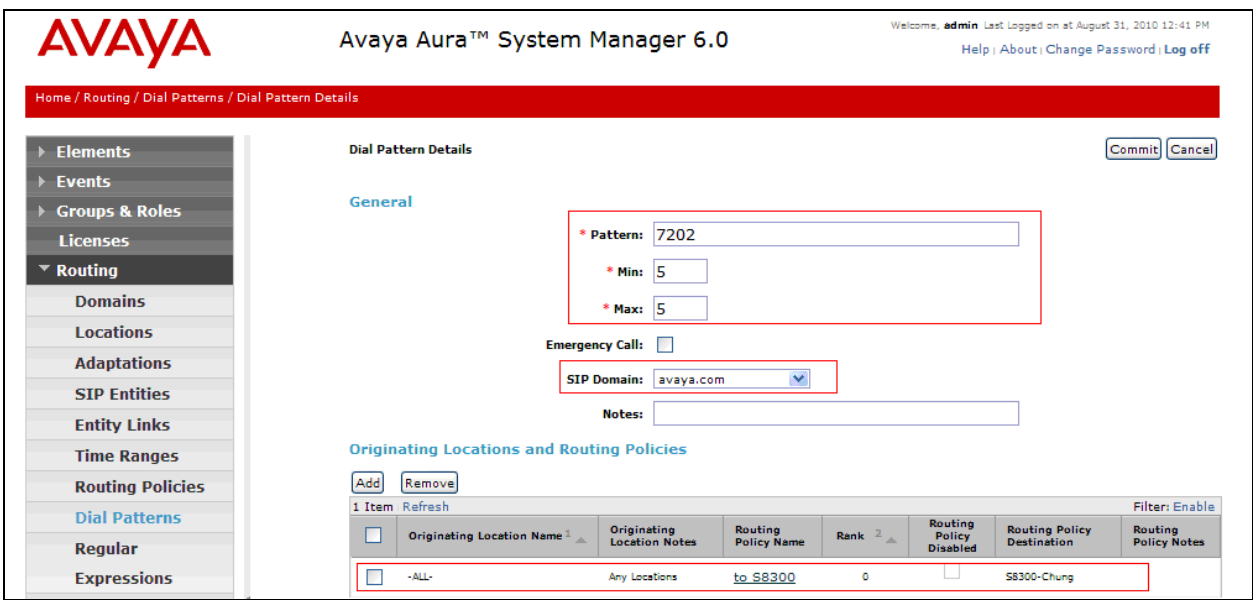
<u>General section</u>

- Enter a unique pattern in the **Pattern** field (e.g. **7202**).
- In the **Min** field enter the minimum number of digits (e.g. **5**).
- In the **Max** field enter the maximum number of digits (e.g. **5**).
- In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI *received* by Session Manager from Communication Manager.

<u>Originating Locations and Routing Policies section</u>

- Click on the **Add** button and a window will open (not shown).
- Click on the box for the appropriate Originating Locations, and Routing Policies (see **Section 6.6**) that pertain to this Dial Pattern.
  - Select the Originating Location to **Apply The Selected Routing Policies to All Originating Location**.
  - Select Routing Policies **to S8300**
  - Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition. The following screen shows the dial pattern used for 7202X during the compliance test. Repeat steps for the remaining Dial Patterns.



6.8. Configure Managed Elements

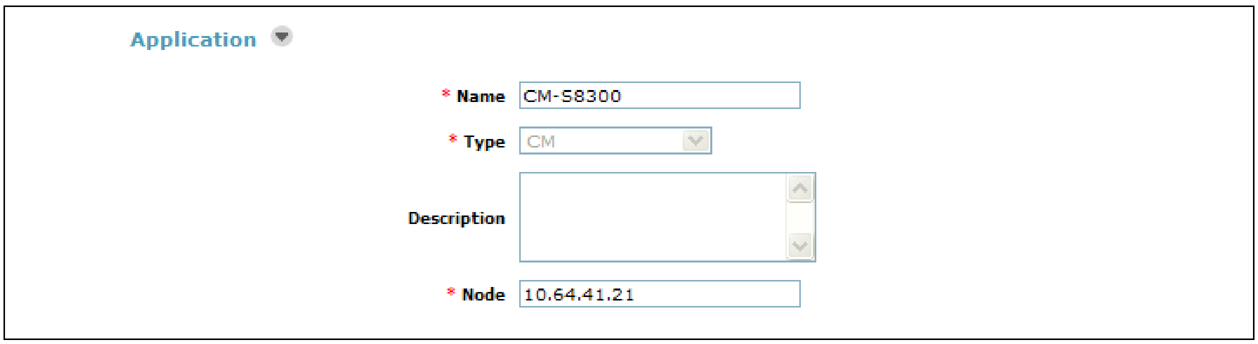
To define a new Managed Element, navigate to **Elements → Inventory → Manage Elements**. Click on the **New** button (not shown) to open the **New Entities Instance** page.

In the **New Entities Instance** Page

- In the **Type** field, select **CM** using the drop-down menu, and the **New CM Instance** page opens (not shown).

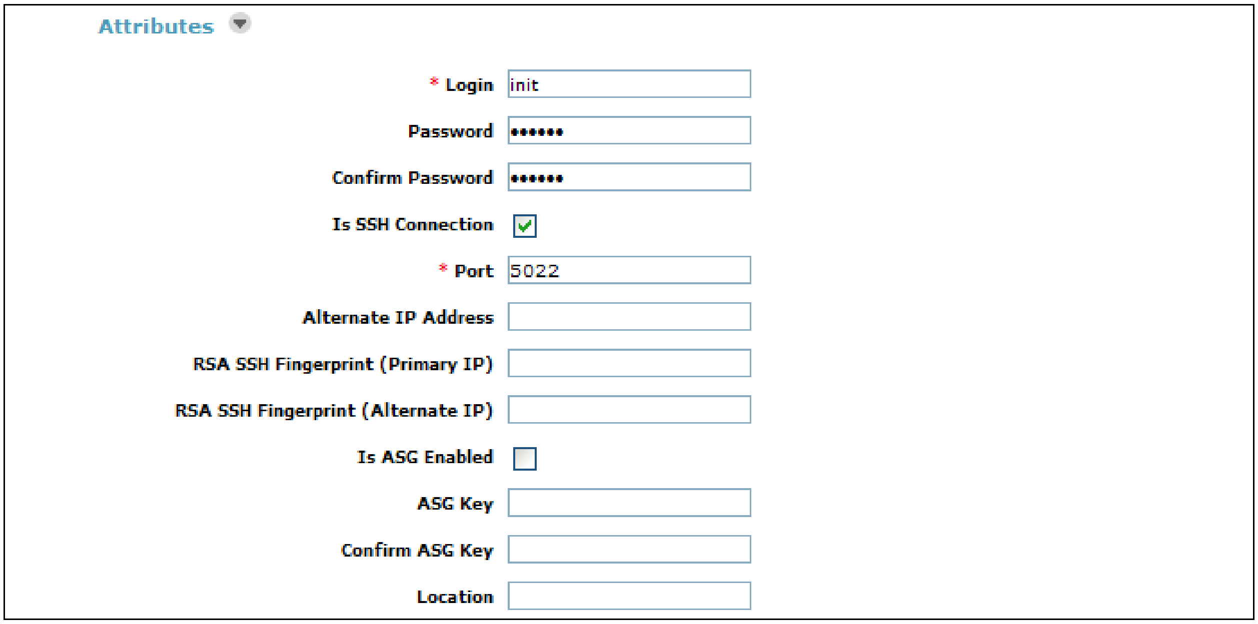
In the New CM Instance Page, provide the following information:

- Application section
    - **Name** – Enter name for Communication Manager (Evolution Server).
    - **Description -** Enter description if desired.
    - **Node** – Enter IP address of the administration interface. During the compliance test, the procr IP address (10.64.41.21) was utilized.

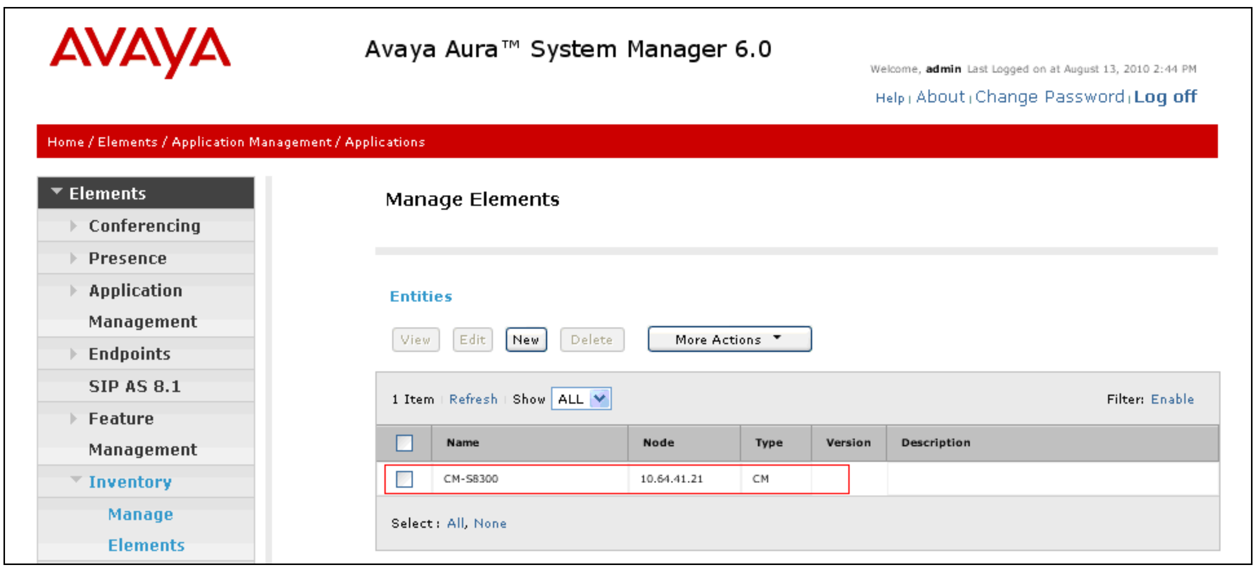


- Leave the fields in the Port and Access Point sections blank. In the SNMP Attributes section, verify the default value of **None** is selected for the Version field.

- Attributes section.
  System Manager uses the information entered in this section to log into Communication Manager using its administration interface. Enter the following values and use default values for remaining fields.
    - **Login** – Enter login used for administration access
    - **Password** – Enter password used for administration access
    - **Confirm Password** – Repeat value entered in above field.
    - **Is SSH Connection** – Check the check box**.**
    - **Port** – Verify **5022** has been entered as default value



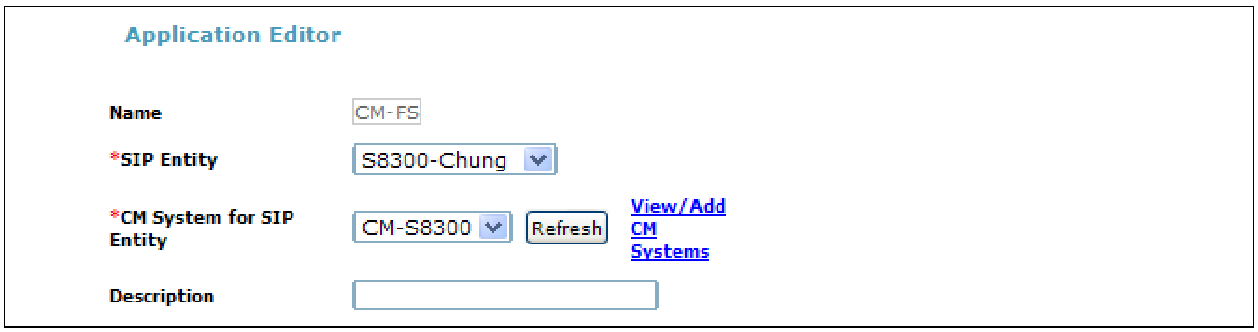
Click **Commit** to save the element. The following screen shows the element created, CM-S8300, during the compliance test.



6.9. Configure Applications

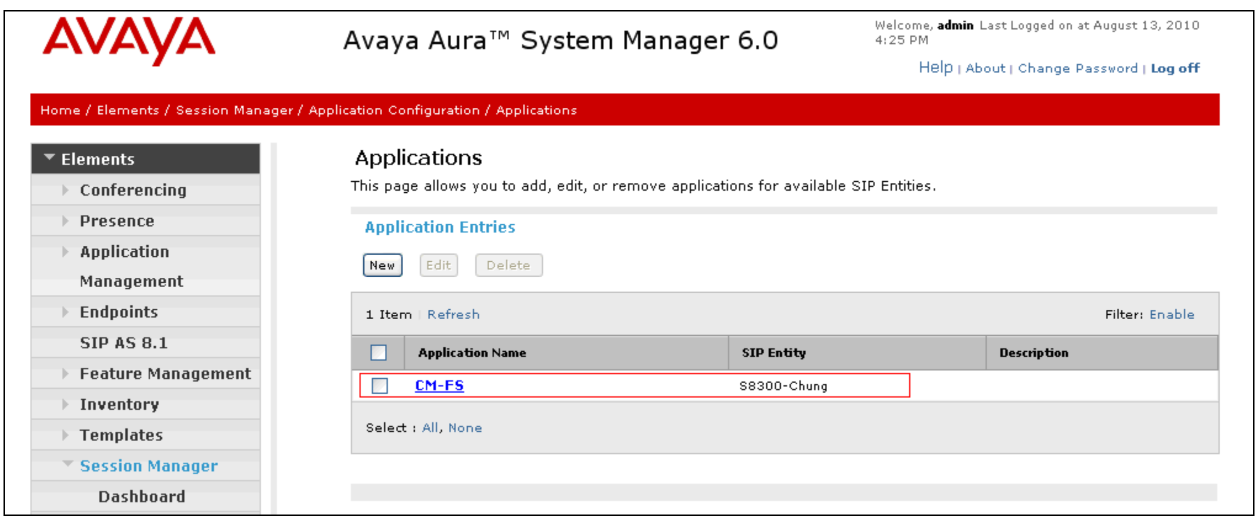
To define a new Application, navigate to **Elements → Session Manager → Application Configuration → Applications**. Click **New** (not shown) to open the Applications Editor page, and provide the following information:

- Application Editor section
  - **Name** – Enter name for the application.
  - **SIP Entity** - Select SIP Entity for Communication Manager defined in **Section 6.3**
  - **CM System for SIP Entity** – Select name of Managed Element defined for Communication Manager in **Section 6.8**
  - **Description** – Enter description if desired.



- Leave fields in the Application Attributes (optional) section blank.

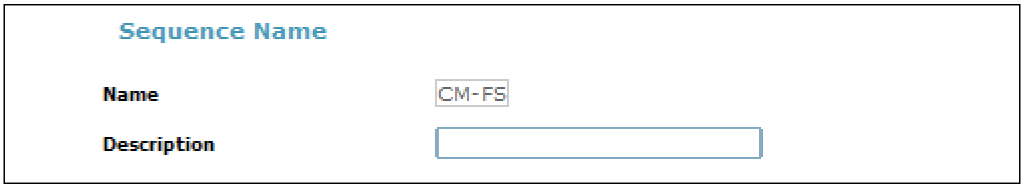
Click the **Commit** button (not shown) to save the Application. The screen below shows the Application, CM-FS, defined for Communication Manager.



6.10. Define Application Sequence

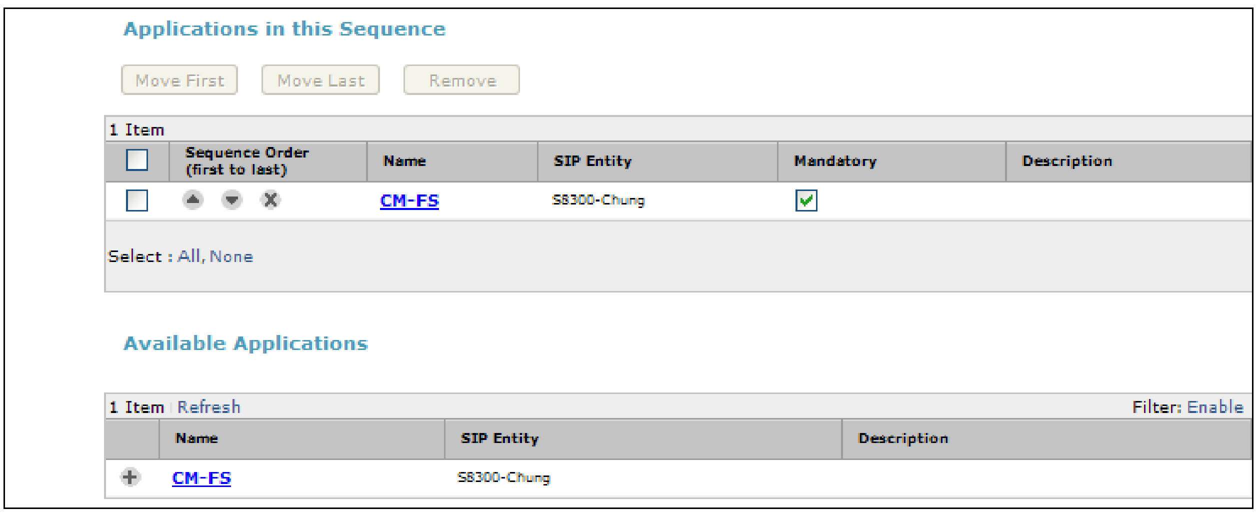
Navigate to **Elements → Session Manager → Application Configuration → Application Sequences**. Click **New** (not shown) and provide the following information:

- Sequence Name section
  - **Name** – Enter name for the application
  - **Description** – Enter description, if desired.

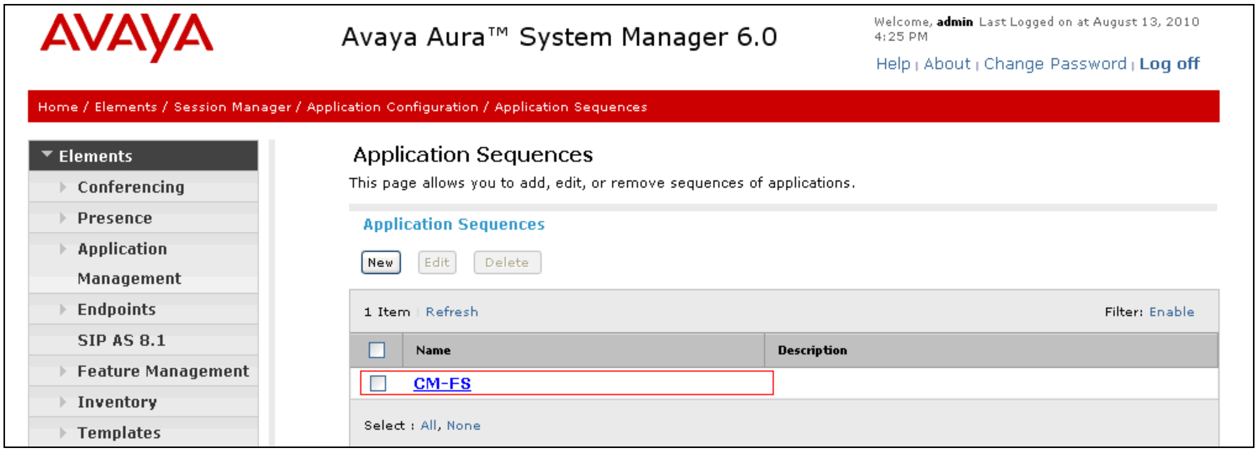


- Available Applications section
  - Click + icon associated with the Application for Communication Manager defined in **Section 6.9** to select this application.
  - Verify a new entry is added to the Applications in this Sequence table as shown below.

Click the **Commit** button (not shown) to save the new Application Sequence.



The screen below shows the Application Sequence, CM-FS, defined during the compliance test.

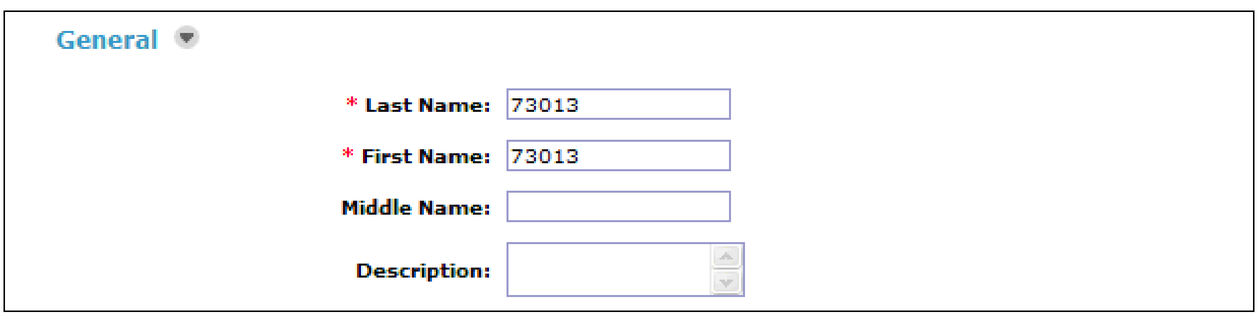


6.11. Configure SIP Users

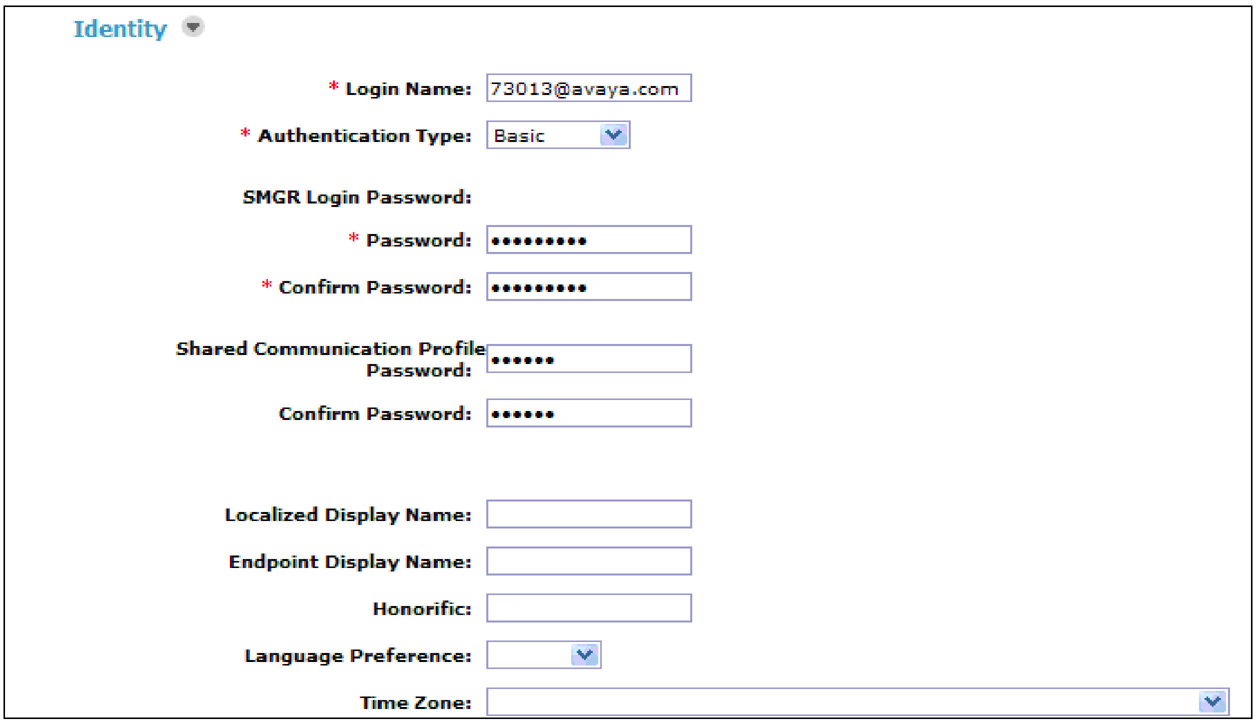
Add new SIP users for each 9600-Series SIP station and Polycom IP 7000 defined in **Section 5.7.** Alternatively, use the option shown in this section to automatically generate the SIP station on Communication Manager after adding a new SIP user.

To add new SIP users, Navigate to **Users → Manage Users**. Click **New** (not shown) and provide the following information:

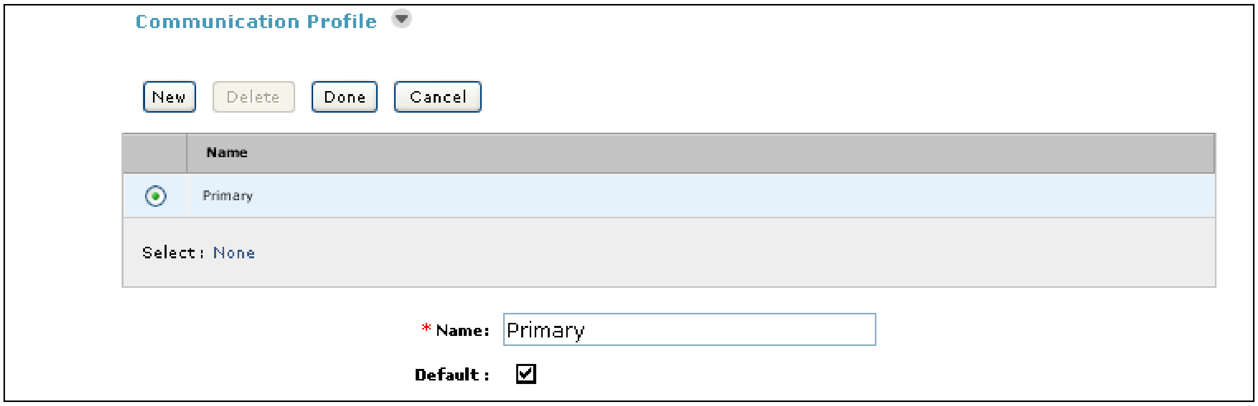
- General section
    - **Last Name** – Enter last name of user.
    - **First Name** – Enter first name of user.



- Identity section
    - **Login Name –** Enter extension number@sip domain defined in **Section 5.3**.
    - **Authentication Type –** Verify **Basic** is selected.
    - **SMGR Login Password –** Enter password to be used to log into System Manager.
    - **Confirm Password –** Repeat value entered above.
    - **Shared Communication Profile Password –** Enter a numeric value used to logon to SIP telephone. [**Note:** this field must match the Security Code field on the STATION form defined in **Section 5.7, if stations were manually added in that section (not shown)**]
    - **Confirm Password** – Repeat numeric password

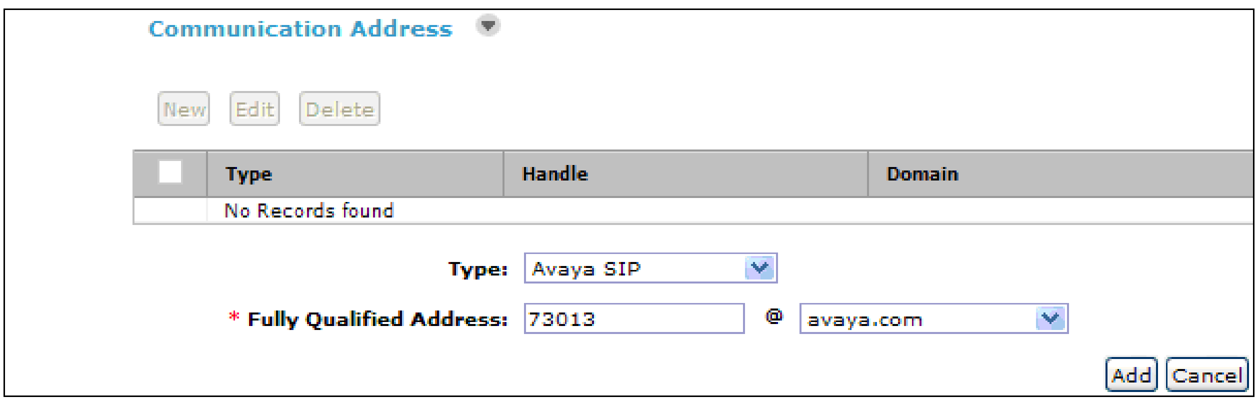


- Communication Profile section
  Verify there is a default entry identified as the **Primary** profile for the new SIP user. If an entry does not exist, select **New** and enter values for the following required attributes:
    - Name – Enter **Primary**.
    - Default – Enter ☑

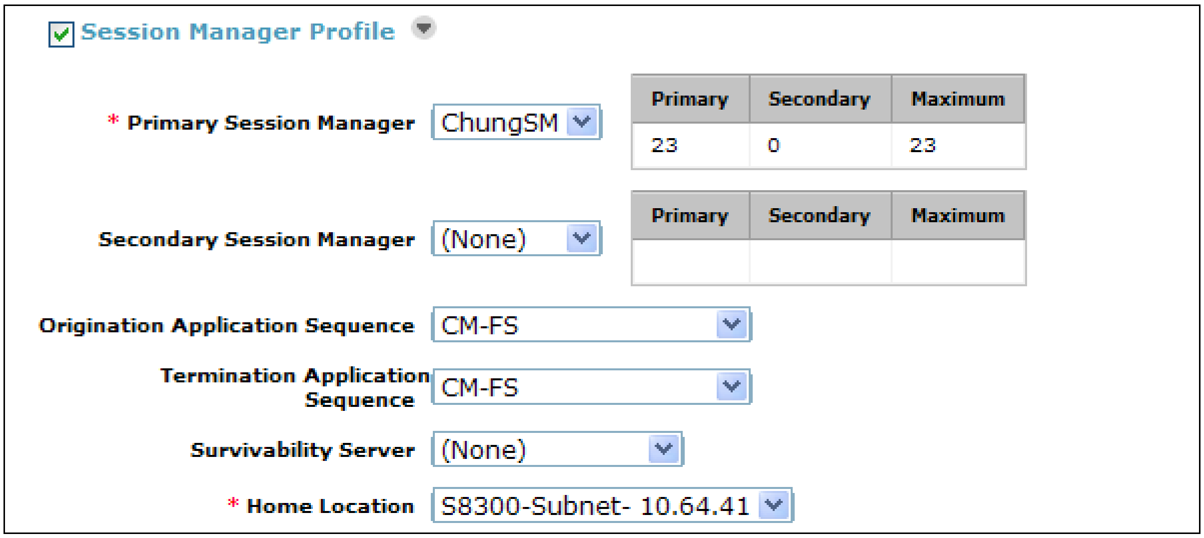


- Communication Address sub-section
  Select **New** to define a **Communication Address** for the new SIP user, and provide the following information.
    - **Type** – Select **Avaya SIP** using drop-down menu.
    - **Full Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

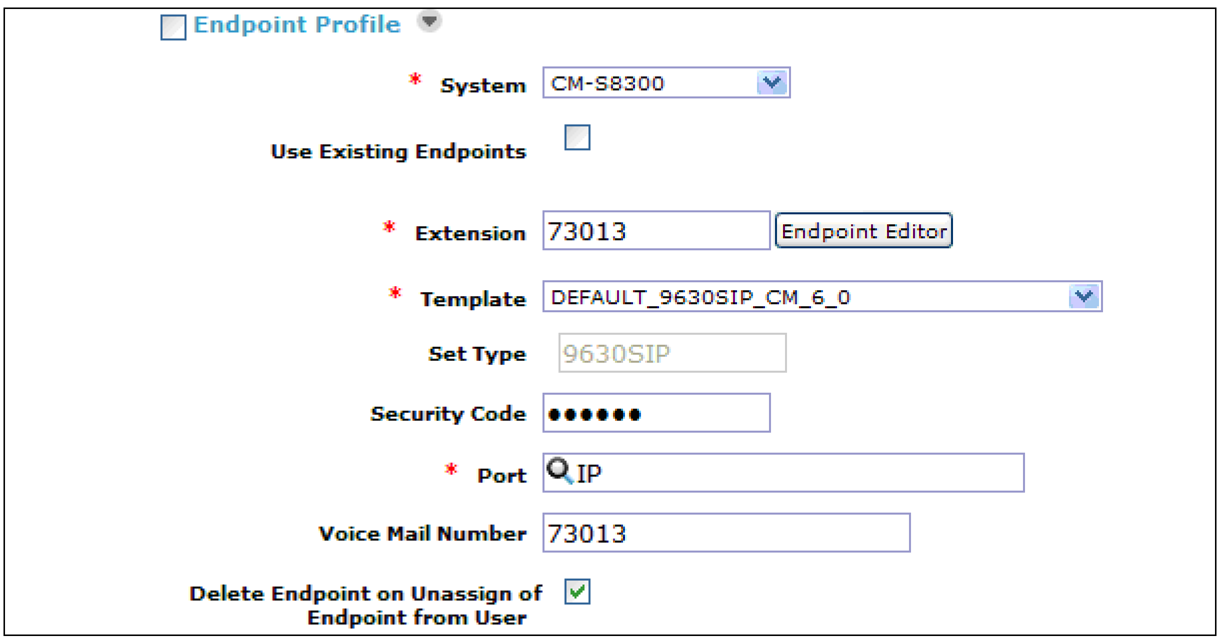
  Click the **Add** button to save the Communication Address for the new SIP user.



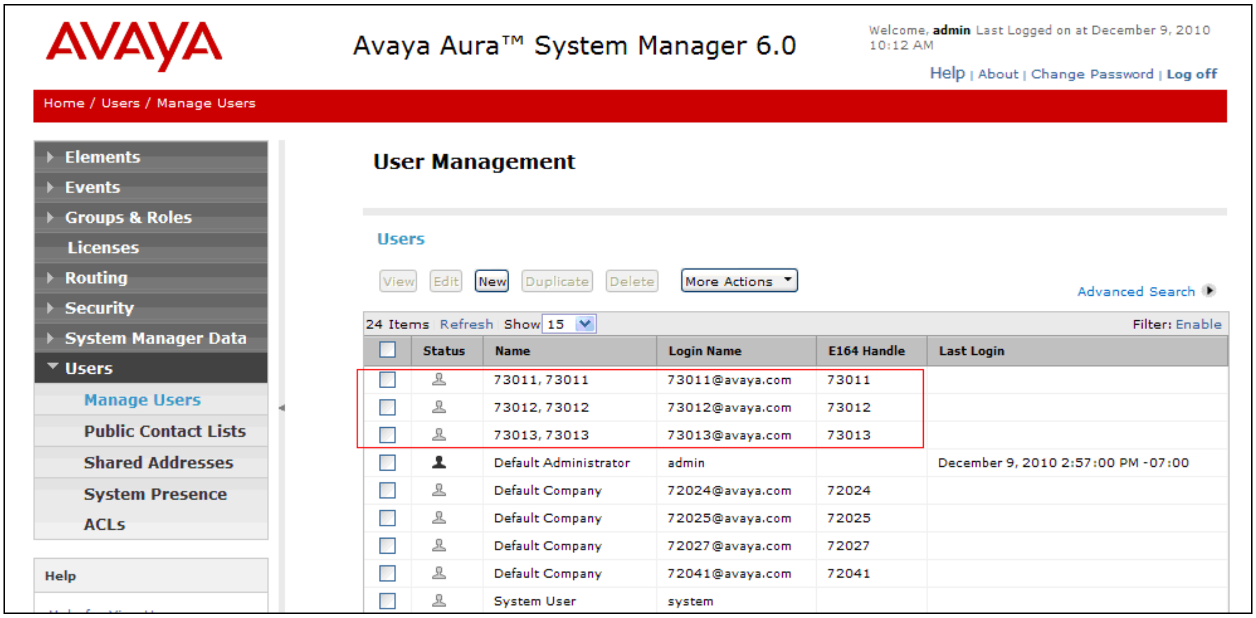
- Session Manager Profile section
    - **Primary Session Manager** – Select one of the Session Managers.
    - **Secondary Session Manager** – Select **(None)** from drop-down menu.
    - **Origination Application Sequence –** Select Application Sequence defined in **Section 6.10** for Communication Manager.
    - **Termination Application Sequence** – Select Application Sequence defined in **Section 6.10** for Communication Manager.
    - **Survivability Server** – Select **(None)** from drop-down menu.
    - **Home Location** – Select Location defined in **Section 6.2**.



- Endpoint Profile section
  - **System** – Select Managed Element defined in **Section 6.8** for Communication Manager
  - **Use Existing Endpoints -** Leave unchecked to automatically create new endpoint when new user is created. Or else, check the box if endpoint is already defined in Communication Manager. When unchecked, the station will be automatically created in Communication Manager.
  - **Extension** - Enter same extension number used in this section.
  - **Template** – Select template for type of SIP phone
  - **Security Code** – Enter numeric value used to logon to SIP telephone. (**Note:** this field must match the value entered for the Shared Communication Profile Password field.
  - **Port** – Select **IP** from drop down menu
  - **Voice Mail Number –** Enter **Pilot Number** for Avaya Modular Messaging if installed. Or else, leave field blank.
  - **Delete Station on Unassign of Endpoint** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.



Click **Commit** to save definition of new user. The following screen shows the created users during the compliance test. The highlight shows users created for Polycom endpoints during the compliance test.

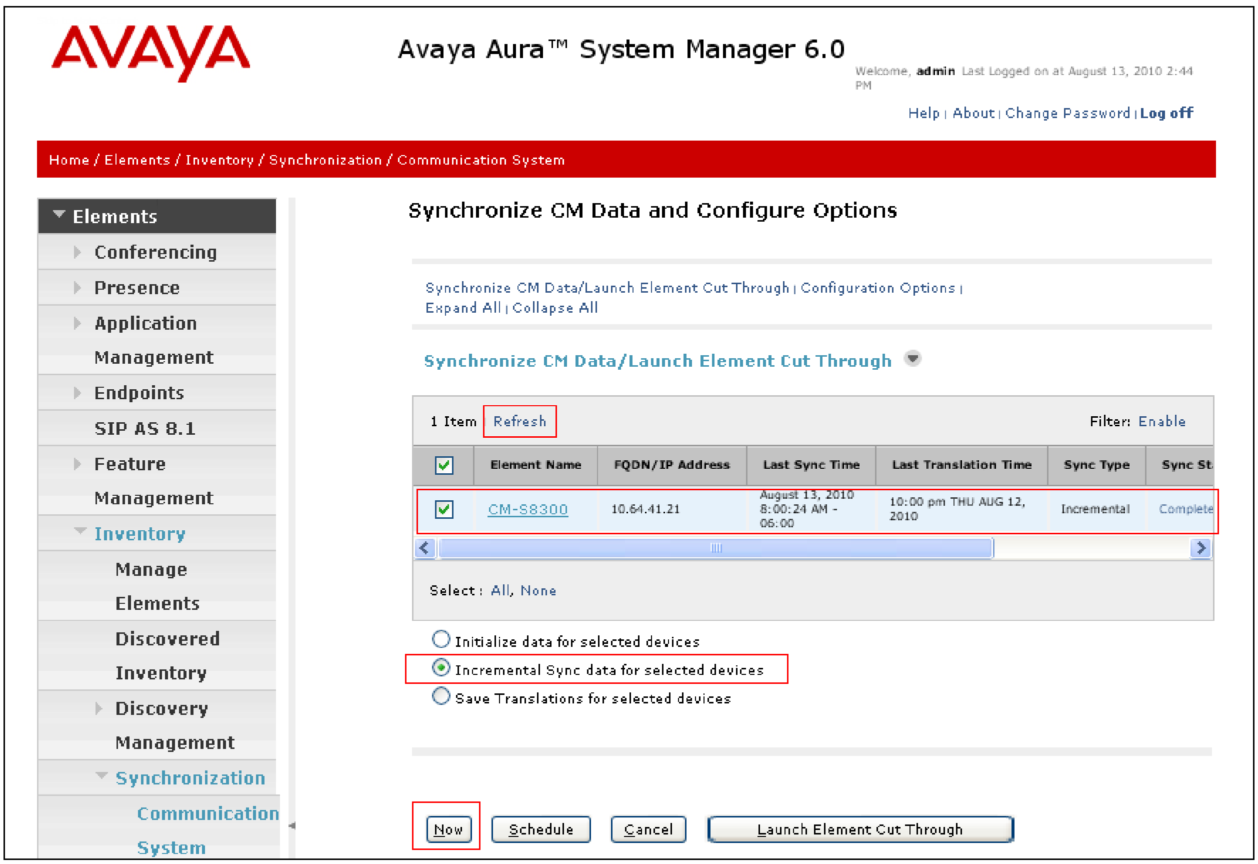


6.12. Synchronization Changes with Avaya Aura® Communication Manager

After completing these changes in System Manager, perform an on demand synchronization. Navigate to **Elements → Inventory → Synchronization → Communication System.**

On the **Synchronize CM Data and Configure Options** page, expand the **Synchronize CM Data/Launch Element Cut Through** table

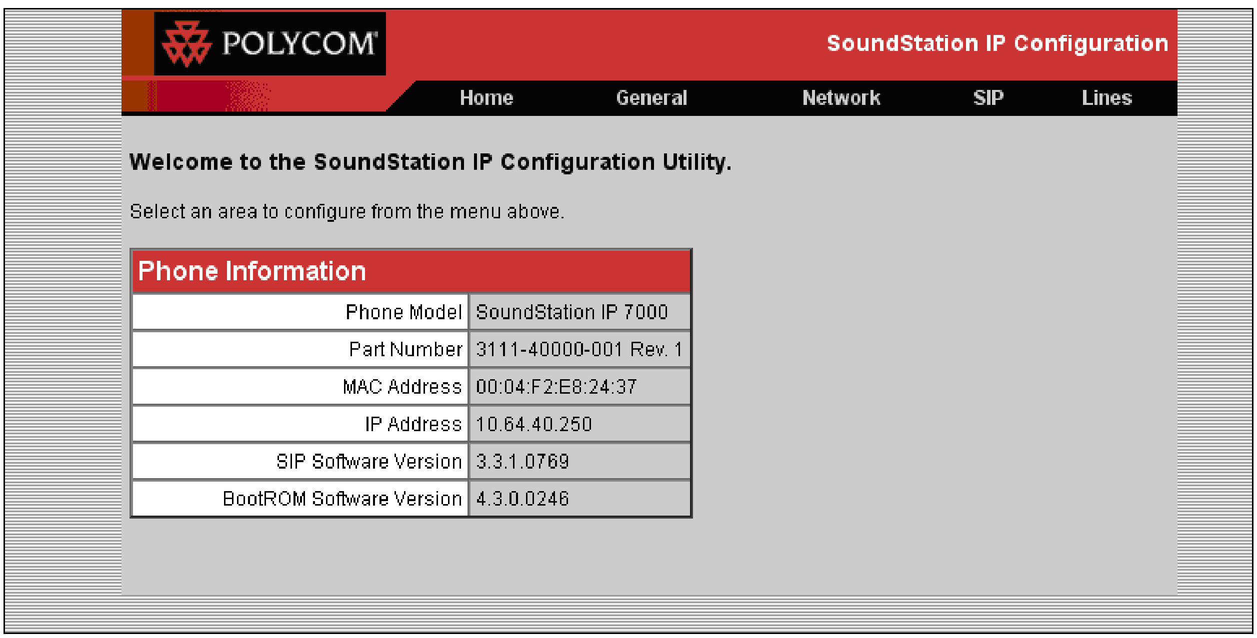
- Click ⦿ to select **Incremental Sync data for selected devices** option. Click **Now** to start the synchronization.
- Use the **Refresh** button in the table header to verify status of the synchronization.
- Verify synchronization successfully completes by verifying the status in the Sync. Status column shows **Completed**.



7. Configure Polycom SoundStation IP 7000

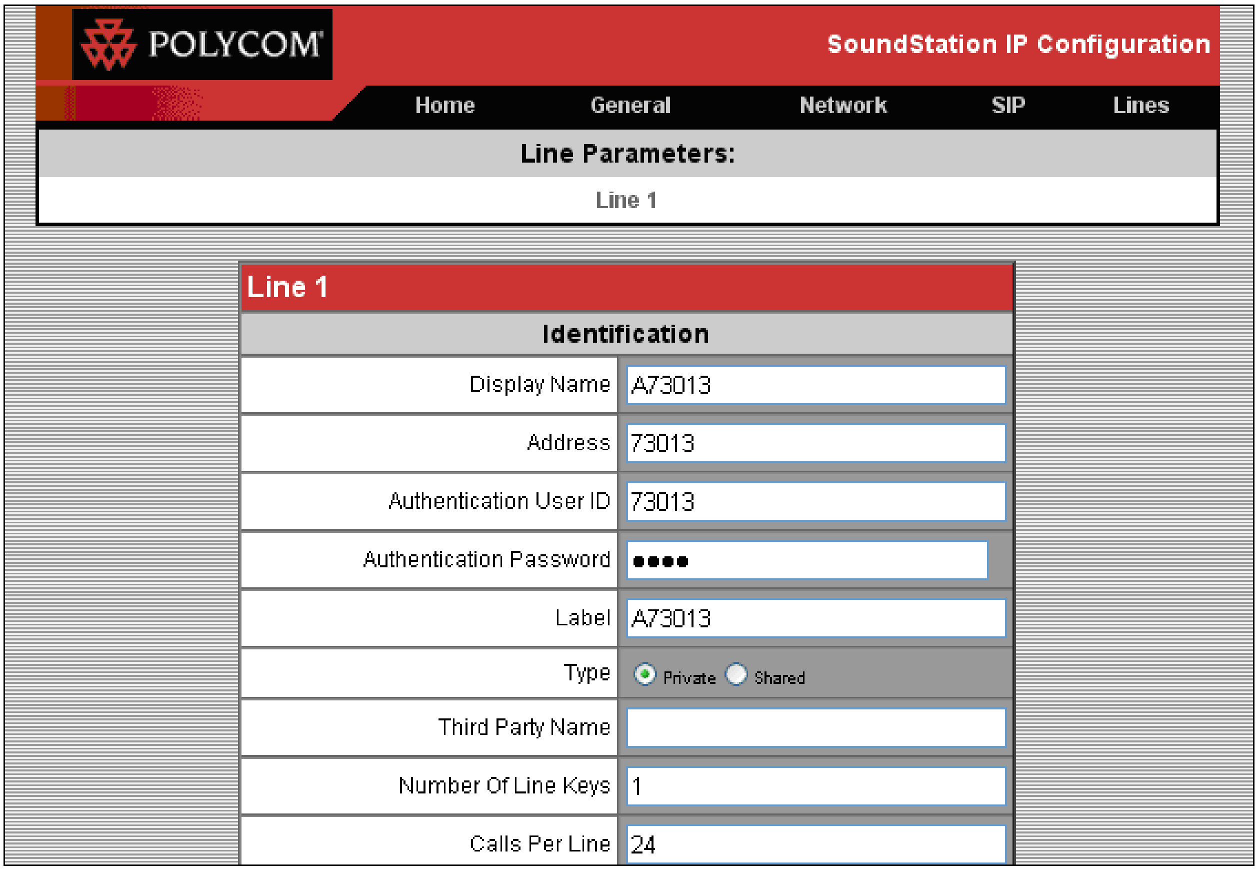
This section provides steps to configure SoundStation IP 7000. The latest firmware was provided by Polycom, firmware version **3.3.1**. The following steps are needed to configure SoundStation IP 7000, to register with Session Manager:

- Power cycle SoundStation IP 7000. While the phone boots up, select the Setup menu from the phone, and enter the administrator password (The factory default password is 456). Provide the following information:
  - **Phone IP address** (during the compliance test, static IP address was utilized)
  - **Subnet Mask**
  - **IP Gateway**
  - In Server Menu
    - Set **Server Type** to **TFTP**.
    - Provide the **Server Address**
  - **DNS Domain**
  - In Syslog Menu
    - Set **Server Address** to the IP address of Session Manager
    - Set **Server Type** to **UDP** (During the compliance test, UDP was utilized)
  - Select the **Exit** button to continue to boot.
- Once the phone is completed the booting process, launch a web browser, enter **http://<IP address of SoundStation IP 7000>** in the URL, and log in with the appropriate credentials.



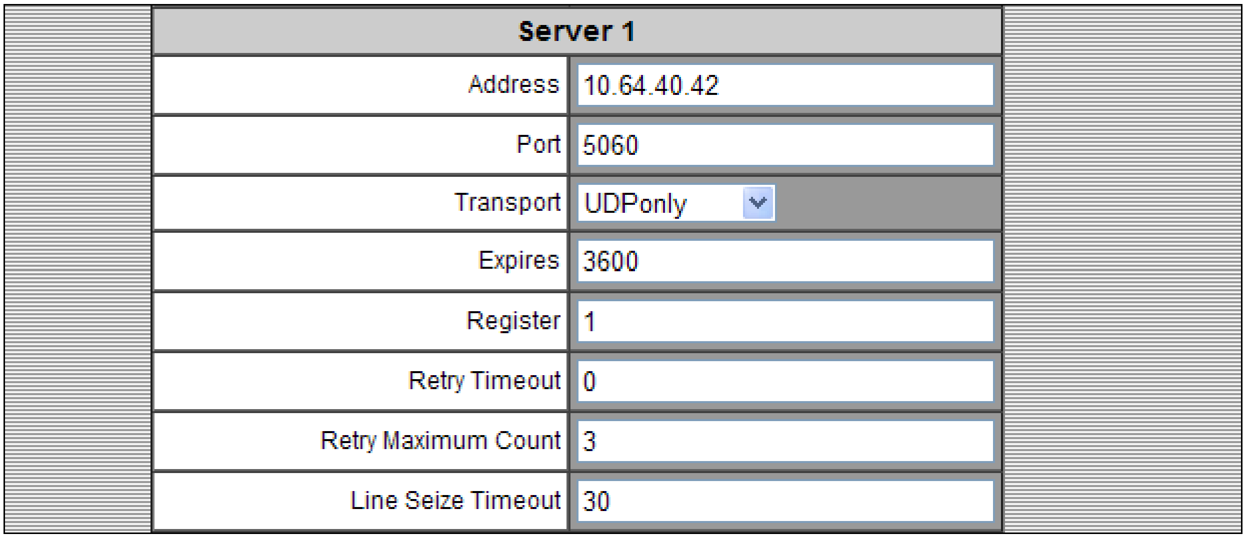
Select **Lines** from the top menu, and provide the following information in the Identification section:

- **Display Name**
- **Address**
- **Authentication User ID**
- **Authentication Password (Security Code created in section 6.11)**
- **Label**



In the Server 1 section, provide the following information:

- **Address** – IP address of the Session Manager server
- **Port** – Enter the port to be used (e.g. **5060** or **5061**).
    - TLS – 5061
    - UDP or TCP – 5060
- **Transport** – UDPonly was select for the compliance test



In the Message Center section, enter the subscriber extension. After the completion, click on the **Submit** button

8. Verification Steps

The following steps may be used to verify the configuration:

The following steps may be used to verify the configuration:

- Verify that SoundStation IP 7000 successfully registers with Session Manager by following the **Elements → Session Manager → System Status → User registrations** link in Session manager.
- Place calls to and from SoundStation IP 7000 and verify that the calls are successfully established with two-way talk path.
- While calls are established, Enter **status trunk <t:r>** command, where **t** is the SIP trunk group configured in **Section 5.6**, and **r** is trunk group member. This will verify whether the call is shuffled or not. Another way is using **traceSM** command from the linux.

9. Conclusion

Polycom SoundStation IP 7000 was compliance tested with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Polycom SoundStation IP 7000 functioned properly for feature and serviceability. During compliance testing, Polycom SoundStation IP 7000 successfully registered with Session Manager, placed and received calls to and from SIP and non-SIP telephones, and executed other telephony features like three-way conference, transfers, hold, etc.

10. Additional References

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, June 2010, Release 6.0, Document Number 03-300509.

[2] *Administering Avaya Aura® Session Manager,* August 2010, Release 6.0, Document Number 03-603324.

[3] *Administering Avaya Aura® System Manager*, June 2010, Release 6.0.

The following document was provided by Polycom and can be found at http://support.polycom.com.

[4] *Administrator's Guide for the Polycom UC Software 3.3.0*, June 2010, 1725-11530-330, Rev. A