Avaya Solution & Interoperability Test Lab

Application Notes for Tenacity ipTTY with Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Tenacity ipTTY to interoperate with Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager.

The overall objective of the interoperability compliance testing is to verify Tenacity ipTTY functionalities in an environment comprised of Avaya Aura™ Communication Manager, Avaya Aura™ Session Manager, and various 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 procedure for configuring Tenacity ipTTY to interoperate with Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager.

Tenacity ipTTY is engineered to enable TTY communications using an existing VoIP/Hybrid PBX infrastructure. The only requirement from the infrastructure is support for 3rd party SIP devices. With Tenacity ipTTY, there is no longer a need for outdated TTY machines or expensive computer modems. Most importantly, with ipTTY, analog telephone lines are not required to facilitate TTY communications. Additionally, the ipTTY supports Hearing Carry Over (HCO), Voice Carry Over (VCO), includes a multi-lined display (versus a single lined display like standard TTY machines) and offers a recent calls list.

1.1. 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 Tenacity ipTTY with Avaya One-X Communicator (SIP), among other Avaya devices. Tenacity ipTTY operations such as inbound calls, outbound calls, call transfer, call forward, DTMF, and Tenacity ipTTY interactions with Session Manager, Communication Manager, and Avaya SIP, H.323 IP telephones, and Avaya One-X Communicator (SIP) were verified. The serviceability testing introduced failure scenarios to see if Tenacity ipTTY can recover from failures.

1.2. Support

Technical support for Tenacity ipTTY solution can be obtained by contacting Tenacity:

- email – support@accessaphone.com
- Phone – (866) 756-0321

2. Reference Configuration

Figure 1 illustrates a sample configuration consisting of an Avaya S8300D Server, an Avaya G450 Media Gateway, a Session Manager, a System Manager, and Tenacity ipTTY. The solution described herein is also extensible to other Avaya 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 4600 Series H.323 IP Telephones, Avaya 9600 Series SIP IP Telephones, and Avaya 9600 Series H.323 IP Telephones are included in **Figure 1** to demonstrate calls between the SIP-based Tenacity ipTTY and Avaya SIP, H.323, and digital telephones.

During the compliance test, Avaya One-X Communicator and ipTTY were installed into a same PC.

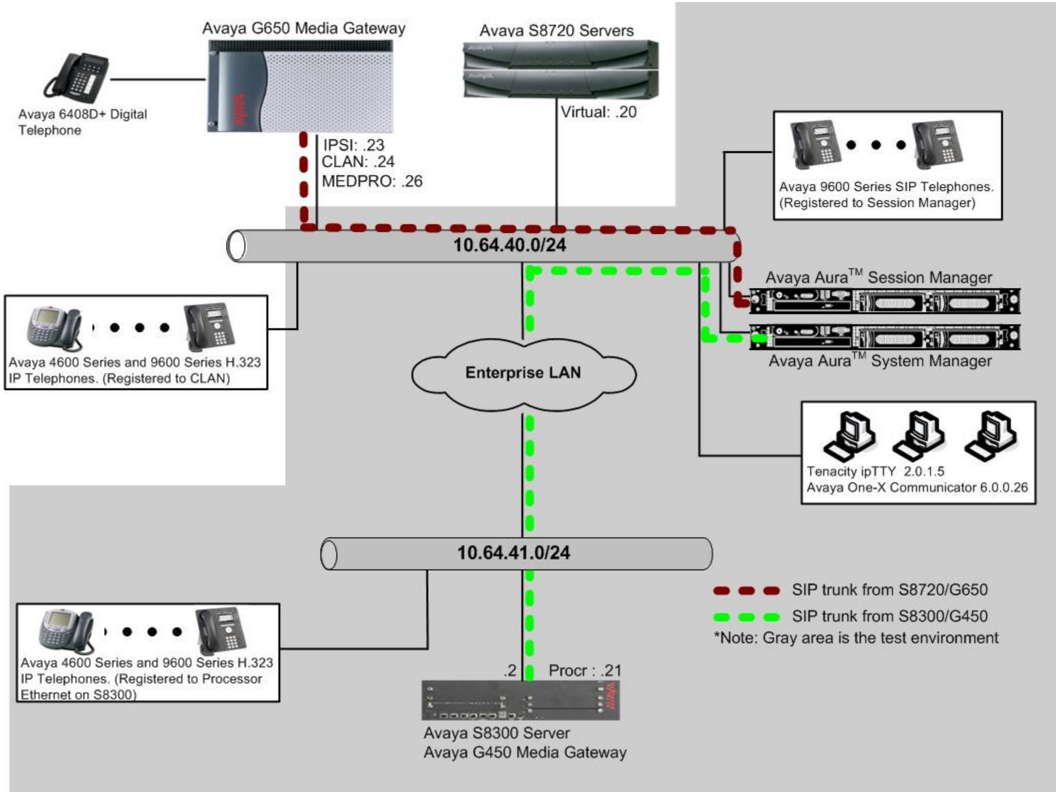


Figure 1: Test Configuration of Tenacity ipTTY

3. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300D Media Server with Avaya G450 Media Gateway		Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18246
Avaya Aura™ System Manager		Avaya Aura™ System Manager 6.0 (6.0.0.0-556)
Avaya Aura™ Session Manager		Avaya Aura™ Session Manager 6.0 (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 One-X Communicator		6.0.0.26
Avaya 4600 and 9600 Series SIP Telephones		
	9620 (SIP) 9630 (SIP) 9650 (SIP)	2.5 2.5 2.5
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		-
Tenacity ipTTY		2.0.1.5

4. Configure Avaya Aura™ Communication Manager

In the compliance test, Communication Manager was set up as an Evolution Server (Full Call Model). 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. All SIP telephones are configured as off-PBX telephones in Communication Manager.

4.1. 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: Standard
       Location: 2                                 System ID (SID): 1
       Platform: 28                                Module ID (MID): 1

                                                              USED
                                Platform Maximum Ports: 6400  185
                                      Maximum Stations: 500   19
                              Maximum XMOBILE Stations: 2400  0
                    Maximum Off-PBX Telephones - EC500: 10    0
                    Maximum Off-PBX Telephones -   OPS: 500   9
                    Maximum Off-PBX Telephones - PBFMC: 10    0
                    Maximum Off-PBX Telephones - PVFMC: 10    0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 0     0
```

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  20
           Maximum Concurrently Registered IP Stations: 2400  3
             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: 10    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    0
           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: 8     0
```

4.2. 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 4.3** for configuring IP network region to specify which codec sets may be used within and between network regions. During the compliance test, G.711MU was utilized.

```
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
```

4.3. 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 5.1**.
- Codec Set – Set the codec set number as provisioned in **Section 4.2**.

```
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
```

4.4. 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 along with its IP address.

```
change node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
CLAN                10.64.40.24
SM-1                10.64.40.42
default             0.0.0.0
procr               10.64.41.21
procr6              ::
```

4.5. Configure SIP Signaling

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 that the field is set to **n**. Setting this filed to **y** will cause Communication Manager to function as a Feature Server.
- Transport Method – Set to **tls** (Transport Layer Security).
- Near-end Node Name – Set to **procr** as displayed in **Section 4.4**.
- Far-end Node Name – Set to the Session Manager name configured in **Section 4.4**.
- Far-end Network Region – Set to the region configured in **Section 4.3**.
- Far-end Domain – Set to **avaya.com**. This should match the Authoritative Domain value in **Section 4.3**.

```
add signaling-group 92
                                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? n                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

4.6. Configure Trunk Group

To configure the trunk group, enter the **add tunk-group <t>** command, where **t** is an available 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.
- Service Type – Set the Service Type field to **tie**.
- Signaling Group – Set to the Group Number field value configured in the SIGNALING GROUP form.
- 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: 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: 20
```

On **Page 3**, set the Numbering Format field to **unk-pvt.**

```
add trunk-group 92                                              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
```

4.7. Configure SIP Endpoint

This section describes the steps for administering SIP stations in Communication Manager and associating with OPS station extensions. Enter the **add station <s>** command, where **s** is an extension valid in the provisioned dial plan. The following fields were configured for the compliance test.

- Type – Set to **9630SIP**.
- Name – Enter a descriptive name

Repeat this step as necessary to configure additional SIP endpoint extensions.

```
add station 72027                                               Page   1 of   6
                                     STATION

Extension: 72027                        Lock Messages? n                BCC: 0
     Type: 9630SIP                       Security Code: *                 TN: 1
     Port: IP                          Coverage Path 1:                  COR: 1
     Name: 72027                       Coverage Path 2:                  COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                Location:                  Time of Day Lock Table:
              Loss Group: 19
                                                 Message Lamp Ext: 72027

        Display Language: english                  Button Modules: 0

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

                                                         IP Video? n
```

On **Page 6**, set the SIP Trunk field to **aar**. By configuring this page, off-pbx-telephone station-mapping will be automatically generated.

```
add station 72027                                               Page   6 of   6
                                     STATION
SIP FEATURE OPTIONS
         Type of 3PCC Enabled: None
                   SIP Trunk: aar
```

The following shows the result of the STATION TO OFF-PBX TELEPHONE MAPPING form after creating all SIP endpoints.

```
list off-pbx-telephone station-mapping

                    STATION TO OFF-PBX TELEPHONE MAPPING

Station         Appl   CC  Phone Number     Config Trunk  Mapping      Calls
Extension                                   Set    Select Mode         Allowed

72021           OPS        72021            1  /   aar    both         all
72022           OPS        72022            1  /   aar    both         all
72023           OPS        72023            1  /   aar    both         all
72027           OPS        72027            1  /   aar    both         all
72028           OPS        72028            1  /   aar    both         all
72029           OPS        72029            1  /   aar    both         all
```

4.8. Configure Route Pattern

For the trunk group created in **Section 4.6**, define the route pattern by entering the **change route-pattern <r>** command, where **r** is an unused route pattern number. The route pattern consists of a list of trunk groups that can be used to route a call. The following screen shows route-pattern 92 will utilize the trunk group 92 to route calls. The default values for the other fields may be used.

```
change route-pattern 92                                           Page   1 of   3
                    Pattern Number: 92  Pattern Name: IMS SIP trunk
                             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: 92   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                                            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
```

4.9. Configure AAR Analysis

For the AAR Analysis Table, create the dial string that will map calls to the ipTTY via the route pattern created in **Section 4.8**. Enter the **change aar analysis <x>** command, where **x** is a starting partial digit (or full digit). The dialed string created in the AAR Digit Analysis table should contain a map to the ipTTY system extension, which is configured as x72031. During the configuration of aar table, the Call Type field was set to **unku**.

```
change aar analysis 720                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 3

          Dialed              Total     Route     Call    Node   ANI
          String             Min  Max  Pattern    Type    Num    Reqd
    72031                     5    5      92       unku            n
```

5. Configure Avaya Aura™ Session Manager

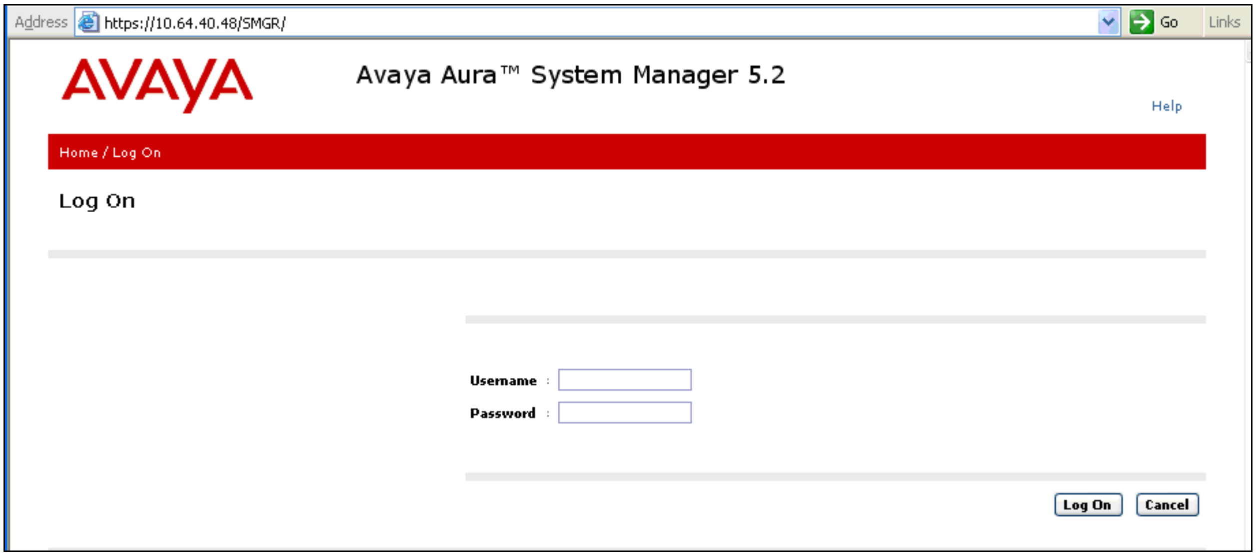
This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the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

5.1. Configure SIP Domain

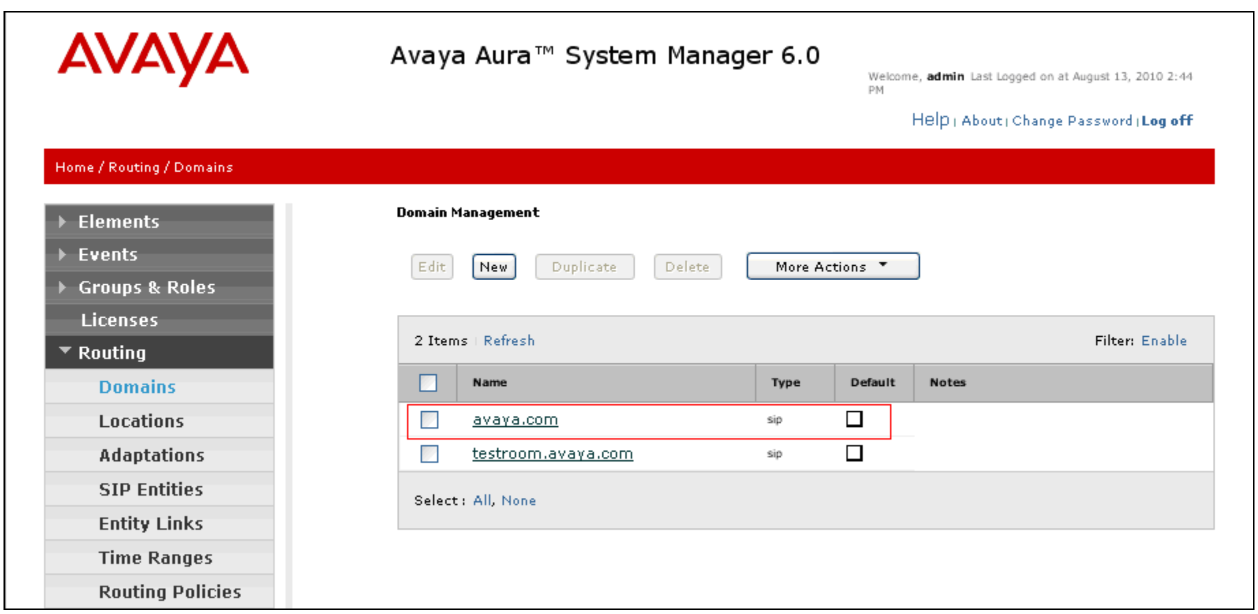
Launch a web browser, enter **https://<IP address of System Manager>/SMGR** in the URL, and log in with the appropriate credentials.



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

- **Name –** Enter the Authoritative Domain name specified in **Section 4.3**, which is **avaya.com**.
- **Type** – Select **SIP**

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



5.2. 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 (not shown) to create a new SIP Entity location.

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

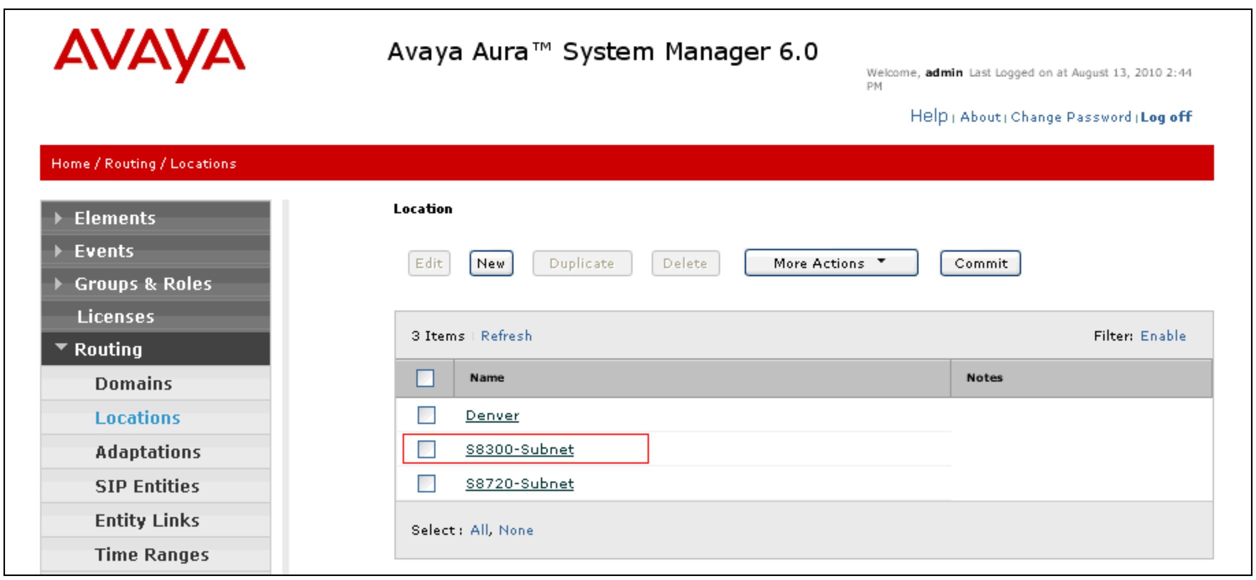
- Enter a descriptive Location name in the Name field (e.g. **S8300-Subnet**).
- Enter a description in the Notes field if desired.

In the **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.



5.3. 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

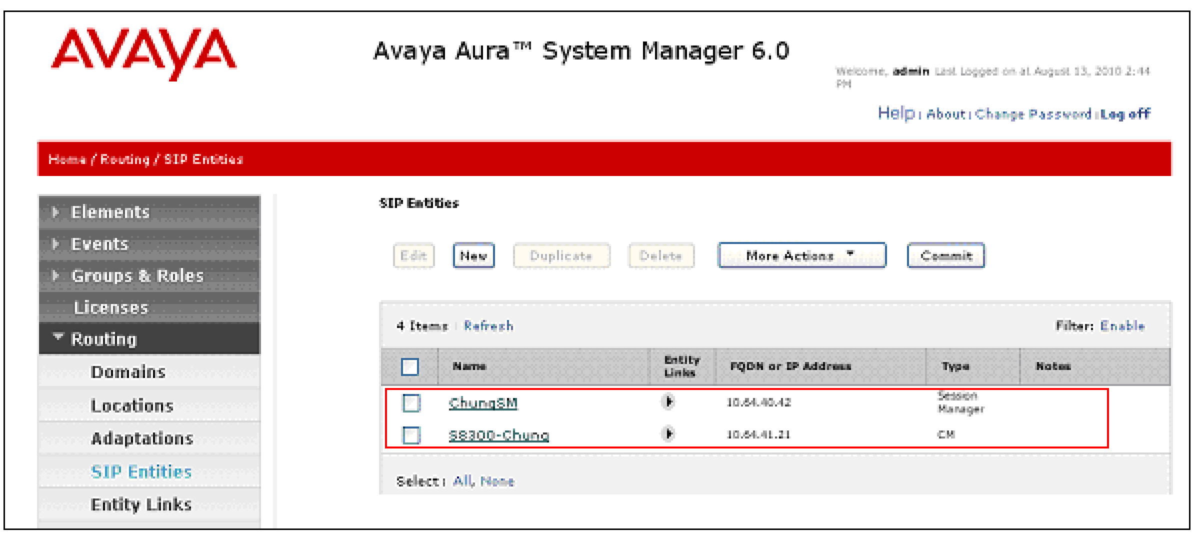
Navigate to **Routing → SIP Entities**, and click on the **New** button (not shown) to create a new SIP entity. Provide the following information:
In the **General** section**,** enter the following values and use default values for remaining fields.

- 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 on 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.

In the **Sip Link Monitoring** section:

- Select a desired option. During the compliance test, **Use Session Manager Configuration** option was utilized.

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



5.4. Configure Entity Links

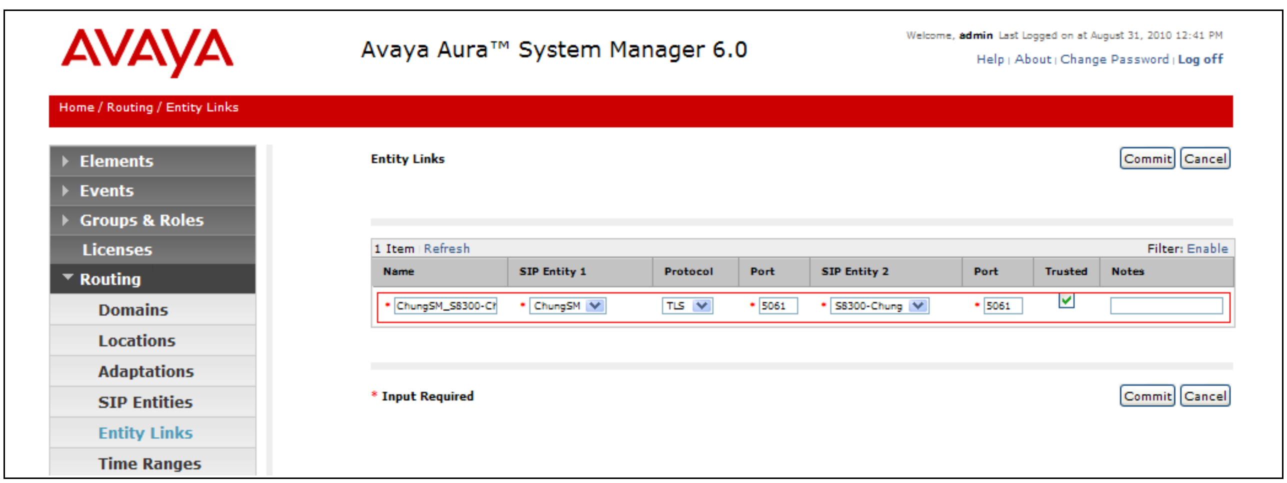
Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ⇔ Communication Manager

Navigate to **Routing → Entity Links**, and click on the **New** button (not shown) to create a new entity link. 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 5.3** (e.g. **ChungSM**).
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- In the **SIP Entity 2** drop down menu, select one of the two entities in the bullet list above (which were created in **Section 5.3**). 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.
- In the **Protocol** drop down menu, select the protocol to be used.
- 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.



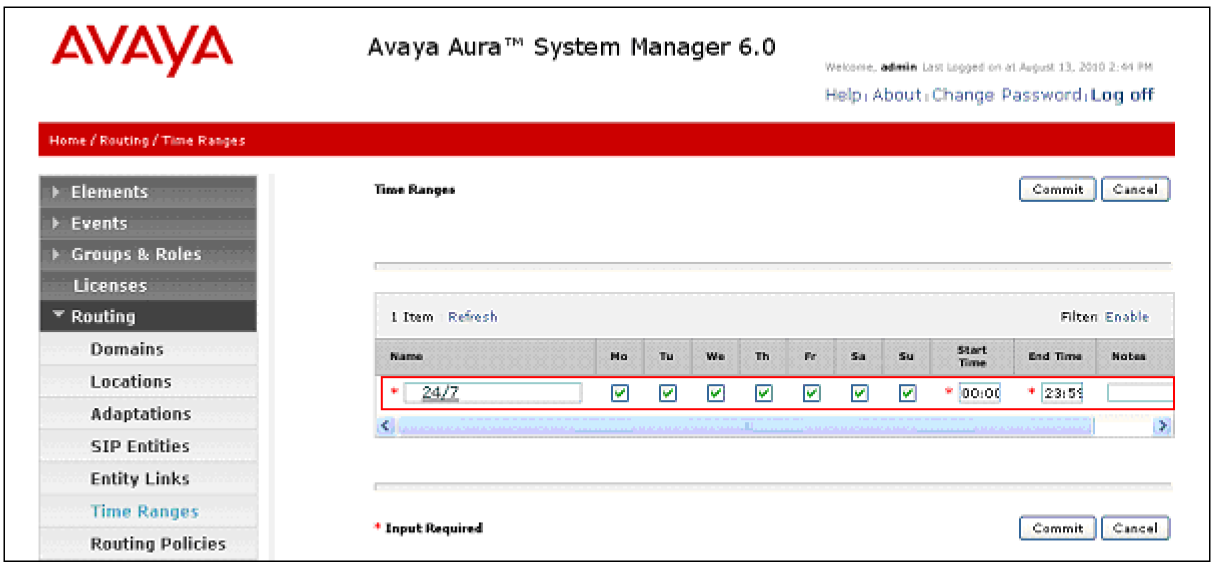
5.5. Time Ranges

The Time Ranges form allows admission control criteria to be specified for Routing Policies (**Section 5.6**). 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.



5.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 5.3**) with Time of Day admission control parameters (**Section 5.5**) and Dial Patterns (**Section 5.7**). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Communication Manager.

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

General section

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

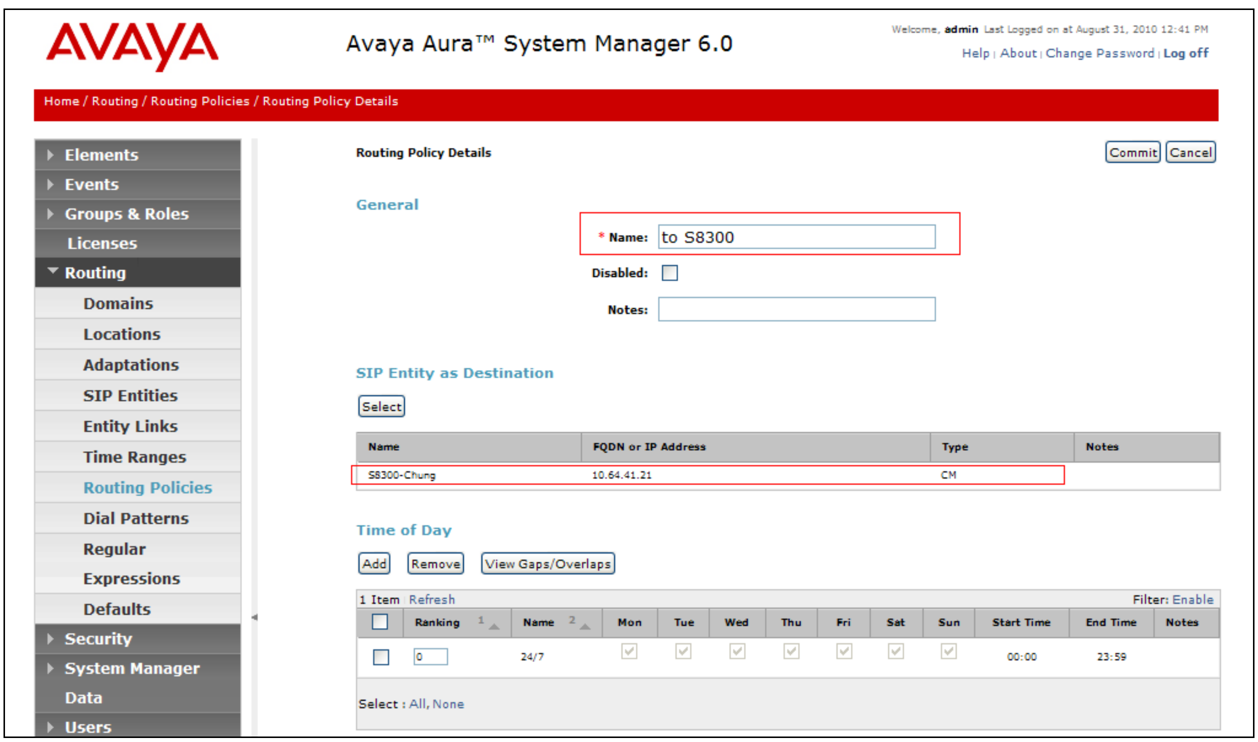
SIP Entity as Destination section

- Click the **Select** button.
- Select the SIP Entity that will be the destination for this call (not shown).
- 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.



5.7. Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In addition, the domain in the request URI is also examined.

To add a Dial Pattern, select **Routing → Dial Patterns,** and click on the **New** button (not shown) on the right. During the compliance test, a 5 digit dial plan was utilized. Provide the following information:

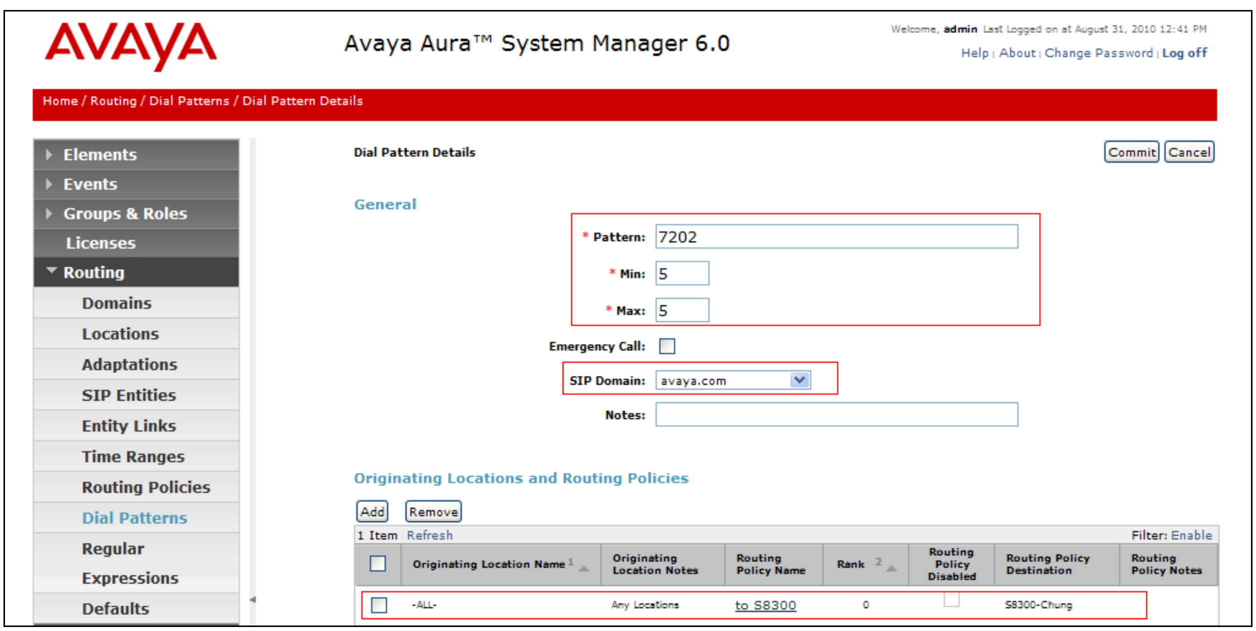
General section

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

Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (not shown).
- Click on the boxes for the appropriate Originating Locations and Routing Policies (see **Section 5.6**) that pertain to this Dial Pattern.
    - Originating Location Name to **All**
    - Routing Policy Name **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.

5.8. Configure Managed Elements

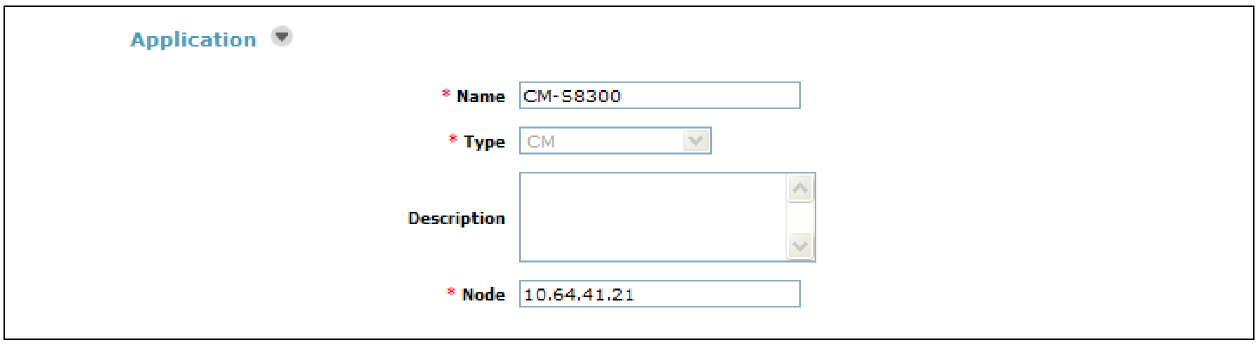
To define a new Managed Element, navigate to **Elements → Inventory → Manage Elements**. Click on the **New** button (not shown) to open the **New Entities Instance** page.

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).

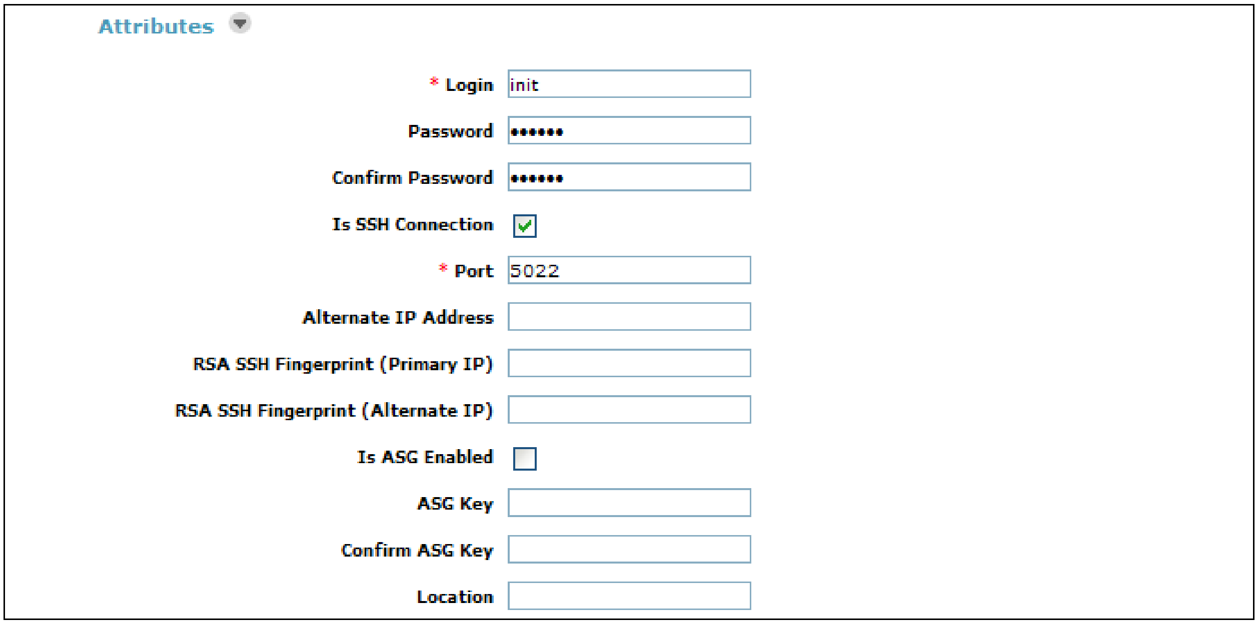
In the New CM Instance Page, provide the following information:

- 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.

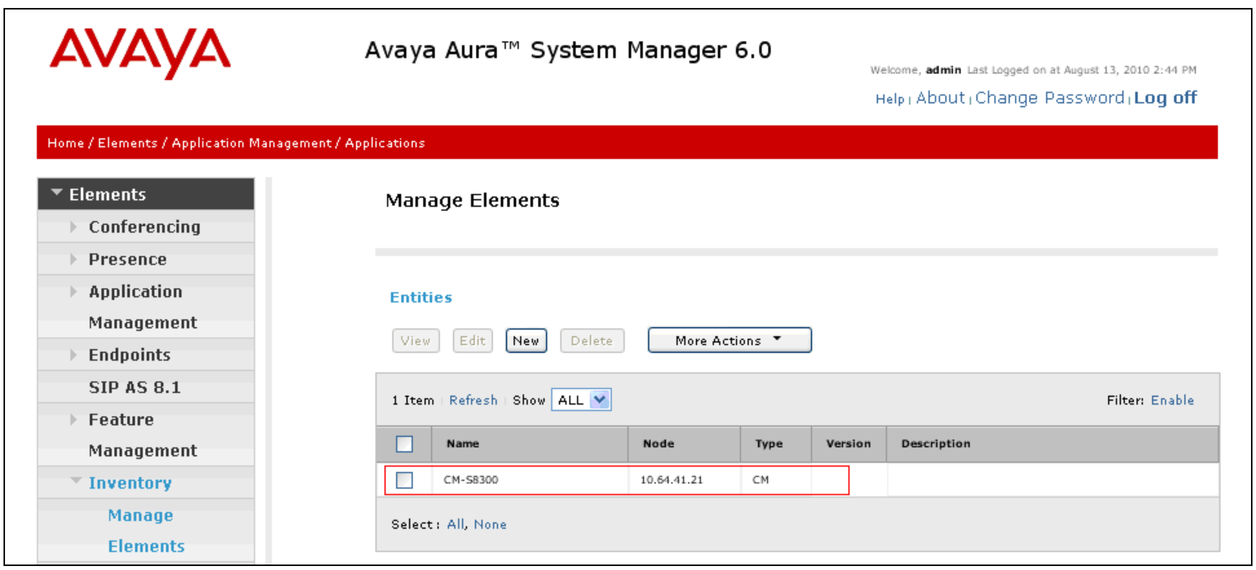


- Leave the fields in the Port and Access Point sections blank. In the SNMP Attributes section, verify the default value of **None** is selected for the Version field.

- 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



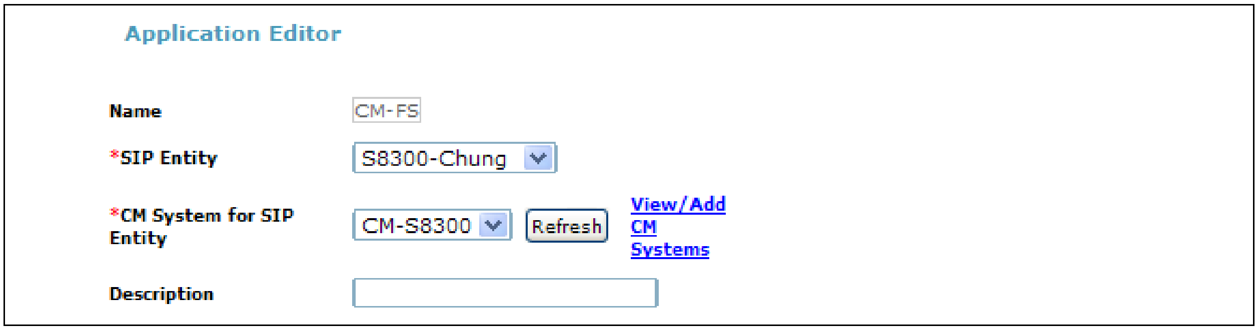
Click **Commit** to save the element. The following screen shows the element created, CM-S8300, during the compliance test.



5.9. Configure Applications

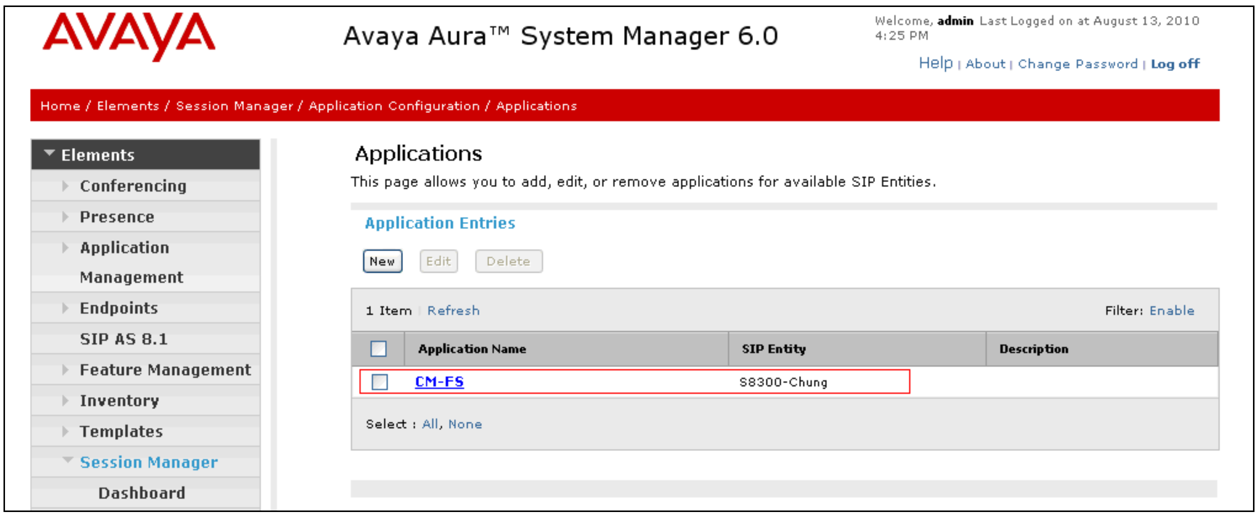
To define a new Application, navigate to **Elements → Session Manager → Application Configuration → Applications**. Click **New** (not shown) to open the Applications Editor page, and provide the following information:

- Application Editor section
  - Name – Enter name for the application.
  - SIP Entity - Select SIP Entity for Communication Manager defined in **Section 5.3**
  - CM System for SIP Entity – Select name of Managed Element defined for Communication Manager in **Section 5.8**
  - Description – Enter description if desired.



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

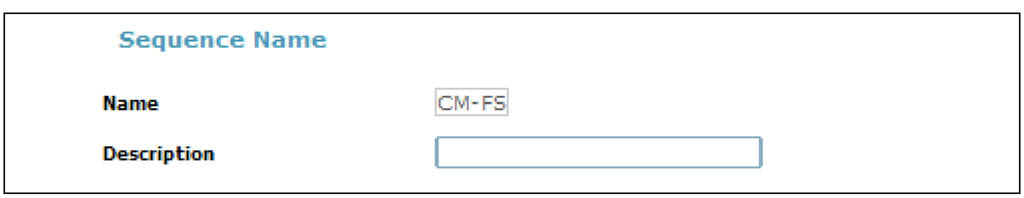
Click the **Commit** button (not shown) to save the Application. The screen below shows the Application, CM-FS, defined for Communication Manager.



5.10. Define Application Sequence

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

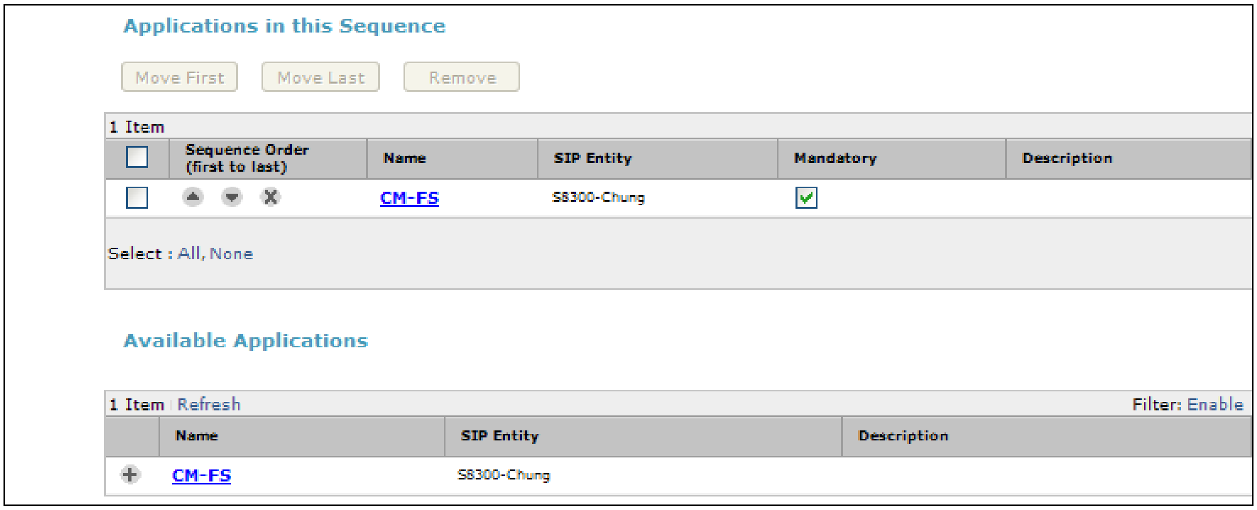
- Sequence Name section
  - **Name** – Enter name for the application
  - **Description** – Enter description, if desired.



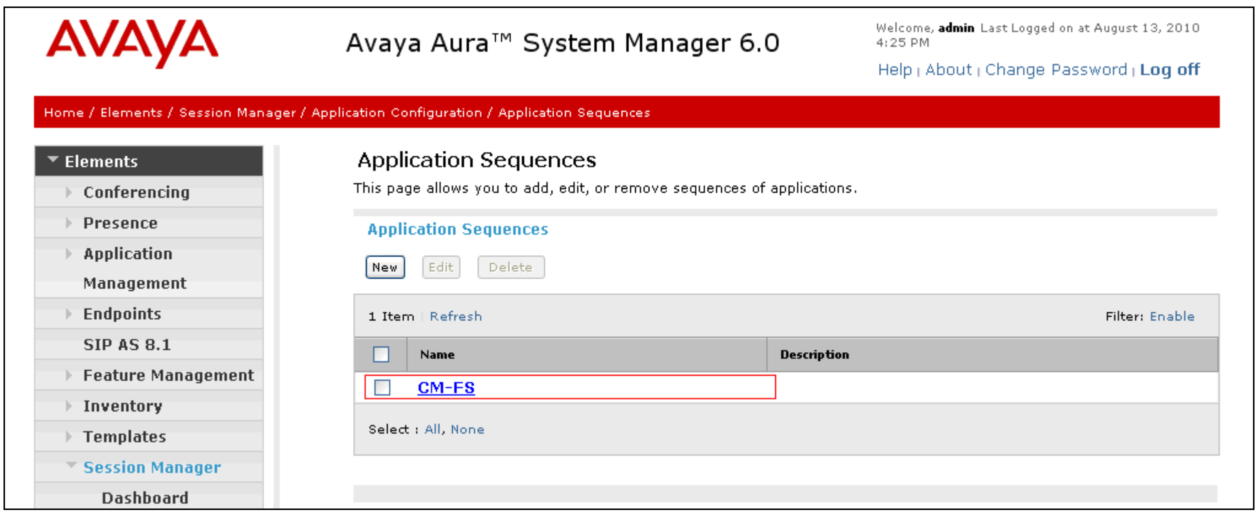
- Available Applications section
  - Click + icon associated with the Application for Communication Manager defined in **Section 5.9** to select this application.

- 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.

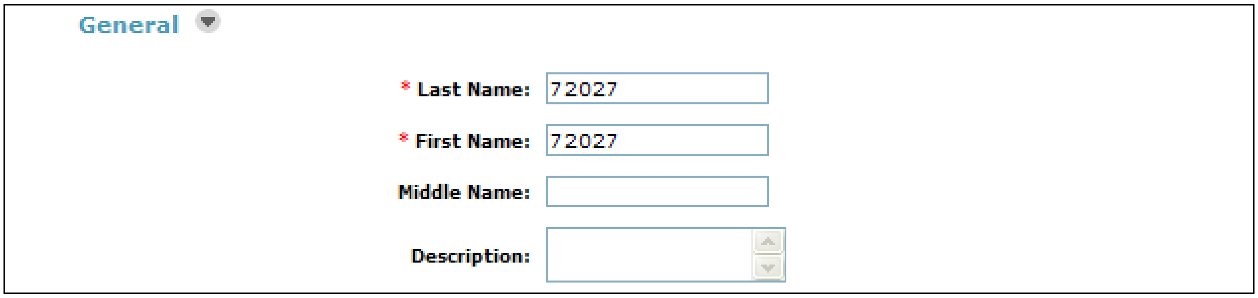


5.11. Configure SIP Users

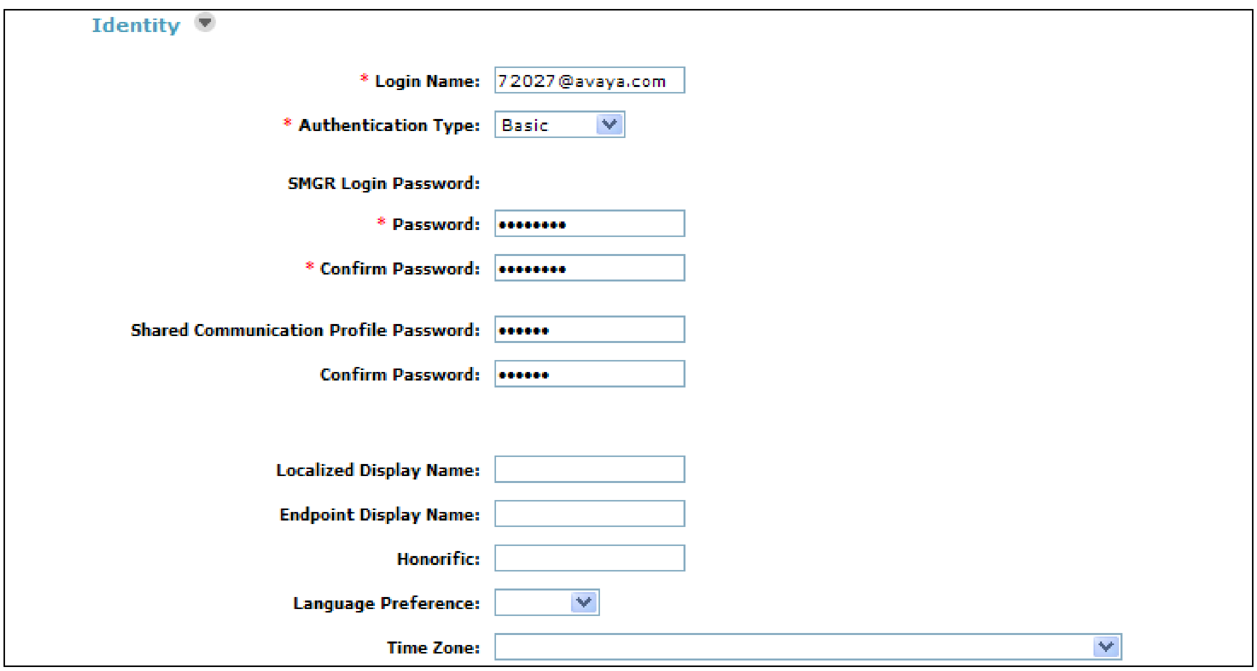
Add new SIP users for each 9600-Series SIP station defined in **Section 4.7.** Alternatively, use the option to automatically generate the SIP station after adding a new SIP user.

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

- <u>General section</u>
  - Last Name – Enter last name of user.
  - First Name – Enter first name of user.

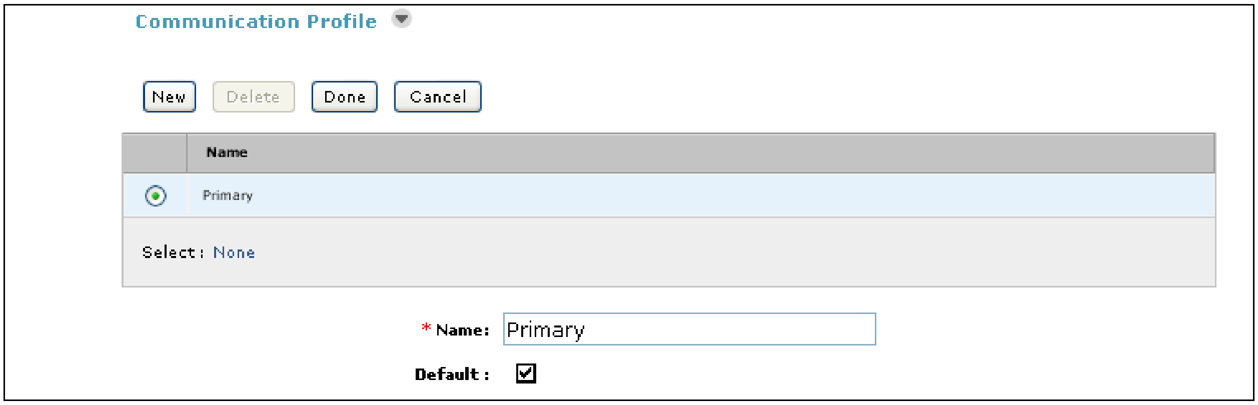


- <u>Identity section</u>
  - Login Name – Enter extension number@sip domain defined in **Section 4.3**.
  - Authentication Type – Verify **Basic** is selected.
  - SMGR Login Password – Enter password to be used to log into System Manager.
  - Confirm Password – Repeat value entered above.
  - Shared 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 4.7**)
  - Confirm Password – Repeat numeric password



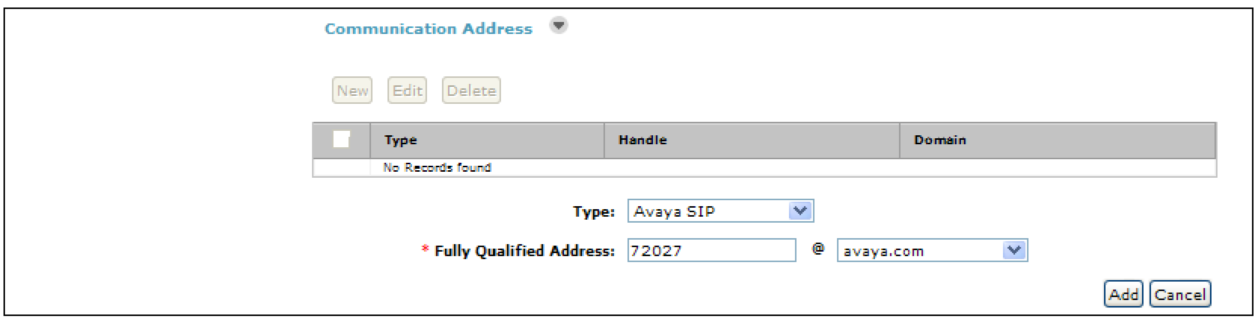
- <u>Communication Profile section</u>
  Verify there is a default entry identified as the **Primary** profile for the new SIP user. If an entry does not exist, select **New** and enter values for the following required attributes:

- Name – Enter **Primary**.
- Default – Enter ☑

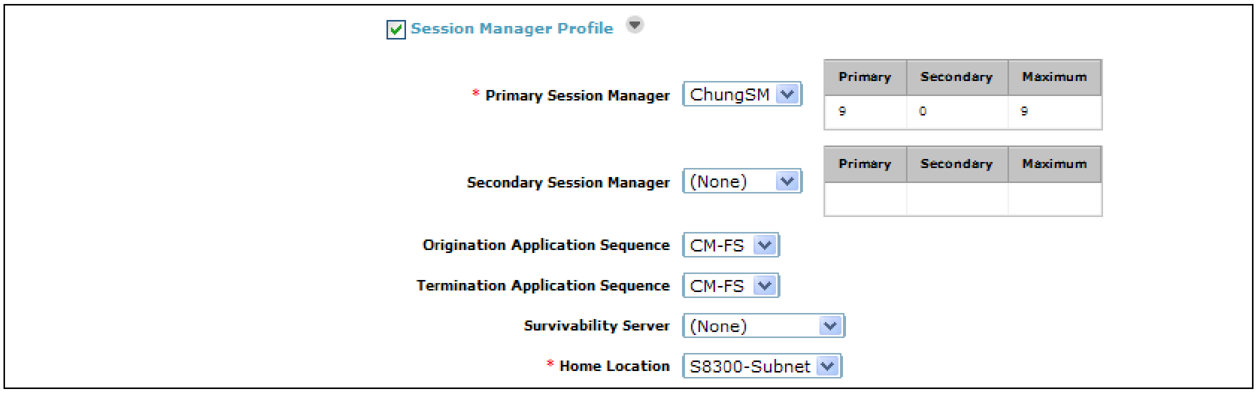


- Communication Address sub-section
  Select **New** to define a **Communication Address** for the new SIP user, and provide the following information.
  - Type – Select **Avaya SIP** using drop-down menu.
  - Full Qualified Address – Enter same extension number and domain used for Login Name, created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

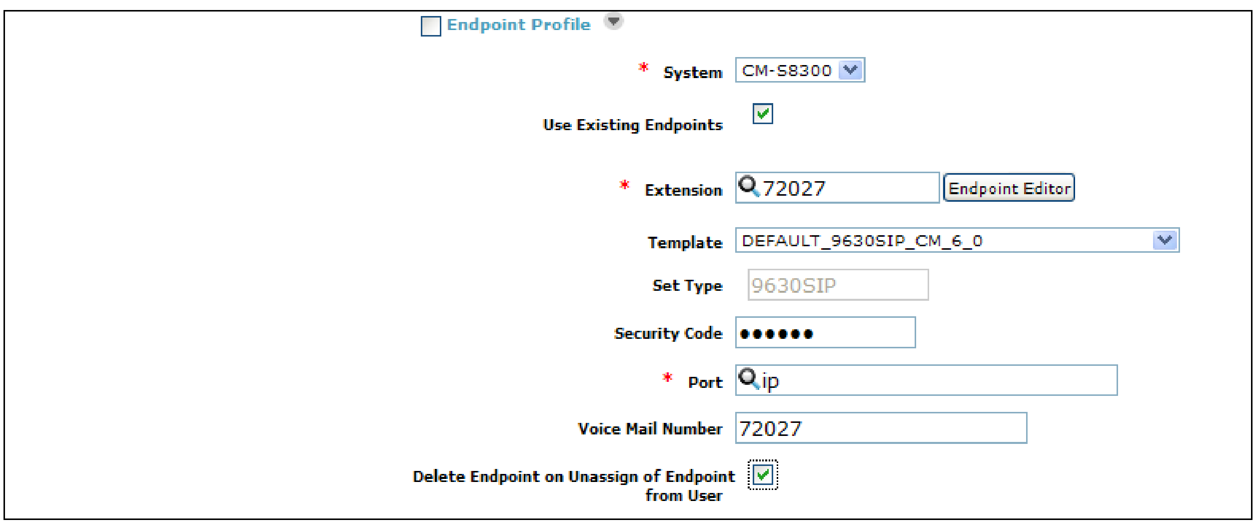
  Click the **Add** button to save the Communication Address for the new SIP user.



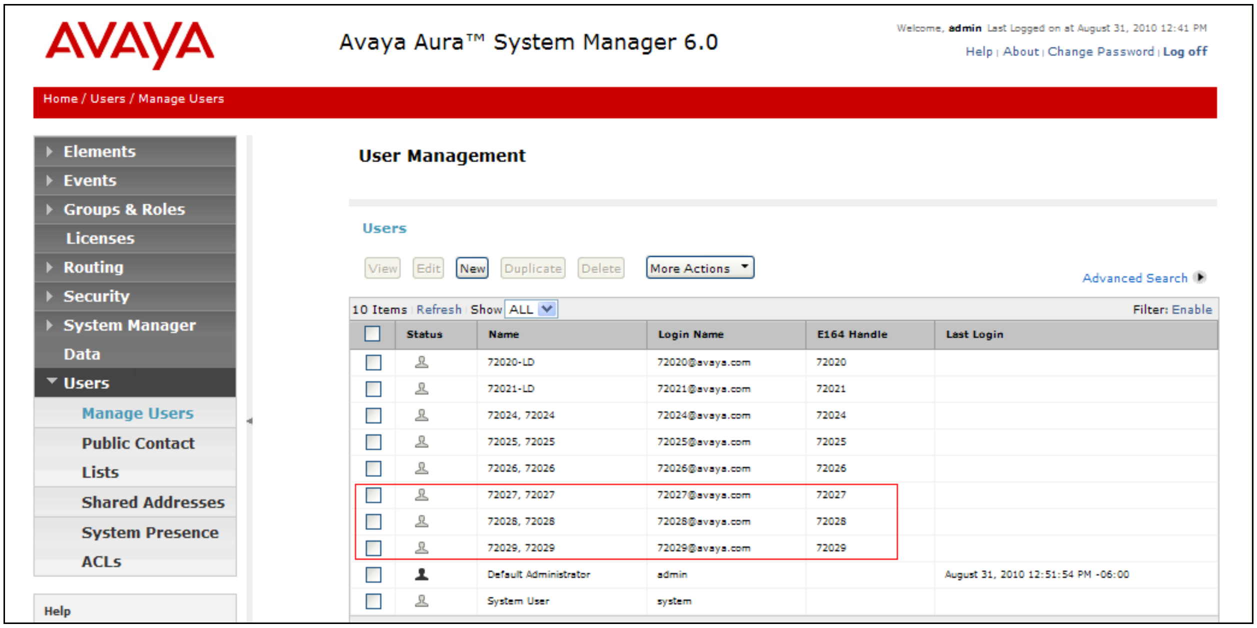
- Session Manager Profile section
  - Primary Session Manager – Select one of the Session Managers.
  - Secondary Session Manager – Select **(None)** from drop-down menu.
  - Origination Application Sequence – Select Application Sequence defined in **Section 5.10** for Communication Manager.
  - Termination Application Sequence – Select Application Sequence defined in **Section 5.10** for Communication Manager.
  - Survivability Server – Select **(None)** from drop-down menu.
  - Home Location – Select Location defined in **Section 5.2**.



- <u>Endpoint Profile section</u>
  - System – Select Managed Element defined in **Section 5.8** 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.
  - Extension - Enter same extension number used for **Login Name** previously.
  - 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 the ipTTY endpoints.

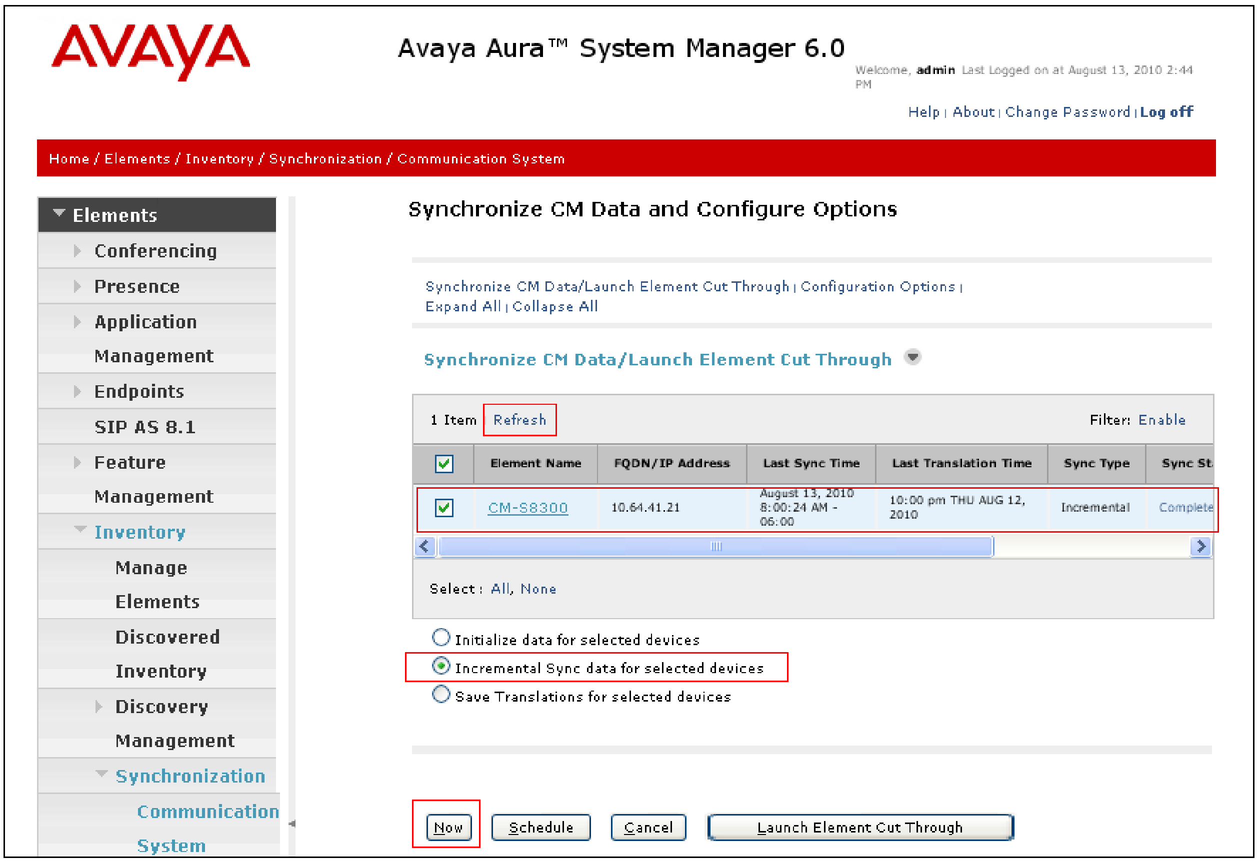

AVAYA
Avaya Aura™ System Manager 6.0
Welcome, admin Last Logged on at August 31, 2010 12:41 PM
Help | About | Change Password | Log off
Home / Users / Manage Users
Elements
Events
Groups & Roles
Licenses
Routing
Security
System Manager Data
Users
Manage Users
Public Contact Lists
Shared Addresses
System Presence ACLs
Help
User Management
Users
View Edit New Duplicate Delete More Actions
Advanced Search
10 Items Refresh Show ALL
Filter: Enable
Status Name Login Name E164 Handle Last Login
72020-LD 72020@avaya.com 72020
72021-LD 72021@avaya.com 72021
72024, 72024 72024@avaya.com 72024
72025, 72025 72025@avaya.com 72025
72026, 72026 72026@avaya.com 72026
72027, 72027 72027@avaya.com 72027
72028, 72028 72028@avaya.com 72028
72029, 72029 72029@avaya.com 72029
Default Administrator admin August 31, 2010 12:51:54 PM -06:00
System User system

5.12. 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.**

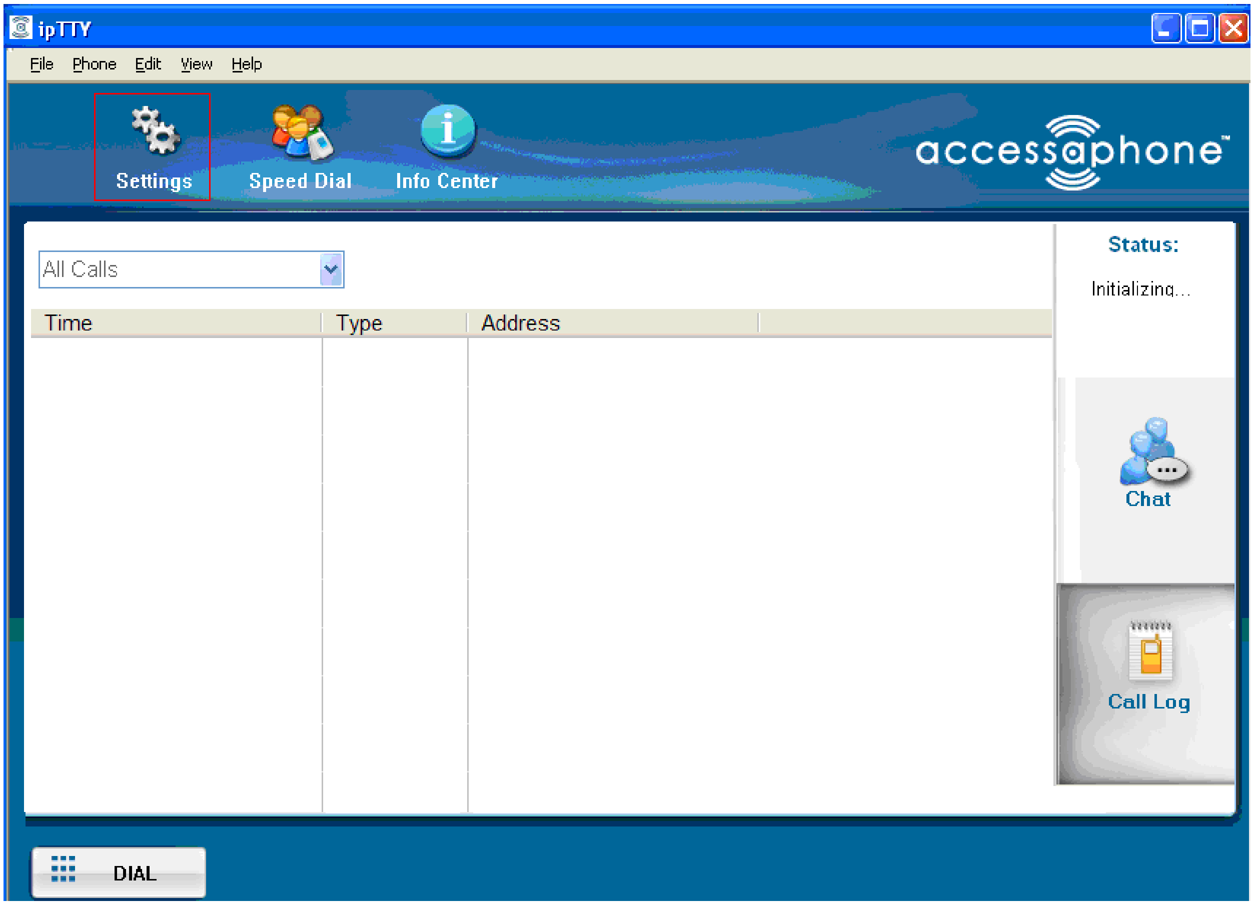
On the Synchronize CM Data and Configure Options page, expand the Synchronize CM Data/Launch Element Cut Through table

- 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**.



6. Configure Tenacity ipTTY

This section provides steps to configure Tenacity ipTTY. The latest firmware was provided by Tenacity. To start the Tenacity ipTTY application, double click the ipTTY icon (). Select the **Settings** button to configure the ipTTY for interfacing with Session Manager.

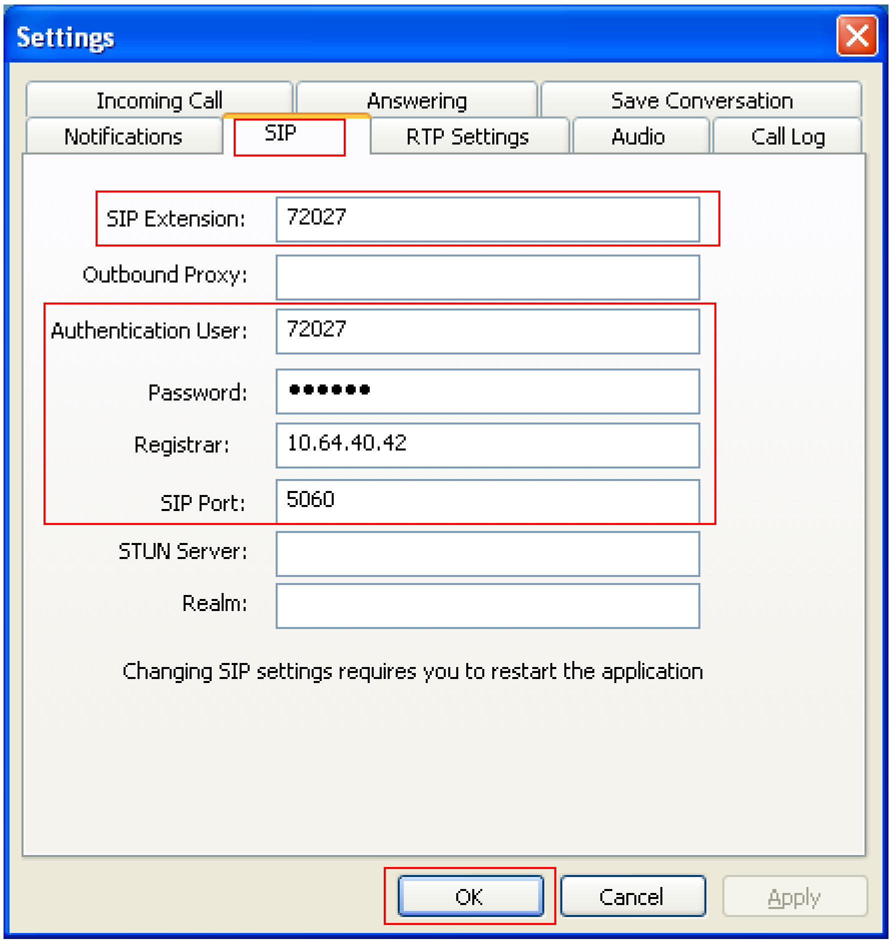


Select the **SIP** tab, and provide the following information:

- SIP Extension – Enter the user extension created in **Section 5.11**.
- Authentication User – username (usually the same as the SIP Extension)
- Password – Enter the password created in **Section 5.11**.
- Registrar – Enter the IP address of Session Manager.
- SIP Port – The default port is utilized.

Click on the **OK** button, after the completion.

Note*: In order for the settings to take effect, the ipTTY must be closed and reopened.*



7. General Test Approach and Test Results

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

- Tenacity ipTTY successfully registers with Session Manager.
- Calls can be successfully established between Tenacity ipTTY and Avaya SIP and H.323 telephones.
- Tenacity ipTTY successfully negotiates the right codec (G.711MU). Tenacity ipTTY supports only G.711MU codec.
- Tenacity ipTTY successfully transfers a call.
- Tenacity ipTTY successfully forwards a call.
- Successfully tested DTMF.
- Successfully left messages on Avaya IA770 Audix.
- Successfully retrieve messages from Avaya IA770 Audix.
- Successfully transfer a TTY call from Avaya One-X Communicator to ipTTY in the same PC.
- Successfully enabled audio on an ipTTY, and tested with Avaya IP telephones and an Avaya One-X Communicator.

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

The test objectives were verified. For serviceability testing, the Tenacity ipTTY operated properly after recovering from failures such as cable disconnects, and resets of the Tenacity ipTTY and the Session Manager.

During the compliance test, when connected to the voicemail server to leave or retrieve message, gobbled text were observed, meaning the translation from voice to text was not performed properly. This issue is being investigated by Tenacity ipTTY developers.

During a voice call between an One-X Communicator and an ipTTY, low grade voice was observed from the ipTTY side.

8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that Tenacity ipTTY successfully registers with Session manager by following the **Elements ➔ Session Manager ➔ System Status ➔ User Registrations** link on the System manager Web Interface.
- Place calls to and from Tenacity ipTTY 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 4.6**, and **r** is the trunk group member used for a call.

9. Conclusion

Tenacity ipTTY was compliance tested with Communication Manager (Version 6.0) and Session Manager (Version 6.0). Tenacity ipTTY (Version 2.0.1.5) functioned properly for feature and serviceability. Tenacity ipTTY successfully registered with Session Manager, placed and received calls to and from SIP and non-SIP telephones, and executed other telephony features like transfer, forward, and voicemail. During compliance testing, Tenacity ipTTY and Avaya One-X Communicator were successfully installed into the same PC. Some observations are noted in **Section 7**.

10. Additional References

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

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

The following document was provided by Tenacity.

[3] *Tenacity ipTTY Quick Start Guide*, Document Version 1.2, October 2009.

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.