Avaya Solution & Interoperability Test Lab

Application Notes for VTech 2-Line Hospitality S2x20 SIP Phones Version 39.3.68.07 with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager 6.3 – Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and VTech Hospitality SIP Phones.

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

The purpose of the document is to summarize configurations, test notes, and issues if any during the compliance test between VTech Hospitality SIP phones and Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The VTech SIP Hospitality Phones are available in a single or dual-line phone, and in two styles as well as offering a corded and cordless option. There are two models VTech Cordless S2420 and Corded S2220 used for the compliance test. The S2420 and S2220 phones were included in the testing. All of these models share core hardware and SIP firmware. The primary differences with these phones are either cosmetic, or corded versus wireless handsets. These variations do not impact the interoperability between the base station and the Avaya infrastructure, so use of any of these models can be expected to yield the same results as those observed in the testing described in these Application Notes.

2. General Test Approach and Test Results

The compliance test focused on the interoperability between the VTech Hospitality SIP Phones, Avaya Aura® Session Manager and Avaya Aura® Communication Manager including the ability to make and receive calls from PSTN endpoints and Avaya SIP, H.323, and Digital phones.

As the purpose of these phones is for hotel guest rooms, certain functionality considered to be standard on Avaya endpoints is not supported and therefore was not tested. For example, the VTech phones do not support multiple line appearances. More details on these limitations are described in the Test Results in **Section 2.2**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

VTech SIP phones register with Session Manager and thus are able to use Communication Manager application sequencing in a similar manner to Avaya SIP endpoints. The following areas were tested in the compliance test:

- Registration of VTech phone to Session Manager.
- Basic call features: Answer, Hold/Resume, Mute/Un-mute, Drop, Decline, Message Waiting Indicator, DTMF, Call Park, Call Pickup, Call Waiting, Call Forward, Transfer, and Conference.
- Codec negotiation, Media Shuffling, and Session Refresh Interval.
- Hospitality features: Automatic Wakeup Call and Housekeeping status.
- Serviceability test which consisted of the VTech SIP phones re-registering with Session Manager following loss of network connections, and server reboots.

2.2. Test Results

The objectives described in **Section 2.1** were verified. All test cases were executed and passed.

2.3. Support

Information, Documentation and Technical support for VTech Hotel Phones can be obtained at:

- Phone: +1 (888) 907-2007
- http://vtechhotelphones.com

3. Reference Configuration

Figure 1 illustrates the test configuration diagram showing the integration of the VTech SIP phone to the Avaya Solution. VTech Hospitality SIP phone registers to Session Manager via SIP and use the telephony features from Communication Manager. The system test had T1 link from Communication Manager to real PSTN for test cases related to PSTN calls. A SIP trunk was setup to an Avaya Communication Server 1000E (CS1000E) to test that the VTech phone made/received off-net calls. Avaya Aura® Messaging was used as the voice mail system.

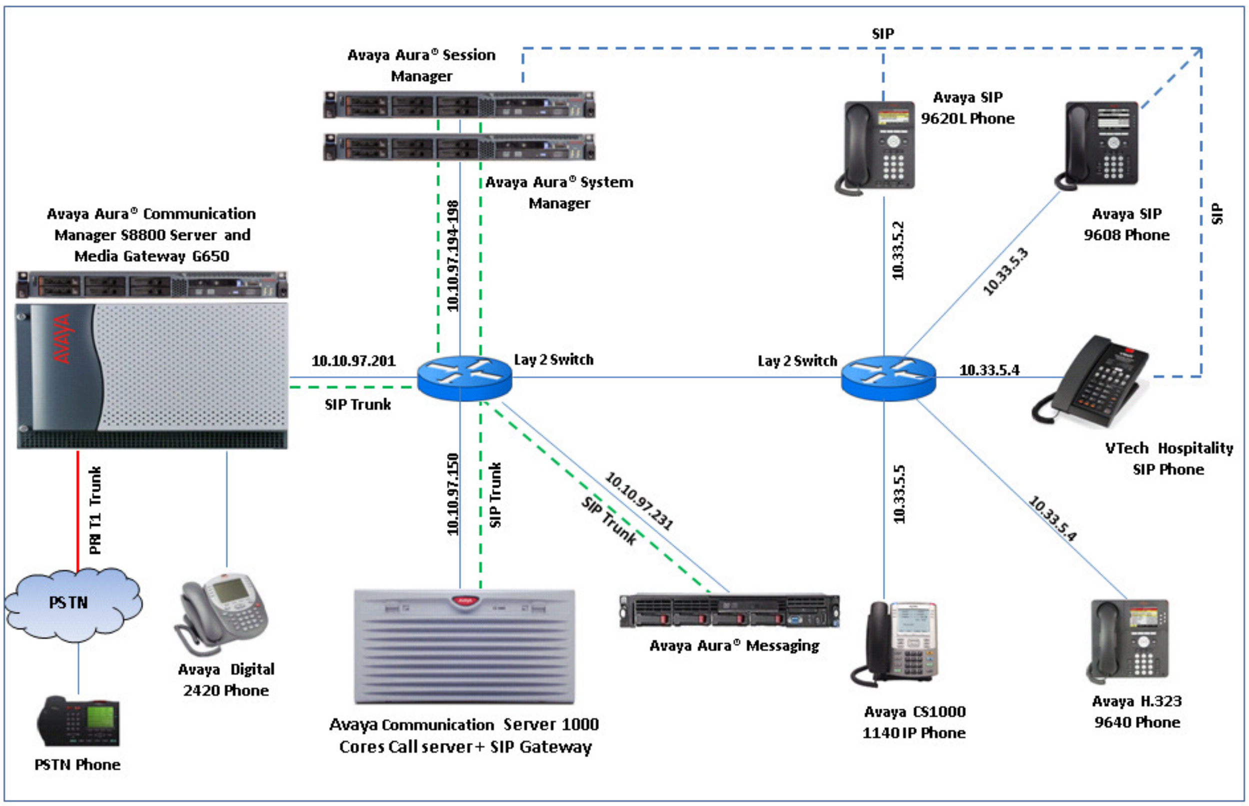


Figure 1: Test configuration diagram

4. Equipment and Software Validated

The following equipment and software were used for the compliance test provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on an Avaya S8800 Server	R6.3.0 – FP2 Build R016x.03.0.124.0 Patch 20553
Avaya Aura® System Manager running on an Avaya S8800 Server	R6.3.0 – FP2 Build 6.3.0.8.5682
Avaya Aura® Session Manager running on an Avaya S8800 Server	R6.3.0 – FP2 Build 6.3.2.632001
Avaya Aura® Messaging running on an Avaya S8800 Server	R6.1 SP2 Build R016x.00.1.510.1
Avaya Media Gateway G650 • IP Server interface TN2312BP • IP Media Processor TN2302AP	 HW06 - FW043 HW20 - FW117
Avaya Communication Server 1000E running on an Avaya CPPM card	R7.5
Avaya 9608 IP Deskphone (with Avaya one-X® H.323 firmware)	6.2313
Avaya 9611 IP Deskphone (with Avaya one-X® H.323 firmware)	6.2.3
Avaya 9620 IP Deskphone (with Avaya one-X® SIP firmware)	2.6.9.1
Avaya Digital Deskphone 2420	6.0
VTech SIP Phone S2420	SIP_39.3.68.07
VTech SIP Phone S2220	SIP_39.3.68.07
VTech SIP Phone S2210	SIP_39.3.68.07

5. Configure Avaya Aura® Communication Manager

It is assumed that Communication Manager is already installed and configured. This section describes the necessary configurations for VTech SIP phone to work with Communication 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. VTech SIP phone 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: 65000 214
                                     Maximum Stations: 41000 38
                             Maximum XMOBILE Stations: 41000 0
                   Maximum Off-PBX Telephones - EC500: 41000 4
                   Maximum Off-PBX Telephones -   OPS: 41000 24
                   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   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: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 6
             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: 41000 0
                   Maximum Video Capable IP Softphones: 18000 1
                       Maximum Administered SIP Trunks: 24000 130
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   1
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   1
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

5.2. Administer 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.

```
change ip-codec-set 1                                             Page   1 of   2
                            IP Codec Set
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.729            n          2        20
 3: G.722-64K                   2        20
```

5.3. Administer 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** – Enter the appropriate name for the Authoritative Domain. During the compliance test, the authoritative domain is set to **bvwdev.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: 1          Authoritative Domain: bvwdev.com
    Name:                       Stub Network Region: n
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. Administer IP Node Name

This section describes the steps for setting IP node name for Session Manager's SIP signaling interface 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
SM63                    10.10.97.198
GW                      10.10.97.193
default                 0.0.0.0
procr                   10.10.97.201
```

5.5. Administer SIP Signaling IP

This section describes the steps for administering a signaling group in Communication Manager for signaling 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**.
- **Transport Method** – Set to **tcp**.
- **Near-end Node Name** - Set to **procr** as displayed in **Section 5.4**.
- **Far-end Node Name** - Set to the **Session Manager** name configured in **Section 5.4**.
- **Far-end Network Region** - Set to the region configured in **Section 5.3**.
- **Far-end Domain** - Set to **bvwdev.com**. This should match the SIP Domain value in **Section 6.1**.

```
add signaling-group 1                                           Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? y          Priority Video? n        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                  Far-end Node Name: SM63
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1

Far-end Domain: bvwdev.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. Administer SIP Trunk

This section describes the steps for administering a trunk 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.
- **Service Type** – Enter **tie**.
- **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 1                                                   Page   1 of  21
                                TRUNK GROUP

Group Number: 1                   Group Type: sip            CDR Reports: n
  Group Name: SIP trunk to SM            COR: 1        TN: 1        TAC: #001
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 15
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session. 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.

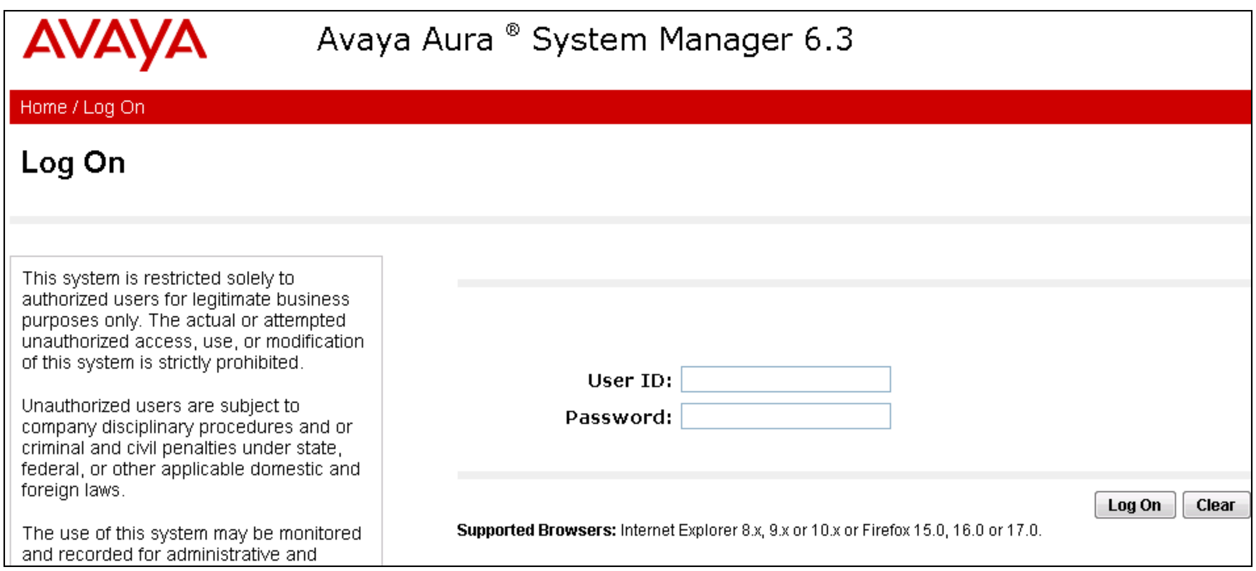
This section assumes that Session Manager and System Manager have been installed, and network connectivity exists between the two platforms.

The following steps describe for configuring Session Manager.

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

6.1. Administer SIP Domain

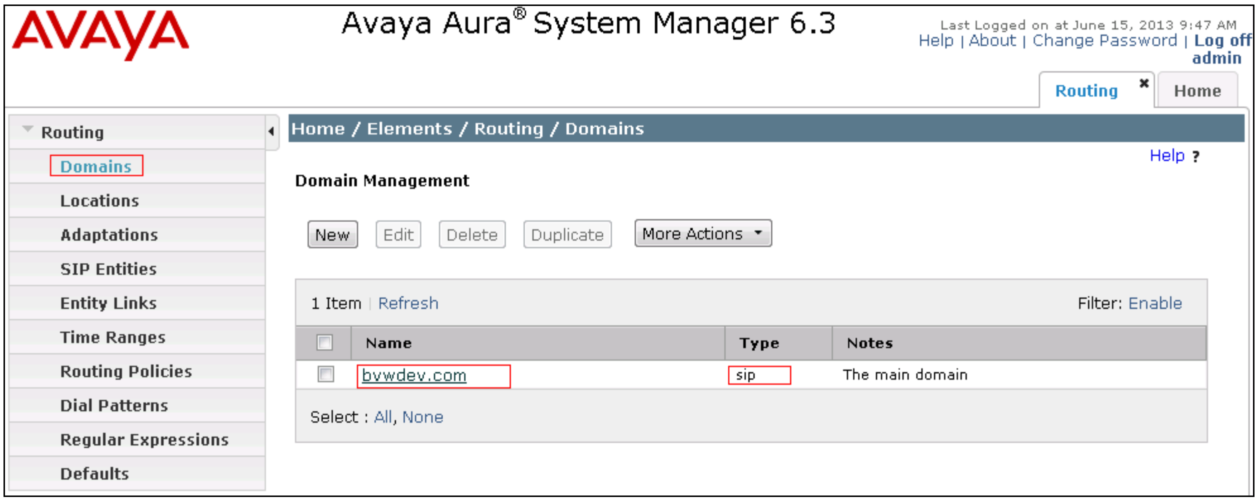
Launch a web browser, enter **https://<IP address of System Manager>** or **http://<FQDN of System Manager>** in the URL, and log in with the appropriate credentials.



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

- **Name –**Enter the Authoritative Domain name specified in **Section** Error! Reference source not found., which is **bvwdev.com**.
- **Type** – Select **SIP**.

Click **Commit** to save (not shown). The following screen shows the Domains page used during the compliance test.



6.2. Administer Locations

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

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

<u>General section</u>

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

- Enter a descriptive Location in the **Name** field (e.g. **Subnet 10.10.97.0**).
- Enter a description in the **Notes** field if desired.

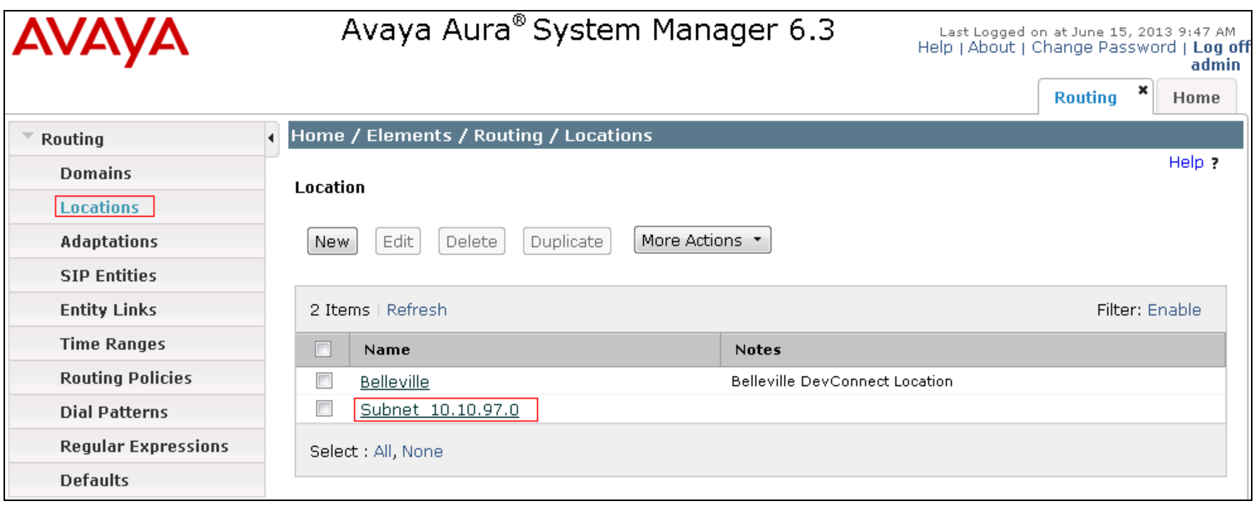
<u>Location Pattern section</u>

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

- The IP address information for the **IP address Pattern** (e.g. **10.10.97.***).
- A description in the **Notes** field if desired.

Repeat these 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 (not shown).

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



6.3. Administer SIP Entities

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

- Session Manager.
- Communication Manager (Avaya S8800 Server).

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

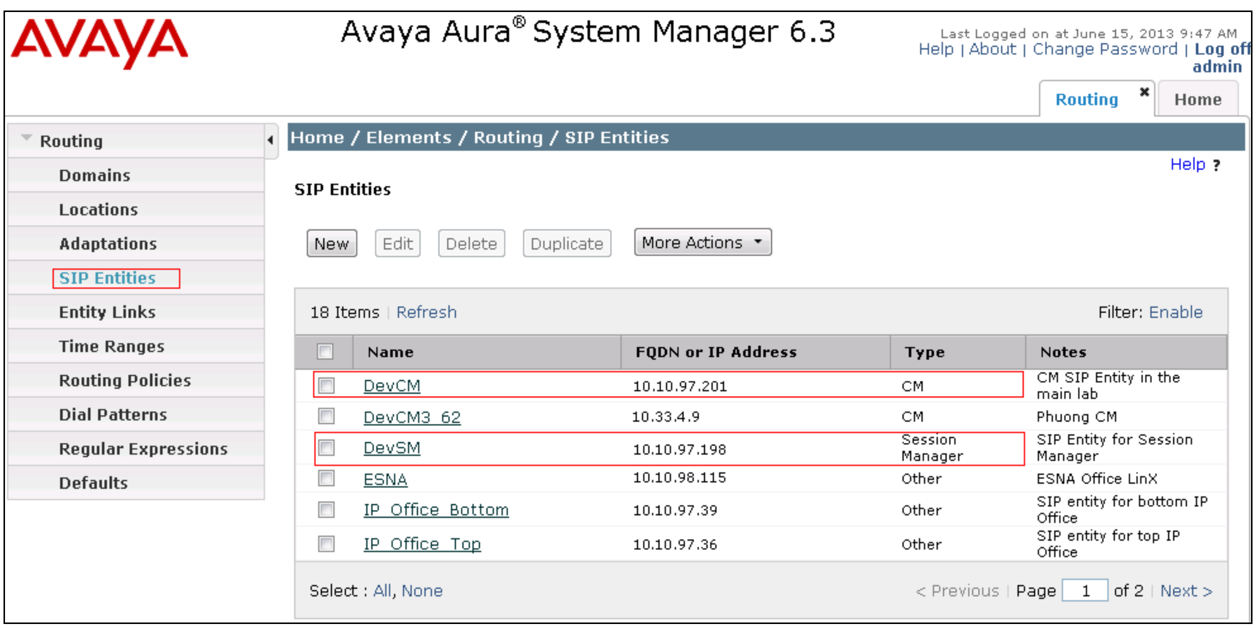
<u>General section</u>

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

- **Name**: Enter a descriptive name.
- **FQDN or IP Address:** Enter the IP address of the signaling interface on each:
  - Communication Manager
  - Session Manager virtual SM-100
- 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 (not shown). The following screen shows the SIP Entities page used during the compliance test.

Repeat all the steps for each new entity.



6.4. Administer Entity Links

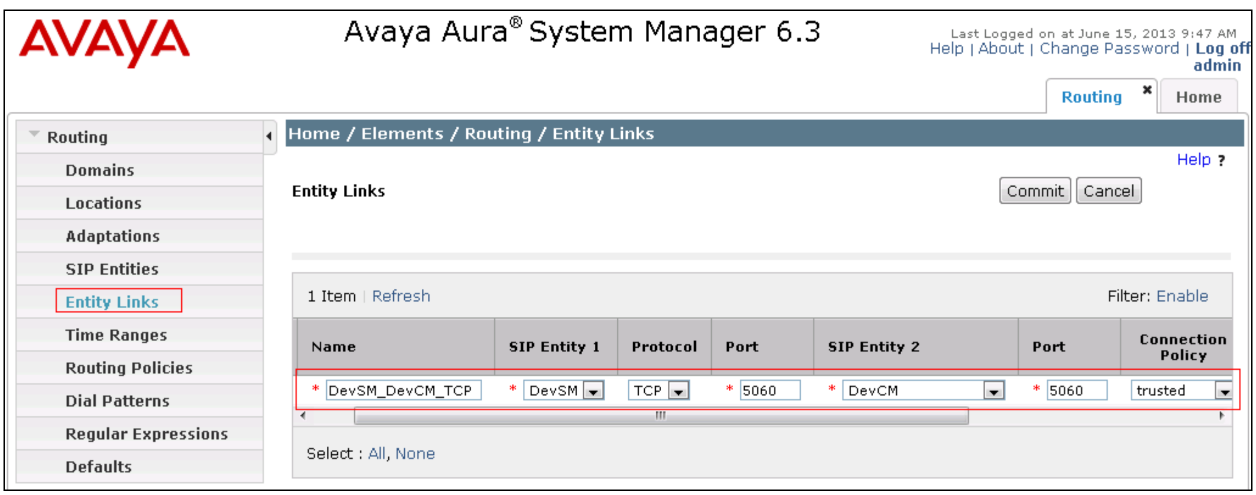
Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ⇔Communication Manager (Avaya S8800 Server).

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

- **Name**: Enter a descriptive name.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section** Error! Reference source not found. (e.g. **DevSM**).
- 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
  - 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** Error! Reference source not found., e.g. **DevCM**).
- 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 (not shown). The following screen shows an Entity Links page used during the compliance test.



6.5. Administer Routing Policy

Routing Policies associate destination SIP Entities (**Section** Error! Reference source not found.) with Time of Day admission control parameters (**Section** Error! Reference source not found.) and Dial Patterns (**Section** Error! Reference source not found.). 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:

<u>General section</u>

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

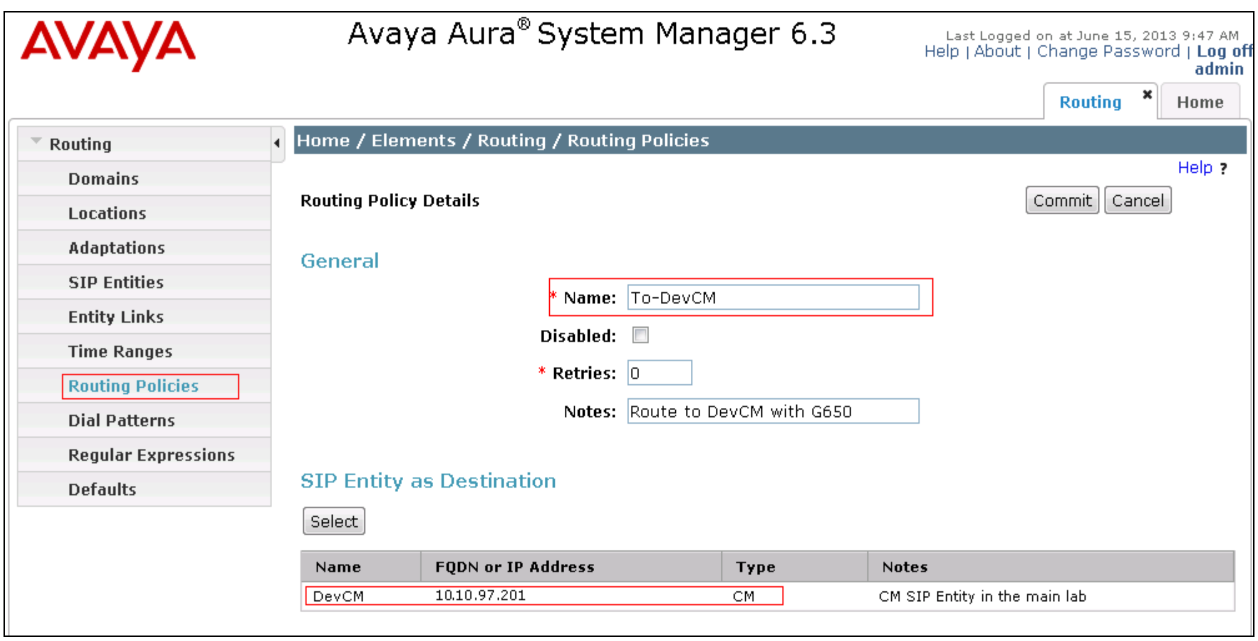
<u>SIP Entity as Destination section</u>

- 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.

<u>Time of Day section</u>

- Leave default values.

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



6.6. Administer Dial Pattern

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.

- 53 – SIP endpoints in Avaya S8800 Server.

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

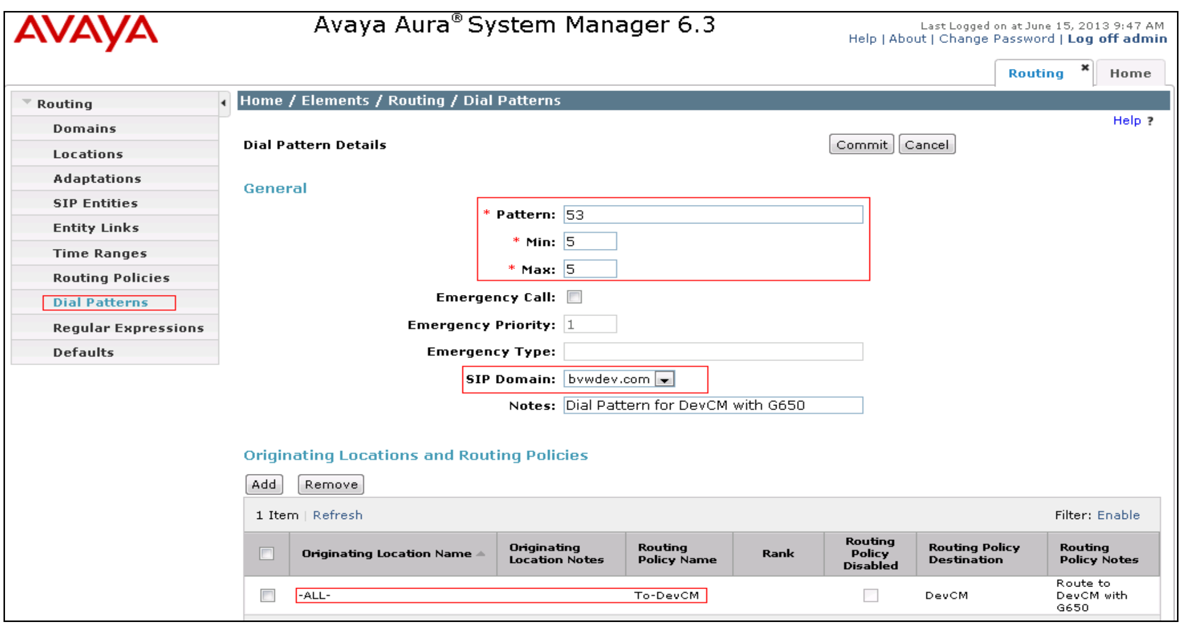
General section

- Enter a unique pattern in the **Pattern** field (e.g. **53**).
- 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** drop down menu select the domain that will be contained in the Request URI received by Session Manager from Communication Manager.

Originating Locations and Routing Policies section

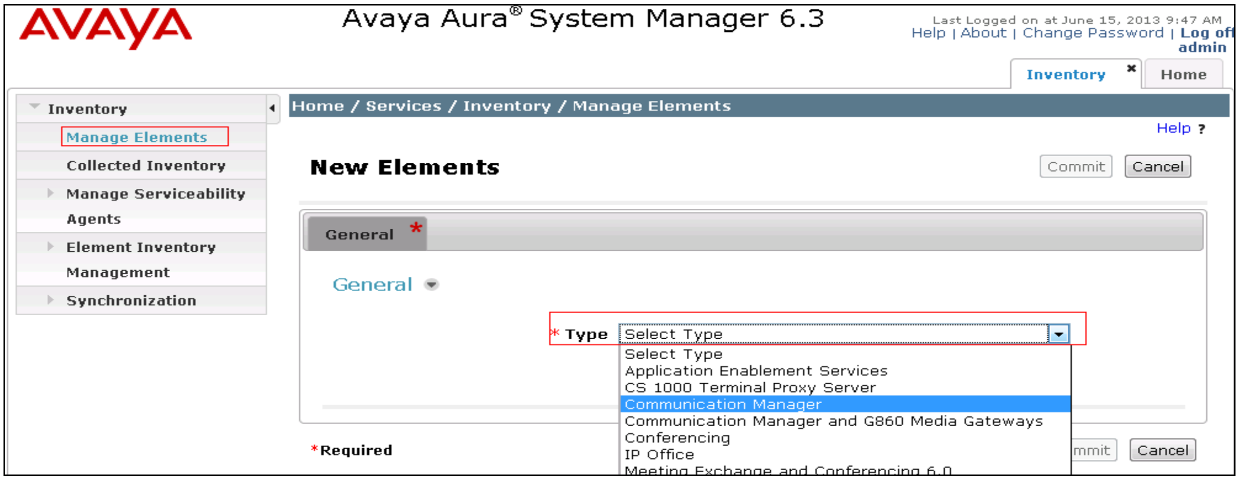
- Click on the **Add** button and a window will open (not shown).
- Click on the box for the appropriate Originating Locations, and Routing Policies (see **Section 6.5**) that pertain to this Dial Pattern.
  - Select the Originating Location to apply the selected routing policies to **All**.
  - Select Routing Policies to **To-DevCM**.
  - Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition (not shown). The following screen shows the dial pattern used for **53xxx** during the compliance test. Repeat steps for the remaining Dial Patterns.



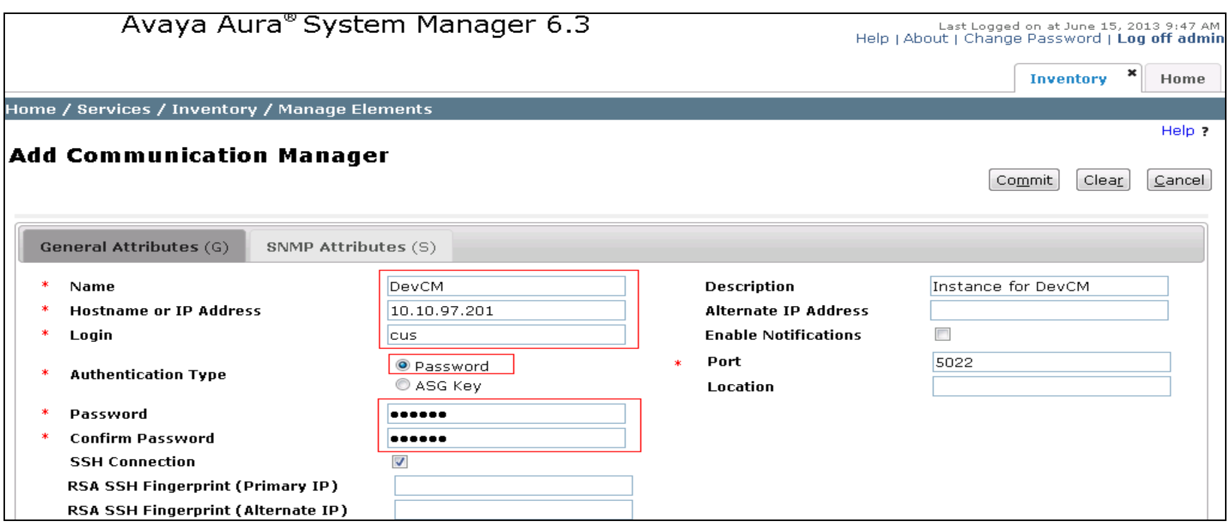
6.7. Administer Manage Element

To define a new Manage Element, navigate to **Elements→Inventory→Manage Elements**. Click on the **New** button (screen not shown) to open the **New Elements** page; in the **General** tab select **Communication Manager** in the **Type** dropdown menu.



The **Add Communication Manager** page is displayed. In the **General Attribute** tab:

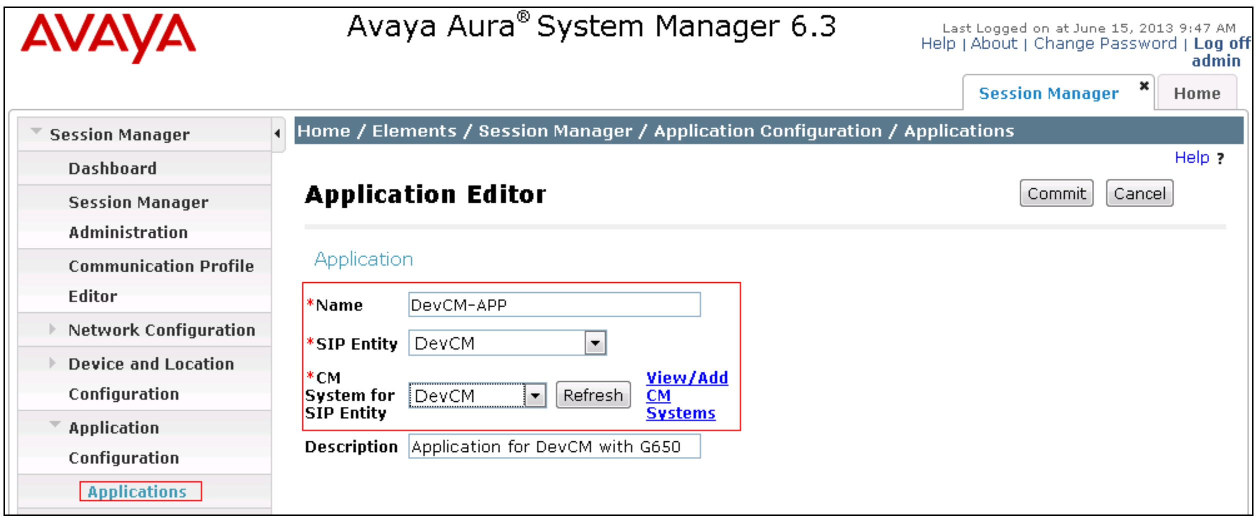
- **Name** - enter a descriptive name, e.g. **DevCM**.
- **Host name or IP Address** - enter IP address of CM **10.10.97.201**.
- **Login** - enter the user name "**cus**". Note that the user name "**cus**" was created in installing new Communication Manager, it can be any name.
- **Authentication Type** - select **Password**.
- **Password** - enter a password for username "**cus**".
- **Confirm Password** - enter the password again.
- Keep other field at default.
- Click **Commit** button to save the element.



6.8. Administer Applications

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

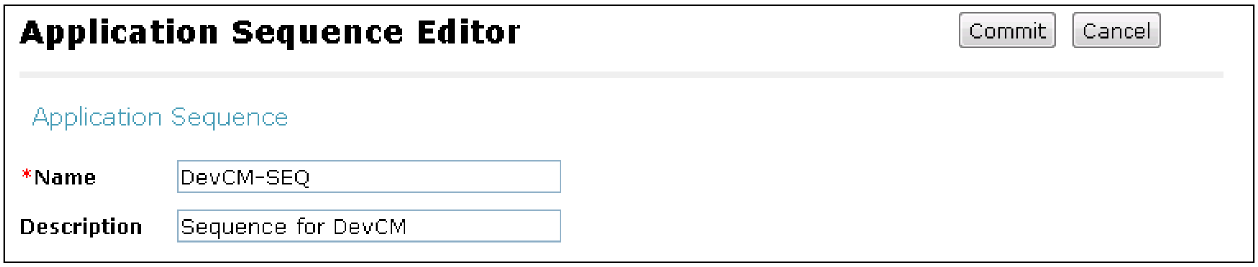
- Application Editor section
  - **Name –** Enter name for the application.
  - **SIP Entity**–Select the SIP Entity for Communication Manager defined in **Section** Error! Reference source not found..
  - **CM System for SIP Entity –**Select the name of the Managed Element defined for Communication Manager in **Section 6.7**.
  - **Description–** Enter description if desired.
- Leave the fields in the Application Attributes (optional) section blank.
- Click **Commit** button to save the Application.



6.9. Administer Application Sequence

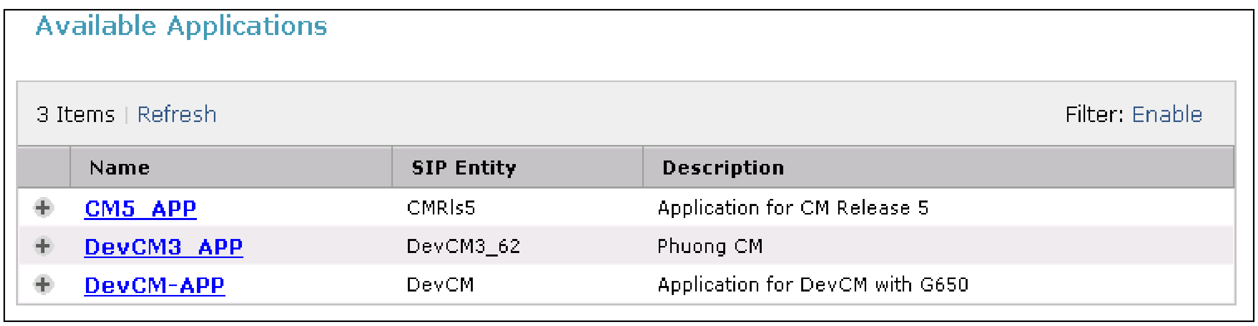
Navigate to **Elements → Session Manager → Application Configuration → Application Sequences**. Click **New** (screen not shown) and provide the following information:

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



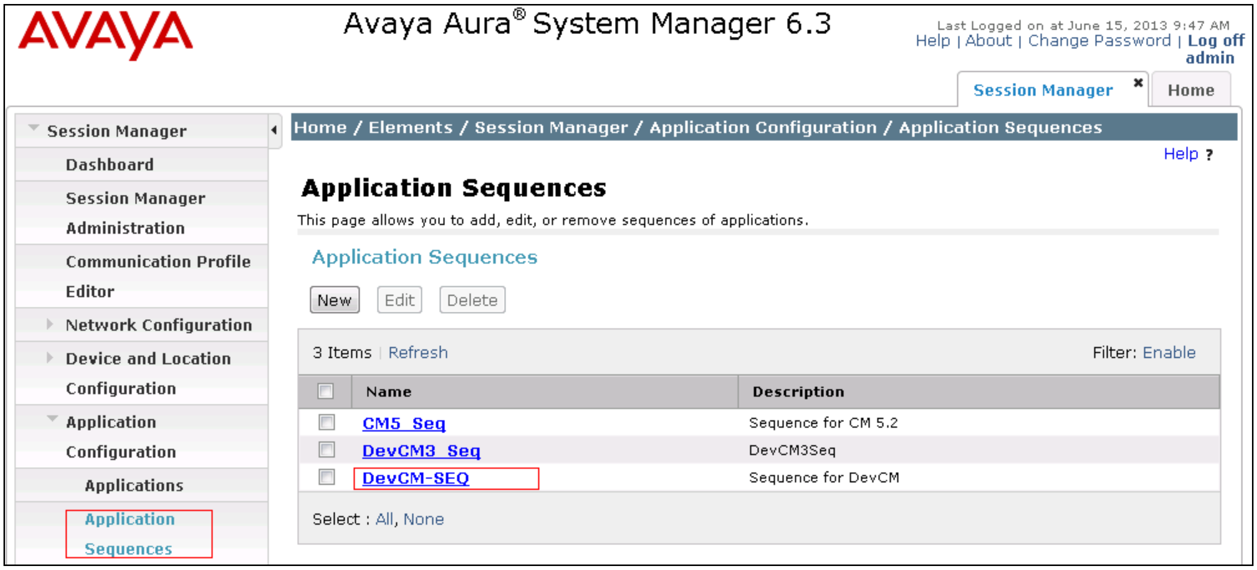
- Available Applications section
  - Click icon associated with the Application for Communication Manager defined in **Section** Error! Reference source not found. to select this application.
  - Verify a new entry is added to the Applications in this Sequence table as shown below.

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



	Name	SIP Entity	Description
+	CM5_APP	CMRls5	Application for CM Release 5
+	DevCM3_APP	DevCM3_62	Phuong CM
+	DevCM-APP	DevCM	Application for DevCM with G650

The screen below shows the Application Sequence, **DevCM-SEQ**, defined during the compliance test.

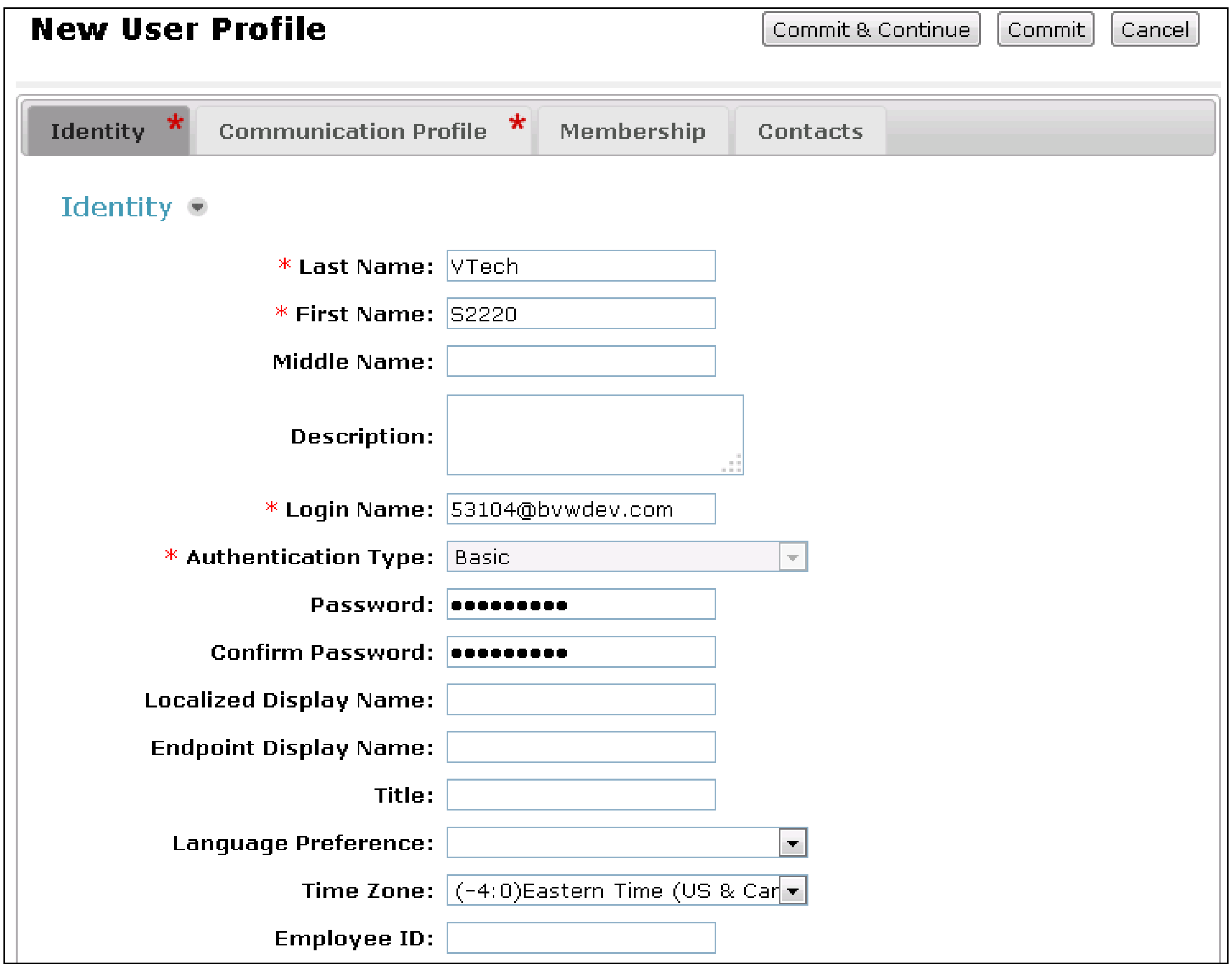


6.10. Administer SIP User

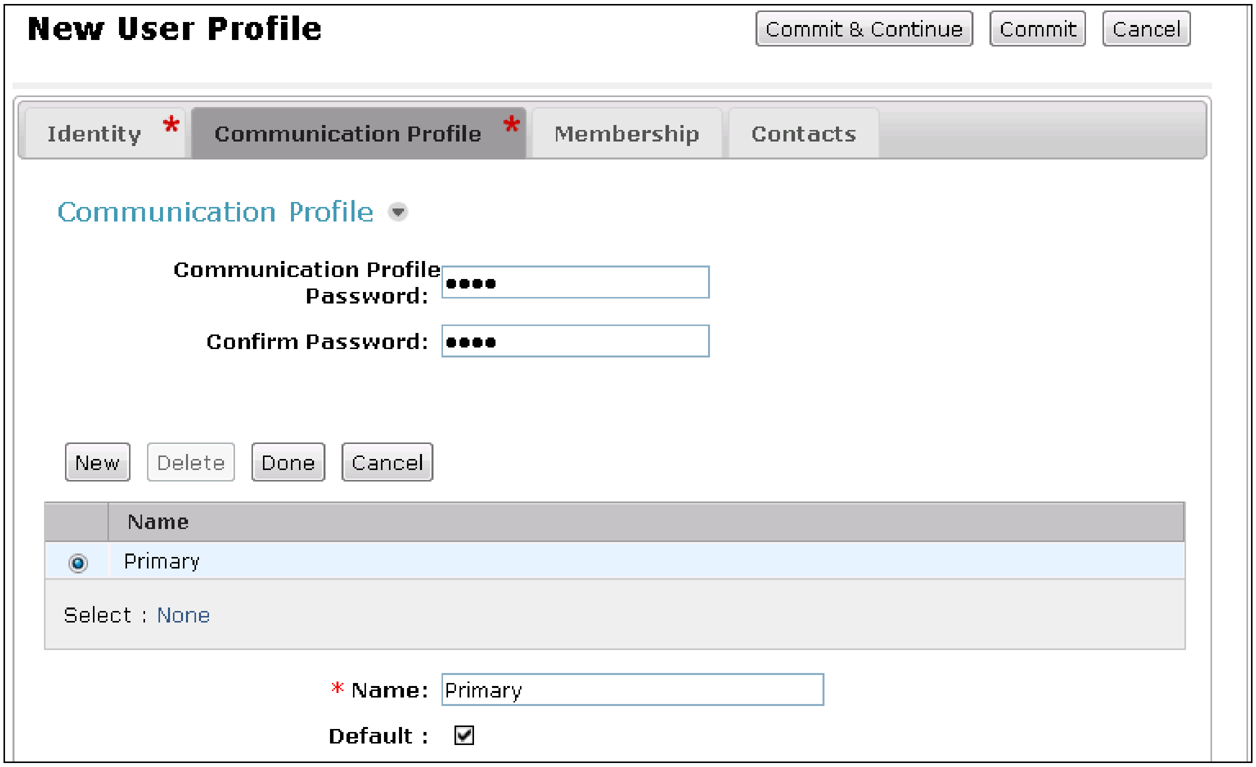
When adding new SIP user, use the option to automatically generate the SIP station in Communication Manager, after adding a new SIP user.

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

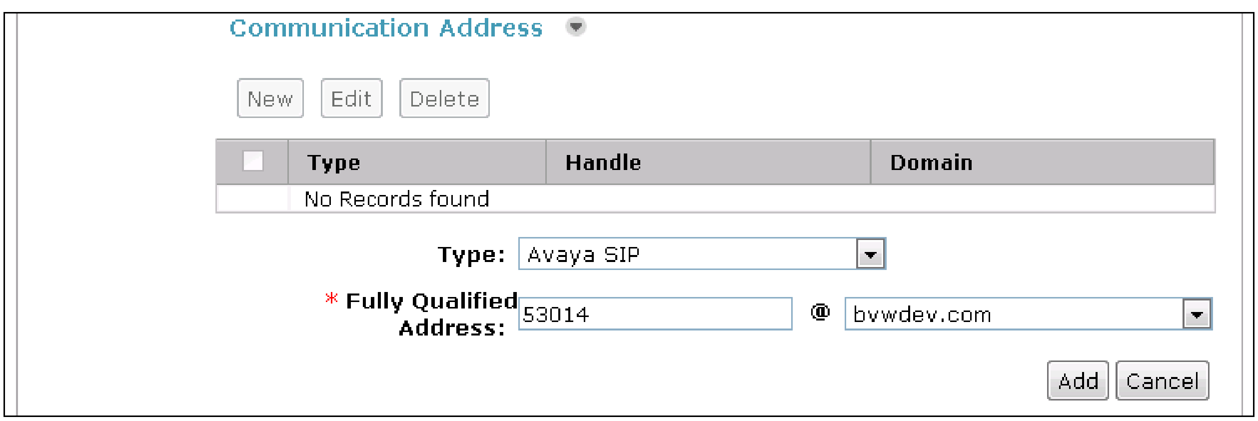
- <u>Identity section</u>
  - **Last Name –** Enter last name of user.
  - **First Name –** Enter first name of user.
  - **Login Name –** Enter extension number@sip domain. The sip domain is defined as Authoritative Domain in **Section 6.1**.
  - **Authentication Type –** Verify **Basic** is selected.
  - **Password –** Enter password to be used to log into System Manager.
  - **Confirm Password –** Repeat value entered above.



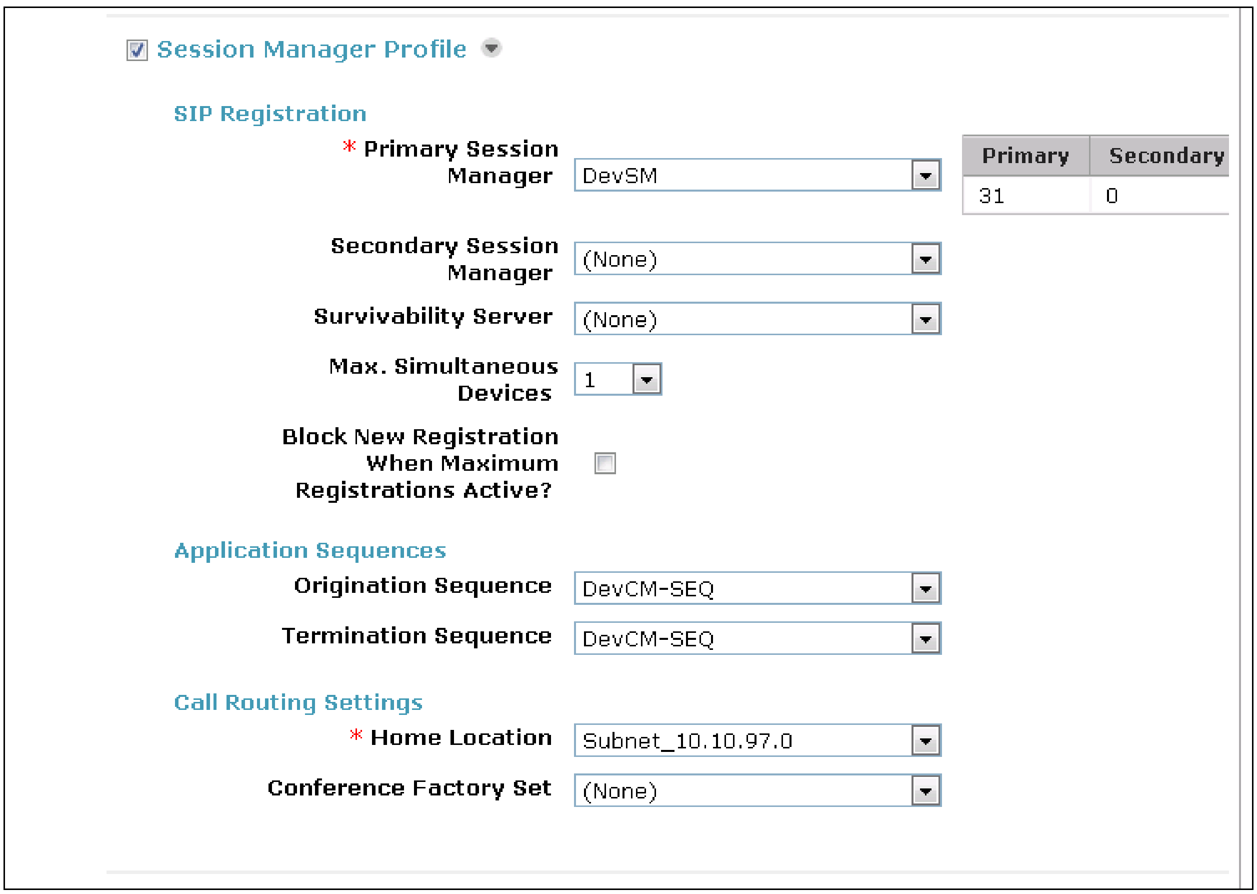
- <u>Communication Profile section</u>
  - **Communication Profile Password –** Type Communication profile password in this field.
  - **Confirm Password –** Repeat value entered above.



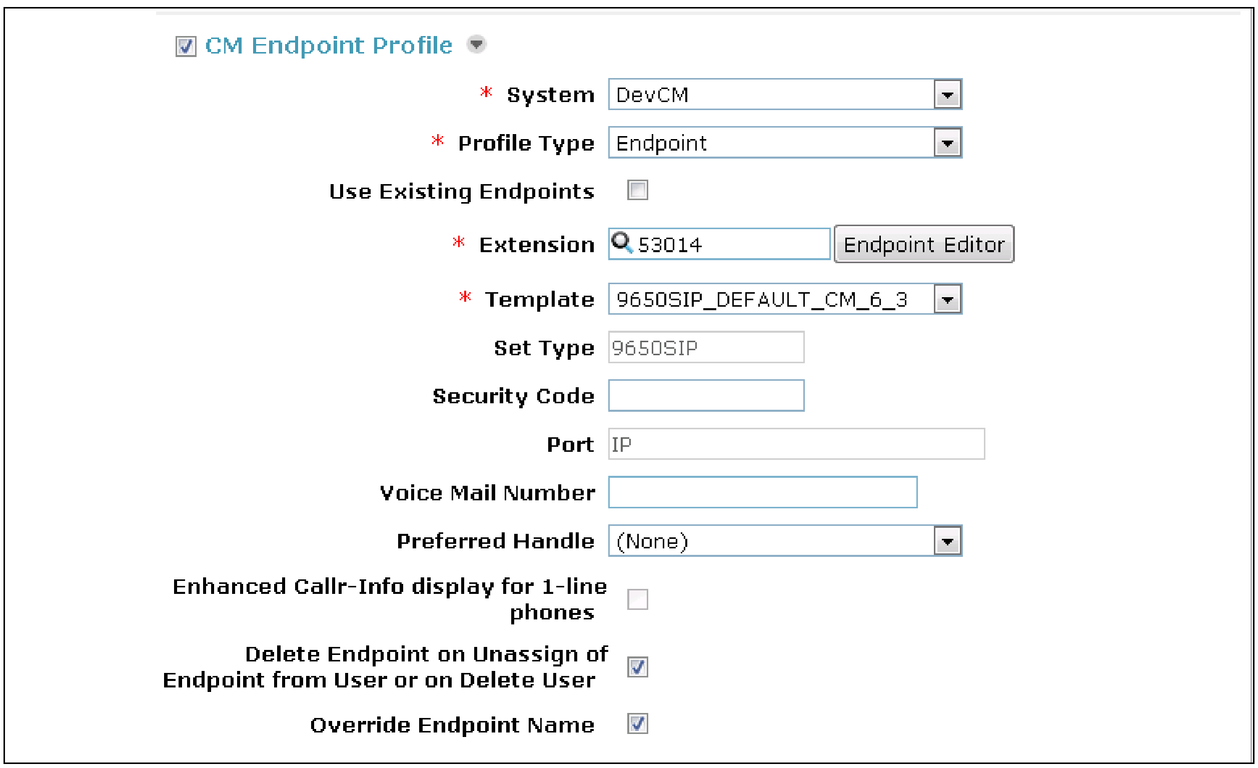
- <u>Communication Profile sub-section</u>
  - **Fully Qualified Address –** Enter the extension of the user.
  - Click **Add** button.



- 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 6.8** for Communication Manager.
  - **Termination Application Sequence** – Select Application Sequence defined in **Section 6.8** for Communication Manager.
  - **Survivability Server** – Select **(None)** from drop-down menu.
  - **Max**. Simultaneous – Select number of devices can use this SIP user. The Session Manager supports up to 10 devices to register to one SIP user and this feature is only available from Release 6.3.
  - **Home Location** – Select Location defined in **Section 6.2**.



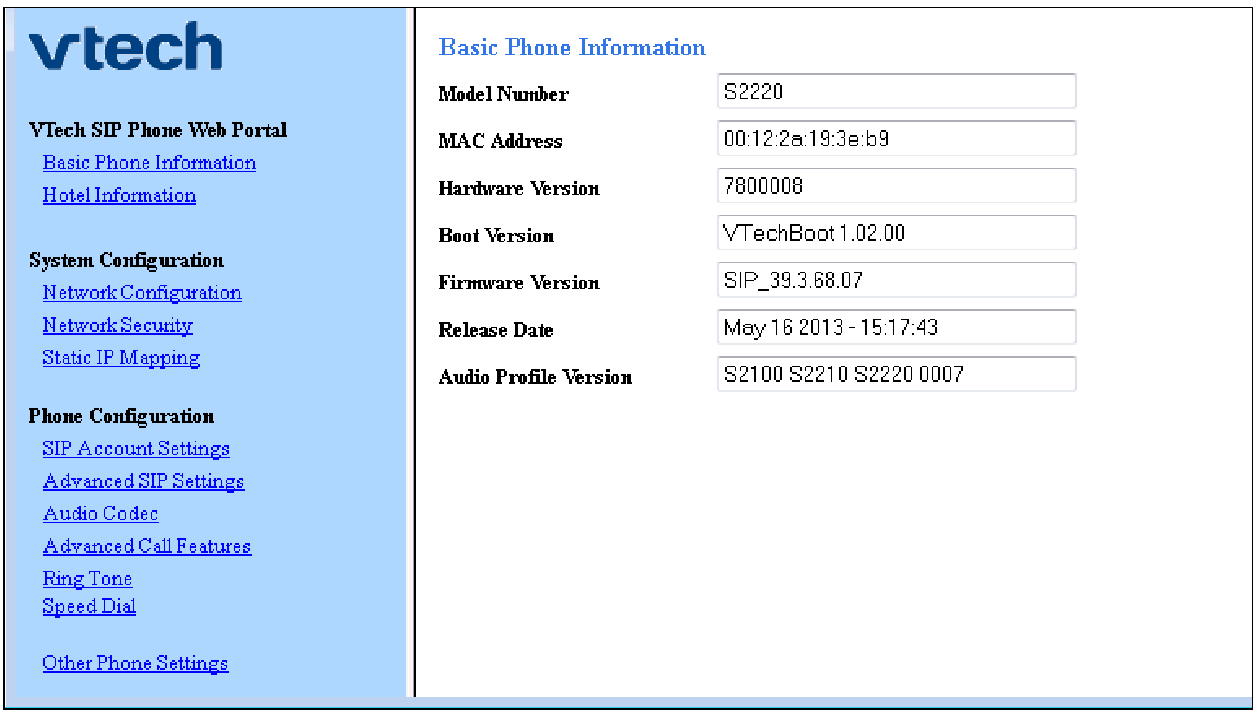
- <u>CM Endpoint Profile section</u>
    - **System** – Select Manage Element defined in **Section 6.7**.
    - **Profile Type** – Select **Endpoint**.
    - **Use Existing Endpoints -** Leave unchecked to automatically create new endpoint when new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
    - **Extension** - Enter same extension number used in this section.
    - **Template** – Select template for type of SIP phone.
    - **Security Code** – Leave it as default (blank).
    - **Port** – Select **IP** from drop down menu.
    - **Voice Mail Number –** Enter **Pilot Number** for Avaya Modular Messaging if installed. Or else, leave field blank. This feature is not used during the compliance test.
    - **Delete Station on Unassign of Endpoint** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.
    - **Override Endpoint Name** – Checked.



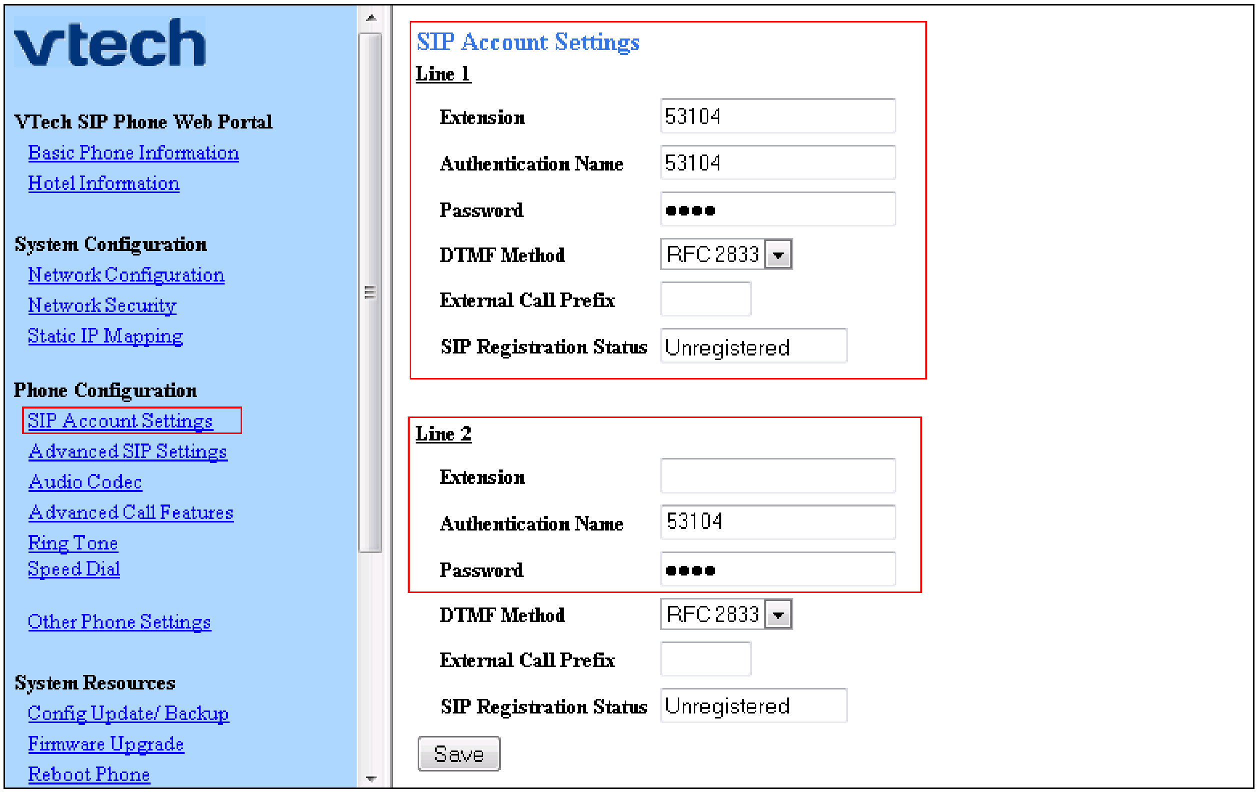
7. Configure VTech SIP Phone

VTech SIP Hotel Phones are configured using a web browser. The phones use DHCP by default and are powered over their Ethernet port. In the tested configuration, the phones were connected to the LAN via an Avaya BayStack 5510-PWR network switch on a segment with a DHCP server. Using the admin tools on the DHCP server provided a way to discover IP Addresses.

Enter the URL of the phone such as **http://<host or IP address>**. When prompted, login using ‘root’ for the user account, and the appropriate password (not shown). The initial screen is shown below and all navigation is via the navigation tree on the left panel. Some of the links lead to configuration settings that are not yet supported. See the VTech documentation for more details [4]. The home page of the VTech phone is displayed in the screen below.

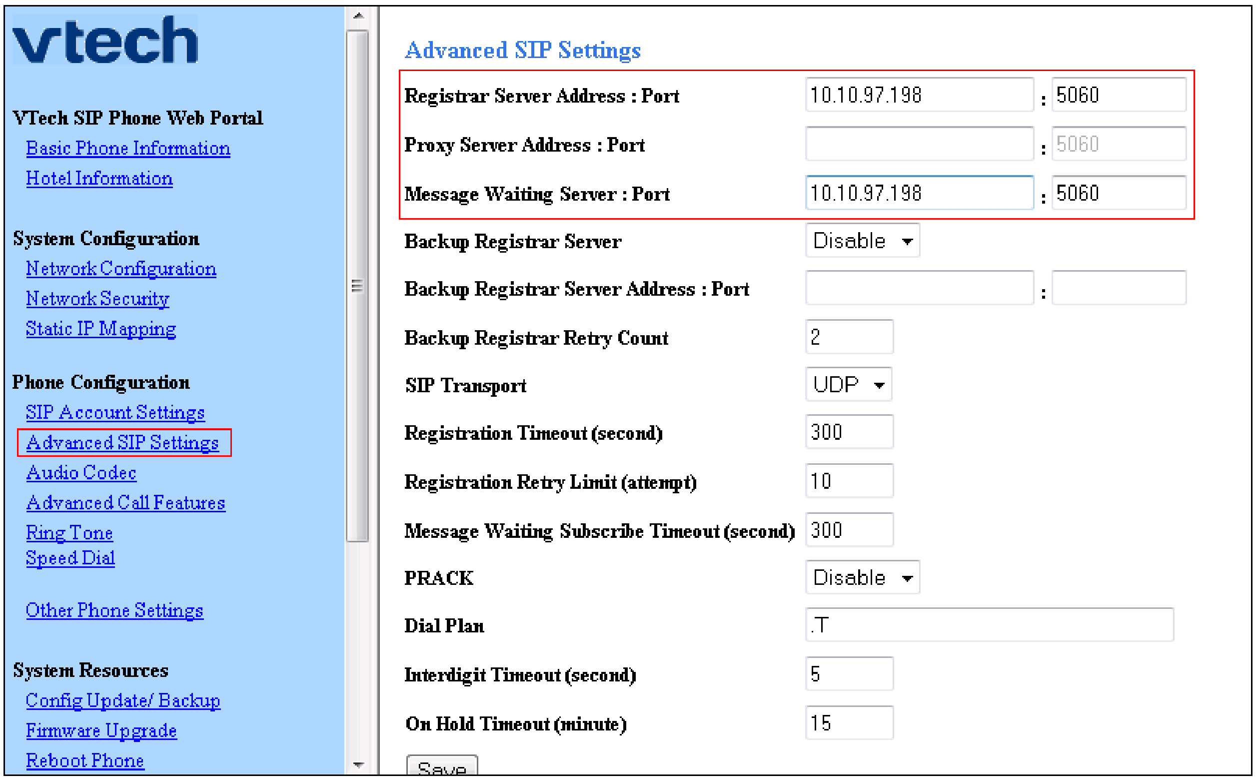


To register VTech SIP phone to Session Manager, click on the **SIP Account Settings** under the **Phone Configuration** category in the left navigation pane. The **SIP Account Settings** page is displayed in the right. Enter the username and its Communication Profile password as configured in **Section 6.10**. In the Line 2, enter the same Authentication Name and password as in the Line 1, this configuration is for call waiting and conference features to work on the VTech 2-Line SIP phone. Click the **Save** button to save the change.

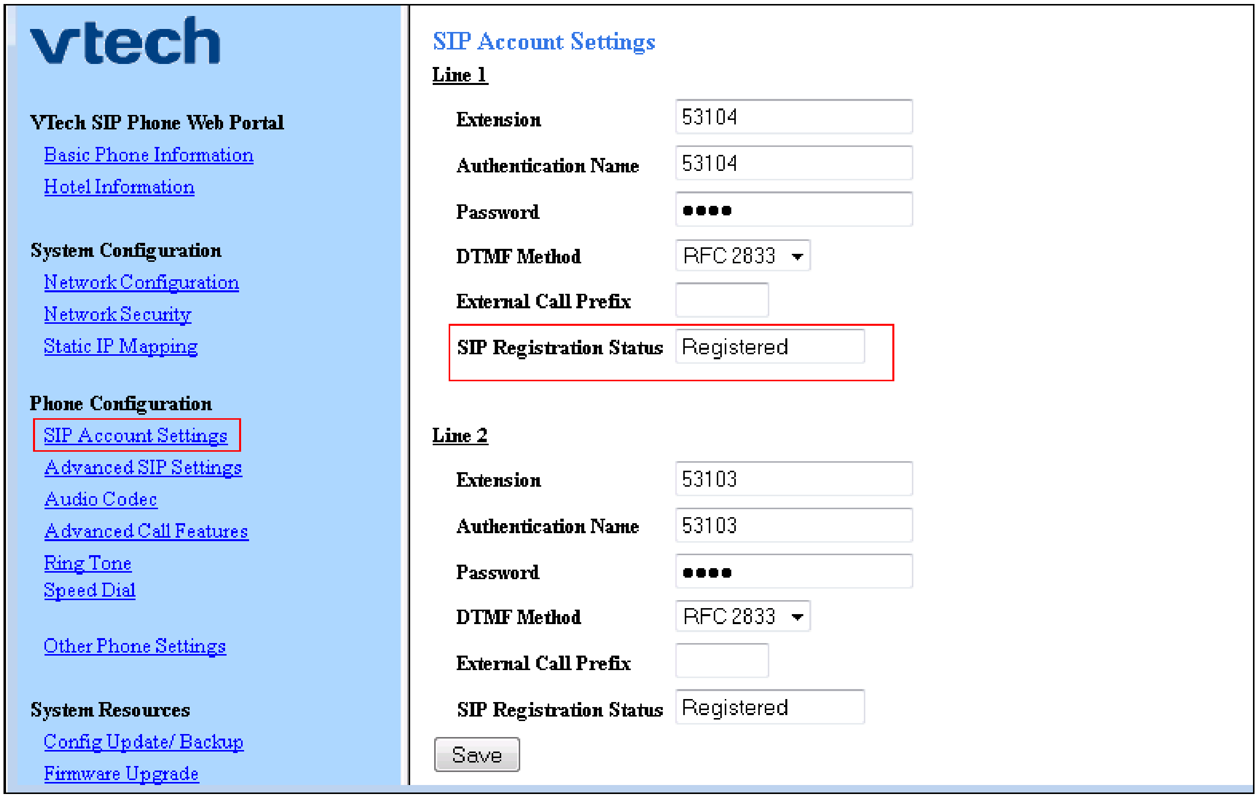


Click on **Advanced SIP Settings**, the **Advance SIP Settings** is displayed in the right. Enter the Session Manager IP **10.10.97.198** in the **Register Server Address** and **Messaging Waiting Server** fields with port **5060**. Note that in order Session Manager sends MWI message to VTech phone, the VTech phone must subscribe MWI feature to Session Manager therefore the Session Manager IP **10.10.97.198** must be inputted in the **Message Waiting Server** field. Keep other fields at default.

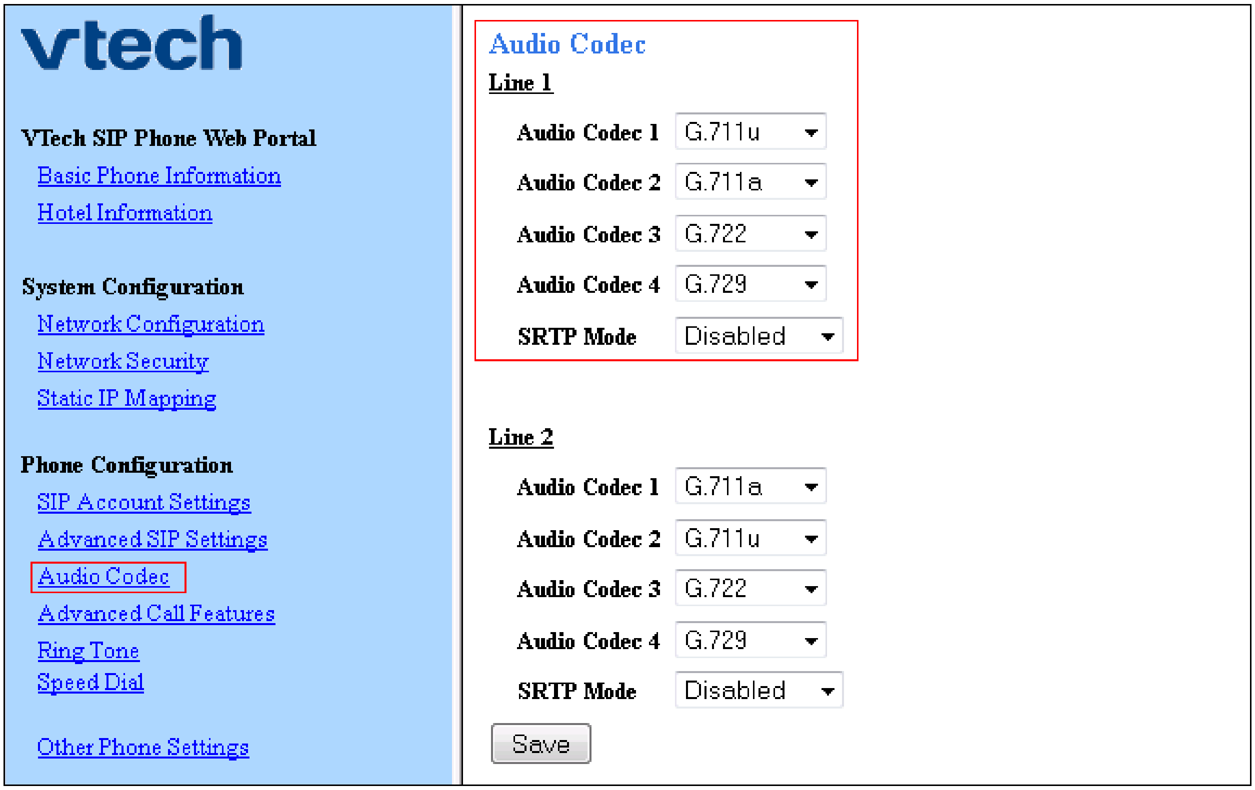
Click **Save** button to save the change. The VTech SIP phone needs a reboot for changes take effect. Reboot the phone by click on Reboot Phone link in the left navigation pane.



After the VTech phone rebooted, if the VTech phone is successfully registered to the Session Manager the SIP Registration Status will show as "Registered" as the screen below.



To configure audio codec, click on **Audio Codec** link in the left navigation pane. The **Audio Codec** page is displayed in the right. During the compliance test, the codec **G.711u** was configured as first priority for calls as shown in the screen below.



8. Verification Steps

Calls were placed to and from the VTech phones manually. Confirmation of functionality was generally observed by listening for audio on connected calls. Tracing was used on Avaya Aura® Session Manager, and using Wireshark on a locally connected PC to review SIP messages to and from the phones.

9. Conclusion

The VTech Hospitality SIP Phones successfully interoperated with the Avaya Aura ® Communication Manager and Avaya Aura® Session Manager as described in these Application Notes. There were some observations noted in **Section 2.2**.

10. Additional References

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

[1] *Implementing Avaya Aura® Session Manager*, Issue 2, Release 6.3, May 2013.
[2] *Administering Avaya Aura® Communication Manager,* Issue 8, Release 6.3, May 2013.
[3] *Administering Avaya Aura® System Manager,* Release 6.3, Issue 2, May 2013.

Product information for VTech SIP Hotel Phones may be found at http://vtechhotelphones.com.

[4] *VTech SIP Phone System Integration Guide,* Document ID 91-004252-010-100, Version 5

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.