Avaya Solution & Interoperability Test Lab

Application Notes for PIVOT™ by Spectralink (87-Series) Wireless SIP Telephones and Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 0.1

Abstract

These Application Notes describe the procedures for configuring PIVOT™ by Spectralink (87-Series) Wireless SIP Telephones which were compliance tested with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

The overall objective of the interoperability compliance testing is to verify Pivot Telephones functionalities in an environment comprised of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, various Avaya 9600 Series IP Deskphones.

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 Pivot Telephones which were compliance tested with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Pivot Telephones registers to Session Manager via UDP.

Pivot (87-Series) expands the Spectralink 8000 Portfolio of Voice over Wi-Fi handsets to deliver enterprise-grade, on-site voice mobility with a user-friendly interface presented on an extensible application platform.

Based on the industry standard Android™ operating system, it is a WorkSmart solution - differentiated by its intuitive touchscreen design, HD voice quality, seamless Voice over Wi-Fi roaming without dropouts, durability, broad telephony and WLAN interoperability, and predictable return on investment.

PIVOT further enhances the customer value proposition with two enhanced standards-based application interfaces, an optional, high-performance integrated barcode scanner and an industrial-grade accelerometer. In partnership with the Spectralink applications development ecosystem, PIVOT enables new opportunities for end-user productivity solutions.

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 references [1], [2], [3], and [4].

2. General Test Approach and Test Results

The general test approach was to place calls to and from Pivot and exercise basic telephone operations. The main objectives were to verify the following:

- Registration
- Codecs (G.711MU and G.729A)
- Inbound calls
- Outbound calls
- Hold/Resume
- Call termination (origination/destination)
- Three party conference (origination/destination)
- Avaya Feature Name Extension (FNE)
    - Call Park
    - Call Pickup
    - Call Forward (Unconditional, Busy/no answer)
- MWI
- Voicemail
- Serviceability

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 Pivot. Pivot operations such as inbound calls, outbound calls, hold/resume, transfer, conference, Feature Name Extension (FNE), and Pivot 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 Pivot can recover from failures.

2.2. Test Results

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

2.3. Support

Technical support on Pivot can be obtained through the following:

North America
Phone: +1-800-775-5330
Email: nolarma@spectralink.com
Web: http://support.spectralink.com

EMEA
Phone: +33-176774541
Email: emeaom@spectralink.com
Web: http://support.spectralink.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of an Avaya S8300D Server, an Avaya G450 Media Gateway, a Session Manager server, and Pivot. 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, an Avaya 4600 Series H.323 IP Telephone, 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 Pivot and Avaya SIP, H.323, and digital telephones.

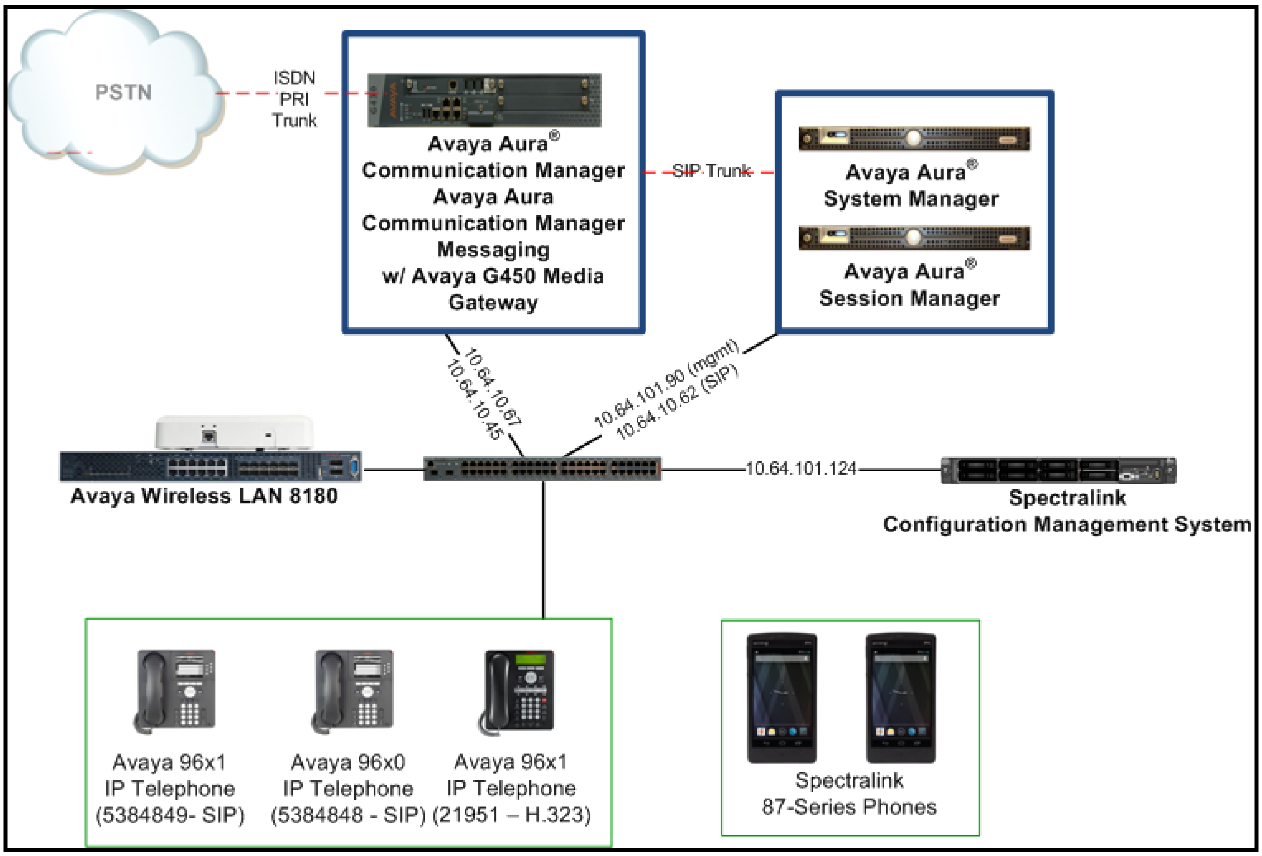


Figure 1: Test Configuration of Pivot

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya Aura® Communication Manager Avaya Aura® Communication Manager Messaging	R016x.03.0.124.0
Avaya Aura® System Manager	6.3.5.0
Avaya Aura® Session Manager	6.3.5
Avaya G650 Media Gateway	30.21.1
Avaya 9600 Series Deskphones	
96x1 (SIP) 96x1 (SIP) 96x0 (SIP)	2.6.4 2.6.4 2.6.4
Avaya 4600 and 9600 Series H.323 Telephones	
Pivot Phones	JZO54K 1.0.0.4037
Spectralink Configuration Management System	1.0.2

5. Configure the 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. Pivot 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.

```
change 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  401
                                      Maximum Stations: 2400  63
                              Maximum XMOBILE Stations: 2400  0
                    Maximum Off-PBX Telephones - EC500: 9600  0
                    Maximum Off-PBX Telephones -   OPS: 9600  11
                    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.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000  147
           Maximum Concurrently Registered IP Stations: 2400  4
             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  1
                       Maximum Administered SIP Trunks: 4000  148
  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. For the compliance testing, G.711MU, G.729A 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: G.729             n         2        20
 3:
 4:
 5:
 6:
 7:
```

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** – Enter the appropriate name for the 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: 1       Authoritative Domain: avaya.com
    Name: Default                 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? y
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 44
        Audio PHB Value: 44
        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 along with its IP address.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
8730TR1             10.64.10.74
AAEP                10.64.101.26
SM_10_62            10.64.10.62
AuraSBC-Inside      10.64.10.112
AuraSM              10.64.21.31
AvayaIQ             10.64.50.15
CM                  10.64.10.67
CMS                 10.64.10.85
CM_101_12           10.64.101.12
CRYSTAL_SM          10.64.60.19
CTLog               10.64.10.56
Chung               10.64.41.21
FAXPN1              10.64.22.16
FaxServer           10.64.10.170
GFI                 10.64.101.81
Gateway001          10.64.10.1
( 16 of 31   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

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.**
- **Near-end Node Name** - Set to **procr**.
- **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 **avaya.com**. This should match the SIP Domain value in **Section 6.1**.
- **Direct IP-IP Audio Connections** – Set to **y**, since Media Shuffling is enabled during the compliance test

```
add signaling-group 10                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP 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: SM_10_62
 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): 6
```

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.

```
change trunk-group 10                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 10                   Group Type: sip          CDR Reports: y
  Group Name: to_SM_10_62                 COR: 1        TN: 1        TAC: *010
   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: 10
                                                     Number of Members: 10
```

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.

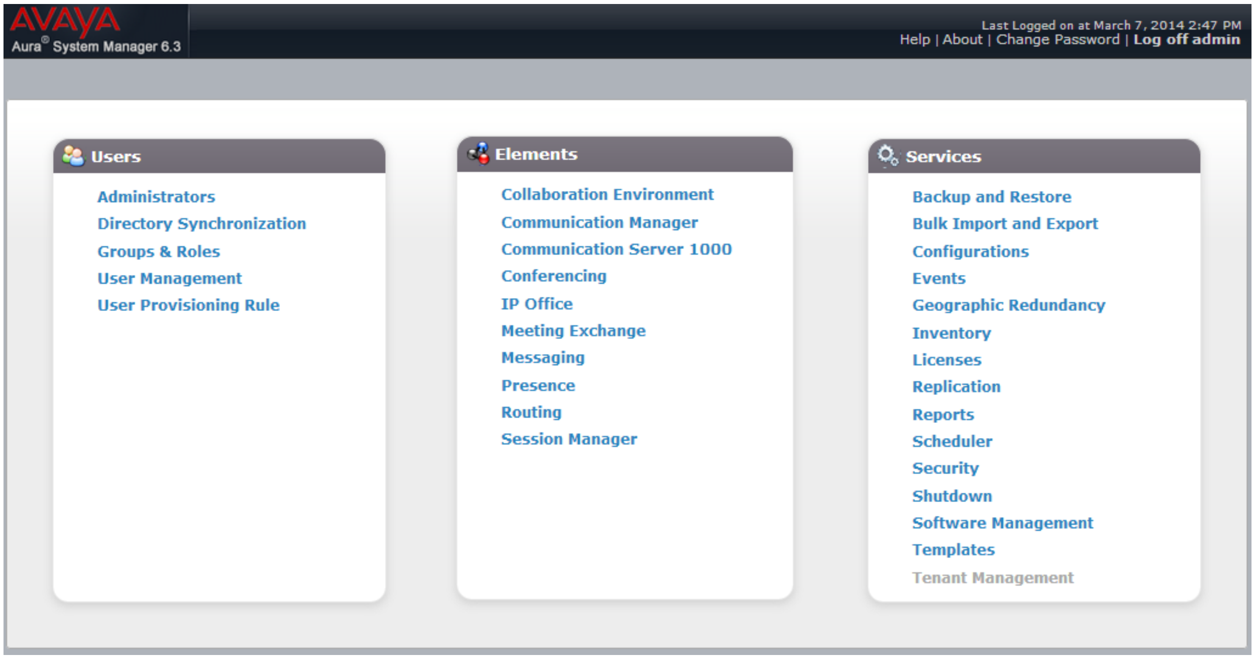
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

In this section, the following topics are discussed:

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- User Management

6.1. Configure SIP Domain

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

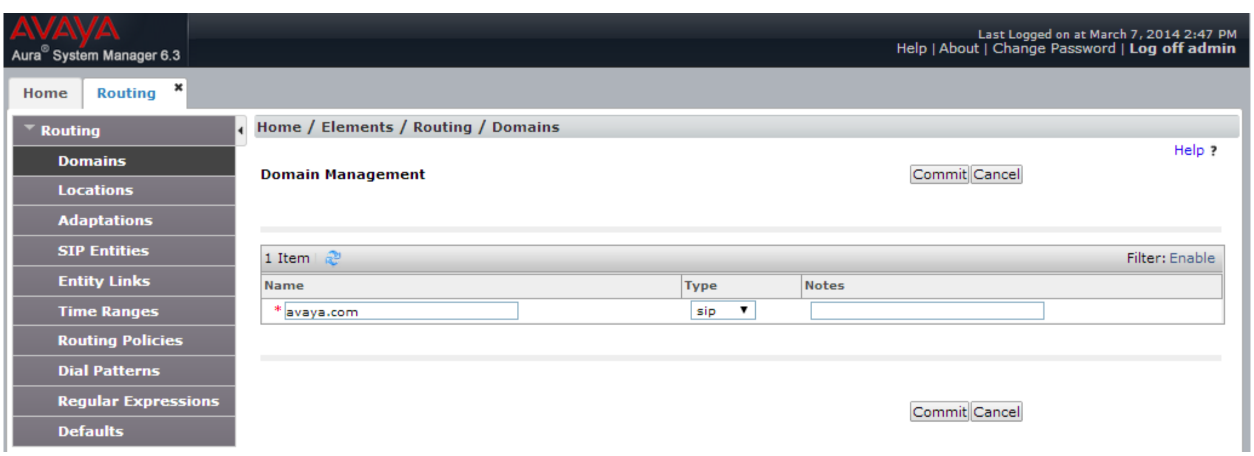


In the main menu, navigate to **Elements → Routing → Domains**, and click on the **New** button (not shown) to create a new SIP Domain. Enter the following values and use default values for remaining fields:

- **Name** – Enter the Authoritative Domain Name specified in **Section 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.

From the main menu, navigate to **Elements → Routing → Locations**, and click on the **New** button (not shown) to create a new SIP endpoint location.

General section

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

- Enter a descriptive Location name in the **Name** field (e.g. **Test Room 1**).
- Enter a description in the **Notes** field if desired.

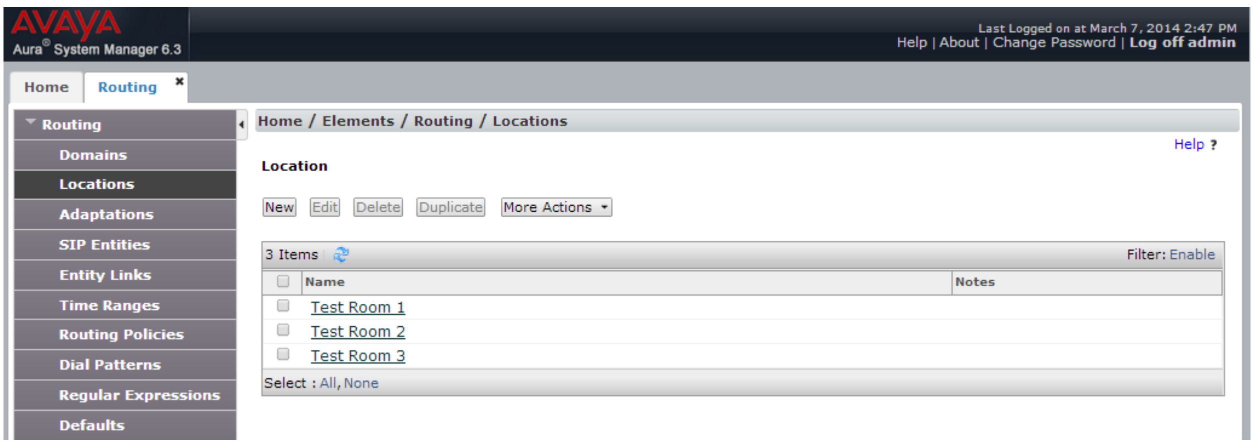
Location Pattern section

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

- Enter the IP address information for the **IP address Pattern** field (e.g. **10.64.10.***).
- 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.

The following screen shows the Locations list 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. This entity was created prior to the compliance test.
- Communication Manager. This entity was created prior to the compliance test.

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

General section

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

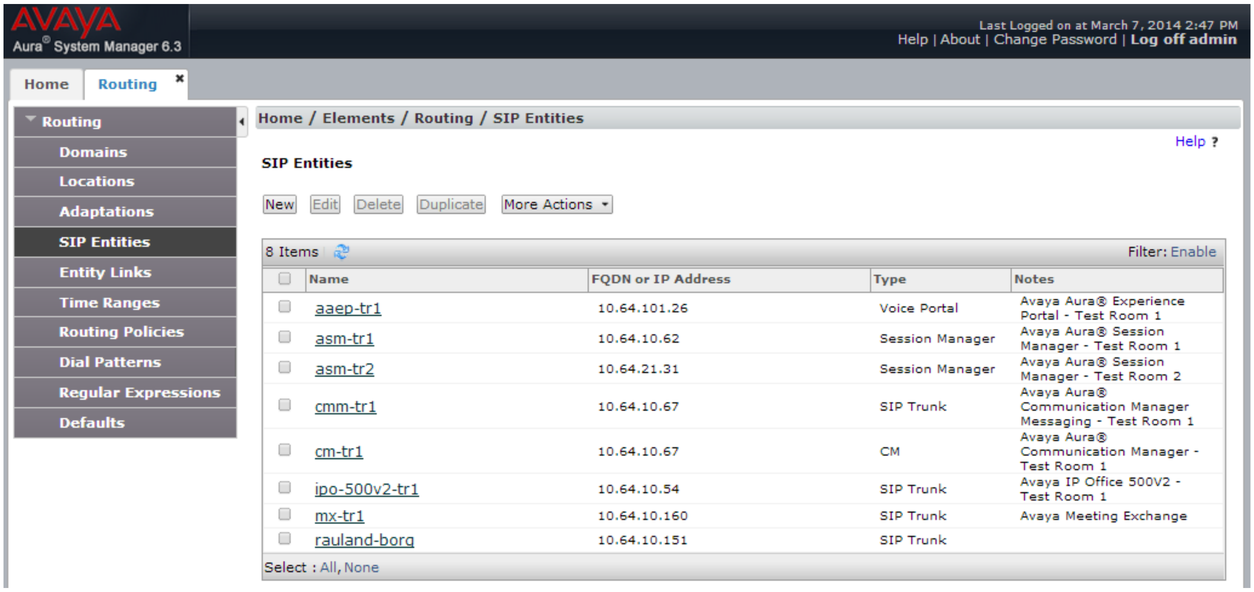
- Enter a descriptive Entity name in the **Name** field.
- Enter IP address for signaling interface on each Communication Manager, Session Manager, or 3rd party device in the **FQDN or IP Address** field
- From the **Type** drop down menu select a type that best matches the SIP Entity.
    - For Communication 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.

SIP Link Monitoring section

- 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). This entity link was created prior to the compliance test.

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 shown in **Section 6.3** (e.g. **SM_10_62**).
- 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 Communication Manager SIP entity
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- Enter a description in the **Notes** field if desired.
- Accept the other default values.

Click on the **Commit** button to save each Entity Link definition.

Repeat the steps to define Entity Link using a different protocol.

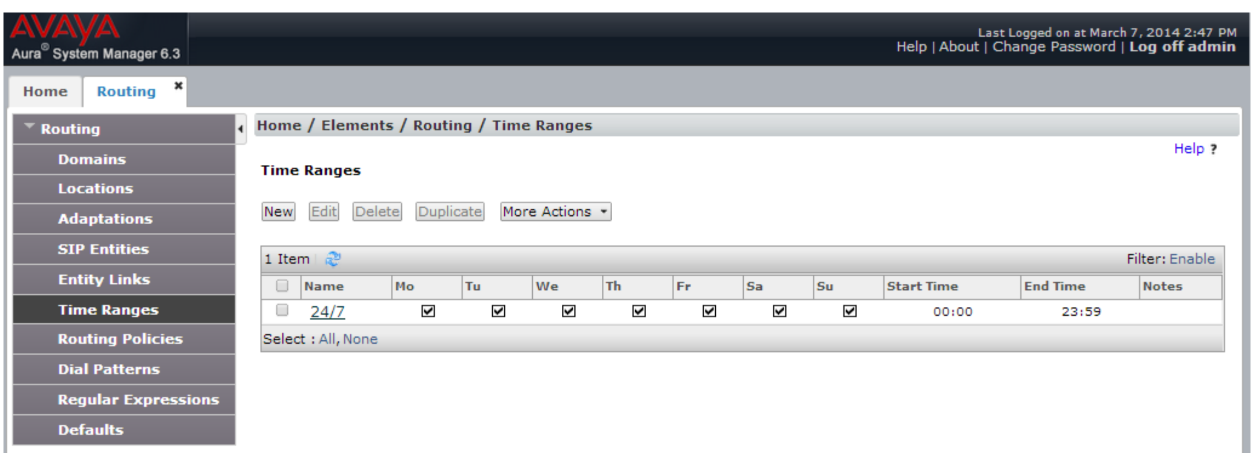
6.5. Time Ranges

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 Time Range 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:

- Calls to/from 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

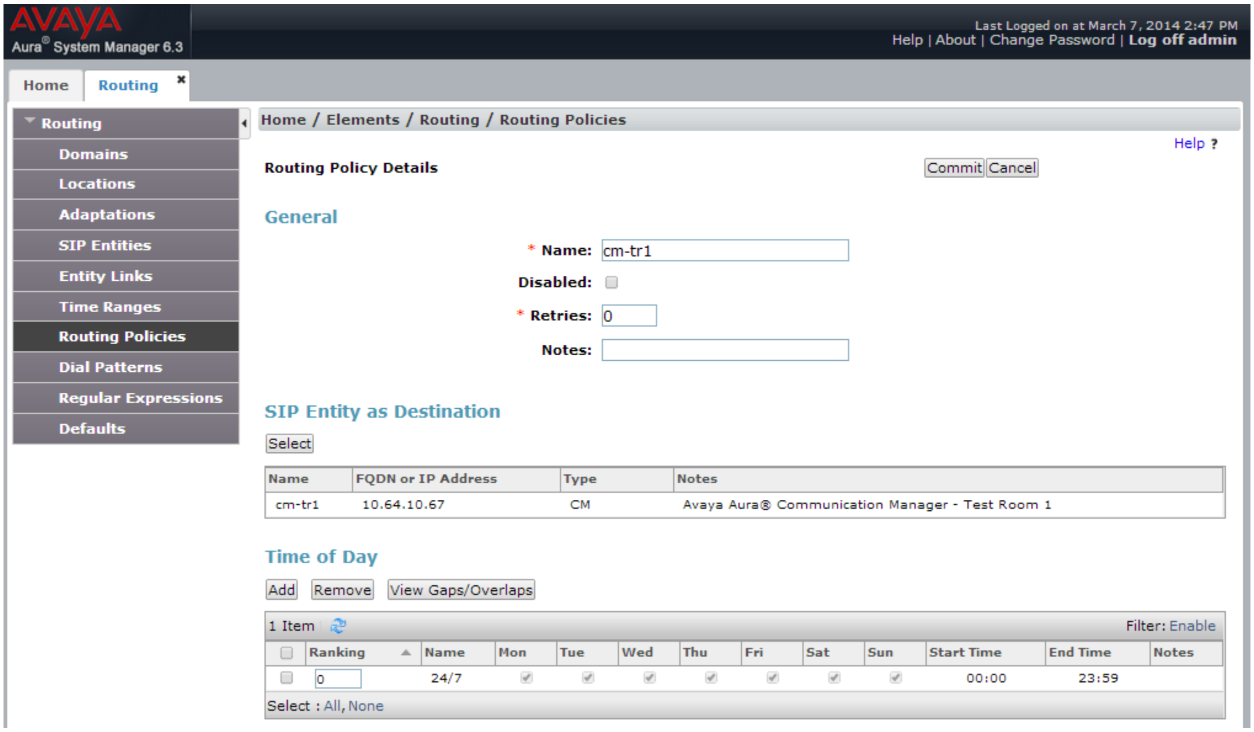
- Enter a descriptive name in the **Name** field.
- Enter a description in the **Notes** field if desired.

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 the entity, **cm-tr1**, during the compliance test.



6.7. 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. In the compliance test, the following dial patterns are defined from Session Manager.

- 2555x and 2500x – SIP and H323 endpoints in Avaya S8300D Server

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

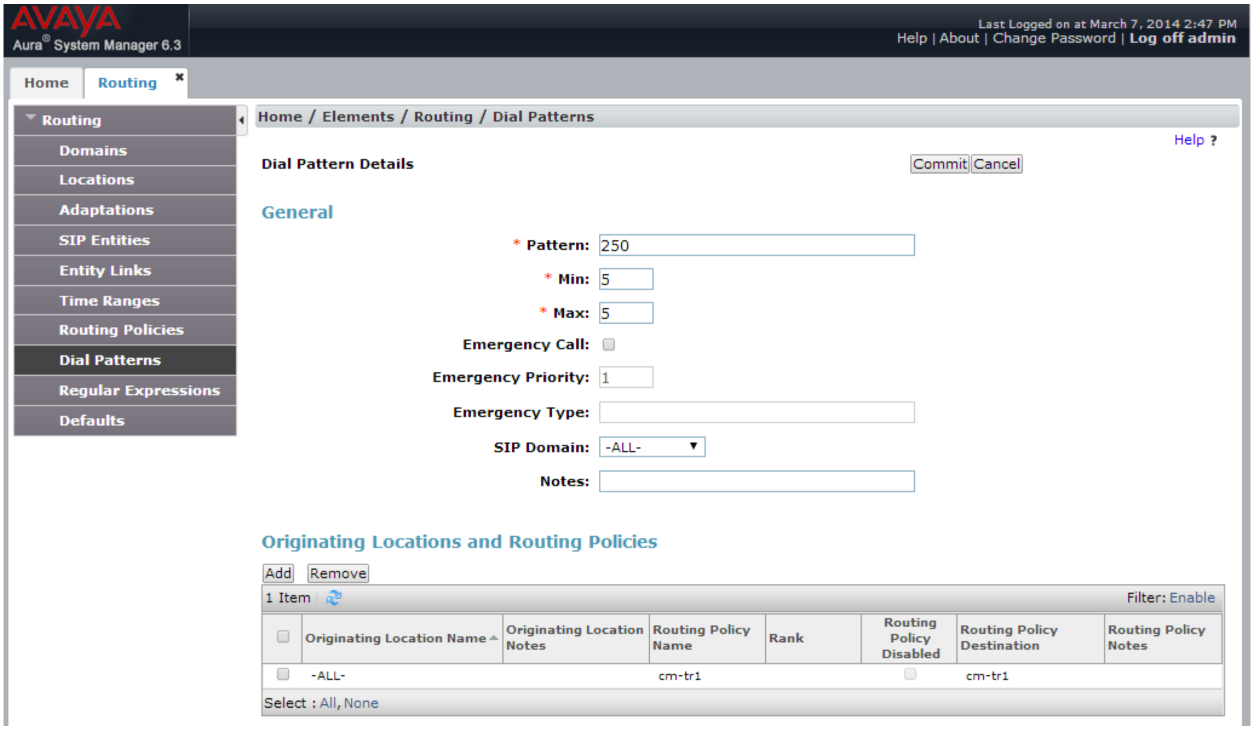
General section

- Enter a unique pattern in the **Pattern** field (e.g. **250**).
- 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 6.6**) that pertain to this Dial Pattern.
  - Originating Location –Check the **Apply The Selected Routing Policies to All Originating Locations** box.
  - Routing Policies **cm-tr1**.
  - 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 the S8300D during the compliance test.


AVAYA
Aura® System Manager 6.3
Last Logged on at March 7, 2014 2:47 PM
Help | About | Change Password | Log off admin
Home
Routing
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home / Elements / Routing / Dial Patterns
Help ?
Dial Pattern Details
Commit
Cancel
General
* Pattern: 250
* Min: 5
* Max: 5
Emergency Call:
Emergency Priority: 1
Emergency Type:
SIP Domain: -ALL-
Notes:
Originating Locations and Routing Policies
Add
Remove
1 Item
Filter: Enable
Originating Location Name
Originating Location Notes
Routing Policy Name
Rank
Routing Policy Disabled
Routing Policy Destination
Routing Policy Notes
-ALL-
cm-tr1
cm-tr1
Select : All, None

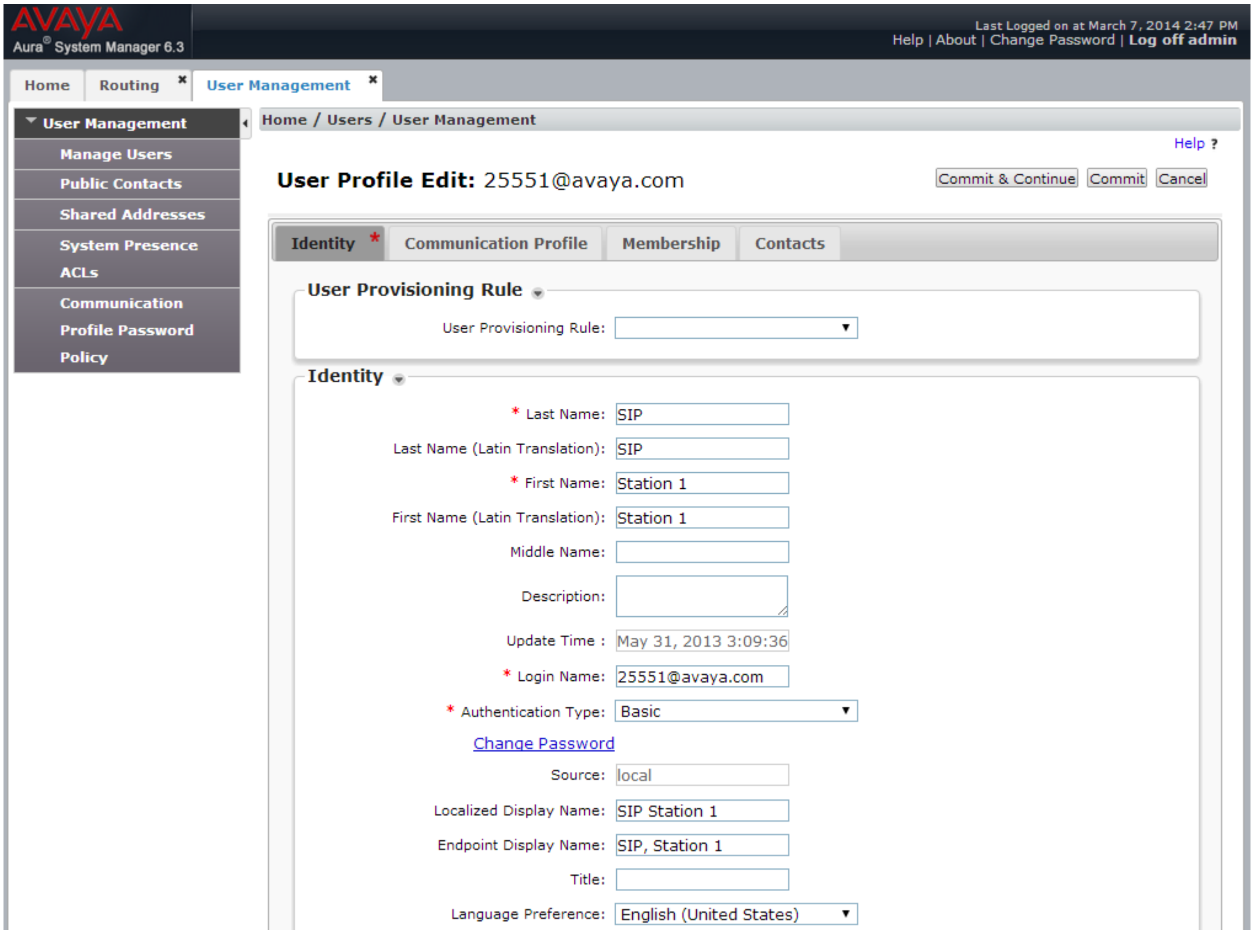
6.8. Configure SIP Users

During the compliance test, no special users were created for this solution. All users were created prior to the compliance test. However, the steps to configure a user are included.
Add new SIP users for each Spectralink 87-Series phone.

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

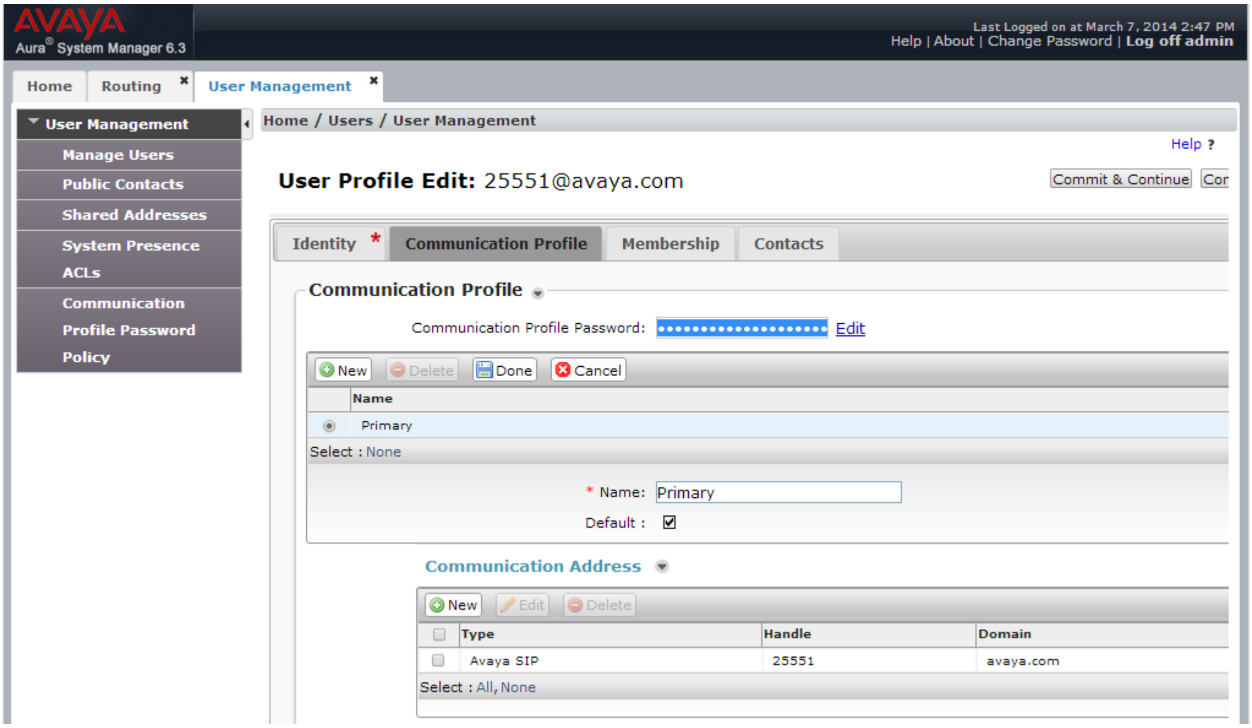
- Identity section
  - **Last Name –** Enter last name of user.
  - **First Name –** Enter first name of user.

  - **Login Name –** Enter extension number@sip domain name. The domain name is 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.
  - Enter **Localized Display Name**
  - Enter **Endpoint Display Name**
  - Select **English** as **Language Preference**
  - Set the appropriate **Time Zone.**



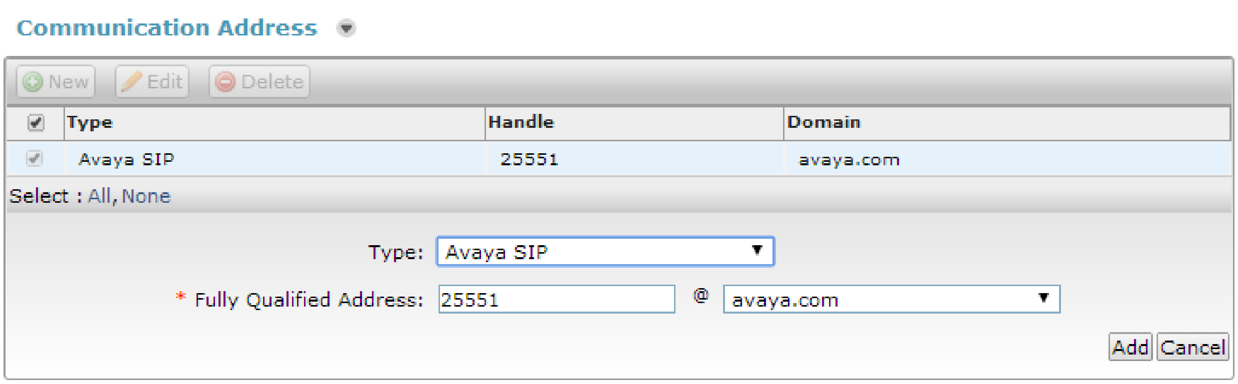
- <u>Communication Profile section</u>
  Provide the following information:
  - **Communication Profile Password** – Enter a numeric value used to logon to SIP telephone.
  - **Confirm Password** – Repeat numeric password

  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 ☑



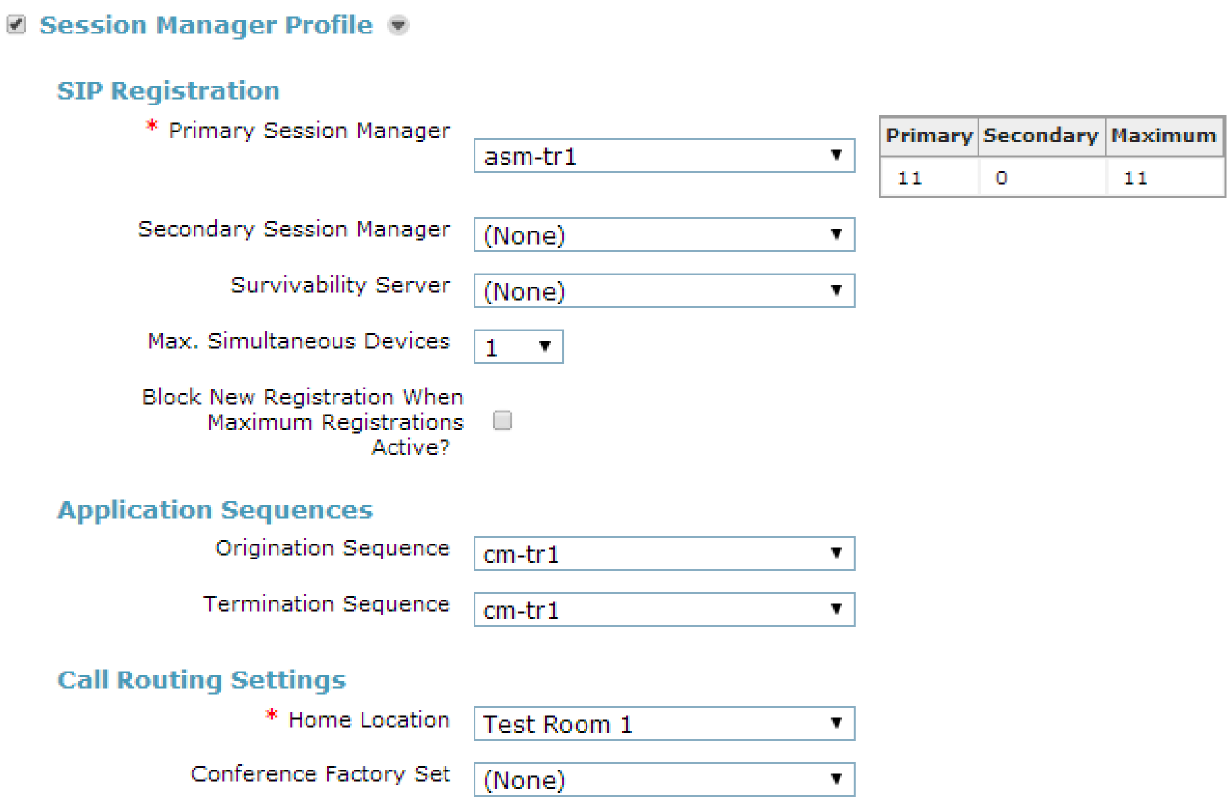
- Communication Address sub-section
  Select **New** to define a **Communication Address** for the new SIP user, and provide the following information.
    - **Type** – Select **Avaya SIP** using drop-down menu.
    - **Fully Qualified Address** – Enter same extension number and domain used for Login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

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

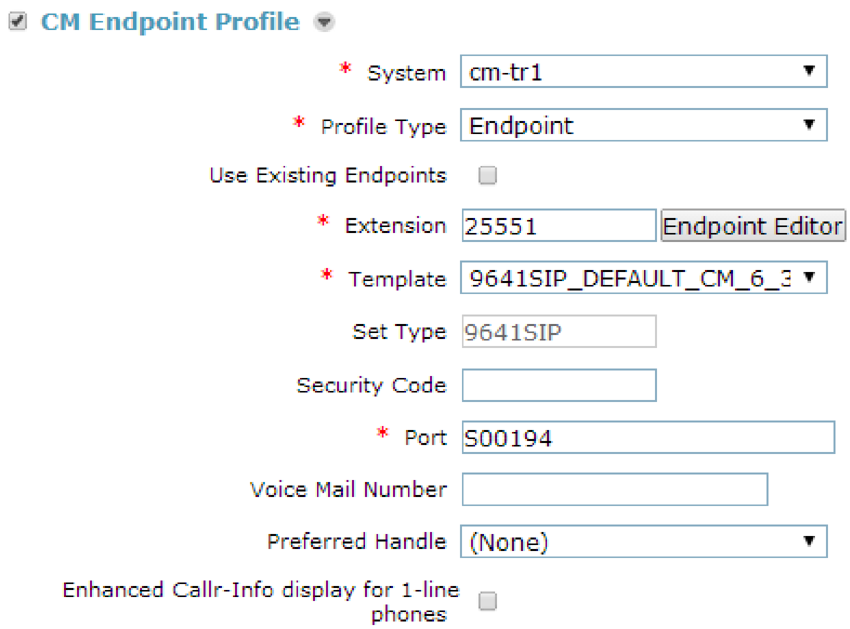


- Session Manager Profile section
    - **Primary Session Manager** – Select one of the Session Managers.
    - **Secondary Session Manager** – Select **(None)** from drop-down menu.
    - **Origination Application Sequence –** Select Application Sequence defined (not shown) for Communication Manager.

- **Termination Application Sequence** – Select Application Sequence defined (not shown) for Communication Manager.
- **Survivability Server** – Select **(None)** from drop-down menu.
- **Home Location** – Select Location defined in **Section 6.2**.



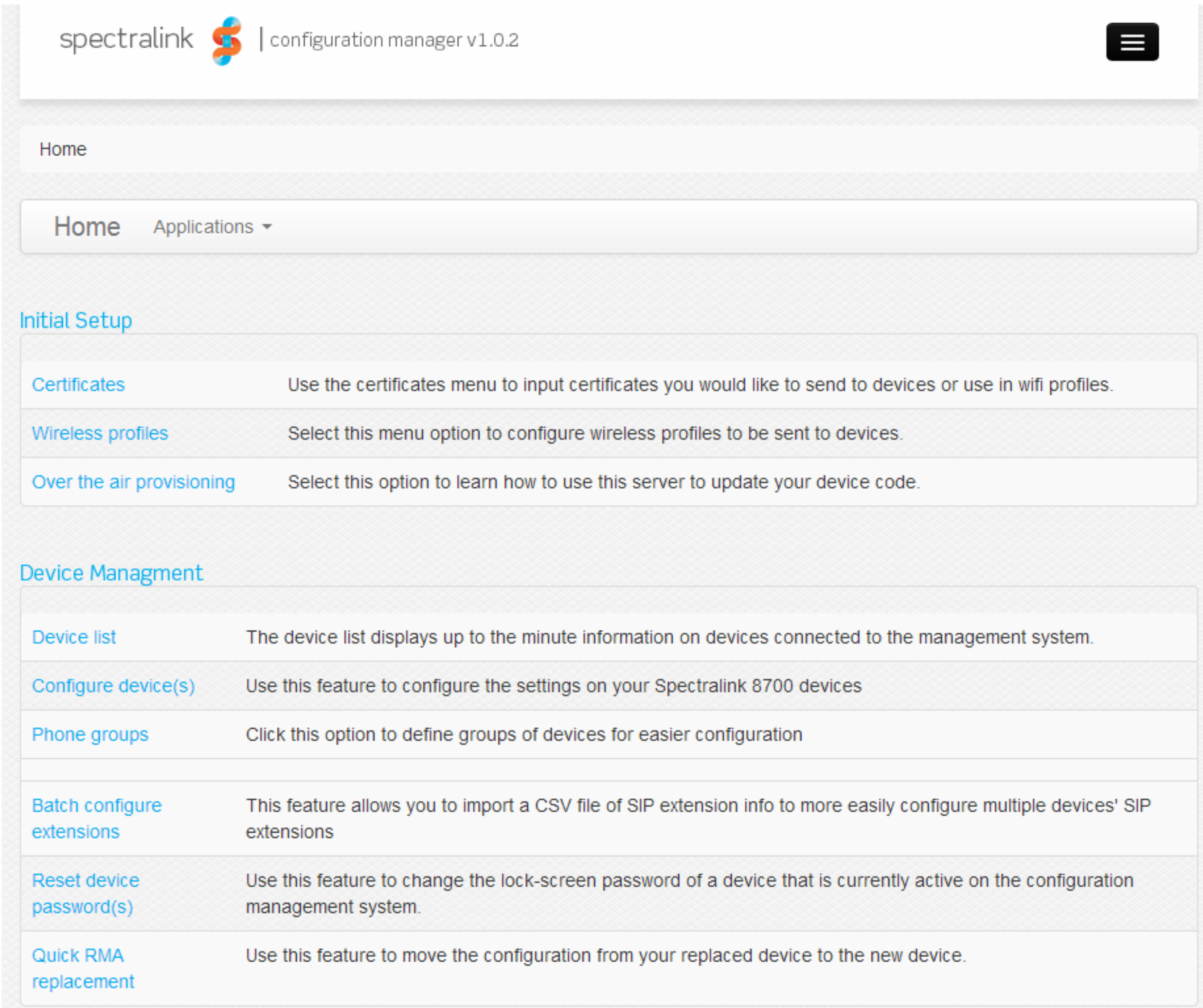
- Endpoint Profile section
  - **System** – Select Managed Element defined in **System Manager** (not shown) for Communication Manager.
  - **Use Existing Endpoints -** Leave unchecked to automatically create a new endpoint on Communication Manager when the new user is created. Or else, check the box 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. During the compliance test, DEFAULT_9630SIP_CM_6_0 was selected.
  - **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. 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.


CM Endpoint Profile
* System
cm-tr1
* Profile Type
Endpoint
Use Existing Endpoints
* Extension
25551
Endpoint Editor
* Template
9641SIP_DEFAULT_CM_6_3
Set Type
9641SIP
Security Code
* Port
S00194
Voice Mail Number
Preferred Handle
(None)
Enhanced Callr-Info display for 1-line phones

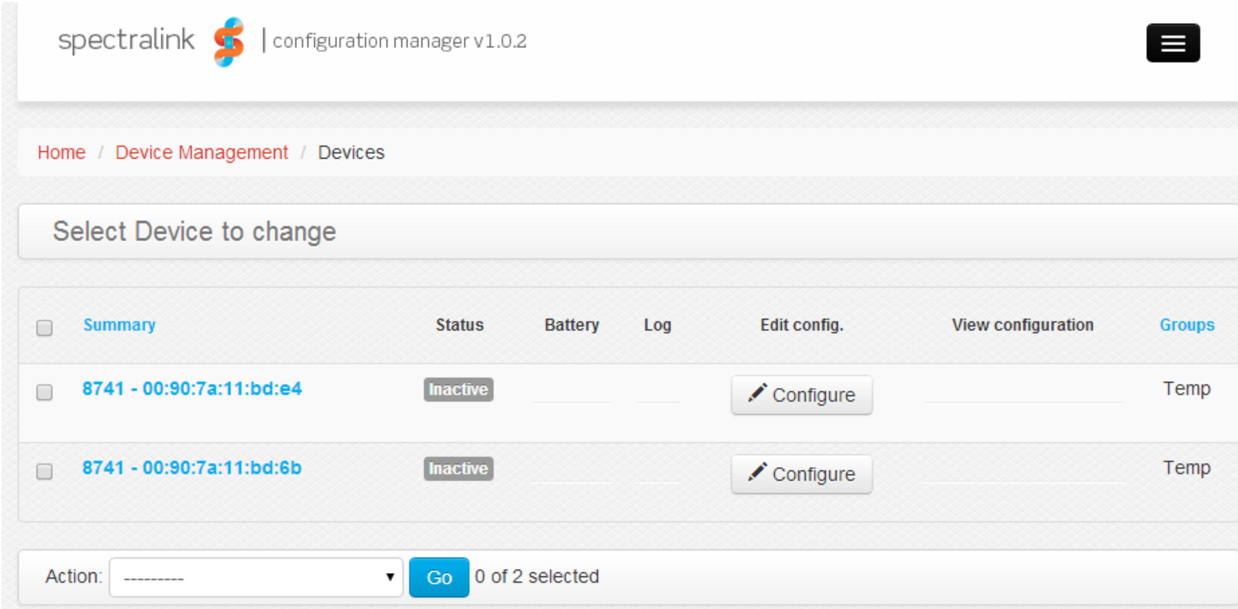
7. Configure Pivot

Configuration for Pivot phones is done via Spectralink Configuration Management system (CMS). CMS can be reached via browser, http://<CMS-IP-Address>

Provide the login credentials and log in.

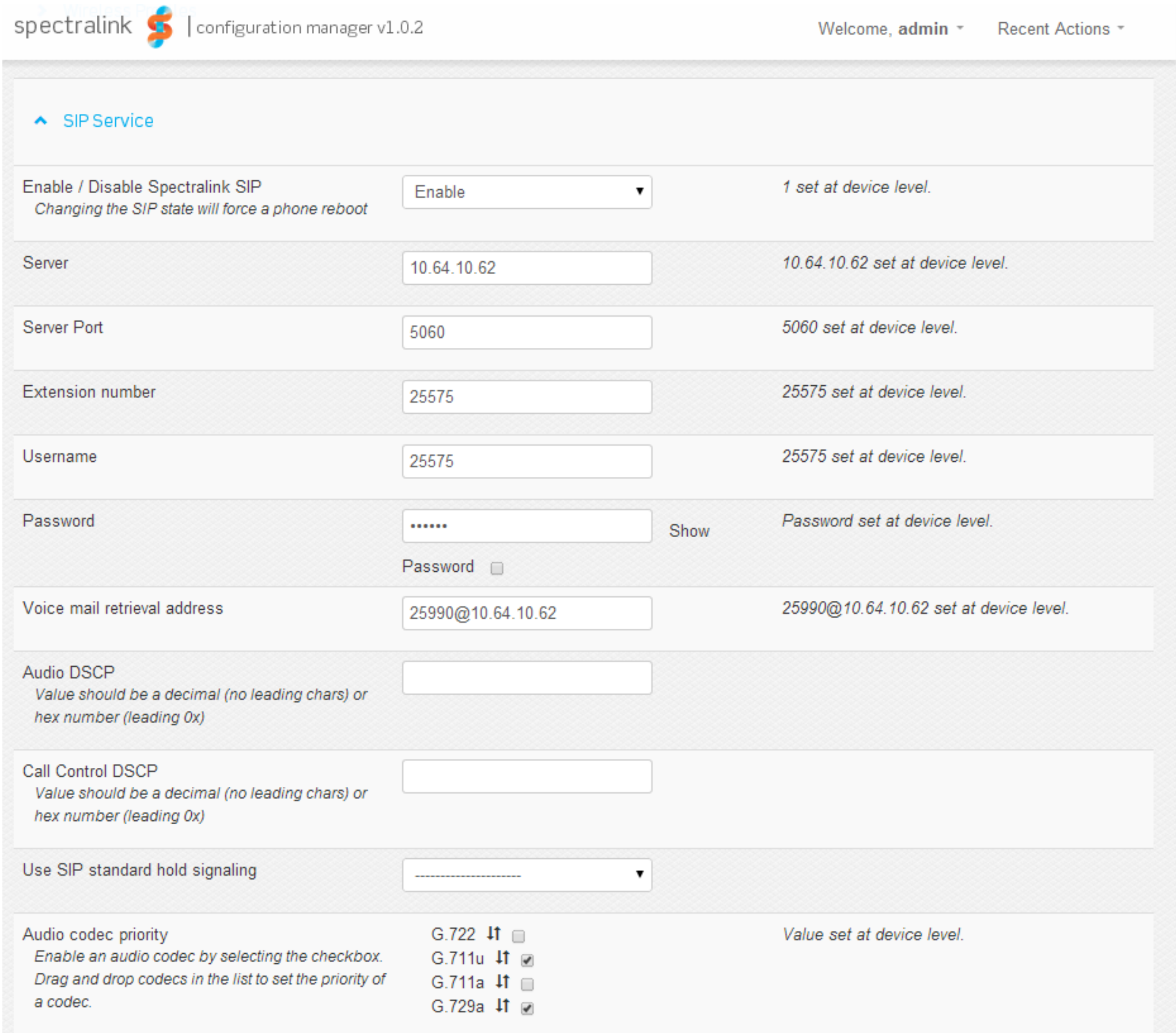


Once the phones are connected to WiFi, CMS automatically detects them. To view all the phones that are detected by CMS, select **Device List**.



Select **Configure,** to configure SIP Settings. On the **Configure Device** page, select **SIP Service**.

- Set **Enable /Disable Spectralink SIP** to **Enable**
- For **Server,** type in the SIP address of Session Manager
- For **Server Port**, type in the port number of Session Manager
- In the **Username** and **Password** field, type in the username and password that was created in **Section 6.8**.
- In the **Voice mail retrieval address** field, type in the address used for retrieving voice messages. In this case, Communication Manager Messaging was used.



8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that Pivot successfully registers with Session Manager server by following the **Session Manager →System Status → User Registrations** link on the System Manager Web Interface.
- Place calls to and from Spectralink 87-Series 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.

9. Conclusion

Pivot was compliance tested with Communication Manager (Version 6.3) and Session Manager (Version 6.3). Spectralink 87-Series (1.0.0.4037) functioned properly for feature and serviceability. During compliance testing, Pivot 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*, December 2013, Release 6.3, Document Number 03-300509.

[2] *Administering Avaya® Session Manager*, October 2013, Release 6.3, Issue 3

[3] *Administering Avaya® System Manager*, October 2013, Release 6.3.Issue 3

The following documentation was provided by Spectralink and can be found at http://support.spectralink.com/

[1 *Spectralink 87-Series Administration Guide*

[2] *PIVOT by Spectralink User Guide*

[3] *PIVOT by Spectralink Quick Start Guide*

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.