Avaya Solution & Interoperability Test Lab

Application Notes for Spectralink IP-DECT Server with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Spectralink IP-DECT Server 400 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Spectralink IP-DECT Server 400 is a wireless solution that can be deployed as a standalone system or with optional external Spectralink base stations. Spectralink IP-DECT Server 400 controls the traffic in the air from Spectralink handsets and works as the link between the handsets and Avaya Aura® Session Manager. The Spectralink handsets used for the compliance test included the Spectralink 7202, 7522, and 7622 Handsets. In addition, an optional Spectralink Base Station was used to verify roaming. Spectralink IP-DECT Server 400 interfaces to Avaya Aura® Session Manager via SIP (as SIP endpoints).

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 configuration steps required to integrate Spectralink IP-DECT Server 400 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Spectralink IP-DECT Server 400 is a wireless solution that can be deployed as a standalone system or with optional external Spectralink base stations. Spectralink IP-DECT Server 400 controls the traffic in the air from Spectralink handsets and works as the link between the handsets and Avaya Aura® Session Manager. The Spectralink handsets used for the compliance test included the Spectralink 7202, 7522, and 7622 Handsets. In addition, an optional Spectralink Base Station was used to verify roaming. Spectralink IP-DECT Server 400 interfaces to Avaya Aura® Session Manager via SIP (as SIP endpoints).

The IP-DECT Server family also includes models 200 and 6500, as detailed in **Attachment 1**. Since the products share the same firmware version, these Application Notes also apply to them.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between Spectralink 72-, 75-, and 76-Series Handsets and Avaya SIP/H.323 telephones and exercising basic telephony features, such as hold, mute, and transfer. The Spectralink handsets gained network access via the base station integrated in the Spectralink IP-DECT Server 400 or an optional standalone Spectralink Base Station. Additional telephony features, such as call forward, follow me, call park/unpark, and call pickup were also verified using Communication Manager Features Access Codes (FACs).

The serviceability testing focused on verifying that Spectralink IP-DECT Server 400 came back into service after re-connecting the Ethernet connect or rebooting the Spectralink IP-DECT Server 400 and Spectralink handsets.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and Spectralink IP-DECT Server 400 utilized enabled capabilities of Secure SIP (SIPS), including TLS/SRTP.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of Spectralink handsets with Session Manager. IP-DECT Server 400 controls the traffic in the air and works as the link between the Spectralink handsets and Session Manager.
- Calls between Spectralink handsets and Avaya SIP/H.323 deskphones with Direct IP Media (Shuffling) enabled and disabled. Shuffling was verified with Spectralink handsets and Avaya SIP deskphones only.
- Calls between Spectralink handsets and the PSTN.
- TLS transport protocol using SIPS URI.
- Calls with TLS/SRTP enabled.
- Support of G.711 and G.729 codecs.
- Proper recognition of DTMF tones.
- Basic telephony features, including hold, mute, redial, multiple calls, blind/attended transfer, and long duration calls.
- Extended telephony features using Communication Manager FACs for Call Forward, Follow Me, Call Unpark, and Call Pickup.
- Roaming of Spectralink handsets from Spectralink IP-DECT Server 400 to Spectralink Base Station.
- Proper system recovery after a restart of Spectralink IP-DECT Server 400 and Spectralink handsets and loss of IP connectivity.

2.2. Test Results

All test cases passed with the following observations noted:

- Spectralink 72-, 75-, and 76- Series Handsets do not support the initiation of 3-party conference calls.

- Spectralink IP-DECT Server 400 does not support SDP Capability Negotiation (RFC5939) so the **IP Codec Set** form on Communication Manager should only be set for one Media Encryption method (i.e., *1-srtp-aescm128-hmac80*); otherwise, SRTP would not be negotiated for the call and the call would fail. When SRTP is enabled on the IP-DECT Server 400, encrypted SRTCP is also automatically enabled and required. Therefore, **Encrypted SRTCP** in the **IP Codec Set** form should be set to *enforce-enc-srtcp*.

- To support calls with other Avaya IP deskphones that don’t support SRTP or encrypted SRTCP, a separate IP Network Region with a different, and more flexible, **IP Codec Set** should be used. For example, Avaya H.323 Deskphones don’t support encrypted SRTCP and Avaya 1600 Series IP Deskphones don’t support SRTP or encrypted SRTCP. This

IP Codec Set should allow no media encryption and/or media encryption supported by the IP endpoints. In addition, **Encrypted SRTCP** should be set to *best-effort* so that it isn't required for Avaya H.323 Deskphones that don't support it.

- Calls between Spectralink handsets and Avaya H.323 Deskphones shouldn't be shuffled. Since Spectralink IP-DECT Server 400 automatically enables and requires encrypted SRTCP when it is configured for SRTP, shuffling (i.e., Direct IP Media) with Avaya H.323 Deskphones should be disabled. If Communication Manager attempts to shuffle these calls, it would send unencrypted SRTCP in the SDP of the re-Invite message, used to shuffle the call, to the Spectralink handsets, which the IP-DECT Server 400 would reject by dropping the call.

2.3. Support

For technical support on the Spectralink IP-DECT Server, Spectralink Base Station, or Spectralink 72-, 75-, and 76-Series Handsets, contact Spectralink Technical Support via phone, email, or website.

- **Phone:** +1 (800) 775-5330
- **Web:** http://support.spectralink.com/
- **Email:** technicalsupport@spectralink.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Spectralink IP-DECT Server 400, Spectralink Base Station (optional), and Spectralink 72-, 75-, and 76- Series Handsets with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Spectralink handsets registered with Session Manager via SIP through the Spectralink IP-DECT Server 400. The Spectralink Base Station is an optional component that was used to verify roaming of the Spectralink handsets. An Avaya G450 Media Gateway was connected to the PSTN via an ISDN-PRI trunk and media resources were available in the G450 Media Gateway and Avaya Aura® Media Server. Avaya Aura® System Manager was used to configure Session Manager and Avaya Aura® Messaging served as the voicemail system. Avaya 96x1 Series H.323 and SIP Deskphones were used for placing and receiving calls.

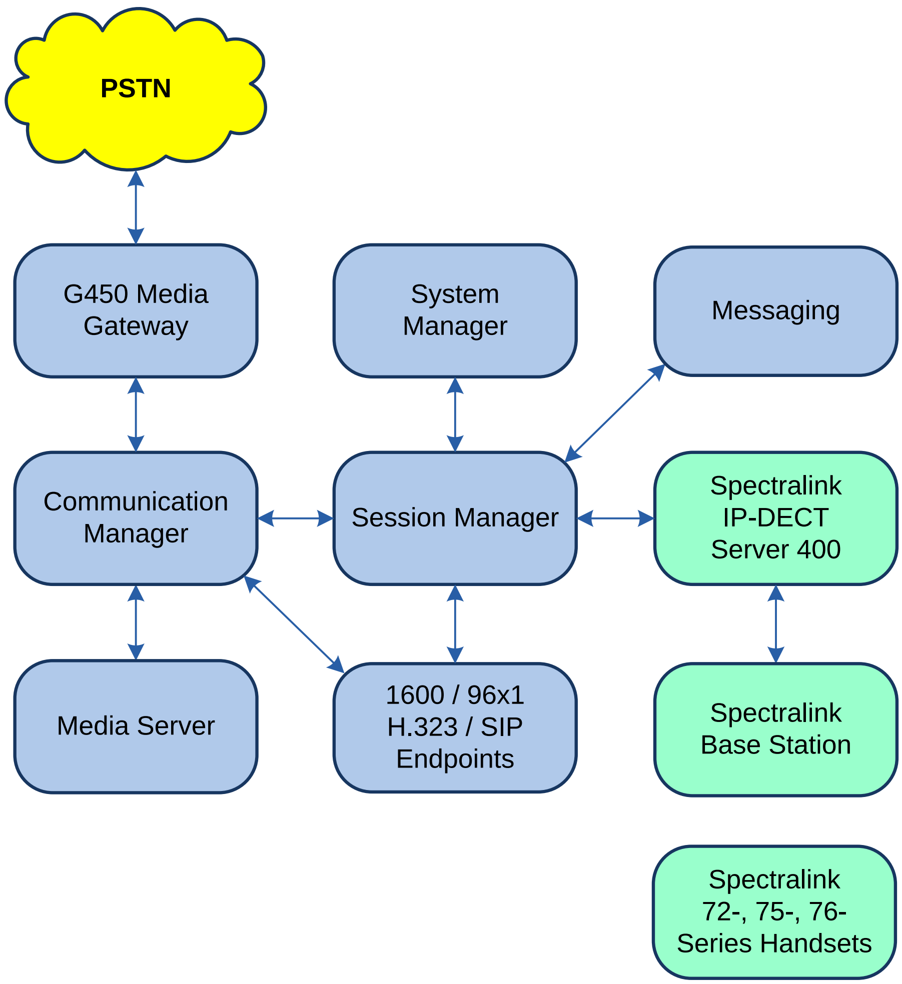


Figure 1: Avaya SIP Network with Spectralink IP-DECT Server 400, Spectralink Base Station, and Spectralink 72-, 75-, and 76-Series Handsets

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.0.1.1.0-FP1SP1 (R018x.00.0.822.0 with Patch 25183)
Avaya G450 Media Gateway	FW 40.25.0
Avaya Aura® Media Server	v.8.0.0.173
Avaya Aura® System Manager	8.0.1.1 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.1.1.039340 Service Pack 1
Avaya Aura® Session Manager	8.0.1.1.801103
Avaya Aura® Messaging	7.1.3.1.0-FP3SP1
Avaya 96x1 Series IP Deskphone	6.8003 (H.323) 7.1.5.0.11 (SIP)
Avaya 1600 Series IP Deskphone	1.3120 (H.323)
Spectralink IP-DECT Server 400	PCS19Ac
Spectralink Base Station	PCS19Ac
Spectralink 72-Series Handset	18F
Spectralink 75- and 76-Series Handsets	19B

5. Configure Avaya Aura® Communication Manager

This section provides the procedure for configuring Communication Manager. The procedure includes the following areas:

- Verify Communication Manager license
- Administer IP Node Names
- Administer IP Network Region and IP Codec Set
- Administer SIP Trunk Group to Session Manager
- Administer AAR Call Routing

Use the System Access Terminal (SAT) to configure Communication Manager and log in with appropriate credentials.

Note: It is assumed that basic configuration, such as voicemail coverage, has already been configured. The SIP station configuration for Spectralink IP-DECT Server 400 is configured through Avaya Aura® System Manager in **Section 6.2**.

5.1. Verify License

Using the SAT, verify that the Off-PBX Telephones (OPS) option is enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

```
display system-parameters customer-options                      Page   1 of  12
                                OPTIONAL FEATURES

     G3 Version: V18                              Software Package: Enterprise
       Location: 2                                System ID (SID): 1
       Platform: 28                               Module ID (MID): 1

                                                                USED
                                Platform Maximum Ports: 48000    99
                                      Maximum Stations: 36000 28
                              Maximum XMOBILE Stations: 36000 0
                    Maximum Off-PBX Telephones - EC500: 41000 0
                    Maximum Off-PBX Telephones -   OPS: 41000 17
                    Maximum Off-PBX Telephones - PBFMC: 41000 0
                    Maximum Off-PBX Telephones - PVFMC: 41000 0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 313   0


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

On **Page 5**, verify that the **Media Encryption Over IP** option is enabled.

```
change system-parameters customer-options                       Page   5 of  12
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                                IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                          ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                            ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                   ISDN-PRI? y
              ESS Administration? y                 Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                       Malicious Call Trace? y
     External Device Alarm Admin? y                   Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                   Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y                 Multimedia IP SIP Trunking? y
                       IP Trunks? y

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

5.2. Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
devcon-aes          10.64.102.119
devcon-ams          10.64.102.118
devcon-sm           10.64.102.117
procr               10.64.102.115
procr6              ::

( 6  of 6    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
```

5.3. Administer IP Network Region and IP Codec Set

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Aura® Media Server. The **IP Network Region** form also specifies the **Codec Set** to be used for calls routed over the SIP trunk to Session Manager.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: avaya.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: 50999
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
```

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to IP-DECT Server 400. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set '1' was specified in IP Network Region '1' shown above. The default settings of the **IP Codec Set** form are shown below. IP-DECT Server 400 was tested using G.711 and G.729 codecs. Specify the desired codecs in the **IP Codec Set** form as per customer requirements.

```
change ip-codec-set 1                                           Page   1 of   2

                          IP CODEC SET
    Codec Set: 1

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

To enable SRTP, set **Media Encryption** to *1-srtp-aescm128-hmac80* and **Encrypted SRTCP** to *enforce-enc-srtcp*. These strict settings are required because IP-DECT Server 400 doesn't currently support SDP Capability Negotiation (RFC5939) and when SRTP is enabled, encrypted SRTCP is also automatically enabled and required. Communication Manager must provide the exact capabilities supported by IP-DECT Server 400.

Note: To support calls with other Avaya IP deskphones that don't support SRTP or encrypted SRTCP, a separate IP Network Region with a different, more flexible, **IP Codec Set** should be used. This **IP Codec Set** should specify no media encryption and/or media encryption methods supported by the IP endpoints. In addition, **Encrypted SRTCP** should be set to *best-effort* since Avaya H.323 Deskphones don't support encrypted SRTCP. This IP Codec Set should also be used for Avaya Aura® Messaging (requires different SIP trunk to Session Manager than the one covered in **Section 5.4** that uses the same **IP Network Region** and **IP Codec Set** as the H.323 deskphones).

For these calls, shuffling (i.e., Direct IP Media) should also be disabled. If Communication Manager attempts to shuffle the call, it would send unencrypted SRTCP in the SDP of the re-Invite message (used to shuffle the call), which the IP-DECT Server 400 would reject by dropping the call.

The **IP Network Map** form may be used to associate certain IP endpoints with a specific IP Network Region.

```
     Media Encryption                     Encrypted SRTCP: enforce-enc-srtcp
 1: 1-srtp-aescm128-hmac80
 2:
 3:
```

5.4. Administer SIP Trunk to Session Manager

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Set the **Enforce SIPS URI for SRTP** field to *y*.
- Specify Communication Manager (*procr*) and the Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **Direct IP-IP Audio Connections** field was enabled on this form.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.
- Enable **Initial IP-IP Direct Media**.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

```
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                    Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: devcon-sm
 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? y
H.323 Station Outgoing Direct Media? n         Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to IP-DECT Server 400 (i.e., Spectralink handsets) and Avaya SIP deskphones. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Configure the other fields in bold and accept the default values for the remaining fields.

Note: Since Avaya Aura® Messaging doesn't support encrypted SRTCP, a separate signaling and trunk group are required that is associated with a different **IP Network Region** and **IP Codec Set**, similar to Avaya H.323 Deskphones. Refer to the note in **Section 5.3**.

```
add trunk-group 10                                                    Page   1 of  22
                                TRUNK GROUP

Group Number: 10                   Group Type: sip           CDR Reports: y
  Group Name: To devcon-sm                COR: 1        TN: 1        TAC: 1010
   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
```

5.5. AAR Call Routing

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and enter add an entry that routes digits beginning with "78" to route pattern 10 as shown below.

```
change aar analysis 78                                                   Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 1

          Dialed          Total     Route    Call   Node  ANI
          String        Min  Max  Pattern    Type   Num   Reqd
    78                  5    5     10        lev0         n
```

Configure a preference in **Route Pattern** 10 to route calls over SIP trunk group 10 as shown below.

```
change route-pattern 10                                         Page   1 of   3
                    Pattern Number: 10     Pattern Name: To devcon-sm
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                           DCS/ IXC
    No          Mrk Lmt List Del  Digits                             QSIG
                             Dgts                                    Intw
 1: 10   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 Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               unk-unk   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
```

6. Configure Avaya Aura® Session Manager

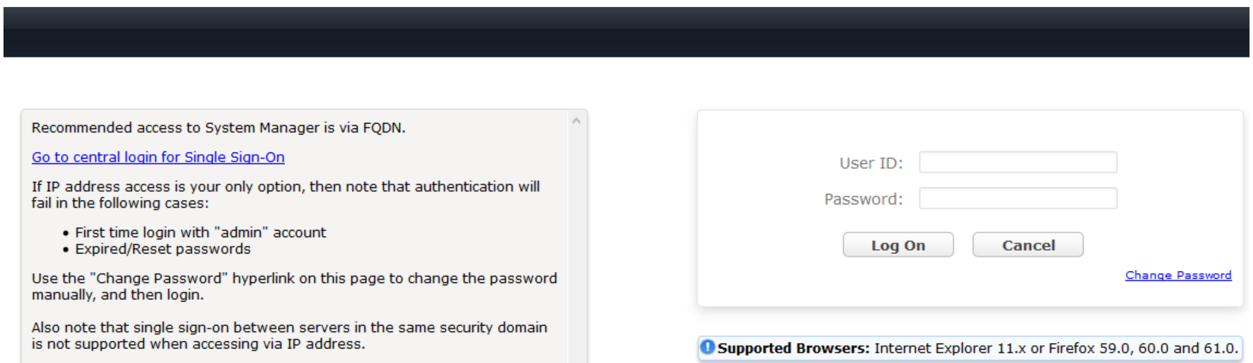
This section provides the procedure for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Set Network Transport Protocol for IP-DECT Server 400
- Administer SIP User

Note: It is assumed that basic configuration of Session Manager has already been performed. This section will focus on the configuration of a SIP user for the Spectralink solution.

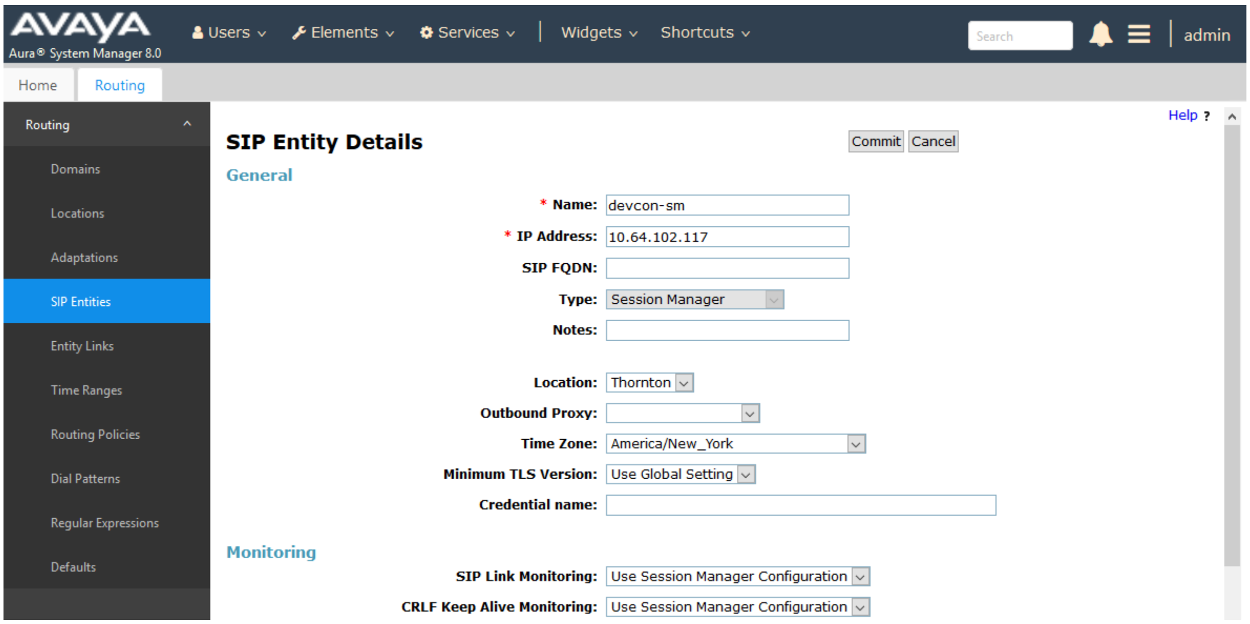
6.1. Launch System Manager

Access the System Manager Web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the System Manager server. Log in using the appropriate credentials.

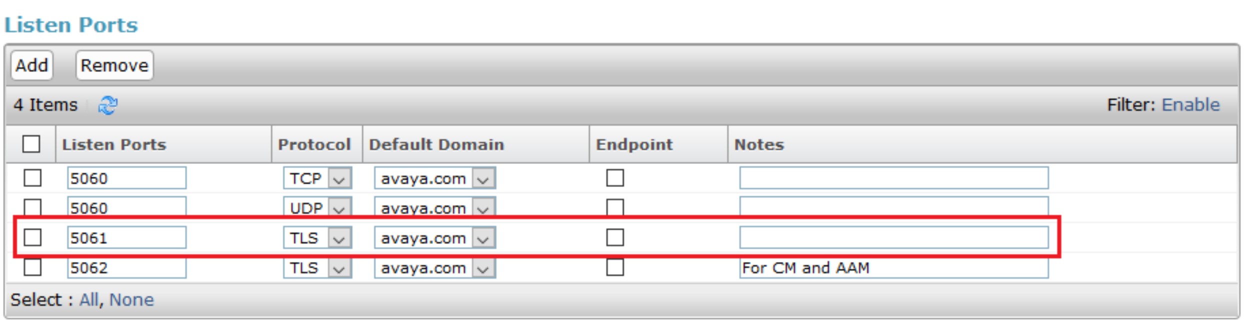


6.2. Set Network Transport Protocol for Spectralink IP-DECT Server 400

From the System Manager **Home** screen, select **Elements → Routing → SIP Entities** and edit the SIP Entity for Session Manager shown below.

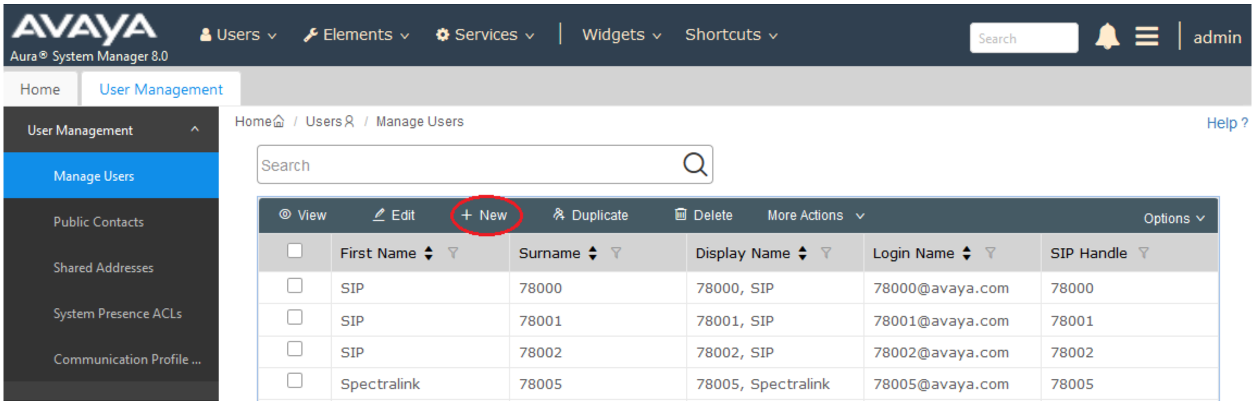


Scroll down to the **Listen Ports** section and verify that the transport network protocol used by IP-DECT Server 400 is specified in the list below. For the compliance test, the solution used TLS network transport.



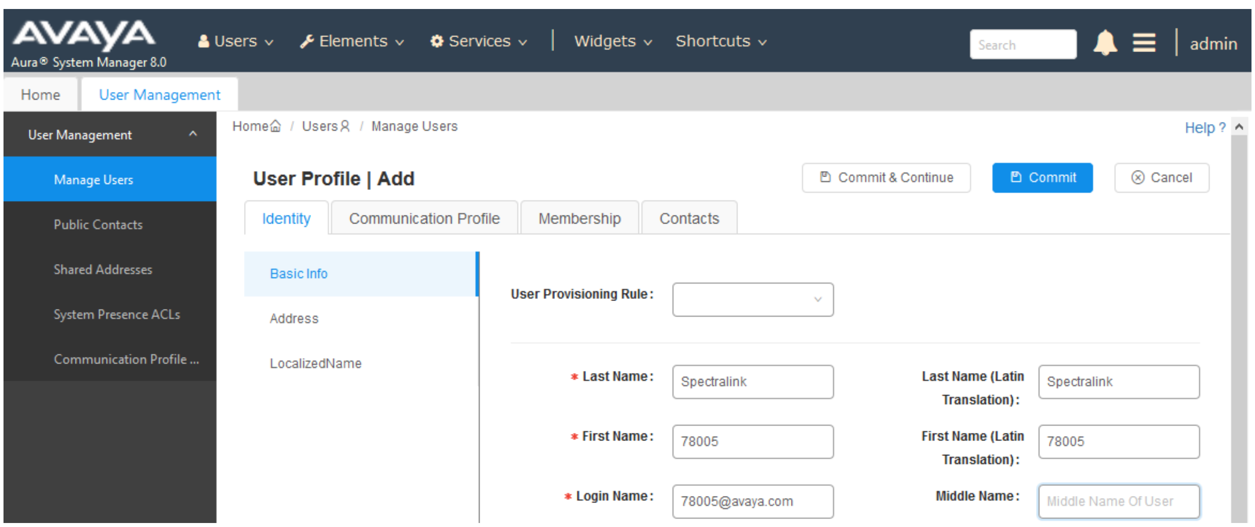
6.3. Administer SIP User

In the **Home** screen (not shown), select **Users → User Management → Manage Users** to display the **User Management** screen below. Click **New** to add a user.



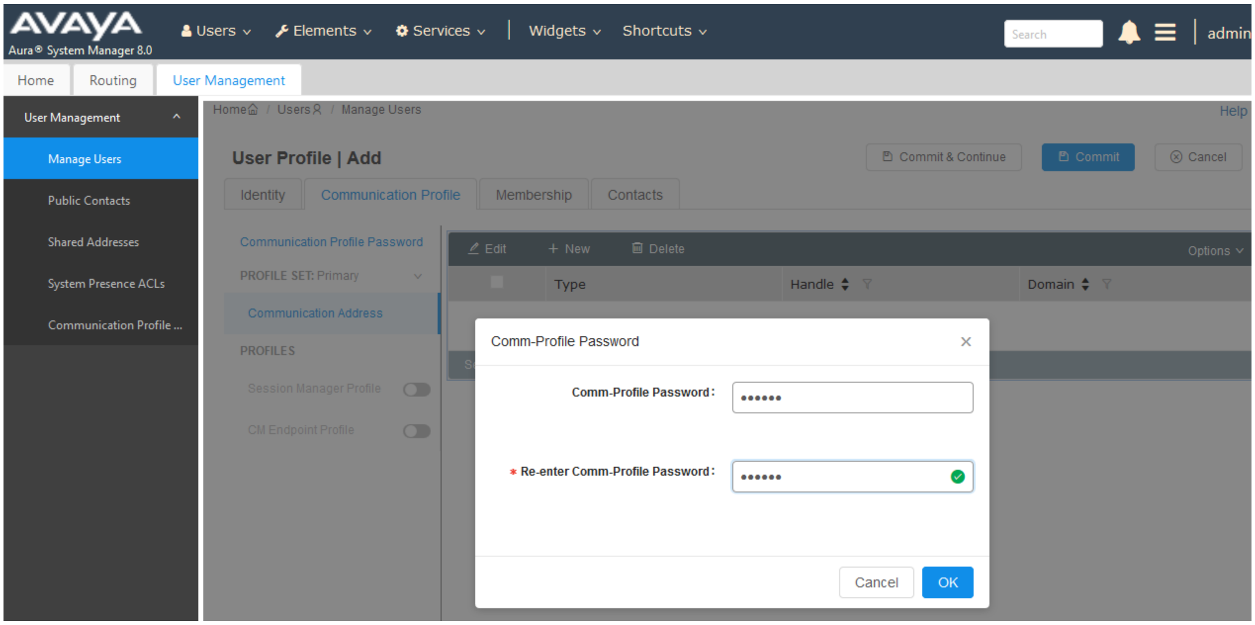
6.3.1. Identity

The **User Profile | Add** screen is displayed. Enter desired **Last Name** and **First Name**. For **Login Name**, enter "*<ext>*@*<domain>*", where "*<ext>*" is the desired Spectralink SIP extension and "*<domain>*" is the applicable SIP domain name from **Section 5.3**. Retain the default values in the remaining fields.



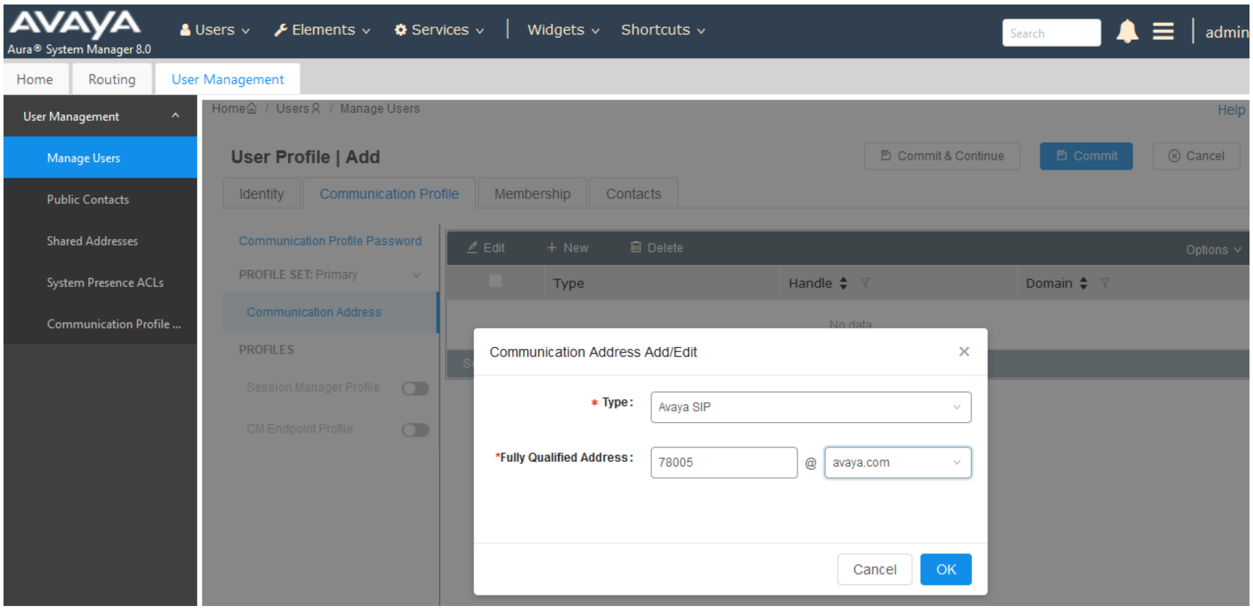
6.3.2. Communication Profile

Select the **Communication Profile** tab. Next, click on **Communication Profile Password**. For **Comm-Profile Password** and **Re-enter Comm-Profile Password**, enter the desired password for the SIP user to use for registration. Click **OK**.



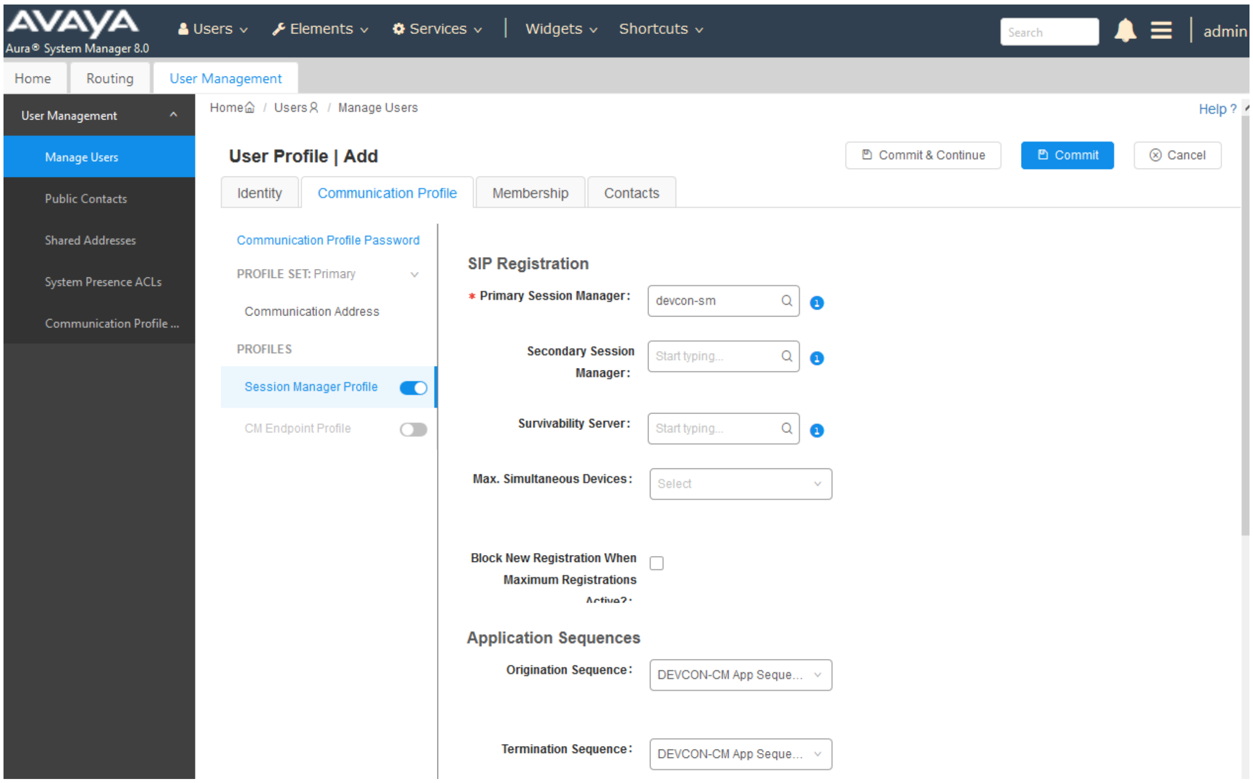
6.3.3. Communication Address

Click on **Communication Address** and then click **New** to add a new entry. The **Communication Address Add/Edit** dialog box is displayed as shown below. For **Type**, select *Avaya SIP*. For **Fully Qualified Address**, enter the SIP user extension and select the domain name to match the login name from **Section 6.3.1**. Click **OK**.

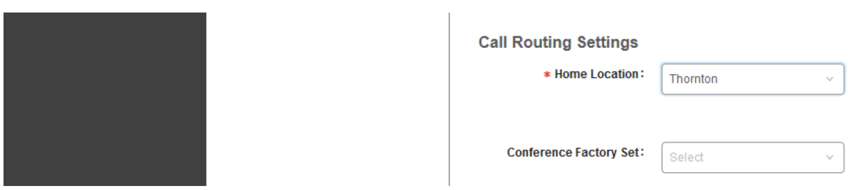


6.3.4. Session Manager Profile

Click on toggle button by **Session Manager Profile**. For **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence**, and **Home Location**, select the values corresponding to the applicable Session Manager and Communication Manager. Retain the default values in the remaining fields.

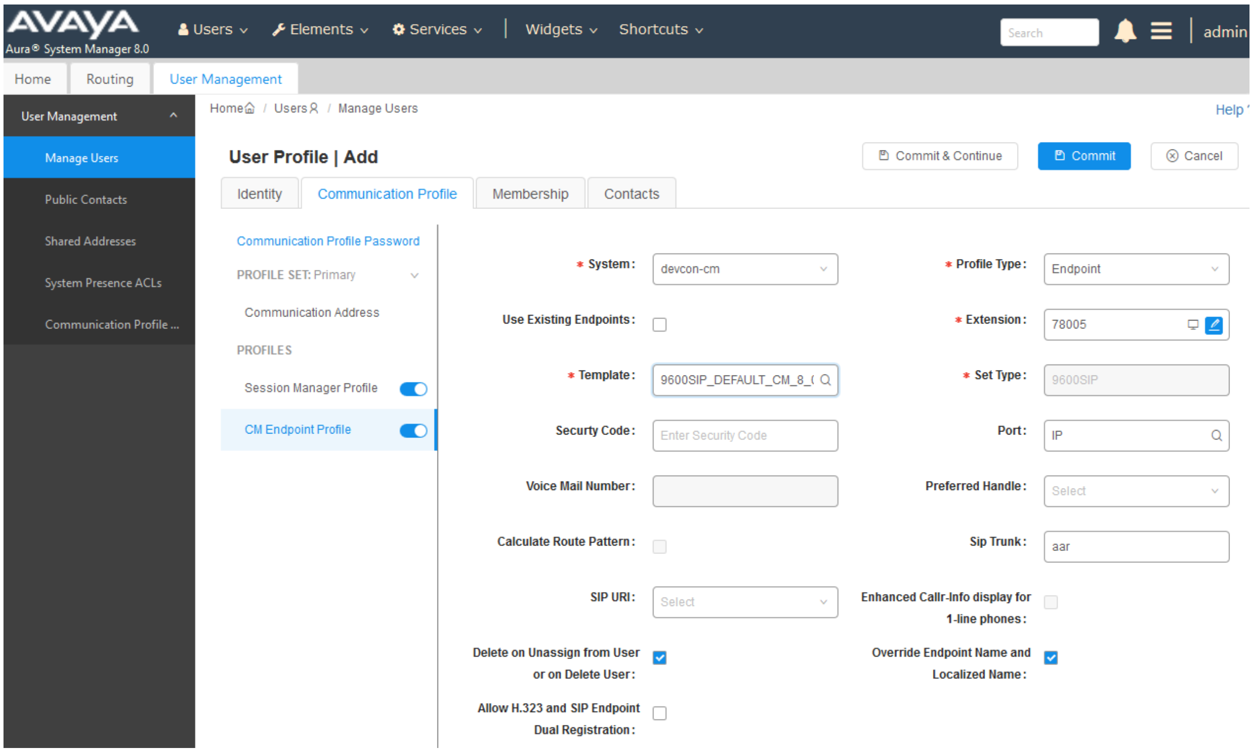


Scroll down to the **Call Routing Settings** section to configure the **Home Location**.

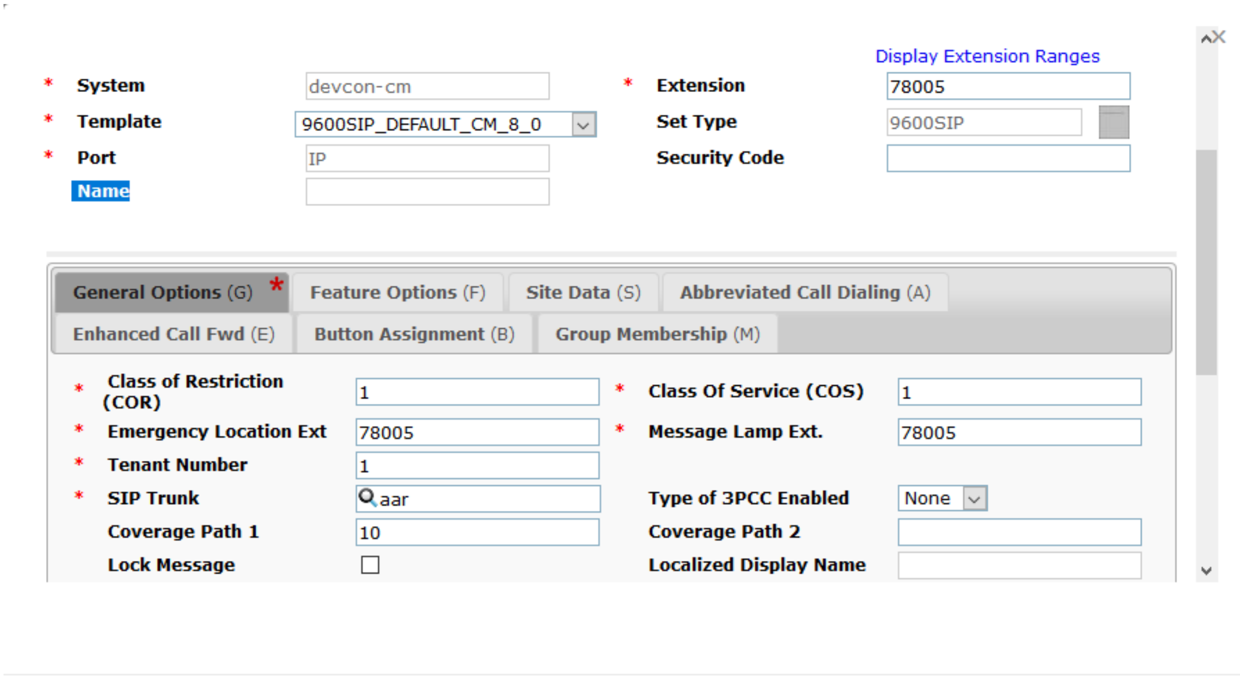


6.3.5. CM Endpoint Profile

Click on the toggle button by **CM Endpoint Profile**. For **System**, select the value corresponding to the applicable Communication Manager. For **Extension**, enter the SIP user extension from **Section 6.3.1**. For **Template**, select *9600SIP_DEFAULT_CM_8_0*. For **Port**, click and select *IP*. Retain the default values in the remaining fields. Click on the Endpoint Editor (i.e, Edit icon in Extension field) to configure the **Coverage Path**.



Navigate to the **General Options** tab and set the **Coverage Path 1** field to the voicemail coverage path. Click **Done** (not shown) to return to the previous web page and then **Commit** to save the configuration (not shown).



7. Configure Avaya 96x1 Series SIP Deskphones

The 46xxsettings.txt file is used to specify certain system parameters. It is used by Avaya H.323 and SIP Deskphones, but this section will cover four parameters that are applicable to SIP deskphones only.

- **SDPCAPNEG** Specifies whether SDP capability negotiation is supported. By default, it is enabled.
- **ENFORCE_SIPS_URI** Enable this option to support SIPS URI.
- **MEDIAENCRYPTION** Specifies the media encryption (SRTP) options supported. In the example below, *aescm128-hmac80* (option 1) is supported as specified in the **IP Codec Set** in **Section 5.3**.
- **ENCRYPT_SRTCP** Enable this option to encrypt SRTCP.

```
## SDPCAPNEG specifies whether or not SDP capability negotiation is enabled.
##  Value  Operation
##    0    SDP capability negotiation is disabled
##    1    SDP capability negotiation is enabled (default)
##  This parameter is supported by:
##       J129 SIP R1.0.0.0 and later
##       96x1 SIP R6.0 and later
##       H1xx SIP R1.0 and later
##       96x0 SIP R2.6 and later
SET SDPCAPNEG 1
##
## ENFORCE_SIPS_URI specifies whether a SIPS URI must be used for SRTP.
##  Value  Operation
##    0    Not enforced
##    1    Enforced (default)
##  This parameter is supported by:
##       J129 SIP R1.0.0.0 and later; not applicable for 3PCC environment
##       96x1 SIP R6.0 and later
##       H1xx SIP R1.0 and later
##       96x0 SIP R2.6 and later
SET ENFORCE_SIPS_URI 1
##
## MEDIAENCRYPTION specifies which media encryption (SRTP) options will be supported.
##  Up to 2 or 3 options may be specified in a comma-separated list.
##  2 options are supported by:
##     1. Prior releases to 96x1 SIP 7.0.0
##     2. H1xx SIP R1.0 and later
##     3. 96x0 SIP R1.0 to R2.6.14.1
##  3 options are supported by 96x1 SIP R7.0.0 and later, H1xx SIP R1.0.1 and later
##  and J129 SIP R1.0.0.0 and later.
##  For 96x0 SIP R2.6.14.5 and later, up to 3 options may be specified, but only the
##  first two supported options are used.
##  Options should match those specified in CM IP-codec-set form.
##     1 = aescm128-hmac80
##     2 = aescm128-hmac32
##     3 = aescm128-hmac80-unauth
##     4 = aescm128-hmac32-unauth
##     5 = aescm128-hmac80-unenc
##     6 = aescm128-hmac32-unenc
##     7 = aescm128-hmac80-unenc-unauth
##     8 = aescm128-hmac32-unenc-unauth
##     9 = none (default)
```

```
##    10 = aescm256-hmac80
##    11 = aescm256-hmac32
##  Options 10 and 11 are supported by 96x1 SIP R7.0.0 and later, H1xx SIP R1.0.1 and
##  later and J129 SIP R1.0.0.0 and later.
##  Note: The list of media encryption (SRTP) options is ordered from high (left) to
##  the low (right) options. The phone will publish this list in the SDP-OFFER
##  or choose from SDP-OFFER list according to the list order defined in
##  MEDIAENCRYPTION. Please note that  Avaya Communication Manager has the capability
##  to change the list order in the SDP-OFFER (for audio only) when the SDP-OFFER pass
##  through CM.
##  This parameter is supported by:
##       Avaya Equinox 3.1.2 and later; supported values: 1,2,9,10 and 11. The default
##       value is 1,2,9.
##       Avaya Vantage Basic Application SIP R1.0.0.0 and later; supported values:
##       1,2,9,10 and 11. The default value is 1,2,9.
##       J129 SIP R1.0.0.0 and later
##       96x1 SIP R6.0 and later
##       H1xx SIP R1.0 and later
##       96x0 SIP R1.0 and later
SET MEDIAENCRYPTION 1,9
##
## ENCRYPT_SRTCP specifies whether RTCP packets are encrypted or not. SRTCP is only
## used if SRTP is enabled using
## MEDIAENCRYTION (values other than 9 (none) are configured).
## This parameter controls RTCP encryption for RTCP packets exchanged between peers.
## RTCP packets sent to Voice Monitoring Tools are always sent unencrypted.
##  Value  Operation
##   0          SRTCP is disabled (default).
##   1     SRTCP is enabled.
##  This parameter is supported by:
##       Avaya Equinox 3.1.2 and later
##       96x1 SIP R7.1.0.0 and later
##       Avaya Vantage Basic Application SIP R1.0.0.0 and later
##       J129 SIP R1.0.0.0 and later
SET ENCRYPT_SRTCP 1
```

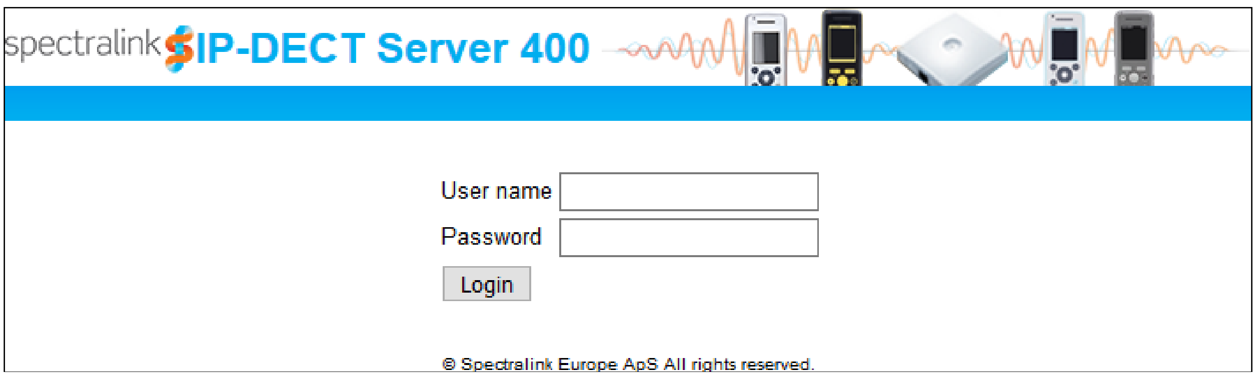
8. Configure Spectralink IP-DECT Server 400

This section provides the procedures for configuring Spectralink IP-DECT Server 400. The procedures fall into the following areas:

- Launch web interface
- Administer network settings
- Administer SIP settings, including SIP port, transport protocol, Message Waiting Indicator (MWI) and audio codecs
- Add SIP Users
- Import TLS certificate

8.1. Launch Web Interface

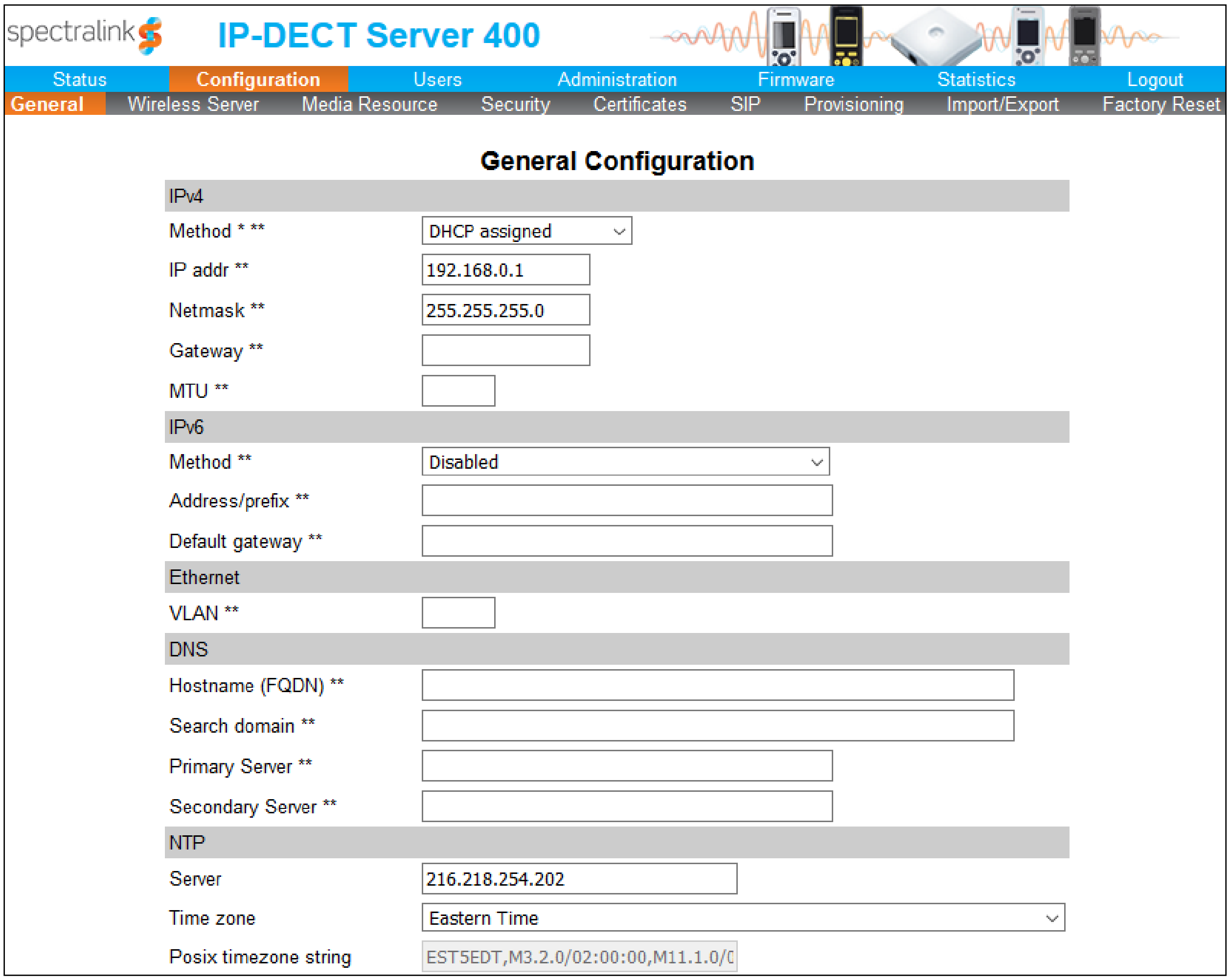
Spectralink IP-DECT Server 400 was configured through the web interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of IP-DECT Server 400. Log in using the appropriate credentials and then click **OK**.



8.2. Administer Network Settings

To configure network settings, click **Configuration** and then select the **General** tab. The Spectralink IP-DECT Server 400 is pre-configured to use DHCP, but a static IP address may be used. However, for the compliance test, DHCP was used as shown below.

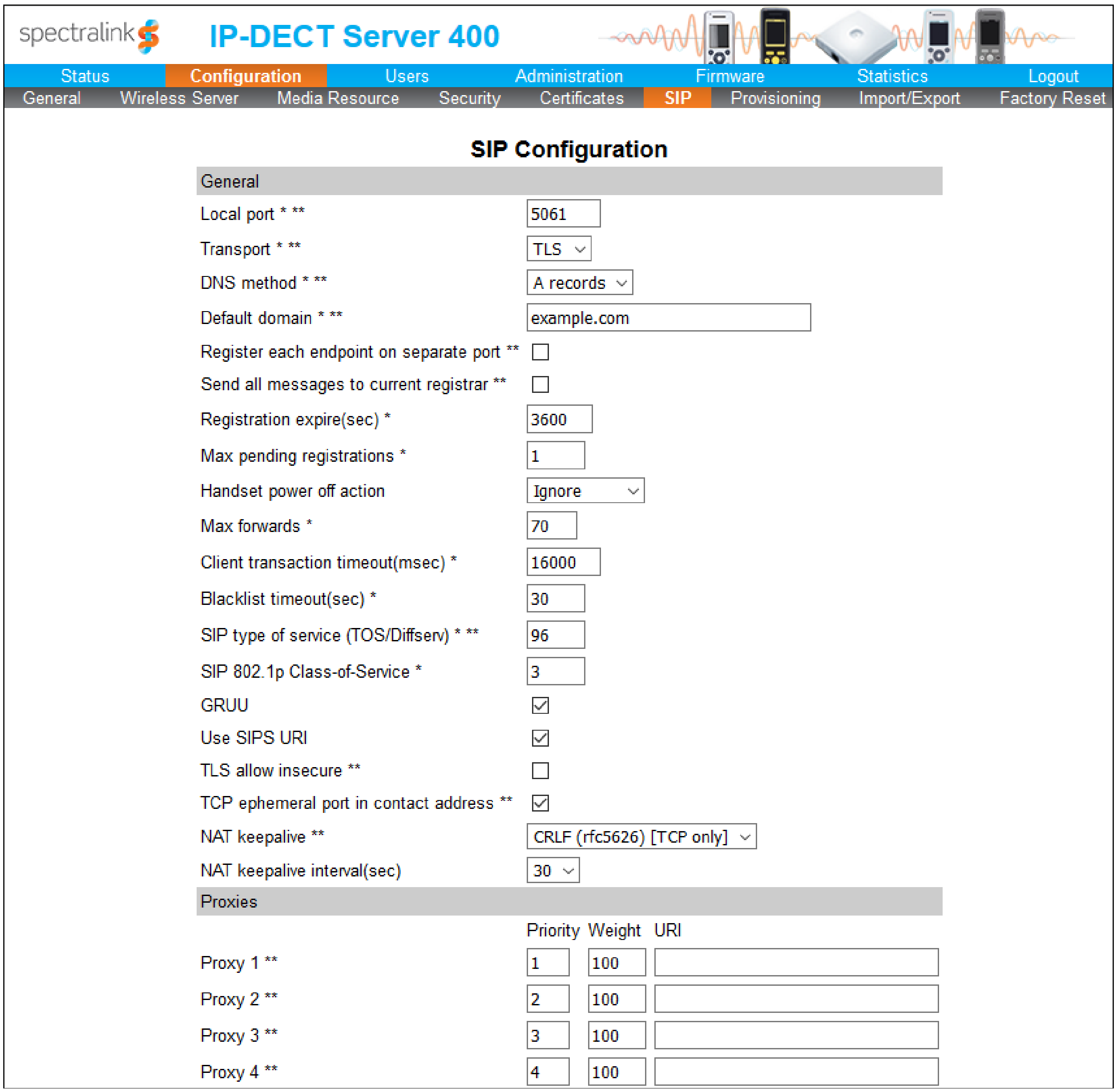
Since TLS transport is going to be used, verify that the NTP server is configured properly to avoid any issues with the TLS certificates installed in **Section 8.5**.



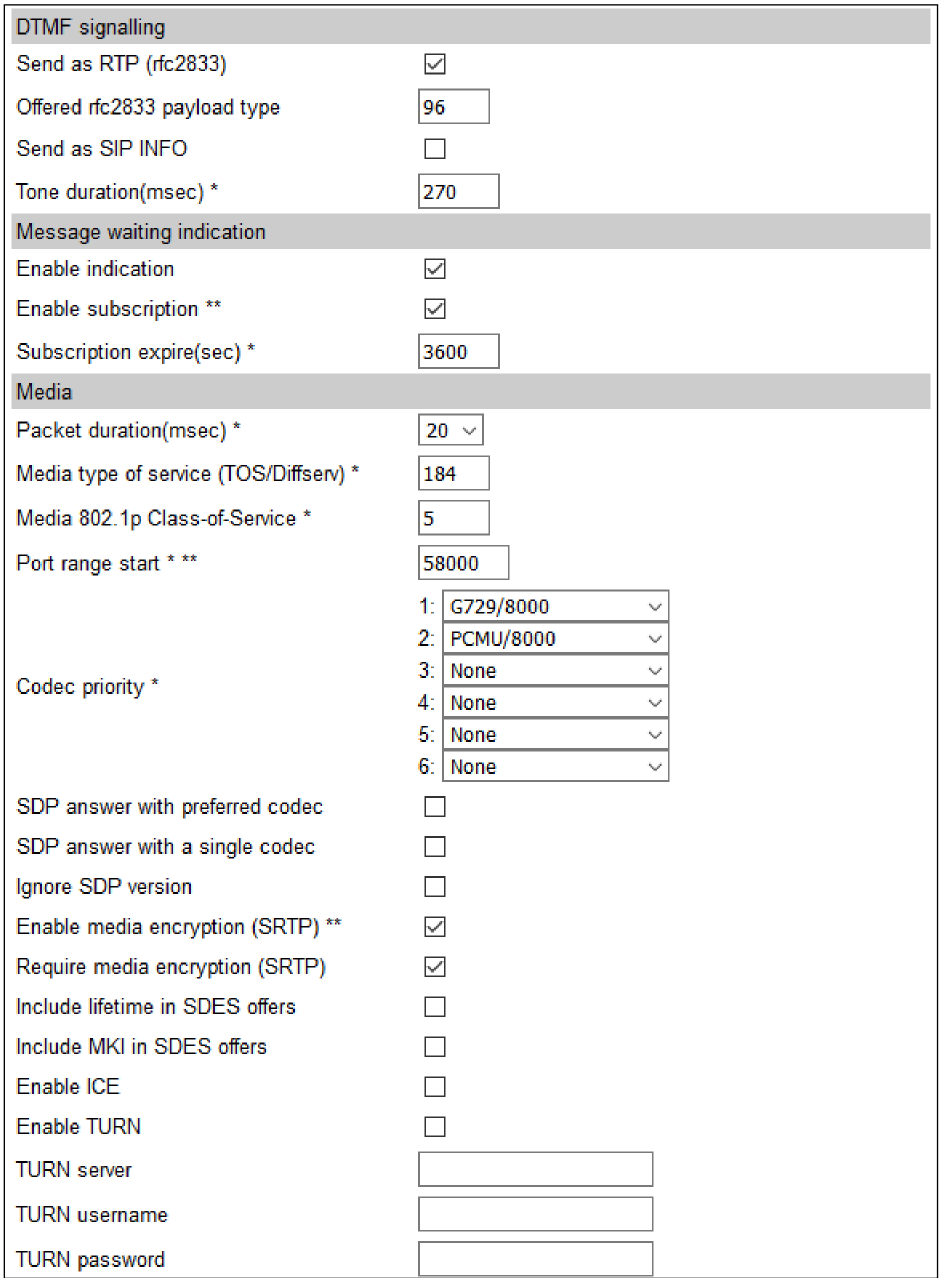
8.3. Administer SIP Settings

To configure SIP settings, click **Configuration** and then select the **SIP** tab. Configure the following fields:

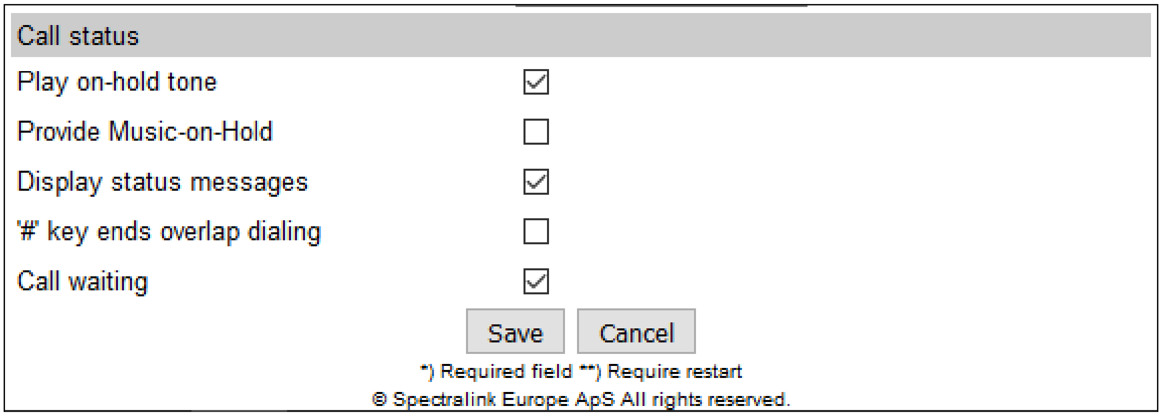
- **Local port** Specify TLS port 5061 depending on the transport protocol to be used.
- **Transport** Specify TLS transport protocol.
- **Use SIPS URI** Enable this option.
- **TCP ephemeral port in contact address** Enable this field for TLS transport.



Scroll down to the **Message waiting indication** and **Media** sections. In the **Message waiting indication** section, select the **Enable indication** and **Enable subscription** check boxes as shown below. This is required to support updates to the Message Waiting Indicator (MWI) lamp. In the **Media** section, allow G.711 and G.729 and select the **Enable media encryption (SRTP)** and **Require media encryption (SRTP)** check boxes as shown below.

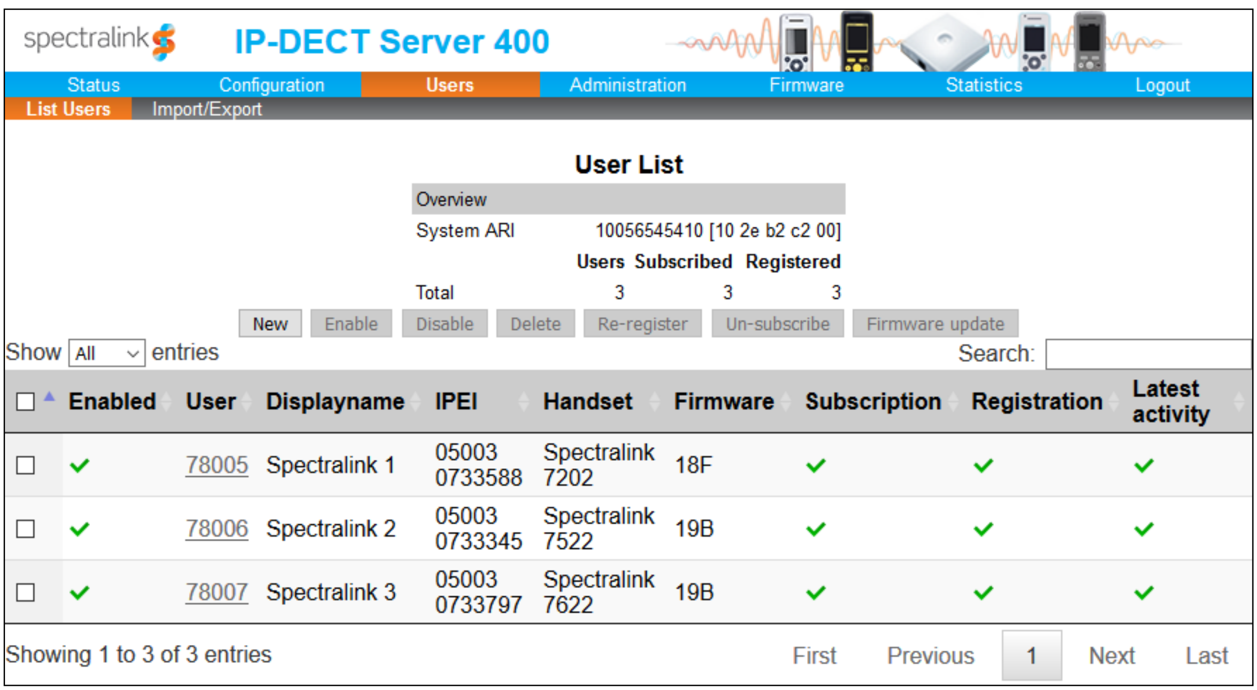


Use the default settings for the **Call Status** section shown below. Click **Save**.



8.4. Add SIP Users

To create a SIP user for one of the Spectralink handsets, click **Users** and then the sub-tab **List Users**. Next, click on the **New** button shown below.



In the **User** page shown below, configure the following fields.

Under **DECT device**:

- **IPEI** Type the IPEI number of the handset.

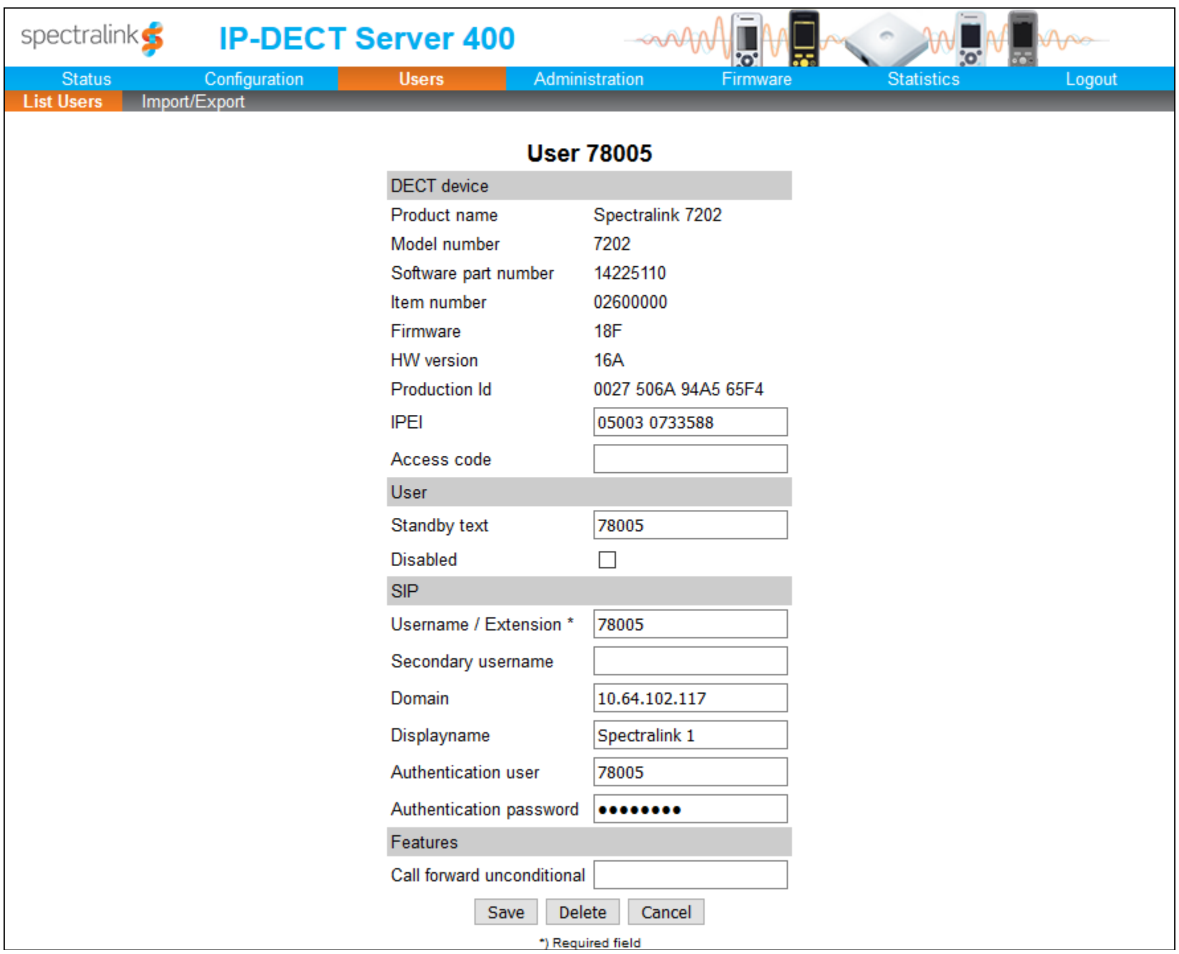
Under **User**:

- **Standby text** Enter the text to be displayed on the handset (e.g., SIP extension).

Under **SIP**:

- **Username / Extension** Set a user name or extension for handset.
- **Domain** Specify the IP address of the Session Manager signaling interface (e.g., *10.64.102.117*).
- **Displayname** Specify a display name for the handset (e.g., *Spectralink 1*).
- **Authentication user** Set to the SIP extension configured in **Section 6.3.3**.
- **Authentication password** Enter the password configured in the **Comm-Profile Password** field in **Section 6.3.2**.

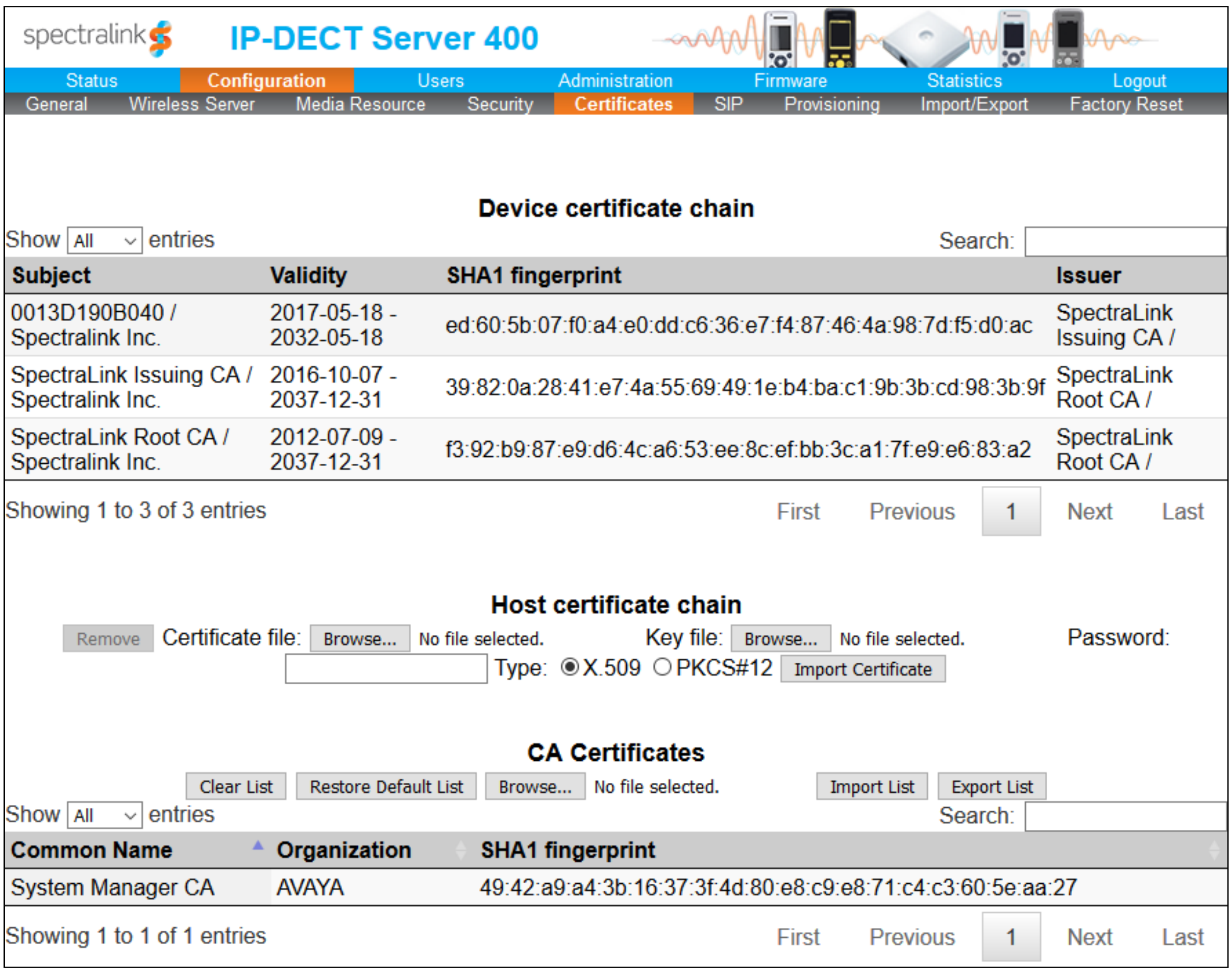
Retain the default values for the other fields. Click **Save**.



8.5. Import TLS Certification

This section is required for TLS transport and covers how to import the TLS certificate into IP-DECT Server 400. For the compliance test, Avaya Aura® System Manager was used as the certificate authority. The TLS was exported from System Manager as described in the Managing Certificates section of Chapter 20, Security, in **[2]**.

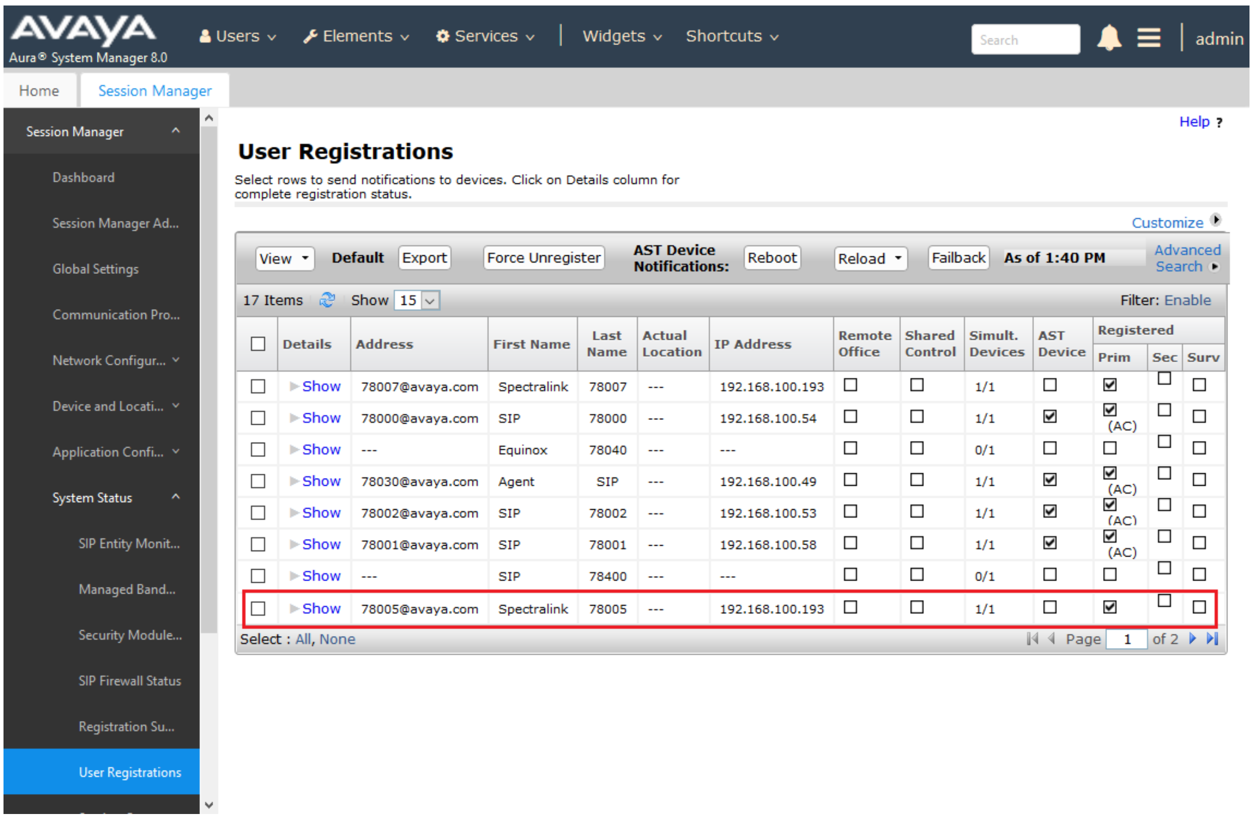
To import the TLS certificate, click **Configuration** and then click **Certificates**. In the **CA Certificates** section, click the **Browse** button to select the TLS certificate, and then click **Import List** to import the certificate. Once imported, the certificate will be listed as shown below. Note the *SystemManager CA* certificate.



9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Spectralink IP-DECT Server 400.

1. Verify that Spectralink handsets have successfully registered with Session Manager. In System Manager, navigate to **Elements → Session Manager → System Status → User Registrations** to check the registration status.



2. Establish a call between Spectralink handset and a local Avaya deskphone. The **status trunk** command may be used to view the active call status. The trunk that is being monitored here is the trunk to Session Manager. This command should specify the trunk group and trunk member used for the call. On **Page 2**, **Audio Connection Type** will set to *ip-direct* if the call is shuffled. The **Codec Type** is also displayed.

```
status trunk 10/1                                              Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                             Port
   Near-end:  10.64.102.115                        : 5061
    Far-end:  10.64.102.117                        : 5061
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.711MU
   Audio      IP Address                             Port
   Near-end:  192.168.100.58                       : 5004
    Far-end:  192.168.100.193                      : 58116

 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:               Video Far-end Codec:
```

Page 3 will indicate if SRTP is enabled for the call as shown below.

```
status trunk 10/1                                              Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00001
T00001:TX:192.168.100.193:58116/g711u/20ms/1-srtp-aescm128-hmac80
T00006:RX:192.168.100.58:5004/g711u/20ms/1-srtp-aescm128-hmac80

dst port: T00006
```

3. While the call is active, basic telephony features can be exercised to verify proper operation.

10. Conclusion

These Application Notes described the configuration steps required to integrate Spectralink IP-DECT Server 400 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Spectralink IP-DECT 400 allowed Spectralink 72-, 75-, and 76-Series Handsets to register with Avaya Aura® Session Manager and establish calls to H.323 stations, SIP stations, and the PSTN with Secure SIP, including TLS/SRTP. In addition, basic telephony features were verified. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

11. References

This section references the Avaya documentation relevant to these Application Notes. The Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager,* Release 8.0.x, Issue 4, May 2019.

[2] *Administering Avaya Aura® System Manager for Release 8.0.1*, Release 8.0.x, Issue 9, May 2019.

[3] *Administering Avaya Aura® Session Manager*, Release 8.0.1, Issue 3, December 2018.

[4] *Spectralink IP-DECT Server 200/400/6500 Installation and Configuration Guide,* 14215700-IG, Edition 11.0, March 2019.

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.

spectralink
solving every day

Avaya Devconnect

June 13th 2019

Declaration of conformance for Spectralink IP-DECT Platform

We, Spectralink Corporation, hereby confirm that the following IP-DECT servers

- IP DECT Server 200
- IP DECT Server 400
- IP DECT Server 6500

are based on the same platform and therefore:

- Use identical SIP stack
- Use identical XML-RPC API for messaging
- Use the same firmware version PCS19Ac to support each platform

The difference in the two IP DECT server types is their scalability – maximum configuration:

- IP DECT Server 200
    - 6 simultaneous calls
    - 12 handsets(Users)
    - Single cell (0 additional Base stations to the one active in Server)
- IP DECT Server 400
    - 12 Simultaneous calls
    - 30 Handsets(Users)
    - 3 IP DECT Base stations (Additional to the one active in the Server)
- IP DECT Server 6500
    - Redundancy
    - 1.024 Simultaneous call
    - 4.095 handsets(Users)
    - 1.024 IP DECT Base stations

Best regards

Martin Praest
Director Business Development