



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., *l-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.

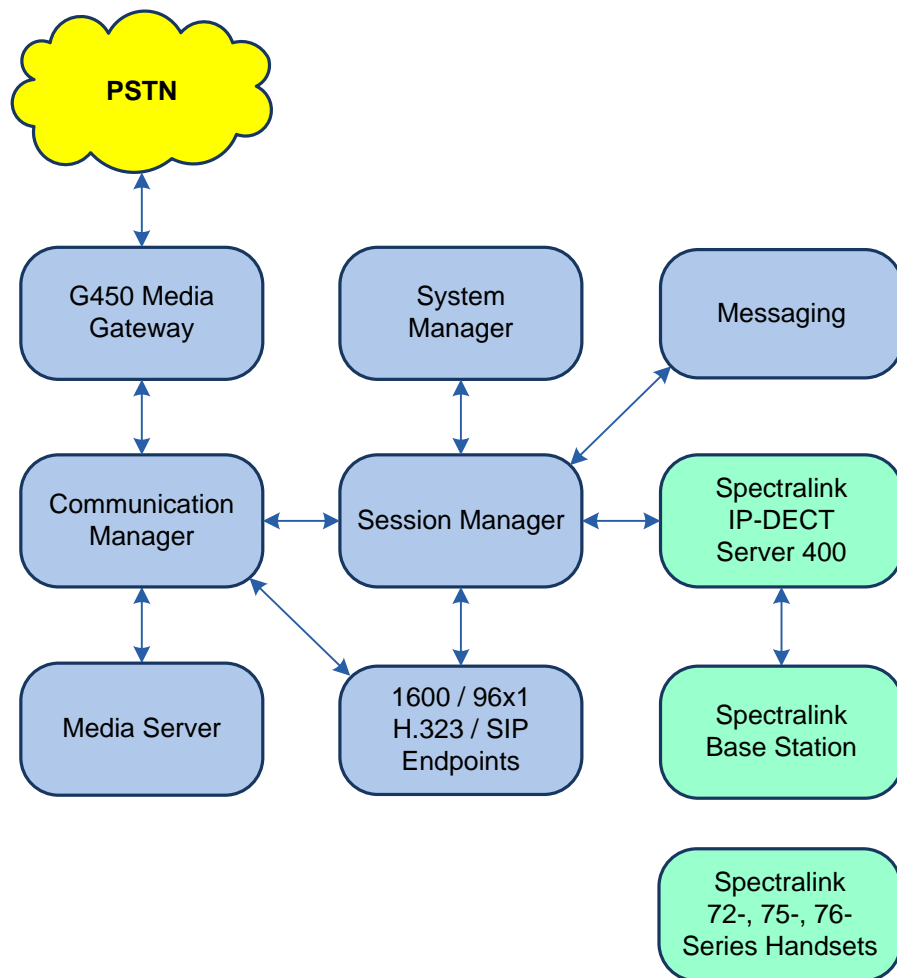


Figure 1: Avaya SIP Network with Spectralink IP-DECT Server 400, Spectralink Base Station, and Spectralink 72-, 75-, and 76-Series Handsets

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: <i>enforce-enc-srtcp</i>
1: <i>1-srtp-aescm128-hmac80</i>	
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		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? y
		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	Night Service:	
Dial Access? n			
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 String	Total Min Max	Route Pattern	Call Type
			Node Num
			ANI 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				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.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.

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.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Routing' menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

- Name:** devcon-sm
- IP Address:** 10.64.102.117
- SIP FQDN:**
- Type:** Session Manager
- Notes:**
- Location:** Thornton
- Outbound Proxy:**
- Time Zone:** America/New_York
- Minimum TLS Version:** Use Global Setting
- Credential name:**
- SIP Link Monitoring:** Use Session Manager Configuration
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration

Buttons for 'Commit' and 'Cancel' are located at the top right of the form.

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.

Listen Ports

Add Remove

4 Items Filter: Enable



<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	avaya.com	<input type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	avaya.com	<input type="checkbox"/>	
<input type="checkbox"/>	5062	TLS	avaya.com	<input type="checkbox"/>	For CM and AAM

Select : All, None

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.

AVAYA
Aura System Manager 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search   | admin

Home User Management

User Management ▾

Manage Users


Public Contacts






Shared Addresses

System Presence ACLs

Communication Profile ...

Home / Users / Manage Users

Search 

 View
  Edit
  **New**
 Duplicate
  Delete
 More Actions ▾
 Options ▾

<input type="checkbox"/>	First Name ▴ ▾	Surname ▴ ▾	Display Name ▴ ▾	Login Name ▴ ▾	SIP Handle ▾
<input type="checkbox"/>	SIP	78000	78000, SIP	78000@avaya.com	78000
<input type="checkbox"/>	SIP	78001	78001, SIP	78001@avaya.com	78001
<input type="checkbox"/>	SIP	78002	78002, SIP	78002@avaya.com	78002
<input type="checkbox"/>	Spectralink	78005	78005, Spectralink	78005@avaya.com	78005

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.

AVAYA

Aura® System Manager 8.0

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

User Management

User Management

Home / Users / Manage Users

Help ?

User Profile | Add

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Basic Info

User Provisioning Rule:

* Last Name:

Spectralink

Last Name (Latin Translation):

Spectralink

* First Name:

78005

First Name (Latin Translation):

78005

* Login Name:

78005@avaya.com

Middle Name:

Middle Name Of User

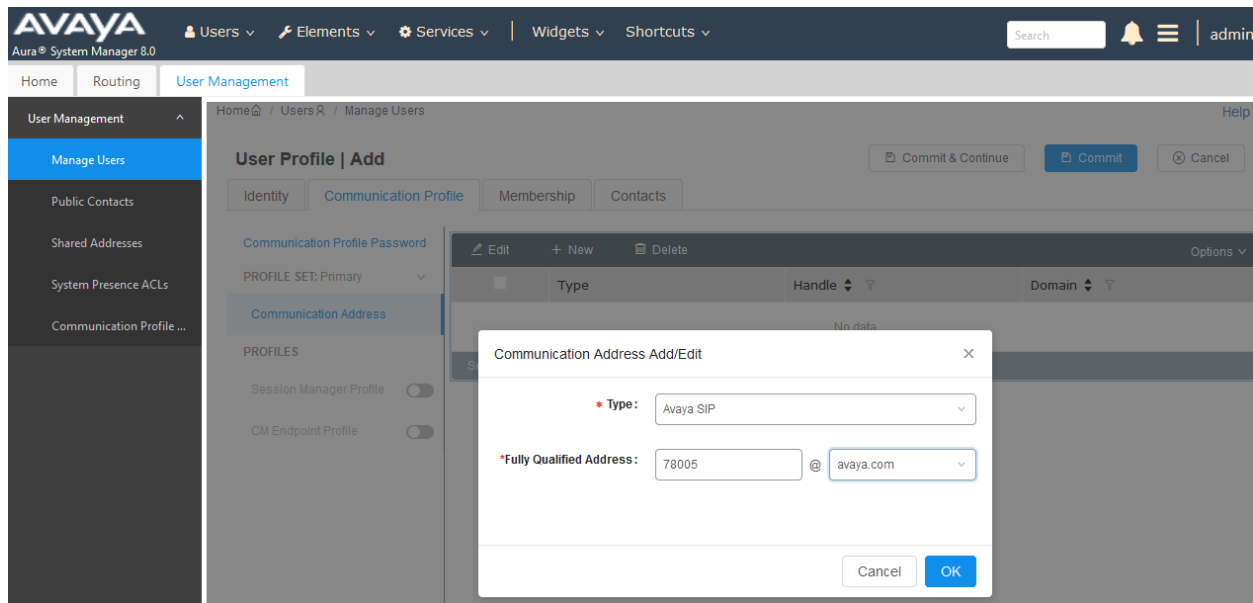
6.3.2. Communication Profile

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**.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, version information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows the 'User Management' section with options like Manage Users, Public Contacts, Shared Addresses, System Presence ACLs, and Communication Profile. The main content area is titled 'User Profile | Add' and features tabs for Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section with a dropdown for 'PROFILE SET: Primary' and a 'Communication Address' section. A modal window titled 'Comm-Profile Password' is open, containing two password input fields: 'Comm-Profile Password' and 'Re-enter Comm-Profile Password'. The 'Re-enter' field has a green checkmark icon, indicating the passwords match. The modal also includes 'Cancel' and 'OK' buttons.

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.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows 'User Management' with options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profile...'. The main content area is titled 'User Profile | Add' and has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section with 'PROFILE SET: Primary' and 'Communication Address'. Below this is a 'PROFILES' section with a 'Session Manager Profile' toggle (turned on) and a 'CM Endpoint Profile' toggle (turned off). The 'SIP Registration' section includes fields for 'Primary Session Manager' (devcon-sm), 'Secondary Session Manager' (Start typing...), and 'Survivability Server' (Start typing...). The 'Application Sequences' section includes 'Origination Sequence' (DEVCON-CM App Sequ...) and 'Termination Sequence' (DEVCON-CM App Sequ...). The 'Call Routing Settings' section is partially visible at the bottom.

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

The screenshot shows the 'Call Routing Settings' section. It includes a 'Home Location' dropdown menu set to 'Thornton' and a 'Conference Factory Set' dropdown menu set to 'Select'.

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**.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon are also present. The main navigation pane on the left shows 'User Management' with sub-options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profile ...'. The 'Manage Users' option is selected. The main content area is titled 'User Profile | Add' and contains four tabs: 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active. It features a 'Communication Profile Password' section with a dropdown for 'PROFILE SET: Primary' and a 'Communication Address' field. Below this is a 'PROFILES' section with two toggle switches: 'Session Manager Profile' (disabled) and 'CM Endpoint Profile' (enabled). The main configuration area includes fields for 'System' (devcon-cm), 'Profile Type' (Endpoint), 'Extension' (78005), 'Set Type' (9600SIP), 'Template' (9600SIP_DEFAULT_CM_8_0), 'Security Code' (Enter Security Code), 'Voice Mail Number', 'Port' (IP), 'Preferred Handle' (Select), 'Sip Trunk' (aar), 'SIP URI' (Select), 'Calculate Route Pattern' (disabled), 'Delete on Unassign from User or on Delete User' (checked), 'Allow H.323 and SIP Endpoint Dual Registration' (disabled), 'Enhanced Callr-Info display for 1-line phones' (disabled), and 'Override Endpoint Name and Localized Name' (checked). At the top right of the form are buttons for 'Commit & Continue', 'Commit', and 'Cancel'.

<p>* System <input type="text" value="devcon-cm"/></p> <p>* Template <input type="text" value="9600SIP_DEFAULT_CM_8_0"/> ▼</p> <p>* Port <input type="text" value="IP"/></p> <p>Name <input type="text"/></p>	<p>* Extension <input type="text" value="78005"/></p> <p>Set Type <input type="text" value="9600SIP"/></p> <p>Security Code <input type="text"/></p>
---	---

[Display Extension Ranges](#)

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
## MEDIAENCRYPTION (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**.

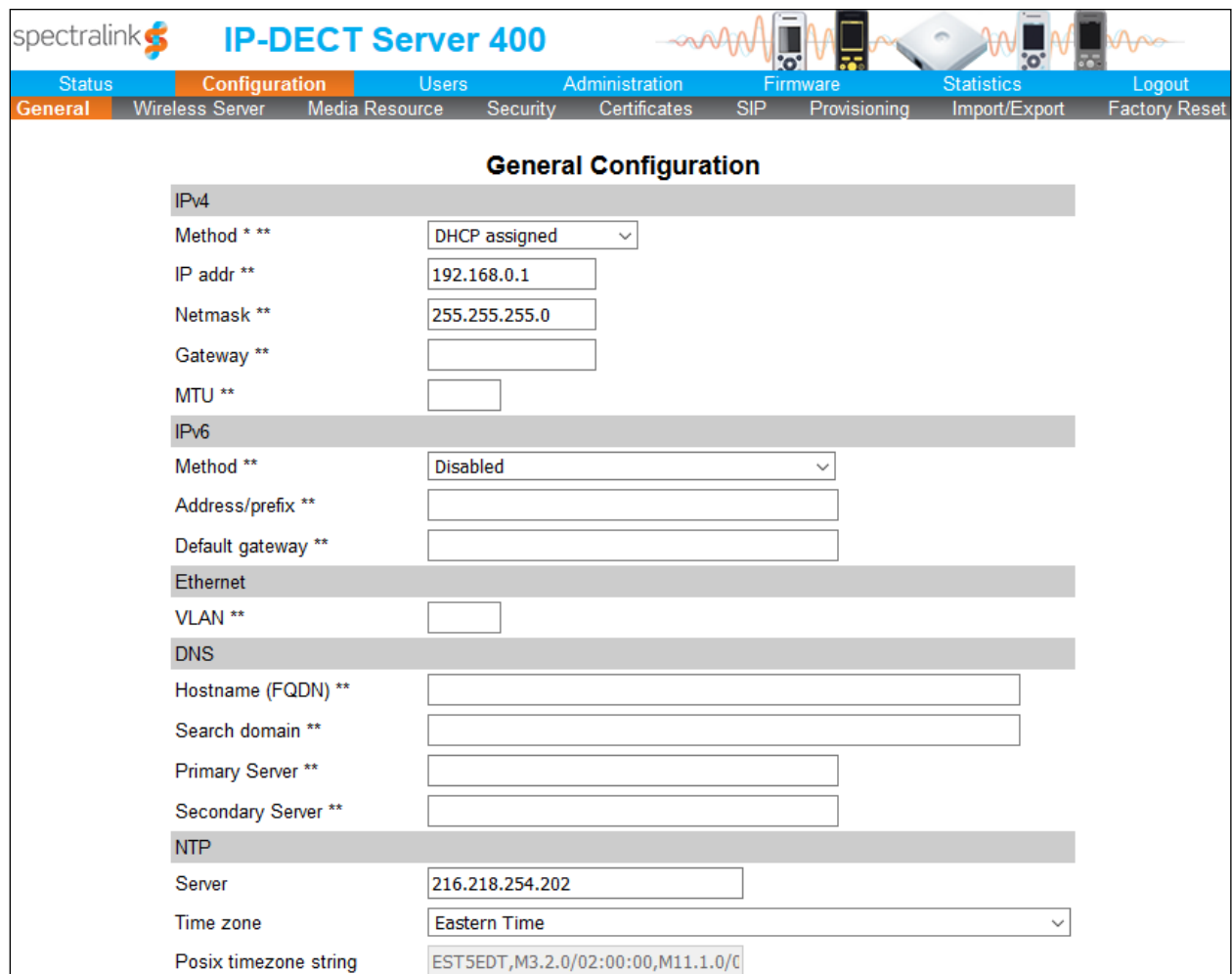


The screenshot shows the web interface for the Spectralink IP-DECT Server 400. At the top, there is a header with the Spectralink logo and the text "IP-DECT Server 400" in blue. To the right of the header is a decorative graphic featuring a blue waveform and several mobile phones. Below the header is a large white area containing the login form. The form has two input fields: "User name" and "Password". Below these fields is a "Login" button. At the bottom of the page, there is a small copyright notice: "© Spectralink Europe ApS All rights reserved."

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**.



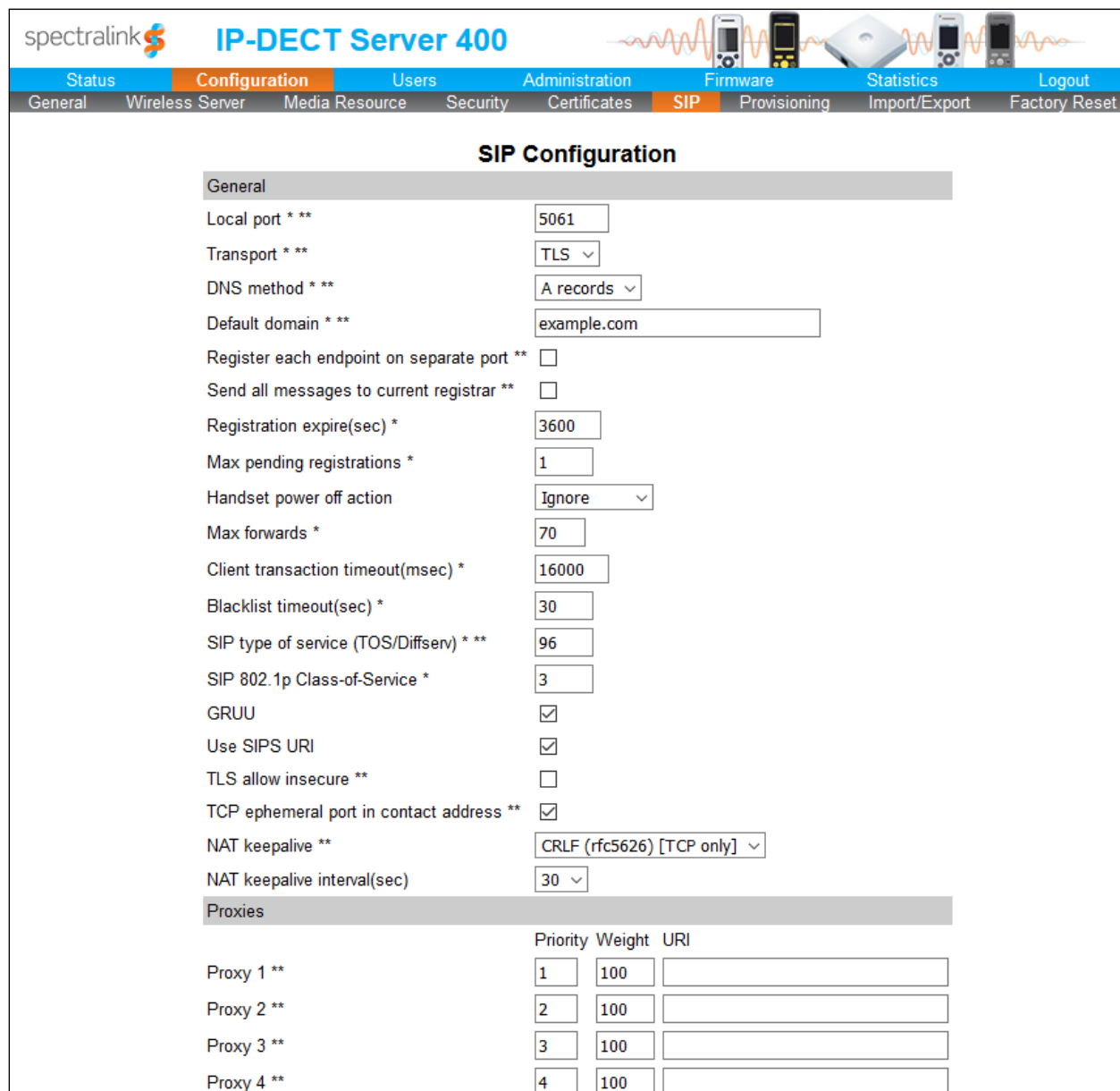
The screenshot displays the web interface for the Spectralink IP-DECT Server 400. The top navigation bar includes tabs for Status, Configuration (selected), Users, Administration, Firmware, Statistics, and Logout. Below this, a secondary bar shows sub-tabs: General (selected), Wireless Server, Media Resource, Security, Certificates, SIP, Provisioning, Import/Export, and Factory Reset. The main content area is titled "General Configuration" and contains several sections with configuration fields:

- IPv4**: Method (DHCP assigned), IP addr (192.168.0.1), Netmask (255.255.255.0), Gateway, and MTU.
- IPv6**: Method (Disabled), Address/prefix, and Default gateway.
- Ethernet**: VLAN.
- DNS**: Hostname (FQDN), Search domain, Primary Server, and Secondary Server.
- NTP**: Server (216.218.254.202), Time zone (Eastern Time), and Posix timezone string (EST5EDT,M3.2.0/02:00:00,M11.1.0/C).

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.



The screenshot displays the 'SIP Configuration' page for the Spectralink IP-DECT Server 400. The page has a navigation bar with tabs: Status, Configuration (selected), Users, Administration, Firmware, Statistics, and Logout. Below the navigation bar, there are sub-tabs: General, Wireless Server, Media Resource, Security, Certificates, SIP (selected), Provisioning, Import/Export, and Factory Reset.

The main content area is titled 'SIP Configuration' and is divided into two sections: 'General' and 'Proxies'.

General Section:

Field	Value
Local port * **	5061
Transport * **	TLS
DNS method * **	A records
Default domain * **	example.com
Register each endpoint on separate port **	<input type="checkbox"/>
Send all messages to current registrar **	<input type="checkbox"/>
Registration expire(sec) *	3600
Max pending registrations *	1
Handset power off action	Ignore
Max forwards *	70
Client transaction timeout(msec) *	16000
Blacklist timeout(sec) *	30
SIP type of service (TOS/Diffserv) * **	96
SIP 802.1p Class-of-Service *	3
GRUU	<input checked="" type="checkbox"/>
Use SIPS URI	<input checked="" type="checkbox"/>
TLS allow insecure **	<input type="checkbox"/>
TCP ephemeral port in contact address **	<input checked="" type="checkbox"/>
NAT keepalive **	CRLF (rfc5626) [TCP only]
NAT keepalive interval(sec)	30

Proxies Section:

Proxy	Priority	Weight	URI
Proxy 1 **	1	100	
Proxy 2 **	2	100	
Proxy 3 **	3	100	
Proxy 4 **	4	100	

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.



DTMF signalling	
Send as RTP (rfc2833)	<input checked="" type="checkbox"/>
Offered rfc2833 payload type	96
Send as SIP INFO	<input type="checkbox"/>
Tone duration(msec) *	270
Message waiting indication	
Enable indication	<input checked="" type="checkbox"/>
Enable subscription **	<input checked="" type="checkbox"/>
Subscription expire(sec) *	3600
Media	
Packet duration(msec) *	20
Media type of service (TOS/Diffserv) *	184
Media 802.1p Class-of-Service *	5
Port range start * **	58000
Codec priority *	1: G729/8000 2: PCMU/8000 3: None 4: None 5: None 6: None
SDP answer with preferred codec	<input type="checkbox"/>
SDP answer with a single codec	<input type="checkbox"/>
Ignore SDP version	<input type="checkbox"/>
Enable media encryption (SRTP) **	<input checked="" type="checkbox"/>
Require media encryption (SRTP)	<input checked="" type="checkbox"/>
Include lifetime in SDES offers	<input type="checkbox"/>
Include MKI in SDES offers	<input type="checkbox"/>
Enable ICE	<input type="checkbox"/>
Enable TURN	<input type="checkbox"/>
TURN server	
TURN username	
TURN password	

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

Call status	
Play on-hold tone	<input checked="" type="checkbox"/>
Provide Music-on-Hold	<input type="checkbox"/>
Display status messages	<input checked="" type="checkbox"/>
# key ends overlap dialing	<input type="checkbox"/>
Call waiting	<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	
<small>*) Required field **) Require restart © Spectralink Europe ApS All rights reserved.</small>	

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.


IP-DECT Server 400


[Status](#)
[Configuration](#)
[Users](#)
[Administration](#)
[Firmware](#)
[Statistics](#)
[Logout](#)

[List Users](#)
[Import/Export](#)

User List

Overview

System ARI 10056545410 [10 2e b2 c2 00]

Users

Subscribed

Registered

Total 3 3 3

Show All entries Search:

<input type="checkbox"/>	Enabled	User	Displayname	IPEI	Handset	Firmware	Subscription	Registration	Latest activity
<input type="checkbox"/>	✓	78005	Spectralink 1	05003 0733588	Spectralink 7202	18F	✓	✓	✓
<input type="checkbox"/>	✓	78006	Spectralink 2	05003 0733345	Spectralink 7522	19B	✓	✓	✓
<input type="checkbox"/>	✓	78007	Spectralink 3	05003 0733797	Spectralink 7622	19B	✓	✓	✓

Showing 1 to 3 of 3 entries

First
Previous
1
Next
Last

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**.

The screenshot shows the 'User 78005' configuration page in the IP-DECT Server 400 web interface. The page has a top navigation bar with tabs: Status, Configuration, Users (selected), Administration, Firmware, Statistics, and Logout. Below the navigation bar are sub-tabs: List Users and Import/Export. The main content area is titled 'User 78005' and contains several sections: 'DECT device' with fields for Product name (Spectralink 7202), Model number (7202), Software part number (14225110), Item number (02600000), Firmware (18F), HW version (16A), Production Id (0027 506A 94A5 65F4), IPEI (05003 0733588), and Access code. The 'User' section has fields for Standby text (78005) and a Disabled checkbox. The 'SIP' section has fields for Username / Extension * (78005), Secondary username, Domain (10.64.102.117), Displayname (Spectralink 1), Authentication user (78005), and Authentication password (masked with dots). The 'Features' section has a field for Call forward unconditional. At the bottom are 'Save', 'Delete', and 'Cancel' buttons, and a note: '(*) Required field'.

User 78005	
DECT device	
Product name	Spectralink 7202
Model number	7202
Software part number	14225110
Item number	02600000
Firmware	18F
HW version	16A
Production Id	0027 506A 94A5 65F4
IPEI	05003 0733588
Access code	
User	
Standby text	78005
Disabled	<input type="checkbox"/>
SIP	
Username / Extension *	78005
Secondary username	
Domain	10.64.102.117
Displayname	Spectralink 1
Authentication user	78005
Authentication password	••••••••
Features	
Call forward unconditional	



Save Delete Cancel

(*) Required field

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.

spectralink IP-DECT Server 400

Status

Configuration

Users

Administration

Firmware

Statistics

Logout

General

Wireless Server

Media Resource

Security

Certificates

SIP

Provisioning

Import/Export

Factory Reset

Device certificate chain

Show

All

 entries

Search:

Subject	Validity	SHA1 fingerprint	Issuer
0013D190B040 / Spectralink Inc.	2017-05-18 - 2032-05-18	ed:60:5b:07:f0:a4:e0:dd:c6:36:e7:f4:87:46:4a:98:7d:f5:d0:ac	SpectraLink Issuing CA /
SpectraLink Issuing CA / Spectralink Inc.	2016-10-07 - 2037-12-31	39:82:0a:28:41:e7:4a:55:69:49:1e:b4:ba:c1:9b:3b:cd:98:3b:9f	SpectraLink Root CA /
SpectraLink Root CA / Spectralink Inc.	2012-07-09 - 2037-12-31	f3:92:b9:87:e9:d6:4c:a6:53:ee:8c:ef:bb:3c:a1:7f:e9:e6:83:a2	SpectraLink Root CA /

Showing 1 to 3 of 3 entries

First Previous

1

 Next Last

Host certificate chain

Remove

 Certificate file:

Browse...

 No file selected. Key file:

Browse...

 No file selected. Password:

Type: ☒ X.509 ☐ PKCS#12

Import Certificate

CA Certificates

Clear List

Restore Default List

Browse...

 No file selected.

Import List

Export List

Show

All

 entries

Search:

Common Name	Organization	SHA1 fingerprint
System Manager CA	AVAYA	49:42:a9:a4:3b:16:37:3f:4d:80:e8:c9:e8:71:c4:c3:60:5e:aa:27

Showing 1 to 1 of 1 entries

First Previous

1

 Next Last

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.

AVAYA Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Session Manager

Session Manager

Dashboard

Session Manager Ad...

Global Settings

Communication Pro...

Network Configur...

Device and Locati...

Application Confi...

System Status

SIP Entity Monit...

Managed Band...

Security Module...

SIP Firewall Status

Registration Su...

User Registrations

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

View ▾ Default Export Force Unregister AST Device Notifications: Reboot Reload ▾ Failback As of 1:40 PM Advanced Search ▾

17 Items Show 15 Filter: Enable

<input type="checkbox"/>	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered	Prim	Sec	Surv
<input type="checkbox"/>	Show	78007@avaya.com	Spectralink	78007	---	192.168.100.193	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	78000@avaya.com	SIP	78000	---	192.168.100.54	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Equinox	78040	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	78030@avaya.com	Agent	SIP	---	192.168.100.49	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	78002@avaya.com	SIP	78002	---	192.168.100.53	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	78001@avaya.com	SIP	78001	---	192.168.100.58	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	SIP	78400	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	78005@avaya.com	Spectralink	78005	---	192.168.100.193	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Select : All, None Page 1 of 2

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.

©2019 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.

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

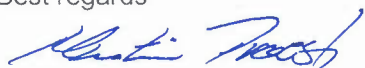
are based on the same platform and therefore:

- 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