



DevConnect Program

Application Notes for Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones register with Avaya Aura® Session Manager as SIP endpoints. The following Spectralink Versity 97 Series Wi-Fi Smartphones were used for the compliance test: Versity 9740 and Versity 9753. Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones communicate with the Avaya Aura® environment over an 802.11 wireless network.

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 Avaya DevConnect Program.

1. Introduction

These Application Notes describe the configuration steps required to integrate the Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones register with Avaya Aura® Session Manager as SIP endpoints. The following Spectralink Versity 97 Series Wi-Fi Smartphones were used for the compliance test: Versity 9740 and Versity 9753. Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones communicate with the Avaya Aura® environment over an 802.11 wireless network.

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 Versity, Avaya SIP / H.323 deskphones, and the PSTN, and exercising basic telephony features, such as hold, mute, transfer and conference. Additional telephony features, such as call forward, call coverage, call park/unpark, and call pickup were also verified using Communication Manager Feature Access Codes (FACs).

The serviceability testing focused on verifying that the Spectralink Versity came back into service after re-connecting the access point and rebooting the phones.

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 these DevConnect Application Notes 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 Versity 97 Series Enterprise Wi-Fi Smartphones used TLS/SRTP encryption features.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of Spectralink Versity with Session Manager.
- Calls between Spectralink Versity and Avaya SIP/H.323 deskphones with Direct IP Media (Shuffling) enabled and disabled.
- Calls between Spectralink Versity and the PSTN.
- Support of TLS transport protocol for secure SIP signaling.
- Support of SRTP for secure media.
- Support of G.711, G.729, and G.722 codecs.
- Proper recognition of DTMF tones.
- Basic telephony features, including hold, mute, redial, multiple calls, blind/attended transfer, attended conference, and long duration calls.
- Extended telephony features using Communication Manager FACs for Call Forward, Follow Me, Call Park/Unpark, and Call Pickup.
- Voicemail coverage, MWI support, and logging into voicemail system to retrieve voice messages.
- Use of programmable buttons on the Spectralink Versity.
- Proper system recovery after a restart of the Spectralink Versity or a reboot of the access point.

2.2. Test Results

All test cases passed.

2.3. Support

For technical support on Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones, contact Spectralink Technical Support at:

- Phone: 1-800-775-5330
- Website: <https://support.spectralink.com/s/>
- Email: technicalsupport@spectralink.com

3. Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya SIP-based network that includes the following products:

- Avaya Aura® Communication Manager with an Avaya G430 Media Gateway.
- Media resources in Avaya G430 Media Gateway and Avaya Aura® Media Server.
- Avaya Aura® Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP deskphones.
- Session Manager connected to the PSTN via Avaya Session Border Controller (SBC).
- Avaya Aura® System Manager used to configure Session Manager.
- Avaya 96x1 Series H.323 Deskphones and Avaya J100 Series SIP Deskphones.
- Spectralink Varsity Enterprise Wi-Fi Smartphones, including the Varsity 9740 and Varsity 9753.

Spectralink Varsity Enterprise Wi-Fi Smartphones registered with Session Manager and were configured as Off-PBX Stations (OPS) on Communication Manager.

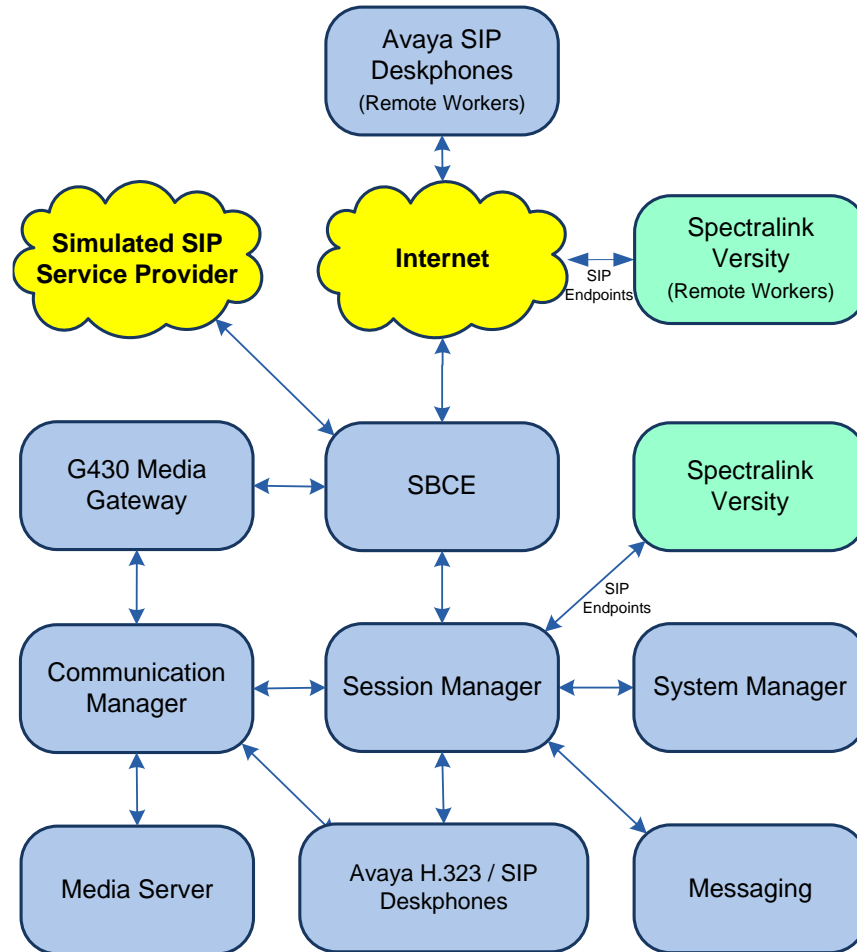


Figure 1: Avaya SIP Network with Spectralink Varsity 97 Series Enterprise Wi-Fi Smartphones

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	10.1.3.1.0-FP3SP1
Avaya G430 Media Gateway	FW 42.22.0
Avaya Aura® Media Server	10.1.0.125
Avaya Aura® System Manager	10.1.3.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.3.1.0716149 Service Pack 1
Avaya Aura® Session Manager	10.1.3.1.1013103
Avaya Session Border Controller	10.1.2.0-64-23285
Avaya Messaging	11.0.0.3204
Avaya 96x1 Series IP Deskphones	6.8.5.4.10 (H.323)
Avaya J100 Series IP Phones	4.1.1.0.7 (SIP)
Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones on Android 13	23.379684-a11 (Biz Phone Application)

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 Versity is configured through System Manager in **Section 6.2**.

5.1. Verify Communication Manager 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: V20                                     Software Package: Enterprise
Location: 2                                         System ID (SID): 1
Platform: 28                                       Module ID (MID): 1

                                USED
Platform Maximum Ports: 48000                       154
Maximum Stations: 36000                             36
Maximum XMOBILE Stations: 36000                     0
Maximum Off-PBX Telephones - EC500: 41000           0
Maximum Off-PBX Telephones - OPS: 41000           27
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.)
```

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 Avaya Media Gateway or Avaya Aura® Media Server. The **IP Network Region** form also specifies the **IP 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
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 Spectralink Versity. 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. Spectralink Versity was tested using G.711, G.722 and G.729 codecs. Specify the desired codecs in the **IP Codec Set** form as per customer requirements.

To enable SRTP, **Media Encryption** was set to *1-srtp-aescm128-hmac80* and **Encrypted SRTCP** was left at the default value of *best-effort*. Note that RTP, which would be indicated by *none* under **Media Encryption**, must not be excluded to enforce SRTP. Spectralink Versity uses encrypted SRTCP when SRTP is enabled.

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

                                IP MEDIA PARAMETERS

Codec Set: 1

  Audio      Silence      Frames      Packet
  Codec      Suppression  Per Pkt    Size (ms)
1: G.711MU      n           2          20
2:
3:
4:
5:
6:
7:

  Media Encryption                      Encrypted SRTCP: best-effort
1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3:
4:
5:
```


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 *n*.
- 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*.
- **Initial IP-IP Direct Media** was enabled.

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? y                                         Priority Video? n           Enforce SIPS URI for SRTP? n
  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 Spectralink Versity, Avaya SIP deskphones, and Avaya Messaging. 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 default values for the remaining fields.

```

add trunk-group 10                                     Page 1 of 5
                                     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

```

Page 5 of the SIP trunk group was configured as follows.

```

add trunk-group 10                                     Page 5 of 5
                                     PROTOCOL VARIATIONS
                                     Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                                     Send Transferring Party Information? n
                                     Network Call Redirection? n
                                     Send Diversion Header? n
                                     Support Request History? y
                                     Telephone Event Payload Type: 101
                                     Convert 180 to 183 for Early Media? n
                                     Always Use re-INVITE for Display Updates? n
Resend Display UPDATE Once on Receipt of 481 Response? n
                                     Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
Accept Redirect to Blank User Destination? n
Enable Q-SIP? n
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
Request URI Contents: may-have-extra-digits

```

5.5. Administer 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	Total 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 No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits	DCS/ QSIG Intw	IXC
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 Dgts	Numbering Format	LAR	
0	1	2	M	4	W	Request					
1:	y	y	y	y	y	n	n		rest	unk-unk	none
2:	y	y	y	y	y	n	n		rest		none

6. Configure Avaya Aura® Session Manager

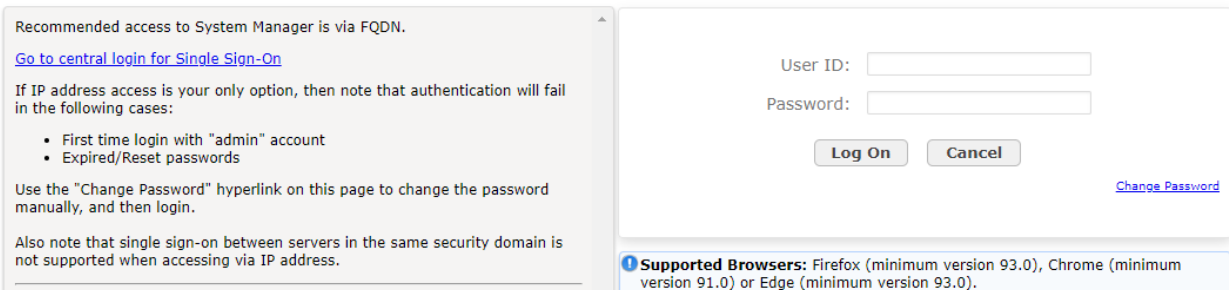
This section provides the procedure for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Set Network Transport Protocol for Spectralink Versity Enterprise Wi-Fi Smartphones
- 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 Spectralink Versity Enterprise Wi-Fi Smartphones.

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: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

6.2. Set Network Transport Protocol for Spectralink Versity Enterprise Wi-Fi Smartphones

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 10.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu items (Elements, Services, Widgets, Shortcuts). The main content area is titled "SIP Entity Details" and is divided into two sections: "General" and "Monitoring".

General Section:

- Name:** devcon-sm
- IP Address:** 10.64.102.117
- SIP FQDN:** (empty)
- Type:** Session Manager
- Notes:** (empty)
- Location:** Thornton
- Outbound Proxy:** (empty)
- Time Zone:** America/New_York
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)

Monitoring Section:

- SIP Link Monitoring:** Use Session Manager Configuration
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration

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

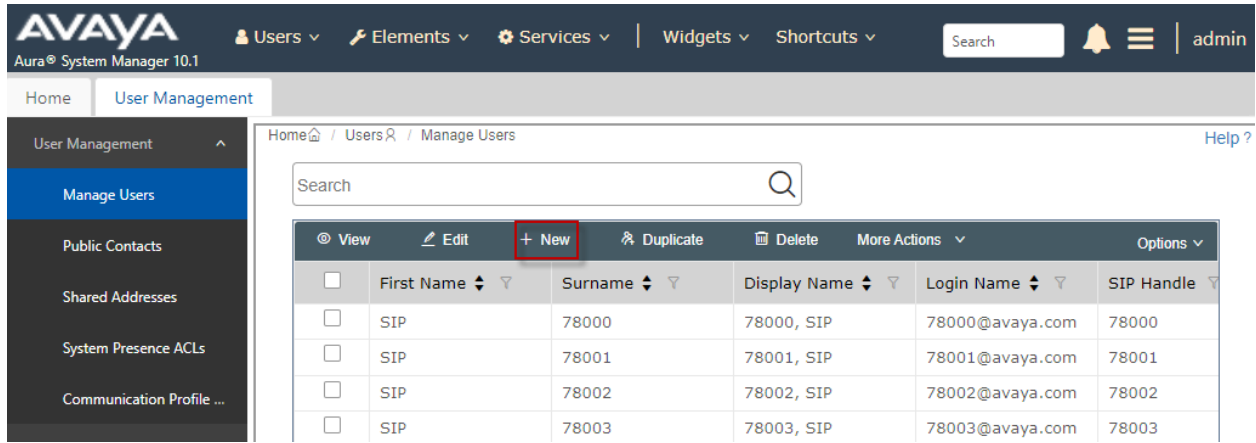
Listen Ports

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	avaya.com	<input checked="" type="checkbox"/>	

Select : All, None

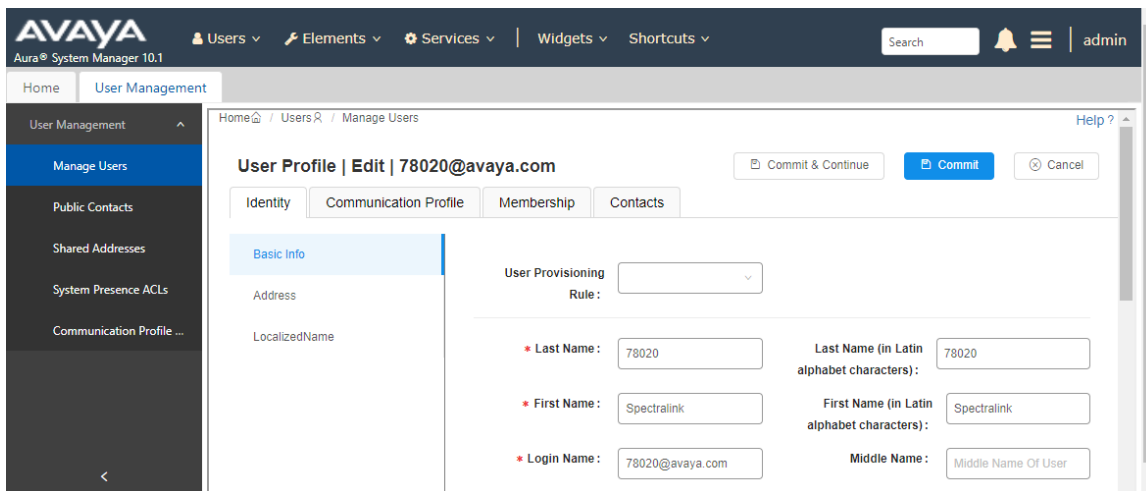
6.3. Administer SIP User

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.



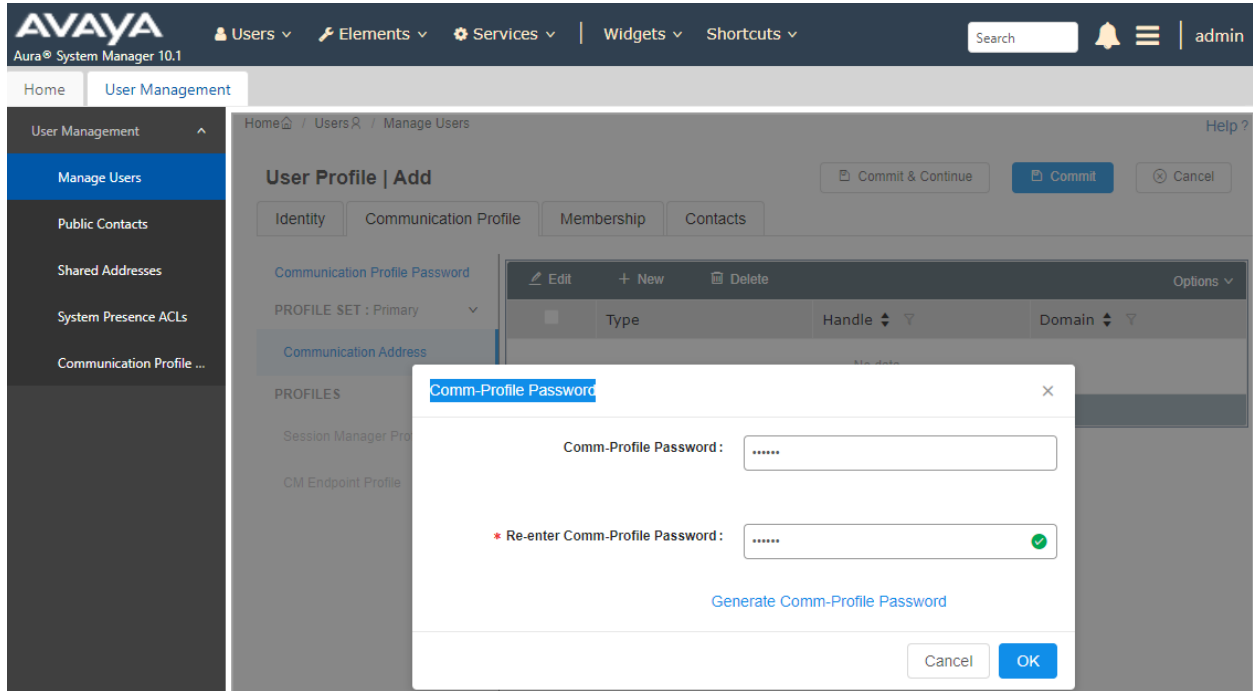
6.3.1. Identity

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



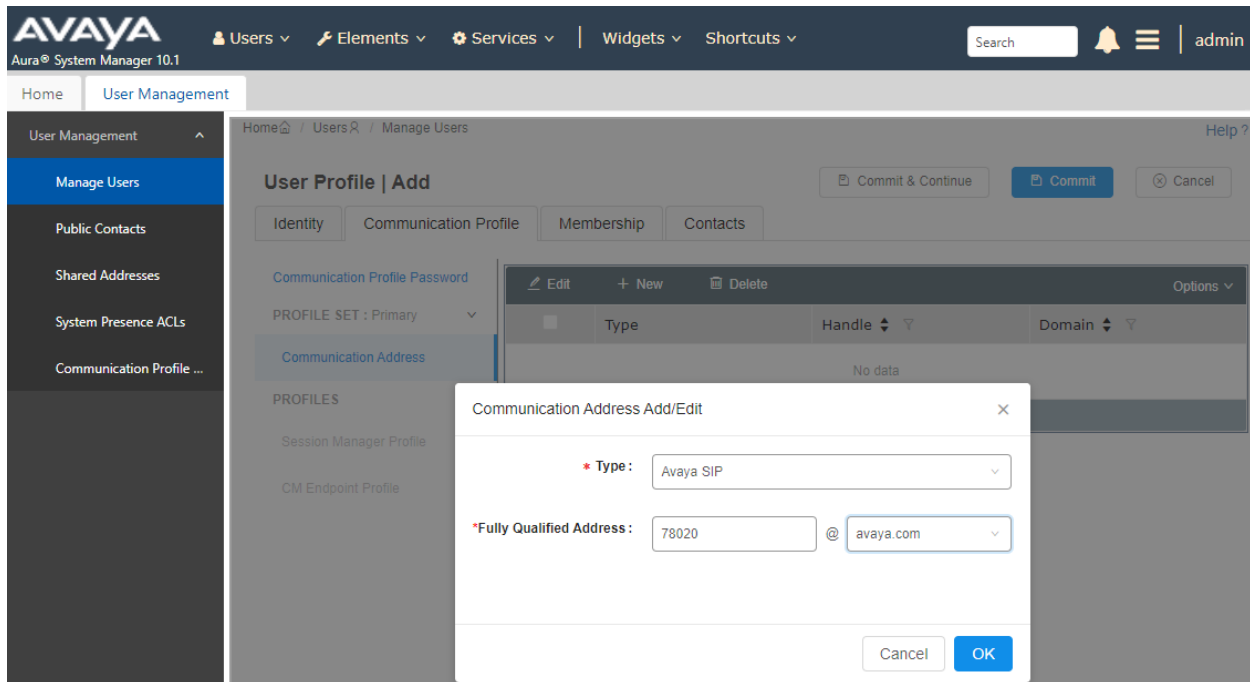
6.3.2. Communication Profile

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.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and user profile 'admin' are also visible. 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 'PROFILE SET : Primary' dropdown and a 'Communication Address' field. Below this is a 'PROFILES' section with a 'Session Manager Profile' toggle set to 'On' and a 'CM Endpoint Profile' toggle set to 'Off'. The 'SIP Registration' section contains several fields: 'Primary Session Manager' (devcon-sm), 'Secondary Session Manager' (Start typing...), 'Survivability Server' (Start typing...), 'Max. Simultaneous Devices' (Select), and a checkbox for 'Block New Registration When Maximum Penetrations Active?'. The 'Application Sequences' section includes 'Origination Sequence' and 'Termination Sequence', both set to 'DEVCON-CM App S...'. Action buttons 'Commit & Continue', 'Commit', and 'Cancel' are located at the top right of the form.

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

The screenshot shows the 'Call Routing Settings' section of the configuration page. It includes a 'Home Location' field with the value 'Thornton' and a 'Conference Factory Set' dropdown menu currently 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 *9641SIP_DEFAULT_CM_8_1*. 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 10.1 interface. The top navigation bar includes the Avaya logo, navigation menus for Users, Elements, Services, Widgets, and Shortcuts, a search bar, and a user profile for 'admin'. 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'. Below this is a 'PROFILES' section with two toggle switches: 'Session Manager Profile' (off) and 'CM Endpoint Profile' (on). The main configuration area contains several fields: 'System' (devcon-cm), 'Profile Type' (Endpoint), 'Extension' (78020), 'Set Type' (9641SIP), 'Template' (9641SIP_DEFAULT_CM_8_1), 'Security Code' (Enter Security Code), 'Port' (IP), 'Voice Mail Number', 'Preferred Handle' (Select), 'Calculate Route Pattern' (off), 'SIP URI' (Select), 'Delete on Unassign from User or on Delete User' (checked), 'Override Endpoint Name and Localized Name' (checked), and 'Allow H.323 and SIP Endpoint Dual Registration' (off). Buttons for 'Commit & Continue', 'Commit', and 'Cancel' are located at the top right of the form.

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).

Help ?

New Endpoint

Done

[Save As Template]

* System	<input type="text" value="devcon-cm"/>	* Extension	<input type="text" value="78020"/>
* Template	<input type="text" value="9641SIP_DEFAULT_CM_8_1"/>	Set Type	<input type="text" value="9641SIP"/>
* Port	<input type="text" value="IP"/>	Security Code	<input type="text"/>
Name	<input type="text"/>		

[Display Extension Ranges](#)

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
Button Assignment (B)	Profile Settings (P)	Group Membership (M)		

* Class of Restriction (COR)	<input type="text" value="1"/>	* Class Of Service (COS)	<input type="text" value="1"/>
* Emergency Location Ext	<input type="text" value="78020"/>	* Message Lamp Ext.	<input type="text" value="78020"/>
* Tenant Number	<input type="text" value="1"/>	Type of 3PCC Enabled	<input type="text" value="None"/>
* SIP Trunk	<input type="text" value="aar"/>	Coverage Path 2	<input type="text"/>
Coverage Path 1	<input type="text" value="15"/>	Localized Display Name	<input type="text"/>
Lock Message	<input type="checkbox"/>	Enable Reachability for Station Domain Control	<input type="text" value="system"/>
Multibyte Language	<input type="text" value="Not Applicable"/>		

7. Configure Avaya Session Border Controller

These Application Notes assume that the SBC is already configured to support remote workers. No additional configuration is required to support Spectralink Versity as a remote worker. However, it would be useful to show how the **Media Rule** was configured to support SRTP for calls to Spectralink Versity as a remote worker. This media rule is assigned to an **End Point Policy Group**, which in turn is assigned to **Subscriber Flows** and **Server Flows**.

The screenshot shows the Avaya Session Border Controller configuration interface. At the top, there is a navigation bar with 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. Below this is the main header 'Avaya Session Border Controller' with the AVAYA logo on the right. On the left is a navigation menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'Application Rules', 'Border Rules', 'Media Rules', 'Security Rules', 'Signaling Rules', 'Charging Rules', 'End Point Policy Groups', 'Session Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The 'Media Rules' section is selected and highlighted in red. The main content area is titled 'Media Rules: RTP-SRTP' and contains an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons, and a description field with the text 'Click here to add a description.'. Below this are four tabs: 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active and shows two sections: 'Audio Encryption' and 'Video Encryption'. The 'Audio Encryption' section has a table with the following rows: 'Preferred Formats' (SRTP_AES_CM_128_HMAC_SHA1_80, SRTP_AES_CM_128_HMAC_SHA1_32, RTP), 'Encrypted RTCP' (checked), 'MKI' (unchecked), 'Lifetime' (Any), 'Interworking' (checked), 'Symmetric Context Reset' (checked), and 'Key Change in New Offer' (unchecked). The 'Video Encryption' section has a table with the following rows: 'Preferred Formats' (RTP), 'Interworking' (checked), 'Symmetric Context Reset' (checked), and 'Key Change in New Offer' (unchecked). Below these sections is a 'Miscellaneous' section with a table containing 'Capability Negotiation' (unchecked). An 'Edit' button is located at the bottom right of the configuration area.

8. Configure Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones

This section covers the SIP configuration of the Spectralink Versity Enterprise Wi-Fi Smartphones. Refer to [5] in **Section 11** for more information on configuring Spectralink Versity. The configuration was performed via the **Biz Phone Settings** menu on the smartphone. The procedure covers the following areas:

- Configure DHCP Server
- Configure DNS Server
- Configure SIP Phone Settings

8.1. Configure DHCP Server

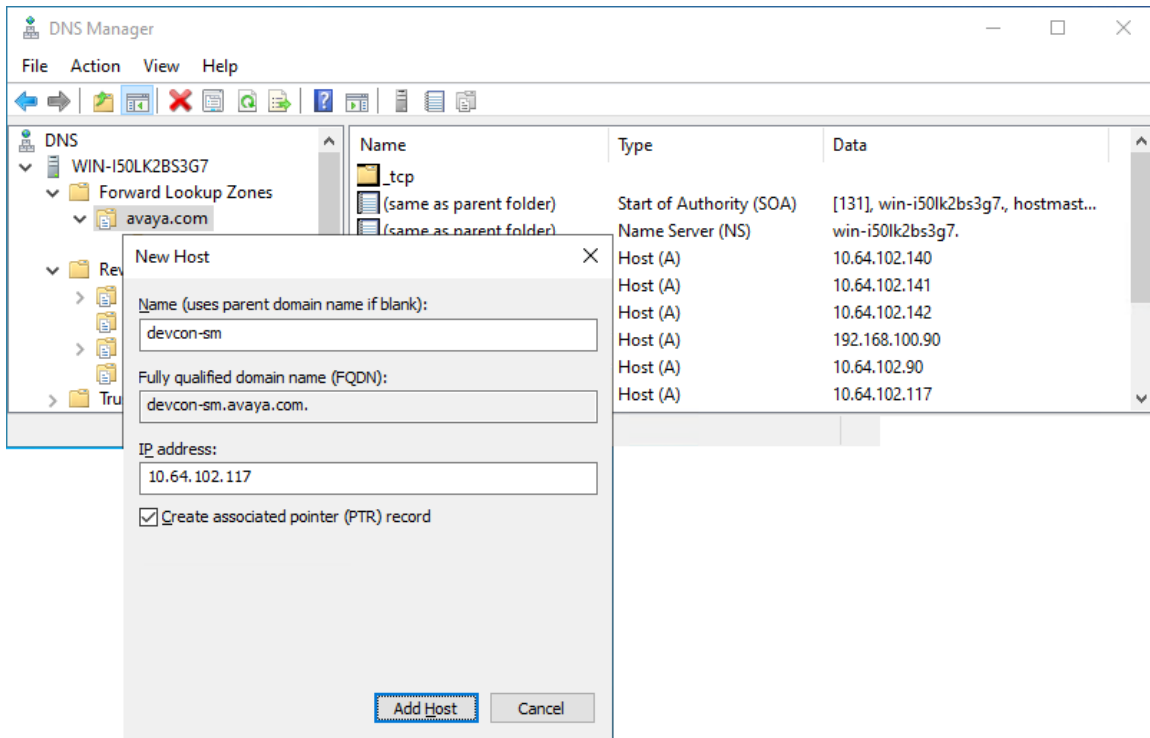
Spectralink Versity must first acquire several IP network settings before proceeding with provisioning. These settings were automatically obtained from a DHCP server. Alternatively, Spectralink Versity could be configured with static IP addresses, but for the compliance test, a DHCP server was used. In addition to obtaining IPv4 addresses from the DHCP server for each Spectralink Versity, the DHCP server also provided the following settings:

- Option 3: Default Gateway
- Option 6: DNS Server (optional)

8.2. Configure DNS Server

Spectralink Versity uses the Server Name Indication (SNI) extension in the TLS handshake (i.e., CHello message), where it would specify the FQDN of Session Manager. Note that specifying the Session Manager IP address in the SNI is not allowed. In order for the TLS handshake to complete successfully and for Spectralink Versity to use the appropriate domain name in SIP messages during call establishment, a DNS Service Location (SRV) record associated with the domain name (e.g., *avaya.com*) is required. As mentioned, the SRV record would be associated with *avaya.com* domain, which will point to the Session Manager DNS A record (e.g., *devcon-sm.avaya.com*). Spectralink Versity would configure the SIP server as *avaya.com* (SRV record), which would then be resolved to the Session Manager IP address. Note that this is only required when Spectralink Versity is registered directly to Session Manager. If Spectralink Versity is registered as a remote worker through SBC, then the SIP server can simply be configured as the SBC public IP address servicing remote workers as SNI options were not used.

On the DNS server, create a **New Host (A or AAAA)** record for Session Manager as shown below. In this example, FQDN *devcon-sm.avaya.com* maps to IP address *10.64.102.117*.



Next, create a SRV record for domain name *avaya.com* as shown below. This SRV record will resolve to Session Manager. The domain name *avaya.com* will be configured as the SIP server on Spectralink Versity in **Section 8.3**.

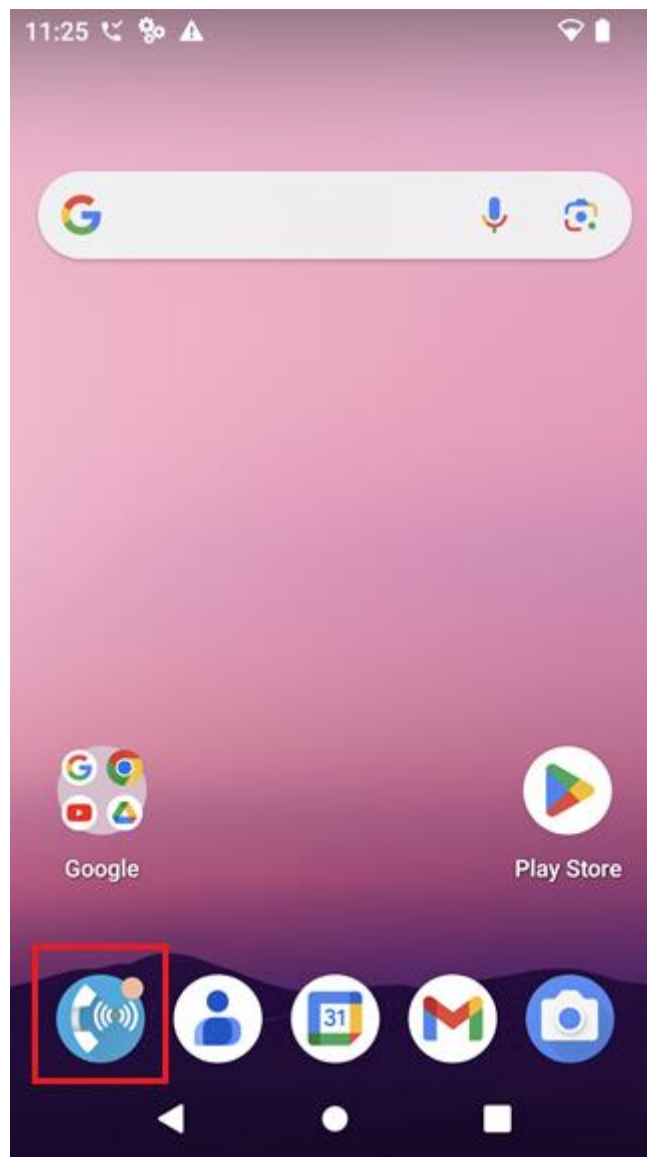
The image shows a 'New Resource Record' dialog box with the following fields and values:

- Service Location (SRV)** (Section Header)
- Domain:** avaya.com
- Service:** _sip
- Protocol:** _tcp
- Priority:** 1
- Weight:** 0
- Port number:** 5061
- Host offering this service:** devcon-sm.avaya.com

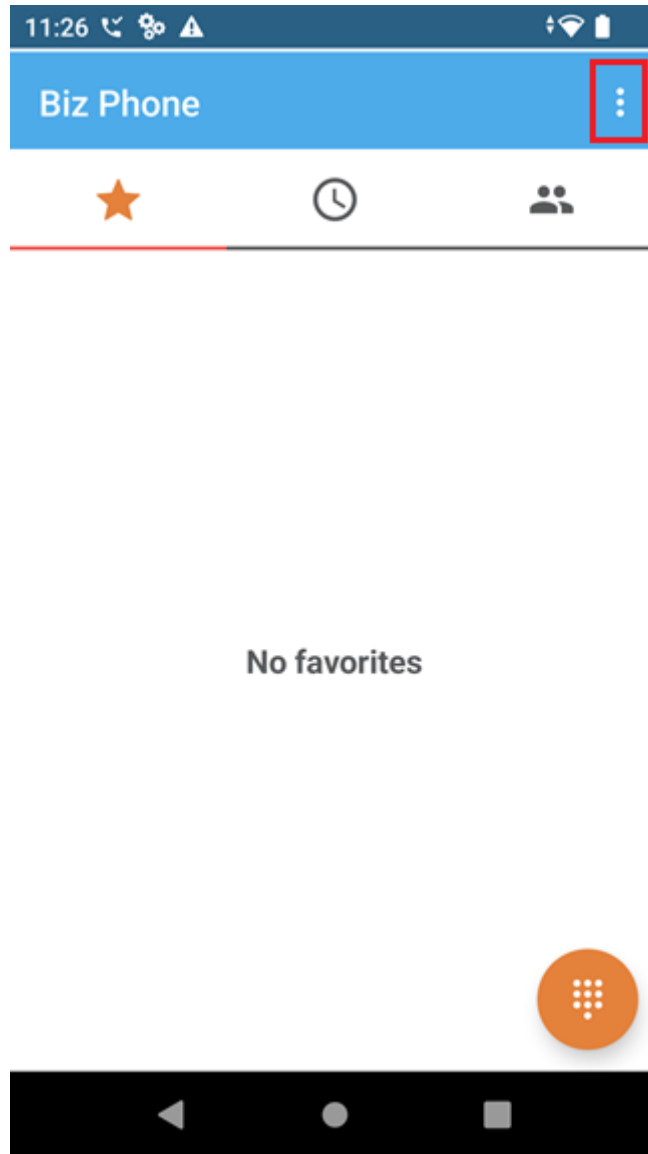
Buttons at the bottom: OK, Cancel, Help.

8.3. Configure SIP Phone Settings

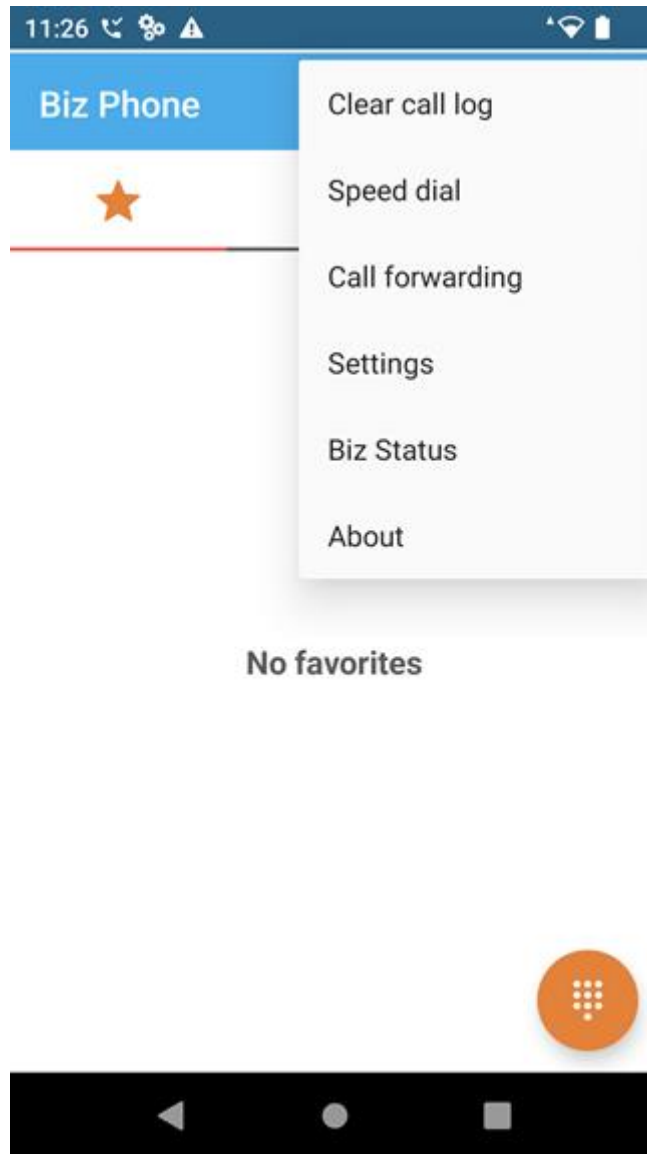
Click on the **Biz Phone** app icon on the smartphone as shown below.



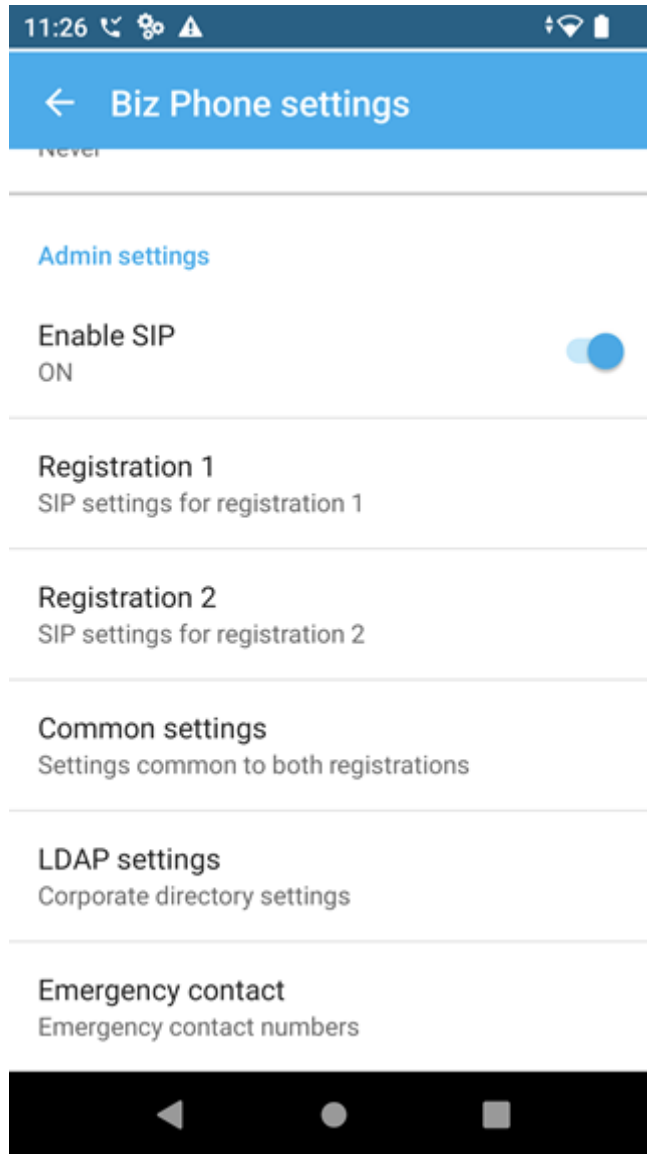
In the **Biz Phone** screen shown below, click on the overflow menu (i.e., 3 dots in upper right-hand corner).



From the menu, select **Settings** to access the **Biz Phone settings**.

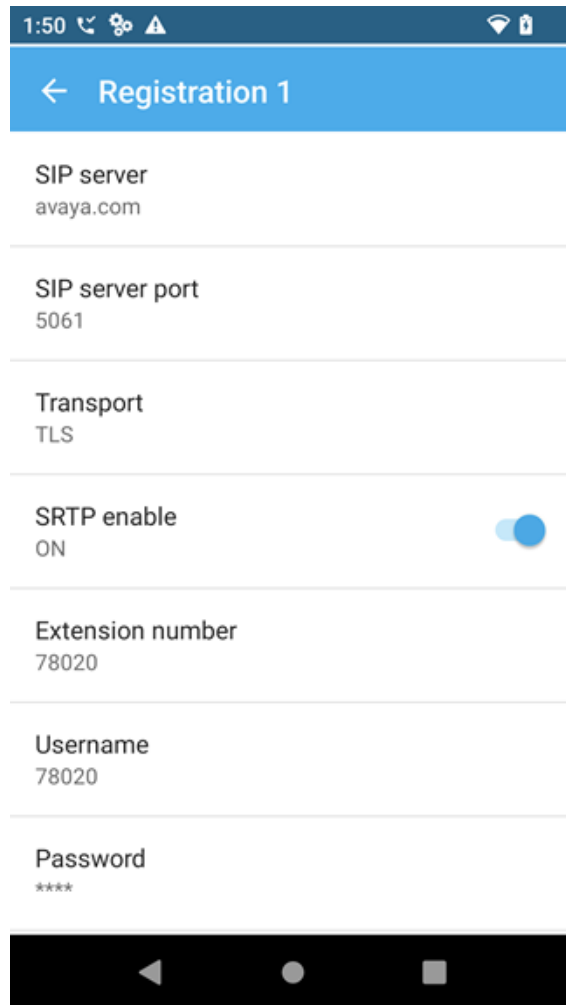


Under the **Admin settings** section, turn on the **Enable SIP** option as shown below and select the **Registration 1** option to display the SIP settings.



In the **Registration 1** screen, configure the following parameters:

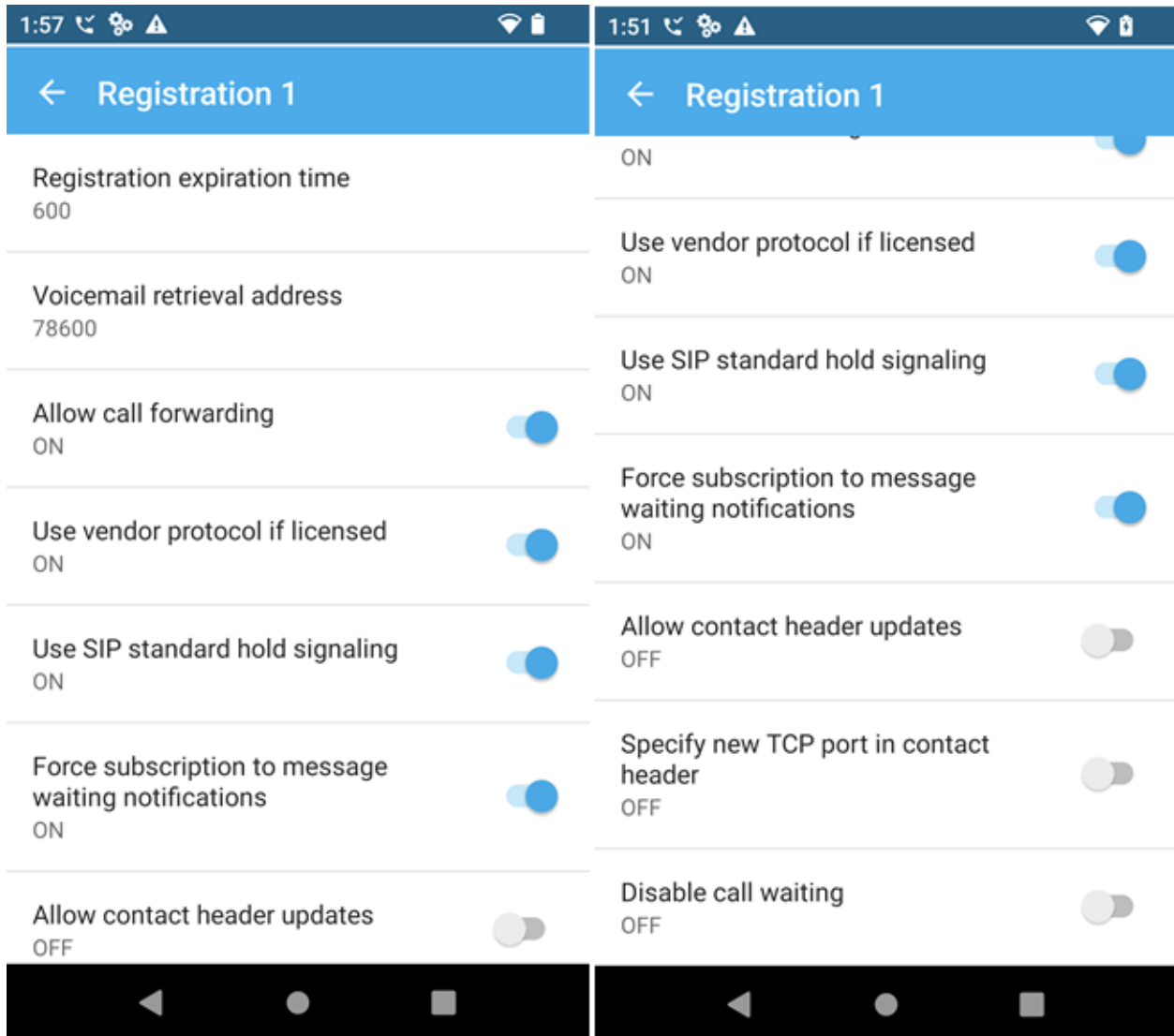
- **SIP server:** Set to DNS SRV record (e.g., *avaya.com*) that points to Session Manager DNS record (e.g., *devcon-sm.avaya.com*), if registered directly to Session Manager. If registered as a remote worker, specify the SBC public IP address (e.g., *10.64.101.102*).
- **SIP server port:** Set to appropriate SIP port (e.g., *5061*)
- **Transport:** Set to *TLS* transport protocol. Follow **Section 8.4** on installing the TLS certificate on Android.
- **SRTP enable:** Enable SRTP.
- **Extension number:** Set to the SIP extension (e.g., *78020*).
- **Username:** Set to the SIP extension (e.g., *78020*).
- **Password:** Set to the SIP password specified as the **Comm-Profile Password** in **Section 6.3.2**.



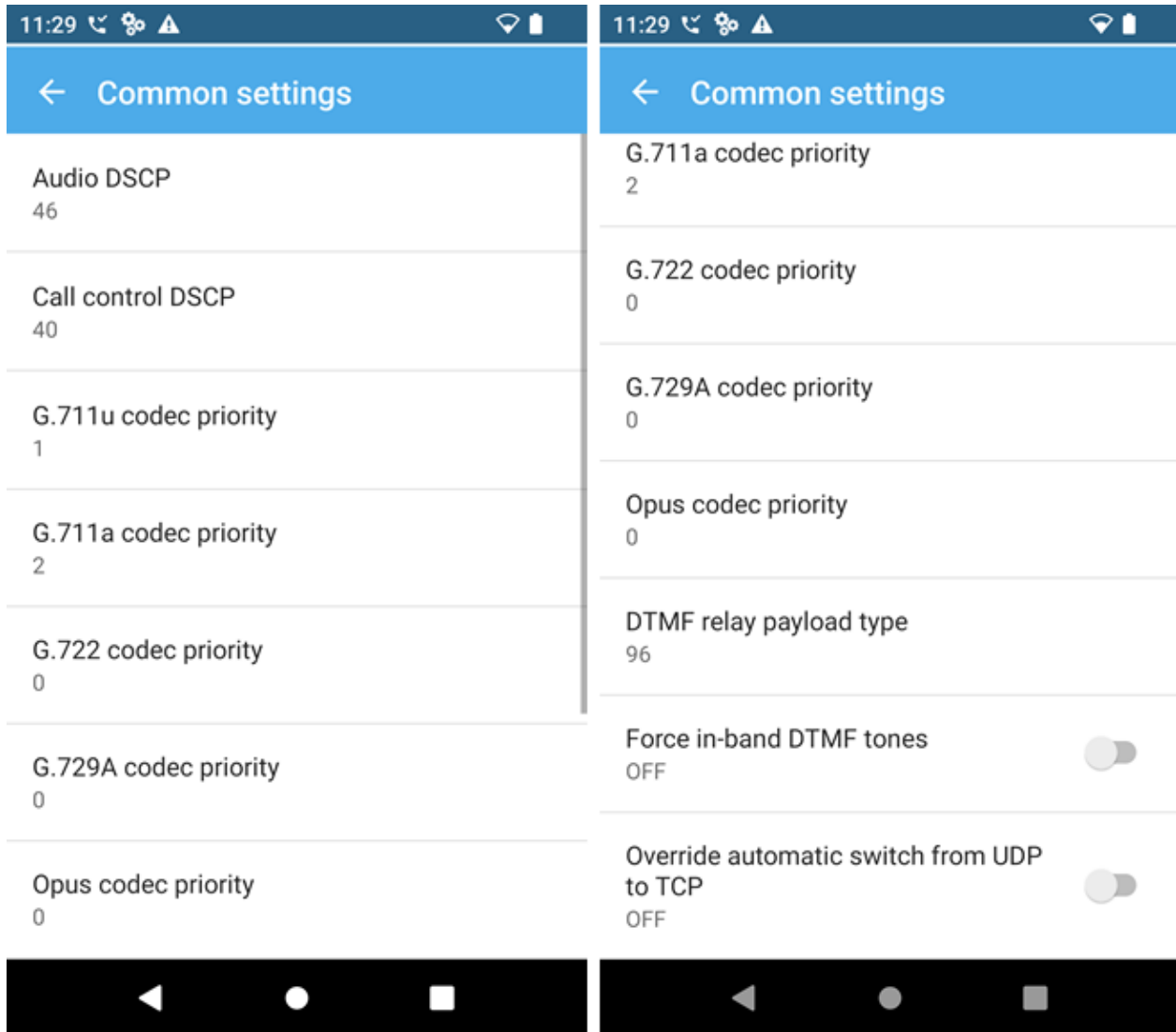
Scroll down to the bottom half of the **Registration 1** screen and configure the following parameters:

- **Registration expiration time:** Set to *600* secs to match Session Manager.
- **Voicemail retrieval address:** Set to the Messaging pilot number (e.g., *78600*).
- **Force subscription to message Waiting notifications:** Enable this option.
- **Disable call waiting:** Set to *OFF*.

Accept the default values for the remaining parameters.

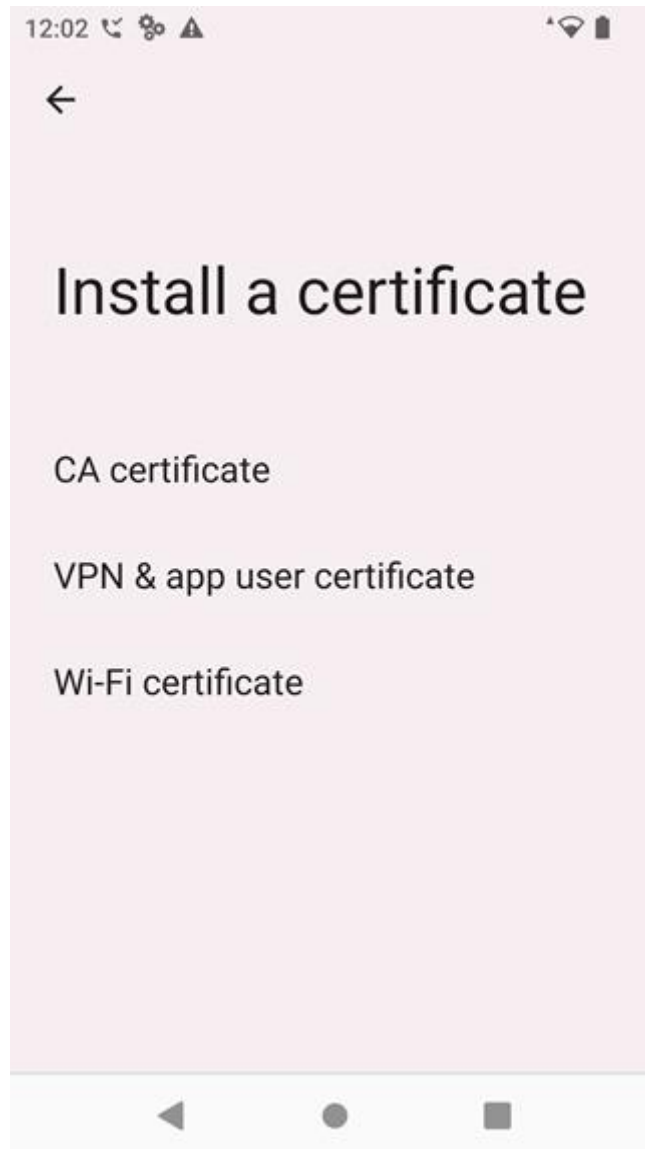


In the main screen of the **Biz Phone** application, select **Common settings** (not shown) to prioritize the codecs as needed. In this configuration, G.711 was enabled.

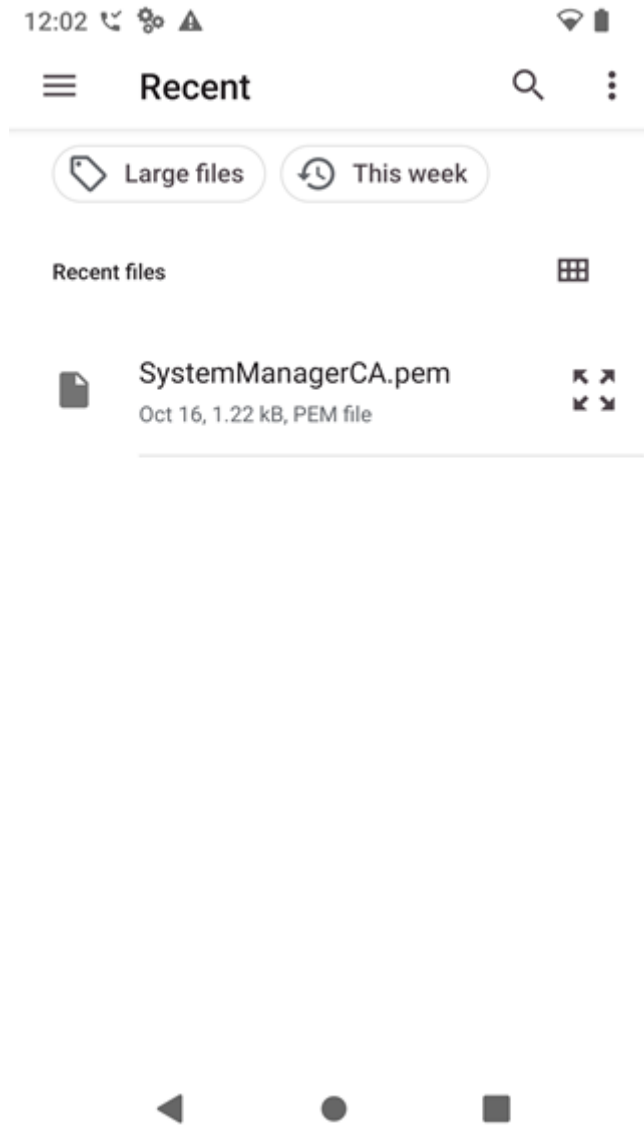


8.4. Install CA Certificate

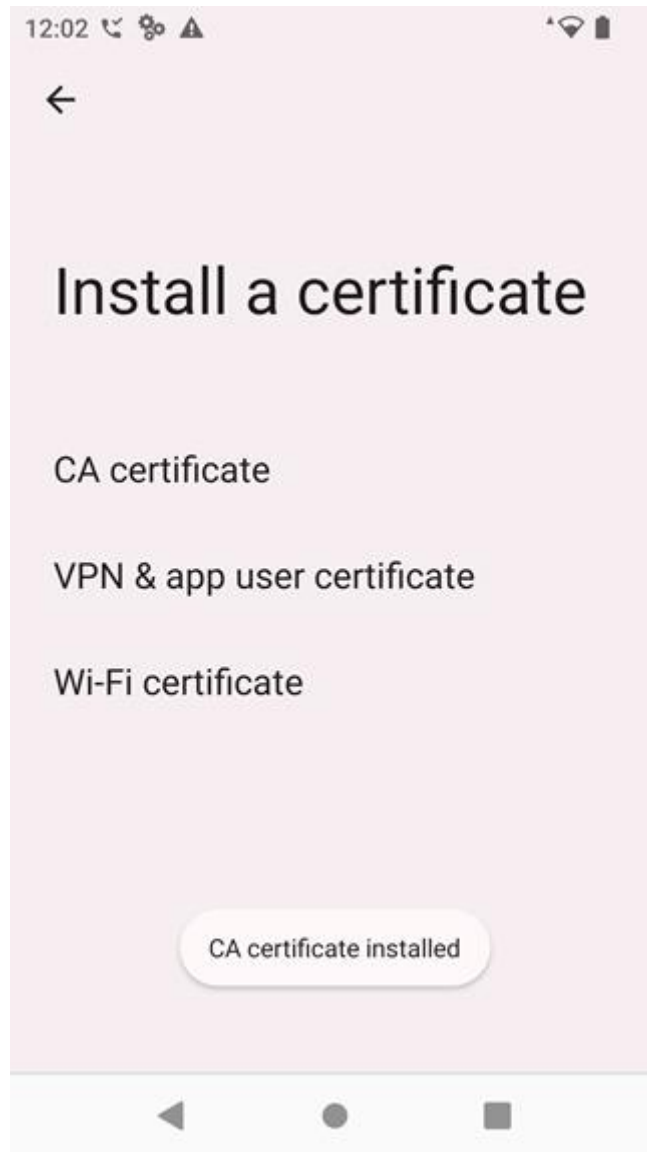
To establish secure TLS communication, a certificate must be installed that allows Versity to trust Session Manager. For the compliance test, Avaya Aura® System Manager was used as the certificate authority (CA). Download the trusted CA certificate to the Versity smartphone, called `SystemManagerCA.pem` in this example. On the Versity smartphone, navigate to **Settings** → **Security** → **More security settings** → **Encryption & credentials** → **Trusted Certificates** → **CA certificate** → **Install a Certificate** to display the following screen. Click on **CA certificate**.



The downloaded files, including the CA certificate, should be displayed. Click on the CA certificate to install it.



The following screen indicates that the CA certificate was installed.



9. Verification Steps

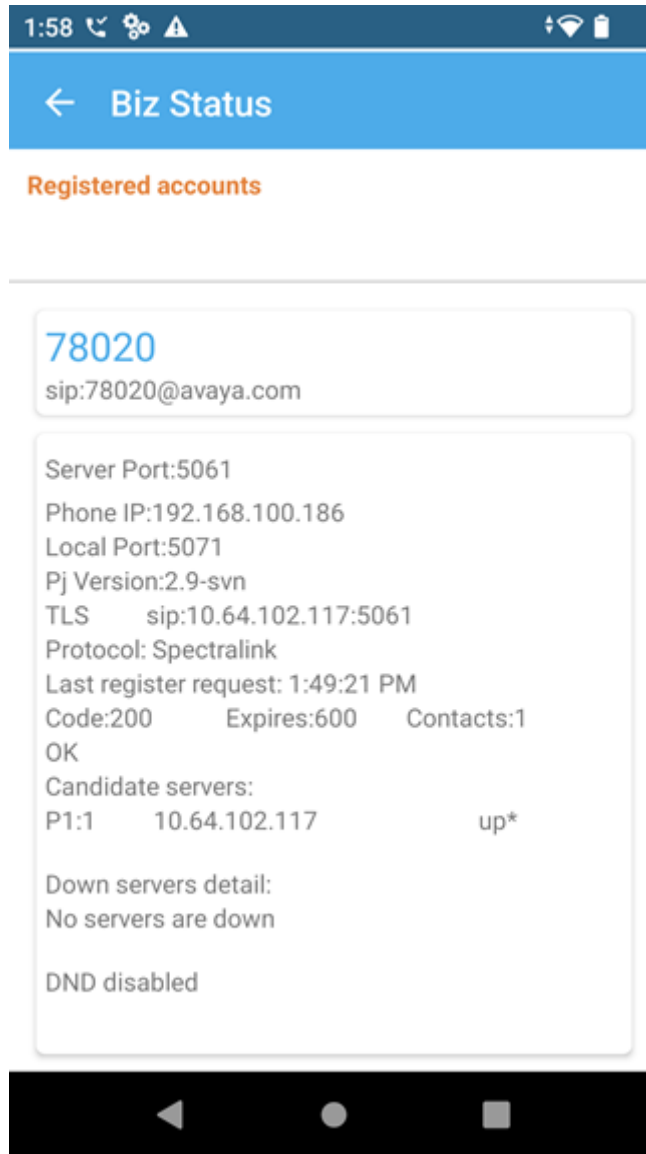
This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones.

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

The screenshot shows the Avaya Aura System Manager 10.1 interface. The main content area is titled "User Registrations" and contains a table of 27 items. The table has the following columns: Details, Address, First Name, Last Name, Actual Location, IP Address, Policy, Shared Control, Simult. Devices, AST Device, and Registered (Prim, Sec, 3rd, 4th, Surv, Visiting). The row for "Spectralink" with IP address 192.168.100.186 is highlighted in red, and its "Prim" registration checkbox is checked. The interface also includes a navigation menu on the left, a search bar at the top, and various control buttons like "View", "Export", "Force Unregister", "AST Device Notifications", "Reboot", "Reload", and "Fallback".

Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered					
										Prim	Sec	3rd	4th	Surv	Visiting
<input type="checkbox"/>	...	78400	Talkaphone	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	...	SIP	78000	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	...	Avtec	78010	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	...	Spectralink	78022	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	78020@avaya.com	Spectralink	78020	---	192.168.100.186	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	...	Talkaphone	78005	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	...	Vantage	78042	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	...	Workplace	78040	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	...	CU360	78043	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	...	Snom	78011	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	...	Remote	78801	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Alternatively, the registration status can also be checked on Spectralink Versity by opening the **Biz Status** application. Note that the server status on the last line indicates an *up** status.



- If Spectralink Versity is registered as a remote worker, the SBC would also provide a registration status by navigating to **Status → User Registrations**.

Device: SBCE Help

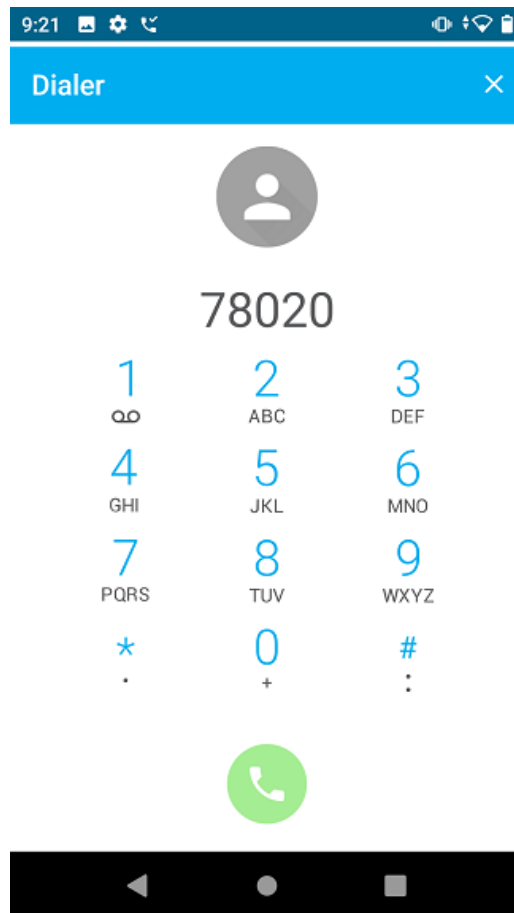
User Registrations AVAYA

Displaying entries 1 to 3 of 3.

AOR	SIP Instance	SBC Device	SM Address	Registration State
<input type="text" value="78002@avaya.com"/>	<input type="text" value="c81fead0d23d"/>	<input type="text" value="SBCE"/>	<input type="text" value="10.64.102.117(PRIMARY)"/>	REGISTERED(ACTIVE)
<input type="text" value="78020@10.64.101.102"/>	<input type="text" value="00907AB72AE5"/>	<input type="text" value="SBCE"/>	<input type="text" value="10.64.102.117(PRIMARY)"/>	REGISTERED
<input type="text" value="78050@10.64.101.102"/>	<input type="text" value="89b7f09f39f3"/>	<input type="text" value="SBCE"/>	<input type="text" value="10.64.102.117(NONE)"/>	REGISTERED

1

- Outbound calls may be placed from the Spectralink Versity Dialer shown below along with the extension.



6. Establish a call between Spectralink Versity and a local Avaya SIP 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.

```
status trunk 10/1                                     Page 2 of 3
                                                    CALL CONTROL SIGNALING
Near-end Signaling Loc: PROCN
  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 Tunned 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:  192.168.100.59                          : 2048
  Far-end:   192.168.100.186                         : 16384
Video Near:
Video Far:
Video Port:
Video Near-end Codec:                               Video Far-end Codec:
```

Page 3 indicates that SRTP is being used.

```
status trunk 10/1                                     Page 3 of 3
                                                    SRC PORT TO DEST PORT TALKPATH
src port: T000001
T000001:TX:192.168.100.186:16384/g711u/20ms/1-srtp-aescm128-hmac80
T000004:RX:192.168.100.59:2048/g711u/20ms/1-srtp-aescm128-hmac80
dst port: T000004
```

10. Conclusion

These Application Notes described the configuration steps required to integrate Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Spectralink Versity 97 Series Enterprise Wi-Fi Smartphones successfully registered with Avaya Aura® Session Manager as SIP endpoints using TLS, established calls using SRTP, and basic telephony features were verified. All feature and serviceability test cases were completed successfully.

11. Additional References

This section references the Avaya and Spectralink documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, June 2023, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 12, September 2023, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023, available at <http://support.avaya.com>.
- [4] *Administering Avaya Session Border Controller*, Release 10.1.x, Issue 5, October 2023, available at <http://support.avaya.com>.
- [5] *Spectralink Versity 97-Series User Guide*, available at <https://support.spectralink.com/s/product-documents/products?type=handsets&category=wifi>

©2023 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.