



Application Notes for Spectralink DECT Server 2500/8000 with Avaya IP Office Server Edition - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Spectralink DECT Server 2500/8000 with Avaya IP Office Server Edition and Avaya IP Office 500 V2 Expansion System. Spectralink DECT Server 2500 is a modular DECT wireless mobility solution that supports SIP telephony. The Spectralink DECT Server 2500/8000 supports external Spectralink Base Stations that control the traffic in the air from Spectralink 72-, 75-, and 76-Series Handsets and register as SIP endpoints with Avaya IP Office Server Edition. The Spectralink DECT Server 2500 provides all the benefits of the larger Spectralink DECT Server 8000 but tailored to meet the needs of smaller businesses. For this compliance test, the Spectralink DECT Server 2500 was used.

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 DECT Server 2500/8000 with Avaya IP Office Server Edition and Avaya IP Office 500 V2 Expansion System. Spectralink DECT Server 2500 is a modular DECT wireless mobility solution that supports SIP telephony. The Spectralink DECT Server 2500/8000 supports external Spectralink Base Stations that control the traffic in the air from Spectralink 72-, 75-, and 76-Series Handsets and register as SIP endpoints with Avaya IP Office Server Edition. The Spectralink DECT Server 2500 provides all the benefits of the larger Spectralink DECT Server 8000 but tailored to meet the needs of smaller businesses. For this compliance test, the Spectralink DECT Server 2500 was used.

The Spectralink DECT Server 2500 is a proxy for the Spectralink DECT handsets. On one side, it handles the SIP communication with Avaya IP Office Server Edition, and on the other side, it handles the communication with the handsets. The Spectralink Base Station enables the DECT Server 2500 to "talk" with the handsets.

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 handsets and Avaya SIP/H.323 deskphones and exercising basic telephony features, such as hold, mute, and transfer. The Spectralink handsets gained network access via an external base station connected to the Spectralink DECT Server 2500. Additional telephony features, such as call forward, follow me, call park/unpark, and call pickup were also verified using short codes on Avaya IP Office Server Edition.

The serviceability testing focused on verifying that Spectralink DECT Server 2500 came back into service after re-connecting the Ethernet cable to the IP network or rebooting the Spectralink DECT Server 2500 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 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 these Application Notes, the interface between Avaya systems and Spectralink DECT Server 2500 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 IP Office Server Edition and IP Office 500 V2 Expansion System. DECT Server 2500 controls the traffic in the air and works as the link between the Spectralink handsets and IP Office.
- Calls between Spectralink handsets and Avaya SIP/H.323 deskphones with Direct Media enabled and disabled. Direct Media was verified with Spectralink handsets and Avaya SIP deskphones only.
- Calls between Spectralink handsets and the PSTN.
- TLS transport protocol.
- Calls with TLS/SRTP enabled.
- Calls using SIPS URI.
- Support of G.711 codec.
- Proper recognition of DTMF tones.
- Basic telephony features, including hold, mute, redial, multiple calls, blind/attended transfer, and long duration calls.
- Voicemail coverage, MWI support, and logging into voicemail system to retrieve messages.
- Extended telephony features using IP Office short codes for Call Forward, Follow Me, Call Park/Unpark, and Call Pickup.
- Proper system recovery after a restart of DECT Server 2500 and Spectralink handsets and loss of IP connectivity.

2.2. Test Results

All test cases passed with the following observations noted:

- Spectralink 72-, 75-, 76-Series Handsets do not support the initiation of 3-party conference calls.
- Spectralink DECT Server 2500 does not support SDP Capability Negotiation (RFC5939) so IP Office should only offer SRTP in the SIP SDP. If RTP and SRTP are both offered, the call will not be established. In addition, when SRTP is enabled on the Spectralink DECT Server 2500, encrypted SRTCP is automatically enabled and required. Therefore, IP Office should only offer encrypted SRTCP. In other words, IP Office must enforce SRTP and encrypted SRTCP for calls involving the Spectralink DECT Server 2500.

2.3. Support

For technical support on the Spectralink DECT Server 2500/8000, 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 (North America)
+33 176774541 (France)
+49 (0) 8005889000 (Germany)
+45 76 281 281 (Rest of EMEA)
+61-2-90370834 (Asia Pacific)
- **Web:** <https://support.spectralink.com/>
- **Email:** technicalsupport@spectralink.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Spectralink DECT Server 2500, Spectralink Base Station, and Spectralink 72-, 75-, and 76- Series Handsets with Avaya IP Office Server Edition and Avaya IP Office 500 V2 Expansion System. The Spectralink DECT handsets communicated with the Spectralink DECT Server 2500 via a Spectralink Base Station. The Spectralink DECT handsets were registered to IP Office Server Edition or IP Office 500 V2 Expansion System via SIP by the Spectralink DECT Server 2500.

IP Office Server Edition connected to the PSTN via SIP and IP Office 500 V2 Expansion System connected to the PSTN via ISDN-PRI. An embedded voicemail system was used. Avaya 96x1 Series H.323 Deskphones, J100 Series SIP Deskphones, 1120e SIP Deskphones, and digital telephones were used for placing and receiving calls.

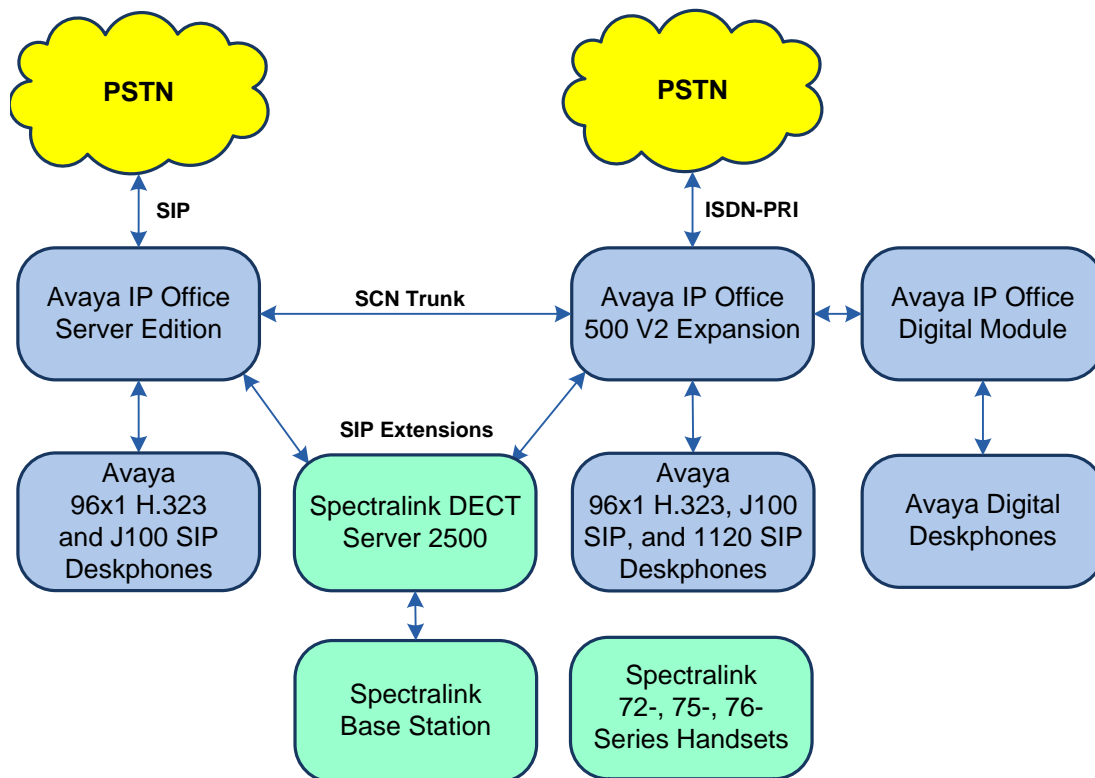


Figure 1: Avaya SIP Network with Spectralink DECT Server 2500, Spectralink Base Station, and Spectralink 72-, 75-, and 76-Series Handsets

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition	11.0.4.1.0 build 1
Avaya IP Office 500 V2 Expansion	11.0.4.1.13 build 1
Avaya 96x1 Series IP Deskphone	6.8304 (H.323)
Avaya J129/J169 SIP Deskphones	4.0.3.1.4
Avaya 1120E IP Deskphone	SIP 1120e.04.04.26.00
Spectralink DECT Server 2500	PCS19Bc
Spectralink Digital Base Station	16E
Spectralink 7202 Handset	18F
Spectralink 7522 and 7622 Handsets	19B

Note: These Application Notes also apply to the Spectralink DECT Server 8000, which uses the same firmware and SIP stack as the Spectralink DECT Server 2500. These two DECT server types differ in scalability only.

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with IP Office Server Edition in all configurations.

5. Configure Avaya IP Office Server Edition

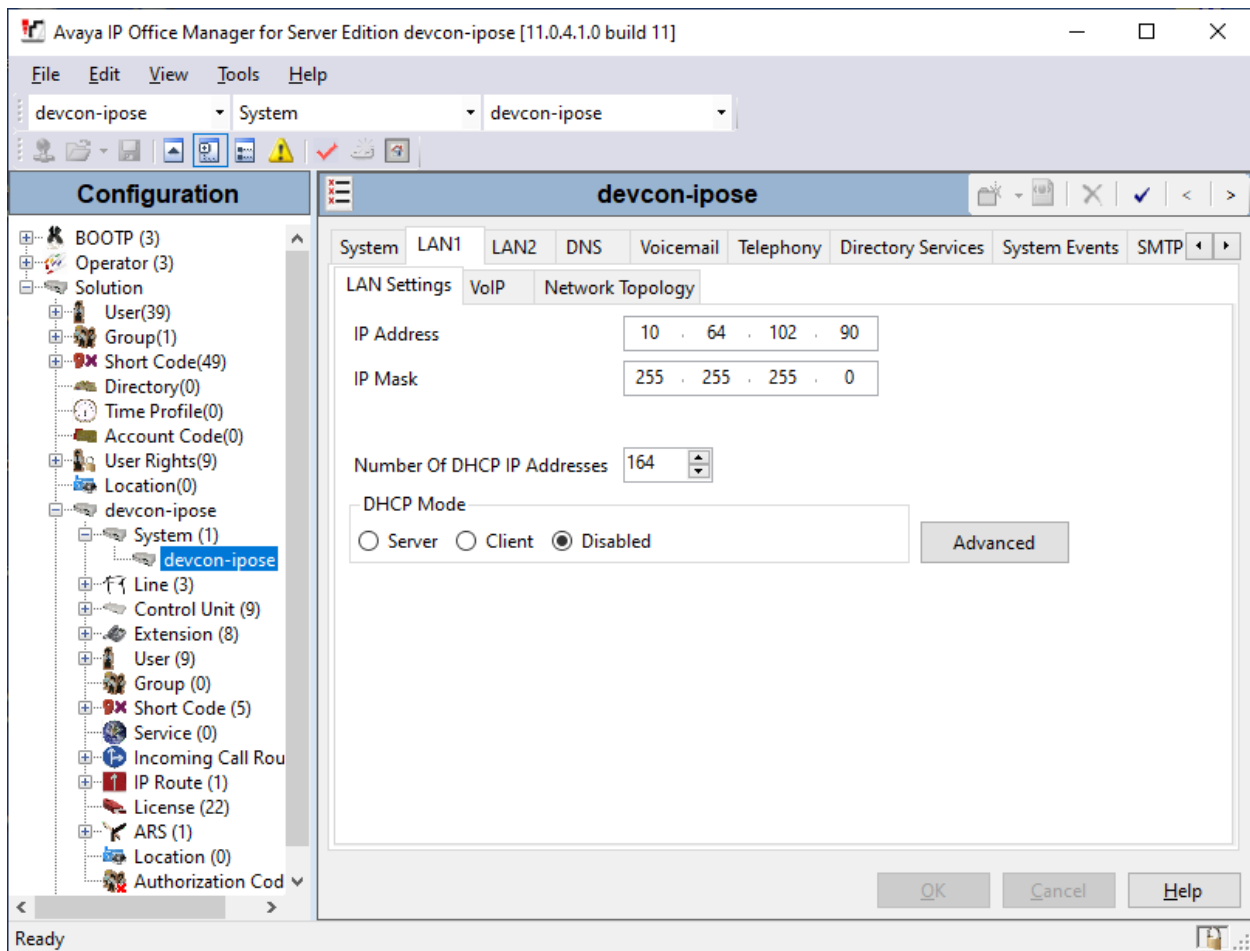
This section provides the procedures for configuring Avaya IP Office Server Edition. The procedures include the following areas:

- Obtain LAN IP address
- Administer SIP registrar
- Administer SIP extension for Spectralink handset
- Administer SIP user for Spectralink handset

Note: This section covers the configuration of Avaya IP Office Server Edition, but the configuration is the same for Avaya IP Office 500 V2 Expansion System.

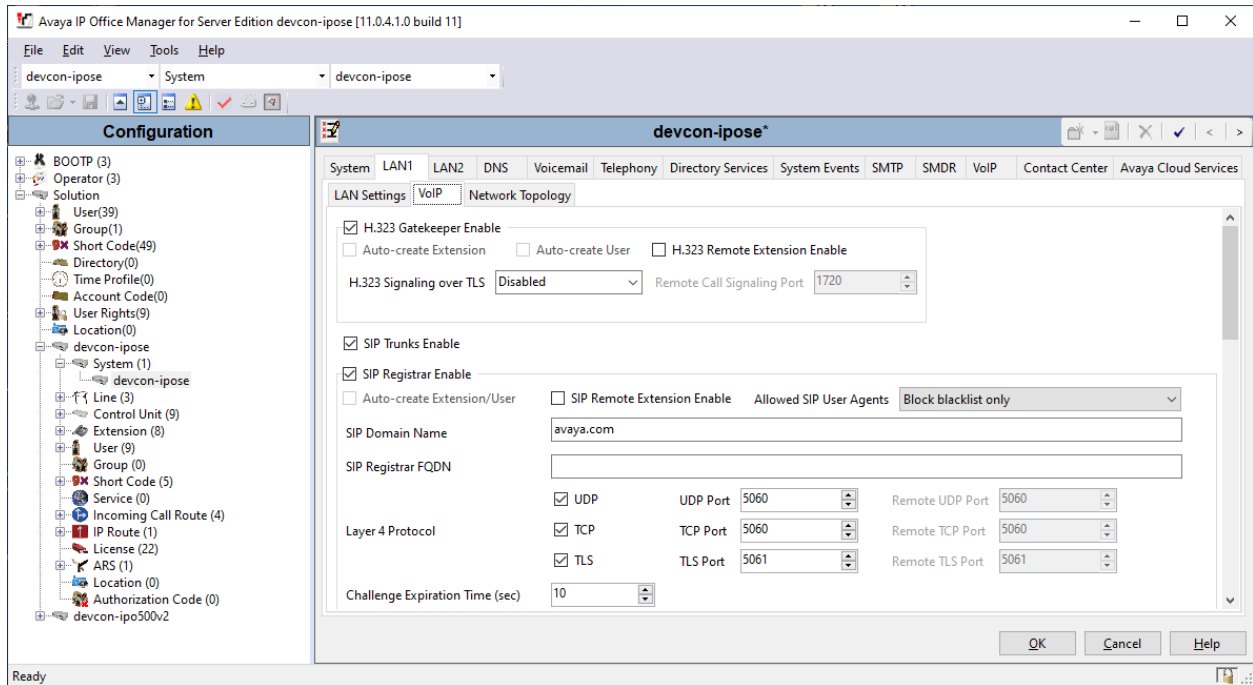
5.1. Obtain LAN IP Address

From the configuration tree in the left pane, select **System** to display the **System** screen for the IP Office Server Edition in the right pane. Select the **LAN1** tab, followed by the **LAN Settings** sub-tab in the right pane. Make a note of the **IP Address**, which will be used later to configure the DECT Server 2500.



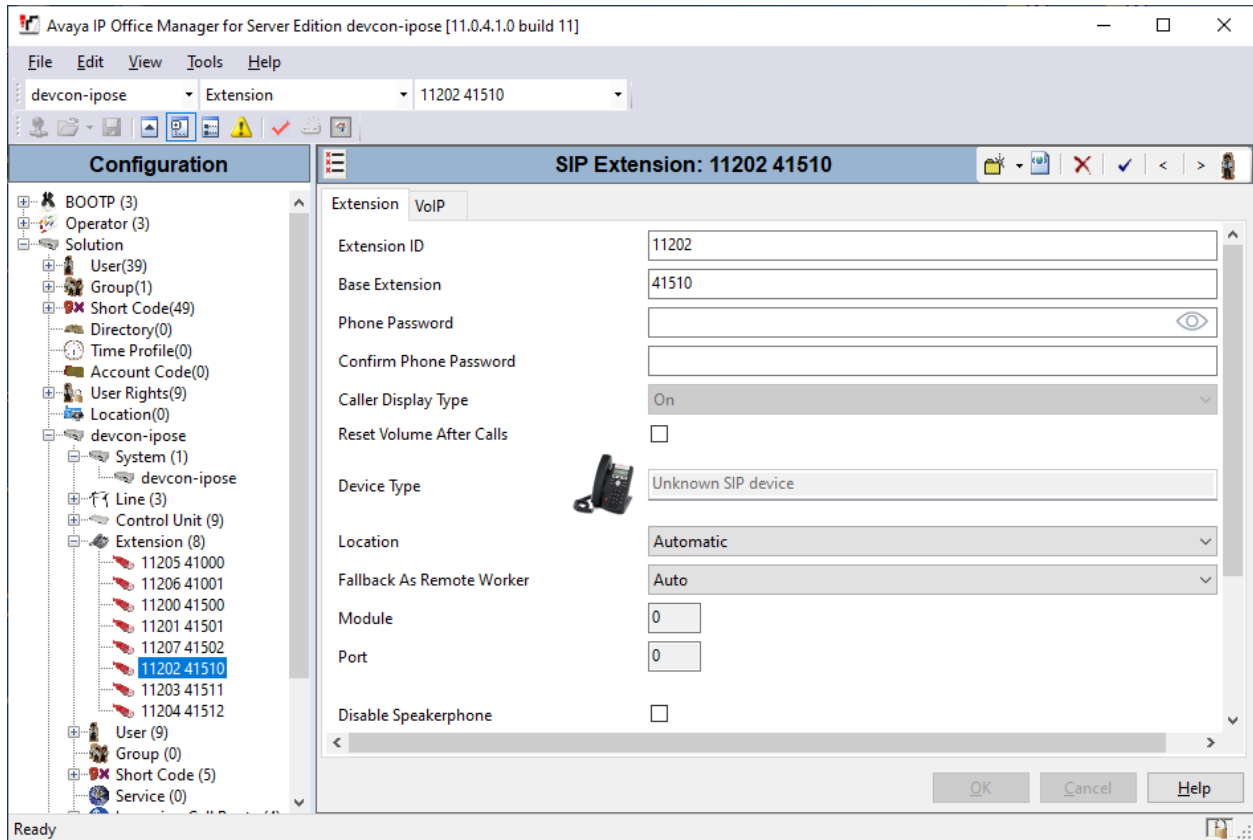
5.2. Administer SIP Registrar

Select the **VoIP** sub-tab. Ensure that **SIP Registrar Enable** is checked and enter a valid **Domain Name**. In the compliance testing, the **Domain Name** field was set to *avaya.com*. TLS transport protocol was enabled for the **Layer 4 Protocol**, which was used by the DECT Server 2500.



5.3. Administer SIP Extension for Spectralink Handsets

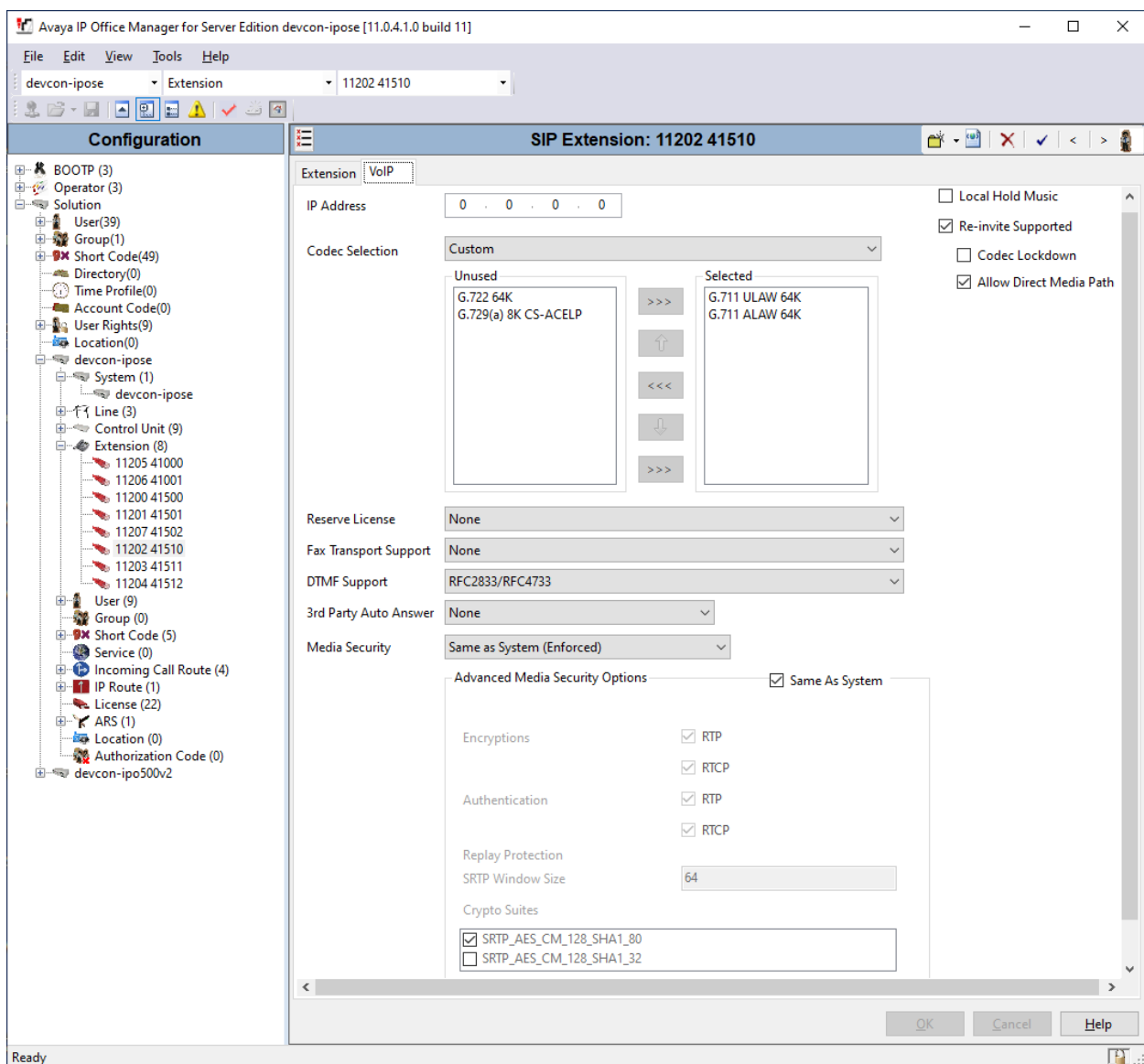
From the configuration tree in the left pane, right-click on **Extension** and select **New → SIP** from the pop-up list to add a new SIP extension. Enter the desired extension for the **Base Extension** field as shown below. In this example, Spectralink handset was assigned extension **41510**. This is the extension that the handset will use to register with IP Office Server Edition.



Select the **VoIP** tab and select the G.711 codecs to be used with the DECT Server 2500. Enable **Allow Direct Media Path** so that audio/RTP flows directly between two SIP endpoints without using media resources in Avaya IP Office Server Edition.

Media Security was enabled for SIP extensions registered by the DECT Server 2500. Since the DECT Server 2500 does not support SDP Capability Negotiation (RFC5939), IP Office Server Edition should only offer SRTP in the SIP SDP. Therefore, the **Media Security** field must be set to *Enforced*. In addition, when SRTP is enabled on the DECT Server 2500, encrypted SRTCP is required so encrypted SRTCP was enabled in the **Advanced Media Security Options** section.

Note: Refer to **APPENDIX 1** for additional notes on the Media Security settings for other Avaya devices and their impact on Direct Media.



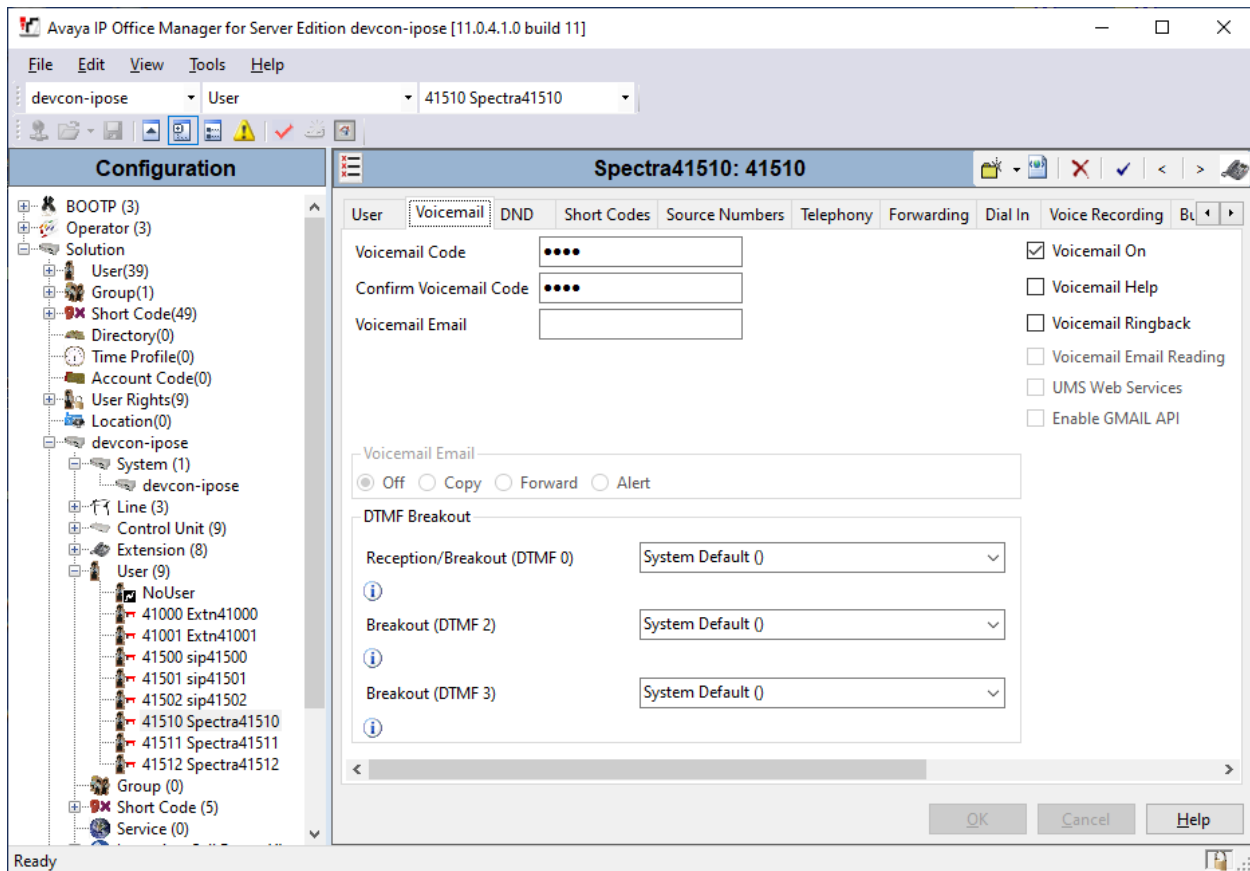
5.4. Administer SIP User for Spectralink Handsets

From the configuration tree in the left pane, right-click on **User** and select **New** from the pop-up list. Enter desired values for the **Name** and **Full Name** fields. For the **Extension** field, enter the SIP extension created above.

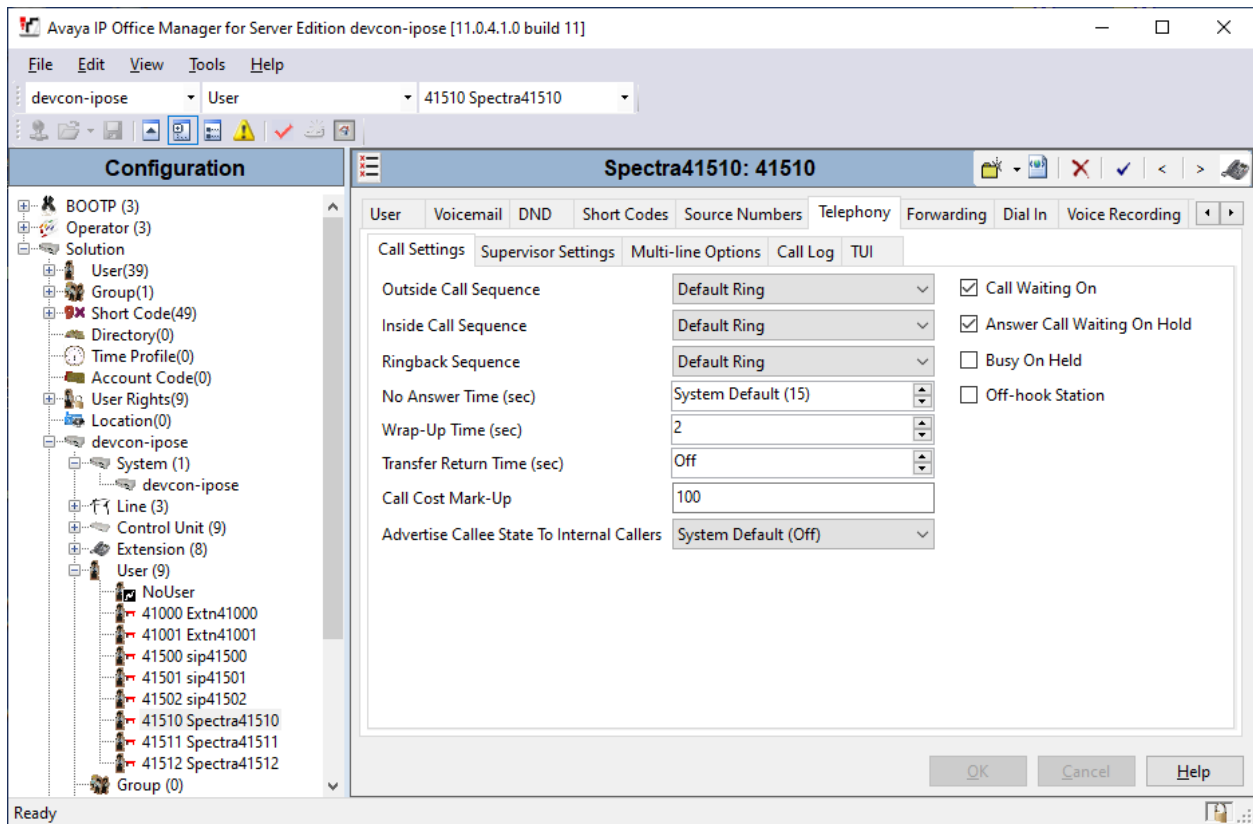
The screenshot shows the 'Avaya IP Office Manager for Server Edition devcon-ipose [11.0.4.1.0 build 11]' window. The left pane displays a configuration tree with 'User' selected. The right pane shows the configuration for 'Spectra41510: 41510'. The 'User' tab is active, showing fields for Name, Password, Confirm Password, Unique Identity, Conference PIN, Confirm Audio, Conference PIN, Account Status (Enabled), Full Name (Spectralink), Extension (41510), Email Address, Locale, Priority (5), System Phone Rights (None), Profile (Basic User), and checkboxes for Receptionist, Enable Softphone, Enable one-X Portal Services, Enable one-X TeleCommuter, Enable Remote Worker, Enable Desktop/Tablet VoIP client, Enable Mobile VoIP Client, Send Mobility Email, Web Collaboration, and Exclude From Directory. The 'Device Type' is set to 'Unknown SIP device'. The 'User Rights' field is empty. The status bar at the bottom indicates 'Ready'.

Field	Value
Name	Spectra41510
Password	
Confirm Password	
Unique Identity	
Conference PIN	
Confirm Audio	
Conference PIN	
Account Status	Enabled
Full Name	Spectralink
Extension	41510
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Basic User
Receptionist	<input type="checkbox"/>
Enable Softphone	<input type="checkbox"/>
Enable one-X Portal Services	<input type="checkbox"/>
Enable one-X TeleCommuter	<input type="checkbox"/>
Enable Remote Worker	<input type="checkbox"/>
Enable Desktop/Tablet VoIP client	<input type="checkbox"/>
Enable Mobile VoIP Client	<input type="checkbox"/>
Send Mobility Email	<input type="checkbox"/>
Web Collaboration	<input type="checkbox"/>
Exclude From Directory	<input type="checkbox"/>
Device Type	Unknown SIP device
User Rights	

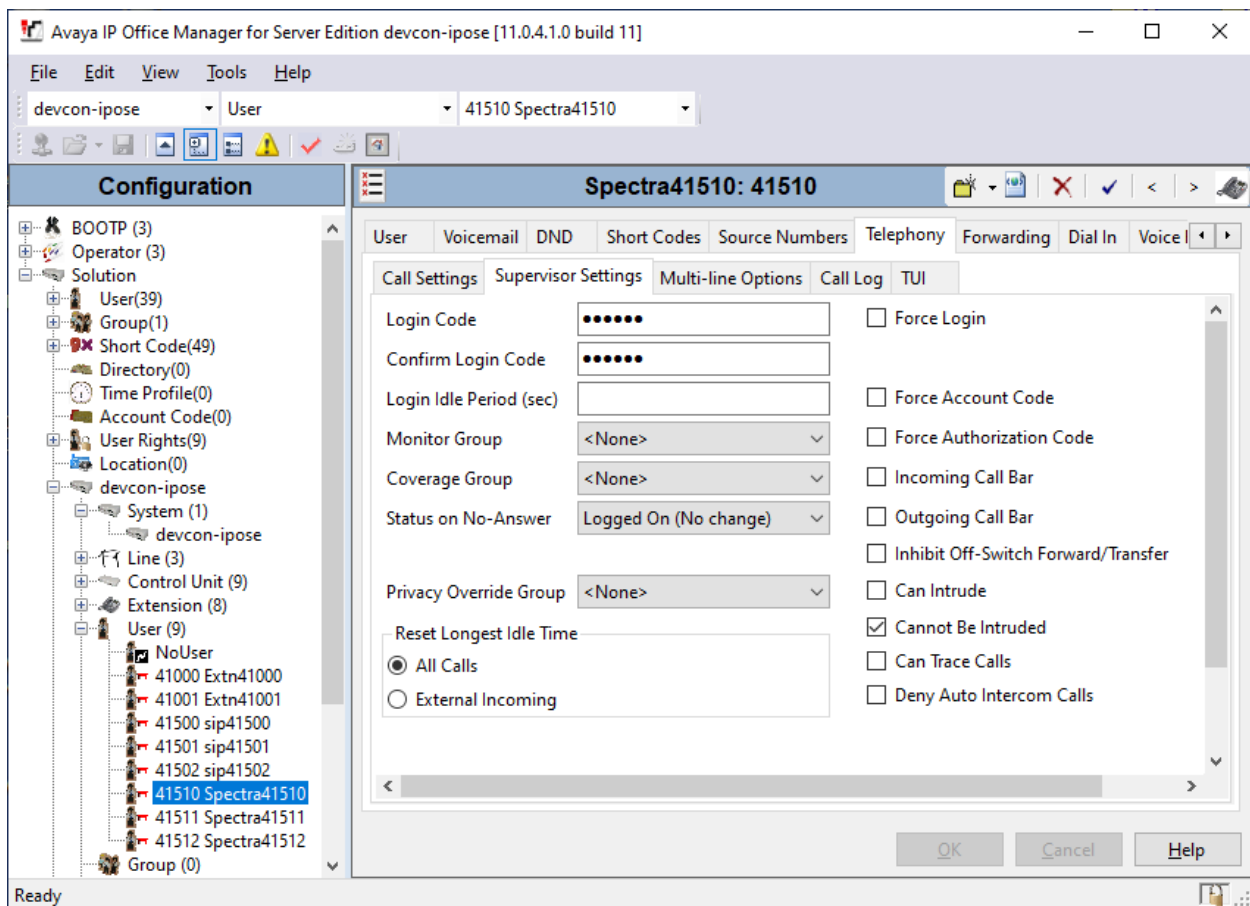
Select the **Voicemail** tab and select **Voicemail On** to enable voicemail for the Spectralink handset.



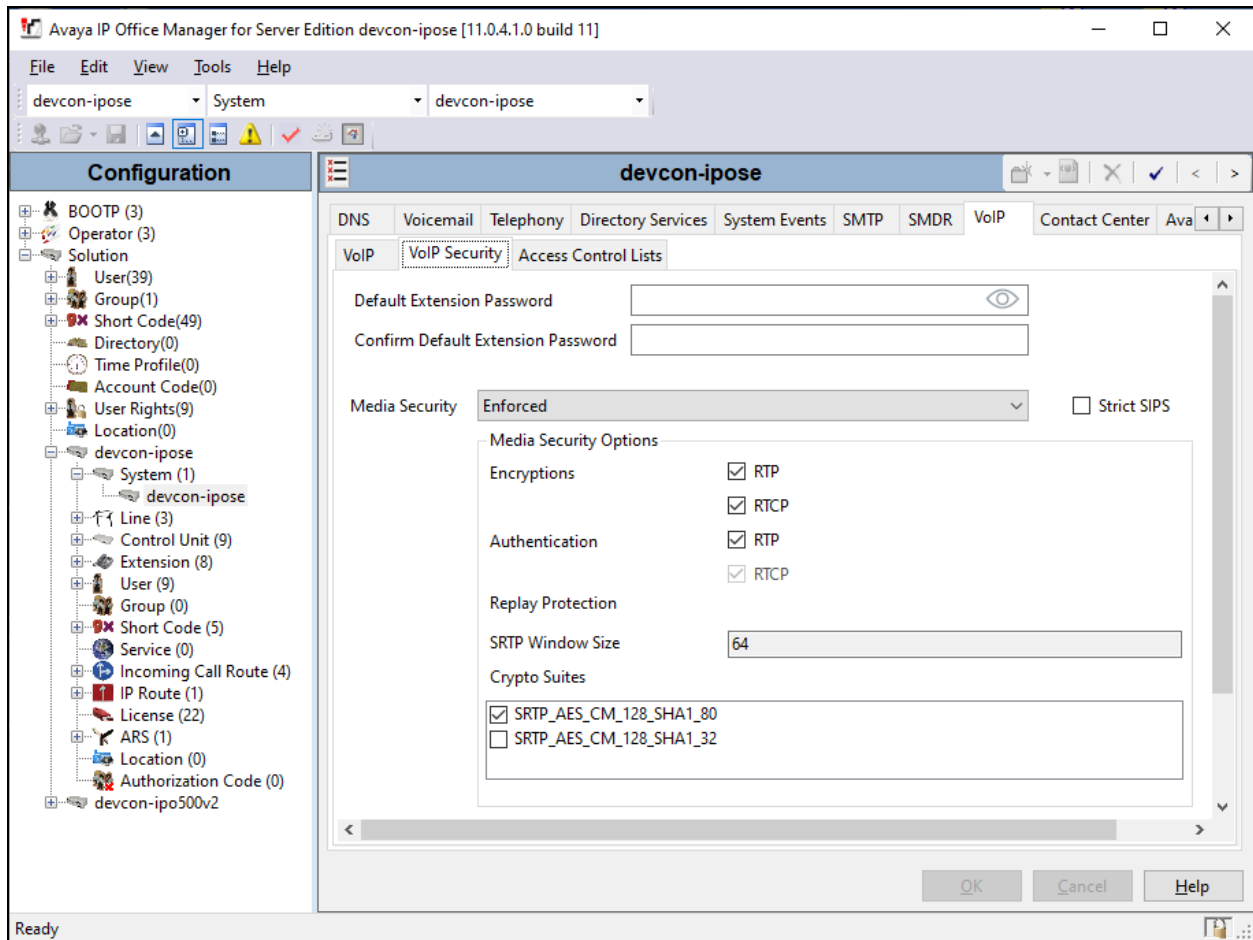
Note: Call Waiting is required to allow a secondary incoming call to the Spectralink handset; otherwise, a second incoming call would be denied.



Select the **Supervisor Settings** sub-tab and enter a desired **Login Code**. The **Login Code** is the password that will be used by the DECT Server 2500 to register the SIP extension with IP Office Server Edition.



The following screen displays the default **Media Security** settings that may be used.



6. 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 Avaya J100 Series 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 **Media Security** settings of 96x1 H.323/SIP Extensions (not shown).
- **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 SRTCP.
## 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

```

7. Configure 1120e SIP Deskphones

The 11xxsettings.txt file is used to specify certain system parameters for Avaya 1120e SIP Deskphones. To enable encrypted SRTCP, set **USE_UNENCRYPTED_SRTCP** to *NO*.

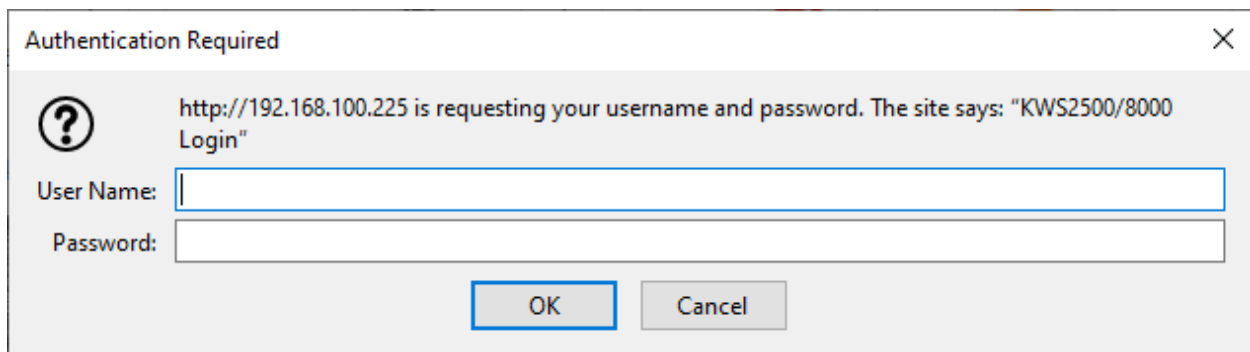
8. Configure Spectralink DECT Server 2500

This section provides the procedures for configuring Spectralink DECT Server 2500. 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 DECT Server 2500 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 DECT Server 2500. Log in using the appropriate credentials and then click **OK**.



The image shows a standard Windows-style dialog box titled "Authentication Required" with a close button (X) in the top right corner. On the left side, there is a question mark icon. To the right of the icon, the text reads: "http://192.168.100.225 is requesting your username and password. The site says: 'KWS2500/8000 Login'". Below this text are two input fields: "User Name:" followed by a text box, and "Password:" followed by a password box. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

8.2. Administer Network Settings

To configure network settings, click **Installation** and then select the **Network** tab. The Spectralink DECT server 2500 is pre-configured to use DHCP, but a static IP address may be used. However, for the compliance test, a static IP address 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 'Network Configuration' page of the Spectralink DECT Server 2500/8000. The page has a top navigation bar with tabs: Installation, Configuration, Users, Base Station, Statistics, Diagnose, Firmware, App Demo, and Reboot. Below this is a sub-navigation bar with links: Server Hardware & Firmware, Network (selected), Certificates, Licence, Company Info, E-mail Report, and Factory & Import. The main content area is titled 'Network Configuration' and includes a 'Help' button. A 'Refresh' button is located below the title. The 'Date & Time' section has a 'Manual' radio button (unselected) and a 'Use NTP Server' radio button (selected). Below these are input fields for 'Date (click to pick)' (2020-01-20) and 'Time (hh:mm:ss)' (12:36:43). A 'Display Date & Time on DECT Server' button is also present. The 'NTP Server' field contains the IP address 50.205.244.25, and the 'Time Zone' dropdown menu is set to 'Eastern Time'. A 'Save' button is at the bottom of the form.

Scroll down to the **IP Setting** section to set the IP network parameters for the DECT Server 2500 as shown below.

IP Setting	
Shelf/Card No.	1 (Primary) <input type="button" value="v"/> CPU <input type="button" value="v"/>
Use DHCP **	<input type="checkbox"/>
Address * **	192.168.100.225
Subnet Mask **	255.255.255.0
Gateway **	192.168.100.1
VLAN ID **	
IPv6 Enable **	No <input type="button" value="v"/>
Hostname (FQDN) **	
Use Automatic DNS **	<input checked="" type="checkbox"/>
HTTP Port **	80
EMD TCP/IP Port **	10000
<input type="button" value="Save"/>	

8.3. Administer SIP Settings

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

- **Local port** Specify TLS port 5061. The port may vary depending on customer's network.
- **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 of the 'DECT Server 2500/8000' web interface. The interface has a top navigation bar with tabs: Installation, Configuration (selected), Users, Base Station, Statistics, Diagnose, Firmware, App Demo, and Reboot. Below this is a sub-navigation bar with tabs: DECT Server, SIP (selected), Analogue Phone Line, Phonebook, Provisioning, and TAP. The main content area is titled 'SIP Configuration' and contains a 'General' section with the following settings:

General	
Local Port **	5061
Transport * **	TLS ▾
DNS method * **	A records ▾
Default Domain **	10.64.102.90
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 ▾

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 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	<input type="text" value="96"/>
Send as SIP INFO	<input type="checkbox"/>
Tone duration (msec) *	<input type="text" value="270"/>
Message Waiting Indication	
Enable indication	<input checked="" type="checkbox"/>
Enable subscription **	<input checked="" type="checkbox"/>
Subscription expire (sec) *	<input type="text" value="3600"/>
Media	
Packet duration (msec) *	<input type="text" value="20"/> ▾
Media type of service (TOS/Diffserv) * **	<input type="text" value="184"/>
Media 802.1p Class-of-Service *	<input type="text" value="5"/>
Port range start * **	<input type="text" value="58000"/>
Codec Priority *	<div>1: <input type="text" value="PCMU/8000"/> ▾</div> <div>2: <input type="text" value="PCMA/8000"/> ▾</div> <div>3: <input type="text" value="None"/> ▾</div> <div>4: <input type="text" value="None"/> ▾</div> <div>5: <input type="text" value="None"/> ▾</div> <div>6: <input type="text" value="None"/> ▾</div>
SDP answer with preferred codec	<input type="checkbox"/>
SDP answer with a single codec	<input type="checkbox"/>
Ignore SDP version	<input type="checkbox"/>
Enable RTP encryption **	<input checked="" type="checkbox"/>
Require RTP encryption	<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	<input type="text"/>
TURN username	<input type="text"/>
TURN password	<input type="text"/>

8.4. Add SIP Users

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

	Service Status	SIP Status	Local Number	Name	Standby Text	CFU Number	SIP Username	Line Type	Product name	SW PCS
<input type="checkbox"/>	✓	200	41510	Spectralink 7202	41510		41510	SIP line & phone	Spectralink 7202	18F
<input type="checkbox"/>	✓	200	41511	Spectralink 7622	41511		41511	SIP line & phone	Spectralink 7622	19B
<input type="checkbox"/>	✓	200	41512	Spectralink 7522	41512		41512	SIP line & phone	Spectralink 7522	19B

In the **Add new entry (phone and/or line)** page shown below, configure the following fields.

Under **DECT Device**:

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

Under **User**:

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

Add new entry (phone and/or line)

Interface

Line Type: SIP

DECT device

Model

Software part Number

Firmware

HW version

IPEI: 05003 0733588

Access Code

User

Local Number (DN): 41510

Standby Text: 41510

Disabled: ☐

Absent in single charger: ☐

Absent in multi charger: ☐

Under **SIP**:

- **Username / Extension** Set a username or extension for handset.
- **Domain** Specify the IP address of IP Office Server Edition (e.g., *10.64.102.117*).
- **Displayname** Specify a display name for the handset (e.g., *Spectralink 1*).
- **SIP Auth Username** Set to the SIP extension configured in **Section 5.3**.
- **SIP Auth Password** Enter the password configured in the **Login Code** field in **Section 5.4**.

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

SIP	
SIP Username	<input type="text" value="41510"/>
Domain	<input type="text" value="10.64.102.90"/>
Displayname	<input type="text" value="Spectralink 1"/>
SIP Auth Username	<input type="text" value="41510"/>
SIP Auth Password	<input type="text" value="123456"/>
Features	
Master Handset	<input type="checkbox"/>
CFU Number	<input type="text"/>
TX Gain [-12:12] dB	<input type="text" value="0"/>
RX Gain [-12:12] dB	<input type="text" value="0"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

8.5. Import TLS Certification

This section is required for TLS transport and covers how to import the TLS certificate into DECT Server 2500. 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 **Installation** 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.

The screenshot displays the DECT Server 2500/8000 web interface. The top navigation bar includes tabs for Installation, Configuration, Users, Base Station, Statistics, Diagnose, Firmware, App Demo, and Reboot. Below this, a secondary bar shows Server Hardware & Firmware, Network, Certificates (selected), Licence, Company Info, E-mail Report, and Factory & Import. The main content area is divided into three sections: Device certificate chain, Host certificate chain, and CA Certificates. The Device certificate chain section has a table with headers Subject, Validity, SHA1 fingerprint, and Issuer. The Host certificate chain section includes a Remove button, fields for Certificate file, Key file, and Password, a Type selector (X.509 or PKCS#12), and an Import Certificate button. Below this is another table with headers Subject, Validity, SHA1 fingerprint, and Issuer. The CA Certificates section features buttons for Clear List, Restore Default List, Export List, Import List, and a Browse... button. Below these buttons is a table with headers Common Name, Organization, and SHA1 fingerprint, showing a single entry for System Manager CA.

Subject	Validity	SHA1 fingerprint	Issuer
---------	----------	------------------	--------

Host certificate chain

Remove Certificate file: [Browse] No file selected Key file: [Browse] No file selected Password: [] Type: ☐ X.509 ☒ PKCS#12 [Import Certificate]

Subject	Validity	SHA1 fingerprint	Issuer
---------	----------	------------------	--------

CA Certificates

Clear List Restore Default List Export List Import List [Browse...] No file selected.

Common Name	Organization	SHA1 fingerprint
System Manager CA	AVAYA	ac:28:4f:d0:2b:bf:b4:dc:50:88:f4:3f:fb:80:c1:b9:05:64:89:9a

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya IP Office and Spectralink DECT Server 2500.

1. Verify that Spectralink handsets have successfully registered with IP Office. In **IP Office System Status**, navigate to the SIP extension and verify **Media Stream** is set to **SRTP**, **Layer 4 Protocol** is set to **TLS**, and **Current State** is set to **Idle**.

The screenshot displays the Avaya IP Office System Status web interface. The title bar indicates the connection is to 'devcon-ipose (10.64.102.90) - IP Office Linux PC 11.0.4.1.0 build 11'. The main header shows the Avaya logo and the page title 'IP Office System Status'. A navigation menu on the left includes links for System, Alarms (25), Extensions (7), Trunks (3), Active Calls, Resources, Voicemail, IP Networking, and Locations. The 'Extensions (7)' menu is expanded, showing a list of extensions with '41510' selected. The main content area, titled 'Extension Status', displays the configuration for extension 41510. The configuration includes fields for Extension Number, IP address, Standard Location, Registrar, Telephone Type, User-Agent SIP header, Media Stream (SRTP), Layer 4 Protocol (TLS), Current User Extension Number, Current User Name, Forwarding, Twinning, Do Not Disturb, Message Waiting, Number of New Messages, Phone Manager Type, SIP Device Features, License Reserved, Last Date and Time License Allocated, Packet Loss Fraction, Jitter, Round Trip Delay, Connection Type, Codec, and Remote Media Address. Below the configuration fields is a table showing the current state of the extension. The table has columns for Call Ref, Current State, Time in State, Calling Number or Called Number, Direction, and Other Party on Call. The current state is 'Idle' and the time in state is '02:56:29'. At the bottom of the interface, there are buttons for Trace, Trace All, Pause, Ping, Call Details, Print..., and Save As... The status bar at the bottom right shows the time '2:34:53 PM' and the status 'Online'.

Call Ref	Current State	Time in State	Calling Number or Called Number	Direction	Other Party on Call
	Idle	02:56:29			

- Alternatively, the SIP registration and DECT Subscription status may be verified by navigating to **Users → Overview** in the DECT Server 2500 web interface. These columns should contain a green checkmark as shown below.

	Service Status	DECT Subscription	SIP Status Code	Latest Activity	Local Number	Name	Line Type
<input type="checkbox"/>	✓	✓	200	Msg. call	41510	Spectralink 7202	SIP line & phone
<input type="checkbox"/>	✓	✓	200	Msg. call	41511	Spectralink 7622	SIP line & phone
<input type="checkbox"/>	✓	✓	200	Msg. call	41512	Spectralink 7522	SIP line & phone

- Establish a call between Spectralink handset and a local Avaya SIP deskphone. In **IP Office System Status**, navigate to the SIP extension and verify that the **Connection Type** is **S RTP Direct Media** as shown below.

Call Ref	Current State	Time in State	Calling Number or Called Number	Direction	Other Party on Call
553	Connected	00:00:14	40501	Outgoing	Line: 1 IP Office 192.168.100

- 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 DECT Server 2500 with Avaya IP Office Server Edition and Avaya IP Office 500 V2 Expansion System. Spectralink DECT 2500 allowed Spectralink 72-, 75-, and 76-Series Handsets to register with Avaya IP Office Server Edition 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 IP Office Platform with Manager*, Release 11.0, February 2019.
- [2] *Administering Avaya Aura® System Manager for Release 8.1.x*, Release 8.1.x, Issue 4, October 2019.
- [3] *Administering Avaya Aura® Session Manager*, Release 8.0.1, Issue 3, December 2018.
- [4] *Spectralink DECT Server 8000 and Spectralink DECT Server 2500 Configuration Guide*, 14184634 version 6.0, K016, June 2015.

APPENDIX 1: Media Security Settings

This section provides guidelines for the Media Security settings on the Extension tab for Avaya H.323 / SIP Deskphones and Spectralink handsets. In addition, it provides the Media Security settings for the Web Socket SCN trunk between IP Office Server Edition and IP Office 500 V2 Expansion System. It specifies the valid settings for these extensions/trunks and the impact on Direct Media. For all the devices in the table, SRTP and SRTP_AES_CM_128_SHA_80 were enabled. The only difference in the media settings is whether encrypted SRTCP was enabled or disabled. In summary, Avaya H.323 Deskphones don't support encrypted SRTCP so it was disabled for those deskphones.

Device	Media Security	Media Settings	Notes
96x1 H.323	Preferred	Disable Encrypted SRTCP	Media Security of <i>Preferred</i> or <i>Enforced</i> is supported for 96x1 H.323 extensions. Local H.323 calls used Direct Media.
1120e SIP	Enforced	Enable Encrypted SRTCP	If Media Security is set to <i>Preferred</i> with encrypted SRTCP enabled, SIP calls won't use Direct Media. Need to set Media Security to <i>Enforced</i> for SIP calls to use Direct Media.
J129 SIP	Enforced	Enable Encrypted SRTCP	Media Security set to <i>Enforced</i> so that SIP calls will be shuffled.
J169 SIP	Preferred	Enable Encrypted SRTCP	Media Security of <i>Enforced</i> is invalid option for J169 SIP. Need to set Media Security to <i>Preferred</i> ; however, SIP calls with this extension will not use Direct Media for calls routed over the Web Socket to another IP Office system.
Web Socket	Enforced	Enable Encrypted SRTCP	Enabling SRTCP prevents H.323 calls routed over the Web Socket from using Direct Media. H.323 phones don't support encrypted SRTCP.
Spectralink	Enforced	Enable Encrypted SRTCP	Spectralink DECT Server 2500 doesn't support RFC 5939, SDP Cap Negotiation. This requires that Media Security on the Extension VoIP tab to be set to <i>Enforced</i> and encrypted SRTCP be enabled.

©2020 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.