



## **Application Notes for Spectralink IP-DECT Server with Avaya IP Office Server Edition - Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required to integrate Spectralink IP-DECT Server 400 with Avaya IP Office Server Edition 11.1 and Avaya IP Office 500 V2 Expansion System 11.1. Spectralink IP-DECT Server 400 is a wireless solution that can be deployed as a standalone system or operate/manage 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 IP Office. The Spectralink handsets used for the compliance test included the Spectralink 7202, 7522, and 7622 Handsets. In addition, an optional Spectralink Base Station was also used to verify roaming. Spectralink IP-DECT Server 400 interfaces to Avaya IP Office as SIP endpoints. These Application Notes also apply to the Spectralink IP-DECT Server 200, 6500, and Virtual IP-DECT Server, which are like the IP-DECT Server 400 and only differ in their scalability.

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 IP Office Server Edition and Avaya IP Office 500 V2 Expansion System. Spectralink IP-DECT Server 400 is a wireless solution that can be deployed as a standalone system or operate/manage 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 IP Office. The Spectralink handsets used for the compliance test included the Spectralink 7202, 7522, and 7622 Handsets. In addition, an optional Spectralink Base Station was also used to verify roaming. Spectralink IP-DECT Server 400 interfaces to Avaya IP Office as SIP endpoints. These Application Notes also apply to the Spectralink IP-DECT Server 200, 6500, and Virtual IP-DECT Server, which are like the IP-DECT Server 400 and only differ in their scalability.

The IP-DECT Server family also includes models 200, 6500, and Virtual IP-DECT Server, 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 7000 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 Spectralink IP-DECT Server 400. Additional telephony features, such as call forward, follow me, call park/unpark, and call pickup were also verified using Avaya IP Office Short Codes.

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 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 IP-DECT Server 400 utilized 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. IP-DECT Server 400 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 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.
- 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.
- Roaming of Spectralink handsets from Spectralink IP-DECT Server 400 to Spectralink Base Station.
- Proper system recovery after a restart of 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 IP-DECT Server 400 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 IP-DECT Server 400, 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 IP-DECT Server 400.
- During the TLS handshake between IP-DECT Server 400 and IP Office Server Edition, IP-DECT Server 400 used TLSv1.2 and successfully established the TLS session with IP Office Server Edition. However, during the TLS handshake with IP Office 500 V2 Expansion, IP-DECT Server 400 used TLSv1 causing IP Office 500 V2 Expansion to reject the cipher suites in the initial TLS Hello message. To use TLSv1.2 with IP Office

500 V2 Expansion, the **Enable legacy TLS** option had to be enabled on IP-DECT Server 400. This resulted in the TLS session being established successfully.

- If SIP registration fails for whatever reason (e.g., invalid SIP extension or password), there is no indication on the Spectralink handset that it hasn't successfully registered. If the Spectralink handset cannot communicate with the IP-DEC Server 400 or optional base station, the Spectralink handset display "No Signal."
- Spectralink 7000 Series Handsets do not support the initiation of 3-party conference calls.

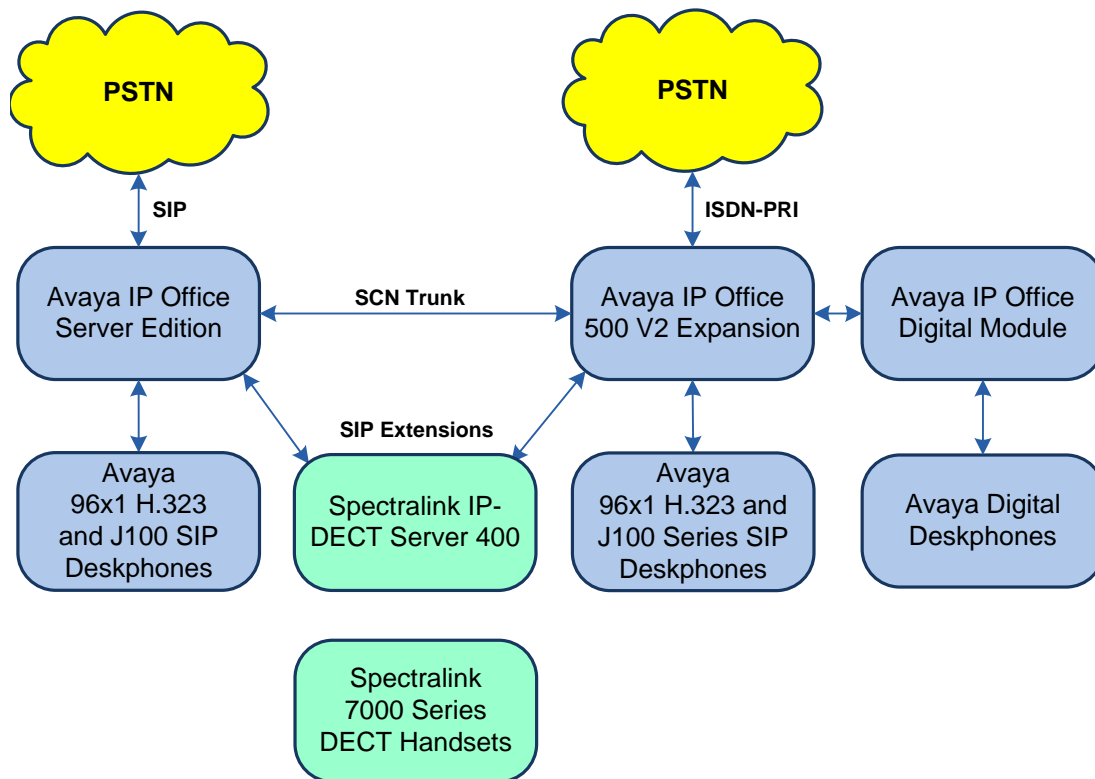
## 2.3. Support

For technical support on the Spectralink IP-DECT Server 200/400/6500/Virtual, Spectralink Base Station, or Spectralink 7000 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](mailto: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 7000 Series Handsets with Avaya IP Office Server Edition and Avaya IP Office 500 V2 (Expansion System). The Spectralink handsets registered with Avaya IP Office 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. Avaya Embedded Voicemail served as the voicemail system. Avaya 96x1 Series H.323 Deskphones and an Avaya J100 Series SIP Deskphones were used for placing and receiving calls. An optional Spectralink base station (not shown) may also be used.



**Figure 1: Avaya SIP Network with Spectralink IP-DECT Server 400 and Spectralink 7000 Series DECT 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	11.1.1.0.0 build 209
Avaya IP Office 500 V2 Expansion	11.1.1.0.0 build 209
Avaya 96x1 Series IP Deskphone	6.8304 (H.323)
Avaya J129/J169 SIP Deskphones	4.0.7.1.5
Spectralink IP-DECT Server 400	PCS21Ad
Spectralink Digital Base Station	PCS21Ad
Spectralink 7000 Series Handsets	20G

**Note:** These Application Notes also apply to the Spectralink IP-DECT server 6500, which uses the same firmware as the Spectralink IP-DECT Server 400 and uses the same SIP stack and XML-RPC API for messaging. These two IP 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

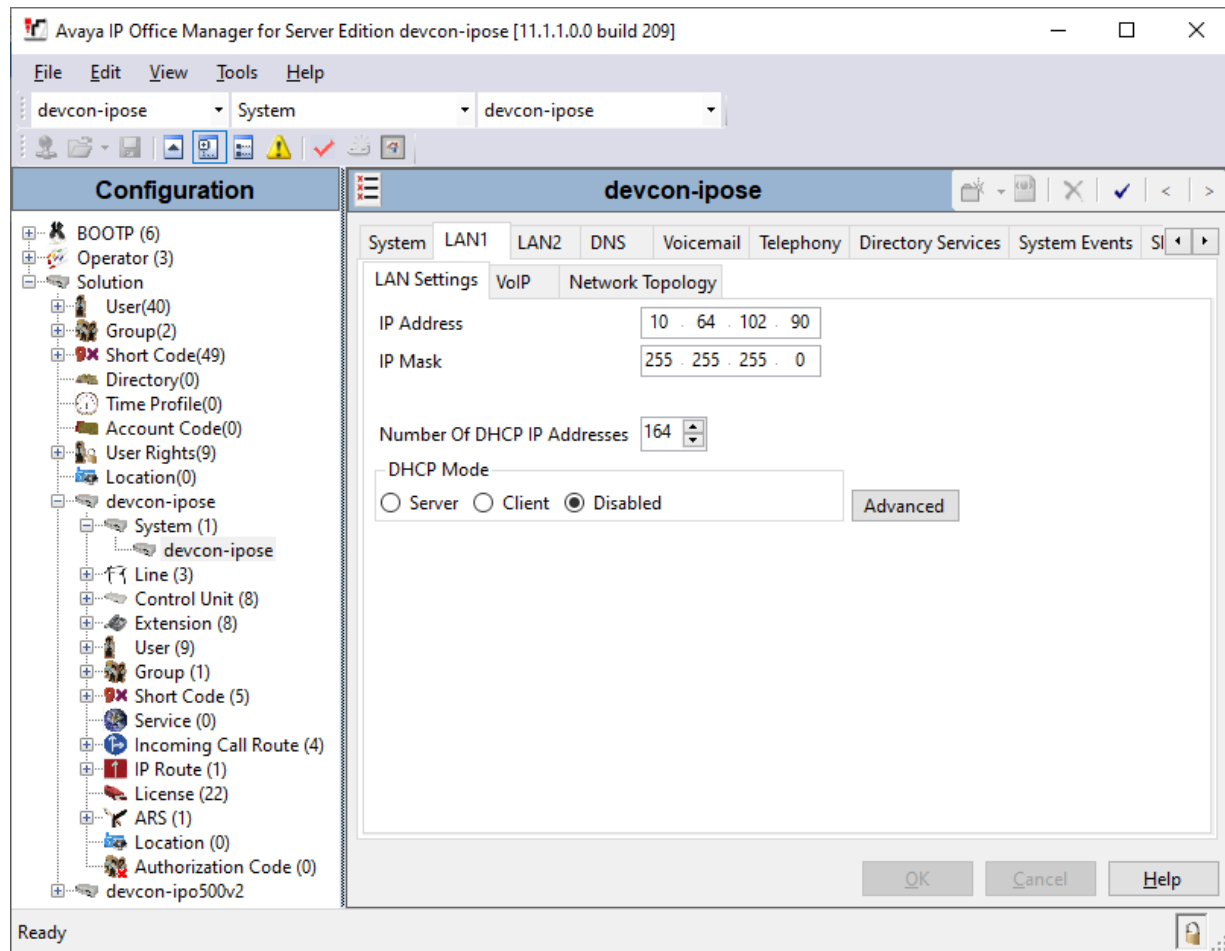
This section provides the procedures for configuring Avaya IP Office Server Edition. The procedures include the following areas:

- 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.

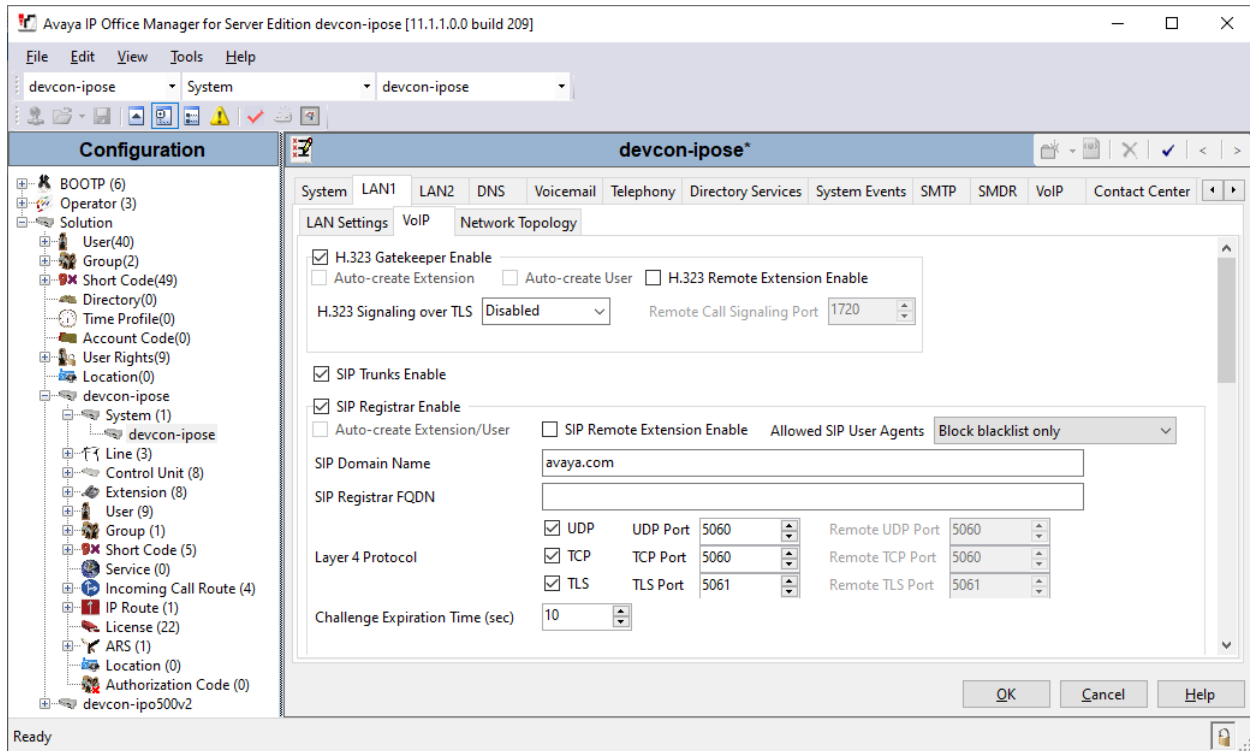
### 5.1. Obtain LAN IP Address

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 IP-DECT Server 400.



## 5.2. Administer SIP Registrar

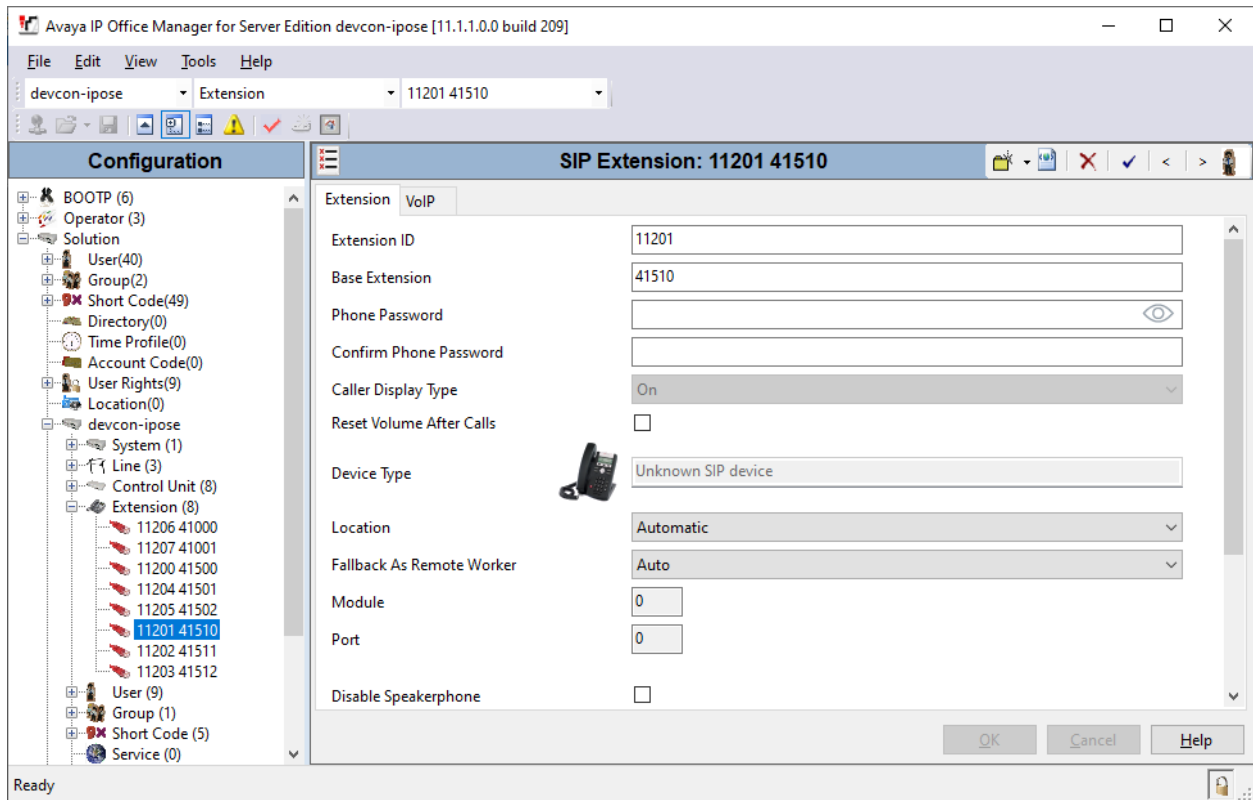
Select the **VoIP** sub-tab. Ensure that **SIP Registrar Enable** is checked and enter a valid **Domain Name**. In the compliance testing, the **Domain Name** field was set to *avaya.com*. TLS transport protocol was enabled for the **Layer 4 Protocol**, which was also used by the IP-DECT Server 400.





### 5.3. Administer SIP Extension for Spectralink Handsets

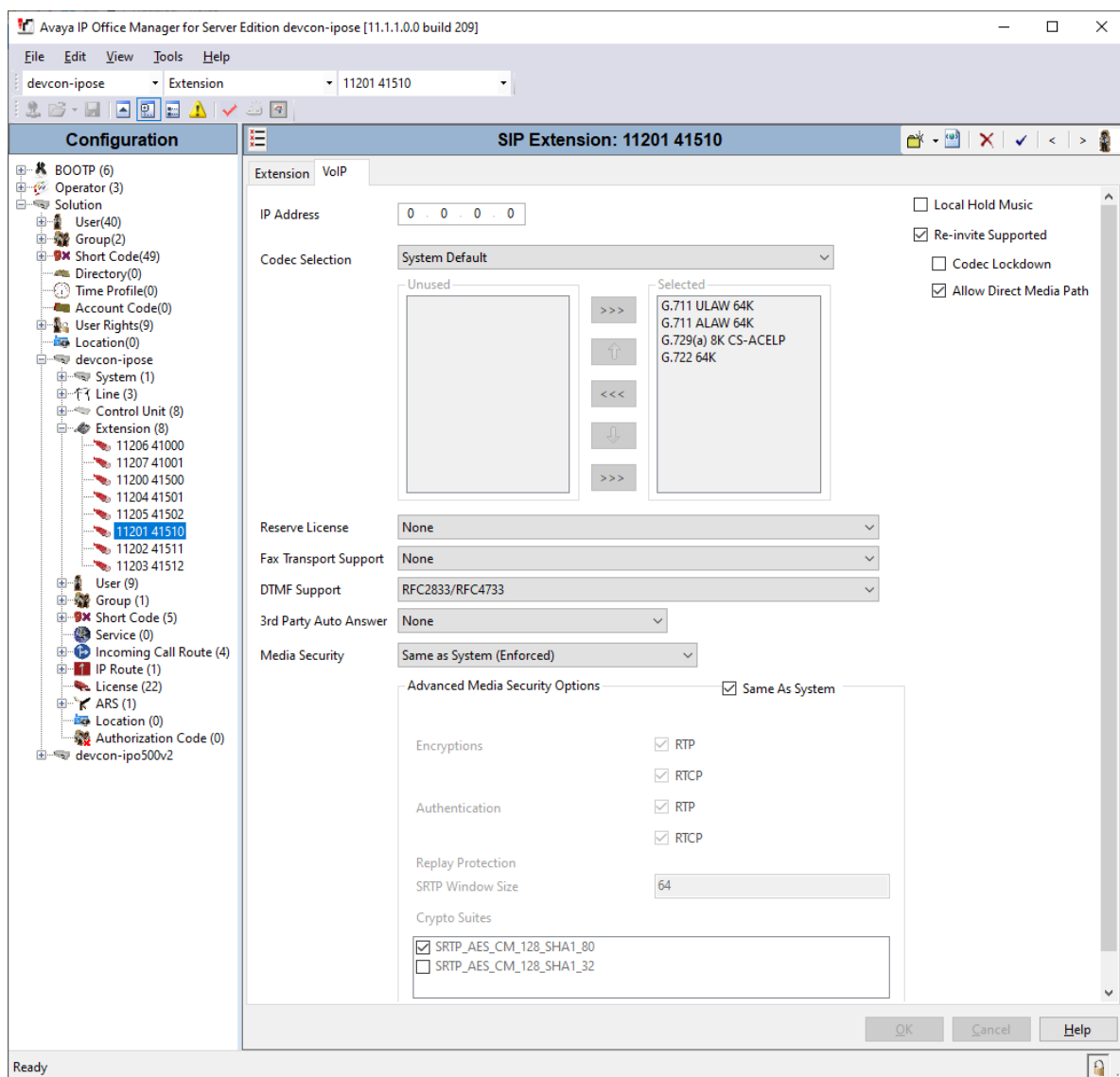
From the configuration tree in the left pane, right-click on **Extension** and select **New → SIP** from the pop-up list (not shown) to add a new SIP extension. Enter the desired extension for the **Base Extension** field as shown below. In this example, Spectralink handset was assigned extension **41510**. This is the extension that the IP-DECT Server 400 will use to register the handsets with IP Office Server Edition.



Select the **VoIP** tab. The system default was used for the codec selection. 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 IP-DECT Server 400. Since the IP-DECT Server 400 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 IP-DECT Server 400, 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 (not shown). 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 configuration window. The title bar indicates the version is 11.1.1.0.0 build 209. The menu bar includes File, Edit, View, Tools, and Help. The breadcrumb trail shows the path: devcon-ipose > User > 41510 Spectra41510. The left pane displays a configuration tree with various nodes, including BOOTP, Operator, Solution, User(40), Group(2), Short Code(49), Directory(0), Time Profile(0), Account Code(0), User Rights(9), Location(0), devcon-ipose, System(1), Line(3), Control Unit(8), Extension(8), and User(9). The 'User(9)' node is expanded, showing a list of users, with '41510 Spectra41510' selected. The right pane shows the configuration for 'Spectra41510: 41510'. The 'User' tab is active, displaying fields for Name, Password, Confirm Password, Unique Identity, Conference PIN, Confirm Audio, Conference PIN, Account Status, Full Name, Extension, Email Address, Locale, Priority, System Phone Rights, Profile, 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, Exclude From Directory, Device Type, User Rights, and User Rights view. The 'Name' field is set to 'Spectra41510', 'Full Name' is 'Spectralink', 'Extension' is '41510', 'Account Status' is 'Enabled', 'Profile' is 'Basic User', 'Device Type' is 'Unknown SIP device', and 'User Rights view' is 'User data'. The status bar at the bottom indicates 'Ready'.

Avaya IP Office Manager for Server Edition devcon-ipose [11.1.1.0.0 build 209]

File Edit View Tools Help

devcon-ipose > User > 41510 Spectra41510

**Configuration**

**Spectra41510: 41510**

User Voicemail DND Short Codes Source Numbers Telephony Forwarding Dial In Voice Recording Buttons

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

☐ 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

☐ Exclude From Directory

Device Type Unknown SIP device

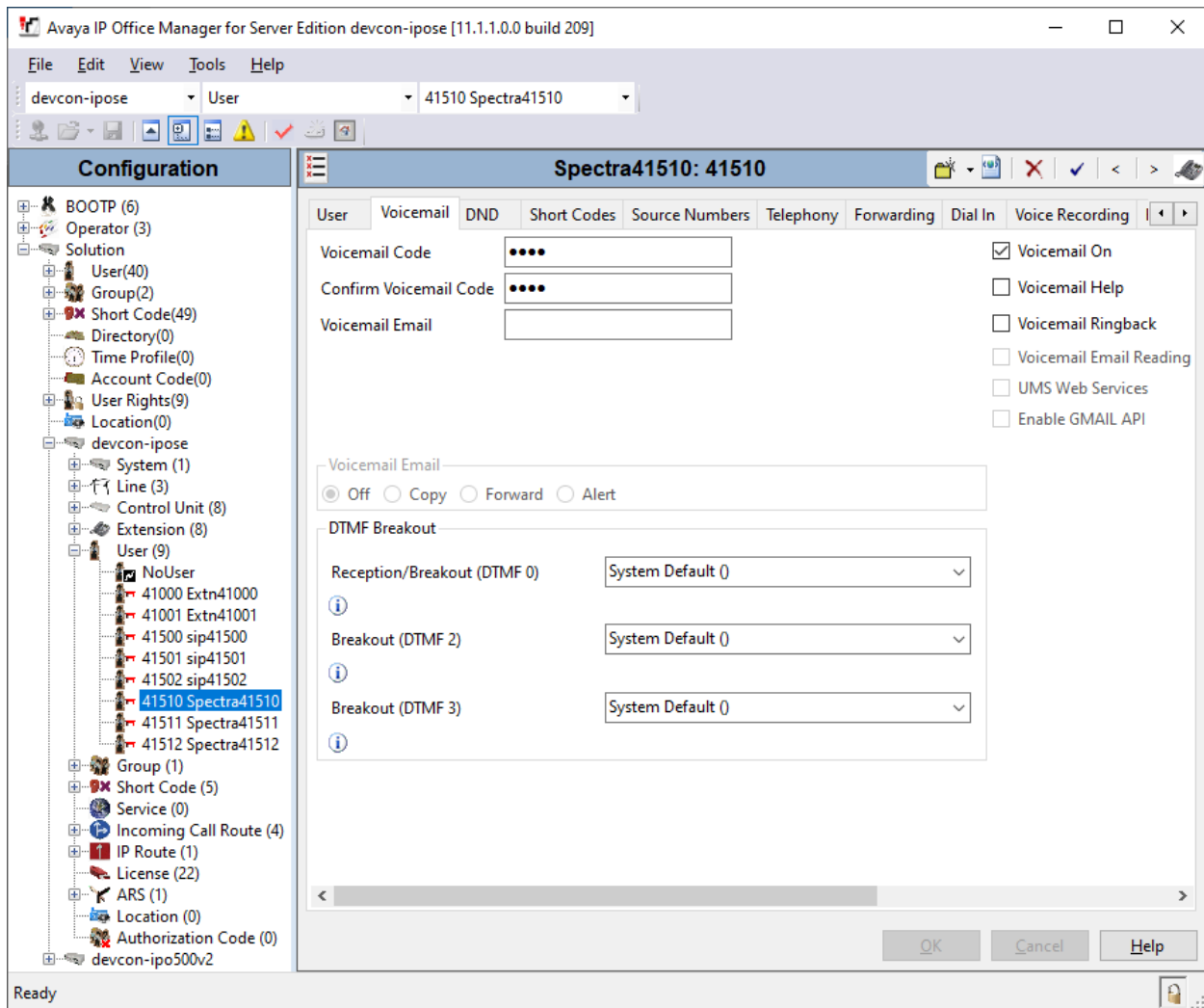
User Rights

User Rights view User data

OK Cancel Help

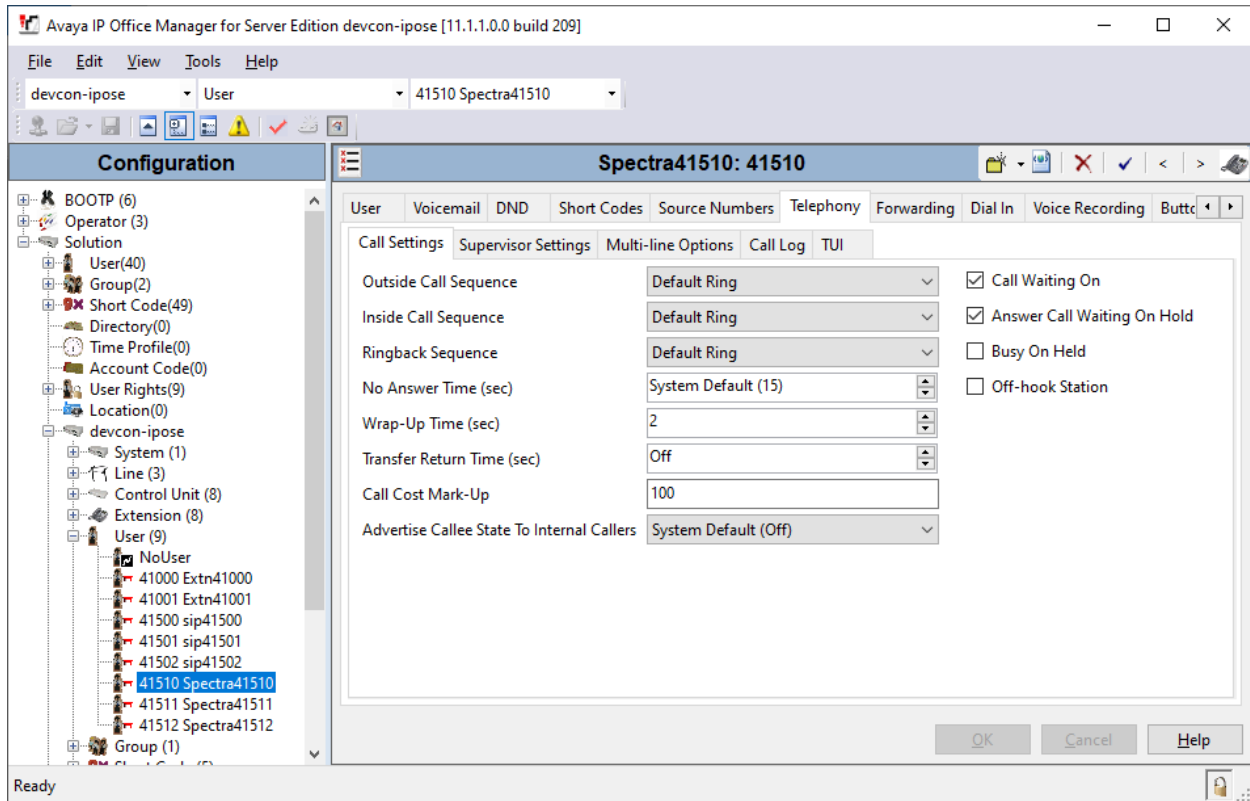
Ready

Select the **Voicemail** tab and select **Voicemail On** to enable voicemail for the Spectralink handset. Specify a **Voicemail Code** to be used when logging into voicemail.

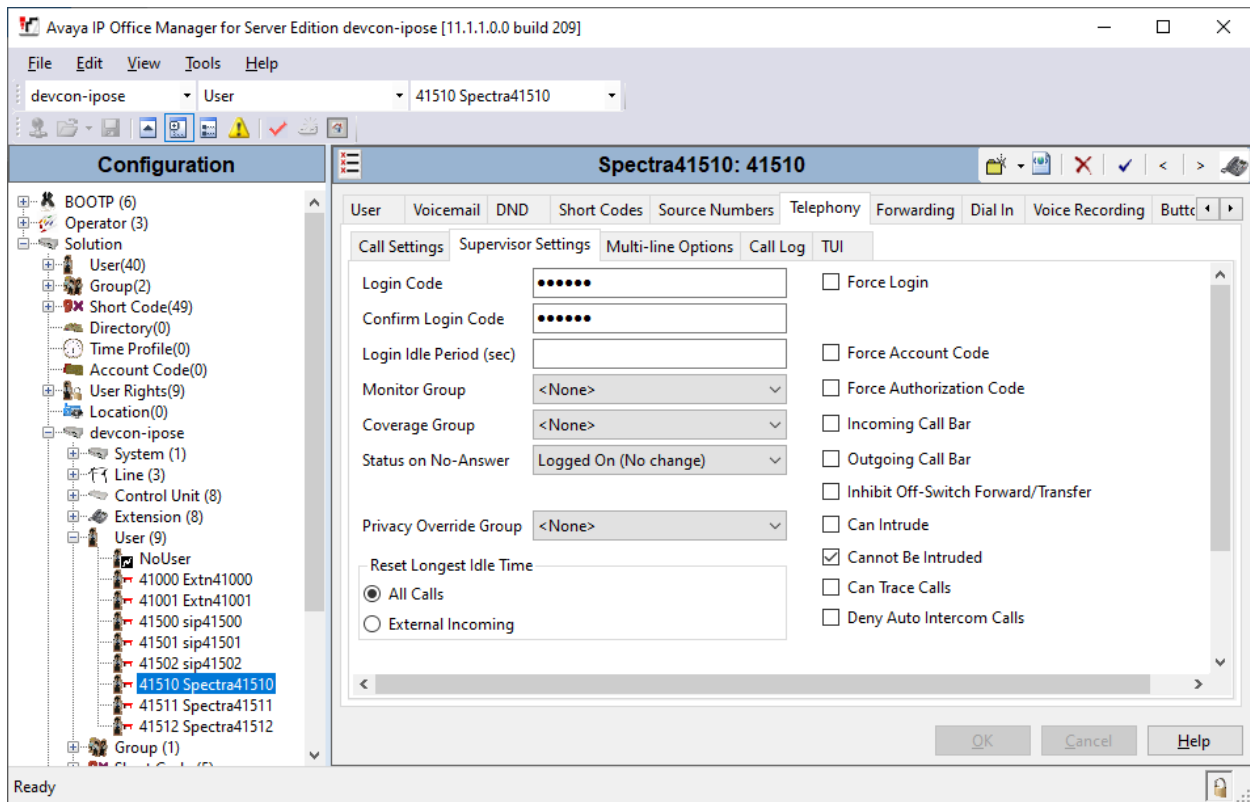


Select the **Telephony** tab followed by the **Call Settings** sub-tab. Note the settings below for the user.

**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 IP-DECT Server 400 to register the SIP extension with IP Office Server Edition.



## 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

```



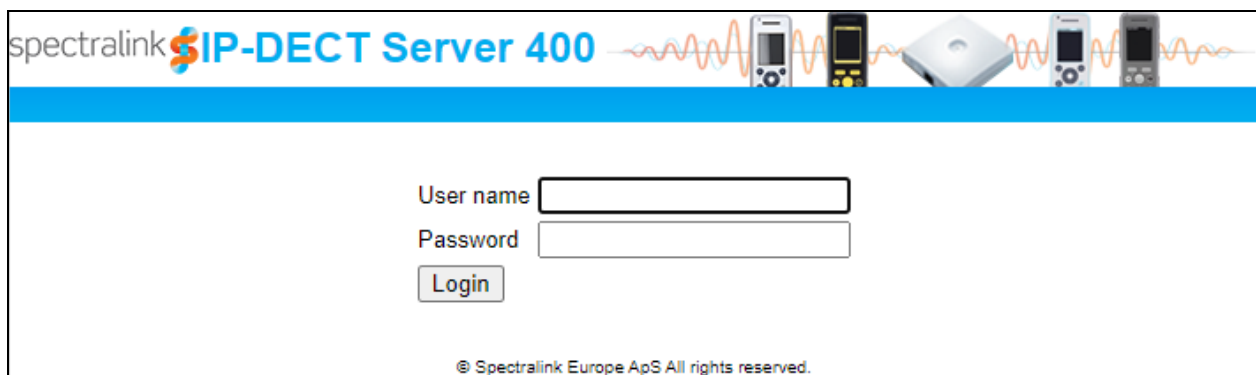
## 7. Configure Spectralink IP-DECT Server 400

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
- Enable legacy TLS
- Import TLS certificate

### 7.1. 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 **Login**.



The screenshot shows the web interface of the Spectralink IP-DECT Server 400. The header features the Spectralink logo and the text "SIP-DECT Server 400" in blue, followed by a decorative orange waveform and icons of various mobile devices. Below the header is a blue horizontal bar. The main content area contains a login form with the following elements:

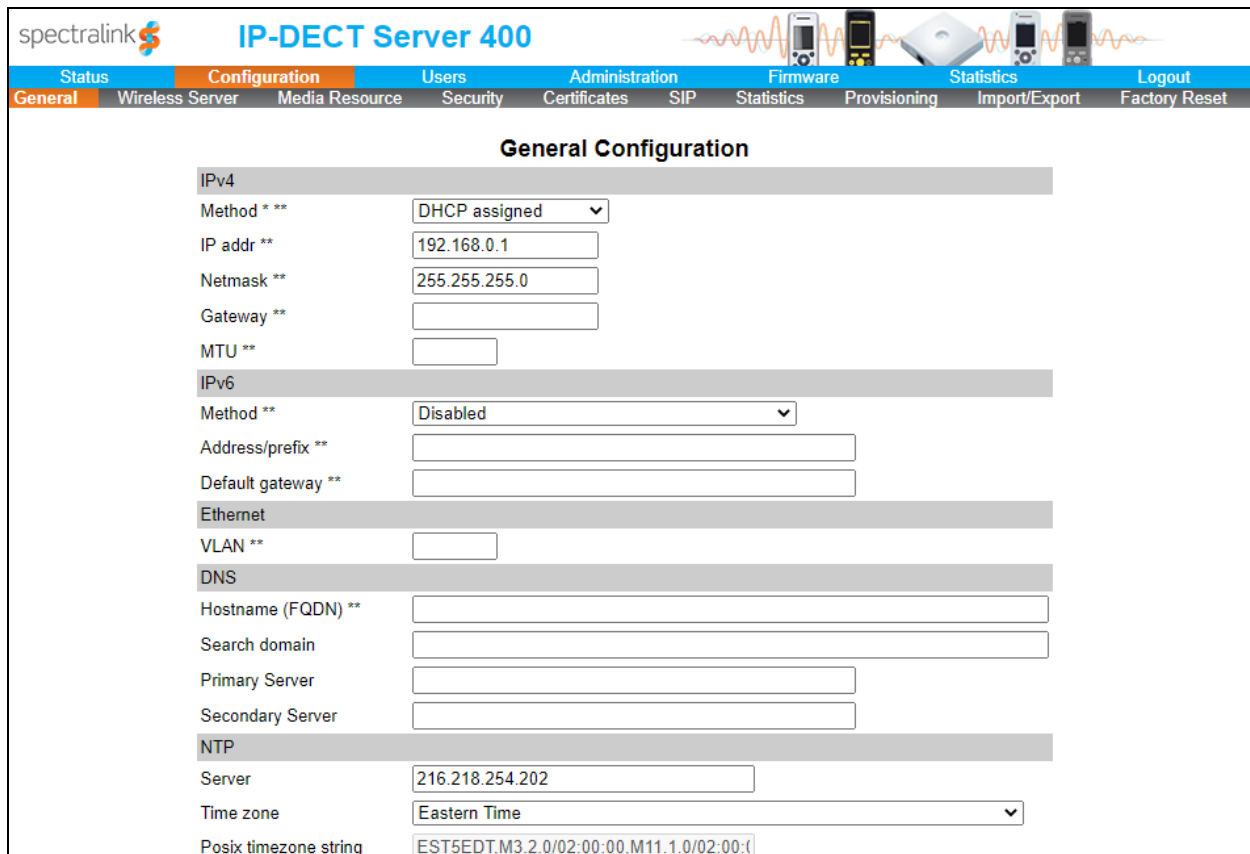
- A label "User name" followed by a text input field.
- A label "Password" followed by a text input field.
- A "Login" button below the password field.

At the bottom of the page, there is a copyright notice: "© Spectralink Europe ApS All rights reserved."

## 7.2. 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 also be used. 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 7.5**.



The screenshot displays the web interface of 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, Statistics, 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,M11.1.0/02:00:00).

### 7.3. 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.

Note that the SIP proxy is not configured here, but in the **SIP User** configured in **Section 7.4**.

The screenshot displays the 'IP-DECT Server 400' web interface. The top navigation bar includes tabs for Status, Configuration, Users, Administration, Firmware, Statistics, Provisioning, Import/Export, and Logout. The 'Configuration' tab is active, and the 'SIP' sub-tab is selected. The main content area is titled 'SIP Configuration' and contains a 'General' section with the following settings:

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"/>
Allow internal routing fallback	<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
Send Hold before REFER	<input checked="" type="checkbox"/>
Send BYE with REFER	<input checked="" type="checkbox"/>
Convert SIP URI to phone number	<input checked="" type="checkbox"/>

Below the General section is the 'Proxies' section, which contains a table with the following data:

Proxy	Priority	Weight	URI
Proxy 1	1	100	
Proxy 2	2	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.729 and G.711 and select the **Enable media encryption (SRTP)** and **Require media encryption (SRTP)** check boxes as shown below.



<b>DTMF signalling</b>	
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"/>
<b>Message waiting indication</b>	
Enable indication	<input checked="" type="checkbox"/>
Enable subscription	<input checked="" type="checkbox"/>
Subscription expire(sec) *	<input type="text" value="3600"/>
<b>Media</b>	
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="G729/8000"/></div> <div>2: <input type="text" value="PCMU/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>
Add G729A media type for G.729 codec	<input type="checkbox"/>
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	<input type="text"/>
TURN username	<input type="text"/>
TURN password	<input type="text"/>

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"/>
Allow automatic offhook	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

## 7.4. Add SIP Users

To create a SIP user for one of the Spectralink handsets, click **Users** and then the **SIP** tab. 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]

Total

SIP users

Subscribed

Registered

3

3

3

Show All entries
 Search:

<input type="checkbox"/>	Enabled	User	Displayname	IPEI	Handset	Firmware	Subscription	Registration	Latest activity
<input type="checkbox"/>	✓	41510	Spectralink 1	05003 0733588	Spectralink 7202	20G	✓	✓	✓
<input type="checkbox"/>	✓	41511	Spectralink 2	05003 0733345	Spectralink 7522	20G	✓	✓	✓
<input type="checkbox"/>	✓	41512	Spectralink 3	05003 0733797	Spectralink 7622	20G	✓	✓	✓

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).

User 41510	
DECT device	
Product name	Spectralink 7202
Model number	7202
Software part number	14225110
Item number	02600000
Firmware	20G
HW version	16A
Software version	1422 5110 PCS 20GA
Production Id	0027 506A 94A5 65F4
IPEI	<input type="text" value="05003 0733588"/>
Access code	<input type="text"/>
User	
Standby text	<input type="text" value="41510"/>
DECT to DECT	<input type="checkbox"/>
Disabled	<input type="checkbox"/>

Under **SIP**:

- **Username / Extension** Set a username or extension for handset.
- **Domain** Specify the IP address of IP Office Server Edition (e.g., *10.64.102.90*).
- **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	
Username / Extension *	<input type="text" value="41510"/>
Secondary username	<input type="text"/>
Domain	<input type="text" value="10.64.102.90"/>
Displayname	<input type="text" value="Spectralink 1"/>
Authentication user	<input type="text" value="41510"/>
Authentication password	<input type="password" value="....."/>
Features	
Call forward unconditional	<input type="text"/>
Admin rights	<input type="checkbox"/>
<div>Save Delete Cancel</div>	

## 7.5. Enable Legacy TLS

To enable the **Enable Legacy TLS** option, click **Configuration** and then the **Security** sub-tab. In the Security Configuration page, enter the **Current password** and select **Enable legacy TLS** as shown below. Click **Save**. Refer to **Section 2.2** for details.

The screenshot displays the 'Security Configuration' page for the 'IP-DECT Server 400'. The page is divided into two main sections: 'Administrator Authentication' and 'Data protection'. In the 'Administrator Authentication' section, the 'Current password' field is filled with '\*\*\*\*', 'New username' is 'admin', and 'New password' and 'New password again' fields are empty. 'Strict password requirements' is unchecked, and 'Password expiration' is set to 'Never'. In the 'Data protection' section, 'Allow unencrypted HTTP' is unchecked, 'Enable legacy TLS' is checked, 'Allow remote logging' is unchecked, and 'Remove user passwords from exported data' is unchecked. At the bottom, there are 'Save' and 'Cancel' buttons. A legend at the bottom indicates that '\*' denotes a required field and '\*\*' denotes a field that requires a restart.

Administrator Authentication	
Current password *	****
New username *	admin
New password	
New password again	
Strict password requirements	<input type="checkbox"/>
Password expiration	Never

Data protection	
Allow unencrypted HTTP	<input type="checkbox"/>
Enable legacy TLS	<input checked="" type="checkbox"/>
Allow remote logging	<input type="checkbox"/>
Remove user passwords from exported data	<input type="checkbox"/>

Save Cancel

\*) Required field \*\*) Require restart



## 7.6. 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 **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.

spectralink **IP-DECT Server 400**

Status Configuration Users Administration Firmware Statistics Logout  
General Wireless Server Media Resource Security **Certificates** SIP Statistics Provisioning Import/Export Factory Reset

Device certificate chain

Show  entries Search:

Subject	Validity	SHA1 fingerprint	Key ID	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	ea:f2:1b:f9:e2:3b:4c:2a:cd:3b:e6:c8:d4:a3:a6:01:92:75:4b:f5	SpectraLink Issuing CA
SpectraLink Issuing CA	2016-10-07 - 2041-10-07	39:82:0a:28:41:e7:4a:55:69:49:1e:b4:ba:c1:9b:3b:cd:98:3b:9f	6d:23:0d:e8:ce:9a:b4:06:32:10:67:04:e0:40:35:b4:05:06:1f:e6	SpectraLink Root CA
SpectraLink Root CA	2012-07-09 - 2044-07-09	f3:92:b9:87:e9:d6:4c:a6:53:ee:8c:ef:bb:3c:a1:7f:e9:e6:83:a2	43:c4:58:6f:a1:02:39:a8:85:85:ca:2d:6e:53:8b:16:31:5d:f5:c2	SpectraLink Root CA

Showing 1 to 3 of 3 entries First Previous **1** Next Last

Host key

Key file:  No file chosen Password:

Show  entries Search:

Algorithm	Bits	Key ID
No data available in table		

Showing 0 to 0 of 0 entries First Previous **1** Next Last

Host certificate chain

Certificate file:  No file chosen Password:  Type: ☒ X.509 ☐ PKCS#12

CA Certificates

No file chosen

Show  entries Search:

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

## 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya IP Office and Spectralink IP-DECT Server 400.

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 system is running on a Linux PC (11.1.1.0.0 build 209). 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 (12), Extensions (7), Trunks (3), Active Calls, Resources, Voicemail, IP Networking, and Locations. The "Extensions (7)" section is expanded, showing a list of extensions: 41000, 41001, 41501, 41502, 41510 (selected), 41511, and 41512. The main content area displays the "Extension Status" for extension 41510. The status information is organized into two columns. The left column lists various configuration parameters, and the right column shows their values. Below this, a table displays the current state of the extension, including its current state, time in state, and other call-related information. 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 as 11:33:49 AM and the system is online.

Avaya IP Office System Status - devcon-ipose (10.64.102.90) - IP Office Linux PC 11.1.1.0.0 build 209

**AVAYA** IP Office System Status

Help Snapshot LogOff Exit About

**System**

**Alarms (12)**

**Extensions (7)**

41000

41001

41501

41502

▶ 41510

41511

41512

**Trunks (3)**

Active Calls

**Resources**

**Voicemail**

**IP Networking**

Locations

**Extension Status**

Extension Number: 41510

IP address: 192.168.100.191

Standard Location: None

Registrar: Primary

Telephone Type: Unknown SIP Device

User-Agent SIP header: KWS400/PCS21Ad98964 14218500 0013d190b040

Media Stream: SRTP

Layer 4 Protocol: TLS

Current User Extension Number: 41510

Current User Name: Spectra41510

Forwarding: Off

Twinning: Off

Do Not Disturb: Off

Message Waiting: Off

Number of New Messages: 0

Phone Manager Type: None

SIP Device Features: REFER,UPDATE

License Reserved: No

Last Date and Time License Allocated: 4/14/2021 10:53:00 AM

Packet Loss Fraction: Connection Type:

Jitter: Codec:

Round Trip Delay: Remote Media Address:

Call Ref	Current State	Time in State	Calling Number or Called Number	Direction	Other Party on Call
	Idle	00:40:49			

Trace Trace All Pause Ping Call Details Print... Save As...

11:33:49 AM Online

2. Alternatively, the SIP registration and DECT Subscription status may be verified by navigating to **Users** → **List Users** in the IP-DECT Server 400 web interface. These columns should contain a green checkmark as shown below.

**IP-DECT Server 400**

Navigation: Status | Configuration | **Users** | Administration | Firmware | Statistics | Logout

Sub-navigation: **List Users** | Import/Export

**User List**

Overview

System ARI: 10056545410 [10 2e b2 c2 00]

SIP users: 3    Subscribed: 3    Registered: 3

Total: 3

Buttons: New | Enable | Disable | Delete | Re-register | Un-subscribe | Firmware update

Show: All entries    Search:

<input type="checkbox"/>	Enabled	User	Displayname	IPEI	Handset	Firmware	Subscription	Registration	Latest activity
<input type="checkbox"/>	✓	41510	Spectralink 1	05003 0733588	Spectralink 7202	20G	✓	✓	✓
<input type="checkbox"/>	✓	41511	Spectralink 2	05003 0733345	Spectralink 7522	20G	✓	✓	✓
<input type="checkbox"/>	✓	41512	Spectralink 3	05003 0733797	Spectralink 7622	20G	✓	✓	✓

Showing 1 to 3 of 3 entries    First    Previous    1    Next    Last

- 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 **SRTP Direct Media** as shown below.

The screenshot displays the Avaya IP Office System Status web interface. The title bar indicates the application is running on a Linux PC. The main content area is titled "IP Office System Status" and shows the configuration for extension 41510. The left sidebar contains a navigation menu with options like System, Alarms, Extensions, Trunks, Active Calls, Resources, Voicemail, and IP Networking. The main panel is divided into two sections: "Extension Status" and a call log table.

**Extension Status**

Extension Number:	41510
IP address:	192.168.100.191
Standard Location:	None
Registrar:	Primary
Telephone Type:	Unknown SIP Device
User-Agent SIP header:	KWS400/PCS21Ad98964 14218500 0013d190b040
Media Stream:	SRTP
Layer 4 Protocol:	TLS
Current User Extension Number:	41510
Current User Name:	Spectra41510
Forwarding:	Off
Twinning:	Off
Do Not Disturb:	Off
Message Waiting:	Off
Number of New Messages:	0
Phone Manager Type:	None
SIP Device Features:	REFER,UPDATE
License Reserved:	No
Last Date and Time License Allocated:	4/14/2021 10:53:00 AM
Packet Loss Fraction:	
Jitter:	
Round Trip Delay:	
Connection Type:	SRTP Direct Media
Codec:	G711 Mu
Remote Media Address:	192.168.100.191

**Call Log Table:**

Call Ref	Current State	Time in State	Calling Number or Called Number	Direction	Other Party on Call
442	Connected	00:00:10		Outgoing	Extn 41511, Spectra41511

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 as 11:34:34 AM and the system is "Online".

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

## 9. Conclusion

These Application Notes described the configuration steps required to integrate Spectralink IP-DECT Server 400 with Avaya IP Office Server Edition and Avaya IP Office 500 V2 Expansion System. Spectralink IP-DECT 400 allowed Spectralink 7000 Series Handsets to register with Avaya IP Office Server Edition and establish calls to H.323 stations, SIP stations, and the PSTN while using 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**.

## 10. References

This section references the Avaya documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com> and the Spectralink documentation is available at <https://support.spectralink.com/products/dect/spectralink-ip-dect-server-400>.

- [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 IP-DECT Server 200/400/6500 Installation and Configuration Guide*, 722-0210-000 Rev: A, November 2020.

## 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 security 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	<b>Media Security</b> 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 <b>Media Security</b> is set to <i>Preferred</i> with encrypted SRTCP enabled, SIP calls won't use Direct Media. Need to set <b>Media Security</b> to <i>Enforced</i> for SIP calls to use Direct Media.
J129 SIP	Enforced	Enable Encrypted SRTCP	<b>Media Security</b> set to <i>Enforced</i> so that SIP calls will be shuffled.
J169 SIP	Preferred	Enable Encrypted SRTCP	<b>Media Security</b> of <i>Enforced</i> is invalid option for J169 SIP. Need to set <b>Media Security</b> 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.
Spectralink	Enforced	Enable Encrypted SRTCP	Spectralink IP-DECT Server 400 doesn't support RFC 5939, SDP Cap Negotiation. This requires that <b>Media Security</b> on the <b>Extension</b> VoIP tab to be set to <i>Enforced</i> and encrypted SRTCP be enabled.
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.
SIP Trunk to SBCE	Preferred	Enable Encrypted SRTCP	<b>Media Security</b> of <i>Preferred</i> . SIP calls aren't shuffled.

---

**©2021 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](mailto:devconnect@avaya.com).

To whom it may concern.

May 6<sup>th</sup> 2021

## Spectralink IP-DECT Platform Interoperability with Avaya IP Office 11

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 share firmware file.

In addition, for the

- Spectralink Virtual IP-DECT Server

This product shares the same code base as above as IP-DECT server 200/400/6500, only virtualized to run on a Virtual server (ex. VM-ware) and therefore also share the same SIP stack. This is for Spectralink considered the Spectralink IP-DECT servers and a product family.

Only differentiation between the IP-DECT Servers are scalability:

- IP-DECT Server 200 – 12 handsets (0 IP Base stations/Single Cell)
- IP-DECT Server 400 – 60 handsets + 9 IP Base stations
- IP-DECT Server 6500 – 4.096 handsets and 1.024 IP-Base stations
- Spectralink Virtual IP-DECT Server 4.096 handsets and 4.096 IP Base stations

With above we view the latest test of Spectralink IP-DECT Server 400 on Avaya IP Office 11 to cover above.

Best regards



Martin Praest  
Director Business Development