



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Rauland Responder Enterprise with Avaya IP Office Server Edition – Issue 1.0**

### **Abstract**

These Application Notes describe a compliance-tested configuration consisting of the Rauland Responder Enterprise solution and Avaya IP Office Server Edition.

The Rauland Responder Enterprise solution is a complete nurse call system with associated Staff Management applications ensuring calls for assistance from patient rooms are immediately routed to the proper staff for response.

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 a compliance-tested configuration consisting of the Rauland Responder Enterprise (hereafter known as Responder) solution and Avaya IP Office Server Edition (hereafter known as IP Office).

The Responder solution is a complete nurse call system with associated Staff Management applications ensuring calls for assistance from patient rooms are immediately routed to the proper staff for response.

Responder Enterprise solution consists of Responder SIP Server, Responder Application Server and several Responder call point devices. The Responder SIP Server connects directly to IP Office Primary Server using SIP Lines (trunks). Calls from a patient room could be initiated by a patient (pain, assistance needed, etc.), or hospital staff (room cleaning, linens, etc.) with the push of a button. Staff using Avaya phones can be incorporated into the system so that calls to a nurse, for example, would route via IP Office, and to be able to call the patient room in return. This adds the benefit of staff having access to other resources in the hospital using Avaya endpoints.

Hospital staff members who are responsible for direct communication with patient rooms generally roam using wireless phones. During compliance testing, only Avaya Deskphones were used.

## 2. General Test Approach and Test Results

The compliance test focused on the ability for Responder endpoints to initiate and receive calls to and from IP Office using direct SIP trunk connectivity.

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 Responder did not include use of any specific encryption features as requested by Rauland.

### 2.1. Interoperability Compliance Testing

The compliance test validated the ability of Responder to route calls to and from patient rooms to Avaya endpoints. Additionally, testing validated the ability for the Responder solution to recover from common outages such as network outages and server reboots.

Responder endpoints are designed with limited functionality. Responder endpoints are not designed for multi-line functions like Hold, Conference and Transfer.

### 2.2. Test Results

The objectives described in **Section 2.1** were verified with the following observation.

- Responder only supports G.711MU codec.

### 2.3. Support

Information, Documentation and Technical support for Rauland products can be obtained at:

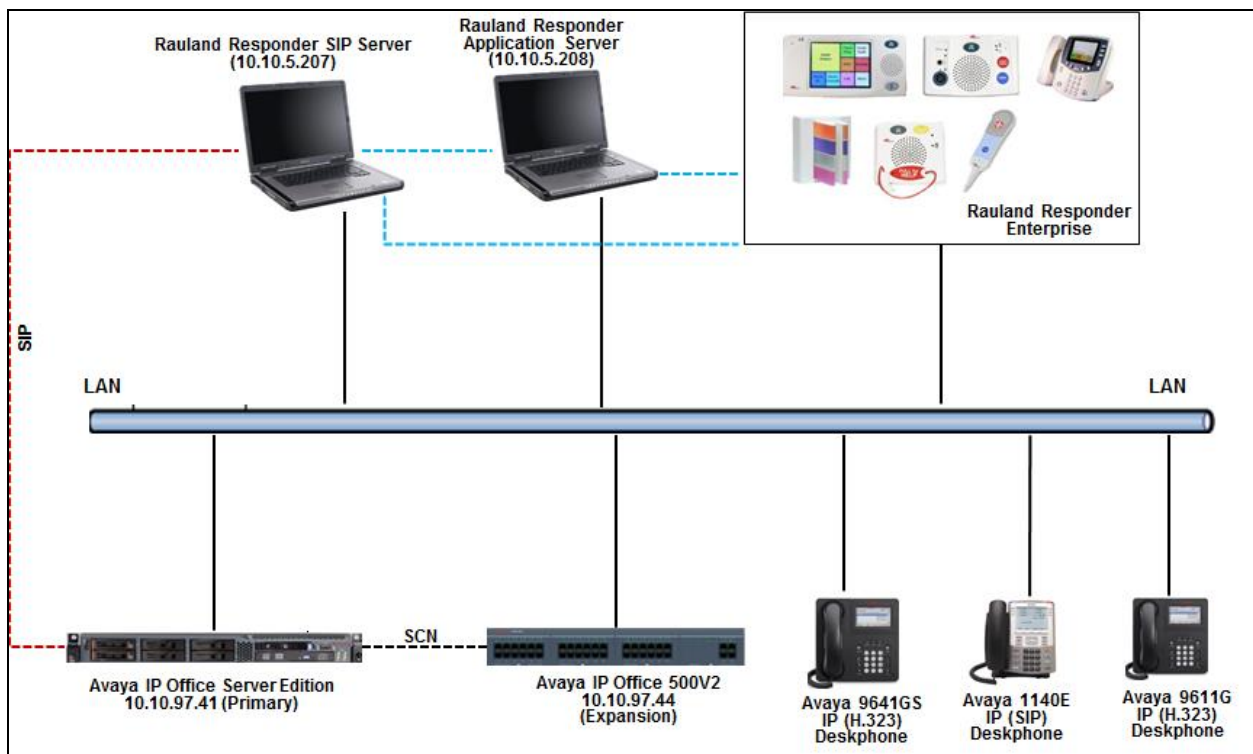
- Phone: +1 800 752 7725 (toll free) / +1 847 590 7100 (from outside the US)
- Web: <http://www.rauland.com/>

### 3. Reference Configuration

**Figure 1** illustrates the compliance test configuration consisting of:

- Avaya IP Office Server (Primary)
- Avaya IP Office 500V2 (Expansion)
- Various H.323 and SIP endpoints
- Responder SIP Server
- Responder Application Server
- Responder Communication Endpoints

Calls routed to and from IP Office used SIP trunks between the Responder SIP server and IP Office.



**Figure 1 – Rauland Responder Enterprise Compliance Test Configuration**

## 4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

Equipment/Software	Release/Version
Avaya IP Office Server (Primary)	11.0.0.1.0 build 8
Avaya IP Office 500V2 (Expansion)	11.0.0.1.0 build 8
Avaya IP Deskphones: 1140E (SIP on Server) 1140E (SIP on Expansion) 9641GS (H323 on Server) 9611G (H323 on Expansion)	 04.04.23.00 04.04.23.00 6.6604 6.6604
Rauland Nurse Call	Enterprise SR1 SP1
Rauland Application Server running on Windows 2012 R2 OS	Enterprise SR1 SP1
Rauland Apps	Enterprise SR1 SP1
Rauland DB	Enterprise SR1 SP1
Responder SIP Server running on Windows 7 Pro OS	3.8.4.2

***Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office IP500V2 and also when deployed with IP Office Server Edition in all configurations.***

## 5. Avaya IP Office Configuration

The document assumes that Avaya IP Office Server Edition has been installed and configured to work with a 500V2 expansion. This section only describes the details on how to configure the IP Office Server Edition (Primary) since the SIP line connectivity was only configured between Primary and Responder during this compliance testing. Similar configuration pertains to IP Office 500V2 (Expansion) box too if a SIP line connectivity needs to be established between Expansion and Responder.

Configuration and verification operations on the Avaya IP Office illustrated in this section were all performed using Avaya IP Office Manager. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. The configuration operations described in this section can be summarized as follows:

- Launch Avaya IP Office Manager
- Verify IP Office license
- Obtain LAN IP address
- Enable SIP trunks
- Administer SIP line
- Administer incoming call route
- Administer short code
- Save Configuration

## 5.1. Launch Avaya IP Office Manager

From a PC running the IP Office Manager application, select **Start → IP Office → Manager** to launch the Manager application. Select the proper IP Office system, and log in using the appropriate credentials (not shown). The Avaya IP Office Manager for Server Edition screen is displayed as shown in the screen below. Click on **Configuration** that is highlighted on the right side of the screen below.

The screenshot displays the Avaya IP Office Manager for Server Edition application. The window title is "Avaya IP Office Manager for Server Edition DevCon IPO Sev1 [11.0.0.1.0 build 8]". The interface includes a menu bar (File, Edit, View, Tools, Help) and a toolbar. The left sidebar, labeled "Configuration", shows a tree view of system components: BOOTP (7), Operator (3), Solution, User(46), Group(8), Short Code(60), Directory(0), Time Profile(0), Account Code(1), User Rights(13), Location(6), DevCon IPO Sev1, and DevCon IPOS Exp. The main area, titled "Server Edition", contains a "Summary" section with the following details:

- Hardware Installed:**
  - Control Unit: IPO-Linux-PC
  - Secondary Server: NONE
  - Expansion Systems: .44
  - System Identification: 858b6d69e18abf9f4755e57c276072a18ad0aa4
- System Settings:**
  - IP Address: .41
  - Sub-Net Mask: 255.255.255.240
  - System Locale: United States (US English)
  - System Location: 4: BVWFLR1###613
  - Device ID: 1
  - Number of Extensions on System: 27

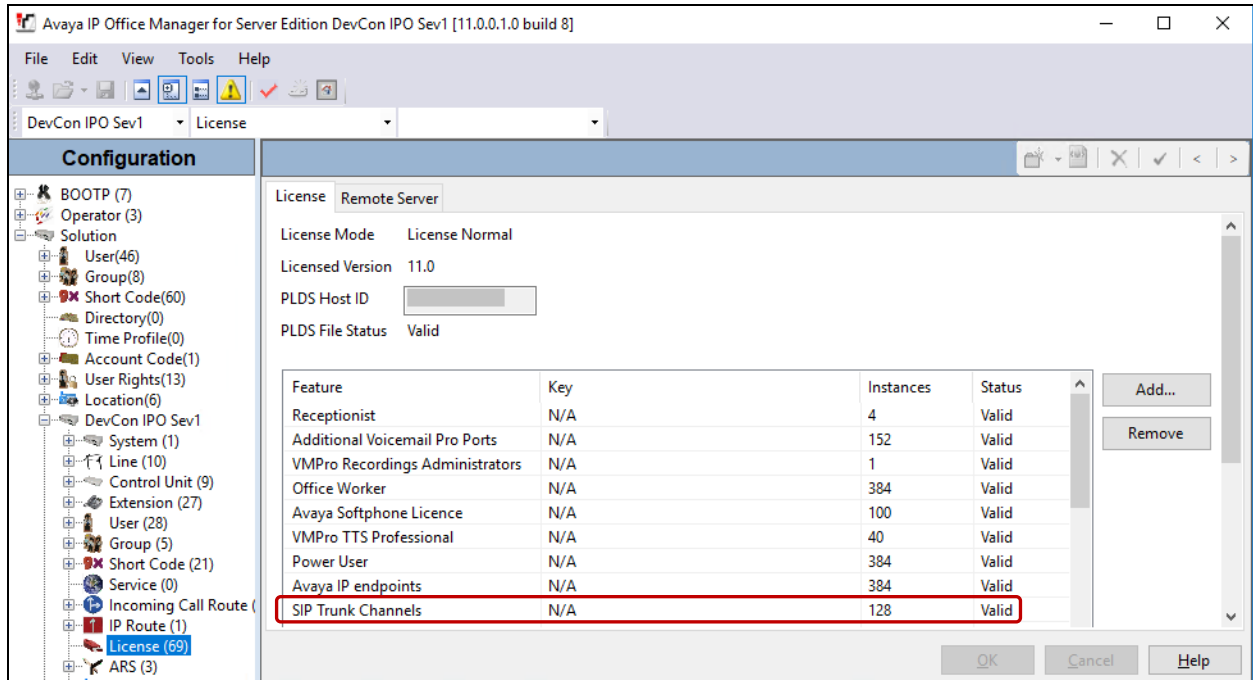
On the right side, an "Open..." menu is visible with the following options: Configuration (highlighted), System Status, Voicemail Administration, Resiliency Administration, On-boarding, IP Office Web Manager, Help, Set All Nodes to Select, and Set All Nodes License Source.

At the bottom of the window, a table lists the system components and their configurations:

Description	Name	Address	Primary Link	Users Configured	Extensions Configured
Solution				46	65
Primary Server	DevCon IPO Sev1	.41		27	27
Expansion System	DevCon IPOS Exp	.44	Bothway	19	38

## 5.2. Verify IP Office License

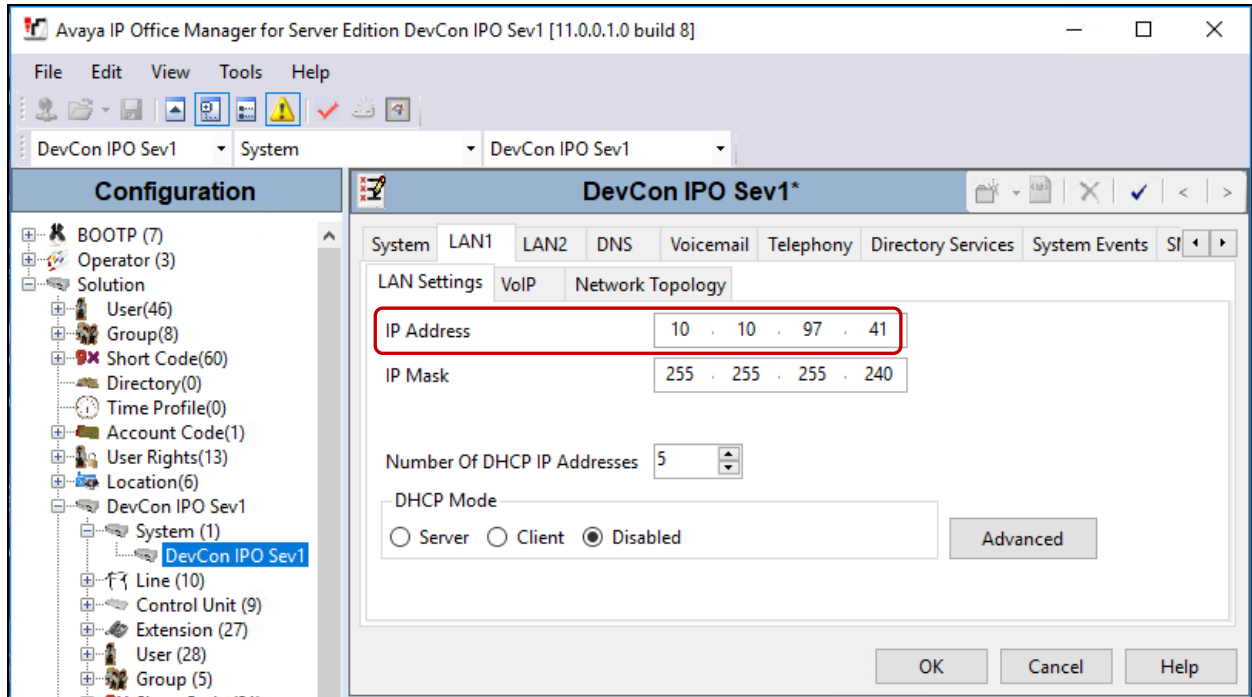
Once the **Avaya IP Office Manager for Server Edition** screen is displayed, from the configuration tree in the left pane, select the Primary System, which in this case is **DevCon IPO Sev1** and click on **License** to display the **License** screen in the right pane. Verify that the **Feature** for **SIP Trunk Channels Status** is “Valid”, and that the **Instances** value is sufficient for the desired maximum number of simultaneous calls. If there is insufficient capacity of SIP Trunks, contact an Avaya representative to make the appropriate changes.





### 5.3. Obtain LAN IP Address

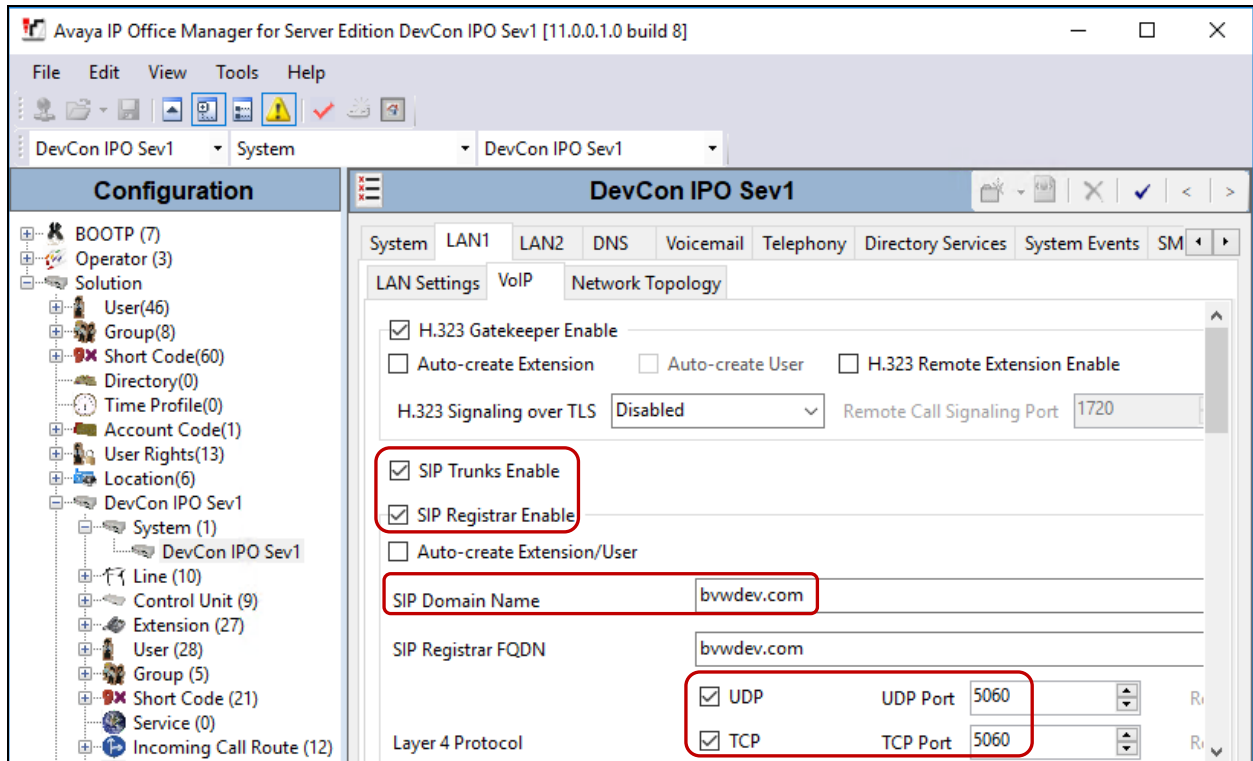
From the configuration tree in the left pane, navigate to **DevCon IPO Sev1** → **System (1)** to display the **DevCon IPO Sev1** screen in the right pane, where **DevCon IPO Sev1** is the name of the IP Office Primary system. Select the **LAN1** tab, followed by the **LAN Settings** sub-tab in the right pane. Make a note of the **IP Address**, which will be used later while configuring the Responder SIP Server in **Section 6**. Note that IP Office can support SIP trunks on the LAN1 and/or LAN2 interfaces, and the compliance testing used the LAN1 interface.



## 5.4. Enable SIP Trunks

Select the **VoIP** sub-tab and ensure the configuration is as shown below:

- Check **SIP Trunks Enable** box.
- Check **SIP Registrar Enable** box.
- **Domain Name:** During compliance testing “bvwddev.com” was used.
- Check **UDP** and **TCP** protocol with the correct port numbers.

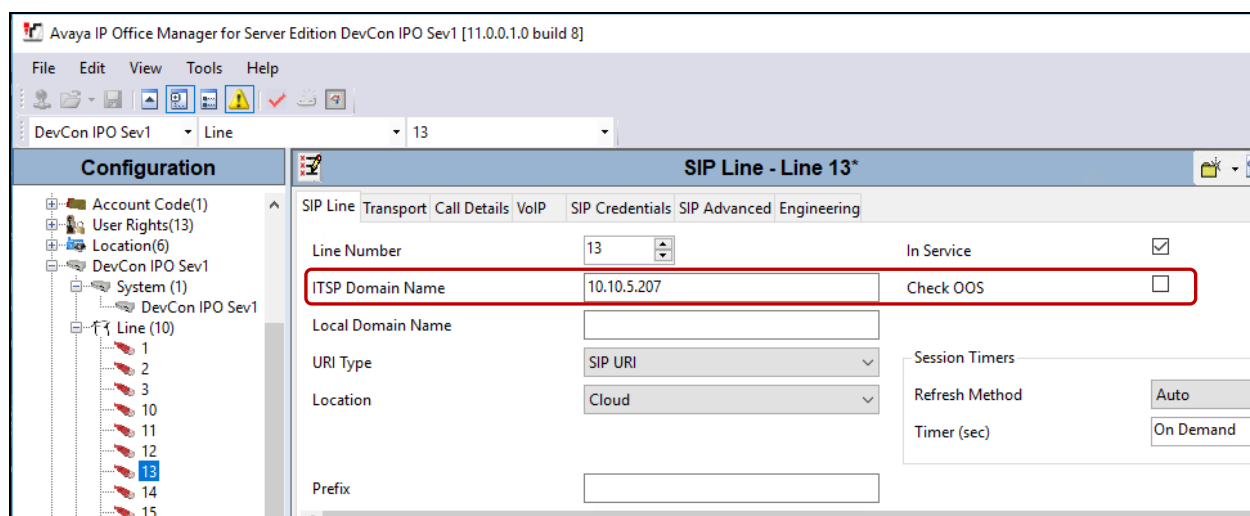


## 5.5. Administer SIP Line

From the configuration tree in the left pane, right-click on **Line**, now select **New → SIP Line** from the pop-up list to add a new SIP line (not shown). During compliance testing **Line 13** was added. Select the **SIP Line** tab in the right pane and configure the following:

- **ITSP Domain Name:** IP address of the Responder SIP Server.
- Uncheck the **Check OOS** box.

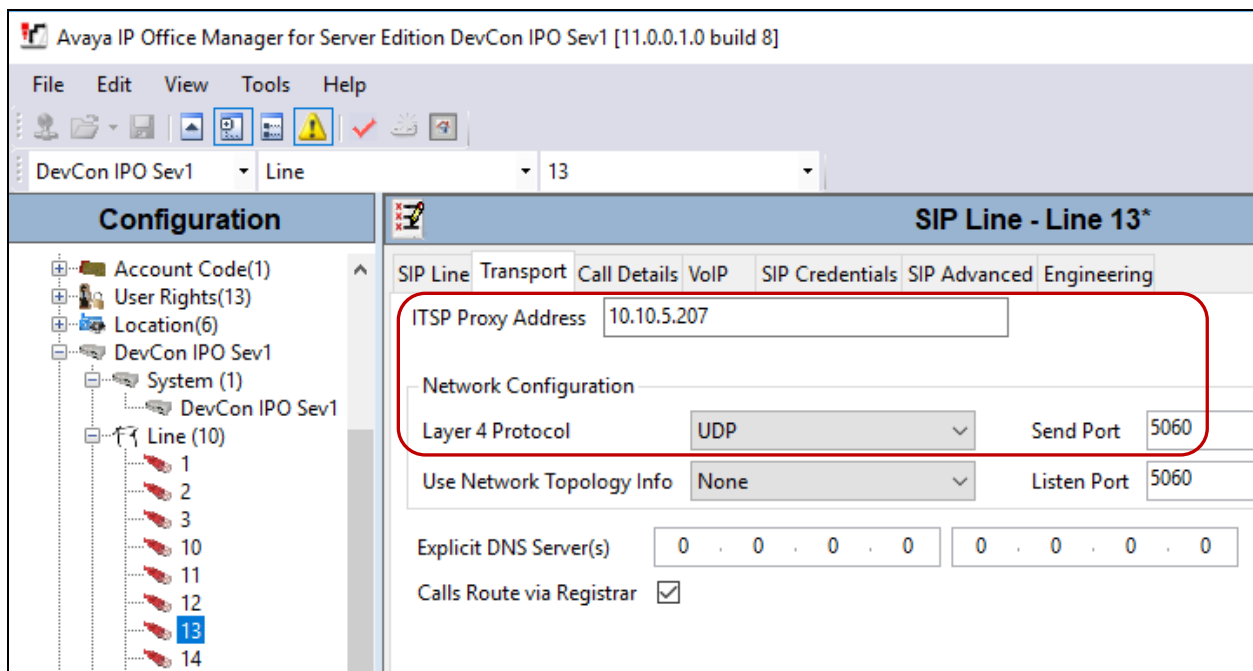
Retain default values for all other fields.



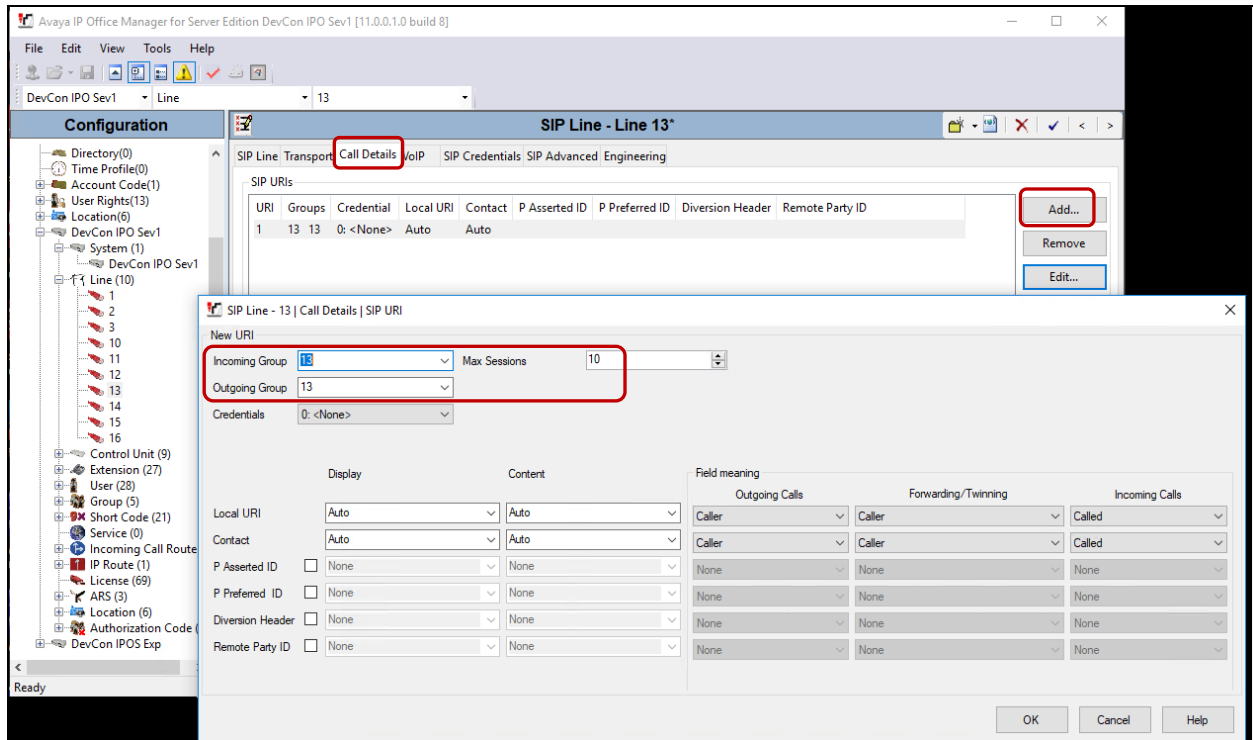
Select the **Transport** tab in the right pane and configure the following:

- **ITSP Proxy Address:** IP address of the Responder SIP Server.
- Under **Network Configuration** → **Layer 4 protocol**, select “UDP” and its **Send port** as “5060”.

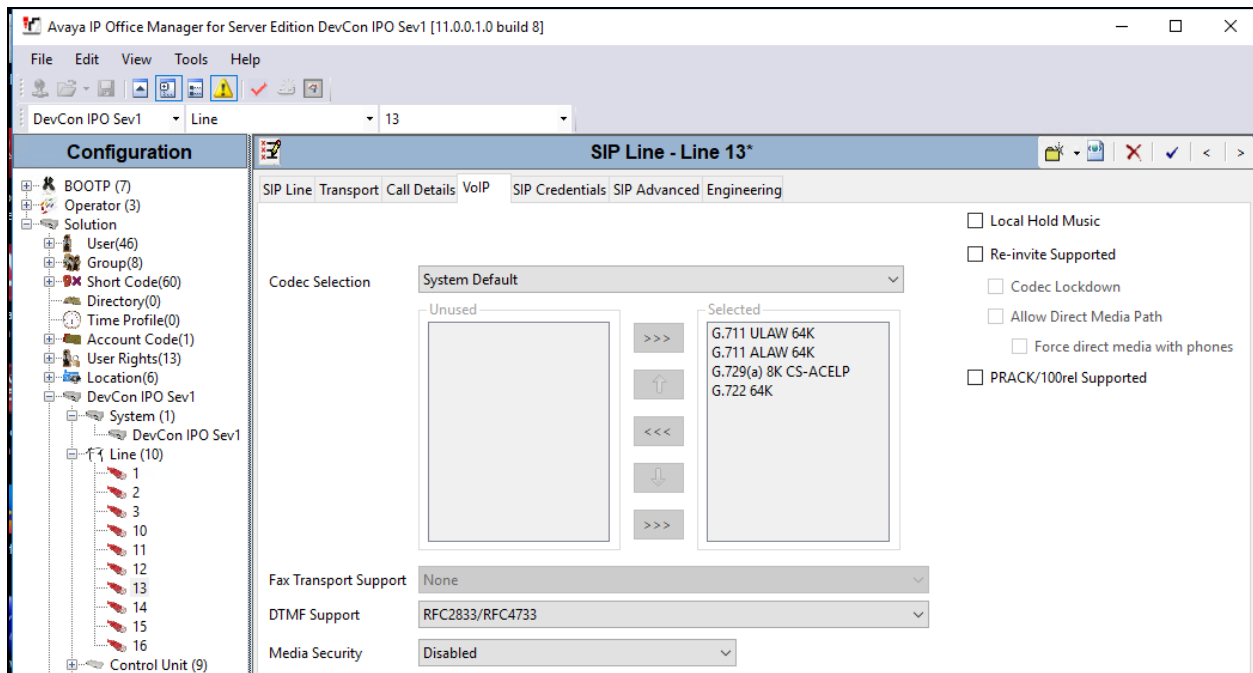
Retain default values for all other fields.



Select the **Call Details** tab and under **SIP URIs** click on **Add** to display the **New URI** section. Screen below shows the already added new SIP URI. Enter an unused group number such as “13” for **Incoming Group** and **Outgoing Group**. Set **Max Sessions** to the maximum number of simultaneous calls allowed, during compliance testing “10” was configured. Retain the default values in the remaining fields. Click **OK**.

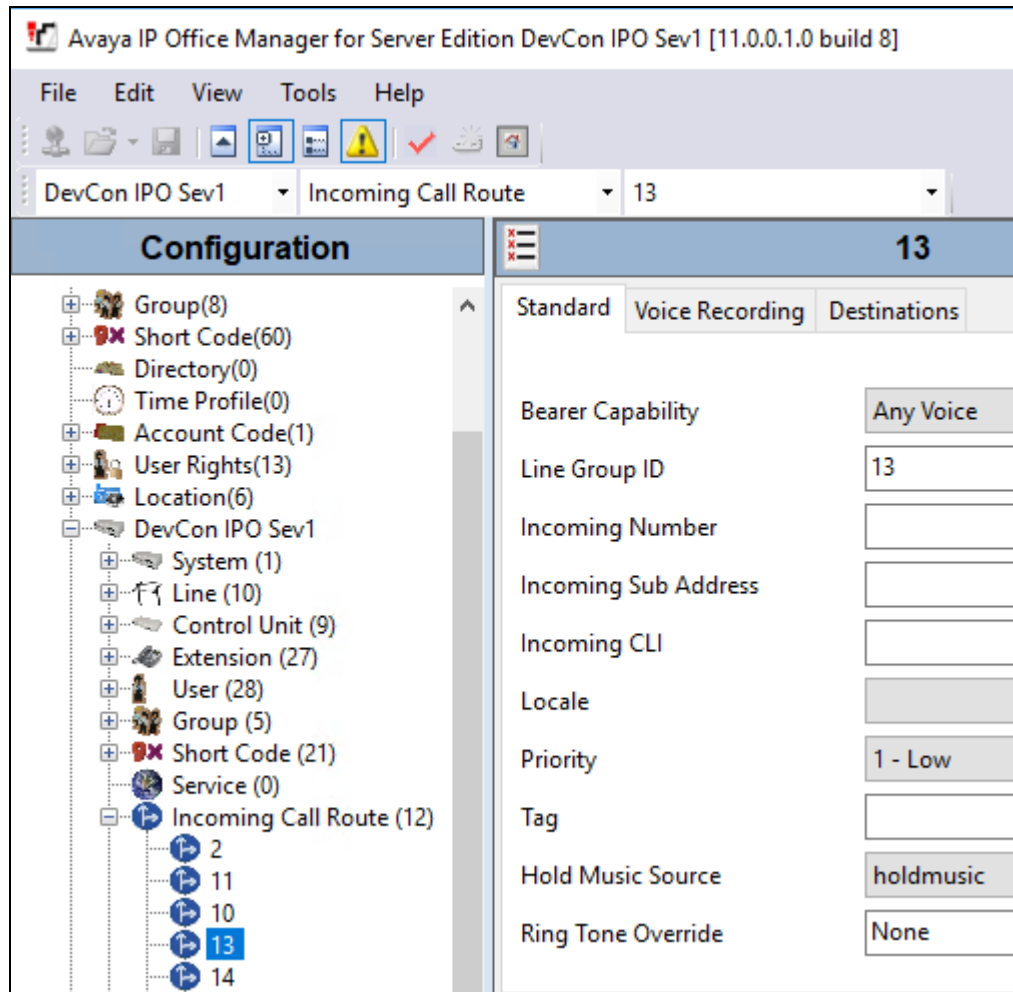


Select the **VoIP** tab. The default **Codec Selection** in the system is shown below and the same was used for compliance testing. Note that Responder only supports **G.711ULAW** codec as mentioned in **Section 2.2**.

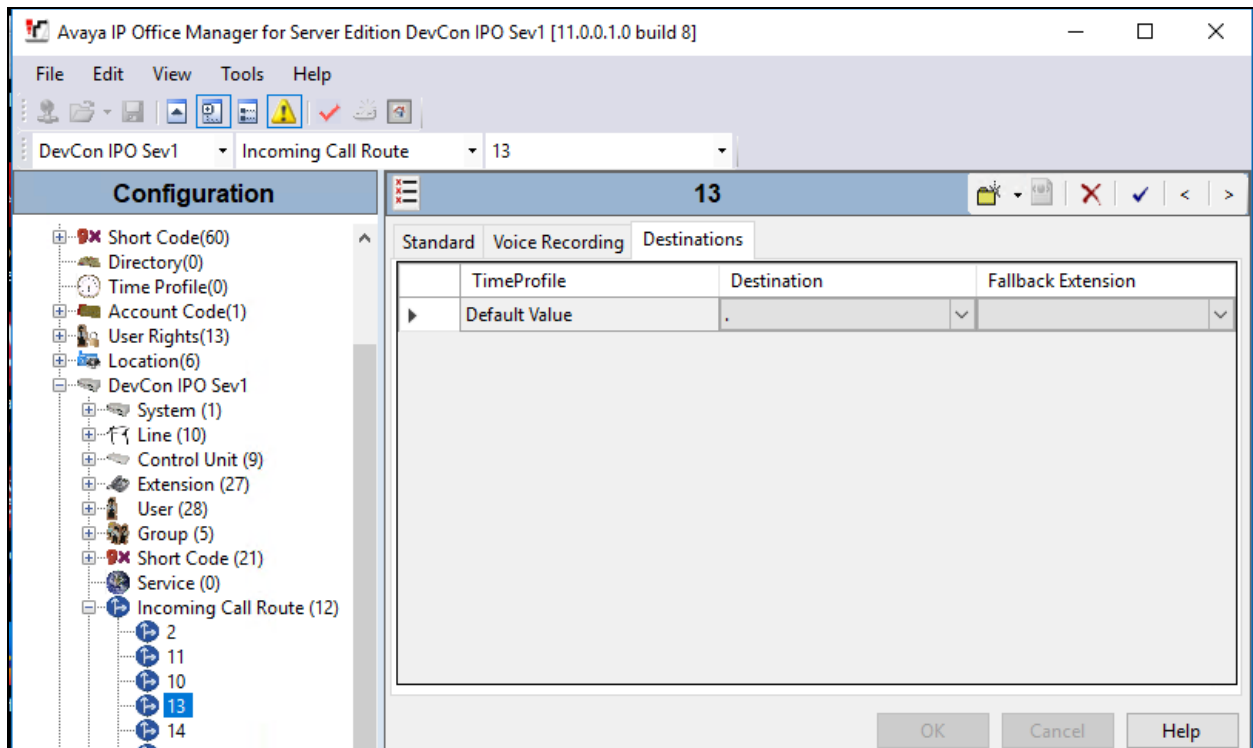


## 5.6. Administer Incoming Call Route

From the configuration tree seen in the left pane, right-click on the **Incoming Call Route**. Select **New** from the pop-up list (not shown) to add a new route. For **Line Group Id**, select the incoming group number from **Section 5.5**, in this case “13”. Retain default values for all other fields.



Select the **Destinations** tab. For **Destination**, enter “.” to match any dialed number from Responder and click on the **OK** button to complete the configuration.





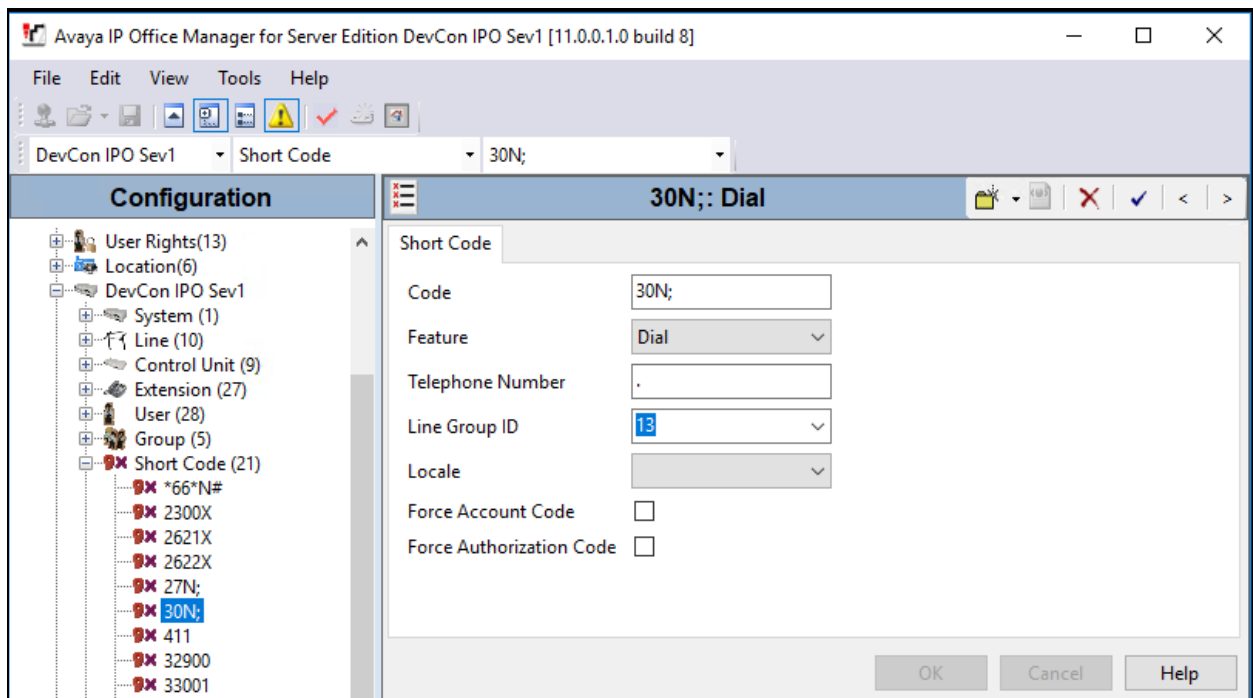
## 5.7. Administer Short Code

From the configuration tree in the left pane, right-click on **Short Code** and select **New** from the pop-up list (not shown) to add a new short code to route calls to Responder. In the compliance testing, 30xxx dialing plan was used for calls to be routed over the SIP trunks to Responder.

Configure the following values:

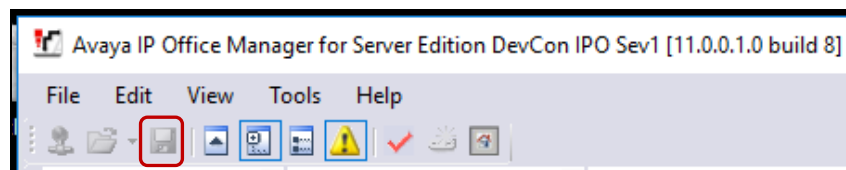
- **Code:** Enter “30N;”.
- **Feature:** Keep the default value of “Dial”.
- **Telephone Number:** Enter “.”.
- **Line Group ID:** Select “13” which is the outgoing group number configured in **Section 5.5**.

Retain default values for all other fields and click on **OK** to complete the configuration.



## 5.8. Save Configuration

Navigate to **File → Save Configuration** (not shown) in the menu bar at the top of the screen or click on the **Save** Icon as shown below to save the configuration performed in the preceding sections.



## 6. Configure Rauland Responder Enterprise

The Responder solution is typically implemented by Rauland engineers or their resale partners. When integrated with a third-party SIP PBX, it is always deployed with a Rauland SIP Server which serves two purposes. First, Rauland SIP Server is commonly deployed with a variety of SIP capable PBX solutions giving the Responder equipment a common and predictable SIP interface that is adaptable to many environments. Second, the Rauland SIP Server can provide registrar services without requiring provisioning for each Responder endpoint thus significantly reducing the implementation and ongoing administration of the solution.

The Responder equipment will be provisioned completely by Rauland engineers based on site requirements and will be configured to use the Rauland SIP server for all calls destined to endpoints outside of the Responder endpoints.

The focus of this section will be on administration of the Responder applications, and configuration of the Rauland SIP Server to properly route SIP calls and RTP.

## 6.1. Rauland Responder Enterprise Configuration Details

Administration for the solution required the following steps:

- Configure Endpoints
- Assign Endpoints to User
- User Login and Device Assignment
- Assign Staff to Patient Rooms

### 6.1.1. Configure Endpoints

Typically, hospital staff use wireless phones to enable instant communications with staff and patient rooms. During this compliance testing, a variety of H.323 and SIP deskphones which were previously configured on IP Office were administered in the Responder applications to associate the endpoints with the hospital staff.

The Responder applications are accessed from the Windows PC used by a staff administrator and/or at nurse stations throughout the hospital. These PCs are used by staff to clock in and manage patient room assignments. The applications are launched from **Start → All Programs → Responder 5 Applications**.

In the top left corner is a drop-down list that navigates to the various applications. Each requires an appropriate login (not shown). Select **Administration → Devices** in the upper left drop-down list (not shown) to add or modify phones. Enter the appropriate **Device Name/Extension**, **Type**, and a **Description**. The illustration below shows several devices used in the test environment, extensions “26xxx” were H.323 and SIP devices administered on IP Office.

Click **OK** at the bottom of the screen (not shown) to complete edits on this screen.

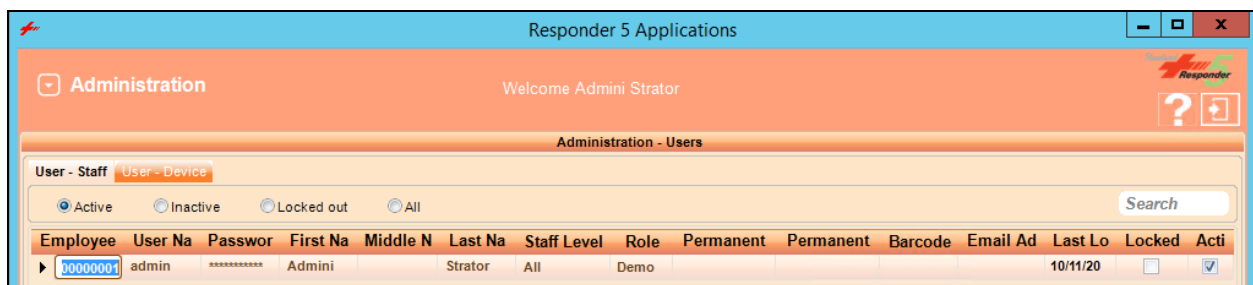
Facility Name	Device Name/Extension	Type	Description	Barcode	Currently Assigned To	User Device	Active	SIP Cancel
▶ All	26003@5.207	Wireless P				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All	26009@5.207	Wireless Phon				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All	26109@5.207	Wireless Phon				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All	26114@5.207	Wireless Phon			Admini Strator	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
*						<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

### 6.1.2. Assign Endpoints to User

Select **Administration** → **Devices** in the upper left drop-down list (not shown) to add or modify users and to assign devices to the users. This task is only necessary for statically assigned device assignments. Users who share devices can enter the device they are using for a shift when they login as described in **Section 6.1.3**.

Users can be created or modified on the **User** → **Creation** tab (user creation is beyond the scope of these application notes, see Responder documentation for details of this task). Devices (phones) are created on the **User - Device** tab as shown below.

Click **OK** (not shown) to complete edits on this screen.



### 6.1.3. User Login and Device Assignment

At the beginning of a shift, or return to duty from breaks, users will scan their Hospital ID badge bar code with a scanner connected to the PC which will automatically log them in to the **My Profile** screen.

From this screen, a **Wireless Phone** and/or **Pager** number can be entered; duty status updated, and break status entered. The **My Assignments** and **My Preferences** tabs are available for staff to review the patient rooms they are assigned to and modify user preferences. The details of these tasks are beyond the scope of these Application Notes.

Click **Update** or **Update and Exit** (not shown) to commit the changes.

Responder 5 Applications

Welcome Admini Strator

My Profile

My Status My Assignments My Preferences

User

B... Strator, Admini ID...

This is a built-in...

☒ Call ☐ Serv ☒ Urgt

Phone 26003@...

1

2

3

Close

My Status Demo

Devices

Please scan or enter your wireless device (s):

Wireless Phone 26003@

Additional De...

Location Ba...

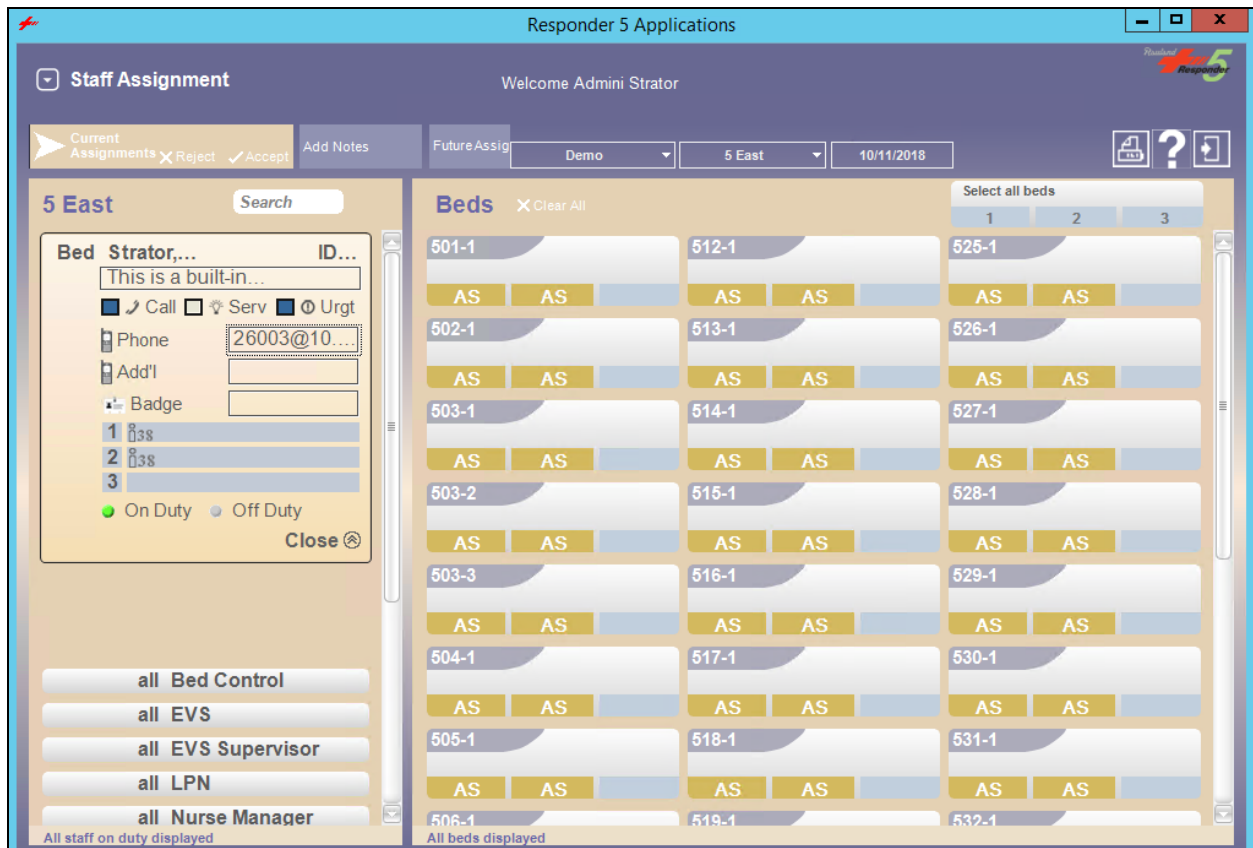
Update Update and Exit

Duty

5 East	ON	OFF
All	ON	OFF
All Units	ON	OFF
Bed Control	ON	OFF
Code Blue	ON	OFF
EVS	ON	OFF
EVS 5 East	ON	OFF
EVS Surgery	ON	OFF

#### 6.1.4. Assign Staff to Patient Rooms

This task is typically performed by shift supervisors. Staff can be assigned to patient rooms on the **Staff Assignment** screen which is accessed from the drop-down menu at the upper left of the Responder 5 Applications. In the illustration below, “26003” is assigned to a room “501-1” by clicking on the Staff name in the left column, then clicking on the assignment space below the patient name. The staff member’s initials will appear as below when the staff member has been successfully assigned to a patient.



## 6.2. Configure Rauland SIP Server

All administration is performed via web browser by navigating to the hostname or IP Address of the Rauland SIP Server. Administration for the solution required the following steps:

- Login to SIP Server System
- Configure SIP Server System Tab
- Configure SIP Server SIP Tab
- Configure SIP Server RTP Tab
- Configure Dial Plan Routing Rules

### 6.2.1. Login to SIP Server System

Launch the SIP Server Sign in page by opening a web browser and typing the following in the URL <http://<IP Address>:18080/sip/>, where IP Address is the address of the SIP Server. Enter a valid **User** and **Password** and click on the **SIGN IN** button.



The screenshot shows the login interface for the Rauland Responder SIP Server. At the top left is the Rauland Responder logo, and at the top right is a blue header bar with the text "SIP Server". In the center, the text "Sign in" is displayed in green. Below this, a red-bordered box contains a warning message: "This is a LAB use license. This license is issued to be used only for internal LAB use by the organization to whom it has been issued, and not for any other purposes." Underneath the warning box are two input fields: "User" and "Password". Below the "Password" field is a checkbox labeled "REMEMBER ME". At the bottom of the form is a large green button labeled "SIGN IN".

## 6.2.2. Configure SIP Server System Tab

The following **System** properties were pre-configured for the test environment.

The screenshot shows the Raoulnd Responder web interface. The left sidebar contains a navigation menu with categories: SIP Server (RAULAND, SIP-TAP Settings, SIP SERVER), Registered Clients, Active Sessions, User Authentication, Dial Plan, Aliases, Logs, CDR, Push Notification, Domains, Configuration, SYSTEM, and MAINTENANCE. The main content area is titled 'System' and has tabs for System, SIP, RTP, Database/Radius, and Advanced. The 'System' tab is active, showing a 'General' section with fields for Server Name (your-sip-sv), Server Description (your SIP Server), and Server Location (your-place). Below this is a 'Network' section with fields for Interface address 1 through 5, Remote Address Pattern 1 through 5, Auto interface discovery (radio buttons for on and off, with 'off' selected), External IP address pattern, and Internal IP address pattern.

System	SIP	RTP	Database/Radius	Advanced
<h3>System</h3> <p><b>General</b></p> <p>Server Name: <input type="text" value="your-sip-sv"/></p> <p>Server Description: <input type="text" value="your SIP Server"/></p> <p>Server Location: <input type="text" value="your-place"/></p> <p><b>Network</b></p> <p>Interface address 1: <input type="text"/></p> <p>Remote Address Pattern 1: <input type="text"/></p> <p>Interface address 2: <input type="text"/></p> <p>Remote Address Pattern 2: <input type="text"/></p> <p>Interface address 3: <input type="text"/></p> <p>Remote Address Pattern 3: <input type="text"/></p> <p>Interface address 4: <input type="text"/></p> <p>Remote Address Pattern 4: <input type="text"/></p> <p>Interface address 5: <input type="text"/></p> <p>Remote Address Pattern 5: <input type="text"/></p> <p>Auto interface discovery: <input type="radio"/> on <input checked="" type="radio"/> off</p> <p>External IP address pattern: <input type="text"/></p> <p>Internal IP address pattern: <input type="text"/></p>				



IPv6

IPv6

☐ on ☒ off

RFC3484's policy table for Address Selection

☐ on ☒ off

DNS

DNS SRV

☐ on ☒ off

DNS AAAA

☐ on ☒ off

DNS Server

DNS SRV Failover

☐ on ☒ off

Caching period for resolved name (sec)

Caching period for unknown name (sec)

Caching period for error (sec)

UPnP

Enable/Disable

☐ enable ☒ disable

Default router IP address

Cache size

Cache period (sec,0=disable)

Refresh Interval (sec,0=disable)

Java

Java VM arguments

< MENU

Save

Your changes will be in effect after restart.

### 6.2.3. Configure SIP Server SIP Tab

The following SIP properties were pre-configured for the test environment.

**SIP Server**

**RAULAND**

SIP-TAP  
Settings

**SIP SERVER**

Registered Clients  
Active Sessions  
User Authentication  
Dial Plan  
Aliases  
Logs  
CDR  
Push Notification  
Domains  
Configuration

**SYSTEM**

**MAINTENANCE**

Start/Shutdown  
Software Maintenance

**SIP**

This is a LAB use license.

**SIP exchanger**

Session Limit (-1=unlimited)

Local Port

B2B-UA mode ☐ on ☒ off

Check Maximum UDP packet size ☐ on ☒ off

Maximum UDP packet size

**NAT traversal**

Keep address/port mapping ☒ on ☐ off

Interval (ms)

Method ☐ Blank packet ☒ OPTIONS

Add 'rport' parameter (Send) ☐ on ☒ off

Add 'rport' parameter (Receive) ☐ on ☒ off

**Authentication**

REGISTER ☐ on ☒ off

INVITE ☐ on ☒ off

MESSAGE ☐ on ☒ off

SUBSCRIBE ☐ on ☒ off

Realm (ex: domain name)

Auth-user=user in "To:" (Register) ☐ yes ☒ no

Auth-user=user in "From:" ☐ yes ☒ no

Terminating character for user-info

FQDN only ☐ yes ☒ no

Nonce Expires (seconds)

**Registration**

Adjusted Expires

<b>Upper Registration</b>	
On/Off	<input type="radio"/> on <input checked="" type="radio"/> off
Register Server	<input type="text"/>
Protocol	<input checked="" type="radio"/> UDP <input type="radio"/> TCP <input type="radio"/> TLS
<b>Thru Registration</b>	
On/Off	<input checked="" type="radio"/> on <input type="radio"/> off
<b>Timeout (0=unlimited)</b>	
Ringing Timeout (ms)	<input type="text" value="240000"/>
Talking Timeout (ms)	<input type="text" value="259200000"/>
Upper/Thru Timeout(ms)	<input type="text" value="40000"/>
<b>Dial Plan</b>	
Maximum history records	<input type="text" value="50"/>
<b>Miscellaneous</b>	
100 Trying	<input type="radio"/> any requests <input checked="" type="radio"/> only for initial
Check Request-URI's validity	<input type="radio"/> yes <input checked="" type="radio"/> no
Server/User-Agent	<input type="text"/>
<b>TCP</b>	
TCP-handling	<input checked="" type="radio"/> on <input type="radio"/> off
Queue Size	<input type="text" value="50"/>
Maximum Active Connections (0=unlimited)	<input type="text" value="0"/>
<b>TLS</b>	
TLS-handling	<input type="radio"/> on <input checked="" type="radio"/> off
Queue Size	<input type="text" value="50"/>
Maximum Active Connections (0=unlimited)	<input type="text" value="0"/>
Enable TLS 1.0 or older	<input checked="" type="radio"/> enable <input type="radio"/> disable
Request Client Certificate	<input type="radio"/> on <input checked="" type="radio"/> off

WS (WebSocket)

WS-handling

☐ on
☒ off

Listen port

10080

Queue Size

50

Maximum Active Connections (0=unlimited)

0

WSS (WebSocket over TLS)

WSS-handling

☐ on
☒ off

Listen port

10081

Queue Size

50

Maximum Active Connections (0=unlimited)

0

Key and Certificate

Peer Certification Validation

☒ on
☐ off

File Type

☒ Certificate (.pem .der .cer .crt .ce

Private Key File

No File

Browse...

No

Certificate File

No File

Browse...

No

Performance Optimization (Proxy)

Initial threads

10

Maximum Sessions per thread

50

Performance Optimization (Registrar)

Initial threads

0

Maximum Sessions per thread

10

Performance Optimization (Dispatcher)

Multiple Dispatcher

☐ yes
☒ no

Number of Dispatchers

8

<

MENU

Save

Your changes will be in effect after restart.

RS; Reviewed:  
SPOC 1/7/2019

Solution & Interoperability Test Lab Application Notes  
©2019 Avaya Inc. All Rights Reserved.

28 of 34  
REnt\_IPO11

## 6.2.4. Configure SIP Server RTP Tab

On the **RTP** screen, set **RTP Relay** to “on”, **RTP relay (UA on this machine)** to “auto” and **RTP relay even with ICE** to “no” and click **Save** to complete entries. Note, the **Minimum** and **Maximum Port** range settings should be sufficient to handle the maximum number of concurrent RTP sessions between systems.

The screenshot shows the Raoulant Responder web interface. The left sidebar contains a menu with categories: SIP Server (RAULAND), SIP SERVER, SYSTEM, and MAINTENANCE. The main content area is titled 'RTP' and contains several configuration sections. A red box at the top states 'This is a LAB use license.' The 'RTP exchanger' section includes settings for RTP relay (on), RTP relay (UA on this machine) (auto), RTP relay even with ICE (no), Minimum Port (10000), Maximum Port (29999), Minimum Port (Video) (0), Maximum Port (Video) (0), Port mapping (source port), Send UA's remote address (auto), and Send before receiving (behind NAT) (no). The 'Timeout (0=unlimited)' section shows RTP Session Timeout (ms) set to 600000. The 'Identify Media Streams' section includes Label Attribute (RFC4574) (on), Content Attribute (RFC4796) (on), and Order of the 'm' line (on). A 'Save' button is at the bottom, with a note: 'Your changes will be in effect after restart.'

System	SIP	RTP	Database/Radius	Advanced
<b>RTP</b>				
This is a LAB use license.				
<b>RTP exchanger</b>				
RTP relay		<input checked="" type="radio"/> on <input type="radio"/> auto		
RTP relay (UA on this machine)		<input checked="" type="radio"/> auto <input type="radio"/> off		
RTP relay even with ICE		<input type="radio"/> yes <input checked="" type="radio"/> no <input type="radio"/> auto		
Minimum Port		<input type="text" value="10000"/> 5000 RTP sessions available with these port settings.		
Maximum Port		<input type="text" value="29999"/>		
Minimum Port (Video)		<input type="text" value="0"/> 0 RTP sessions (Video) available with these port settings.		
Maximum Port (Video)		<input type="text" value="0"/>		
Port mapping		<input type="radio"/> sdp <input checked="" type="radio"/> source port		
Send UA's remote address		<input type="radio"/> yes <input type="radio"/> no <input checked="" type="radio"/> auto		
Send before receiving (behind NAT)		<input type="radio"/> yes <input checked="" type="radio"/> no		
<b>Timeout (0=unlimited)</b>				
RTP Session Timeout (ms)		<input type="text" value="600000"/>		
<b>Identify Media Streams</b>				
Label Attribute (RFC4574)		<input checked="" type="radio"/> on <input type="radio"/> off		
Content Attribute (RFC4796)		<input checked="" type="radio"/> on <input type="radio"/> off		
Order of the 'm' line		<input checked="" type="radio"/> on <input type="radio"/> off		
<b>Save</b>		Your changes will be in effect after restart.		

**Dial Plan** rules that was used is illustrated below. For calls routing from Session Manager, the **DELETE Inbound Call** rule was used. For calls routing to IP Office, the **To IPOffice** rule was used.

RS; Reviewed: Solution & Interoperability Test Lab Application Notes 30 of 34  
SPOC 1/7/2019 ©2019 Avaya Inc. All Rights Reserved. REnt IPO11

## 7. Verification Steps

Calls were placed to and from Responder endpoints, and two-way audio was confirmed. The nature of these devices is simple, one-way communications with Hospital staff; complex calls like transfer and conference are not supported on the patient room devices.

On the Responder SIP Server, the **Registered Clients** screen will confirm if Responder endpoints are successfully registered as shown below.

**Registered Clients**

This is a LAB use license.

Show Filter

Unregister

User	Contact URI (Source IP Address)	Details
<input type="checkbox"/> 30505@207	sip:30505@207:60219 (207.60219)	Expires : 3600 Priority User Agent : X-Lite release 5.3 Transport : UDP Time Update : Thu Oct 11 13:0
<input type="checkbox"/> a5*r501*b1@50f13e83-94b7-e811-8114-0800273baef6.r5demo-srv.dev-r5ead.net	sip:a5*r501*b1@r5demo-srv.dev-r5ead.net:5060 (208.5060)	Expires : 3600 Priority User Agent : R5E.Agent Transport : UDP Time Update : Thu Oct 11 13:3
<input type="checkbox"/> a5*r501*b101@50f13e83-94b7-e811-8114-0800273baef6.r5demo-srv.dev-r5ead.net	sip:a5*r501*b101@r5demo-srv.dev-r5ead.net:5060 (208.5060)	Expires : 3600 Priority User Agent : R5E.Agent Transport : UDP Time Update : Thu Oct 11 13:3
<input type="checkbox"/> a5*r501*b102@50f13e83-94b7-e811-8114-0800273baef6.r5demo-srv.dev-r5ead.net	sip:a5*r501*b102@r5demo-srv.dev-r5ead.net:5060 (208.5060)	Expires : 3600 Priority User Agent : R5E.Agent Transport : UDP Time Update : Thu Oct 11 13:3
<input type="checkbox"/> a5*r503*b1@50f13e83-94b7-e811-8114-0800273baef6.r5demo-srv.dev-r5ead.net	sip:a5*r503*b1@r5demo-srv.dev-r5ead.net:5060 (208.5060)	Expires : 3600 Priority User Agent : R5E.Agent Transport : UDP Time Update : Thu Oct 11 13:3
<input type="checkbox"/> a5*r503*b2@50f13e83-94b7-e811-8114-0800273baef6.r5demo-srv.dev-r5ead.net	sip:a5*r503*b2@r5demo-srv.dev-r5ead.net:5060 (208.5060)	Expires : 3600 Priority User Agent : R5E.Agent Transport : UDP Time Update : Thu Oct 11 13:3

From the **IP Office System Status** window, user can see the status of the SIP trunk connectivity to the Responder SIP Server and the state of the channels. Screen below shows the SIP trunk “In Service” state and one of the channels on an active call.

The screenshot displays the AVAYA IP Office System Status window. The left sidebar shows a navigation menu with options like System, Alarms (16), Extensions (7), Trunks (10), Line: 1 through Line: 16, Active Calls, Resources, Voicemail, IP Networking, and Locations. The main content area is titled 'IP Office System Status' and has tabs for Status, Utilization Summary, and Alarms. The 'Status' tab is active, showing a 'SIP Trunk Summary' section with the following details:

- Line Service State: In Service
- Peer Domain Name: 10.10.5.207
- Resolved Address: 10.10.5.207
- Line Number: 13
- Number of Administered Channels: 10
- Number of Channels in Use: 1
- Administered Compression: G711 Mu, G711 A, G729 A, G722
- Enable Faststart: Off
- Silence Suppression: Off
- Media Stream: RTP
- Layer 4 Protocol: UDP
- SIP Trunk Channel Licenses: 128
- SIP Trunk Channel Licenses in Use: 1
- SIP Device Features:

A green circular progress indicator shows 0.78% utilization. Below the summary is a table with 15 columns: Channel Number, URI, Call G..., Ref, Current State, Time in State, Remote Media A..., Co..., Conne..., Caller ID or Dial..., Other Party on Call, Direction of Cal, Round Trip D..., Receive Jitter, Receive Packe..., Transmit Jitter, and Transmit Packe... The table shows one active call (Channel 1) and five idle channels (Channels 2-6).

Channel Number	URI	Call G...	Ref	Current State	Time in State	Remote Media A...	Co...	Conne...	Caller ID or Dial...	Other Party on Call	Direction of Cal	Round Trip D...	Receive Jitter	Receive Packe...	Transmit Jitter	Transmit Packe...
1	1	77		Conne...	00:00:19	10.10.5...	G7...	VCM (...)		Extn 26014, Pri	Outgoing	0ms	0ms	0%	0ms	0%
2				Idle	2 days...											
3				Idle	2 days...											
4				Idle	2 days...											
5				Idle	2 days...											
6				Idle	2 days...											

At the bottom of the window, there are buttons for Trace, Trace All, Pause, Ping, Call Details, Graceful Shutdown, Force Out of Service, Print..., and Save As... The status bar at the bottom right shows the time as 4:22:39 PM and the system is Online.



## 8. Conclusion

These Application Notes describe the procedures required to configure Rauland Responder Enterprise to interoperate with endpoints registered to Avaya IP Office Server Edition via direct SIP trunks using a Responder SIP Server as a SIP registrar and Proxy for the Responder side of the solution.

All feature functionality test cases described in **Section 2.1** were passed with the observations pointed in **Section 2.2**.

## 9. Additional References

This section references the product documentation relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Deploying IP Office™ Platform Server Edition Solution*, Release 11.0, May 2018.
- [2] *Deploying IP Office Essential Edition (IP500 V2)*, Release 11.0, 15-601042 Issue 33k - (Tuesday, October 9, 2018).
- [3] *Administering Avaya IP Office™ Platform with Manager*, Release 11.0, Issue 17a, August 2018.

Product information for Rauland products can be found at <http://www.rauland.com/>.

---

**©2018 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).