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.

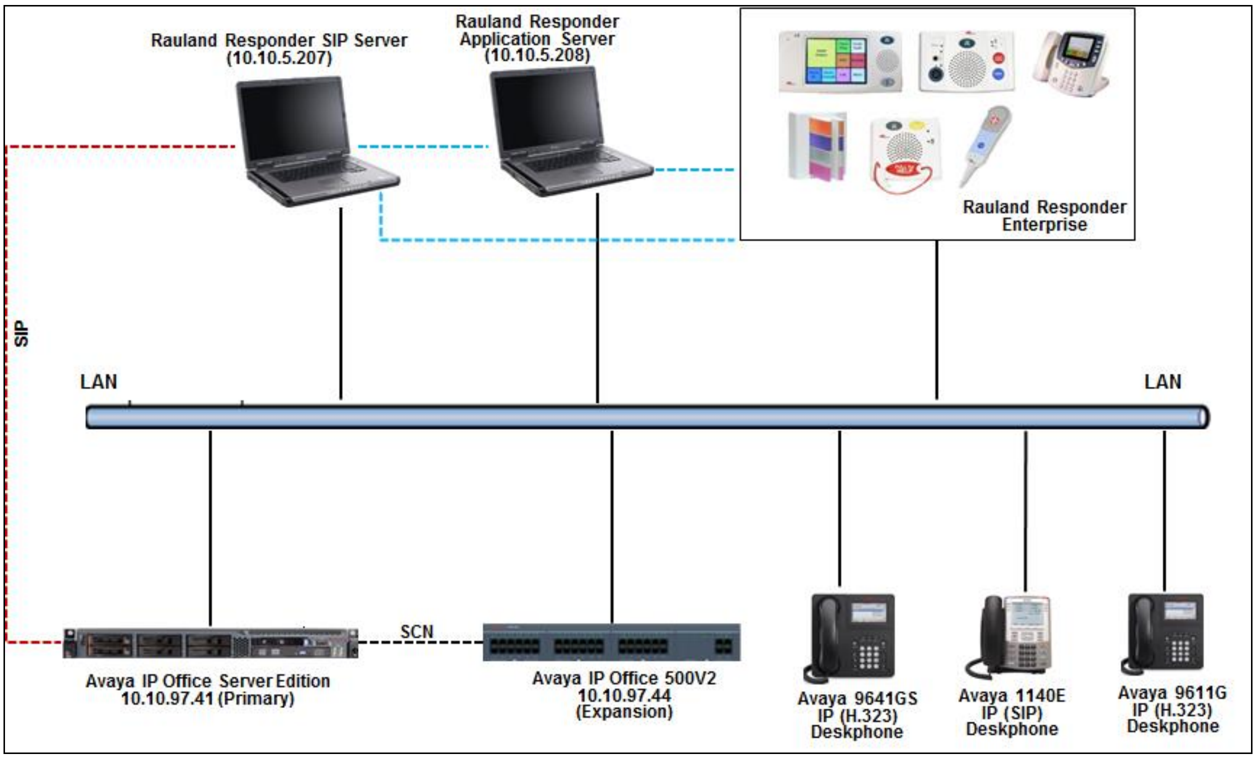


Figure 1 – Rauland Responder Enterprise Compliance Test Configuration

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

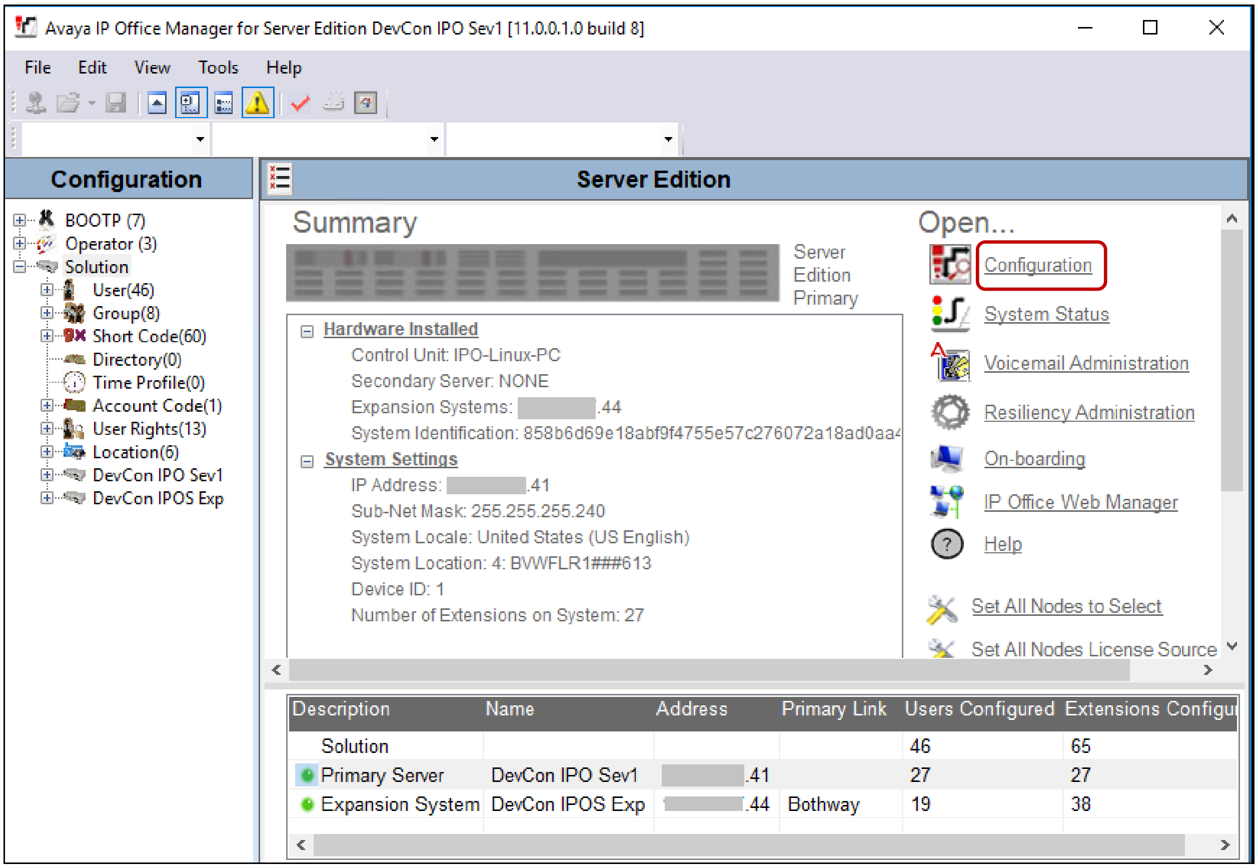
The document assumes that Avaya IP Office Server Edition has been installed and configured to work with a 500V2 expansion. This section only describes the details on how to configure the IP Office Server Edition (Primary) since the SIP line connectivity was only configured between Primary and Responder 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

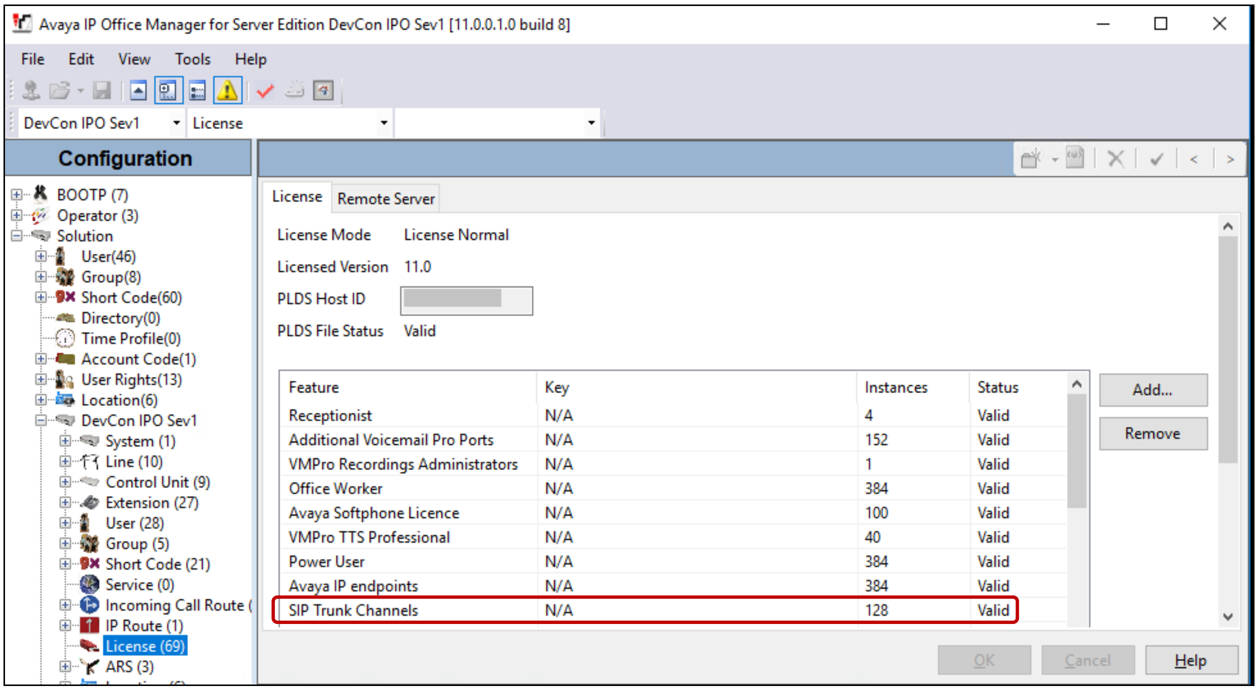
5.1. Launch Avaya IP Office Manager

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.



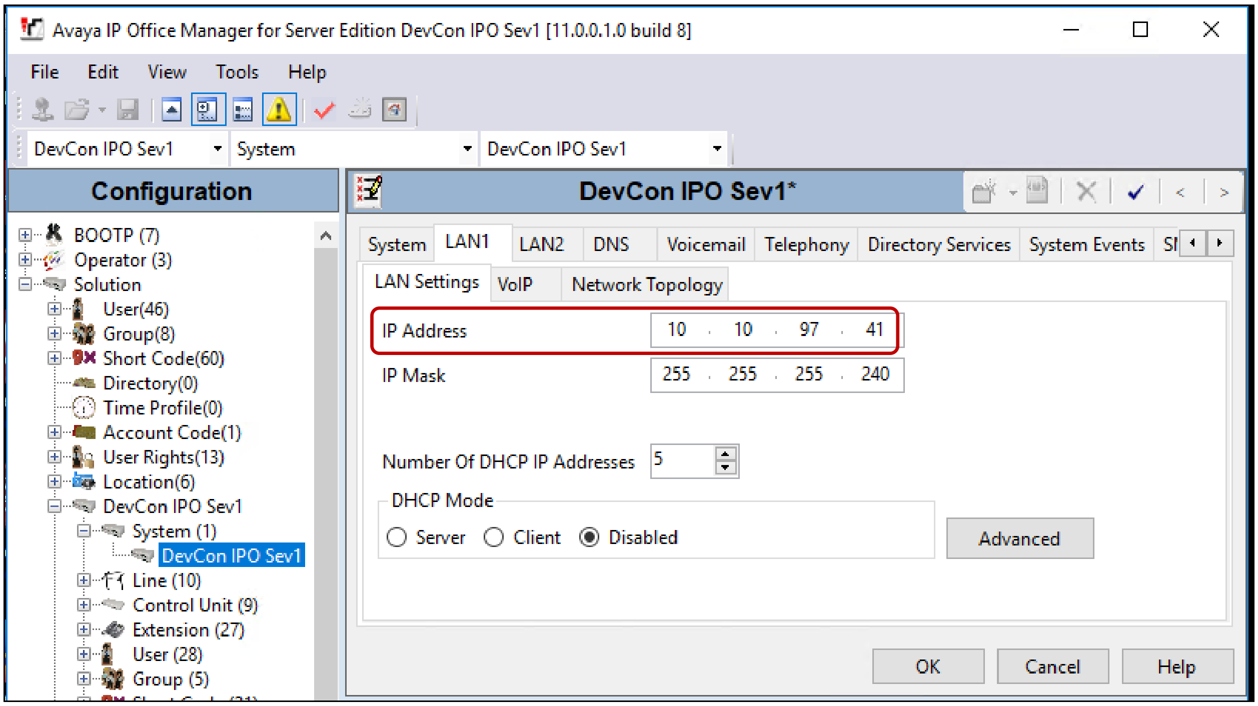
5.2. Verify IP Office License

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

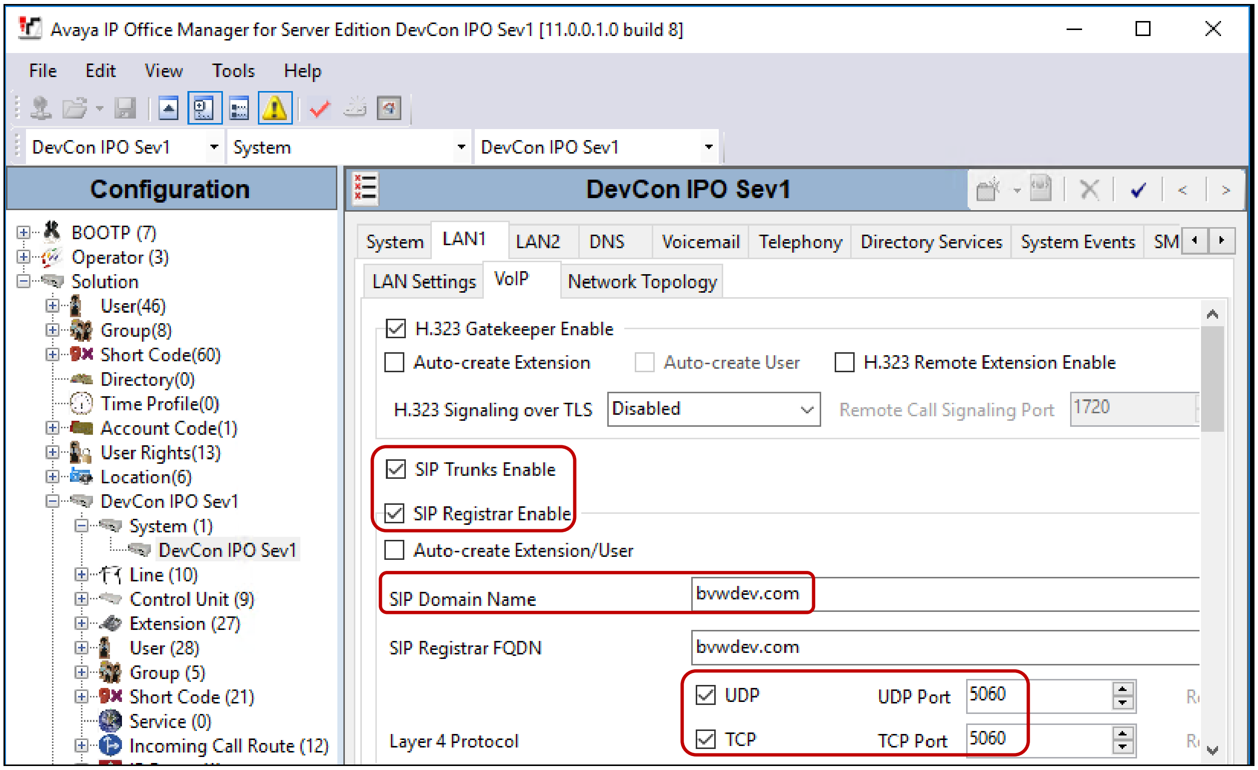
From the configuration tree in the left pane, navigate to **DevCon IPO Sev1 → System (1)** to display the **DevCon IPO Sev1** screen in the right pane, where **DevCon IPO Sev1** is the name of the IP Office Primary system. Select the **LAN1** tab, followed by the **LAN Settings** sub-tab in the right 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 "bvwdev.com" was used.
- Check **UDP** and **TCP** protocol with the correct port numbers.

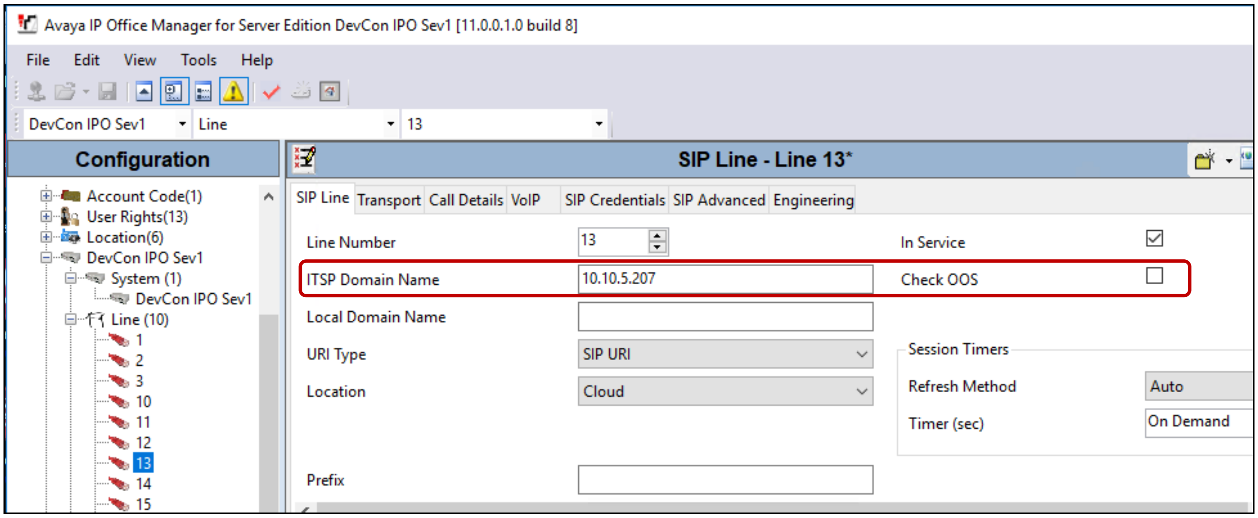


5.5. Administer SIP Line

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.

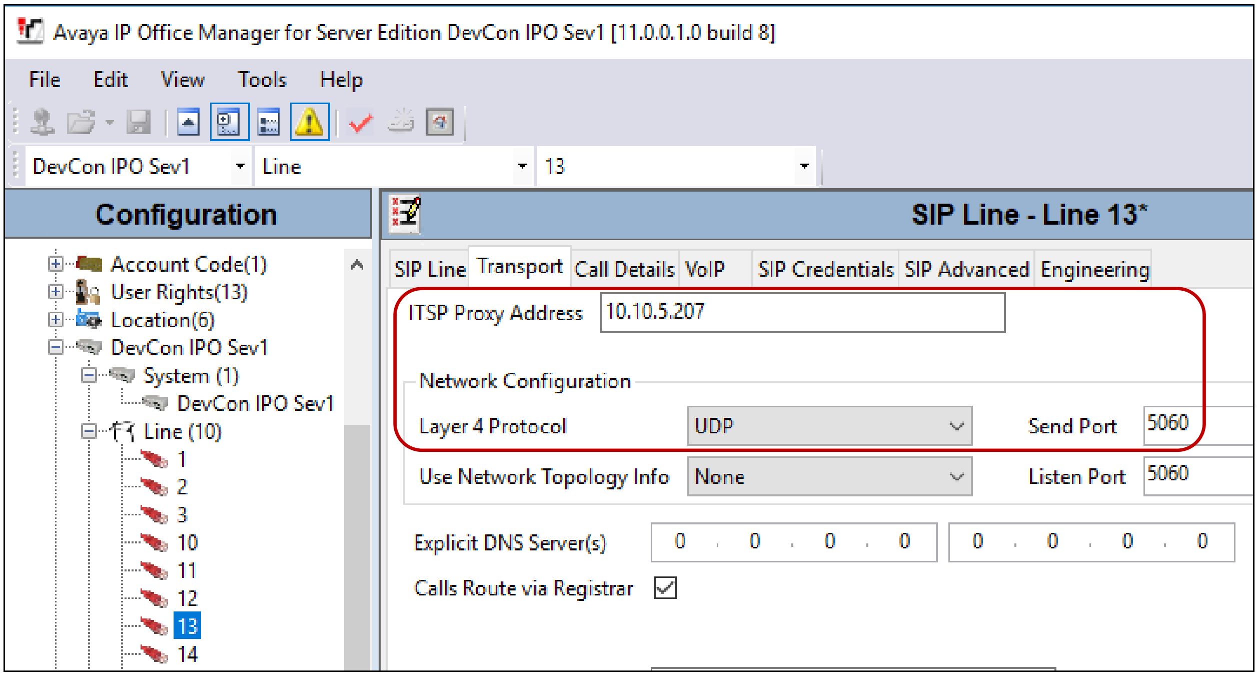
Retain default values for all other fields.



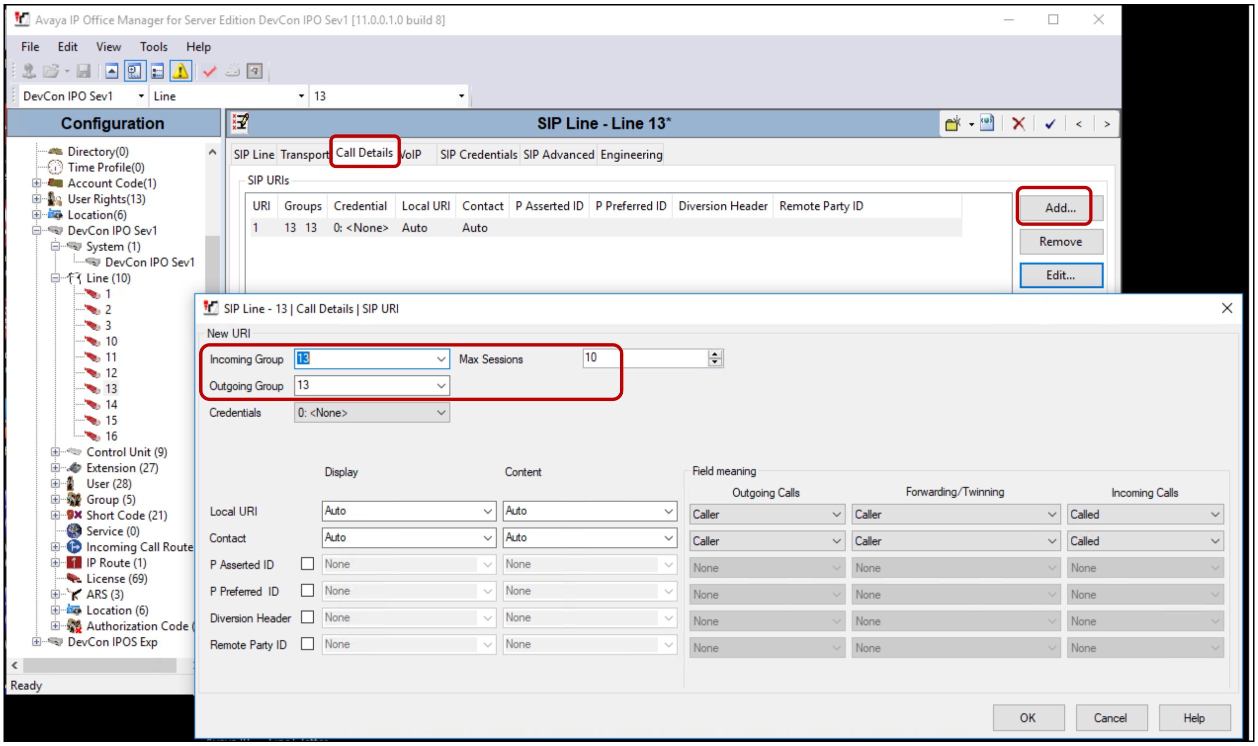
Select the **Transport** tab in the right pane and configure the following:

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

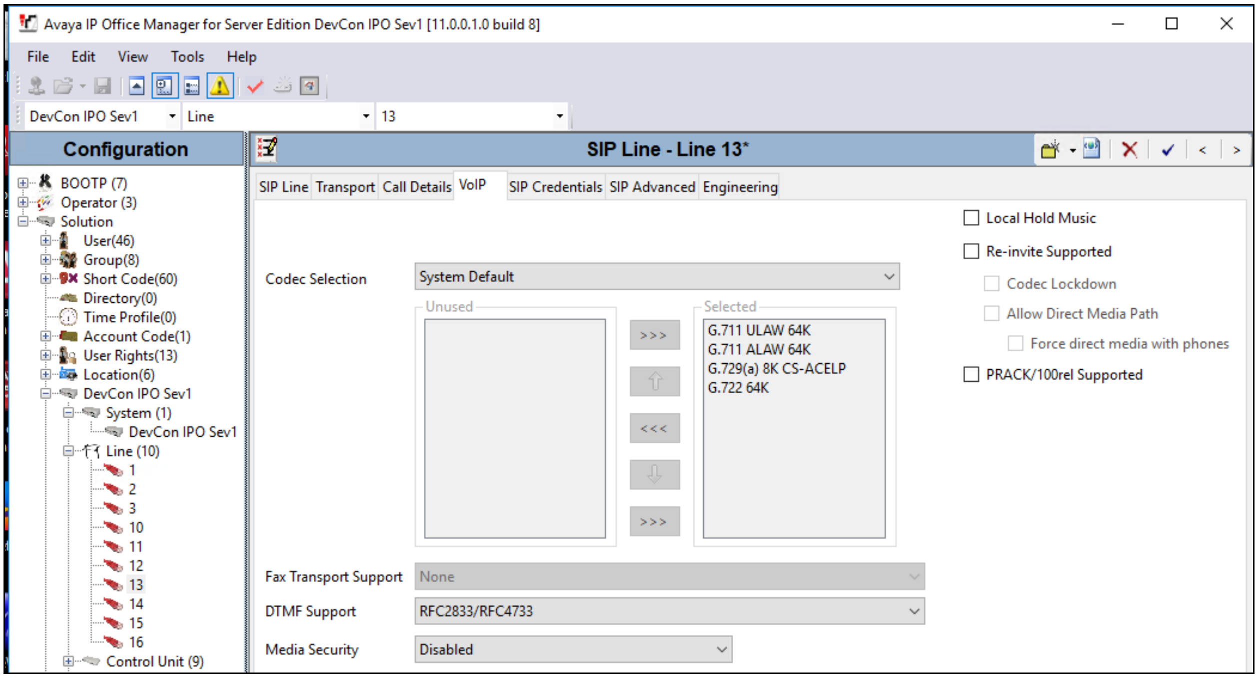
Retain default values for all other fields.



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**.

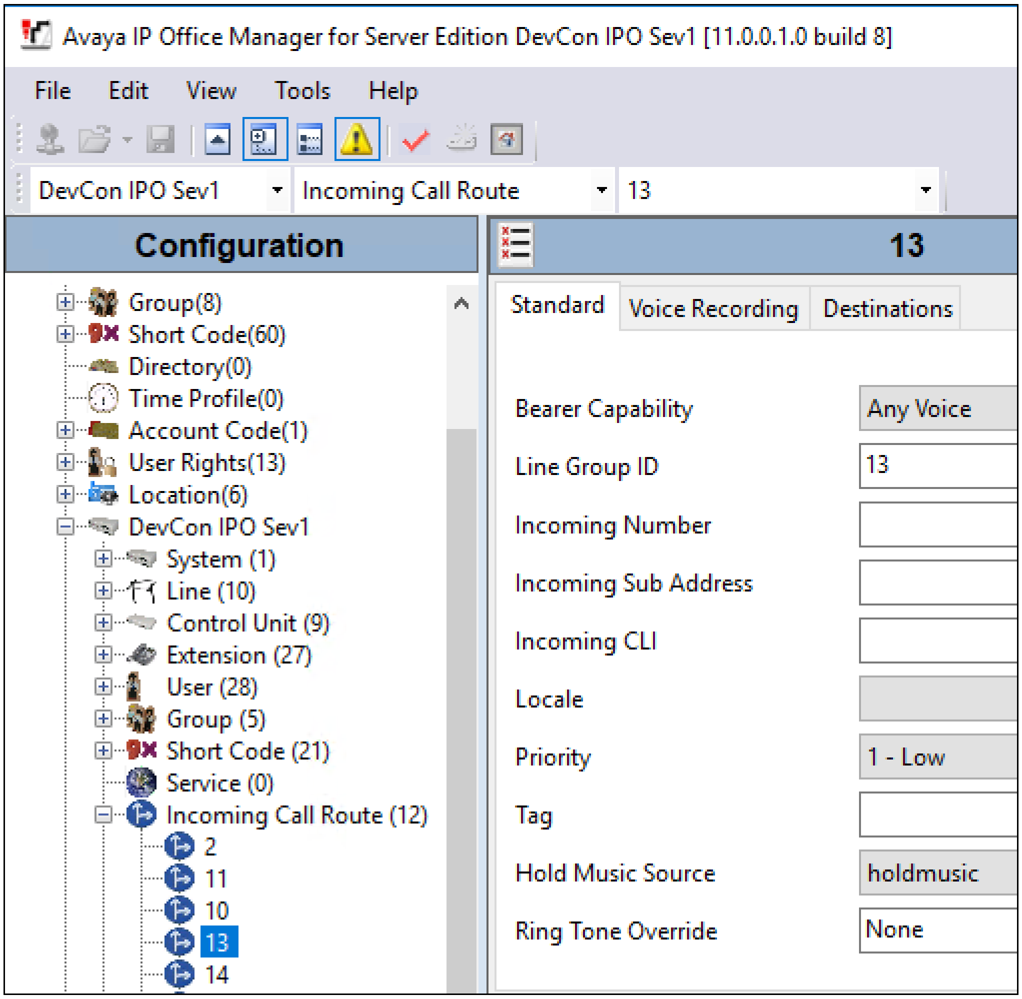


Select the **VoIP** tab. The default **Codec Selection** in the system is shown below and the same was used for compliance testing. Note that Responder only supports **G.711ULAW** codec as mentioned in **Section 2.2**.

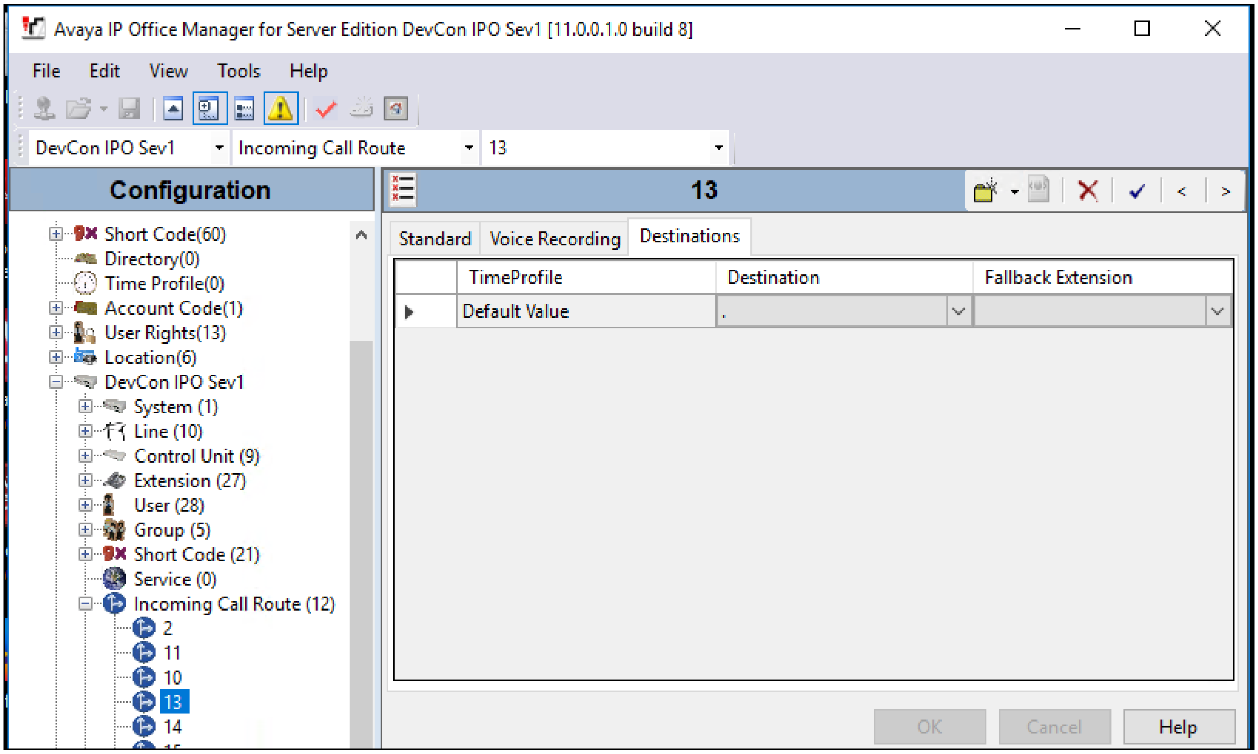


5.6. Administer Incoming Call Route

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.



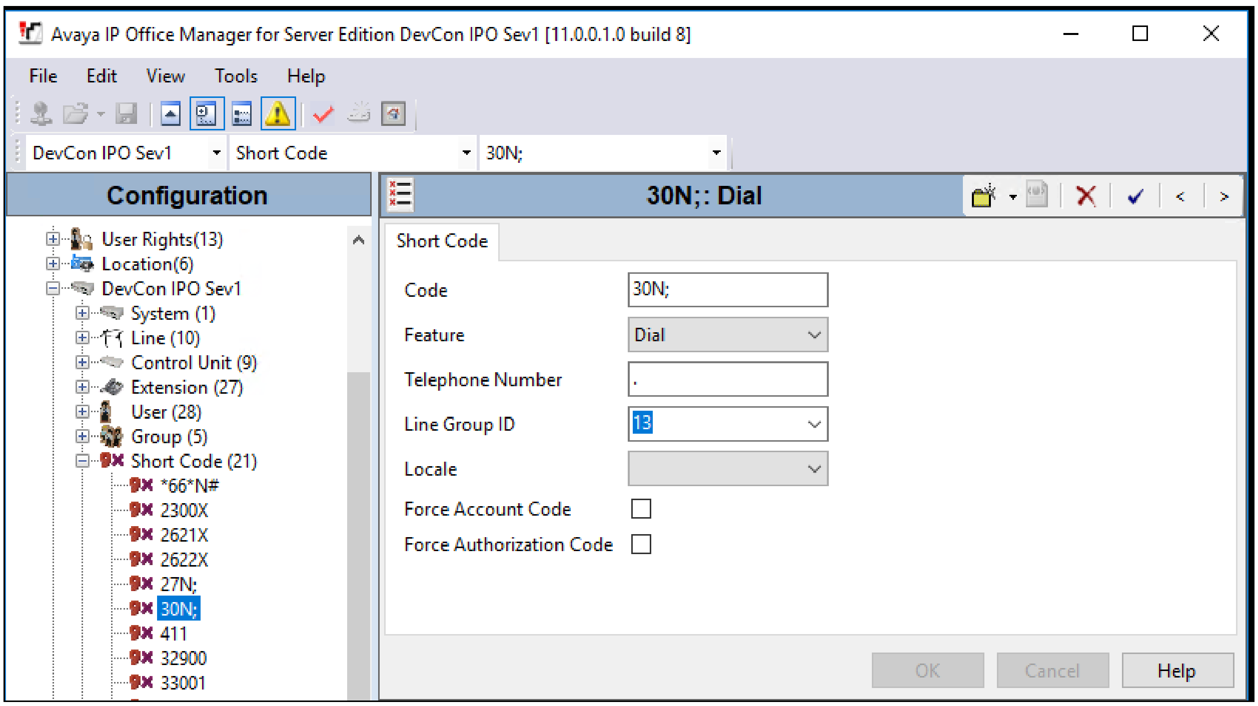
5.7. Administer Short Code

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:

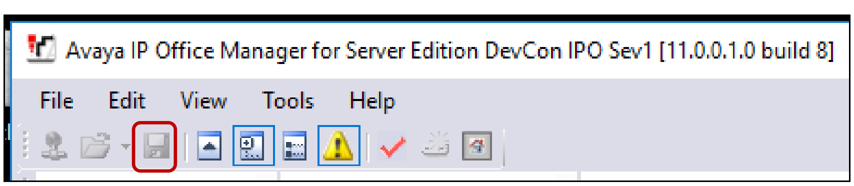
- **Code**: Enter "30N;".
- **Feature**: Keep the default value of "Dial".
- **Telephone Number**: Enter ".".
- **Line Group ID**: Select "13" which is the outgoing group number configured in **Section 5.5.**

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

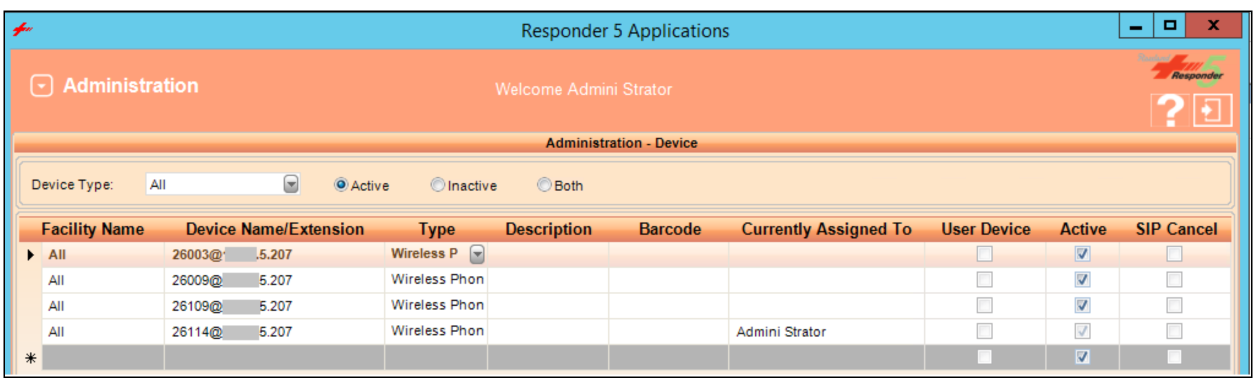
6.1.1. Configure Endpoints

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.

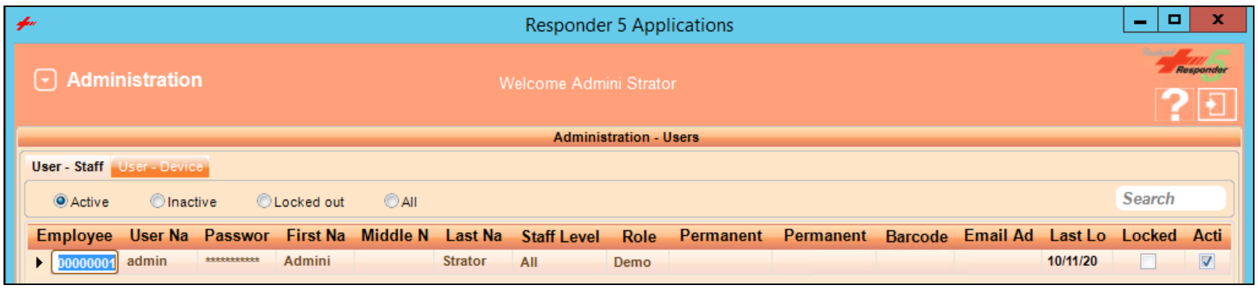


6.1.2. Assign Endpoints to User

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.

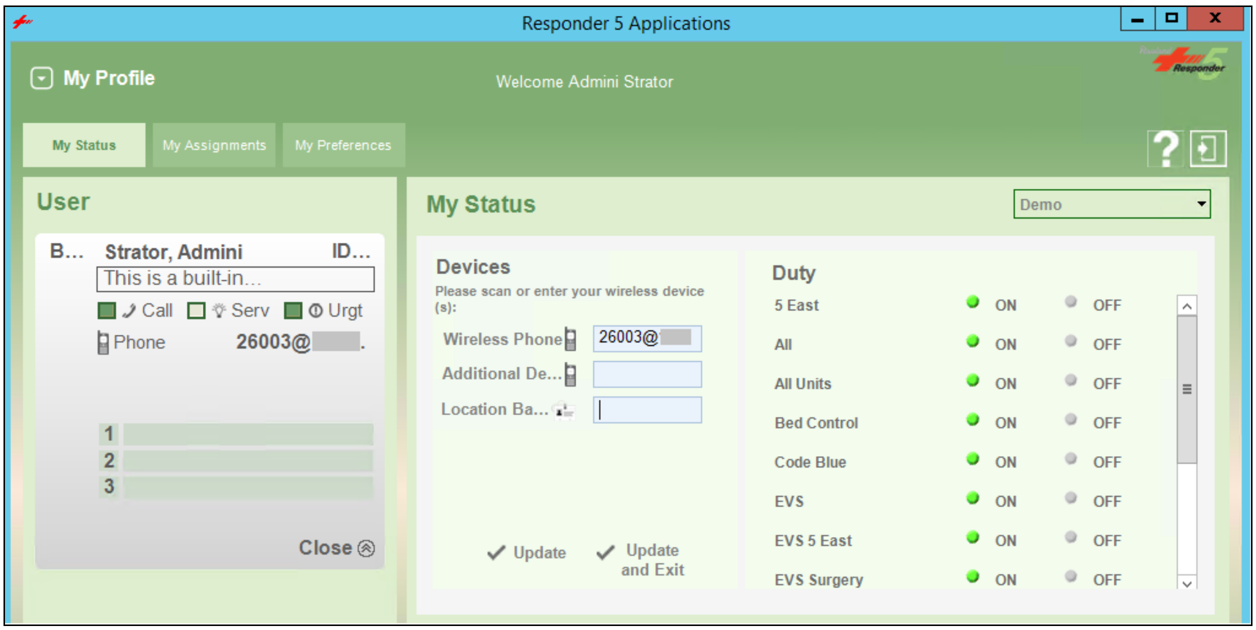


6.1.3. User Login and Device Assignment

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.

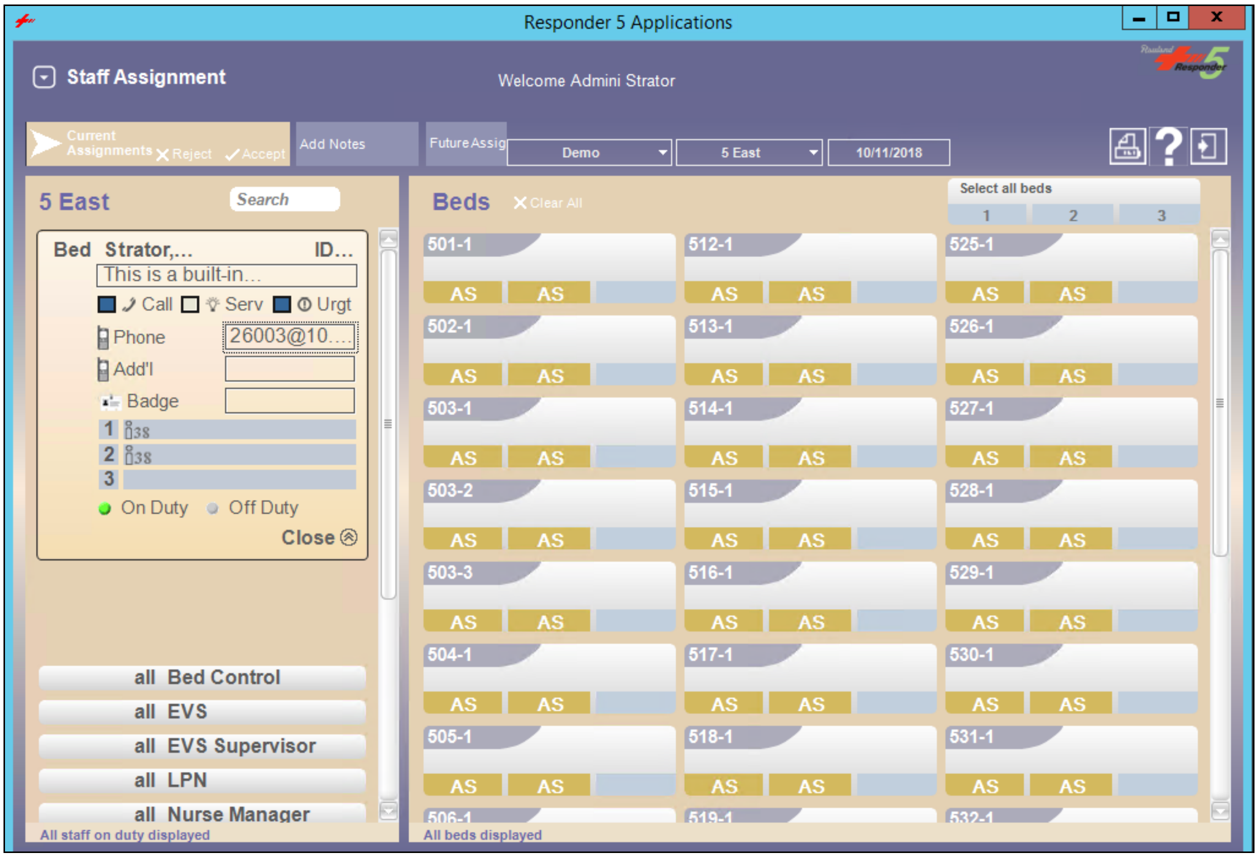
From this screen, a **Wireless Phone** and/or **Pager** number can be entered; duty status updated, and break status entered. The **My Assignments** and **My Preferences** tabs are available for staff to review the patient rooms they are assigned to and modify user preferences. The details of these tasks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

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



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:

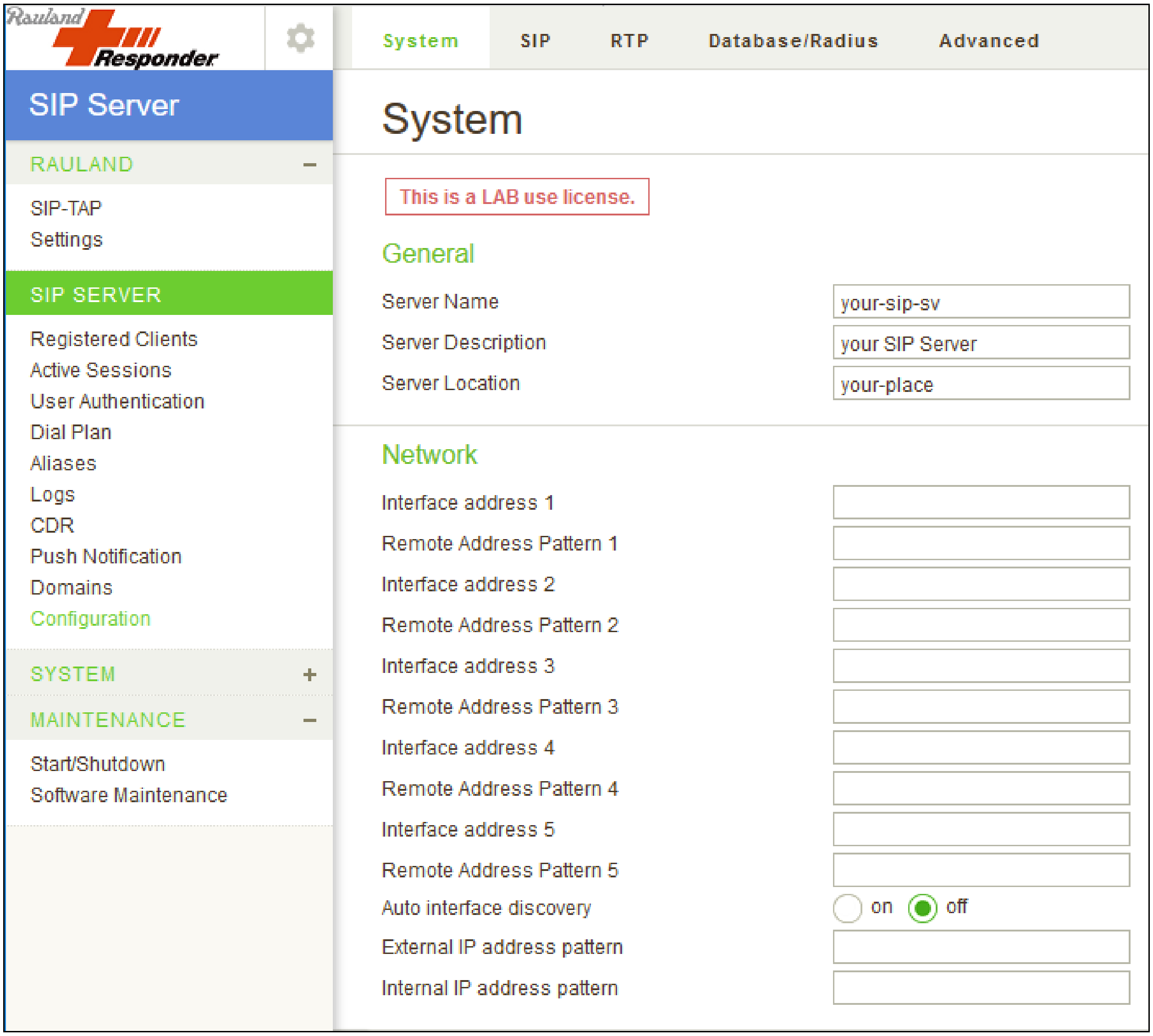
- Login to SIP Server System
- Configure SIP Server System Tab
- Configure SIP Server SIP Tab
- Configure SIP Server RTP Tab
- Configure Dial Plan Routing Rules

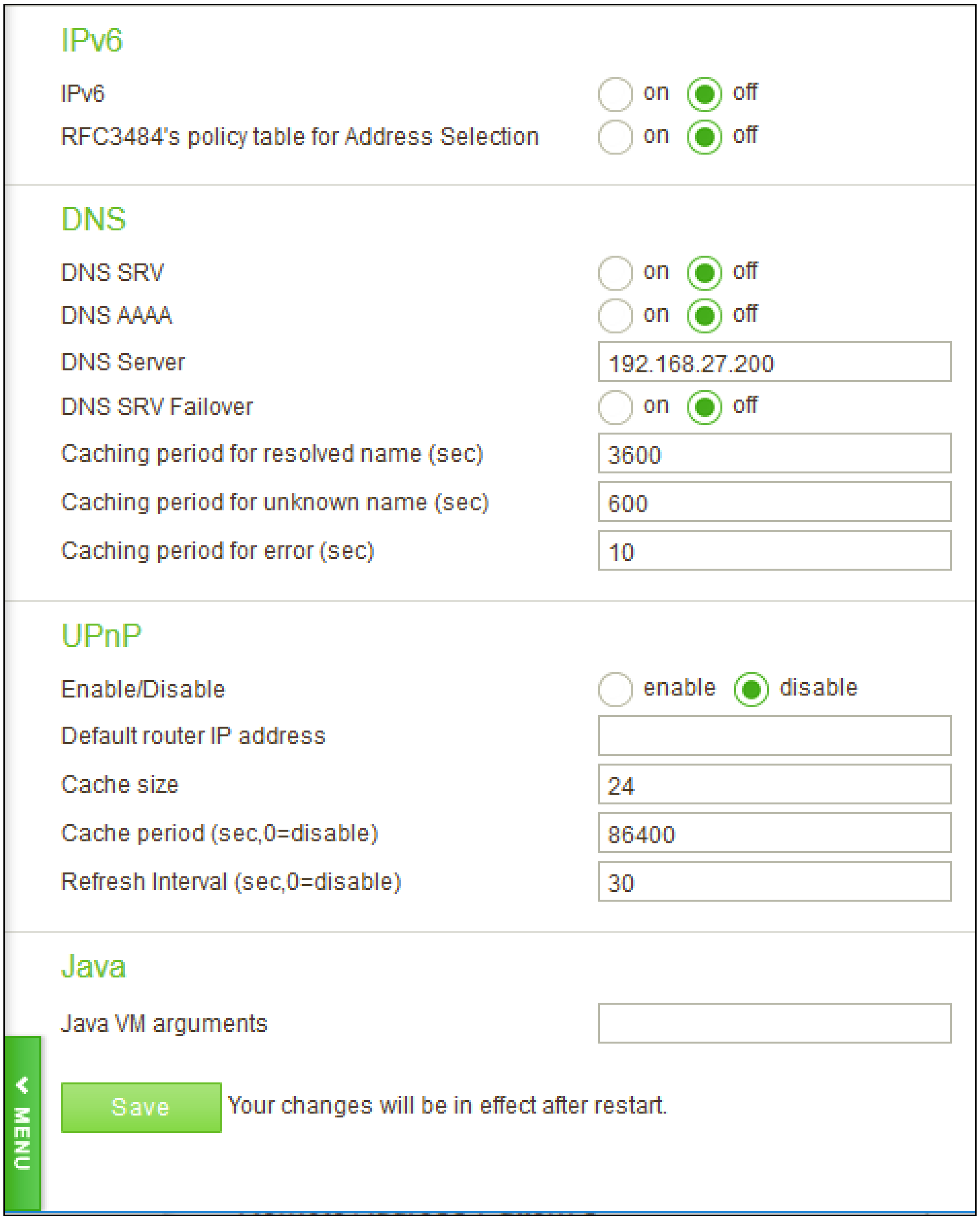
6.2.1. Login to SIP Server System

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.

6.2.2. Configure SIP Server System Tab

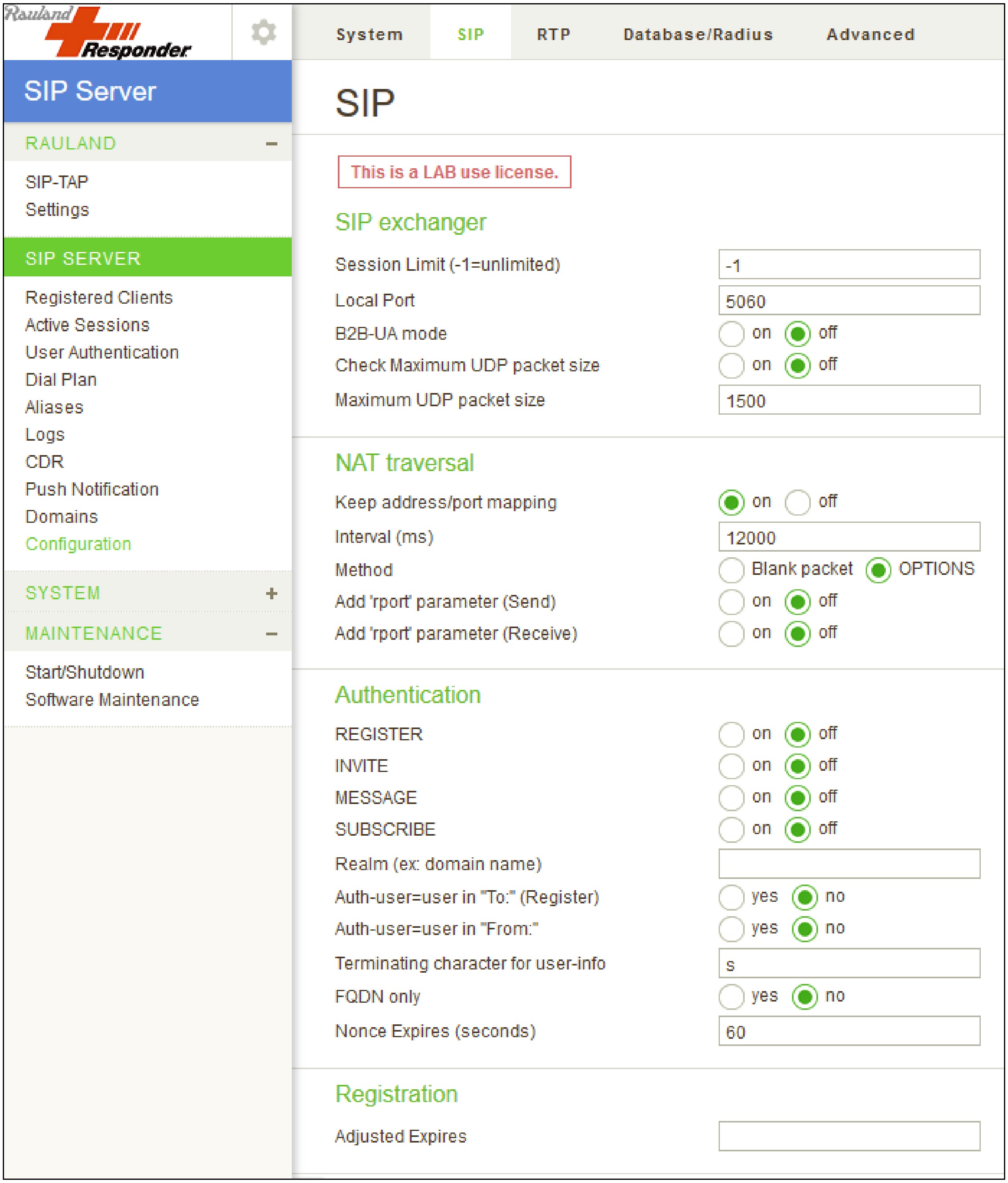
The following **System** properties were pre-configured for the test environment.

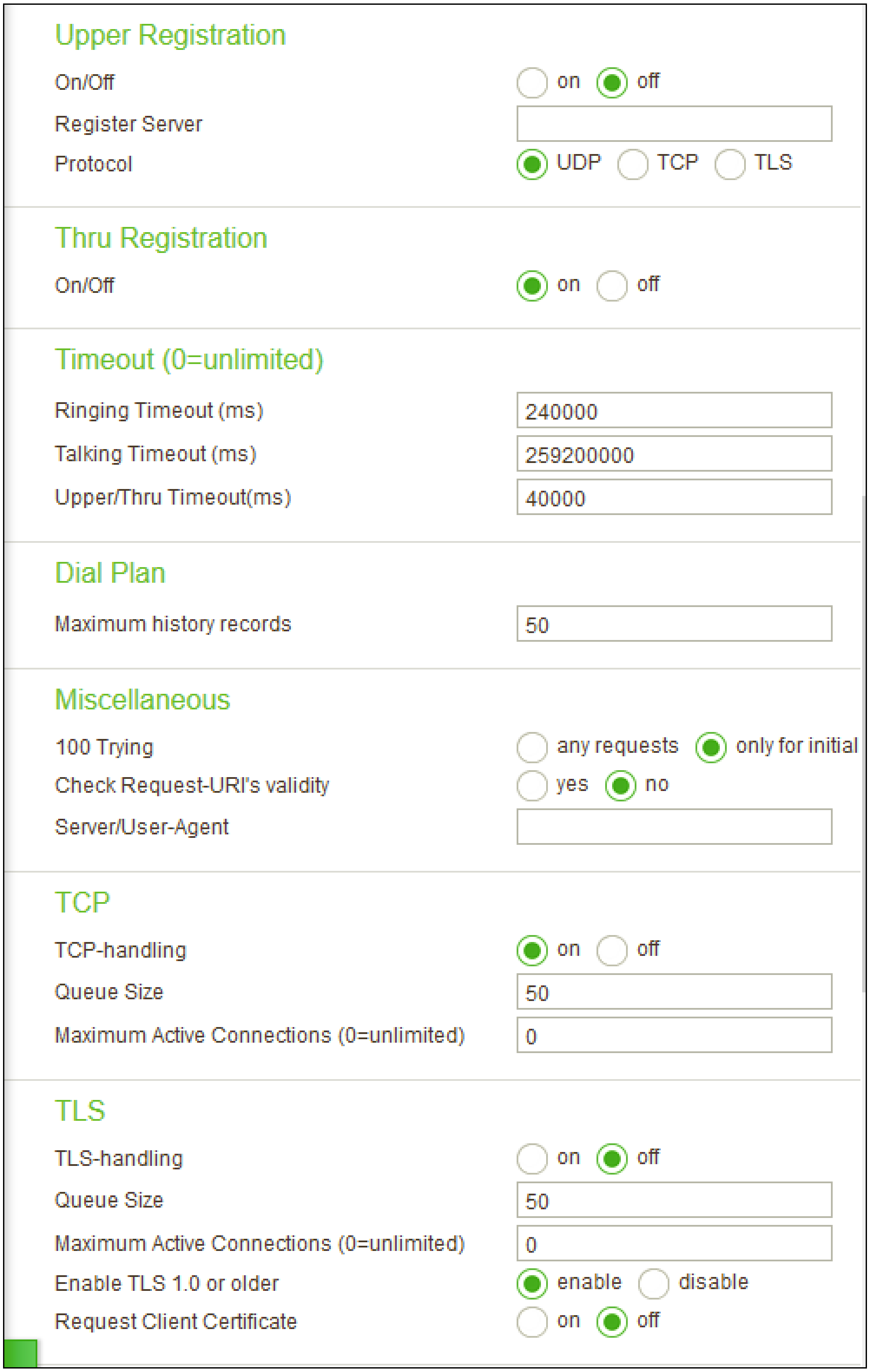



IPv6
IPv6
on off
RFC3484's policy table for Address Selection
on off
DNS
DNS SRV
on off
DNS AAAA
on off
DNS Server
192.168.27.200
DNS SRV Failover
on off
Caching period for resolved name (sec)
3600
Caching period for unknown name (sec)
600
Caching period for error (sec)
10
UPnP
Enable/Disable
enable disable
Default router IP address
Cache size
24
Cache period (sec,0=disable)
86400
Refresh Interval (sec,0=disable)
30
Java
Java VM arguments
MENU
Save
Your changes will be in effect after restart.

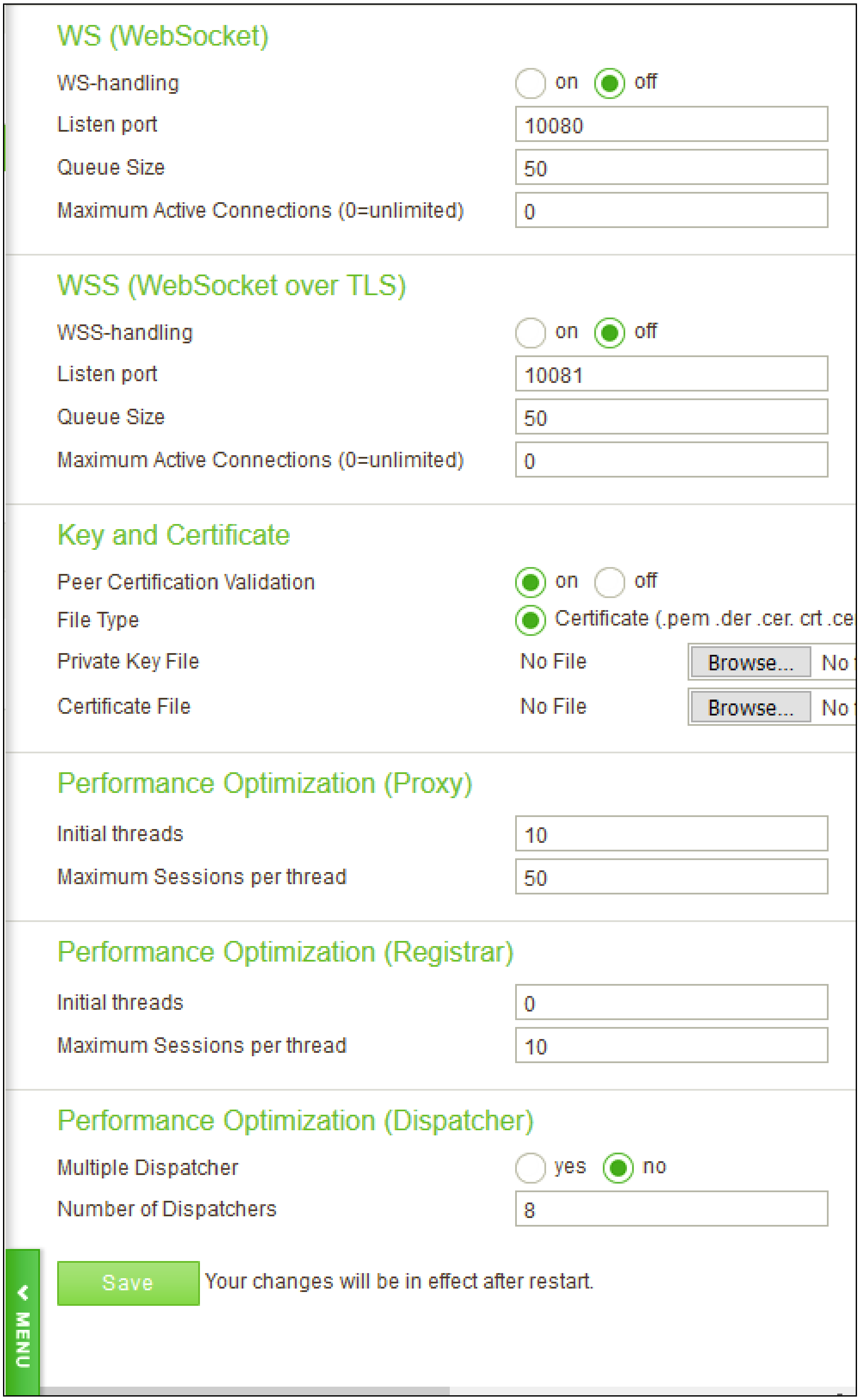
6.2.3. Configure SIP Server SIP Tab

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



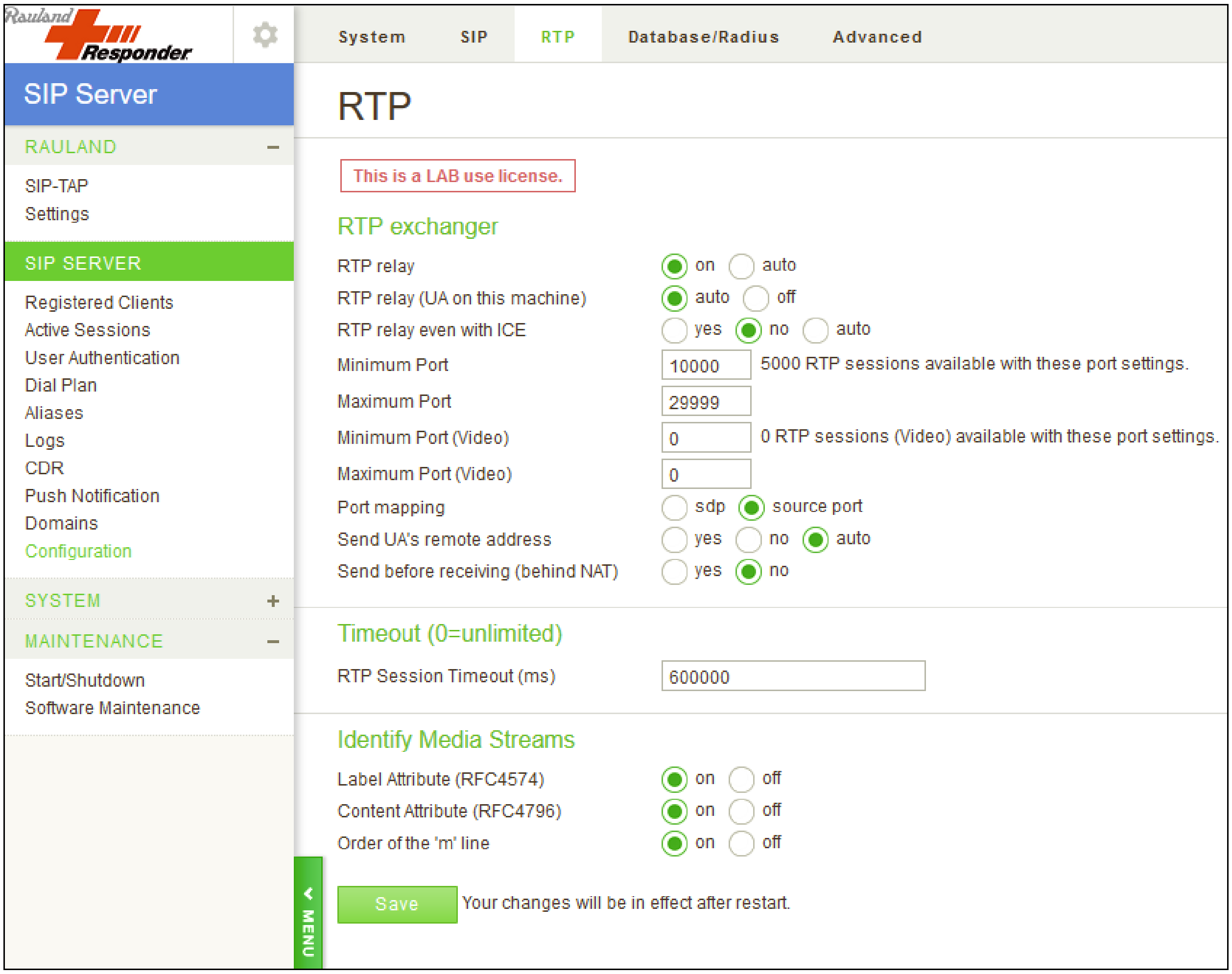


Upper Registration
On/Off
on
off
Register Server
Protocol
UDP
TCP
TLS
Thru Registration
On/Off
on
off
Timeout (0=unlimited)
Ringing Timeout (ms)
240000
Talking Timeout (ms)
259200000
Upper/Thru Timeout(ms)
40000
Dial Plan
Maximum history records
50
Miscellaneous
100 Trying
any requests
only for initial
Check Request-URI's validity
yes
no
Server/User-Agent
TCP
TCP-handling
on
off
Queue Size
50
Maximum Active Connections (0=unlimited)
0
TLS
TLS-handling
on
off
Queue Size
50
Maximum Active Connections (0=unlimited)
0
Enable TLS 1.0 or older
enable
disable
Request Client Certificate
on
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...
Certificate File
No File
Browse...
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
Save
Your changes will be in effect after restart.
MENU

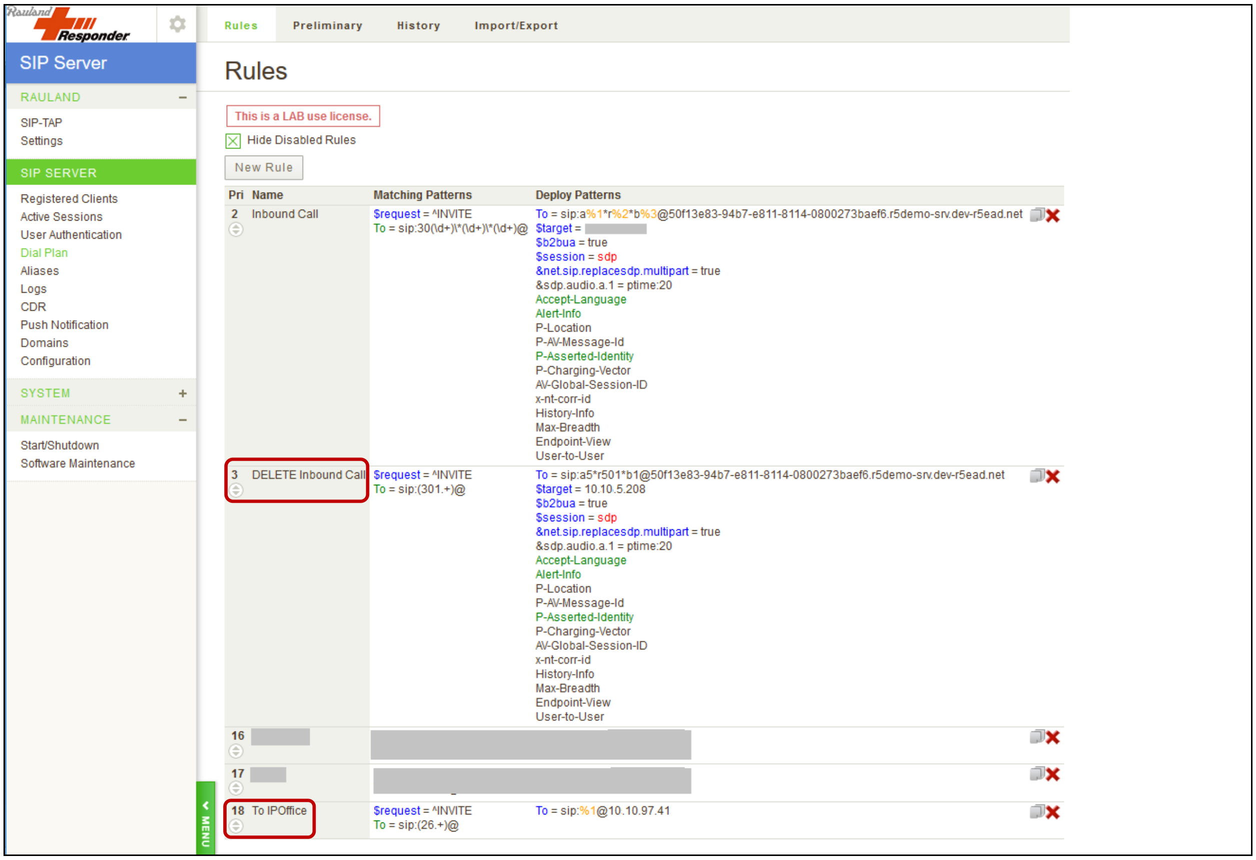
6.2.4. Configure SIP Server RTP Tab

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.



6.2.5. Configure Dial Plan Routing Rules

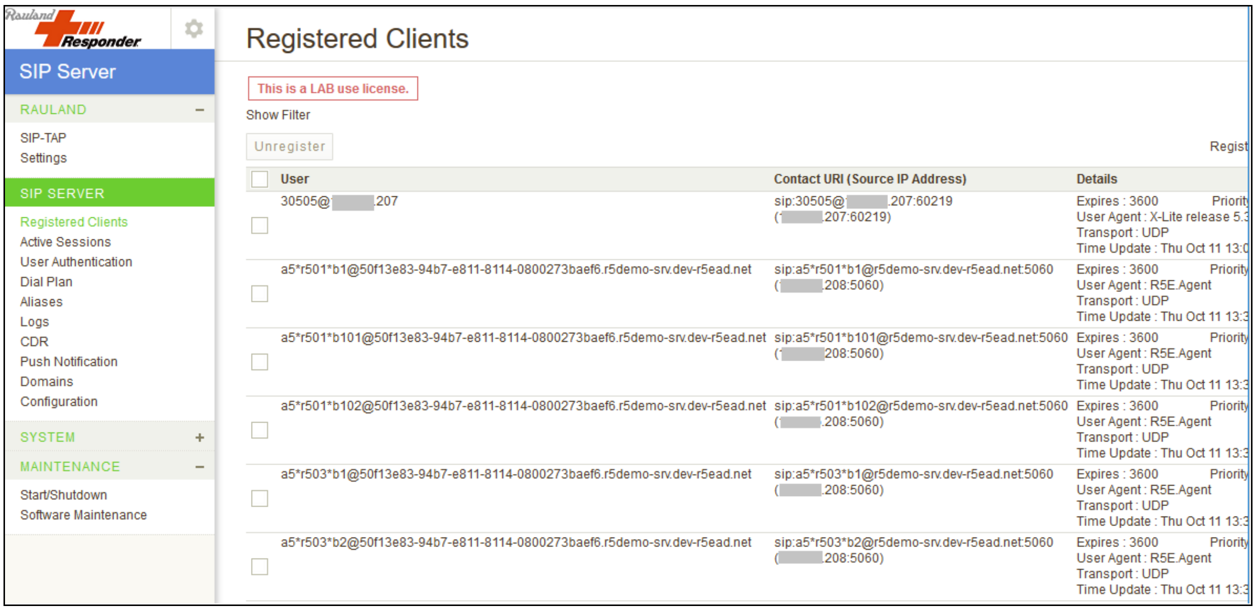
Dial Plan rules that was used is illustrated below. For calls routing from Session Manager, the **DELETE Inbound Call** rule was used. For calls routing to IP Office, the **To IPOffice** rule was used.



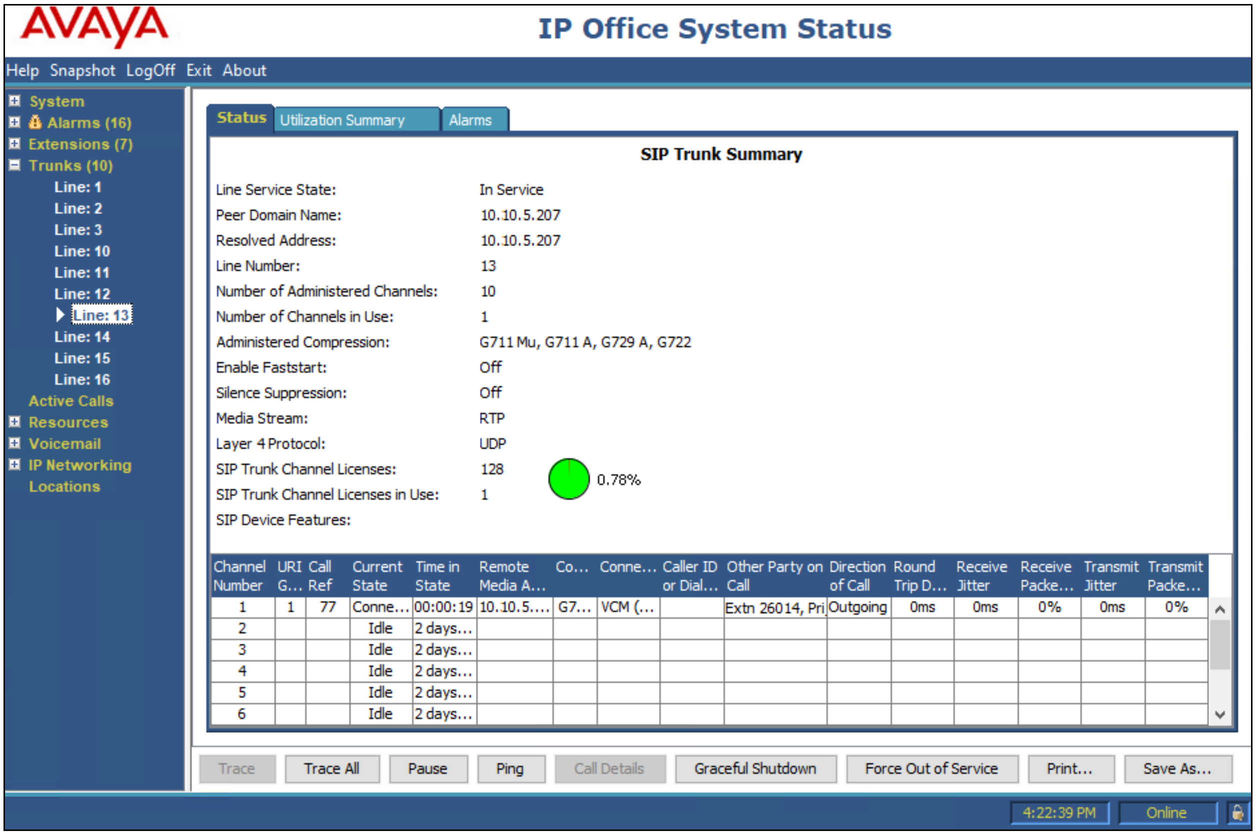
7. Verification Steps

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.



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.



Channel Number	URI G...	Call Ref	Current State	Time in State	Remote Media A...	Co...	Conne...	Caller ID or Dial...	Other Party on Call	Direction of Call	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...											

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/.

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.