Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Rauland Responder Enterprise with Avaya Aura® Session Manager and Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of the Rauland Responder Enterprise solution, Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

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.

©2019 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe a compliance-tested configuration consisting of the Rauland Responder Enterprise (hereafter referred as Responder) solution, Avaya Aura® Session Manager (hereafter referred as Session Manager) and Avaya Aura® Communication Manager (hereafter referred as Communication Manager).

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 to Communication Manager using SIP trunks via the Session Manager. Calls from a patient room can 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 through Session Manager to Communication Manager, 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 Desk phones were used.

©2019 Avaya Inc. All Rights Reserved.

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 Session Manager and Communication Manager.

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

©2019 Avaya Inc. All Rights Reserved.

2.2. Test Results

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

- Responder does not support Initial IP-IP Direct Media when shuffling is turned on. During compliance testing, Initial IP-IP Direct Media was turned off. Refer to **Section 5.1.3** for further details.
- 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/

©2019 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya Aura® Media Server
- Avaya G450 Media Gateway
- Various H.323 and SIP endpoints
- Responder SIP Server
- Responder Application Server
- Responder Communication Endpoints

Calls routed to and from the Communication Manager used SIP trunks between the Responder SIP server and Session Manager, and in turn SIP trunks between Session Manager and Communication Manager.

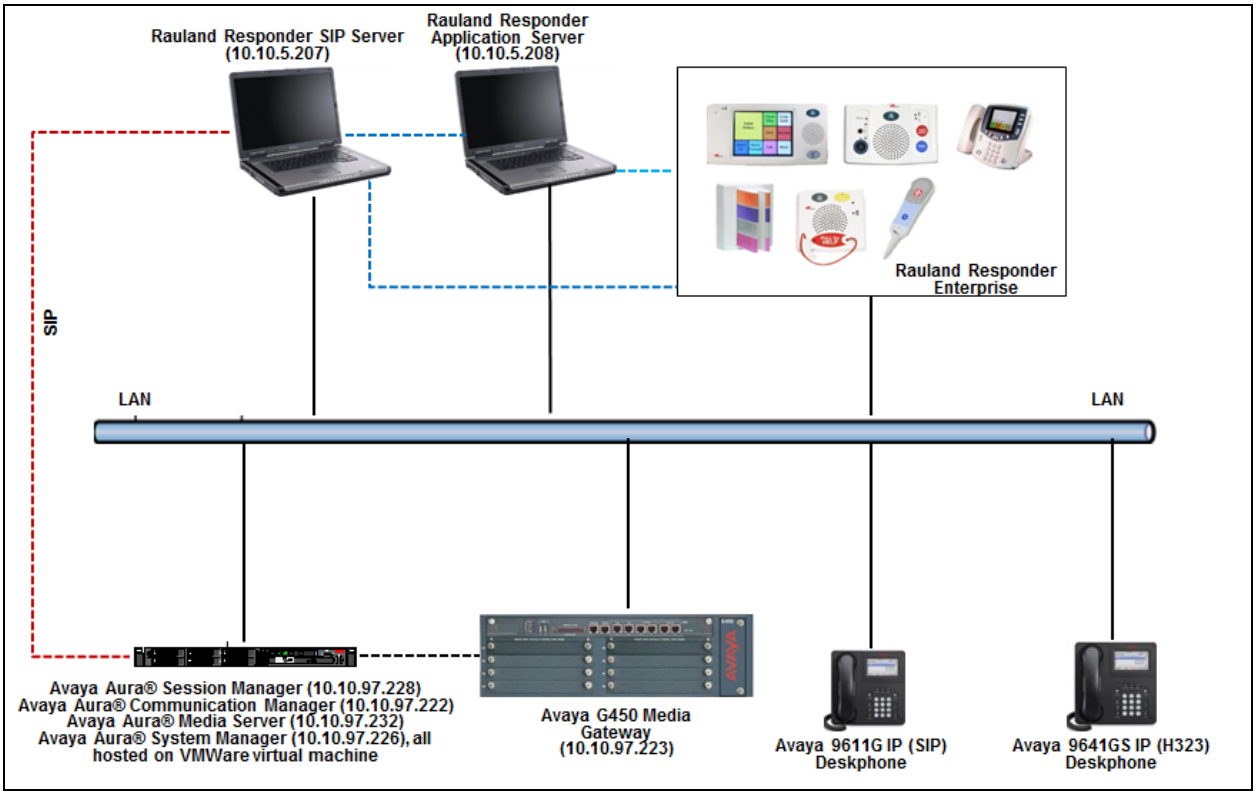


Figure 1 – Rauland Responder Enterprise Compliance Test Configuration

©2019 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtual server	8.0.0.0.822
Avaya Aura® Media Server running on virtual server	8.0.0.117
Avaya G450 Media Gateway	40.10.0/1
Avaya Aura® System Manager running on virtual server	8.0.0.0.931077
Avaya Aura® Session Manager running on virtual server	8.0.0.0.800035
Avaya IP Deskphones - 9641GS (H.323) - 9611G (SIP)	 6.6604 7.1.3.0.8
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

©2019 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on the Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of the Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

5.1. Configure Communication Manager Details

Calls were routed to Responder endpoints using a 5-digit 30xxx pattern. All calls routed via a SIP trunk between Communication Manager and Session Manager using TLS transport. Existing SIP Trunks were in place in the environment. The steps below outline modifications made to accommodate the Responder solution. Therefore, some details required for SIP trunks may be omitted.

It is implied a working system is already in place. The configuration operations described in this section can be summarized as follows: (Note: During Compliance Testing all inputs not highlighted in Bold were left as Default)

- Verify License
- Administer SIP trunk group
- Administer SIP signaling group
- Administer SIP trunk group members
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer dial plan
- Administer uniform dial plan
- Administer AAR analysis

©2019 Avaya Inc. All Rights Reserved.

5.1.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

If additional license is required, contact an authorized Avaya Sales or Reseller representative.

```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 10
           Maximum Concurrently Registered IP Stations: 18000 5
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 41000 0
                   Maximum Video Capable IP Softphones: 18000 1
                       Maximum Administered SIP Trunks: 30000 34
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 688   0
```

5.1.2. Administer SIP Trunk Group

Use the "add trunk-group n" command, where "n" is an available trunk group number, in this case "1". Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Type:** "sip".
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** "tie".

```
add trunk-group 1                                           Page   1 of  22
                                TRUNK GROUP

Group Number: 1                     Group Type: sip           CDR Reports: y
  Group Name: Trunk to SM on VM           COR: 1        TN: 1        TAC: #001
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                          Member Assignment Method: auto
                                                   Signaling Group: 1
                                                 Number of Members: 24
```


©2019 Avaya Inc. All Rights Reserved.

Navigate to **Page 3** and enter "private" for **Numbering Format**.

```
add trunk-group 1                                          Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                       Maintenance Tests? y



                     Numbering Format: private
                                             UUI Treatment: shared
                                           Maximum Size of UUI Contents: 128
                                              Replace Restricted Numbers? n
                                             Replace Unavailable Numbers? n

                                               Hold/Unhold Notifications? y
                                  Modify Tandem Calling Number: no
```


©2019 Avaya Inc. All Rights Reserved.

5.1.3. Administer SIP Signaling Group

Use the "add signaling-group n" command, where "n" is an available signaling group number, in this case "1". Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Type:** "sip".
- **Transport Method:** "tls".
- **Near-end Node Name:** An existing C-LAN node name or "procr".
- **Far-end Node Name:** The existing node name for Session Manager.
- **Near-end Listen Port:** An available port for integration with Session Manager.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** An existing network region to use with Session Manager.
- **Far-end Domain:** The applicable domain name for the network.
- **Direct IP-IP Audio Connections:** "y".
- **Initial IP-IP Direct Media?:** "n", as mentioned in **Section 2.2**.

```
display signaling-group 1                                        Page   1 of   2
                              SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                    Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                  Far-end Node Name: SM-VM
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: bvwdev.com
                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? y
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```


©2019 Avaya Inc. All Rights Reserved.

5.1.4. Administer SIP Trunk Group Members

Use the "change trunk-group n" command, where "n" is the trunk group number from **Section 5.1.2**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Signaling Group:** The signaling group number from **Section 5.1.3**.
- **Number of Members:** The desired number of members, in this case "24".

```
  change trunk-group 1                                          Page   1 of  22
                                  TRUNK GROUP

  Group Number: 1                    Group Type: sip           CDR Reports: y
    Group Name: Trunk to SM on VM           COR: 1        TN: 1        TAC: #001
     Direction: two-way        Outgoing Display? y
   Dial Access? n                                    Night Service:
  Queue Length: 0
  Service Type: tie                   Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 1
                                                   Number of Members: 24
```

5.1.5. Administer IP Network Region

Use the "change ip-network-region n" command, where "n" is the existing far-end network region number used by the SIP signaling group from **Section 5.1.3**.

For **Authoritative Domain**, enter the applicable domain for the network. Enter a descriptive **Name**. Enter "yes" for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with Responder.

```
change ip-network-region 1                                      Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: bvwdev.com
    Name: Region1               Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
```


©2019 Avaya Inc. All Rights Reserved.

Navigate to **Page 4**, and specify this codec set to be used for calls with network regions used by Avaya endpoints and by the trunk to the PSTN. In the compliance testing, network region "1" was used by the Avaya endpoints and by the trunk to the PSTN.

```
change ip-network-region 1                                      Page   4 of  20

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    1                                                               all
 2
```

5.1.6. Administer IP Codec Set

Use the "change ip-codec-set n" command, where "n" is the codec set number from **Section 5.1.5**. Update the audio codec types in the **Audio Codec** fields as necessary. As per the observation noted in **Section 2.2** only configure G.711MU. The codec shown below was used in the compliance testing.

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

                           IP CODEC SET
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
```


©2019 Avaya Inc. All Rights Reserved.

5.1.7. Administer Route Pattern

Use the "change route-pattern n" command, where "n" is an existing route pattern number to be used to reach Responder, in this case "1". Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.1.2**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1      Pattern Name: To SM on VM
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No. Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                                 Dgts                                   Intw
 1: 1    0                        0                                      n   user
 2:                                                                      n   user
 3:                                                                      n   user
 4:                                                                      n   user
 5:                                                                      n   user
 6:                                                                      n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
 1: y y y y y n  n            rest                                lev0-pvt  none
```

5.1.8. Administer Private Numbering

Use the "change private-numbering 0" command, to define the calling party number to send to Responder. Add an entry for the trunk group defined in **Section 5.1.2**. In the example shown below, all calls originating from a 5-digit extension beginning with 56 and routed to trunk group 1 will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 5  56             1                           5     Total Administered: 4
                                                      Maximum Entries: 540
```


©2019 Avaya Inc. All Rights Reserved.

5.1.9. Administer Dial Plan

This section provides a sample dial plan used for routing calls with dialed digits 30xxx to Responder. Use the "change dialplan analysis 0" command, and add an entry to specify the use of digits pattern 30, as shown below

```
display dialplan analysis                                        Page   1 of  12
                            DIAL PLAN ANALYSIS TABLE
                                  Location: all            Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1           4   ext
   30          5   udp
```

5.1.10. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 30xxx to Responder. Note that other routing methods may be used. Use the "change uniform-dialplan 0" command and add an entry to specify the use of AAR for routing of digits 30xxx, as shown below.

```
change uniform-dialplan 0                                        Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                    Insert              Node
  Pattern       Len Del       Digits     Net Conv Num
 30              5   0                   aar  n
```

5.1.11. Administer AAR Analysis

Use the "change aar analysis 0" command and add an entry to specify how to route calls to 30xxx. In the example shown below, calls with digits 30xxx will be routed as an AAR call using route pattern "1" from **Section 5.1.7**.

```
change aar analysis 0                                            Page   1 of   2
                            AAR DIGIT ANALYSIS TABLE
                                  Location: all            Percent Full: 2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
         30                   5    5     1        aar          n
```


©2019 Avaya Inc. All Rights Reserved.

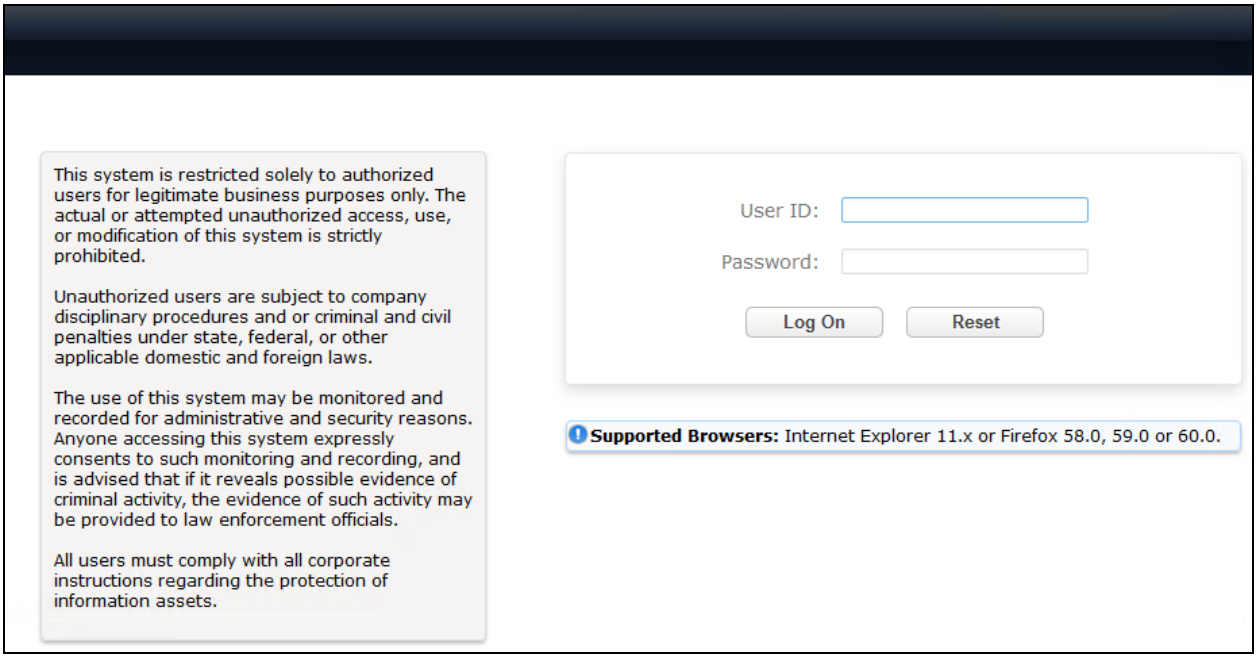
6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer Domain
- Administer locations
- Administer Adaptation
- Administer SIP entities
- Administer routing policies
- Administer dial patterns

6.1. Launch System Manager

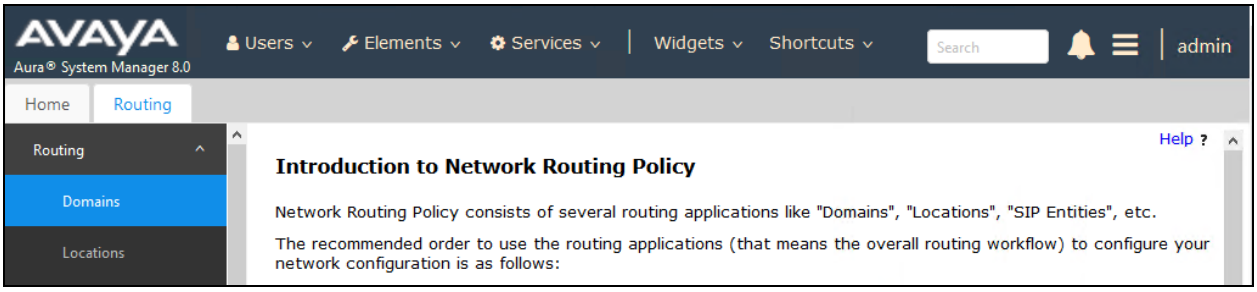
Access the System Manager web interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of System Manager. Log in using the appropriate credentials.



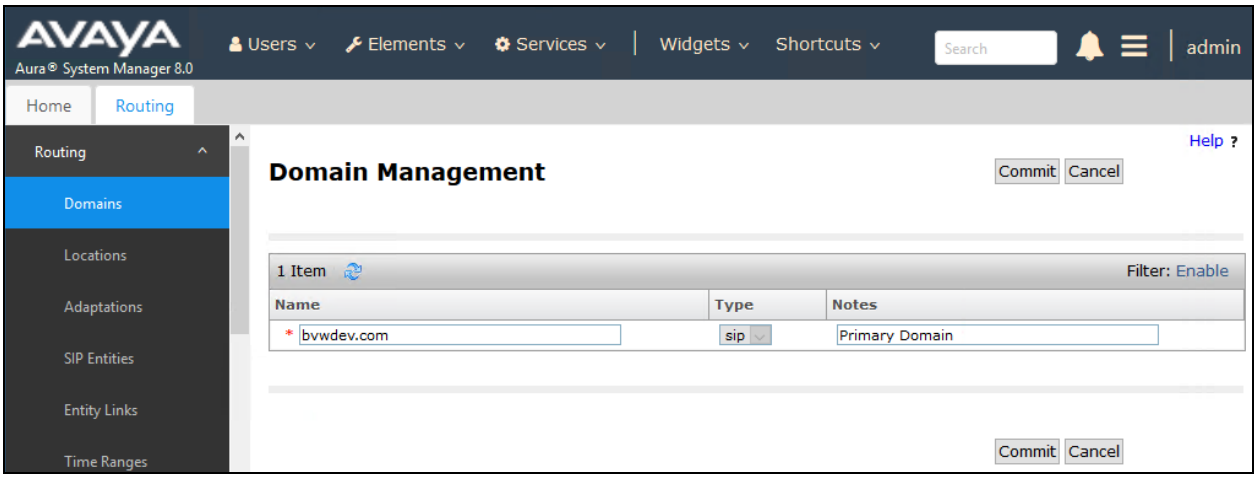
©2019 Avaya Inc. All Rights Reserved.

6.2. Administer Domain

In the subsequent screen (not shown), select **Elements → Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Domains** from the left pane, and click **New** in the subsequent screen (not shown) to add a new domain



The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select "sip" from the **Type** drop down menu and provide any optional **Notes**.



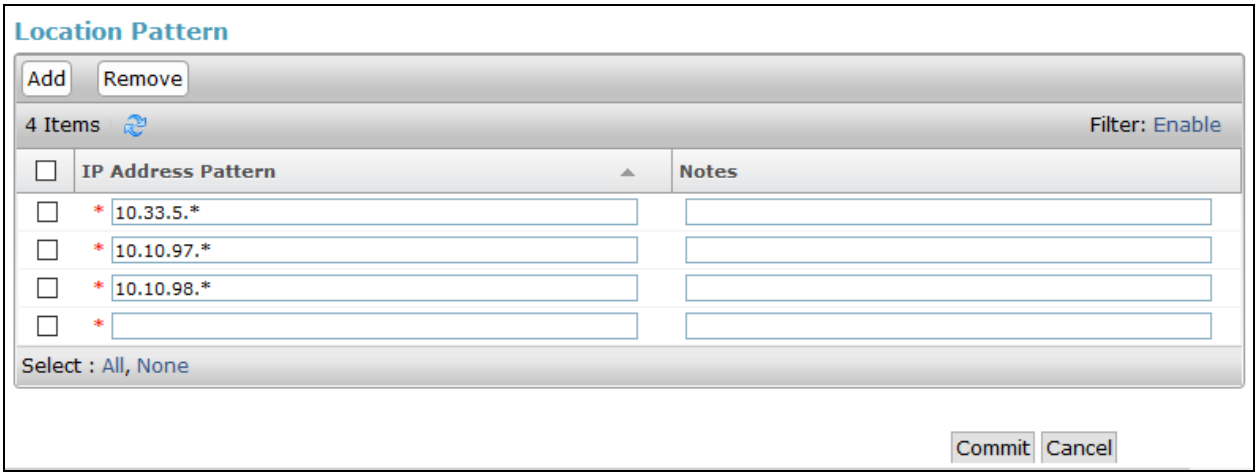
©2019 Avaya Inc. All Rights Reserved.

6.3. Administer Locations

Select **Locations** from the left pane and click **New** in the subsequent screen (not shown) to add a new location for Responder.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.

Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of all devices involved in the compliance testing in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.



©2019 Avaya Inc. All Rights Reserved.

6.4. Administer Adaptation

During compliance test, to make the call from and to Communication Manager via Session Manager, Adaptation to translate IP address into domain name is used for Responder SIP entity. Below are the steps that were used during compliance testing to create the needed Adaptation. Select **Adaptations** on the left panel menu and then click on the **New** button in the main window (not shown).

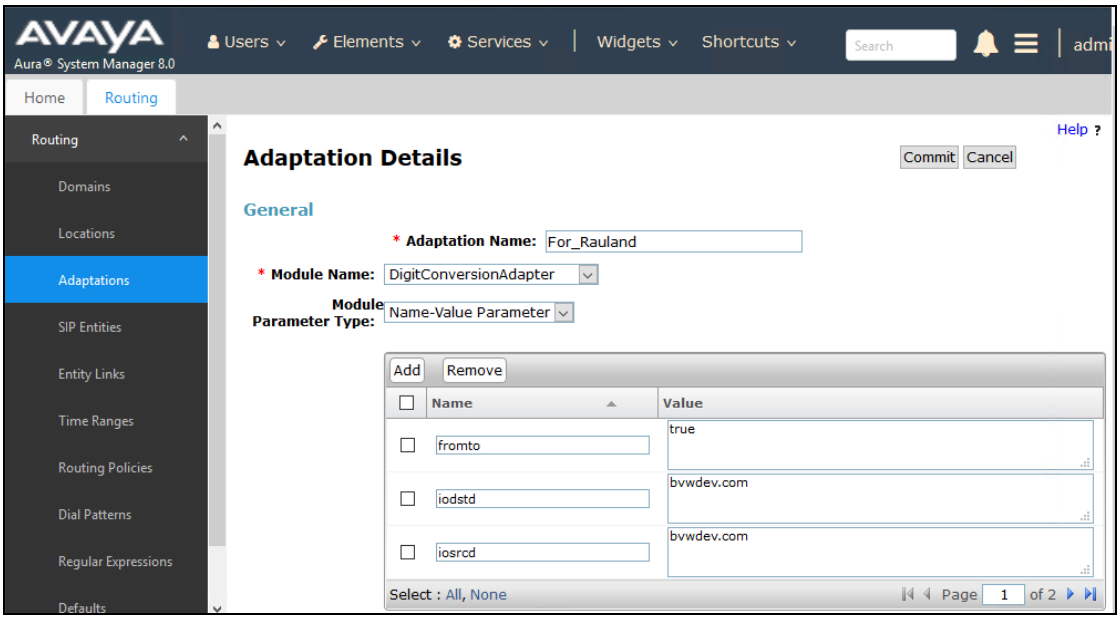
Enter the following for the Responder Adaptation.

- **Adaptation Name** An informative name (e.g., **change IP to Domain Responder**).
- **Module Name** Select **DigitConversionAdapter**.
- **Module Parameter Type** Select **Name-Value Parameter**.

Click **Add** to add a new row for the following values as shown below table:

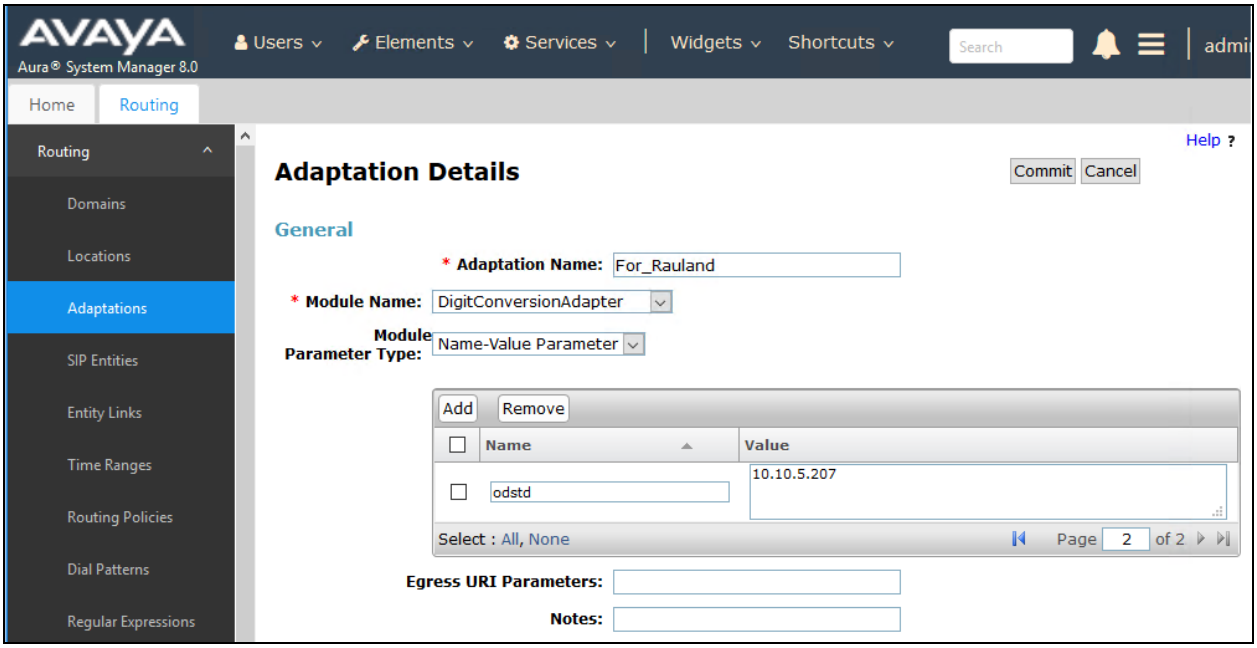
Name	Value
fromto	true
iodstd	Enter the domain name of system, ex: **bvwdev.com**
iosrcd	Enter the domain name of system, ex: **bvwdev.com**
odstd	Enter IP address of Responder SIP Server, ex: **10.10.5.207**

Once the correct information is entered click the **Commit** button. Below is the screenshot showing the Adaptation created for Responder.



©2019 Avaya Inc. All Rights Reserved.

The screenshot showing the continuation of the Adaptation values configured for Responder:



©2019 Avaya Inc. All Rights Reserved.

6.5. Administer SIP Entities

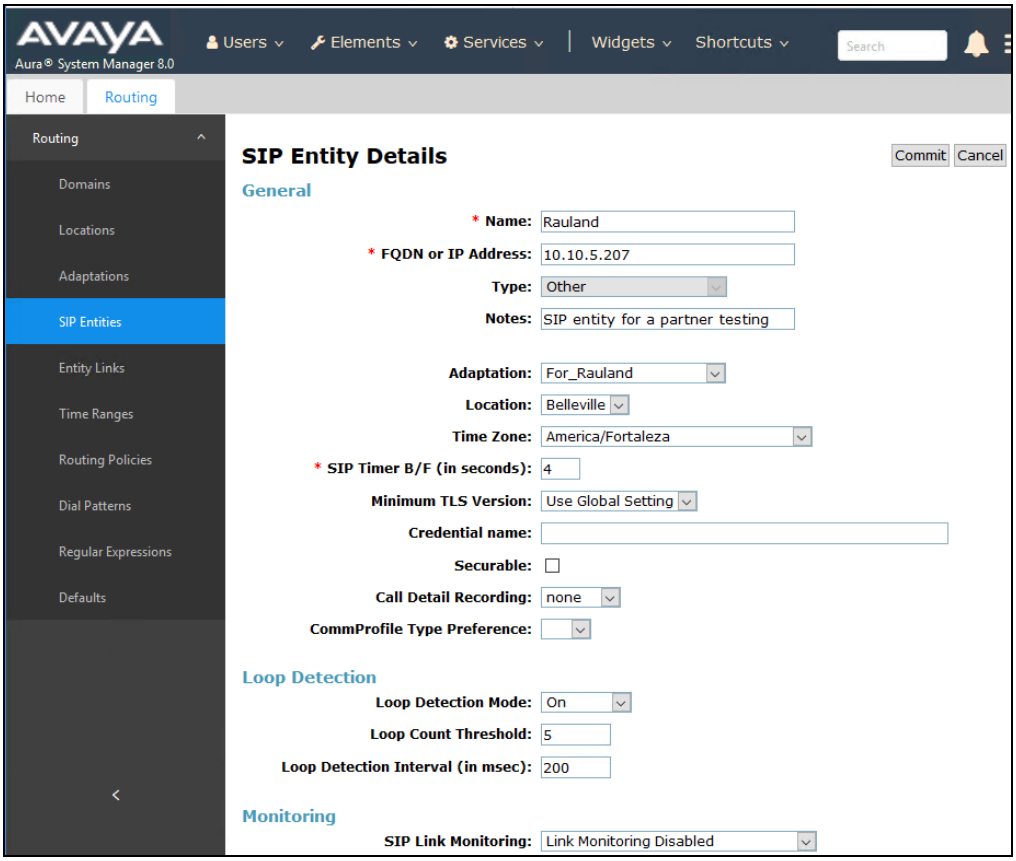
Add two new SIP entities, one for Responder and one for the new SIP trunks with Communication Manager.

6.5.1. SIP Entity for Responder Enterprise

Select **SIP Entities** from the left pane and click **New** in the subsequent screen (not shown) to add a new SIP entity for Responder.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of Responder SIP Server.
- **Type:** "Other"
- **Notes:** Any desired notes.
- **Adaptation:** Select the adaptation configured in **Section 6.4**
- **Location:** Select the Responder location name from **Section 6.3**.
- **Time Zone:** Select the applicable time zone.
- **SIP Link Monitoring:** Select "Link Monitoring Disabled".

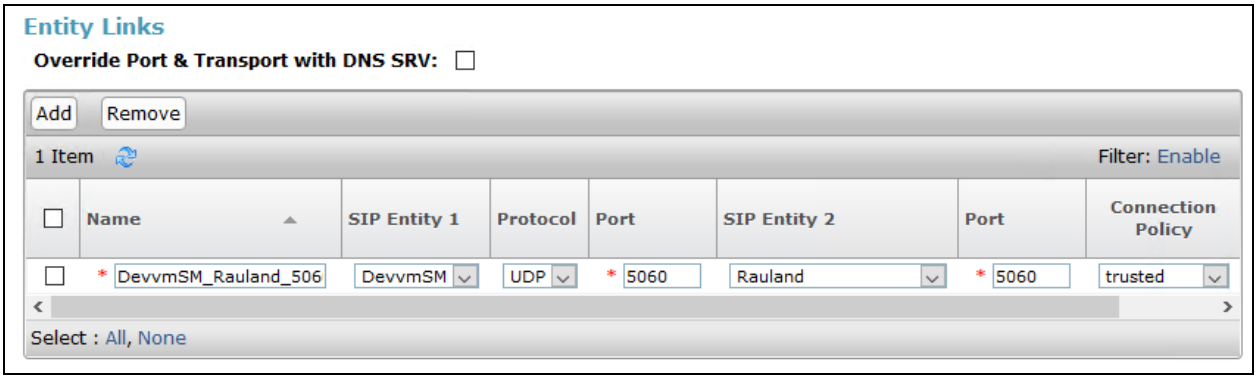


©2019 Avaya Inc. All Rights Reserved.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case "DevvmSM".
- **Protocol:** "UDP".
- **Port:** "5060".
- **SIP Entity 2:** The Responder entity name from this section.
- **Port:** "5060".
- **Connection Policy:** "trusted".

Note that only UDP protocol was tested.



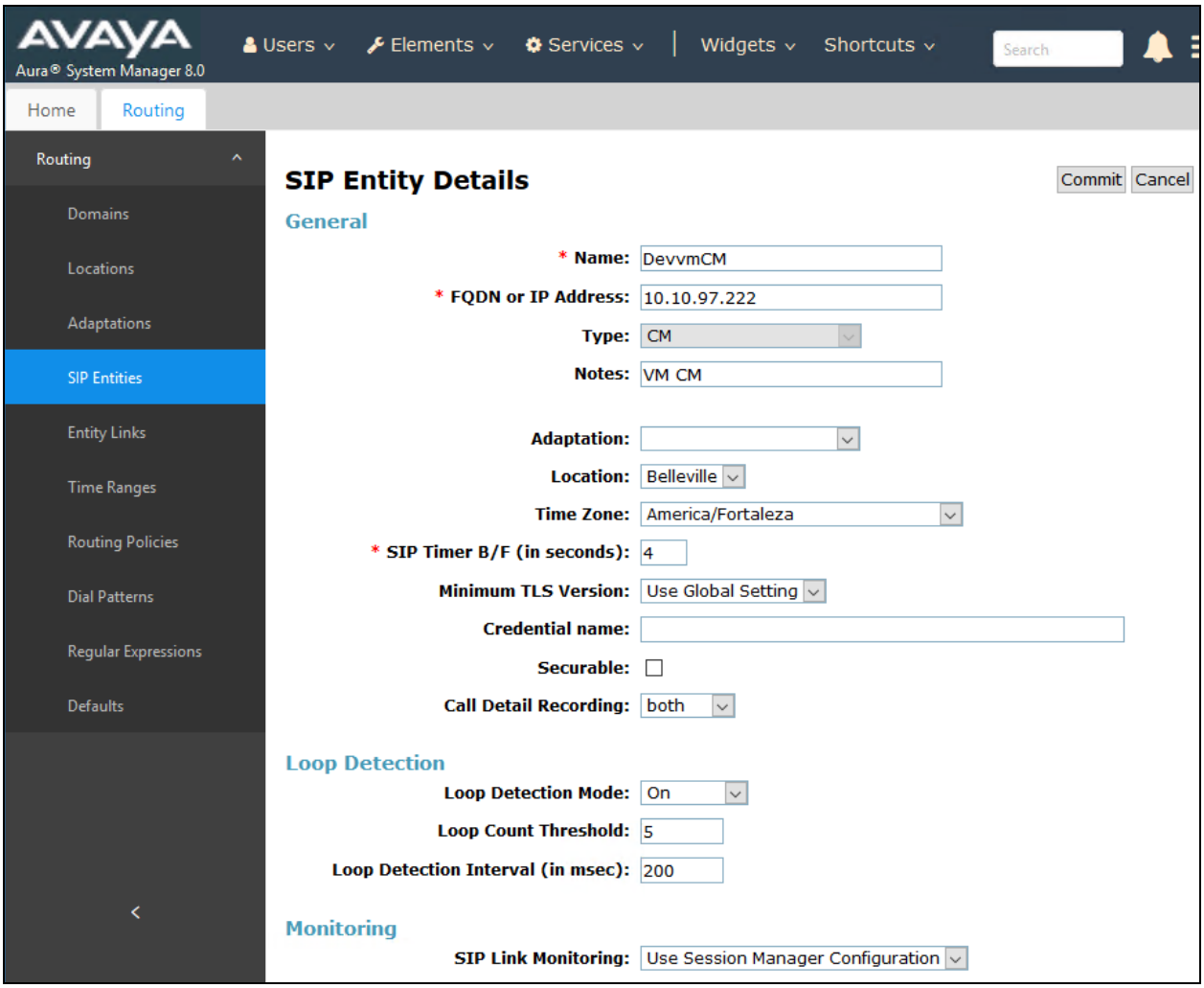
©2019 Avaya Inc. All Rights Reserved.

6.5.2. SIP Entity for Communication Manager

Select **SIP Entities** from the left pane and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager. Note that this SIP entity is used for integration with Responder.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

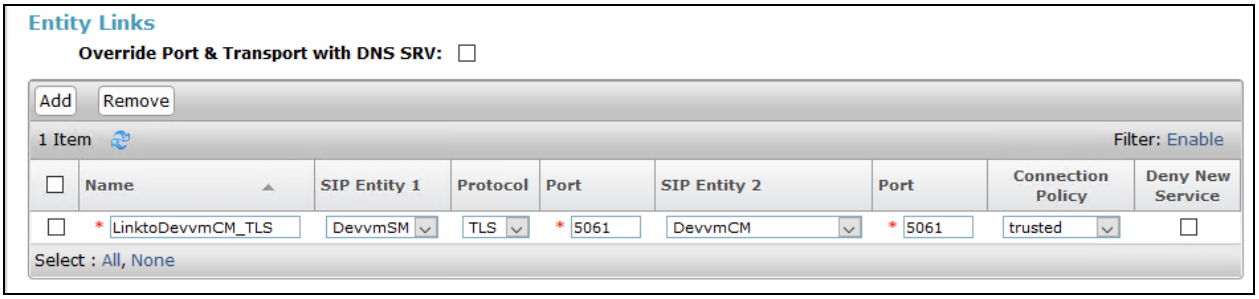
- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of an existing CLAN or the processor interface.
- **Type:** "CM"
- **Notes:** Any desired notes.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.



©2019 Avaya Inc. All Rights Reserved.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case "DevvmSM".
- **Protocol:** The signaling group transport (TLS) method from **Section 5.1.3**.
- **Port:** The signaling group listen port (5061) number from **Section 5.1.3**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group listen port (5061) number from **Section 5.1.3**.
- **Connection Policy:** "trusted"



©2019 Avaya Inc. All Rights Reserved.

6.6. Administer Routing Policies

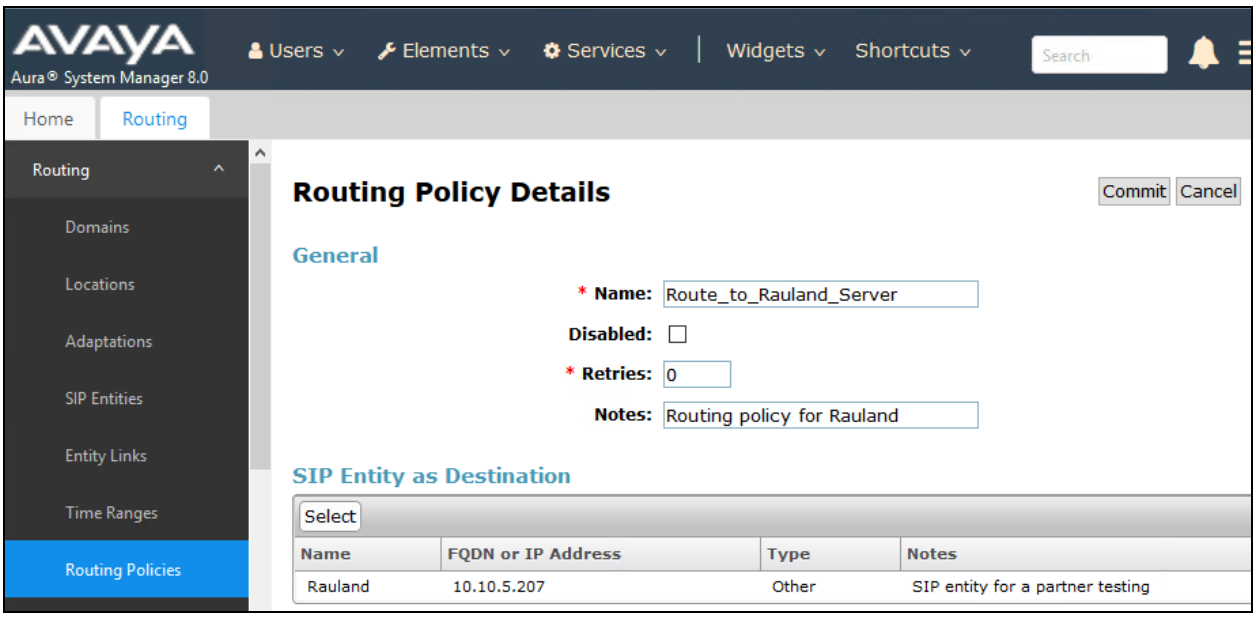
Add two new routing policies, one for Responder and one for the new SIP trunks with Communication Manager.

6.6.1. Routing Policy for Responder Enterprise

Select **Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for Responder.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Responder entity name from **Section 6.5.1**. The screen below shows the result of the selection.



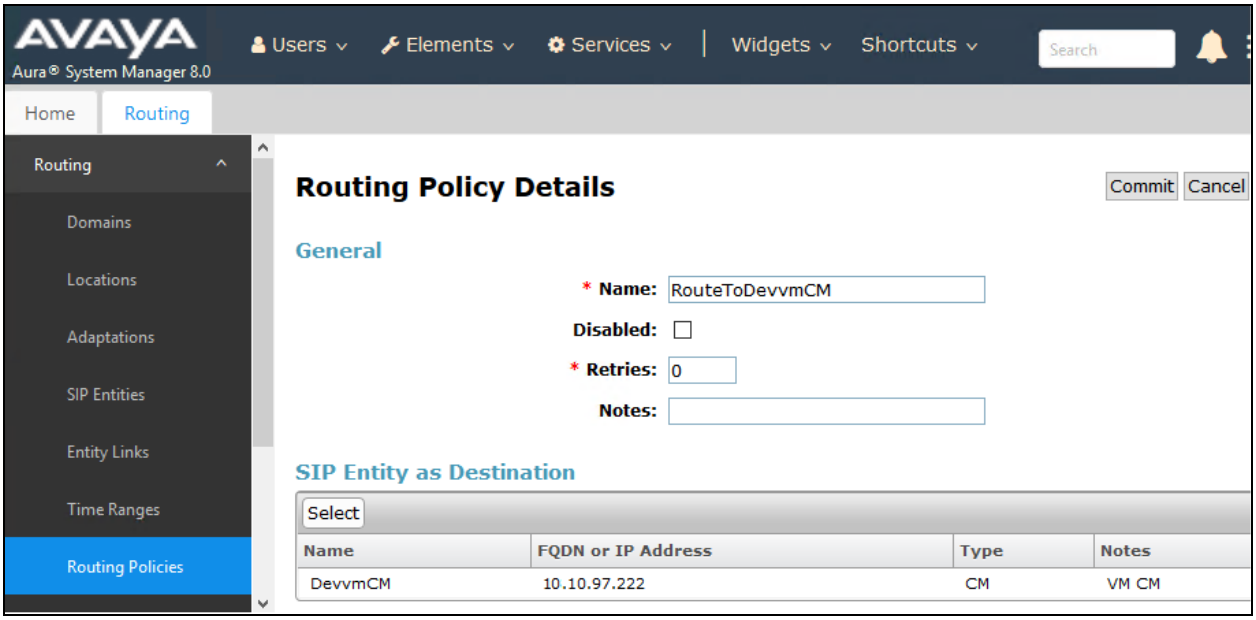
©2019 Avaya Inc. All Rights Reserved.

6.6.2. Routing Policy for Communication Manager

Select **Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.5.2**. The screen below shows the result of the selection.



©2019 Avaya Inc. All Rights Reserved.

6.7. Administer Dial Patterns

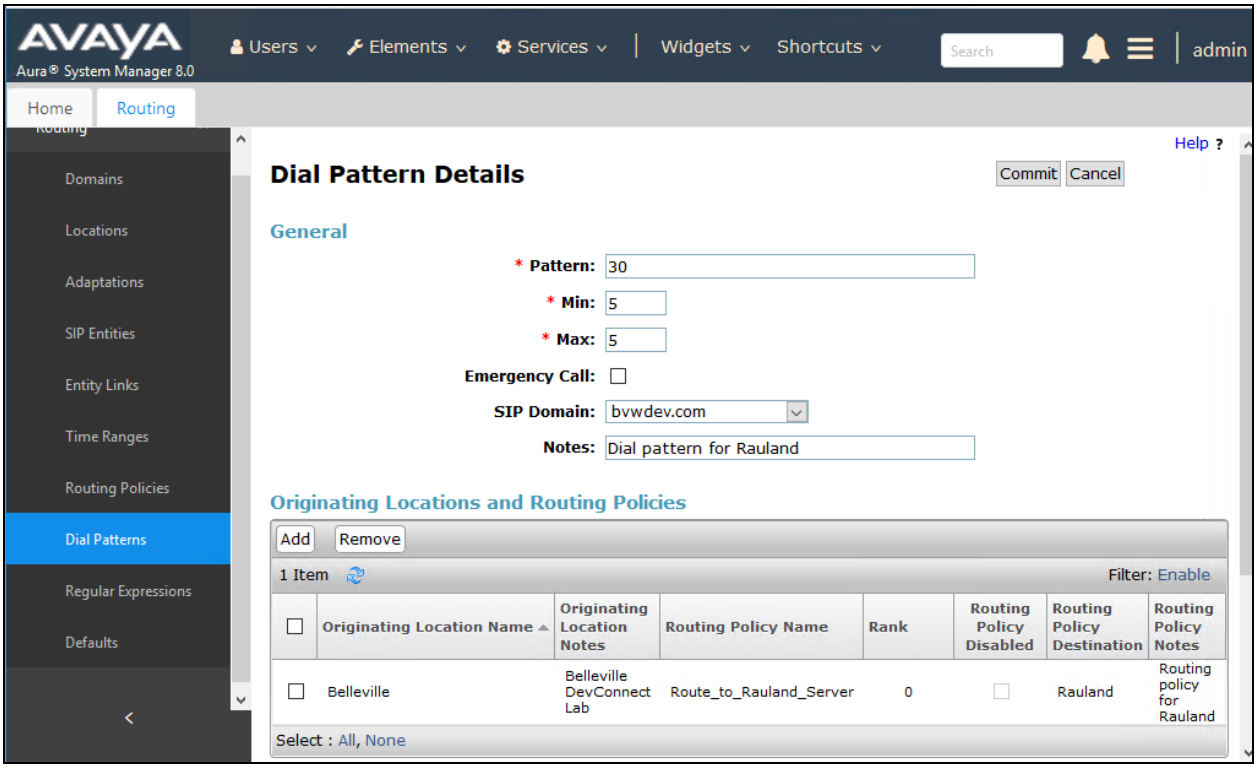
Add a new dial pattern for Responder and Communication Manager.

6.7.1. Dial Pattern for Responder Enterprise

Select **Dial Patterns** from the left pane and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Responder. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case "30".
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 5.1.3**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Responder. In the compliance testing, the entry allowed for call originations from all Communication Manager endpoints in locations "Belleville". The Responder routing policy from **Section 6.6.1** was selected as shown below.



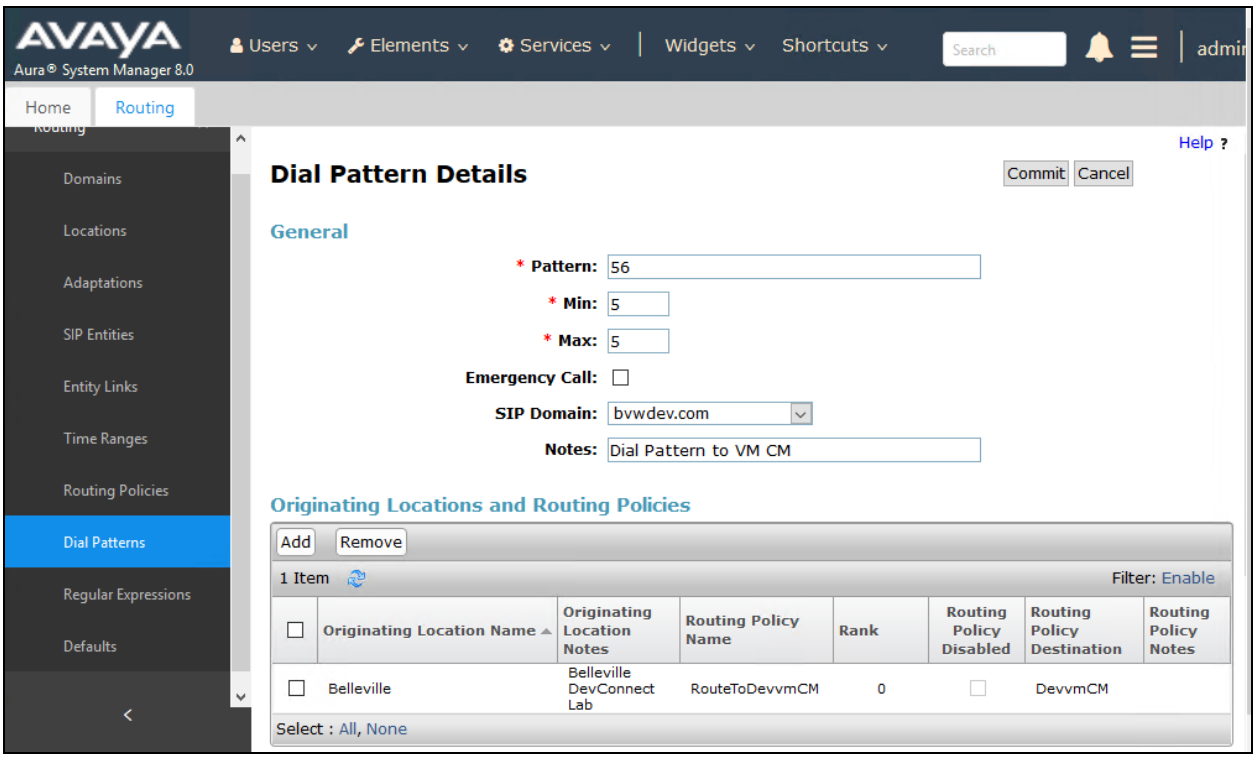
©2019 Avaya Inc. All Rights Reserved.

6.7.2. Dial Pattern for Communication Manager

Select **Dial Patterns** from the left pane and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Communication Manager. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case "56".
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 5.1.3**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Communication Manager. In the compliance testing, the entry allowed for call originations from all Responder endpoints in locations "Belleville". The Communication Manager routing policy from **Section 6.6.2** was selected as shown below.



©2019 Avaya Inc. All Rights Reserved.

7. 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.

©2019 Avaya Inc. All Rights Reserved.

7.1. 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

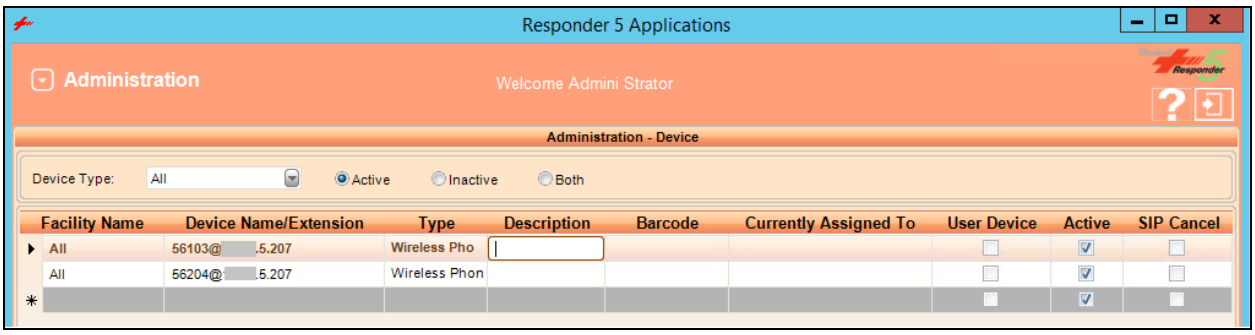
7.1.1. Configure Endpoints

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 Communication Manager 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 "56xxx" were H.323 and SIP devices administered on Communication Manager.

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



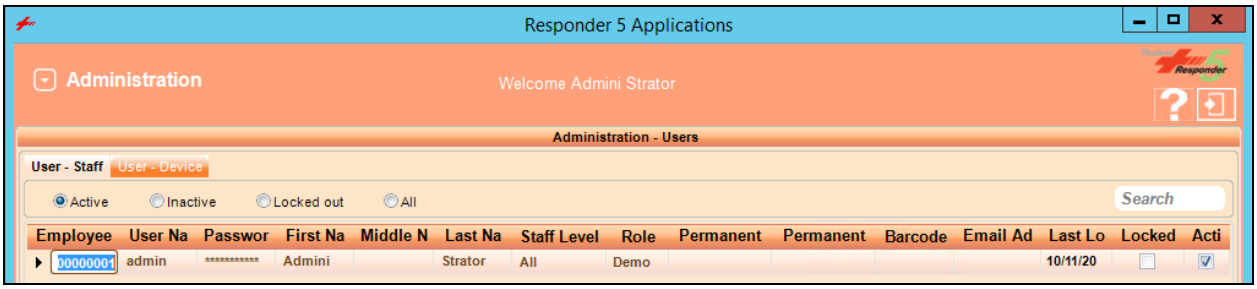
©2019 Avaya Inc. All Rights Reserved.

7.1.2. 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 7.1.3**.

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.



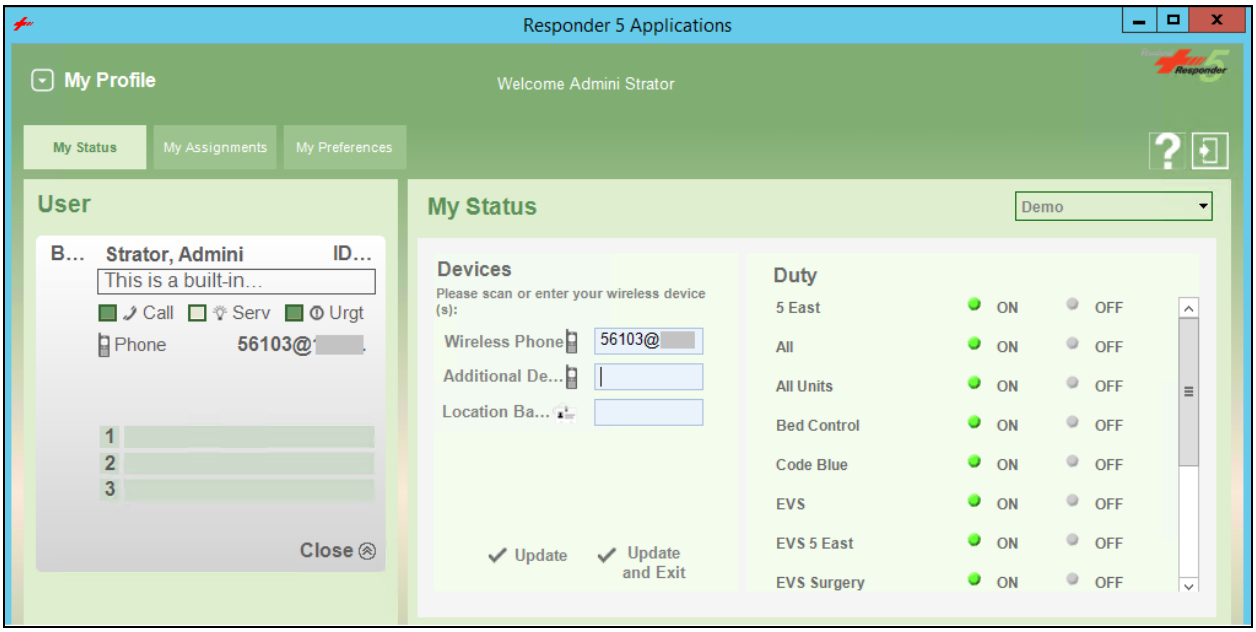
©2019 Avaya Inc. All Rights Reserved.

7.1.3. 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.

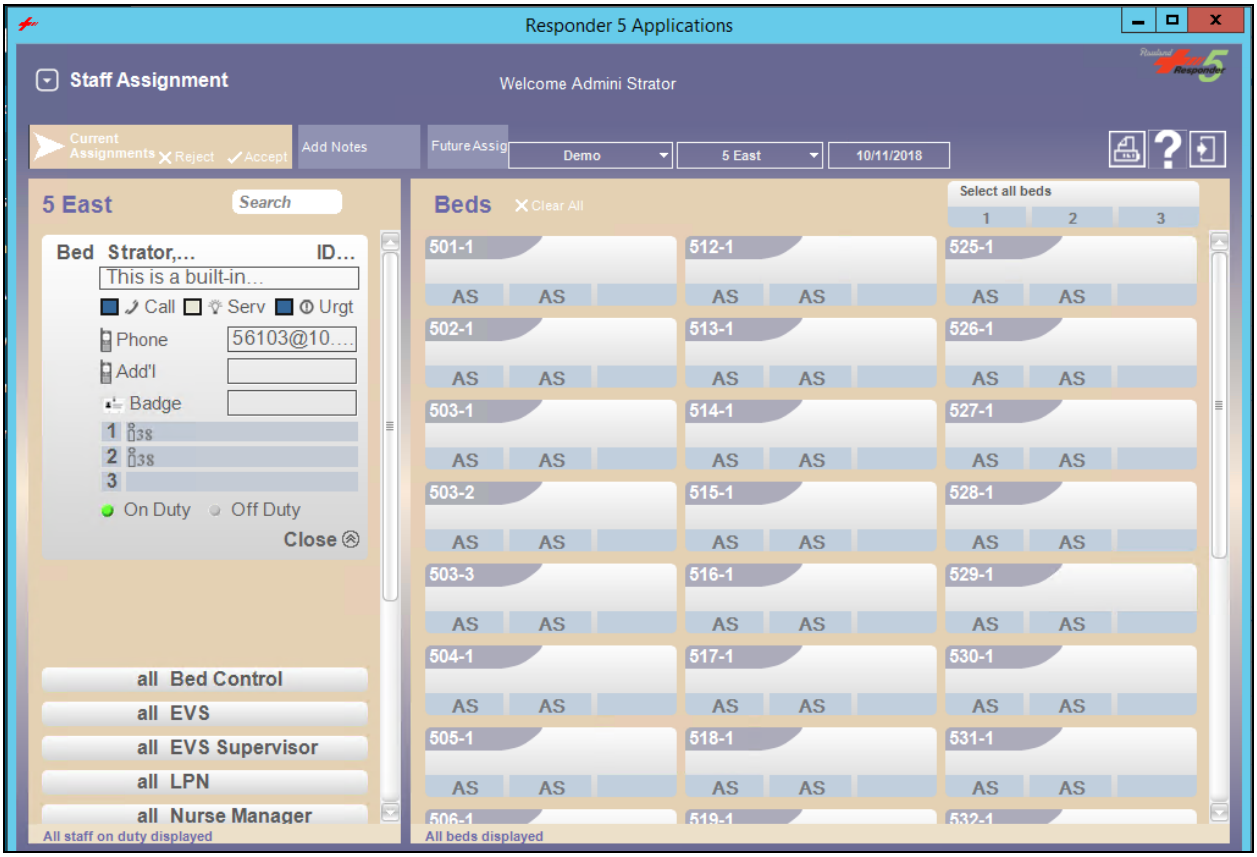
Click **Update** or **Update and Exit** (not shown) to commit the changes.



©2019 Avaya Inc. All Rights Reserved.

7.1.4. 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, "56103" 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.



©2019 Avaya Inc. All Rights Reserved.

7.2. 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

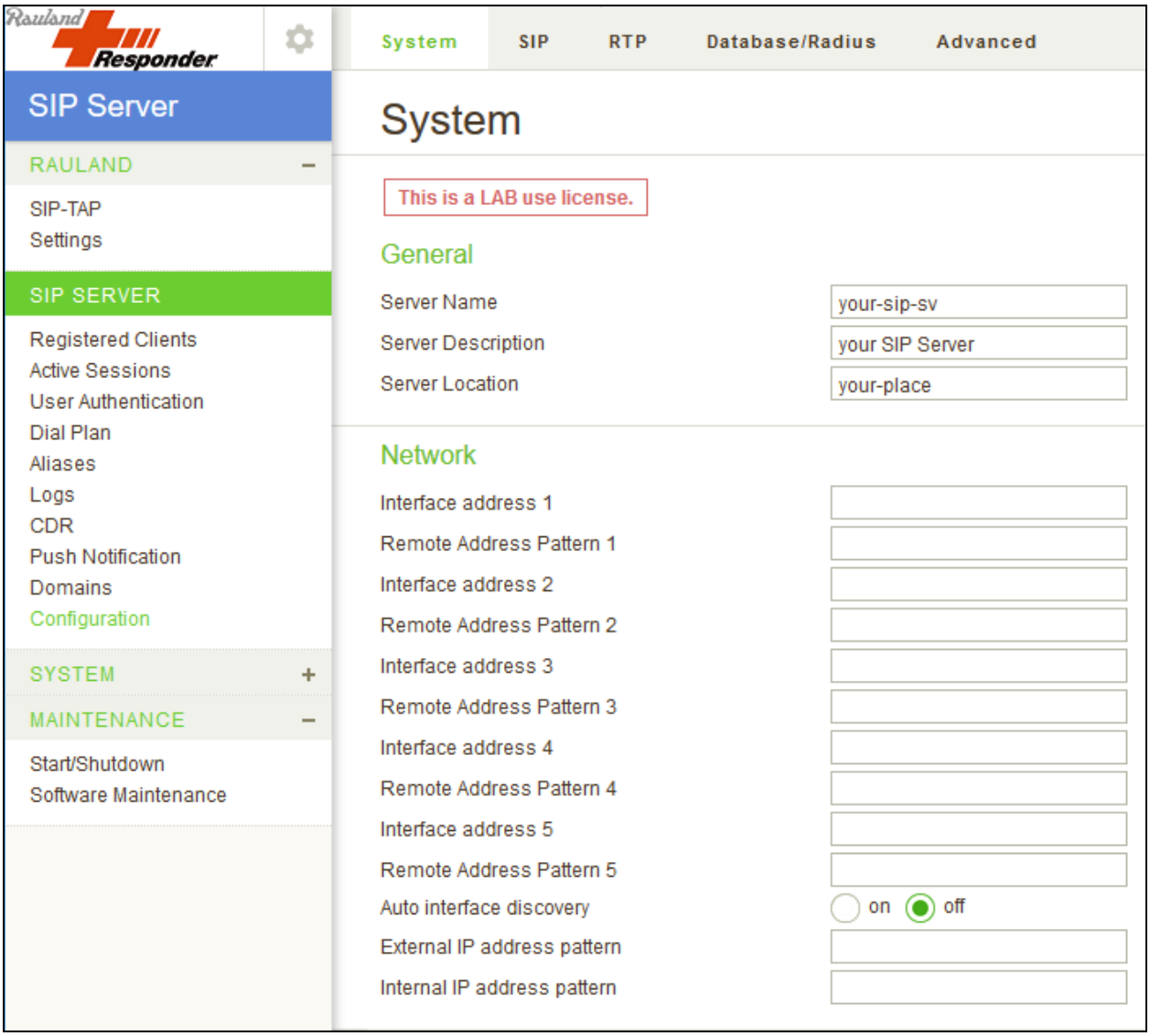
7.2.1. Login to SIP Server System

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.

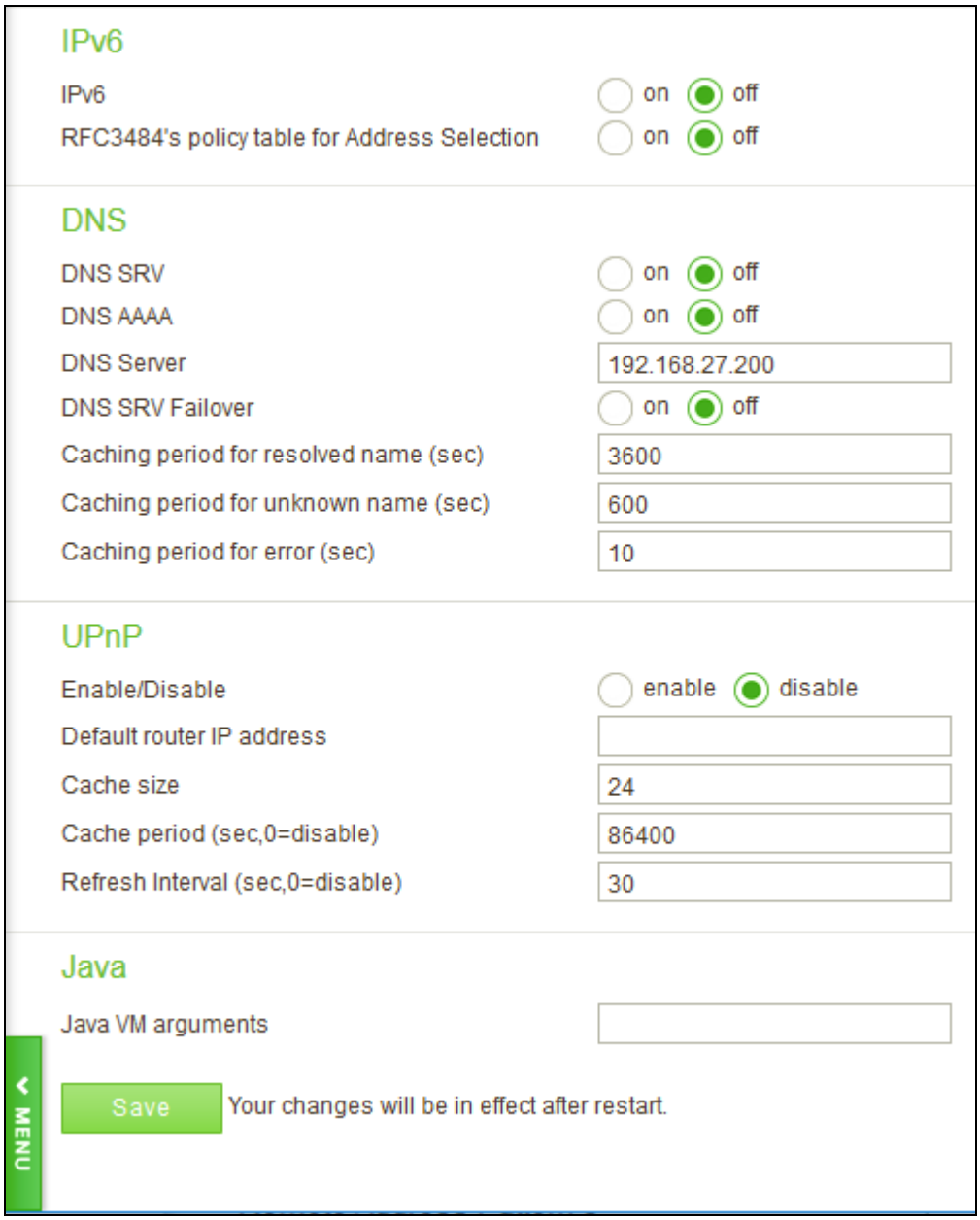
©2019 Avaya Inc. All Rights Reserved.

7.2.2. Configure SIP Server System Tab

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



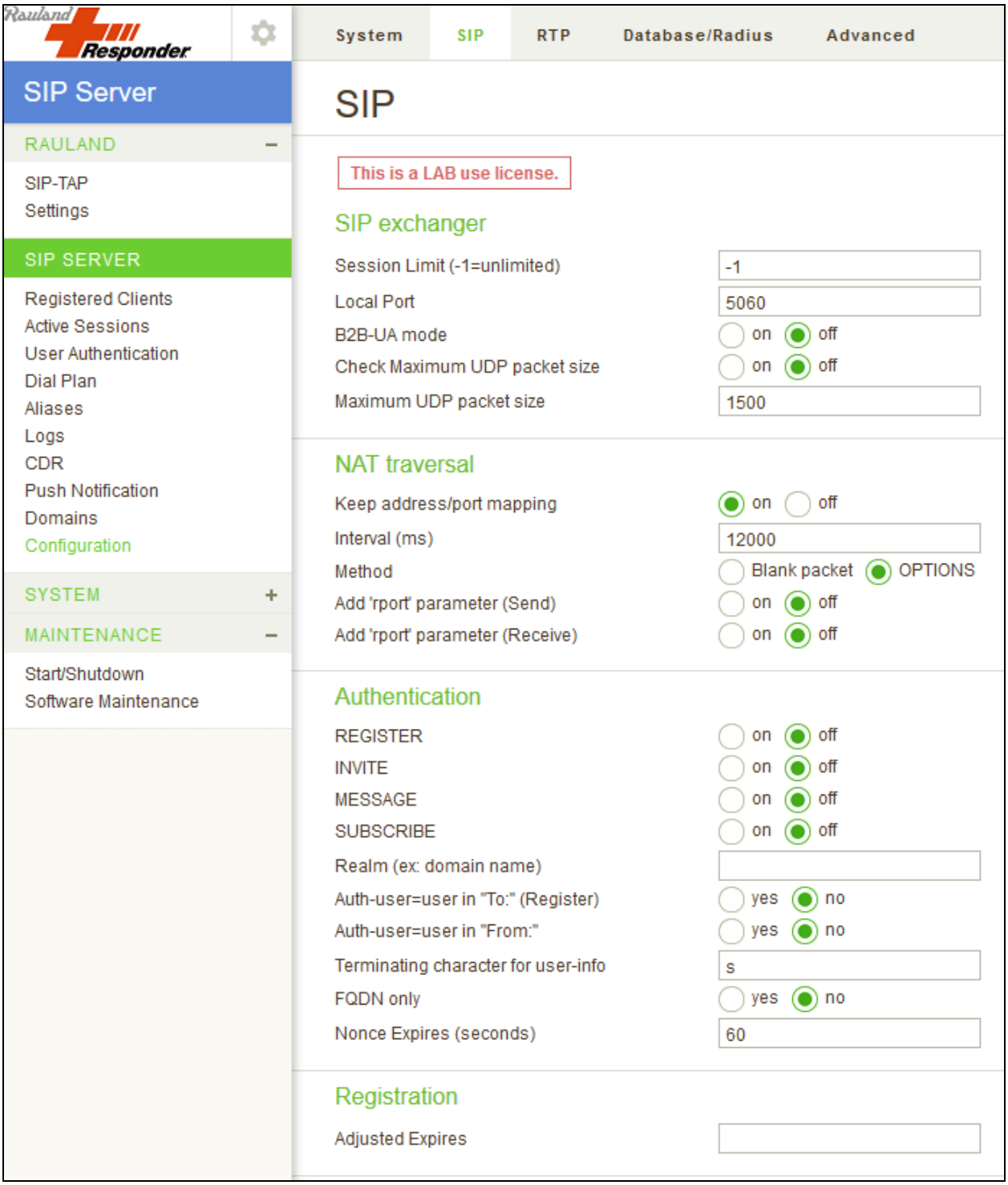
©2019 Avaya Inc. All Rights Reserved.



©2019 Avaya Inc. All Rights Reserved.

7.2.3. Configure SIP Server SIP Tab

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



©2019 Avaya Inc. All Rights Reserved.

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	

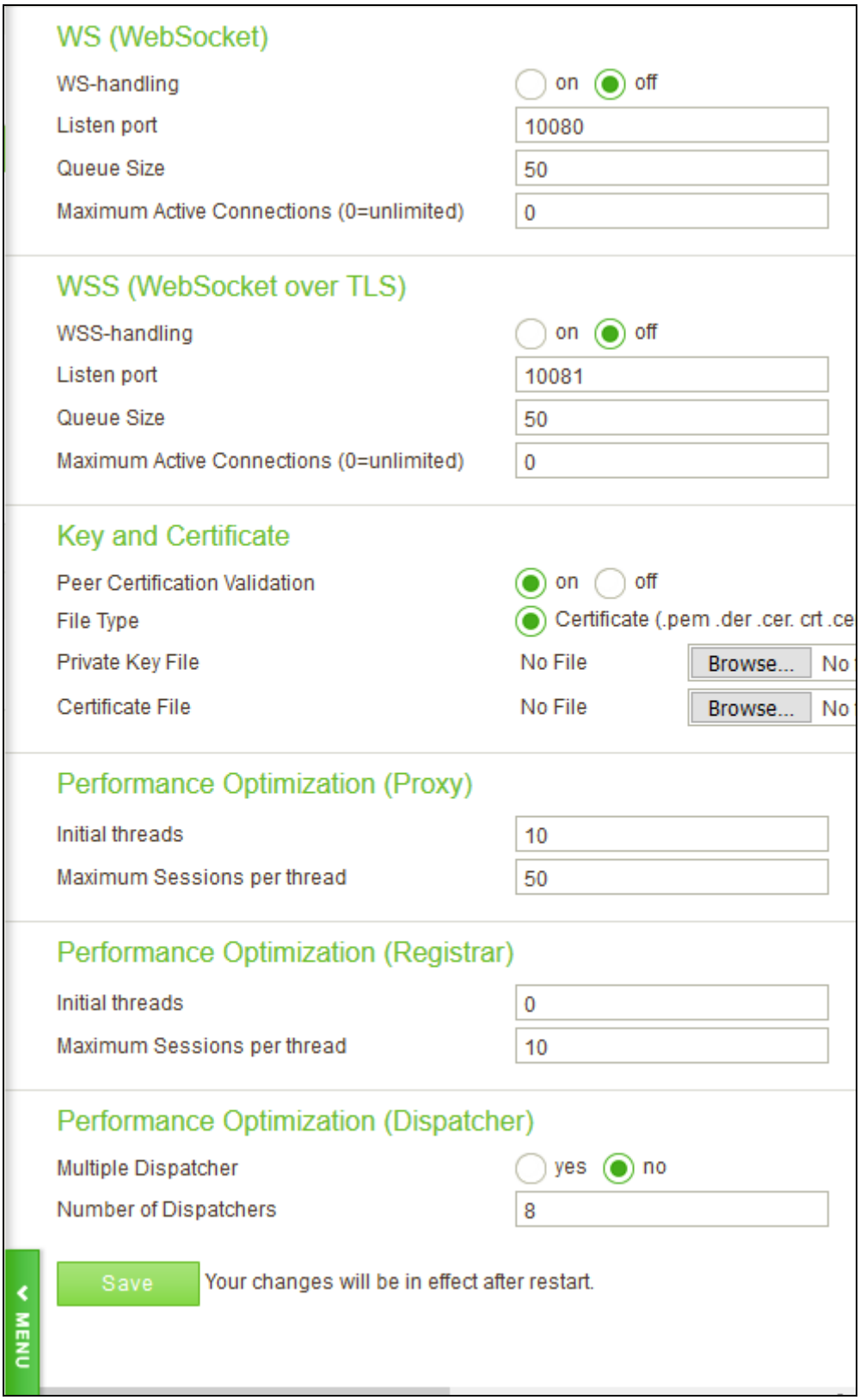
TCP

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

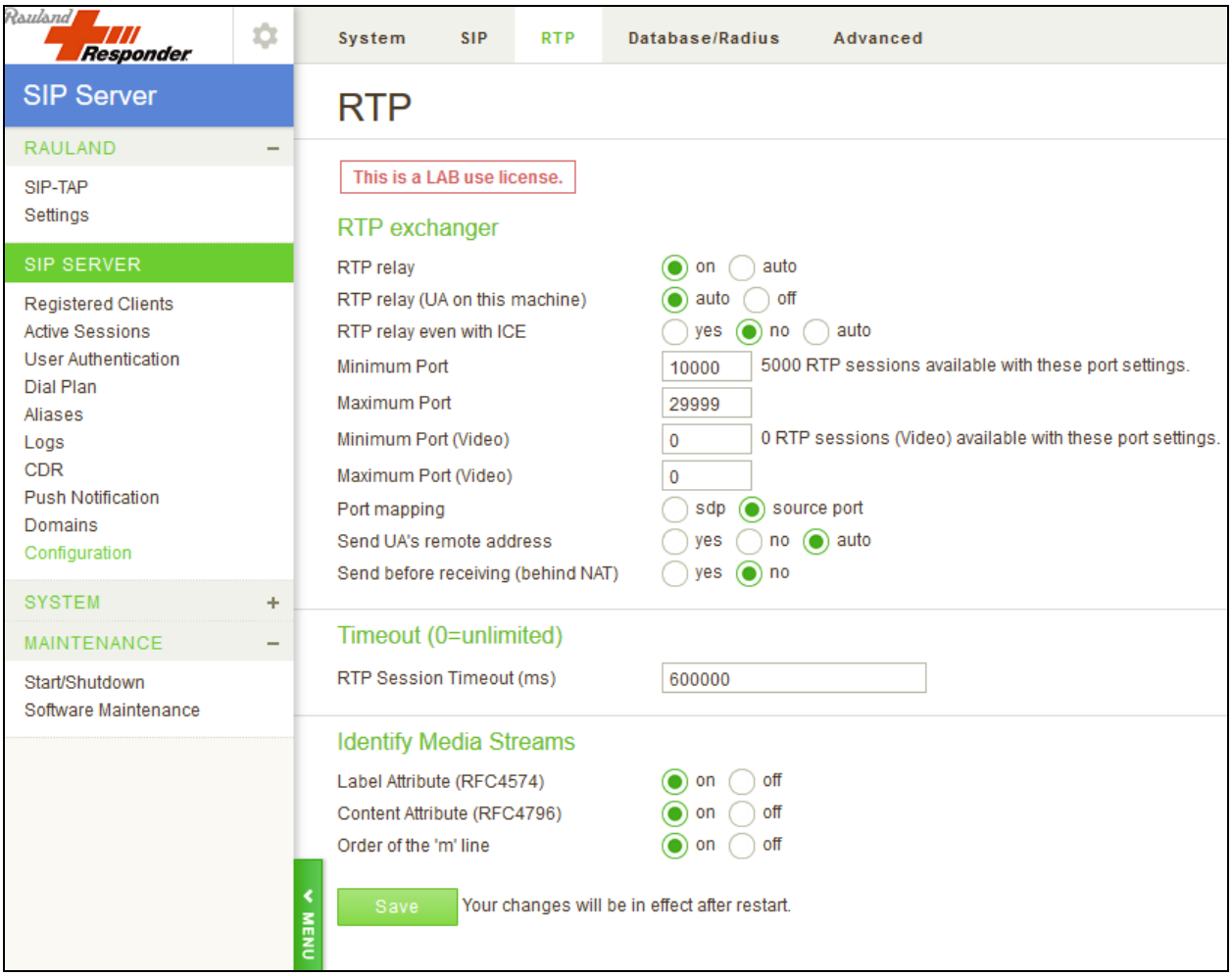
©2019 Avaya Inc. All Rights Reserved.



©2019 Avaya Inc. All Rights Reserved.

7.2.4. Configure SIP Server RTP Tab

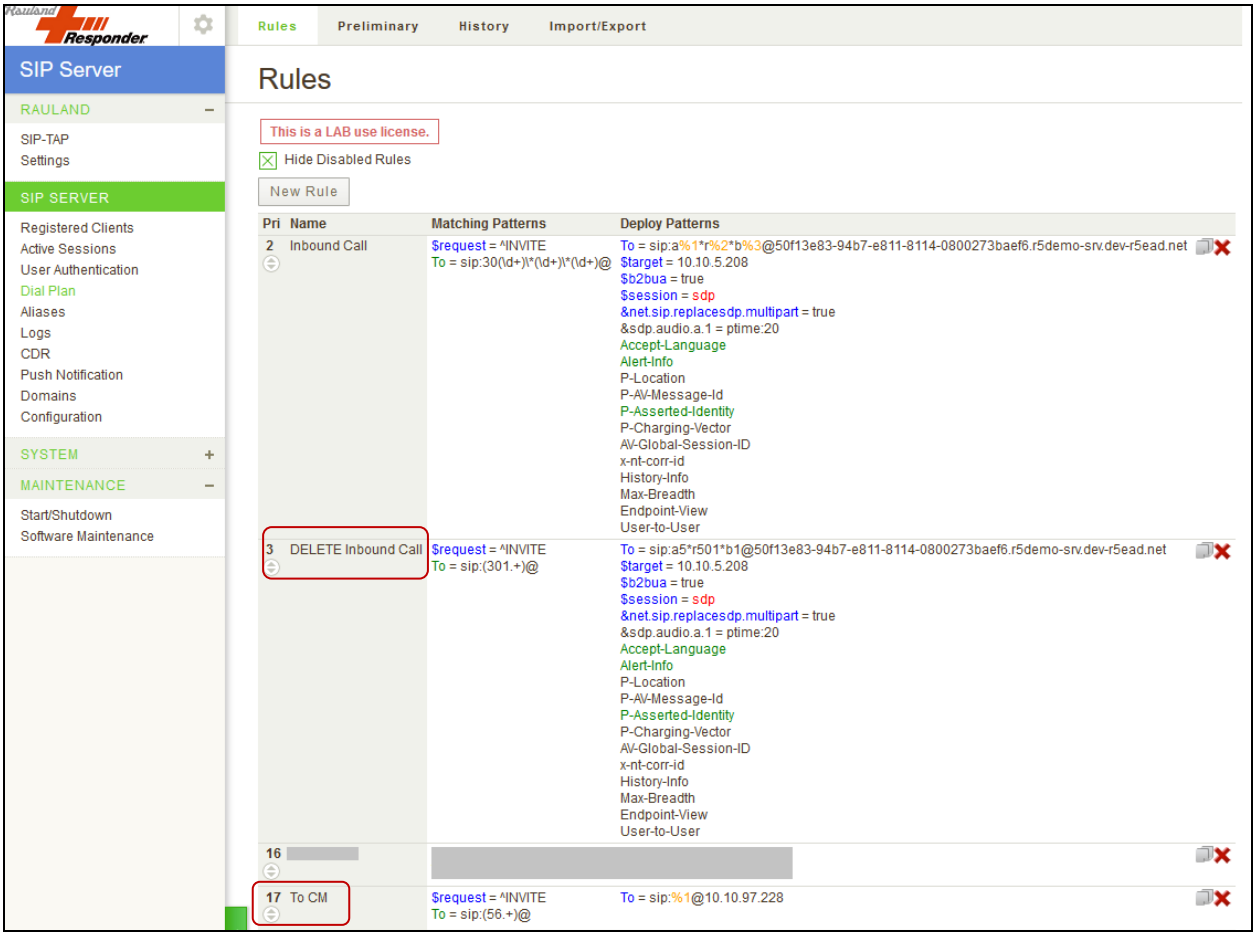
On the **RTP** screen, set **RTP Relay** to “on”, **RTP relay (UA on this machine)** to “auto” and **RTP relay even with ICE** to “no” and click **Save** to complete entries. Note, the **Minimum** and **Maximum Port** range settings should be sufficient to handle the maximum number of concurrent RTP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



©2019 Avaya Inc. All Rights Reserved.

7.2.5. 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 Communication Manager, the **To CM** rule was used.

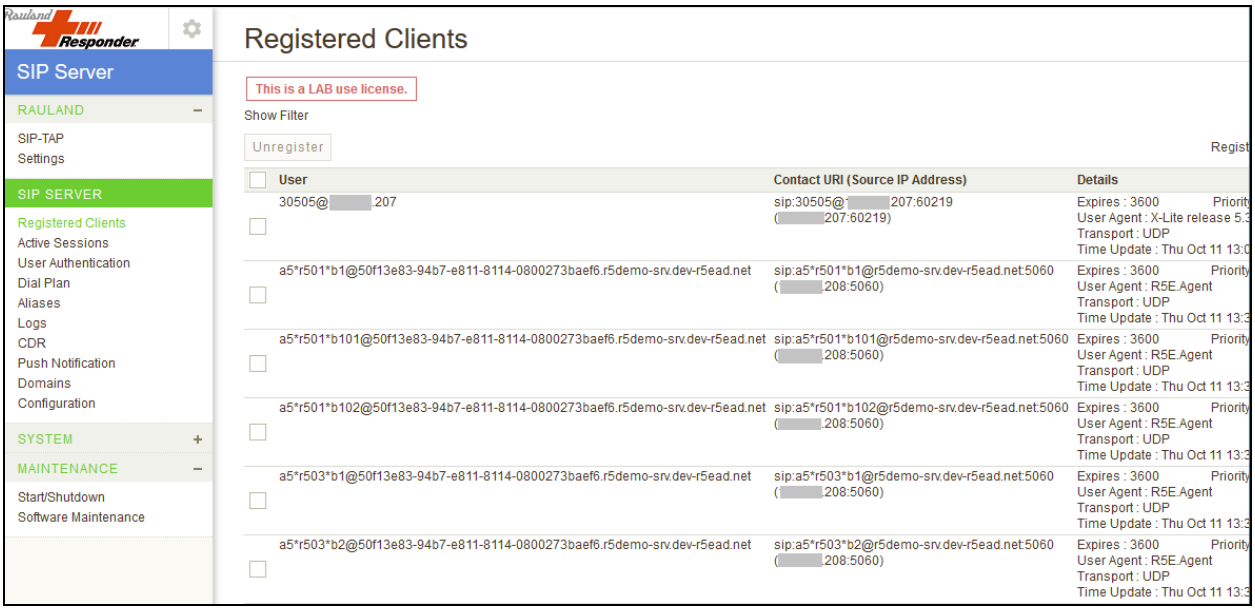


©2019 Avaya Inc. All Rights Reserved.

8. 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 hold, transfer and conference are not supported on the patient room devices.

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



©2019 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the procedures required to configure Rauland Responder Enterprise to interoperate with endpoints registered to Avaya Aura® Communication Manager via Avaya Aura® Session Manager using a Rauland 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**.

10. 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 Avaya Aura® Communication Manager in Virtual Appliance*, Release 8.0, Issue 3 September 2018.
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.0, Issue 1 July 2018.
3. *Administering Avaya Aura® Communication Manager*, Release 8.0, Issue 1 July 2018.
4. *Avaya Aura® Communication Manager Screen Reference*, Release 8.0, Issue 2 August 2018.
5. *Deploying Avaya Aura® Session Manager in Virtual Appliance*, Release 8.0, Issue 2 September 2018.
6. *Administering Avaya Aura® Session Manager*, Release 8.0, Issue 2 August 2018.
7. *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.0, Issue 2 September 2018.
8. *Administering Avaya Aura® System Manager for Release 8.0*, Release 8.0, Issue 4 September 2018.
9. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0, Issue 2 July 2018.
10. *Implementing and Administering Avaya Aura® Media Server*, Release 8.0, Issue 2 July 2018.

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

©2019 Avaya Inc. All Rights Reserved.

©2019 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.