Application Notes for Configuring Rauland-Borg Responder® 5 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager R6.3 – Draft 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of the Rauland-Borg Responder® 5 solution, Avaya Aura® Session Manager and Avaya Aura® Communication Manager R6.3.

The Rauland-Borg Responder® 5 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.

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-Borg Responder® 5 solution, Avaya Aura® Session Manager and Avaya Aura® Communication Manager R6.3.

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. It should be noted that the solution involves the use of a third party Brekeke SIP Server which is sold and supported by Rauland-Borg as a standard element of any solution involving SIP PBX integrations.

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 talk 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. The Compliance Test used a variety of wireless devices, including 3600 series SIP and IP wireless sets, Avaya one-X® Mobile SIP for Apple iOS devices (iPhone and iPad), and Avaya Flare Experience® for iPad as well as several stationary desksets.

2. General Test Approach and Test Results

The compliance test focused on the ability for Rauland Responder® 5 endpoints to initiate and receive calls to and from Session Manager and Communication Manager.

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. These functions were successfully carried out on Avaya devices registered to Session Manager and Communication Manager while connected to calls with Responder endpoints.

2.2. Test Results

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

The Responder Branch Regional Controller (BRC) media processing unit does not support media shuffling.

- Attempts by the Avaya Media Gateway, or Media Resource/Processing boards to offer direct audio connections between IP endpoints and the BRC failed. The impact of this was that additional DSP resources were required on the Avaya Media Gateways and Media Resource/Processing boards to accommodate connections to Responder endpoints. A customer should ensure that adequate VoIP resources are available based on expected call traffic.

2.3. Support

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

- Phone: 1-847-590-7130
- Web: http://www.rauland.com/

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager R6.3
- Avaya Aura® Session Manager R6.3
- Avaya Aura® System Manager R6.3
- Various IP, SIP and Digital endpoints. Note that most endpoints were wireless.
- Brekeke SIP Server
- Rauland-Borg Responder® 5 Branch Regional Controller
- Rauland-Borg Responder® 5 Communication Endpoints

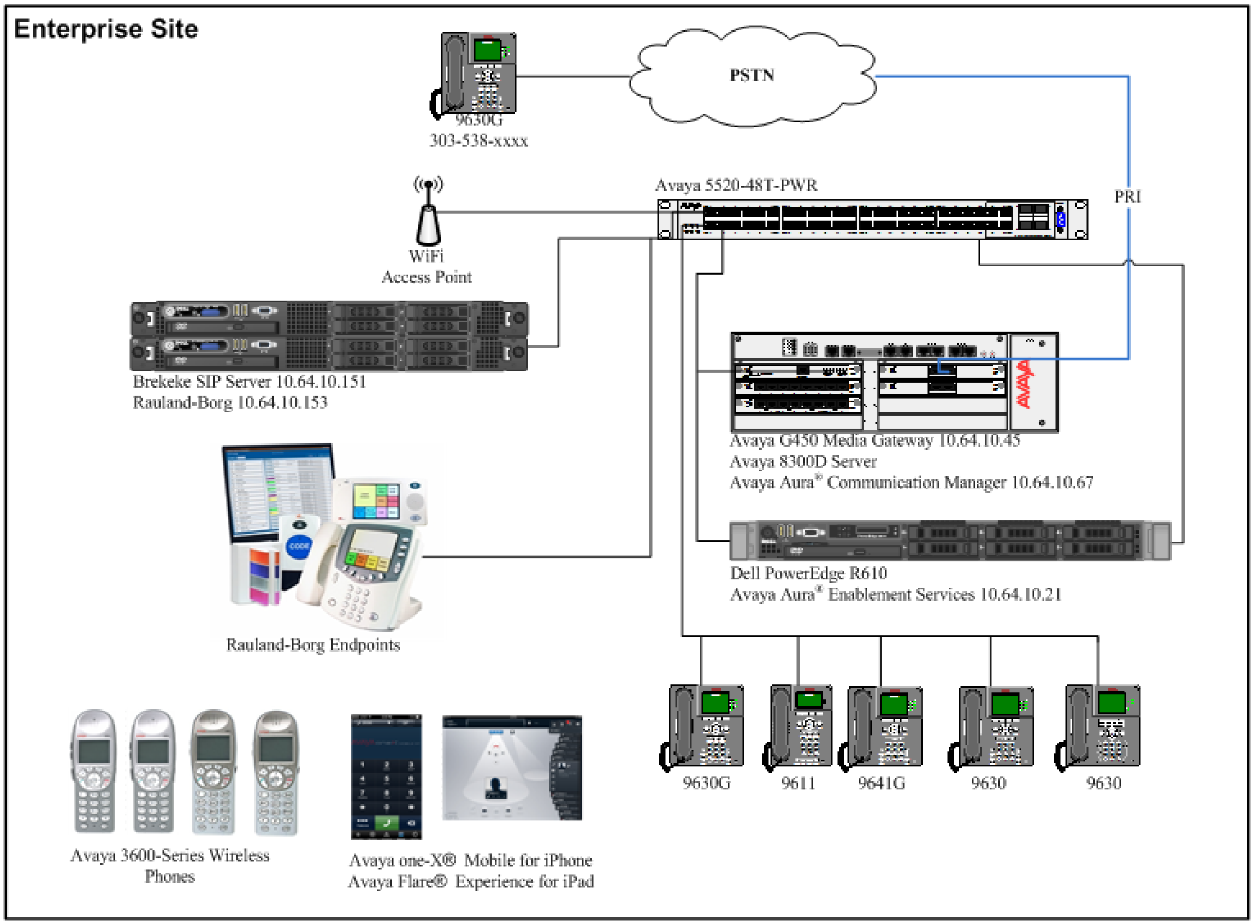

Enterprise Site
9630G
303-538-xxxx
PSTN
PRI
WiFi
Access Point
Avaya 5520-48T-PWR
Brekeke SIP Server 10.64.10.151
Rauland-Borg 10.64.10.153
Avaya G450 Media Gateway 10.64.10.45
Avaya 8300D Server
Avaya Aura® Communication Manager 10.64.10.67
Dell PowerEdge R610
Avaya Aura® Enablement Services 10.64.10.21
Rauland-Borg Endpoints
9630G
9611
9641G
9630
9630
Avaya 3600-Series Wireless Phones
Avaya one-X® Mobile for iPhone
Avaya Flare® Experience for iPad

Figure 1 – Rauland-Borg Responder® 5 Compliance Test Configuration

4. Equipment and Software Validated

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

Equipment	Version
Avaya S8300D Server - Avaya Aura® Communication Manager	R6.3 SP5
HP GL360 - Avaya Aura® Session Manager	R6.3 SP5
VMWare Virtual Appliance – Avaya Aura® System Manager	R6.3 SP3
Avaya G450 Media Gateway	31.20.1
Avaya Phones 3600 Series Wireless SIP Phones 3600 Series Wireless H.323 Phones 96x1 Series SIP Phones 96x1 Series H.323 Phone Phones 96x0 Series SIP Phone Phones	 201.513 117.056 6.3.1 6.3.1 2.6.11
Apple iPad 2 – Avaya Flare® Experience Apple iPhone 5s – Avaya one-X ®Mobile SIP	1.1.1 R6.2
Responder 5 endpoints and media gateway (BRC)	R5 – T12 SP2
Windows 2003 Server - Responder® 5 Applications	R5 – T12 SP2
Windows 2008R2 Server - Brekeke SIP Server	R3.243

5. Configure Avaya Aura® Communication Manager

Configuration of Communication Manager required standard station administration which will not be covered in these Application Notes. In addition, routing was configured to enable calls originating from Communication Manager and Session Manager registered endpoints to be able to reach the Responder endpoints.

5.1. Configure Communication Manager Details

Calls were routed to Rauland endpoints using a 3 digit 1xx pattern. All calls routed via 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.

Administration for the solution required the following steps:

- Confirm Licensing
- Add node-names
- Add SIP Signaling Group
- Add SIP Trunk Group
- Change Route Pattern
- Change AAR Analysis
- Confirm IP codecs

Step **Description**

1. **Confirm Licensing**

Using the **display system-parameters customer-options** command, confirm that the system has capacity for additional SIP Trunks. If additional license are required, contact an authorized Avaya Sales or Reseller representative.

```
display system-parameters customer-options                      Page   2 of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 1000  0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 100   3
                   Maximum Video Capable IP Softphones: 100   2
                       Maximum Administered SIP Trunks: 800   20
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

2. **Add node-names**

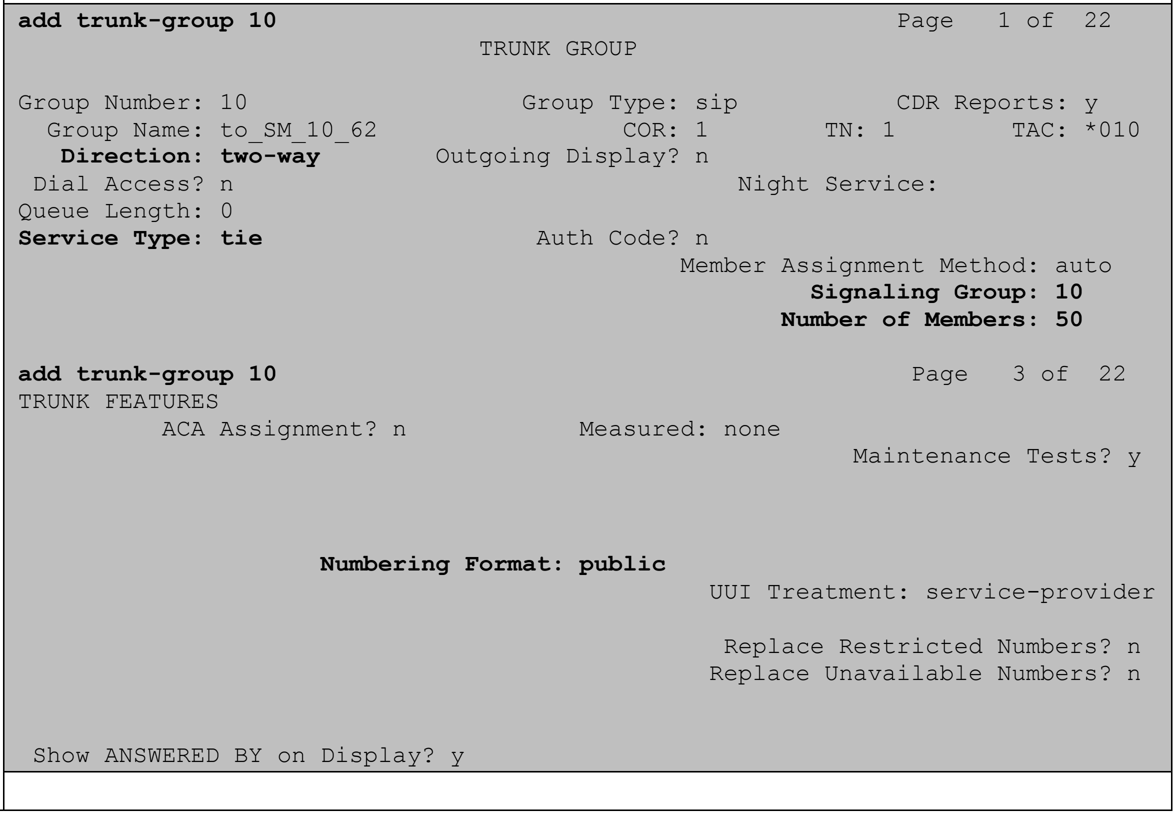
Communication Manager uses the node-names ip table as a host lookup table. Host names used in subsequent steps will refer to these. Using the **change node-names ip** command, entries were added for Session Manager (***SM_10_62***) and the processor Ethernet interface on Communication Manager (***procr***).

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
procr               10.64.10.67
SM_10_62            10.64.10.62
```

Step	Description
3.	**Add SIP Signaling Group** A signaling group was added using the **add signaling group 10** command with the following settings (settings not highlighted are default): **Group Type**: ***sip*** **Transport Method**: ***tls*** **Near-end Node Name**: ***procr*** **Far-end Node Name**: ***SM_10_62*** **Near-end Listen Port**: ***5061*** **Far-end Listen Port**: ***5061*** **Far-end Domain**: ***avaya.com*** (Match the domain on Session Manager). **Direct IP-IP Audio Connections: *n.*** (Responder does not support media shuffling) **DTMF over IP: *rtp-payload***

```
add signaling-group 10                                      Page   1 of   2
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? y        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

   Near-end Node Name: procr                  Far-end Node Name: SM_10_62
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: avaya.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? n
Session Establishment Timer(min): 3                       IP Audio Hairpinning? n
         Enable Layer 3 Test? y
```

Step	Description
4.	**Add SIP Trunk Group** Using the **add trunk-group 10** command, trunk group 10 was created with the following settings (settings not highlighted are default): **Group Type:** ***sip*** **Group Name:** ***to_SM_10_62*** **TAC:** ****010*** **Direction:** ***two-way*** **Service Type:** ***tie*** **Signaling Group:** ***10*** **Number of Members:** ***50*** **Numbering Format:** ***public***



```
add trunk-group 10                                           Page   1 of  22
                                TRUNK GROUP

Group Number: 10                   Group Type: sip           CDR Reports: y
  Group Name: to_SM_10_62                 COR: 1        TN: 1        TAC: *010
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 10
                                                     Number of Members: 50

add trunk-group 10                                            Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


 Show ANSWERED BY on Display? y
```

Step | **Description**

5.

Change Route Pattern

Route Pattern 10 was configured to use Trunk Group 10 for calls to Responder and Session Manager registered endpoints using the **change route-pattern 10** command with the following settings (settings not highlighted are default):

Pattern Name: ***SM***
Grp No: ***10*** (This specifies the Trunk Group to use)
FRL: ***0*** (This can be used as a security setting to restrict access to trunks based on Class Of Restriction, 0 is least restrictive).

```
change route-pattern 10                                        Page   1 of   3
                    Pattern Number: 202 Pattern Name: SM
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 10   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  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

6.

Change AAR Analysis

Using the **change aar analysis 1** command, dialed strings of ***3*** digits beginning with a ***1*** were instructed to use the ***Route Pattern 10*** configured in the previous step. Note all Responder endpoints used a 3 digit 1xx extension.

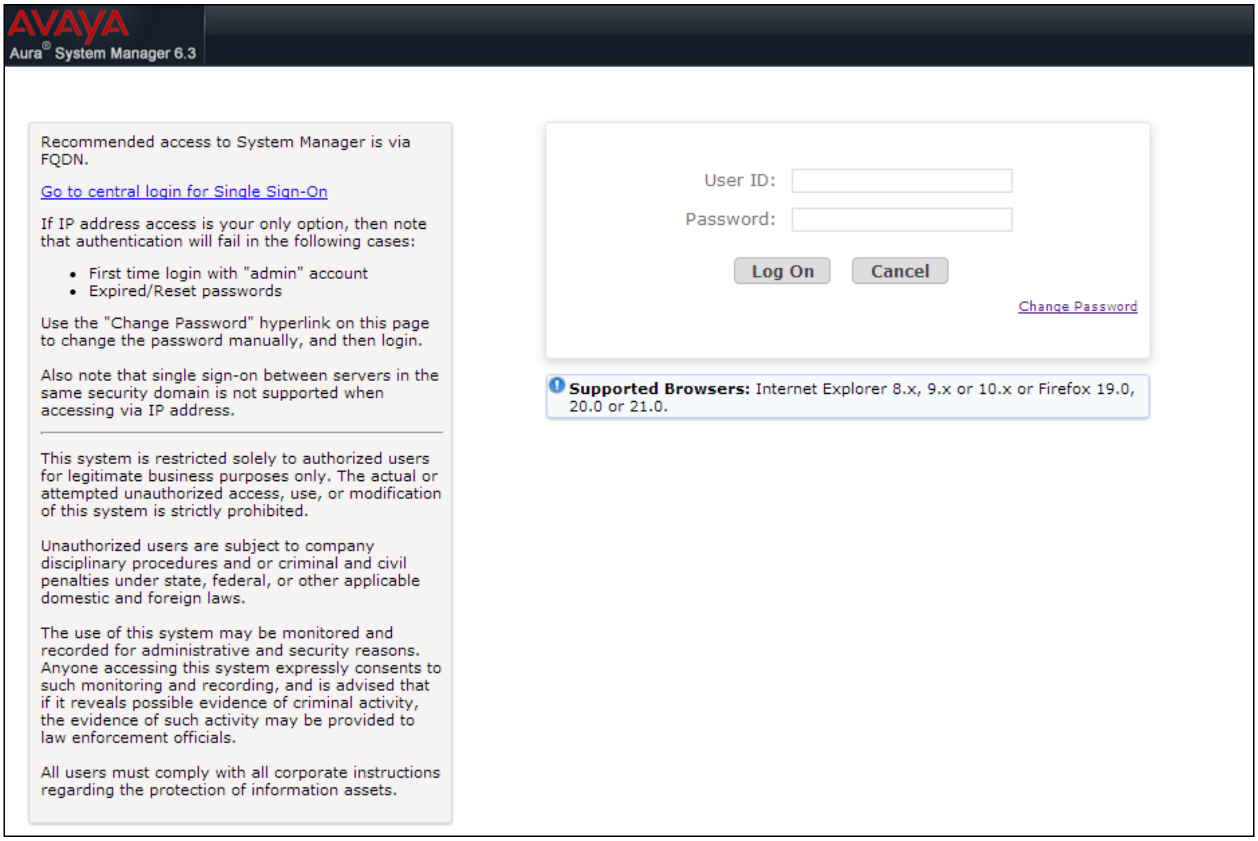
```
change aar analysis 1                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    2

          Dialed           Total      Route    Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    1                     3    3     10        aar          n
```

Step	Description
7.	**Confirm IP codecs** Use the **change ip-codec-set n** command to add or change RTP codecs. In the test environment, codec set 1 was used for all endpoints and trunks. **G.711MU** was used for all calls with responder endpoints, the Responder BRC does not support G.729. As the media gateway was required to be connected to all calls, the gateways were able to transcode RTP enabling different codecs to be used for each leg of the call.

```
change 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: G.729             n          2        20
```

6. Configure Avaya Aura® Session Manager

Session Manager is administered via the Avaya Aura® System Manager web interface. In a browser, navigate to **https//:<hostname>/** and login with appropriate credentials. Use the hostname or IP Address of the System Manager server in the URL.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

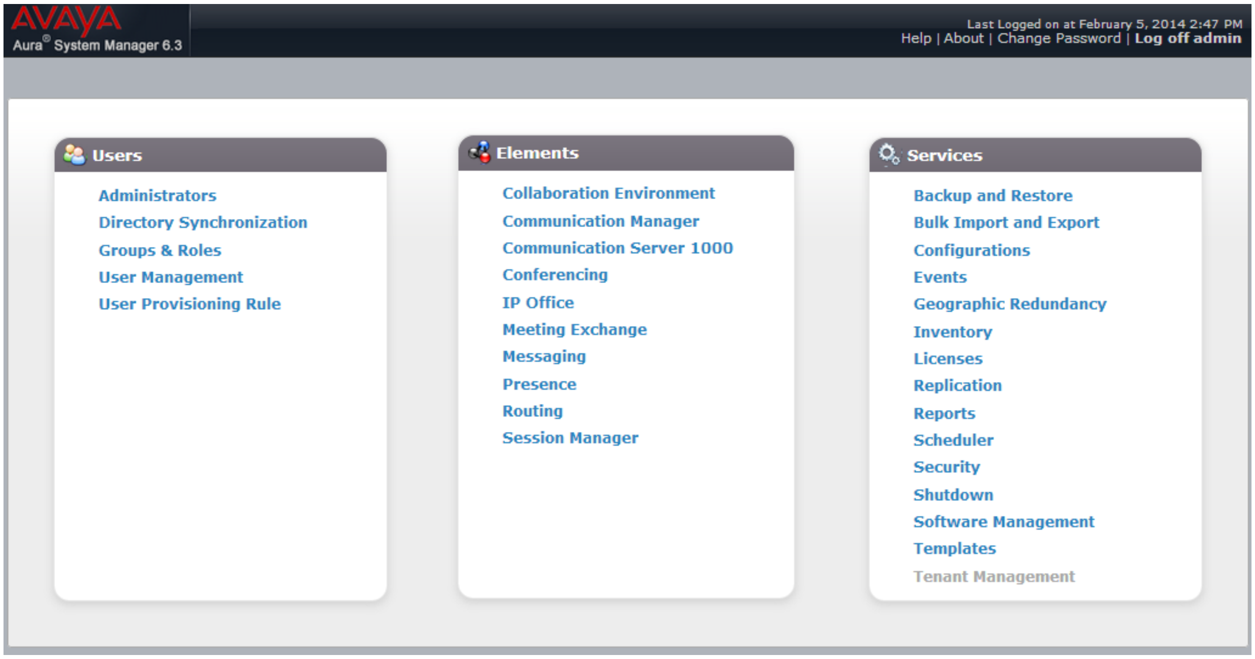
All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 19.0, 20.0 or 21.0.

All navigation is performed by clicking links in the navigation links on the System Manager landing page as demonstrated below.



6.1. Configure Session Manager Details

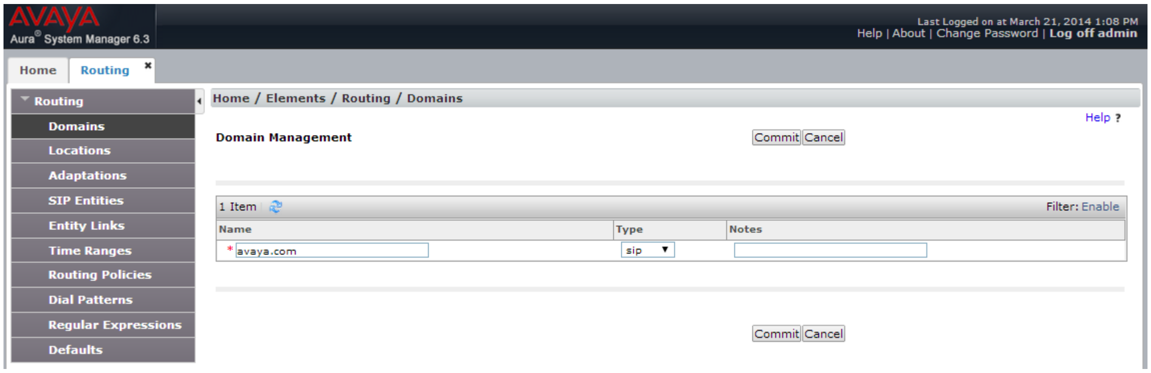
Administration for the solution required the following steps:

- Add a Domain
- Add a Location
- Add a SIP Entity
- Add a SIP Entity Link
- Create an Adaptation Rule
- Create a Routing Policy
- Create a Dial Pattern

1. Navigate to **Routing → Domains** and select **New** to a domain.

- **Name:** Type in a domain name that was used in **Section 5.1 Step 3**.
- **Type:** ***sip*** – selected from the list.

Click **Commit** to save changes.



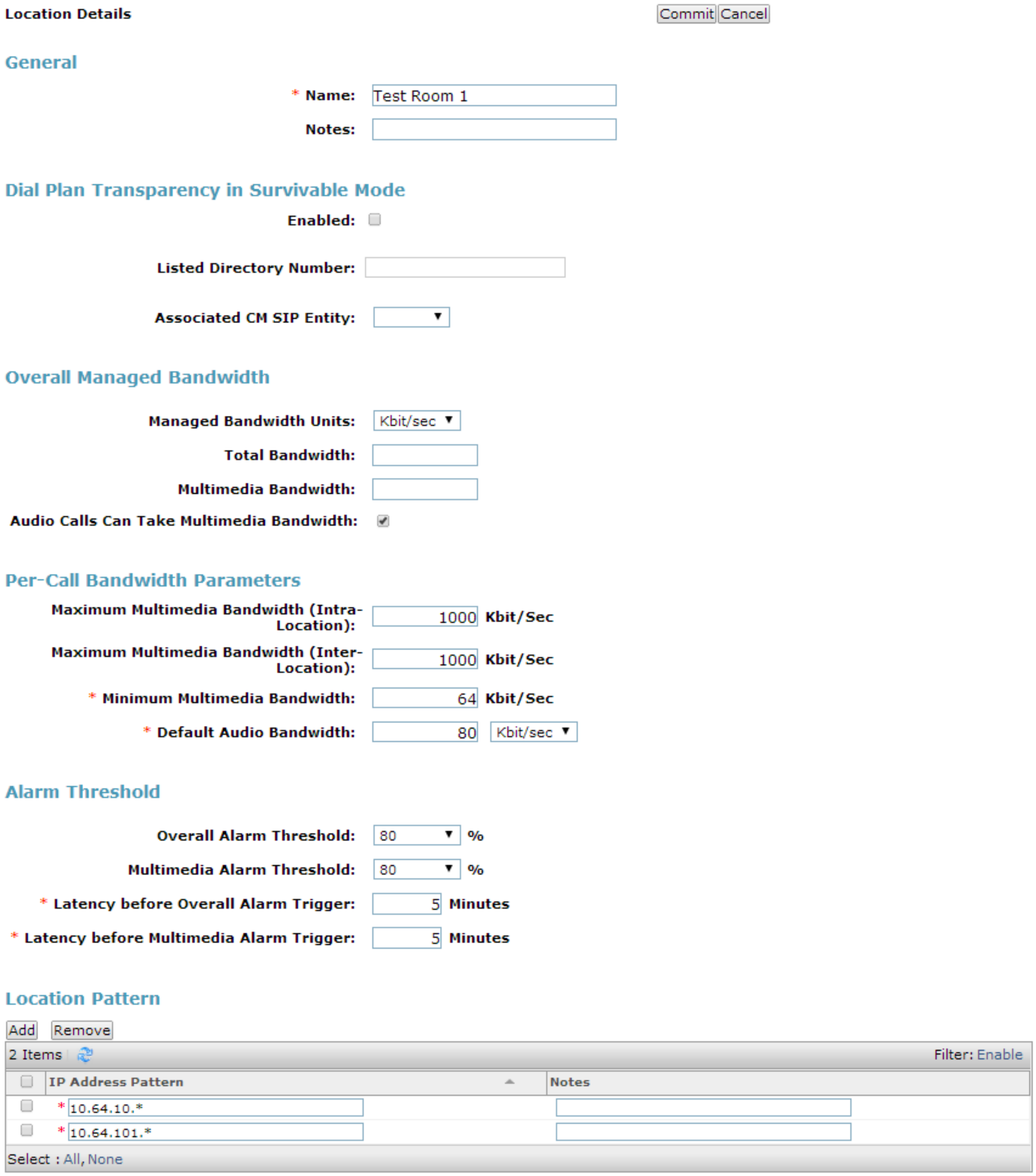
Domain Management

Name	Type	Notes
* avaya.com	sip	

2. Navigate to **Routing → Locations** and select **New** to add a new location.

- **Name:** Enter a descriptive name (***Test Room 1***)
- Add a pattern for the range subnets that are used in **IP Address Pattern *(10.64.10.*)***

Click **Commit** to save changes.



Location Details

General

* Name:	Test Room 1
Notes:	

Dial Plan Transparency in Survivable Mode

Enabled:	□
Listed Directory Number:	
Associated CM SIP Entity:	

Overall Managed Bandwidth

Managed Bandwidth Units:	Kbit/sec
Total Bandwidth:	
Multimedia Bandwidth:	
Audio Calls Can Take Multimedia Bandwidth:	☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):	1000	Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):	1000	Kbit/Sec
* Minimum Multimedia Bandwidth:	64	Kbit/Sec
* Default Audio Bandwidth:	80	Kbit/sec

Alarm Threshold

Overall Alarm Threshold:	80	%
Multimedia Alarm Threshold:	80	%
* Latency before Overall Alarm Trigger:	5	Minutes
* Latency before Multimedia Alarm Trigger:	5	Minutes

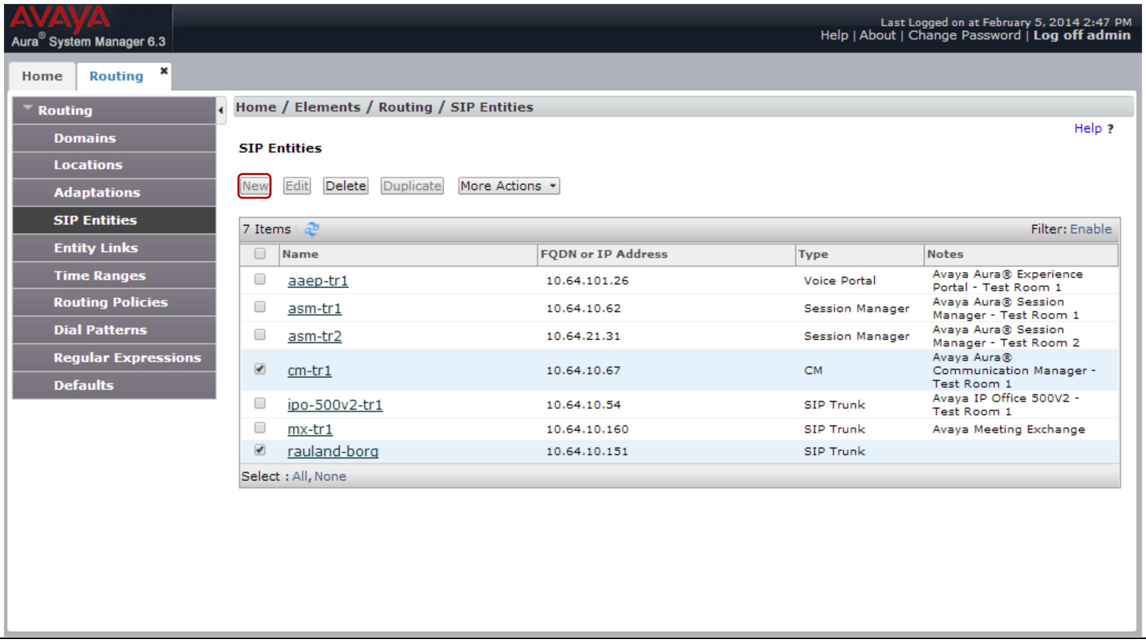
Location Pattern

□	IP Address Pattern	Notes
□	* 10.64.10.*	
□	* 10.64.101.*	

3.

Add a SIP Entity

Navigate to **Routing → SIP Entities** and click **New** to add a new SIP Entity for the Brekeke SIP Server. In the illustration below, the entities for Communication Manager (***cm-tr1***) and the Brekeke SIP Server (***rauland-borg***) are illustrated:



SIP Entities

7 Items Filter: Enable

☐	Name	FQDN or IP Address	Type	Notes
☐	aaep-tr1	10.64.101.26	Voice Portal	Avaya Aura® Experience Portal - Test Room 1
☐	asm-tr1	10.64.10.62	Session Manager	Avaya Aura® Session Manager - Test Room 1
☐	asm-tr2	10.64.21.31	Session Manager	Avaya Aura® Session Manager - Test Room 2
☑	cm-tr1	10.64.10.67	CM	Avaya Aura® Communication Manager - Test Room 1
☐	ipo-500v2-tr1	10.64.10.54	SIP Trunk	Avaya IP Office 500V2 - Test Room 1
☐	mx-tr1	10.64.10.160	SIP Trunk	Avaya Meeting Exchange
☑	rauland-borg	10.64.10.151	SIP Trunk	

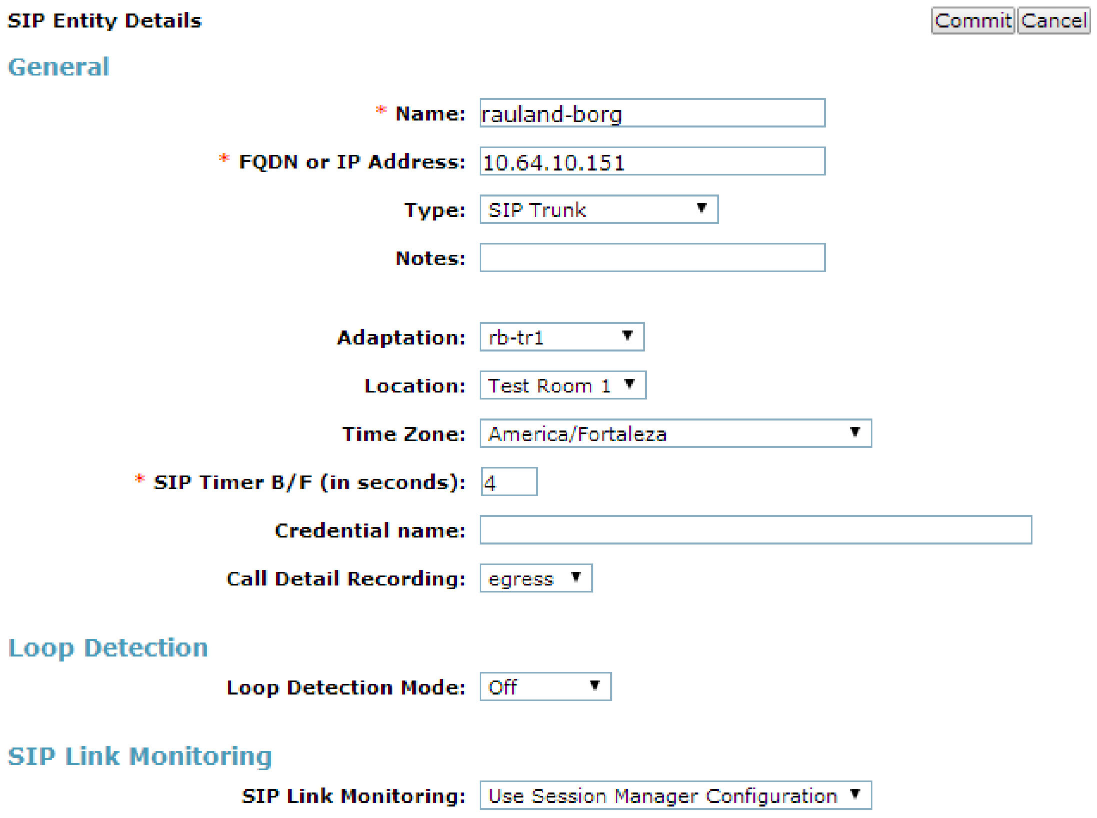
Select : All, None

Add a SIP Entity (Continued)

On the SIP Entity Details screen which appears when the New button is pressed above, enter the following:

- **Name**: Enter a descriptive name for the entity (***rauland-borg***).
- **FQDN or IP Address:** ***10.64.10.151*** was the address used by the Brekeke SIP server in the test configuration.
- **Type:** ***SIP Trunk***
- **Notes:** useful for quick glance identification on other screens.
- **Adaptation:** This was modified in a subsequent step with the adaptation called ***rb-tr1*** created in **Step 3** below but is described in this step for brevity.
- **SIP Link Monitoring:** This was set to ***Use Session Manager Configuration***.

Click **Commit** to complete the entries on this screen.



SIP Entity Details

General

* Name: rauland-borg

* FQDN or IP Address: 10.64.10.151

Type: SIP Trunk

Notes:

Adaptation: rb-tr1

Location: Test Room 1

Time Zone: America/Fortaleza

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Note: Communication Manager SIP Entity (***cm-tr1***) was pre-configured and is not shown in this document. Communication Manager SIP Enitity was configured in similar mannar with the exeception of **Type**; it was set to ***CM***.

4.

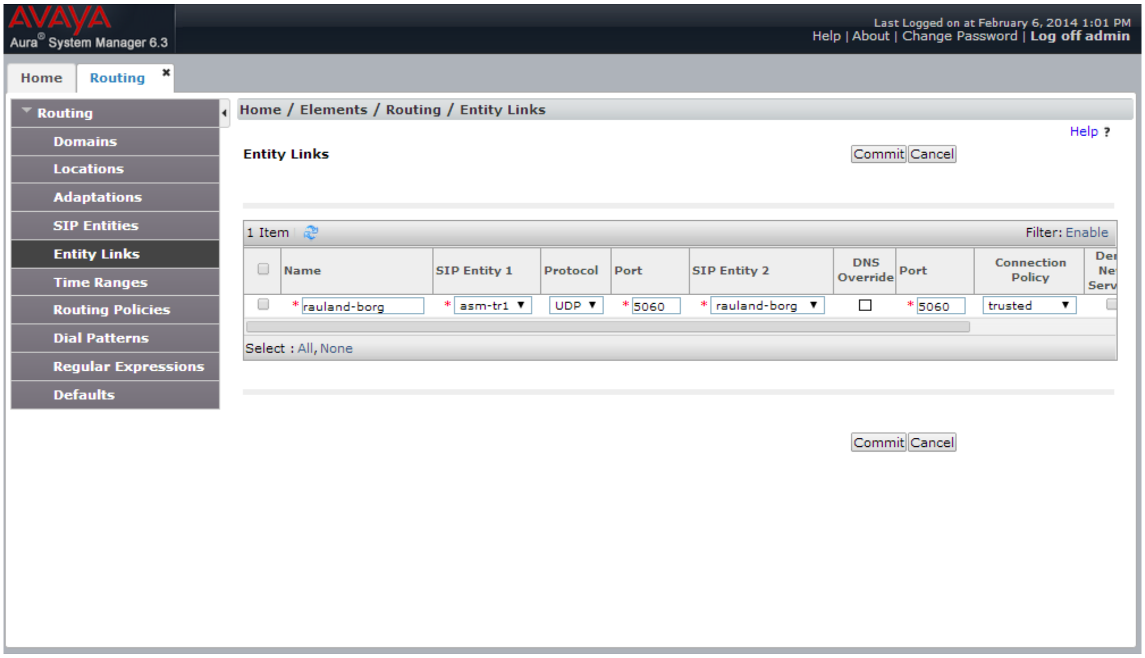
Add a SIP Entity Link

Navigate to **Routing → Entity Links** and click **New** to add a new Entity Link to the Brekeke SIP Server (not shown).

Enter the following to create the Entity Link:

- **Name**: ***rauland-borg*** - A Descriptive name for the Entity Link.
- **SIP Entity 1: *sm-tr1* -** Select the existing Session Manager SIP Entity.
- **SIP Entity 2**: ***rauland-borg*** – Select the newly created SIP entity.
- **Protocol:** use ***UDP*** for the transport protocol.
- **Port: *5060*** – Port 5060 is the standard listen port for the UDP SIP transport protocol.

Click **Commit** to save the entries.



Entity Links

1 Item   Filter: Enable

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Der Ne Serv
□	* rauland-borg	* asm-tr1 ▼	UDP ▼	* 5060	* rauland-borg ▼	□	* 5060	trusted ▼	□

Select : All, None

Note: Communication Manger SIP Entity link was pre-configured and is not shown in this document. Communication Manager SIP Entity was configured in similar manner with the exception of **Protocol**; it was set to ***tls***.

5. **Create an Adaptation Rule**

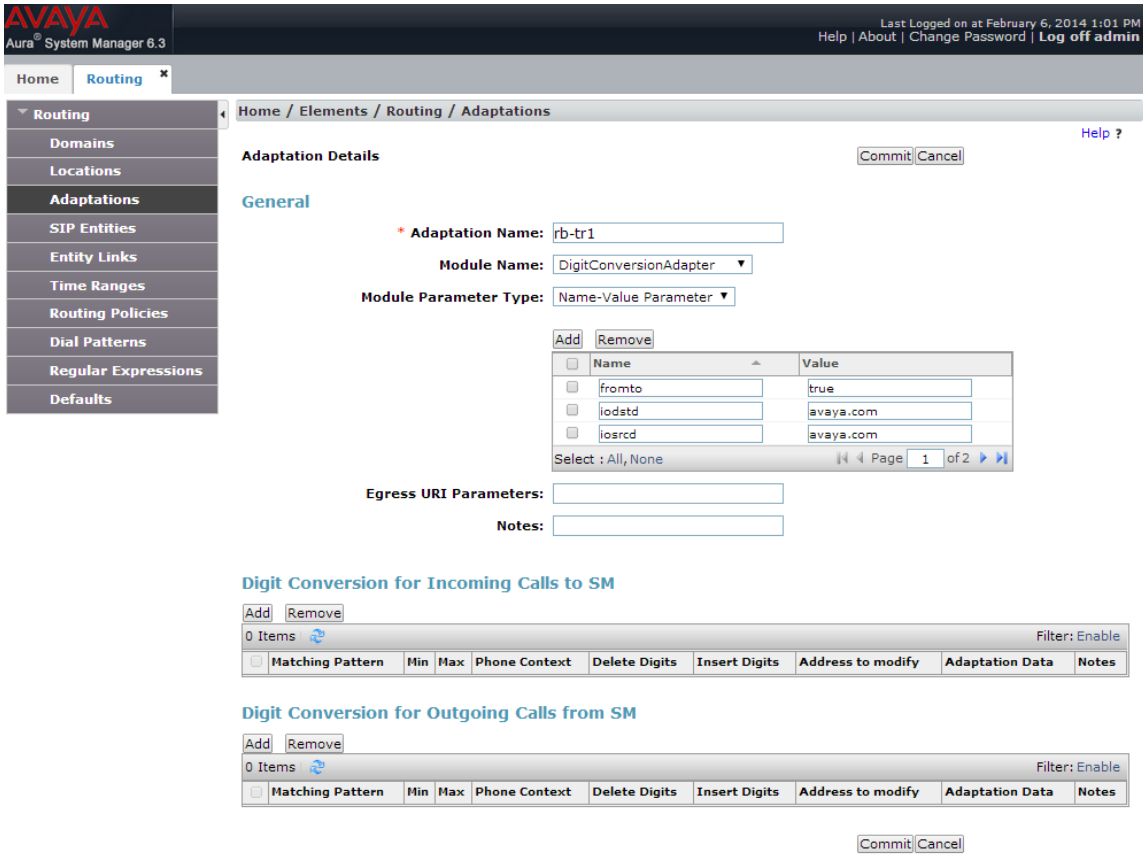
Session Manager used an Adaptation rule for two purposes. First, domains in the To and From headers were modified to reconcile differences in the ***Avaya*** domain used on Session Manager and Communication Manager, and the IP Address of the Brekeke SIP Server used as the domain on that side of the call flow.

Navigate to **Routing → Adaptations** and click **New** (not shown) to add an Adaptation rule. For this rule, the following entries were made:

- **Adaption Name**: ***rb-tr1*** – Any Descriptive name.
- **Module name**: ***DigitConversionAdapter*** – Selected from the list.
- **Module Parameter**: Select ***Add*** and add the following in *Name* and *Value*
  - ***fromto=true***
  - ***iodstd=avaya.com***
  - ***iosrcd=avaya.com***
  - ***osrcd=10.64.10.62***
  - ***odstd=10.64.10.151***

  This defines a rule to modify domains in SIP headers. See product documentation [2] for more information on the use of Adaptation Rules.

Click **Commit** to save the changes, then add the adaptation rule to the SIP Entity form as illustrated in Step 1 above.



Adaptation Details

General

* Adaptation Name:	rb-tr1
Module Name:	DigitConversionAdapter
Module Parameter Type:	Name-Value Parameter

	Name	Value
□	fromto	true
□	iodstd	avaya.com
□	iosrcd	avaya.com

Egress URI Parameters:	
Notes:	

Digit Conversion for Incoming Calls to SM

0 Items

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM

0 Items

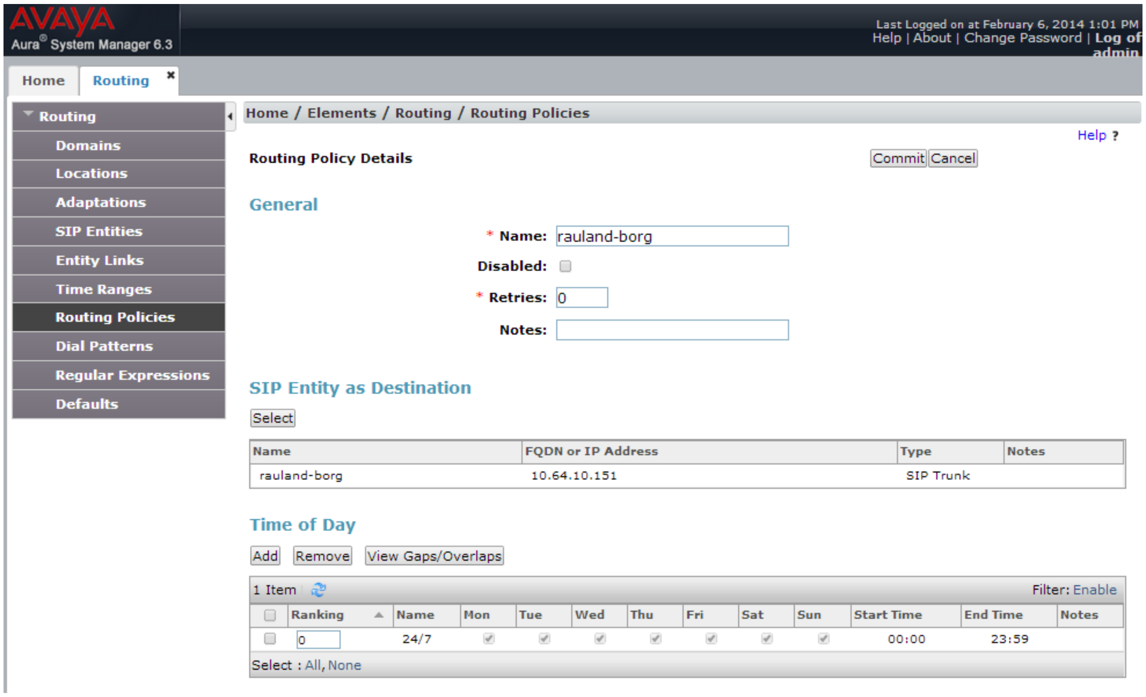
□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

6. **Create a Routing Policy**

Routing Policies require definition of a Routing Policy, and definition of Dial Patterns. A new Routing Policy is created first, leaving the Dial Pattern undefined, then a Dial Pattern is defined, then the Dial Pattern is applied to the Routing Policy.

Navigate to **Routing → Routing Policies** and click the **New** button (not shown). On the **Routing Policy Details** page, provide a **Name** and **Notes** as desired for the policy. Click the **Select** button to select the **SIP Entity as Destination** (not shown). The ***rauland-borg*** SIP Entity was selected as the Destination.

Click **Commit** to save the entries.



Routing Policy Details

General

* Name: rauland-borg

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
rauland-borg	10.64.10.151	SIP Trunk	

Time of Day

1 Item

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	

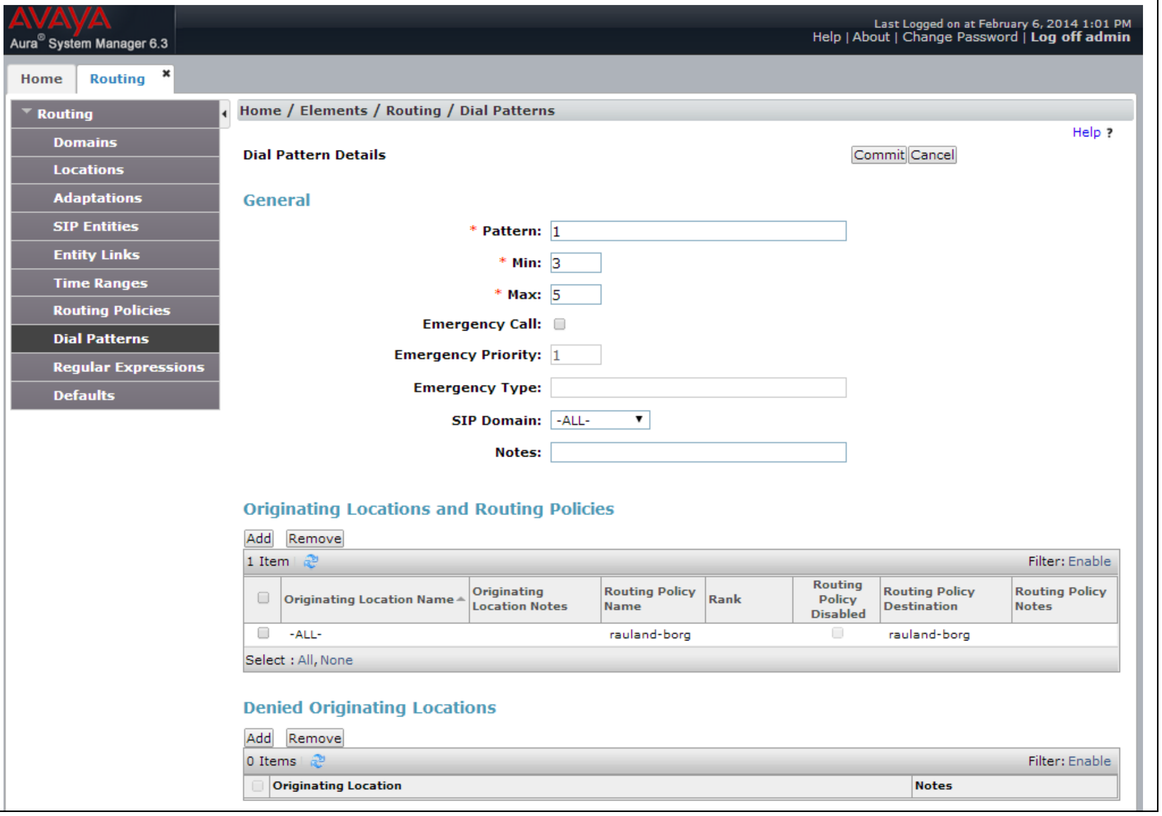
7. **Create a Dial Pattern**

To create a Dial Pattern, navigate to **Routing → Dial Patterns** and select **New** (not shown).

Enter the following:

- **Pattern:** ***1*** – the leading digits to match on the To header for SIP messages.
- **Min and Max**: ***3*** – The number of digits in the dialed number to match.
- **SIP Domain**: ***All*** – The SIP Domain can be used to implement domain based routing rules, this option was not used in the compliance test.
- **Originating Locations and Routing Policies:** See the next page for details of this step.

Click on the **Commit** button to save the entries after the step on the following page is completed.



Dial Pattern Details

General

* Pattern:	1
* Min:	3
* Max:	5
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		rauland-borg		□	rauland-borg	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Filter: Enable

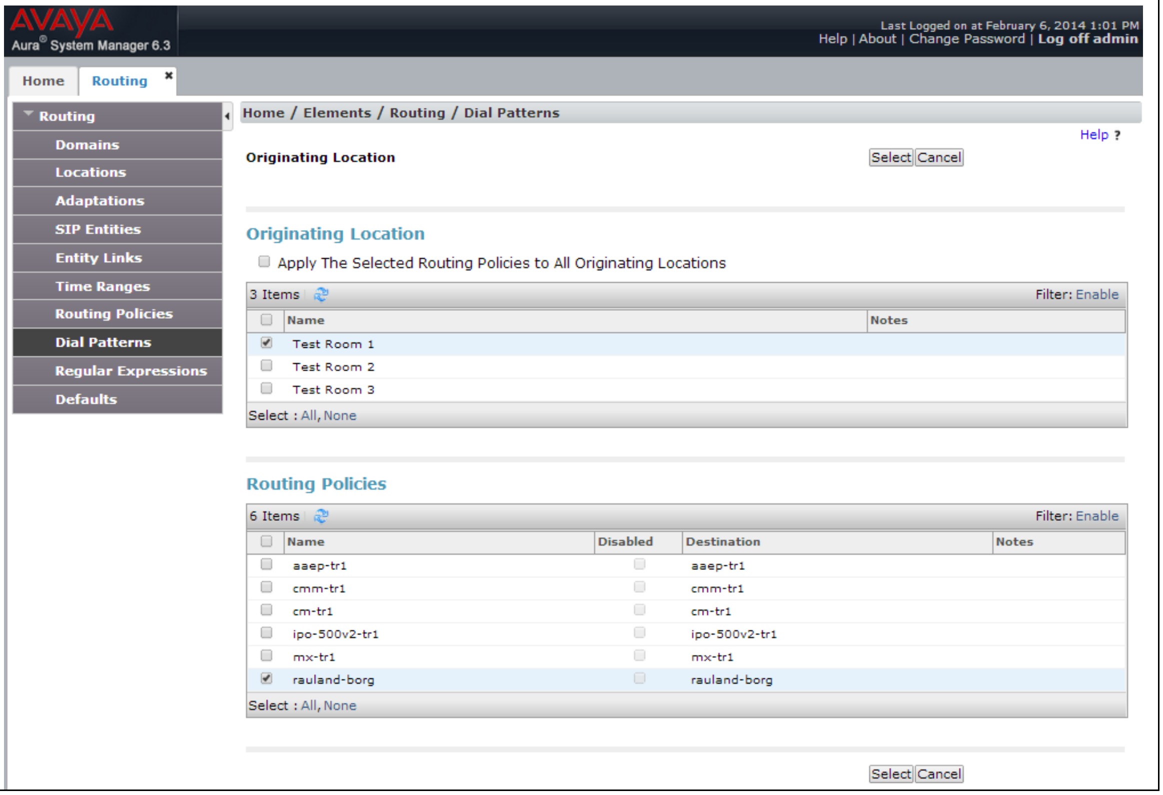
□	Originating Location	Notes

Create a Dial Pattern (Continued)

When the **Add** button is clicked on the **Originating Locations and Routing Policies** section for the **Dial Pattern Detail** page, the following will appear.

The **Originating Location** can be defined as any location that originates a SIP request. In the compliance test, location based routing was not used so the **Apply The Selected Routing Policies to All Originating Locations** option was selected.

The ***raland-borg*** policy defined is Step 4 was selected in the **Routing Policies** section. Click the **Save** button (not shown) to save these changes and return to the **Dial Pattern Details** page.



Originating Location

Originating Location

□ Apply The Selected Routing Policies to All Originating Locations

3 Items — Filter: Enable

□	Name	Notes
☑	Test Room 1	
□	Test Room 2	
□	Test Room 3	

Select : All, None

Routing Policies

6 Items — Filter: Enable

□	Name	Disabled	Destination	Notes
□	aaep-tr1	□	aaep-tr1	
□	cmm-tr1	□	cmm-tr1	
□	cm-tr1	□	cm-tr1	
□	ipo-500v2-tr1	□	ipo-500v2-tr1	
□	mx-tr1	□	mx-tr1	
☑	rauland-borg	□	rauland-borg	

Select : All, None

7. Configure Responder® 5

The Responder solution is typically implemented by Rauland resale partners. When integrated with a third party SIP PBX, it is always deployed with a Brekeke SIP server which serves two purposes. First, Brekeke 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 Brekeke SIP Server is capable of providing 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 resale partners based on site requirements, and will be configured to use the Brekeke 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 Brekeke SIP Server to properly route SIP calls and RTP.

7.1. Responder 5 Configuration Details

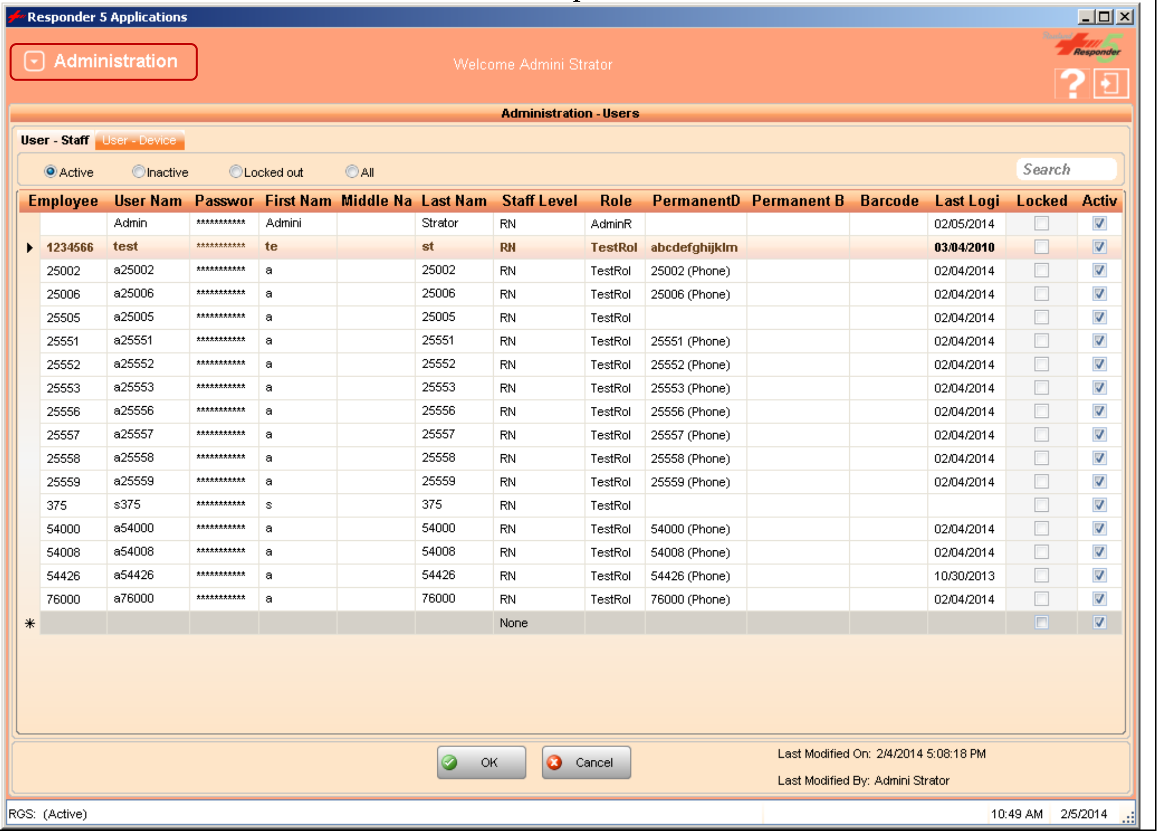
Step	Description
1.	**Configure Endpoints**

Typically, hospital staff use wireless phones to enable instant communications with staff and patient rooms. In the tested confirmation, a variety of IP and SIP wireless devices which were previously configured on Communication Manager and Session 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 a number of devices used in the test environment, extensions ***25xxx*** were IP and SIP devices administered on Communication Manager and Session Manager.

Click **OK** at the bottom of the screen to complete edits on this screen.



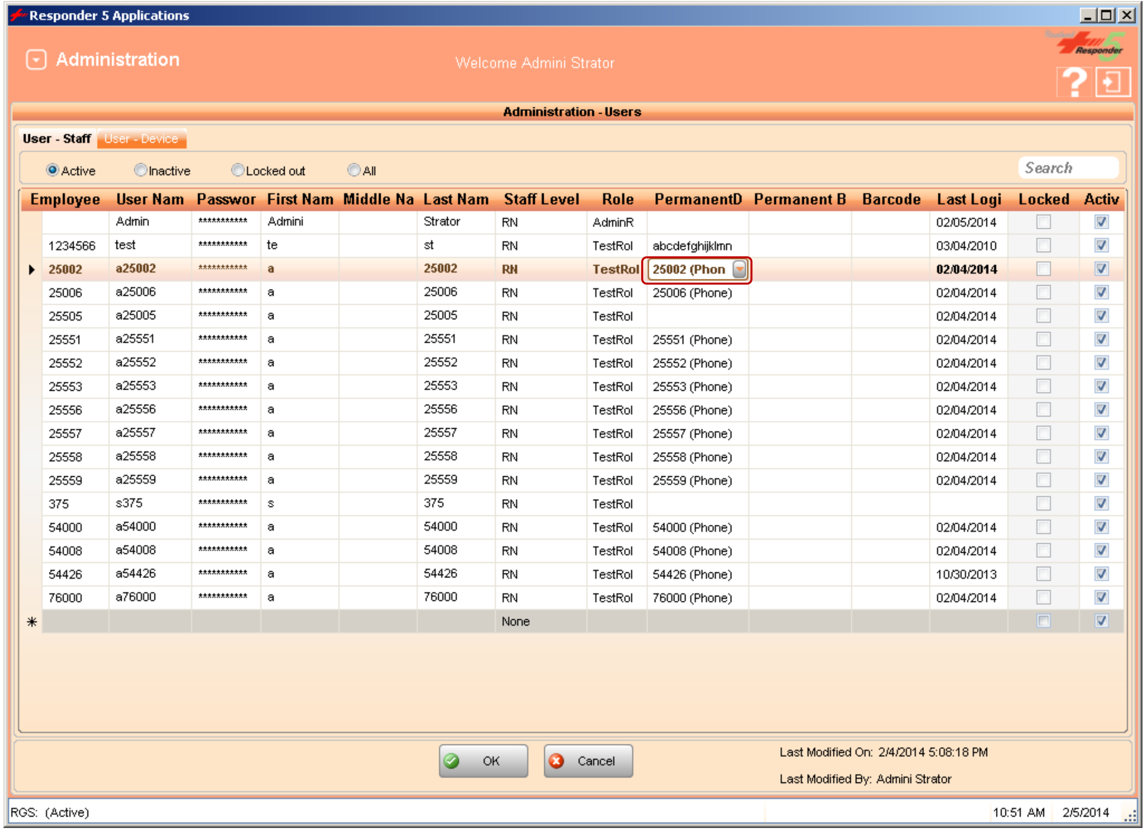
● Active ○ Inactive ○ Locked out ○ All

	Employee	User Nam	Passwor	First Nam	Middle Na	Last Nam	Staff Level	Role	PermanentD	Permanent B	Barcode	Last Logi	Locked	Activ
		Admin	***********	Admini		Strator	RN	AdminR				02/05/2014	☐	☑
▶	1234566	test	***********	te		st	RN	TestRol	abcdefghijklm			03/04/2010	☐	☑
	25002	a25002	***********	a		25002	RN	TestRol	25002 (Phone)			02/04/2014	☐	☑
	25006	a25006	***********	a		25006	RN	TestRol	25006 (Phone)			02/04/2014	☐	☑
	25505	a25005	***********	a		25005	RN	TestRol				02/04/2014	☐	☑
	25551	a25551	***********	a		25551	RN	TestRol	25551 (Phone)			02/04/2014	☐	☑
	25552	a25552	***********	a		25552	RN	TestRol	25552 (Phone)			02/04/2014	☐	☑
	25553	a25553	***********	a		25553	RN	TestRol	25553 (Phone)			02/04/2014	☐	☑
	25556	a25556	***********	a		25556	RN	TestRol	25556 (Phone)			02/04/2014	☐	☑
	25557	a25557	***********	a		25557	RN	TestRol	25557 (Phone)			02/04/2014	☐	☑
	25558	a25558	***********	a		25558	RN	TestRol	25558 (Phone)			02/04/2014	☐	☑
	25559	a25559	***********	a		25559	RN	TestRol	25559 (Phone)			02/04/2014	☐	☑
	375	s375	***********	s		375	RN	TestRol					☐	☑
	54000	a54000	***********	a		54000	RN	TestRol	54000 (Phone)			02/04/2014	☐	☑
	54008	a54008	***********	a		54008	RN	TestRol	54008 (Phone)			02/04/2014	☐	☑
	54426	a54426	***********	a		54426	RN	TestRol	54426 (Phone)			10/30/2013	☐	☑
	76000	a76000	***********	a		76000	RN	TestRol	76000 (Phone)			02/04/2014	☐	☑
✳							None						☐	☑

Last Modified On: 2/4/2014 5:08:18 PM

Last Modified By: Admini Strator

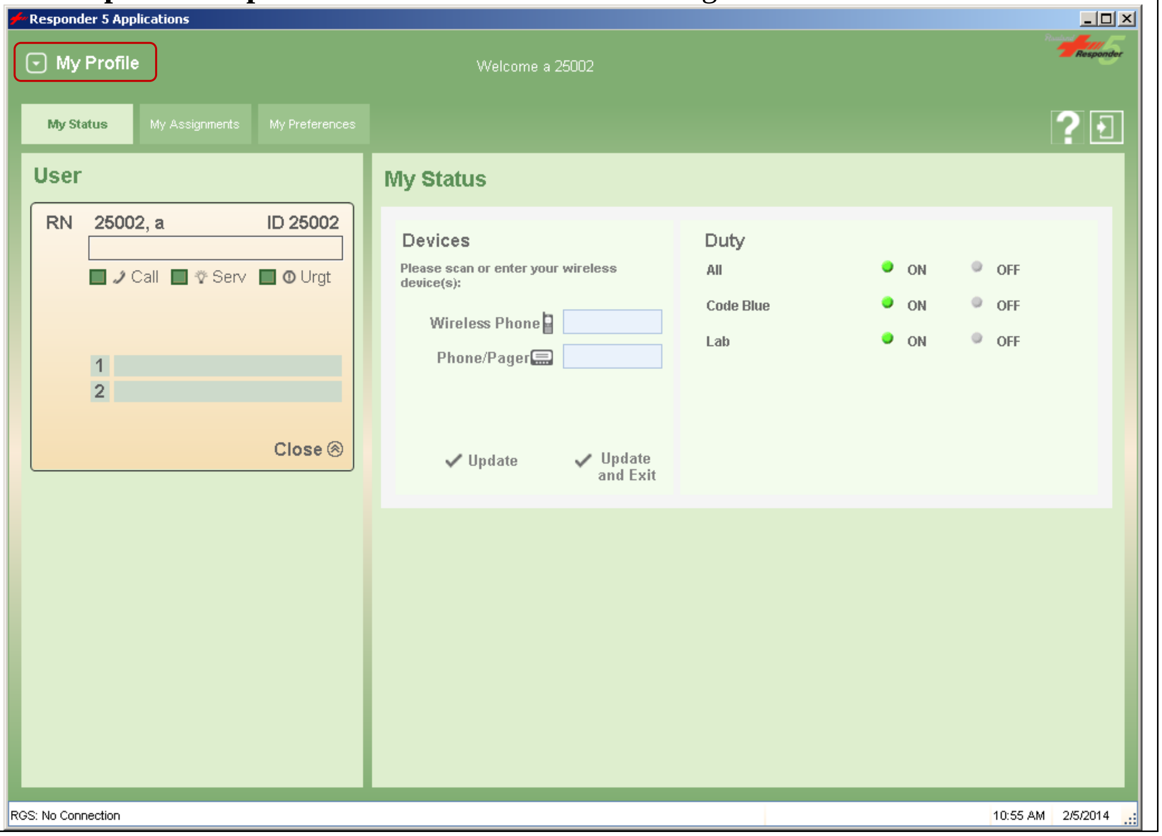
RGS: (Active) 10:49 AM 2/5/2014

Step	Description
2.	**Assign Endpoints to Users** 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 are able to enter the device they are using for a shift when they login as described in **Step 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 – General** tab as shown below. In the illustration below, devices were selected from a list of phones (from the list in **Step 1** above) in the **PermanentDevice** column for each user. Click **OK** to complete edits on this screen. 

	Employee	User Nam	Passwor	First Nam	Middle Na	Last Nam	Staff Level	Role	PermanentD	Permanent B	Barcode	Last Logi	Locked	Activ
		Admin	***********	Admini		Strator	RN	AdminR				02/05/2014	□	☑
	1234566	test	***********	te		st	RN	TestRol	abcdefghijklmn			03/04/2010	□	☑
▶	25002	a25002	***********	a		25002	RN	TestRol	25002 (Phon			02/04/2014	□	☑
	25006	a25006	***********	a		25006	RN	TestRol	25006 (Phone)			02/04/2014	□	☑
	25505	a25005	***********	a		25005	RN	TestRol				02/04/2014	□	☑
	25551	a25551	***********	a		25551	RN	TestRol	25551 (Phone)			02/04/2014	□	☑
	25552	a25552	***********	a		25552	RN	TestRol	25552 (Phone)			02/04/2014	□	☑
	25553	a25553	***********	a		25553	RN	TestRol	25553 (Phone)			02/04/2014	□	☑
	25556	a25556	***********	a		25556	RN	TestRol	25556 (Phone)			02/04/2014	□	☑
	25557	a25557	***********	a		25557	RN	TestRol	25557 (Phone)			02/04/2014	□	☑
	25558	a25558	***********	a		25558	RN	TestRol	25558 (Phone)			02/04/2014	□	☑
	25559	a25559	***********	a		25559	RN	TestRol	25559 (Phone)			02/04/2014	□	☑
	375	s375	***********	s		375	RN	TestRol					□	☑
	54000	a54000	***********	a		54000	RN	TestRol	54000 (Phone)			02/04/2014	□	☑
	54008	a54008	***********	a		54008	RN	TestRol	54008 (Phone)			02/04/2014	□	☑
	54426	a54426	***********	a		54426	RN	TestRol	54426 (Phone)			10/30/2013	□	☑
	76000	a76000	***********	a		76000	RN	TestRol	76000 (Phone)			02/04/2014	□	☑
✳							None						□	☑

Last Modified On: 2/4/2014 5:08:18 PM
Last Modified By: Admini Strator

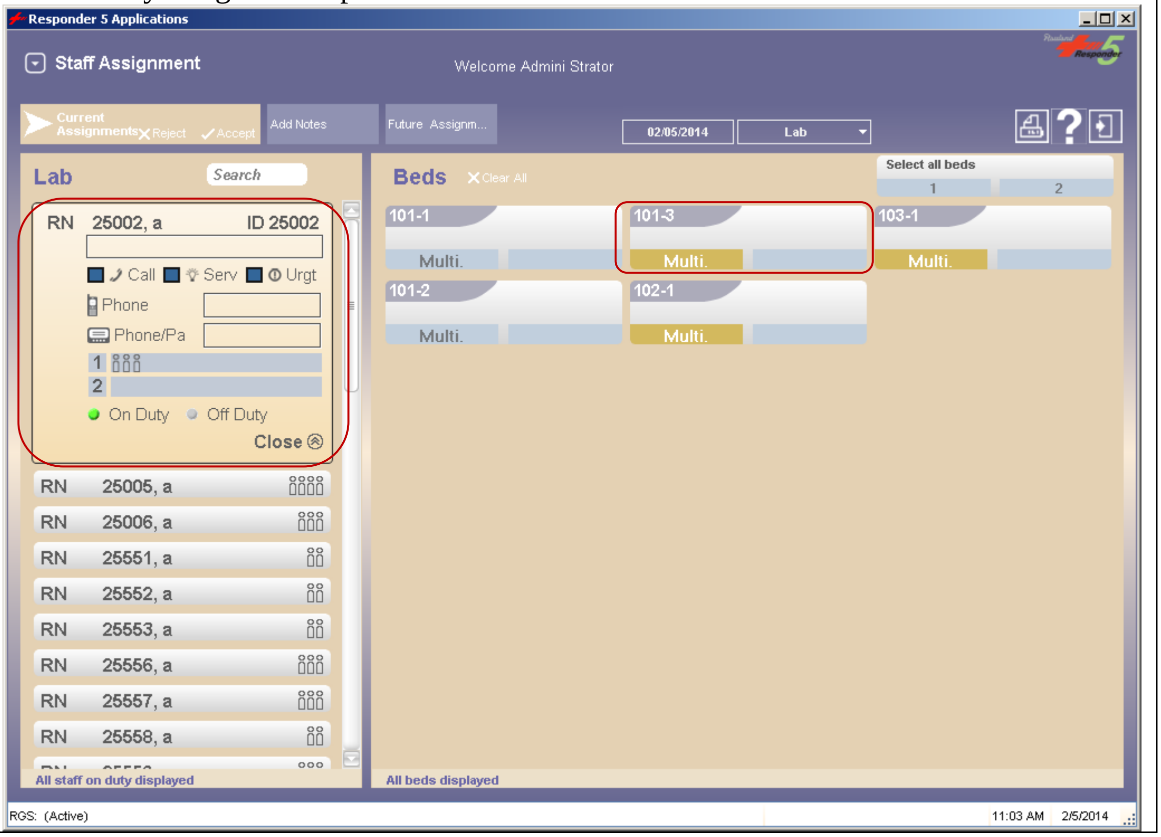
RGS: (Active) 10:51 AM 2/5/2014

Step	Description
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** to commit the changes.  Responder 5 Applications My Profile Welcome a 25002 My Status · My Assignments · My Preferences User RN 25002, a ID 25002 🟩 Call 🟩 Serv 🟩 Urgt 1 2 Close My Status Devices Please scan or enter your wireless device(s): Wireless Phone Phone/Pager ✓ Update ✓ Update and Exit Duty All ● ON ○ OFF Code Blue ● ON ○ OFF Lab ● ON ○ OFF RGS: No Connection 10:55 AM 2/5/2014

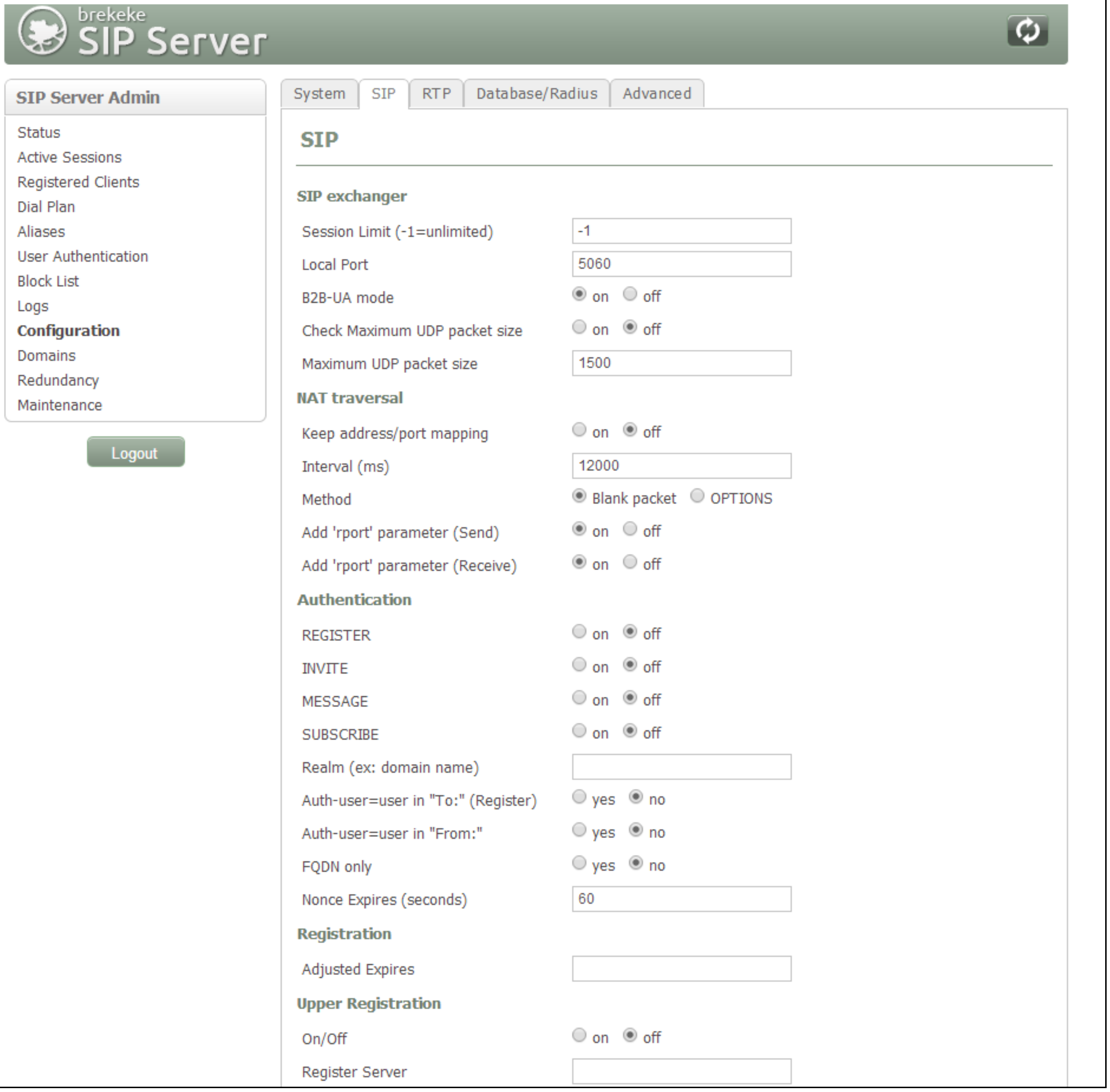
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>

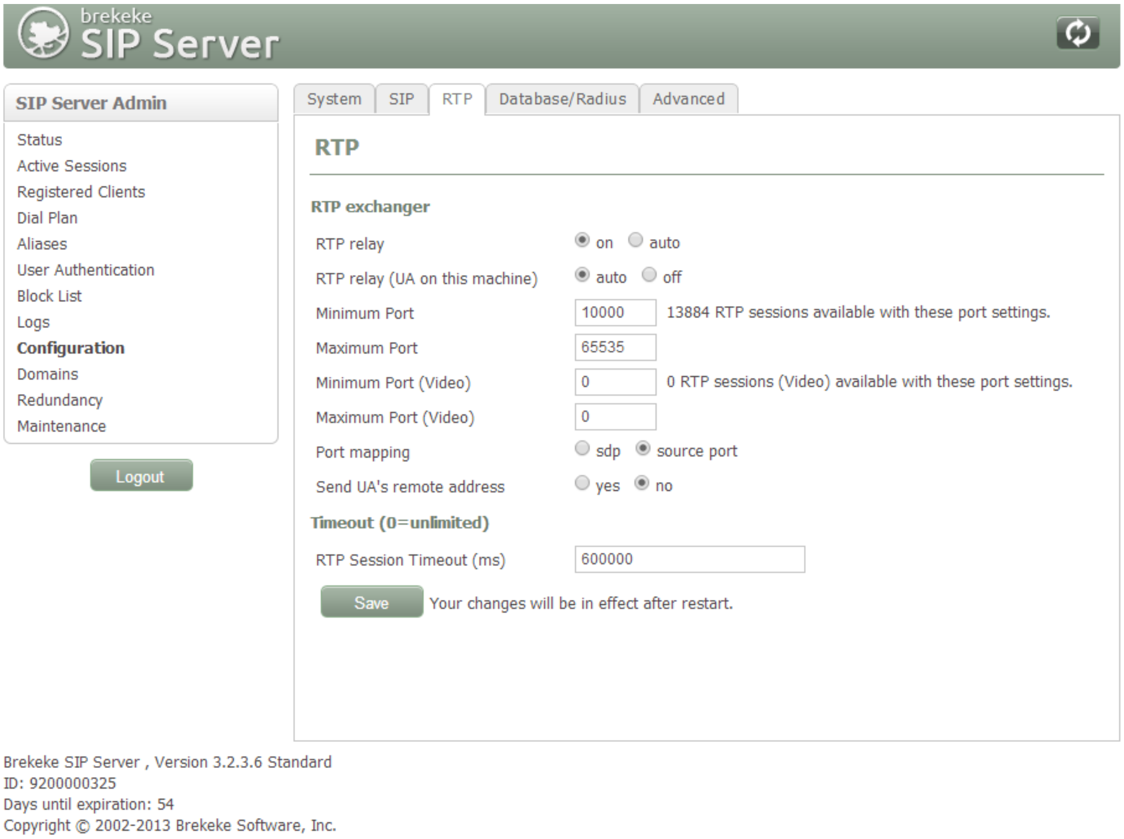
Assign Staff to Patient Rooms

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, ***25002*** is assigned to room **101-3, 103-1** and **102-1** by clicking on the Staff name in the left column, then clicking on the assignment space below the patient name. The staff members initials (***GA*** in this case) will appear as below when the staff member has been successfully assigned to a patient.



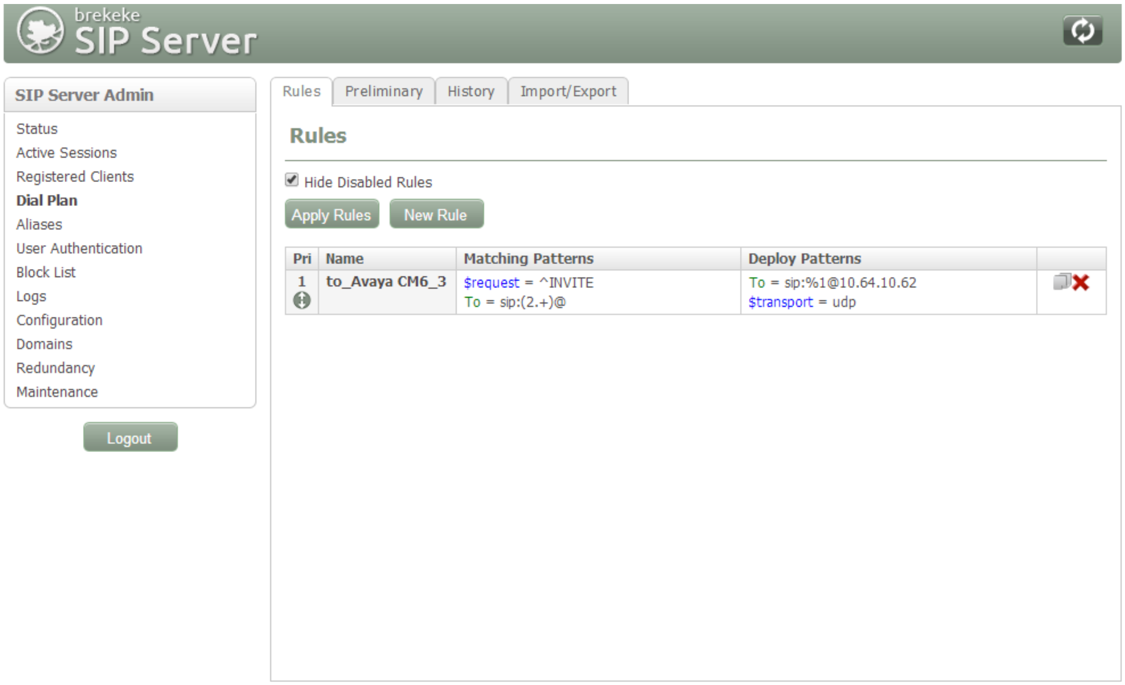
</td></tr>
</table>

Step	Description
5.	**Configure Brekeke SIP Server SIP Properties** The following SIP settings were pre-configured for the test environment. All administration is performed via web browser by navigating to the hostname or IP Address of the Brekeke server. Ensure that **B2B-UA mode** is set to ***on***.  brekeke SIP Server SIP Server Admin Status Active Sessions Registered Clients Dial Plan Aliases User Authentication Block List Logs Configuration Domains Redundancy Maintenance Logout System SIP RTP Database/Radius Advanced SIP SIP exchanger Session Limit (-1=unlimited): -1 Local Port: 5060 B2B-UA mode: ● on ○ off Check Maximum UDP packet size: ○ on ● off Maximum UDP packet size: 1500 NAT traversal Keep address/port mapping: ○ on ● off Interval (ms): 12000 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 FQDN only: ○ yes ● no Nonce Expires (seconds): 60 Registration Adjusted Expires: Upper Registration On/Off: ○ on ● off Register Server:

Step	Description
6.	**Configure RTP Relay settings** The tested configuration required that all media (RTP) send to and from Rauland endpoints be connected through the Brekeke SIP Server. This was required in order to overcome an incompatibility between the Rauland and Avaya media servers as described in **Section 2**. On the **Configuration → RTP** screen, set **RTP Relay** to ***on***, **RTP relay (UA on this machine)** to ***auto***, **Port mapping** to ***source port*** 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.  brekeke SIP Server SIP Server Admin Status Active Sessions Registered Clients Dial Plan Aliases User Authentication Block List Logs Configuration Domains Redundancy Maintenance Logout System SIP RTP Database/Radius Advanced RTP RTP exchanger RTP relay ● on ○ auto RTP relay (UA on this machine) ● auto ○ off Minimum Port 10000 13884 RTP sessions available with these port settings. Maximum Port 65535 Minimum Port (Video) 0 0 RTP sessions (Video) available with these port settings. Maximum Port (Video) 0 Port mapping ○ sdp ● source port Send UA's remote address ○ yes ● no Timeout (0=unlimited) RTP Session Timeout (ms) 600000 Save Your changes will be in effect after restart. Brekeke SIP Server , Version 3.2.3.6 Standard ID: 9200000325 Days until expiration: 54 Copyright © 2002-2013 Brekeke Software, Inc.

Step	Description
7.	**Configure Dial Plan Routing rules**

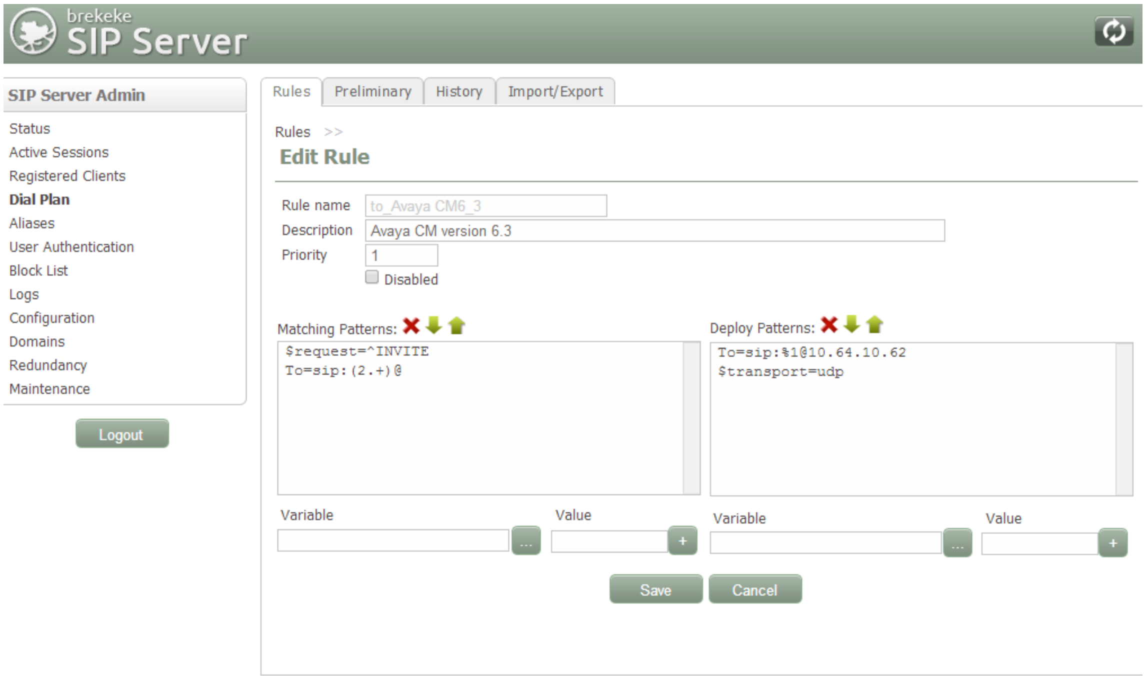
Dial Plan rules that was used is illustrated below. For calls routing to Session Manager, the **to_Avaya CM6_3** rule was used.



☑ Hide Disabled Rules

Pri	Name	Matching Patterns	Deploy Patterns
1	to_Avaya CM6_3	$request = ^INVITE To = sip:(2.+)@	To = sip:%1@10.64.10.62 $transport = udp

Click **Save** to commit the changes on this screen.



Rule name: to_Avaya CM6_3
Description: Avaya CM version 6.3
Priority: 1
□ Disabled

Matching Patterns:

```
$request=^INVITE
To=sip:(2.+)@
```

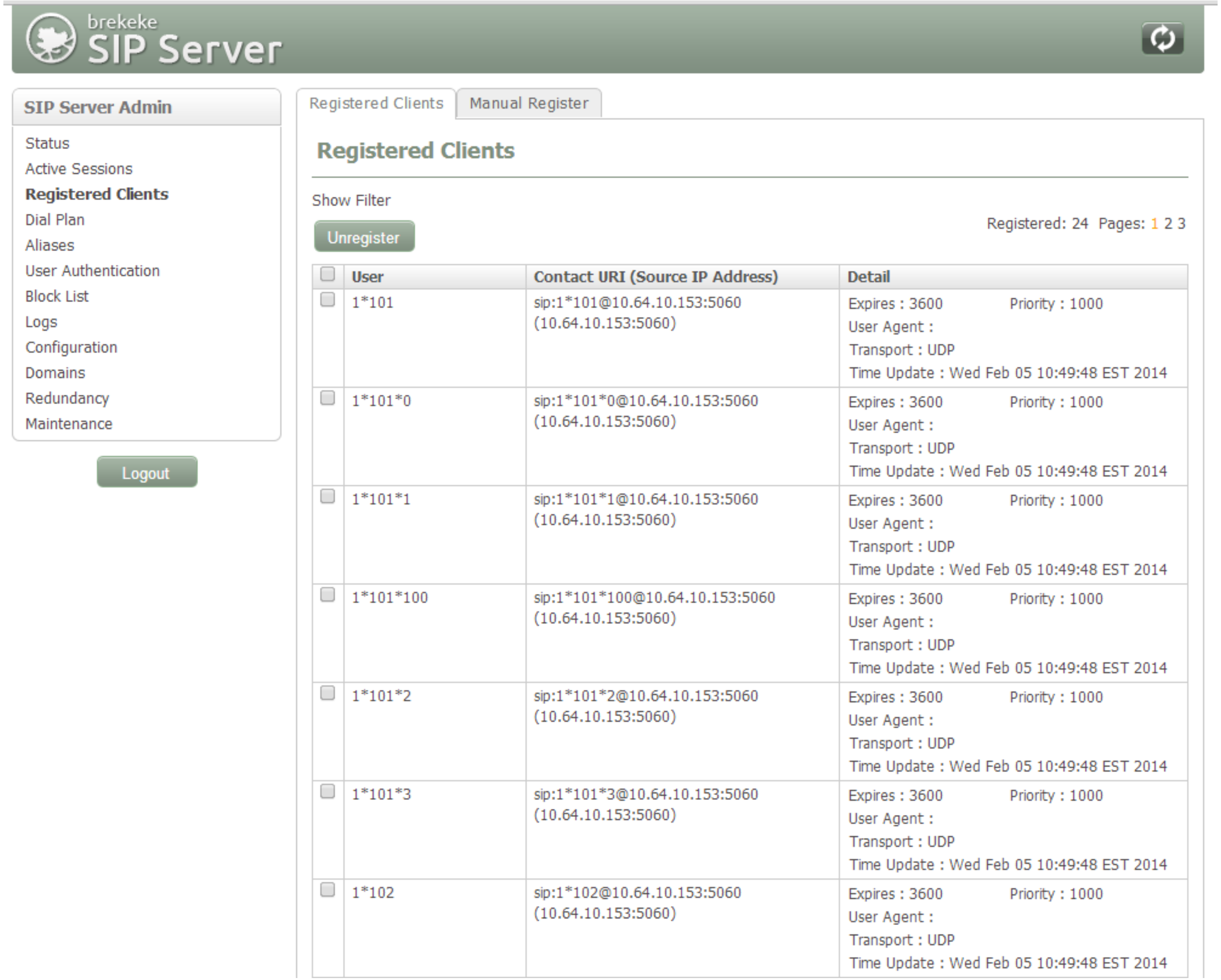
Deploy Patterns:

```
To=sip:%1@10.64.10.62
$transport=udp
```

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 transfer and conference are not supported on the patient room devices, but Avaya endpoints were tested to confirm conference and transfer functionality.

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



Registered Clients

Registered: 24 Pages: 1 2 3

☐	User	Contact URI (Source IP Address)	Detail
☐	1*101	sip:1*101@10.64.10.153:5060 (10.64.10.153:5060)	Expires : 3600 Priority : 1000 User Agent : Transport : UDP Time Update : Wed Feb 05 10:49:48 EST 2014
☐	1*101*0	sip:1*101*0@10.64.10.153:5060 (10.64.10.153:5060)	Expires : 3600 Priority : 1000 User Agent : Transport : UDP Time Update : Wed Feb 05 10:49:48 EST 2014
☐	1*101*1	sip:1*101*1@10.64.10.153:5060 (10.64.10.153:5060)	Expires : 3600 Priority : 1000 User Agent : Transport : UDP Time Update : Wed Feb 05 10:49:48 EST 2014
☐	1*101*100	sip:1*101*100@10.64.10.153:5060 (10.64.10.153:5060)	Expires : 3600 Priority : 1000 User Agent : Transport : UDP Time Update : Wed Feb 05 10:49:48 EST 2014
☐	1*101*2	sip:1*101*2@10.64.10.153:5060 (10.64.10.153:5060)	Expires : 3600 Priority : 1000 User Agent : Transport : UDP Time Update : Wed Feb 05 10:49:48 EST 2014
☐	1*101*3	sip:1*101*3@10.64.10.153:5060 (10.64.10.153:5060)	Expires : 3600 Priority : 1000 User Agent : Transport : UDP Time Update : Wed Feb 05 10:49:48 EST 2014
☐	1*102	sip:1*102@10.64.10.153:5060 (10.64.10.153:5060)	Expires : 3600 Priority : 1000 User Agent : Transport : UDP Time Update : Wed Feb 05 10:49:48 EST 2014

9. Conclusion

These Application Notes describe the procedures required to configure Rauland-Borg Responder® 5 to interoperate with endpoints registered to Avaya Aura® Session Manager and Avaya Aura® Communication Manager using a Brekeke SIP Server as a SIP registrar and Proxy for the Responder 5 side of the solution.

Caution is advised to pay particular attention to the observations noted in **Section 2** above when planning to implement this solution.

10. Additional References

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

Avaya

[1] *Administering Avaya Aura® Communication Manager*, Release 6.3, Document 03-300509, Issue 9, October 2013

[2] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 3, October 2013

[3] *Application Notes for Configuring Rauland-Borg Responder® 5 to Interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager R6.0.1*

Rauland-Borg

Product information for Rauland-Borg 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.