Avaya Solution & Interoperability Test Lab

Application Notes for Movitas MvPBX and Movitas Mobile SIP Apps with Avaya Aura® Session Manager and Avaya Aura® Communication Manager – 1.0

Abstract

These Application Notes describe configuration steps required for Movitas MvPBX and Movitas Mobile SIP Apps with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

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

The objective of this compliance test was to validate the interoperability of Avaya Aura® Session Manager and Avaya Aura® Communication Manger with Movitas MvPBX system and its respective iPhone, Android and Blackberry SIP apps. The testing included multiple call scenarios including calls between Avaya Endpoints (desk phones), Movitas SIP apps users and calls to PSTN lines via Avaya Aura® Communication Manager and Avaya Aura Session Manager®. Primary objective of this test was to test Avaya Aura® Communication Manager's Extension to Cellular (EC500) that route calls to Movitas SIP apps and Avaya Endpoints simultaneously.

2. General Test Approach and Test Results

The general test approach was to verify that calls are routed to/from Avaya Aura® Communication Manager and Avaya Aura® Session Manager to Movitas SIP apps via Movitas MvPBX. Avaya Aura® Communication Manager's Extension to Cellular (EC500) feature was used to send calls to two simultaneous phones at the same time. EC500 feature provides the ability to route calls to an Avaya Extension and a non-Avaya phone, at the same time. During interoperability testing, calls were routed to an Avaya extension and a SIP phone using EC500.

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.

2.1. Interoperability Compliance Testing

During the compliance there were 4 extensions associated with Avaya Aura® Communication Manager and Avaya Aura® Session Manager; Front Desk, Room 1, Room 2, Room 3; Room extensions were associated with 4 respective SIP Users in the Movitas MvPBX system. Avaya Endpoints included Avaya Analog Phone, Avaya Digital Phone, Avaya H.323 Phone and Avaya SIP Phone.

Movitas SIP User is a SIP application installed on a smart mobile devices; iPhone, Android and Blackberry. These SIP Users are registered to the Movitas MvPBX system. Any call that comes in to one of the three Avaya extensions will also ring their associated SIP User in the smart phone. The call can be accepted either at Avaya Endpoint or Movitas SIP User. Whichever phone answers the call, the other stops ringing and becomes idle.

The focus of this testing was to verify the SIP Trunk interoperability between Avaya Aura® Session Manager and Movitas MvPBX in placing multiple call scenarios between two systems. The following test areas were practiced in the compliance testing:

- SIP Trunk registration of Movitas MvPBX to Avaya Aura® Session Manager.
- Calls from PSTN to Avaya Extension and SIP User.

- Calls from SIP User to Avaya Extension.
- Calls from Avaya Extension to another Avaya Extension and a SIP User.
- Calls from SIP User to a PSTN Line.
- Calls from SIP User to another SIP User and Avaya Extensions
- SIP settings compatibility for codec support and packet size negotiation.

2.2. Test Results

All Test Cases Passed

2.3. Support

Technical support for Movitas can be obtained through the following:

- Phone: 888-343-3721
- Email: support@movitas.com

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya G430 Media Gateway
- Avaya IP (H.323 and SIP) Phones
- Avaya Digital Phones
- Avaya Analog Phones
- Movitas SIP PBX Server; MvPBX
- Movitas SIP Users

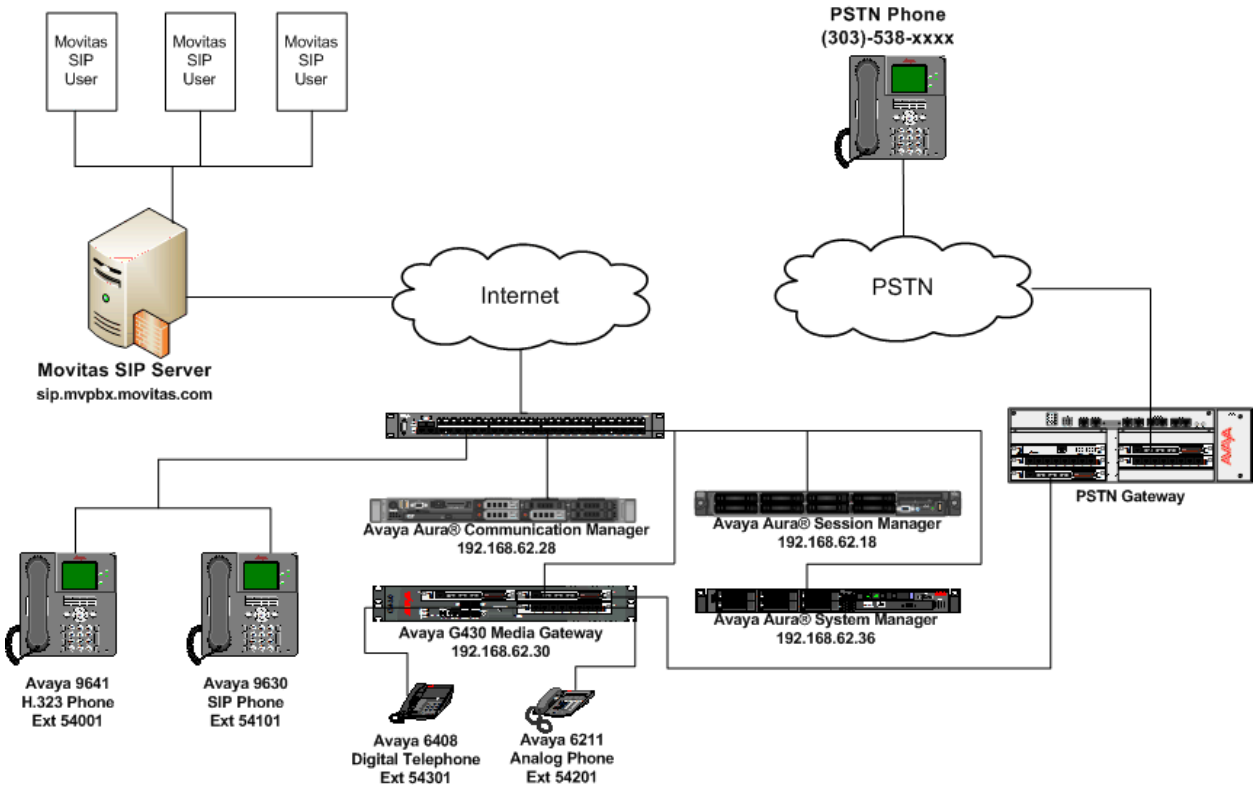


Figure 1 – Test Configuration

4. Equipment and Software Validated

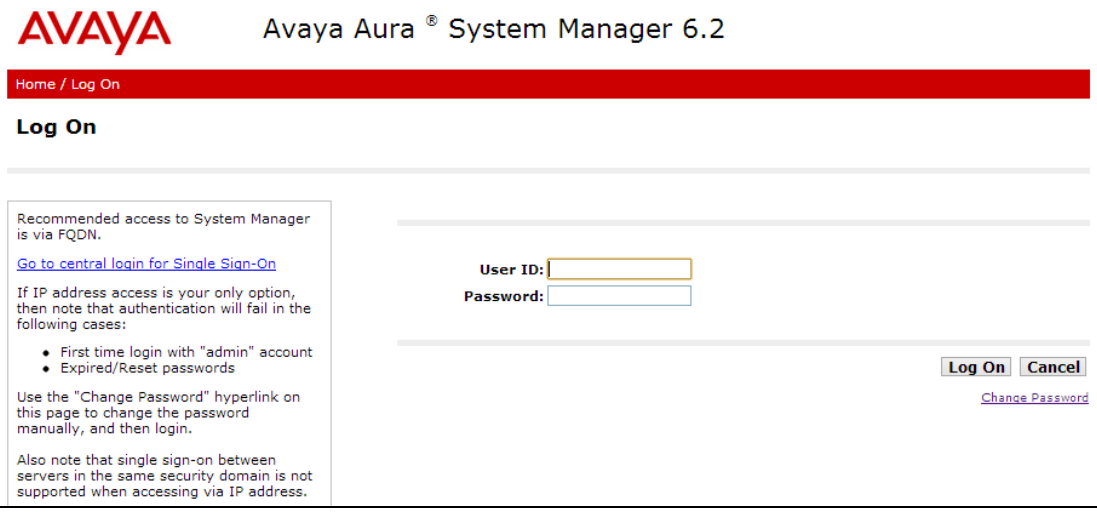
The following equipment and version were used in the reference configuration described above:

Equipment/Software	Release/Version	Description
Avaya Aura®Communication Manager	6.2 SP3	Runs Avaya Aura® Communication Manager call processing software.
Avaya G430 Media Gateway : MM710BP (DS1) MM712AP (DCP) MM711(AMM)	FW 31.20.1	Supports analog, DCP and IP phones.
Avaya Aura® Session Manager	6.2 SP3	SIP Routing Engine
Avaya Aura® System Manager	6.2	Administers Session Manager
Movitas MvPBX	ab6eb8c2 Rev 89984ed	Movitas PBX
Blackberry 9360 Movitas Phone	7.0 2.0.3	Runs Movitas Phone app
iPhone 4S MovitasPhone	5.1.1 2.0.3	Runs Movitas Phone app
Samsung Galaxy SII MovitasPhone	4.0.3 2.0.3	Runs Movitas Phone app

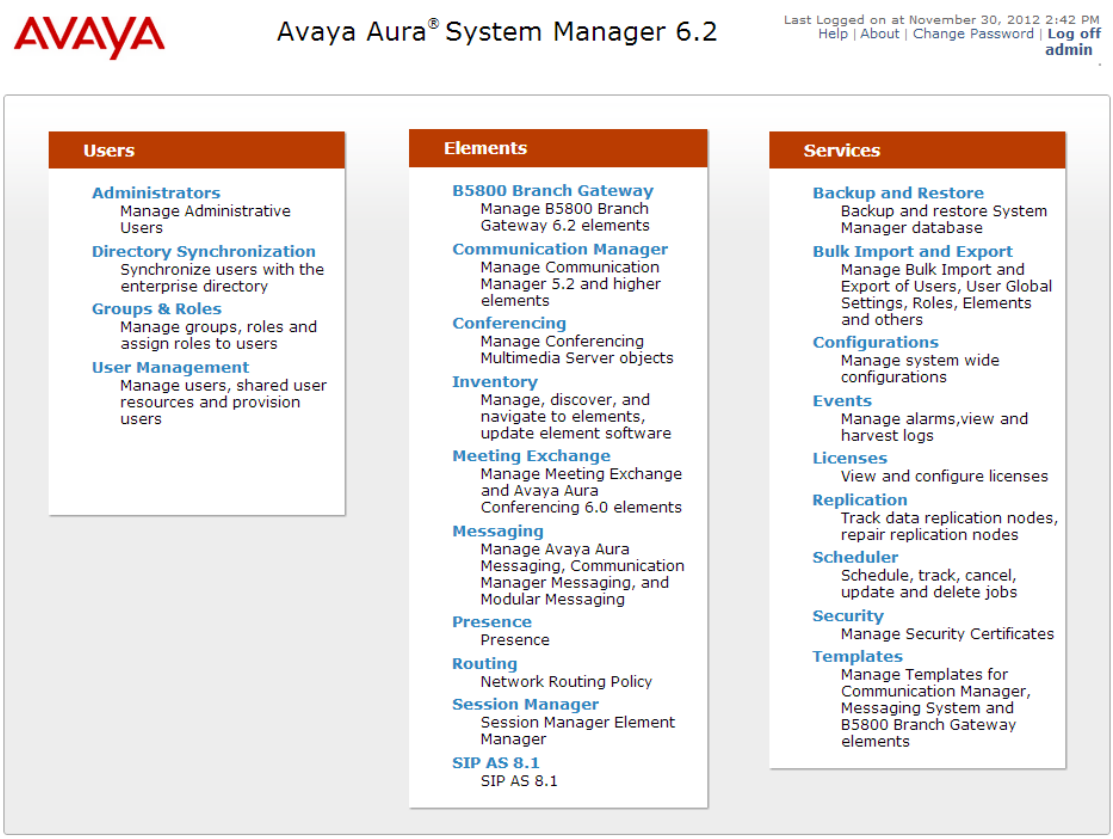
5. Configure Avaya Aura® Session Manager

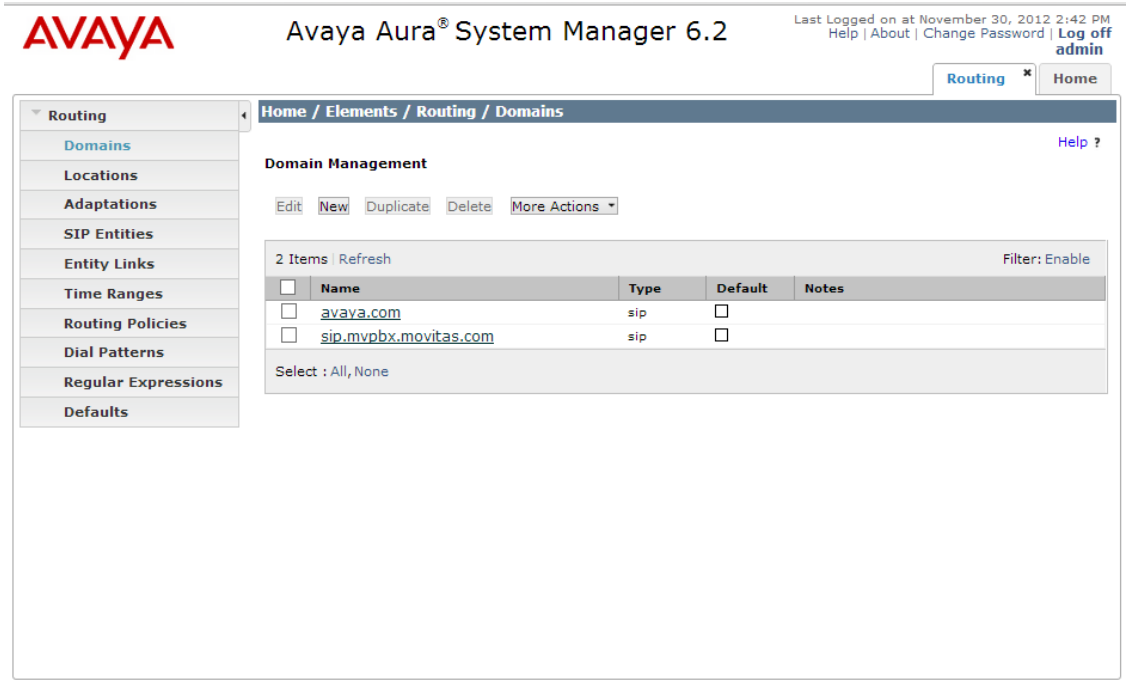
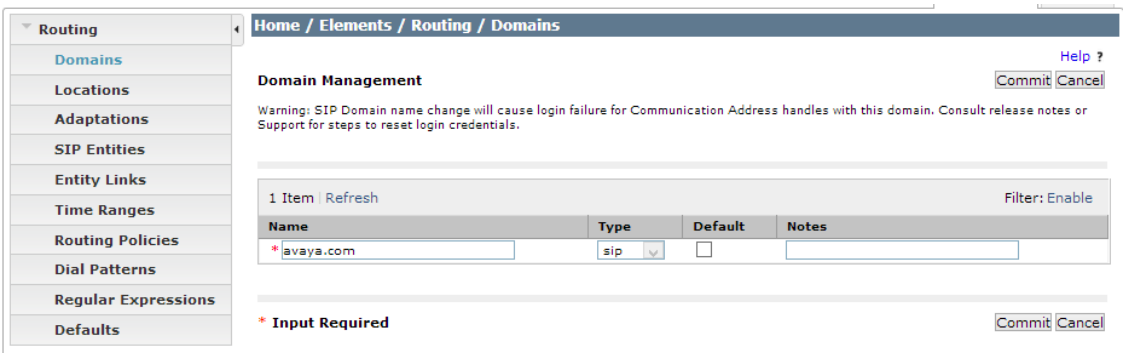
This section provides the steps for configuring Session Manager to communicate with Movitas MvPBX. For more details, see the administration guide.

5.1. Configuration details

Step	Description
1.	Avaya Aura® Session Manager is configured using browser access to Avaya Aura® System Manager. Enter the URL of System Manager **https://<hostname>/network-login/SMGR** where <hostname> is the ip address or qualified domain name of the System Manager. Log in using appropriate credentials. 

Step	Description
2.	The home page is a navigation screen as shown below. Each of these links will open a new tab within the webpage. Click on **Routing**.



Step	Description
3.	**Add a Domain** On the left pane, click on **Domains** • On the **Domains** page, click on **New**. 
4.	• For the **Name** field, type in a domain. • Set **Type** to **sip.** • **Commit** changes after done. For Compliance testing, avaya.com sip domain was used within Avaya environment. sip.mbpbx.movitas.com domain was used when routing calls to MvPBX. Repeat steps **3-4** to add another domain. 

Step	Description
5.	**Add a Location** On the left pane, click on **Locations**. • On the **Location** page, click on **New**. 

Step	Description
6.	• Enter the **Name** of the location • Under **Location Pattern** click on **Add** ○ Type in **IP Address Pattern** for the location • **Commit** changes after done. For Compliance testing the following information was used.

Location Details Commit Cancel

General

* **Name:** Public

Notes:

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

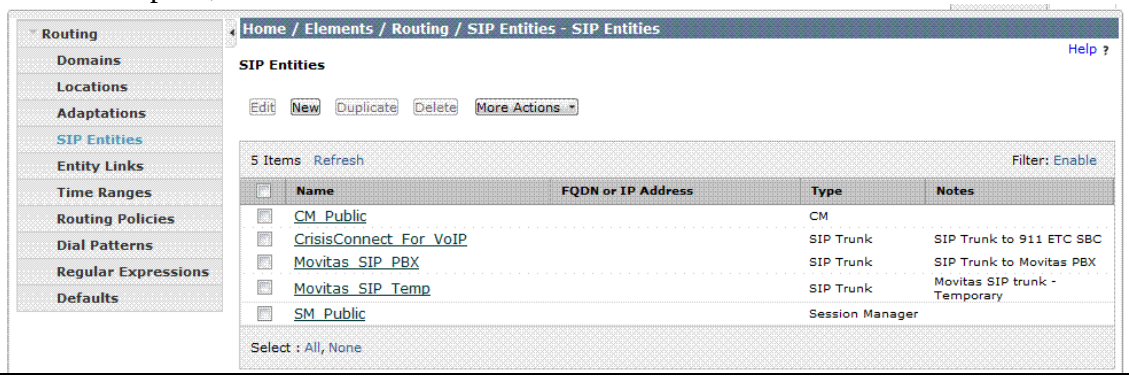
Add Remove

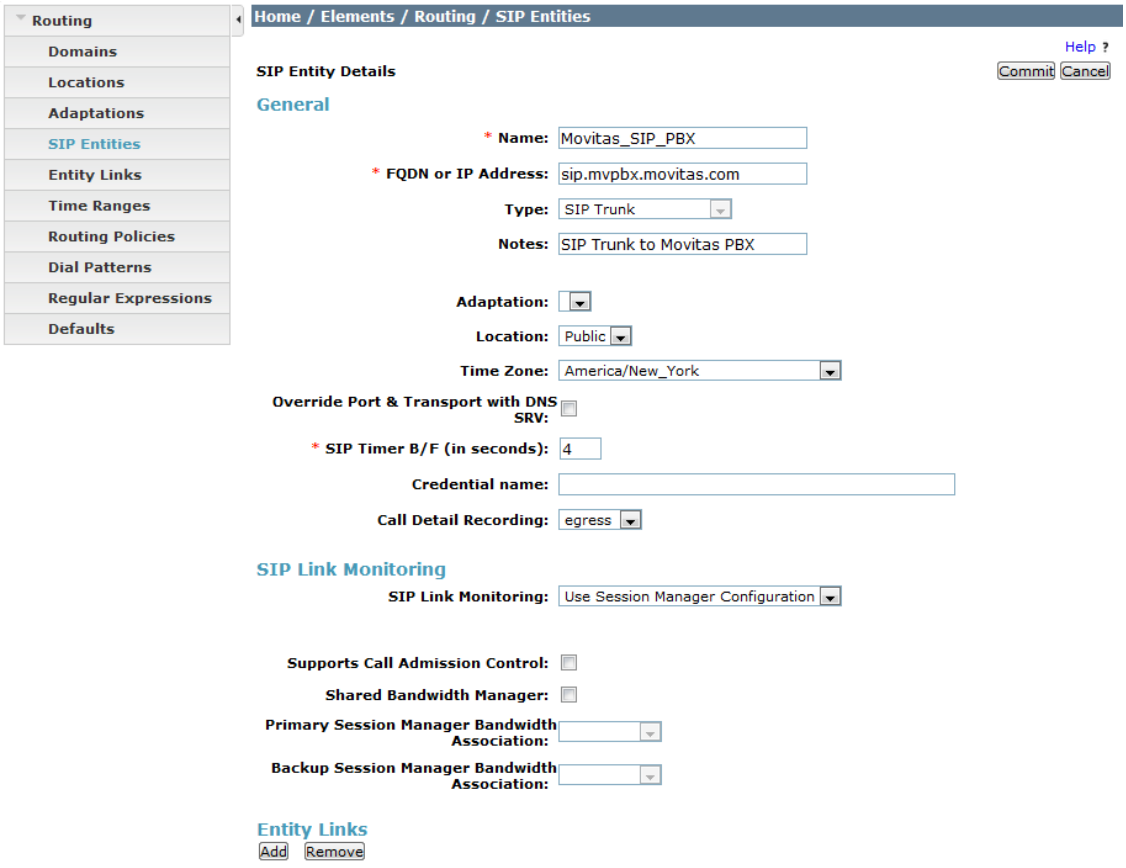
3 Items | Refresh Filter: Enable

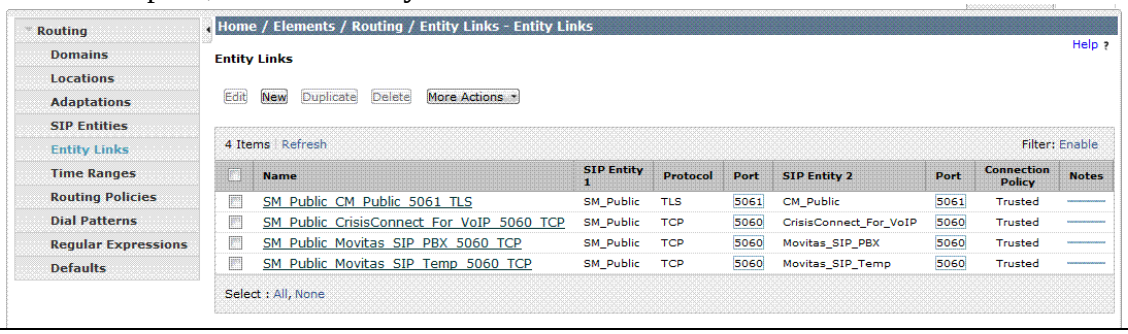
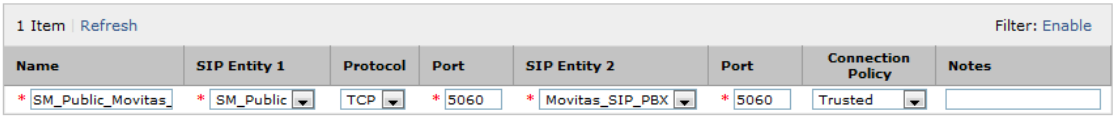
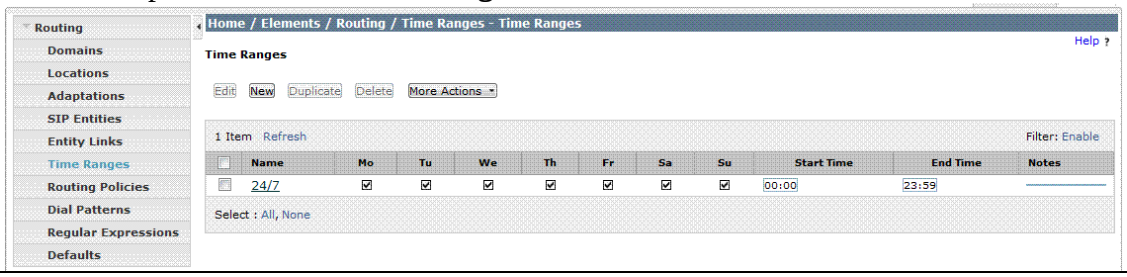
	IP Address Pattern	Notes
☐	* 192.168.62.*	
☐	*	
☐	*	

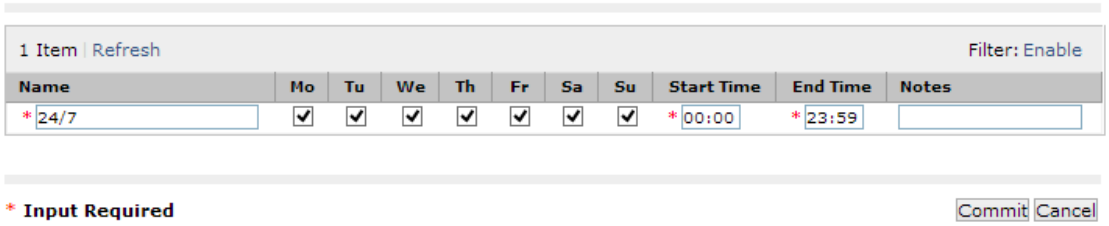
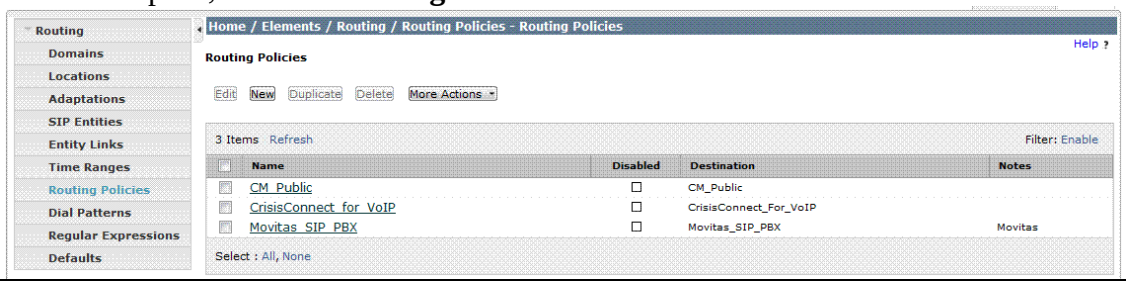
Select : All, None

* **Input Required** Commit Cancel

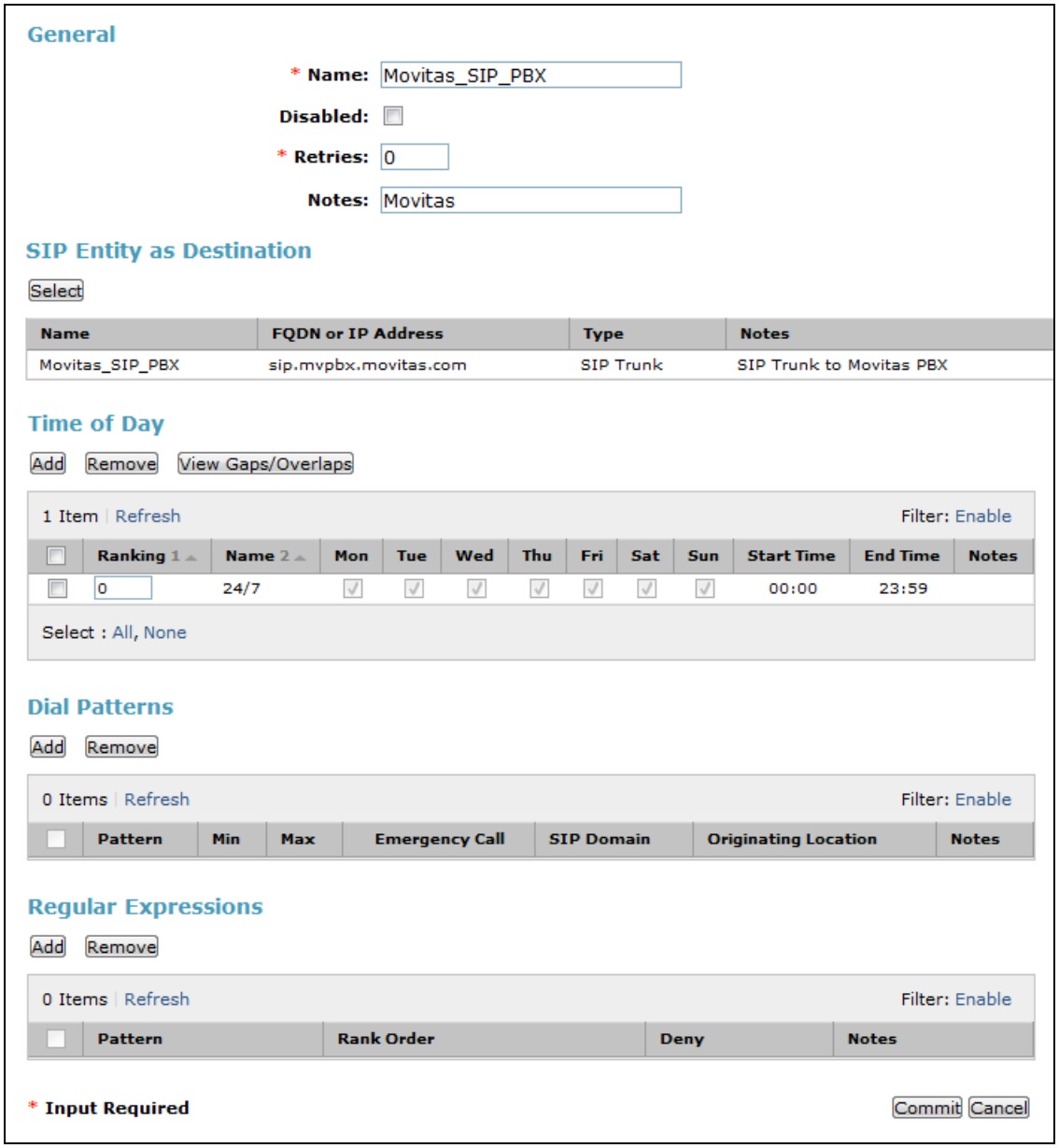
Step	Description
7.	On the left pane, click on **SIP Entities.** 

Step	Description
8.	**Add a SIP Entity** On the **SIP Entity** page, click on **New**. • Enter the **Name** and **FQDN or IP Address** • Set **Type** to **SIP Trunk** • Set **Location** to the location added in earlier in this section • Set **Time Zone** to desired time zone • **Commit** changes after done For Compliance testing the following information was used. Also, please note that SIP Entities for Avaya Aura® Communication Manager and Avaya Aura® Session Manager was also added for this configuration, but is not shown in this document. 

Step	Description
9.	On the left pane, click on **Entity Links** 
10.	**Add an Entity Link** On the **Entity Link** page, click on **New**. • Add a **Name.** • Set **SIP Entity 1** to SM_Public, which is SIP Entity name of Avaya Aura® Session Manager and was pre-configured . • Set the **Protocol Type** and type in **Port.** • Set **SIP Entity 2** as added in **Step 8** and set the **Port.** • Set the **Connection Policy** to be **Trusted.** • **Commit** changes after done. For Compliance testing the following information was used. 
11.	On the left pane, Click on **Time Ranges** 

Step	Description
12.	**Add a Time Range** On the Time Range page, click on **New.** • Type in the **Name** of the time range. • Select the Days and **Start Time** and **End Time** used for all days. • **Commit** changes after done. For Compliance testing the following information was used. 
13.	On the left pane, click on **Routing Policies** 

Step	Description
14.	On the **Routing Policy** page, click on **New** • Type in the **Name** for Routing Policy • Click on **Select** under **SIP Entity as a Destination**. ○ Select SIP Entity configured in **Step 10**. • Select a **Time Range** added in **Step 12**. • **Commit** changes after done. For Compliance testing the following information was used. Routing Policy for Communication Manager was pre-configured and is not shown in this document.



General

* **Name:** Movitas_SIP_PBX

Disabled:

* **Retries:** 0

Notes: Movitas

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Movitas_SIP_PBX	sip.mvpbx.movitas.com	SIP Trunk	SIP Trunk to Movitas PBX

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	

Select : All, None

Dial Patterns

Add Remove

0 Items | Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Regular Expressions

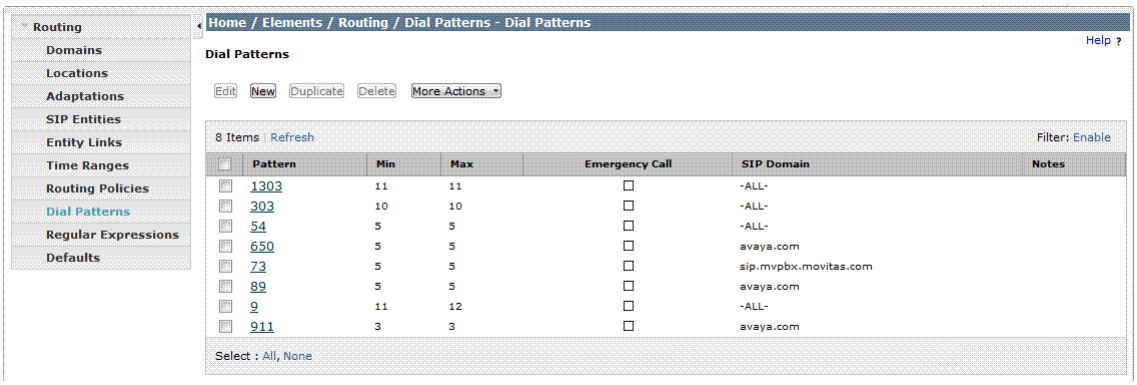
Add Remove

0 Items | Refresh Filter: Enable

Pattern	Rank Order	Deny	Notes

* **Input Required**

Commit Cancel

Step	Description
15.	On the left pane, click on **Dial Patterns** 

Step	Description

16.	On **Dial Patterns** page, click on **New**.
	For compliance testing the following pattern was used.
	All calls dialed with 5 digits and started with 7, routed to Movitas MvPBX.
	• Set **Pattern** to **7.**
	• Set **Min** and **Max to 5.**
	• Set **SIP Domain** to **–ALL-.**
	• Click on **Add** under **Originating Locations and Routing Policies,** screenshot not shown for this step.
	  ○ Select location configured in **Step 6.**
	  ○ Select Routing Policy configured in **Step 14.**
	  ○ Click on **Select** once done.
	• **Commit** changes after done
	Dial Pattern for Communication Manager was pre-configured and is not shown in this document.

Dial Pattern Details Commit Cancel

General

* **Pattern:** 7
* **Min:** 5
* **Max:** 5
Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: -ALL-
Notes:

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh Filter: Enable

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Public		Movitas-PBX	0	☐	Movitas-PBX	Movitas

Select : All, None

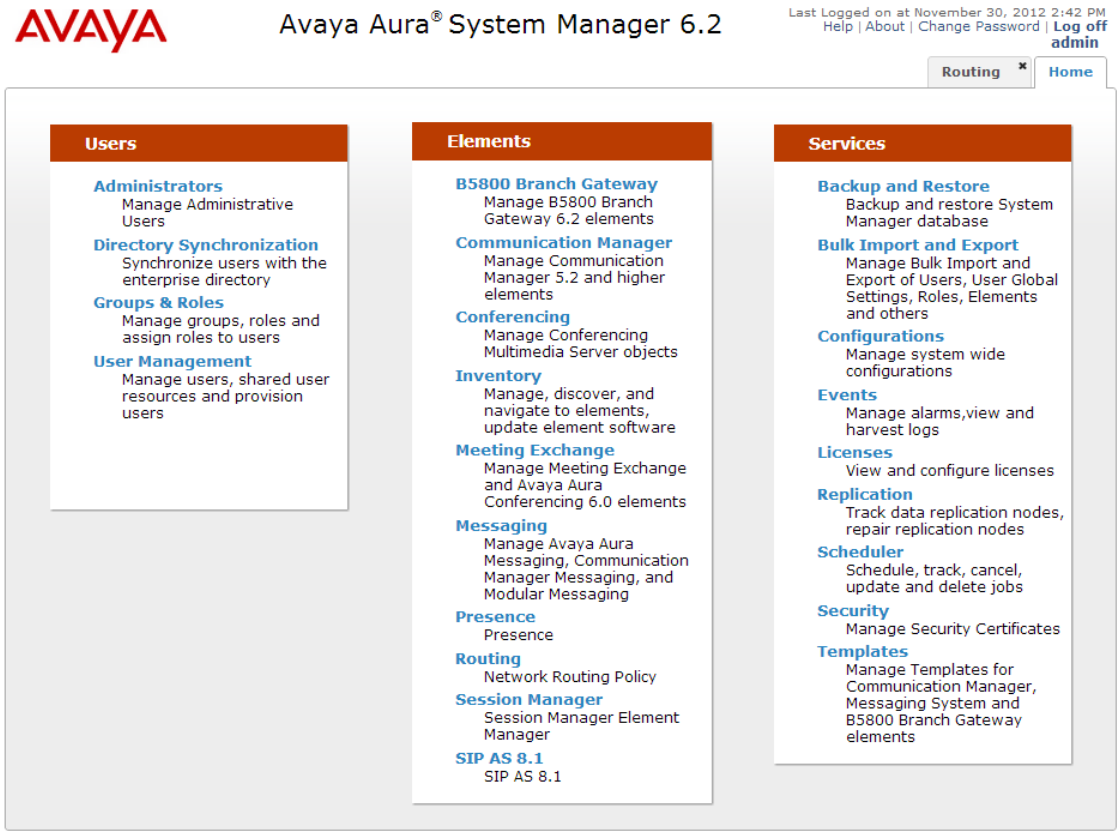
Denied Originating Locations

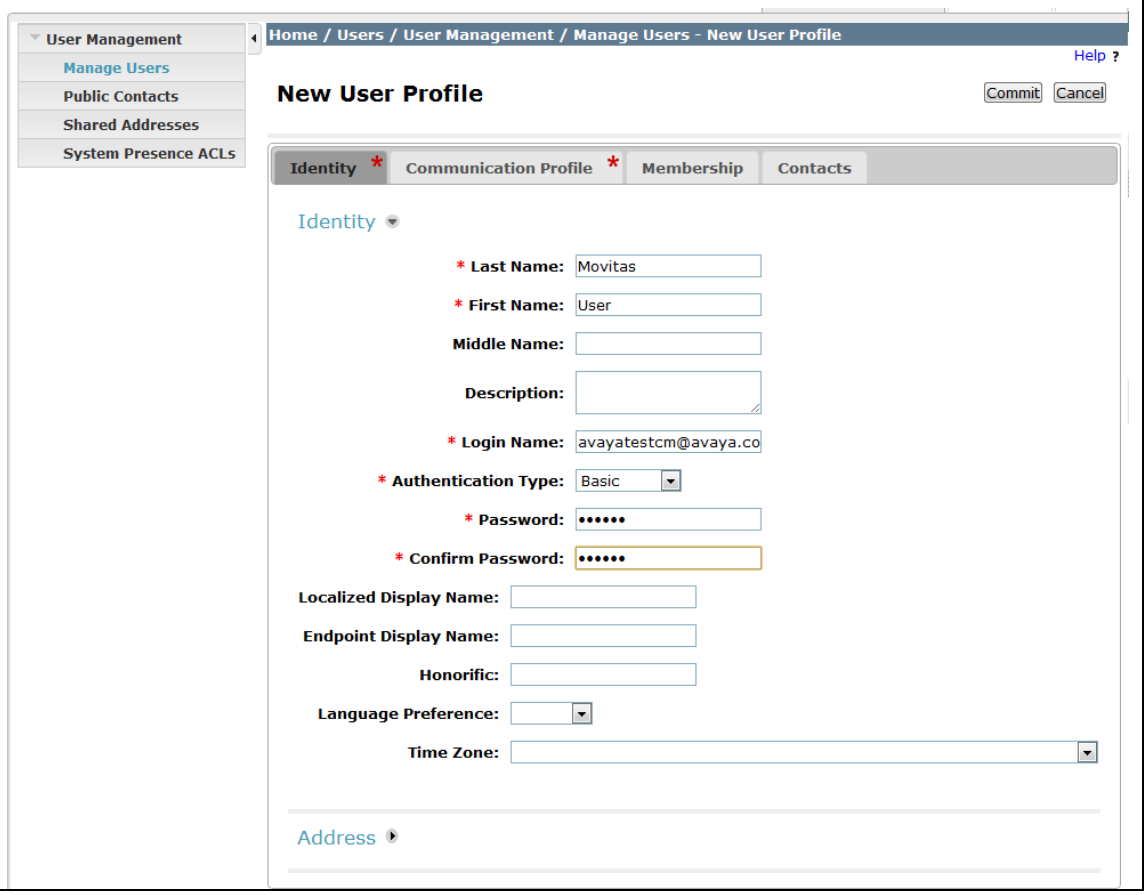
Add Remove

0 Items | Refresh Filter: Enable

☐	Originating Location	Notes

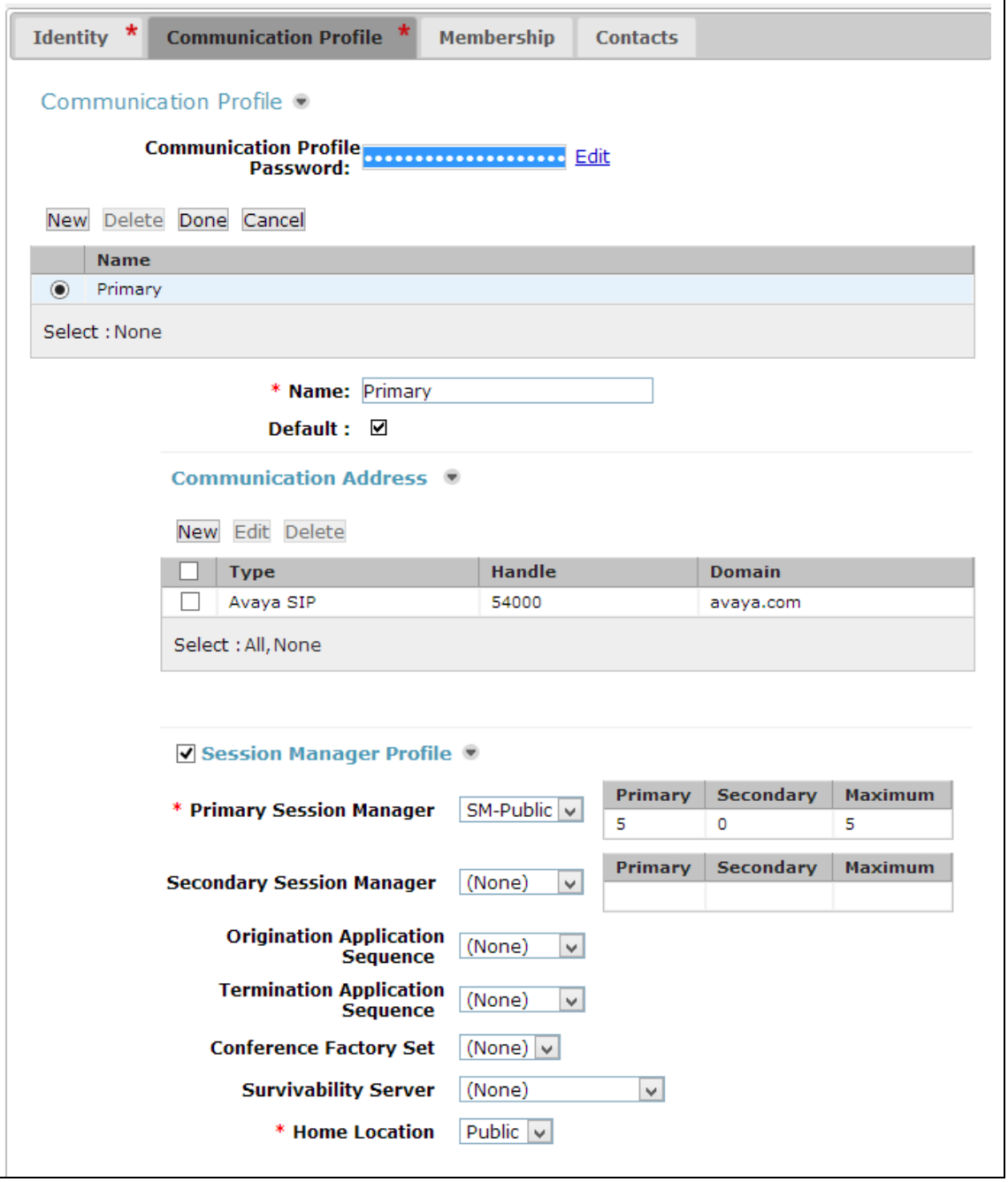
* **Input Required** Commit Cancel

Step	Description
17.	Go back to the **Home** screen by click **Home** tab on the right top corner, and click on **User Management**. 

Step	Description
18.	Click on **Manage Users** and then **New** (Not shown). The user added in this section was used by Movitas MvPBX for registering with Avaya Aura® Session Manager. Under the **Identity** tab: • Set **Last Name** and **First Name** • Set **Login Name** to **avayatestcm@avaya.com** and set the **Password**. 

Step	Description

19.	Under the **Communication Profile** tab:
	• Set the **Communication Profile Password** and **Confirm Password**.
	• Under **Confirm Password,** click on **New**
	  o Set the **Handle** and **Domain** to an extension that will be used by MvPBX to register.
	  o For Compliance testing, information shown in the following screen shot was used.
	• Check the **Session Manager** Profile box and set the **Primary Session Manager** to configured Session Manager.
	• Check the **CM Endpoint Profile** box (not shown).
	  o Set **System** to configured Avaya Aura® Communication Manager
	• Note: Avaya Aura® Communication Manager was pre-configured.
	  o Set **Profile Type** to **Endpoint**.
	  o Set **Extension** same as the **Handle** used in this step.
	  o Set **Security Code** to a desired value. This information will be used when registering MvPBX.
	  o Set **Port** to **IP**.
	• **Commit** the changes.
	
	Screenshot on next page

Step	Description
	

6. Configure Avaya Aura® Communication Manager

This section describes Avaya Aura® Communication Manager configuration to support connectivity to Avaya Aura® Session Manager and related functionality.

The configuration of Avaya Aura® Communication Manager was performed using the System Access Terminal (SAT). After completion of the configuration, perform a **save translation** command to make the changes permanent. Please note that some administration was already performed prior to this test effort. If needed, please refer to *Administering Avaya Aura® Communication Manager* for more details.

6.1. Trunk Configuration – for SIP Trunks to Avaya Aura® Session Manager

This section summarizes the configuration of the SIP trunk that connects the Avaya Aura® Communication Manager to Avaya Aura® Session Manager

Step	Description
1.	**System Parameters – Customer Options** Use the **display system-parameters customer-options** command to verify that the options highlighted below are enabled on Page 4.

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                               IP Stations? y
            Enable 'dadmin' Login? y
            Enhanced Conferencing? y                       ISDN Feature Plus? y
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? n
    Enterprise Survivable Server? n                           ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? n               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? n                  Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? n                 Multifrequency Signaling? y
      Global Call Classification? n          Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y       Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? n                Multimedia IP SIP Trunking? y
                      IP Trunks? y

            IP Attendant Consoles? n
```

Step	Description

2.	**Node Names**
	Use the **change node-names ip** command to create a node name for Avaya Aura® Session Manager The example below shows the node names and IP addresses used for the compliance test. These node names will be used in the administration of other forms in Avaya Aura® Communication Manager.
	
	`change node-names ip` `Page 1 of 2`
	`IP NODE NAMES`
	`Name IP Address`
	`default 0.0.0.0`
	`procr 192.168.62.28`
	`procr6 ::`
	`sm 192.168.62.18`

Step	Description
3.	**IP network region** Avaya Aura® Communication Manager, Avaya Aura® Session Manager and VoIP (H.323/SIP) endpoints were located in a single IP network region (IP network region 1) using the parameters described below. Use the **change ip-network-region 1** command to view these settings. By default, all elements will also be in IP network region 1 unless specifically placed in a separate region using the **ip-network-map** command. The example below shows the values used for the compliance test. ▪ A descriptive name was entered for the **Name** field. ▪ The **Codec Set** field was set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected. This is the codec set that will be used for calls between the Movitas and Avaya Aura® Communication Manager, via Avaya Aura® Session Manager since all components are in IP network region 1. ▪ Enter a domain that was used in Session Manager configuration in **Authoritative Domain**. The default values were used for all other fields. change ip-network-region 1 Page 1 of 20 IP NETWORK REGION Region: 1 Location: 1 **Authoritative Domain: avaya.com** **Name: Public Domain** 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: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS H.323 IP ENDPOINTS RSVP Enabled? n H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5

Step	Description
4.	**Codecs** Use the **change ip-codec-set 1** command to define the codecs used by IP codec set 1. change ip-codec-set 1 Page 1 of 2 IP Codec Set Codec Set: 1 **Audio Codec / Silence Suppression / Frames Per Pkt / Packet Size(ms)** **1: G.711MU n 2 20** **2:** 3:

Step	Description

5.	**Signaling Group**
	Use the **add signaling-group *n*** command, where ***n*** is an unused signaling group, to create a new signaling group for each SIP trunk to Avaya Aura® Session Manager. For compliance test, signaling group 1 was created for the trunk to Avaya Aura® Session Manager. Signaling group 1 was configured using the parameters highlighted below. Default values were used for all other fields.
	▪ Set the **Group Type** to ***sip***.
	▪ Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Avaya Aura® Communication Manager. Node names are defined using the **change node-names ip** command (**Step 2**).
	▪ Set the **Far-end Node Name** to ***sm***. This node name maps to the IP address of the Avaya Aura® Session Manager as defined using the **change node-names ip** command (**Step 2**).
	▪ Set the **Near-end Listen Port** and **Far-end Listen Port** to ***5061***.
	▪ Set the **Far-end Network Region** to ***1***. This is the IP network region which contains the Avaya Aura® Session Manager.
	▪ Set **DTMF over IP** to **in-band.**
	▪ Set **Far-end Domain** to the domain configured in Session Manager.
	▪ The default values were used for all other fields.
	
	`add signaling-group 1`
	`SIGNALING GROUP`
	
	`Group Number: 1 **Group Type: sip**`
	`IMS Enabled? n Transport Method: tls`
	`Q-SIP? n SIP Enabled LSP? n`
	`IP Video? n Enforce SIPS URI for SRTP? y`
	`Peer Detection Enabled? y Peer Server: SM`
	
	`Near-end Node Name: procr` **`Far-end Node Name: sm`**
	`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: in-band` `Direct IP-IP Audio Connections? y`
	`Session Establishment Timer(min): 3 IP Audio Hairpinning? n`
	`Enable Layer 3 Test? y Initial IP-IP Direct Media? n`
	`H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6`

Step	Description
6.	**Trunk Group** Use the **add trunk-group *n*** command, where ***n*** is an unused trunk group, to create a new trunk group for each SIP trunk to Avaya Aura® Session Manager. For the compliance test, trunk group 1 was created for the trunk to Avaya Aura® Session Manager. Trunk group 1 was configured using the parameters highlighted below. On **Page 1**: ▪ Set the **Group Type** to ***sip***. ▪ Enter a descriptive name for the **Group Name**. ▪ Enter an available trunk access code (**TAC**) that is consistent with the existing dial plan in the **TAC** field. ▪ Set the **Service Type** to ***tie***. ▪ Set the **Member Assignment Method** to ***auto***. ▪ Set the **Signaling Group** to the signaling group shown in the previous step. ▪ Set the **Number of Members** field to the number of channels available in this trunk. For the compliance test, the number of members was chosen to be ***10***. ▪ Set **Outgoing Display** to ***y*** ▪ The default values were used for all other fields. add trunk-group 1 Page 3 of 21 TRUNK GROUP Group Number: 1 **Group Type: sip** CDR Reports: y **Group Name: to_SM** COR: 1 TN: 1 **TAC: *004** 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: 10**

Step	Description

7.	**Trunk Group – continued**
	On **Page 3**:
	▪ It is required that the **Send Name** field is set to ***y*** and the **Send Calling Number** field is set to ***y***.
	▪ Set the **Format** field to ***public***. This field specifies the format of the calling party number sent to the far-end.
	▪ The default values were used for all other fields.
	
	`add trunk-group 1 Page 3 of 21`
	`TRUNK FEATURES`
	`ACA Assignment? n Measured: none`
	`Internal Alert? n Maintenance Tests? y`
	`Data Restriction? n NCA-TSC Trunk Member:`
	`Send Name: y Send Calling Number: y`
	`Used for DCS? n Send EMU Visitor CPN? n`
	`Suppress # Outpulsing? n` **`Format: public`**
	`UUI IE Treatment: service-provider`
	`Replace Restricted Numbers? n`
	`Replace Unavailable Numbers? n`
	`Send Connected Number: n`
	`Hold/Unhold Notifications? n`
	`Send UUI IE? y Modify Tandem Calling Number? n`
	`Send UCID? n`
	`Send Codeset 6/7 LAI IE? y`

8.	**Automatic Route Selection (ARS)**
	For the compliance test, ARS was used to route calls to EC500 extension that was 5 digits long and leading digit was 7. Use the **change ars analysis** command to create an entry in the ARS table.
	• Set **Dialed String** to ***7***
	• Set **Total Min** and **Max** to ***5***
	• Set **Route Pattern** to ***1***
	• Set **Call Type** to ***svcl***
	
	`change ars analysis 7 Page 1 of 2`
	`ARS DIGIT ANALYSIS TABLE`
	`Location: all Percent Full: 2`
	
	`Dialed Total Route Call Node ANI`
	`String Min Max Pattern Type Num Reqd`
	`7 5 5 1 svcl n`

Step	Description
9.	**Route Patterns** Use the **change route pattern *n*** command, where ***n*** is an unused route pattern. The example below shows route pattern 1 used in the compliance test. Route pattern 1 was accessed when ARS matches on a dialed string of 7xxxx. For the first entry, set the **Grp No.** field to the trunk group of Avaya Aura® Session Manager (trunk group 1). Set the Facility Restriction Level (**FRL**) of the trunk to an appropriate level to allow authorized users to access the trunk. The level of ***0*** is the least restrictive.

```
change route-pattern 1                                          Page   1 of   3
                   Pattern Number: 1   Pattern Name:
                            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: 1    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
```

6.2. Trunk Configuration – for ISDN/PRI to PSTN

ISDN calls to PSTN were also tested.

Step	Description
1.	**System Parameters – Customer Options** Use the **display system-parameters customer-options** command to verify that the options highlighted below are enabled. If this option is disabled please check with Avaya sales or business partner to get appropriate license.

```
display system-parameters customer-options                      Page   4 of  11
                               OPTIONAL FEATURES

   Emergency Access to Attendant? y                               IP Stations? y
            Enable 'dadmin' Login? y
            Enhanced Conferencing? y                       ISDN Feature Plus? y
                     Enhanced EC500? y       ISDN/SIP Network Call Redirection? n
    Enterprise Survivable Server? n                           ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
                  ESS Administration? n               Local Survivable Processor? n
         Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? n                  Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n    Mode Code for Centralized Voice Mail? n
                  Flexible Billing? n
   Forced Entry of Account Codes? n                 Multifrequency Signaling? y
      Global Call Classification? n          Multimedia Call Handling (Basic)? y
              Hospitality (Basic)? y       Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? n                Multimedia IP SIP Trunking? y
                       IP Trunks? y

            IP Attendant Consoles? n
```

Step	Description

2.	**Add DS1**
	Use the **add ds1** ***Board-location*** command to add a DS1. In this case, board V2 was used. The gateway used for this testing, was connected to another Avaya Media Gateway which had access to PSTN. This configuration pertains to the Media Gateway G430 as show in the **Test Configuration** diagram.
	• Set **Signaling Mode** to ***isdn-pri***
	• Set **Name** to a desired name
	• Set **Line Coding** to ***b8zs***
	• Set **Protocol Version** to ***b***
	
	`add ds1 01V2 Page 1 of 2`
	`DS1 CIRCUIT PACK`
	`Location: 001V2 **Name: PSTN**`
	`Bit Rate: 1.544 **Line Coding: b8zs**`
	`Line Compensation: 1 Framing Mode: esf`
	`**Signaling Mode: isdn-pri**`
	`Connect: network`
	`TN-C7 Long Timers? n Country Protocol: 1`
	`Interworking Message: PROGress **Protocol Version: b**`
	`Interface Companding: mulaw CRC? n`
	`Idle Code: 11111111`
	`DCP/Analog Bearer Capability: 3.1kHz`
	`T303 Timer(sec): 4`
	`Slip Detection? n Near-end CSU Type: other`
	`Echo Cancellation? n Block Progress Indicator? n`

3.	**Signaling Group**
	Use the **add signaling-group** ***n*** command, where ***n*** is an unused signaling group, to create a new signaling group for each ISDN to PSTN Gateway. For the compliance test, signaling group 3 was created for the trunk to the PSTN Gateway.
	▪ Set the **Group Type** to ***isdn-pri***.
	▪ Set the **Trunk Group for Channel Selection** field to the trunk group created in the next step. This cannot be done until the trunk group is created. Thus, initially this field is left blank and later changed to the correct value after the trunk group is created. A separate trunk group will be created for each signaling-group.
	▪ Set **Primary D-Channel** as the 24th channelfor ds1 added in **Step 2**.
	▪ The default values were used for all other fields.
	
	`add signaling-group 3 Page 1 of 5`
	`SIGNALING GROUP`
	`Group Number: 3 **Group Type: isdn-pri**`
	`Associated Signaling? y Max number of NCA TSC: 0`
	`**Primary D-Channel: 001V224** Max number of CA TSC: 0`
	`Trunk Group for NCA TSC:`
	`Trunk Group for Channel Selection: X-Mobility/Wireless Type: NONE`
	`TSC Supplementary Service Protocol: a Network Call Transfer? n`

Step	Description

4.	**Trunk Group**
	Use the **add trunk-group *n*** command, where ***n*** is an unused trunk group, to create a new trunk group for each ISDN/PRI to PSTN gateway. For the compliance test, trunk group 3 was created for the trunk to the Media Gateway as shown in the **Test Configuration** diagram.
	
	On **Page 1**:
	▪ Set the **Group Type** to ***isdn***.
	▪ Enter a descriptive name for the **Group Name**.
	▪ Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
	▪ Set the **Carrier Medium** to ***PRI/BRI***.
	▪ Set the **Service Type** to ***public-ntwrk***.
	▪ The default values were used for all other fields.
	
	`add trunk-group 3 Page 1 of 21`
	`TRUNK GROUP`
	
	`Group Number: 3 Group Type: isdn CDR Reports: r`
	`Group Name: PSTN COR: 1 TN: 1 TAC: *003`
	`Direction: two-way Outgoing Display? y Carrier Medium: PRI/BRI`
	`Dial Access? y Busy Threshold: 255 Night Service:`
	`Queue Length: 0`
	`Service Type: public-ntwrk Auth Code? n TestCall ITC: rest`
	`Far End Test Line No:`
	`TestCall BCC: 4`

Step	Description
5.	**Trunk Group – Continued** On Page 3: ▪ Set **Send Name** to ***y***. ▪ Set **Send Calling Number** to ***y***. ▪ Set **Format** to ***Public***. ▪ Set **Connected Number** to ***y***. add trunk-group 3 Page 3 of 21 TRUNK FEATURES ACA Assignment? n Measured: none Wideband Support? n Maintenance Tests? y Data Restriction? n NCA-TSC Trunk Member: **Send Name: y** **Send Calling Number: y** Used for DCS? n Send EMU Visitor CPN? n Suppress # Outpulsing? n **Format: public** Outgoing Channel ID Encoding: preferred UUI IE Treatment: service-provider Replace Restricted Numbers? n Replace Unavailable Numbers? n **Send Connected Number: y** Network Call Redirection: none Hold/Unhold Notifications? n Send UUI IE? y Modify Tandem Calling Number: no Send UCID? n Send Codeset 6/7 LAI IE? y Ds1 Echo Cancellation? n Apply Local Ringback? n US NI Delayed Calling Name Update? n Show ANSWERED BY on Display? y Network (Japan) Needs Connect Before Disconnect? n
6.	**Trunk Group – Continued** On Page 5, type in define all 23 ports for the ds1 added in **Step 3**. Ports are defined in the format such that **Port** value is set as board name followed by channel number. In our case the board was 001V2 and channel numbers 01-04 were used, as seen the box below. add trunk-group 3 Page 5 of 21 TRUNK GROUP Administered Members (min/max): 1/4 GROUP MEMBER ASSIGNMENTS Total Administered Members: 4 Port Code Sfx Name Night Sig Grp **1: 001V201 MM710 3** **2: 001V202 MM710 3** **3: 001V203 MM710 3** **4: 001V204 MM710 3**

Step	Description

7.	**Automatic Route Selection (ARS)**
	For the compliance test, an entry was added to route call to PSTN by dialing an 11 digit Telephone Number (TN) and 10 digit TN. The entry is highlighted below which is used to route calls to PSTN by dialing 1303xxxxxxx. This dialed string is mapped to route pattern ***3*** which routes calls to trunk 3 connected to the PSTN.
	
	`change ars analysis 13 Page 1 of 2`
	`ARS DIGIT ANALYSIS TABLE`
	`Location: all Percent Full: 2`
	
	`Dialed String Total Min Max Route Pattern Call Type Node Num ANI Reqd`
	`1303 11 11 3 hnpa n`

8.	**Route Pattern – PSTN Trunk**
	This route pattern is used in cases where the SIP Users or Avaya Extensions need to be used to calls the PSTN number. Avaya Aura® Communication Manager will then route the call out the PSTN trunk.
	• Set **Grp No** to trunk group in **Step 4, 3**.
	• Set **FRL** to **0**.
	
	`change route-pattern 4 Page 1 of 3`
	`Pattern Number: 4 Pattern Name:`
	`SCCAN? n Secure SIP? n`
	`Grp No FRL NPA Pfx Mrk Hop Lmt Toll List No. Del Dgts Inserted Digits DCS/ QSIG Intw IXC`
	`1: 3 0 n user`
	`2: n user`
	`3: n user`
	`4: n user`
	`5: n user`
	`6: n user`
	
	`BCC VALUE 0 1 2 M 4 W TSC Request CA-TSC ITC BCIE Service/Feature PARM No. Dgts Subaddress Numbering Format LAR`
	`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`

6.3. EC500 Configuration

Step	Description
1.	**EC500 – Digital and IP stations** Use **change off-pbx-telephone station-mapping *n*** to map an EC500 extension where ***n*** is the Avaya Digital or H.323 Extension. ▪ Set **Application** to ***EC500*** ▪ Set **Phone Number** to the SIP User extension on MvPBX. Note that this phone number must comply with the ars analysis for calls starting with digit 7 in **Section 6.1**. ▪ Set **Trunk Selection** to ***ars***

```
change off-pbx-telephone station-mapping 54006                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                    Selection   Set     Mode
 54001           EC500         -     70001            ars        1
                               -
                               -
                               -
                               -
                               -
                               -
```

Step	Description
2.	**EC500 – Analog station** EC500 for analog station is achieved by adding a virtual IP station and assigning bridge functionality. To add a virtual station, use **add station *n*** command, where ***n*** is an available extension. On Page 1: • Set the type to **9630**. • Type in **Name**.

```
add station 40201                                          Page   1 of   5
                                    STATION

Extension: 40201                        Lock Messages? n               BCC: 0
     Type: 9630                         Security Code:                  TN: 1
     Port: IP                         Coverage Path 1:                 COR: 1
     Name: Analog EC500               Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19          Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 40201
           Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
```

On Page 4, under **BUTTON ASSIGNMENTS**

- On a new line, type in **abrdg-appr**.
- For **Ext.** type in the Analog extension which needs EC500 functionality.

```
add station 40201                                          Page   4 of   5

                                    STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                       Cord Length: 0
   Building:                                         Set Color:

ABBREVIATED DIALING
     List1:                     List2:                     List3:



BUTTON ASSIGNMENTS
 1: call-appr                           5:
 2: call-appr                           6:
 3: call-appr                           7:
 4: abrdg-appr  Ext: 54201              8:

    voice-mail
```

Step	Description

	Use **change off-pbx-telephone station-mapping *n*** to map an EC500 extension where ***n*** is the Avaya virtual extension added above.
	▪ Set **Application** to ***EC500***.
	▪ Set **Phone Number** to the SIP User extension on MvPBX.
	▪ Set **Trunk Selection** to ***ars***.
	
	`change off-pbx-telephone station-mapping 54006 Page 1 of 3`
	`STATIONS WITH OFF-PBX TELEPHONE INTEGRATION`
	
	`Station Application Dial CC Phone Number Trunk Config Dual`
	`Extension Prefix Selection Set Mode`
	`40201 EC500 - 70201 ars 1`
	`-`
	`-`
	`-`
	`-`
	`-`
	`-`

7. Configure Movitas

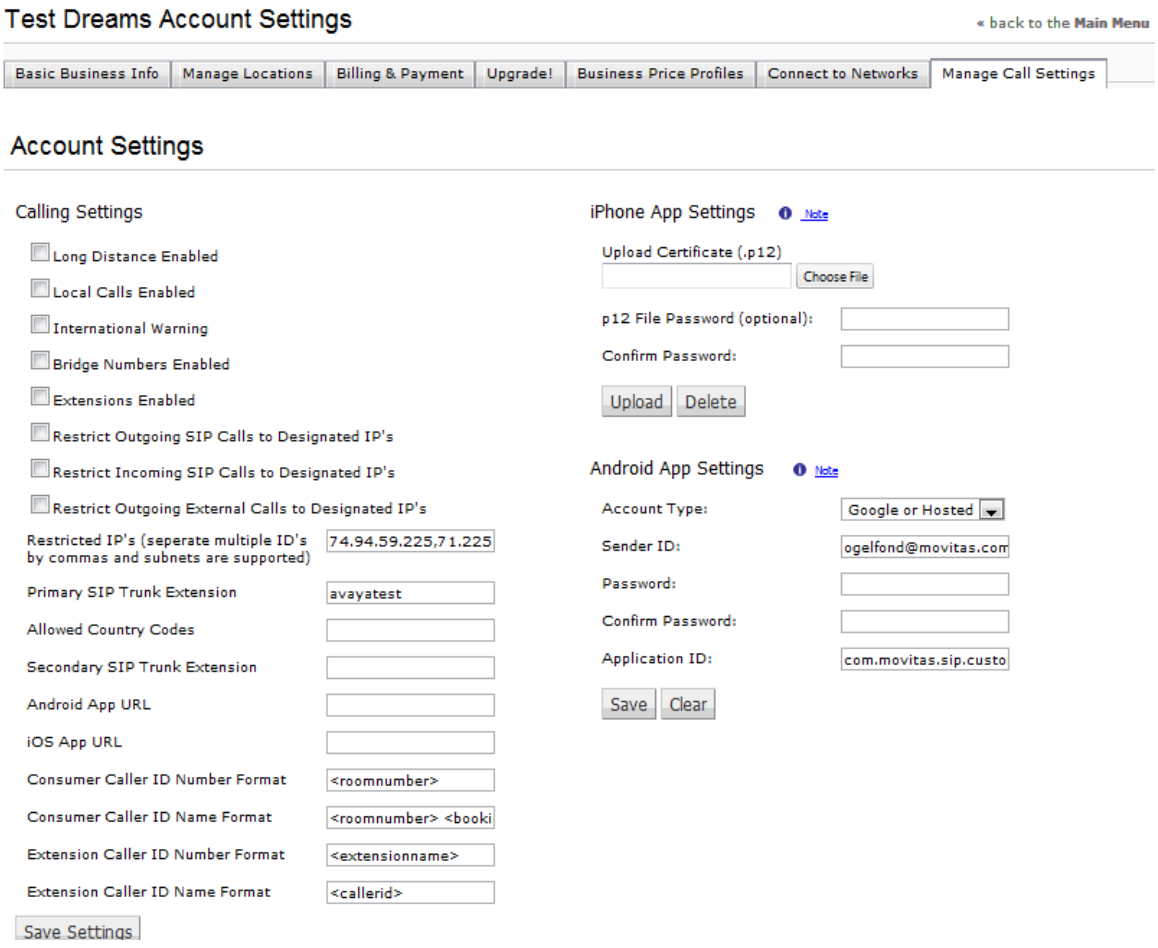
Configuration for Movitas MvPBX was performed by a Movitas Engineer. This document assumes that the Movitas MvPBX system was properly installed and configured by a Movitas Engineer. This section provides the steps of how to configure Movitas MvPBX working with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

7.1. Configure Business Account

As a partner on Movitas.com, a business account is established by signing up, choosing a name for the account and providing any necessary billing information. Once this is established the content, users, designs and business extensions can be managed via the Movitas interface.

7.2. Enable the Business Account for Calling

After a business account is established, a Movitas admin can set up the business to enable calling functionality on the Account Settings Price Profile page. This can be done by logging into the Movitas system, clicking on **Account Settings** in the top right, and then clicking on the **Price Profile** tab. Note: This is only available to Movitas Admins and not all admins. Once calling is enabled, this will result in an additional account setting tab where the SIP trunk can be set, IP addresses can be setup to restrict calls to certain sites, push notifications can be configured and more. For Avaya Aura® Communication Manager testing, the only required field is the SIP Trunk, which will be assigned in **Step 7.3** below.



7.3. Configure SIP Trunk in MvPBX

Once a business is setup, Movitas can assign a SIP Trunk username and password for the Avaya system. The required settings for this are:

- **Name**: a short name to use as an identifier for the trunk
- **Full name**: a human-friendly used to describe the trunk

- **Secret**: the password used for authentication from user created in System Manager**Host**: the IP address of the Avaya Aura® Session Manager that will be connected to as a user
- **Transport**: should be set to UDP
- **Directmedia**: should be set to nonat
- **Register**: registration entry for MvPBX (ex. 54000@avaya.com:movitas:54000@205.168.62.18/54000~3600)
- **Default county code**: the numerical country code for outgoing international call parsing
- **PSTN prefix**: prefix for outbound calls
- **From Domain**: from domain where calls will come from (ex. avaya.com)

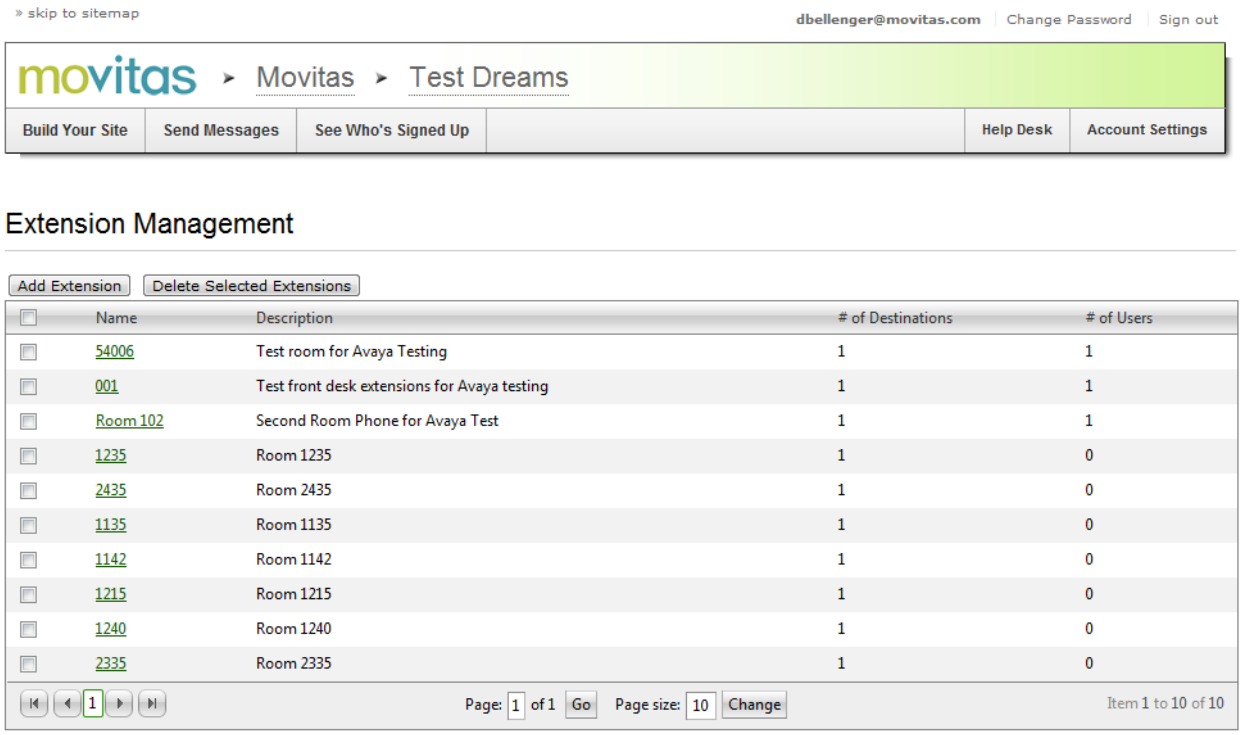
Once established the credentials are provided to complete the setup in Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

7.4. Assign SIP Trunk to Business Account

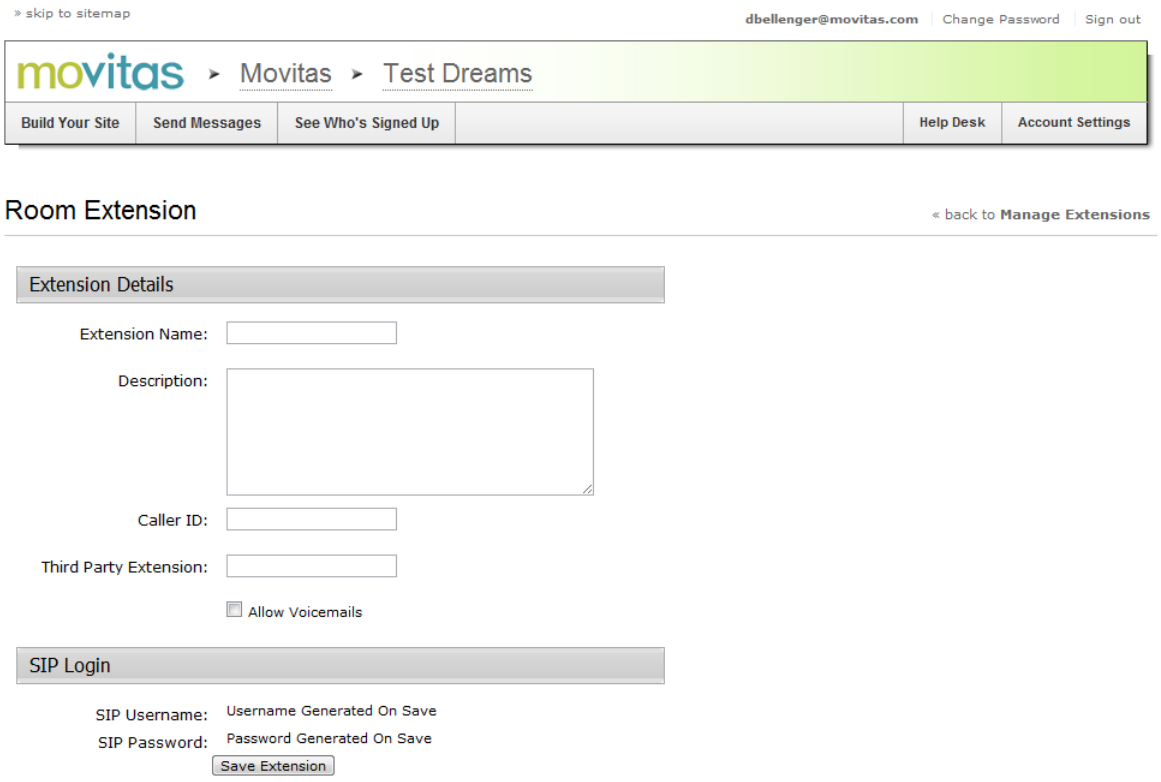
Following the trunk creation, the account administrator can return to the business account for the application and enter the SIP Trunk name into the **Primary SIP Trunk** field.

7.5. Setup Business Extensions

Once the trunk is established, administrators can navigate to the room extensions page where they can create and manage extensions.



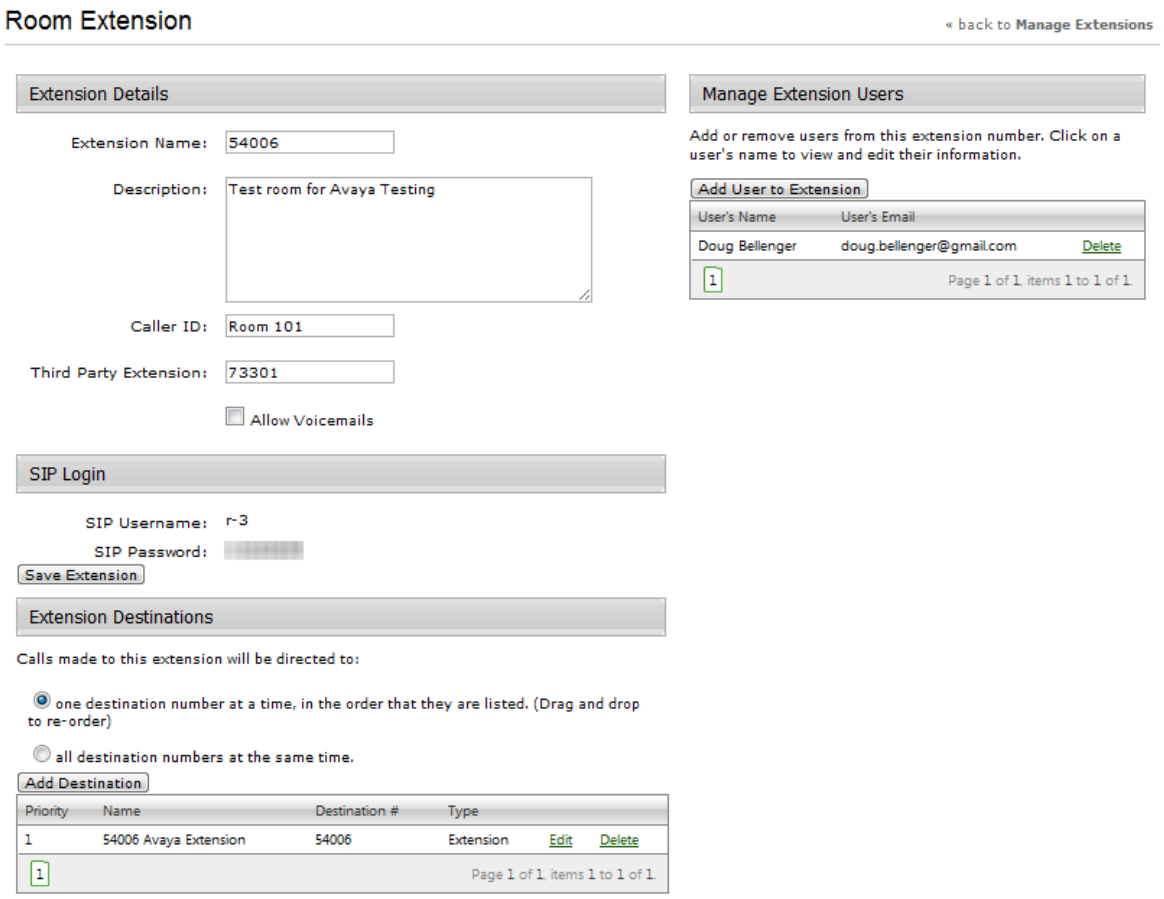
Then click "**Add Extension**" to be taken to the new extension page shown below:



The information that should be added is

- **Extension Name** – a familiar name that can be used to identify the extension (ex. Room 101)
- **Description** – a description of the name if required
- **Caller ID** – if a different caller ID is required for the extension it can be entered here. (Note: caller ID and caller Number for consumer extensions and business extensions can also be formatted on the call settings page using variables such as room number, first name, last name, booking last name, caller ID, extension name, etc).
- **Third Party Extension** – for Avaya implementations, the PCA number should be added here in order to map calls to these extensions. This number must be unique for each business extension

Once all the settings are complete, click **Save Extension** and the extension will now be enabled and call destinations can be configured such as users, DID's, SIP extensions, or Avaya Aura® Communication Manager extensions. An example of the updated page is below.



7.6. Setup Call Destinations for the Extension

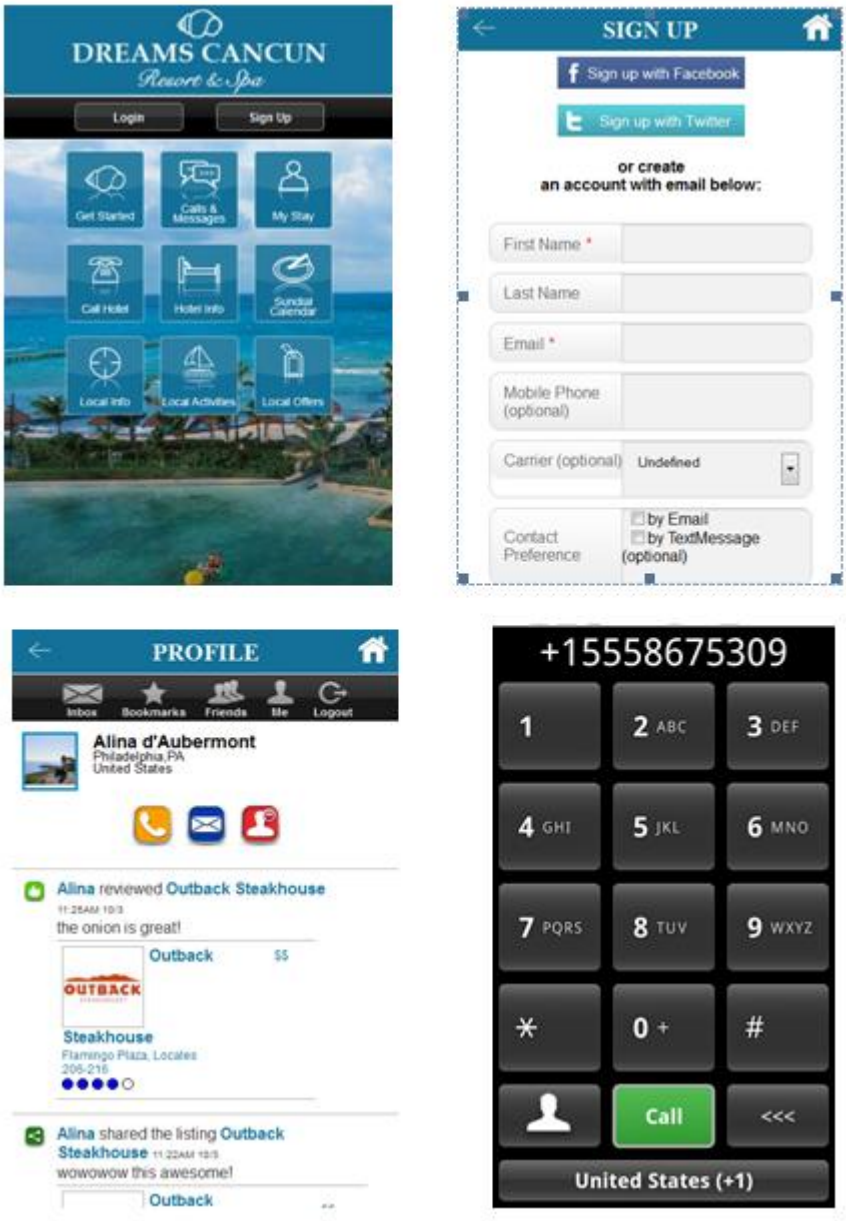
In order to forward calls from a user to the room, in addition to setting up the Third Party Extension with the appropriate redirect number, the Direct Number (DN) also should be added as an extension as shown above. (Warning: setting up the redirect number as a call destination is not recommended due to the creation of a loop between the two systems). In addition to hotel extensions, a call destination can be pointed at a SIP address, a DID, or a user in the system.

7.7. Deploy Applications Via App Stores

In order to complete the setup of the applications, Movitas will package the content and calling functionality into the required apps and enter them into the appropriate app store. Once completed the application will be available for download and the content and extensions can be updated via the Movitas portal. Any changes to the SIP Trunk for the business, IP addresses or other settings can be updated as well.

7.8. User Creates Account on Application

In order to place calls via the application following the setup, a user will signup for an account, log in to the application and then they will be registered with MvPBX automatically. Once they are logged in, they can navigate to the dialpad where they can dial an extension direct or dial another user account.

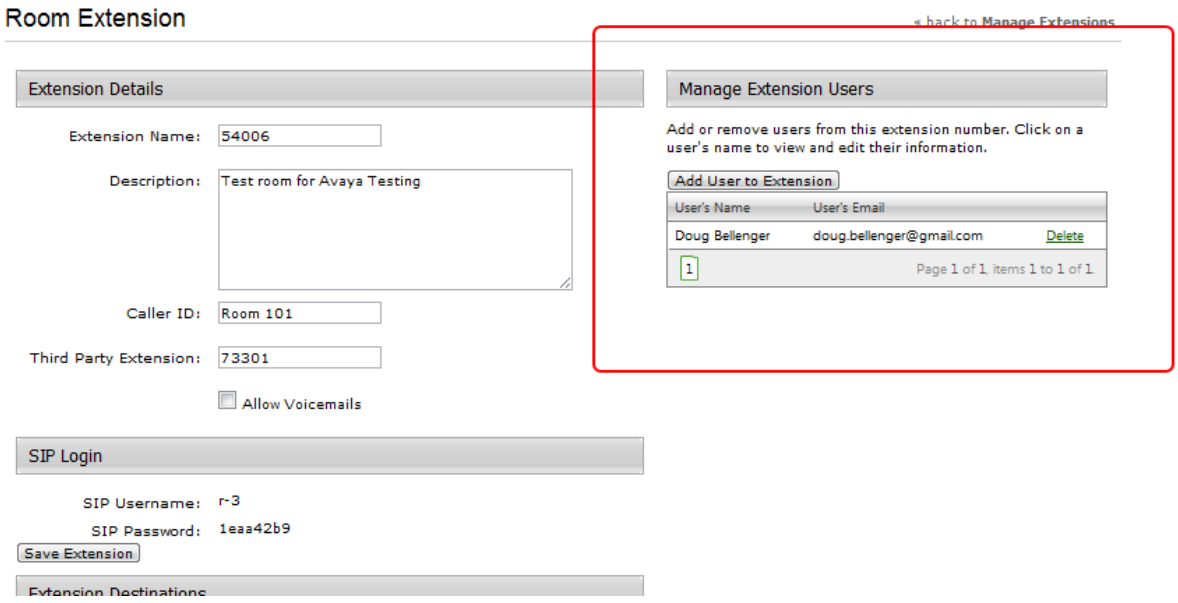


Note: The above shows an example hotel website with the following sections:

- Top Left: Home screen with icons related to hotel services, local information, and guest communication tools
- Top Right: An example of a sign up page for the hotel application
- Bottom Right: An example profile for a user from the application
- Bottom Left: An example dial pad from the Android application for the hotel

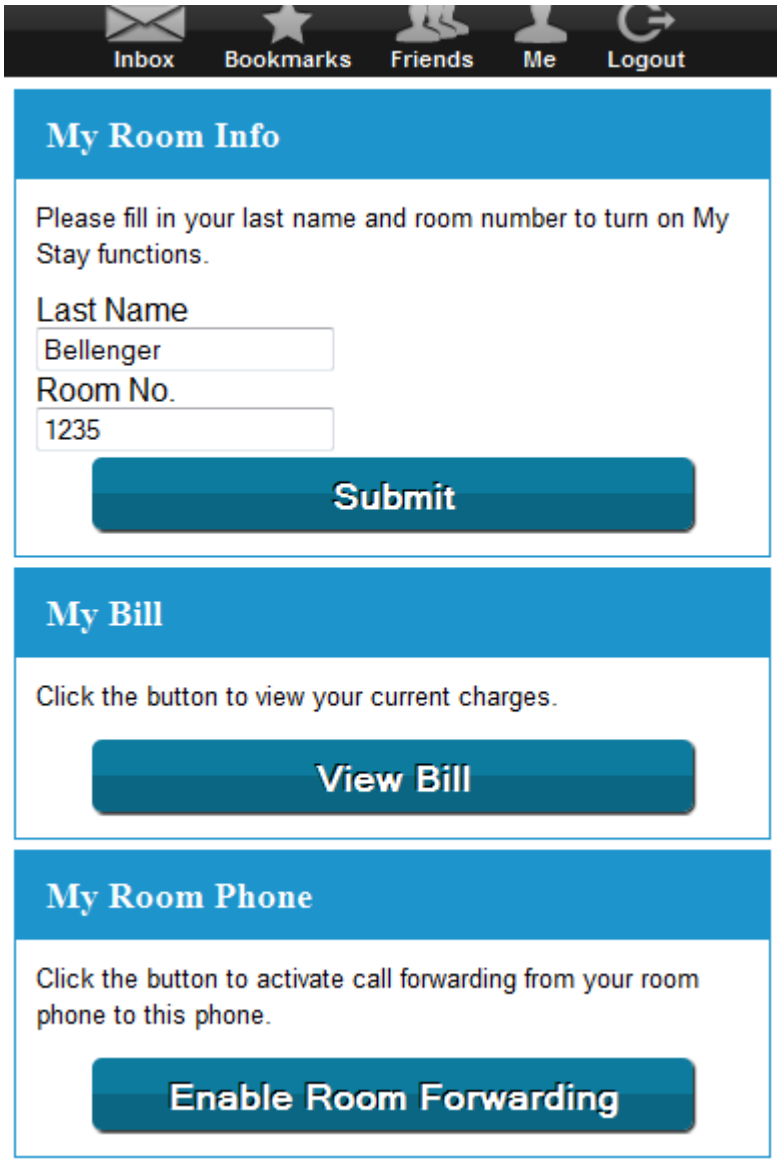
7.9. Assign User Such as Front Desk to Extension

Once a user account is setup, administrators can assign users to extensions by accessing the business extension from the extension management page in **Section 7.5** and the clicking on the extension to manage. When on the extension management page, an administrator can assign a user to an extension by adding their email address under the **Manage Extension Users** section on the right side of the page. A user can also be deleted from this page by clicking the "delete" link by their name once they have been added.



7.10. Assigning User to Room Phone From Application

Pending the availability of web services into a Property Management System (PMS) for a specific client, for example a hotel, a page may be setup to enable forwarding of the room phone as outlined below. This will associate the user with the appropriate extension that calls can be forwarded or received from. This can also be handled by web services and will need to be established custom for each implementation by Movitas.



Note: This is an example of a page setup for hotels that allows their guests to enable room forwarding from Communication Manager to the application for the length of their stay. At the end of their stay calls will no longer be forwarded to them based on their checkout date.

8. Verification Steps

The following are typical steps to verify the interoperability between the Movitas system and Avaya Aura® Communication Manager and Avaya Aura® Session Manager

- Place a call to Front Desk phone which is one of three Avaya extensions associated with Movitas SIP users.
- The Front Desk phone in the Avaya Aura® Communication Manager rings and the Movitas SIP user associated with the Front Desk phone also rings.
- Accept the call on the Movitas SIP user, the Front Desk phone in Avaya Aura® Communication Manager stops ringing and become idle.
- Check two-way audio path between the caller and Movitas SIP user

9. Conclusion

All of the executed test cases have passed and met the objectives as outlined in **Section 2**. The Movitas SIP MvPBX system and its respective iPhone, Android and Blackberry applications are considered compliant with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

10. Additional References

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

Avaya

[1] *Administering Avaya Aura® Communication Manager*, Doc # 03-603558, Release 6.0.1, Issue 1.3, December 2010.

[2] *Administering Avaya Aura® Session Manager*, Doc # 03-603324, Release 6.1 November 2010

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.