



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Speakerbus iTurret with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the steps required to connect Speakerbus iTurret to Avaya Aura® Session Manager and Avaya Aura® Communication Manager as a SIP User. Avaya Aura® Communication Manager features can be made available in addition to the standard features supported on the iTurret.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps required to connect Speakerbus iTurret to Avaya Aura® Session Manager and Avaya Aura® Communication Manager as a SIP user. Also described, is how Avaya Aura® Communication Manager features can be made available in addition to the standard features supported by iTurret. In this configuration, the Off-PBX Stations (OPS) feature set is extended from Avaya Aura® Communication Manager to the Speakerbus iTurret, providing the iTurret deskstation with enhanced calling features.

The table below provides a summary of the supported features available on iTurret with the Avaya SIP offer. Some features are supported locally on the iTurret, while others are only available with Communication Manager and Session Manager with OPS. In addition to basic calling capabilities, the Internet Engineering Task Force (IETF) has defined a supplementary set of calling features, often referred to as the SIPPING-19 [5]. This provides a useful framework to describe product capabilities and compare features supported by various equipment vendors. Additional features beyond the SIPPING-19 can be extended to the iTurret using OPS.

Some OPS features listed in the following table can be invoked by dialing a Feature Name Extension (FNE). A speed dial button on iTurret can also be programmed to an FNE. Other features, such as Exclusion/Privacy and Call Forwarding, are available by using the AST (Advanced SIP Telephony) FNU (Feature Name URI). Communication Manager automatically handles many other standard features via OPS, such as call coverage, trunk selection using Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS), Class of Service (COS), Class of Restriction (COR), and voice messaging. Details on operation and administration of OPS can be found in References [2] and [3]. The Avaya SIP solution requires all SIP telephones to be configured on Communication Manager as OPS. Items in the table below shown in **bold** were tested using an FNU or FNE.

FEATURE	SUPPORTED		COMMENTS
	Locally at the phone	With Avaya SIP Offer	
Basic Calling Features			
Extension to Extension Call	Yes	Yes	
Basic Call to legacy phones	No	Yes	
Speed Dial Buttons	Yes	Yes	
Message Waiting Support	Yes	Yes	

FEATURE	SUPPORTED		COMMENTS
	Locally at the phone	With Avaya SIP Offer	
SIPPING-19 Features			
Call Hold	Yes	Yes	
Consultation Hold	Yes	Yes	
Unattended Transfer	Yes	Yes	
Attended Transfer	Yes	Yes	
Call Forward All	Yes	Yes	Local menu option on iTurret and FNU
Call Forward Busy/No answer	Yes	Yes	Local menu option on iTurret and FNU
Call Forward Cancel	Yes	Yes	Local menu option on iTurret and FNU
3-way conferencing (3 rd party added)	Yes	Yes	
3-way conferencing (3 rd party joins)	Yes	Yes	
Find me	No	Yes	Via OPS Coverage Paths
Incoming call screening	No	Yes	Via OPS Class Of Restriction
Outgoing call screening	No	Yes	Via OPS Class Of Restriction
Call Park/Unpark	No	Yes	Via OPS FNE
Call Pickup	No	Yes	Via OPS FNE
Automatic Redial	No	Yes	Via OPS FNE
OPS – Selected Additional Station-Side Features			
Conference on answer	No	Yes	Via OPS FNE
Directed call pickup	No	Yes	Via OPS FNE
Drop last added party	No	Yes	Via OPS FNE
Exclusion/Privacy	Yes	Yes	Local hard key on iD808 iTurret using FNU
Last number dialed	Yes	Yes	Via OPS FNE
Priority Call	No	Yes	Via OPS FNE, iTurret doesn`t support distinctive ring indication
Send All Calls	No	Yes	Via OPS FNE
Send All Calls Cancel	No	Yes	Via OPS FNE
Transfer to Voicemail	No	Yes	Via OPS FNE
Whisper Page	No	Yes	Via OPS FNE

Table 1

2. General Test Approach and Test Results

To verify interoperability of the iTurret with Communication Manager and Session Manager, calls were made between the iTurret deskstations and Avaya SIP, H.323 and Digital stations exercising common PBX features. The telephony features were activated and deactivated using buttons and menu options on the iTurret, FNEs, and FNUUs.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/Smartphones that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/Smartphones for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the iTurret did not include use of any specific encryption features as requested by Speakerbus.

Note: Compliance testing was carried out using UDP as the transport for signaling.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of the iTurret deskstation with Session Manager
- Calls between the iTurret and Avaya SIP, H.323, and digital Stations
- Hold/Retrieve operations
- Supervised/blind transfers and Conference
- G.711, G.722-64k and G.729 codec support
- COR restricted calls
- Bridged appearances
- Barge in and Privacy
- PSTN calls
- Voicemail and message waiting indicators (MWI)
- Extended telephony features using Communication Manager Feature Name Extensions (FNEs) shown in bold in **Table 1**
- Call forwarding (busy and no-answer) and Send All Calls using Call Forwarding and Send All Call FNU's
- Serviceability testing after an iTurret restart and loss of IP connection

2.2. Test Results

All the test cases passed successfully with the following observations.

1. In a particular scenario, where there are three iTurret deskstations each having the bridged appearances of the other two iTurret deskstations, there are issues observed with 'Barge In' and 'Privacy'.
 - If a call is made from User 1 to User 3 and then User 2 barges into the call (either to User 1 ext or to User 2 ext), hangs up and barges in a second time, upon hanging up for the second time in succession all calls are dropped. This behaviour is the same for Avaya SIP phones. Avaya is investigating this issue.
 - With the same call in place (User 1 to User 3) and User 1 presses the 'Privacy Key'. When User 2 tries to barge into User 1's call, User 2 is refused as expected but when User 2 tries again it results in all calls being dropped. This behavior is the same for Avaya SIP phones. Avaya is investigating this issue.

2.3. Support

For technical support of Speakerbus products contact the Speakerbus Service Desk:

- Web: <http://www.speakerbus.com>
- Email: support@speakerbus.com
- Telephone: +1 (646) 289 4700 in North America
+44 (0) 870 240 7252 in Europe
+65 6590 9228 in Asia

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Manager, Session Manager along with a Media Gateway and a Media Server. System Manager was used to provision Communication Manager and Session Manager. Speakerbus iTurrets were connected to the LAN and connect to Session Manager as a SIP user. SIP, Digital and H.323 telephones were used to place calls to and receive calls from the Speakerbus iTurrets. Avaya Aura® Messaging was used to provide and test voicemail and Message Waiting facilities.

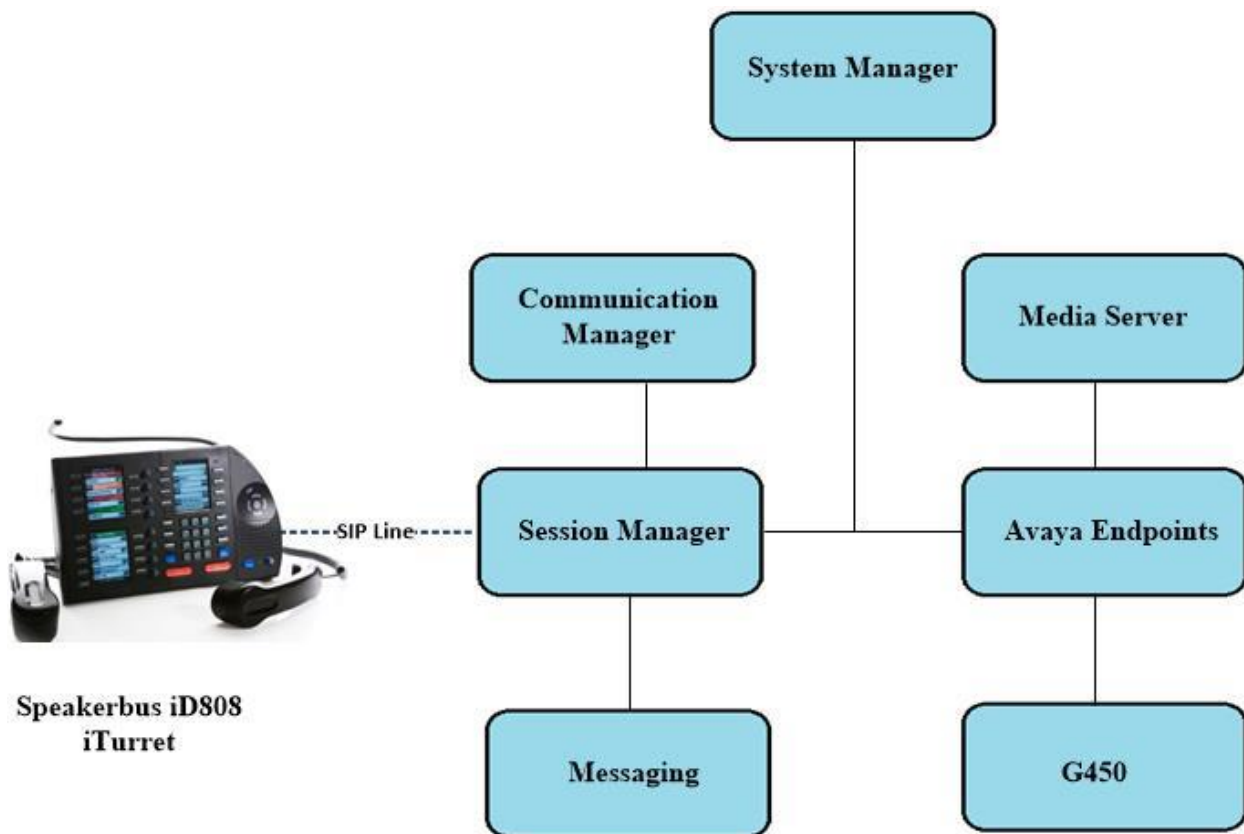


Figure 1: Avaya Aura® Communication Manager and Avaya Aura® Session Manager with Speakerbus solution

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya Equipment/Software	Release/Version
Avaya Aura® System Manager	System Manager 8.1.1.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.1.0.0310912 Feature Pack 1
Avaya Aura® Session Manager	Session Manager R8.1 Build No. – 8.1.1.0.811021
Avaya Aura® Communication Manager	R8.1.1.0.0 – FP1 R018x.01.0.890.0 Update ID 01.0.890.0-25763
Avaya Aura® Media Server	8.0.0.169
Avaya Media Gateway G430	41.16.0/1
Avaya 96x1 H323 Deskphone	6.8304
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya J179 H323 Deskphone	6.8.304
Avaya J129 SIP Deskphone	3.0.0.0.20
Avaya 9408 Digital Deskphone	V2.0
Speakerbus Equipment/Software	Release/Version
Speakerbus iCMS with iManager	v3.750.5.0
Speakerbus iTurret	v3.422.1.0

5. Configure Avaya Aura® Communication Manager

No specific changes were made on Communication Manager to facilitate the connection of the iTurret with Session Manager. The iTurret utilizes some of the features provided by Communication Manager. These features along with the dial plan, SIP trunk and coverage path are displayed in this section to provide the reader with some helpful information on how the Communication Manager was setup for compliance testing.

Every site will have a unique setup, the information contained in the System Parameters Features or the System Parameters Customer Options will be suited to that particular site. The information provided in this section serves to show how this system was setup during compliance testing and is not an instruction guide to setup the Communication Manager for the iTurret to work. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

Configuration and verification operations on Communication Manager illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The Communication Manager information displayed in this section can be summarized as follows:

- System Parameters and Features
- SIP Trunk
- Call Routing for iTurret
- Feature Access Codes (FACs)
- Feature Name Extensions (FNEs)
- Class of Service (COS)
- Class of Restriction (COR)
- Coverage Path

Note: Any settings not in **Bold** in the following screen shots may be left as default.

5.1. Verify System Parameters and Features

Each Communication Manager system will have its own setup with different System Parameters and Features configured depending on the requirement of the customer. Here is a snapshot of some of these values that were configured on the DevConnect lab for compliance testing.

5.1.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 1**, verify that the **Maximum Off-PBX Telephones** allowed in the system is sufficient. One OPS station is required per iTurret device.

display system-parameters customer-options	Page	1 of 12
OPTIONAL FEATURES		
G3 Version: V18	Software Package: Enterprise	
Location: 2	System ID (SID): 1	
Platform: 28	Module ID (MID): 1	
	USED	
Platform Maximum Ports:	6400	82
Maximum Stations:	2400	22
Maximum XMOBILE Stations:	2400	0
Maximum Off-PBX Telephones - EC500:	9600	0
Maximum Off-PBX Telephones - OPS:	9600	18
Maximum Off-PBX Telephones - PBFMC:	9600	0
Maximum Off-PBX Telephones - PVFMC:	9600	0
Maximum Off-PBX Telephones - SCCAN:	0	0
Maximum Survivable Processors:	313	0
(NOTE: You must logoff & login to effect the permission changes.)		

On **Page 2** of the **System-Parameters Customer-Options** form, verify that the number of **Maximum Administered SIP Trunks** supported by the system is sufficient.

display system-parameters customer-options	Page	2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks:	4000	0
Maximum Concurrently Registered IP Stations:	1000	2
Maximum Administered Remote Office Trunks:	4000	0
Max Concurrently Registered Remote Office Stations:	1000	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Reg Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	2400	0
Maximum Video Capable IP Softphones:	1000	1
Maximum Administered SIP Trunks:	4000	50
Max Administered Ad-hoc Video Conferencing Ports:	4000	0
Max Number of DS1 Boards with Echo Cancellation:	80	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.1.2. Define System Features

Use the **change system-parameters features** command to administer system wide features for SIP endpoints. Those related to features listed in Error! Reference source not found. are shown in bold. These are all standard Communication Manager features that are also available to OPS stations. On **Page 18**, set the **Whisper Page Tone Given To** field to **all**.

```
display system-parameters features                                     Page 18 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

INTERCEPT TREATMENT PARAMETERS
    Invalid Number Dialed Intercept Treatment: tone
        Invalid Number Dialed Display:
    Restricted Number Dialed Intercept Treatment: tone
        Restricted Number Dialed Display:
    Intercept Treatment On Failed Trunk Transfers? n

WHISPER PAGE
    Whisper Page Tone Given To: all

6400/8400/2420J LINE APPEARANCE LED SETTINGS
    Station Putting Call On Hold: green    wink
        Station When Call is Active: steady
    Other Stations When Call Is Put On Hold: green    wink
        Other Stations When Call Is Active: green
            Ringing: green    flash
            Idle: steady

                                Pickup On Transfer? y
```

On **Page 19** make sure **Directed Call Pickup** is set to **y**.

```
display system-parameters features                                     Page 19 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

IP PARAMETERS
    Direct IP-IP Audio Connections? y          IP Audio Hairpinning? n
        Synchronization over IP? n Allow SIP-H323 Video in SDP? n
    Initial INVITE with SDP for secure calls? y
        SIP Endpoint Managed Transfer? n

    Expand ISDN Numbers to International for 1XCES? n

CALL PICKUP
    Maximum Number of Digits for Directed Group Call Pickup: 4
        Call Pickup on Intercom Calls? y          Call Pickup Alerting? y
    Temporary Bridged Appearance on Call Pickup? y          Directed Call Pickup? y
        Extended Group Call Pickup: simple
        Enhanced Call Pickup Alerting? n

    Call Pickup for Call to Coverage Answer Group? y
        Display Information With Bridged Call? n
    Keep Bridged Information on Multiline Displays During Calls? y
        PIN Checking for Private Calls? n
```

5.2. Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the **procr** and the Session Manager (**sm81xvmpg**). The host names will be displayed throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```
display node-names ip
                                IP NODE NAMES
      Name                      IP Address
IPOffice                      10.10.40.25
aes81xvmpg                    10.10.40.38
ams81vmpg                     10.10.40.39
default                        0.0.0.0
g430                          10.10.40.15
procr                        10.10.40.37
procr6                         ::
sm81xvmpg                   10.10.40.32
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.1.1**. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

```
display ip-network-region 1
                                IP NETWORK REGION
Region: 1
Location: 1      Authoritative Domain: devconnect.local
      Name: Default region
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
```

In the **IP Codec Set** form, select the audio codecs supported by the iTurret. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference. Note the **Media Encryption** includes a setting of **none** to allow for unencrypted media.

display ip-codec-set 1		Page 1 of 2	
IP MEDIA PARAMETERS			
Codec Set: 1			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711A	n	2	20
2: G.711MU	n	2	20
3: G.729A	n	2	20
4: G.722-64k	n	2	20
Media Encryption		Encrypted SRTCP: enforce-unenc-srtcp	
1: 1-srtp-aescm128-hmac80			
2: none			
3:			

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. The configuration of the Signaling group used to send calls from Communication Manager to Session Manager for SIP users is as follows.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the appropriate setting, in this case it was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm81xvmpg**).
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- **Far-end Domain** was set to the domain used during compliance testing.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- **Initial IP-IP Direct Media** is set to **n**.
- The default values for the other fields may be used.

change signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: sm81xvmpg	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: devconnect.local		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? Y	IP Audio Hairpinning? n	
	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

The Trunk Groups used to send calls between Communication Manager and Session Manager was setup as follows. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

change trunk-group 1		Page 1 of 21
TRUNK GROUP		
Group Number: 1	Group Type: sip	CDR Reports: y
Group Name: SIP TRK	COR: 1	TN: 1 TAC: *11
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	

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field was set to a value of 600 to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away. This may be changed if required by Speakerbus.

change trunk-group 1	Page 2 of 21
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
	Redirect On OPTIM Failure: 5000
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 600	
Disconnect Supervision - In? y Out? y	
XOIP Treatment: auto	Delay Call Setup When Accessed Via IGAR? n

Settings on **Page 3** can be left as default. However, the **Numbering Format** in the example below is set to **private**.

change trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private
	UUI Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

Settings on **Page 4** are as follows.

change trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? y	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

5.3. Configure Call Routing for SIP phones

For compliance testing all calls beginning with 11 with a total length of 4 digits were to be sent across the SIP trunk to Session Manager as all SIP phones begin with 11. Automatic Alternate Routing (aar) was used to route the calls.

5.3.1. Administer Dial Plan

Use the **change dialplan analysis** command to define the dial plan used in the system. This includes all telephone extensions, OPS Feature Name Extensions (FNEs), and Feature Access Codes (FACs). To define the FNEs for the OPS features listed in Error! Reference source not found., a Feature Access Code (FAC) must also be specified for the corresponding feature. In the sample configuration, telephone extensions are four digits long and begin with **1** and **2**, FNEs are also four digits beginning with **1**, and the FACs have formats as indicated with a **Call Type** of **fac**.

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	4	ext						
2	4	ext						
3	4	udp						
4	4	udp						
8	1	fac						
9	1	fac						
*	3	fac						

...# 3 fac

5.3.2. Administer Route Selection for SIP Phones

Use the **change aar analysis x** command to further configure the routing of the dialed digits. Calls to SIP phones begin with **11** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

change aar analysis 4							Page	1 of	2
AAR DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 1		
Dialed	Total		Route	Call	Node	ANI			
String	Min	Max	Pattern	Type	Num	Reqd			
11	4	4	1	lev0		n			

Use the **change route-pattern n** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 1** is used to route calls to trunk group (**Grp No**) **1**. This is the SIP Trunk configured in **Section 5.2**.

change route-pattern 1												Page	1 of	4	
Pattern Number: 1												Pattern Name: SIPPhones			
SCCAN? n												Secure SIP? n			
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC		
No			Mrk	Lmt	List	Del	Digits					QSIG			
												Intw			
1:	1	0										n	user		
2:												n	user		
3:												n	user		
4:												n	user		
5:												n	user		
	BCC VALUE		TSC	CA-TSC		ITC BCIE Service/Feature				PARM	No.	Numbering	LAR		
	0	1	2	M	4	W	Request						Dgts	Format	
1:	y	y	y	y	y	n	n	unre				lev0-pvt		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	

5.4. Define Feature Access Codes (FACs)

A FAC (feature access code) should be defined for each feature that will be used via the OPS FNEs. These are the FAC's that were used during compliance testing, these will be configured differently for every site. The FACs used in the sample configuration are shown in bold.

change feature-access-codes		Page	1 of 12
FEATURE ACCESS CODE (FAC)			
Abbreviated Dialing List1 Access Code:	*11		
Abbreviated Dialing List2 Access Code:	*12		
Abbreviated Dialing List3 Access Code:	*13		
Abbreviated Dial - Prgm Group List Access Code:	*10		
Announcement Access Code:	*27		
Answer Back Access Code:	#02		
Attendant Access Code:			
Auto Alternate Routing (AAR) Access Code:	8		
Auto Route Selection (ARS) - Access Code 1:	9	Access Code 2:	
Automatic Callback Activation:	*05	Deactivation:	#05
Call Forwarding Activation Busy/DA:	*03 All: *04	Deactivation:	#04
Call Forwarding Enhanced Status:	*73 Act: *74	Deactivation:	#74
Call Park Access Code:	*02		
Call Pickup Access Code:	*09		
CAS Remote Hold/Answer Hold-Unhold Access Code:			
CDR Account Code Access Code:	*14		
Change COR Access Code:			
Change Coverage Access Code:			
Conditional Call Extend Activation:		Deactivation:	
Contact Closure Open Code:		Close Code:	

display feature-access-codes		Page	2 of 12
FEATURE ACCESS CODE (FAC)			
Contact Closure Pulse Code:			
Data Origination Access Code:			
Data Privacy Access Code:			
Directed Call Pickup Access Code:	*29		
Directed Group Call Pickup Access Code:			
Emergency Access to Attendant Access Code:			
EC500 Self-Administration Access Codes:	*61 *62 *63 *64		
Enhanced EC500 Activation:	*60	Deactivation:	#60
Enterprise Mobility User Activation:		Deactivation:	
Extended Call Fwd Activate Busy D/A All:	*06	Deactivation:	#06
Extended Group Call Pickup Access Code:			
Facility Test Calls Access Code:			
Flash Access Code:			
Group Control Restrict Activation:		Deactivation:	
Hunt Group Busy Activation:	*30	Deactivation:	#30
ISDN Access Code:			
Last Number Dialed Access Code:	*08		
Leave Word Calling Message Retrieval Lock:	*15		
Leave Word Calling Message Retrieval Unlock:	#15:		

FEATURE ACCESS CODE (FAC)

Leave Word Calling Send A Message: *16
 Leave Word Calling Cancel A Message: #16
 Limit Number of Concurrent Calls Activation: *18 Deactivation: #18
 Malicious Call Trace Activation: *17 Deactivation: #17
 Meet-me Conference Access Code Change:
 Message Sequence Trace (MST) Disable:

 PASTE (Display PBX data on Phone) Access Code: *28
 Personal Station Access (PSA) Associate Code: *20 Dissociate Code: #20
Per Call CPN Blocking Code Access Code: *24
Per Call CPN Unblocking Code Access Code: #24
 Posted Messages Activation: Deactivation:
 Priority Calling Access Code: *07
 Program Access Code: *00

 Refresh Terminal Parameters Access Code: #28
 Remote Send All Calls Activation: #11 Deactivation:
 Self Station Display Activation:
Send All Calls Activation: *01 Deactivation: #01
 Station Firmware Download Access Code:

FEATURE ACCESS CODE (FAC)

Station Lock Activation: *71 Deactivation: #71
 Station Security Code Change Access Code: *22
 Station User Admin of FBI Assign: Remove:
 Station User Button Ring Control Access Code:
 Terminal Dial-Up Test Access Code:
 Terminal Translation Initialization Merge Code: *21 Separation Code: #22
 Transfer to Voice Mail Access Code: *23
 Trunk Answer Any Station Access Code:
 User Control Restrict Activation: Deactivation:
 Voice Coverage Message Retrieval Access Code:
 Voice Principal Message Retrieval Access Code:
Whisper Page Activation Access Code: *25
 3PCC H323 Override SIP Station Activation: Deactivation:

 PIN Checking for Private Calls Access Code:
 PIN Checking for Private Calls Using ARS Access Code:
 PIN Checking for Private Calls Using AAR Access Code:

5.5. Define Feature Name Extensions (FNEs)

The OPS FNEs can be defined using the **display off-pbx-telephone feature-name-extensions set 1** command. The following screens show in bold the FNEs defined for use with the sample configuration.

```
display off-pbx-telephone feature-name-extensions set 1      Page    1 of    3

EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME
      Set Name: PG

      Active Appearance Select:
            Automatic Call Back: 1301
      Automatic Call-Back Cancel: 1302
            Call Forward All:
      Call Forward Busy/No Answer:
            Call Forward Cancel:
            Call Park: 1303
            Call Park Answer Back: 1304
            Call Pick-Up: 1309
      Calling Number Block:
      Calling Number Unblock:
      Conditional Call Extend Enable:
      Conditional Call Extend Disable:
            Conference Complete:
            Conference on Answer:
            Directed Call Pick-Up: 1310
      Drop Last Added Party:
```

```
display off-pbx-telephone feature-name-extensions set 1      Page    2 of    3

EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME

      Exclusion (Toggle On/Off):
      Extended Group Call Pickup:
            Held Appearance Select:
            Idle Appearance Select:
            Last Number Dialed: 1305
            Malicious Call Trace:
      Malicious Call Trace Cancel:
            Off-Pbx Call Enable:
            Off-Pbx Call Disable:
            Priority Call:
            Recall:
            Send All Calls: 1306
            Send All Calls Cancel: 1307
            Transfer Complete:
            Transfer On Hang-Up:
            Transfer to Voice Mail:
            Whisper Page Activation: 1311
```

5.6. Configure Class of Service (COS)

The COS used for compliance testing is displayed below. Use the **change cos 1** command to set the appropriate service permissions to support OPS features (shown in bold). For the sample configuration a COS of **1** was used.

display cos-group 1																Page	1 of	2
CLASS OF SERVICE	COS Group: 1					COS Name: PG Default												
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
Auto Callback	n	y	y	n	y	n	y	n	y	n	y	n	y	n	y	n		
Call Fwd-All Calls	n	y	n	y	y	n	n	y	y	n	n	y	y	n	n	y		
Data Privacy	n	y	n	n	n	y	y	y	y	n	n	n	n	y	y	y		
Priority Calling	n	y	n	n	n	n	n	n	n	y	y	y	y	y	y	y		
Console Permissions	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Off-hook Alert	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Client Room	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Restrict Call Fwd-Off Net	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y		
Call Forwarding Busy/DA	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Personal Station Access (PSA)	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Extended Forwarding All	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Extended Forwarding B/DA	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Trk-to-Trk Transfer Override	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
QSIG Call Offer Originations	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Contact Closure Activation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		

display cos-group 1													Page	2 of	2	
	CLASS OF SERVICE															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
VIP Caller	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Masking CPN/Name Override	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Call Forwarding Enhanced	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y
Priority Ip Video	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Ad-hoc Video Conferencing	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
MOC Control:	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Match BCA Display To Principal	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
DCC Activation/Deactivation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Bridging Exclusion Override	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n

5.7. Configure Class of Restriction (COR)

The COR that was used during compliance testing is shown below. To use the Directed Call Pickup feature, the **Can Be Picked Up By Directed Call Pickup** and **Can Use Directed Call Pickup** fields must be set to **y**.

display cor 1	Page 1 of 43
CLASS OF RESTRICTION	
COR Number: 1	
COR Description: PG Default	
FRL: 0	APLT? y
Can Be Service Observed? y	Calling Party Restriction: none
Can Be A Service Observer? y	Called Party Restriction: none
Time of Day Chart: 1	Forced Entry of Account Codes? n
Priority Queuing? n	Direct Agent Calling? n
Restriction Override: none	Facility Access Trunk Test? y
Restricted Call List? n	Can Change Coverage? n
Access to MCT? y	Fully Restricted Service? n
Group II Category For MFC: 7	Hear VDN of Origin Annc.? n
Send ANI for MFE? n	Add/Remove Agent Skills? y
MF ANI Prefix:	Automatic Charge Display? n
Hear System Music on Hold? y	PASTE (Display PBX Data on Phone)? n
Can Be Picked Up By Directed Call Pickup? y	
Can Use Directed Call Pickup? y	
Group Controlled Restriction: inactive	

5.8. Coverage Path

The coverage path configuration is shown below. The default values shown for **Busy**, **Don't Answer**, and **DND/SAC/Goto Cover** can be used for the **Coverage Criteria**.

display coverage path 1		
COVERAGE PATH		
Coverage Path Number: 1		
Cvg Enabled for VDN Route-To Party? n	Hunt after Coverage? n	
Next Path Number:	Linkage	
COVERAGE CRITERIA		
Station/Group Status	Inside Call	Outside Call
Active?	n	n
Busy?	y	y
Don't Answer?	y	y
All?	n	n
DND/SAC/Goto Cover?	y	y
Holiday Coverage?	n	n
		Number of Rings: 4
COVERAGE POINTS		
Terminate to Coverage Pts. with Bridged Appearances? n		
Point1: h6	Rng: 4	Point2:
Point3:		Point4:
Point5:		Point6:

6. Configure Avaya Aura® Session Manager

This section describes aspects of the Session Manager configuration required for interoperating with Speakerbus. It is assumed that the Domains, Locations, SIP entities for each Session Manager, Communication Manager and Aura Messaging, Entity Links, Routing Policies, Dial Patterns and Application Sequences have been configured.

Session Manager is managed via System Manager. Using a web browser, access **<https://<ip-addr of System Manager>/SMGR>**. In the **Log On** screen, enter appropriate **User ID** and **Password** and click the **Log On** button.

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:
 [Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

Once logged in navigate to **Elements** and click on **Routing** highlighted below.

Avaya Aura® System Manager 8.0

Users | Elements | Services | Widgets | Shortcuts

System Resource Utilization

Alarms

Application State

Information

Shortcuts

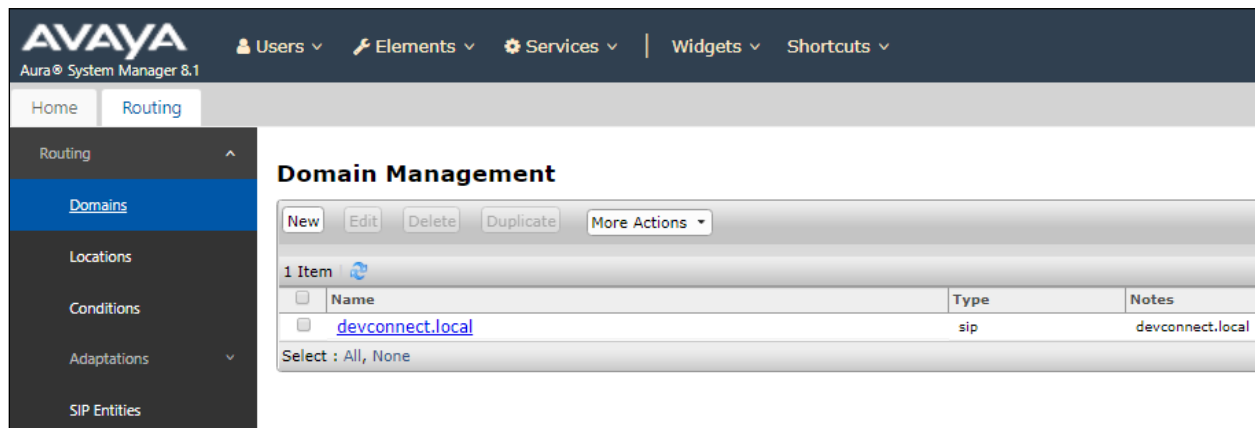
Routing

6.1. Domains and Locations

Note: It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

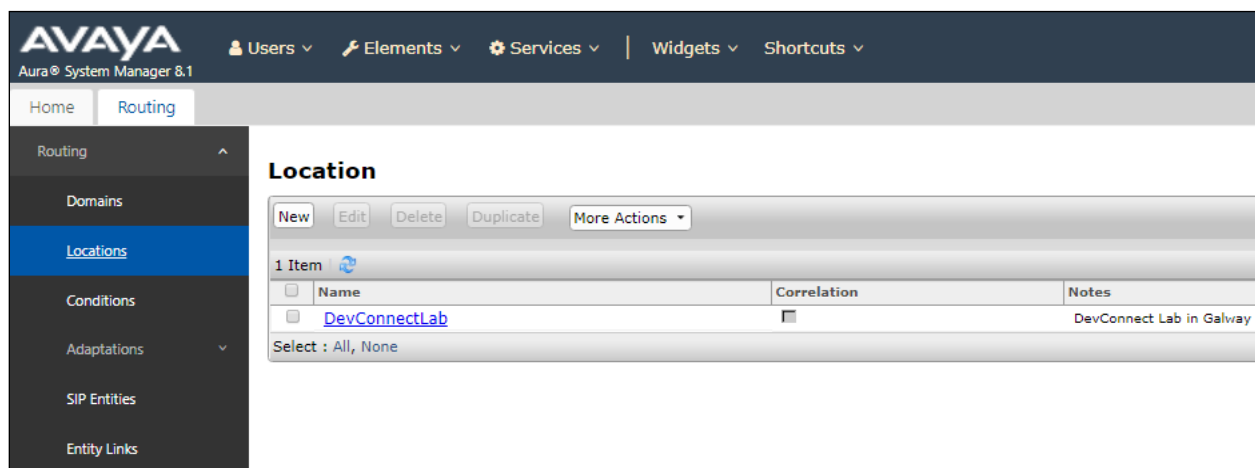
6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **devconnect.local** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.



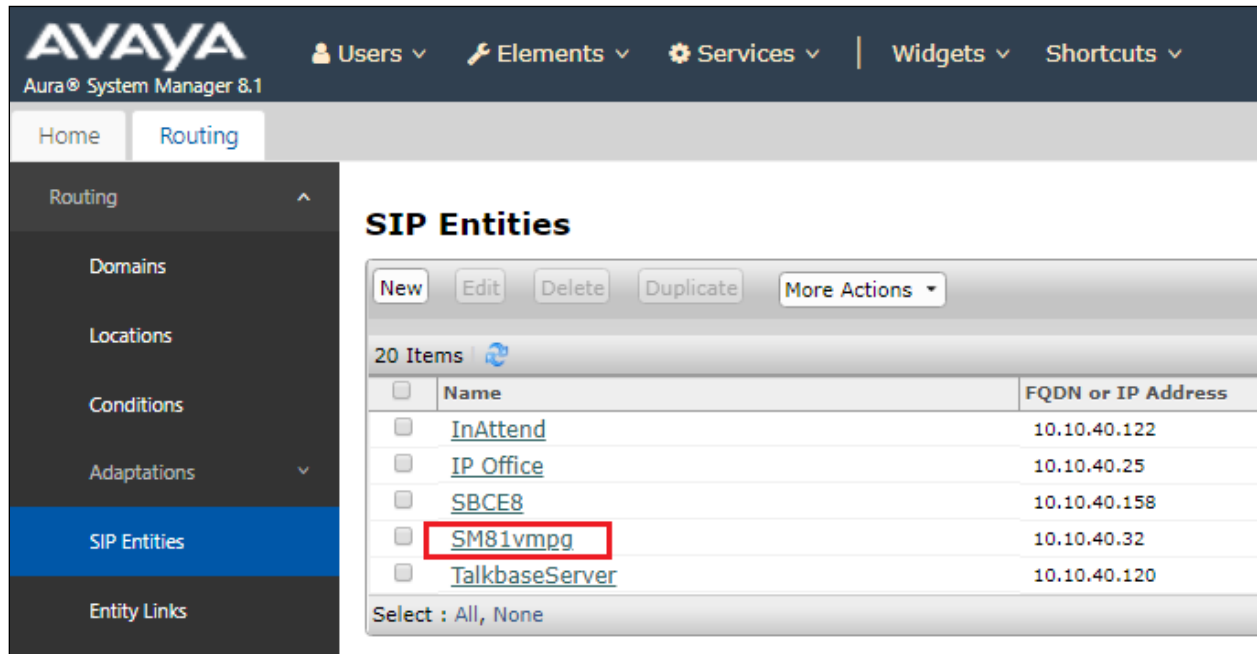
6.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab_PG** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.



6.2. Configure UDP Port for Speakerbus Registration

Each Session Manager Entity must be configured so that the iTurret can register to it using UDP. From the web interface click **Routing** → **SIP Entities** → <Session Manager> (SM81vmpg in the example below).

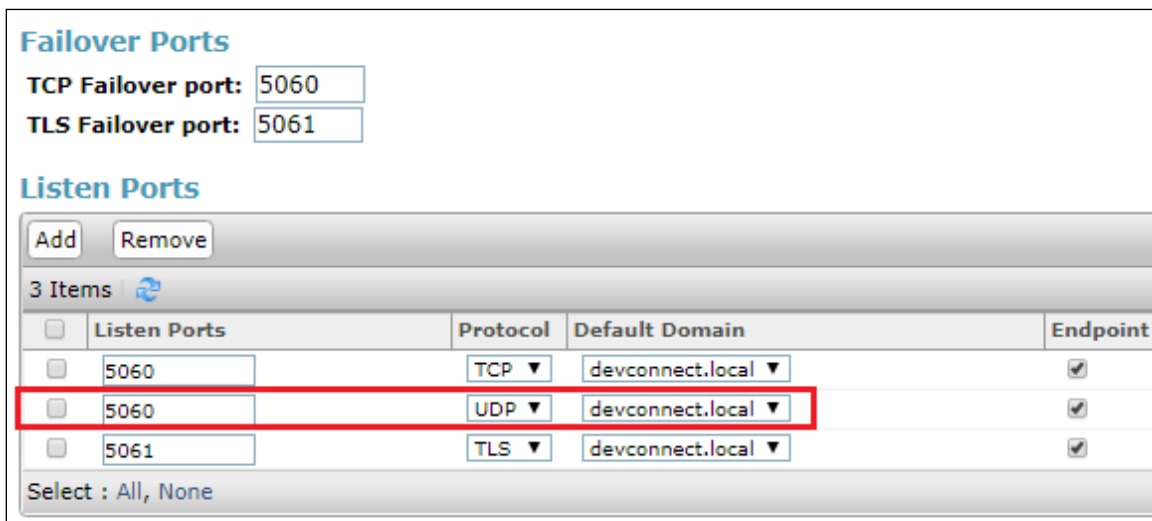


The screenshot shows the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Routing' menu with 'SIP Entities' selected. The main content area displays the 'SIP Entities' configuration page. It includes a table with 20 items, showing the following entities:

Name	FQDN or IP Address
InAttend	10.10.40.122
IP Office	10.10.40.25
SBCE8	10.10.40.158
SM81vmpg	10.10.40.32
TalkbaseServer	10.10.40.120

The 'SM81vmpg' entity is highlighted with a red box. Below the table, there is a 'Select : All, None' option.

In the **Port** section, ensure that port **5060** of type **UDP** is added as shown below. This is the port the iTurret sends its SIP registration to. Select the appropriate SIP domain from the drop-down list. Click **Commit** when done (not shown).



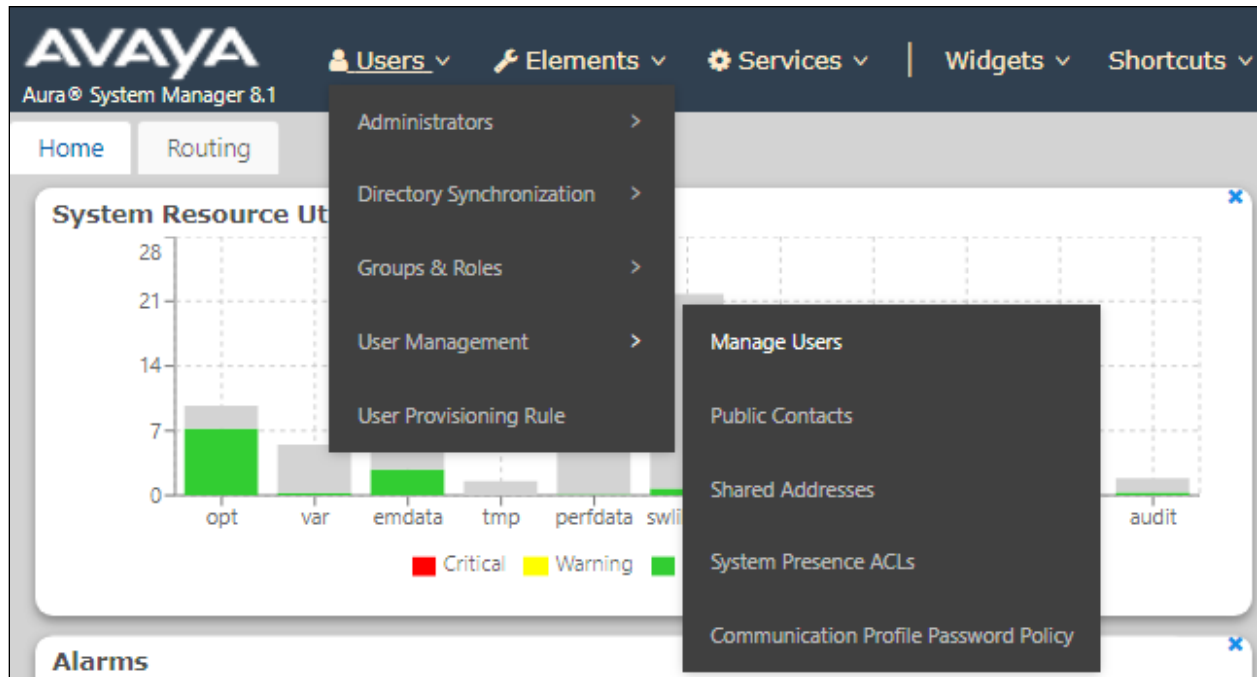
The screenshot shows the 'Listen Ports' configuration page. It includes a table with 3 items, showing the following ports:

Listen Ports	Protocol	Default Domain	Endpoint
5060	TCP	devconnect.local	✓
5060	UDP	devconnect.local	✓
5061	TLS	devconnect.local	✓

The row for port 5060 with protocol UDP is highlighted with a red box. Below the table, there is a 'Select : All, None' option.

6.3. Add Primary iTurret User

A user must be added for each iTurret. Click **User Management** → **Manage Users**. Click on **New**, (not shown).



The iTurret uses ‘bridged appearance’ to enable calls to be presented and picked up at different iTurret endpoints. A site may have a group of say five iTurrets all with each other’s extensions represented as bridged appearances so as each of them will display and can answer each other’s calls. This may be different on every site and in some cases perhaps only two out of the five may have bridged appearances there is no set rule on how the buttons should or would be configured. What is shown in the next section is one iTurret which has its own call appearance and bridged appearances of extensions 1161 and 1162. It also has bridged appearances of 1170 and 1171 which are ‘Privacy’ extensions used specifically for privacy.

A user of a multi-appearance telephone can activate Privacy, a Manual Exclusion to keep the participants with appearance of the same extension from bridging on to an existing call. To use manual exclusion, the user presses the privacy button, either before the user places the call, or when the user is active on the call. If the user presses the privacy button while others are bridged onto the call, the iTurret rejects the privacy request with a message but keeps the call active. To turn off manual exclusion, the user presses the privacy button.

Note: The following screens will display an existing user 1160, the screens will show an edited user instead of a new user but the information that is displayed is the very same as that required to add a new user.

Configure as following in the **Identity** tab.

- **First Name** and **Last Name** Enter an identifying name
- **Login Name** Enter the extension number followed by the domain, in this case **1160@devconnect.local**
- **Time Zone** Enter the appropriate time zone

The screenshot shows the 'User Profile | Edit | 1160@devconnect.local' form with the 'Identity' tab selected. The form contains various fields for user information. On the left, there is a sidebar with 'Basic Info' selected. The main form area has a 'User Provisioning Rule' dropdown. Below it, there are fields for 'Last Name' (User1), 'First Name' (Speakerbus), and 'Login Name' (1160@devconnect.local). There are also fields for 'Description', 'Password', 'Confirm Password', 'Endpoint Display Name' (User1, Speakerbus), 'Language Preference' (English (United States)), 'Employee ID', and 'Company'. On the right side, there are fields for 'Last Name (in Latin alphabet characters)' (User1), 'First Name (in Latin alphabet characters)' (Speakerbus), 'Middle Name' (Middle Name Of User), 'Email Address' (Email Address Of User), 'User Type' (Basic), 'Localized Display Name' (User1, Speakerbus), 'Title Of User' (Title Of User), 'Time Zone' ((0.0)GMT : Dublin, Edinburgh, L...), and 'Department' (Department Of User). At the top right, there are buttons for 'Commit & Continue', 'Commit', and 'Cancel'.

Click the **Communication Profile** tab and in the **Communication Profile Password** and **Confirm Password** fields, enter a numeric password. This will be used to register the iTurret during login. Click **OK** to continue.

The screenshot shows the 'User Profile | Edit | 1160@devconnect.local' form with the 'Communication Profile' tab selected. The form is dimmed, and a modal dialog box titled 'Comm-Profile Password' is open in the foreground. The dialog box has two input fields: 'Comm-Profile Password' and 'Re-enter Comm-Profile Password'. The 'Re-enter' field has a green checkmark icon next to it. Below the fields is a blue link that says 'Generate Comm-Profile Password'. At the bottom of the dialog box are 'Cancel' and 'OK' buttons. In the background, the 'Communication Profile' tab is active, showing a 'Communication Profile Password' section with a 'PROFILE SET : Primary' dropdown, a 'Communication Address' section, and a 'PROFILES' section with three toggle switches: 'Session Manager Profile' (on), 'Avaya Breeze® Profile' (off), and 'CM Endpoint Profile' (on).

Select **Avaya SIP** from the drop-down list. In the **Fully Qualified Address** field enter the extension number as required and select the appropriate **Domain** from the drop down list. Click **OK** when done.

The screenshot shows the 'User Profile | Edit | 1160@devconnect.local' interface. The 'Communication Profile' tab is active. On the left, the 'Communication Address' section is highlighted. A modal dialog box titled 'Communication Address Add/Edit' is open. It contains the following fields:

- * Type :** A dropdown menu with 'Avaya SIP' selected.
- *Fully Qualified Address :** Two input fields. The first contains '1160' and the second contains 'devconnect.local'.

At the bottom of the dialog are 'Cancel' and 'OK' buttons.

Place a tick in the **Session Manager Profile** bar and configure the **Primary Session Manager**.

The screenshot shows the 'User Profile | Edit | 1160@devconnect.local' interface. The 'Communication Profile' tab is active. On the left, the 'Session Manager Profile' toggle is turned on. The main area is titled 'SIP Registration' and contains the following configuration options:

- * Primary Session Manager :** A search field with 'SM81vmpg' entered.
- Secondary Session Manager :** A search field with 'Start typing...' entered.
- Survivability Server :** A search field with 'Start typing...' entered.
- Max. Simultaneous Devices :** A dropdown menu with '1' selected.

Configure the **Origination Application Sequence**, **Termination Application Sequence** and **Home Location**, this location should be that displayed in **Section 6.1.2**.

Application Sequences

Origination Sequence:

CMAPPSEQ

Termination Sequence:

CMAPPSEQ

Emergency Calling Application Sequences

Emergency Calling Origination Sequence:

Select

Emergency Calling Termination Sequence:

Select

Call Routing Settings

* Home Location:

DevConnectLab

Conference Factory Set:

Select

Call History Settings

Enable Centralized Call History?: ☐

Place a tick in the **CM Endpoint Profile** bar and configure as follows:

- **System** Select the relevant Communication Manager SIP Entity from the drop-down list
- **Profile Type** Select **Endpoint** from the drop-down list
- **Extension** Enter the required extension number, in this case **1160**
- **Template** Select **DEFAULT_9630SIP_CM_8_1** from the drop-down list
- **Port** Enter **IP**
- **Sip Trunk** This was set to **aar** for compliance testing

Click on the Endpoint Editor icon, highlighted, to open the Communication Manger configuration for this extension. This will allow the buttons to be administered as well as changes to Class of Service and Class of Restriction and other features.

User Profile | Edit | 1160@devconnect.local

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile ☒

Avaya Breeze® Profile ☐

CM Endpoint Profile ☒

* System: cm81xvmpg

* Profile Type: Endpoint

Use Existing Endpoints: ☐

* Extension: 1160

Template: 9630SIP_DEFAULT_CM_8_1

* Set Type: 9630SIP

Security Code: Enter Security Code

Port: IP

Voice Mail Number: 6666

Preferred Handle: Select

Calculate Route Pattern: ☒

Sip Trunk: aar

SIP URI: Select

Delete on Unassign from User or on Delete User: ☒

Override Endpoint Name and Localized Name: ☒

Allow H.323 and SIP Endpoint Dual Registration: ☐

Click on the **General Options** tab and enter the following:

- **Class of Restriction (COR)** Enter the **COR** as configured in **Section 5.7**
- **Emergency Location Ext** Enter **1160** (the extension for this user)
- **Tenant Number** Enter the appropriate **Tenant Number**
- **SIP Trunk** Enter **aar**
- **Class of Service (COS)** Enter the **COS** as configured in **Section 5.6**
- **Message Lamp Ext.** Enter **1160** (the extension for this user)
- **Coverage Path 1** If voicemail is being used then set this to the coverage path setup for voicemail, as per **Section 5.8**

Edit Endpoint Done

[Save As Template]

System	<input type="text" value="cm81xvmppg"/>	Extension	<input type="text" value="1160"/>
Template	<input type="text" value="9630SIP_DEFAULT_CM_8_1"/>	Set Type	<input type="text" value="9630SIP"/>
Port	<input type="text" value="IP"/>	Security Code	<input type="text"/>
Name	<input type="text" value="User1, Speakerbus"/>		

General Options (G) *
Feature Options (F)
Site Data (S)
Abbreviated Call Dialing (A)
Enhanced Call Fwd (E)

Button Assignment (B)
Group Membership (M)

<p>* Class of Restriction (COR) <input type="text" value="1"/></p> <p>* Emergency Location Ext <input type="text" value="1160"/></p> <p>* Tenant Number <input type="text" value="1"/></p> <p>* SIP Trunk <input type="text" value="aar"/></p> <p>Coverage Path 1 <input type="text"/></p> <p>Lock Message <input type="checkbox"/></p> <p>Multibyte Language <input type="text" value="Not Applicable"/></p>	<p>* Class Of Service (COS) <input type="text" value="1"/></p> <p>* Message Lamp Ext. <input type="text" value="1160"/></p> <p>Type of 3PCC Enabled <input type="text" value="None"/></p> <p>Coverage Path 2 <input type="text"/></p> <p>Localized Display Name <input type="text" value="User1, Speakerbus"/></p> <p>Enable Reachability for Station Domain Control <input type="text"/></p>
---	---

SIP URI

Primary Session Manager

IPv4: <input type="text"/>	IPv6: <input type="text"/>
----------------------------	----------------------------

Secondary Session Manager

IPv4: <input type="text"/>	IPv6: <input type="text"/>
----------------------------	----------------------------

Click on the **Feature Options** tab. The screen shot below shows the Feature Options that were used during compliance testing. Ensure that **Bridged Call Alerting** is ticked as shown below, the other features are ticked as default.

General Options (G) * **Feature Options (F)** Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E)

Button Assignment (B) Group Membership (M)

Active Station Ringing: single ▼

MWI Served User Type: None ▼

Per Station CPN - Send Calling Number: None ▼

IP Phone Group ID:

Remote Soft Phone Emergency Calls: as-on-local ▼

LWC Reception: spe ▼

AUDIX Name: None ▼

Speakerphone: 2-way ▼

Short/Prefixed Registration Allowed: default ▼

EC500 State: enabled ▼

Bridging Tone for This Extension: None ▼

Auto Answer Coverage After Forwarding: none ▼

Display Language: english ▼

Hunt-to Station:

Loss Group: 19

Survivable COR: internal ▼

Time of Day Lock Table: None ▼

Voice Mail Number: 6666

Music Source:

Features

- ☐ Always Use
- ☐ IP Audio Hairpinning
- ☒ Bridged Call Alerting
- ☐ Bridged Idle Line Preference
- ☒ Coverage Message Retrieval
- ☐ Data Restriction
- ☒ Survivable Trunk Dest
- ☐ Bridged Appearance Origination Restriction
- ☒ Restrict Last Appearance
- ☐ Turn on mute for remote off-hook attempt
- ☐ IP Hoteling
- ☐ Idle Appearance Preference
- ☐ IP SoftPhone
- ☒ LWC Activation
- ☐ CDR Privacy
- ☒ Precedence Call Waiting
- ☒ Direct IP-IP Audio Connections
- ☐ H.320 Conversion
- ☐ IP Video
- ☐ Per Button Ring Control

*Required

Done

Click on the **Button Assignments tab (Main Buttons)** and configure Buttons **1, 2** and **3** as **call-appr**. For compliance testing several bridged appearances were configured to test ‘Barge In’ and ‘Privacy’ buttons **4, 5** and **6** were set to extension **1161** and **7, 8** and **9** were set to **1162**.

General Options (G) *						Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)		Enhanced Call Fwd (E)	
Button Assignment (B)						Group Membership (M)							
Main Buttons													
1	call-appr ▼												
2	call-appr ▼												
3	call-appr ▼												
4	brdg-appr ▼	Button	1	Ext	1161								
5	brdg-appr ▼	Button	2	Ext	1161								
6	brdg-appr ▼	Button	3	Ext	1161								
7	brdg-appr ▼	Button	1	Ext	1162								
8	brdg-appr ▼	Button	2	Ext	1162								

Click on **Feature Buttons** and configure as per screen shot below. There were two SIP Users configured as 'Privacy Users' these were extensions 1170 and 1171. To allow this user (1160) use Privacy, the privacy extension must be added as bridged appearances on this user's buttons as shown below. Buttons **10, 11 and 12** were set to extension **1170** and **13, 14 and 15** were set to extension **1171**. (Click **Commit** when done (not shown). Other features such as Call Forward and Call Forward Busy Deactivated as well as Exclusion are also added as buttons as shown.

General Options (G) * Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E)							
Button Assignment (B) Group Membership (M)							
Main Buttons Feature Buttons Button Modules Phone View							
9	brdg-appr ▼	Button	3	Ext	1162	Ring	
10	brdg-appr ▼	Button	1	Ext	1170	Ring	
11	brdg-appr ▼	Button	2	Ext	1170	Ring	
12	brdg-appr ▼	Button	3	Ext	1170	Ring	
13	brdg-appr ▼	Button	1	Ext	1171	Ring	
14	brdg-appr ▼	Button	2	Ext	1171	Ring	
15	brdg-appr ▼	Button	3	Ext	1171	Ring	
16	None ▼						
17	None ▼						
18	None ▼						
19	None ▼						
20	None ▼						
21	None ▼						
22	call-fwd ▼	Extension					
23	cfwd-busyda ▼	Extension					
24	exclusion ▼						

Click on **Commit** at the top of the screen to save the new user.

The screenshot shows the 'Communication Profile' tab for user 1160. The left sidebar has 'CM Endpoint Profile' selected. The main form area contains various configuration fields:

- System:** cm81xvmpg
- Profile Type:** Endpoint
- Extension:** 1160
- Set Type:** 9630SIP
- Port:** S000005
- Preferred Handle:** Select
- Sip Trunk:** aar
- Use Existing Endpoints:** ☐
- Template:** Start typing...
- Security Code:** Enter Security Code
- Voice Mail Number:** 6666
- Calculate Route Pattern:** ☐
- SIP URI:** Select
- Enhanced Callr-Info Display for 1-line phones:** ☐
- Delete on Unassign from User or on Delete User:** ☒
- Override Endpoint Name and Localized Name:** ☒
- Allow H.323 and SIP Endpoint Dual Registration:** ☐

6.4. Configure Privacy Users

Privacy users are configured on System Manager as bridged appearances on the primary user. Add a 'Privacy User' in the same way as the primary user was configured in **Section 6.3**. Two privacy users 1170 and 1171 were created to be used by the primary user 1160. Following the same procedure as **Section 6.3**, under the **Identity** tab, enter a suitable **Name** and **Time Zone**.

The screenshot shows the 'Identity' tab for user 1170. The left sidebar has 'Basic Info' selected. The main form area contains various configuration fields:

- User Provisioning Rule:** (empty dropdown)
- Last Name:** Privacy User 1
- First Name:** Speakerbus
- Login Name:** 1170@devconnect.local
- Description:** Description Of User
- Password:** (empty field)
- Confirm Password:** (empty field)
- Endpoint Display Name:** Privacy User 1, Speakerbus
- Language Preference:** English (United States)
- Last Name (in Latin alphabet characters):** Privacy User 1
- First Name (in Latin alphabet characters):** Speakerbus
- Middle Name:** Middle Name Of User
- Email Address:** Email Address Of User
- User Type:** Basic
- Localized Display Name:** Privacy User 1, Speakerbus
- Title Of User:** Title Of User
- Time Zone:** (0:0)GMT : Dublin, Edinburgh, L...

A **Communication Profile** and **Session Manager Profile** are added as per **Section 6.3**, (not shown here). Click on **CM Endpoint Profile** and enter the same **Template** information, that being **9630SIP_DEFAULT_CM_8_1**. Enter the appropriate **Extension** number (**1170**) and click on the “configure extension” icon, highlighted on the screen below.

User Profile | Edit | 1170@devconnect.local

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile ☒

Avaya Breeze® Profile ☐

CM Endpoint Profile ☒

* System : cm\$txvmpg

Use Existing Endpoints : ☐

Template : 9630SIP_DEFAULT_CM_8_1

Security Code : Enter Security Code

Voice Mail Number :

Calculate Route Pattern : ☒

SIP URI : Select

Override Endpoint Name and Localized Name : ☒

* Profile Type : Endpoint

* Extension : 1170

* Set Type : 9630SIP

Port : IP

Preferred Handle : Select

Sip Trunk : aar

Delete on Unassign from User or on Delete User : ☒

Allow H.323 and SIP Endpoint Dual Registration : ☐

The same COR and COS that were selected for the primary user in **Section 6.3** can be used for this privacy user (not shown).

Click on the **Feature Options** tab. The screen shot below shows the Feature Options that were used during compliance testing. Ensure that **Bridged Call Alerting** is ticked as shown below, the other features are ticked as default.

General Options (G) * **Feature Options (F)** Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E)

Button Assignment (B) Group Membership (M)

Active Station Ringing: single ▼

MWI Served User Type: None ▼

Per Station CPN - Send Calling Number: None ▼

IP Phone Group ID:

Remote Soft Phone Emergency Calls: as-on-local ▼

LWC Reception: spe ▼

AUDIX Name: None ▼

Speakerphone: 2-way ▼

Short/Prefixed Registration Allowed: default ▼

EC500 State: enabled ▼

Bridging Tone for This Extension: None ▼

Auto Answer Coverage After Forwarding: none ▼

Display Language: english ▼

Hunt-to Station:

Loss Group: 19

Survivable COR: internal ▼

Time of Day Lock Table: None ▼

Voice Mail Number: 6666

Music Source:

Features

- ☐ Always Use
- ☐ IP Audio Hairpinning
- ☒ Bridged Call Alerting
- ☐ Bridged Idle Line Preference
- ☒ Coverage Message Retrieval
- ☐ Data Restriction
- ☒ Survivable Trunk Dest
- ☐ Bridged Appearance Origination Restriction
- ☒ Restrict Last Appearance
- ☐ Turn on mute for remote off-hook attempt
- ☐ IP Hoteling
- ☐ Idle Appearance Preference
- ☐ IP SoftPhone
- ☒ LWC Activation
- ☐ CDR Privacy
- ☒ Precedence Call Waiting
- ☒ Direct IP-IP Audio Connections
- ☐ H.320 Conversion
- ☐ IP Video
- ☐ Per Button Ring Control

*Required

Done

Click on the **Button Assignments tab (Main buttons)** and configure Buttons **1, 2 and 3** as **call-appr**. For compliance testing, buttons **4, 5 and 6** were configured as **brdg-appr** to extension **1160** (Primary iTurret User).

General Options (G) * Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E)				
Button Assignment (B) Group Membership (M)				
Main Buttons Feature Buttons Button Modules Phone View				
1	call-appr ▼			
2	call-appr ▼			
3	call-appr ▼			
4	brdg-appr ▼	Button 1	Ext 1160	
5	brdg-appr ▼	Button 2	Ext 1160	
6	brdg-appr ▼	Button 3	Ext 1160	
7	None ▼			
8	None ▼			

Click on the **Feature Buttons** tab and ensure that Exclusion is set on one of the buttons, in this case **Button 24** was configured as **exclusion**.

General Options (G) * Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E)				
Button Assignment (B) Group Membership (M)				
Main Buttons Feature Buttons Button Modules Phone View				
9	None ▼			
10	None ▼			
11	None ▼			
12	None ▼			
13	None ▼			
14	None ▼			
15	None ▼			
16	None ▼			
17	None ▼			
18	None ▼			
19	None ▼			
20	None ▼			
21	None ▼			
22	call-fwd ▼	Extension		
23	cfwd-busyda ▼	Extension		
24	exclusion ▼			

*Required

Done

7. Speakerbus iTurret Configuration

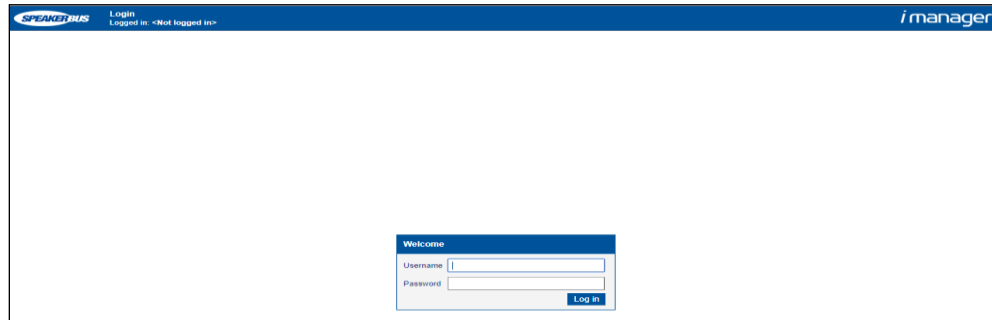
This section provides the procedure for configuring the Speakerbus iTurret via the iManager Centralised Management System (iCMS). The iCMS comprises of three components, the iManager web portal application, the iCMS communication service and the iCMS database. The iManager web portal application consists of a series of configuration web pages that allow administrators to manage the iTurret devices. The procedure for configuring an iTurret falls into the following areas.

- Launch iManager Web Portal
- Create/Verify User Policies
- Create/Verify Device Policies
- Create Network Services
- Create Site and Call Region
- Set up device defaults
- Announce iTurrets Deskstations
- Create Users
- Create PBX (SIP Server)
- Create Dial Plan
- Create Call and Privacy Appearances
- Assign User Permissions
- Assign Ownership (of Appearances to Users)
- Assign Default Call Appearances
- Program iTurret Layout Profiles
- Synchronize Deskstations

Note: This section displays some the configuration screens that may have already been configured.

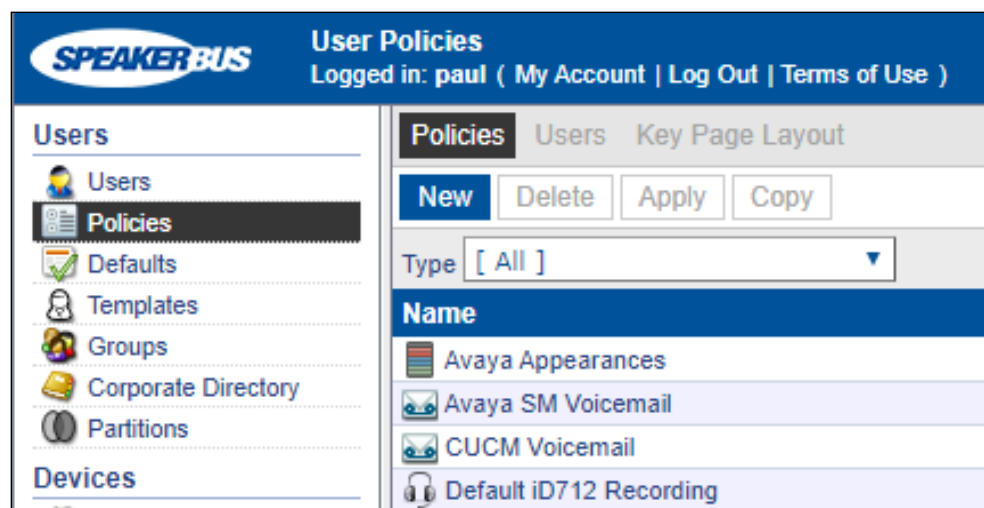
7.1. Launch iManager Web Portal

To access the iManager software interface, open a web browser and type the iManager web address, <http://<ServerIP>/imanager>. Enter the appropriate credentials and click **Log in**.

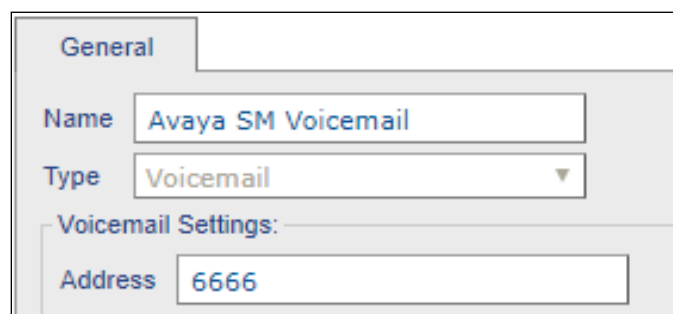


7.2. Creating/Verifying User policies

Select **Users** → **Policies** in the left pane and click on **New**.



Enter an identifying **Name**, in the **Type** dropdown box select **Voicemail**, and enter a valid address for the voicemail server, in this case a pre-configured hunt group number for voicemail access is used. Click **OK** once completed (not shown).



Select **Users** → **Policies** in the left pane. Select and view the **Default Privileges** policy, (no changes to this should be required, however, it is referred to later in these Application Notes).

SPEAKERBUS User Policies
 Logged in: paul (My Account | Log Out | Terms of Use)

Users

- Users
- Policies**
- Defaults
- Templates
- Groups
- Corporate Directory
- Partitions

Devices

- Deskstations
- Gateways
- CloudBase
- Policies
- Defaults

Call Servers

- PBXs
- PBX Appearances

Network

- Sites
- Call Regions
- Voice Services
- Network Services

Security

- Administrators
- Roles

System

- Preferences
- Audit Log
- Reports
- System
- Licensing

Policies Users Key Page Layout

New Delete Apply Copy

Type [All]

Name
Avaya Appearances
Avaya SM Voicemail
CUCM Voicemail
Default iD712 Recording
Default iDUCX Recording
Default iTurret Recording
Default Preferences
Default Privileges
Default SE708 Recording
iCS Appearances
No recording
No recording (aria)
Voice Services

K < Page: 1 > X

General	iTurret
Allow Group Talk Barge	<input checked="" type="checkbox"/>
Allow Call Forwarding	<input checked="" type="checkbox"/>
Allow # To Complete Dialling	<input checked="" type="checkbox"/>
Allow Do Not Disturb	<input checked="" type="checkbox"/>
Allow User Page Editing	<input checked="" type="checkbox"/>
Allow Fixed Key Editing	<input checked="" type="checkbox"/>
Allow Alert Profile Editing	<input checked="" type="checkbox"/>
Allow Personal Directory Editing	<input checked="" type="checkbox"/>
Allow CTI	<input checked="" type="checkbox"/>
Allow SIPTAPI	<input checked="" type="checkbox"/>
Allow Recording Tone Control	<input checked="" type="checkbox"/>

Select **Users** → **Policies** in the left pane. Select the **Default Preferences** policy, click the **iTurret** tab and review the default settings (no changes should be needed to these; however, they are referred to later in these Application Notes).

The screenshot displays the SPEAKERBUS User Policies management interface. The left-hand navigation pane shows a tree structure with categories: Users, Policies (selected), Defaults, Templates, Groups, Corporate Directory, Partitions, Devices, Call Servers, Network, Security, and System. Under the Policies category, several policies are listed, including 'Default Preferences', which is currently selected. The main content area shows a list of policies with columns for Name and Type. Below the list, there are tabs for 'General' and 'iTurret'. The 'iTurret' tab is active, showing various configuration settings for the iTurret feature, such as Display Language, Time Display Format, Conferencing Mode, and Screen Saver settings. The interface is logged in as 'paul' and includes links for 'My Account', 'Log Out', and 'Terms of Use'.

7.3. Creating/Verifying Device Policies

Select **Devices** → **Policies** in the left pane. Select the **Default RTP Media & SIP** policy (no changes should be needed to these; however, they are referred to later in these Application Notes).

The screenshot displays the SPEAKERBUS web interface for managing Device Policies. The left sidebar contains a navigation menu with categories: Users, Devices, Call Servers, Network, Security, and System. The 'Policies' option under the 'Devices' category is selected. The main content area shows a list of policies, with 'Default RTP Media & SIP' highlighted. Below the list, the configuration details for this policy are shown in a 'General' tab. The policy name is 'Default RTP Media & SIP' and its type is 'RTP Media & SIP'. The RTP Media Settings include 'Time To Live' (120), 'DSCP Value' (0), and 'RTCP DSCP Value' (0). The SIP RTP Media Settings include 'Preferred Codec' (G.711 A-Law), 'Preferred Intercom Codec' (G.711 A-Law), 'Preferred ARIA Codec' (G.711), and 'Voice Activity Detection' (unchecked). The SIP Signalling Settings include 'Allow UDP SIP Signalling' (checked) and 'DSCP Value' (0).

SPEAKERBUS Device Policies
Logged in: paul (My Account | Log Out | Terms of Use)

Users
Users
Policies
Defaults
Templates
Groups
Corporate Directory
Partitions

Devices
Deskstations
Gateways
CloudBase
Policies
Defaults

Call Servers
PBXs
PBX Appearances

Network
Sites
Call Regions
Voice Services
Network Services

Security
Administrators
Roles

System
Preferences
Audit Log
Reports
System
Licensing

Policies Devices Collections
New Delete Apply Copy
Type [All]
Name
Default Call Logging
Default Device Recording
Default Digital E1 Trunk
Default Digital T1 Trunk
Default Ethernet Port
Default Gateway RTP
Default iCMS Connection
Default iD712 Recording
Default iDUCX Recording
Default iTurret Ethernet Ports
Default iTurret Recording
Default RTP Media & SIP
Default SbRTP
Default SE708 Recording
Default SNMP
No Logging
No Recording

Page: 1

General
Name: Default RTP Media & SIP
Type: RTP Media & SIP
RTP Media Settings:
Time To Live: 120
DSCP Value: 0
RTCP DSCP Value: 0
SIP RTP Media Settings:
Preferred Codec: G.711 A-Law
Preferred Intercom Codec: G.711 A-Law
Preferred ARIA Codec: G.711
Voice Activity Detection: ☐
SIP Signalling Settings:
Allow UDP SIP Signalling: ☒
DSCP Value: 0

Staying on Policies, select and view the **Default SbRTP** policy (no changes should be needed to these; however they are referred to later in these Application Notes).

The screenshot displays the Avaya iTurret configuration interface. At the top, there are tabs for 'Policies', 'Devices', and 'Collections'. Below these are buttons for 'New', 'Delete', 'Apply', and 'Copy'. A 'Type' dropdown menu is set to '[All]'. A list of policies is shown, with 'Default SbRTP' highlighted. Below the list, there are navigation controls including 'Page: 1 2' and a search icon. The 'General' tab is selected for the 'Default SbRTP' policy. The configuration fields are as follows:

General	
Name	Default SbRTP
Type	SbRTP Media
SbRTP Media Settings:	
RTP Payload Code	96
Time To Live	1
DSCP Value	0
Bandwidth	Standard
Packet Size	4 ms
Voice Activity Detection	<input checked="" type="checkbox"/>
Lost Packet Tolerance (%)	50
Sample Slip Tolerance (%)	100
iSeries Compatibility	Version 3.0
SbRTP Inactivity Timeout	500 ms
RTCP Keep Alive	<input type="checkbox"/>

7.4. Creating Network Services

A network service is an addressable entity that a device uses to contact the relevant service when and where required. Defining network services here merely defines the network service configuration, it does not cause it to be used by any devices. Network services can be assigned to devices via the device configuration or via a policy, depending on the network service type.

To create an NTP Server, select **Network** → **Network Services** in the left pane, click **New** and select NTP Server from the dropdown menu (later not seen).

Network Services
Logged in: neith (My Account | Log Out | Terms of Use) TRIAL LICENCE: 59 DAYS LEFT

Users
Users
Policies
Defaults
Templates
Groups
Corporate Directory
Partitions

Devices
Desktops
Gateways
CloudBase
Policies
Defaults

Call Servers
PBXs
PBX Appearances
Policies

Network
Sites
Call Regions
Voice Services
Network Services

Network Services
Devices
Call Regions
Collections

New Delete Apply

Type [All] Status [All]

Name	Type	Private Address
CMS Comms	iCMS Communications Server	10.10.40.73

Page: 1

General

Complete the following fields:

- **Name** Enter a descriptive name for the site
- **Private Address** Enter the ip address of the NTP server

Note: Refer to the *Speakerbus iManager Administrator's Guide*.

Click **OK** once completed.

7.5. Creating Site and Call Region

A site represents the location where the Speakerbus iSeries equipment is installed. To create a Site, select **Network** → **Sites** in the left pane, click **New**.

Note 1: A Default Site is available and can be used if required.

The screenshot shows the 'Sites' configuration page in the Speakerbus iSeries interface. The left sidebar contains a tree view with the following categories and items:

- Users**
 - Users
 - Policies
 - Defaults
 - Templates
 - Groups
 - Corporate Directory
 - Partitions
- Devices**
 - Deskstations
 - Gateways
 - CloudBase
 - Policies
 - Defaults
- Call Servers**
 - PBXs
 - PBX Appearances
 - Policies
- Network**
 - Sites** (selected)
 - Call Regions
 - Voice Services
 - Network Services

The main content area has a top bar with 'New', 'Delete', and 'Apply' buttons. Below this is a 'Name' field with a dropdown menu showing 'Default Site'. There are navigation buttons (K, <, >, X) and a search icon. The bottom section is labeled 'General'.

Complete the following fields:

- **Name** Enter a descriptive name for the site
- **Remote Site** Leave unticked for most cases

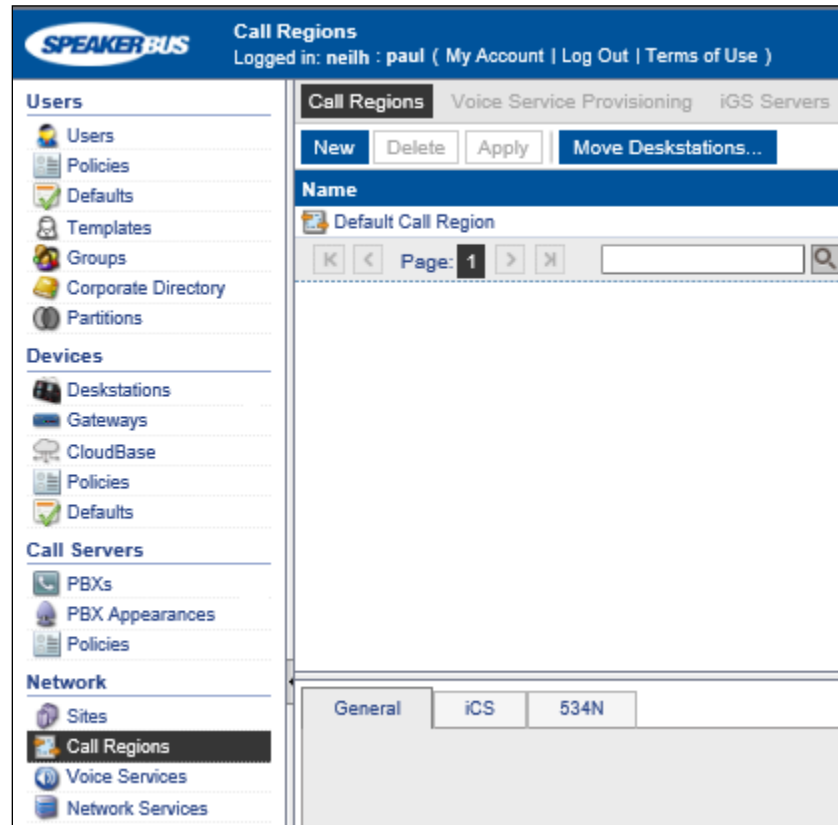
Click **OK** once completed.

Note 2: Only tick remote site when using an iTurret device at home connecting to a corporate network via a VPN link.

A call region represents part of an organisation's network over which all devices associated with the call region can communicate call audio and call signalling.

To create a Call Region, select **Network** → **Call Region** in the left pane, click **New**.

Note 3: A Default Call Region is available and can be used if required.



Complete the following fields:

- **Name** Enter a descriptive name for the call region
- **Partition Checking** Leave unticked for most cases
- **Priority for P2P** Leave unticked for most cases
- **IGMP Auto-leave** Leave unticked for most cases
- **DMVS Intercom Calls** Leave unticked for most cases

Note: Refer to the *Speakerbus iManager Administrator's Guide*.

Click **OK** once completed.

7.6. Check Device Defaults

The default configuration is used when a new device is created either from an auto-announce or from iManager. Select **Device** → **Defaults** in the left pane.

The screenshot shows the 'Device Defaults' configuration page in the Speakerbus iManager. The left sidebar has a 'Users' section and a 'Devices' section. The 'Devices' section is expanded, showing 'Defaults' selected. The main area has tabs for 'General', 'CloudBase', 'IP', 'Network', 'Management', 'Deskstation', 'Gateway', and 'Recording'. The 'General' tab is active, showing fields for 'Site' (Default Site), 'Call Region' (Default Call Region), 'iG330 Configuration Mode' (Device Web Page), 'Firmware' (None), and a table for 'Filenames' with columns 'Type', 'Enabled', and 'Filename'. The table has one row for 'iD100' with 'Enabled' checked and 'Filename' 'iD100_UG_x_xxx_x_x.r0'.

Confirm the following fields are set:

General Tab

- **Site** Set with what created in **Section 7.5**
- **Call Region** Set with what created in **Section 7.5**

IP Tab

- **NTP Server** Set with what created in **Section 7.4**

Network Tab

- **SbRTP Media Policy** is set to **Default SbRTP**
- **RTP Media Policy** is set to **Default RTP Media & SIP** (use the link to go to the policy to change the audio codec used, default is G.711 A-law)
- **Ethernet Ports Policy** is set to **Default Ethernet Ports**
- **Time zone** is set to the relevant time zone

Management Tab

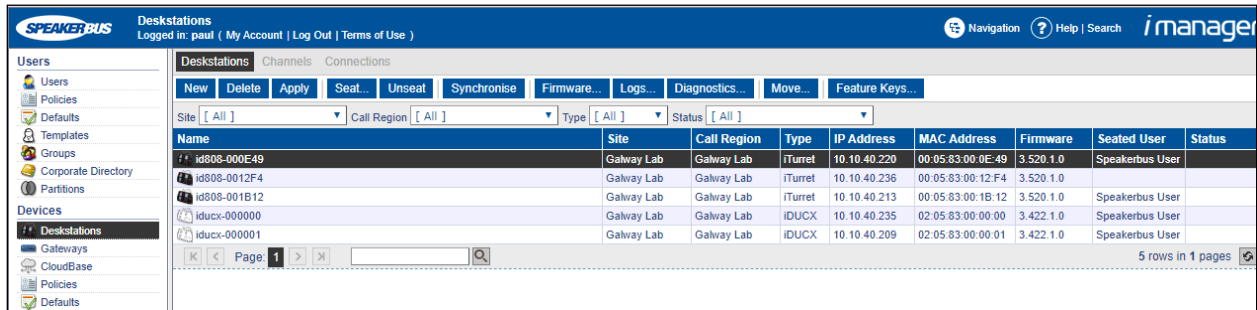
- **iCMS Communication Policy** is set to the default
- **iCMS Communication Server** is set to Auto-Locate iCMS if using DHCP / DNS
- **Enable Live Updates** Ticked

Note: Refer to the *Speakerbus iManager Administrator's Guide*.

Click **APPLY** once completed.

7.7. Announce iTurret Deskstation

The iTurret deskstations will automatically announce to the iCMS server if appropriate **DHCP** and **DNS** records were created prior to the iTurret deskstations being connected to the IP network and powered up. To view the newly registered deskstations, select **Devices** → **Deskstations** in the left pane, confirm they are seen as below.

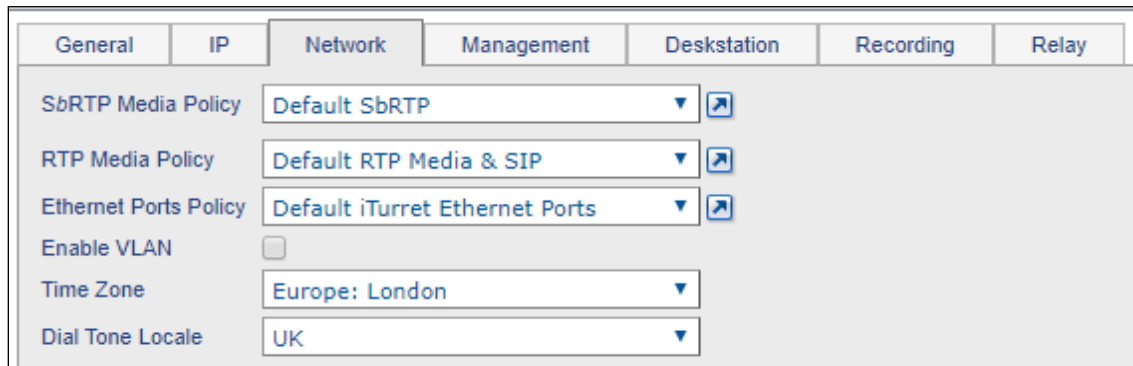


The screenshot shows the iManager interface with the 'Deskstations' tab selected. The left sidebar shows 'Users' and 'Devices' sections. The main area displays a table of registered deskstations.

Name	Site	Call Region	Type	IP Address	MAC Address	Firmware	Seated User	Status
id808-000E49	Galway Lab	Galway Lab	iTurret	10.10.40.220	00:05:83:00:0E:49	3.520.1.0	Speakerbus User	
id808-0012F4	Galway Lab	Galway Lab	iTurret	10.10.40.236	00:05:83:00:12:F4	3.520.1.0	Speakerbus User	
id808-001B12	Galway Lab	Galway Lab	iTurret	10.10.40.213	00:05:83:00:1B:12	3.520.1.0	Speakerbus User	
iducx-000000	Galway Lab	Galway Lab	iDUCX	10.10.40.235	02:05:83:00:00:00	3.422.1.0	Speakerbus User	
iducx-000001	Galway Lab	Galway Lab	iDUCX	10.10.40.209	02:05:83:00:00:01	3.422.1.0	Speakerbus User	

In the **Network** tab, verify the following are configured as mentioned above:

- **SbRTP Media Policy** is set to **Default SbRTP**
- **RTP Media Policy** is set to **Default RTP Media & SIP** (use the link to go to the policy to change the audio codec used, default is G.711 A-law)
- **Ethernet Ports Policy** is set to **Default Ethernet Ports**

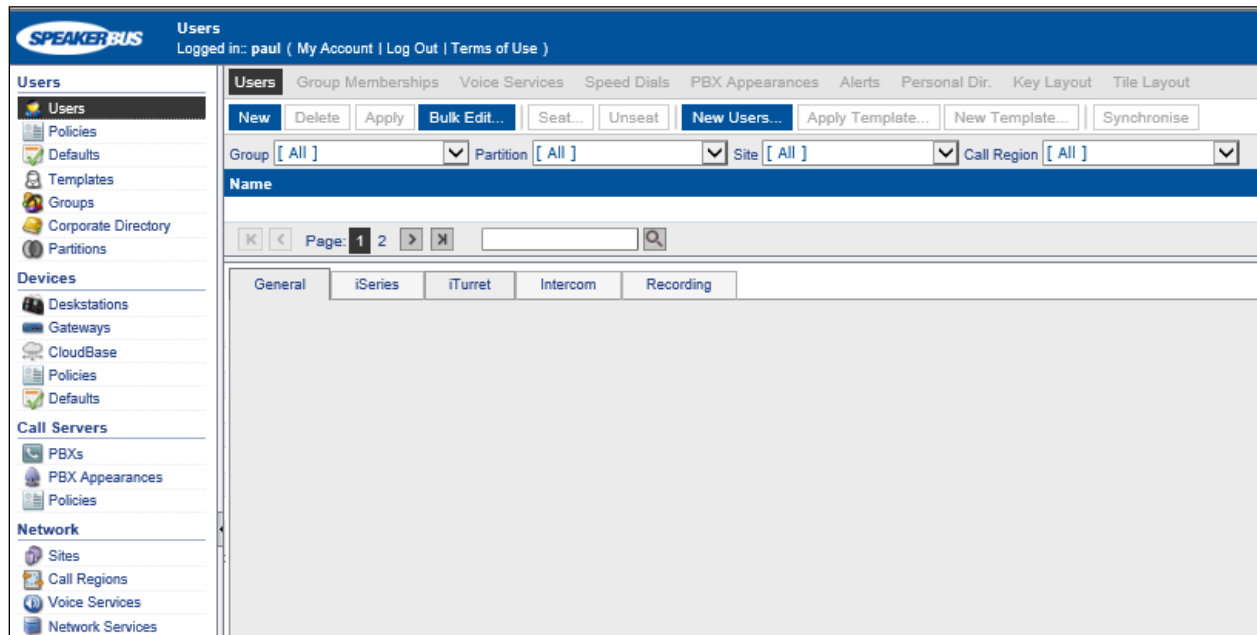


The screenshot shows the 'Network' configuration tab with the following settings:

General	IP	Network	Management	Deskstation	Recording	Relay
SbRTP Media Policy	Default SbRTP					
RTP Media Policy	Default RTP Media & SIP					
Ethernet Ports Policy	Default iTurret Ethernet Ports					
Enable VLAN	<input type="checkbox"/>					
Time Zone	Europe: London					
Dial Tone Locale	UK					

7.8. Create Users

To create a User, select **Users** → **Users**, click **New**.



Confirm the following fields are set:

General Tab

- **Name** Enter a descriptive name for the call region
- **Privileges Policy** This should be set to the default in **Section 7.2**
- **Preferences Policy** This should be set to the default in **Section 7.2**

iTurret Tab

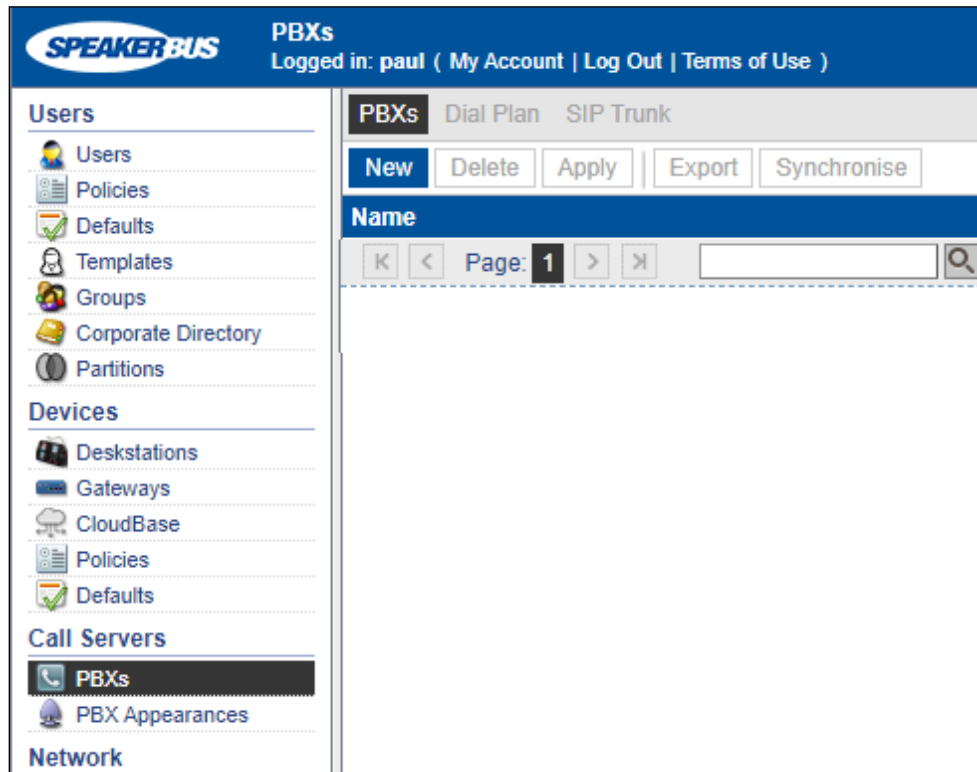
- **Logon Name** Enter a relevant logon name (8 – 16 characters in length)
- **Logon Password** Enter a relevant logon password
- **Verify Password** Enter a relevant logon password (should match above)
- **Voicemail Policy** This should be set to the policy in **Section 7.2**

All other areas can be left at defaults (refer to the *Speakerbus iManager Administrator's Guide*).

Click **OK** once completed.

7.9. Create PBX (SIP Server)

To create a PBX, select **Call Servers** → **PBXs**, click **New**.



Complete the following fields:

- **Name** Enter a descriptive name for the SIP/PBX server
- **Type** Select **Avaya** from the dropdown list
- **Port** Enter **5060**
- **Registrar Address** Enter the IP address of the Primary Session Manager security module
- **SIP Domain** Enter the appropriate SIP Domain

Note 1: A server locator record (SRV) for the registrar address and SIP domain may be created on DNS if the registrar address is set to **devconnect.local**, in the example below it will not be required. Refer to the *Speakerbus iManager Administrator's Guide* for the correct configuration of DNS.

Note 2: If using failover, then a second PBX will be created and added to the **Secondary PBX** dropdown box.

General	Inbound	Outbound
General:		
Name	Galway SM	
Type	Avaya	
Port	5060	
Avaya PBX Settings:		
Registrar Address	10.10.40.32	
SIP Domain	devconnect.local	
Secondary PBX	[None]	
Tertiary PBX	[None]	
Registration Delay (s)	30	
Registration Timeout (s)	30	
Registration Attempts	3	
Ad-Hoc Conferencing	<input type="checkbox"/>	

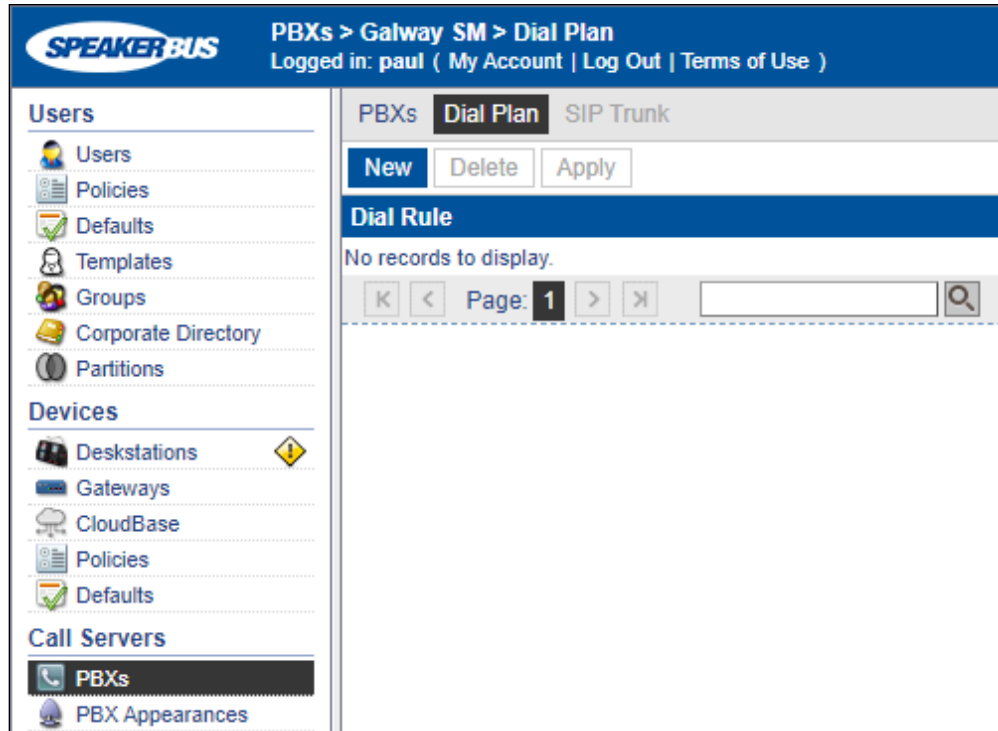
The **Outbound** and **Inbound** tabs are left with their default values, Click **OK** (not shown).

General	Inbound	Outbound
Internal:		
Length	4	
Prefix		
Local:		
Length	4	
Prefix		
National:		
Length	10	
Prefix		
International:		
Prefix		

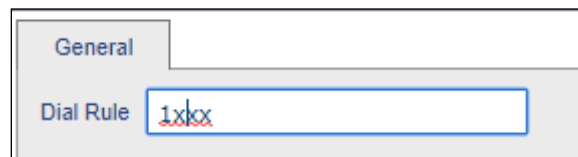
General	Inbound	Outbound
Internal:		
Length	4	
Prefix		
Local:		
Length	6	
Prefix		
National:		
Length	11	
Prefix		
International:		
Access Code	00	
Prefix		

7.10. Create Dial Plan

To create a PBX specific dial plan, select **Call Servers** → **PBXs**, select the **Dial Plan** tab, click **New**.



Under the **General** tab fill in the **Dial Rule**. Press **OK** when completed.



Repeat this for all valid extension formats.

7.11. Create Call and Privacy Appearances

Three call appearances must be created for each iTurret device. One is for the main appearance, and one for each of the privacy appearances (handset 1 and handset 2). As previously explained, three extensions are configured in System Manager for this purpose. To create the main appearance, click **Call Servers → PBX Appearances** in the left pane, click on **New**.

The screenshot shows the Speakerbus web interface for managing PBX Appearances. The left sidebar contains a navigation menu with categories: Users, Devices, Call Servers, and Network. Under 'Call Servers', 'PBX Appearances' is selected. The main content area has a header 'PBX Appearances' with a login status 'Logged in: paul (My Account | Log Out | Terms of Use)'. Below the header are tabs for 'PBX Appearances', 'User Permissions', and 'Group Permissions'. The 'PBX Appearances' tab is active, showing a list of appearances. At the top of the list are buttons for 'New', 'Delete', 'Apply', 'Assign Ownership...', and 'Clear Ownership'. Below these are dropdown menus for 'PBX' (set to '[All]') and 'Type' (set to '[All]'). The list of appearances includes: Matt Cheattle, Neil Higgs, Paul Greaney, Russell McLean, Speakerbus User PV1, Speakerbus User PV1, Speakerbus User PV2, Speakerbus User PV2, Speakerbus User 1 (highlighted), Speakerbus User 2, Speakerbus User 3, Speakerbus User 4, Speakerbus User 5, and Tim Game. At the bottom of the list is a pagination control showing 'Page: 1' and a search icon.

Select the PBX created in **Section 7.5** (in this case **Galway SM**), then select the **Type** of appearance to be created (which is **Call** in this case) and configure the following under the **General** tab:

- Provide a descriptive name for the appearance in the **Name** field, such as the extension or user's name.
- Set the **Long Label** field to the label that will be displayed for the call appearance button on the iTurret deskstation. The **Address** field should also be set to the appearance extension.
- Set the **Maximum Appearance** field to the number of call appearances configured on the station in System Manager (the number of call appearance buttons dictates the number of calls on the system the user can have directed to them). When all of the call appearances are not idle the user is considered busy and no further calls can be routed to them. Up to a

maximum of 10 call appearances may be configured on Communication Manager for each iTurret deskstation.

- Check the **Message Indication** checkbox for voice mail purposes and the **Allow Outbound Calls**.
- The **Authentication Name** and **Authentication Password** fields should be set to the extension and password configured on System Manager in **Section 6.3**. These are the credentials that the iTurret deskstation will use to authenticate and register with Session Manager. Use the default values for the other fields. Click **OK** (not shown).

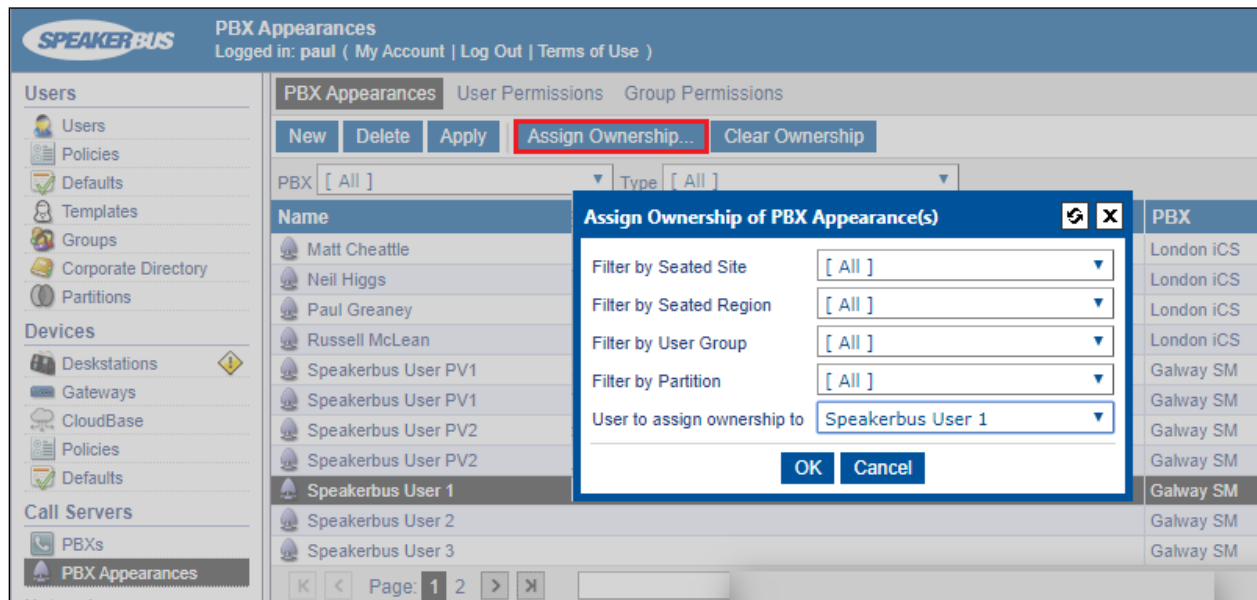
The screenshot shows the 'General' tab of a configuration window. At the top, there's a 'PBX' dropdown menu set to 'Galway SM' and a 'Type' dropdown menu set to 'Call'. Below these is a section titled 'Call Appearance Settings:'. It contains several fields: 'Name' (Speakerbus User 1), 'Long Label' (empty), 'Address' (1160), 'Maximum PBX Appearances' (3), 'Outbound Calls' (Allow All), 'Message Indication' (checked checkbox), and 'Authentication Name' (1160). At the bottom right of this section is a blue button labeled 'Change PBX Authentication Password...'.

Repeat the procedure for the two corresponding privacy appearances. Click the **New** button to add another appearance. In the **General** tab select the **PBX** created in **Section 7.5**, set the **Type** field to **Privacy 1** and complete the **Address**, **Authentication Name** and **Authentication Password** fields. The last two fields should be identical to the setup in System Manager for registration to occur. Press **OK** (not shown) to commit the created appearance.

The screenshot shows the 'General' tab of a configuration window for a privacy appearance. The 'PBX' dropdown is set to 'Galway SM' and the 'Type' dropdown is set to 'Privacy 1'. Below is a section titled 'Privacy Appearance Settings:'. It contains fields: 'Name' (Speakerbus User PV1), 'Long Label' (Speakerbus User 1 PV1), 'Address' (1170), and 'Authentication Name' (1170). A blue button labeled 'Change PBX Authentication Password...' is at the bottom right.

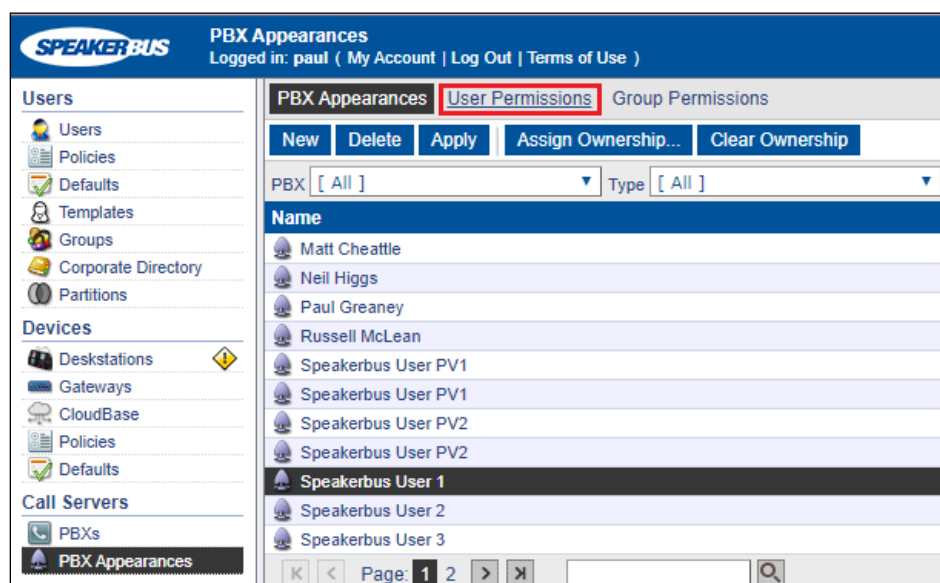
7.12. Assign Ownership

Appearance ownership must be assigned to a user as it enables the iTurret to distinguish between the owner of the call appearance as opposed to someone who is bridged on to that appearance. Select **Call Servers** → **PBX Appearances** in the left pane and click on the **Assign Ownership** button. Filter accordingly and select the user from the **User to assign ownership to** drop down list. Click **OK**.



7.13. Assign User Permissions

Appearance permissions must be assigned to the created users. Select **Call Servers** → **PBX Appearances** in the left pane, select the **Call Appearance** from the list, and select the **User Permissions** tab at the top of the page.



Select the user to give permissions to and select **Allow** from the **Permissions** drop down list and click **Apply**.

PBX Appearances **User Permissions** Group Permissions

Apply

Group [All] Partition [All] Site [All] Call Region

Name

- Speakerbus User 1
- Speakerbus User 2
- Speakerbus User 3
- Speakerbus User 4
- Speakerbus User 5

Page: 1

General

Permission Allow

7.14. Set Default Appearance

Select **Users** → **Users** in the left pane.

SPEAKERBUS Users Logged in: paul (My Account | Log Out | Terms of Use) Navigation Help Search iManager

Users Group Memberships Voice Services Speed Dials PBX Appearances Alerts Personal Dir. Key Layout Tile Layout

New Delete Apply Seat... Unseat New Users... Apply Template... New Template... Synchronise

Group [All] Partition [All] Site [All] Call Region [All]

Name	iSeries Logon	iTurret Logon	Intercom Logon	Dial Number	Seated Device
Speakerbus User 1		russellmclean		3001	id808-001B12
Speakerbus User 2		timothygame		3002	id808-000E49
Speakerbus User 3		neilhiggs		3004	iducx-000000
Speakerbus User 4		mattcheattle		3003	iducx-000001
Speakerbus User 5		paulgreaney			

Page: 1 5 rows in 1 pages

Within the **General** tab fill in the following:

- **Default PBX Appearance Type** Select Call from the drop-down list
- **Default PBX Appearance** Select the appropriate user from the drop-down list

Click **APPLY** (not shown) once completed.

The screenshot shows the 'General' tab of a configuration window. The 'Name' field is 'Speakerbus User 1'. 'Privileges Policy' and 'Preferences Policy' are both set to 'Default'. 'Default PBX Appearance Type' is set to 'Call'. 'Default PBX Appearance' is set to 'Speakerbus User 1'. 'Quiet Office' is 'Disabled'. 'Cisco Device Name Prefix' is 'russellmclean'. 'Additional Info #1' and 'Additional Info #2' are empty. 'iCS Registration Name' is 'MASTER-8'. A 'Change iCS Registration Password...' button is at the bottom.

Within the **iTurret** tab, provide the **login** credentials by clicking on the **Change Password** button and enter a **Login Name** and **Password** (not shown) and enter the following:

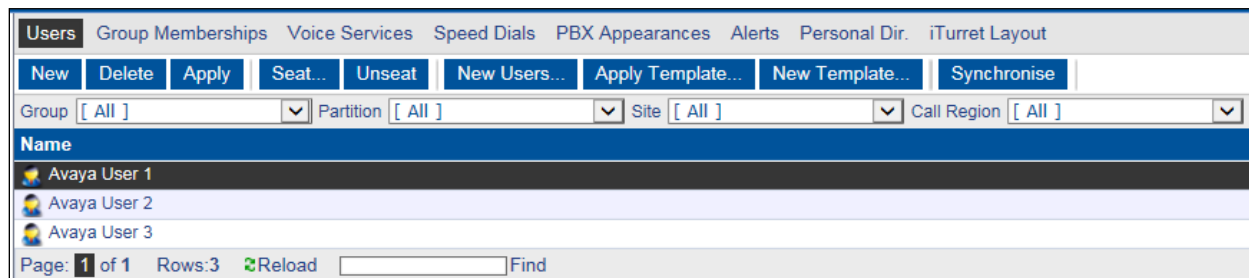
- **Voicemail Policy** Select the voicemail policy as configured in **Section 7.2**
- **Move to Idle Handset Mode** Select **Move Call** from the drop-down list
- **Enable Latching** Tick **Group Button 1, 2, 3 and 4**

Click **APPLY** (not shown) once completed (although, this page will be revisited later to configure the default call appearance for this user).

The screenshot shows the 'iTurret' tab of a configuration window for user 'russellmclean'. The 'Login Name' is 'russellmclean'. 'Voicemail Policy' is 'Avaya SM Voicemail'. Under 'iE801', 'Group Button' 1, 2, 3, and 4 are all checked. Under 'Preferences', 'Move To Idle Handset' is 'Move Call', 'Auto Hold/Clear' is 'Off', 'Answer On Idle Handset' is 'Off', 'Handset Push Button Mode' is 'Push to mute', 'Double-Tap Speaker To Handset' is checked, 'Auto-Hide Menu' is unchecked, 'Enable Key Press Tones' is unchecked, 'Enable Loud Listen Mode' is unchecked, and 'Intercom Audio Device' is 'Handset'. Under 'Device Preferences', 'Speaker Source' is 'Gooseneck', 'Handset 1 Volume' and 'Handset 2 Volume' are both '10', 'Acoustic Shock Protection Override' is checked, and 'Handsfree Microphone Type' is 'Gooseneck'.

Repeat the previous steps to add more users.

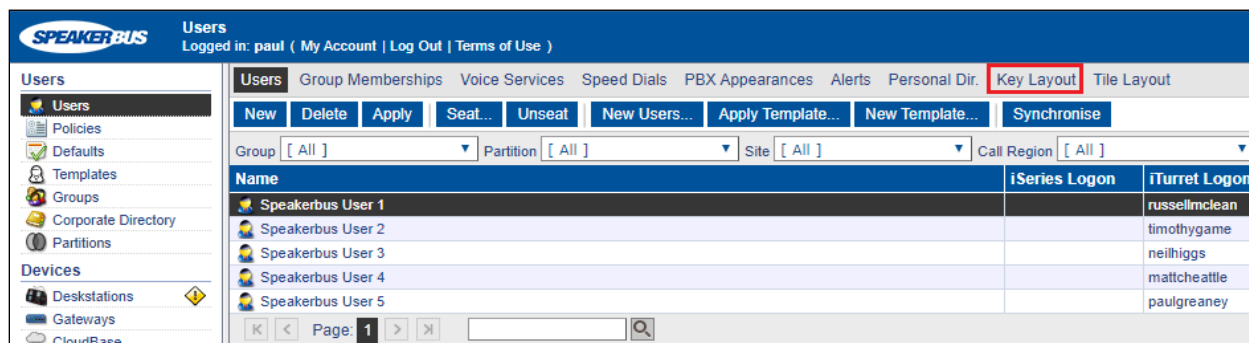
Once you have added the users, you can set up the PBX appearances for these users and then add them as Defaults PBX Appearance, see subsequent sections for further details.



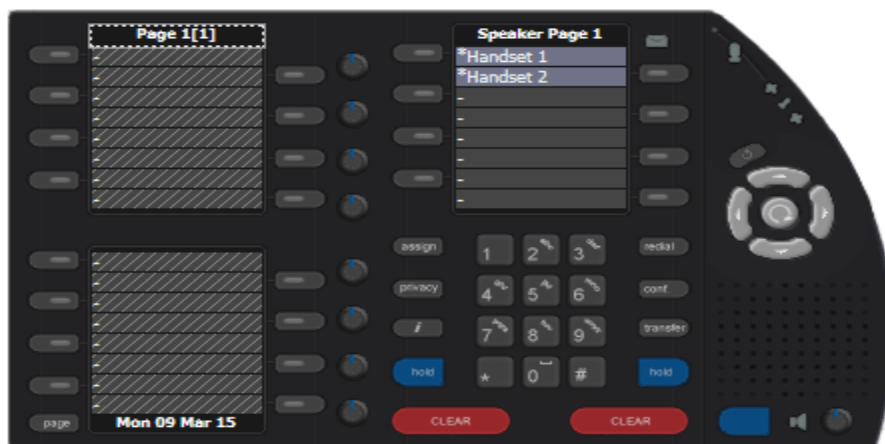
7.15. Program iTurret Layout Profiles

The programming of the iTurret Deskstations can be carried out by Speakerbus or Avaya engineer. For information on the types of keys available and administration of the iTurret layout, refer to the *Speakerbus iManager Administrator's Guide*.

To add the above appearances to the iTurret layout, go to the user and select the **Key Layout** tab as per the screenshot below.



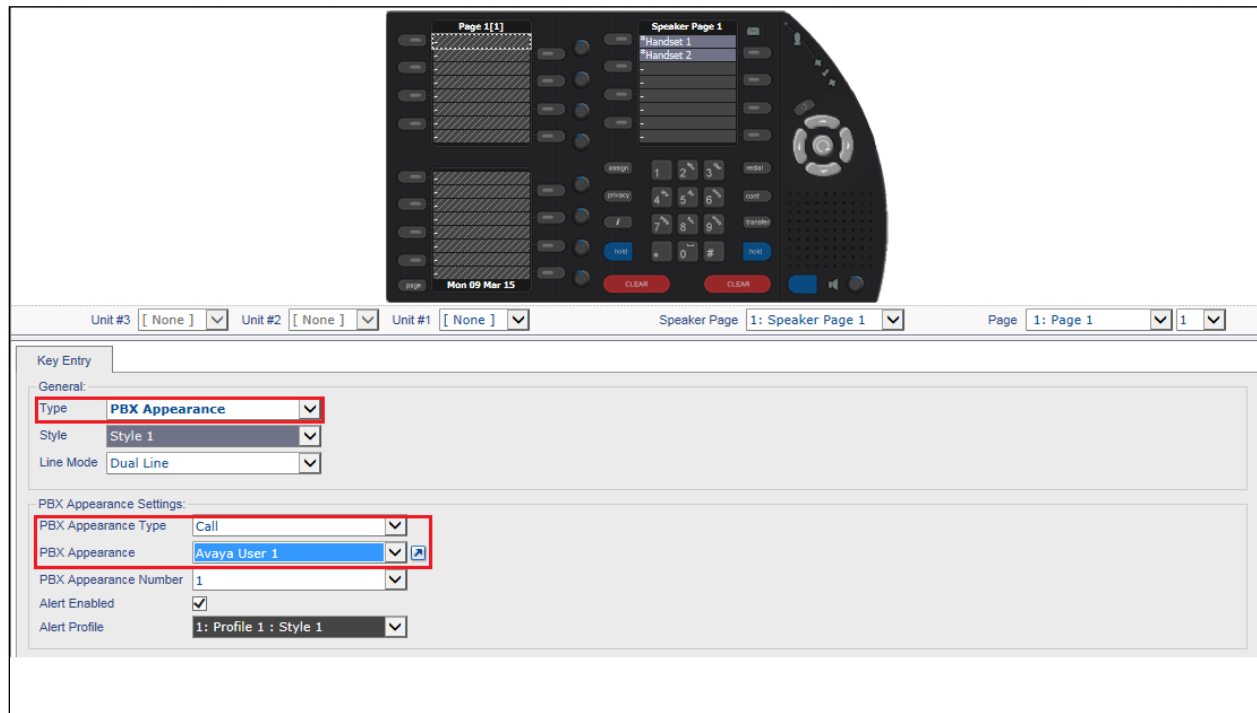
When selected the following layout is observed for a blank iTurret profile with ***Handset 1** and ***Handset 2** configured.



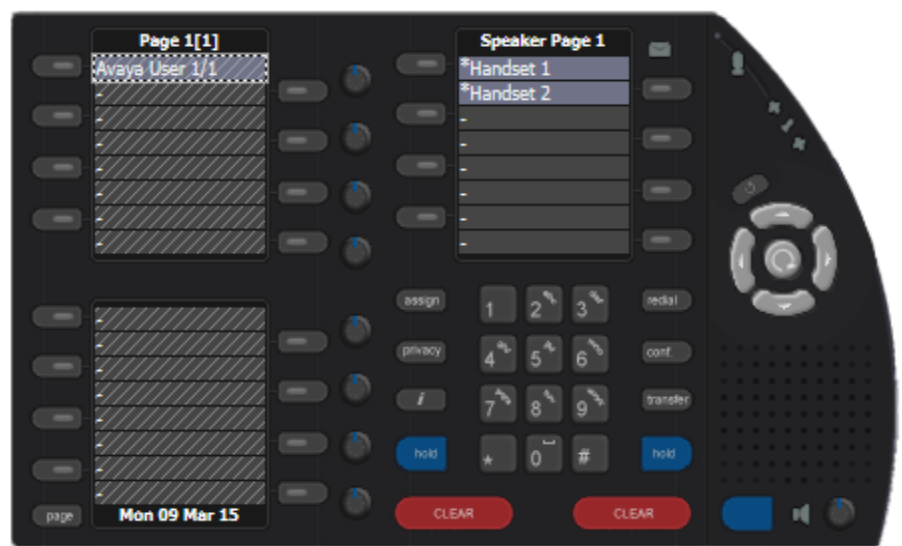
To add the keys for the call appearances, select a key (with hatching) and enter the following:

- **Type** Select **PBX Appearance** from the drop-down box
- **PBX Appearance Type** Select **Call**, from the drop-down box
- **PBX Appearance** Select the appearance given to this user (i.e. **Avaya User 1**)

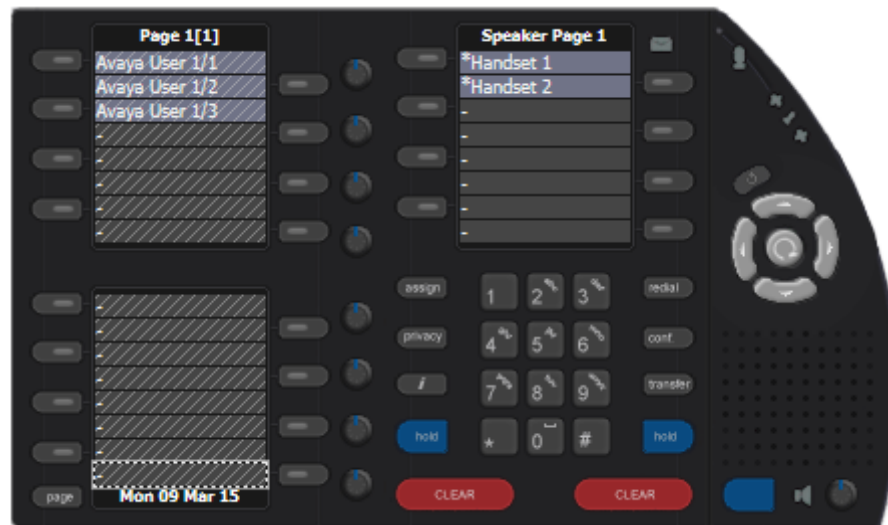
Click the **OK** button (not shown).



Once done the layout will look as follows.



Add two further instances of this appearance to the next two keys in the same way as above. The new iTurret layout will look as follows.

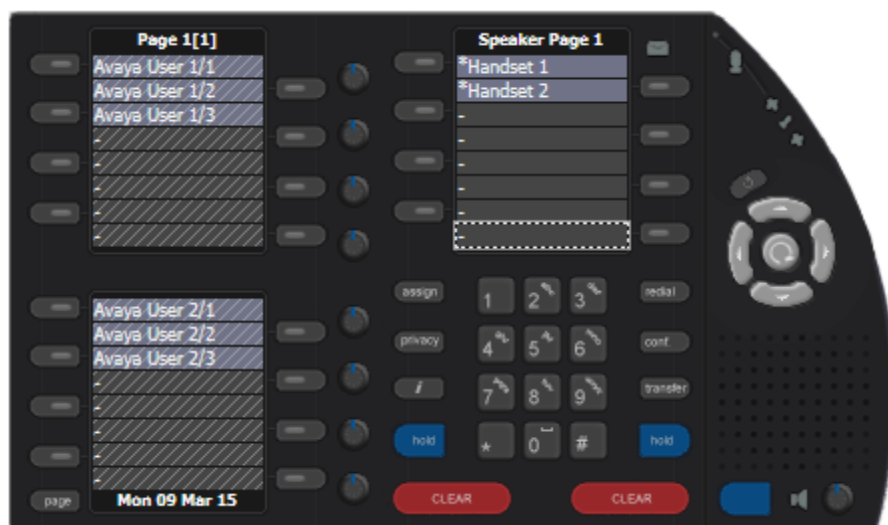


7.15.1. Add bridged appearances

To add bridged appearances, repeat **Section 7.11** and enter the following:

- **Type** Select **PBX Appearance** from the drop-down box
- **PBX Appearance Type** Select **Call**, from the drop-down box
- **PBX Appearance** Select the call appearance you have permissions to, but isn't owned by this user (thus, it's a bridged appearance)

Click the **OK** button (not shown). Repeat this step three times. The example below shows Avaya User 2 three times.



7.15.2. Add dynamic keys

Add three dynamic keys under the **handset 2 key** in the iTurret Layout using the procedure in **Section 7.11**, select the next available key under ***Handset 2** key and select **Dynamic** from the **Type** drop down box. The remaining fields are left at default. Click the **OK** button. Repeat this step three times. The example below shows the three dynamic keys added.



7.15.3. Add Do Not Disturb key

To add a single function key for **Do Not Disturb**, in the iTurret Layout, using the procedure in **Section 7.11**, select the next available key under the last **Dynamic** key and enter the following:

- **Type** Select **Function** from the drop-down box.
- **Function Type** Select **Do Not Disturb** from the drop-down box

Click the **OK** button. Once done the layout will look as below.



7.15.4. Add soft function keys

To add two soft function keys, in the iTurret Layout, using the procedure in **Section 7.11**, select the next available key under the Do Not Disturb key and enter the following:

- **Type** Select **Soft Function** from the drop-down box.
- **Function Type** Select **General** from the drop-down box

Click the **OK** button. Repeat this step two times. Once done the layout will look as below.



For more information on the types of keys available and adding, editing or removing, refer to the *Speakerbus iManager Administrator's Guide*.

7.16. Synchronise Deskstations

Any changes made to the profile within iManager will be updated on the iTurret device after **OK** or **Apply** is pressed. However, some changes will require a synchronization to push the new configuration to the iTurret without disruption to the user. Select **Devices → Deskstations** and select the desired deskstations.

SPEAKERBUS Deskstations									
Logged in: paul (My Account Log Out Terms of Use)									
Navigation ? Help Search i manager									
Users Users Policies Defaults Templates Groups Corporate Directory Partitions Devices Deskstations Gateways CloudBase Policies Defaults Call Servers PBXs PBX Appearances Network	Deskstations Channels Connections								
	New Delete Apply Seat Unseat Synchronise Firmware... Logs... Diagnostics... Move... Feature Keys...								
	Site [All] Call Region [All] Type [All] Status [All]								
	Name	Site	Call Region	Type	IP Address	MAC Address	Firmware	Seated User	Status
	id808-000E49	Galway Lab	Galway Lab	iTurret	10.10.40.220	00:05:83:00:0E:49	3.520.1.0	Speakerbus User	
	id808-0012F4	Galway Lab	Galway Lab	iTurret	10.10.40.236	00:05:83:00:12:F4	3.520.1.0		
	id808-001B12	Galway Lab	Galway Lab	iTurret	10.10.40.213	00:05:83:00:1B:12	3.520.1.0	Speakerbus User	
	iducx-000000	Galway Lab	Galway Lab	IDUCX	10.10.40.235	02:05:83:00:00:00	3.422.1.0	Speakerbus User	
	iducx-000001	Galway Lab	Galway Lab	IDUCX	10.10.40.209	02:05:83:00:00:01	3.422.1.0	Speakerbus User	
	K < Page 1 > Q								5 rows in 1 pages

Click the **Synchronise** button.

Deskstations			Channels	Connections		
New	Delete	Apply	Seat...	Unseat	Synchronise	Firmware...
Site	[All]	▼	Call Region	[All]	▼	Type [
Name						
id808-000E49						
id808-0012F4						
id808-001B12						
iducx-000000						
iducx-000001						
Page: 1						

8. Verification Steps


This section provides the tests that can be performed to verify correct configuration of the Avaya and Speakerbus solution.

8.1. Verify iTurret registration with Avaya Aura® Session Manager

To verify that the iTurret have successfully registered with Session Manager, from the System Manager Web interface click **Session Manager** → **System Status** → **User Registrations** (not shown). This will display a summary of registered stations on each Session Manager as shown below.

User Registrations												
Select rows to send notifications to devices. Click on Details column for complete registration status.												
View Default Export Force Unregister AST Device Notifications: Reboot Reload Failback As of 2:54 PM Customize Advanced Search Filter: Enable												
18 Items Show 15												
Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
Show	1173@devconnect.local	Speakerbus	Privacy User 4	DevConnectLab	10.10.40.209			1/1		✓		
Show	1172@devconnect.local	Speakerbus	Privacy User 3	DevConnectLab	10.10.40.209			1/1		✓		
Show	1171@devconnect.local	Speakerbus	Privacy User 2	DevConnectLab	10.10.40.213			1/1		✓		
Show	1170@devconnect.local	Speakerbus	Privacy User 1	DevConnectLab	10.10.40.213			1/1		✓		
Show	1163@devconnect.local	Speakerbus	User4	DevConnectLab	10.10.40.209			1/1		✓		
Show	1162@devconnect.local	Speakerbus	User3	DevConnectLab	10.10.40.235			1/1		✓		
Show	1161@devconnect.local	Speakerbus	User2	DevConnectLab	10.10.40.220			1/1		✓		
Show	1160@devconnect.local	Speakerbus	User1	DevConnectLab	10.10.40.213			1/1		✓		
Show	1101@devconnect.local	J129 SIP	1101	DevConnectLab	10.10.40.194			1/1	✓	✓ (AC)		
Show	1100@devconnect.local	SIP Ext	1100	DevConnectLab	10.10.40.210			1/5	✓	✓ (AC)		
Show	---	IX Workplace	SIP 1105	---	---			0/2				
Show	---	SIP	Ext 1152	---	---			0/1				
Show	---	SIP	Ext 1153	---	---			0/1				
Show	---	SIP	Ext 1150	---	---			0/3				
Show	---	Equinox Vantage	1102	---	---			0/1				
Select : All, None Page 1 of 2												

8.2. Verify iTurret status

On the iTurret, verify that the status icons are green . These status icons indicate whether iTurret is connected to the network, iCMS server, and SIP registrar (i.e. Session Manager). Refer to **Section 10** for more details.

9. Conclusion

These Application Notes describe the compliance tested configuration of the Speakerbus iTurret with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. All tests passed with observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1
- [3] *Administering Avaya Aura® Session Manager*, Release 8.1
- [4] *Administering Avaya Aura® System Manager*, Release 8.1
- [5] *Speakerbus Administrator's Guide iManager PN AGiCMS V3.76, Revision 35, February 2020*

Product Documentation for Speakerbus can be requested from info@speakerbus.com

©2020 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.