



Avaya Solution & Interoperability Test Lab

Application Notes for Speakerbus iD808 *i Turret* with Avaya Aura[®] Communication Manager and Avaya Aura[®] SIP Enablement Services - Issue 1.0

Abstract

These Application Notes describe the steps required to connect Speakerbus iD808 *i Turret* to a SIP infrastructure consisting of Avaya Aura[®] Communication Manager and Avaya Aura[®] SIP Enablement Services. Also described is how Avaya Aura[®] Communication Manager features can be made available to the standard features supported in the iD808 deskstations. In this configuration, the Off-PBX Station (OPS) feature set is extended from Avaya Aura[®] Communication Manager to the Speakerbus iD808 *i Turret*, providing the iD808 deskstations with enhanced calling features.

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 iD808 *i Turrets* to a SIP infrastructure consisting of Avaya Aura® SIP Enablement Services and Avaya Aura® Communication Manager. Also described is how Avaya Aura® Communication Manager features can be made available in addition to the standard features supported in the *i Turret*. In this configuration, the Off-PBX Stations (OPS) feature set is extended from Avaya Aura® Communication Manager to the Speakerbus iD808 *i Turret*, providing the iTurret deskstation with enhanced calling features. The configuration steps described are also applicable to other Linux-based Avaya Servers and Media Gateways running Avaya Aura® Communication Manager.

The following table provides a summary of the supported features available on *i Turret* with the Avaya SIP offer. Some features are supported locally in *i Turret*, while others are only available with Avaya Aura® Communication Manager and Avaya Aura® SIP Enablement Services 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 [6]. 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 *i Turret* 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 *i Turret* can also be programmed to a FNE. Other features, such as Exclusion/Privacy and Call Forwarding, are available by using the AST (Advanced SIP Telephony) FNU (Feature Name URI). Avaya Aura® 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/Class Of Restriction (COS/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 in Avaya Aura® Communication Manager as OPS.

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	
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 <i>i Turret</i> and FNU
Call Forward Busy/No Answer	Yes	Yes	Local menu option on <i>i Turret</i> and FNU
Call Forward Cancel	Yes	Yes	Local menu option on <i>i Turret</i> 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			
Automatic Call Back	No	Yes	Via OPS FNE
Automatic Call-Back Cancel	No	Yes	Via OPS FNE
Conference on Answer	No	Yes	Via OPS FNE
Directed Call Pick-Up	No	Yes	Via OPS FNE
Drop Last Added Party	No	Yes	Via OPS FNE
Exclusion/Privacy	Yes	Yes	Local hard key on <i>i Turret</i> and FNU
Last Number Dialed	Yes	Yes	Via OPS FNE
Priority Call	No	Yes	Via OPS FNE, <i>i Turret</i> does not support distinctive ring indication
Send All Calls	No	Yes	Via OPS FNE
Send All Calls Cancel	No	Yes	Via OPS FNE
Transfer to Voice Mail	No	Yes	Via OPS FNE
Whisper Page	No	Yes	Via OPS FNE

Table 1: SIP Features Table

2. General Test Approach and Test Results

To verify interoperability of Speakerbus iD808 *i Turret* with Communication Manager and SIP Enablement Services, calls were made between iTurret deskstations and Avaya SIP, H.323 and Digital stations using various codec settings and exercising common PBX features. The telephony features were activated and deactivated using buttons and menu options on *i Turret*, FNEs, and FNUs. The PBX features listed in **Section 1** were covered. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of *i Turret* with SIP Enablement Services
- Calls between *i Turret* and Avaya SIP, H.323, and digital stations
- G.711 and G729 codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus
- Proper operation of voicemail with message waiting indicators (MWI)
- PBX features including Multiple Call Appearances, Hold, Transfer, and Conference
- Extended telephony features using Communication Manager Feature Name Extensions (FNEs) such as Call Forwarding, Conference On Answer, Call Park, Call Pickup, Automatic Redial and Send All Calls. See **Table 1** for the complete list of features
- Exclusion/Privacy using the Exclusion FNU
- Proper system recovery after an *i Turret* restart and loss of IP connection
- Correct *i Turret* behavior during SES failovers and simulated network failures

2.1. Test Results

During testing the Speakerbus iD808 *i Turret* completed all scenarios with results in all cases as expected.

2.2. Support

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

Web: <http://www.speakerbus.com>

Email: info@speakerbus.com

Telephone: (646) 289-4700 in North America

+44 (0) 870 240 7252 in Europe

+65 6222 4577 in Asia

3. Reference Configuration

The configuration used as an example in these Application Notes is shown in **Figure 1**. The diagram illustrates an enterprise site with an Avaya SIP-based network, including a pair of SIP Enablement Services, a pair of Avaya S8730 Servers with a G650 Media Gateway running Communication Manager, and Avaya IP endpoints. Avaya Modular Messaging provides voice mail service. The enterprise site also contains three Speakerbus iD808 *i Turret* deskstations that register with SIP Enablement Services and are configured as OPS stations on Communication Manager. Communication Manager extends the telephony functionality that is supported by the SIP-based iTurret devices through the use of Feature Name Extensions (FNEs) and FNUs. The *i cms* server contains the *i manager* application for configuring the iTurret deskstations.

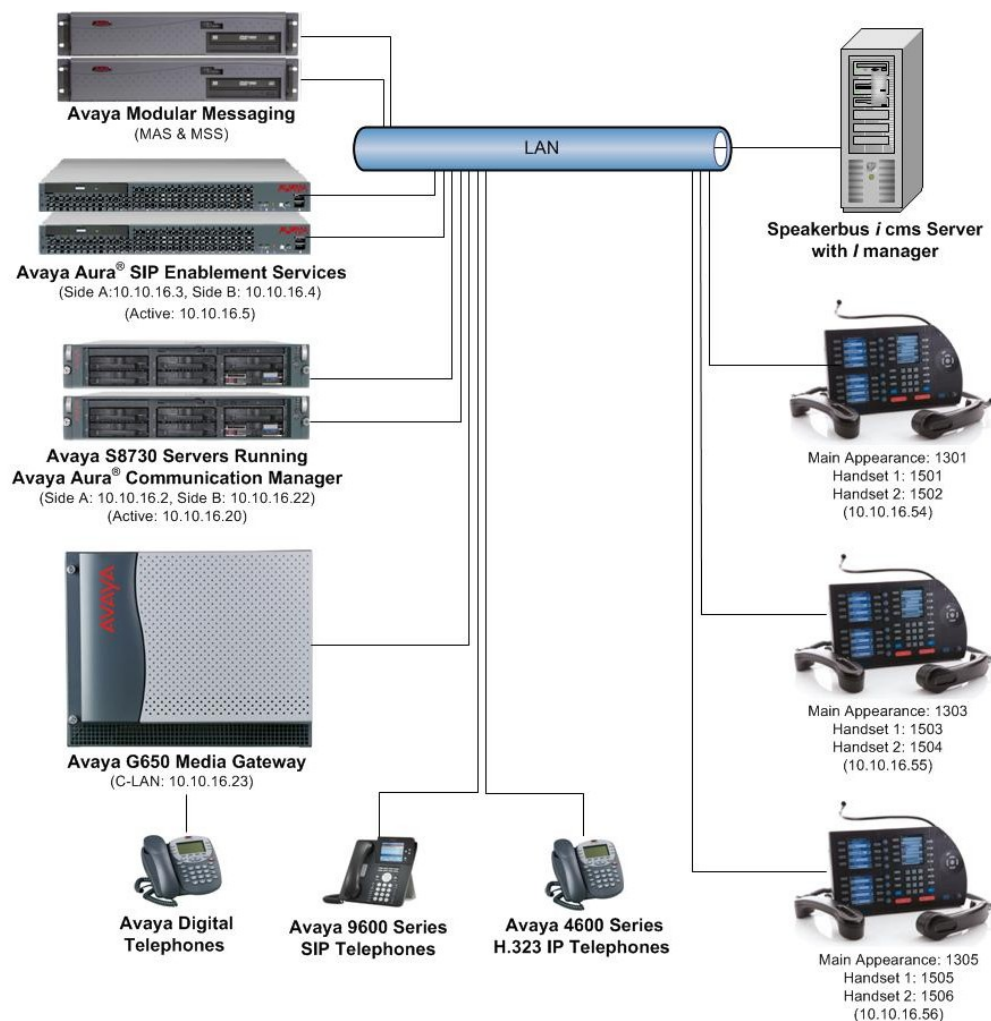


Figure 1: Speakerbus iD808 *i Turret* with Avaya SIP Solution

4. Equipment and Software Validated

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

Hardware Component	Version
Avaya S8730 Servers (Redundant Pair)	Avaya Aura [®] Communication Manager 5.2.1 (R015x.02.1.016.4) with Service Pack 0 (Patch 18433)
Avaya G650 Media Gateway TN2302AP Media Processor	HW32 FW120
Avaya S8500B Servers (Redundant Pair)	Avaya Aura [®] SIP Enablement Services 5.2.1(SES-5.2.1.0-016.4) with Service Pack 2
Avaya S3500 Servers Modular Messaging	Avaya Modular Messaging 5.2
Avaya 9600 Series IP Telephones	3.1 (H.323)
Avaya 9600 Series IP Telephones	2.6.4.0 (SIP)
Avaya Digital Telephones	--
Avaya Analog Telephones	--
Speakerbus iD808 <i>i Turret</i>	1.30
Speakerbus <i>i cms</i> Server with <i>i manager</i> Administration on Windows 2003 Server	1.400.7.0

5. Configure Aura® Avaya Communication Manager

This section describes the steps for configuring the Speakerbus iD808 *i Turret* as an Off-PBX Station (OPS), administering support for the OPS features indicated in **Table 1**, and configuring a SIP trunk between Communication Manager and SIP Enablement Services. Use the System Access Terminal (SAT) to configure Communication Manager. Log in with the appropriate credentials.

5.1. Verify System Capacity

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 iD808 device.

display system-parameters customer-options			Page	1 of 10
OPTIONAL FEATURES				
G3 Version: V15	Software Package: Standard			
Location: 2	RFA System ID (SID): 1			
Platform: 6	RFA Module ID (MID): 1			
			USED	
Platform Maximum Ports:			48000	282
Maximum Stations:			36000	48
Maximum XMOBILE Stations:			0	0
Maximum Off-PBX Telephones - EC500:			200	0
Maximum Off-PBX Telephones - OPS:			200	18
Maximum Off-PBX Telephones - PBFMC:			0	0
Maximum Off-PBX Telephones - PVFMC:			0	0
Maximum Off-PBX Telephones - SCCAN:			0	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 10
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	200	0
Maximum Concurrently Registered IP Stations:	18000	1
Maximum Administered Remote Office Trunks:	0	0
Maximum Concurrently Registered Remote Office Stations:	0	0
Maximum Concurrently Registered IP eCons:	0	0
Max Concur Registered Unauthenticated H.323 Stations:	0	0
Maximum Video Capable Stations:	0	0
Maximum Video Capable IP Softphones:	0	0
Maximum Administered SIP Trunks:	300	138
Maximum Administered Ad-hoc Video Conferencing Ports:	0	0
Maximum Number of DS1 Boards with Echo Cancellation:	100	0
Maximum TN2501 VAL Boards:	128	0
Maximum Media Gateway VAL Sources:	0	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	0	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.2. Define System Features

Use the **change system-parameters features** command to administer system wide features for SIP endpoints. Those related to features listed in **Table 1** are shown in bold. These are all standard Communication Manager features that are also available to OPS stations. On **Page 17**, set the **Whisper Page Tone Given To** field to **all**

change system-parameters features		Page 17 of 18
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 18** make sure **Directed Call Pickup** is set to **y**.

change system-parameters features	Page 18 of 18
FEATURE-RELATED SYSTEM PARAMETERS	
IP PARAMETERS	
Direct IP-IP Audio Connections?	y
IP Audio Hairpinning?	y
SDP Capability Negotiation for SRTP?	n
CALL PICKUP	
Maximum Number of Digits for Directed Group Call Pickup:	4
Call Pickup on Intercom Calls?	y
Call Pickup Alerting?	n
Temporary Bridged Appearance on Call Pickup?	y
Directed Call Pickup?	y
Extended Group Call Pickup:	none
Enhanced Call Pickup Alerting?	n
Display Information With Bridged Call?	n
Keep Bridged Information on Multiline Displays During Calls?	y
PIN Checking for Private Calls?	n

5.3. Define the 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 **Table 1**, 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**, 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: 1			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	ext	7	4	ext				
1	4	ext	88	4	ext				
2	4	udp	89	4	ext				
3005	8	udp	9	1	fac				
3015	9	udp	*	3	fac				
31	4	udp	#	3	fac				
33	4	udp							
37	4	udp							
38	5	aar							
4	1	fac							
5	3	dac							
6	3	fac							
61	4	ext							
66	4	ext							
663	4	ext							

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. Use **change feature-access-codes** to define the required access codes. The FACs used in the sample configuration is shown in bold.

```
change feature-access-codes                                     Page 1 of 9
                                FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code:
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
Announcement Access Code:
Answer Back Access Code: *24
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: 4
Auto Route Selection (ARS) - Access Code 1: 9    Access Code 2:
Automatic Callback Activation: *25    Deactivation: #25
Call Forwarding Activation Busy/DA: *21    All: *20    Deactivation: #20
Call Forwarding Enhanced Status:    Act:    Deactivation:
Call Park Access Code: *26
Call Pickup Access Code: *27
CAS Remote Hold/Answer Hold-Unhold Access Code:
CDR Account Code Access Code:
Change COR Access Code:
Change Coverage Access Code:
Conditional Call Extend Activation:    Deactivation:
Contact Closure    Open Code:    Close Code:
```

```
change feature-access-codes                                     Page 2 of 9
                                FEATURE ACCESS CODE (FAC)
Contact Closure    Pulse Code:

Data Origination Access Code:
Data Privacy Access Code:
Directed Call Pickup Access Code: *28
Directed Group Call Pickup Access Code:
Emergency Access to Attendant Access Code:
EC500 Self-Administration Access Codes:
Enhanced EC500 Activation:    Deactivation:
Enterprise Mobility User Activation:    Deactivation:
Extended Call Fwd Activate Busy D/A    All:    Deactivation:
Extended Group Call Pickup Access Code:
Facility Test Calls Access Code:
Flash Access Code:
Group Control Restrict Activation:    Deactivation:
Hunt Group Busy Activation:    Deactivation:
ISDN Access Code:
Last Number Dialed Access Code: *29
Leave Word Calling Message Retrieval Lock:
Leave Word Calling Message Retrieval Unlock:
```

FEATURE ACCESS CODE (FAC)

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

 PASTE (Display PBX data on Phone) Access Code:
 Personal Station Access (PSA) Associate Code: Dissociate Code:
Per Call CPN Blocking Code Access Code: *34
 Per Call CPN Unblocking Code Access Code: *35
 Posted Messages Activation: Deactivation:
Priority Calling Access Code: *30
 Program Access Code:

 Refresh Terminal Parameters Access Code:
 Remote Send All Calls Activation: Deactivation:
 Self Station Display Activation:
Send All Calls Activation: *31 Deactivation: #31
 Station Firmware Download Access Code:

FEATURE ACCESS CODE (FAC)

Station Lock Activation: Deactivation:
 Station Security Code Change Access Code:
 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: Separation Code:
Transfer to Voice Mail Access Code: *32
 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: *33

 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 **change off-pbx-telephone feature-name-extensions** command. The following screens show in bold the FNEs defined for use with the sample configuration.

```
change off-pbx-telephone feature-name-extensions set 1          Page 1 of 2
EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME
Set Name: Speakerbus FNEs

Active Appearance Select: 1700
Automatic Call Back: 1701
Automatic Call-Back Cancel: 1702
Call Forward All: 1703
Call Forward Busy/No Answer: 1704
Call Forward Cancel: 1705
Call Park: 1706
Call Park Answer Back: 1707
Call Pick-Up: 1708
Calling Number Block: 1709
Calling Number Unblock: 1710
Conditional Call Extend Enable: 1711
Conditional Call Extend Disable: 1712
Conference Complete: 1713
Conference on Answer: 1714
Directed Call Pick-Up: 1715
Drop Last Added Party: 1716
```

```
change off-pbx-telephone feature-name-extensions set 1          Page 2 of 2
EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME

Exclusion (Toggle On/Off): 1717
Extended Group Call Pickup:
Held Appearance Select: 1718
Idle Appearance Select: 1719
Last Number Dialed: 1720
Malicious Call Trace:
Malicious Call Trace Cancel:
Off-Pbx Call Enable:
Off-Pbx Call Disable:
Priority Call: 1725
Recall: 1726
Send All Calls: 1727
Send All Calls Cancel: 1728
Transfer Complete: 1729
Transfer On Hang-Up: 1730
Transfer to Voice Mail: 1731
Whisper Page Activation: 1732
```

5.6. Configure Class of Service (COS)

Use the **change cos** command to set the appropriate service permissions to support OPS features (shown in bold). For the sample configuration a COS of **1** was used. Priority call indication (e.g., distinctive ring) is not supported on the *i Turret* when using the Priority FNE. However, the iD808 does support a distinctive-ring/alerting mechanism locally on the turret, not covered in testing.

change cos																Page	1 of	2
	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	y	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	n	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	n	y	y	y	y	y	y	y	y	y	n	y	y	y	y		
Call Forwarding Busy/DA	n	y	n	n	n	n	n	n	n	n	n	y	n	n	n	n		
Personal Station Access (PSA)	n	y	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	y	n	n	n	n		
QSIG Call Offer Originations	n	n	n	n	n	n	n	n	n	n	n	y	n	n	n	n		
Contact Closure Activation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		

5.7. Configure Class of Restriction (COR)

Use the **change cor n** command where **n** is the number of the COR being configured, to enable applicable calling features. 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**. In the sample configuration, the *i Turrets* were assigned to COR 1.

change cor 1		Page 1 of 23	
CLASS OF RESTRICTION			
COR Number: 1			
COR Description: Default			
FRL: 0		APLT? y	
Can Be Service Observed? y		Calling Party Restriction: none	
Can Be A Service Observer? y		Called Party Restriction: none	
Partitioned Group Number: 1		Forced Entry of Account Codes? n	
Priority Queuing? n		Direct Agent Calling? n	
Restriction Override: all		Facility Access Trunk Test? n	
Restricted Call List? n		Can Change Coverage? n	
Access to MCT? y		Fully Restricted Service? n	
Group II Category For MFC: 7			
Send ANI for MFE? n			
MF ANI Prefix:		Automatic Charge Display? n	
Hear System Music on Hold? y		PASTE (Display PBX Data on Phone)? y	
Can Be Picked Up By Directed Call Pickup? y		Can Use Directed Call Pickup? y	
		Group Controlled Restriction: inactive	

5.8. Add Coverage Path

Use the **add coverage path n** command where **n** is the number of the coverage path to be added. Configure **Point 1** in the coverage path to one used to the voice messaging hunt group, which is group **h89** in the sample configuration. The default values shown for **Busy**, **Don't Answer**, and **DND/SAC/Goto Cover** can be used for the **Coverage Criteria**.

add coverage path 89		Page 1 of 1	
COVERAGE PATH			
Coverage Path Number: 89			
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	Number of Rings: 2
All?	n	n	
DND/SAC/Goto Cover?	y	y	
Holiday Coverage?	n	n	
COVERAGE POINTS			
Terminate to Coverage Pts. with Bridged Appearances? n			
Point1: h89	Rng:	Point2:	
Point3:		Point4:	
Point5:		Point6:	

5.9. Add Stations

The Speakerbus iD808 *i Turret* requires up to three stations for each device. The first station is referred to as the main appearance. The second and third stations are referred to as the privacy handsets. The privacy handsets are needed when privacy is required. If the privacy feature is not needed, then only the first station is required.

5.9.1. Main Appearance Station

Use the **add station** command to add a station for each *i Turret* to be supported. To configure the main appearance, on **Page 1** use **9630** for the station **Type** and include the **Coverage Path** for voice messaging, if applicable. Use the **COS** and **COR** values administered in **Sections 4.6** and **4.7**. Enter a descriptive name in the **Name** field. Use the default values for the all other fields.

add station 1301		Page 1 of 5
STATION		
Extension: 1301	Lock Messages? n	BCC: 0
Type: 9630	Security Code:	TN: 1
Port: IP	Coverage Path 1: 89	COR: 1
Name: iTurret 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 1301	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	

On **Page 2**, if this *i Turret* will have a bridged appearance for another telephone (see **Page 4** for this station), then **Bridged Call Alerting** should be set to **y**, so that this *i Turret* will ring when the other telephone is called. Set the **MWI Served User Type** field to the appropriate value to allow message waiting indication to be sent to the *i Turret*. Use the default values for the all other fields.

Note: By default, the **Restrict Last Appearance** field is set to **y** to reserve the last the last call appearance for outgoing calls from the *i Turret*, this should not be altered.

add station 1301		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? y	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number? y	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced		
MWI Served User Type: qsig-mwi	Display Client Redirection? n	
	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? N	
Emergency Location Ext: 1301	Direct IP-IP Audio Connections? y	
Precedence Call Waiting? y	Always Use? n IP Audio Hairpinning? n	

On **Page 4** under the heading **BUTTON ASSIGNMENTS**, fill in the number of call appearances that are to be supported for *i Turret*. In this example, the first station for *i Turret* was configured with four call appearances. Locally, *i Turret* will actually be configured with 3 call appearances since the last appearance is restricted as configured on **Page 2**. Multiple bridged line appearances are configured for this example station. Button assignments **5** and **6** relate to the second and third stations corresponding to two stations that will be used as the privacy handsets at *i Turret*.

Note: These stations are configured in **Section 5.9.2** and these bridged appearance buttons cannot be configured until those stations have been added. If privacy is not needed for *i Turret*, then these bridged appearances are not required.

add station 1301		Page 4 of 5	
STATION			
SITE DATA			
Room:		Headset?	n
Jack:		Speaker?	n
Cable:		Mounting:	d
Floor:		Cord Length:	0
Building:		Set Color:	
ABBREVIATED DIALING			
List1:	List2:	List3:	
BUTTON ASSIGNMENTS			
1: call-appr	5: brdg-appr	B:1	E:1501
2: call-appr	6: brdg-appr	B:1	E:1502
3: call-appr	7:		
4: call-appr	8:		
voice-mail Number:			

Continue on **Page 5** under the **BUTTON ASSIGNMENTS** section, enter the function button names (shown in bold) for OPS FNEs that will be used at *i Turret*. Configure function buttons **call-fwd**, **cfwd-bsyda** and if required, **auto-cback** and **no-hld-cnf**.

add station 1301		Page 5 of 5	
STATION			
BUTTON ASSIGNMENTS			
9:			
10:			
11:			
12:			
13: auto-cback			
14: no-hld-cnf			
15: cfwd-bsyda Ext:			
16: call-fwd Ext:			
17:			
18:			
19:			
20:			

Only the FNEs shown in the table below require the station to have a corresponding function button.

FNE Name	Function Button
Automatic Callback, Automatic Callback Cancel	auto-cback
Call Forward All	call-fwd
Call Forward Busy/No Answer	cfwd-bsyda
Conference on Answer	no-hld-cnf

5.9.2. Privacy Handset Stations

Use the **add station** command to add a station for each privacy handset. On **Page 1** use **9630** for the station **Type**. A coverage path is not required for this station. Use the **COS** and **COR** values administered in **Sections 5.6** and **5.7**. Enter a descriptive name in the **Name** field. Use the default values for the all other fields.

add station 1501		Page 1 of 5
STATION		
Extension: 1501	Lock Messages? n	BCC: 0
Type: 9630	Security Code:	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: HS1 of 1301	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 1501	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? n	
	Customizable Labels? y	
	Customizable Labels? y	

On **Page 2**, the **Bridged Call Alerting** field should be set to **y**.

add station 1501		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? y	Restrict Last Appearance? y	
Active Station Ringing: single	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced		
MWI Served User Type:	Display Client Redirection? n	
AUDIX Name:	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 1501	Always Use? n IP Audio Hairpinning? n	
Precedence Call Waiting? y		

On **Page 4** of the first Privacy Handset station, one call appearance should be configured along with a feature button for the **exclusion** feature (required for privacy), and bridged appearances for each call appearance of the first station (main appearance) all shown in bold below.

add station 1501		Page 4 of 5
STATION		
SITE DATA		
Room:	Headset? n	
Jack:	Speaker? n	
Cable:	Mounting: d	
Floor:	Cord Length: 0	
Building:	Set Color:	
ABBREVIATED DIALING		
List1:	List2:	
	List3:	
BUTTON ASSIGNMENTS		
1: call-appr	5: brdg-appr B:3 E:1301	
2: exclusion	6:	
3: brdg-appr B:1 E:1301	7:	
4: brdg-appr B:2 E:1301	8:	
voice-mail Number:		

Below is the configuration of the third station for handset 2. Use the **add station** command to add a station for each privacy handset. On **Page 1** use **9630** for the station **Type**. A coverage path is not required for this station. Use the **COS** and **COR** values administered in **Sections 5.6** and **5.7**. Enter a descriptive name in the **Name** field. Use the default values for the all other fields.

add station 1502		Page	1 of 5
STATION			
Extension: 1502	Lock Messages? n	BCC: 0	
Type: 9630	Security Code:	TN: 1	
Port: IP	Coverage Path 1:	COR: 1	
Name: HS2 of 1301	Coverage Path 2:	COS: 1	
	Hunt-to Station:		
STATION OPTIONS			
Loss Group: 19	Time of Day Lock Table:		
	Personalized Ringing Pattern: 1		
	Message Lamp Ext: 1502		
Speakerphone: 2-way	Mute Button Enabled? y		
Display Language: english	Button Modules: 0		
Survivable GK Node Name:			
Survivable COR: internal	Media Complex Ext:		
Survivable Trunk Dest? y	IP SoftPhone? n		
	IP Video? n		
	Customizable Labels? y		

On **Page 2**, the **Bridged Call Alerting** field should be set to **y**.

Add station 1502		Page	2 of 5
STATION			
FEATURE OPTIONS			
LWC Reception: spe	Auto Select Any Idle Appearance? n		
LWC Activation? y	Coverage Msg Retrieval? y		
LWC Log External Calls? n	Auto Answer: none		
CDR Privacy? n	Data Restriction? n		
Redirect Notification? y	Idle Appearance Preference? n		
Per Button Ring Control? n	Bridged Idle Line Preference? n		
Bridged Call Alerting? y	Restrict Last Appearance? y		
Active Station Ringing: single			
	EMU Login Allowed? n		
H.320 Conversion? n	Per Station CPN - Send Calling Number?		
Service Link Mode: as-needed	EC500 State: enabled		
Multimedia Mode: enhanced			
MWI Served User Type:	Display Client Redirection? n		
AUDIX Name:	Select Last Used Appearance? n		
	Coverage After Forwarding? s		
	Multimedia Early Answer? n		
	Direct IP-IP Audio Connections? y		
Emergency Location Ext: 1502	Always Use? n IP Audio Hairpinning? n		
Precedence Call Waiting? y			

On **Page 4** of the second privacy handset station, one call appearance should be configured along with a feature button for the **exclusion** feature (required for privacy), and bridged appearances for each call appearance of the first station (main appearance) all shown in bold below

add station 1502		Page 4 of 5	
STATION			
SITE DATA			
Room:		Headset?	n
Jack:		Speaker?	n
Cable:		Mounting:	d
Floor:		Cord Length:	0
Building:		Set Color:	
ABBREVIATED DIALING			
List1:	List2:	List3:	
BUTTON ASSIGNMENTS			
1: call-appr		5: brdg-appr	B:3 E:1301
2: exclusion		6:	
3: brdg-appr	B:1 E:1301	7:	
4: brdg-appr	B:2 E:1301	8:	
voice-mail Number:			

Note: If a bridged appearance is required for another *i Turret* or telephone, a bridged appearance button must be added to all three stations corresponding to the *i Turret* device.

5.10. Administer Off PBX Station Mapping

Use the **change off-pbx-telephone station-mapping** command to map the Communication Manager extensions (1301, 1501, and 1502) to the same SIP Enablement Services Communication Manager extension. Enter the field values shown. For the sample configuration, the **Trunk Selection** value indicates the SIP trunk group between Communication Manager and SIP Enablement Services. The SIP trunk group is configured in **Section 5.11**. The **Configuration Set** value can reference a set that has the default settings.

change off-pbx-telephone station-mapping 1301							Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode		
1301	OPS	-		1301	6	1			
1501	OPS	-		1501	6	1			
1502	OPS	-		1502	6	1			

On **Page 2**, change the **Call Limit** to match the number of call appearances on the station form. Also, verify that **Mapping Mode** is set to **both** (the default value for a newly added station). It is recommended that 10 be used for the primary stations call limit as this is the Avaya maximum and would not have to be subsequently changed if bridged appearances are added to the user.

change off-pbx-telephone station-mapping 1301							Page	2 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station Extension	Appl Name	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location			
1301	OPS	10	both	all	none				
1501	OPS	10	both	all	none				
1502	OPS	10	both	all	none				

5.11. Configure SIP Trunk

In the **IP Node Names** form, assign an IP address and host name for the C-LAN board in the Avaya G650 Media Gateway and for active SIP Enablement Services IP address. The host names will be used throughout the other configuration screens of Communication Manager.

```
change node-names ip
                                IP NODE NAMES
      Name                      IP Address
CLAN1                        10.10.16.23
Gateway                       10.10.16.1
MedPro1                       10.10.16.24
SM100                         10.10.16.11
default                       0.0.0.0
procr                         0.0.0.0
sesactive                   10.10.16.5
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on SIP Enablement Services. In this configuration, the domain name is **sip.avaya.com**. By default, **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G650 Media Gateway. 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 SIP Enablement Services as **ip-network region 1** is specified in the SIP signaling group.

```
change ip-network-region 1
                                IP NETWORK REGION
      Region: 1
Location: 1      Authoritative Domain: sip.avaya.com
      Name: Default Region
MEDIA PARAMETERS
      Codec Set: 1
      UDP Port Min: 2048
      UDP Port Max: 8001
      Intra-region IP-IP Direct Audio: yes
      Inter-region IP-IP Direct Audio: yes
      IP Audio Hairpinning? y
DIFFSERV/TOS PARAMETERS
      RTCP Reporting Enabled? y
      Call Control PHB Value: 46
      Audio PHB Value: 46
      Video PHB Value: 26
      RTCP MONITOR SERVER PARAMETERS
      Use Default Server Parameters? y
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 codec's supported for calls routed over the SIP trunk to *i Turret* deskstations. The form is accessed via the **change ip-codec-set 1** command. 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; the example below includes **G.711A** (a-law), **G.711MU** (mu-law) and **G.729**, which are supported by the iD808 deskstations.

change ip-codec-set 1

Page 1 of 2

IP Codec Set

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711A	n	2	20
2: G.711MU	n	2	20
3: G.729	n	2	20
4:			
5:			
6:			
7:			

Media Encryption

1: none

2:

3:

Prior to configuring a SIP trunk group for communication with SIP Enablement Services, a SIP signaling group must be configured. Configure the Signaling Group form shown as follows:

- Set the **Group Type** field to **sip**
- Set the **Transport Method** to the desired transport method; **tcp** (transport control protocol) or **tls** (Transport Layer Security). **Note:** For transparency, tcp was used during this compliance test but the recommended method is tls
- Specify the node names for the C-LAN board in the G650 Media Gateway and the active SIP Enablement Services 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
- Ensure that the recommended port value of **5060** for tcp is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields **Note:** If tls is used then the recommended port value is 5061
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field
- Enter the domain name of SIP Enablement Services in the **Far-end Domain** field. In this configuration, the domain name is **sip.avaya.com**. This domain is specified in the Uniform Resource Identifier (URI) of the “SIP To Address” in the INVITE message. Mis-configuring this field may prevent calls from being successfully established to other SIP endpoints or to the PSTN
- If calls to/from SIP endpoints are to be shuffled, then the **Direct IP-IP Audio Connections** field must be set to **y**
- The **DTMF over IP** field should be set to the default value of **rtp-payload**. Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used

add signaling-group 6		Page 1 of 1
SIGNALING GROUP		
Group Number: 6	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
IP Video? n		
Near-end Node Name: CLAN1	Far-end Node Name: sesactive	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain: sip.avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? y	
Enable Layer 3 Test? n	Direct IP-IP Early Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to *i Turret* deskstations. 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. 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.

add trunk-group 6		Page 1 of 21	
TRUNK GROUP			
Group Number: 6	Group Type: sip	CDR Reports: y	
Group Name: SES OPS	COR: 1	TN: 1	TAC: 506
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Signaling Group: 6	
		Number of Members: 30	

On **Page 3** of the trunk group form, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number sent to the far-end.

add trunk-group 6		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: public		UUI Treatment: service-provider	
		Replace Restricted Numbers? y	
		Replace Unavailable Numbers? y	
Show ANSWERED BY on Display? y			

Configure the **Public/Unknown Numbering Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 4-digit extension beginning with **1** and whose calls are routed over SIP trunk group **6** have the number sent to the far-end for display purposes.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	1	6		4	Total Administered: 1 Maximum Entries: 9999

6. Configure Avaya Aura® SIP Enablement Services

This section covers the administration of SIP Enablement Services. SIP Enablement Services is configured via an Internet browser using the Administration web interface. It is assumed that SIP enablement Services software and the license file have already been installed. For additional information on installation tasks refer to [4].

6.1. Logging into Avaya Aura® SIP Enablement Services

To access the administration web interface, enter **http://<ip-addr>/admin** as the URL in an Internet browser, where <ip-addr> is the active IP address of SIP Enablement Services. Log in with the appropriate credentials and then select the **Administration → SIP Enablement Services** (not shown). The main screen is displayed, as shown below.



AVAYA Integrated Management SIP Server Management

Help Exit Primary Server: [1] sessvra Duplicate Server: [2] sessvrb

Top

- ± Users
 - Address Map Priorities
- ± Adjunct Systems
- ± Aggregator
- ± Certificate Management
- ± Conferences
 - Emergency Contacts
- ± Export/Import to ProVision
- ± Hosts
 - IM logs
- ± Communication Manager Servers
- ± Communication Manager Extensions
- ± Server Configuration
- ± SIP Phone Settings
- ± Survivable Call Processors
- System Status
- ± Trace Logger
- ± Trusted Hosts

Top	
Manage Users	Add and delete Users.
Manage Address Map Priorities	Adjust Address Map Priorities.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Event Aggregators	Add/Delete Event Aggregators.
Certificate Management	Manage Certificates.
Manage Conferencing	Add and delete Conference Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Export Import to ProVision	Export and import data using ProVision on this host.
Manage Hosts	Add and delete Hosts.
IM logs	Download IM Logs.
Manage Communication Manager Servers	Add and delete Communication Manager Servers.
Manage Communication Manager Extensions	Add and delete Communication Manager Extensions.
Server Configuration	View Properties of the system.

6.2. Verify System Properties

From the left pane of the Administration web interface, expand the **Server Configuration** option and select **System Properties**. In the **System Properties** screen, enter the **SIP Domain** name assigned to the Avaya SIP-based network. For the **SIP License Host** field, enter the fully qualified domain name or the IP address of the local host unless the WebLM server is not co-resident with this server.

Note: Separate licenses are needed for each SIP Enablement Services server. After configuring the **System Properties** screen, click the **Update** button.

HelpExit

Primary Server: [1] sessvra Duplicate Server: [2] sessvrb

Top

Users

Address Map Priorities

Adjunct Systems

Aggregator

Certificate Management

Conferences

Emergency Contacts

Export/Import to ProVision

Hosts

IM logs

Communication Manager Servers

Communication Manager Extensions

Server Configuration

Admin Setup

IM Log Settings

License

SNMP Configuration

System Properties

SIP Phone Settings

Survivable Call Processors

System Status

Trace Logger

Trusted Hosts

View System Properties

SES VersionSES-5.2.1.0-016.4

System ConfigurationCabled Duplex

Host TypeSES combined home-edge

SIP Domain*

Note that the DNS domain is avaya.com

If you are unsure about this field, most often the SIP domain should be the root level DNS domain. For example, for a DNS domain of eastcoast.example.com, the SIP domain would likely be configured to example.com. This allows SIP calls and instant messages to users with handles of the format handle@example.com

SIP License Host*

DiffServ/TOS Parameters

Call Control PHB Value*

802.1 Parameters

Priority Value*

Management System Access Loginadmin

Management System Access Password

DB Log Leveldisabled

Update

6.3. Create a Host

After setting up the domain in the **System Properties** screen, create a host entry for SIP Enablement Services. The following example shows the **Edit Host** screen since the host had already been configured. Enter the active IP address of SIP Enablement Services in the **Host IP Address** field. The **Profile Service Password** was specified during the system installation. Next, verify the **Host Type** field. In this example, both servers in the redundant pair were configured as an **SES combined home/edge** during the initial setup. The **Link Protocols** selected defaults to TLS but in this example **TCP** was used. The default values for the other fields may be used as shown below.

AVAYA Integrated Management SIP Server Management

Help Exit Primary Server: [1] sessvra Duplicate Server: [2] sessvrb

Edit Host

Host IP Address* 10.10.16.5

Profile Service Password*

Host Type SES combined home-edge

Parent none

Listen Protocols ☒ UDP ☒ TCP ☒ TLS

Link Protocols ☐ UDP ☒ TCP ☐ TLS

Access Control Policy (Default) ☐ Allow All ☒ Deny All

Emergency Contacts Policy ☒ Allow ☐ Deny

Minimum Registration (seconds) 900 Registration Expiration Timer (seconds)* 86400

Subscription Expiration Timer (seconds)* 86400

Line Reservation Timer (seconds)* 30

Outbound Routing Allowed From ☒ Internal ☒ External

OutboundProxy Port ☐ UDP ☐ TCP

☒ TLS

Outbound Direct Domains

Default Ringer Volume* 5 Default Ringer Cadence 2

Default Receiver Volume* 5 Default Speaker Volume* 5

VMM Server Address

VMM Server Port 5005 VMM Report Period 5

Fields marked * are required.

Update

6.4. Add Avaya Aura® Communication Manager Interface

Under the **Communication Manager Servers** option in the Administration web interface, select **Add** to add the Avaya Media Server in the enterprise site since a SIP trunk is required between Communication Manager and SIP Enablement Services. In this screen, enter a descriptive name in the **Communication Manager Server Interface Name** field and select the home server from the drop down menu in the **Host** field. Select TCP for the **Link Type** and enter the IP address of the C-LAN board in the Avaya G650 Media gateway in the **SIP Trunk IP Address** field. Refer to [4] for additional information on configuring the remaining fields.

[Help](#) [Exit](#) Primary Server: [1] sessvra Duplicate Server: [2] sessvrb

Top

- Users
 - Address Map Priorities
- Adjunct Systems
- Aggregator
- Certificate Management
- Conferences
 - Emergency Contacts
- Export/Import to ProVision
- Hosts
 - IM logs
- Communication Manager Servers
 - Communication Manager Extensions
 - Server Configuration
 - SIP Phone Settings
 - Survivable Call Processors
 - System Status
- Trace Logger
- Trusted Hosts

Add Communication Manager Server Interface

Communication Manager Server Interface Name*

Host

SIP Trunk

SIP Trunk Link Type☒ TCP ☐ TLS

SIP Trunk IP Address*

Communication Manager Server

Communication Manager Server Admin Address*
(see Help)

Communication Manager Server Admin Port*

Communication Manager Server Admin Login*

Communication Manager Server Admin Password*

Communication Manager Server Admin Password Confirm*

SMS Connection Type☒ SSH ☐ Telnet ☐ Not Available

Note: If the Communication Manager Server connection type is changed and the admin port value is not also changed, changing connection type to SSH will change the admin port to 5022 when Add or Update is clicked and changing connection type to Telnet will change admin port to 5023 when Add or Update is clicked.

Fields marked * are required.

Add

SJW; Reviewed:
SPOC 4/5/2011

Solution & Interoperability Test Lab Application Notes
©2011 Avaya Inc. All Rights Reserved.

32 of 68
iD808-Aura-521

6.5. Add User

Three users are required for each Speakerbus iD808 *i Turret* registering with SIP Enablement Services, one for the main appearance and two for the handset appearances. The handset appearances are required to support privacy with Communication Manager. The procedure to add all three users is the same. In the **Add User** screen, enter the extension of the SIP endpoint in the **Primary Handle** field. Enter a user password in the **Password** and **Confirm Password** fields. In the **Host** field, select the SIP Enablement Services server hosting the domain (*avaya.com*) for this user. Enter the **First Name** and **Last Name** of the user. To associate the extension for this user with a Communication Manager extension, select the **Add Communication Manager Extension** checkbox. Calls from this user will always be routed through Communication Manager over the SIP trunk. Click the **Add** button to commit entries.

AVAYA Integrated Management
SIP Server Management

Help Exit Primary Server: [1] sessvra Duplicate Server: [2] sessvrb

Add User

Primary Handle* 1301

User ID

Password*

Confirm Password*

Host* 10.10.16.5

First Name* iTurret

Last Name* iD808 1301

Address 1 Avaya

Address 2 DevConnectLab

Office

City

State

Country

Zip

Survivable Call Processor none

Add Communication Manager Extension ☒

Fields marked * are required.

Add

The **Add Communication Manager Extension** screen is displayed. In the **Add Communication Manager Extension** screen, enter the **Extension** configured in Communication Manager for the previously added user. Usually, the Communication Manager extension and the user extension are the same (recommended). Click the **Add** button.

The screenshot displays the Avaya Integrated Management SIP Server Management interface. The top header features the Avaya logo on the left and the text 'Integrated Management SIP Server Management' on the right. Below the header, a status bar indicates 'Primary Server: [1] sessvra' and 'Duplicate Server: [2] sessvrb'. A left-hand navigation menu lists various system components, including Users, Address Map Priorities, Adjunct Systems, Aggregator, Certificate Management, Conferences, Emergency Contacts, Export/Import to ProVision, Hosts, IM logs, Communication Manager Servers, Communication Manager Extensions, Server Configuration, SIP Phone Settings, Survivable Call Processors, System Status, Trace Logger, and Trusted Hosts. The main content area is titled 'Add Communication Manager Extension' and contains the instruction 'Add Communication Manager extension for user 1301.' Below this, there is a form with an 'Extension' field containing the value '1301' and a 'Communication Manager Server' dropdown menu set to 'CoreCM'. A note states 'Fields marked * are required.' and an 'Add' button is positioned at the bottom of the form.

AVAYA Integrated Management SIP Server Management

Help Exit Primary Server: [1] sessvra Duplicate Server: [2] sessvrb

Add Communication Manager Extension

Add Communication Manager extension for user 1301.

Extension 1301

Communication Manager Server CoreCM

Fields marked * are required.

Add

7. Speakerbus iD808 i Turret Configuration

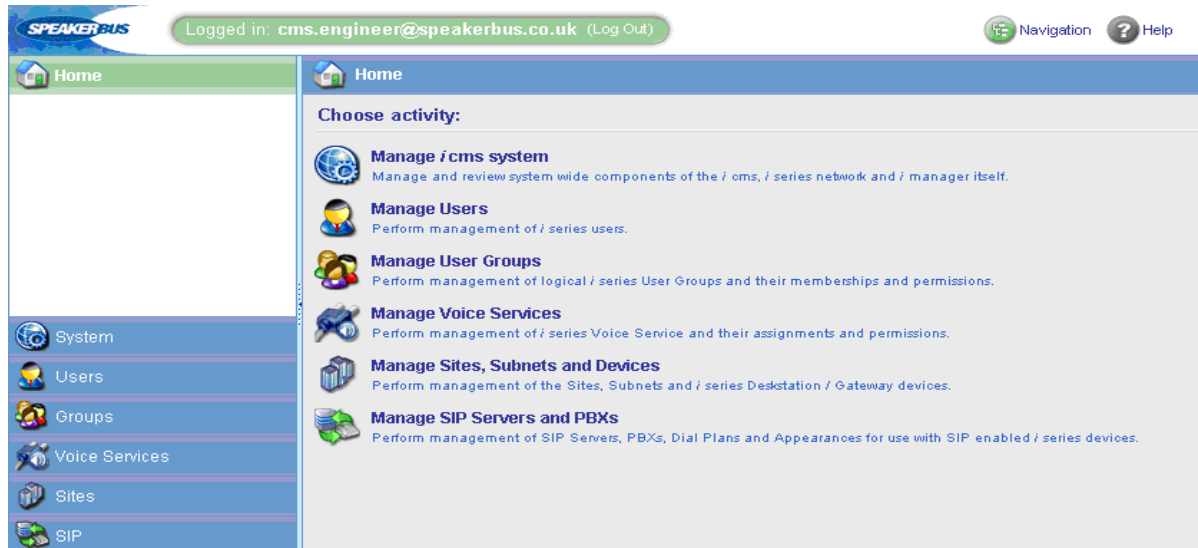
This section provides the procedure for configuring the Speakerbus iD808 *i Turret* using *i* manager Administration. The *i* manager allows users to manage the iD808 *i Turret* devices from a single workstation through a point-and-click interface using a web browser. The procedures for configuring an *i Turret* fall into the following areas:

- Launch *i* manager
- Verify Product Key
- Create Site
- Create Subnet
- Create/Announce Deskstations
- Create PBX
- Create Dial Plan
- Create Appearances
- Create Users
- Create Groups
- Assign User Permissions
- Assign Ownership (of Appearances to Users)
- Assign Default Call Appearances
- Programming iD808 Deskstations (iD808 Layout)
- Assign Appearances to Deskstation Keys (iD808 Layout)
- Assign Bridged Call Appearances to Deskstations (iD808 Layout)
- Synchronize Deskstations/Live Updates
- Feature Name Extensions (FNEs)

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

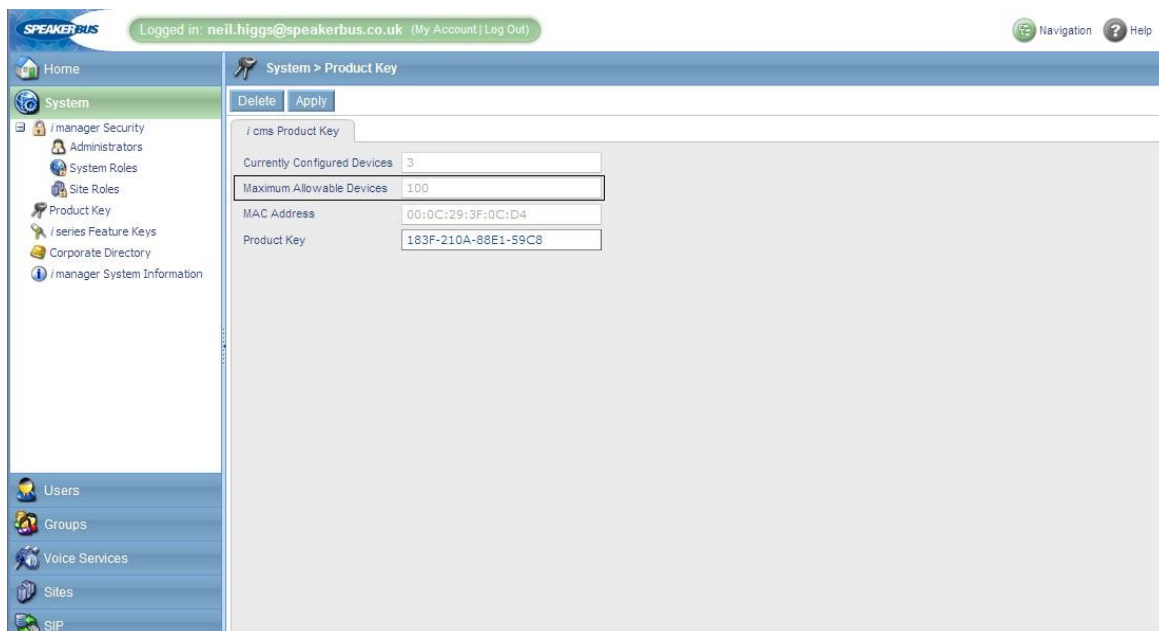
7.1. Launch *i* manager

To access the *i* manager software interface, open a web browser and type the *i* manager web address, for example, <http://10.10.16.50/imanager>. Press the **Enter** key. In the *i* manager logon page, enter the appropriate credentials. The *i* manager home page is displayed as shown below.



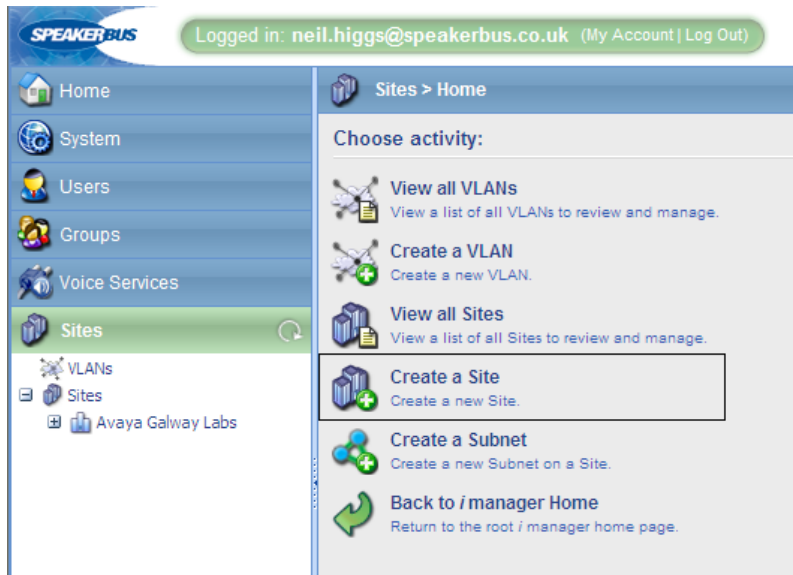
7.2. Verify Product Key

In the left “Navigation” Pane, navigate to **System → Product Key** to verify that a valid key is installed and sufficient devices are allowed.

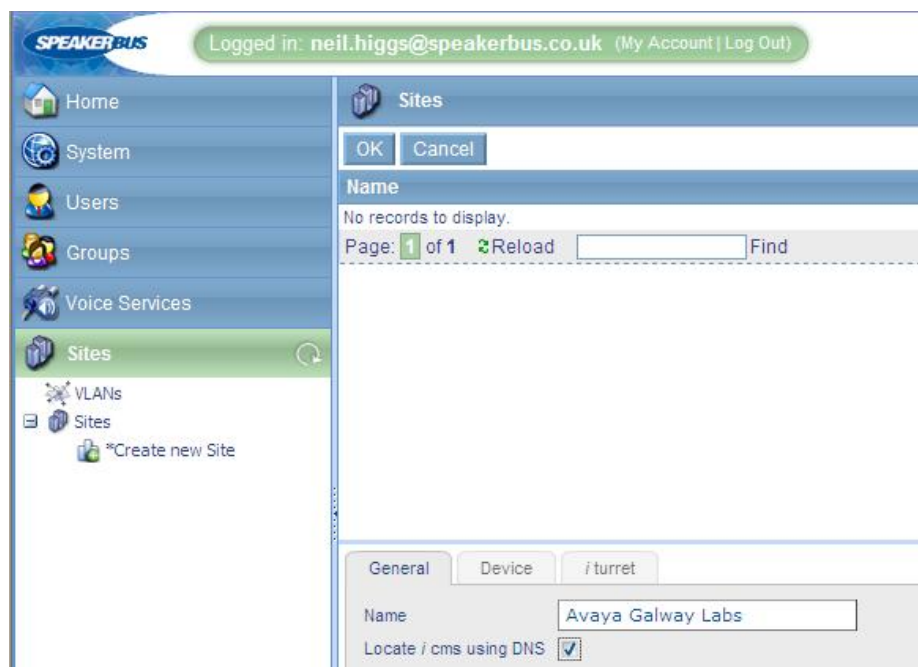


7.3. Create Site

Configure a site representing the location where the Speakerbus iTurret devices are installed. Click **Sites** in the navigation pane, click on **Create a Site** in the right pane. The **Sites** page is displayed.



In the **General** tab of the **Sites** page, set the **Name** field to a descriptive name and select the **Locate i cms using DNS** checkbox. When this option is selected, *i Turret* will use the DNS server to locate *i cms* server IP address. Refer to note [5] for the correct configuration of DNS.



In the *i Turret* tab, set the **NTP Time Zone** (network time protocol time zone) and configure the password for logging into the iTurret deskstation by clicking the **Set Admin Password** button. The NTP Server field may be set to the IP address of the NTP server if one is used. Click **Apply**. The site will be now listed under **Sites**.

The screenshot displays the Speakerbus web interface. At the top, a green status bar indicates the user is logged in as neil.higgs@speakerbus.co.uk with links for 'My Account' and 'Log Out'. The left sidebar contains a navigation menu with options: Home, System, Users, Groups, Voice Services, Sites (highlighted), VLANs, and a sub-menu for Sites including '*Create new Site'. The main content area is titled 'Sites' and shows a table with 'No records to display.' Below the table are pagination controls: 'Page: 1 of 1', a 'Reload' button, and a 'Find' input field. At the bottom, there is a configuration panel with three tabs: 'General', 'Device', and 'i turret' (selected). The 'i turret' tab contains the following fields: 'NTP Server' (text input), 'Backup NTP Server' (text input), 'Time Zone' (dropdown menu set to 'Europe: London'), 'Dial Tone Locale' (dropdown menu set to 'UK'), 'Admin Password' (password input field with 10 dots), and 'Verify Password' (password input field with 10 dots).

7.4. Create Subnet

To create a subnet, click on **Create new Subnet** under the newly configured **Avaya Galway Labs** site. In the **General** tab, provide a descriptive name for the subnet and configure the **Subnet Address** and **Default Gateway Address**.

Note: A Service Locator Record (SRV) needs to be added to the DNS server in order to allow the *i Turret* to locate and register to *i cms*. Refer to note [5] for the correct configuration of DNS.

The screenshot shows the 'Subnet' configuration page in the Avaya Galway Labs interface. The left sidebar contains a tree view with 'Sites' selected, showing 'Avaya Galway Labs' and a link to '*Create new Subnet'. The main area has a 'Subnet' section with 'OK' and 'Cancel' buttons. Below it, a table shows 'No records to display.' with pagination 'Page: 1 of 1' and a 'Find' button. The 'General' tab is active, showing fields for 'Name' (10.10.16.x), 'Site' (Avaya Galway Labs), 'Subnet Address' (10.10.16.0), and 'Default Gateway Address' (10.10.16.1). The 'SbRTP' and 'Device' tabs are also visible.

In the **SbRTP** tab, set the **Compatibility** field to **Version 3.0**, leave everything else as default.

The screenshot shows the 'Subnet' configuration page in the Avaya Galway Labs interface, specifically the 'SbRTP' tab. The left sidebar is the same as the previous screenshot. The main area shows the 'SbRTP' tab with fields for 'RTP Payload Code' (96), 'DSCP Value' (0), 'i turret Bandwidth' (Standard), 'Compatibility' (Version 3.0), 'Packet Size' (1 ms), and 'Voice Activity Detection' (unchecked). The 'General' and 'Device' tabs are also visible.

In the **Device** tab, set the ***Turret Logging TFTP Server IP Address*** and make sure the **Live Updates Enabled** tick box is checked (the latter means that changes made in *i* cms will be sent automatically to the turret without the need of synchronization). Click **OK**.

The screenshot displays the Avaya Aura Management Console interface. On the left is a navigation pane with a tree structure: Home, System, Users, Groups, Voice Services, Sites (highlighted), VLANs, Sites, Avaya Galway Labs, and *Create new Subnet. The main content area is titled 'Sites > Avaya Galway Labs > Subnets' and contains 'OK' and 'Cancel' buttons. Below this is a 'Subnet' section with the text 'No records to display.' and a pagination bar showing 'Page: 1 of 1', a 'Reload' button, and a 'Find' input field. At the bottom, there are three tabs: 'General', 'SbRTP', and 'Device' (selected). The 'Device' tab contains three sections: 'General' with 'Enable Auto Discovery' (unchecked), 'i series' with 'Enable API Service' (unchecked), and 'i turret' with 'Logging TFTP Server IP Address' (set to '10.10.16.74') and 'Live Updates Enabled' (checked).

7.5. Create Deskstations

i Turret deskstations will automatically register to this subnet within *i cms* as the appropriate DHCP and DNS records were created prior to iTurret deskstations being connected to the IP network. The newly registered deskstations are automatically displayed in the list.

The screenshot shows the Speakerbus web interface. The top navigation bar includes a logo, a login status "Logged in: neil.higgs@speakerbus.co.uk (My Account | Log Out)", and links for "Navigation" and "Help". The left sidebar contains a menu with "Home", "System", "Users", "Groups", "Voice Services", and "Sites". The "Sites" menu is expanded, showing "VLANs", "Sites", "Avaya Galway Labs", "10.10.16.x", "Gateways", "Deskstations", and "Voice Services". The main content area displays the "Deskstations" page for the "10.10.16.x" site. The page has tabs for "General", "Channels", "Connections", "Recording Streams", and "Ethernet Ports". Below the tabs are buttons for "New", "Delete", "Apply", "Seat...", "Unseat", "Synchronise", and "Firmware...". A table lists the deskstations with columns for Name, Type, IP Address, MAC Address, Firmware, and Seat. The table contains three rows: Device10, Device8, and Device9, all of type "turret". Below the table is a pagination bar showing "Page: 1 of 1", a "Reload" button, and a "Find" input field. At the bottom of the page, there are tabs for "General", "IP", "Network", "Feature Key", "SbRTP", "Deskstation", "Gateway", and "Test Tones".

Name	Type	IP Address	MAC Address	Firmware	Seat
Device10	turret	10.10.16.76	00:05:83:00:14:3A	1.300.16.0	
Device8	turret	10.10.16.75	00:05:83:00:14:D3	1.300.16.0	
Device9	turret	10.10.16.63	00:05:83:00:10:F4	1.300.16.0	

Select a device and change the name to a more descriptive one in the **General** tab.

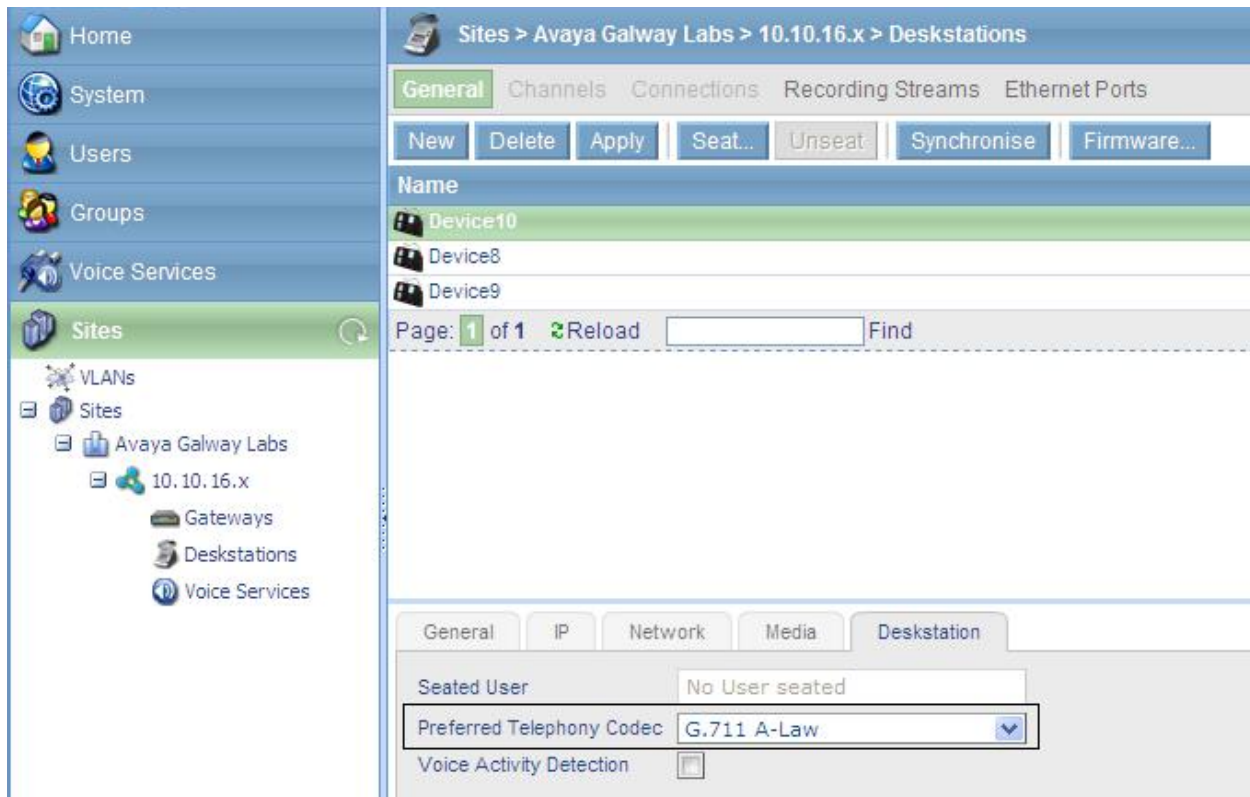
The screenshot shows the Speakerbus web interface. The left sidebar contains navigation links: Home, System, Users, Groups, Voice Services, and Sites. The 'Sites' link is selected, and the breadcrumb trail indicates the path: Sites > Avaya Galway Labs > 10.10.16.x > Deskstations. The main content area has tabs for General, Channels, Connections, Recording Streams, and Ethernet Ports. The 'General' tab is active, displaying a table of devices. The table has columns for Name, Type, IP Address, MAC Address, Firmware, and Seated User. The devices listed are Device8, Device9, and iTurret A. Below the table, there is a form for editing the selected device, iTurret A. The form fields are: Name (iTurret A), Type (i turret), MAC Address (00:05:83:00:14:3A), Firmware Version (1.300.16.0), and Location (empty).

Name	Type	IP Address	MAC Address	Firmware	Seated User
Device8	/ turret	10.10.16.75	00:05:83:00:14:D3	1.300.16.0	
Device9	/ turret	10.10.16.63	00:05:83:00:10:F4	1.300.16.0	
iTurret A	/ turret	10.10.16.76	00:05:83:00:14:3A	1.300.16.0	iTurret A

In the **IP** tab, verify that the **Obtain IP Address using DHCP** and the **Obtain local Domain Name using DHCP** tick boxes are checked (make sure you have a running DHCP and DNS Server on the network with relevant settings in both).

The screenshot shows the Speakerbus web interface with the 'IP' tab selected for the device 'Device10'. The breadcrumb trail is: Sites > Avaya Galway Labs > 10.10.16.x > Deskstations. The 'IP' tab is active, displaying configuration options. The 'Obtain IP Address using DHCP' checkbox is checked, and the IP Address field shows 10.10.16.76. The 'Obtain Local Domain Name using DHCP' checkbox is also checked, and the Local Host Name field shows id808-00143A. Other fields include IE801 #1 IP Address, IE801 #2 IP Address, and DHCP Server Timeout (60).

In the **Deskstation** tab, select a preferred codec. In this configuration, **G.711 A-law** is the preferred codec. Click **Apply**. Repeat these steps for all deskstations.



7.6. Create SIP Server

To create a SIP Server, click **Create a new SIP Server** under the **SIP** directory in the navigation pane. Provide a descriptive name for the SIP server and select **AVAYA** from the **Type** dropdown box. In the **Registrar Address** and **SIP Domain** fields set to **sip.avaya.com**, in this configuration DNS resolves the domain name to 10.10.16.5, the SIP Enablement Services active IP address. After the SIP server is created, the **Port** field will be displayed on this page with the default value of 5060.

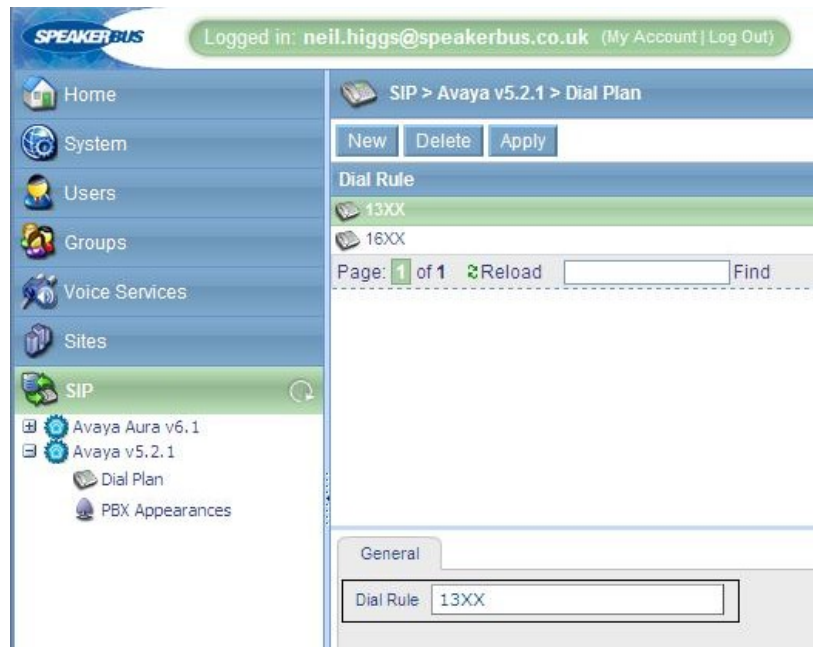
Note: A server locator record (SRV) for the registrar address and SIP domain must be created on DNS. Refer to note [5] for the correct configuration of DNS.

The screenshot shows the Speakerbus web interface. The top navigation bar includes the Speakerbus logo and a login status: "Logged in: neil.higgs@speakerbus.co.uk (My Account | Log Out)". The left sidebar contains a navigation menu with icons for Home, System, Users, Groups, Voice Services, Sites, and SIP. The SIP menu is expanded, showing sub-items: Avaya Aura v6.1, Avaya v5.2.1, Dial Plan, and PBX Appearances. The main content area is titled "SIP > PBXs" and contains buttons for "New", "Delete", and "Apply". Below these is a table listing SIP servers: "Avaya Aura v6.1" and "Avaya v5.2.1". The "Avaya v5.2.1" entry is highlighted. Below the table is a pagination bar showing "Page: 1 of 1", a "Reload" button, and a search field. At the bottom, there is a configuration form for the selected server. The form has three tabs: "General", "Inbound", and "Outbound". The "General" tab is active, showing fields for "Name" (Avaya v5.2.1), "Type" (Avaya), and "Port" (5060). Below these is a "PBX Settings" section with fields for "Registrar Address" (sip.avaya.com) and "SIP Domain" (sip.avaya.com).

The **Outbound** and **Inbound** tabs are left with their default values. Click **OK**.

7.7. Create Dial Plan

Under the **SIP** directory, click **Dial Plan** and then the **New** button to add a dial rule. Dial rules specify the valid digit formats that the iTurret devices are allowed to dial, otherwise the user will have to press OK after entering the dial string on the iTurret device. In this configuration, 4-digit extensions beginning with **13** were used to dial other iTurret devices and Avaya telephones. A dial rule is also required for the voicemail pilot number which was a 4-digit extension beginning with **16**. The example below corresponds to 4-digit extensions beginning with **1**. The X's in the dial rule match any digit. Note that the **X** must be a capital letter. Click **OK**. Repeat this for all valid extension formats, including the handset extensions.



7.8. Create Call and Handset Appearances

Three call appearances need to be created for each iTurret device, 1 for its main appearance, then one each for the privacy handset 1 and privacy handset 2. As previously mentioned, three extensions are also required on Communication Manager and SIP Enablement Services. To create the main appearance, click **PBX Appearances** under the **Avaya PBX**. Click the **New** button, then select the **Type** of appearance you want to create (Call, Privacy 1 or Privacy 2). In 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.









The screenshot shows the SpeakerBus web interface. The top navigation bar includes the SpeakerBus logo and a login status for 'neil.higgs@speakerbus.co.uk'. The left sidebar contains a tree view with categories like Home, System, Users, Groups, Voice Services, Sites, and SIP. Under the SIP category, 'Avaya v5.2.1' is selected, leading to the 'PBX Appearances' page. The main content area has a breadcrumb 'SIP > Avaya v5.2.1 > PBX Appearances' and tabs for 'General', 'User Permissions', and 'Group Permissions'. The 'General' tab is active, showing a list of existing appearances with columns for Name and Ext. Below the list is a 'Page: 1 2 3 4 5 of 5' indicator and a 'Find' search box. A 'New' button is visible. A modal window titled 'Call Appearance Settings' is open, displaying fields for Name (Ext 1302), Long Label (Extension 1302), Address (1302), Maximum PBX Appearances (3), Allow Outbound Calls (checked), Message Indication (checked), Authentication Name (1302), Authentication Password (masked), and Verify Password (masked).

Set the **Maximum Appearances** field to the number of call appearances configured on the station in Communication Manager minus one since the last call appearance is restricted. See the button assignment section of the station form and the second page of the Off-PBX-Telephone Station-Mapping form in **Section 5.10** as an example. The number of call appearance buttons dictates the number of calls on the system the user can have directed to them. When all of a user's call appearances are in-use (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. Check the **Allow Outbound Calls**. The **Authentication Name** and **Authentication Password** fields should be set to the extension and password, respectively, configured on SIP Enablement Services. These are the credentials that the iTurret deskstation will use to authenticate and register with SIP Enablement Services. Use the default values for the other fields as shown below. Click **OK**.

Next, this procedure will be repeated for the two privacy appearances. Click the **New** button to add another appearance. In the **General** tab, set the **Type** field to **Privacy 1**. Then add in the **Address**, **Authentication Name** and **Authentication Password** fields. The latter fields should be identical to that set up in SIP Enablement Services for registration to occur. Press **OK** to commit the created appearance.

The screenshot shows the SpeakerBus web interface. The top navigation bar includes the SpeakerBus logo and a login status: "Logged in: neil.higgs@speakerbus.co.uk (My Account | Log Out)". The left sidebar contains a menu with options: Home, System, Users, Groups, Voice Services, Sites, SIP, Avaya Aura v6.1, Avaya v5.2.1, Dial Plan, and PBX Appearances. The main content area is titled "SIP > Avaya v5.2.1 > PBX Appearances" and has tabs for "General", "User Permissions", and "Group Permissions". The "General" tab is active, showing a list of appearances with columns for Name, Address, Authentication Name, and Authentication Password. The list shows two entries: "Ext 1301" and "Ext 1303". Below the list is a "Page: 1 2 3 4 5 of 5" indicator and a "Find" button. A "General" settings dialog box is open, showing the "Type" field set to "Privacy 1". The "Privacy Appearance Settings" section includes fields for "Address" (1501), "Authentication Name" (1501), "Authentication Password" (masked with dots), and "Verify Password" (masked with dots). "OK" and "Cancel" buttons are visible at the top of the dialog.

Repeat the above procedure to add the Privacy 2 appearance. The call appearances for the previously configured iTurret deskstations are listed below.

SIP > Avaya v5.2.1 > PBX Appearances				
General User Permissions Group Permissions				
New Delete Apply Assign Ownership... Clear Ownership				
Name	Long Label	Address	Type	Owner
 Ext 1301	Extension 1301	1301	Call	Turret User 1
 Ext 1303	Extension 1303	1303	Call	Turret User 2
 Ext 1305	Extension 1305	1305	Call	Turret User 3
 Turret User 1 PV1	Turret User 1 PV1	1501	Privacy 1	Turret User 1
 Turret User 1 PV2	Turret User 1 PV2	1502	Privacy 2	Turret User 1
 Turret User 2 PV1	Turret User 2 PV1	1503	Privacy 1	Turret User 2
 Turret User 2 PV2	Turret User 2 PV2	1504	Privacy 2	Turret User 2
 Turret User 3 PV1	Turret User 3 PV1	1505	Privacy 1	Turret User 3
 Turret User 3 PV2	Turret User 3 PV2	1506	Privacy 2	Turret User 3
Page: 1 of 1 Reload Find				

Repeat the above procedures for adding the Main and Privacy appearances for each iD808 deskstation.

7.9. Create Users

In this section, the users are created. In the navigation panel click on **Users** and in the directory tree expand **User by Site**, click on **Avaya Galway Labs** followed by **New**. In the **General** tab, provide a descriptive name in the **Name** field. Then press **OK**.

The screenshot shows the Speakerbus web interface. The top navigation bar includes 'Home', 'System', and 'Users'. The 'Users' section is expanded, showing 'User Templates', 'Users by Group', 'Users by Site', 'Not seated', and 'Avaya Galway Labs'. The 'Users by Site' section is further expanded, showing 'Not seated' and 'Avaya Galway Labs'. The 'Avaya Galway Labs' section is expanded, showing 'Not seated' and 'Avaya Galway Labs'. The 'General' tab is active, and the 'Name' field is populated with 'iTurret A'. The 'Local Muting' dropdown is set to 'Duplex'.

Logged in: neil.higgs@speakerbus.co.uk (My Account | Log Out)

Users > By Site > *Not seated

General | Group Memberships | Voice Services | PBX Appearances | Alerts | Personal Dir. | /turret Layout

OK Cancel

Name | Logon ID | Logon P

No records to display.

Page: 1 of 1 Reload Find

General | i series | i turret | iE801

Name iTurret A

Local Muting Duplex

In the **iTurret** tab, provide the logon credentials for the user to log into their iTurret deskstation and enter the pilot number for Voicemail in the **Voicemail Server Address** field. This page will be revisited later in **Section 7.13** to configure the default call appearance for this deskstation. Click **Apply**.

Users > By Site > *Not seated

General Group Memberships Voice Services PBX Appearances Alerts Personal Dir. i turret Layout

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

Name	Logon ID
iTurret A	

Page: 1 of 1 Reload Find

General i series i turret iE801

Logon Name iTurretA

Logon Password

Verify Password

Voicemail Server Address 1699

Default PBX Appearance Type [None]

Default PBX Appearance [None]

Dynamic Keys Call Display All Calls

Latching Type Tap Latch

Speaker Activity Indication Timeout (ms) 1500

Always use Large Cisco Profile ☒

Repeat the previous procedure to add more users.

After a user has been created, the user needs to be **seated** on an iTurret deskstation. In the left panel under the **Users** directory tree, click the ***Not seated** link under **Users by Site** to display the list of users. Select the user previously configured (i.e., iTurret A) and click on the **Seat...** button.

The screenshot shows the Avaya Aura User Management web interface. On the left, the 'Users' directory tree is expanded to 'Users by Site', and the '*Not seated' link is selected. The main panel displays a list of users, with 'iTurret A' selected. The 'Seat...' button is highlighted. Below the list, the user's profile is shown with various configuration options.

Name	Logon ID
iTurret A	

Page: 1 of 1 Reload Find

General i series i turret iE801

Logon Name: iTurretA
Change Password...

Voicemail Server Address: 1699

Default PBX Appearance Type: [None]

Default PBX Appearance: [None]

Dynamic Keys Call Display: All Calls

Latching Type: Tap Latch

Speaker Activity Indication Timeout (ms): 1500

Always use Large Cisco Profile: ☒

On the next page, filter options are presented. Filter deskstations in the **Avaya Galway Labs** site, **10.10.16.x** subnet and **i Turret** in products as shown below. The user will be seated on an iTurret deskstation with these properties. Click **Next**.

The screenshot shows the 'Step 1: Select Deskstation filter options' dialog box. It contains four filter options: Site, Subnet, Product, and Show only free Deskstations. The Site is set to 'Avaya Galway Labs', Subnet is '10.10.16.x', and Product is 'i turret'. The 'Show only free Deskstations' checkbox is checked. At the bottom, there are buttons for 'Cancel', '< Back', 'Next >', and 'Finish'.

Step 1: Select Deskstation filter options

Site: Avaya Galway Labs

Subnet: 10.10.16.x

Product: i turret

Show only free Deskstations: ☒

Cancel < Back Next > Finish

In the resulting deskstation list, select the iTurret deskstation where the selected user will be seated. In this example, the user will be seated on the iTurret A deskstation. Select **iTurret A** in the list and click **Finish**.

Step 2: Select a Deskstation to seat the User at

Selected Deskstation:

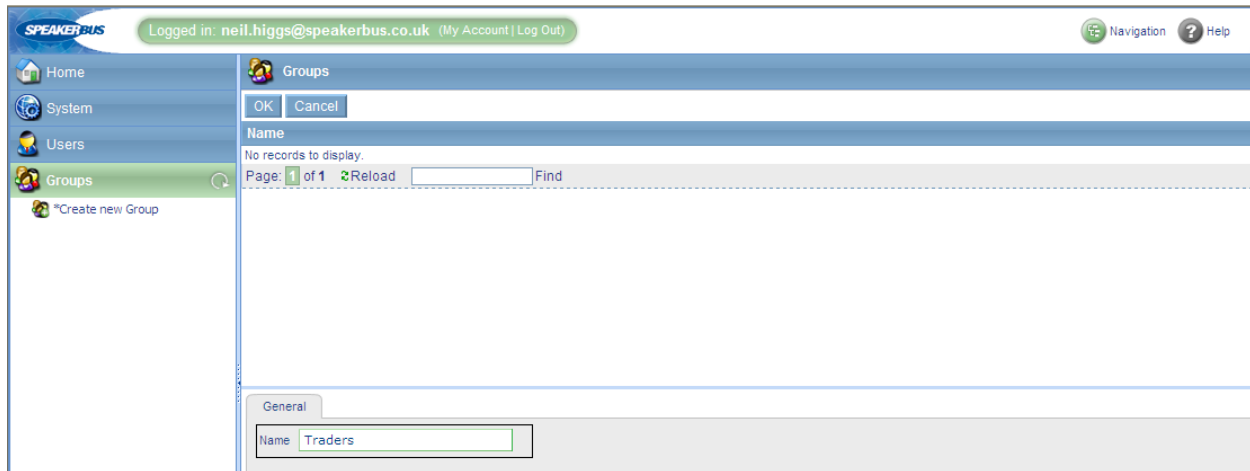
Name	Site	Subnet	Product	IP Address	MAC Address	Seat
Device10	Avaya Galway Labs	10.10.16.x	i turret	10.10.16.76	00:05:83:00:14:3A	
Device8	Avaya Galway Labs	10.10.16.x	i turret	10.10.16.75	00:05:83:00:14:D3	
Device9	Avaya Galway Labs	10.10.16.x	i turret	10.10.16.83	00:05:83:00:10:F4	

Page: 1 of 1 Reload Find

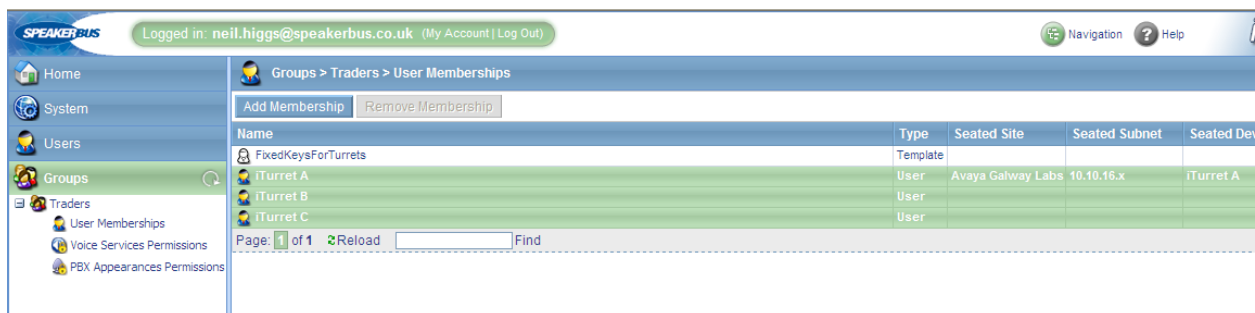
The user has been successfully seated as indicated by the deskstation displayed in the **Seated Device** column on the following page. Repeat this procedure for seating other users.

7.10. Create Group

To create a group; in the navigation pane under the **Groups** directory tree click on **Create new Group**. In the **General** tab, provide a descriptive name in the **Name** field, such as **Traders**. Click **OK**. The **Traders** group has been successfully added.

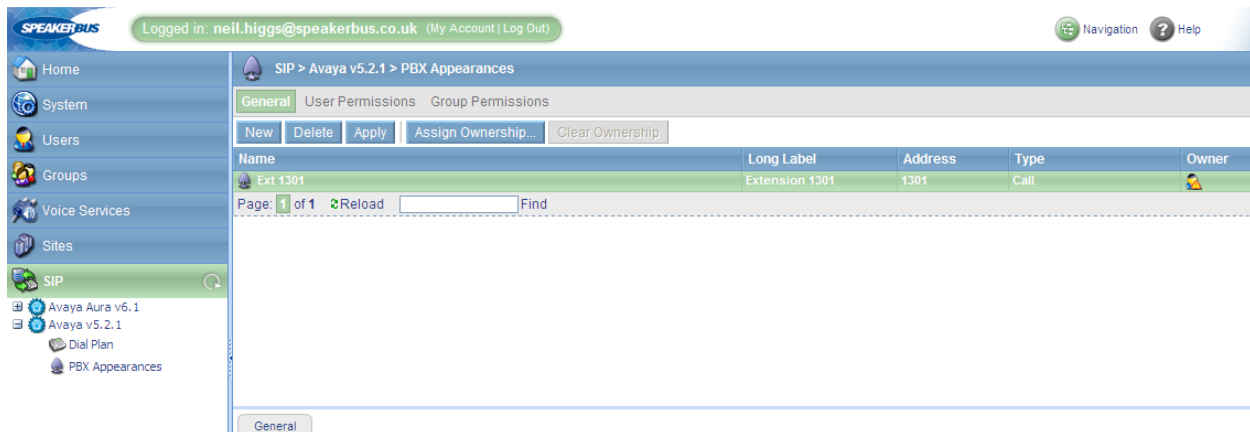


The user is now added to this new group. In the **Groups** directory tree, expand **Traders** and click on **User Memberships** in the left pane. A list of users is displayed. Select all the users to be added to the Traders group as shown below and then click **Add Membership**. The **Is Member** column will then indicate that the selected users are members of the Traders group (not shown).

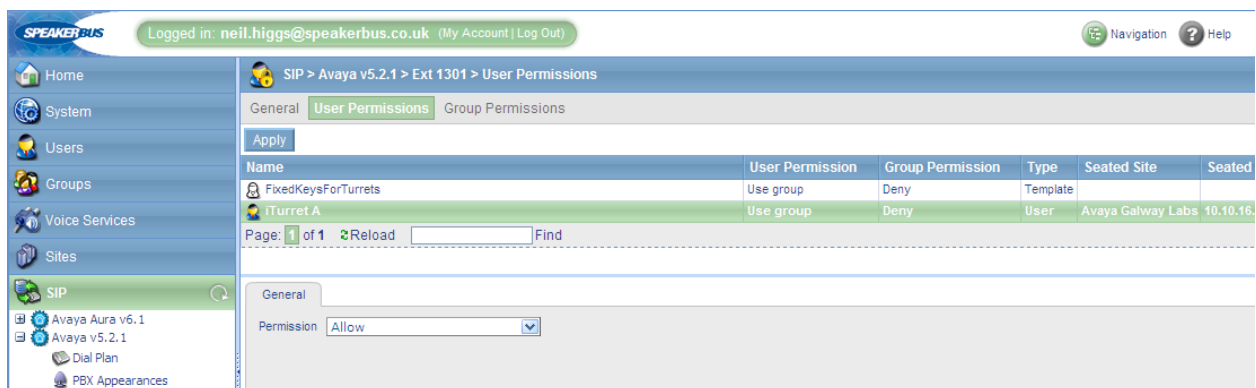


7.11. Assign User Permissions

The next step will be to assign appearances permissions to users. In the navigation pane, expand **Avaya** and click on **PBX Appearances**. The list of appearances is displayed. Select the main call appearance for **iTurret A** (i.e., **1301**) and click **User Permissions**.



On the resulting page select the user to which the appearance will be assigned. Set the **Permission** field to **Allow** as shown below. Click **Apply**. Assign the relevant Privacy 1 and Privacy 2 permissions to this user by repeating this procedure.



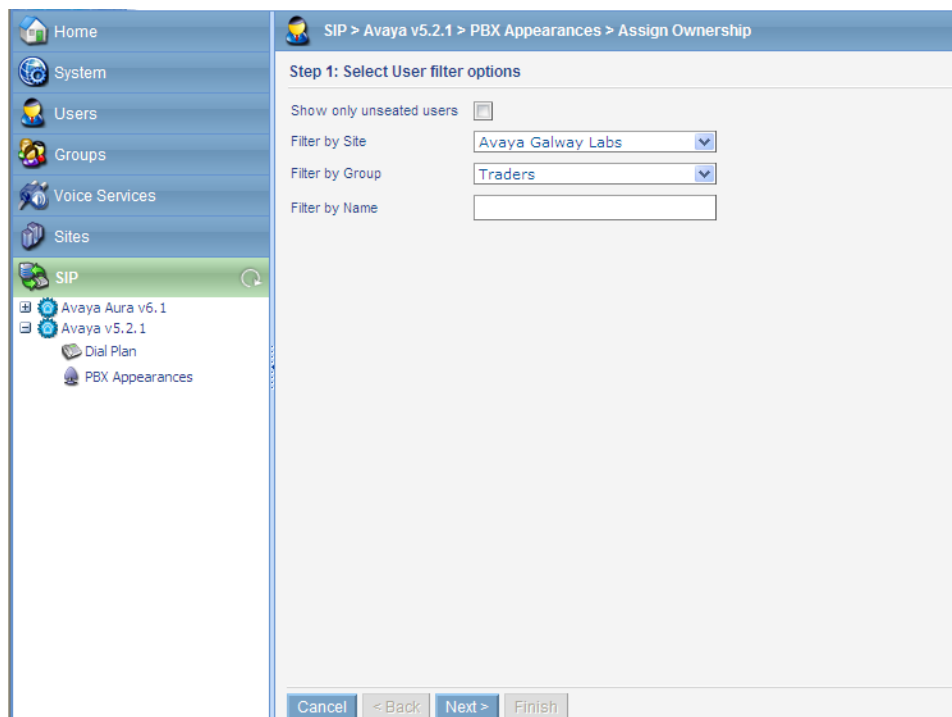
If other users require an appearance as a bridged line then those users must also have permissions to the appearance. For the compliance test, user **iTurret B** and **iTurret C** had a bridged line appearance for 1301, so both users are assigned permissions for appearance 1301 as indicated by the **User Permission** column shown below.

7.12. Assign Ownership

To assign ownership of the appearances to a user, in the navigation pane, expand **Avaya** and click on **PBX Appearances** to display the appearances list as shown below. In the **General** tab, select the main call appearance and click on the **Assign Ownership...** button.



The next page filter options are presented. Filter users in the **Avaya Galway Labs** site and in the **Traders** group as shown below. Click **Next**.



On the next page, select the user to which ownership will be assigned to the main call appearance. In this example, the main call appearance **1301** will be assigned to **iTurret A**. Click **Finish**.

The screenshot shows the Speakerbus web interface. The user is logged in as neil.higgs@speakerbus.co.uk. The navigation menu on the left includes Home, System, Users, Groups, Voice Services, Sites, SIP, and PBX Appearances. The main content area is titled 'SIP > Avaya v5.2.1 > PBX Appearances > Assign Ownership'. It shows 'Step 2: Select a User to assign ownership to'. The 'Selected User' is 'iTurret A'. Below this, there is a table with one row: 'iTurret A'. The page is 'Page: 1 of 1'. At the bottom, there are buttons: 'Cancel', '< Back', 'Next >', and 'Finish'.

Repeat this procedure to assign Privacy 1 and Privacy 2 call appearances to iTurret A.

7.13. Assign Default Call Appearance

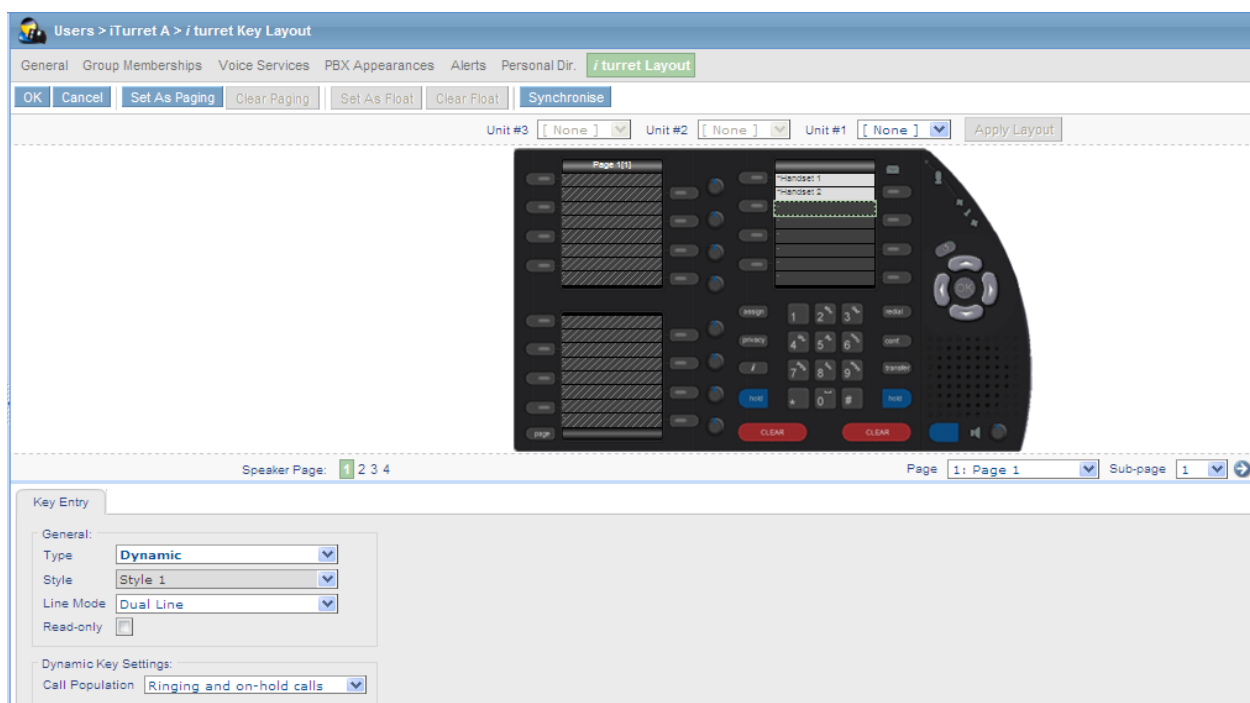
In the **Users** directory tree, navigate to **Users by Site** → **Avaya Galway Labs** and click **10.10.16.x** link to display the users list. Set the **Default Appearance** field to the main call appearance (e.g., **1301**). Click **Apply**.

The screenshot shows the Speakerbus web interface. The user is logged in as neil.higgs@speakerbus.co.uk. The navigation menu on the left includes Home, System, Users, Groups, Voice Services, Sites, SIP, and PBX Appearances. The main content area is titled 'Users'. It shows a list of users with columns for 'Name' and 'Login ID'. The user 'iTurret A' is selected. Below the list, there is a form for 'iTurret A'. The form has tabs for 'General', '/ series', '/ turret', and 'iE801'. The 'General' tab is active. It contains fields for 'Logon Name' (iTurretA), 'Voicemail Server Address' (1699), 'Default PBX Appearance Type' (Call), 'Default PBX Appearance' (Ext 1301), 'Dynamic Keys Call Display' (All Calls), 'Latching Type' (Tap Latch), 'Speaker Activity Indication Timeout (ms)' (1500), and 'Always use Large Cisco Profile' (checked). There is a 'Change Password...' button next to the 'Logon Name' field.

7.14. Programming iTurret Deskstations

This section describes how to create iTurret deskstation keys. The following keys can be created using the iTurret layout page: Dynamic, Appearance, Shortcut, Soft Function, and Speed Dial amongst others. In this configuration, each user will be configured with three Dynamic keys, two Soft Function keys, and one Shortcut key. Although the configuration may vary, this configuration is suitable for most users. In left panel under the **Users** directory tree, expand **Users by Site → Avaya Galway Labs** and click on **10.10.16.x** link to display a list of users. Select a user (e.g., **iTurret A**) and click **iTurret Layout** to display the iTurret key layout for this user.

In the iTurret key layout, click on the key highlighted below Handset 2. In the Key Entry tab, set the **Type** field to **Dynamic**. Click **OK**.



Three Dynamic keys will be added so repeat this step for the next two keys.

Next, configure two Soft Function keys. Select the next available key under the last Dynamic key. In the **Key Entry** tab, set the Type field to **Soft Function** and select **General** from the **soft key type** dropdown box, and click **OK**. Repeat this step for the second Soft Function key.

Users > iTurret A > iTurret Key Layout

General Group Memberships Voice Services PBX Appearances Alerts Personal Dir. iTurret Layout

OK Cancel Set As Paging Clear Paging Set As Float Clear Float Synchronise

Unit #3 [None] Unit #2 [None] Unit #1 [None] Apply Layout

Page 1(1)

Speaker Page: 1 2 3 4 Page 1: Page 1 Sub-page 1

Key Entry

General:

Type: Soft Function

Style: Style 1

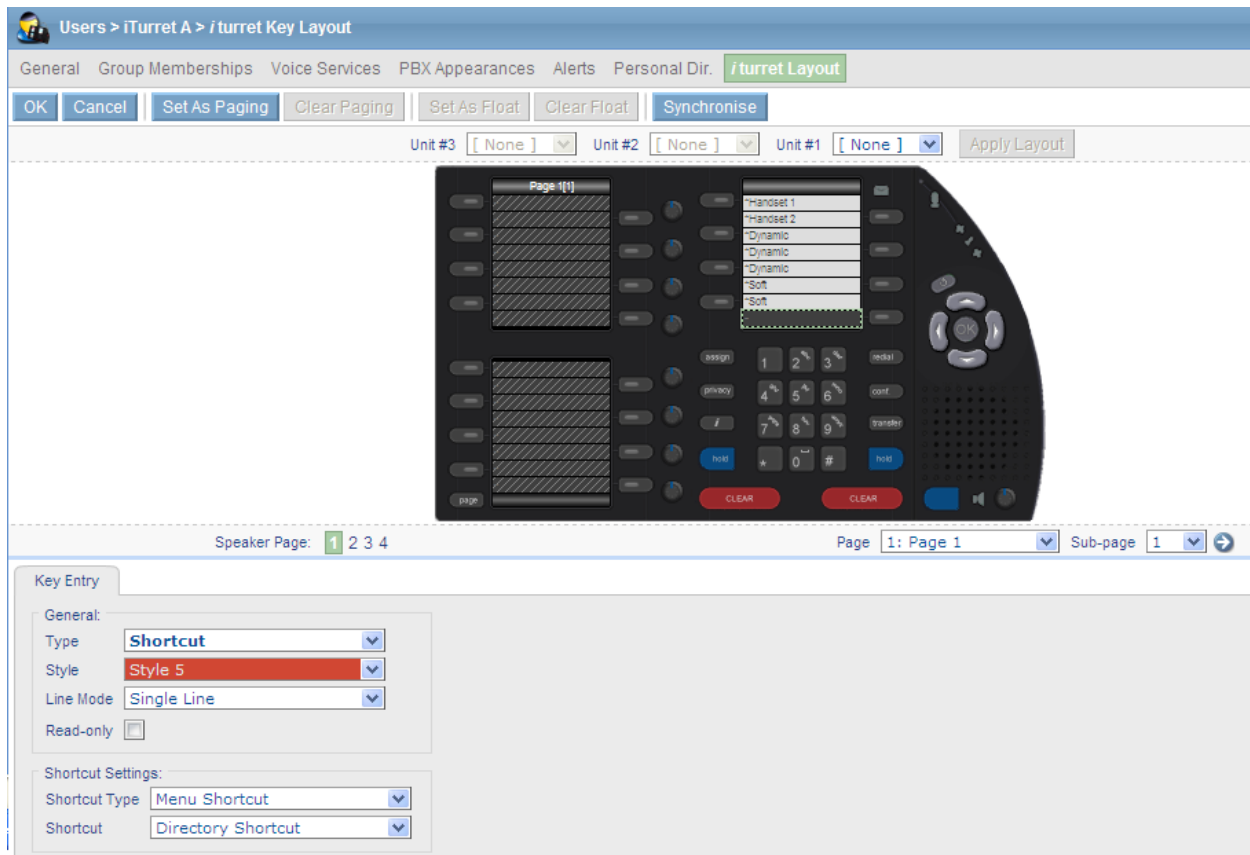
Line Mode: Single Line

Read-only: ☐

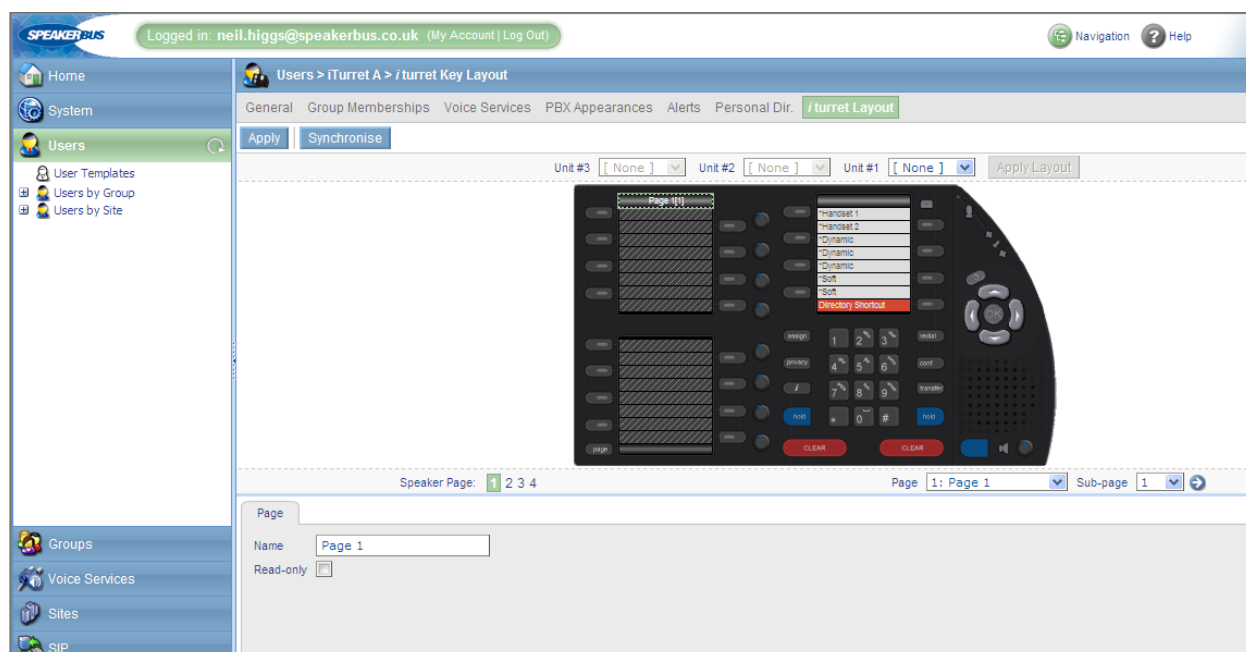
Soft Function Settings:

Soft Function Type: General

Finally, add a Shortcut key under the last Soft Function key. In the **Key Entry** tab, set the **Type** field to **Shortcut**. Set the **Shortcut type** field to **Menu Shortcut**. Set the **Shortcut** field to **Directory Shortcut**. Click **OK**.

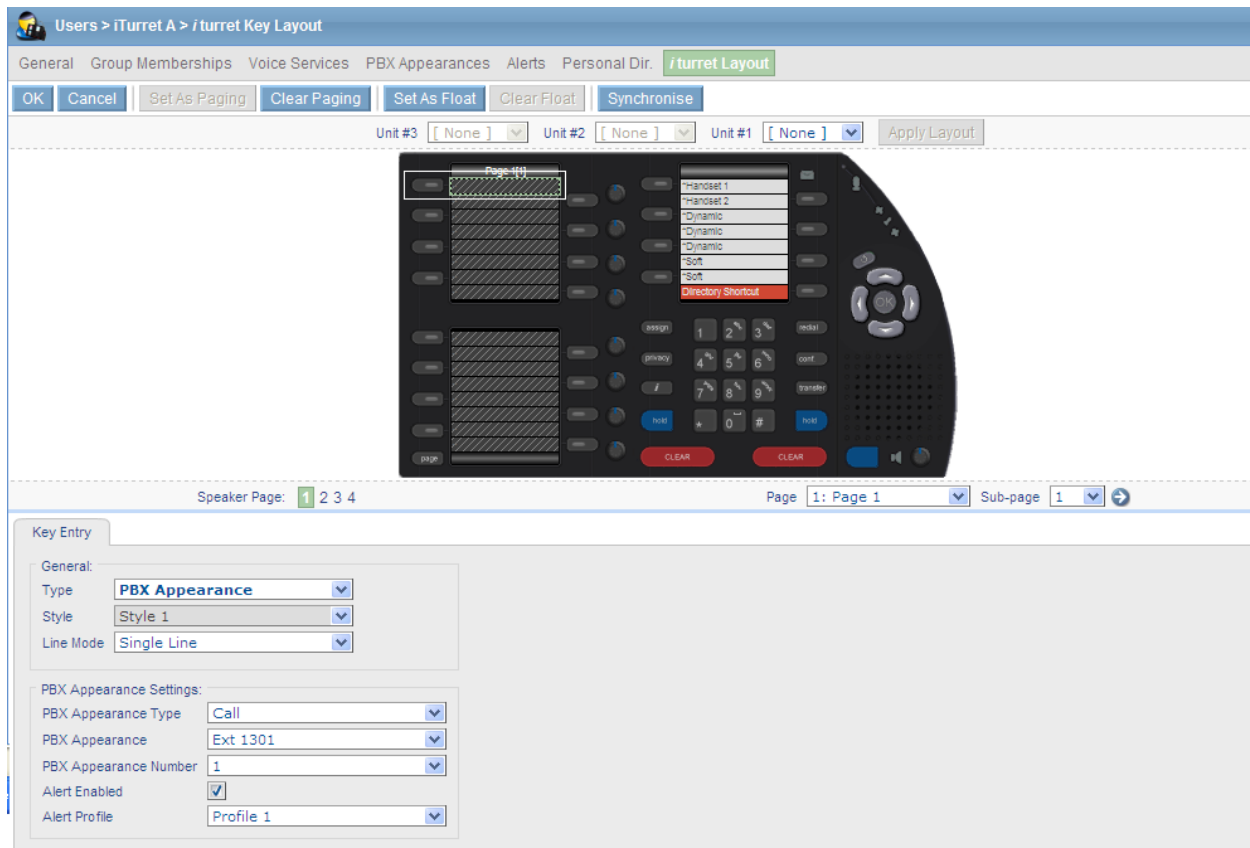


After all of the iD808 keys have been created on the deskstation, the iTurret layout will appear as shown below.



7.15. Assigning Appearances to Deskstation Keys

In the iTurret key layout page, go to **Page 1** of the deskstation by setting the **Page** field to **1** in the **Page** tab and clicking the arrow key to the right. Select the next available key as highlighted by the white box below. The next three keys on this page will be assigned to call appearances. In the **Key Entry** tab, set the **Type** field to **PBX Appearance**. Under the **PBX Appearance Settings**, select the **PBX Appearance Type** (Call in this case), **PBX Appearance** (Ext 1301 in this case), **PBX Appearance Number** (1 in this case) and check **Alert Enabled** and leave Profile 1 as default for **Alert Profile**. Click **OK**. Repeat this procedure to add the next two call appearances.



Users > iTurret A > /turret Key Layout

General Group Memberships Voice Services PBX Appearances Alerts Personal Dir. /turret Layout

OK Cancel Set As Paging Clear Paging Set As Float Clear Float Synchronise

Unit #3 [None] Unit #2 [None] Unit #1 [None] Apply Layout

Speaker Page: 1 2 3 4 Page 1: Page 1 Sub-page 1

Key Entry

General:

Type: PBX Appearance

Style: Style 1

Line Mode: Single Line

PBX Appearance Settings:

PBX Appearance Type: Call

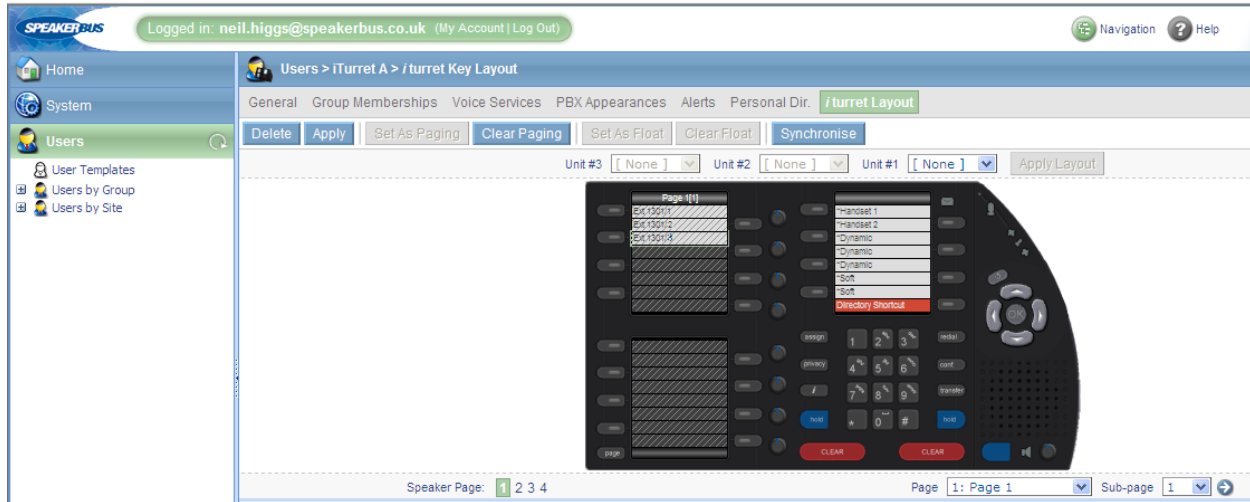
PBX Appearance: Ext 1301

PBX Appearance Number: 1

Alert Enabled: ☒

Alert Profile: Profile 1

Once the three call appearances have been added, the iTurret layout will appear as follows.



7.16. Assign a Bridge Call Appearance to Deskstation

In the iTurret key layout page, go to **Page 1** of the deskstation by setting the **Page** field to **1** in the **Page** tab and clicking the arrow key to the right. Select the next available key in the lower section of page one. The next three keys on this page will be assigned to bridge call appearances. In the **Key Entry** tab, set the **Type** field to **PBX Appearance**. Under the **PBX Appearance Settings**, select the **PBX Appearance Type** (Call in this case), **PBX Appearance** (Ext 1311 in this case), **PBX Appearance Number** (1 in this case) and check **Alert Enabled** and leave Profile 1 as default for **Alert Profile**. Click **OK**.

Repeat this procedure to add the next two bridge call appearances.

Users > iTurret A > / turret Key Layout

General Group Memberships Voice Services PBX Appearances Alerts Personal Dir. / turret Layout

OK Cancel Set As Paging Clear Paging Set As Float Clear Float Synchronise

Unit #3 [None] Unit #2 [None] Unit #1 [None] Apply Layout

Page 1(1)

Speaker Page: 1 2 3 4 Page 1: Page 1 Sub-page 1

Key Entry

General:

Type: **PBX Appearance**

Style: **Style 1**

Line Mode: **Single Line**

PBX Appearance Settings:

PBX Appearance Type: **Call**

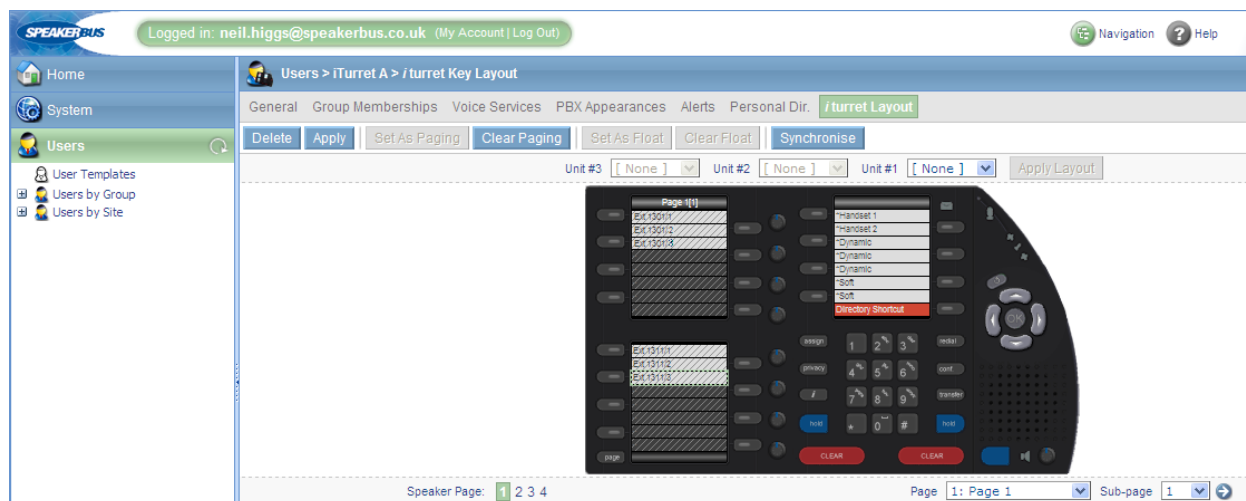
PBX Appearance: **Ext 1311**

PBX Appearance Number: **1**

Alert Enabled: ☒

Alert Profile: **Profile 1**

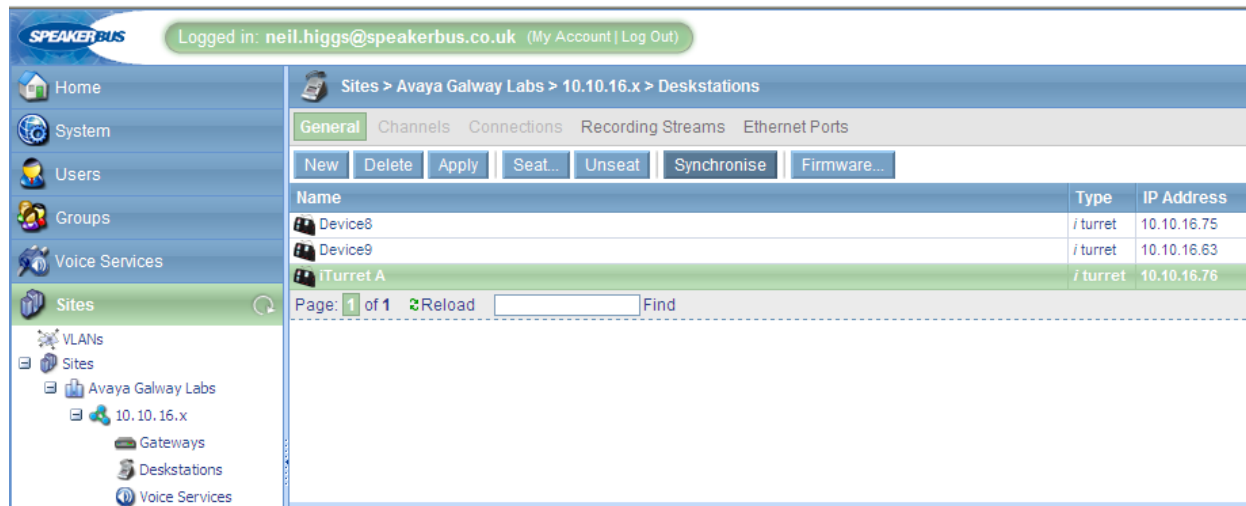
Once the three bridge call appearances have been added, the iD808 layout will appear as follows.



7.17. Synchronise Deskstations

With Live updates enabled, see **Section 7.4** to confirm you have enabled this as default. Any changes you make to the profile within *i cms* will be updated on the device after **OK** or **Apply** is pressed (any changes to site and subnet details will need a synchronization). If you want to synchronise a Turret device manually, go to **Sites** directory tree, expand **Avaya Galway Labs** → **10.10.16.x** and click on **Deskstations** to display the deskstation list. Select the desired deskstations and click the **Synchronise** button. The iTurret deskstation will indicate that they are being synchronized on their displays. After the deskstations have been synchronized, the status icons on the iTurret deskstations corresponding to the network, *i cms*, and SIP registrar status should be green.

Note: Executing a synchronisation will cause active calls on the deskstation being synchronised to drop.



7.18. Feature Name Extensions (FNEs)

FNEs can be accessed by dialing the appropriate number via the dial pad. It is also possible to create FNEs as speed dials by defining the FNE in the corporate or personal directory within *i* cms. Please refer to Speakerbus documentation for further details.

8. Verification Steps

All features shown in **Table 1** were tested using the sample configuration. The following steps can be used to verify and/or troubleshoot installations in the field.

1. On the SpeakerbusiD808 *i Turret*, verify that the status icons are green. These status icons indicate whether *i Turret* is connected to the network, *i cms* server, and SIP registrar (i.e., Avaya SIP Enablement Services). Refer to [5] for more details.
2. Verify that the iTurret deskstations have successfully registered with SIP Enablement Services, from the administration web page navigating to **Users → Search Registered Users** and clicking the **Search** button (not shown) this will display a list of registered user's on SIP Enablement Services as shown below.

The screenshot displays the Avaya Integrated Management SIP Server Management web interface. The top navigation bar includes the Avaya logo, 'Integrated Management SIP Server Management', and server status: 'Primary Server: [1] sessvra Duplicate Server: [2] sessvrb'. A left sidebar lists various management options like Users, Address Map, and Conferences. The main content area is titled 'Registered Users on 10.10.16.5' and shows a table of registered contacts. The table has three columns: 'Handle and Name', 'Address', and 'Expires'. Two contacts are listed: one for '1301@sip.avaya.com' and another for '1501@sip.avaya.com'.

Handle and Name	Address	Expires
<input type="checkbox"/> 1301@sip.avaya.com iTurret1, iD808	sip:1301@10.10.16.196;avaya-sc-enabled;transport=tcp	Wed, 07 Apr 2010 14:39:03 IST
<input type="checkbox"/> 1501@sip.avaya.com HS1 1301, Privacy	sip:1501@10.10.16.59;avaya-sc-enabled;transport=tcp	Wed, 07 Apr 2010 11:34:27 IST

3. Verify basic feature set administration by making calls from one *i Turret* to another *i Turret* and phones. Test supported features according to **Table 1** and feature deployment plans at the site.
4. Verify extended OPS features by dialing the Feature Name Extensions and listening for the confirmation tones.
5. Call an *i Turret* that currently has no voice messages, and leave a message. Verify that the message waiting indicator illuminates on the called *i Turret*. Call the voice messaging system from *i Turret* and use the voice messaging menus to retrieve and delete the voice message, verifying that DTMF is interpreted correctly by the system, and that the message waiting indicator extinguishes.

9. Conclusion

These Application Notes have described the administration steps required to use Speakerbus iD808 *i Turret* with Avaya Aura® Communication Manager and Avaya Aura® SIP Enablement Services. Both basic and extended feature sets were covered as shown in **Table 1**.

10. 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 5.2, May 2009, Issue 5.0, Document Number 03-300509.
- [2] *Avaya Extension to Cellular User Guide Avaya Aura® Communication Manager*, Nov 2009
- [3] *SIP Support in Avaya Aura® Communication Manager Running on the Avaya S8xxx Servers*, May 2009, Issue 9, Document Number 555-245-206.
- [4] *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura® SIP Enablement Services*, Nov 2009, Issue 8.0, Document Number 03-600768.
- [5] *Speakerbus i manager Administrator's Guide*, V1.220, Revision 6, March 2010.
- [6] *Session Initiation Protocol Service Examples draft-ietf-sipping-service-examples-15*, Internet-Draft, 11th July 2008, available at <http://tools.ietf.org/html/draft-ietf-sipping-service-examples-15>

©2011 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.