



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 iD808 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</i> turret and FNU
Call Forward Busy/No Answer	Yes	Yes	Local menu option on <i>i</i> turret and FNU
Call Forward Cancel	Yes	Yes	Local menu option on <i>i</i> turret 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</i> turret and FNU
Last Number Dialed	Yes	Yes	Via OPS FNE
Priority Call	No	Yes	Via OPS FNE, <i>i</i> turret 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 Avaya Aura[®] Communication Manager and Avaya Aura[®] SIP Enablement Services, calls were made between iD808 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.

2.1. 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, G729 and G.722 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 SIP Enablement Services (SES) failovers and simulated network failures

2.2. Test Results

Speakerbus iD808 *i* turret successfully passed interoperability testing. All of the PBX features listed in **Table 1** were covered.

2.3. 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 iD808 devices through the use of Feature Name Extensions (FNEs) and FNUs. The *i* cms server contains the *i* manager application for configuring the iD808 deskstations.

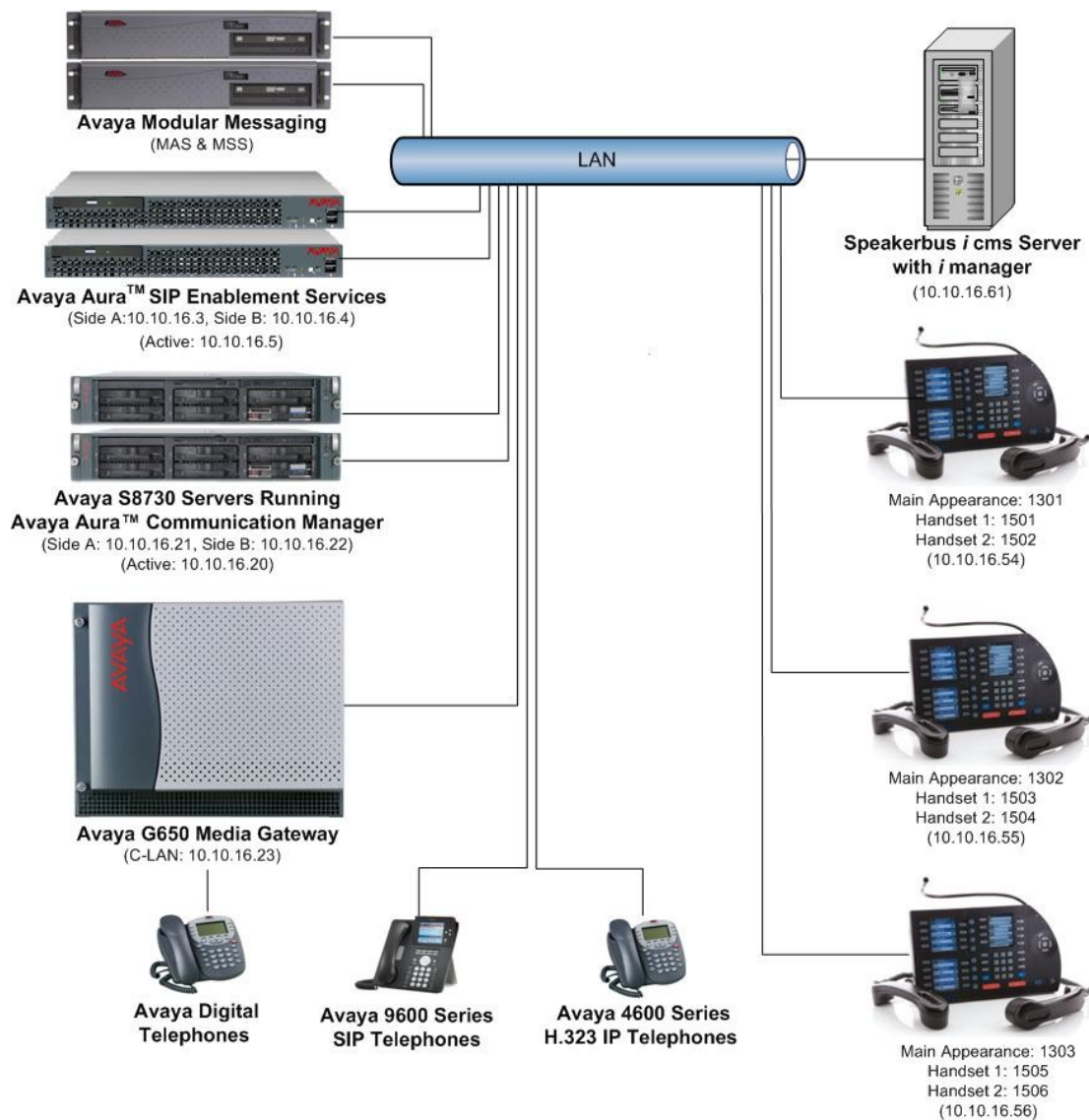


Figure 1: Speakerbus iD808 *i* turret with Avaya SIP Solution

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 4.01 (Patch 18433)
Avaya G650 Media Gateway TN2602AP Media Processor TN799DP CLAN	HW08 FW57 HW01 FW38
Avaya S8500B Servers (Redundant Pair)	Avaya Aura [®] SIP Enablement Services 5.2.1(SES-5.2.1.0-016.4) with Service Pack 3b
Avaya S3500 Servers Modular Messaging	Avaya Modular Messaging 5.2
Avaya 4600 Series IP Telephone	3.1 (H.323)
Avaya 9600 Series IP Telephones	2.6.2.0 (SIP)
Avaya Digital Telephones	--
Avaya Analog Telephones	--
Speakerbus iD808 <i>i</i> turret Avaya Interface Version	1.20
Speakerbus <i>i</i> cms Server with <i>i</i> manager Administration on Windows 2003 Server	1.300.7.0

5. Configure Avaya Aura® 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 **Whisper Page Tone Given 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 are 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 5.6** and **5.7**. 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: 123456	TN: 1
Port: S00010	Coverage Path 1: 89	COR: 1
Name: iTurret 1	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: 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 to 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 the *i* turret.

Note: Stations 1501 and 1502 are configured in **Section 5.9.2** and these bridged appearance buttons cannot be configured until those stations have been added.

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: brdg-appr	B:1	E:1302
4: call-appr	8: brdg-appr	B:2	E:1302
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: brdg-appr	B:3	E:1302	
10: brdg-appr	B:1	E:1303	
11: brdg-appr	B:2	E:1303	
12: brdg-appr	B:3	E:1303	
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: S00013	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: brdg-appr B:1 E:1302	
3: brdg-appr B:1 E:1301	7: brdg-appr B:2 E:1302	
4: brdg-appr B:2 E:1301	8: brdg-appr B:3 E:1302	
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: S00014	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: brdg-appr	B:1	E:1302
3: brdg-appr	B:1	E:1302	
4: brdg-appr	B:2	E:1302	
	8: brdg-appr	B:3	E:1302
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 in the display screen below. 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 **Config Set** value can reference a set that has the default settings.

diaply 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.

display 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      Intra-region IP-IP Direct Audio: yes
                        Inter-region IP-IP Direct Audio: yes
                        IP Audio Hairpinning? y
      UDP Port Min: 2048
      UDP Port Max: 8001
DIFFSERV/TOS PARAMETERS
      Call Control PHB Value: 46      RTCP Reporting Enabled? y
      Audio PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
      Video PHB Value: 26      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
      H.323 Link Bounce Recovery? y      RSVP Enabled? n
      Idle Traffic Interval (sec): 20
      Keep-Alive Interval (sec): 5
      Keep-Alive Count: 5
```

In the **IP Codec Set** form, select the audio codecs supported 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 sued 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		
Dial Access? n	Night Service:		
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	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	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 in to 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] sessvraDuplicate 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*

sip.avaya.com

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*

10.10.16.3

DiffServ/TOS Parameters

Call Control PHB Value*46

802.1 Parameters

Priority Value*6

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 ☒ Internal ☒ External

OutboundProxy Port ☐ UDP ☐ TCP

OutboundDirectDomains

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

MMc; Reviewed:
SPOC 2/8/2011

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

30 of 62
iD808-SESCM521

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 (*sip.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.



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* iD808

Last Name* iTurret1

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 instruction, there is a form with two fields: 'Extension' with the value '1301' and 'Communication Manager Server' with a dropdown menu set to 'CoreCM'. A note states 'Fields marked * are required.' At the bottom of the form is an 'Add' button.

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 Deskstations
- Create SIP Server
- Create PBX
- Create Dial Plan
- Create Call and Handset Appearances
- Create Users
- Create Groups
- Assign User Permissions
- Assign Ownership (of Appearances to Users)
- Assign Default Call Appearances
- Programming iD808 Deskstations
- Assign Appearances to Deskstation Keys
- Assign Bridged Call Appearances to Deskstations
- Synchronise Deskstations
- Feature Name Extensions (FNEs)

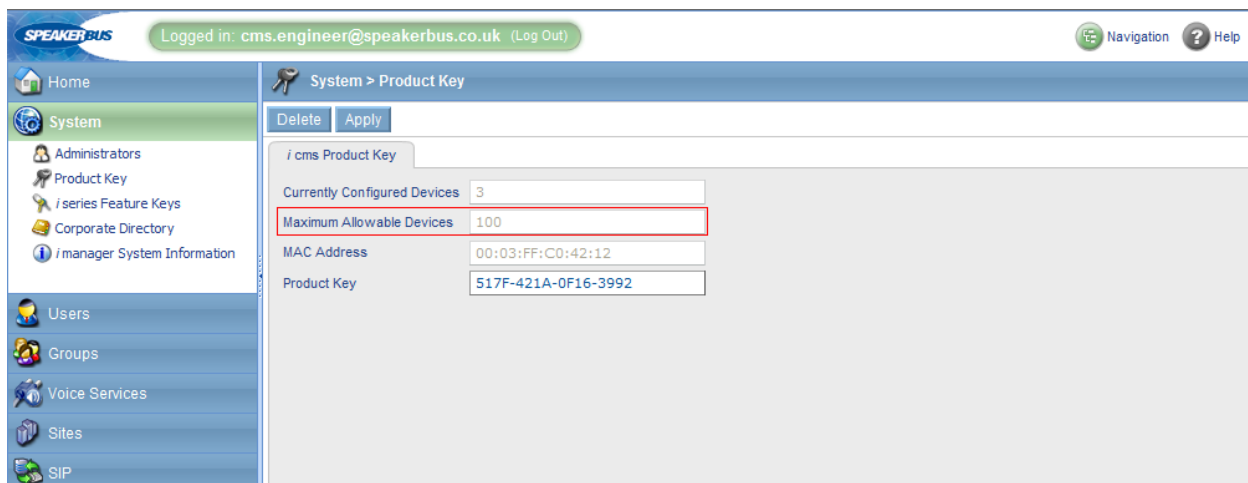
7.1. Launch *i* manager

To access the *i* manager software interface, open a web browser and type the *i* manager web address, for example, <http://10.10.16.61/imanager>. Press the **Enter** key. At *i* manager logon page enter the appropriate credentials. The *i* manager home page is displayed as shown below.



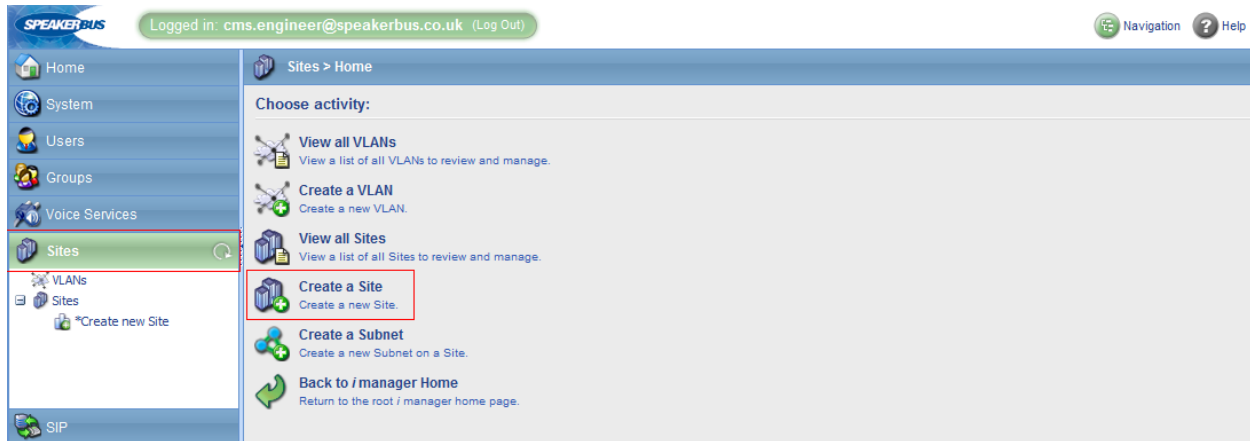
7.2. Verify Product Key

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

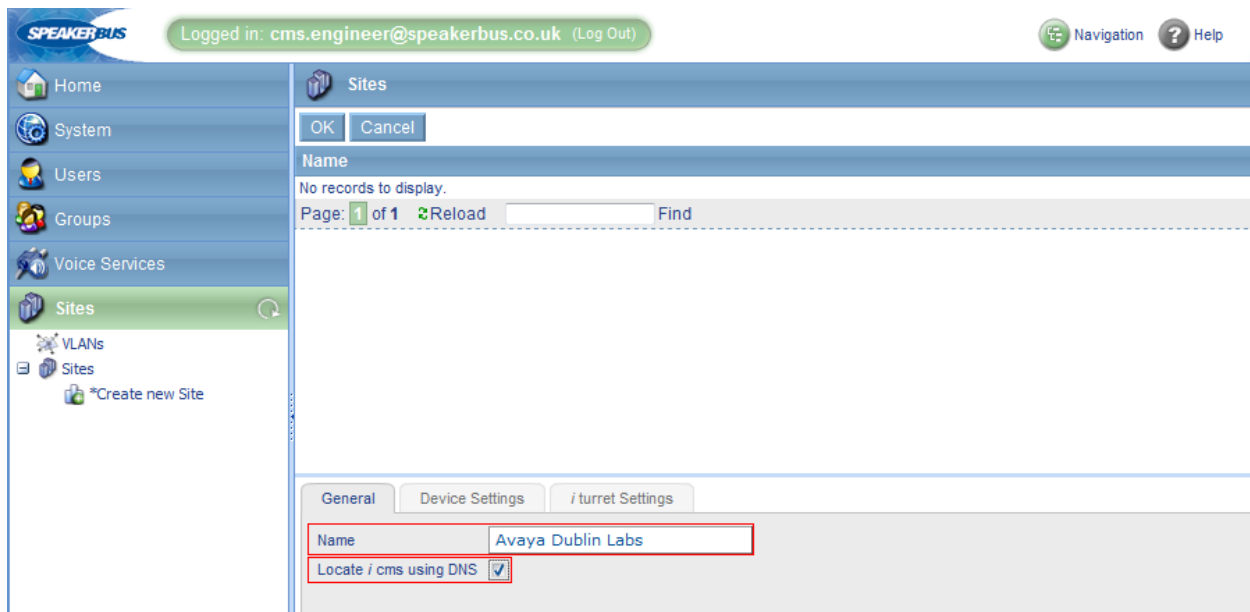


7.3. Create Site

Configure a site representing the location where the Speakerbus iD808 devices are installed. Click **Sites** in the left 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 [5] for correct configuration of DNS.



In the **iTurret Settings** tab, set the **NTP Time Zone** (network time protocol time zone) and configure the password for logging into the engineering tools menu of the iD808 deskstation by populating the **Admin Password** and **Verify Password** fields. The NTP Server field may be set to the IP address of the NTP server if one is used. Click **OK**.

Note: A Service Locator Record (SRV) needs to be added to the DNS server in order to allow the iD808 to locate and register to *i cms*. Refer to [5] for more details.

Speakerbus
Logged in: cms.engineer@speakerbus.co.uk (Log Out) Navigation ? Help

Home System Users Groups Voice Services Sites VLANs Sites *Create new Site SIP

Sites
OK Cancel
Name / cms IP
No records to display.
Page: 1 of 1 Reload Find

General Device Settings / turret Settings
NTP Server
Backup NTP Server
NTP Time Zone Europe: London
Dial Tone Locale UK
Admin Password
Verify Password *

7.4. Create Subnet

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

Speakerbus
Logged in: cms.engineer@speakerbus.co.uk (Log Out) Navigation ? Help

Home System Users Groups Voice Services Sites VLANs Sites Avaya Dublin Labs *Create new Subnet SIP

Sites > Avaya Dublin Labs > Subnets
OK Cancel
Subnet Sut
No records to display.
Page: 1 of 1 Reload Find

General SbRTP / turret
Name 10.10.16.x
Site Avaya Dublin Labs
Subnet Address 10.10.16.0
Default Gateway Address 10.10.16.1

In the **SbRTP** tab, set the **Compatibility** field to **Version 3.0**. Click **OK**.

The screenshot shows the Speakerbus web interface. The left sidebar contains navigation links: Home, System, Users, Groups, Voice Services, Sites (selected), VLANs, and SIP. The main content area is titled 'Sites > Avaya Dublin Labs > Subnets'. It features a table with one row for a subnet, showing 'No records to display.' and pagination 'Page: 1 of 1'. Below the table are three tabs: 'General', 'SbRTP' (selected), and 'i turret'. The 'SbRTP' tab contains several configuration fields: 'RTP Payload Code' (96), 'DSCP Value' (0), 'Bandwidth' (Standard), 'Compatibility' (Version 3.0, highlighted with a red box), 'Packet Size' (1 ms), and 'Voice Activity Detection' (checkbox). The top of the interface shows the user is logged in as 'cms.engineer@speakerbus.co.uk'.

In the **i turret** tab, enter the IP address of a TFTP server that will store log files for troubleshooting purposes

This screenshot shows the same Speakerbus interface, but with the 'i turret' tab selected. The 'SbRTP' tab is now inactive. The 'i turret' tab contains a single configuration field: 'Logging TFTP Server IP Address' with the value '10.10.16.55' entered (highlighted with a red box). The rest of the interface, including the sidebar and the subnet table, remains the same as in the previous screenshot.

7.5. Create Deskstations

iD808 deskstations will automatically register to this subnet within iCMS as the appropriate DHCP and DNS records were created prior to iD808 deskstations being connected to the IP network. The newly registered deskstations are automatically displayed in the list.

The screenshot shows the Speakerbus iCMS interface. The user is logged in as cms.engineer@speakerbus.co.uk. The navigation menu on the left includes Home, System, Users, Groups, Voice Services, and Sites. The Sites menu is expanded, showing Avaya Dublin Labs, 10.10.16.x, Gateways, Deskstations, and Voice Services. The main content area displays the Deskstations list for the 10.10.16.x subnet. The list has columns for Name, Type, IP Address, MAC Address, Firmware, and a partial 'Sea' column. Three devices are listed: Device21, Device22, and Device23, all of type 'turret'. The first row (Device21) is highlighted with a red border. Below the list, there are tabs for General, IP Settings, Network, Feature Key, SBRTP, Deskstation, Gateway, and Test Tones. The General tab is selected.

Name	Type	IP Address	MAC Address	Firmware	Sea
Device21	turret	10.10.16.59	00:05:83:00:14:C3	1.200.14.0	
Device22	turret	10.10.16.60	00:05:83:00:10:BF	1.200.14.0	
Device23	turret	10.10.16.58	00:05:83:00:14:4C	1.200.14.0	

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

The screenshot shows the Speakerbus iCMS interface with the Deskstation configuration page. The user is logged in as cms.engineer@speakerbus.co.uk. The navigation menu on the left is the same as in the previous screenshot. The main content area displays the configuration for a deskstation. The tabs at the top are General, IP Settings, Network, Media, and Deskstation. The General tab is selected. The configuration fields are: Name (tTurretA), Type (turret), MAC Address (00:05:83:00:14:C3), Firmware Version (1.200.14.0), and Location (empty). The Name field is highlighted with a red border.

Name	Type	IP Address	MAC Address	Firmware	Sea
tTurretA	turret	10.10.16.59	00:05:83:00:14:C3	1.200.14.0	
Device22	turret	10.10.16.60	00:05:83:00:10:BF	1.200.14.0	
Device23	turret	10.10.16.58	00:05:83:00:14:4C	1.200.14.0	

In the **IP Settings** tab, verify that the **Obtain IP Address using DHCP** and the **Obtain local Domain Name using DHCP** check boxes are selected.

The screenshot shows the Speakerbus web interface. The left sidebar contains navigation links: Home, System, Users, Groups, Voice Services, Sites, VLANs, Avaya Dublin Labs, 10.10.16.x, Gateways, Deskstations, and Voice Services. The main content area is titled 'Sites > Avaya Dublin Labs > 10.10.16.x > Deskstations'. It features a table with columns: Name, Type, IP Address, MAC Address, and Firmware. The table lists three devices: Device21, Device22, and Device23, all of type 'i turret'. Below the table, there are tabs for General, IP Settings, Network, Media, and Deskstation. The IP Settings tab is active, showing checkboxes for 'Obtain IP Address using DHCP' and 'Obtain Local Domain Name using DHCP', both of which are checked. Other fields include IP Address (10.10.16.59), IE801 #1 IP Address, IE801 #2 IP Address, and DHCP Server Timeout (60).

Name	Type	IP Address	MAC Address	Firmware
Device21	i turret	10.10.16.59	00:05:83:00:14:C3	1.200.14.0
Device22	i turret	10.10.16.60	00:05:83:00:10:BF	1.200.14.0
Device23	i turret	10.10.16.58	00:05:83:00:14:4C	1.200.14.0

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

The screenshot shows the Speakerbus web interface with the Deskstation tab selected. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Sites > Avaya Dublin Labs > 10.10.16.x > Deskstations'. It features a table with columns: Name, Type, IP Address, MAC Address, and Firmware. The table lists three devices: Device21, Device22, and Device23, all of type 'i turret'. Below the table, there are tabs for General, IP Settings, Network, Media, and Deskstation. The Deskstation tab is active, showing a 'Seated User' field with the value 'No User seated'. The 'Preferred Telephony Codec' is set to 'G.711 A-Law'. There is also a 'Voice Activity Detection' checkbox which is unchecked.

Name	Type	IP Address	MAC Address	Firmware
Device21	i turret	10.10.16.59	00:05:83:00:14:C3	1.200.14.0
Device22	i turret	10.10.16.60	00:05:83:00:10:BF	1.200.14.0
Device23	i turret	10.10.16.58	00:05:83:00:14:4C	1.200.14.0

7.6. Create SIP Server

To create a SIP Server, click **Create a new SIP Server** under the **SIP** directory in the left pane. Provide a descriptive name for the SIP server and set the **Registrar Address** and **SIP Domain** fields to **sip.avaya.com**. In this configuration, DNS resolves the domain name to 10.10.16.5, the SIP Enablement Services active IP address. Click **OK**. After the SIP server is created, the **Port** field will be displayed on this page with the default value of 5060. The default value was used in this configuration (Not shown).

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

The screenshot shows the Speakerbus web interface. The left navigation pane has 'SIP' selected, with a sub-link '*Create new SIP Server'. The main content area is titled 'SIP > SIP Servers' and contains a table with columns 'Name', 'Registrar Address', and 'SIP D'. Below the table is a 'General' tab with three input fields: 'Name' (Avaya), 'Registrar Address' (sip.avaya.com), and 'SIP Domain' (sip.avaya.com). The fields are highlighted with a red border.

7.7. Create PBX

Select the **SIP** directory and click **Create new PBX**. Provide a descriptive name/text for the PBX in the **Name** and **Version** fields and set the **Type** field to **Avaya**. The **Outbound** and **Inbound** tabs are left with their default values. Click **OK**.

The screenshot shows the Speakerbus web interface. The left navigation pane has 'SIP' selected, with a sub-link '*Create new PBX'. The main content area is titled 'SIP > Avaya > PBXs' and contains a table with columns 'Name' and 'Type'. Below the table are three tabs: 'General', 'Inbound', and 'Outbound'. The 'General' tab is active, showing three input fields: 'Name' (Avaya), 'Type' (Avaya), and 'Version' (5.2.1). The fields are highlighted with a red border.

7.8. Create Dial Plan

Under the **SIP** directory, click **Dial Plan** and then the **New** button to add a dial rule (not shown). Dial rules specify the valid digit formats that the iD808 devices are allowed to dial, otherwise the user will have to press OK after entering the dial string on the iD808 device. In this configuration, 4-digit extensions beginning with **1** were used to dial other iD808 devices and Avaya telephones. A dial rule is also required for the voice mail pilot number which was a 4-digit extension beginning with **8**. 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.

The screenshot shows the Speakerbus web interface. The top navigation bar includes the Speakerbus logo, a login status for 'cms.engineer@speakerbus.co.uk', and links for 'Navigation' and 'Help'. The left sidebar contains a tree view with categories: Home, System, Users, Groups, Voice Services, Sites, and SIP. Under the SIP category, there are sub-items: Avaya, Avaya, Dial Plan, and PBX Appearances. The main content area is titled 'SIP > Avaya > Avaya > Dial Plan' and contains 'OK' and 'Cancel' buttons. Below this is a 'Dial Rule' section with the text 'No records to display.' and a pagination bar showing 'Page: 1 of 1' with 'Reload' and 'Find' links. At the bottom, there is a 'General' tab with a 'Dial Rule' field containing the text '1XXX'.

7.9. Create Call and Handset Appearances

Three call appearances need to be created for each iD808 device, 1 for its main appearance. 1 call appearance is required for privacy handset 1 and another for 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 which is under the **SIP** directory. Click the **New** button on the next page to add a new appearance (not shown). 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 iD808 deskstation. In this example, the label was set to iTurretA followed by the extension number 1301. The **Address** field should also be set to the appearance extension. Set the **Type** field to **Call**.

Logged in: cms.engineer@speakerbus.co.uk (Log Out) Navigation ? Help

SIP > Avaya > Avaya > PBX Appearances

General User Permissions Group Permissions

OK Cancel

Name	Long Label	Type	Status
No records to display.			
Page: 1 of 1 Reload Find			

General Advanced

Name 1301

Type Call

Long Label iTurretA 1301

Address 1301

Owner

Scheme SIP

In the **Advanced** tab, 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 in **Section 5.9.1** 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 iD808 deskstation. Select the **Message Indication** checkbox for voice mail purposes. 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 iD808 deskstation will use to authenticate and register with SIP Enablement Services. Use the default values for the other fields as shown below. Click **OK**.

The screenshot shows the Speakerbus web interface. The user is logged in as cms.engineer@speakerbus.co.uk. The navigation menu on the left includes Home, System, Users, Groups, Voice Services, Sites, and SIP. The SIP menu is expanded, showing Avaya, Avaya, Dial Plan, and PBX Appearances. The PBX Appearances page is displayed, showing a table with columns Name, Long Label, Type, Status, and Add. Below the table, the 'Advanced' tab is selected, and the following fields are visible:

Group Number	0
Maximum PBX Appearances	3
Allow Outbound Calls	<input checked="" type="checkbox"/>
Message Indication	<input checked="" type="checkbox"/>
Authentication Name	1301
Authentication Password	•••••
Verify Password	•••••

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 **Name** and **Address** fields to the extension of handset 1 and the **Long Label** field to the name of the handset. In this example, the extension is **1501**. Review the previous section for a description of these fields. Set the **Type** field to **Privacy** 1.

Logged in: cms.engineer@speakerbus.co.uk (Log Out)

Navigation ? Help

SIP > Avaya > Avaya > PBX Appearances

General User Permissions Group Permissions

OK Cancel

Name	Long Label	Type	Status
1301	iTurretA 1301	Call	

Page: 1 of 1 Reload Find

General Advanced

Name 1501

Type Privacy 1

Long Label iTurretA P1

Address 1501

Owner

Scheme SIP

In the **Advanced** tab, configure the **Authentication Name** and **Authentication Password** fields with the credentials for registering with SIP Enablement Services. For the Privacy appearances, the **Maximum Appearances** field should be set to **0** since no calls will be made to the Privacy appearances directly. The **Message Indication** checkbox does not need to be enabled since the handset appearances are not voice mail subscribers. Privacy appearances are hidden on the iD808 deskstation and need to be defined in order for privacy to work on the iD808 with Communication Manager. Click **OK**.

The screenshot shows the Speakerbus web interface. The left sidebar contains navigation links: Home, System, Users, Groups, Voice Services, Sites, and SIP. The main content area is titled 'SIP > Avaya > Avaya > PBX Appearances'. It has tabs for 'General', 'User Permissions', and 'Group Permissions'. The 'General' tab is active, showing a table with one entry: '1301' with 'Long Label' 'iTurretA 1301', 'Type' 'Call', and 'Status' 'Active'. Below the table, there are input fields for 'Group Number' (0), 'Maximum PBX Appearances' (0), 'Allow Outbound Calls' (checked), 'Message Indication' (unchecked), 'Authentication Name' (1501), 'Authentication Password' (masked with dots), and 'Verify Password' (masked with dots). The 'Advanced' tab is also visible at the bottom.

Repeat the above procedure to add the Privacy 2 appearance. The three call appearances for the previously configured iD808 deskstation are listed below.

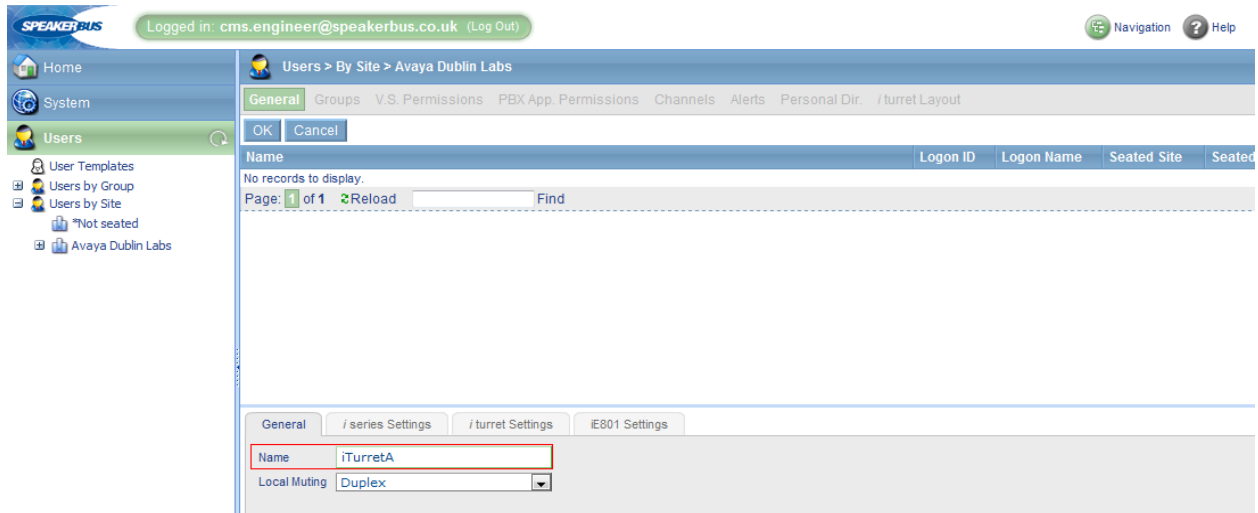
The screenshot shows the Speakerbus web interface. The left sidebar contains navigation links: Home, System, Users, Groups, Voice Services, Sites, and SIP. The main content area is titled 'SIP > Avaya > Avaya > PBX Appearances'. It has tabs for 'General', 'User Permissions', and 'Group Permissions'. The 'General' tab is active, showing a table with three entries: '1301' with 'Long Label' 'iTurretA 1301', 'Type' 'Call', 'Status' 'Active', and 'Address' '1301'; '1501' with 'Long Label' 'iTurretA P1', 'Type' 'Privacy 1', 'Status' 'Active', and 'Address' '1501'; and '1502' with 'Long Label' 'iTurretA P2', 'Type' 'Privacy 2', 'Status' 'Active', and 'Address' '1502'. The table has columns for Name, Long Label, Type, Status, and Address. The 'Advanced' tab is also visible at the bottom.

Name	Long Label	Type	Status	Address
1301	iTurretA 1301	Call	Active	1301
1501	iTurretA P1	Privacy 1	Active	1501
1502	iTurretA P2	Privacy 2	Active	1502

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

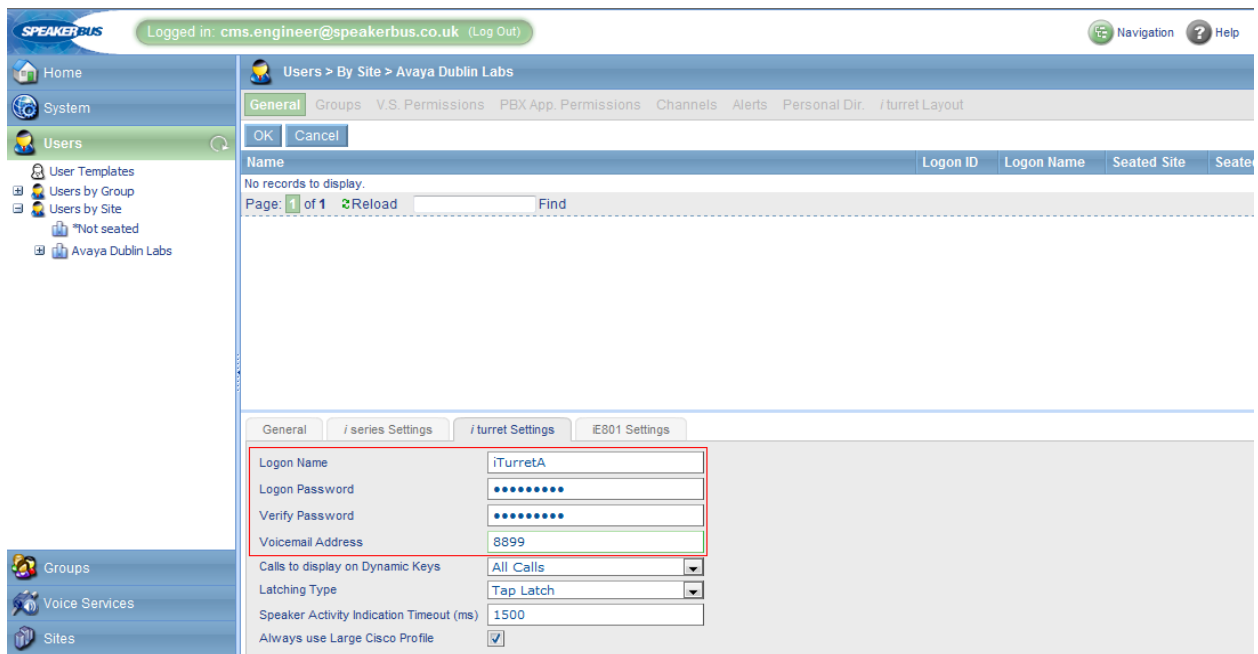
7.10. Create Users

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



The screenshot shows the Speakerbus web interface. The top navigation bar includes 'Home', 'System', and 'Users'. The left sidebar shows a directory tree with 'Users' expanded, and 'Avaya Dublin Labs' selected. The main content area displays the 'Users > By Site > Avaya Dublin Labs' page. The 'General' tab is active, and the 'Name' field is highlighted with a red box, containing the text 'iTurretA'. The 'Local Muting' dropdown is set to 'Duplex'.

In the **i turret Settings** tab, provide the logon credentials for the user to log into their iD808 deskstation and enter the pilot number for Voicemail in the **Voicemail Address** field. This page will be revisited later in **Section 7.14** to configure the default call appearance for this deskstation. Click **OK**.



The screenshot shows the Speakerbus web interface. The top navigation bar includes 'Home', 'System', and 'Users'. The left sidebar shows a directory tree with 'Users' expanded, and 'Avaya Dublin Labs' selected. The main content area displays the 'Users > By Site > Avaya Dublin Labs' page. The 'i turret Settings' tab is active, and the 'Logon Name', 'Logon Password', 'Verify Password', and 'Voicemail Address' fields are highlighted with a red box. The 'Logon Name' field contains 'iTurretA', the 'Logon Password' and 'Verify Password' fields contain masked text, and the 'Voicemail Address' field contains '8899'. Other fields include 'Calls to display on Dynamic Keys' (All Calls), 'Latching Type' (Tap Latch), 'Speaker Activity Indication Timeout (ms)' (1500), and 'Always use Large Cisco Profile' (checked).

Repeat the previous procedure to add more users.

After a user has been created, the user needs to be **seated** on an iD808 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.

Logged in: cms.engineer@speakerbus.co.uk (Log Out)

Navigation ? Help

Home System Users

Users by Site

*Not seated

Avaya Dublin Labs

Users > By Site > *Not seated

General Groups V.S. Permissions PBX App. Permissions Channels Alerts Personal Dir. / turret Layout

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

Name	Logon ID	Logon Name	Seated Site	Seated
iTurretA		iTurretA		
iTurretB		iTurretB		
iTurretC		iTurretC		

Page: 1 of 1 Reload Find

General / series Settings / turret Settings IE801 Settings

Name iTurretA

Local Muting Duplex

Seated at Device User not seated

On the next page, filter options are presented. Filter deskstations in the **Avaya Dublin Labs** site and in the **10.10.16.x** subnet as shown below. The user will be seated on an iD808 deskstation with these properties. Click **Next**.

Logged in: cms.engineer@speakerbus.co.uk (Log Out)

Navigation ? Help

Home System Users

Users by Site

*Not seated

Avaya Dublin Labs

Groups Voice Services Sites SIP

Users > By Site > *Not seated > iTurretA > Seat User

Step 1: Select Deskstation filter options

Site Avaya Dublin Labs

Subnet 10.10.16.x

Product [All]

Show only free Deskstations ☒

Cancel < Back Next > Finish

In the resulting deskstation list, select the iD808 deskstation where the selected user will be seated. In this example, the user will be seated on the iTurretA deskstation. Select **iTurretA** in the list and click **Finish**.

The screenshot shows the 'Users > By Site > *Not seated > iTurretA > Seat User' page. The 'Step 2: Select a Deskstation to seat the User at' section has a 'Selected Deskstation' dropdown set to 'iTurretA'. Below is a table of available deskstations:

Name	Site	Subnet	Product	IP Address	MAC Address	Se
iTurretA	Avaya Dublin Labs	10.10.16.x	i turret	10.10.16.59	00:05:83:00:14:C3	
iTurretB	Avaya Dublin Labs	10.10.16.x	i turret	10.10.16.60	00:05:83:00:10:BF	
iTurretC	Avaya Dublin Labs	10.10.16.x	i turret	10.10.16.58	00:05:83:00:14:4C	

At the bottom, there are navigation buttons: Cancel, < Back, Next >, and Finish.

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.

The screenshot shows the 'Users > By Site > Avaya Dublin Labs' page. The 'General' tab is active, displaying a table of seated users:

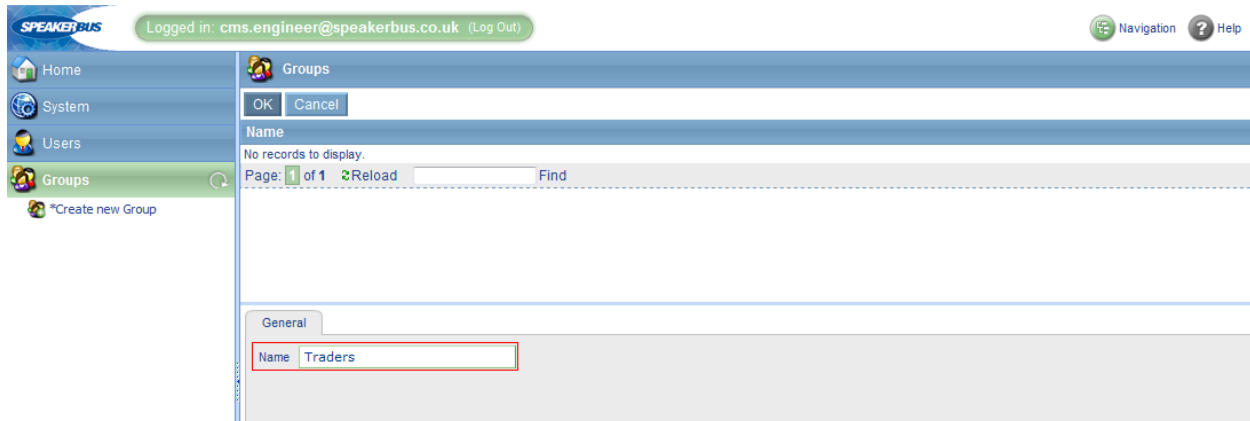
Name	Logon ID	Logon Name	Seated Site	Seated Subnet	Seated Device
iTurretA		iTurretA	Avaya Dublin Labs	10.10.16.x	iTurretA
iTurretB		iTurretB	Avaya Dublin Labs	10.10.16.x	iTurretB
iTurretC		iTurretC	Avaya Dublin Labs	10.10.16.x	iTurretC

Below the table, the 'iTurretC' configuration details are shown under the 'General' tab:

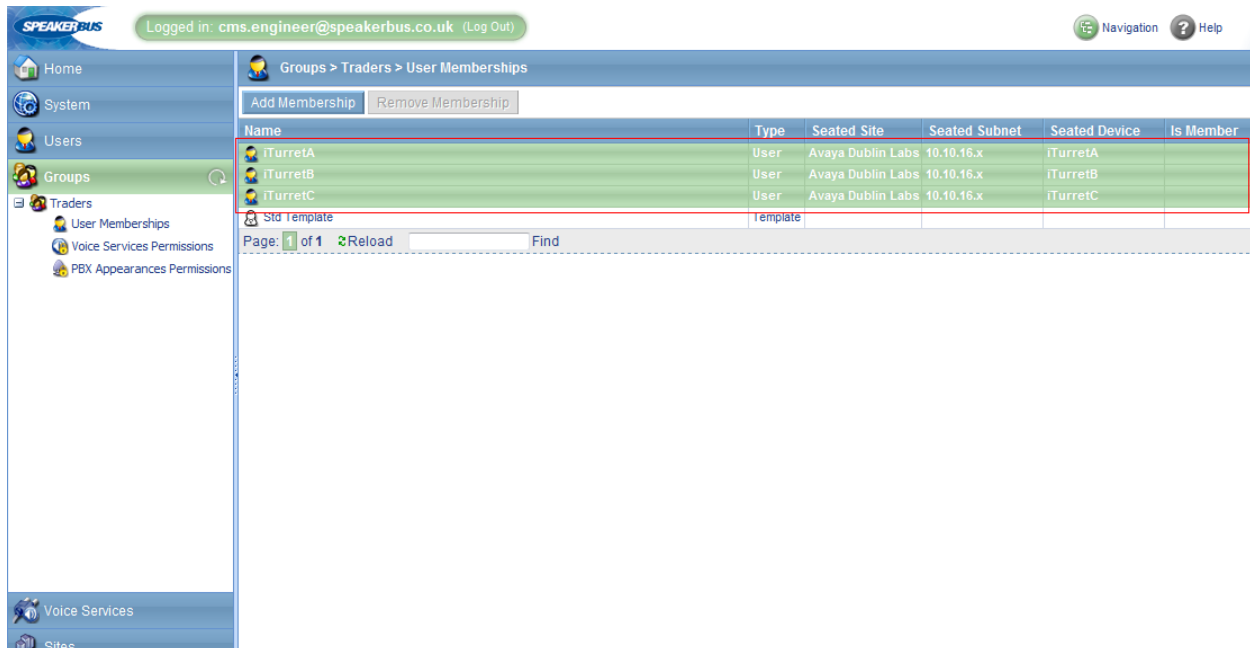
- Name: iTurretC
- Local Muting: Duplex
- Seated at Site: Avaya Dublin Labs
- Seated at Subnet: 10.10.16.x
- Seated at Device: iTurretC

7.11. Create Groups

To create a group; in the left panel 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.



Users are 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).



7.12. Assign User Permissions

The next step will be to assign appearance permissions to users. In the left panel under the **SIP** directory tree, expand **Avaya** → **Avaya** and click on **PBX Appearances**. The list of appearances is displayed. Select the main call appearance for **iTurretA** (i.e., **1301**) and click **User Permissions**.

Logged in: cms.engineer@speakerbus.co.uk (Log Out)

SIP > Avaya > Avaya > PBX Appearances

General **User Permissions** Group Permissions

New Delete Apply Assign Ownership... Clear Ownership

Name	Long Label	Type	Status	Address
1301	iTurretA 1301	Call		1301
1302	iTurretB 1302	Call		1302
1303	iTurretC 1303	Call		1303
1501	iTurretA P1	Privacy 1		1501
1502	iTurretA P2	Privacy 2		1502
1503	iTurretB P1	Privacy 1		1503
1504	iTurretB P2	Privacy 2		1504
1505	iTurretC P1	Privacy 1		1505
1506	iTurretC P2	Privacy 2		1506

Page: 1 of 1 Reload Find

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.

Logged in: cms.engineer@speakerbus.co.uk (Log Out)

SIP > Avaya > Avaya > 1301 > User Permissions

General **User Permissions** Group Permissions

Apply

Name	User Permission	Group Permission	Type	Seated Site	Seated Subnet	Seated Device
iTurretA	Use group	Deny	User	Avaya Dublin Labs	10.10.16.x	iTurretA
iTurretB	Use group	Deny	User	Avaya Dublin Labs	10.10.16.x	iTurretB
iTurretC	Use group	Deny	User	Avaya Dublin Labs	10.10.16.x	iTurretC

Page: 1 of 1 Reload Find

General

Permission **Allow**

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 **iTurretB** and **iTurretC** 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.

Logged in: cms.engineer@speakerbus.co.uk (Log Out)

SIP > Avaya > Avaya > 1301 > User Permissions

General **User Permissions** Group Permissions

Apply

Name	User Permission	Group Permission	Type	Seated Site	Seated Subnet	Seated Device
iTurretA	Allow		User	Avaya Dublin Labs	10.10.16.x	iTurretA
iTurretB	Allow		User	Avaya Dublin Labs	10.10.16.x	iTurretB
iTurretC	Allow		User	Avaya Dublin Labs	10.10.16.x	iTurretC

Page: 1 of 1 Reload Find

7.13. Assign Ownership

To assign ownership of the appearances to a user, in the left panel under the **SIP** directory tree, expand **Avaya** → **Avaya** and click on **PBX Appearances** to display the appearances list as shown below. Select the appearance that a user will be assigned ownership of and click on the **Assign Ownership...** button.

The screenshot shows the Speakerbus web interface. The left sidebar has a tree view with 'SIP' expanded, showing 'Avaya' and 'PBX Appearances'. The main panel is titled 'SIP > Avaya > Avaya > PBX Appearances'. It has tabs for 'General', 'User Permissions', and 'Group Permissions'. Below the tabs are buttons: 'New', 'Delete', 'Apply', 'Assign Ownership...', and 'Clear Ownership'. A table lists appearances with columns: Name, Long Label, Type, Status, and Address. The first row (Name: 1301) is highlighted. Below the table is a 'Page: 1 of 1' indicator and a 'Find' search box. At the bottom is a configuration form with 'General' and 'Advanced' tabs. The 'General' tab is active, showing fields for Name (1301), Type (Call), Long Label (iTurretA 1301), Address (1301), Owner, and Scheme (SIP).

Name	Long Label	Type	Status	Address
1301	iTurretA 1301	Call		1301
1302	iTurretB 1302	Call		1302
1303	iTurretC 1303	Call		1303
1501	iTurretA P1	Privacy 1		1501
1502	iTurretA P2	Privacy 2		1502
1503	iTurretB P1	Privacy 1		1503
1504	iTurretB P2	Privacy 2		1504
1505	iTurretC P1	Privacy 1		1505
1506	iTurretC P2	Privacy 2		1506

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

The screenshot shows the 'Assign Ownership' page in the Speakerbus interface. The left sidebar is the same as the previous screenshot. The main panel is titled 'SIP > Avaya > Avaya > 1301 > Assign Ownership'. It has a section 'Step 1: Select User filter options'. Below this section are three filter options: 'Show only unseated users' (checkbox), 'Filter by Site' (dropdown menu showing 'Avaya Dublin Labs'), and 'Filter by Group' (dropdown menu showing 'Traders'). There is also a 'Filter by Name' text input field. At the bottom are buttons: 'Cancel', '< Back', 'Next >', and 'Finish'.

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

Logged in: cms.engineer@speakerbus.co.uk (Log Out)

SIP > Avaya > Avaya > 1301 > Assign Ownership

Step 2: Select a User to assign ownership to

Selected User: iTurretA

Name	Seated Site	Seated Subnet	Seated Device
iTurretA	Avaya Dublin Labs	10.10.16.x	iTurretA
iTurretB	Avaya Dublin Labs	10.10.16.x	iTurretB
iTurretC	Avaya Dublin Labs	10.10.16.x	iTurretC

Page: 1 of 1 Reload Find

Cancel < Back Next > Finish

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

7.14. Assign Default Call Appearances

In the **Users** directory tree, navigate to **Users by Site** → **Avaya Dublin Labs** and click **10.10.16.x** link to display the users list. Select a user to assign a default appearance to and then select the **i turret Settings** tab. Set the **Default PBX Appearance Type** to **Call** and select the appropriate default appearance (e.g., **1301**) from the **Default PBX Appearance** drop down menu. Click **Apply**.

Logged in: cms.engineer@speakerbus.co.uk (Log Out)

Users > By Subnet > Avaya Dublin Labs > 10.10.16.x

General Groups V.S. Permissions PBX App. Permissions Channels Alerts Personal Dir / turret Layout

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

Name	Logon ID	Logon Name	Seated Site	Seated Subnet	Seated Device
iTurretA		iTurretA	Avaya Dublin Labs	10.10.16.x	iTurretA
iTurretB		iTurretB	Avaya Dublin Labs	10.10.16.x	iTurretB
iTurretC		iTurretC	Avaya Dublin Labs	10.10.16.x	iTurretC

Page: 1 of 1 Reload Find

General / series Settings / turret Settings IE801 Settings

Logon Name: iTurretA Change Password...

Voicemail Address: 8899

Default PBX Appearance Type: Call

Default PBX Appearance: 1301

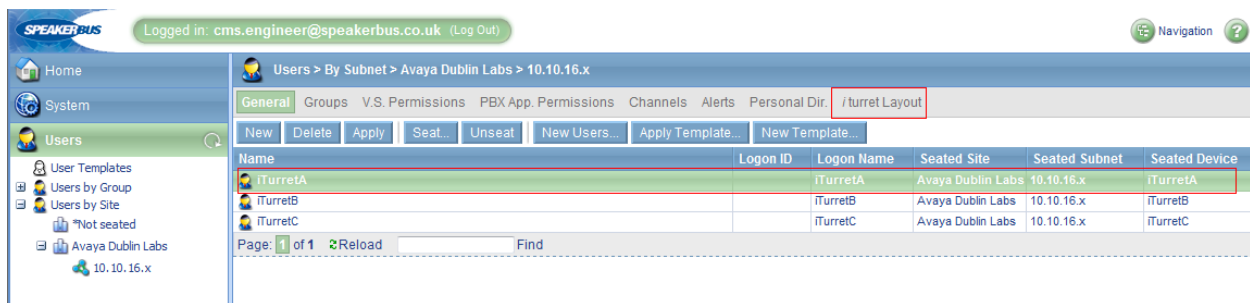
Calls to display on Dynamic Keys: All Calls

Latching Type: Tap Latch

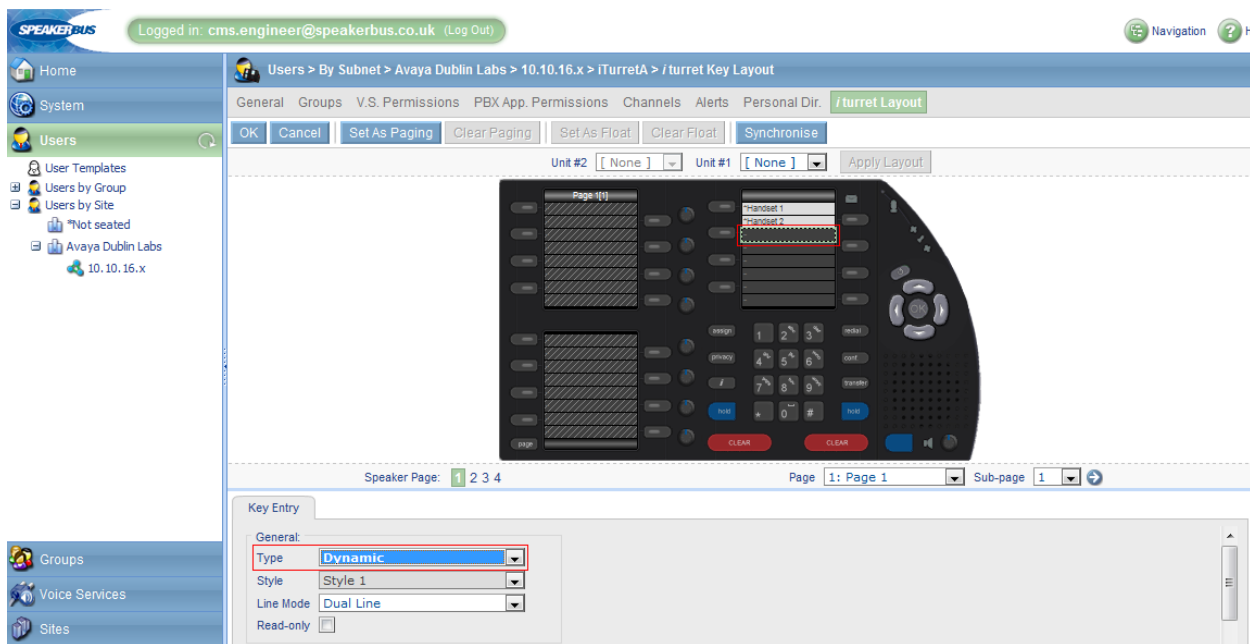
Speaker Activity Indication Timeout (ms): 1500

7.15. Programming iD808 Deskstations

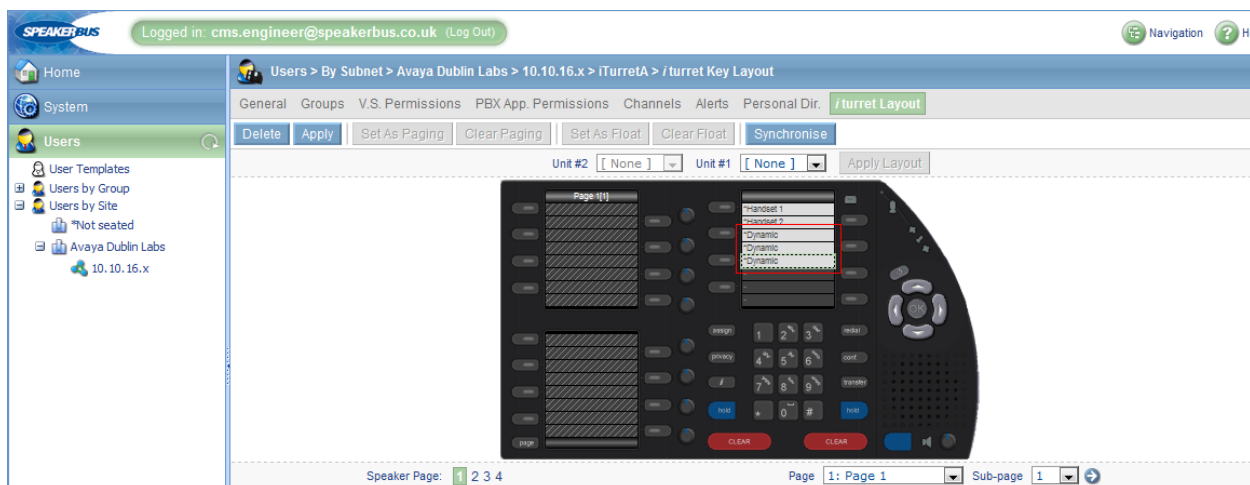
This section describes how to create iD808 deskstation keys. The following keys can be created using the iTurret layout page: Dynamic, Appearance, Shortcut, Soft Function, and Speed Dial amongst others. In this configuration, each user will be configured with three Dynamic keys, two Soft Function keys, 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 Dublin Labs** and click on **10.10.16.x** link to display a list of users. Select a user (e.g., iTurretA) and click **iTurret Layout** to display the iD808 key layout for this user.



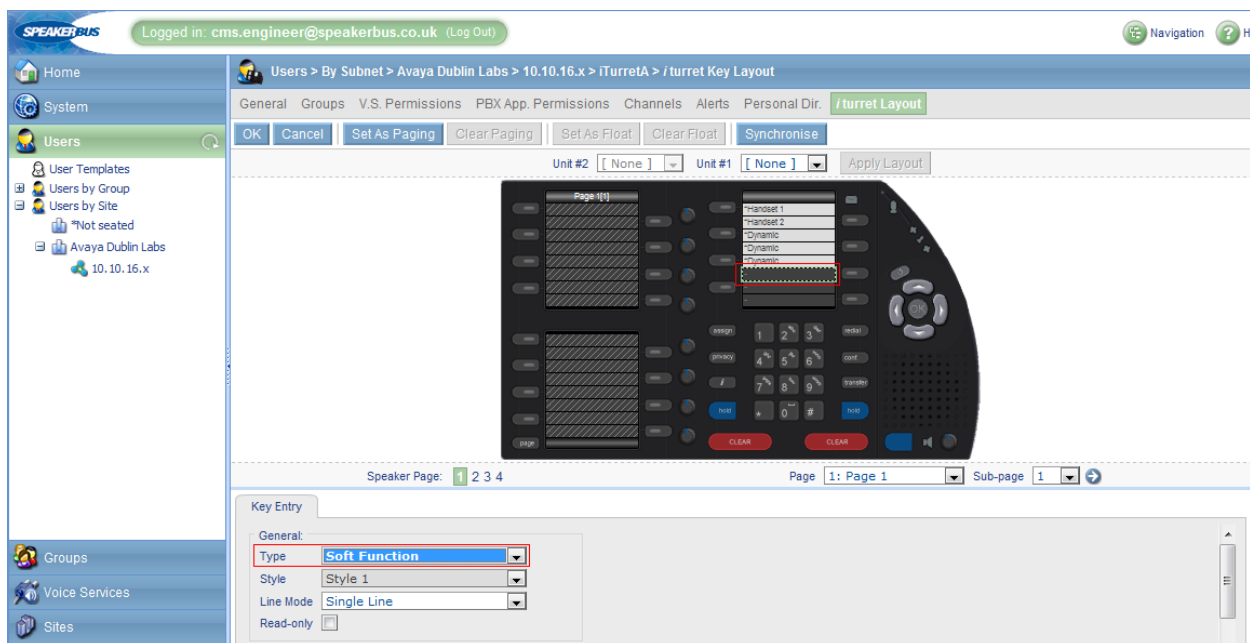
In the iTurret key layout, click on the key highlighted below Handset 2. In the Key Entry tab, set the **Type** field to **Dynamic**. Click **OK**.



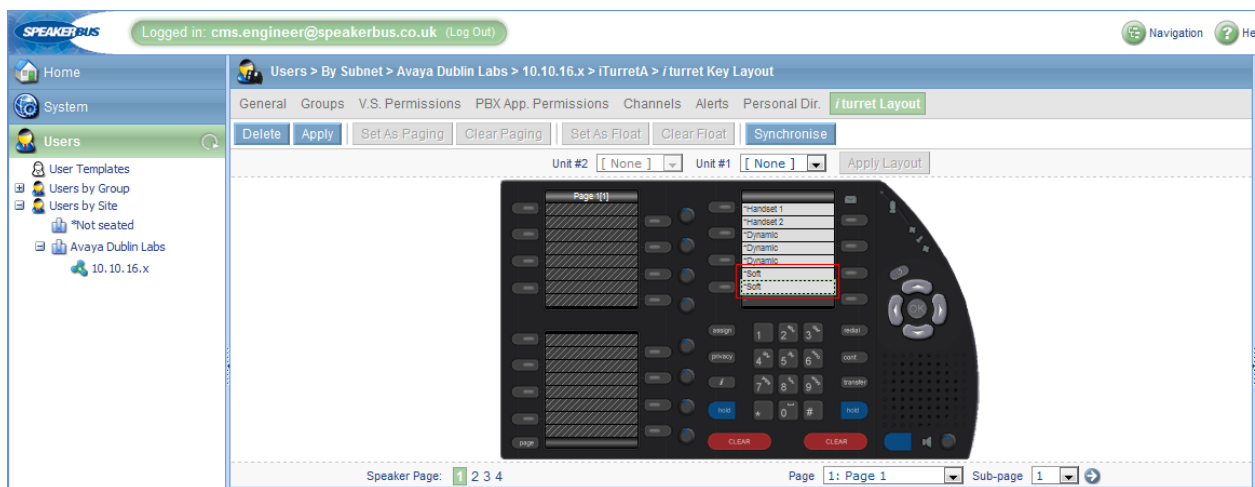
Three Dynamic keys will be added so repeat this step for the next two keys. The iTurret layout will appear as shown below once the three dynamic keys have been added.



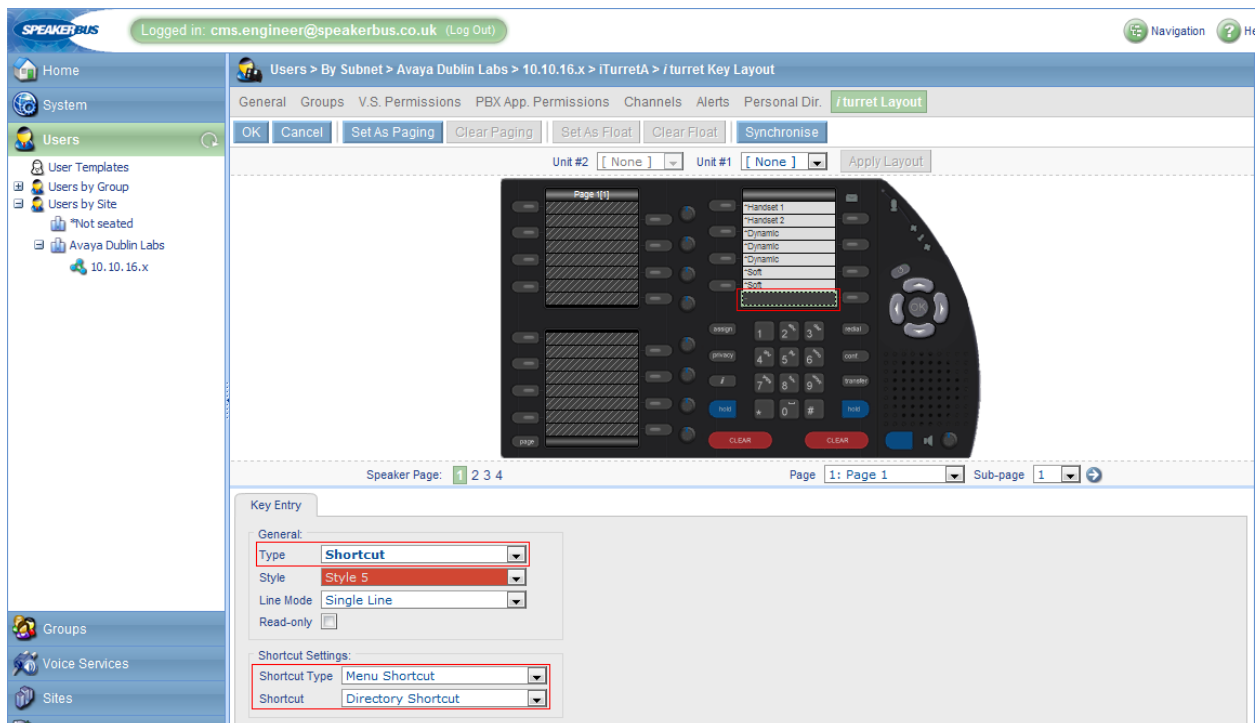
Next, configure two Soft Function keys. Select the next available key under the last Dynamic key. In the **Key Entry** tab, set the **Type** field to **Soft Function** and click **OK**. Repeat this step for the second Soft Function key.



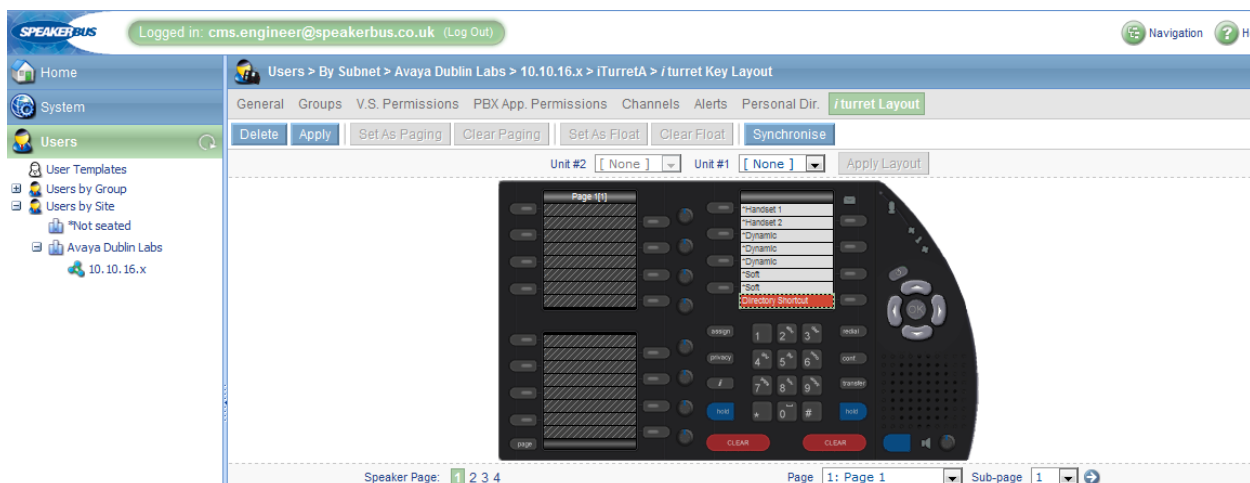
Once the two Soft Function keys have been created, the iD808 layout will be appear as shown below.



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**.

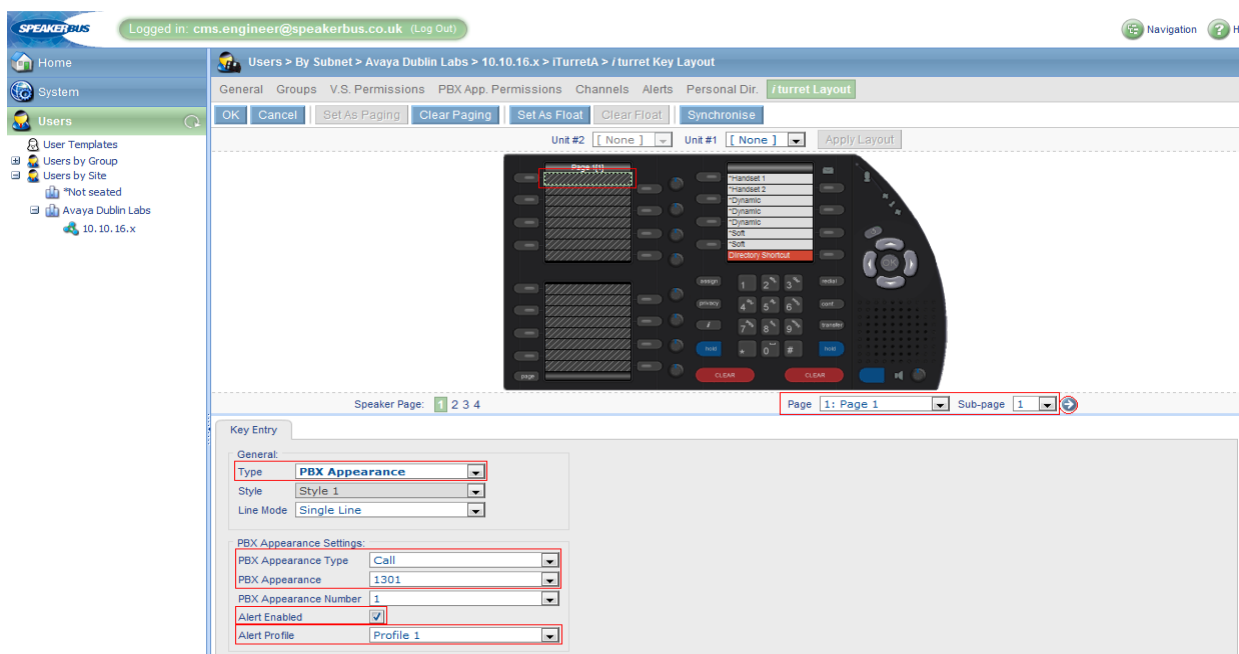


After all of the iTurret keys have been created on the deskstation, the iTurret layout will appear as shown below.



7.16. Assigning Appearances to Deskstation Keys

In the iTurret key layout page, go to **Page 1** of the deskstation by setting the **Page** and **Sub Page** fields to **1** and clicking the arrow key to the right. Select the next available key as highlighted by the red 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** section, set the **PBX Appearance Type** field to **Call** and the **PBX Appearance** field to the main call appearance (e.g., 1301). Select the **Alert Enabled** checkbox so the deskstation rings when a call is received on this call appearance. The **Alert Profile** field is set to a particular ring type specified in **Profile 1**. Click **OK**. Repeat this procedure to add the next two call appearances.



[SPEAKERBUS](#)
 Logged in: cms.engineer@speakerbus.co.uk (Log Out)
 [Navigation](#)

[Home](#)
[System](#)
[Users](#)

[User Templates](#)
[Users by Group](#)
[Users by Site](#)
[*Not seated](#)
[Avaya Dublin Labs](#)
[10.10.16.x](#)

Users > By Subnet > Avaya Dublin Labs > 10.10.16.x > iTurretA > / turret Key Layout

[General](#)
[Groups](#)
[V.S. Permissions](#)
[PBX App. Permissions](#)
[Channels](#)
[Alerts](#)
[Personal Dir.](#)
[/ turret Layout](#)

[Delete](#)
[Apply](#)
[Set As Paging](#)
[Clear Paging](#)
[Set As Float](#)
[Clear Float](#)
[Synchronise](#)

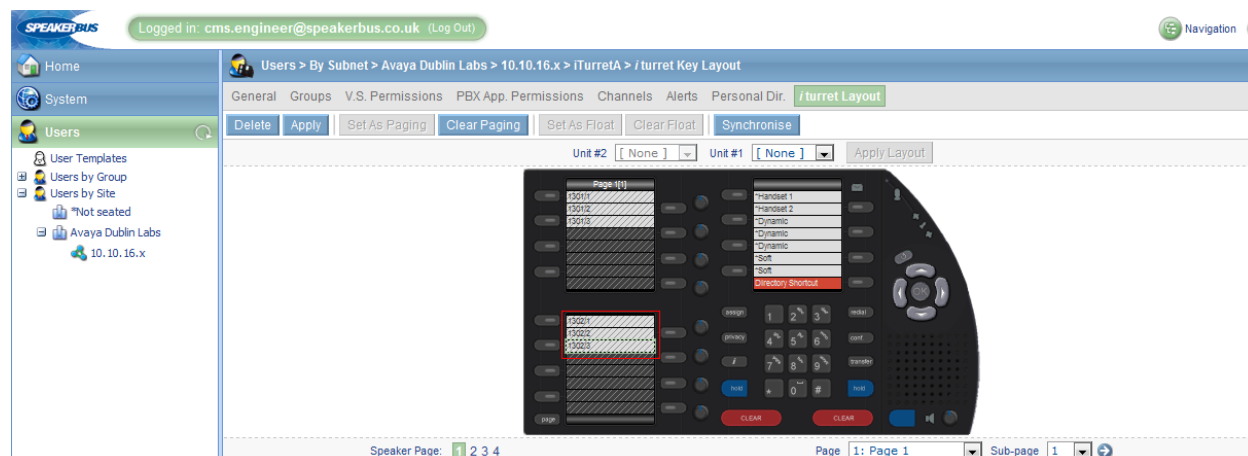
Unit #2 [\[None \]](#)
 Unit #1 [\[None \]](#)
[Apply Layout](#)

Speaker Page: [1](#) [2](#) [3](#) [4](#)
 Page [1](#): [Page 1](#)
 Sub-page [1](#)

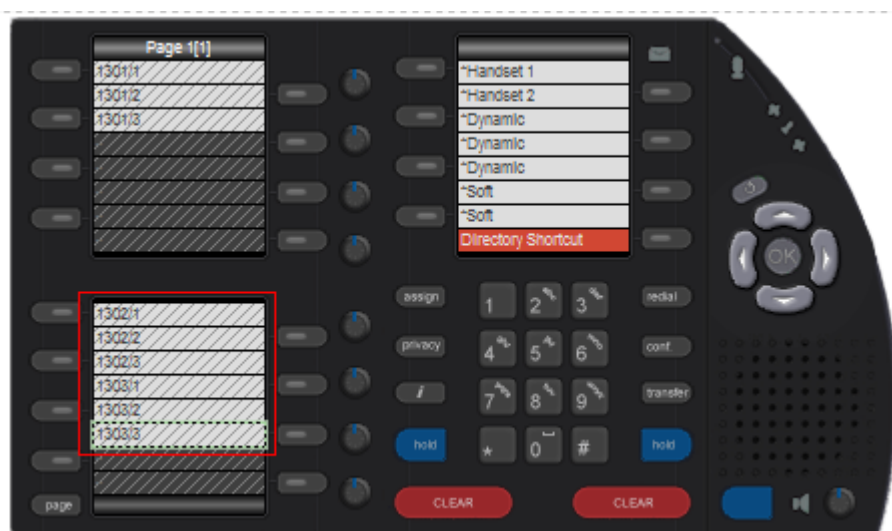
In the iTurret key layout page, go to Page 1 of the deskstation by setting the **Page** and **Sub Page** fields to **1** and clicking the arrow key to the right. Select the next available key in the lower section of page one. The next three keys on this page will be assigned to bridged call appearances. In the **Key Entry** tab, set the **Type** field to **PBX Appearance**. Under the **PBX Appearance Settings** section, set the **PBX Appearance Type** field to **Call** and the **PBX Appearance** field to the main call appearance of iTurretB (e.g., 1302). Set the **PBX Appearance Number** field to the number of line appearance that will be bridged (1 for 1st line appearance, 2 for the 2nd line appearance, etc.). Repeat this procedure to add the next two bridged call appearances.

MMc; Reviewed:
SPOC 2/8/2011

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



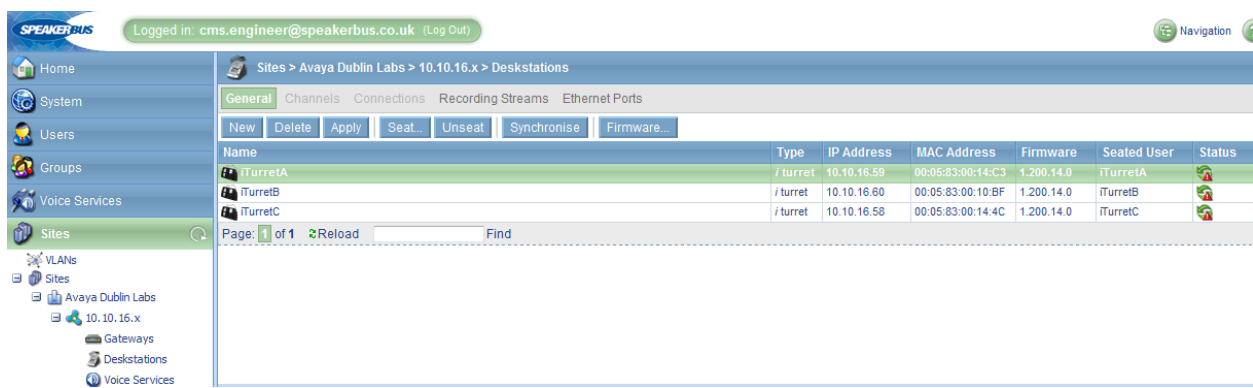
Further bridged call appearances may be added by repeating the procedure outlined in this section. For the compliance test each iTurret was configured with bridged call appearances for the other two iTurrets used in the test configuration. As illustrated below






7.18. Synchronise Deskstations

To send the new configuration to the iTurret deskstations, the deskstations need to be synchronised with iCMS. Under the **Sites** directory tree, expand **Avaya Dublin 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 synchronised on their displays. After the deskstations have been synchronised, the status icons on the iD808 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.



Name	Type	IP Address	MAC Address	Firmware	Seated User	Status
iTurretA	i turret	10.10.16.59	00:05:83:00:14:C3	1.200.14.0	iTurretA	
iTurretB	i turret	10.10.16.60	00:05:83:00:10:BF	1.200.14.0	iTurretB	
iTurretC	i turret	10.10.16.58	00:05:83:00:14:4C	1.200.14.0	iTurretC	

7.19. 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 iCMS. Please refer to [5] 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.

1. On the Speakerbus iD808 *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 iD808 deskstations have successfully registered with SIP Enablement Services, from the administration web page navigate to **Users** → **Search Registered Users** and click the **Search** button (not shown) this will display a list of registered users on SIP Enablement Services as shown below.

Registered Users on 10.10.16.5

Registered and Provisioned Users | Registered Users | Provisioned Users | Search | Refresh |

Showing 1 to 4 of 4 registered contacts.

Handle and Name	Address	Expires
<input type="checkbox"/> 1301@sip.avaya.com iTurret1, iD808	sip:1301@10.10.16.59	Mon, 04 Oct 2010 18:30:32 IST
<input type="checkbox"/> 1501@sip.avaya.com HS1 1301, Privacy	sip:1501@10.10.16.59	Mon, 04 Oct 2010 18:31:08 IST
<input type="checkbox"/> 1502@sip.avaya.com HS2 1301, Privacy	sip:1502@10.10.16.59	Mon, 04 Oct 2010 18:25:35 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**
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 the *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 describe the administration steps required to use Speakerbus iD808 *i* turrets 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 AuraTM Communication Manager*, May 2009, Issue 5.0, Document Number 03-300509.
- [2] *Avaya Extension to Cellular User Guide Avaya AuraTM Communication Manager*, Nov 2009
- [3] *SIP Support in Avaya AuraTM Communication Manager Running on the Avaya S8xxx Servers*, May 2009, Issue 9, Document Number 555-245-206.
- [4] *Installing, Administering, Maintaining, and Troubleshooting Avaya AuraTM SIP Enablement Services*, Nov 2009, Issue 8.0, Document Number 03-600768.
- [5] *Speakerbus i manager Administrator's Guide*, 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.