



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for configuring Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2 to Interoperate with Speakerbus iD808 iTurret – Issue 1.0**

### **Abstract**

These Application Notes describe the steps required to connect Speakerbus iD808 iTurret to a SIP infrastructure consisting of Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Also described is how Avaya Aura® Communication Manager features can be made available in addition 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 iTurret, 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 iTurret to a SIP infrastructure consisting of Avaya Aura® Session Manager 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 by iTurret. In this configuration, the Off-PBX Stations (OPS) feature set is extended from Avaya Aura® Communication Manager to the Speakerbus iD808 iTurret, providing the iTurret deskstation with enhanced calling features.

The following table provides a summary of the supported features available on iTurret with the Avaya SIP offer. Some features are supported locally in iTurret, while others are only available with Avaya Aura® Communication Manager and Avaya Aura® Session Manager with OPS. In addition to basic calling capabilities, the Internet Engineering Task Force (IETF) has defined a supplementary set of calling features, often referred to as the SIPING-19 [6]. This provides a useful framework to describe product capabilities and compare features supported by various equipment vendors. Additional features beyond the SIPING-19 can be extended to iTurret using OPS.

Some OPS features listed in the following table can be invoked by dialing a Feature Name Extension (FNE). A speed dial button on iTurret can also be programmed to 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 (COS), Class Of Restriction (COR), and voice messaging. Details on operation and administration of OPS can be found in References [2] and [3]. The Avaya SIP solution requires all SIP telephones to be configured in Avaya Aura® Communication Manager as OPS. Items in the table below shown in **bold** were tested using an FNU or FNE.

FEATURE	SUPPORTED		COMMENTS
	Locally at the phone	With Avaya SIP Offer	
SIPPING-19 Features			
Call Hold	YES	YES	
Consultation Hold	YES	YES	
Unattended Transfer	YES	YES	
Attended Transfer	YES	YES	
Call Forward All	YES	YES	Local menu option on iTurret and FNU
Call Forward Busy/No answer	YES	YES	Local menu option on iTurret and FNU
Call Forward Cancel	YES	YES	Local menu option on iTurret and FNU
3-way conferencing (3 <sup>rd</sup> party added)	YES	YES	
3-way conferencing (3 <sup>rd</sup> 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 6300/6301
Call Pickup	NO	YES	Via OPS FNE 6312
Automatic Redial	NO	YES	Via OPS FNE n/a
OPS – Selected Additional Station-Side Features			
Conference on answer	NO	YES	Via OPS FNE 6302
Directed call pickup	NO	YES	Via OPS FNE 6303
Drop last added party	NO	YES	Via OPS FNE 6304
Exclusion/Privacy	YES	YES	Local hard key on iTurret using FNU
Last number dialed	YES	YES	Via OPS FNE 6306
Priority Call	NO	YES	Via OPS FNE 6307, iTurret doesn`t support distinctive ring indication
Send All Calls	NO	YES	Via OPS FNE 6308
Send All Calls Cancel	NO	YES	Via OPS FNE 6309
Transfer to Voicemail	NO	YES	Via OPS FNE 6310
Whisper Page	NO	YES	Via OPS FNE 6311

Table 1

## 2. General Test Approach and Test Results

To verify interoperability of the iD808 iTurret with Communication Manager and Session Manager, 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 iTurret, FNEs, and FNUs.

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

## 2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of iTurret with Session Manager
- Calls between iTurret and Avaya SIP, H.323, and digital stations with correct calling/called name presentation
- Direct IP-IP Media (shuffling)
- Correct SIP signaling
- G.711, G.722-64k and G.729 codec support
- COR restricted calls
- Multi appearance call handling
- Hold/Retrieve operations
- Consultation calls
- Supervised and blind transfers
- Conferencing
- Bridged appearances
- Privacy
- PSTN calls
- Proper recognition of DTMF transmissions by navigating voicemail menus
- Proper operation of voicemail with message waiting indicators (MWI)
- Extended telephony features using Communication Manager Feature Name Extensions (FNEs) shown in bold in the table above
- Exclusion/Privacy using the Exclusion FNU
- Call forwarding (busy and no-answer) and Send All Calls using Call Forwarding and Send All Call FNU's.
- Proper system recovery after an iTurret restart and loss of IP connection
- Proper failover to alternate Session Manager

## 2.2. Test Results

All tests were executed successfully.

## 2.3. Support

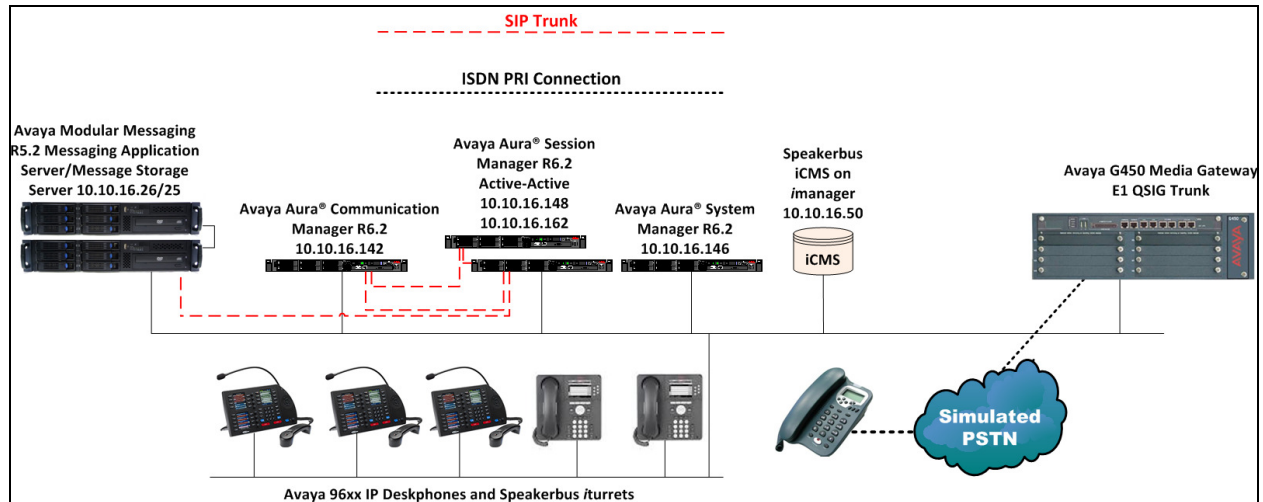
For technical support of Speakerbus products contact the Speakerbus Service Desk:

- Web: <http://www.speakerbus.com>
- Email: [info@speakerbus.com](mailto: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

An Avaya S8800 Server running Communication Manager R6.2 serving H323 endpoints with an Avaya G450 Media Gateway was configured along with Session Manager R6.2 hosted on an Avaya S8800 Server serving SIP endpoints. An additional Session Manager hosted as a virtual appliance was used to provide failover in an active-active configuration. System Manager hosted

on an Avaya S8800 Server is used to provision Communication Manager and Session Manager. Speakerbus iTurrets were connected to the LAN and managed by the iManager application running on a local Windows server. Simulated connection to the PSTN was provided by an E1 QSIG trunk connected to the Avaya G450 Media Gateway. Avaya Modular Messaging provided voicemail.



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

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 SP5 build R016x.02.0.823.0-20396
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 SP3
Avaya Aura® Session Manager running as a Virtual Appliance	R6.2 SP3
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 SP4
Avaya Modular Messaging running on S3500 Servers	5.2 Patch 8 MAS - 9.2.150.13
Avaya 9630 IP Deskphone	<ul style="list-style-type: none"><li>• H323 S3.105S</li><li>• SIP 2.6.8.4</li></ul>
Speakerbus iCMS with iManager Administration running on Windows Server	v2.100
Speakerbus iTurret	v2.1/ v1.40 SIP revision

## 5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring the iTurret as an Off-PBX Station (OPS), administering support for the OPS features indicated in **Error! Reference source not found.**, and configuring a SIP trunk between Communication Manager and Session Manager. Unless otherwise stated, administration of Communication manager is performed using the System Access Terminal (SAT).

## 5.1. Define System Features

Enter the command **change system-parameters features** to administer system wide features for SIP endpoints. Those related to features listed in **Error! Reference source not found.** are shown in bold. On **Page 18**, set the **Whisper Page Tone Given To** field to **all**

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

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

WHISPER PAGE
    Whisper Page Tone Given To: all

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

Pickup On Transfer? y
```

On **Page 18** make sure **Directed Call Pickup** is set to **y**.

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

IP PARAMETERS
    Direct IP-IP Audio Connections? y
        IP Audio Hairpinning? n
        Synchronization over IP? n
    SDP Capability Negotiation for SRTP? y
    SIP Endpoint Managed Transfer? 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
```

## 5.2. Define the Dial Plan

Use the **change dialplan analysis** command to define the dial plan used in the system. This includes all station extensions, OPS Feature Name Extensions (FNEs), and Feature Access Codes (FACs). To define the FNEs for the OPS features listed in **Error! Reference source not found.**, a Feature Access Code (FAC) must also be specified for the corresponding feature. In the sample configuration, telephone extensions are four digits long and begin with **6**, FNEs are also four digits beginning with **6**, and the FACs have formats as indicated with a **Call Type** of **fac**.

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			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	attd						
1	3	fac						
2	10	udp						
4	4	udp						
5	4	ext						
<b>6</b>	<b>4</b>	<b>ext</b>						
7	3	dac						
8	4	udp						
9	1	fac						
<b>*</b>	<b>3</b>	<b>fac</b>						



### 5.3. 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 10
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: *14			
<b>Answer Back Access Code: *15</b>			
Auto Alternate Routing (AAR) Access Code: *00			
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:	
Automatic Callback Activation:		Deactivation:	
Call Forwarding Activation Busy/DA: All: *03		Deactivation: *04	
Call Forwarding Enhanced Status: Act:		Deactivation:	
<b>Call Park Access Code: *01</b>			
<b>Call Pickup Access Code: *02</b>			
CAS Remote Hold/Answer Hold-Unhold Access Code:			
CDR Account Code Access Code: *51			
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 10
FEATURE ACCESS CODE (FAC)			
Contact Closure Pulse Code:			
Data Origination Access Code:			
Data Privacy Access Code:			
<b>Directed Call Pickup Access Code: *16</b>			
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:			
<b>Last Number Dialed Access Code: *17</b>			
Leave Word Calling Message Retrieval Lock:			
Leave Word Calling Message Retrieval Unlock:			

**change feature-access-codes****Page 3 of 10**

## FEATURE ACCESS CODE (FAC)

Leave Word Calling Send A Message: \*86  
Leave Word Calling Cancel A Message: \*87  
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: \*22  
Per Call CPN Unblocking Code Access Code: \*23  
Posted Messages Activation: Deactivation:  
Priority Calling Access Code: \*18  
Program Access Code:  
  
Refresh Terminal Parameters Access Code:  
Remote Send All Calls Activation: Deactivation:  
Self Station Display Activation:  
**Send All Calls Activation: \*19 Deactivation: \*20**  
Station Firmware Download Access Code:

**change feature-access-codes****Page 4 of 10**

## 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:  
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: \*21**  
3PCC H323 Override SIP Station Activation: Deactivation:  
  
PIN Checking for Private Calls Access Code:  
PIN Checking for Private Calls Using ARS Access Code:  
PIN Checking for Private Calls Using AAR Access Code:

## 5.4. Define Feature Name Extensions (FNEs)

The OPS FNEs can be defined using the **change off-pbx-telephone feature-name-extensions set 1** 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:

Active Appearance Select:
Automatic Call Back:
Automatic Call-Back Cancel:
Call Forward All:
Call Forward Busy/No Answer:
Call Forward Cancel:
Call Park: 6300
Call Park Answer Back: 6301
Call Pick-Up: 6312
Calling Number Block:
Calling Number Unblock:
Conditional Call Extend Enable:
Conditional Call Extend Disable:
Conference Complete:
Conference on Answer:
Directed Call Pick-Up: 6303
Drop Last Added Party:
```

```
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):
Extended Group Call Pickup:
Held Appearance Select:
Idle Appearance Select:
Last Number Dialed: 6306
Malicious Call Trace:
Malicious Call Trace Cancel:
Off-Pbx Call Enable:
Off-Pbx Call Disable:
Priority Call:
Recall:
Send All Calls: 6308
Send All Calls Cancel: 6309
Transfer Complete:
Transfer On Hang-Up:
Transfer to Voice Mail:
Whisper Page Activation: 6311
```

## 5.5. Configure Class of Service (COS)

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

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

## 5.6. 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 *iTurrets* were assigned to COR 1.

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

## 5.7. Configure SIP Trunks to each Session Manager

Enter the command **change node-names ip** and enter the **IP Address** assigned for the **procr**, **sm1** and **sm2** where **sm1** and **sm2** are the SIP signaling interfaces for each Session Manager.

change node-names ip	Page 1 of 2
IP NODE NAMES	
Name	IP Address
default	0.0.0.0
gateway	10.10.16.1
<b>procr</b>	<b>10.10.16.142</b>
procr6	::
<b>sm2</b>	<b>10.10.16.162</b>
<b>sm1</b>	<b>10.10.16.148</b>
( 15 of 15 administered node-names were displayed )	
Use 'list node-names' command to see all the administered node-names	
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name	

Enter the command **add signaling-group 1** where signaling group 1 is the first SIP signaling group. The following are configured:

- **Group Type** – set to **sip**
- **Transport Method** – configure as **tls**
- **Near-end Node Name** – enter the **procr** node name
- **Far-end Node Name** – enter the **sm1** node name
- **Near-end Listen Port** and **Far-end Listen Port** – by default for TLS this is **5061**
- **Far-end Network Region** – set to the relevant IP Network Region, in this case **1**

<b>add signaling-group 1</b>		<b>Page 1 of 2</b>
SIGNALING GROUP		
Group Number: 1	<b>Group Type: sip</b>	
IMS Enabled? n	<b>Transport Method: tls</b>	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
<b>Near-end Node Name: procr</b>	<b>Far-end Node Name: sm1</b>	
<b>Near-end Listen Port: 5061</b>	<b>Far-end Listen Port: 5061</b>	
	<b>Far-end Network Region: 1</b>	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Configure accordingly for each signaling group required to each Session Manager.

display signaling-group 5		Page	1 of	2
SIGNALING GROUP				
Group Number: 5	Group Type: sip			
IMS Enabled? n	Transport Method: tls			
Q-SIP? n				
IP Video? n	Enforce SIPS URI for SRTP? y			
Peer Detection Enabled? y	Peer Server: SM			
Near-end Node Name: procr		Far-end Node Name: sm2		
Near-end Listen Port: 5061		Far-end Listen Port: 5061		
		Far-end Network Region: 1		
Far-end Domain:				
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n		
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n		
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? y		
Enable Layer 3 Test? y		IP Audio Hairpinning? n		
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? n		
		Alternate Route Timer(sec): 6		

Enter the command **add trunk-group 1** where trunk-group 1 is the first trunk group between Communication Manager and the first Session Manager. On **Page 1** configure the following:

- **Group Type** – enter **sip**
- **Group Name** – enter an identifying name
- **TAC** – enter a TAC appropriate to the dialplan
- **Service Type** – set to **public-ntwrk**
- **Member Assignment Method** – set to **auto**
- **Signaling Group** – configure with the signaling group to the first Session Manager
- **Number of Members** – configure as required, in this case **30**

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: TRUNK TO sm61	COR: 1	TN: 1	TAC: 701
Direction: two-way	Outgoing Display? y		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 1		
	Number of Members: 30		

On **Page 3** configure the **Numbering Format** as **private**.

<b>add trunk-group 1</b>	<b>Page 3 of 21</b>
TRUNK FEATURES	
ACA Assignment? n	Measured: both
	Maintenance Tests? y
<b>Numbering Format: private</b>	
	UI Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y	

Repeat for the SIP trunk-group to the second Session Manager.

<b>add trunk-group 5</b>	<b>Page 1 of 21</b>		
TRUNK GROUP			
Group Number: 5	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: trunk to sm2</b>	COR: 1	TN: 1	<b>TAC: 705</b>
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
<b>Service Type: public-ntwrk</b>	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 5		
	Number of Members: 30		



```

add trunk-group 5                                     Page 3 of 21
TRUNK FEATURES
    ACA Assignment? n                                Measured: both
                                                    Maintenance Tests? y

    Numbering Format: private
                                                    UUI Treatment: service-provider

                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n

    Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y

```

## 5.8. Configure Route Pattern

Enter the command **change route-pattern 1** where route pattern 1 is used to route calls between Communication Manager and Session Manager. Enter an identifying **Pattern Name**. Ensure that both SIP trunk-groups are configured in the **Grp No** fields and enter an **FRL** as appropriate. In the instance where all the channels in trunk-group 1 are in use, or trunk-group 1 is out of service, traffic between Communication Manager and Session Manager will route over trunk-group 5.

```

change route-pattern 1                               Page 1 of 3
    Pattern Number: 1    Pattern Name: to SMS
        SCCAN? n        Secure SIP? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/ IXC
    No      Mrk Lmt List Del  Digits      QSIG
                                     Dgts      Intw
1: 1      0
2: 5      0
3:
4:
5:
6:

    BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W      Request      Dgts Format      Subaddress
1: y y y y y n  n          rest          none
2: y y y y y n  n          rest          none
3: y y y y y n  n          rest          none
4: y y y y y n  n          rest          none
5: y y y y y n  n          rest          none
6: y y y y y n  n          rest          none

```

## 5.9. Configure IP-Codec Set

Enter the command **change ip-codec-set 1** and enter the required codecs. For the purposes of the compliance test, IP-network-region 1 uses ip-codec-set 1.

change ip-codec-set 1

Page1 of 2

IP Codec Set

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: G.722-64K		2	20
2: G.711MU	n	2	20
3: G.711A	n	2	20
4: G.729	n	2	20
5:			
6:			
7:			

Media Encryption

1: none

2:

3:

## 5.10. Configure Private Numbering

Enter the command **change private-numbering 0** and configure as follows:

**Ext Len** – set to the extension length of the SIP extension number, in this case **4**

**Ext Code** – set to the first digit of the SIP extension number, in this case **6**

**Trk Grp** – enter the SIP trunk groups configured above, in this case **1** and **5**

**Total Len** – enter the total length of the SIP extension number, in this case **4**

change private-number 0				Page	1 of	2
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp(s)	Prefix	Len		
4	6	1		4	Total Administered: 3	
4	6	5		4	Maximum Entries: 540	

## 6. Configure Avaya Aura® Session Manager

This section illustrates relevant aspects of the Session Manager configuration required for interoperating with Speakerbus.

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

**AVAYA** Avaya Aura® System Manager 6.2

Home / Log On

### Log On

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

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

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

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

User ID:

Password:

**Log On**

[Change Password](#)

It is assumed that the Domains, Locations, SIP entities for each Session Manager, Communication Manager and Modular Messaging, Entity Links, Routing Policies, Dial Patterns and Application Sequences have been configured.

## 6.1. Configure UDP Port for Speakerbus Registration

Each Session Manager Entity must be configured so that the iTurret can register to it using UDP. From the web interface click **Routing → SIP Entities → sm1** where **sm1** is the first Session Manager entity. In the **Port** section click **Add** and enter the following:

- **Port** – enter **5060** which is the UDP port the iTurret sends its SIP registration to
- **Protocol** – select **UDP** from the drop down list
- **Default Domain** – select the appropriate SIP domain from the drop down list

Click **Commit** (not shown) when done.

**Port**

TCP Failover port:

TLS Failover port:

**Add** **Remove**

4 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/>	<input type="text" value="avaya.com"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="TCP"/>	<input type="text" value="avaya.com"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	<input type="text" value="TLS"/>	<input type="text" value="avaya.com"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5080"/>	<input type="text" value="TCP"/>	<input type="text" value="avaya.com"/>	<input type="text"/>

Select : [All](#), [None](#)

Repeat accordingly on the alternative Session Manager.

## 6.2. Add Primary iTurret User

A user must be added for each iTurret. Click **User Management** → **Manage Users** → **New** and configure as follows:

- **First Name** and **Last Name** – enter an identifying name
- **Login Name** – enter the extension number followed by the domain, in this case **6031@avaya.com**
- **Authentication Type** – select **Basic** from the drop down list
- **Password** and **Confirm Password** – enter and confirm a password

Home / Users / User Management / Manage Users [Help ?](#)

### New User Profile

[Commit & Continue](#) [Commit](#) [Cancel](#)

**Identity** \* **Communication Profile** \* **Membership** **Contacts**

**Identity** ▾

\* **Last Name:**

\* **First Name:**

**Middle Name:**

**Description:**

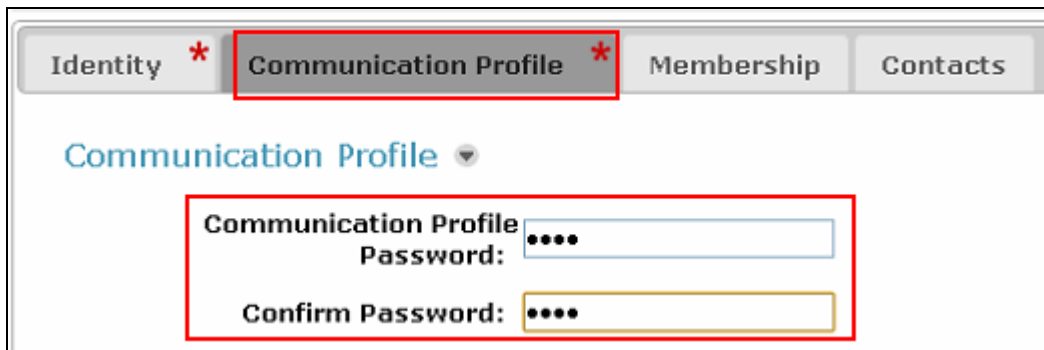
\* **Login Name:**

\* **Authentication Type:**  ▾

\* **Password:**

\* **Confirm Password:**

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



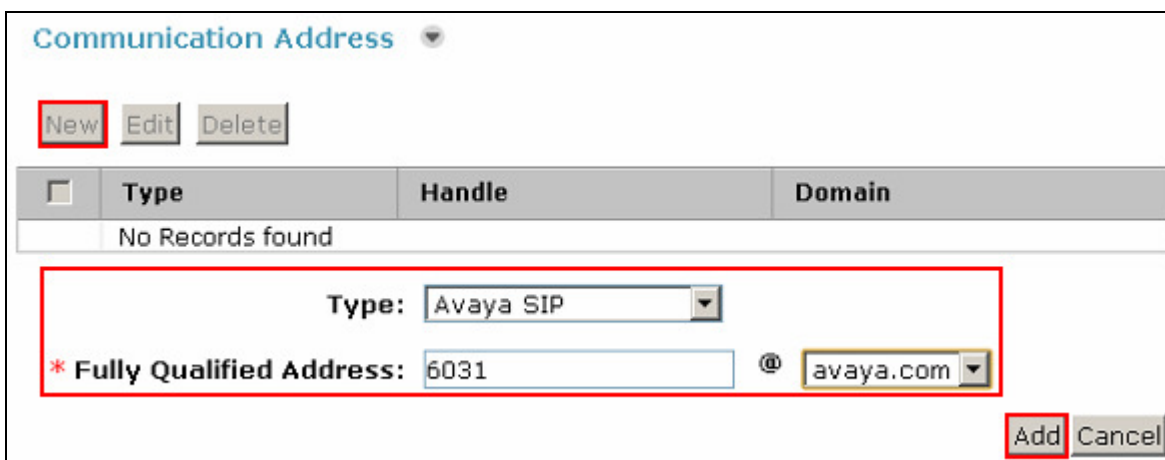
Identity \* **Communication Profile \*** Membership Contacts

Communication Profile ▼

Communication Profile Password: ....

Confirm Password: ....

In the **Communication Address** section click **New**. In the **Fully Qualified Address** field enter the extension number as required, and select the appropriate **Domain** from the drop down list. Click **Add** when done.



Communication Address ▼

**New** Edit Delete

<input type="checkbox"/>	Type	Handle	Domain
No Records found			

Type: Avaya SIP ▼

\* Fully Qualified Address: 6031 @ avaya.com ▼

**Add** Cancel

Place a tick in the **Session Manager Profile** check box and configure the **Primary Session Manager**, **Secondary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence** and **Home Location**, from the respective drop down lists. The Primary and Secondary Session Manager are **sm1** and **sm2** respectively.

☒ **Session Manager Profile**

\* **Primary Session Manager**

sm1

**Secondary Session Manager**

sm2

Primary	Secondary	Maximum
28	0	28

Primary	Secondary	Maximum
0	14	14

**Origination Application Sequence**

CM62AppSeq

**Termination Application Sequence**

CM62AppSeq

**Conference Factory Set**

(None)

**Survivability Server**

(None)

\* **Home Location**

DevConnectLab

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

- **System** – select the relevant Communication Manager SIP Entity from the drop down list
- **Profile Type** – select **Endpoint** from the drop down list
- **Extension** – enter the required extension number, in this case **6031**
- **Template** – select **DEFAULT\_9630SIP\_CM\_6\_2** from the drop down list
- **Port** – enter **IP**

Click **Commit** (not shown) when done.

The screenshot shows a configuration form for a CM Endpoint Profile. A red box highlights the top section containing the 'CM Endpoint Profile' checkbox (checked), the 'System' dropdown (set to 'CM62'), and the 'Profile Type' dropdown (set to 'Endpoint'). Another red box highlights the 'Extension' field (containing '6031') and the 'Template' dropdown (set to 'DEFAULT\_9630SIP\_CM\_6\_2'). A third red box highlights the 'Port' field (containing 'IP'). Other fields include 'Use Existing Endpoints' (unchecked), 'Set Type' (set to '9630SIP'), 'Security Code' (empty), 'Voice Mail Number' (empty), 'Preferred Handle' (set to '(None)'), 'Delete Endpoint on Unassign of Endpoint from User or on Delete User' (unchecked), and 'Override Endpoint Name' (checked).

☒ **CM Endpoint Profile**

\* **System** CM62

\* **Profile Type** Endpoint

Use Existing Endpoints ☐

\* **Extension** 6031 Endpoint Editor

\* **Template** DEFAULT\_9630SIP\_CM\_6\_2

**Set Type** 9630SIP

**Security Code**

\* **Port** IP

**Voice Mail Number**

**Preferred Handle** (None)

Delete Endpoint on Unassign of Endpoint from User or on Delete User ☐

**Override Endpoint Name** ☒



### 6.3. Configure Privacy Users

Privacy users are configured on System Manager as bridged appearances to the Primary User. Add a Privacy User in the same way as the Primary User is configured in **Section 6.2**. In this case the Privacy Users created for Extension 6031 are extensions 6041 and 6051.

### 6.4. Configure Privacy Endpoint

Click **Communication Manager** → **Endpoints** → **Manage Endpoints** and select the relevant privacy endpoint and click **Edit**, in this case **Extension 6041**.

Communication Manager | Home / Elements / Communication Manager / Endpoints / Manage Endpoints

**Endpoints** [Switch to Classic View]

Select device(s) from Communication Manager List

Show List

Endpoint List

View Edit New Delete Duplicate More Actions Maintenance Advanced Search

66 Items | Refresh | Show 15 | Filter: Enable

<input type="checkbox"/>	Name	Extension	Port	Set Type	COS	COR	User	System
<input type="checkbox"/>	AVAYA GROUP	6020		virtual	1	1		CM62
<input type="checkbox"/>	Speakerbus, 6031	6031	S00095	9630SIP	1	1	6031@avaya.com	CM62
<input type="checkbox"/>	Speakerbus, 6032	6032	S00096	9630SIP	1	1	6032@avaya.com	CM62
<input type="checkbox"/>	Speakerbus, 6033	6033	S00097	9630SIP	1	1	6033@avaya.com	CM62
<input checked="" type="checkbox"/>	Bridge, 6041	6041	S00098	9630SIP	1	1	6041@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6042	6042	S00099	9630SIP	1	1	6042@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6043	6043	S00100	9630SIP	1	1	6043@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6051	6051	S00101	9630SIP	1	1	6051@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6052	6052	S00102	9630SIP	1	1	6052@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6053	6053	S00104	9630SIP	1	1	6053@avaya.com	CM62

Click the **Button Assignments** tab and configure as shown below, where buttons **2, 3** and **4** are configured as **brdg-appr** for **Button 1, 2** and **3** of Primary User **Extn 6031**. Ensure that button **5** is configured as **exclusion**.

<b>System</b>	CM62	<b>Extension</b>	6041
<b>Template</b>	Select	<b>Set Type</b>	9630SIP
<b>Port</b>	S00098	<b>Security Code</b>	*****
<b>Name</b>	Bridge, 6041		

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)
Enhanced Call Fwd (E)	Button Assignment (B)	Group Membership (M)	

Main Buttons	Feature Buttons	Button Modules			
1	call-appr				
2	brdg-appr	Button	1	Ext	6031
3	brdg-appr	Button	2	Ext	6031
4	brdg-appr	Button	3	Ext	6031
5	exclusion				
6	Select				
7	Select				
8	Select				

Repeat as necessary for additional Privacy Users, as shown below for **Extension 6051**.

<b>System</b>	CM62	<b>Extension</b>	6051
<b>Template</b>	Select	<b>Set Type</b>	9630SIP
<b>Port</b>	S00101	<b>Security Code</b>	●●●●●●
<b>Name</b>	Bridge, 6051		

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)
Enhanced Call Fwd (E)	Button Assignment (B)	Group Membership (M)	

Main Buttons	Feature Buttons	Button Modules			
1	call-appr				
2	brdg-appr	Button	1	Ext	6031
3	brdg-appr	Button	2	Ext	6031
4	brdg-appr	Button	3	Ext	6031
5	Select				
6	Select				
7	Select				
8	Select				

## 6.5. Configure iTurret Endpoint

Click **Communication Manager** → **Endpoints** → **Manage Endpoints** and select the relevant Primary User endpoint and click **Edit**, in this case **Extension 6031**.

The screenshot shows the 'Endpoints' management page in the Avaya Communication Manager interface. The left sidebar contains a navigation menu with options like 'Call Center', 'Coverage', 'Endpoints', 'Alias Endpoint', 'Intra Switch CDR', 'Manage Endpoints', 'Off PBX Endpoint', 'Mapping', 'Site Data', 'Xmobile', 'Configuration', 'Groups', 'Network', 'Parameters', and 'System'. The main content area is titled 'Endpoints' and includes a breadcrumb trail: 'Home / Elements / Communication Manager / Endpoints / Manage Endpoints'. Below the title, there is a link to 'Select device(s) from Communication Manager List' and a 'Show List' button. The 'Endpoint List' section features a toolbar with buttons for 'View', 'Edit' (highlighted with a red box), 'New', 'Delete', 'Duplicate', 'More Actions', and 'Maintenance'. Below the toolbar, a table displays a list of endpoints. The table has columns for 'Name', 'Extension', 'Port', 'Set Type', 'COS', 'COR', 'User', and 'System'. The row for 'Speakerbus, 6031' is highlighted with a red box. The table also includes a 'Filter: Enable' option and a 'Show 15' dropdown.

<input type="checkbox"/>	Name	Extension	Port	Set Type	COS	COR	User	System
<input type="checkbox"/>	AVAYA GROUP	6020		virtual	1	1		CM62
<input checked="" type="checkbox"/>	Speakerbus, 6031	6031	S00095	9630SIP	1	1	6031@avaya.com	CM62
<input type="checkbox"/>	Speakerbus, 6032	6032	S00096	9630SIP	1	1	6032@avaya.com	CM62
<input type="checkbox"/>	Speakerbus, 6033	6033	S00097	9630SIP	1	1	6033@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6041	6041	S00098	9630SIP	1	1	6041@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6042	6042	S00099	9630SIP	1	1	6042@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6043	6043	S00100	9630SIP	1	1	6043@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6051	6051	S00101	9630SIP	1	1	6051@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6052	6052	S00102	9630SIP	1	1	6052@avaya.com	CM62
<input type="checkbox"/>	Bridge, 6053	6053	S00104	9630SIP	1	1	6053@avaya.com	CM62

Click the **Feature Options** tab and place a check in the **Bridged Call Alerting** box.

General Options (G) *		<b>Feature Options (F)</b>		Site Data (S)		Abbreviated Call Dialing (A)	
Enhanced Call Fwd (E)		Button Assignment (B)		Group Membership (M)			
Active Station Ringing	single	Auto Answer	none	MWI Served User Type	Select	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	Select	Display Language	english	IP Phone Group ID		Hunt-to Station	
Remote Soft Phone Emergency Calls	Select	Loss Group	19	LWC Reception	spe	Survivable COR	internal
AUDIX Name		Time of Day Lock Table	Select	Speakerphone	Select	Voice Mail Number	
Short/Prefixed Registration Allowed	Select			EC500 State	enabled		
<b>Features</b>							
<input type="checkbox"/> Always Use				<input type="checkbox"/> Idle Appearance Preference			
<input type="checkbox"/> IP Audio Hairpinning				<input type="checkbox"/> IP SoftPhone			
<input checked="" type="checkbox"/> Bridged Call Alerting				<input checked="" type="checkbox"/> LWC Activation			
<input type="checkbox"/> Bridged Idle Line Preference				<input type="checkbox"/> CDR Privacy			
<input checked="" type="checkbox"/> Coverage Message Retrieval				<input checked="" type="checkbox"/> Direct IP-IP Audio Connections			
<input type="checkbox"/> Data Restriction				<input checked="" type="checkbox"/> H.320 Conversion			
<input checked="" type="checkbox"/> Survivable Trunk Dest				<input type="checkbox"/> IP Video			
<input type="checkbox"/> Bridged Appearance Origination Restriction				<input type="checkbox"/> Per Button Ring Control			
<input checked="" type="checkbox"/> Restrict Last Appearance							

Click the **Button Assignments** tab and configure as shown below where buttons **1-4** are configured as **call-appr**, buttons **5** and **6** are configured as **brdg-appr** of **Button 1** of the corresponding Privacy Users. Configure button **7** as **call-fwd** and button **8** as **cfwd-bsyda** in order that the FNU for these features can be activated from the *iTurret*.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)	
Enhanced Call Fwd (E)		Button Assignment (B)		Group Membership (M)			
Main Buttons		Feature Buttons		Button Modules			
1	call-appr						
2	call-appr						
3	call-appr						
4	call-appr						
5	brdg-appr	Button	1	Ext	6041		
6	brdg-appr	Button	1	Ext	6051		
7	call-fwd	Extension					
8	cfwd-bsyda	Extension					

## 6.6. Configure Registration Expiration Timer

The Registration Expiration Timer must be configured in order that SIP endpoints recover from failure of Session Manager with the least amount of downtime. Click **Session Manager → Device and Location Configuration → Device Settings Groups → Default Group**. In the **Server Timer** section configure the **Registration Expiration Timer (secs)** with **Maximum** and **Minimum** values. Click **Save** (not shown) when done. This will cause the endpoints to attempt re-registration at regular intervals. In the event that an endpoint is unable to register to its Primary Session Manager, the endpoint will attempt to register to the alternate Session Manager.

	Maximum	Minimum
Subscription Expiration Timer (secs):	86400	60
Registration Expiration Timer (secs):	90	60

## 7. Speakerbus iTurret Configuration

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

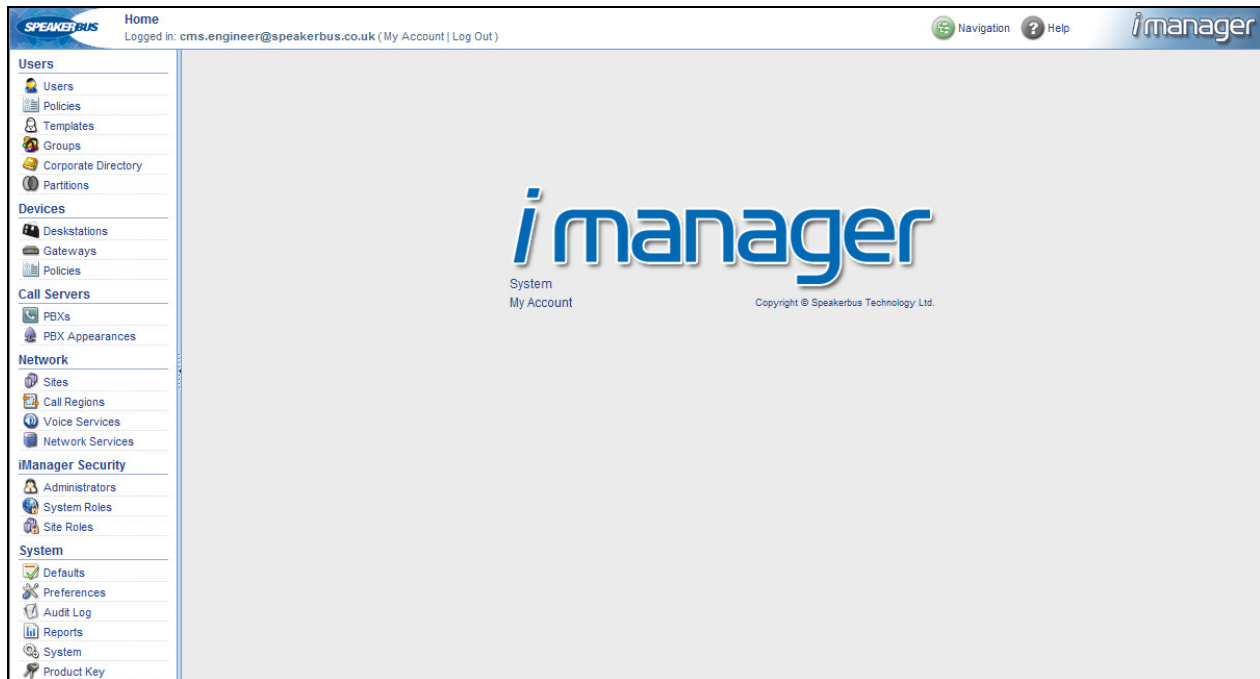
- Launch iManager Web Portal
- Verify Product Key
- Create Site
- Create Call Region
- Create/Verify User Policies
- Create/Verify Device Policies
- Create Network Services
- Confirm Defaults
- Create iTurrets Deskstations
- Create PBX
- Create Dial Plan
- Create Call and Handset Appearances
- Create Users
- Assign User Permissions
- Assign Ownership (of Appearances to Users)
- Assign Default Call Appearances
- Program iTurrets Deskstations (iTurrets Layout)
- Program Appearances to Deskstation Keys (iTurrets Layout)
- Assign Bridged Call Appearances to Deskstations Keys (iTurrets Layout)
- Synchronize Deskstations

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



## 7.1. Launch iManager Web Portal

To access the iManager software interface, open a web browser and type the iManager web address, for example, <http://10.10.16.50/manager>. Press the **Enter** key (not show). In the iManager Web Portal logon page (not shown), enter the appropriate credentials. The iManager Web Portal home page is displayed as shown below.



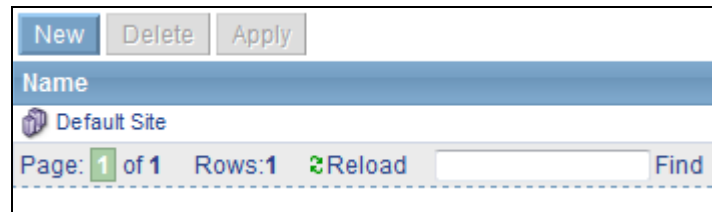
## 7.2. Verify Product Key

Select **System** → **Product Key** in the left pane to verify that a valid key is installed and sufficient devices are allowed.

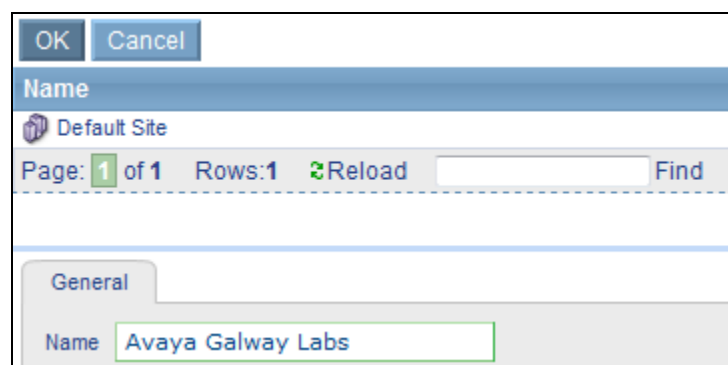
The screenshot shows the 'iCMS Product Key' configuration page. At the top are 'Delete' and 'Apply' buttons. The page has a tabbed interface with the 'iCMS Product Key' tab selected. Below the tabs are four input fields: 'Currently Configured Devices' with a value of '0', 'Maximum Allowable Devices' with a value of '100', 'MAC Address' with a value of '00:0C:29:C1:3A:A3', and 'Product Key' which is currently empty.

### 7.3. Create a Site

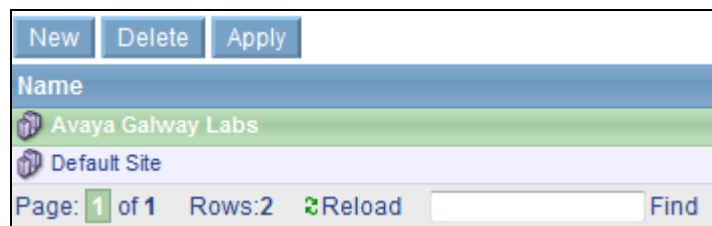
Configure a site representing the location where the Speakerbus iTurret devices are installed. Select **Network** → **Sites** in the left pane (not shown), click on **NEW** as shown below.



Enter an identifying **Name** for the new site, then press **OK**. As shown below.



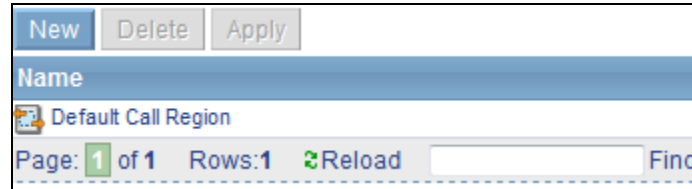
The created site will be visible in the list view as shown below.



**Note:** A default site is available and can be used for a single site setup. Refer to the *Speakerbus iManager Administrator's Guide* for further configuration information.

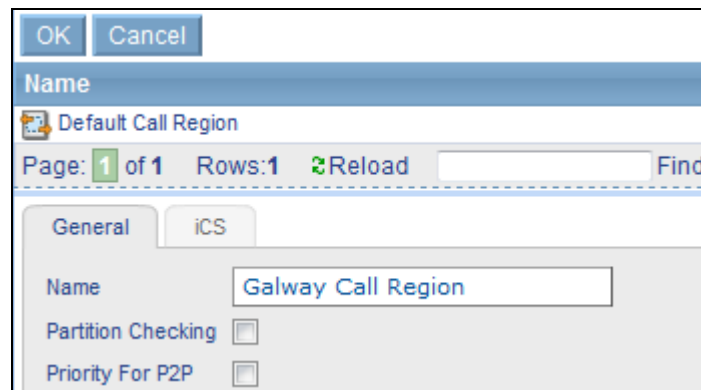
## 7.4. Create a Call Region

Call regions represent part of an organisation's network. Select **Network** → **Call Regions** in the left pane (not shown), click on **NEW** as shown below.



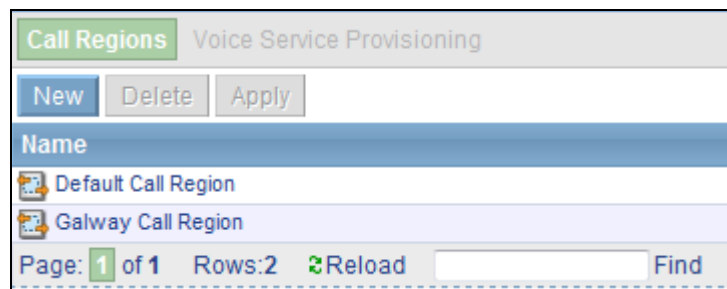
This screenshot shows the top portion of the 'Call Regions' configuration window. At the top are three buttons: 'New' (highlighted in blue), 'Delete', and 'Apply'. Below these is a header bar with the title 'Name'. Underneath is a table with one row containing a folder icon and the text 'Default Call Region'. At the bottom of this section is a status bar showing 'Page: 1 of 1', 'Rows: 1', a 'Reload' button with a circular arrow icon, a search input field, and a 'Find' button.

Enter an identifying **Name** for the new call region, leave the **Partition Checking** and **Priority for P2P** boxes unchecked, and press **OK**. As shown below.



This screenshot shows the 'New' dialog box for creating a call region. It has 'OK' and 'Cancel' buttons at the top. The 'Name' field is highlighted in blue. Below it is a table with one row containing a folder icon and the text 'Default Call Region'. The status bar shows 'Page: 1 of 1', 'Rows: 1', a 'Reload' button, a search input field, and a 'Find' button. Below the table are two tabs: 'General' (selected) and 'iCS'. In the 'General' tab, the 'Name' field contains 'Galway Call Region'. Below this are two checkboxes: 'Partition Checking' and 'Priority For P2P', both of which are unchecked.

The created call region will be visible in the list view as shown below.

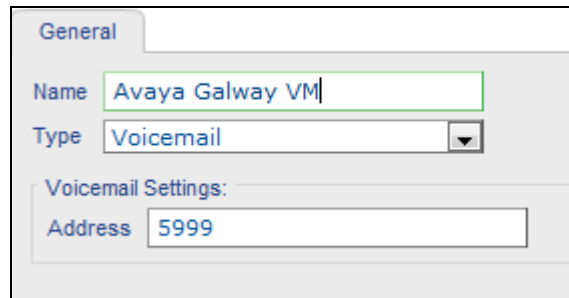


This screenshot shows the 'Call Regions' list view. At the top is a header bar with 'Call Regions' in a green box and 'Voice Service Provisioning' in a grey box. Below this are three buttons: 'New' (highlighted in blue), 'Delete', and 'Apply'. The 'Name' field is highlighted in blue. Below it is a table with two rows: the first row contains a folder icon and 'Default Call Region', and the second row contains a folder icon and 'Galway Call Region'. The status bar shows 'Page: 1 of 1', 'Rows: 2', a 'Reload' button, a search input field, and a 'Find' button.

**Note:** A default call region is available and can be used for a single site setup. Refer to the *Speakerbus iManager Administrator's Guide* for further configuration information.

## 7.5. Creating/Verifying User policies

Select **Users** → **Policies** in the left pane (not shown) and click on **NEW** (not shown). Enter an identifying **Name**, in the **Type** dropdown box select **Voicemail**, and enter a valid address for the voicemail server, in this case a pre-configured hunt group number for voicemail access is used. Click **OK** once completed, as seen below.



General

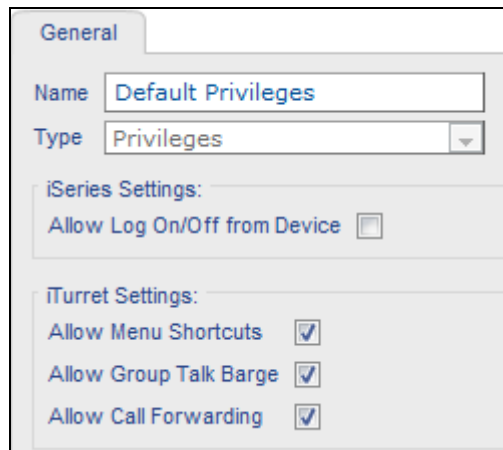
Name: Avaya Galway VM

Type: Voicemail

Voicemail Settings:

Address: 5999

Select **Users** → **Policies** in the left pane (not shown). Select and view the **Default Privileges** policy. (no changes should be needed to this, however it is referred to later in this document)



General

Name: Default Privileges

Type: Privileges

iSeries Settings:

Allow Log On/Off from Device ☒

iTurret Settings:

Allow Menu Shortcuts ☒

Allow Group Talk Barge ☒

Allow Call Forwarding ☒

Select **Users** → **Policies** in the left pane (not shown) Select the **Default Preferences** policy, click the **iTurret** tab and review the default settings. (no changes should be needed to this, but it's referred to later in this document)

The screenshot shows a configuration window with three tabs: General, iSeries, and iTurret. The iTurret tab is selected. Under the iTurret section, the following settings are visible: Dynamic Keys Call Display is set to 'All Calls' (dropdown); Speaker Activity Indication Timeout (ms) is set to '1500' (text field); LED Scheme is set to 'Scheme 1' (dropdown); Conferencing Mode is set to 'Standard' (dropdown); 'Always use Large Cisco Profile' is checked; and 'Log Intercom Calls in Call Register' is checked. Below the iTurret section, under the iE801 section, 'Mute Button Ganging' is checked and 'Group Button Ganging' is unchecked.

## 7.6. Creating/Verifying Device Policies

Select **Devices** → **Policies** in the left pane (not shown). Select and view the **Default RTP** policy. (no changes should be needed to this, however it is referred to later in this document)

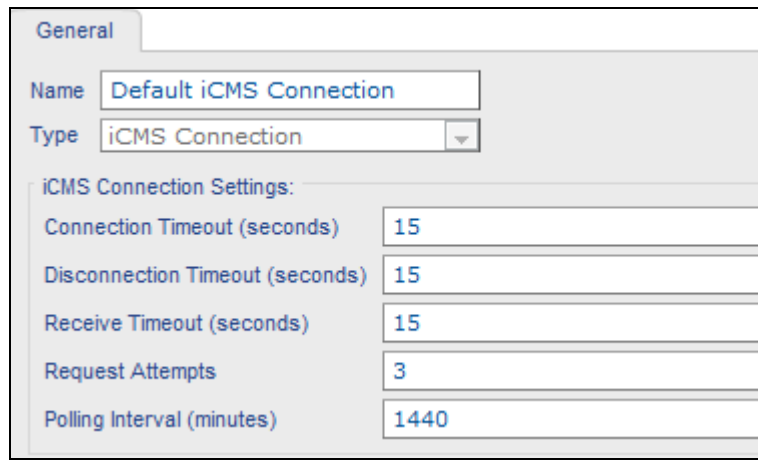
The screenshot shows a configuration window for a policy named 'Default RTP'. The 'General' tab is selected. The 'Name' field contains 'Default RTP' and the 'Type' dropdown is set to 'RTP Media'. Under 'RTP Media Settings', 'Time To Live' is 120, 'DSCP Value' is 0, and 'RTCP DSCP Value' is 0. Under 'SIP RTP Media Settings', 'Preferred Codec' is 'G.711 A-Law', 'Preferred ID712 Codec' is 'G.711 A-Law', and 'Voice Activity Detection' is unchecked.

Select **Devices** → **Policies** in the left pane. Select and view the **Default SbRTP** policy. (no changes should be needed to this, however it is referred to later in this document)

The screenshot shows a configuration window for the 'Default SbRTP' policy. The window has a 'General' tab selected. The 'Name' field is 'Default SbRTP' and the 'Type' is 'SbRTP Media'. Below this, the 'SbRTP Media Settings' section contains the following fields:

Setting	Value
RTP Payload Code	96
Time To Live	1
DSCP Value	0
Bandwidth	Standard
Packet Size	4 ms
Voice Activity Detection	<input checked="" type="checkbox"/>
Lost Packet Tolerance (%)	50
Sample Slip Tolerance (%)	100
iSeries Compatibility	Version 3.0

Select **Devices** → **Policies** in the left pane (not shown). Select and view the **Default iCMS Connection** policy. (no changes should be needed to this, however it is referred to later in this document)

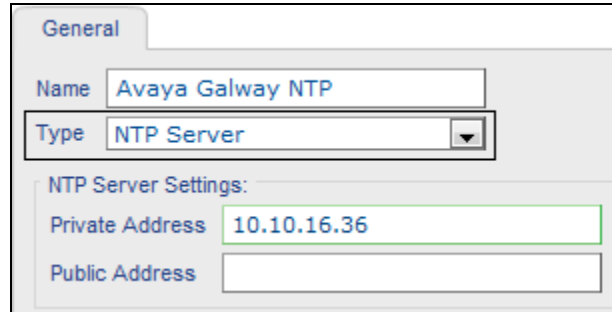


The screenshot shows a configuration window for a policy named "Default iCMS Connection". The "Type" is set to "iCMS Connection". Under the "iCMS Connection Settings" section, the following values are entered: Connection Timeout (seconds) is 15, Disconnection Timeout (seconds) is 15, Receive Timeout (seconds) is 15, Request Attempts is 3, and Polling Interval (minutes) is 1440.

iCMS Connection Settings:	
Connection Timeout (seconds)	15
Disconnection Timeout (seconds)	15
Receive Timeout (seconds)	15
Request Attempts	3
Polling Interval (minutes)	1440

## 7.7. Create Network Services

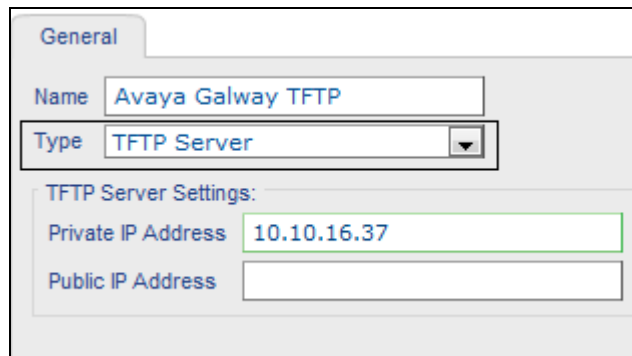
Create records for the NTP and TFTP servers from the Network Services. Select **Network** → **Network Services** in the left pane (not shown), click on **NEW**, enter a descriptive **Name**, in the **Type** dropdown list select **NTP Server** and enter a valid address for an NTP server if available. Press **OK** once completed, as shown below.



The screenshot shows a configuration window for a policy named "Avaya Galway NTP". The "Type" is set to "NTP Server". Under the "NTP Server Settings" section, the "Private Address" is entered as "10.10.16.36" and the "Public Address" field is empty.

NTP Server Settings:	
Private Address	10.10.16.36
Public Address	

Select **Network** → **Network Services** in the left pane, click on **NEW**, enter a descriptive **Name**, in the **Type** dropdown list select **TFTP Server**, and enter a valid address for a TFTP server if available. Press **OK** once completed, as shown below.



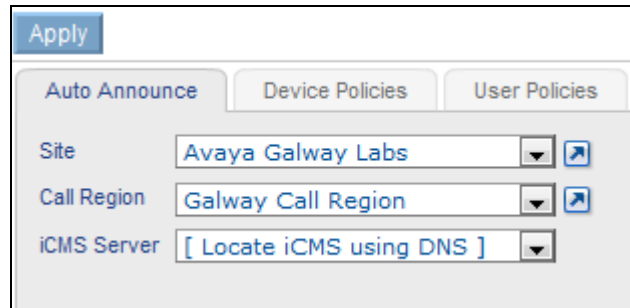
The image shows a configuration window for a TFTP Server. It has a 'General' tab selected. The 'Name' field contains 'Avaya Galway TFTP'. The 'Type' dropdown menu is set to 'TFTP Server'. Below these, there is a section titled 'TFTP Server Settings:' which includes a 'Private IP Address' field with the value '10.10.16.37' and an empty 'Public IP Address' field.

General	
Name	Avaya Galway TFTP
Type	TFTP Server
TFTP Server Settings:	
Private IP Address	10.10.16.37
Public IP Address	



## 7.8. Confirm Defaults

Select **System** → **Defaults** in the left pane (not shown), under the **Auto Announce** tab select the **Site** and **Call Region** created above and confirm that **iCMS Server** is set to **[Locate iCMS using DNS]**. Click **Apply** when completed as shown below:



**Note:** DNS and DHCP must be set up in accordance with the Speakerbus administrator's guide. Refer to the *Speakerbus iManager Administrator's Guide* for further configuration information

## 7.9. Create iTurret Deskstations

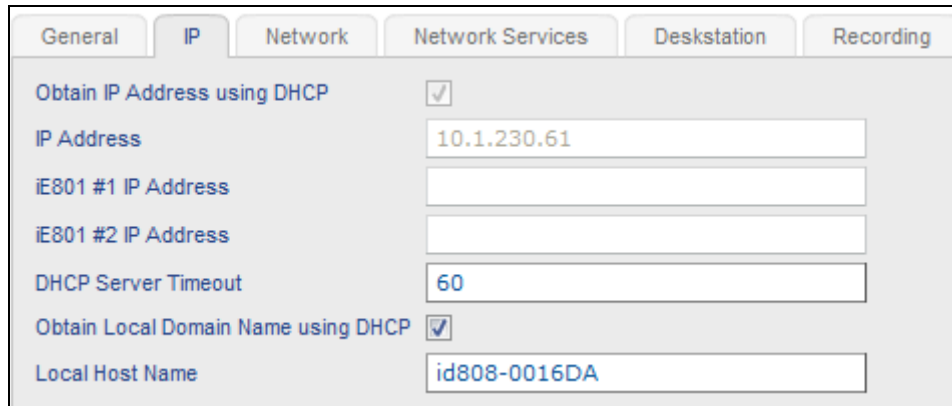
The iTurret deskstations will automatically register to the iCMS server if appropriate **DHCP** and **DNS** records were created prior to the iTurret deskstations being connected to the IP network. To view the newly registered deskstations, select **Devices** → **Deskstations** in the left pane (not shown), confirm they are seen as follows:

Deskstations Channels Connections									
New Delete Apply Seat... Unseat Synchronise Firmware... Logs... Diagnostics... Move... Feature Keys...									
Site Avaya Galway Labs Call Region [ All ] Type [ All ] Status [ All ]									
Name	Site	Call Region	Type	IP Address	MAC Address	Firmware	Seated User	Status	
Id808-001500	Avaya Galway Labs	Galway Call Region	iTurret	10.10.16.50	00:05:83:00:15:00	2.100.7.0			
Id808-001501	Avaya Galway Labs	Galway Call Region	iTurret	10.10.16.51	00:05:83:00:15:01	2.100.7.0			
Id808-001502	Avaya Galway Labs	Galway Call Region	iTurret	10.10.16.52	00:05:83:00:15:02	2.100.7.0			
Page: 1 of 1 Rows: 6 Reload Find									
General									

Select the iTurret deskstation and under the **General** tab enter an identifying **Name**.

General	IP	Network	Network Services	Deskstation	Recording
Name	Turret A				
Type	iTurret				
MAC Address	00:05:83:00:15:00				
Site	Avaya Galway Labs				
Call Region	Galway Call Region				
Firmware Version					
Location					

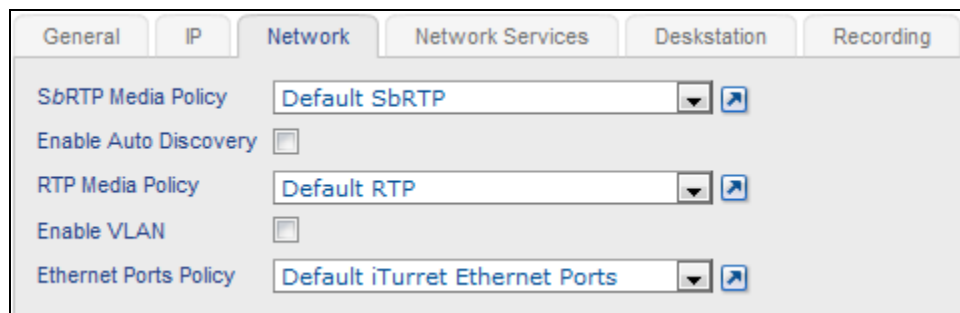
Click the **IP** tab, verify that the **Obtain IP Address using DHCP** and the **Obtain Local Domain Name using DHCP** tick boxes are checked



The screenshot shows the 'IP' tab selected in a settings window. The 'Obtain IP Address using DHCP' checkbox is checked, and the 'IP Address' field contains '10.1.230.61'. The 'Obtain Local Domain Name using DHCP' checkbox is also checked, and the 'Local Host Name' field contains 'id808-0016DA'. Other fields like 'iE801 #1 IP Address', 'iE801 #2 IP Address', and 'DHCP Server Timeout' are present but empty or set to a default value of 60.

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

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



The screenshot shows the 'Network' tab selected. The 'SbRTP Media Policy' is set to 'Default SbRTP', 'RTP Media Policy' is set to 'Default RTP', and 'Ethernet Ports Policy' is set to 'Default iTurret Ethernet Ports'. The 'Enable Auto Discovery' and 'Enable VLAN' checkboxes are unchecked.

In the **Network Services** tab, verify or configure the following:

- **iCMS Server** shows **[Locate iCMS using DNS]**
- **iCMS Connection Policy** shows **Default iCMS Connection**
- **NTP Server**, select the newly created NTP server network service configured above
- **Diagnostics Server**, select the newly created TFTP server network service configured above

The screenshot shows the 'Network Services' tab in a configuration interface. It contains several settings: 'iCMS Server' is set to '[ Locate iCMS using DNS ]'; 'iCMS Connection Policy' is set to 'Default iCMS Connection'; 'SNMP Manager' is set to '[ None ]'; 'NTP Server' is set to 'Avaya Galway NTP (10.10.16.36)'; 'Backup NTP Server' is set to '[ None ]'; and 'Diagnostic Server' is set to 'Avaya Galway TFTP (10.10.16.37)'. Each setting has a dropdown menu and a small icon to its right.

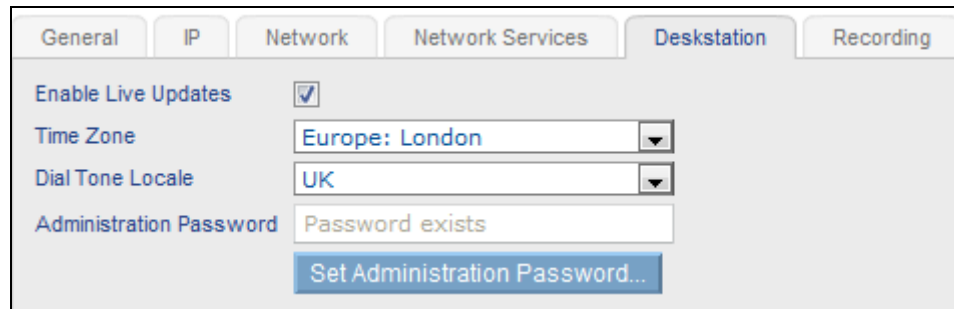
In the **Deskstation** tab ensure that **Enable Live Update** is checked and **Time Zone** and **Dial Tone Locale** are changed to the required setting. Click on **Set Administration Password**.

The screenshot shows the 'Deskstation' tab in a configuration interface. It contains several settings: 'Enable Live Updates' is checked with a checkbox; 'Time Zone' is set to 'Europe: London'; 'Dial Tone Locale' is set to 'UK'; and 'Administration Password' is set to 'No password set'. There is a 'Set Administration Password...' button below the password field.

Enter a valid password and press **OK**.

The screenshot shows a 'Set Administration Password' dialog box. It contains three input fields: 'Device Name' (set to 'Turret A'), 'New Password', and 'Verify Password'. There are 'OK' and 'Cancel' buttons at the bottom.

The Deskstation tab contents now displays the following:

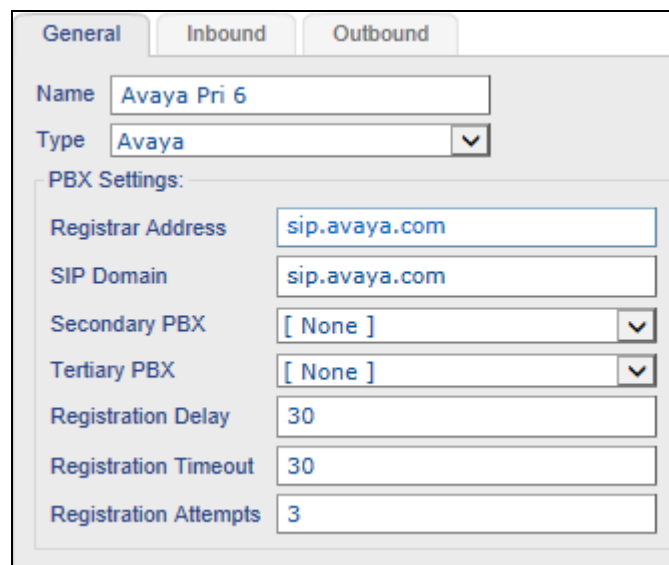


The screenshot shows the 'Deskstation' tab selected among 'General', 'IP', 'Network', 'Network Services', 'Deskstation', and 'Recording'. The 'Enable Live Updates' checkbox is checked. The 'Time Zone' dropdown is set to 'Europe: London'. The 'Dial Tone Locale' dropdown is set to 'UK'. The 'Administration Password' field contains the text 'Password exists'. Below this field is a button labeled 'Set Administration Password...'.

## 7.10. Create PBX (SIP Server)

To create a PBX, select **Call Servers → PBXs**, click **NEW** (not shown) and complete the following fields:

- Provide a descriptive **Name** for the SIP/PBX server
- Select **Avaya** from the **Type** dropdown box
- In the **Registrar Address** and **SIP Domain** fields set to a FQDN address and domain respectively if using DNS to resolve the Session Manager active IP address
- After the PBX is created, the **Port** field will be displayed on this page with the default value of 5060



The screenshot shows the 'PBX Settings' form with tabs for 'General', 'Inbound', and 'Outbound'. The 'Name' field is 'Avaya Pri 6'. The 'Type' dropdown is set to 'Avaya'. The 'PBX Settings' section includes: 'Registrar Address' (sip.avaya.com), 'SIP Domain' (sip.avaya.com), 'Secondary PBX' ([ None ]), 'Tertiary PBX' ([ None ]), 'Registration Delay' (30), 'Registration Timeout' (30), and 'Registration Attempts' (3).

**Note 1:** A server locator record (SRV) for the registrar address and SIP domain must be created on DNS. Refer to the *Speakerbus iManager Administrator's Guide* for the correct configuration of DNS

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

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

## 7.11. Create Dial Plan

To create a PBX specific dial plan, select **Call Servers → PBXs** (not shown), select the **Dial Plan** tab, click **NEW** and then fill in the **Dial Rule**. Press **OK** when completed.

The screenshot shows a web-based configuration interface for a PBX. At the top, there are two tabs: 'PBXs' and 'Dial Plan', with 'Dial Plan' being the active tab. Below the tabs are 'OK' and 'Cancel' buttons. The main content area is titled 'Dial Rule' and contains a table with one row. The table has a 'Dial Rule' column with the value '6XXX'. Below the table is a 'General' tab and a 'Dial Rule' label with a text input field containing '6XXX'.

Repeat this for all valid extension formats.

## 7.12. Create Call and Handset Appearances

Three call appearances must be created for each iTurret device. One is for the main appearance, and one for each of the privacy appearances (handset 1 and handset 2). As previously explained, three extensions are configured in System Manager for this purpose.

To create the main appearance, click **Call Servers → PBX Appearances** in the left pane, click on **NEW**, select the PBX created in **Section 7.10** (in this case **Avaya Pri 6**), then select the **Type** of appearance to be created (**Call** in this case) (not shown) and configure as follows under the **General** tab:

- Provide a descriptive name for the appearance in the **Name** field, such as the extension or user's name.
- Set the **Long Label** field to the label that will be displayed for the call appearance button on the iTurret deskstation. The **Address** field should also be set to the appearance extension.
- Set the **Maximum Appearance** field to the number of call appearances configured on the station in System Manager (the number of call appearance buttons dictates the number of calls on the system the user can have directed to them). When all of the call appearances are not idle the user is considered busy and no further calls can be routed to them. Up to a maximum of 10 call appearances may be configured on Communication Manager for each iTurret deskstation.
- Check the **Message Indication** checkbox for voice mail purposes and the **Allow Outbound Calls**.
- The **Authentication Name** and **Authentication Password** fields should be set to the extension and password configured on System Manager in **Section 6.2**. These are the credentials that the iTurret deskstation will use to authenticate and register with Session Manager. Use the default values for the other fields. Click **OK**.

The screenshot shows the 'General' tab of a configuration window. At the top, there's a 'PBX' dropdown menu set to 'Avaya Pri 6' and a 'Type' dropdown menu set to 'Call'. Below these is a section titled 'Call Appearance Settings:'. It contains several fields: 'Name' (Avaya 6031), 'Long Label' (Avaya 6031), 'Address' (6031), 'Maximum PBX Appearances' (4), 'Allow Outbound Calls' (checked), 'Message Indication' (checked), and 'Authentication Name' (6031). At the bottom of this section is a button labeled 'Set Authentication Password...'.

Repeat the procedure for the two corresponding privacy appearances. Click the **New** button to add another appearance. In the **General** tab select the **PBX** created in **Section 7.10**, set the **Type** field to **Privacy 1** and complete the **Address**, **Authentication Name** and **Authentication Password** fields. The last two fields should be identical to the setup in System Manager for registration to occur. Press **OK** to commit the created appearance.

**General**

PBX: Avaya Pri 6

Type: Privacy 1

**Privacy Appearance Settings:**

Address: 6041

Authentication Name: 6041

Authentication Password: [masked]

Verify Password: [masked]

Repeat the above procedure to add the Privacy 2 appearance.

**General**

PBX: Avaya Pri 6

Type: Privacy 2

**Privacy Appearance Settings:**

Name: Test User Aura 1 PV2

Long Label: Test User Aura 1 PV2

Address: 6051

Authentication Name: 6051

Set Authentication Password...

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

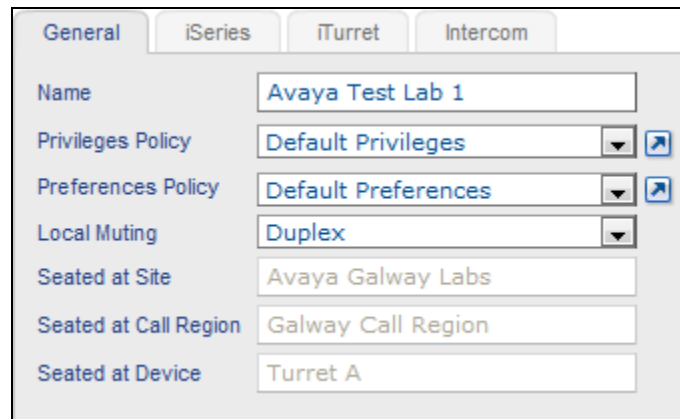
PBX Appearances					
User Permissions Group Permissions					
New Delete Apply Assign Ownership... Clear Ownership					
PBX: Avaya Pri 6 Type: [ All ]					
Name	PBX	Long Label	Address	Type	Owner
Avaya 6031	Avaya Pri 6	Avaya 6031	6031	Call	Test User Aura 1
Avaya 6032	Avaya Pri 6	Avaya 6032	6032	Call	Test User Aura 2
Avaya 6033	Avaya Pri 6	Avaya 6033	6033	Call	Test User Aura 3
Test User Aura 1 PV1	Avaya Pri 6	Test User Aura 1 PV1	6041	Privacy 1	Test User Aura 1
Test User Aura 1 PV2	Avaya Pri 6	Test User Aura 1 PV2	6051	Privacy 2	Test User Aura 1

Page: 1 of 1 Rows: 5 Reload Find



### 7.13. Create Users

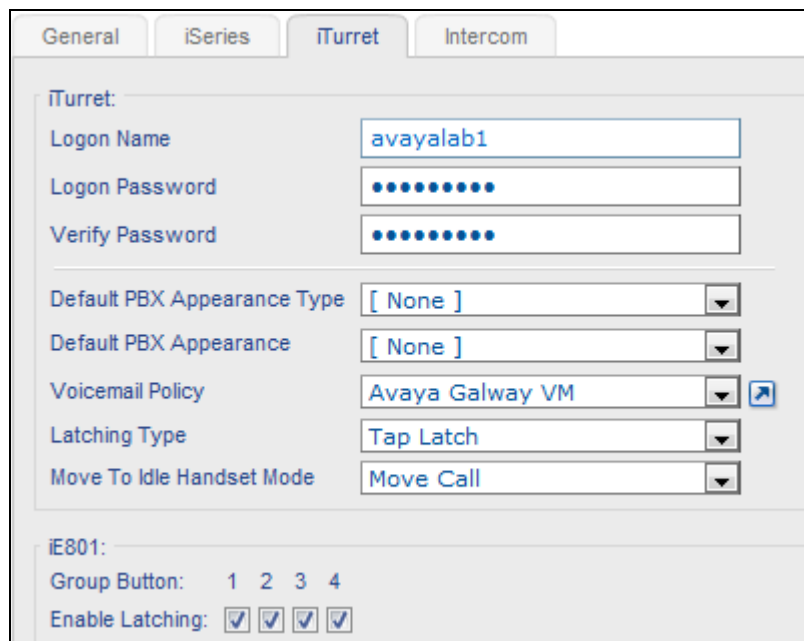
Select **Users** → **Users** in the left pane, click on **NEW**, within the **General** tab fill in a descriptive **name** for the user, leave the **privilege** and **preference policies** at the defaults along with **local muting**:



The screenshot shows the 'General' tab of a user configuration window. The tabs at the top are 'General', 'iSeries', 'iTurret', and 'Intercom'. The 'General' tab is active. The fields are as follows:

Field	Value
Name	Avaya Test Lab 1
Privileges Policy	Default Privileges
Preferences Policy	Default Preferences
Local Muting	Duplex
Seated at Site	Avaya Galway Labs
Seated at Call Region	Galway Call Region
Seated at Device	Turret A

Within the **iTurret** tab, provide the **logon** credentials for the user to log into their iTurret deskstation and assign the **Voicemail Policy** set up in **Section 7.5**.



The screenshot shows the 'iTurret' tab of the user configuration window. The tabs at the top are 'General', 'iSeries', 'iTurret', and 'Intercom'. The 'iTurret' tab is active. The fields are as follows:

Field	Value
iTurret:	
Logon Name	avayalab1
Logon Password	••••••••
Verify Password	••••••••
Default PBX Appearance Type	[ None ]
Default PBX Appearance	[ None ]
Voicemail Policy	Avaya Galway VM
Latching Type	Tap Latch
Move To Idle Handset Mode	Move Call
IE801:	
Group Button:	1 2 3 4
Enable Latching:	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

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

Repeat the previous steps to add more users.

The screenshot shows the 'Users' management interface. At the top, there are tabs for 'Users', 'Group Memberships', 'Voice Services', 'PBX Appearances', 'Alerts', 'Personal Dir.', and 'iTurret Layout'. Below the tabs are buttons: 'New', 'Delete', 'Apply', 'Seat...', 'Unseat', 'New Users...', 'Apply Template...', 'New Template...', and 'Synchronise'. A filter bar shows 'Group [ All ]', 'Partition [ All ]', 'Site [ All ]', and 'Call Region [ All ]'. The main table lists users with columns: Name, iSeries Logon, iTurret Logon, Intercom Logon, Dial Number, and Seated Device. The table contains three rows for 'Avaya Test Lab 1', 'Avaya Test Lab 2', and 'Avaya Test Lab 3'. The 'iTurret Logon' column shows 'avayalab1', 'avayalab2', and 'avayalab3' respectively. At the bottom, it says 'Page: 1 of 1 Rows: 3 Reload Find'.

Name	iSeries Logon	iTurret Logon	Intercom Logon	Dial Number	Seated Device
Avaya Test Lab 1		avayalab1			
Avaya Test Lab 2		avayalab2			
Avaya Test Lab 3		avayalab3			

After a user has been created, that user can then be seated on an iTurret deskstation. Select the user to be seated and click **Seat** from the bar as shown below.

The screenshot shows the 'Users' management interface with the 'Seat...' button highlighted. The table below shows only 'Avaya Test Lab 1' with 'iTurret Logon' 'avayalab1'. Below the table, there are tabs for 'General', 'iSeries', 'iTurret', and 'Intercom'. The 'General' tab is active, showing fields for 'Name' (Avaya Test Lab 1), 'Privileges Policy' (Default Privileges), 'Preferences Policy' (Default Preferences), 'Local Muting' (Duplex), and 'Seated at Device' (User not seated).

Name	iSeries Logon	iTurret Logon
Avaya Test Lab 1		avayalab1

On the next page, filter options are presented. Filter for **iTurret** deskstations in the site configured in **Section 7.3** and the region configured in **Section 7.4** and place a tick in the **Show only free deskstations** check box. Select the appropriate iTurret device from the **Device to seat at** drop down box and click **OK**.

The screenshot shows the 'Seat User at Device' dialog box. It contains the following fields and options: 'User to seat' (Avaya Test Lab 1), 'Filter by Site' (Avaya Galway Labs), 'Filter by Region' (Galway Call Region), 'Filter by Device Type' (iTurret), 'Show only free deskstations' (checked), and 'Device to seat at' (Turret A). There are 'OK' and 'Cancel' buttons at the bottom.

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

Users							Group Memberships		Voice Services		PBX Appearances		Alerts		Personal Dir.		iTurret Layout	
New		Delete		Apply		Seat...		Unseat		New Users...		Apply Template...		New Template...		Synchronise		
Group		[ All ]		Partition		[ All ]		Site		Avaya Galway Labs		Call Region		[ All ]				
Name							iSeries Logon		iTurret Logon		Intercom Logon		Dial Number		Seated Device			
👤 Avaya Test Lab 1									avayalab1						👤 Turret A			
👤 Avaya Test Lab 2									avayalab2						👤 Turret B			
👤 Avaya Test Lab 3									avayalab3						👤 Turret C			
Page:		1 of 1		Rows:		3		🔄Reload				Find						

## 7.14. Assign User Permissions

Appearance permissions must be assigned to the created users. Select **Call Servers → PBX Appearances** in the left pane (not shown), select the **Call Appearance** from the list, and select the **User Permissions** tab at the top of the page:

PBX Appearances

User Permissions

Group Permissions

New

Delete

Apply



Assign Ownership...

Clear Ownership

PBX


Avaya Pri 6

Type [ All ]

Name	PBX	Long Label	Address	Type	Owner
 Avaya 6031	Avaya Pri 6	Avaya 6031	6031	Call	

Page: 1 of 1

Rows: 5

 Reload

Find

Select the user to give permissions to and select **Allow** from the **Permissions** dropdown box.

PBX Appearances User Permissions Group Permissions			
Apply			
Group [ All ] Partition [ All ] Site [ All ] Call Region [ All ] Type [ All ]			
Name	User Permission	Group Permission	Seated Site
Avaya Test Lab 1	Use group	Deny	
General			
Permission Allow			

## 7.15. Assign Ownership

Appearance ownership must be assigned to a user as it enables the iTurret to distinguish between the owner of the call or appearance as opposed to someone who is bridged on to that appearance. Select **Call Servers** → **PBX Appearances** in the left pane, select the **Call Appearance** from the list, and select the **Assign Ownership** button:

Name	PBX	Long Label	Address	Type	Owner
Avaya 6031	Avaya Pri 6	Avaya 6031	6031	Call	

General

PBX: Avaya Pri 6  
Type: Call

Call Appearance Settings:

Name: Avaya 6031  
Long Label: Avaya 6031  
Address: 6031  
Maximum PBX Appearances: 2  
Allow Outbound Calls: ☒  
Message Indication: ☒  
Authentication Name: 6031  
Set Authentication Password

The following screen will appear allowing filtering of users. Filter accordingly and select the user from the **User to assign ownership to** dropdown box. Click **OK**.

Assign Ownership of PBX Appearance(s)

Filter by Seated Site: Avaya Galway Labs  
Filter by Seated Region: Galway Call Region  
Filter by User Group: [ All ]  
Filter by Partition: [ All ]  
User to assign ownership to: Avaya Test Lab 1  
OK Cancel

Repeat the process in both **Section 7.14** and this Section and to assign Privacy 1 and Privacy 2 call appearances to the user.

Name	PBX	Long Label	Address	Type	Owner
Avaya 6031	Avaya Pri 6	Avaya 6031	6031	Call	Avaya Test Lab 1

General

## 7.16. Assign Default Call Appearance

Select **Users** → **Users** in the left pane (not shown), select the user to add a default call appearance to (not shown), and select the **iTurret** tab (as seen below):

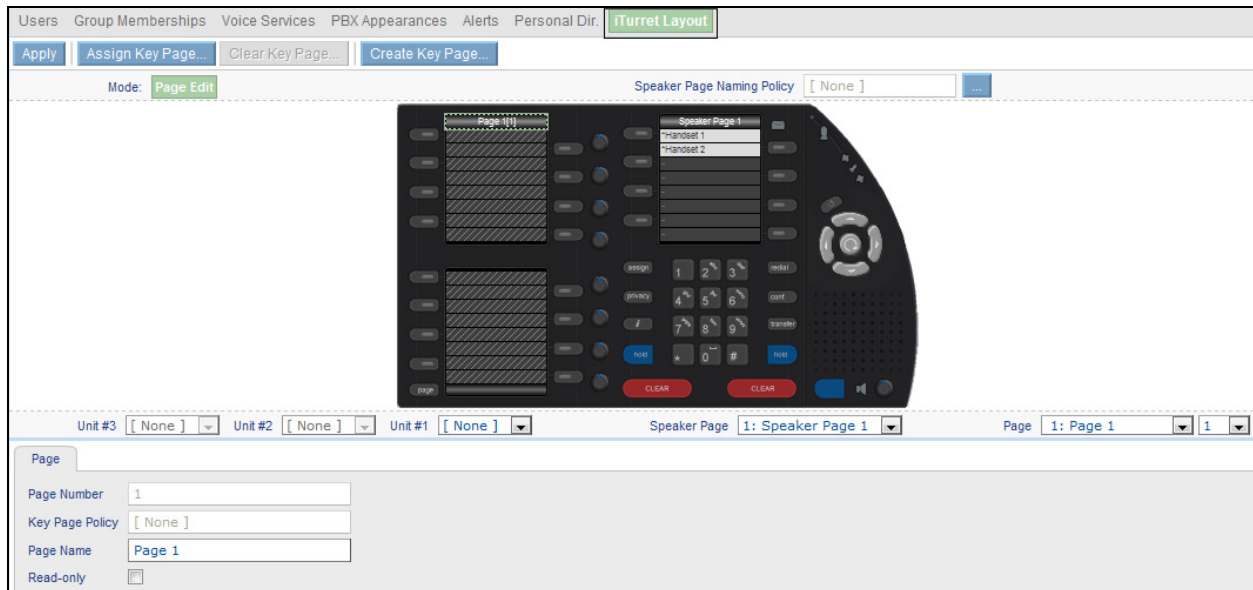
The image shows the 'iTurret' configuration tab in a software interface. It has four tabs: 'General', 'iSeries', 'iTurret' (selected), and 'Intercom'. Under the 'iTurret' section, there are fields for 'Logon Name' (avayalab1), 'Logon Password' (masked with dots), and 'Verify Password' (masked with dots). Below these are several dropdown menus: 'Default PBX Appearance Type' (set to '[ None ]'), 'Default PBX Appearance' (set to '[ None ]'), 'Voicemail Policy' (set to 'Avaya Galway VM'), 'Latching Type' (set to 'Tap Latch'), and 'Move To Idle Handset Mode' (set to 'Move Call'). At the bottom, there is a section for 'iE801' with 'Group Button' (1 2 3 4) and 'Enable Latching' (four checked checkboxes).

Set the **Default PBX Appearance Type** field to **Call** and then set the **Default PBX Appearance** field to the main call appearance (e.g. **6031**), Click **Apply**.

The image shows the 'iTurret' configuration tab with updated settings. The 'Logon Name' is still 'avayalab1', but there is now a 'Change Password...' button next to it. The 'Default PBX Appearance Type' dropdown is now set to 'Call'. The 'Default PBX Appearance' dropdown is set to 'Avaya 6031'. The 'Voicemail Policy' dropdown is set to 'Avaya 6'. The 'Latching Type' is still 'Tap Latch' and 'Move To Idle Handset Mode' is still 'Move Call'. The 'iE801' section at the bottom remains the same with 'Group Button' (1 2 3 4) and 'Enable Latching' (four checked checkboxes).

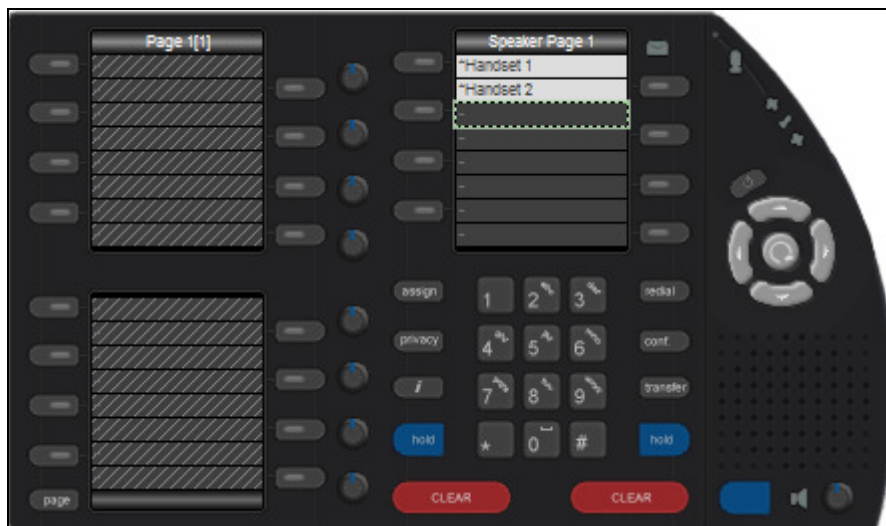
## 7.17. Program iTurret Deskstations

This section describes how to create iTurret deskstation keys. In this configuration, each user will be configured with two Dynamic keys, two Soft Function keys, one function (DND) key and one Shortcut key. Select **Users** → **Users** in the left pane (not shown), select the user to be updated (not shown), then select the **iTurret Layout** tab as shown below:

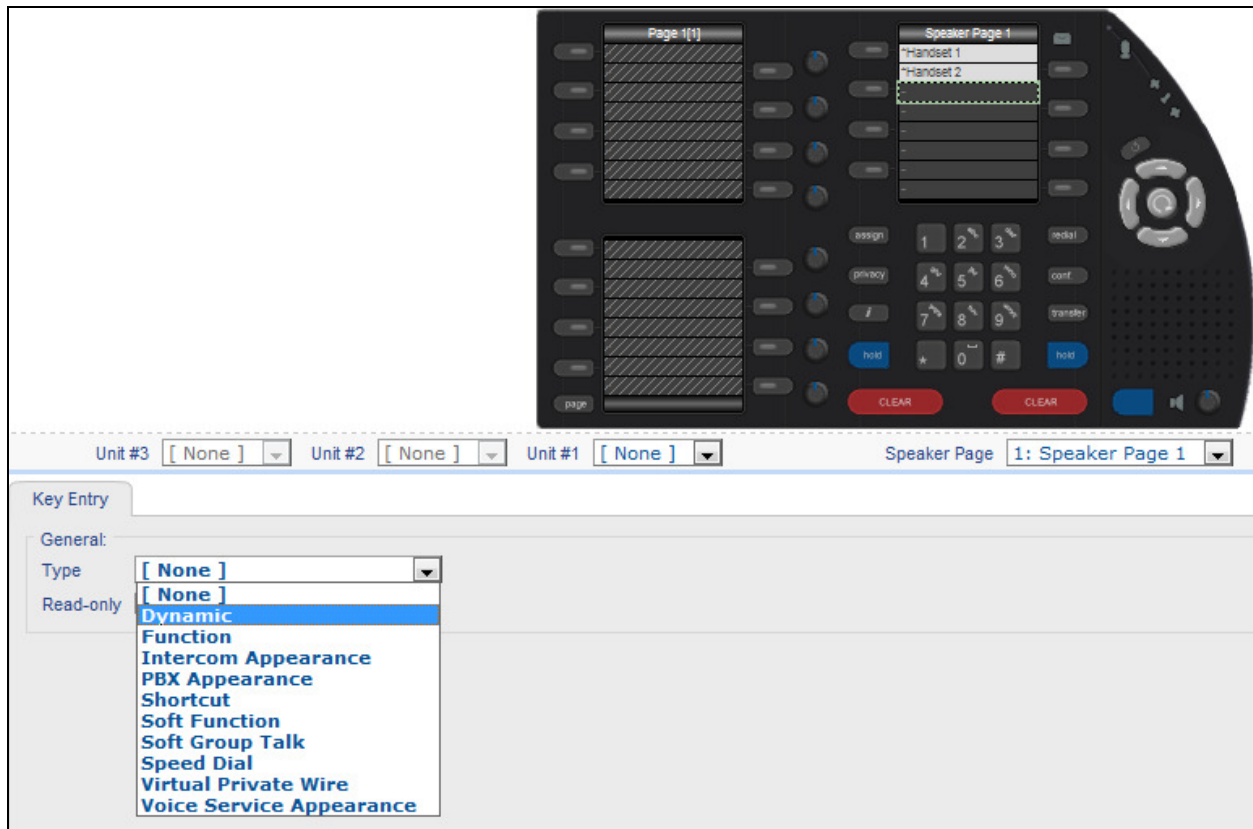


Create two dynamic keys (one after the other) under Handset 2.

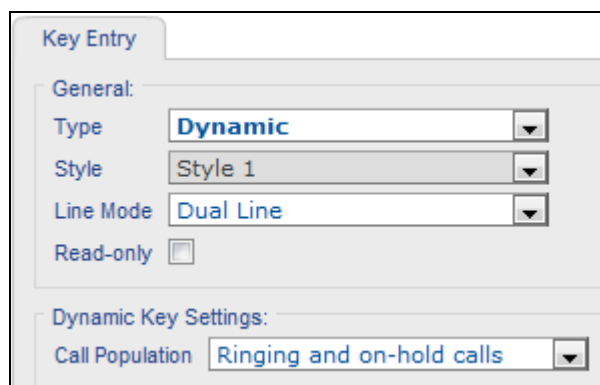
To add the first dynamic key, select the next available fixed key below Handset 2 as seen below:



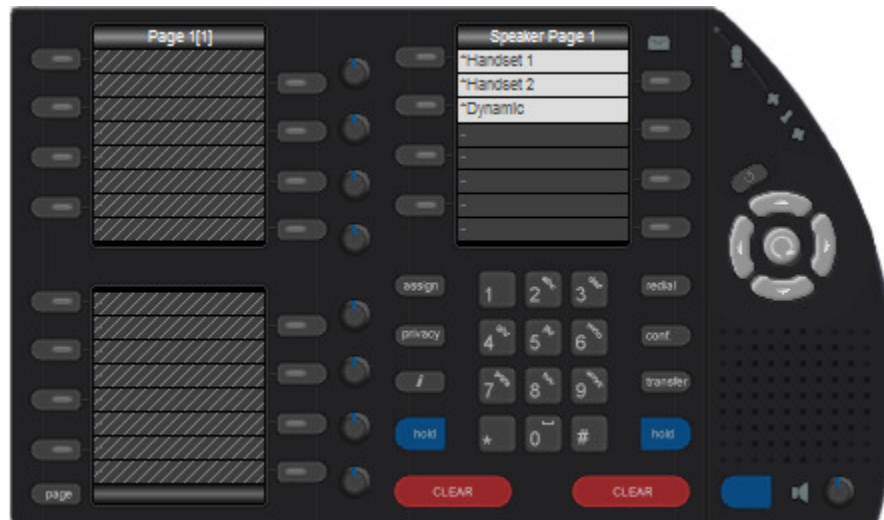
In the **Key Entry** tab, select **Dynamic** from the **Type** field, as seen below:



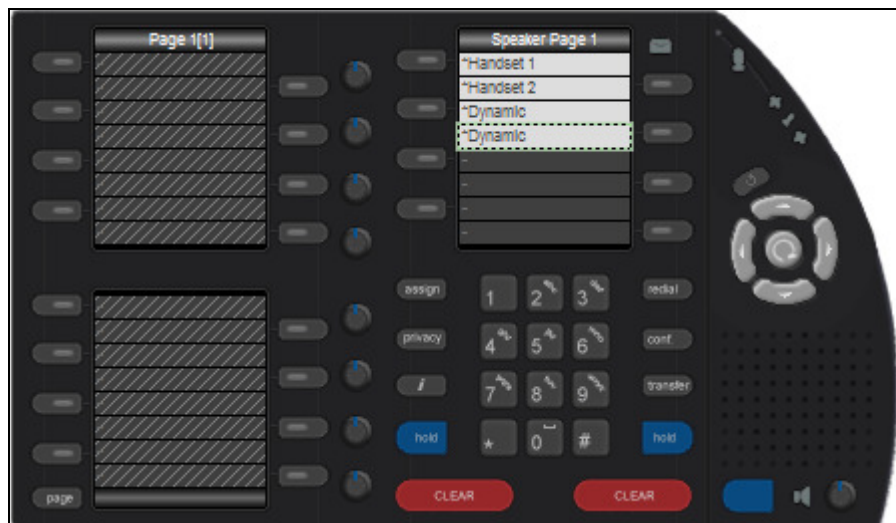
Leave the **Call Population** field at the default **Ringling and on-hold calls**. Click **OK**.



The iTurret layout looks as follows with the first dynamic key assigned:



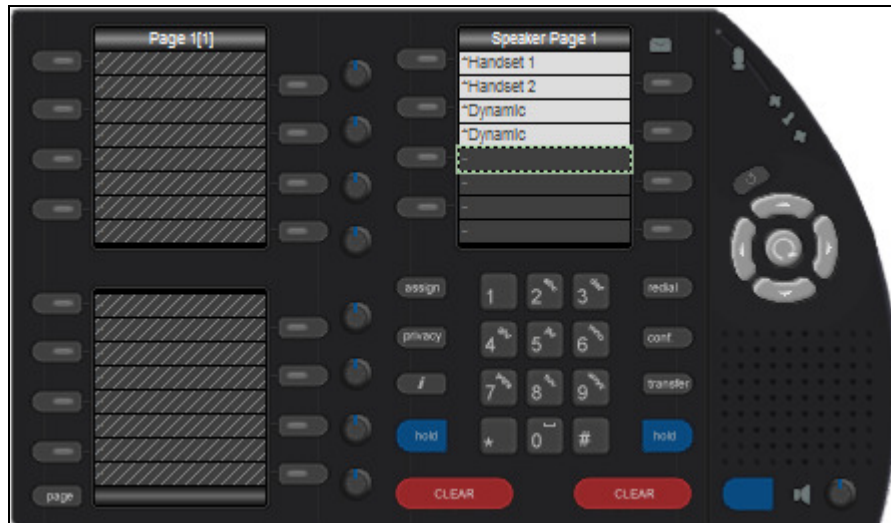
Now add the second dynamic key under the first by following the steps above, once completed the iTurret layout will look as follows:



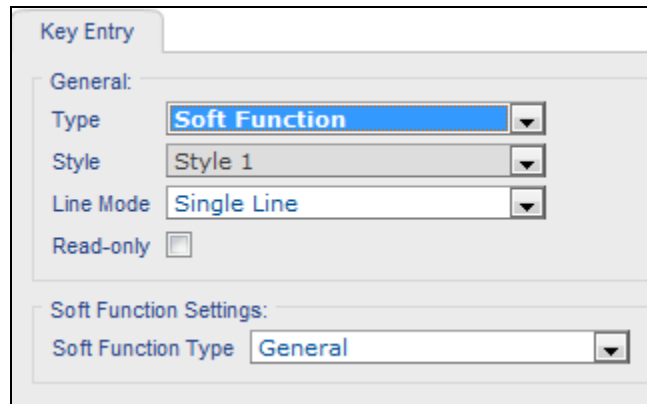
**NOTE:** The **Call Population** field can be set up for different key assignments, which are “Ringing and on-hold calls”, “Ringing calls only”, “On-hold calls only”, “Busy-elsewhere calls only” and “Busy-elsewhere and on-hold calls”. The default is “Ringing and on-hold calls”, but any combination of these can be used depending on the user requirement.



To add the first soft function key, select the next available fixed key as seen below:



Leave the **Soft Function Type** field at the default **General**. Click **OK** (not shown)



Key Entry

General:

Type: **Soft Function**

Style: **Style 1**

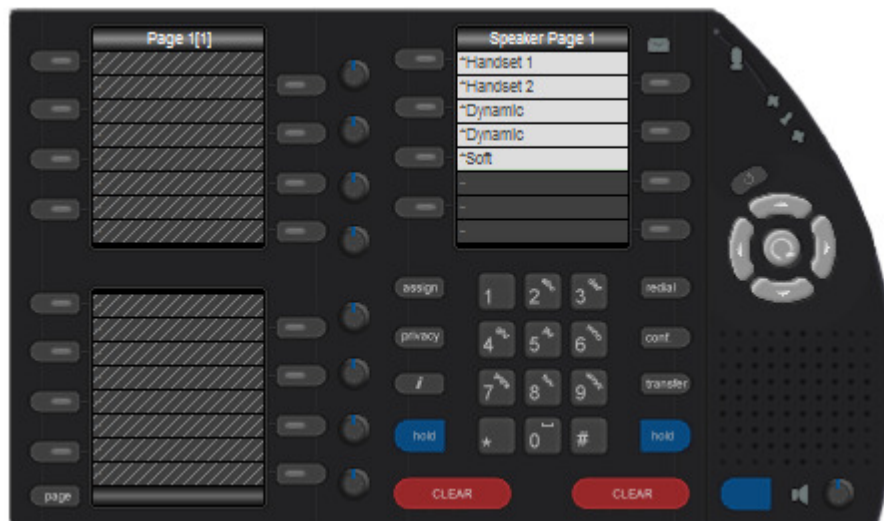
Line Mode: **Single Line**

Read-only: ☐

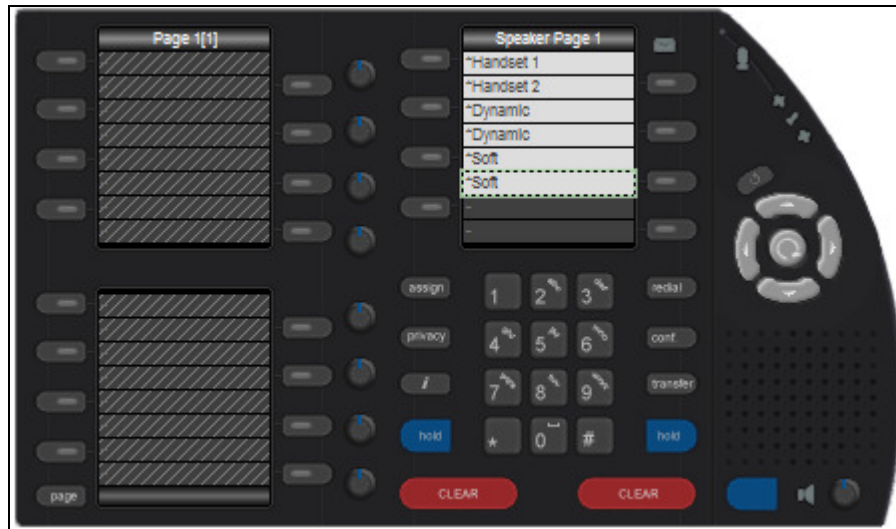
Soft Function Settings:

Soft Function Type: **General**

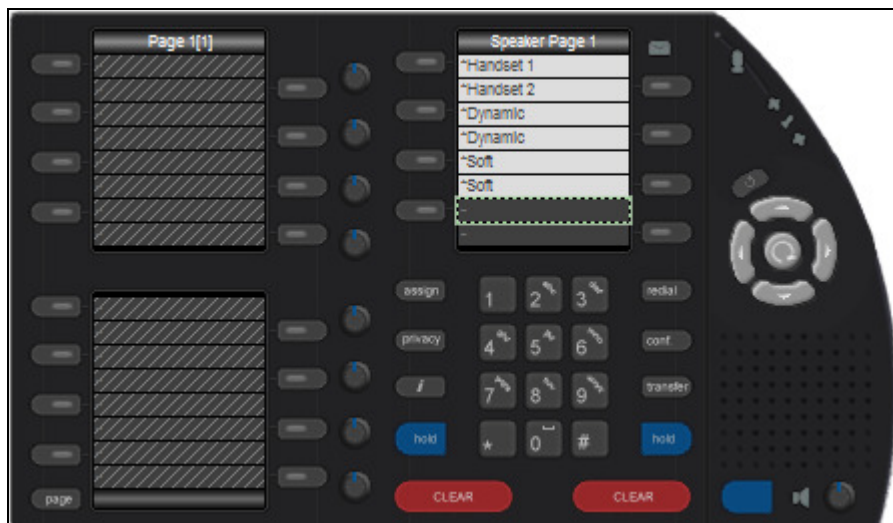
The iTurret layout looks as follows with the first soft function key assigned:



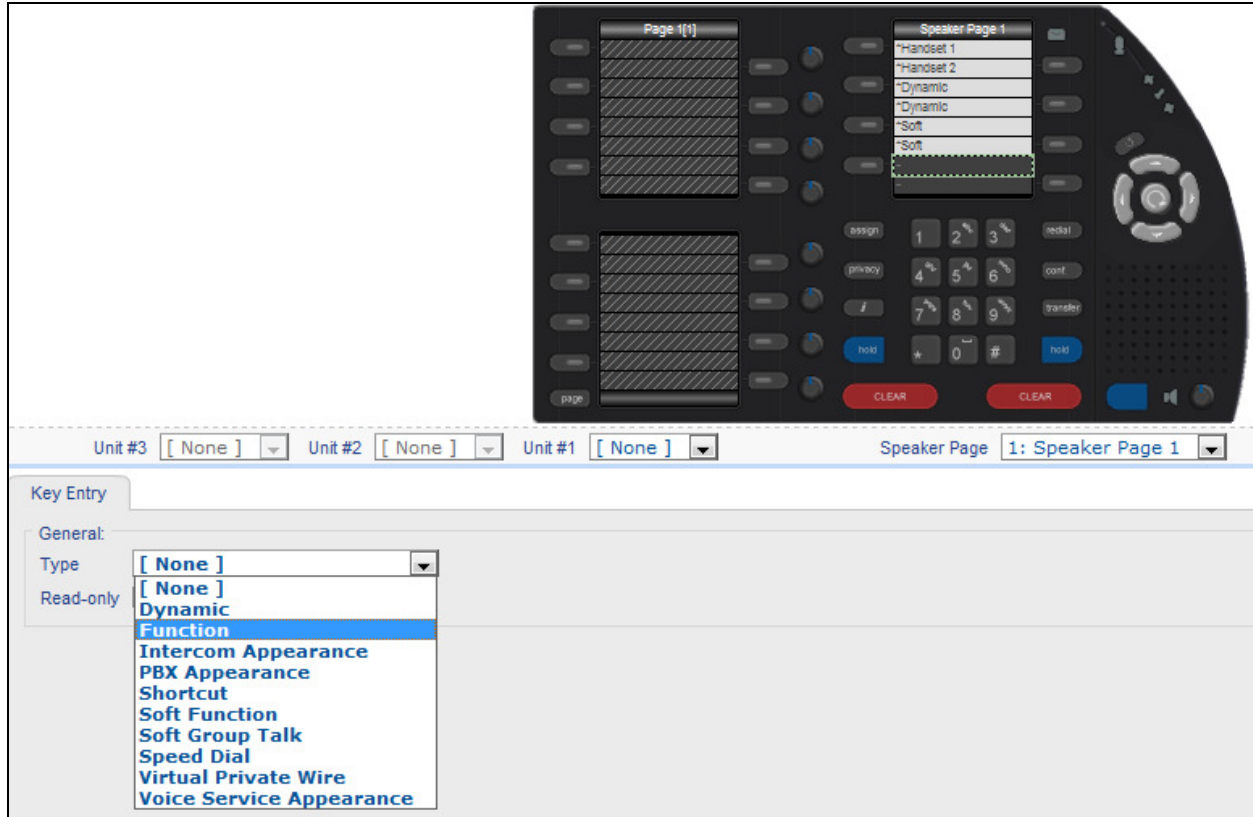
Now add the second soft function key under the first by following the steps above, once completed the iTurret layout will look as follows:



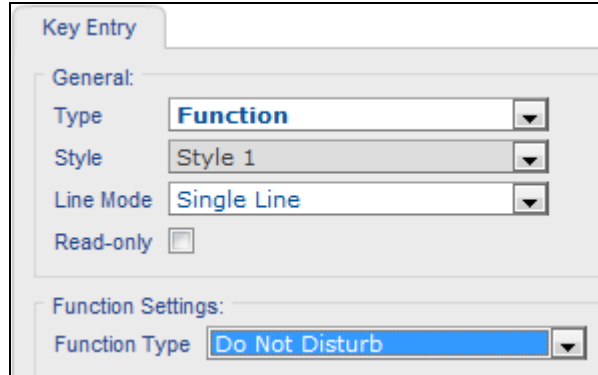
To create a function (Do Not Disturb (DND)) key, select the next available fixed key under the last soft function key, as seen below:



In the Key Entry tab, set **Function** in the **Type** field.

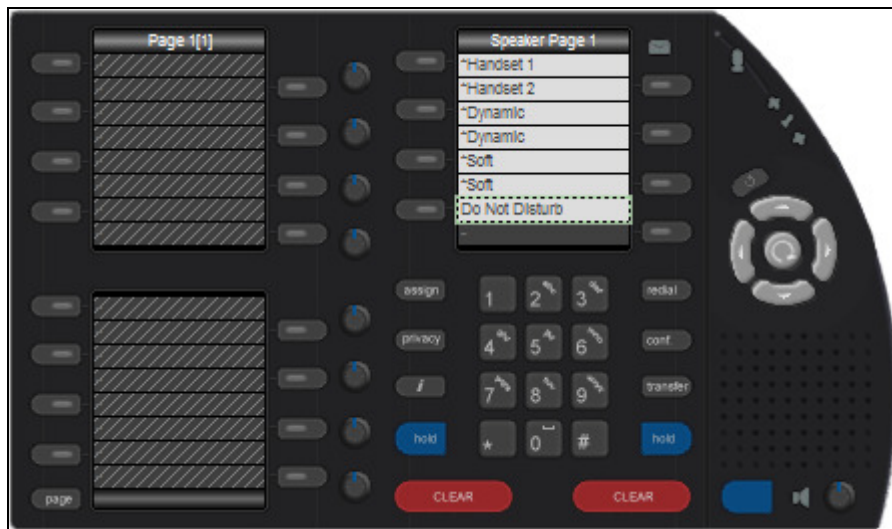


Select **Do Not Disturb** from the **Function Type** dropdown box. Click **OK**.

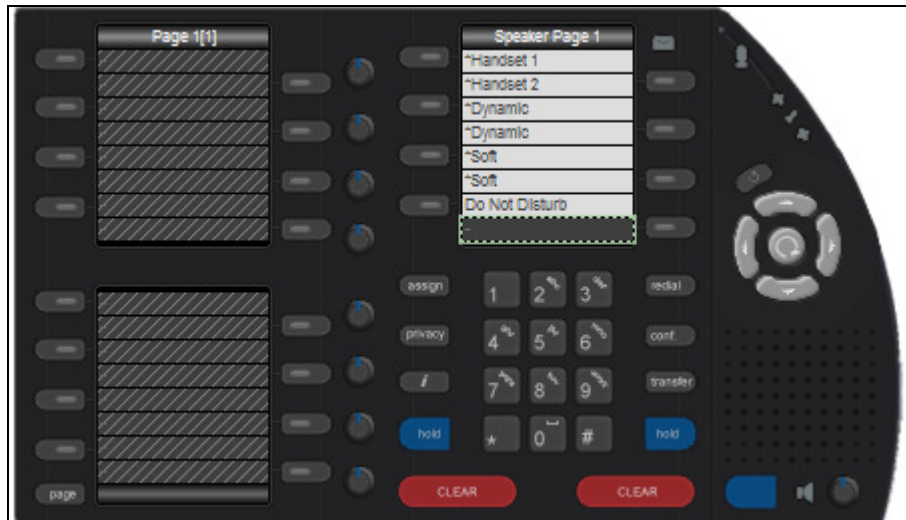


The image shows a 'Key Entry' dialog box with two main sections. The 'General' section contains four dropdown menus: 'Type' (set to 'Function'), 'Style' (set to 'Style 1'), 'Line Mode' (set to 'Single Line'), and a 'Read-only' checkbox which is unchecked. The 'Function Settings' section contains a 'Function Type' dropdown menu set to 'Do Not Disturb'.

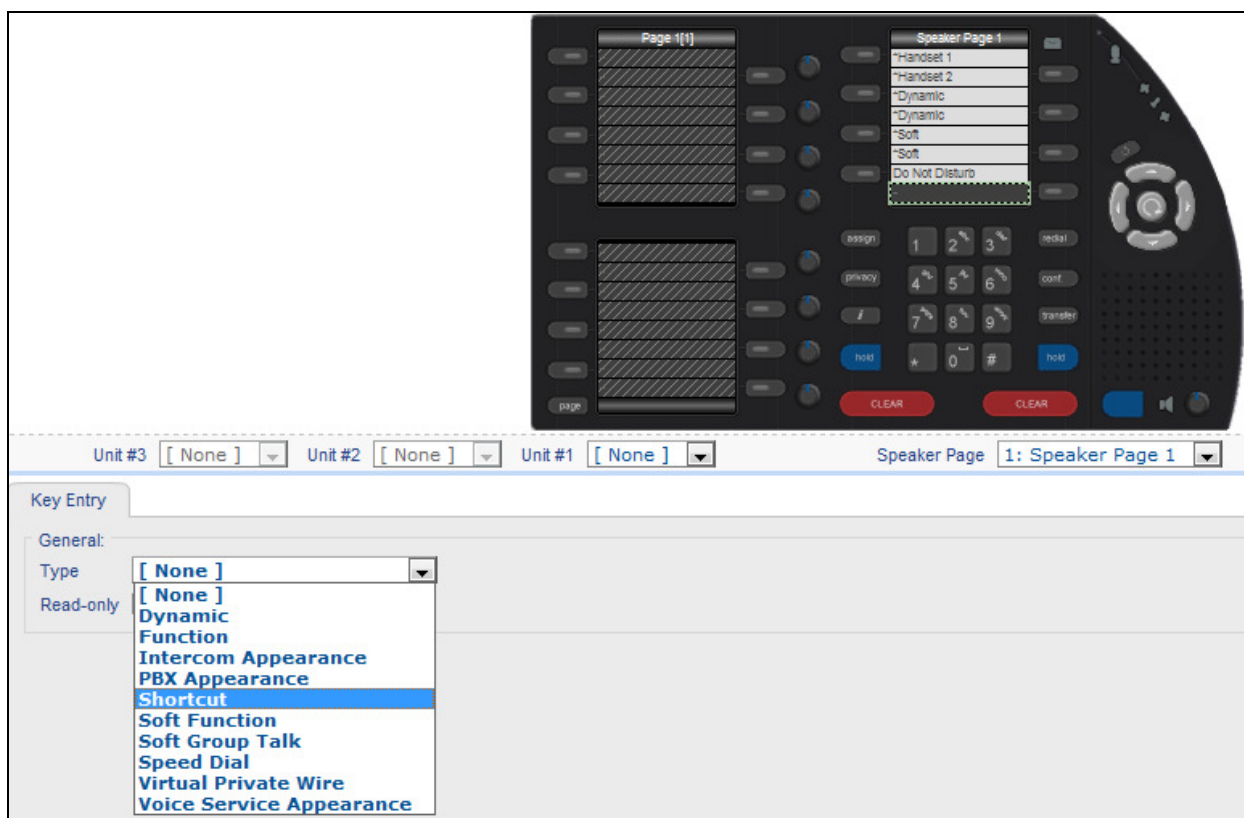
The layout looks as follows:



To create a menu shortcut key, select the next available fixed key under the last function key, as seen below:



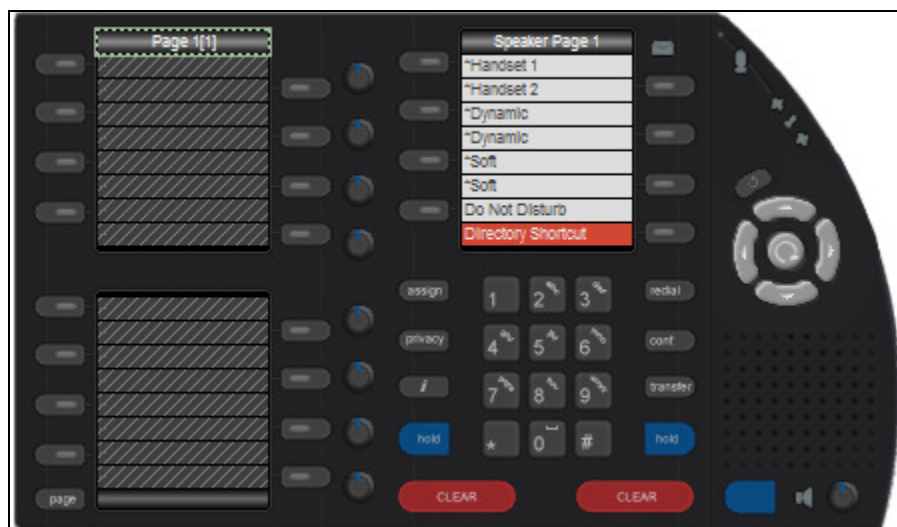
In the Key Entry tab, set **Shortcut** in the **Type** field, as seen below:



Select **Menu Shortcut** from the **Shortcut Type** dropdown box and then **Directory Shortcut** from the **Shortcut** dropdown box. Click **OK**

The screenshot shows a 'Key Entry' dialog box with two main sections. The 'General' section contains three dropdown menus: 'Type' set to 'Shortcut', 'Style' set to 'Style 5' (highlighted in red), and 'Line Mode' set to 'Single Line'. There is also a 'Read-only' checkbox which is unchecked. The 'Shortcut Settings' section contains two dropdown menus: 'Shortcut Type' set to 'Menu Shortcut' and 'Shortcut' set to 'Directory Shortcut' (highlighted in blue).

The iTurret layout will appear as shown below when completed.

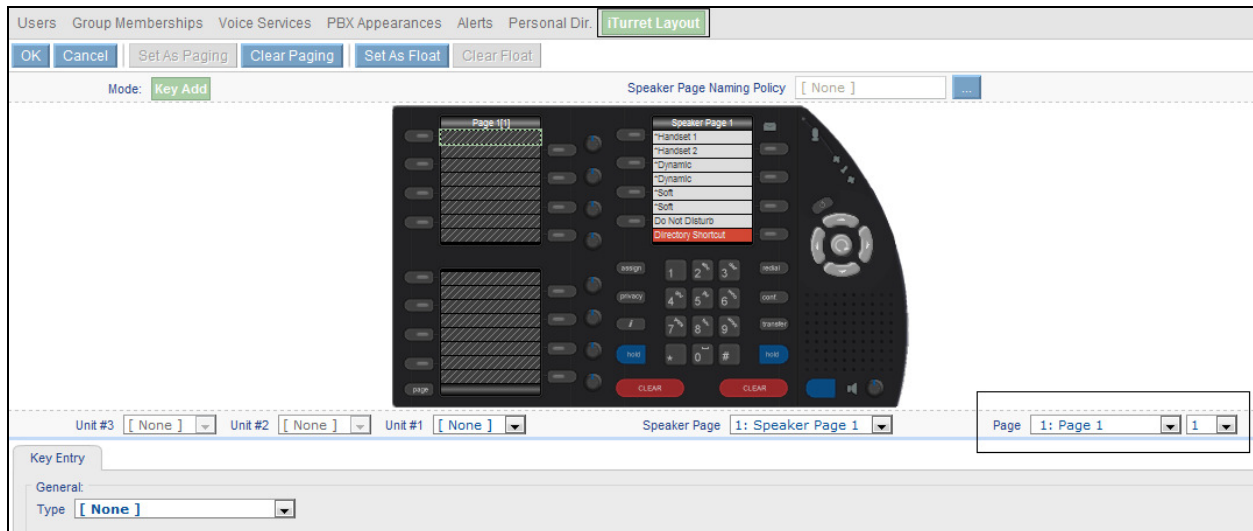




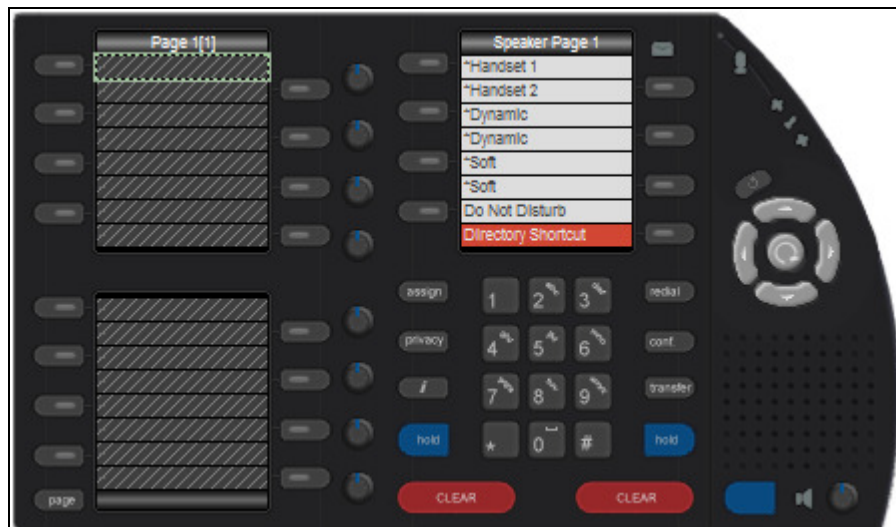
## 7.18. Program Appearances to iTurret Deskstation Keys

This section describes how to create appearance keys for the iTurret deskstation.

Select **Users** → **Users** in the left pane (not shown), select the user to be configured, click the **iTurret Layout** tab and ensure the default page **1:Page 1** is selected from the **Page** dropdown box, as shown below:



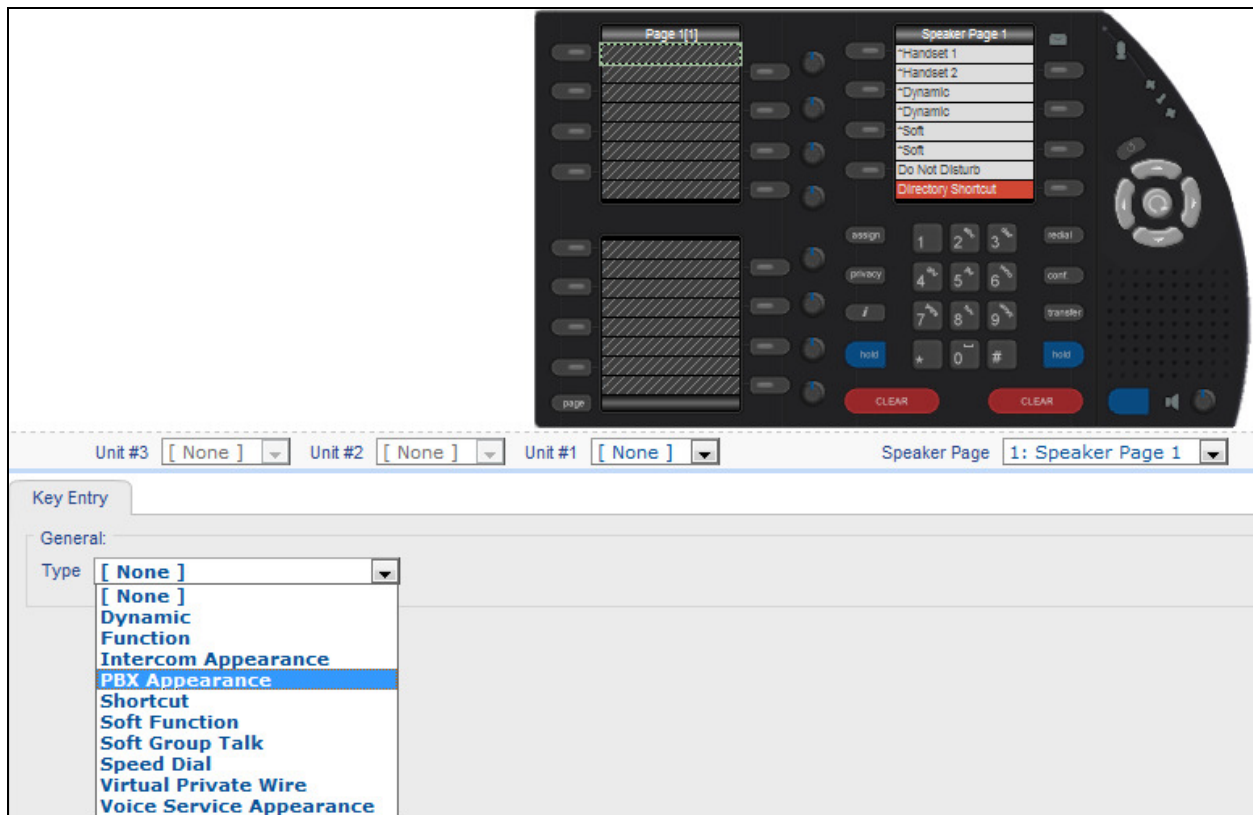
Select the first key on the top left display, as highlighted by a white box, as show below:





The next three keys on this page will be assigned to call appearances.

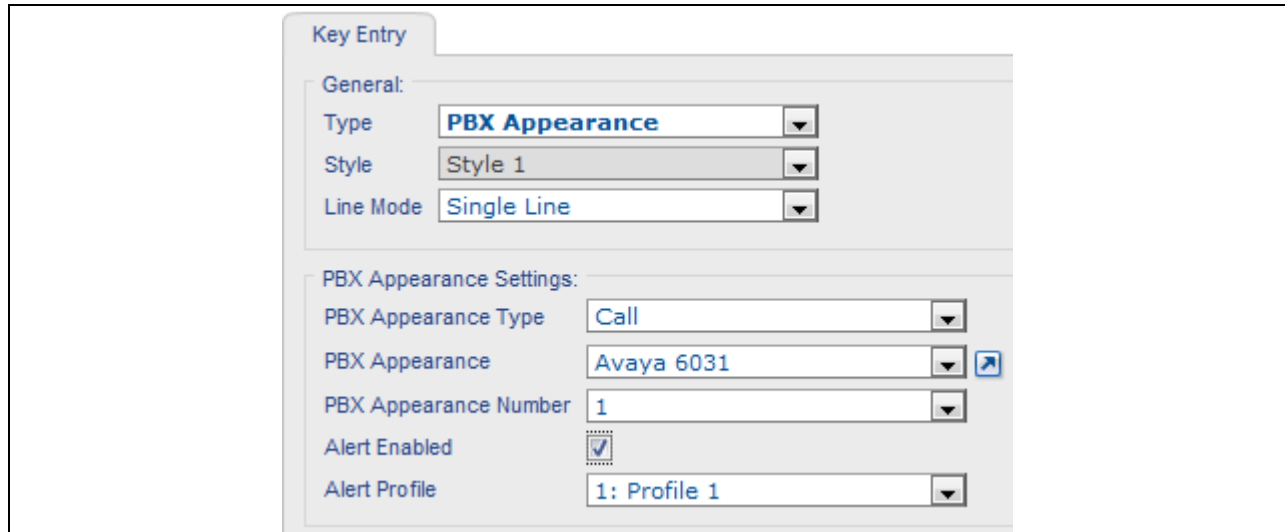
In the **Key Entry** tab select **PBX Appearance** from the **Type** field, as seen below:



Configure the following (as seen on the next screenshot):

- Under the **PBX Appearance Settings**, select the **PBX Appearance Type** (**Call** in this case)
- **PBX Appearance** – select a configured **PBX Appearance**, in this case **Avaya 6031**
- **PBX Appearance Number** (**1** in this case)
- Check **Alert Enabled**
- Leave **1: Profile 1** as default for **Alert Profile**

Once completed, Click **OK**.



The screenshot shows a configuration window titled "Key Entry". It has two main sections: "General" and "PBX Appearance Settings".

**General:**

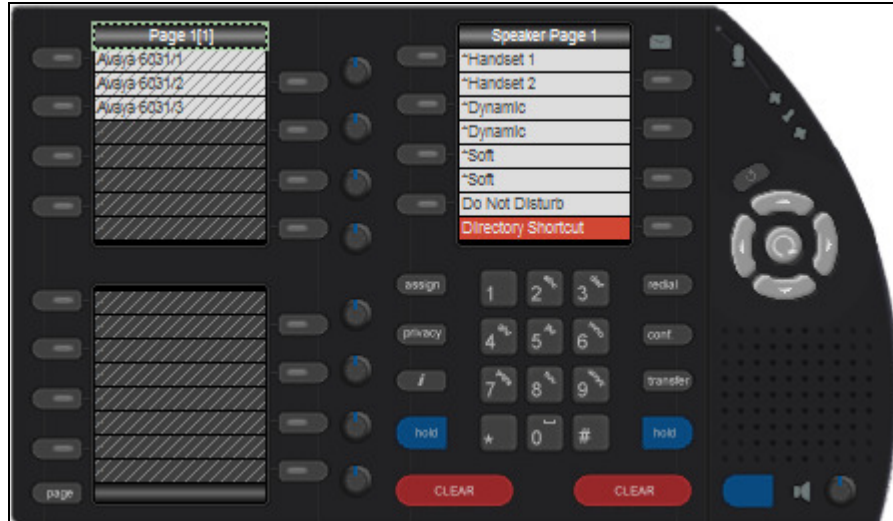
- Type: PBX Appearance
- Style: Style 1
- Line Mode: Single Line

**PBX Appearance Settings:**

- PBX Appearance Type: Call
- PBX Appearance: Avaya 6031
- PBX Appearance Number: 1
- Alert Enabled: ☒
- Alert Profile: 1: Profile 1

**NOTE:** The **PBX Appearance Number** setting will allow the user to be configured with multiple instances of the same extension number thus allowing the user to make and receive multiple calls to and from the same extension number. The **PBX Appearance Number** relates to the **Maximum PBX Appearance** setting configured in **Section 7.12**, which governs how many instances of the extension number are allowed. The **Maximum PBX Appearance** is related to the number of call-appr keys added as feature buttons on the endpoint in System Manager configured in **Section 6.5**. In this example, 4 call-appr keys are administered in System Manager on endpoint 6031, thus the **Maximum PBX Appearance** value in iManager is configured to 4, which allows up to four instances of 6031 to be added on the iTurret layout and have up to four calls to and/or from the iTurret.

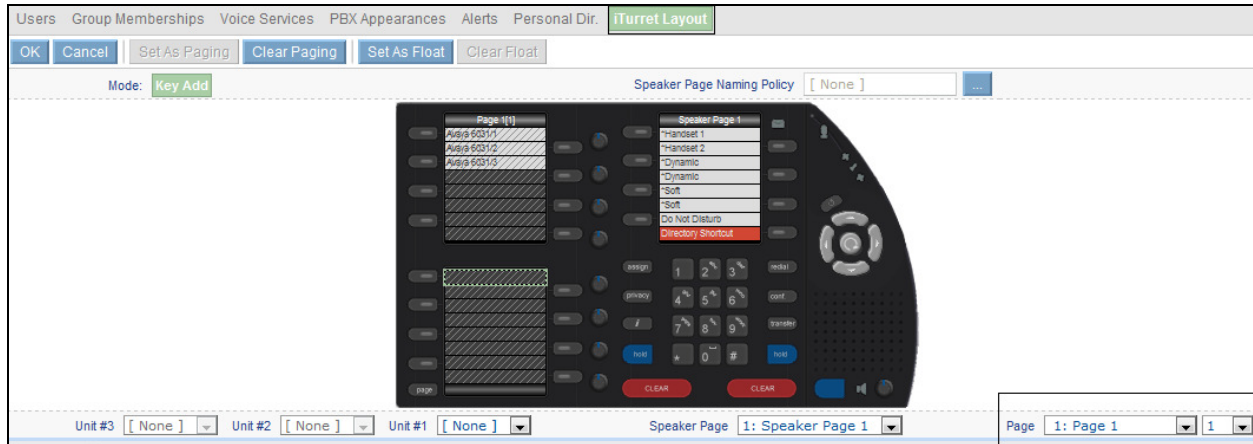
Repeat this procedure to add the next two call appearances and the layout looks as follows:



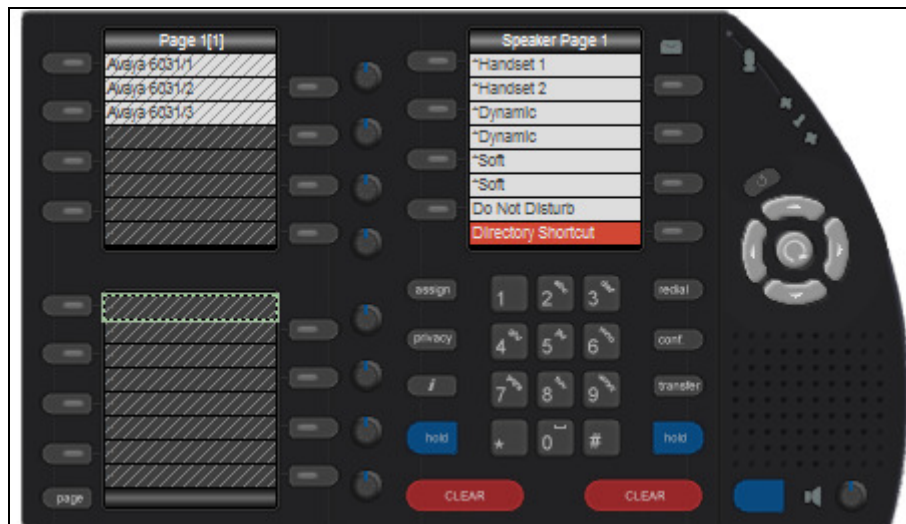
## 7.19. Assign Bridge Call Appearances to iTurret Deskstation Keys

This section describes how to create bridged appearance keys for the iTurret deskstation. Make sure permissions have been set for the call appearance being bridged to this user.

Select **Users** → **Users** in the left pane (not shown), select the user to be configured, click the **iTurret Layout** tab and ensure the default page **1:Page1** is selected from the **Page** dropdown box, as shown below:

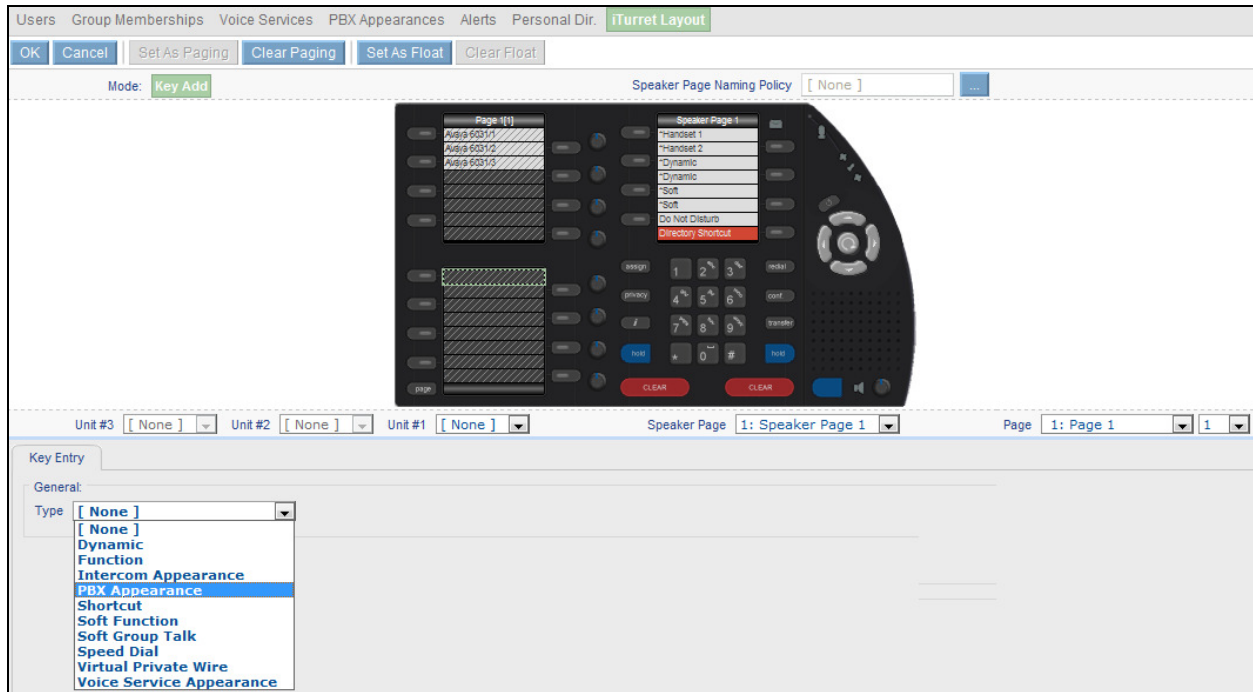


Select the next available key as highlighted by the white box below in the screenshot below.



The next three keys on this page will be assigned to bridged call appearances.

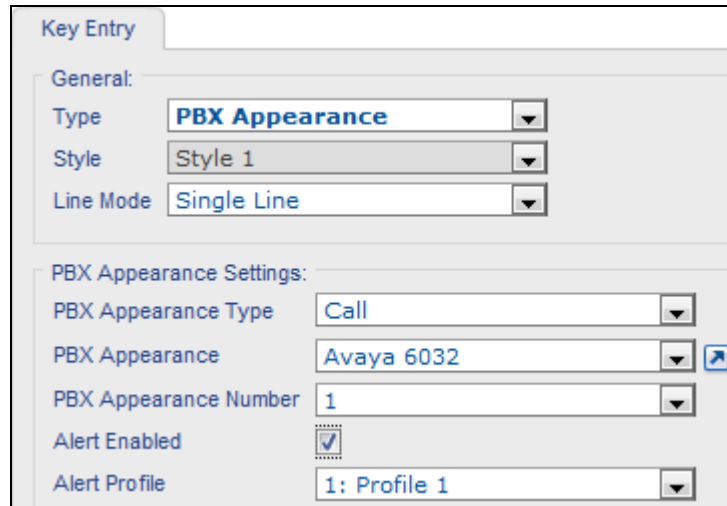
In the **Key Entry** tab configure **PBX Appearance** in the **Type** field as shown in the screenshot below.



Configure the following (as seen on the next screenshot):

- **PBX Appearance Type** – select a configured PBX Appearance, in this case **Avaya 6032**
- **PBX Appearance Number** (**1** in this case)
- Check **Alert Enabled** and leave **1: Profile 1** as default for **Alert Profile**.

Once completed click **OK**.



The screenshot shows a 'Key Entry' configuration window. It has two main sections: 'General' and 'PBX Appearance Settings'. In the 'General' section, 'Type' is set to 'PBX Appearance', 'Style' is 'Style 1', and 'Line Mode' is 'Single Line'. In the 'PBX Appearance Settings' section, 'PBX Appearance Type' is 'Call', 'PBX Appearance' is 'Avaya 6032', 'PBX Appearance Number' is '1', 'Alert Enabled' is checked, and 'Alert Profile' is '1: Profile 1'.

Key Entry	
General:	
Type	PBX Appearance
Style	Style 1
Line Mode	Single Line
PBX Appearance Settings:	
PBX Appearance Type	Call
PBX Appearance	Avaya 6032
PBX Appearance Number	1
Alert Enabled	<input checked="" type="checkbox"/>
Alert Profile	1: Profile 1

**NOTE:** The **PBX Appearance Number** setting will allow the user to be configured with multiple instances of the same extension number thus allowing the user to make and receive multiple calls to and from the same extension number. The PBX Appearance Number relates to the **Maximum PBX Appearance** setting configured in **Section 7.12**, which governs how many instances of the extension number are allowed. The **Maximum PBX Appearance** is related to the number of call-appr keys added as feature buttons on the endpoint in System Manager configured in **Section 6.5**. In this example, 4 call-appr keys are administered in System Manager on endpoint 6032 then the **Maximum PBX Appearance** value in iManager is configured to 4, which allows up to four instances of 6032 to be added on the iTurret layout and have up to four calls to and/or from the iTurret.

Repeat this procedure to add all the bridged call appearances and the layout appears as follows:



## 7.20. Synchronise Deskstations

With Live updates enabled in **Section 7.9** synchronise an iTurret device to push the new configuration to the iTurret without disruption to the user. Select **Devices → Deskstations** (not shown) and select the desired deskstations and click the **Synchronise** button. The iTurret deskstations will indicate that they are being synchronized on their displays. After the deskstations have been synchronized, the status icons on the iTurret deskstations corresponding to the network, iCMS, and SIP registrar status will be green.

Deskstations Channels Connections										
New	Delete	Apply	Seat...	Unseat	Synchronise	Firmware...	Logs...	Diagnostics...	Move...	Feature Keys...
Site		Avaya Galway Labs	Call Region	[ All ]	Type	[ All ]	Status	[ All ]		
Name	Site	Call Region	Type	IP Address	MAC Address	Firmware	Seated User	Status		
Turret A	Avaya Galway Labs	Galway Call Region	iTurret	10.1.230.61	00:05:83:00:16:DA	2.100.7.0	Avaya Test Lab 1			
Turret B	Avaya Galway Labs	Galway Call Region	iTurret	10.1.230.66	00:05:83:00:10:BF	2.100.7.0	Avaya Test Lab 2			
Turret C	Avaya Galway Labs	Galway Call Region	iTurret	10.1.231.60	00:05:83:00:14:C1	2.100.7.0	Avaya Test Lab 3			
Page: 1 of 1		Rows: 3	Reload	Find						

**Note:** Any changes you make to the profile within iManager will be updated on the iTurret device after **OK** or **Apply** is pressed. However, some changes will require a synchronization. Refer to the *Speakerbus iManager Administrator's Guide* for more details.



## 8. Verification Steps

All features shown in **Error! Reference source not found.** were tested using the sample configuration. The following steps can be used to verify the solution.

On the iTurret, verify that the status icons are green. These status icons indicate whether iTurret is connected to the network, iCMS server, and SIP registrar (i.e., Session Manager). Refer to [5] for more details.

To verify that the iTurret have successfully registered with Session Manager, from the System Manager web interface click **Session Manager → System Status → Registration Summary**. This will display a summary of registered stations on each Session Manager as shown below.

Home / Elements / Session Manager / System Status / Registration Summary											
Registration Summary											
Display per Session Manager registration status and send notification to selected AST devices											
AST Device Notifications: <input type="button" value="Reboot"/> <input type="button" value="Reload"/> <input type="button" value="Failback"/> As of 10:45 PM <a href="#">Advanced Search</a>											
2 Items   <a href="#">Refresh</a>   Show <input type="button" value="ALL"/> Filter: <a href="#">Enable</a>											
<input type="checkbox"/>	Session Manager	Type	Primary			Secondary or Survivable			Total		
			Registered	AST	Admin	Registered	AST Failover	Admin	Registered	AST	Admin
<input type="checkbox"/>	sm1	SM	2	2	27	0	0	0	2	2	27
<input type="checkbox"/>	sm2	SM	0	0	0	1	0	13	1	0	13

## 9. Conclusion

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

## 10. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, May 2013, Document Number 03-300509.
- [2] *Avaya Extension to Cellular User Guide Avaya Aura® Communication Manager*, June 2010
- [3] *Implementing Avaya Aura® Session Manager*, Release 6.2, March 2013, Document Number 03-603473.
- [4] *Speakerbus iManager Administrator's Guide*, V1.220, Revision 6, March 2010.
- [5] *Session Initiation Protocol Service Examples draft-ietf-sipping-service-examples-15*, Internet-Draft, 11<sup>th</sup> July 2008, available at <http://tools.ietf.org/html/draft-ietf-sipping-service-examples-15>

---

**©2013 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](mailto:devconnect@avaya.com).