



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

---

# **Application Notes for configuring Speakerbus iD808 iTurret to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 – Issue 1.0**

### **Abstract**

These Application Notes describe the steps required to connect Speakerbus iD808 iTurret to a SIP infrastructure consisting of an Avaya Aura® Communication Manager and an 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.

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

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

# 1. Introduction

These Application Notes describe the steps required to connect Speakerbus iD808 iTurret to a SIP infrastructure consisting of an Avaya Aura® Session Manager and an 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 SIPPING-19 [6]. This provides a useful framework to describe product capabilities and compare features supported by various equipment vendors. Additional features beyond the SIPPING-19 can be extended to iTurret using OPS.

Some OPS features listed in the following table can be invoked by dialing a Feature Name Extension (FNE). A speed dial button on iTurret can also be programmed to an FNE. Other features, such as Exclusion/Privacy and Call Forwarding, are available by using the AST (Advanced SIP Telephony) FNU (Feature Name URI). 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 on the next page shown in **bold** were tested using an FNU or FNE.

FEATURE	SUPPORTED		COMMENTS
	<i>Locally at the phone</i>	<i>With Avaya SIP Offer</i>	
<b>Basic Calling Features</b>			
Extension to Extension Call	YES	YES	
Basic Call to legacy phones	NO	YES	
Speed Dial Buttons	YES	YES	
Message Waiting Support	YES	YES	
<b>SIPPING-19 Features</b>			
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
<b>Call Park/Unpark</b>	<b>NO</b>	<b>YES</b>	<b>Via OPS FNE</b>
<b>Call Pickup</b>	<b>NO</b>	<b>YES</b>	<b>Via OPS FNE</b>
Automatic Redial	NO	YES	Via OPS FNE
<b>OPS – Selected Additional Station-Side Features</b>			
Conference on answer	NO	YES	Via OPS FNE
<b>Directed call pickup</b>	<b>NO</b>	<b>YES</b>	<b>Via OPS FNE</b>
Drop last added party	NO	YES	Via OPS FNE
<b>Exclusion/Privacy</b>	<b>YES</b>	<b>YES</b>	<b>Local hard key on iTurret using FNU</b>
<b>Last number dialed</b>	<b>YES</b>	<b>YES</b>	<b>Via OPS FNE</b>
Priority Call	NO	YES	Via OPS FNE, iTurret doesn't support distinctive ring indication
<b>Send All Calls</b>	<b>NO</b>	<b>YES</b>	<b>Via OPS FNE</b>
<b>Send All Calls Cancel</b>	<b>NO</b>	<b>YES</b>	<b>Via OPS FNE</b>
Transfer to Voicemail	NO	YES	Via OPS FNE
<b>Whisper Page</b>	<b>NO</b>	<b>YES</b>	<b>Via OPS FNE</b>

**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 FNU's.

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

Tests were performed to insure full interoperability between Speakerbus iD808 iTurret and Communication Manager/Session Manager. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully with the following observation:

When the Speakerbus iD808 iTurrets are configured with a backup SIP server (a secondary Session Manager) and, in the likelihood of any active calls during a failover the line associated with the active call will remain unavailable. The remaining lines are still available. This situation can be rectified with a system or iTurret synchronization.

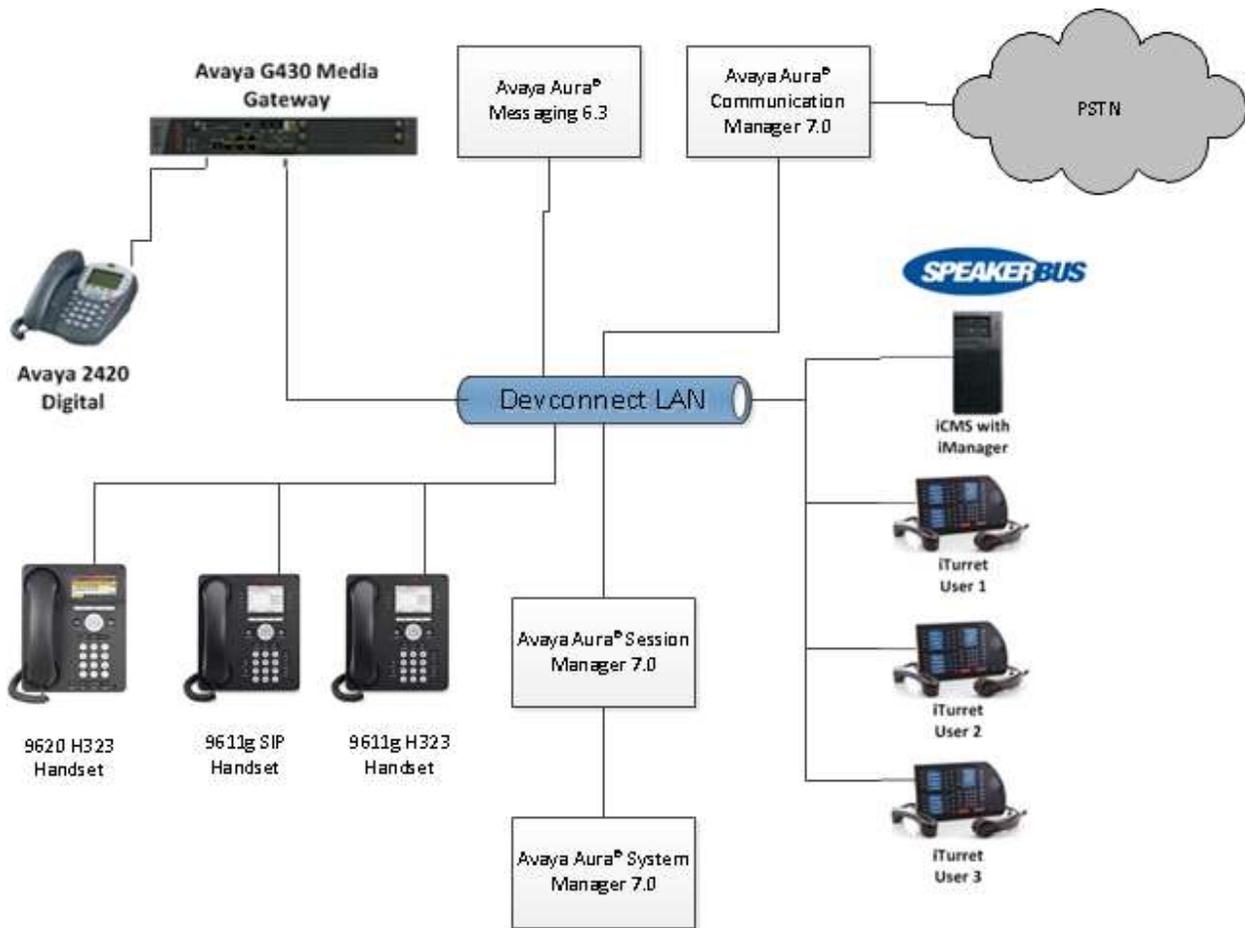
## 2.3. Support

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

**Figure 1** illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Manager and Session Manager. An additional Session Manager was also used to provide failover. System Manager was used to provision Communication Manager and Session Manager. Speakerbus iTurrets were connected to the LAN and managed by the iManager. SIP, Digital and H.323 telephones were configured on Communication Manager to generate outbound/inbound calls to/from the PSTN. Simulated connection to the PSTN was provided by an E1 QSIG trunk connected to the Avaya G430 Media Gateway. Avaya Aura® 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:

<b>Avaya Equipment/Software</b>	<b>Release/Version</b>
Avaya Aura® Communication Manager running on VMware	R7.0 Build R017x.00.0.441.0 S/W update 00.0.441-22477 Platform update PLAT-rhel6.5-0010
Avaya Aura® Session Manager running on VMware	R7.0.0.1.700102
Avaya Aura® Session Manager running on VMware	R7.0.0.1.700102
Avaya Aura® System Manager running on VMware	R7.0.0.1 Build No. 7.0.0.16266-7.0.9.7001011 S/W update 7.0.0.1.4212
Avaya Aura® Messaging running on VMware	R016x.03.0.141.0 S/W update MSG-03.0.141.0-348_0304
Avaya 96xx IP phones 9611G (H.323) 9611G (SIP) 9620G (H323) Avaya 2420 Digital phone	6.5.0 6.6029 3.242 Rel 6.0, FWV 6
Avaya G430 Media Gateway	Version 37.20.0
<b>Speakerbus Equipment/Software</b>	<b>Release/Version</b>
Speakerbus iCMS with iManager Administration running on Windows Server 2008 R2	3.100.11
Speakerbus iD808 iTurret	2.700.6.0 SIP 2.20

## 5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of Communication Manager for this solution. It is implied a working system is already in place, including SIP trunks to two Session Managers (required for failover). For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration described in this section can be summarized as follows:

- Verify System Capacity
- Define System Features
- Define the Dial Plan
- Define Feature Access Codes (FACs)
- Define Feature Name Extensions (FNEs)
- Configure Class of Service (COS)
- Add Coverage Path
- Configure Route Pattern
- Configure IP-Codec Set

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

### 5.1. Verify System Capacity

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 1**, verify that the **Maximum Off-PBX Telephones** allowed in the system is sufficient. One OPS station is required per iD808 device.

```
display system-parameters customer-options                               Page 1 of 10
                                OPTIONAL FEATURES

G3 Version: V16                                     Software Package: Enterprise
Location: 2                                         System ID (SID): 1
Platform: 28                                       Module ID (MID): 1

                                                USED
Platform Maximum Ports: 65000 290
Maximum Stations: 41000 44
Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 41000 0
Maximum Off-PBX Telephones - OPS: 41000 14
Maximum Off-PBX Telephones - PBFMC: 41000 0
Maximum Off-PBX Telephones - PVFMC: 41000 0
Maximum Off-PBX Telephones - SCCAN: 41000 0
Maximum Survivable Processors: 313 0

(NOTE: You must logoff & login to effect the permission changes.)
```

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

```

display system-parameters customer-options                               Page 2 of 10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
    Maximum Administered H.323 Trunks: 12000 16
    Maximum Concurrently Registered IP Stations: 18000 2
    Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
    Maximum Concurrently Registered IP eCons: 414 0
    Max Concur Registered Unauthenticated H.323 Stations: 100 0
    Maximum Video Capable Stations: 41000 1
    Maximum Video Capable IP Softphones: 18000 4
    Maximum Administered SIP Trunks: 24000 180
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
    Maximum Number of DS1 Boards with Echo Cancellation: 522 0
    Maximum TN2501 VAL Boards: 128 0
    Maximum Media Gateway VAL Sources: 250 0
    Maximum TN2602 Boards with 80 VoIP Channels: 128 0
    Maximum TN2602 Boards with 320 VoIP Channels: 128 0
    Maximum Number of Expanded Meet-me Conference Ports: 300 0

(NOTE: You must logoff & login to effect the permission changes.)

```

## 5.2. Define System Features

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

```

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 19** 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
  
```

### 5.3. Define the Dial Plan

Use the **change dialplan analysis** command to define the dial plan used in the system. This includes all telephone extensions, OPS Feature Name Extensions (FNEs), and Feature Access Codes (FACs). To define the FNEs for the OPS features listed in 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 **2** and **3**, FNEs are also four digits beginning with **2**, and the FACs have formats as indicated with a **Call Type** of **fac**.

```

change dialplan analysis                                       Page 1 of 12
                                DIAL PLAN ANALYSIS TABLE
                                Location: all                    Percent Full: 1

    Dialed   Total   Call   Dialed   Total   Call   Dialed   Total   Call
    String   Length  Type   String   Length  Type   String   Length  Type
    1         4       ext    1         4       ext
    11        5       ext    2         4       ext
    2         4       ext   3         4       ext
    3         4       ext   35        4       udp
    35        4       udp    4         4       udp
    4         4       udp    423       4       ext
    423       4       ext    5         3       ext
    5         3       ext    6         4       udp
    6         4       udp    7         1       dac
    7         1       dac    7000      4       udp
    7000      4       udp    8         3       udp
    8         3       udp    9         3       fac
    9         3       fac   *         3       fac
    *         3       fac   #         3       fac
    #         3       fac
  
```

## 5.4. Define Feature Access Codes (FACs)

A FAC (feature access code) should be defined for each feature that will be used via the OPS FNEs. Use **change feature-access-codes** to define the required access codes. The FACs used in the sample configuration are shown in bold.

```
change feature-access-codes                                     Page 1 of 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
Answer Back Access Code: *06

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:
Call Park Access Code: *16
Call Pickup Access Code: *17
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:
Directed Call Pickup Access Code: *23
Directed Group Call Pickup Access Code:
Emergency Access to Attendant Access Code:
EC500 Self-Administration Access Codes:
Enhanced EC500 Activation:                      Deactivation:
Enterprise Mobility User Activation:             Deactivation:
Extended Call Fwd Activate Busy D/A All:        Deactivation:
Extended Group Call Pickup Access Code:
Facility Test Calls Access Code:
Flash Access Code:
Group Control Restrict Activation:              Deactivation:
Hunt Group Busy Activation:                    Deactivation:
ISDN Access Code:
Last Number Dialed Access Code: *30
Leave Word Calling Message Retrieval Lock:
Leave Word Calling Message Retrieval Unlock:
```

change feature-access-codes

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: \*33**  
**Per Call CPN Unblocking Code Access Code: \*34**

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: \*38 Deactivation: \*39**

Station Firmware Download Access Code:

change feature-access-codes

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: \*58**

3PCC H323 Override SIP Station Activation: Deactivation:

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

## 5.5. Define Feature Name Extensions (FNEs)

The OPS FNEs can be defined using the **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: 2699
Call Forward All: 2698
Call Forward Busy/No Answer:
Call Forward Cancel:
Call Park: 2697
Call Park Answer Back: 2696
Call Pick-Up: 2695
Calling Number Block:
Calling Number Unblock:
Conditional Call Extend Enable:
Conditional Call Extend Disable:
Conference Complete:
Conference on Answer:
Directed Call Pick-Up: 2694
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: 2692
Malicious Call Trace:
Malicious Call Trace Cancel:
Off-Pbx Call Enable:
Off-Pbx Call Disable:
Priority Call:
Recall:
Send All Calls: 2691
Send All Calls Cancel: 2690
Transfer Complete:
Transfer On Hang-Up:
Transfer to Voice Mail:
Whisper Page Activation: 2693
```

## 5.6. 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

## 5.7. Configure Class of Restriction (COR)

Use the **change cor n** command where **n** is the number of the COR being configured, to enable applicable calling features. To use the Directed Call Pickup feature, the **Can Be Picked Up By Directed Call Pickup** and **Can Use Directed Call Pickup** fields must be set to **y**. In the sample configuration, the 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
```

## 5.8. Add Coverage Path

Use the **add coverage path n** command where **n** is the number of the coverage path to be added. Configure **Point 1** in the coverage path to one used to the voice messaging hunt group, which is group **h1** in the sample configuration. The default values shown for **Busy**, **Don't Answer**, and **DND/SAC/Goto Cover** can be used for the **Coverage Criteria**.

```

add coverage path 89                                     Page 1 of 1
                                COVERAGE PATH

                                Coverage Path Number: 1
                                Cvg Enabled for VDN Route-To Party? n      Hunt after Coverage? n
                                Next Path Number:                          Linkage

COVERAGE CRITERIA

Station/Group Status   Inside Call   Outside Call
Active?                n             n
Busy?                  y             y
Don't Answer?         y             y           Number of Rings: 2
All?                   n             n
DND/SAC/Goto Cover?   y             y
Holiday Coverage?     n             n

COVERAGE POINTS
Terminate to Coverage Pts. with Bridged Appearances? n
Point1: h1             Rng:         Point2:
Point3:                Point4:
Point5:                Point6:
24: exclusion
  
```

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

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

## 5.9. 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 15.

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									n	user		
2:	15	0									n	user		
3:											n	user		
4:											n	user		
5:											n	user		
6:											n	user		
		BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR		
		0	1	2	M	4	W	Request						
											Dgts	Format		
											Subaddress			
1:	y	y	y	y	y	n	n	rest					none	
2:	y	y	y	y	y	n	n	rest					none	
3:	y	y	y	y	y	n	n	rest					none	
4:	y	y	y	y	y	n	n	rest					none	
5:	y	y	y	y	y	n	n	rest					none	
6:	y	y	y	y	y	n	n	rest					none	

## 5.10. 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                                     Page 1 of 2

                               IP Codec Set

Codec Set: 1

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

Media Encryption
1: none
2:
3:
```

## 5.11. Configure Outgoing Number formats

Communication Manager entries have to be made to allow the calling number to be sent over SIP Trunks. These entries have to be made in both the private and public-unknown numbering tables.

### 5.11.1. 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 **1**
- **Trk Grp** – Enter the SIP trunk groups configured above, in this case **1** and **15**
- **Total Len** – Enter the total length of the SIP extension number, in this case **4**

```
change private-numbering 0                               Page 1 of 2

                               NUMBERING - PRIVATE FORMAT

Ext  Ext      Trk      Private      Total
Len  Code      Grp(s)    Prefix      Len
4    1          1         4           4    Total Administered: 3
4    1          15        4           4    Maximum Entries: 540
```

### 5.11.2. Configure Public Unknown Numbering

Enter the command **change public-unknown-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 **1**
- **Trk Grp** – Enter the SIP trunk groups configured above, in this case **1** and **15**
- **Total Len** – Enter the total length of the SIP extension number, in this case **4**

change public-unknown-numbering 0					Page 1 of 2	
NUMBERING - PUBLIC/UNKNOWN FORMAT						
Ext	Ext	Trk	CPN	Total		
Len	Code	Grp(s)	Prefix	CPN		
				Len		
4	1	1		4	Total Administered: 3	
4	1	15		4	Maximum Entries: 540	

## 6. Configure Avaya Aura® Session Manager

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

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

AVAYA  
Aura System Manager 7.0

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

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

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

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

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

## 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** → **SM70** (not shown) where **SM70** 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** when done.

The screenshot shows the configuration interface for SIP entities. The 'Port' section is highlighted with a red box. It contains the following table:

Port	Protocol	Default Domain	Notes
5060	UDP	devconnect.local	
5060	TCP	devconnect.local	
5061	TLS	devconnect.local	

Below the table are 'Add' and 'Remove' buttons. The 'SIP Responses to an OPTIONS Request' section is also visible, showing a table with columns: Response Code & Reason Phrase, Mark Entity Up/Down, and Notes. At the bottom are 'Commit' and 'Cancel' buttons.

Repeat accordingly on the alternative Session Manager.

## 6.2. Add Primary iTurret User

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

As the addition of stations is considered a very complex configuration, a detailed knowledge of the installation is required. Speakerbus personnel will be required to carry out this configuration.

A user must be added for each iTurret. Click **User Management** → **Manage Users** → **New** (not shown) and configure as following in the **Identity** tab.

- **First Name and Last Name** Enter an identifying name
- **Login Name** Enter the extension number followed by the domain, in this case **2500@devconnect.local**
- **Authentication Type** Select **Basic** from the drop down list
- **Password and Confirm Password** Enter and confirm a password

The screenshot displays the 'Identity' tab of a user provisioning interface. The 'User Provisioning Rule' is set to the default. The 'Identity' section contains the following fields and values:

- Last Name:** User 1
- Last Name (Latin Translation):** User 1
- First Name:** Speakerbus
- First Name (Latin Translation):** Speakerbus
- Middle Name:** (empty)
- Description:** (empty)
- Update Time:** January 13, 2015 4:12
- Login Name:** 2500@devconnect.local
- Authentication Type:** Basic
- New Password:** (masked with asterisks)
- Confirm Password:** (empty)
- Source:** local
- Localized Display Name:** User 1, Speakerbus
- Endpoint Display Name:** User 1, Speakerbus
- Title:** (empty)
- Language Preference:** English (United Kingdom)
- Time Zone:** (0:0)GMT : Dublin, Edinburgh, I.
- Employee ID:** (empty)
- Department:** (empty)
- Company:** (empty)

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

The screenshot shows the 'New User Profile' dialog box with the 'Communication Profile' tab selected. The 'Communication Profile Password' and 'Confirm Password' fields are highlighted with red boxes. The 'New' button is also highlighted with a red box. Below the password fields, there is a 'Name' field with a dropdown menu set to 'Primary'. At the bottom, there are buttons for 'New', 'Delete', 'Done', and 'Cancel'.

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

The screenshot shows the 'Communication Address' dialog box. The 'Type' dropdown is set to 'Avaya SIP'. The 'Fully Qualified Address' field contains '2500' and the 'Domain' dropdown is set to 'devconnect.local'. The 'Add' button is highlighted with a red box. The dialog box also includes a table with columns 'Type', 'Handle', and 'Domain', and a 'Select' dropdown set to 'All, None'.

Type	Handle	Domain
No Records found		

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 **SM70** and **MCSM70\_B** respectively.

**Session Manager Profile** ▼

### SIP Registration

\* Primary Session Manager SM70 ▼  
 Secondary Session Manager MCSM70\_B ▼

Primary	Secondary	Maximum
14	0	14

Primary	Secondary	Maximum
0	10	10

Survivability Server (None) ▼  
 Max. Simultaneous Devices 1 ▼  
 Block New Registration When Maximum Registrations Active?

### Application Sequences

Origination Sequence cm70appseq ▼  
 Termination Sequence cm70appseq ▼

### Call Routing Settings

\* Home Location DevConnectRP ▼

 Conference Factory Set (None) ▼

### Call History Settings

 Enable Centralized Call History?

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 **2500**
- **Template** Select **DEFAULT\_9630SIP\_CM\_7\_0** from the drop down list
- **Port** Enter **IP**

Click on **Endpoint Editor**.

The screenshot shows the 'CM Endpoint Profile' configuration form. The 'CM Endpoint Profile' checkbox is checked. The 'System' dropdown is set to 'CM63'. The 'Profile Type' dropdown is set to 'Endpoint'. The 'Use Existing Endpoints' checkbox is unchecked. The 'Extension' field contains '2500' and has an 'Endpoint Editor' button next to it. The 'Template' dropdown is set to '9630SIP\_DEFAULT\_CM\_7\_0'. The 'Set Type' field contains '9630SIP'. The 'Security Code' field is empty. The 'Port' field contains 'IP'. The 'Voice Mail Number' field is empty. The 'Preferred Handle' dropdown is set to '(None)'. The 'Enhanced Callr-Info display for 1-line phones' checkbox is unchecked. The 'Delete Endpoint on Unassign of Endpoint from User or on Delete User' checkbox is checked. The 'Override Endpoint Name and Localized Name' checkbox is checked.

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

- **Class of Restriction (COR)** Enter the **COR** as configured in **Section 5.7**
- **Emergency Location Ext** Enter **2500**
- **Tenant Number** Enter the required **Tenant Number**
- **SIP Trunk** Enter **AAR**
- **Class of Service (COS)** Enter the **COS** as configured in **Section 5.6**
- **Message Lamp Ext.** Enter **2500**

The screenshot shows the 'General Options (G)' configuration page. The 'General Options (G)' tab is selected. The following fields are highlighted with a red box:

- Class of Restriction (COR): 1
- Emergency Location Ext: 2500
- Tenant Number: 1
- SIP Trunk: aar

Other visible fields include:

- Class of Service (COS): 1
- Message Lamp Ext.: 2500
- Type of 3PCC Enabled: None
- Coverage Path 1: 1
- Coverage Path 2: (empty)
- Lock Message: (checkbox)
- Localized Display Name: User 1, Speakerbus
- Multibyte Language: Not Applicable

Click on the **Feature Options** tab. The screen shot below shows the Feature options that were used during compliance testing.

The screenshot shows the 'Feature Options (F)' configuration page. The 'Feature Options (F)' tab is selected. The page is divided into sections for various settings:

- Active Station Ringing:** single
- MWI Served User Type:** None
- Per Station CPN - Send Calling Number:** None
- IP Phone Group ID:** (empty)
- Remote Soft Phone Emergency Calls:** (empty)
- LWC Reception:** spe
- AUDIX Name:** (empty)
- Speakerphone:** (checkbox)
- Short/Prefixed Registration Allowed:** (checkbox)
- EC500 State:** enabled
- Auto Answer:** none
- Coverage After Forwarding:** system
- Display Language:** english
- Hunt-to Station:** (empty)
- Loss Group:** 19
- Survivable COR:** internal
- Time of Day Lock Table:** None
- Voice Mail Number:** (empty)
- Music Source:** (empty)

**Features:**

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

Click on the **Button Assignments** tab (**Main Buttons**) and configure Buttons 1, 2 and 3 as **call-appr**. During compliance buttons 3 and 4 were configured as **brdg-appr**. Ext **2555** was used to simulate Technical Support extensions.

Button ID	Application	Button	Ext
1	call-appr		
2	call-appr		
3	call-appr		
4	brdg-appr	1	2555
5	brdg-appr	2	2555
6	None		
7	None		
8	None		

Click on **Feature Buttons** and configure as per screen shot below. Click **Commit** when done (not shown).

**Note:** Extensions 2501 and 2502 are the privacy users for iTurret 2500 and button 24 is configured as **exclusion**.

Button ID	Application	Button	Ext
9	None		
10	brdg-appr	1	2501
11	brdg-appr	1	2502
12	None		
13	None		
14	None		
15	None		
16	None		
17	None		
18	None		
19	None		
20	sand-calls		
21	auto-cback		
22	call-fwd		
23	chwd-bsyda		
24	exclusion		

### 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 2500 are extensions 3600 and 3601.

**Note:** The Privacy Users were previously configured and are outside the scope of these Application Notes.

### 6.4. Configure Privacy Endpoint

Click **Communication Manager** → **Endpoints** → **Manage Endpoints** and select the relevant privacy endpoint and click **Edit**, in this case **Extension 3600**.

Name	Extension	Port	Set Type	COS	COR	User	Tenant Number	System
AAACC_AGT1013	1013	S00018	9608	1	1		1	CM63
1016 H323 Ext	1016	S00029	9640	1	1		1	CM63
Fax Machine 1026	1026	002V301	2500	1	1		1	CM63
Digital,1004	1004	002V201	2420	1	1		1	CM63
1015 H323 Ext	1015	S00028	9620	1	1		1	CM63
User 2, Speakerbus	2501	S00069	9630SIP	1	1	2501@devconnect.local	1	CM63
User 1, Speakerbus	2500	S00012	9630SIP	1	1	2500@devconnect.local	1	CM63
PRV-1-2, 3601	3601	S00072	9630SIP	1	1	3601@devconnect.local	1	CM63
<b>PRV-1-1, 3600</b>	<b>3600</b>	S00071	9630SIP	1	1	3600@devconnect.local	1	CM63
User 3, Speakerbus	2502	S00070	9630SIP	1	1	2502@devconnect.local	1	CM63
Support, Technical	2555	S00075	9630SIP	1	1	2555@devconnect.local	1	CM63
PRV 2-2, 3603	3603	S00074	9630SIP	1	1	3603@devconnect.local	1	CM63
PRV 2-1, 3602	3602	S00073	9630SIP	1	1	3602@devconnect.local	1	CM63
NICEVirt3	11000	S00068	4624	1	1		1	CM63
NICEVirt2	11002	S00065	4624	1	1		1	CM63

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

- **Class of Restriction (COR)** Enter the **COR** as configured in **Section 5.7**
- **Emergency Location Ext** Enter **3600**
- **Tenant Number** Enter the required **Tenant Number**
- **SIP Trunk** Enter **AAR**
- **Class of Service (COS)** Enter the **COS** as configured in **Section 5.6**
- **Message Lamp Ext.** Enter **2500**

Class of Restriction (COR)	1	Class Of Service (COS)	1
Emergency Location Ext	3600	Message Lamp Ext.	3600
Tenant Number	1	Type of 3PCC Enabled	None
SIP Trunk	Qaar	Coverage Path 2	
Coverage Path 1		Localized Display Name	PRV-1-1, 3600
Lock Message	<input type="checkbox"/>		
Multibyte Language	Not Applicable		

Click on the **Feature Options** tab. The screen shot below shows the Feature Options that were used during compliance testing.

The screenshot shows the 'Feature Options' configuration page. The 'Feature Options' tab is highlighted in red. The page contains various configuration fields for features like Active Station Ringing, MWI Served User Type, Auto Answer, Coverage After Forwarding, Display Language, Hunt-to Station, Less Group, Survivable COR, Time of Day Lock Table, Voice Mail Number, and Music Source. A 'Features' section at the bottom contains a list of checkboxes for various features, with several checked.

Click on the **Button Assignments** tab (**Main Buttons**) and configure Buttons 1, 2 and 3 as **call-appr**. During compliance buttons 4, 5 and 6 were configured as **brdg-appr** to extension **2500** (Primary iTurret User). Button 7 was configured as **brdg-appr** to extension **2501** (Privacy key for user 2501). Button 8 was configured as **brdg-appr** to extension **2502** (Privacy key for user 2502).

The screenshot shows the 'Button Assignment' configuration page. The 'Button Assignment' tab is highlighted in red. The page shows a table of button assignments for buttons 1 through 8. Buttons 1, 2, and 3 are assigned 'call-appr'. Buttons 4, 5, and 6 are assigned 'brdg-appr' to extension 2500. Button 7 is assigned 'brdg-appr' to extension 2501. Button 8 is assigned 'brdg-appr' to extension 2502.

Button	Assignment	Ext
1	call-appr	
2	call-appr	
3	call-appr	
4	brdg-appr	2500
5	brdg-appr	2500
6	brdg-appr	2500
7	brdg-appr	2501
8	brdg-appr	2502

Click on **Feature Buttons** and configure as per screen shot below. Click **Commit** when done.

**Note:** Button 24 is configured as **exclusion**.

The screenshot shows the 'Button Assignment' configuration window. The 'Feature Buttons' tab is selected. The table below shows the configuration for buttons 9 through 24. Button 24 is highlighted with a red box and is set to 'exclusion'.

Button ID	Feature	Button	Ext
9	brdg-appr	2	2502
10	brdg-appr	1	2555
11	brdg-appr	2	2555
12	None		
13	None		
14	None		
15	None		
16	None		
17	None		
18	None		
19	None		
20	None		
21	None		
22	None		
23	None		
24	exclusion		

\*Required

Buttons: Commit, Schedule, Reset, Cancel

## 6.5. 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** (not shown). 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.

The screenshot shows the 'Server Timer' configuration window. The 'Registration Expiration Timer (secs)' is highlighted with a red box. The 'Maximum' value is 90 and the 'Minimum' value is 60.

	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.

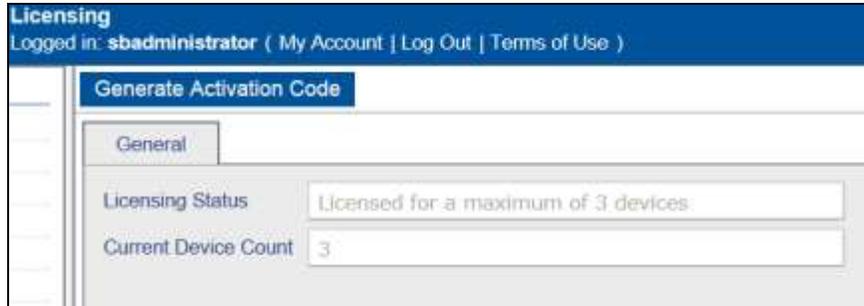
- Launch iManager Web Portal
- Verify Product Key
- Create Site
- Create Call Region
- Create/Verify User Policies
- Create/Verify Device Policies
- Create Network Services
- Confirm Defaults
- Create iTurrets Deskstations
- Create PBX (SIP Server)
- Create Dial Plan
- Create Call and Handset Appearances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

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



## 7.2. Verify Product Key

Select **System** → **Product Key** (not shown) in the left pane to verify that a valid key is installed and sufficient devices are allowed.



The screenshot shows the 'Licensing' page in the iManager Administrator's Guide. The page is titled 'Licensing' and shows the user is logged in as 'sbadministrator'. The 'Generate Activation Code' section is active, and the 'General' tab is selected. The 'Licensing Status' is 'Licensed for a maximum of 3 devices' and the 'Current Device Count' is 3.

## 7.3. Create a Site

Configure a site representing the location where the Speakerbus iTurret devices are installed. Select **Network** → **Sites** (not shown) in the left pane click on **NEW** (not shown) and enter an identifying **Name** for the new site, then press **OK** (not shown).



The screenshot shows the 'General' tab in the 'Create a Site' dialog. The 'Name' field is highlighted with a red box and contains the text 'Galway Lab'.

**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** (not shown) and 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.

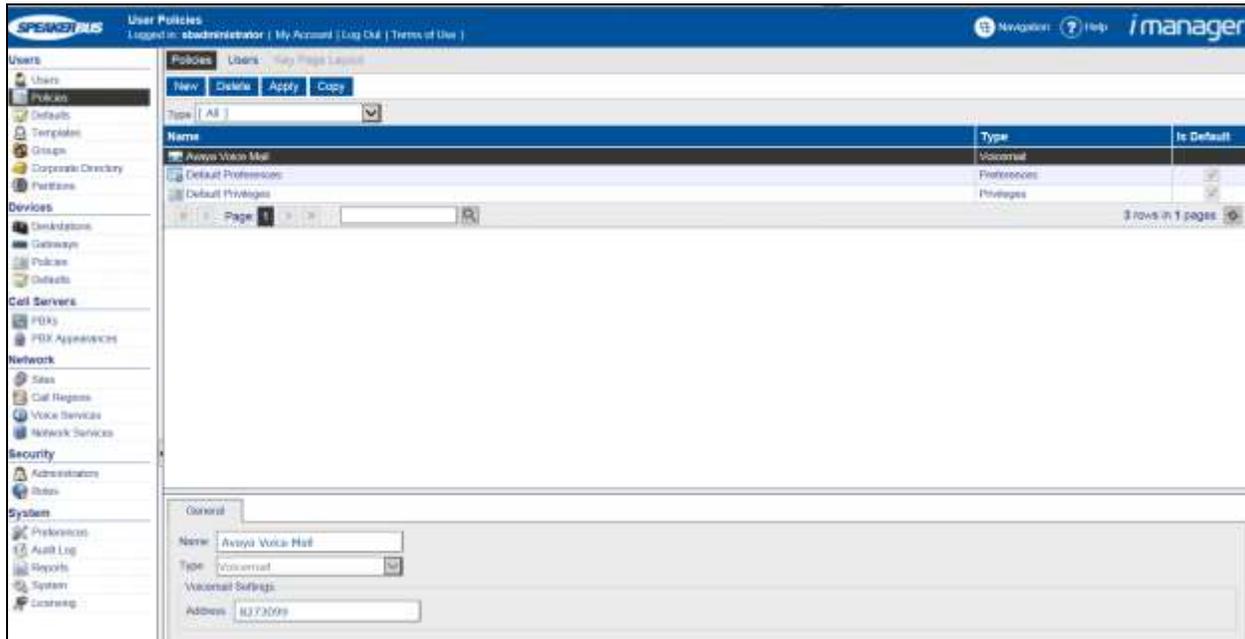


The screenshot shows the 'General' tab in the 'Create a Call Region' dialog. The 'Name' field is highlighted with a red box and contains the text 'Avaya Galway'. The 'Partition Checking' and 'Priority For P2P' checkboxes are unchecked.

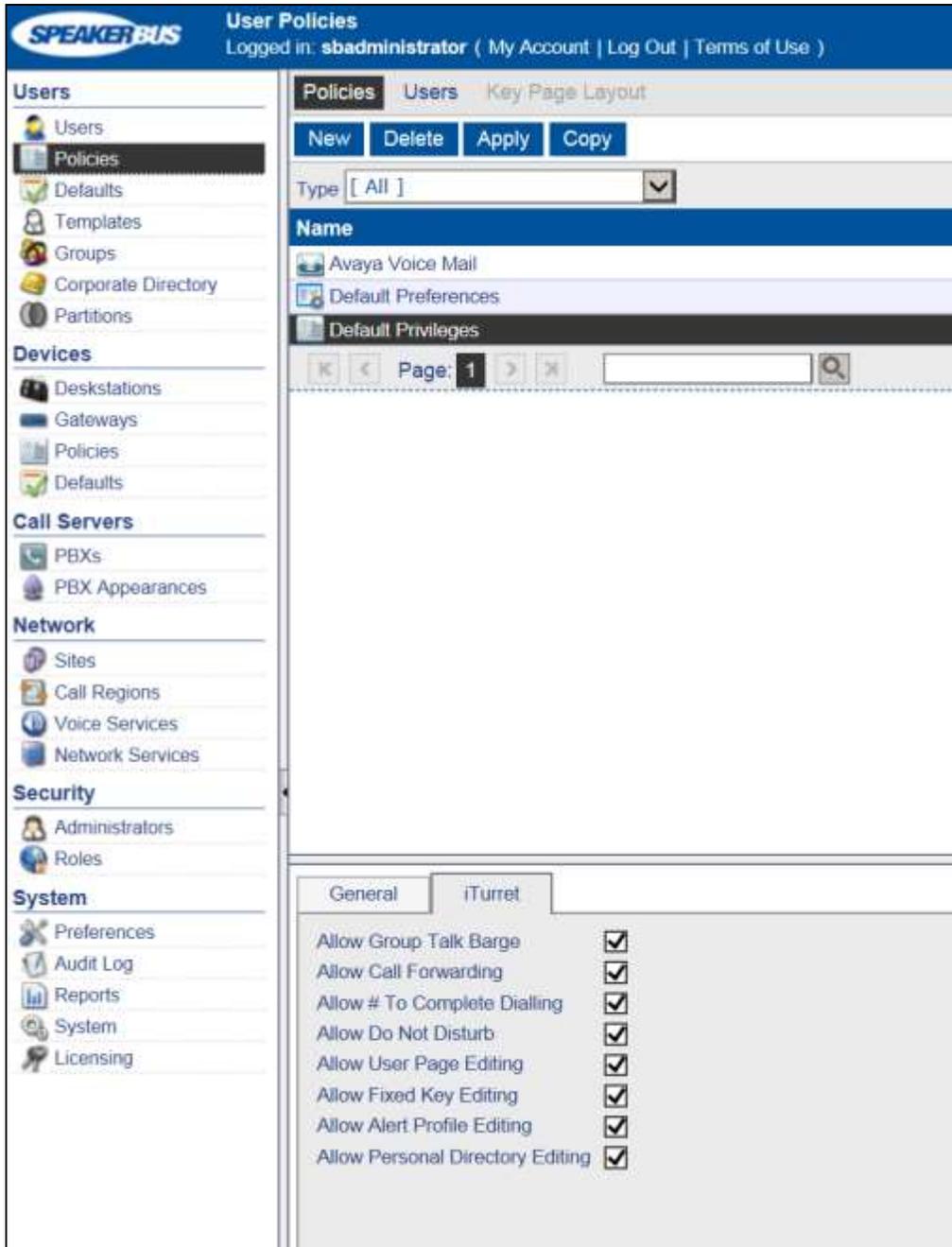
**Note:** A default call region is available and can be used for a single site setup. Refer to the *Speakerbus iManager Administrator's Guide* [5] for further configuration information.

## 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.



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 these Application Notes).



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, however it's referred to later in these Application Notes).

The screenshot displays the Avaya iTurret configuration interface. At the top, there are tabs for 'Policies', 'Users', and 'Key Page Layout'. Below these are buttons for 'New', 'Delete', 'Apply', and 'Copy'. A 'Type' dropdown menu is set to '[ All ]'. A list of policies is shown, with 'Default Preferences' highlighted in red. Below the list, it indicates 'Page: 1 of 1', 'Rows: 3', and a 'Reload' button. The main configuration area has tabs for 'General', 'iSeries', and 'iTurret', with 'iTurret' selected and highlighted in red. The 'iTurret' section contains several settings: 'Display Language' (English), 'Inter-Digit Timeout' (3 seconds), 'Conferencing Mode' (Standard), 'Dynamic Keys Call Display' (All Calls), 'Dynamic Keys Auto-Refresh' (unchecked), 'Screen Saver Auto-Exit' (unchecked), 'Always use Large Cisco Profile' (checked), and 'Log Intercom Calls in Call Register' (checked). Below this is the 'iE801' section with 'Mute Button Ganging' (checked) and 'Group Button Ganging' (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's referred to later in these Application Notes).

The screenshot displays the Avaya Management System interface for configuring policies. At the top, there are tabs for 'Policies' and 'Devices'. Below the tabs are buttons for 'New', 'Delete', 'Apply', and 'Copy'. A 'Type' dropdown menu is set to '[ All ]'. A list of policies is shown, with 'Default RTP' highlighted in red. Below the list, there is a pagination bar showing 'Page: 1 2 of 2 Last>> Rows:11 Reload Find'. The 'Default RTP' policy configuration is shown in the 'General' tab. The 'Name' field is 'Default RTP' and the 'Type' is '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 iTurret Codec' and 'Preferred Intercom Codec' are both set to 'G.711 A-Law', and 'Voice Activity Detection' is unchecked.

Name
Default Call Logging
Default Digital E1 Trunk
Default Digital T1 Trunk
Default Ethernet Port
Default Gateway RTP
Default iCMS Connection
Default Intercom Recording
Default iTurret Ethernet Ports
Default iTurret Recording
<b>Default RTP</b>

Page: 1 2 of 2 Last>> Rows:11 Reload Find

**General**

Name: Default RTP

Type: RTP Media

RTP Media Settings:

Time To Live: 120

DSCP Value: 0

RTCP DSCP Value: 0

SIP RTP Media Settings:

Preferred iTurret Codec: G.711 A-Law

Preferred Intercom Codec: G.711 A-Law

Voice Activity Detection:

Select **Devices** → **Policies** in the left pane (not shown). Select and view the **Default SbRTP** policy (no changes should be needed to this, however it's referred to later in these Application Notes).

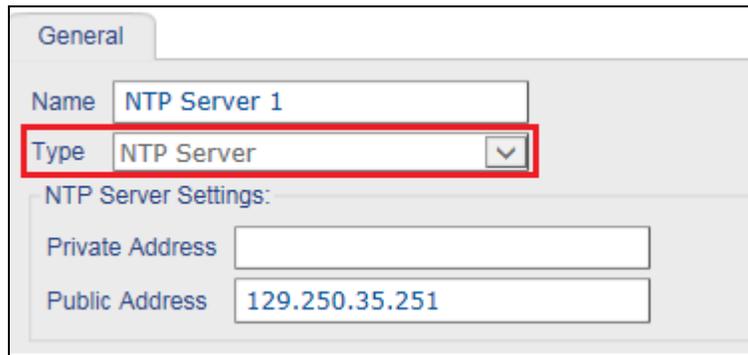
The screenshot displays a web-based configuration interface. At the top, there are two tabs: 'Policies' and 'Devices'. Below the tabs are buttons for 'New', 'Delete', 'Apply', and 'Copy'. A 'Type' dropdown menu is set to '[ All ]'. A table lists policies, with 'Default SbRTP' highlighted in a red box. Below the table is a navigation bar with 'First', 'Page: 1 2 of 2', 'Rows: 11', a 'Reload' button, a search input, and a 'Find' button.

The 'General' configuration tab is active, showing the following settings:

- Name: Default SbRTP
- Type: SbRTP Media
- SbRTP Media Settings:
  - RTP Payload Code: 96
  - Time To Live: 2
  - DSCP Value: 0
  - Bandwidth: Standard
  - Packet Size: 4 ms
  - Voice Activity Detection:
  - Lost Packet Tolerance (%): 50
  - Sample Slip Tolerance (%): 100
  - iSeries Compatibility: Version 3.0

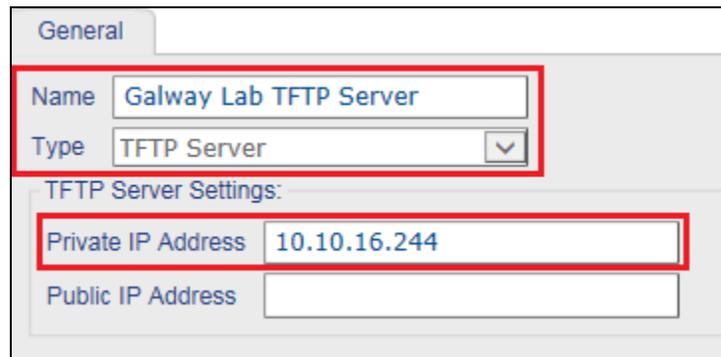
## 7.7. Create Network Services

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** (not shown), 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** (not shown) once completed, as shown below.



The screenshot shows a configuration window titled "General" for an NTP Server. The "Name" field contains "NTP Server 1". The "Type" dropdown menu is set to "NTP Server" and is highlighted with a red box. Below this, the "NTP Server Settings" section includes a "Private Address" field and a "Public Address" field containing the IP address "129.250.35.251".

Select **Network** → **Network Services** in the left pane (not shown), click on **NEW** (not shown), 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 screenshot shows a configuration window titled "General" for a TFTP Server. The "Name" field contains "Galway Lab TFTP Server" and the "Type" dropdown menu is set to "TFTP Server", both highlighted with red boxes. Below this, the "TFTP Server Settings" section includes a "Private IP Address" field containing "10.10.16.244" and an empty "Public IP Address" field, both also highlighted with red boxes.

## 7.8. Confirm Defaults

Select **System** → **Defaults** in the left pane (not shown), under the **General** tab select the **Site** and **Call Region** created above and confirm as per below.

The screenshot shows a configuration interface with several tabs: General, IP, Network, Management, Gateway, and Recording. The 'General' tab is selected and highlighted with a red box. Below the tabs, there are two sections: 'General:' and 'Firmware:'. In the 'General:' section, the 'Site' dropdown is set to 'Galway Lab' and the 'Call Region' dropdown is set to 'Avaya Galway'. Both dropdowns are highlighted with a red box. The 'iG330 Configuration Mode' dropdown is set to 'Device Web Page'. In the 'Firmware:' section, there are several text input fields for filenames: TFTP Server (set to '[ None ]'), iD100 Filename (iD100\_UG\_x\_xxx\_x\_x.r0), iD101 Filename (iD101\_UG\_x\_xxx\_x\_x.r0), iD114 Filename (iD114\_UG\_x\_xxx\_x\_x.r0), iD712 Filename (upgraders/iD712\_upgrade\_x-xxx-x-x.tar.gz.aes), SE708 Filename (upgraders/SE708\_upgrade\_x-xxx-x-x.tar.gz.aes), iTurret Filename (iD808\_upgrader\_x-xxx-x-x.sh), iG114 Filename (iG114\_UG\_x\_xxx\_x\_x.r0), iG124 Filename (iG124\_UG\_x\_xxx\_x\_x.r0), iG214 Filename (iG214\_UG\_x\_xxx\_x\_x.r0), and iG330 Filename (iG330\_upgrader\_x-xxx-x-x.sh).

Under the **Management** tab, set the **Administration Password** and confirm as per below. Click **Apply** when completed.

The screenshot shows the 'Management' tab of a configuration interface. The 'Administration Password' field is highlighted with a red box, and the 'Apply' button is also highlighted with a red box. The 'Set Administration Password...' button is visible below the password field.

## 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 below.

Name	Site	Call Region	Type	IP Address	MAC Address	Firmware	Seated User	Status
Turret 1	Default Site	Default Call Regi	iTurret	10.10.16.122	00:05:63:00:39:EC	2.700.6.0	iTurret User 1	
Turret 2	Default Site	Default Call Regi	iTurret	10.10.16.123	00:05:63:00:50:50	2.700.6.0	iTurret User 2	
Turret 3	Default Site	Default Call Regi	iTurret	10.10.16.126	00:05:63:00:1B:12	2.700.6.0	iTurret User 3	

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

The screenshot shows the 'General' tab of the iTurret configuration interface. The 'Name' field is highlighted with a red box and contains the value 'id808-000D31'. Other fields include 'Type' (iTurret), 'MAC Address' (00:05:83:00:0D:31), 'Firmware Version' (2.510.1.0), 'Site' (Galway Lab), 'Call Region' (Avaya Galway), and 'Location' (empty).

Field	Value
Name	id808-000D31
Type	iTurret
MAC Address	00:05:83:00:0D:31
Firmware Version	2.510.1.0
Site	Galway Lab
Call Region	Avaya Galway
Location	

Click the **IP** tab and enter the **IP address** of the iTurret and the **Default Gateway**.

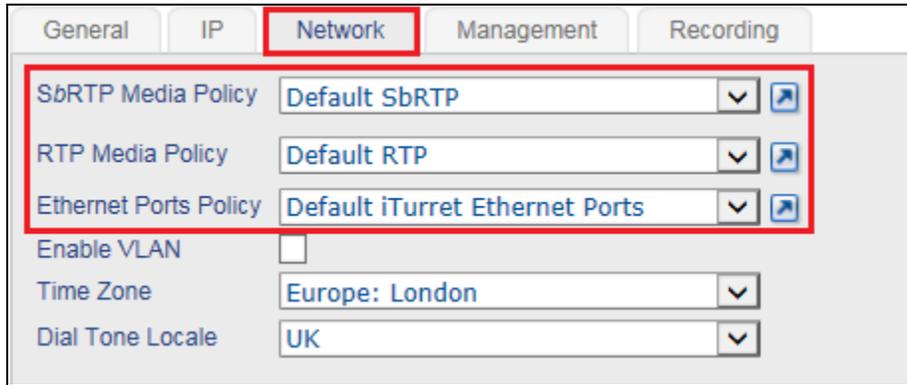
**Note:** If using DHCP check the **Obtain IP Address using DHCP** check box.

The screenshot shows the 'IP' tab of the iTurret configuration interface. The 'Obtain an IP Address using DHCP' checkbox is unchecked. The 'IP Address' field is highlighted with a red box and contains '10.10.16.241'. The 'Subnet Mask' is '255.255.255.0'. The 'Default Gateway' dropdown is highlighted with a red box and shows '10.10.16.1 (10.10.16.1)'. Other fields include 'DNS Server' ([None]), 'Backup DNS Server' ([None]), 'NTP Server' (NTP Server 1 (129.250.35.251)), 'Backup NTP Server' (NTP Server 2 (193.47.164.28)), 'Local Domain Name' (empty), and 'Local Host Name' (id808-000D31).

Field	Value
Obtain an IP Address using DHCP	<input type="checkbox"/>
IP Address	10.10.16.241
iE801 #1 IP Address	
iE801 #2 IP Address	
Subnet Mask	255.255.255.0
Default Gateway	10.10.16.1 (10.10.16.1)
DNS Server	[ None ]
Backup DNS Server	[ None ]
NTP Server	NTP Server 1 (129.250.35.251)
Backup NTP Server	NTP Server 2 (193.47.164.28)
Local Domain Name	
Local Host Name	id808-000D31

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**

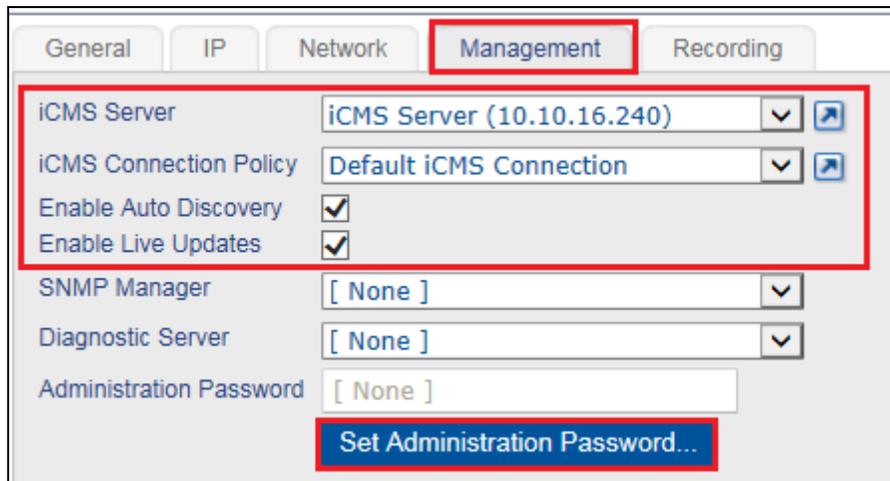


The screenshot shows the 'Network' configuration tab. The 'SbRTP Media Policy' is set to 'Default SbRTP', 'RTP Media Policy' is set to 'Default RTP', and 'Ethernet Ports Policy' is set to 'Default iTurret Ethernet Ports'. Other settings include 'Enable VLAN' (unchecked), 'Time Zone' (Europe: London), and 'Dial Tone Locale' (UK). A red box highlights the three media policy dropdown menus.

In the **Management** tab, verify or configure the following:

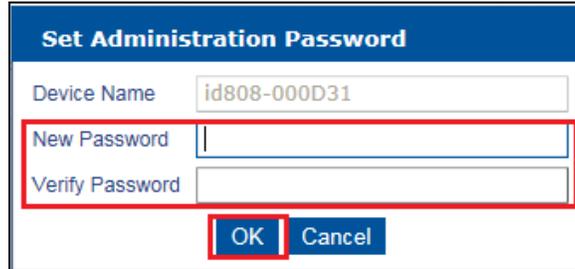
- **iCMS Server** Select the appropriate **iCMS Server** from the drop down list
- **iCMS Connection Policy** Select **Default iCMS Connection** from the drop down list
- **Enable Auto Discovery** Tick the check box
- **Enable Live Updates** Tick the check box

Click on the **Set Administration Password** button.



The screenshot shows the 'Management' configuration tab. The 'iCMS Server' is set to 'iCMS Server (10.10.16.240)', 'iCMS Connection Policy' is set to 'Default iCMS Connection', 'Enable Auto Discovery' and 'Enable Live Updates' are both checked. Other settings include 'SNMP Manager' (None), 'Diagnostic Server' (None), and 'Administration Password' (None). A red box highlights the iCMS settings, and another red box highlights the 'Set Administration Password...' button.

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



The image shows a dialog box titled "Set Administration Password". It has a blue header bar with the title. Below the header, there are three input fields: "Device Name" with the value "id808-000D31", "New Password", and "Verify Password". The "New Password" and "Verify Password" fields are highlighted with a red border. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

## 7.10. Create PBX (SIP Server)

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

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

**Note 1:** A server locator record (SRV) for the registrar address and SIP domain may be created on DNS if the registrar address is set to devconnect.local, in the example below it will not be required. Refer to the *Speakerbus iManager Administrator's Guide* [5] 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.

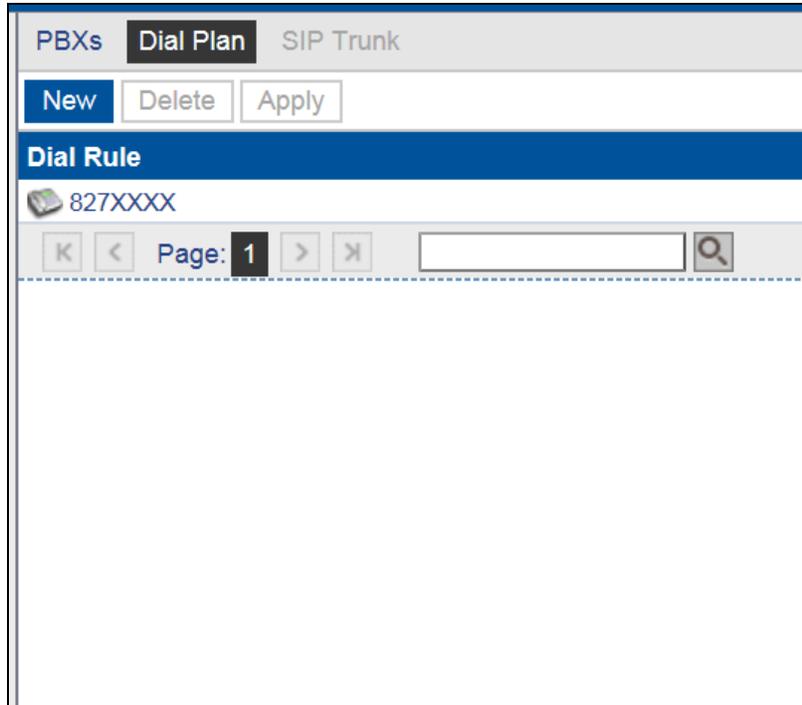
The **Outbound** and **Inbound** tabs are left with their default values, Click **OK** (not shown).



The image shows a dialog box with three tabs: "General", "Inbound", and "Outbound". The "General" tab is selected. The "Name" field contains "Avaya SM 7 SM #1". The "Type" dropdown is set to "Avaya". The "Port" field contains "5060". Below these fields is a section titled "PBX Settings". The "Registrar Address" field contains "10.10.16.77". The "SIP Domain" field contains "devconnect.local". The "Secondary PBX" dropdown is set to "Avaya SM 7 SM #2". The "Tertiary PBX" dropdown is set to "[ None ]". The "Registration Delay" field contains "30". The "Registration Timeout" field contains "30". The "Registration Attempts" field contains "3". The "Ad-Hoc Conferencing" checkbox is checked.

## 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 interface for managing dial plans. At the top, there are three tabs: "PBXs", "Dial Plan" (which is selected and highlighted in black), and "SIP Trunk". Below the tabs is a navigation bar with three buttons: "New" (highlighted in blue), "Delete", and "Apply". Underneath is a blue header bar labeled "Dial Rule". Below this header, there is a text input field containing "827XXXX" with a small icon to its left. Below the input field is a pagination bar with navigation arrows, the text "Page: 1", and a search icon. The main content area below is currently empty.

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 (not shown), click on **NEW** (not shown) select the PBX created in **Section 7.10** (in this case **Avaya 7.0 Primary**), 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** (not shown).

The screenshot shows the 'General' tab of a configuration window. At the top, there are two dropdown menus: 'PBX' with the value 'Avaya SM 7 SM #1' and 'Type' with the value 'Call'. Below these is a section titled 'Call Appearance Settings' containing several fields: 'Name' (Turret 1), 'Long Label' (Turret 1), 'Address' (8275100), 'Maximum PBX Appearances' (3), 'Outbound Calls' (Allow All), 'Message Indication' (checked), and 'Authentication Name' (8275100). A blue button labeled 'Change PBX Authentication Password...' is located at the bottom right of the form.

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** (not shown) to commit the created appearance.

The screenshot shows the 'General' tab of a configuration window. The 'PBX' dropdown is set to 'Avaya SM 7 SM #1' and the 'Type' dropdown is set to 'Privacy 1'. Below these, the 'Privacy Appearance Settings' section contains the following fields: 'Name' (iTurret User 1 PV1), 'Long Label' (iTurret User 1 PV1), 'Address' (8275200), and 'Authentication Name' (8275200). A blue button labeled 'Change PBX Authentication Password...' is located at the bottom right of the settings section.

Repeat the above procedure to add the **Privacy 2** appearance.

The screenshot shows the 'General' tab of a configuration window. The 'PBX' dropdown is set to 'Avaya SM 7 SM #1' and the 'Type' dropdown is set to 'Privacy 2'. Below these, the 'Privacy Appearance Settings' section contains the following fields: 'Name' (iTurret User 1 PV2), 'Long Label' (iTurret User 1 PV2), 'Address' (8275300), and 'Authentication Name' (8275300). A blue button labeled 'Change PBX Authentication Password...' is located at the bottom right of the settings section.

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

Name	iSeries Logon	iTurret Logon	Intercom Logon	Dial Number	Seated Device
iTurret User 1		00001001			Turret 1
iTurret User 2		00001002			Turret 2
iTurret User 3		00001003			Turret 3

### 7.13. Create Users

Select **Users** → **Users** in the left pane (not shown), click on **NEW** (not shown), 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**:

General	iSeries	iTurret	Intercom
Name	iTurret User 1		
Privileges Policy	Default Privileges		
Preferences Policy	Default Preferences		
Local Muting	Duplex		
Latching Type	Tap Latch		
Quiet Office	Disabled		
Seated at Site	Default Site		
Seated at Call Region	Default Call Region		
Seated at Device	Turret 1		
Authentication Name	MASTER-1		
<a href="#">Change PBX Authentication Password...</a>			

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

- **Voicemail Policy** Select the voicemail policy as configured in **Section 7.5**
- **Move to Idle Handset Mode** Select **Move Call** from the drop down list
- **Enable Latching** Tick **Group Button 1, 2,3 and 4**

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

General iSeries iTurret Intercom

iTurret:

Logon Name 00001000

Change Password...

Default PBX Appearance Type Call

Default PBX Appearance Avaya User 1

Voicemail Policy Avaya Voicemail

Move To Idle Handset Mode Move Call

iE801:

Group Button: 1 2 3 4

Enable Latching:

Repeat the previous steps to add more users.

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

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

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

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

Name

Avaya User 1

Avaya User 2

Avaya User 3

Page: 1 of 1 Rows: 3 Reload Find

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.

Name	iSeries Logon	iTurret Logon	Intercom Logon	Dial Number	Seated Device
iTurret User 1		00001001			Turret 1
iTurret User 2		00001002			Turret 2
iTurret User 3		00001003			Turret 3

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 list and click **OK**.

**Seat User at Device**

User to seat: Avaya User 1

Filter by Site: Avaya Galway Labs

Filter by Region: Galway Call Region

Filter by Device Type: iTurret

Show only free deskstations:

Device to seat at: id808-000D31

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					
<a href="#">New</a> <a href="#">Delete</a> <a href="#">Apply</a> <a href="#">Seat...</a> <a href="#">Unseat</a> <a href="#">New Users...</a> <a href="#">Apply Template...</a> <a href="#">New Template...</a> <a href="#">Synchronise</a>					
Group	[ All ]	Partition	[ All ]	Site	[ All ]
Call Region	[ All ]				
Name	iSeries Logon	iTurret Logon	Intercom Logon	Dial Number	Seated Device
Avaya User 1		00001000			id808-000D31
Avaya User 2		00001001			id808-0010B5
Avaya User 3		00001002			id808-0012FC

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					
<a href="#">User Permissions</a> <a href="#">Group Permissions</a>					
<a href="#">Apply</a>					
Group	[ All ]	Partition	[ All ]	Site	[ All ]
Call Region	[ All ]	Permission	[ All ]	Type	[ All ]
Name	User Permission	Group Permission	Seated Site	Seated Call Region	Seated Device
Avaya User 1	Allow		Galway Lab	Avaya Gateway	id808-000D31
Avaya User 2	Allow		Galway Lab	Avaya Gateway	id808-0010B5
Avaya User 3	Allow		Galway Lab	Avaya Gateway	id808-0012FC

Page: 1 of 1 Rows: 3 [Reload](#)  [Find](#)

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

PBX Appearances					
<a href="#">User Permissions</a> <a href="#">Group Permissions</a>					
<a href="#">Apply</a>					
Group	[ All ]	Partition	[ All ]	Site	[ All ]
Call Region	[ All ]	Permission	[ All ]	Type	[ All ]
Name	User Permission	Group Permission	Seated Site	Seated Call Region	Seated Device
Avaya User 1	Allow		Galway Lab	Avaya Gateway	id808-000D31
Avaya User 2	Allow		Galway Lab	Avaya Gateway	id808-0010B5
Avaya User 3	Allow		Galway Lab	Avaya Gateway	id808-0012FC

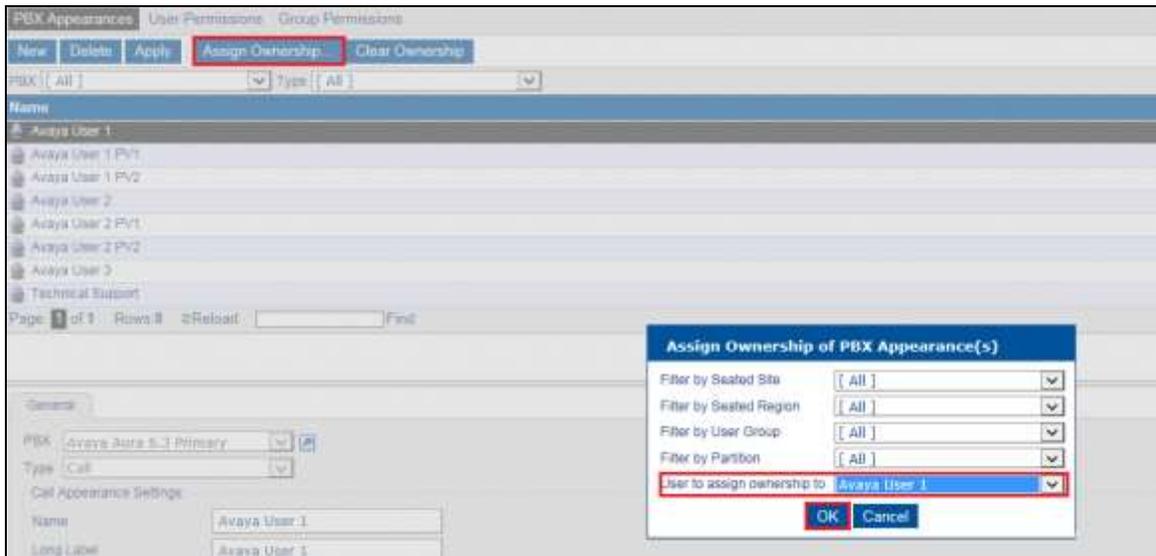
Page: 1 of 1 Rows: 3 [Reload](#)  [Find](#)

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, and click on the **Assign Ownership** button. Filter accordingly and select the user from the **User to assign ownership to** drop down list. Click **OK**.

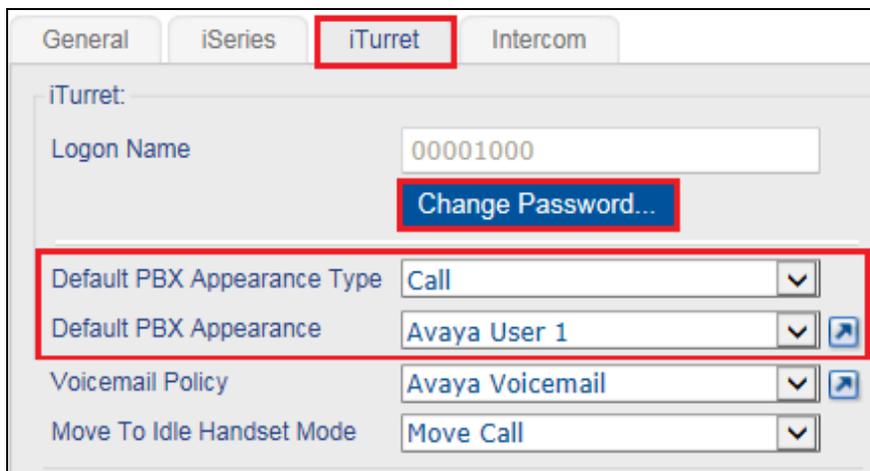


## 7.16. Set Default Appearance

Select **Users** → **Users** in the left pane (not shown), select the user you've created (not shown), within the **iTurret** tab fill in the following:

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

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



## 7.17. Program iTurret Layout Profiles

The programming of the iTurret Deskstations can be carried out by Speakerbus or Avaya engineer. If you need any information on the types of keys available and administration of the iTurret layout, refer to the *Speakerbus iManager Administrator's Guide* [5].

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

The screenshot shows the Avaya iManager Users page. The 'iTurret Layout' tab is selected and highlighted with a red box. Below the user list, the configuration for a user is shown with the following fields:

Name	iSeries Logon	iTurret Logon	Intercom Logon	Dial Number	Seated Device
Avaya User 1		12345900			
Avaya User 2		12345801			
Avaya User 3		12345802			
Colin Home		colinhome			CW 808 Home
Neil 1	newuser2		0008		Neil Desk 2
Neil 10	newuser2		0001		id805-0010B7
Neil 11	newuser3		0002		id805-0010BE
Neil 12	newuser4		0003		id805-0010F6
Neil 13	newuser13		0012		id805-0010FC
Neil 14	newuser14		0013		id805-0010FE
Neil 15	newuser15		0014		id805-0012F4
Neil 16	newuser16		0015		id805-0014B3
Neil 17	newuser17		0016		id805-0014BD
Neil 18	newuser18		0017		id805-0014BF
Neil 2	newuser10		0009		Neil Desk 3
Neil 3	newuser11		0010		Neil Home

The configuration panel for the iTurret tab includes the following settings:

- Logon Name: 12345900
- Change Password: [button]
- Default PBX Appearance Type: [None]
- Default PBX Appearance: [None]
- Vocemail Policy: Avaya CMH
- Move To Idle Handset Mode: Move Call
- Group Buttons: 1 2 3 4
- Enable Latching: [checked] [checked] [checked] [checked]

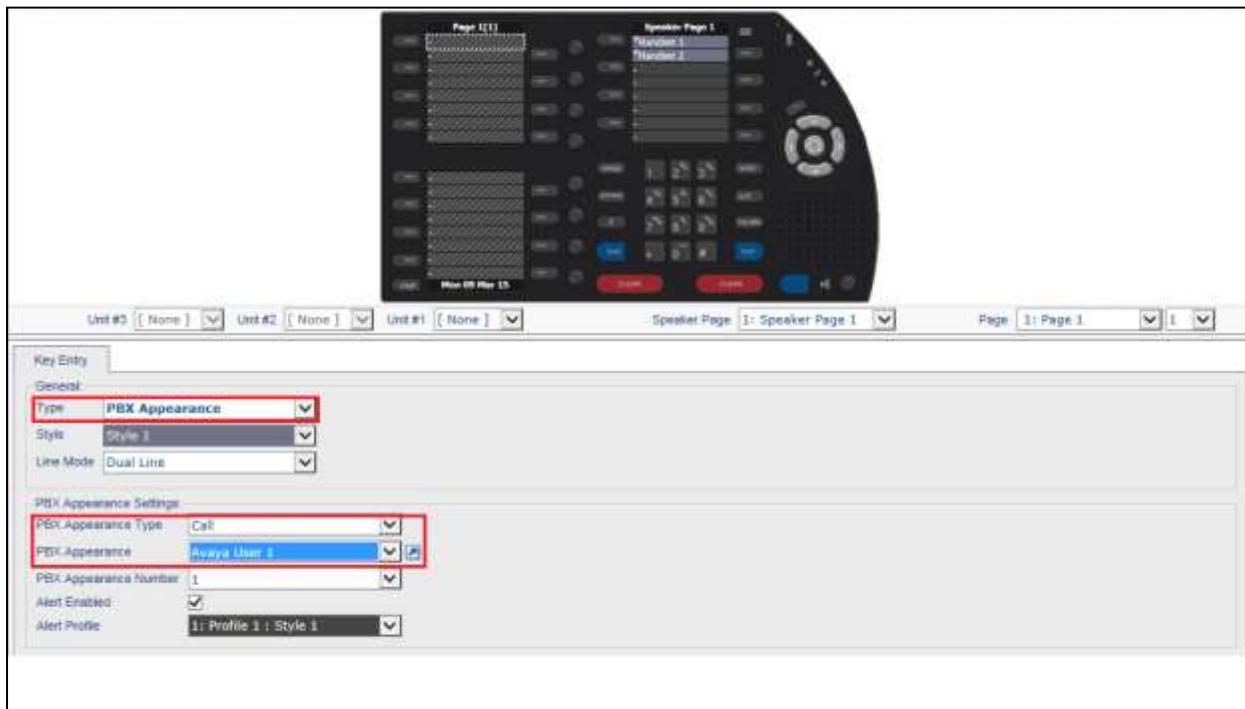
When selected the following layout is displayed for a blank iTurret profile with **\*Handset 1** and **\*Handset 2** configured.



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

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

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



Once done the layout will look as follows.



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



### 7.17.1. Add bridged appearances

To add bridged appearances repeat **Section 7.17** and enter the following:

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

Click the **OK** button (not shown). Repeat this step three times.

The example below shows Avaya User 2 three times.



### 7.17.2. Add dynamic keys

Add three dynamic keys under the **handset 2 key** in the iTurret Layout using the procedure in **Section 7.17**, select the next available key under **\*Handset 2** key and select **Dynamic** from the **Type** drop down box. The remaining fields are left at default. Click the **OK** button. Repeat this step three times.

The example below shows the three dynamic keys added.



### 7.17.3. Add Do Not Disturb key

To add a single function key for **Do Not Disturb**, in the iTurret Layout, using the procedure in **Section 7.17**, select the next available key under the last **Dynamic** key and enter the following:

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

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



#### 7.17.4. Add soft function keys

To add two soft function keys, in the iTurret Layout, using the procedure in **Section 7.17**, select the next available key under the Do Not Disturb key and enter the following:

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

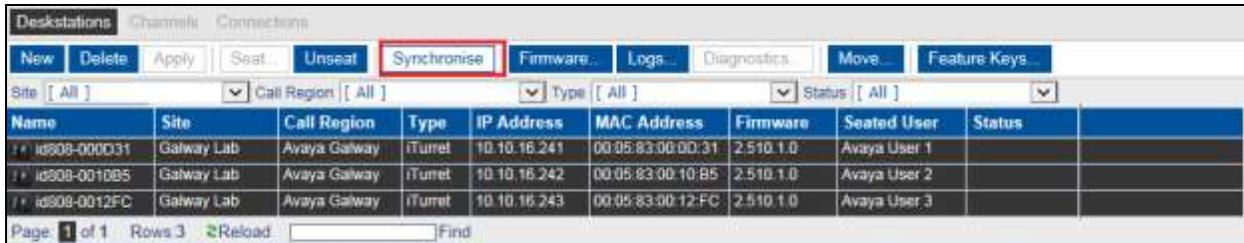
Click the **OK** button. Repeat this step two times. Once done the layout will look as below.



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

## 7.18. 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.



The screenshot shows the iManager interface for Deskstations. At the top, there are tabs for 'Deskstations', 'Channels', and 'Connections'. Below the tabs is a toolbar with buttons: 'New', 'Delete', 'Apply', 'Seat', 'Unseat', 'Synchronise' (highlighted with a red box), 'Firmware...', 'Logs...', 'Diagnostics', 'Move...', and 'Feature Keys...'. Below the toolbar are filters for 'Site [ All ]', 'Call Region [ All ]', 'Type [ All ]', and 'Status [ All ]'. The main area contains a table with the following data:

Name	Site	Call Region	Type	IP Address	MAC Address	Firmware	Seated User	Status
7F id908-000D31	Galway Lab	Avaya Galway	iTurret	10.10.16.241	00:05:83:00:00:31	2.510.1.0	Avaya User 1	
7F id908-0010B5	Galway Lab	Avaya Galway	iTurret	10.10.16.242	00:05:83:00:10:B5	2.510.1.0	Avaya User 2	
7F id908-0012FC	Galway Lab	Avaya Galway	iTurret	10.10.16.243	00:05:83:00:12:FC	2.510.1.0	Avaya User 3	

At the bottom of the table, there is a footer: 'Page 1 of 1 Rows 3 Reload Find'.

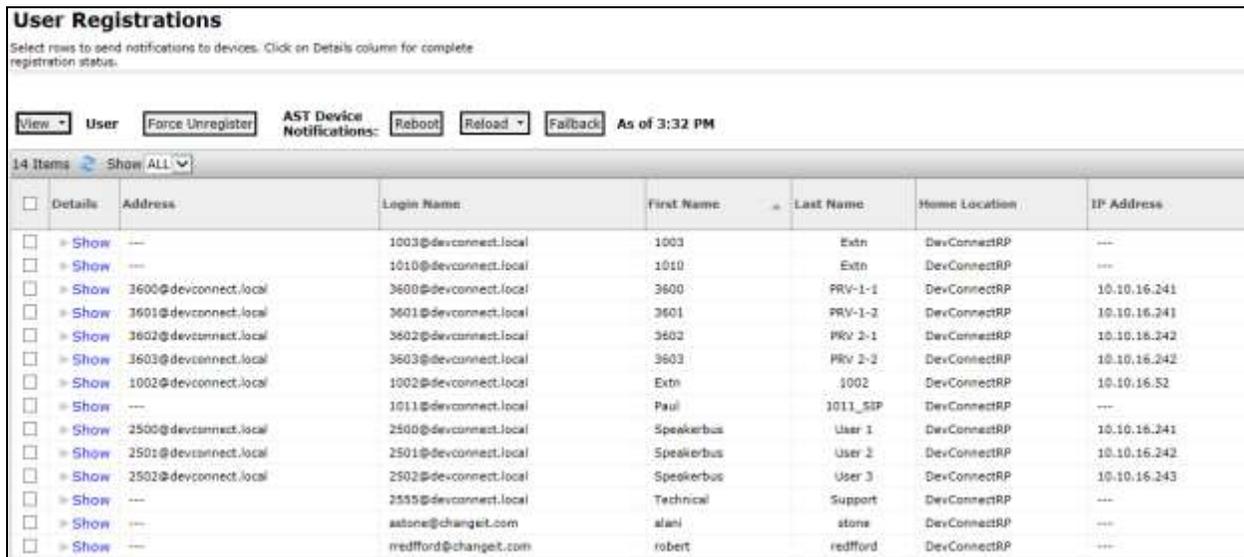
**Note:** Any changes that are made to the profile within iManager will be updated on the iTurret device after **OK** or **Apply** is pressed. However, some changes will require a synchronization. Refer to the *Speakerbus iManager Administrator's Guide* for more details.

## 8. Verification Steps

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

### 8.1. Verify iTurret registration with Avaya Aura® Session Manager

To verify that the iTurret have successfully registered with Session Manager, from the System Manager Web interface click **Session Manager** → **System Status** → **User Registrations**. This will display a summary of registered stations on each Session Manager as shown below. Any stations that are correctly registered will display a valid IP address such as those shown for extensions **2500, 2501** and **2502**.



<input type="checkbox"/>	Details	Address	Login Name	First Name	Last Name	Home Location	IP Address
<input type="checkbox"/>	Show	---	1003@devconnect.local	1003	Extn	DevConnectRP	---
<input type="checkbox"/>	Show	---	1010@devconnect.local	1010	Extn	DevConnectRP	---
<input type="checkbox"/>	Show	3600@devconnect.local	3600@devconnect.local	3600	PRV-1-1	DevConnectRP	10.10.16.241
<input type="checkbox"/>	Show	3601@devconnect.local	3601@devconnect.local	3601	PRV-1-2	DevConnectRP	10.10.16.241
<input type="checkbox"/>	Show	3602@devconnect.local	3602@devconnect.local	3602	PRV-2-1	DevConnectRP	10.10.16.242
<input type="checkbox"/>	Show	3603@devconnect.local	3603@devconnect.local	3603	PRV-2-2	DevConnectRP	10.10.16.242
<input type="checkbox"/>	Show	1002@devconnect.local	1002@devconnect.local	Extn	1002	DevConnectRP	10.10.16.52
<input type="checkbox"/>	Show	---	1011@devconnect.local	Paul	1011_SIP	DevConnectRP	---
<input type="checkbox"/>	Show	2500@devconnect.local	2500@devconnect.local	Speakerbus	User 1	DevConnectRP	10.10.16.241
<input type="checkbox"/>	Show	2501@devconnect.local	2501@devconnect.local	Speakerbus	User 2	DevConnectRP	10.10.16.242
<input type="checkbox"/>	Show	2502@devconnect.local	2502@devconnect.local	Speakerbus	User 3	DevConnectRP	10.10.16.243
<input type="checkbox"/>	Show	---	2555@devconnect.local	Technical	Support	DevConnectRP	---
<input type="checkbox"/>	Show	---	astone@changeit.com	aloni	stone	DevConnectRP	---
<input type="checkbox"/>	Show	---	redfford@changeit.com	robert	redfford	DevConnectRP	---

### 8.2. Verify iTurret status

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

## 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, Release 7.0, August 2015, Document Number 03-300509, Issue 1.*
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 7.0, August 2015, Document Number 555-245-205, Issue 1.*
- [3] *Administering Avaya Aura® Session Manager, Release 7.0, Issue 1 August 2015*
- [4] *Administering Avaya Aura® System Manager, Release 7.0, Issue 1, August, 2015*
- [5] *Speakerbus Administrator's Guide iManager PN AGiCMS V3.1, Revision 21, January 2016*

Product Documentation for Speakerbus can be requested from [info@speakerbus.com](mailto:info@speakerbus.com)

---

**©2016 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).