Avaya Solution & Interoperability Test Lab

Application Notes for Speakerbus iD808 iTurret with Avaya Aura® Communication Manager R5.2.1 and Avaya Aura® SIP Enablement Services R5.2.1 – Issue 1.0

Abstract

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

The following table provides a summary of the supported features available on the Speakerbus iD808 iTurret with the Avaya SIP offer. Some features are supported locally in the Speakerbus iD808 iTurret, while others are only available with Avaya Aura® Communication Manager and Avaya Aura® SIP Enablement Services with OPS. In addition to basic calling capabilities, the Internet Engineering Task Force (IETF) has defined a supplementary set of calling features, often referred to as the SIPPING-19 **[6]**. This provides a useful framework to describe product capabilities and compare features supported by various equipment vendors. Additional features beyond the SIPPING-19 can be extended to the Speakerbus iD808 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 the Speakerbus iD808 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/Class Of Restriction (COS/COR), and voice messaging. Details on operation and administration of OPS can be found in References **[2]** and **[3]**. The Avaya SIP solution requires all SIP telephones to be configured in Avaya Aura® Communication Manager as OPS. Items in the table below shown in **bold** were tested using an 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 (3rd party added)	YES	YES	
3-way conferencing (3rd 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 1706/1707**
Call Pickup	**NO**	**YES**	**Via OPS FNE 1708**
Automatic Redial	NO	YES	Via OPS FNE n/a
OPS – Selected Additional Station-Side Features			
Conference on answer	NO	YES	Via OPS FNE 1714
Directed call pickup	**NO**	**YES**	**Via OPS FNE 1715**
Drop last added party	NO	YES	Via OPS FNE 1716
Exclusion/Privacy	**YES**	**YES**	**Local hard key on iTurret using FNU**
Last number dialed	**YES**	**YES**	**Via OPS FNE 1720**
Priority Call	NO	YES	Via OPS FNE 1725,the iD808 iTurret doesn`t support distinctive ring indication
Send All Calls	**NO**	**YES**	**Via OPS FNE 1727**
Send All Calls Cancel	**NO**	**YES**	**Via OPS FNE 1728**
Transfer to Voicemail	NO	YES	Via OPS FNE 1731
Whisper Page	**NO**	**YES**	**Via OPS FNE 1732**

2. General Test Approach and Test Results

To verify interoperability of the iD808 iTurret with Communication Manager and SIP Enablement Services, calls were made between the iD808 iTurret 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 the iD808 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 the iD808 iTurret with SIP Enablement Services
- Calls between the iD808 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 iD808 iTurret restart and loss of IP connection
- Proper failover to alternate SIP Enablement Services

2.2. Test Results

All tests were executed succesfully.

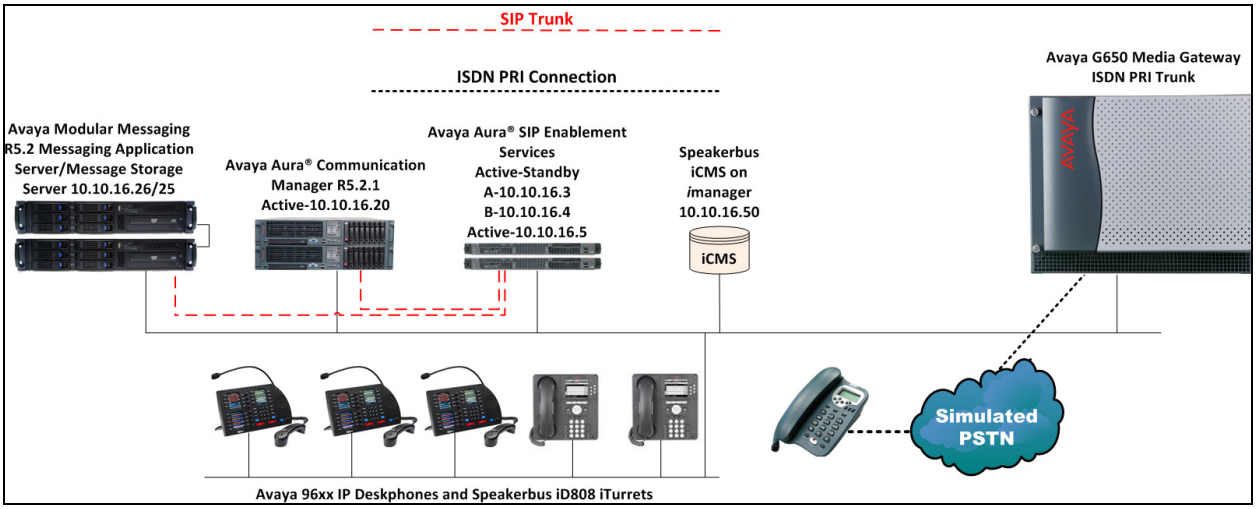
2.3. Support

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

- Web: http://www.speakerbus.com
- Email: info@speakerbus.com
- Telephone: (646) 289-4700 in North America
  +44 (0) 870 240 7252 in Europe
  +65 6222 4577 in Asia

3. Reference Configuration

An S8730 Server pair running Communication Manager R5.2.1 serving H.323 endpoints with a G650 Media Gateway was configured along with SIP Enablement Services R5.2.1 hosted on an S8500 Server pair providing SIP endpoints. The iD808 iTurret was connected to the LAN and managed by the Speakerbus iManager application running on a local Windows server. Simulated connection to the PSTN was provided by an E1 QSIG trunk connected to the G650 Media Gateway. Modular Messaging provided voicemail.



Avaya Aura® Communication Manager and Avaya Aura® SIP Enablement Services with the Speakerbus iD808 iTurret 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 S8730 Server Pair	R5.2.1 SP14 build R015x.02.1.016.4-20102
Avaya Aura® SIP Enablement Services running on Avaya S8500 Server Pair	R5.2.1 SP3b
Avaya Modular Messaging running on S3500 Servers	5.2 Patch 8 MAS - 9.2.150.13
Avaya 9630 IP Deskphone	• H323 S3.105S • SIP 2.6.8.4
Speakerbus iCMS with iManager Administration running on Windows Server	v2.100
Speakerbus iD808 iTurret	v2.1/ v1.40 SIP revision

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring the iD808 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 SIP Enablement Services. Unless otherwise stated, administration of Communication manager is performed using the System Access Terminal (SAT) to configure Communication Manager.

5.1. Define System Features

Enter 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. On **Page 17,** set the **Whisper Page Tone Given To** field to **all**

```
change system-parameters features                                Page  17 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

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

WHISPER PAGE
   Whisper Page Tone Given To: all

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

                               Pickup On Transfer? y
```

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

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

IP PARAMETERS

                   Direct IP-IP Audio Connections? y
                             IP Audio Hairpinning? y

              SDP Capability Negotiation for SRTP? n
CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 4
                   Call Pickup on Intercom Calls? y     Call Pickup Alerting? n
     Temporary Bridged Appearance on Call Pickup? y   Directed Call Pickup? y
                      Extended Group Call Pickup: none
                   Enhanced Call Pickup Alerting? n


                        Display Information With Bridged Call? n
  Keep Bridged Information on Multiline Displays During Calls? y
                  PIN Checking for Private Calls? n
```

5.2. 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 FAC must also be specified for the corresponding feature. In the sample configuration, telephone extensions and FNEs are four digits long begin with **1** and the FACs have formats as indicated with a **Call Type** of **fac**.

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

       Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
       String   Length Type    String   Length Type     String   Length Type
     0            1    ext
     1            4    ext
     5            3    dac
     *            3    fac
     #            3    fac
```

5.3. Define Feature Access Codes (FACs)

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

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

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

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

```
change feature-access-codes                                      Page   3 of   9
                                FEATURE ACCESS CODE (FAC)
            Leave Word Calling Send A Message:
           Leave Word Calling Cancel A Message:
   Limit Number of Concurrent Calls Activation:        Deactivation:
             Malicious Call Trace Activation:        Deactivation:
         Meet-me Conference Access Code Change:
          Message Sequence Trace (MST) Disable:

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

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

```
change feature-access-codes                                      Page   4 of   9
                                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: *50  Separation Code:
                  Transfer to Voice Mail Access Code: *32
                Trunk Answer Any Station Access Code:
                    User Control Restrict Activation:      Deactivation:
        Voice Coverage Message Retrieval Access Code:
       Voice Principal Message Retrieval Access Code:
                 Whisper Page Activation Access Code: *33
           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: SpeakerBus FNEs

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

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

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

5.5. Configure Class of Service (COS)

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

```
change cos                                                  Page   1 of   2
CLASS OF SERVICE

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

5.6. 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 iD808 iTurrets were assigned to COR **1**.

```
change cor 1                                                    Page   1 of  23
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description: Default

                      FRL: 0                                 APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
 Partitioned Group Number: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: all        Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7
         Send ANI for MFE? n             Add/Remove Agent Skills? n
            MF ANI Prefix:              Automatic Charge Display? y
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? y
                        Can Be Picked Up By Directed Call Pickup? y
                                   Can Use Directed Call Pickup? y
                                   Group Controlled Restriction: inactive
```

5.7. Configure SIP Trunk to SIP Enablement Services

These Application Notes assume that a SIP trunk has been configured and the relevant call routing between Communication Manager and SIP Enablement Services is in place. The configuration can be verified as follows. Enter the **change node-names ip** command and note the IP address assigned to the C-LAN and SIP Enablement Services Active Server IP Node Names.

```
change node-names ip                                            Page   1 of   2
                                    IP NODE NAMES
    Name              IP Address
CLAN1               10.10.16.23
Gateway             10.10.16.1
MedPro1             10.10.16.24
default             0.0.0.0
procr               10.10.16.20
sesactive           10.10.16.5
```

Enter the **add signaling-group 6** command, where signaling group 6 is the first available SIP signaling group. The following are configured:

- **Group Type** – set to **SIP**
- **Transport Method** – configure as **TCP**
- **Near-end Node Name** – enter the **CLAN** node name
- **Far-end Node Name** – enter the **sesactive** node name
- **Near-end Listen Port** and **Far-end Listen Port** – by default for TCP this is **5060**
- **Far-end Network Region** – set to the relevant IP Network Region, in this case **1**

```
add signaling-group 6                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 6              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n
     IP Video? n

   Near-end Node Name: CLAN1                 Far-end Node Name: sesactive
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1
Far-end Domain:

                                          Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate               RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                  IP Audio Hairpinning? n
         Enable Layer 3 Test? n                 Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n         Alternate Route Timer(sec): 6
```

Enter the **add trunk-group 6** command, where trunk-group 6 is the trunk group between Communication Manager and SIP Enablement Services. 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 **tie**
- **Signaling Group** – configure with the signaling group to the SIP Enablement Services Active address
- **Number of Members** – configure as required, in this case **10**

```
change trunk-group 6                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 6                    Group Type: sip           CDR Reports: y
  Group Name: SES OPS                     COR: 1        TN: 1        TAC: 506
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                      Signaling Group: 6
                                                    Number of Members: 10
```

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

```
add trunk-group 6                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                     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 **change route-pattern 11** command, where route pattern 11 is used to route calls between Communication Manager and SIP Enablement Services. Enter an identifying **Pattern Name** and ensure that enter the SIP trunk-groups number is configured in the **Grp No** field, enter an **FRL** as appropriate.

```
change route-pattern 11                                        Page   1 of   3
                    Pattern Number: 11  Pattern Name: to ses sip
                              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: 6    0                                                            n   user
 2:                                                                   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
```

5.9. Configure IP-Codec Set

Enter the **change ip-codec-set 1** command 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.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 **1**
- **Trk Grp** – enter the SIP trunk group configured above, in this case **6**
- **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              6                           4     Total Administered: 1
                                                        Maximum Entries: 540
```

5.11. Add Stations

The 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.

5.11.1. Main Appearance Station

Use the **add station** command to add a station for each iD808 iTurret to be supported. To configure the main appearance, on **Page 1** use **9630** for the station **Type** and include the **Coverage Path** for voice messaging, if applicable. Use the **COS** and **COR** values administered in **Sections 5.5** and **5.6**, respectively. Enter a descriptive name in the **Name** field. Use the default values for the all other fields.

```
add station 1031                                          Page   1 of   5
                                     STATION

Extension: 1031                         Lock Messages? n               BCC: 0
     Type: 9630                         Security Code: 123456           TN: 1
     Port: S00010                     Coverage Path 1: 89              COR: 1
     Name: iTurret 1                  Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 1031
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? n
```

On **Page 2**, if this iD808 iTurret will have a bridged appearance for another telephone (see **Page 4** for this station), then **Bridged Call Alerting** should be set to **y**, so that this iD808 iTurret will ring when the other telephone is called. Set the **MWI Served User Type** field to the appropriate value to allow message waiting indication to be sent to the iD808 iTurret. Use the default values for the all other fields.
Note: By default, the **Restrict Last Appearance** field to is set to **y** to reserve the last call appearance for outgoing calls from the iD808 iTurret, this should not be altered.

```
add station 1031                                          Page   2 of   5
                                 STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                       Coverage Msg Retrieval? y
  LWC Log External Calls? n                                 Auto Answer: none
             CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n                  Bridged Idle Line Preference? n
   Bridged Call Alerting? y                      Restrict Last Appearance? y
  Active Station Ringing: single
                                                         EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number? y
       Service Link Mode: as-needed                     EC500 State: enabled
         Multimedia Mode: enhanced
    MWI Served User Type: qsig-mwi              Display Client Redirection? n
                                              Select Last Used Appearance? n
                                                Coverage After Forwarding? s
                                                  Multimedia Early Answer? N
                                              Direct IP-IP Audio Connections? y
  Emergency Location Ext: 1031          Always Use? n IP Audio Hairpinning? n
     Precedence Call Waiting? y
```

On **Page 4** under the heading **BUTTON ASSIGNMENTS**, fill in the number of call appearances that are to be supported for the iD808 iTurret. In this example, the first station for the iD808 iTurret was configured with four call appearances. Locally, the iD808 iTurret will actually be configured with 3 call appearances since the last appearance is restricted as configured on **Page 2**. Multiple bridged line appearances are configured for this example station. Button assignments **5** and **6** relate to the second and third stations corresponding to two stations that will be used as the privacy handsets at the iD808 iTurret.
Note: These stations are configured in **Section 5.11.2** and these bridged appearance buttons cannot be configured until those stations have been added. If privacy is not needed for the iD808 iTurret, then these bridged appearances are not required.

```
add station 1031                                              Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                       Cord Length: 0
   Building:                                         Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:



BUTTON ASSIGNMENTS
 1: call-appr                            5: brdg-appr  B:1  E:1041
 2: call-appr                            6: brdg-appr  B:1  E:1051
 3: call-appr                            7: brdg-appr  B:1  E:1033
 4: call-appr                            8: brdg-appr  B:2  E:1033

    voice-mail Number:
```

Continue on **Page 5** under the **BUTTON ASSIGNMENTS** section, enter the function button names (shown in bold) for OPS FNEs that will be used at the iD808 iTurret. Configure function buttons **call-fwd, cfwd-bsyda,** and if required, **auto-cback** and **no-hld-cnf.**

```
add station 1031                                              Page   5 of   5
                                     STATION

BUTTON ASSIGNMENTS

 9: brdg-appr  B:3  E:1033
10: brdg-appr  B:1  E:1305
11: brdg-appr  B:2  E:1305
12: brdg-appr  B:3  E:1305
13: auto-cback
14: no-hld-cnf
15: cfwd-bsyda Ext:
16: call-fwd   Ext:
17:
18:
19:
20:
```

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

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

5.11.2. Privacy Handset Stations

Use the **add station** command to add a station for each privacy handset. On **Page 1,** use **9630** for the station **Type**. A coverage path is not required for this station. Use the **COS** and **COR** values administered in **Sections 5.5**and **5.6**, respectively. Enter a descriptive name in the **Name** field. Use the default values for the all other fields.

```
add station 1041                                                Page   1 of   5
                                      STATION

Extension: 1041                          Lock Messages? n               BCC: 0
     Type: 9630                          Security Code:                  TN: 1
     Port: S00013                      Coverage Path 1:                 COR: 1
     Name: HS1 of 1031                 Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 1041
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? n

                                                        IP Video? n


                                              Customizable Labels? y

                                              Customizable Labels? y
```

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

```
add station 1041                                          Page   2 of   5
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                         Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: none
             CDR Privacy? n                                Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? y                       Restrict Last Appearance? y
  Active Station Ringing: single
                                                          EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                     EC500 State: enabled
         Multimedia Mode: enhanced
    MWI Served User Type:                        Display Client Redirection? n
             AUDIX Name:                        Select Last Used Appearance? n
                                                  Coverage After Forwarding? s
                                                    Multimedia Early Answer? n
                                               Direct IP-IP Audio Connections? y
  Emergency Location Ext: 1041          Always Use? n IP Audio Hairpinning? n
     Precedence Call Waiting? y
```

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

```
add station 1041                                          Page   4 of   5
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                      Cord Length: 0
   Building:                                        Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:


BUTTON ASSIGNMENTS
 1: call-appr                          5: brdg-appr  B:3  E:1031
 2: exclusion                          6: brdg-appr  B:1  E:1033
 3: brdg-appr  B:1  E:1031             7: brdg-appr  B:2  E:1033
 4: brdg-appr  B:2  E:1031             8: brdg-appr  B:3  E:1033

    voice-mail Number:
```

Below is the configuration of the third station for handset 2. Use the **add station** command to add a station for each privacy handset. On **Page 1** use **9630** for the station **Type**. A coverage path is not required for this station. Use the **COS** and **COR** values administered in **Sections 5.5** and **5.6**, respectively. Enter a descriptive name in the **Name** field. Use the default values for the all other fields.

```
add station 1051                                          Page   1 of   5
                                     STATION

Extension: 1051                         Lock Messages? n               BCC: 0
     Type: 9630                         Security Code:                  TN: 1
     Port: S00014                     Coverage Path 1:                 COR: 1
     Name: HS2 of 1031                Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                              Message Lamp Ext: 1051
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                                         IP Video? n


                                               Customizable Labels? y
```

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

```
Add station 1051                                          Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer: none
             CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? y                       Restrict Last Appearance? y
  Active Station Ringing: single
                                                         EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                     EC500 State: enabled
         Multimedia Mode: enhanced
    MWI Served User Type:                        Display Client Redirection? n
             AUDIX Name:                        Select Last Used Appearance? n
                                                  Coverage After Forwarding? s
                                                    Multimedia Early Answer? n
                                               Direct IP-IP Audio Connections? y
  Emergency Location Ext: 1051          Always Use? n IP Audio Hairpinning? n
     Precedence Call Waiting? y
```

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

```
add station 1051                                          Page   4 of   5
                                   STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                      Cord Length: 0
   Building:                                        Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                            5: brdg-appr  B:3  E:1031
 2: exclusion                            6: brdg-appr  B:1  E:1033
 3: brdg-appr  B:1  E:1031               7: brdg-appr  B:2  E:1033
 4: brdg-appr  B:2  E:1031               8: brdg-appr  B:3  E:1033

    voice-mail Number:
```

Note: If a bridged appearance is required for another iD808 iTurret or telephone, a bridged appearance button must be added to all three stations corresponding to the iD808 iTurret device.

5.12. Administer Off PBX Station Mapping

Use the **change off-pbx-telephone station-mapping** command to map the Communication Manager extensions (1031, 1041, and 1051) to the extension defined on SIP Enablement Services for the corresponding SIP user configured in **Section 6.5**. Enter the field values shown. For the sample configuration, the **Trunk Selection** value indicates the SIP trunk group between Communication Manager and SIP Enablement Services. The **Trunk Selection** value relates to the SIP trunk-group configured in **Section 5.7**. The **Configuration Set** value can reference a set that has the default settings.

```
change off-pbx-telephone station-mapping 1031                    Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                    Selection   Set     Mode
 1031             OPS          -     1031             6          1
 1041             OPS          -     1041             6          1
 1051             OPS          -     1051             6          1
```

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

```
change off-pbx-telephone station-mapping 1301                    Page   2 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Appl    Call        Mapping    Calls       Bridged       Location
 Extension     Name    Limit       Mode       Allowed     Calls
 1031          OPS      10        both        all         none
 1041          OPS      10        both        all         none
 1051          OPS      10        both        all         none
```

6. Configure Avaya Aura® SIP Enablement Services

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

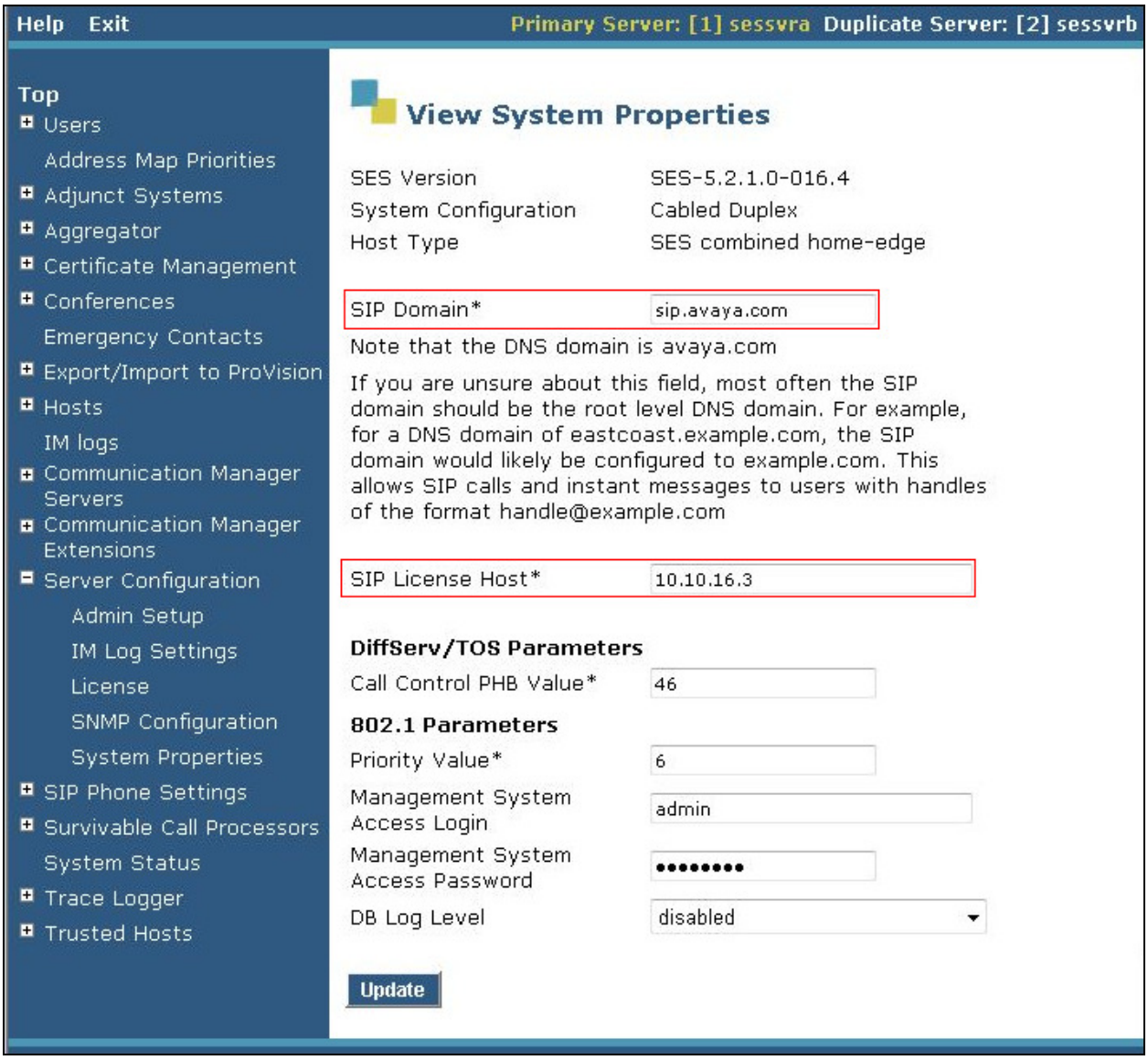
6.1. Logging in to Avaya Aura® SIP Enablement Services

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

6.2. Verify System Properties

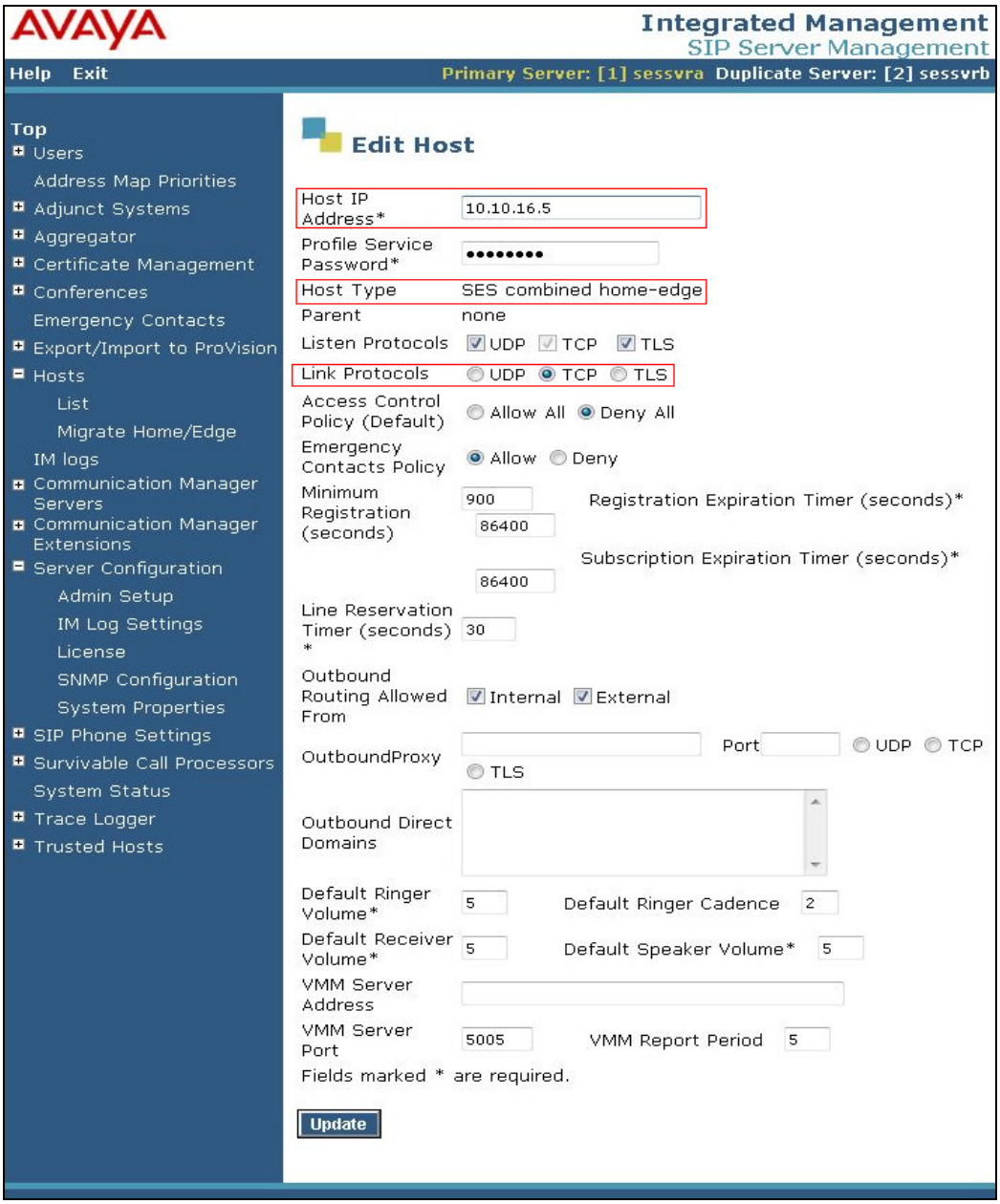
From the left pane of the Administration web interface, expand the **Server Configuration** option and select **System Properties**. In the **System Properties** screen, enter the **SIP Domain** name assigned to the Avaya SIP-based network. For the **SIP License Host** field, enter the fully qualified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

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



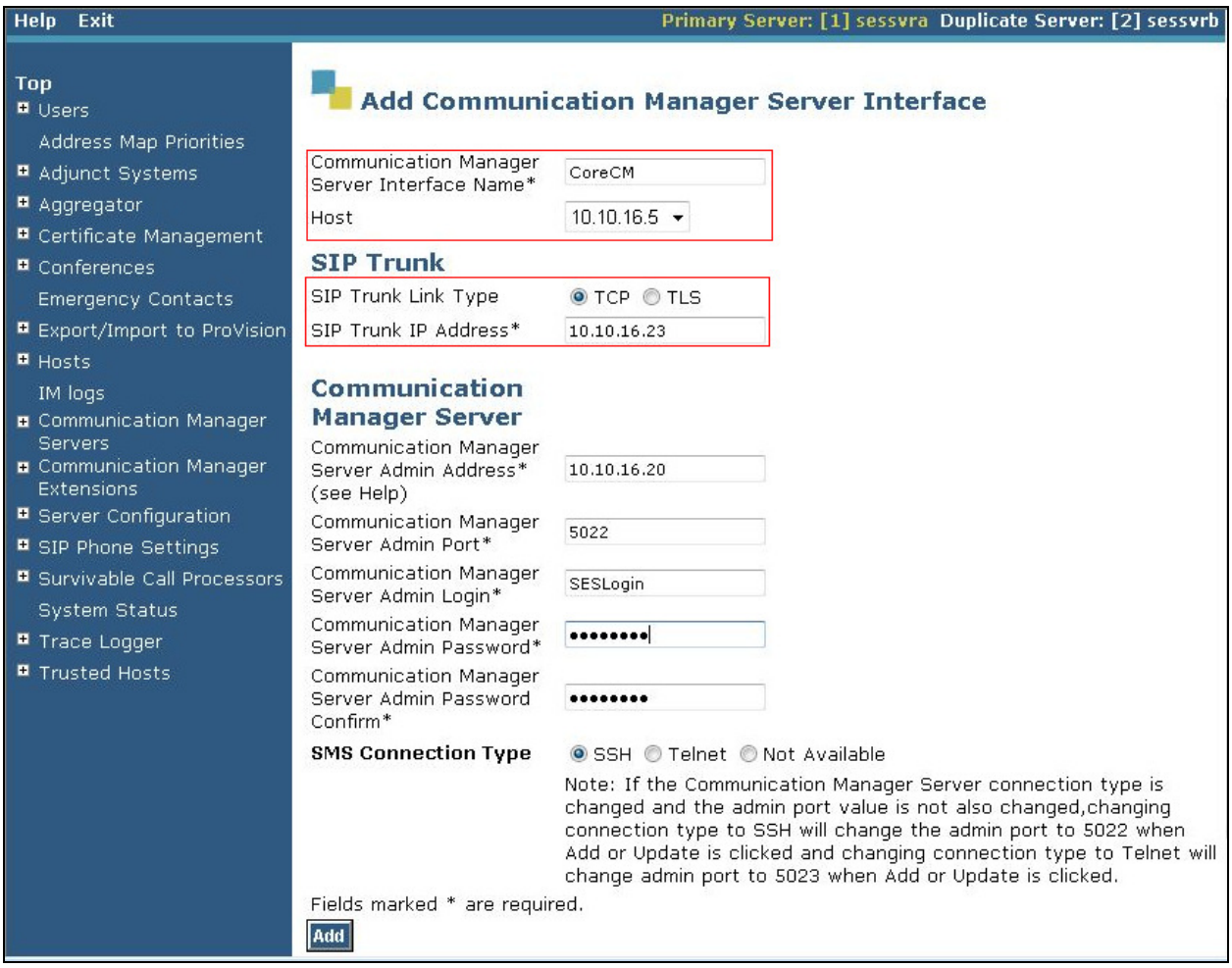
6.3. Create a Host

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



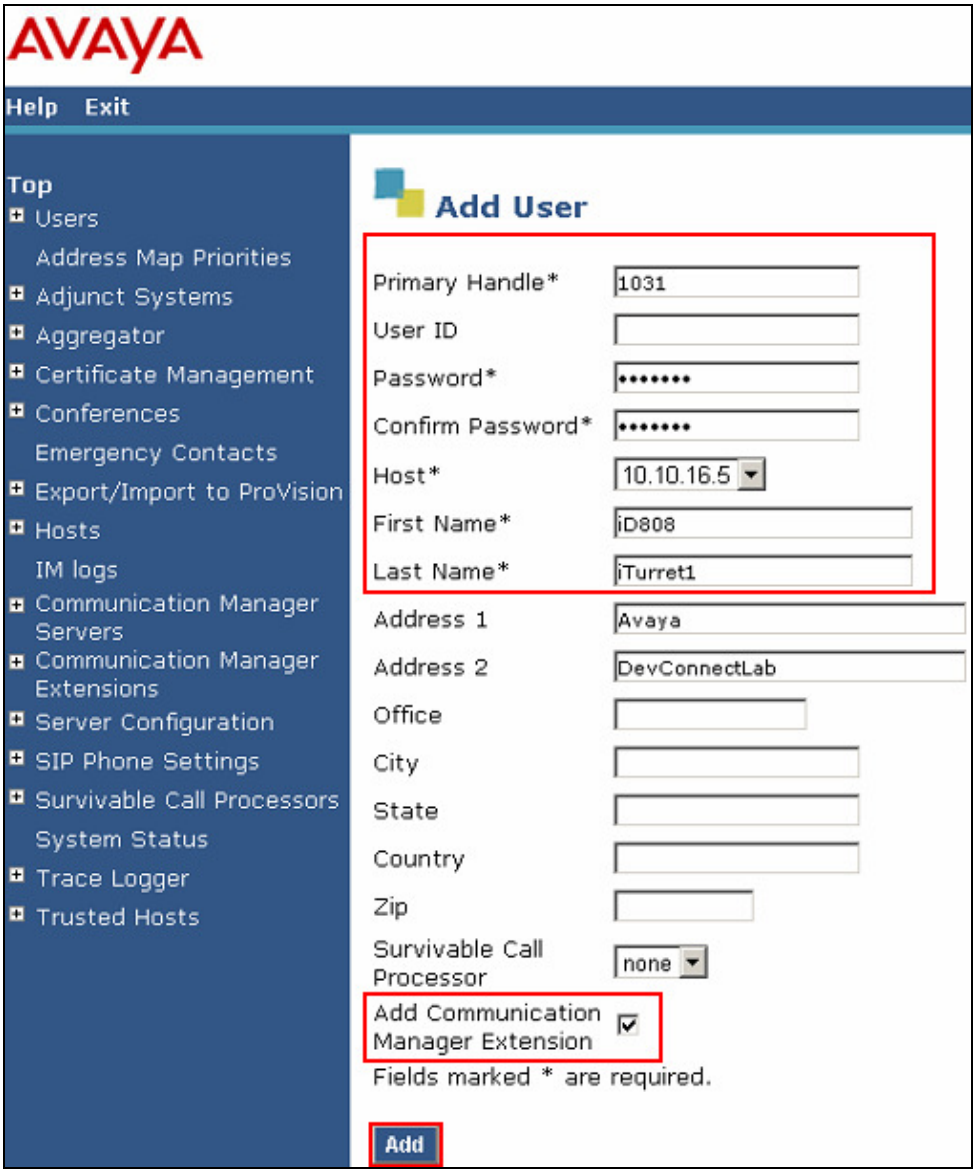
6.4. Add Avaya Aura® Communication Manager Interface

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



6.5. Add User

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



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

7. Speakerbus iD808 iTurret Configuration

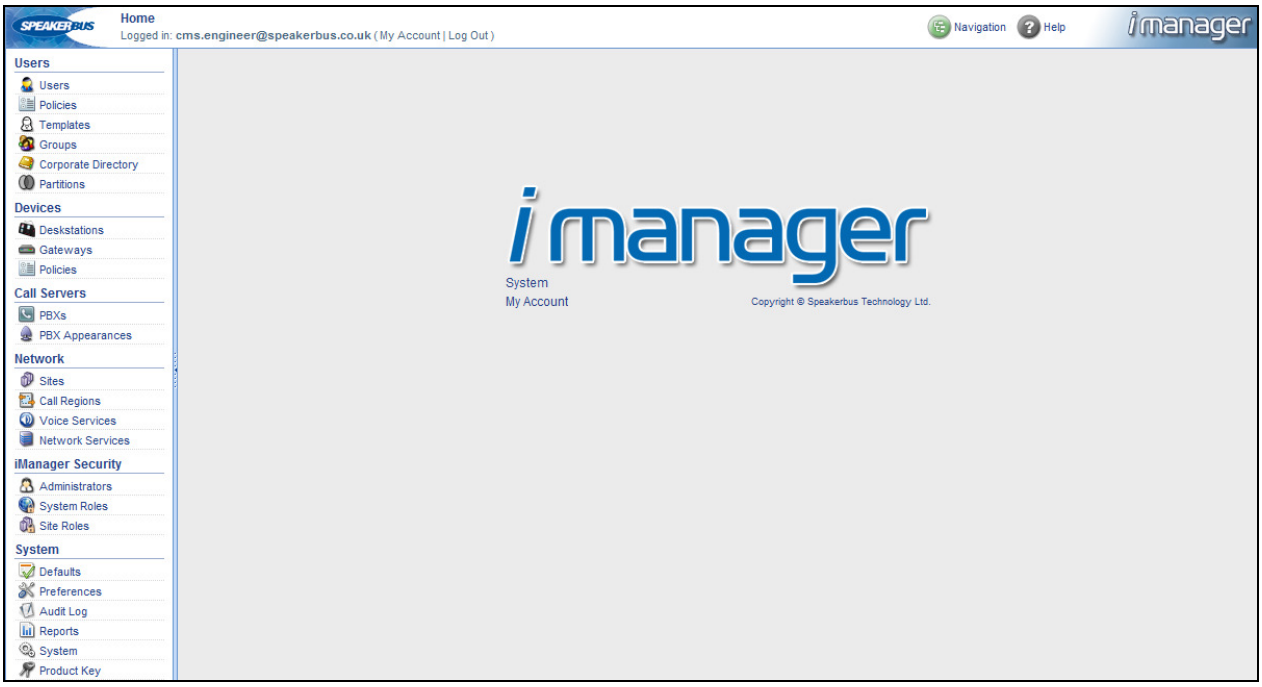
This section provides the procedure for configuring the iD808 iTurret via the iManager Centralised Management System (iCMS). The iCMS is comprised of three components, the iManager web portal application, the iCMS communication service and the iCMS database. The iManager web portal application consists of a series of configuration web pages that allows administrators to manage the iD808 iTurret devices. The procedure for configuring an iD808 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
- Announce iTurrets devices
- Create PBX
- Create Dial Plan
- Create Appearances
- Create Users
- Assign User Permissions
- Assign Ownership (of Appearances to Users)
- Assign Default Call Appearances
- Programming iTurrets Deskstations (iTurrets Layout)
- Assign Appearances to Deskstation Keys (iTurrets Layout)
- Assign Bridged Call Appearances to Deskstations (iTurrets Layout)
- Synchronize Deskstations

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

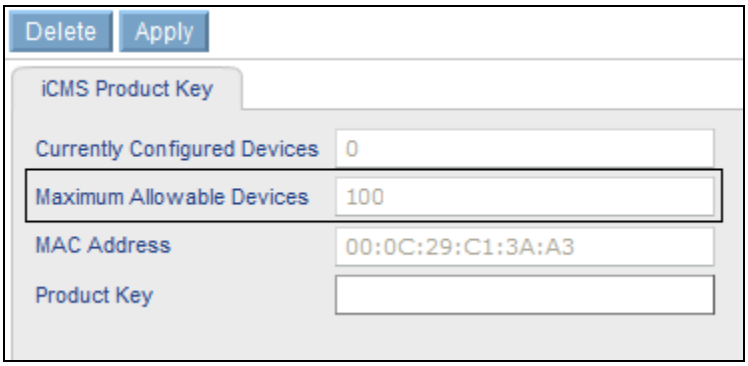
7.1. Launch iManager Web Portal

To access the iManager software interface, open a web browser and type the *i* manager web address, for example, http://10.10.16.50/imanager. 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.



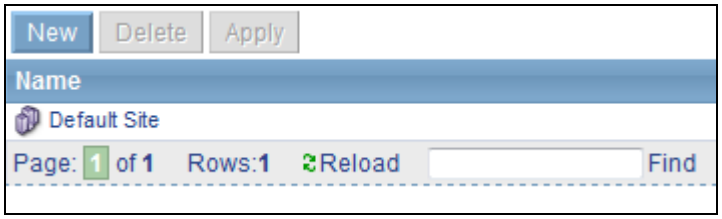
7.2. Verify Product Key

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

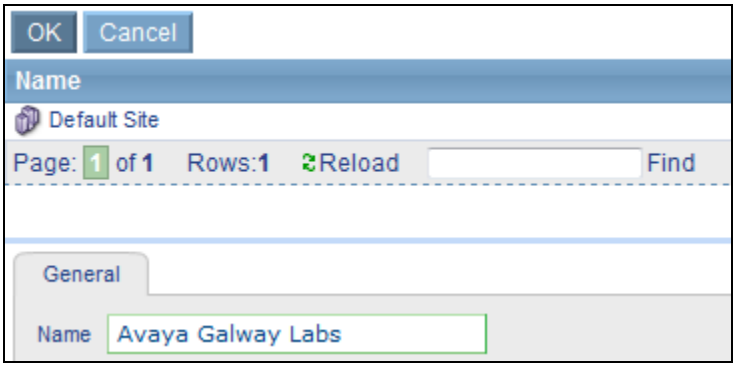


7.3. Create a Site

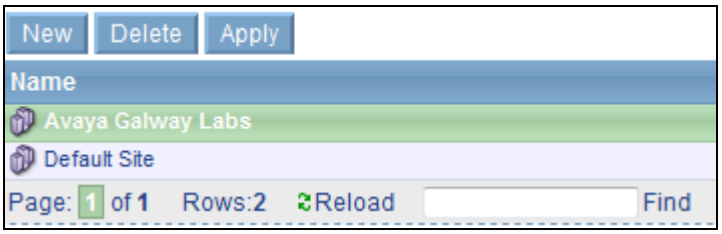
Configure a site representing the location where the iD808 iTurret devices are installed. Select **Network →Sites** in the left pane (not shown), click on **NEW** as shown below.



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



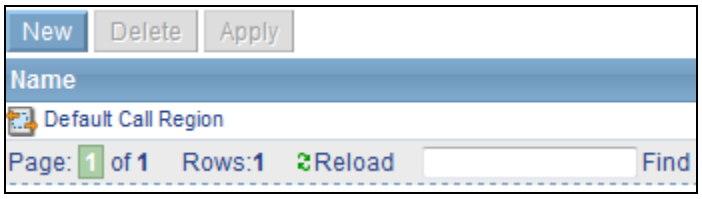
The created site will be visible in the list view as shown below.



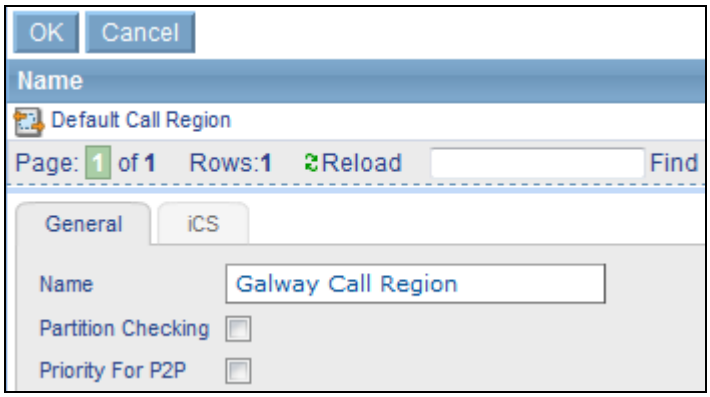
Note: A default site is available and can be used for a single site set up. Refer to the *Speakerbus iManager Administrator`s Guide* for further configuration information.

7.4. Create a Call Region

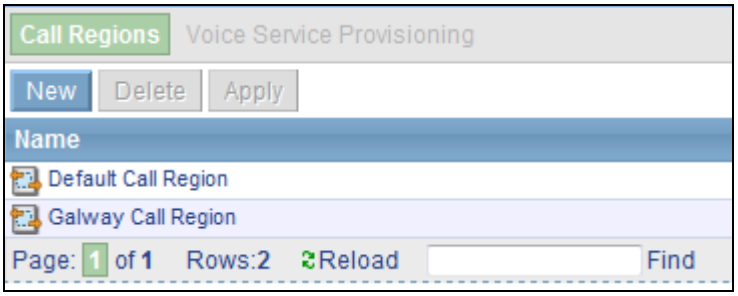
Call regions represent part of an organisation`s network. Select **Network →Call Regions** in the left pane (not shown), click on **NEW** as shown below.



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



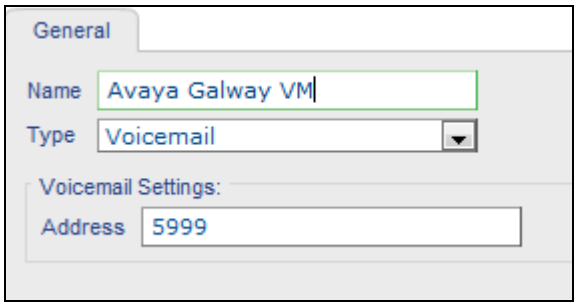
The created call region will be visible in the list view as shown below.



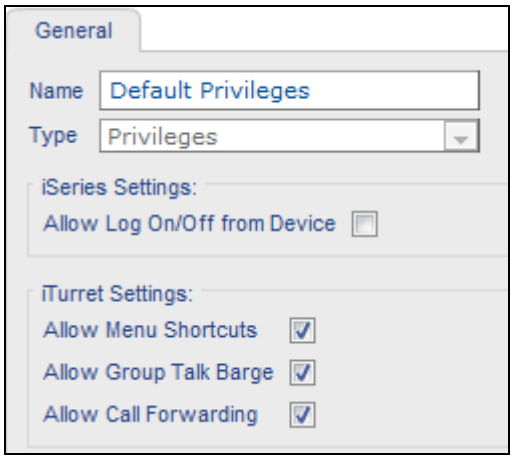
Note: A default call region is available and can be used for a single site set up. Refer to the *Speakerbus iManager Administrator`s Guide* for further configuration information.

7.5. Creating/Verifying User policies

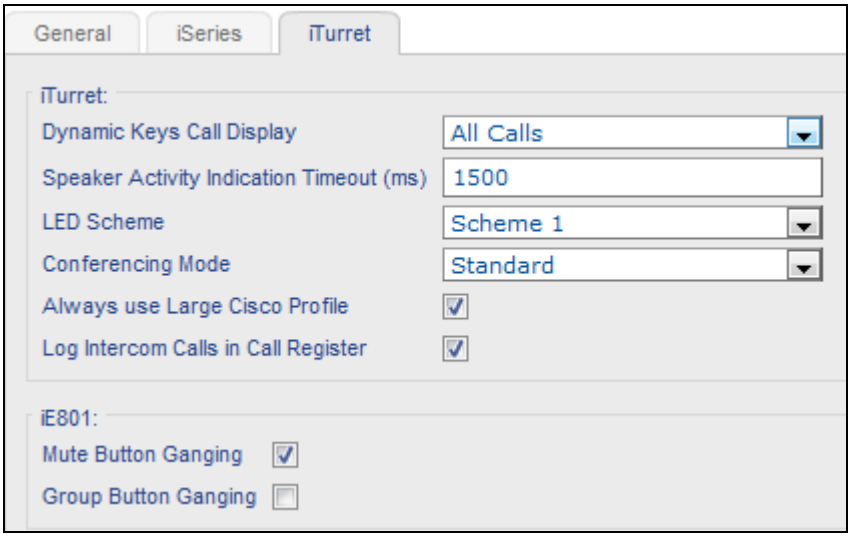
Select **Users → Policies** in the left pane (not shown), click on **NEW** (not shown)**.** Enter an identifying **Name** and in the **Type** dropdown box select **Voicemail,** fill in a valid address for the voicemail server**,** in this case the hunt group number (not shown in these Application Notes) configured 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 for this; however, it is referred to later in this document).

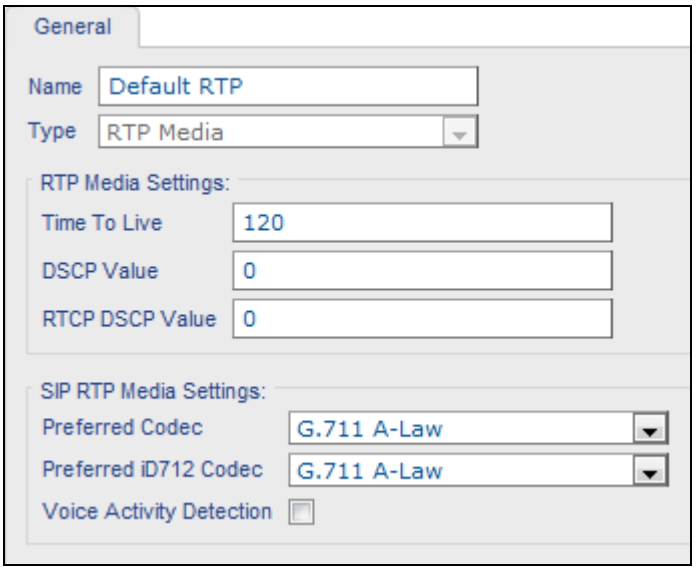


Select **Users → Policies** in the left pane (not shown), select and view the **Default Preferences** policy, click the **iTurret** tab and review the default settings (no changes should be needed for this, but it`s referred to later in this document)

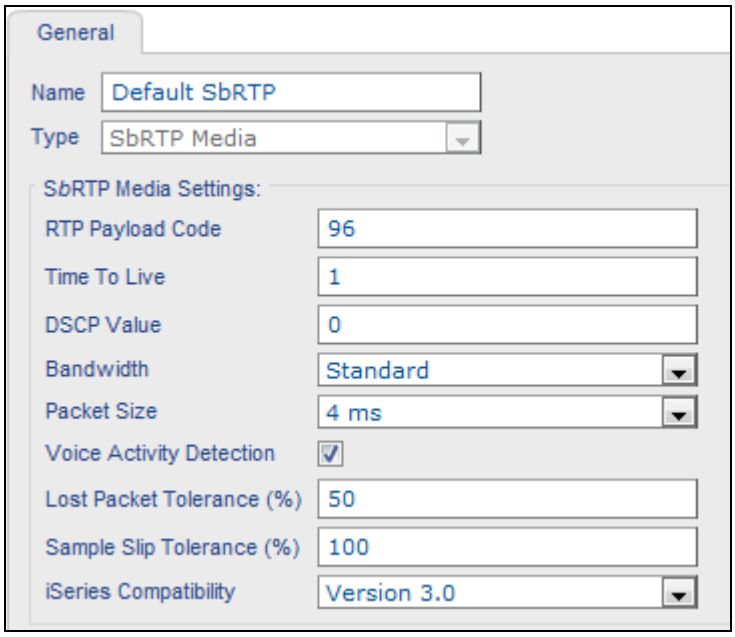


7.6. Creating/Verifying Device policies

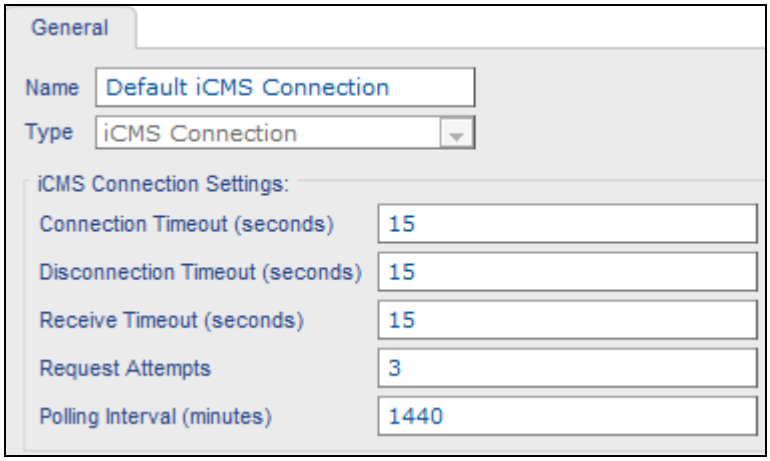
Select **Devices → Policies** in the left pane (not shown), select and view the **Default RTP** policy (no changes should be needed for this; however, it is referred to later in this document)



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

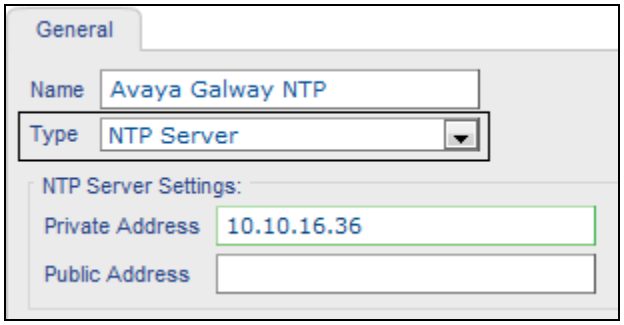


Select **Devices → Policies** in the left pane (not shown), select and view the **Default iCMS Connection** policy (no changes should be needed for this; however, it is referred to later in this document)

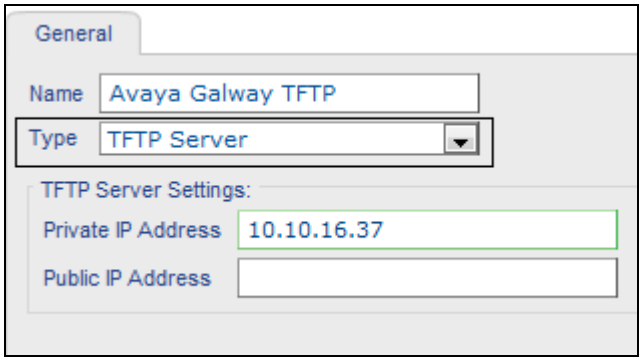


7.7. Create Network Services

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** and in the **Type** dropdown select **NTP Server,** fill in a valid address for an NTP server if available**.** Press **OK** once completed**,** as shown below.

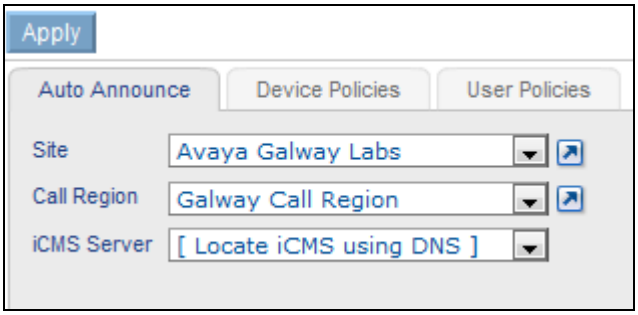


Select **Network → Network Services** in the left pane, click on **NEW** and in the Type dropdown select **TFTP Server,** enter a valid address for a TFTP server if available**.** Press **OK** once completed**,** as shown below.



7.8. Confirm defaults

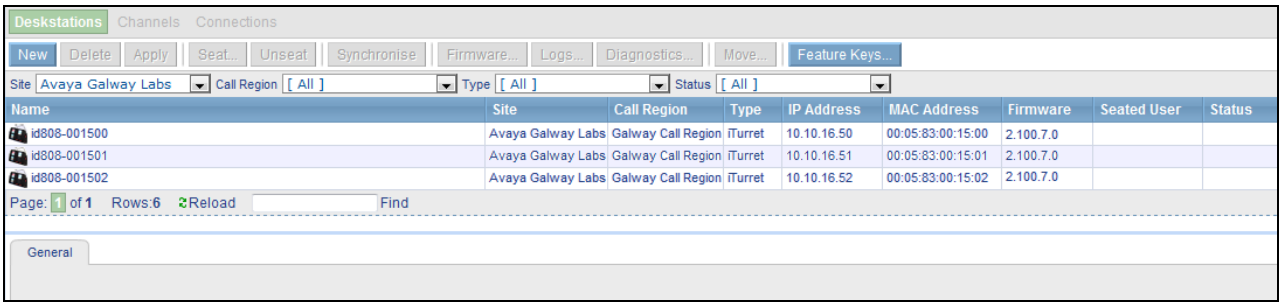
Select **System →Defaults** in the left pane (not shown), under the **Auto-Announce** tab, select the **Site and Call Region** created above and confirm that **iCMS Server** is set to [**Locate iCMS using DNS**]. Click **APPLY** to confirm as shown below:



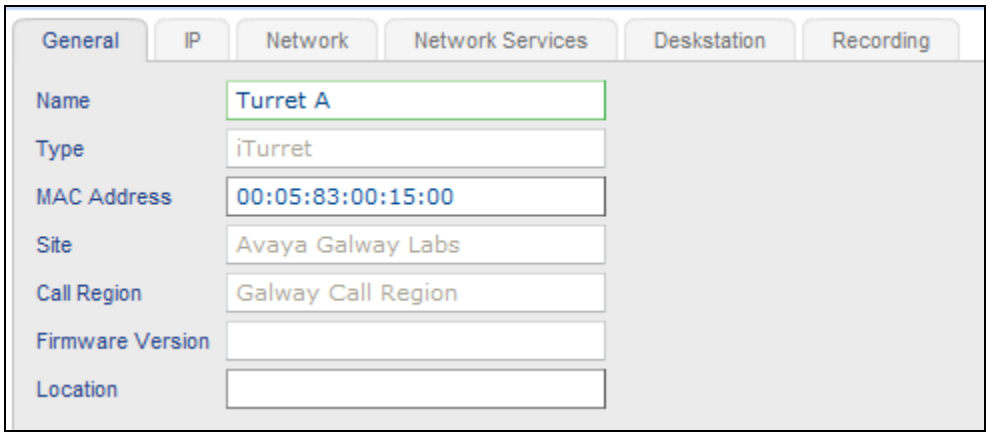
Note: DNS and DHCP must be set up in accordance with the Speakerbus administrators guide. Refer to the *Speakerbus iManager Administrator`s Guide* for further configuration information

7.9. Create iTurret Deskstations

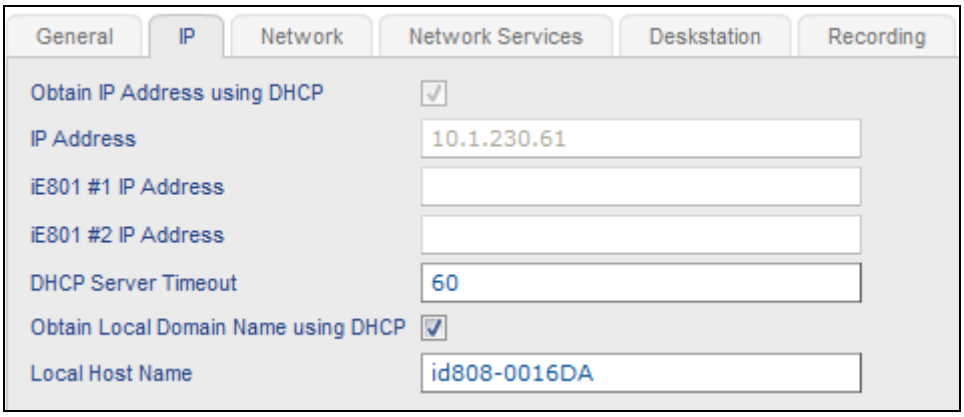
The iD808 iTurrets will automatically register to the iCMS server if appropriate **DHCP** and **DNS** records were created prior to the iD808 iTurret being connected to the IP network. To view the newly registered deskstations, Select **Devices →Deskstations** in the left pane (not shown) and confirm they are seen as follows.



Select the iD808 iTurret and enter an identifying **Name** in the **General** tab.

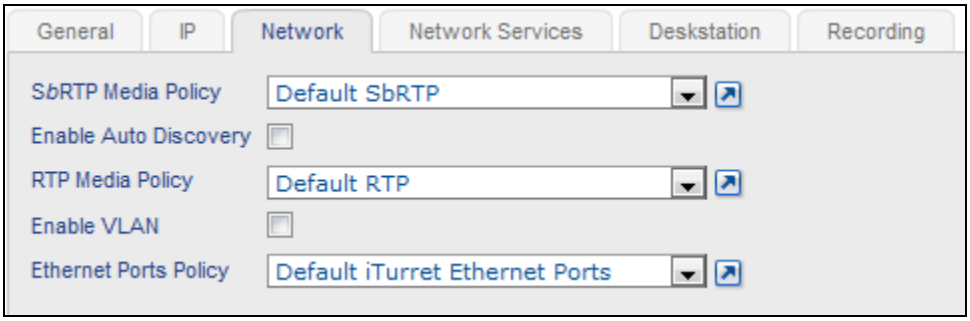


Click the **IP** tab, verify that the **Obtain IP Address using DHCP** and the **Obtain local Domain Name using DHCP** tick boxes are checked



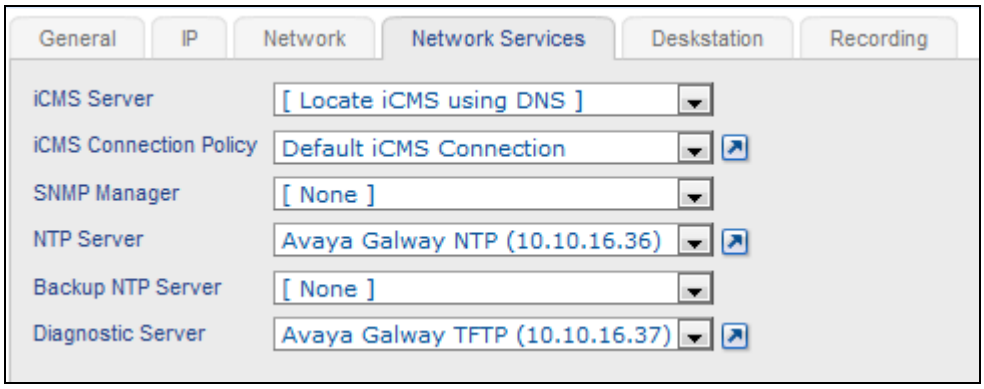
In the **General** tab, verify the following are configured as mentioned above:

- **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**

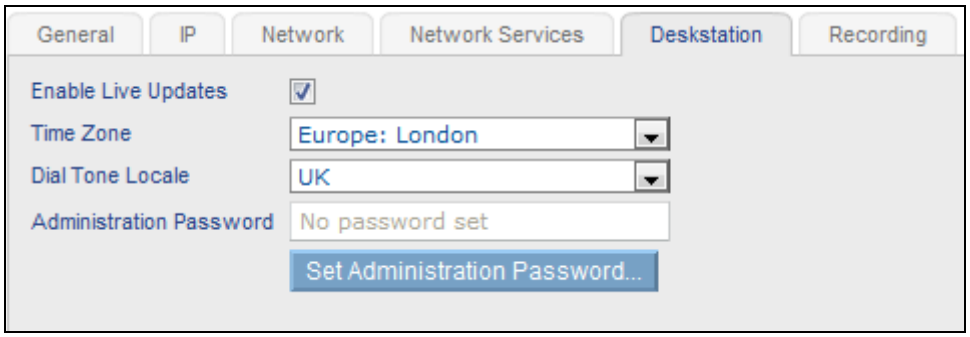


In the **Network Services** tab, verify the following:

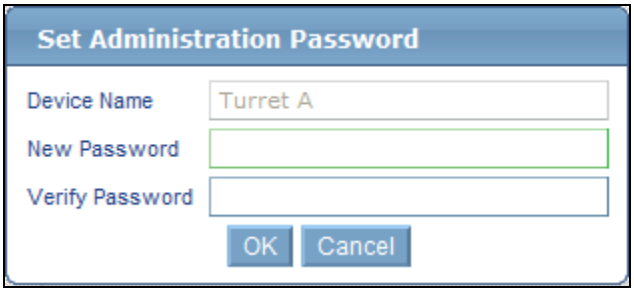
- **iCMS Server** shows **[Locate iCMS using DNS]**
- **iCMS Connection Policy** shows **Default iCMS Connection**
- **NTP Server**, select the newly created ntp server network service configured above
- **Diagnostics Server**, select the newly created TFTP server network service configured above



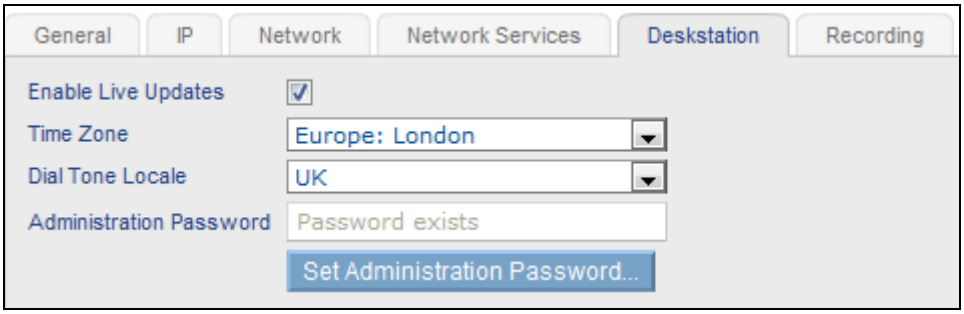
In the **Deskstation** tab, ensure that **Enable Live Update** is checked, the **Time Zone** and **Dial Tone Locale** are set to the required setting and click on **Set Administration Password.**



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



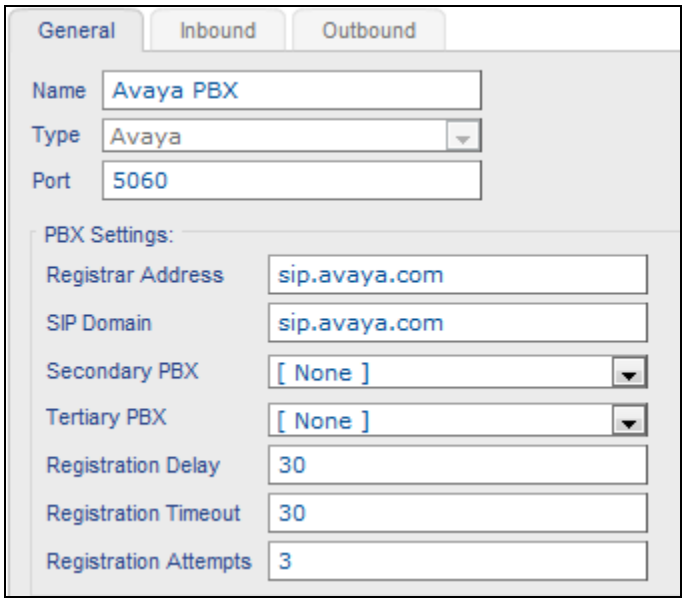
The Deskstation tab contents now displays the following



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 SES active IP address
- After the PBX is created, the **Port** field will be displayed on this page with the default value of 5060



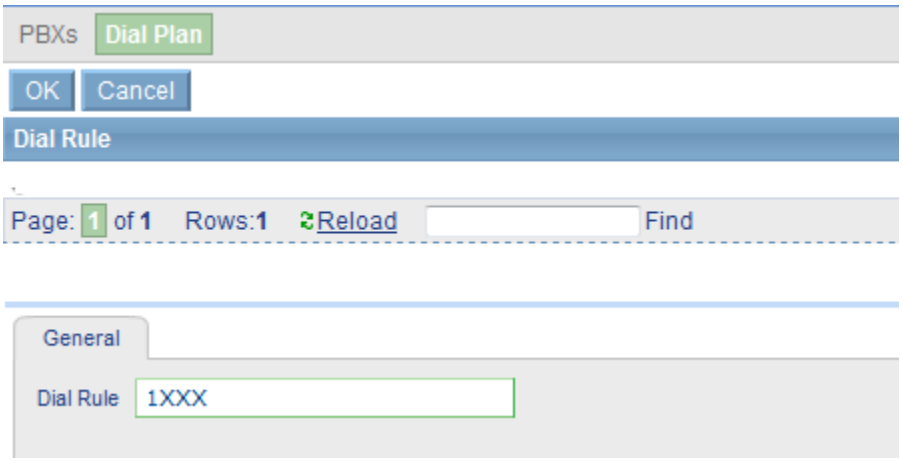
Note 1: A server locater record (SRV) for the registrar address and SIP domain must be created on DNS. Refer to the *Speakerbus iManager Administrator`s Guide* for the correct configuration of DNS

Note 2: If using failover, then a second PBX will be created and this will be 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.



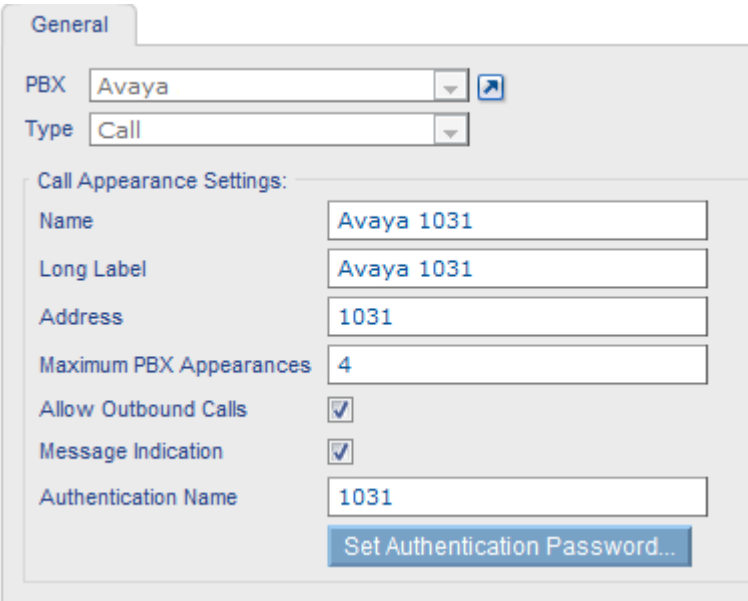
Repeat this for all valid extension formats.

7.12. Create Call and Handset Appearances

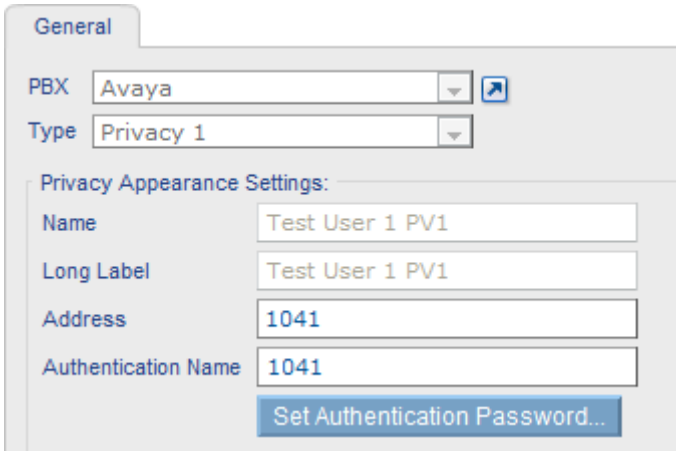
Three call appearances must be created for each iD808 iTurret ~~iTurret~~ device. One is for the main appearance, and one for each of the privacy appearances (handset 1 and handset 2). As previously explained, three extensions are configured in the SES/CM for this purpose.

To create the main appearance, click **Call Servers →PBX Appearances** in the left pane, click on **NEW,** then select the **Type** of appearance to be created (Call, Privacy 1 and Privacy 2) (not shown) and configure as follows under the **General** tab:

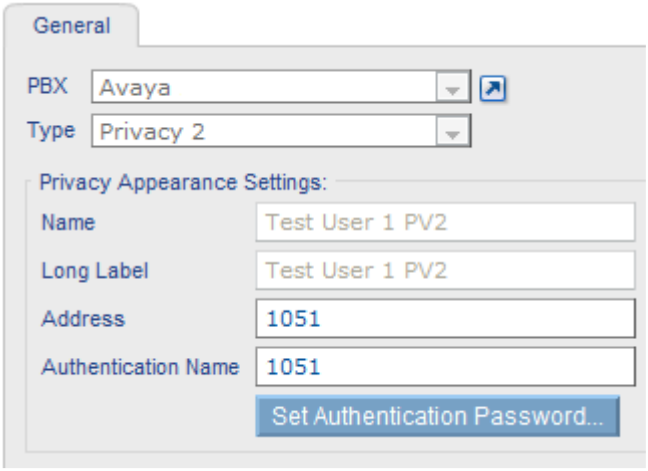
- Provide a descriptive name for the appearance in the **Name** field, such as the extension or user's name.
- Set the **Long Label** field to the label that will be displayed for the call appearance button on the iD808 iTurret. The **Address** field should also be set to the appearance extension.
- 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 a users 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 iD808 iTurret .
- 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, respectively, which have been configured on SES/CM in **Section 6.5.** These are the credentials that the iD808 iTurret will use to authenticate and register with SIP Enablement Services. Use the default values for the other fields. Click **OK**.



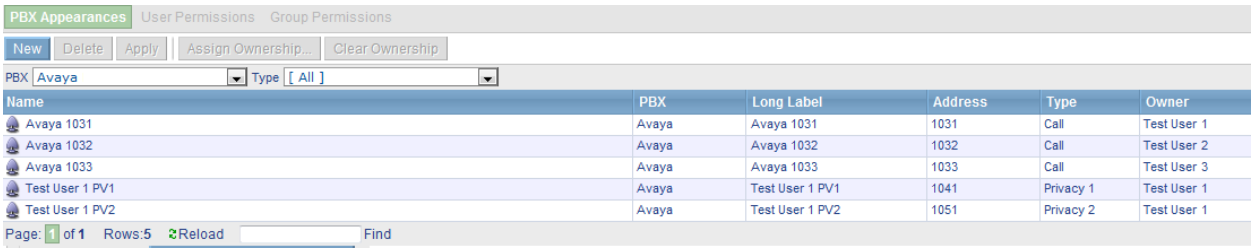
Repeat the procedure for the two corresponding privacy appearances. Click the **New** button to add another appearance. In the **General** tab, set the **Type** field to **Privacy 1** and complete the **Address, Authentication Name** and **Authentication Password** fields. The last two fields should be identical to that set up in SES/CM for registration to occur. Press **OK** to commit the created appearance.



Repeat the above procedure to add the Privacy 2 appearance.



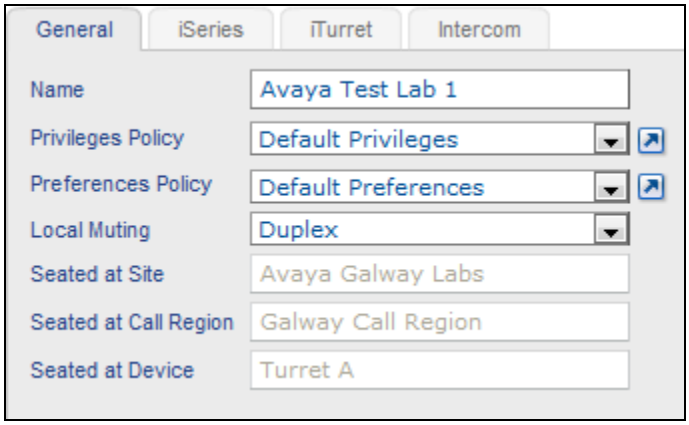
Repeat the above procedures for adding the Main and Privacy appearances for each iD808 iTurret.



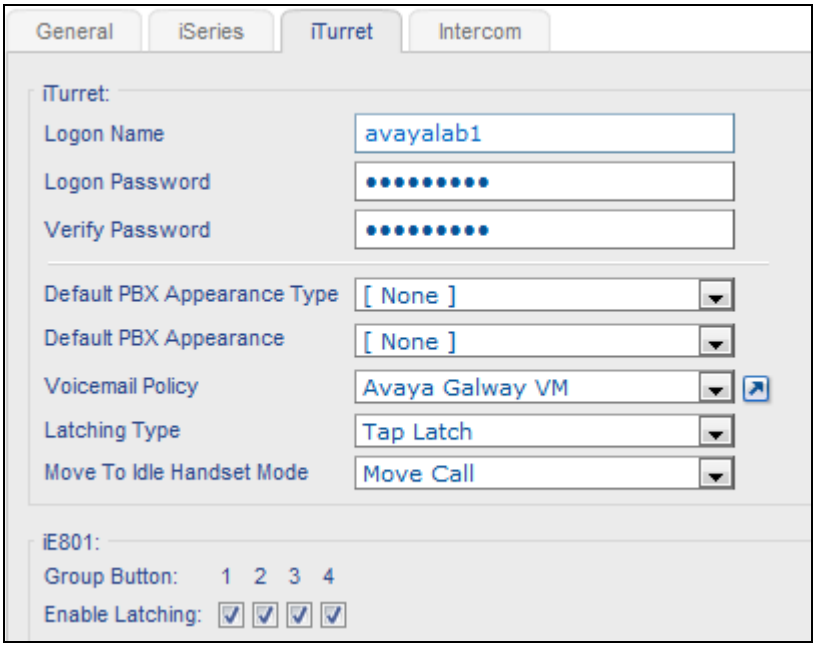
Name	PBX	Long Label	Address	Type	Owner
Avaya 1031	Avaya	Avaya 1031	1031	Call	Test User 1
Avaya 1032	Avaya	Avaya 1032	1032	Call	Test User 2
Avaya 1033	Avaya	Avaya 1033	1033	Call	Test User 3
Test User 1 PV1	Avaya	Test User 1 PV1	1041	Privacy 1	Test User 1
Test User 1 PV2	Avaya	Test User 1 PV2	1051	Privacy 2	Test User 1

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**.

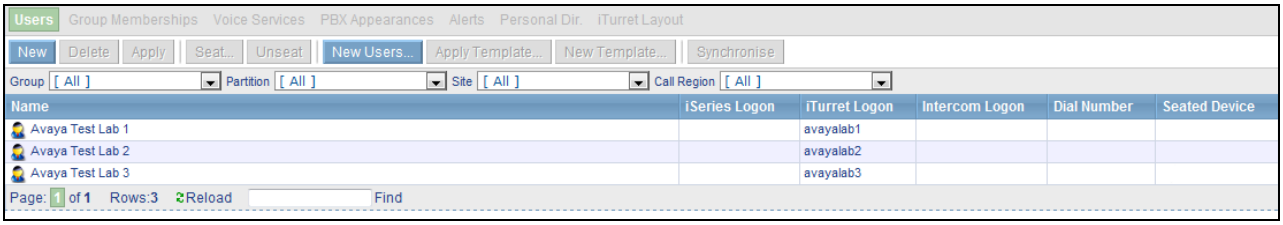


Within the **iTurret** tab, provide the **logon** credentials for the user to log into their iD808 iTurret and assign the voicemail policy set up as seen in the **Voicemail Policy** dropdown box.

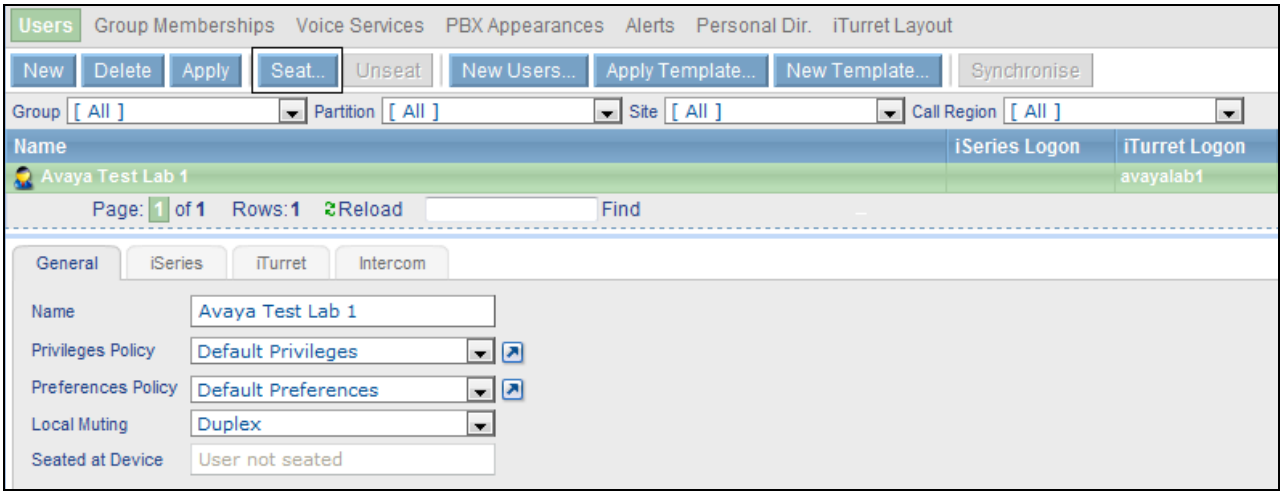


Click **APPLY** (not shown) once complete (although, this page will be revisited later to configure the default call appearance for this user).

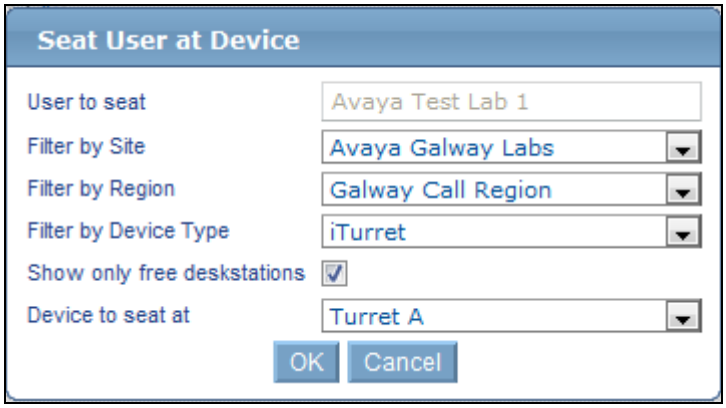
Repeat the previous steps to add more users.



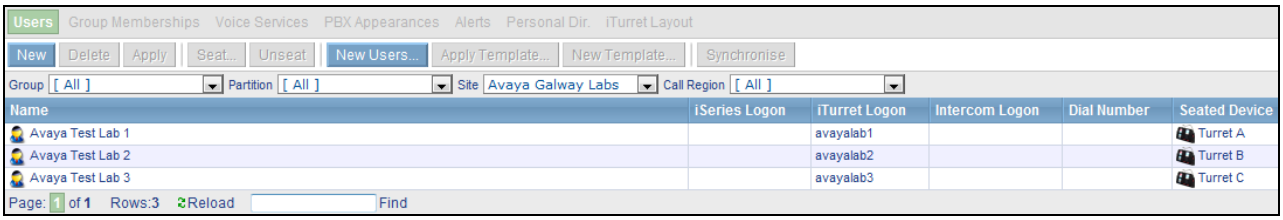
After the user has been created, that user can then be seated on an iD808 iTurret. Select the user to be seated and click **Seat** from the bar as shown below.



On the next page, filter options are presented. **Filter by Device Type iTurret** in the site configured in **Section 7.3** and the region configured in **Section 7.4**, place a tick in the **Show only free deskstations** check box. Select the appropriate iD808 iTurret from the **Device to seat at** drop down box and click **OK**.



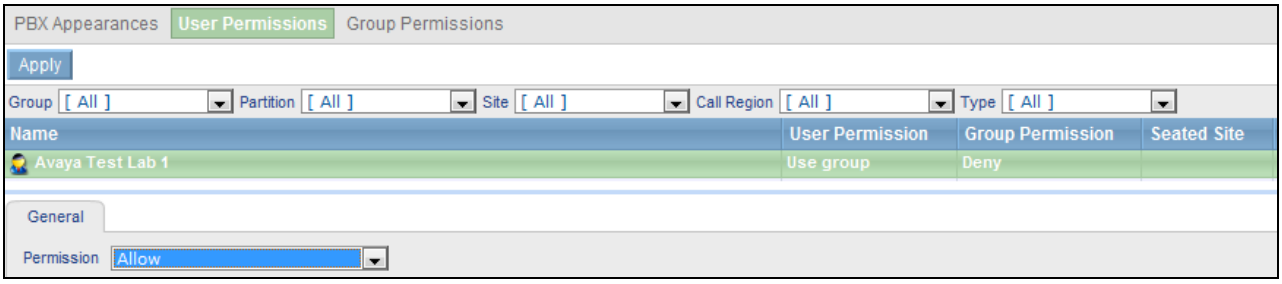
The user has been successfully seated as indicated by the iD808 iTurret in the **Seated Device** column on the following page. Repeat this process for seating all other users.



7.14. Assign User Permissions

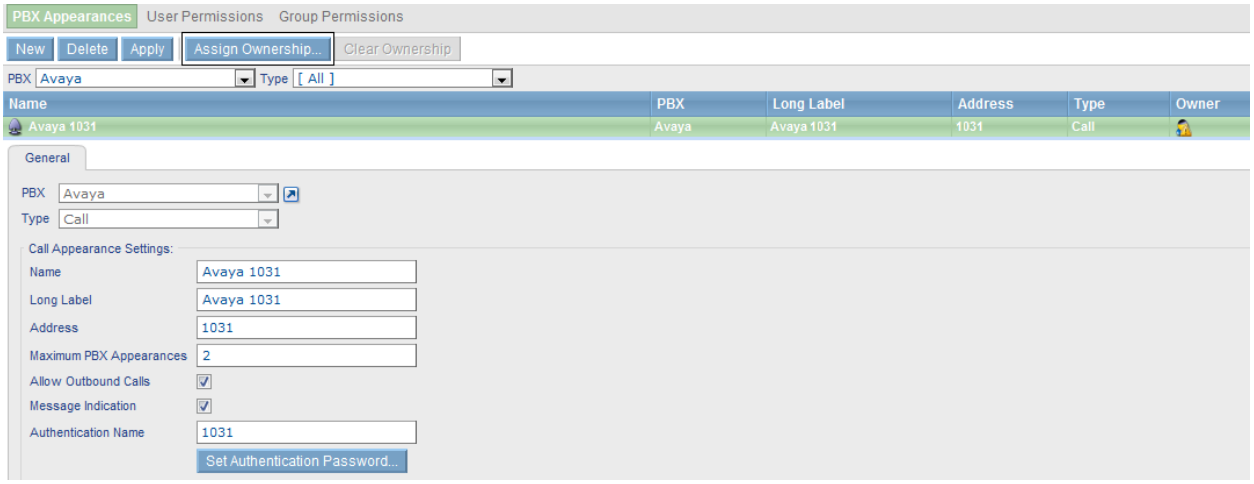
Appearance permissions must be assigned to the created users.
Select **Call Servers →PBX Appearances** in the left pane (not shown), select the **Call Appearance** from the list, and select the **User Permissions** tab at the top of the page.

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

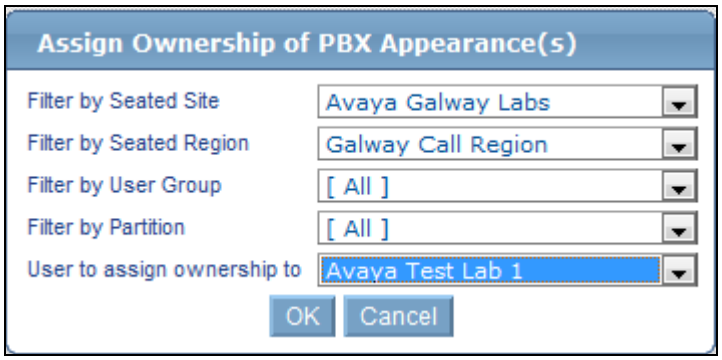


7.15. Assign Ownership

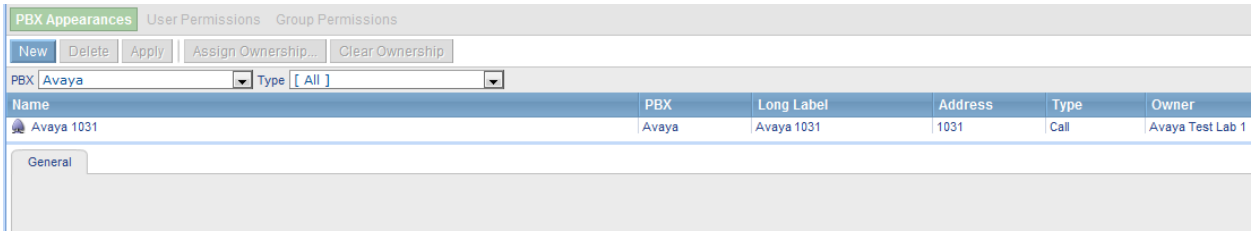
Appearance ownership must be assigned to a user as it enables the iD808 iTurret to distinguish between the owner of the call or appearance as opposed to someone who is bridged on to that appearance. Select **Call Servers →PBX Appearances** in the left pane, select the **Call Appearance** from the list, and select the **Assign Ownership** button.



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**.

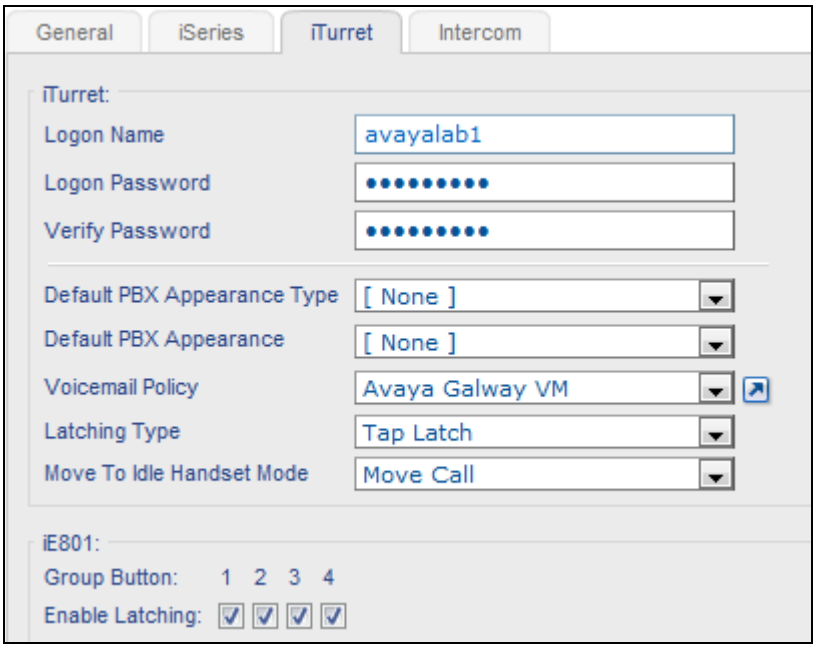


Repeat this process to assign Privacy 1 and Privacy 2 call appearances to User.

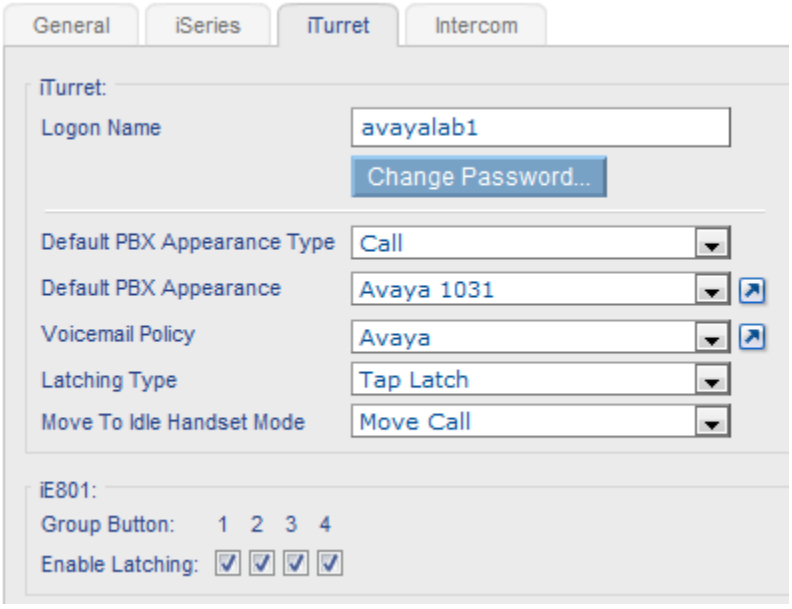


7.16. Assign Default Call Appearance

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



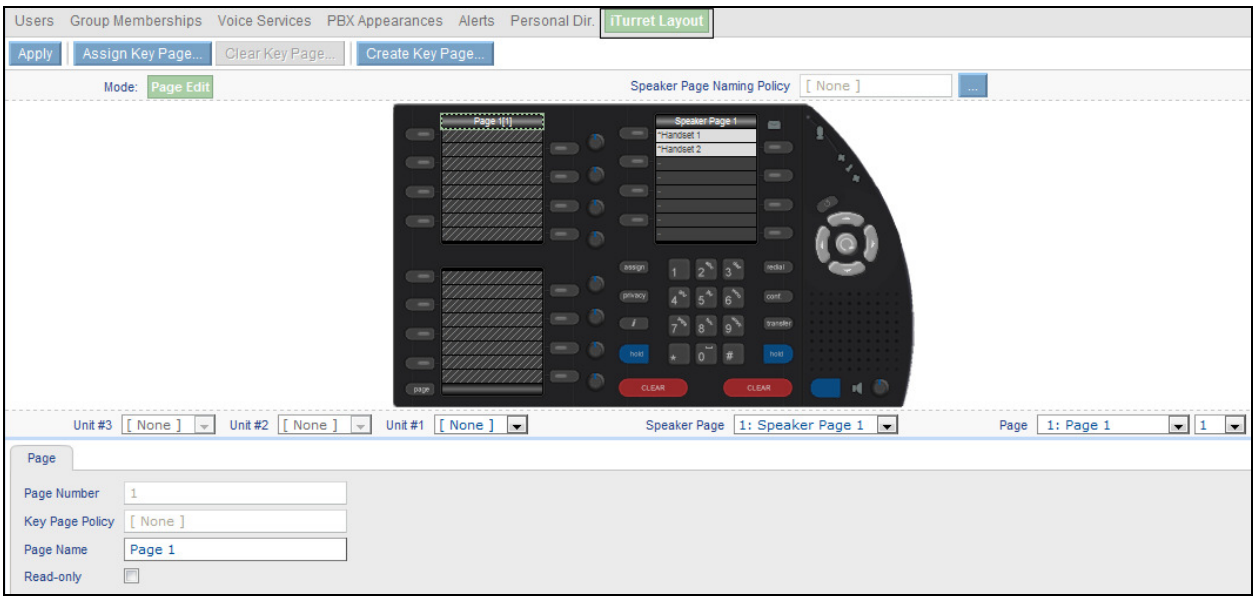
Set the **Default PBX Appearance Type** field to **Call** and then set the **Default PBX Appearance** field to the main call appearance (e.g. **1031**). Click **Apply**.



7.17. Programming iD808 iTurret Deskstations

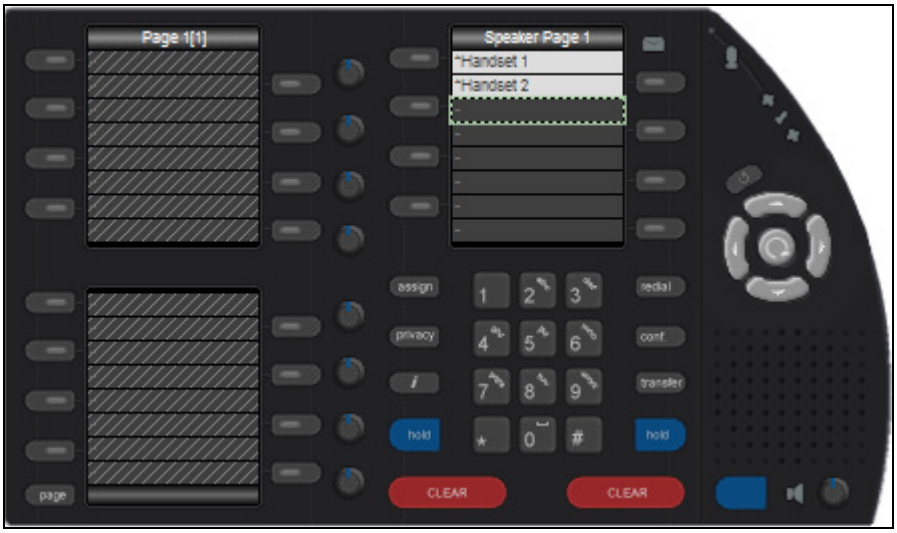
This section describes how to create iD808 iTurret keys. In this configuration, each user will be configured with two Dynamic keys, two Soft Function keys, one function (DND) key and one Shortcut key.

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.

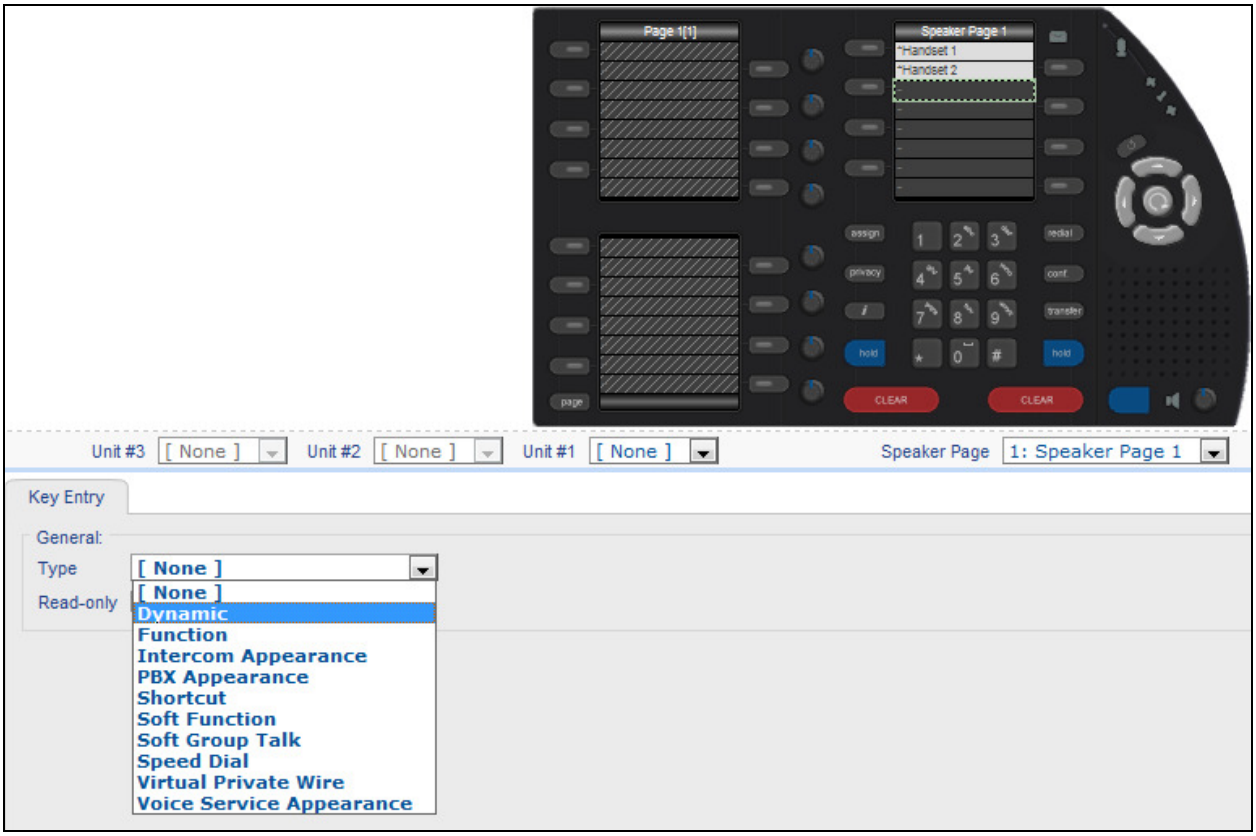


Create two dynamic keys (one after the other) under Handset 2.

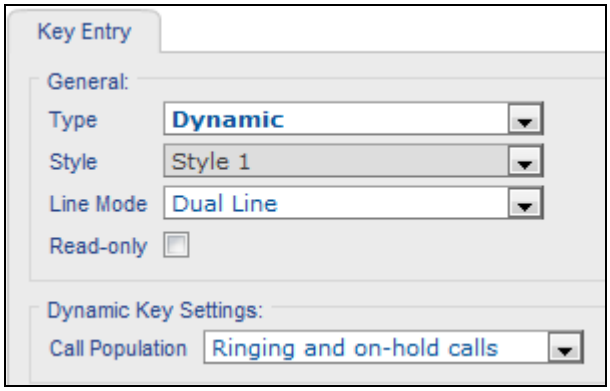
To add the first dynamic key, select the next available fixed key below Handset 2 as seen below.



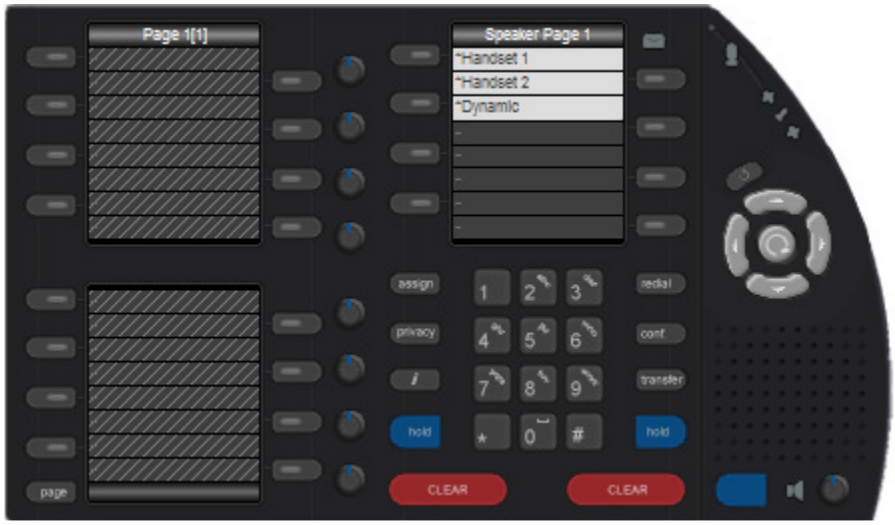
In the **Key Entry** tab, select **Dynamic** from the **Type** field, as seen below.



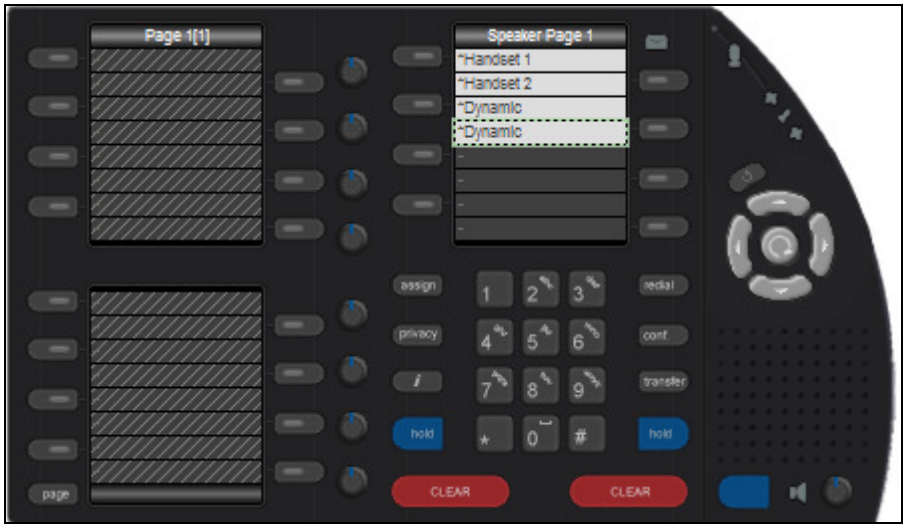
Leave the **Call Population** dropdown at the default **Ringing and on-hold calls**. Click **OK**.



The iD808 iTurret layout looks as follows with the first dynamic key assigned.



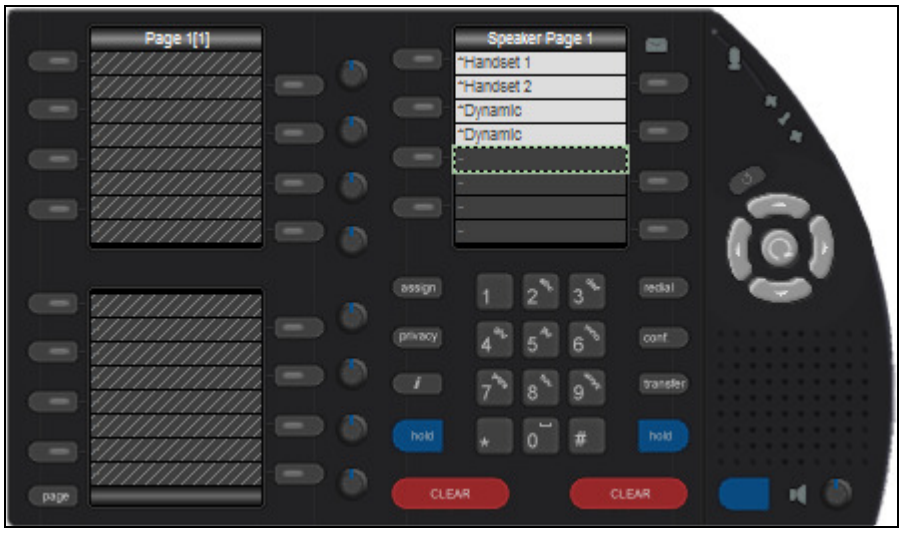
Now add the second dynamic key under the first by following the steps above, once completed the iD808 iTurret layout will look as follows.



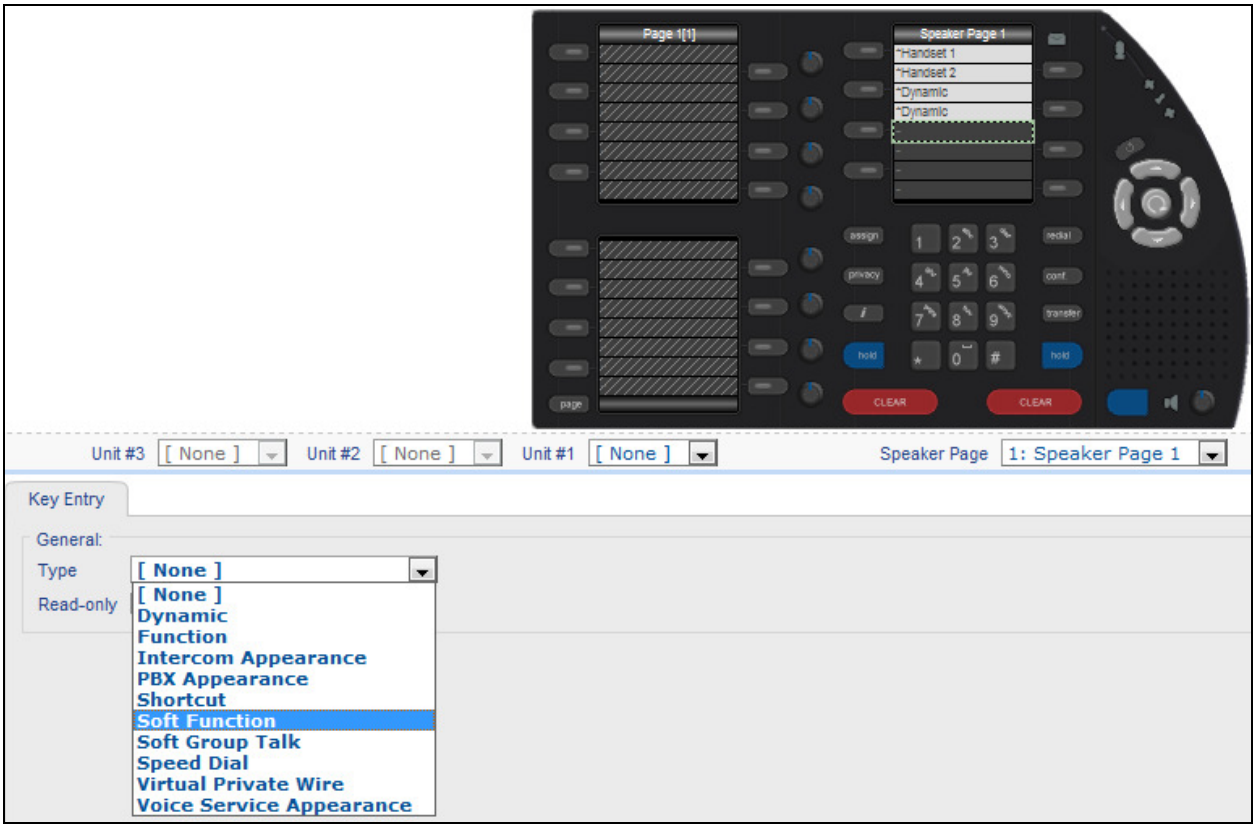
NOTE: The Call Population can be set up for different key assignments, these are “Ringing and on-hold calls”, “Ringing calls only”, “On-hold calls only”, “Busy-elsewhere calls only” and “Busy-elsewhere and on-hold calls”. The default is the “Ringing and on-hold calls”, but any combination of these can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

Create two soft function keys under the second dynamic key.

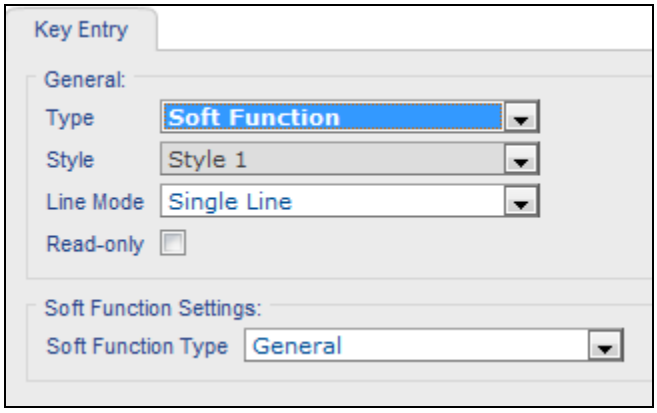
To add the first soft function key, select the next available fixed key under the last soft function key, as seen below.



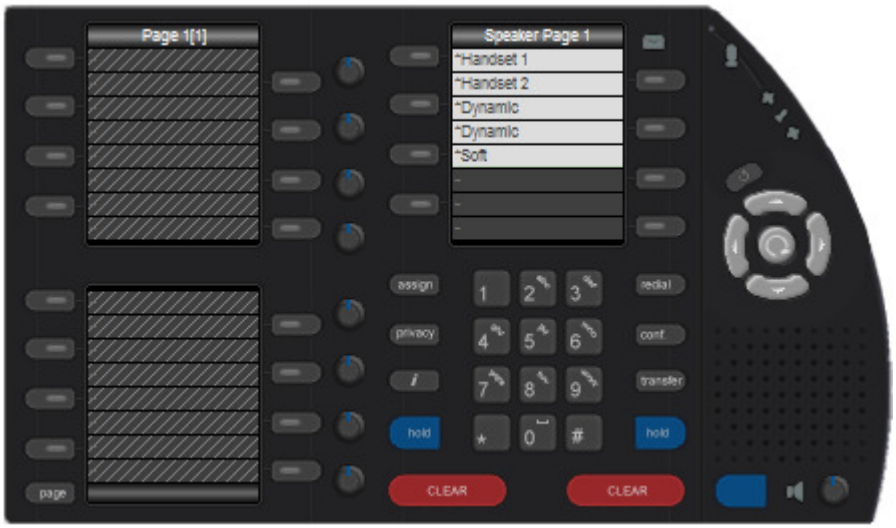
In the **Key Entry** tab, set **Soft Function** in the **Type** field. Leave the **Soft Function Type** dropdown at the default **General**. Click **OK** (not shown).



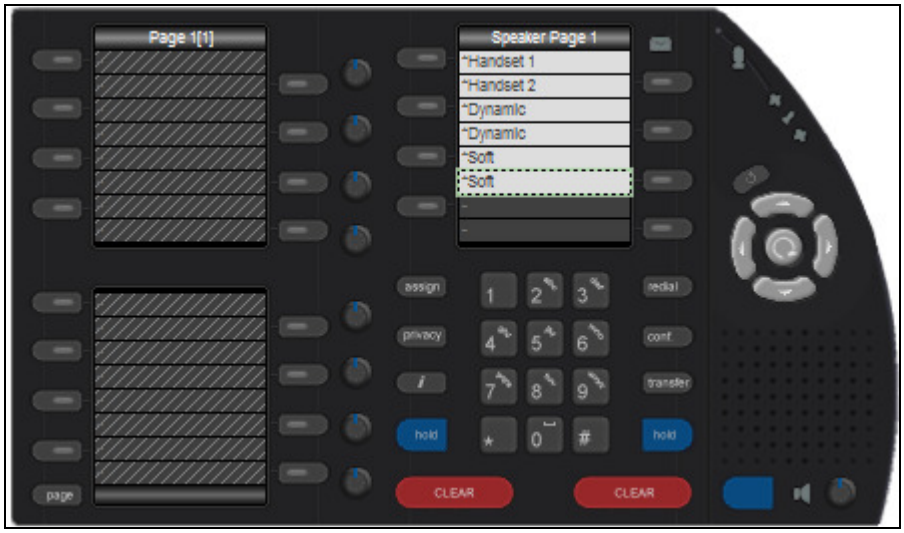
Leave the **Soft Function Type** dropdown at the default **General**. Click **OK** (not shown).



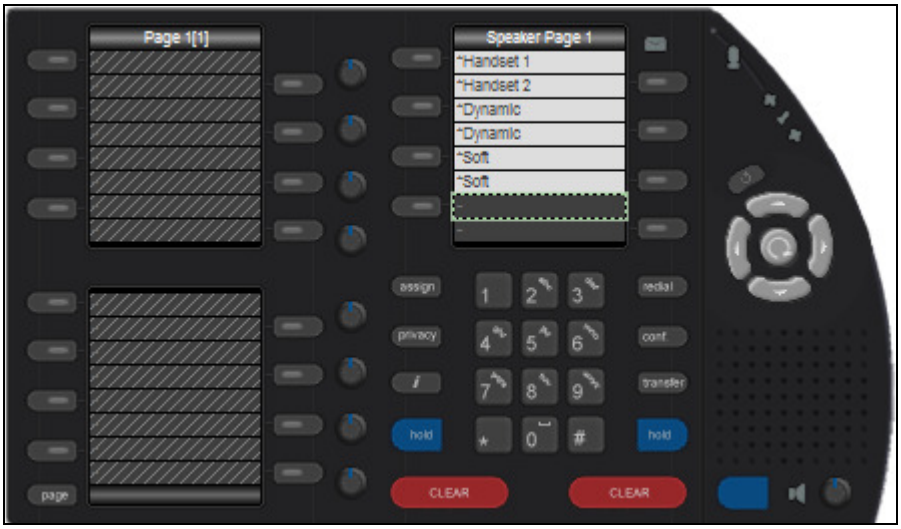
The iD808 iTurret layout looks as follows with the first soft function key assigned.



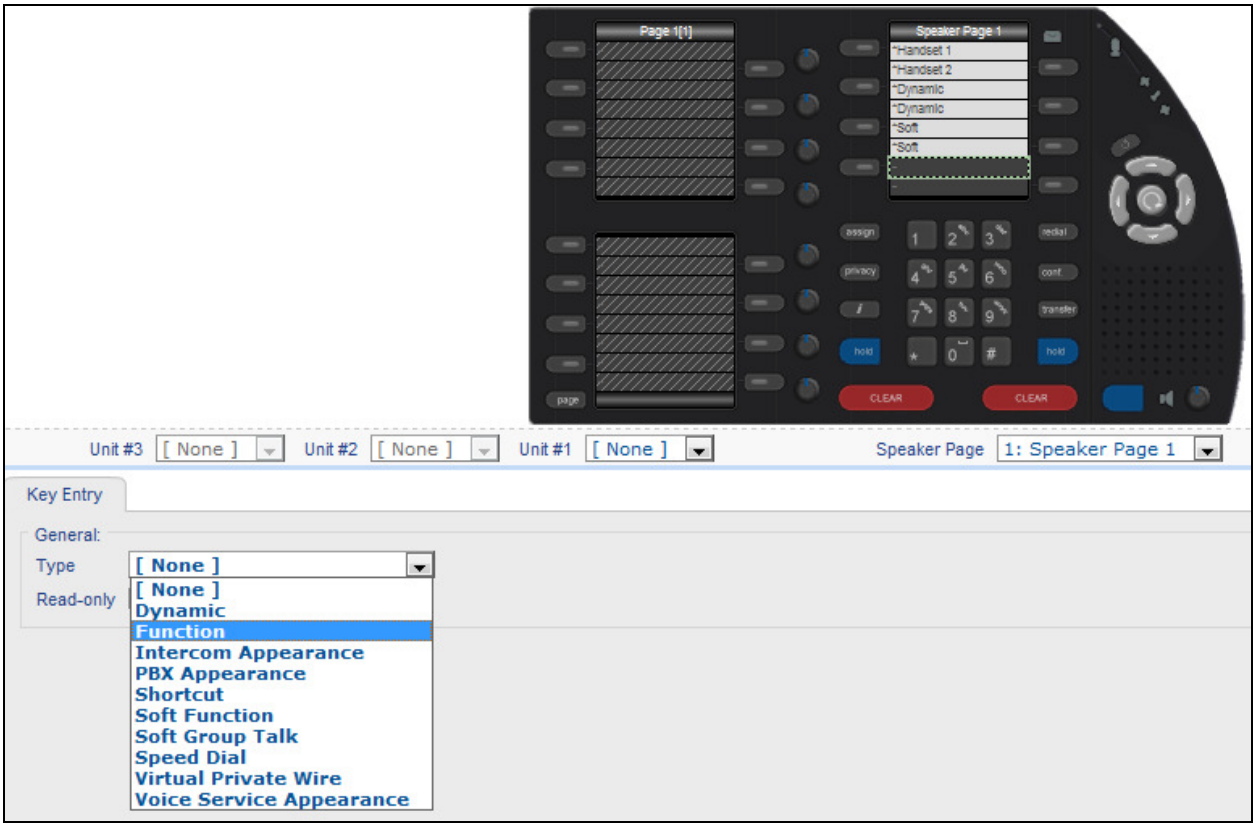
Now add the second soft function key under the first by following the steps above, once completed the iD808 iTurret layout will look as follows.



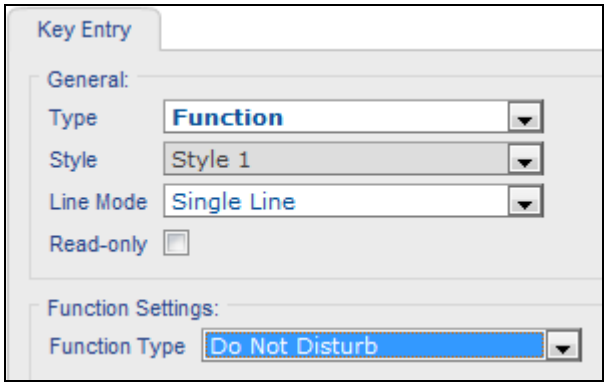
Create a function (Do Not Disturb (DND)) key, select the next available fixed key under the last soft function key, as seen below.



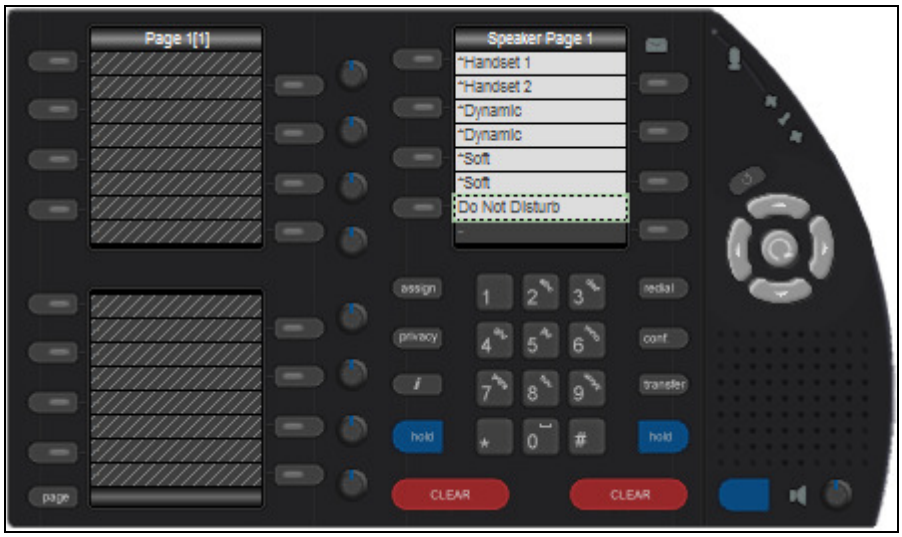
In the Key Entry tab, set **Function** in the **Type** field.



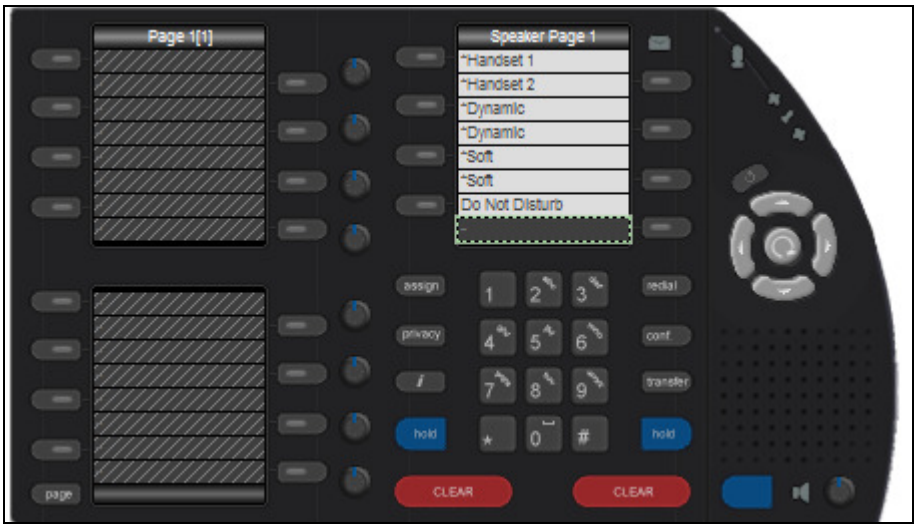
Select **Do Not Disturb** from the **Function Type** dropdown. Click **OK**.



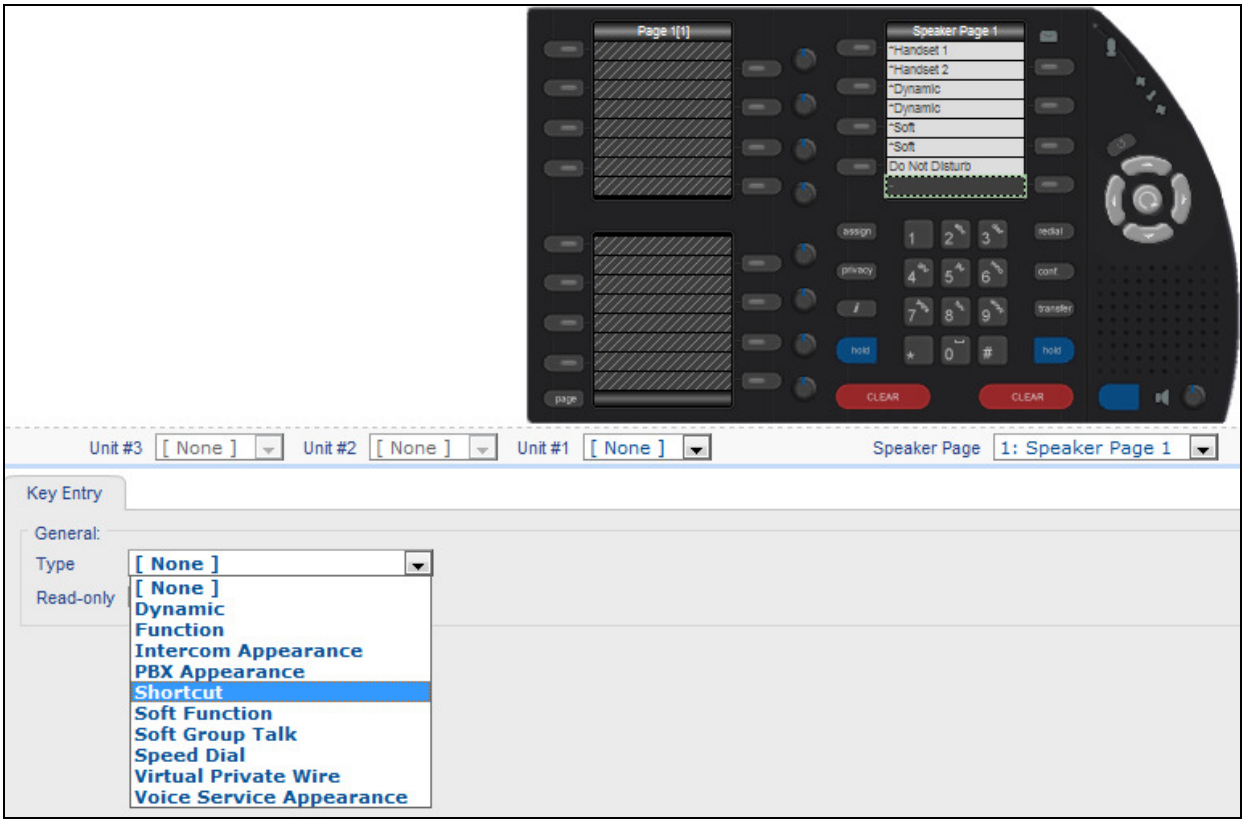
The layout looks as follows.



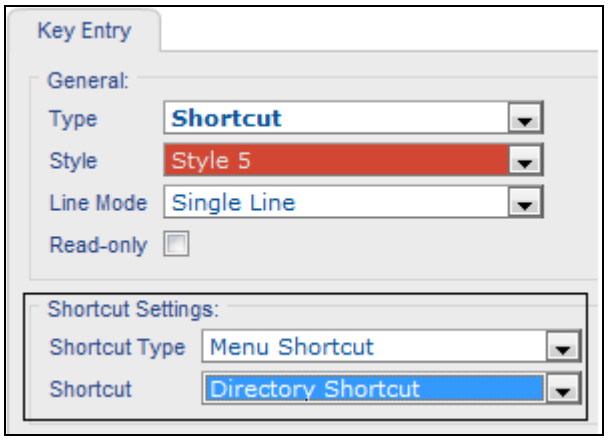
Create a menu shortcut key, select the next available fixed key under the last function key, as seen below:



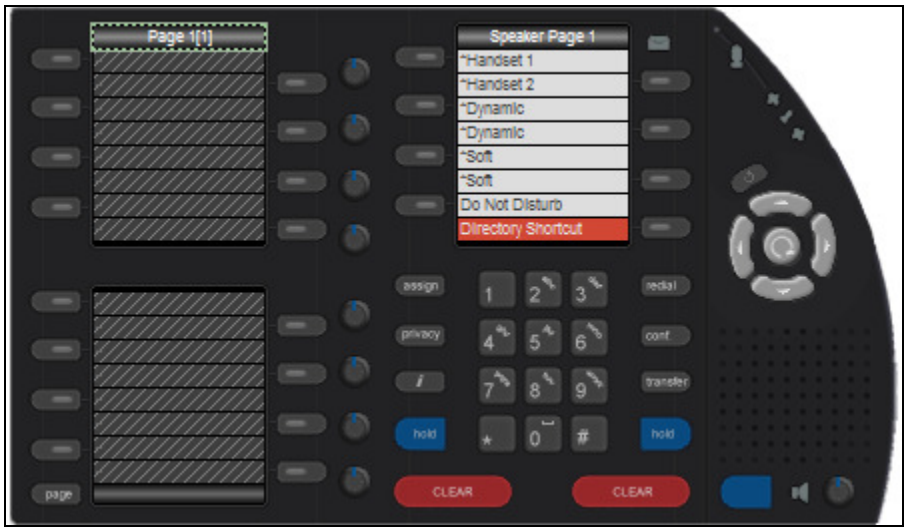
In the **Key Entry** tab, set **Shortcut** in the **Type** field, as seen below:



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



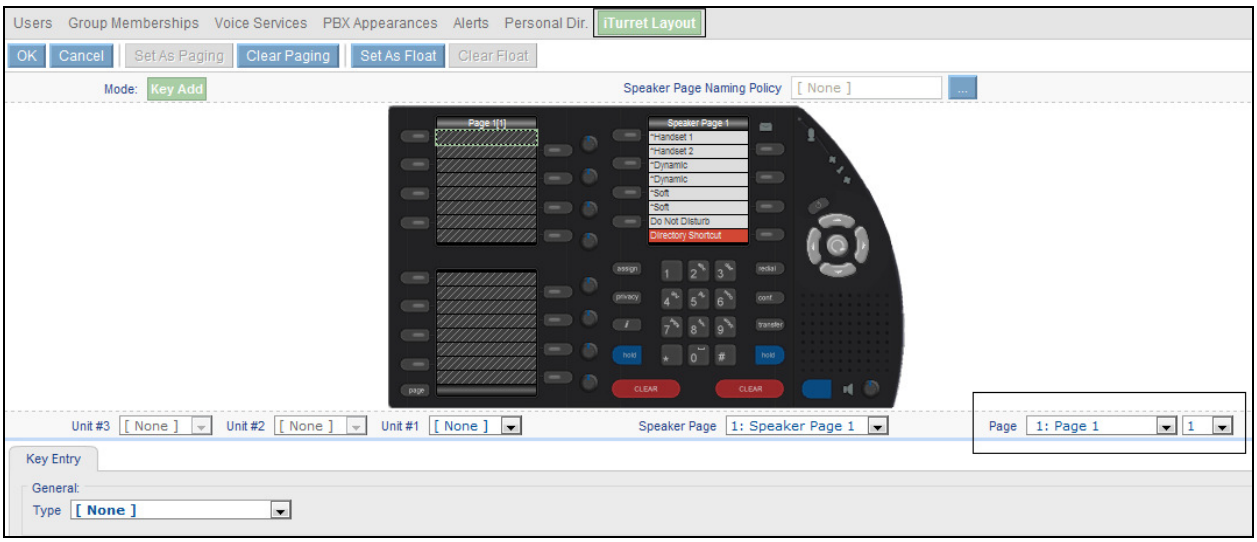
The iD808 iTurret layout will appear as shown below when completed.



7.18. Programming Appearances to iD808 iTurret Keys

This section describes how to create appearance keys for the iD808 iTurret.

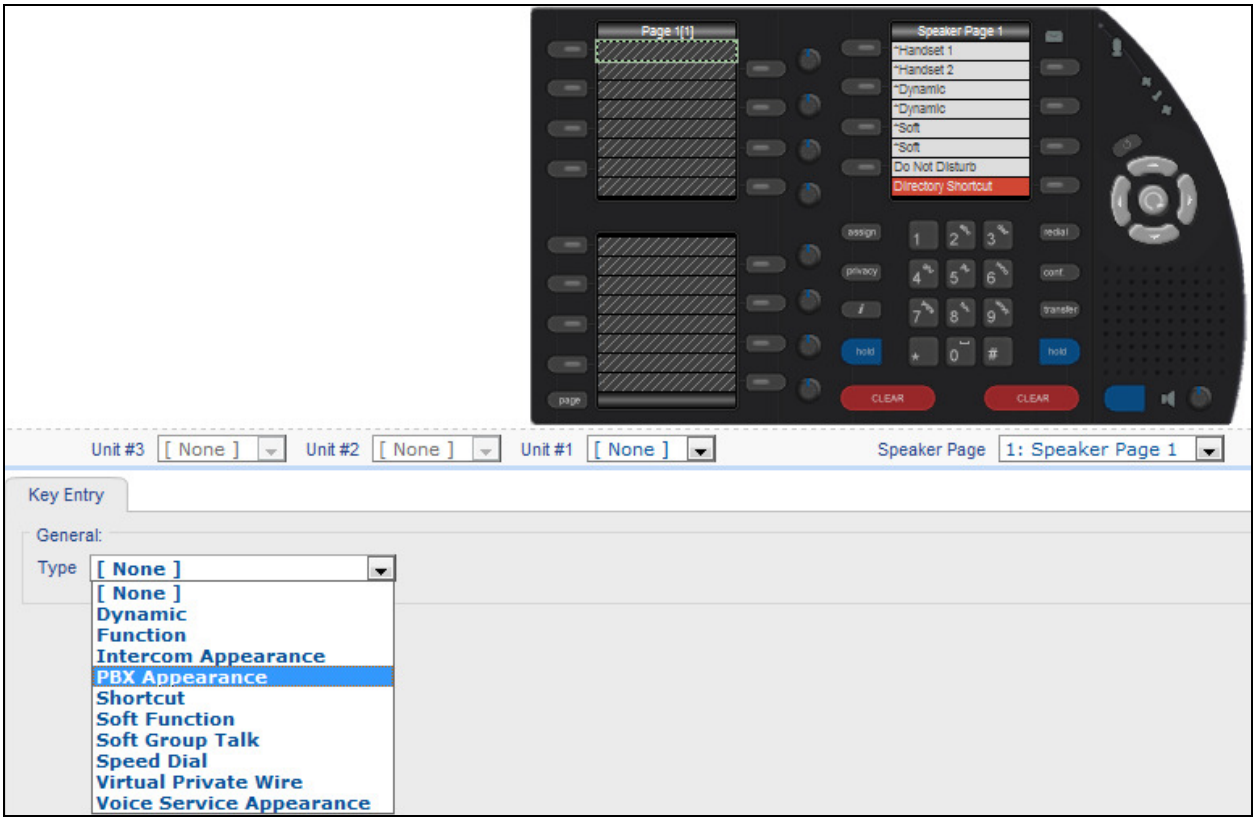
Select **Users →Users** in the left pane (not shown), select the user to be configured and click the **iTurret Layout** tab and ensure the default page **1:Page1** is selected from the **Page** drop down box, as shown below.



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.

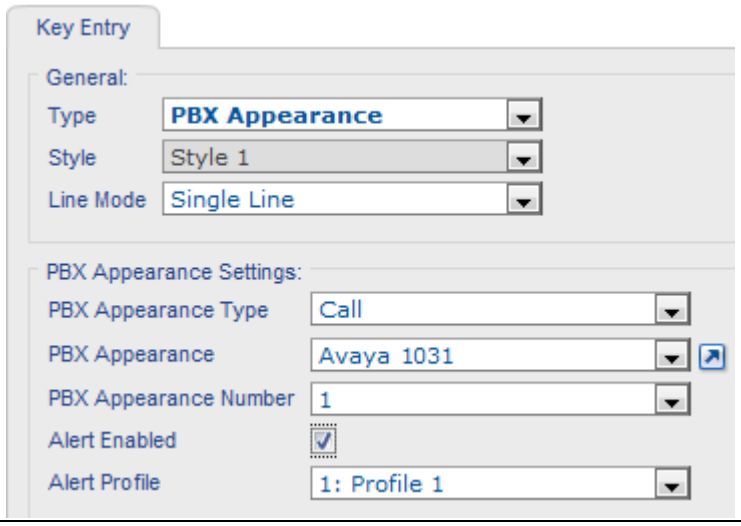
In the **Key Entry** tab select **PBX Appearance** from the **Type** field, as seen below.



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

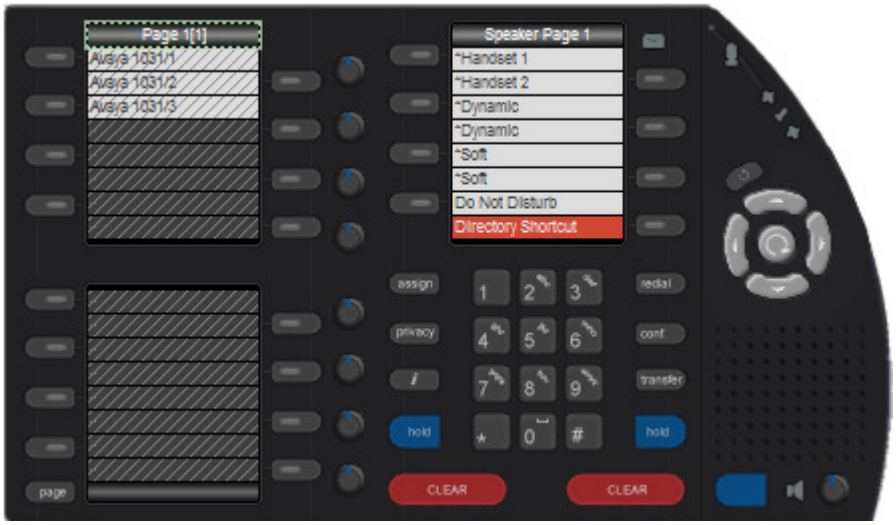
- Under the **PBX Appearance Settings**, select the **PBX Appearance Type** (**Call** in this case)
- **PBX Appearance** – select a configured **PBX Appearance**, in this case **6031**
- **PBX Appearance Number** (**1** in this case)
- Check **Alert Enabled**
- Leave **Profile 1** as default for **Alert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

Once completed, click **OK**.



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 Communication Manager configured in **Section 5.11**. In this example, 4 call-appr keys are administered in Communication Manager on endpoint 1031, then the Max PBX appearance value in iManager is configured to 4, which allows up to four instances of 1031 to be added on the iD808 iTurret layout and have up to four calls to and/or from the iD808 iTurret.

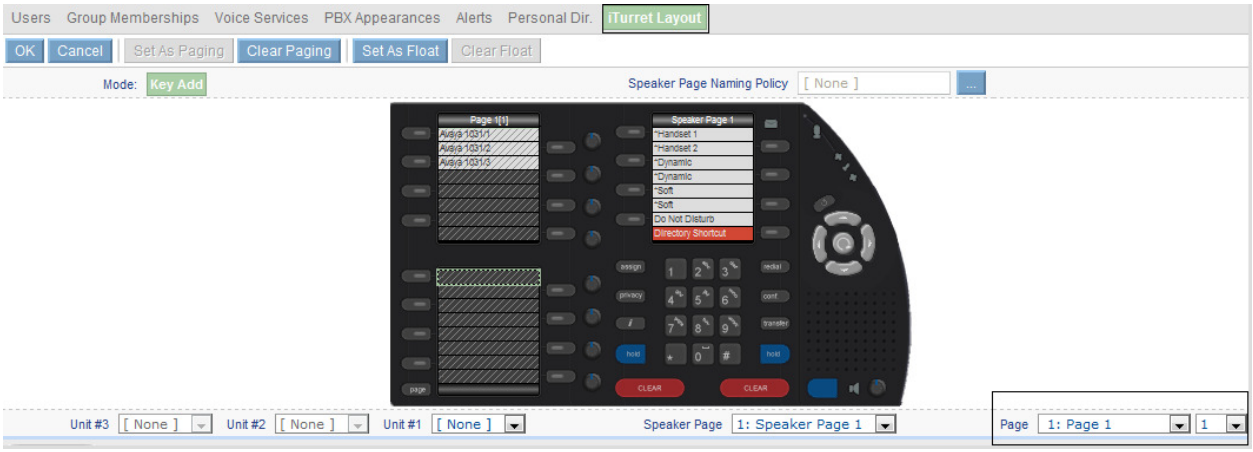
Repeat this procedure to add the next two call appearances and the layout looks as follows.



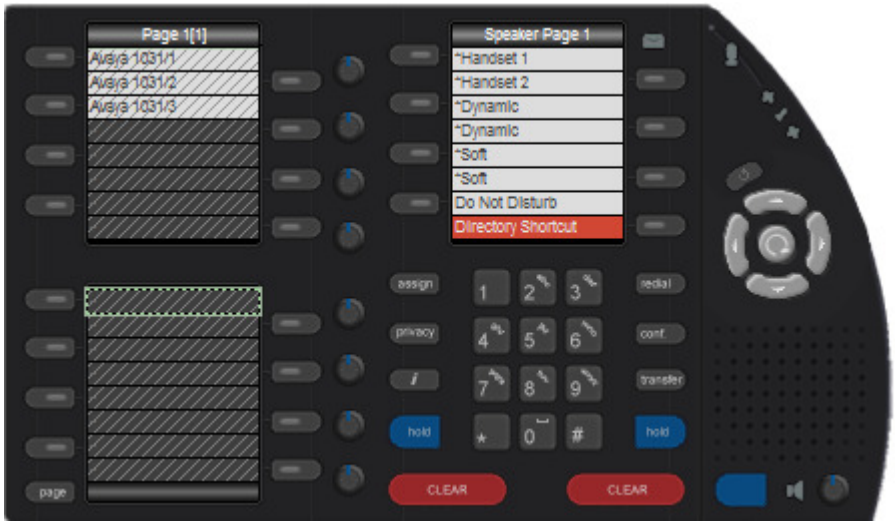
7.19. Assign a Bridge Call Appearance to iD808 iTurret Keys

This section describes how to create bridged appearance keys for the iD808 iTurret. 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 and click the **iTurret Layout** tab and ensure the default page **1:Page1** is selected from the **Page** drop down box, as shown below.

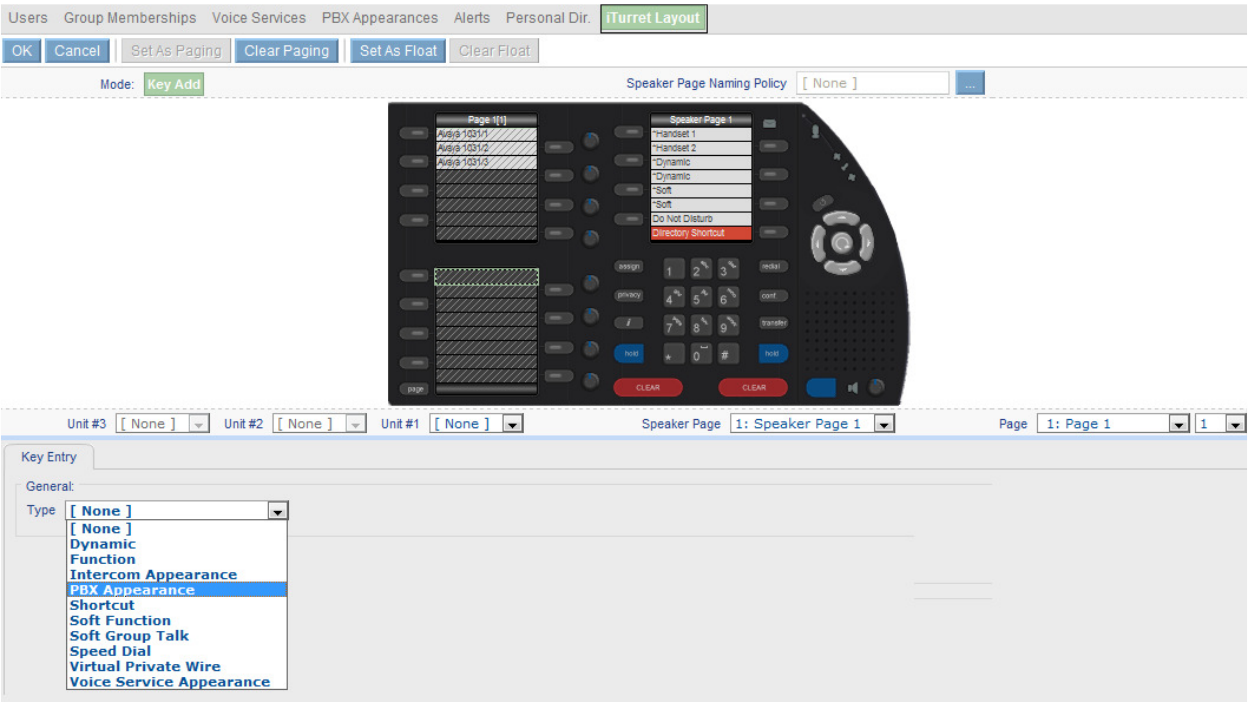


Select the next available key as highlighted by the white box below in the screenshot below.



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

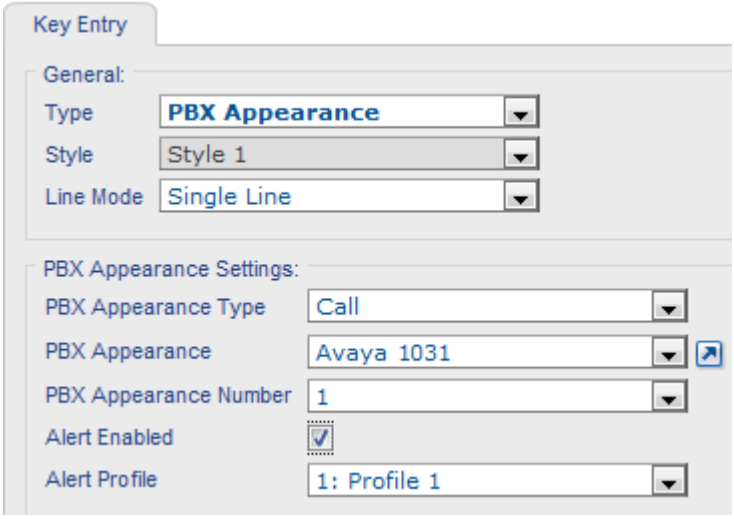
In the **Key Entry** tab configure **PBX Appearance** in the **Type** field as shown in the screenshot below.



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

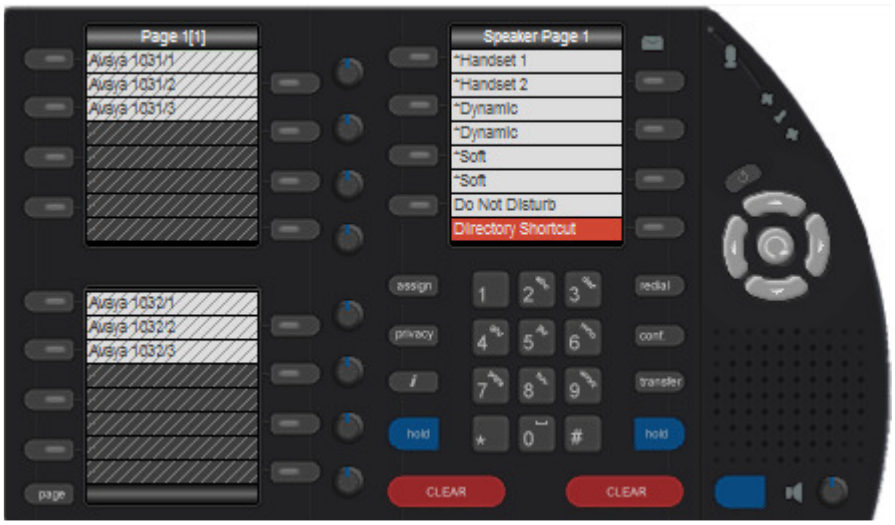
- **PBX Appearance** – select a configured PBX Appearance, in this case **6032**
- **PBX Appearance Number** (1 in this case)
- Check **Alert Enabled** and leave **Profile 1** as default for **Alert Profile**.

Once completed, click **OK**.



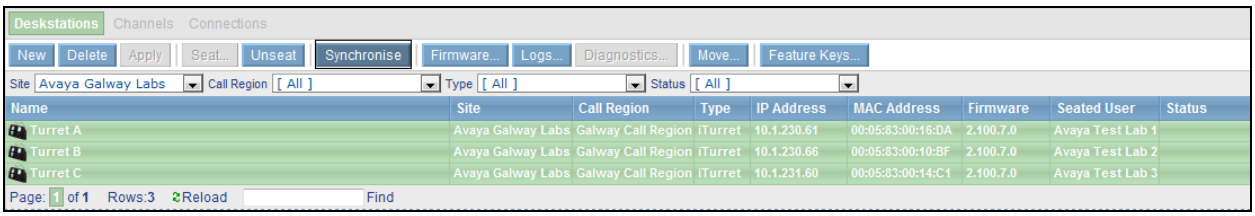
NOTE: The PBX Appearance Number setting will allow the user to be configured with multiple instances of the same extension number thus allowing the user to make and receive multiple calls to and from the same extension number. The PBX Appearance Number relates to the Maximum PBX Appearance setting configured 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 Communicaiton Manager configured in **Section 5.11**. In this example, 4 call-appr keys are administered on Communication Manager for endpoint 1031, then the Max PBX appearance value in iManager is configured to 4, which allows up to four instances of 1031 to be added on the iD808 iTurret layout and have up to four calls to and/or from the iD808 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 iD808 iTurret device. Select **Devices →Deskstations** (not shown) and select the desired deskstations and click the **Synchronise** button. The iD808 iTurrets will indicate that they are being synchronized on their displays. After the deskstations have been synchronized, the status icons on the iD808 iTurret corresponding to the network, iCMS, and SIP registrar status will be green.



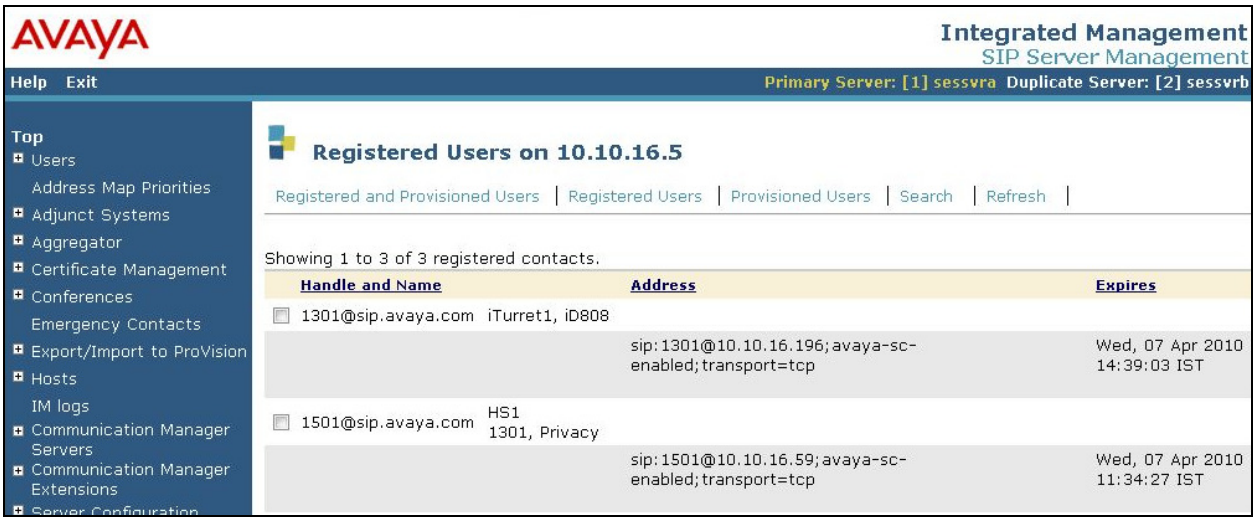
Note: Any changes made to the profile within iManager will be updated on the iD808 iTurret device after **OK** or **Apply** is pressed (some changes will require a synchronization, refer to the *Speakerbus iManager Administrator`s Guide* for more details).

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 iD808 iTurret, verify that the status icons are green. These status icons indicate whether iD808 iTurret is connected to the network, iCMS server, and SIP registrar (i.e., Avaya Aura® SIP Enablement Services). Refer to [5] for more details.

Verify that the iD808 deskstations have successfully registered with SIP Enablement Services. From the administration web page navigate to **Users → Search Registered Users** and click the **Search** button (not shown). This will display a list of registered users on SIP Enablement Services. In the screen below, User 1301 and its corresponding Privacy Handset 1501 are registered.



.

9. Conclusion

These Application Notes describe the compliance tested configuration of the Speakerbus iTurret Solution with Avaya Aura® Communication Manager and Avaya Aura® SIP Enablement Services. All tests passed successfully.

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*, 9th August 2010, Document Number 03-300509.

[2] *Avaya Extension to Cellular User Guide Avaya Aura® Communication Manager*, November 2009

[3] *SIP Support in Avaya Aura® Communication Manager Running on the Avaya S8xxx Servers*, May 2009, Issue 9, Document Number 555-245-206.

[4] *Installing and configuring Avaya Aura® SIP Enablement Services*, 5th January 2011, Document Number 03-603473.

[5] *Speakerbus iManager Administrator's Guide*, V1.220, Revision 6, March 2010.

[6] *Session Initiation Protocol Service Examples draft-ietf-sipping-service-examples-15*, Internet-Draft, 11th July 2008, available at http://tools.ietf.org/html/draft-ietf-sipping-service-examples-15

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.