**Avaya Solution & Interoperability Test Lab**

# Application Notes for configuring Speakerbus iD808 iTurret to Interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 – Issue 1.0

## Abstract


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

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

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

# 1. Introduction

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

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

Some OPS features listed in the following table can be invoked by dialing a Feature Name Extension (FNE). A speed dial button on iTurret can also be programmed to a FNE. Other features, such as Exclusion/Privacy and Call Forwarding, are available by using the AST (Advanced SIP Telephony) FNU (Feature Name URI). Avaya Aura® Communication Manager automatically handles many other standard features via OPS, such as call coverage, trunk selection using Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS), Class Of Service (COS), Class Of Restriction (COR), and voice messaging. Details on operation and administration of OPS can be found in References **[2]** and **[3]**. The Avaya SIP solution requires all SIP telephones to be configured in Avaya Aura® Communication Manager as OPS. Items in the table below shown in **bold** were tested using an FNU or FNE.

| FEATURE | SUPPORTED | | COMMENTS |
|---|---|---|---|
| | *Locally at the phone* | *With Avaya SIP Offer* | |
| **Basic Calling Features** | | | |
| Extension to Extension Call | Yes | Yes | |
| Basic Call to legacy phones | No | Yes | |
| Speed Dial Buttons | Yes | Yes | |
| Message Waiting Support | Yes | Yes | |
| **SIPPING-19 Features** | | | |
| Call Hold | YES | YES | |
| Consultation Hold | YES | YES | |
| Unattended Transfer | YES | YES | |
| Attended Transfer | YES | YES | |
| Call Forward All | YES | YES | Local menu option on 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** |
| **Call Pickup** | **NO** | **YES** | **Via OPS FNE** |
| Automatic Redial | NO | YES | Via OPS FNE |
| **OPS – Selected Additional Station-Side Features** | | | |
| Conference on answer | NO | YES | Via OPS FNE |
| **Directed call pickup** | **NO** | **YES** | **Via OPS FNE** |
| Drop last added party | NO | YES | Via OPS FNE |
| **Exclusion/Privacy** | **YES** | **YES** | **Local hard key on iTurret using FNU** |
| **Last number dialed** | **YES** | **YES** | **Via OPS FNE** |
| Priority Call | NO | YES | Via OPS FNE, iTurret doesn`t support distinctive ring indication |
| **Send All Calls** | **NO** | **YES** | **Via OPS FNE** |
| **Send All Calls Cancel** | **NO** | **YES** | **Via OPS FNE** |
| Transfer to Voicemail | NO | YES | Via OPS FNE |
| **Whisper Page** | **NO** | **YES** | **Via OPS FNE** |

**Table 1**

# 2. General Test Approach and Test Results

To verify interoperability of the iD808 iTurret with Communication Manager and Session Manager, calls were made between iD808 Deskstations and Avaya SIP, H.323 and Digital stations using various codec settings and exercising common PBX features. The telephony features were activated and deactivated using buttons and menu options on iTurret, FNEs, and FNUs.

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

## 2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

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

## 2.2. Test Results

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

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

## 2.3. Support

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

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

# 3. Reference Configuration

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

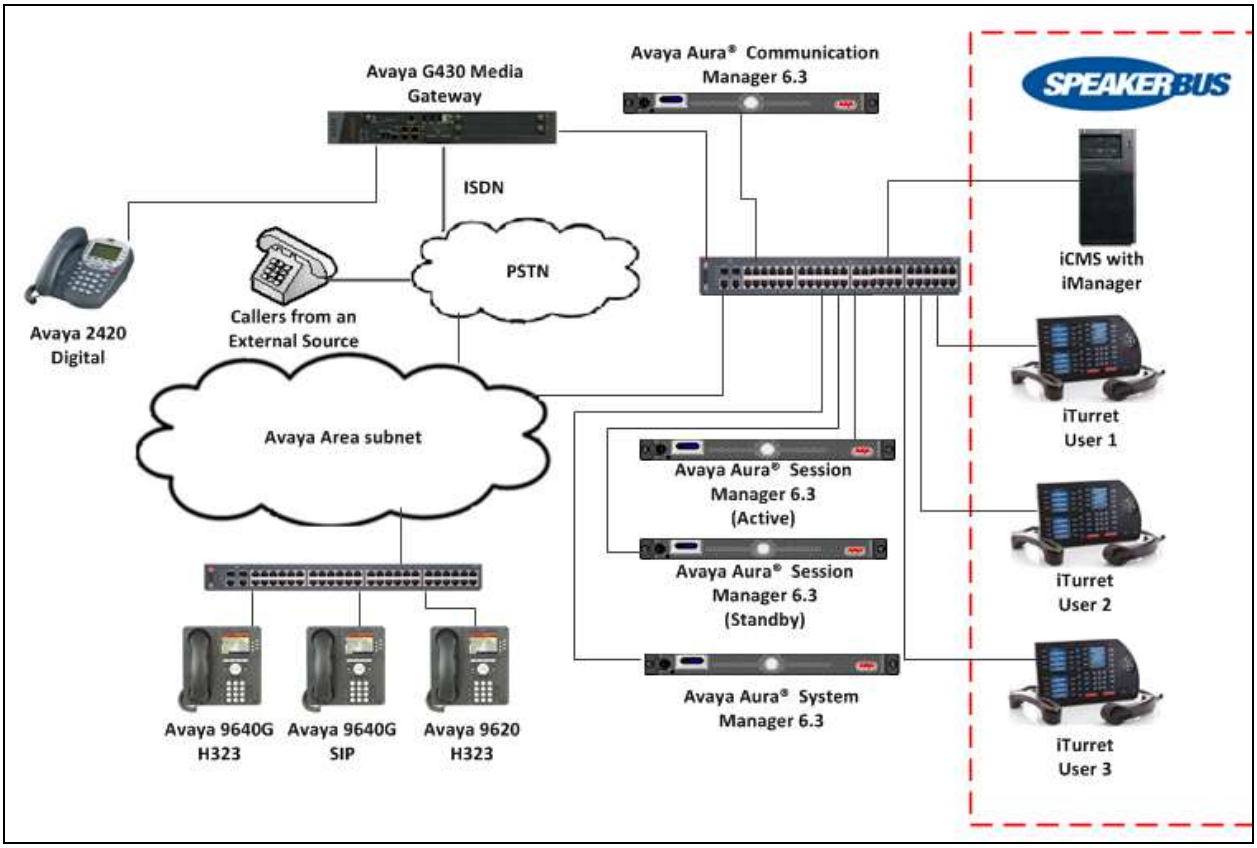



**Figure 1: Avaya Aura® Communication Manager and Avaya Aura® Session Manager with Speakerbus Solution**

# 4. Equipment and Software Validated

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

| **Avaya Equipment/Software** | **Release/Version** |
|---|---|
| Avaya Aura® Communication Manager running on VMware | R6.3 Build R016x.03.0.124.0<br>S/W update 03.0.124.0-21591 |
| Avaya Aura® Session Manager running on VMware | R6.3.11.0.631103 |
| Avaya Aura® Session Manager running on VMware | R6.3.7.0.637008 |
| Avaya Aura® System Manager running on VMware | R6.3.11<br>Build No. 6.3.0.8.5682-6.3.8.4711<br>S/W update 6.3.11.8.2871 |
| Avaya Aura® Messaging running on VMware | R6.3-68.0 |
| Avaya 96xx IP phones<br>9640G (H.323)<br>9620D (H.323)<br>9640G (SIP)<br>Avaya 2420 Digital phone | <br>3.2.2A<br>3.1.1S<br>2.6.10.1<br>Rel 6.0, FWV 6 |
| Avaya G430 Media Gateway<br>Module MM710 (DSP MP20)<br>Avaya Media Gateway DSP module | Version 36.7.0/1<br>Version HW04 FW021<br>MP20 FW 132 |
| **Speakerbus Equipment/Software** | **Release/Version** |
| Speakerbus iCMS with iManager Administration running on Windows Server 2008 R2 | v2.510.4.0 |
| Speakerbus iD808 iTurret | v2.20 SIP |

# 5. Configure Avaya Aura® Communication Manager

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

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

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

## 5.1. Verify System Capacity

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

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

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

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

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

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

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

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

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

## 5.2. Define System Features

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

```
change system-parameters features                             Page  18 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS

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

WHISPER PAGE
   Whisper Page Tone Given To: all

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

                                 Pickup On Transfer? y
```

On **Page 19** make sure **Directed Call Pickup** is set to **y.**

```
change system-parameters features                                Page  19 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS
IP PARAMETERS
                   Direct IP-IP Audio Connections? y
                             IP Audio Hairpinning? n
                          Synchronization over IP? n
              SDP Capability Negotiation for SRTP? y
                    SIP Endpoint Managed Transfer? n

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


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

## 5.3. Define the Dial Plan

Use the **change dialplan analysis** command to define the dial plan used in the system. This includes all telephone extensions, OPS Feature Name Extensions (FNEs), and Feature Access Codes (FACs). To define the FNEs for the OPS features listed in Error! Reference source not found., a Feature Access Code (FAC) must also be specified for the corresponding feature. In the sample configuration, telephone extensions are four digits long and begin with **2** and **3**, FNEs are also four digits beginning with **2**, and the FACs have formats as indicated with a **Call Type** of **fac**.

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

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

```
#            3   fac
```

## 5.4. Define Feature Access Codes (FACs)

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

```
change feature-access-codes                                     Page   1 of  10
                                FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *14
                       Answer Back Access Code: *06

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All: *03    Deactivation: *04
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: *16
                        Call Pickup Access Code: *17
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code: *51
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

```
change feature-access-codes                                     Page   2 of  10
                                FEATURE ACCESS CODE (FAC)
                   Contact Closure  Pulse Code:

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

```
change feature-access-codes                                      Page   3 of  10
                                FEATURE ACCESS CODE (FAC)
            Leave Word Calling Send A Message: *86
           Leave Word Calling Cancel A Message: *87
   Limit Number of Concurrent Calls Activation:        Deactivation:
             Malicious Call Trace Activation:        Deactivation:
         Meet-me Conference Access Code Change:
          Message Sequence Trace (MST) Disable:

 PASTE (Display PBX data on Phone) Access Code:
  Personal Station Access (PSA) Associate Code:        Dissociate Code:
        Per Call CPN Blocking Code Access Code: *33
      Per Call CPN Unblocking Code Access Code: *34
                   Posted Messages Activation:        Deactivation:
                 Priority Calling Access Code: *18
                          Program Access Code:

       Refresh Terminal Parameters Access Code:
              Remote Send All Calls Activation:        Deactivation:
               Self Station Display Activation:
                     Send All Calls Activation: *38    Deactivation: *39
         Station Firmware Download Access Code:
```

```
change feature-access-codes                                      Page   4 of  10
                                FEATURE ACCESS CODE (FAC)
                             Station Lock Activation:      Deactivation:
            Station Security Code Change Access Code:
                    Station User Admin of FBI Assign:      Remove:
        Station User Button Ring Control Access Code:
                  Terminal Dial-Up Test Access Code:
      Terminal Translation Initialization Merge Code:      Separation Code:
                  Transfer to Voice Mail Access Code:
                Trunk Answer Any Station Access Code:
                    User Control Restrict Activation:      Deactivation:
        Voice Coverage Message Retrieval Access Code:
       Voice Principal Message Retrieval Access Code:
                 Whisper Page Activation Access Code: *58
           3PCC H323 Override SIP Station Activation:      Deactivation:

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

## 5.5. Define Feature Name Extensions (FNEs)

The OPS FNEs can be defined using the **change off-pbx-telephone feature-name-extensions set 1** command. The following screens show in bold the FNEs defined for use with the sample configuration.

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

        Active Appearance Select:
             Automatic Call Back:
      Automatic Call-Back Cancel: 2699
                Call Forward All: 2698
     Call Forward Busy/No Answer:
             Call Forward Cancel:
                       Call Park: 2697
           Call Park Answer Back: 2696
                    Call Pick-Up: 2695
           Calling Number Block:
         Calling Number Unblock:
  Conditional Call Extend Enable:
 Conditional Call Extend Disable:
             Conference Complete:
            Conference on Answer:
           Directed Call Pick-Up: 2694
           Drop Last Added Party:
```

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

       Exclusion (Toggle On/Off):
      Extended Group Call Pickup:
          Held Appearance Select:
          Idle Appearance Select:
              Last Number Dialed: 2692
            Malicious Call Trace:
     Malicious Call Trace Cancel:
             Off-Pbx Call Enable:
            Off-Pbx Call Disable:
                   Priority Call:
                          Recall:
                  Send All Calls: 2691
            Send All Calls Cancel: 2690
                Transfer Complete:
             Transfer On Hang-Up:
          Transfer to Voice Mail:
         Whisper Page Activation: 2693
```

## 5.6. Configure Class of Service (COS)

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

```
change cos-group 1                                          Page   1 of   2
CLASS OF SERVICE         COS Group: 1   COS Name:

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

## 5.7. Configure Class of Restriction (COR)

Use the **change cor n** command where **n** is the number of the COR being configured, to enable applicable calling features. To use the Directed Call Pickup feature, the **Can Be Picked Up By Directed Call Pickup** and **Can Use Directed Call Pickup** fields must be set to **y**. In the sample configuration, the iTurrets were assigned to COR **1**.

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

               COR Number: 1
          COR Description:

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

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

## 5.8. Add Coverage Path

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

```
add coverage path 89                                          Page   1 of   1
                                COVERAGE PATH

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

COVERAGE CRITERIA

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

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

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

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

## 5.9. Configure Route Pattern

Enter the command **change route-pattern 1** where route pattern 1 is used to route calls between Communication Manager and Session Manager. Enter an identifying **Pattern Name**. Ensure that both SIP trunk-groups are configured in the **Grp No** fields and enter an **FRL** as appropriate. In the instance where all the channels in trunk-group 1 are in use, or trunk-group 1 is out of service, traffic between Communication Manager and Session Manager will route over trunk-group 15.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: to SMs
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 1    0                                                            n   user
 2: 15   0                                                            n   user
 3:                                                                   n   user
 4:                                                                   n   user
 5:                                                                   n   user
 6:                                                                   n   user

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

## 5.10. Configure IP-Codec Set

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

```
change ip-codec-set 1                                           Page   1 of   2

                           IP Codec Set

    Codec Set: 1

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


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

## 5.11. Configure Private Numbering

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

- **Ext Len** – Set to the extension length of the SIP extension number, in this case **4**
- **Ext Code** – Set to the first digit of the SIP extension number, in this case **1**
- **Trk Grp** – Enter the SIP trunk groups configured above, in this case **1** and **15**
- **Total Len** – Enter the total length of the SIP extension number, in this case **4**

```
change private-number 0                                         Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

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

# 6. Configure Avaya Aura® Session Manager

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

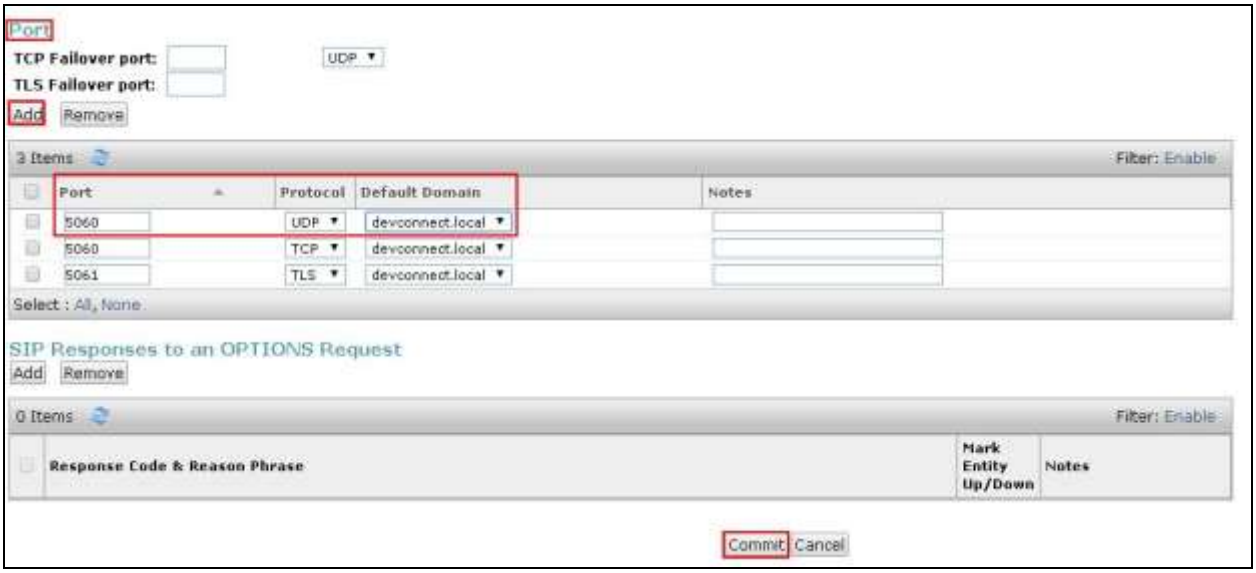
Session Manager is managed via System Manager. Using a web browser, access **https://<ip-addr of System Manager>/SMGR**. In the **Log On** screen, enter appropriate **User ID** and **Password** and click the **Log On** button.

## 6.1. Configure UDP Port for Speakerbus Registration

Each Session Manager Entity must be configured so that the iTurret can register to it using UDP. From the web interface click **Routing → SIP Entities → SM63** (not shown) where **SM63** is the first Session Manager entity. In the **Port** section, click **Add** and enter the following:

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

Click **Commit** when done.



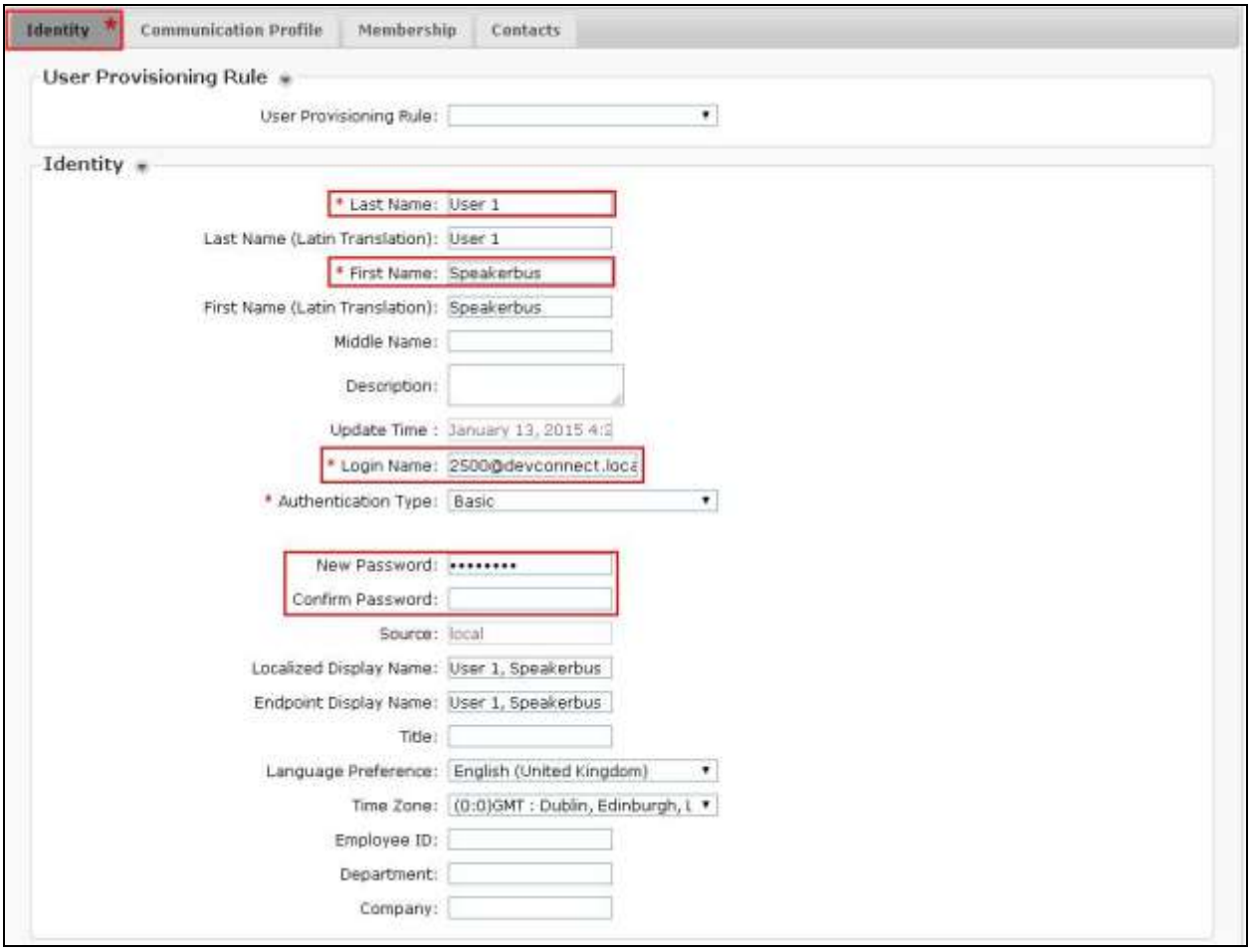

Repeat accordingly on the alternative Session Manager.

## 6.2. Add Primary iTurret User

The Speakerbus iD808 iTurret requires up to three stations for each device. The first station is referred to as the main appearance. The second and third stations are referred to as the privacy handsets. The privacy handsets are needed when privacy is required. If the privacy feature is not needed, then only the first station is required.
As the addition of stations is considered a very complex configuration, a detailed knowledge of the installation is required. Speakerbus personnel will be required to carry out this configuration.

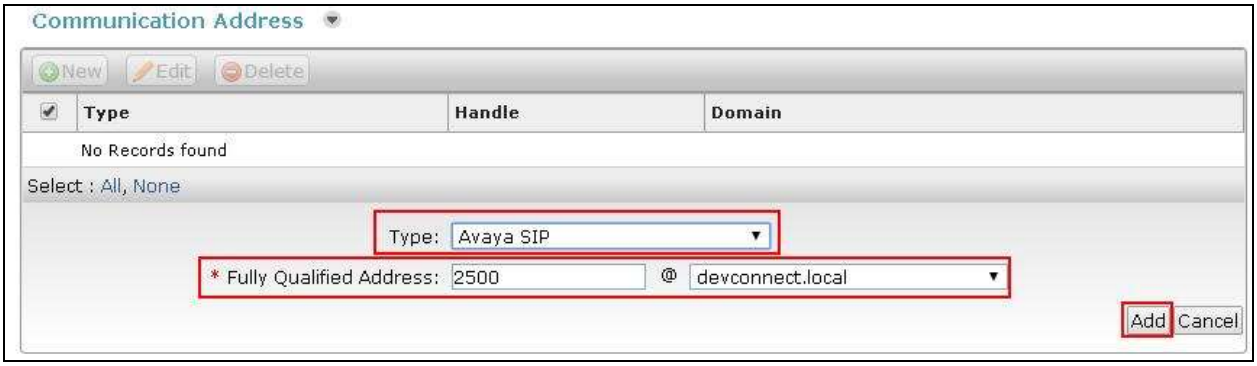
A user must be added for each iTurret. Click **User Management → Manage Users → New** (not shown) and configure as following in the **Identity** tab.

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

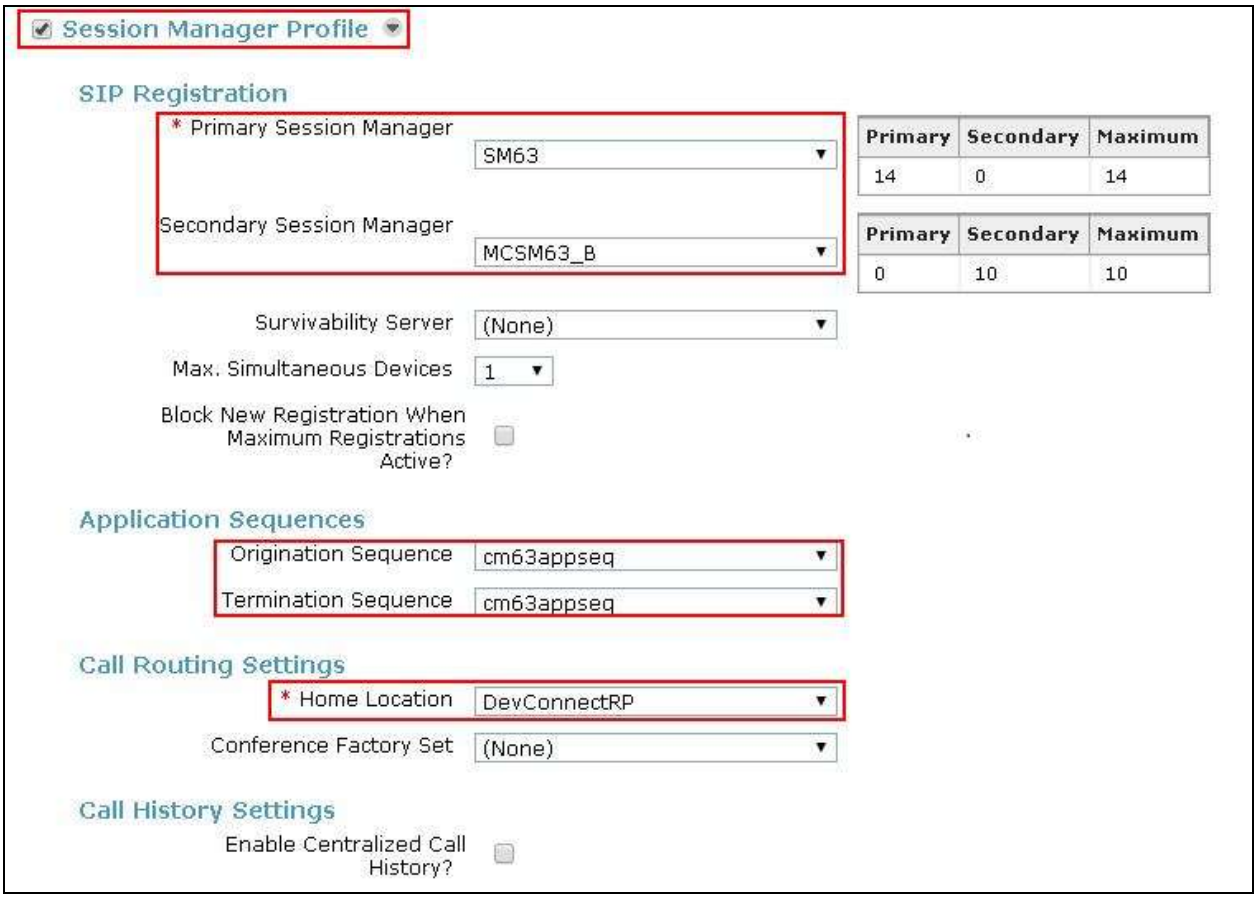


Click the **Communication Profile** tab and in the **Communication Profile Password** and **Confirm Password** fields, enter a numeric password. This will be used to register the iTurret during login. Click **New** to continue.


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



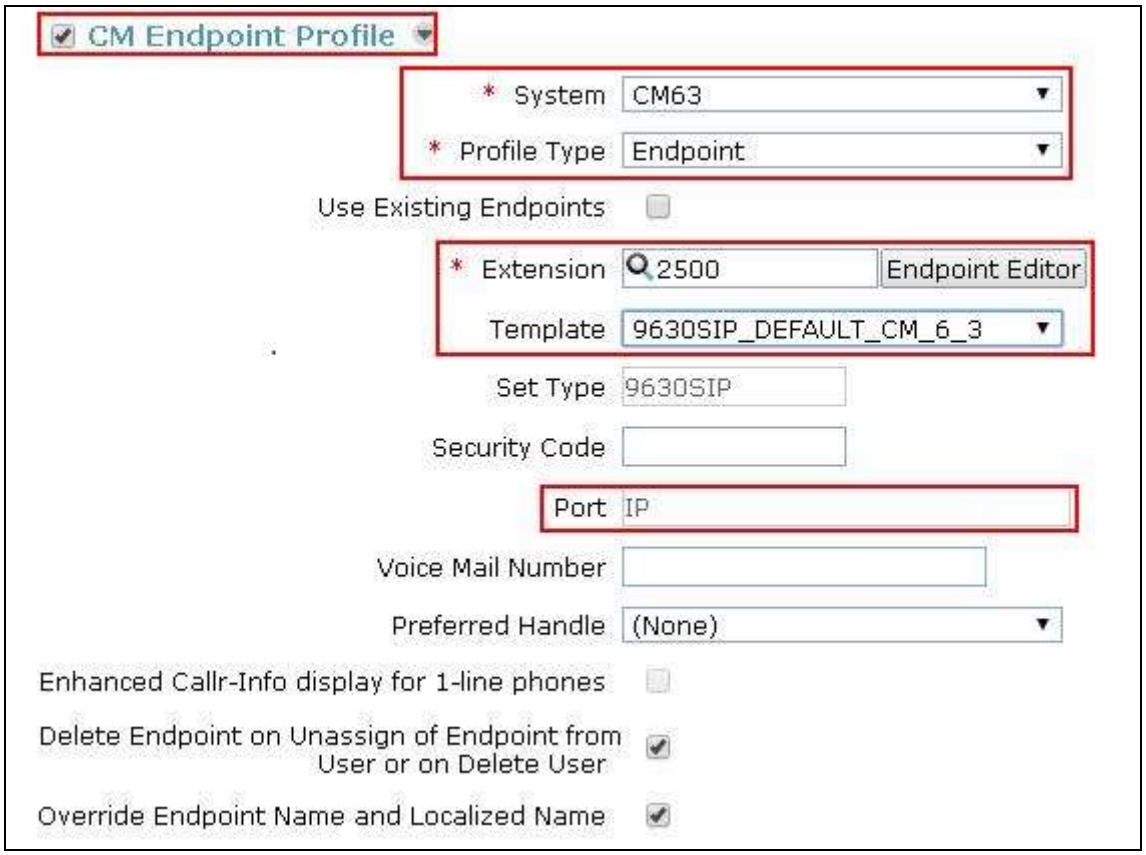
Place a tick in the **Session Manager Profile** check box and configure the **Primary Session Manager, Secondary Session Manager, Origination Application Sequence, Termination Application Sequence** and **Home Location,** from the respective drop down lists. The Primary and Secondary Session Manager are **SM63** and **MCSM63_B** respectively.



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

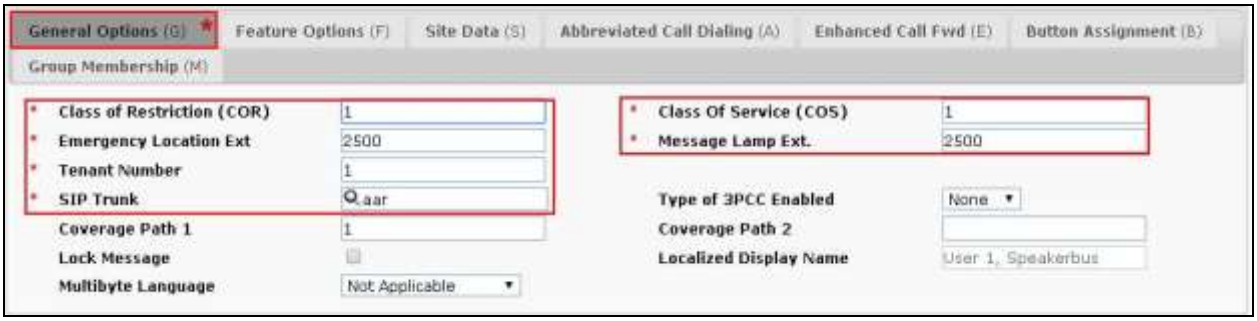
- **System** Select the relevant Communication Manager SIP Entity from the drop down list
- **Profile Type** Select **Endpoint** from the drop down list
- **Extension** Enter the required extension number, in this case **2500**
- **Template** Select **DEFAULT_9630SIP_CM_6_3** from the drop down list
- **Port** Enter **IP**

Click on **Endpoint Editor**.

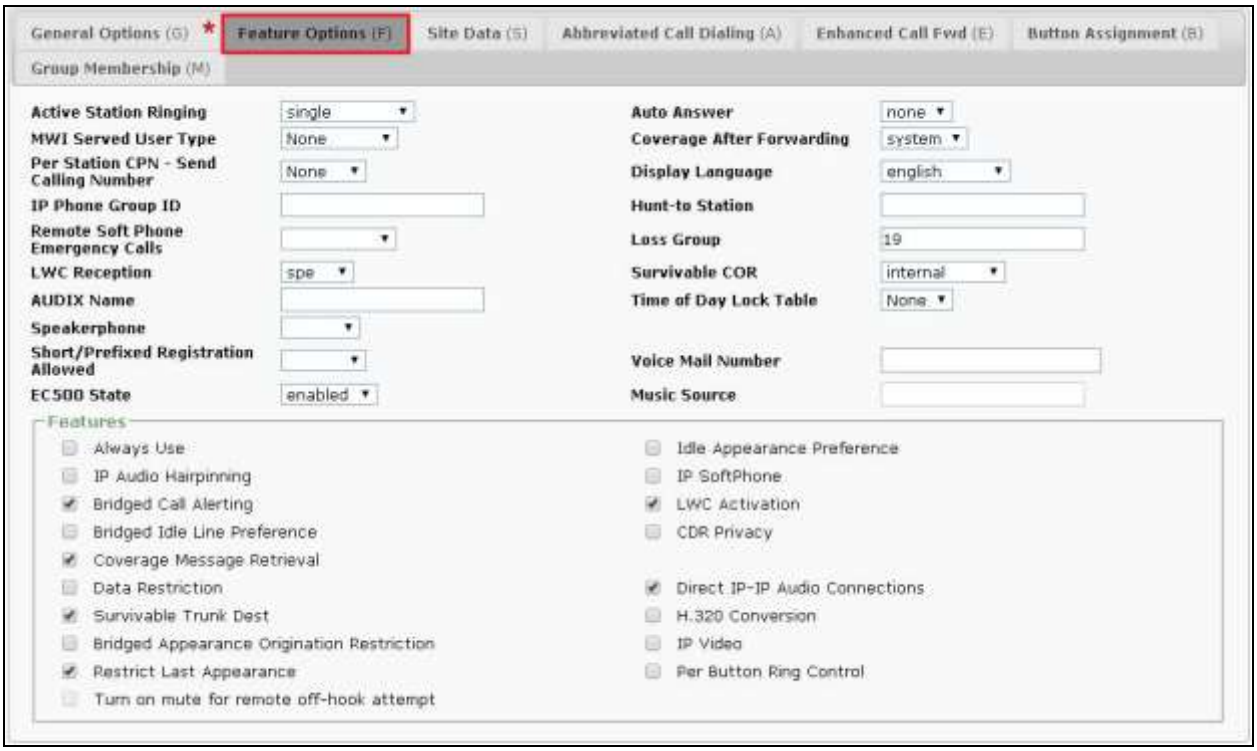


Click on the **General Options** tab and enter the following:

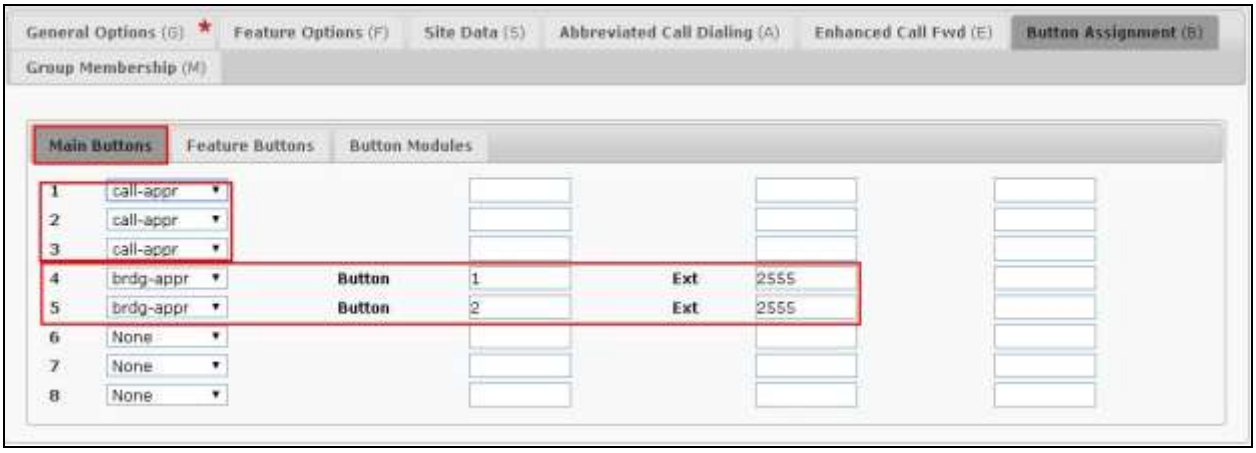
- **Class of Restriction (COR)** — Enter the **COR** as configured in **Section 5.7**
- **Emergency Location Ext** — Enter **2500**
- **Tenant Number** — Enter the required **Tenant Number**
- **SIP Trunk** — Enter **AAR**
- **Class of Service (COS)** — Enter the **COS** as configured in **Section 5.6**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



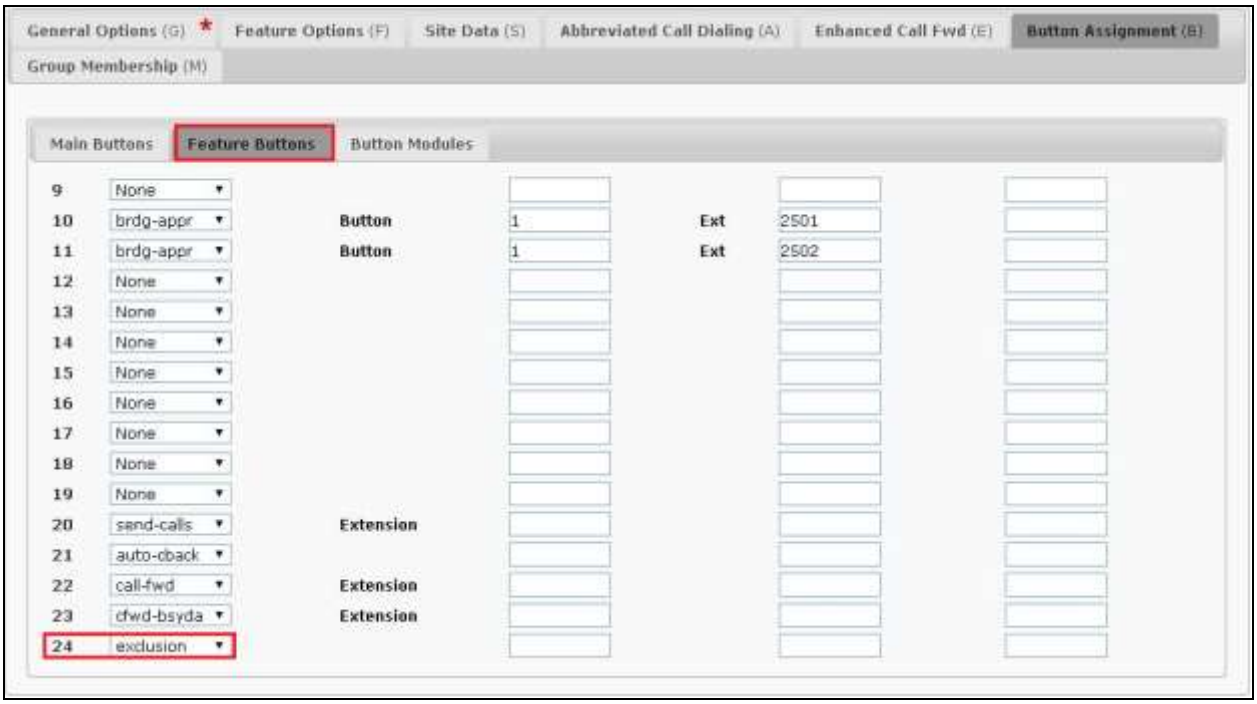

Click on the **Feature Options** tab. The screen shot below shows the Feature options that were used during compliance testing.



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




Click on **Feature Buttons** and configure as per screen shot below. Click **Commit** when done (not shown).
**Note:** Extensions 2501 and 2502 are the privacy users for iTurret 2500 and button 24 is configured as **exclusion**.

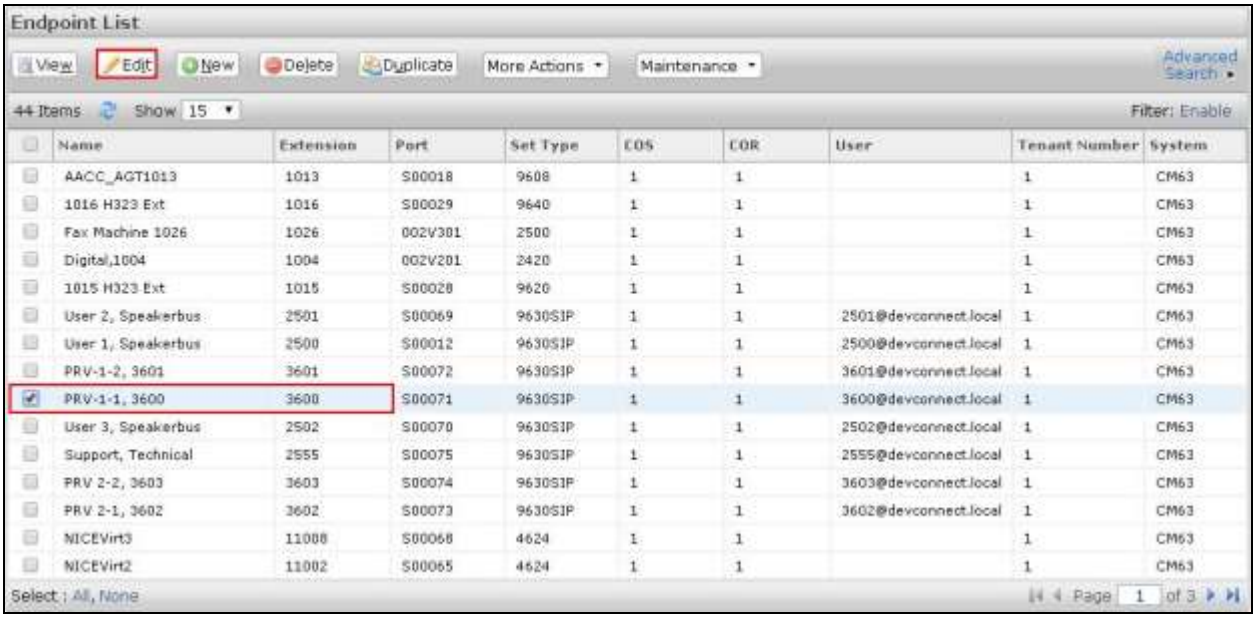


## 6.3. Configure Privacy Users

Privacy users are configured on System Manager as bridged appearances to the Primary User. Add a Privacy User in the same way as the Primary User is configured in **Section 6.2**. In this case the Privacy Users created for Extension 2500 are extensions 3600 and 3601.
**Note:** The Privacy Users were previously configured and are outside the scope of these Application Notes.

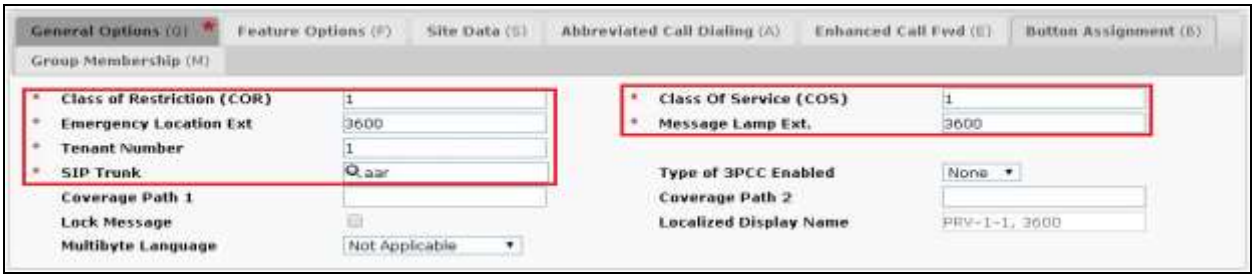
## 6.4. Configure Privacy Endpoint

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

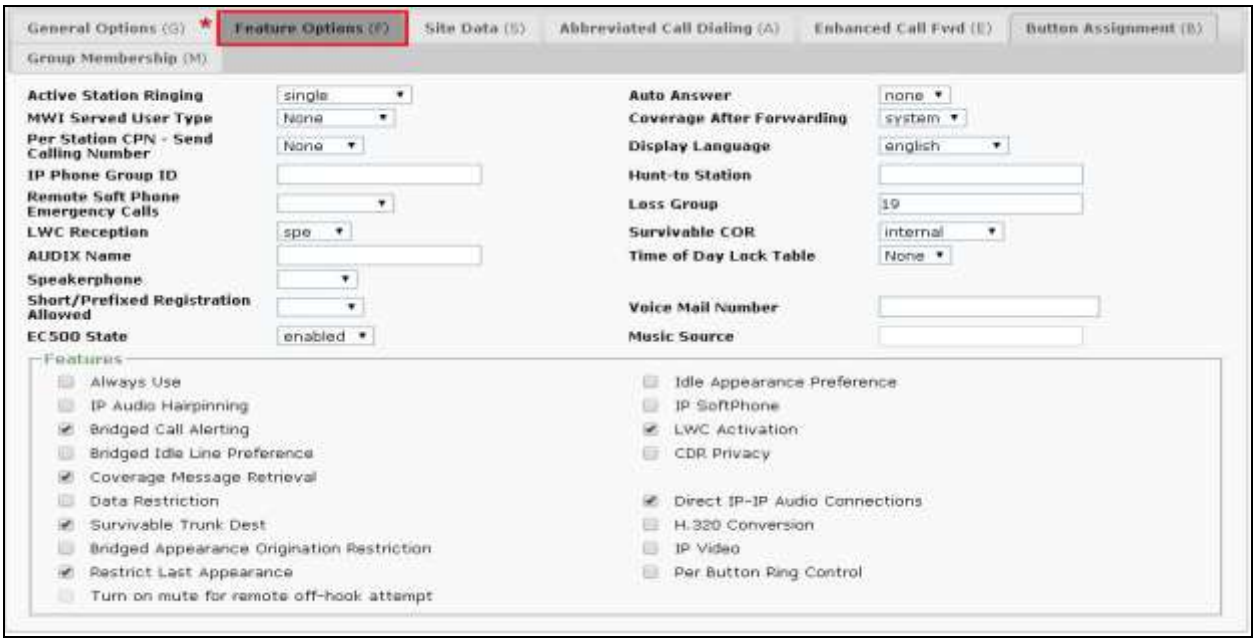



Click on the **General Options** tab and enter the following:

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

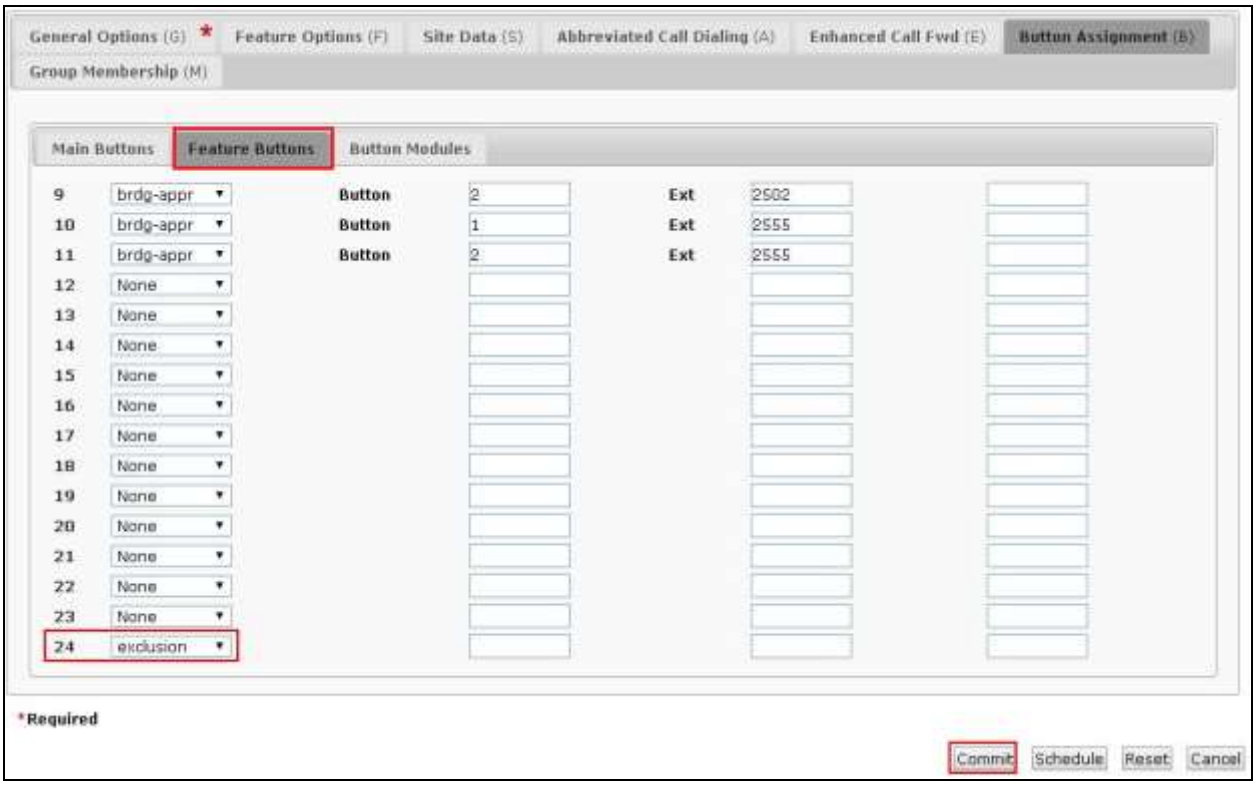


Click on the **Feature Options** tab. The screen shot below shows the Feature options that were used during compliance testing.



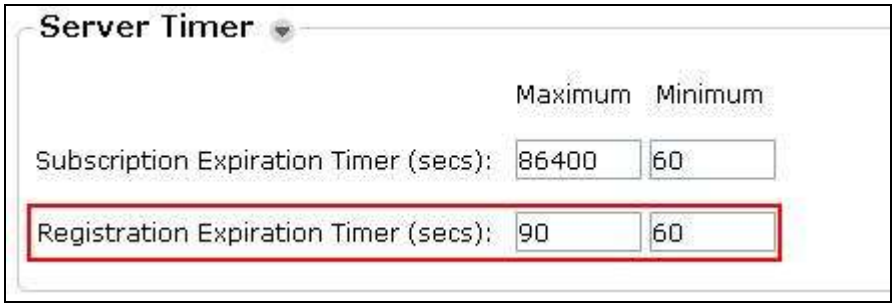

Click on the **Button Assignments tab** (Main buttons) and configure Buttons 1, 2 and 3 as **call-appr**. During compliance buttons 4, 5 and 6 were configured as **brdg-appr** to extension 2500 (Primary iTurret User). Button 7 was configured as **brdg-appr** to extension 2501 (Privacy key for user 2501).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

Click on **Feature Buttons** and configure as per screen shot below. Click **Commit** when done. **Note:** Button 24 is configured as **exclusion**.




## 6.5. Configure Registration Expiration Timer

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



# 7. Speakerbus iTurret Configuration

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

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

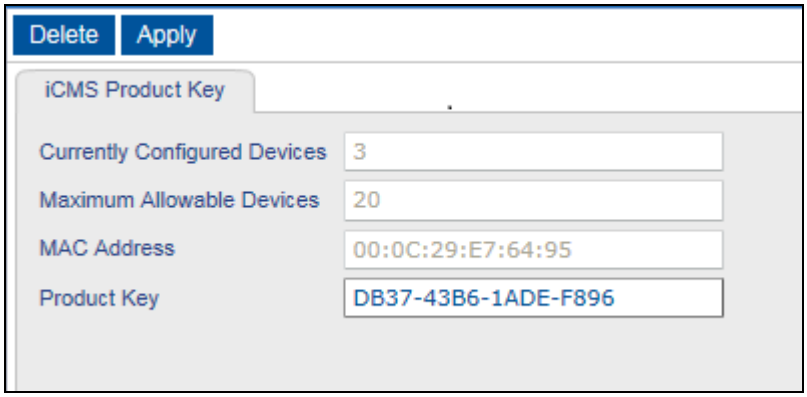
**Note:** This section displays some the configuration screens that may have already been configured.

## 7.1. Launch iManager Web Portal

To access the iManager software interface, open a web browser and type the iManager web address, for example, http://10.10.16.240/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 (not shown) in the left pane to verify that a valid key is installed and sufficient devices are allowed.



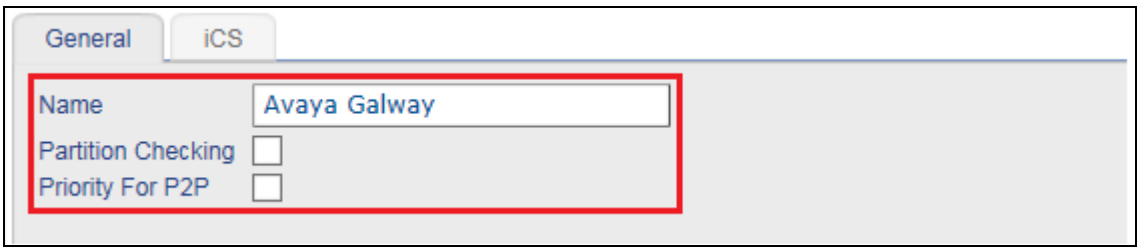
## 7.3. Create a Site

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


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

## 7.4. Create a Call Region

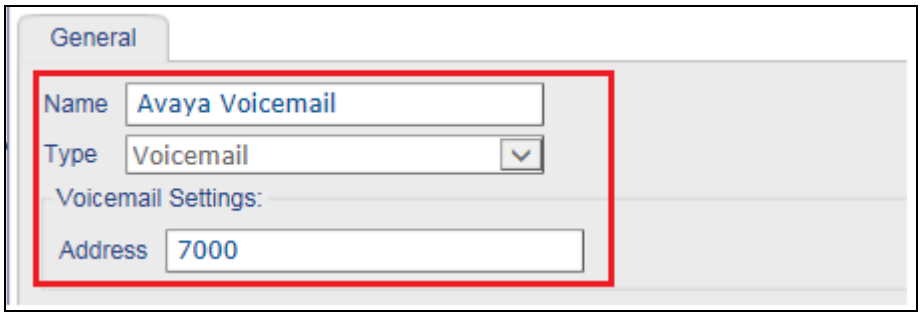
Call regions represent part of an organisation`s network. Select **Network →Call Regions** in the left pane (not shown), click on **NEW** (not shown) and enter an identifying **Name** for the new call region, leave the **Partition Checking** and **Priority for P2P** boxes unchecked, and press **OK** as shown below.



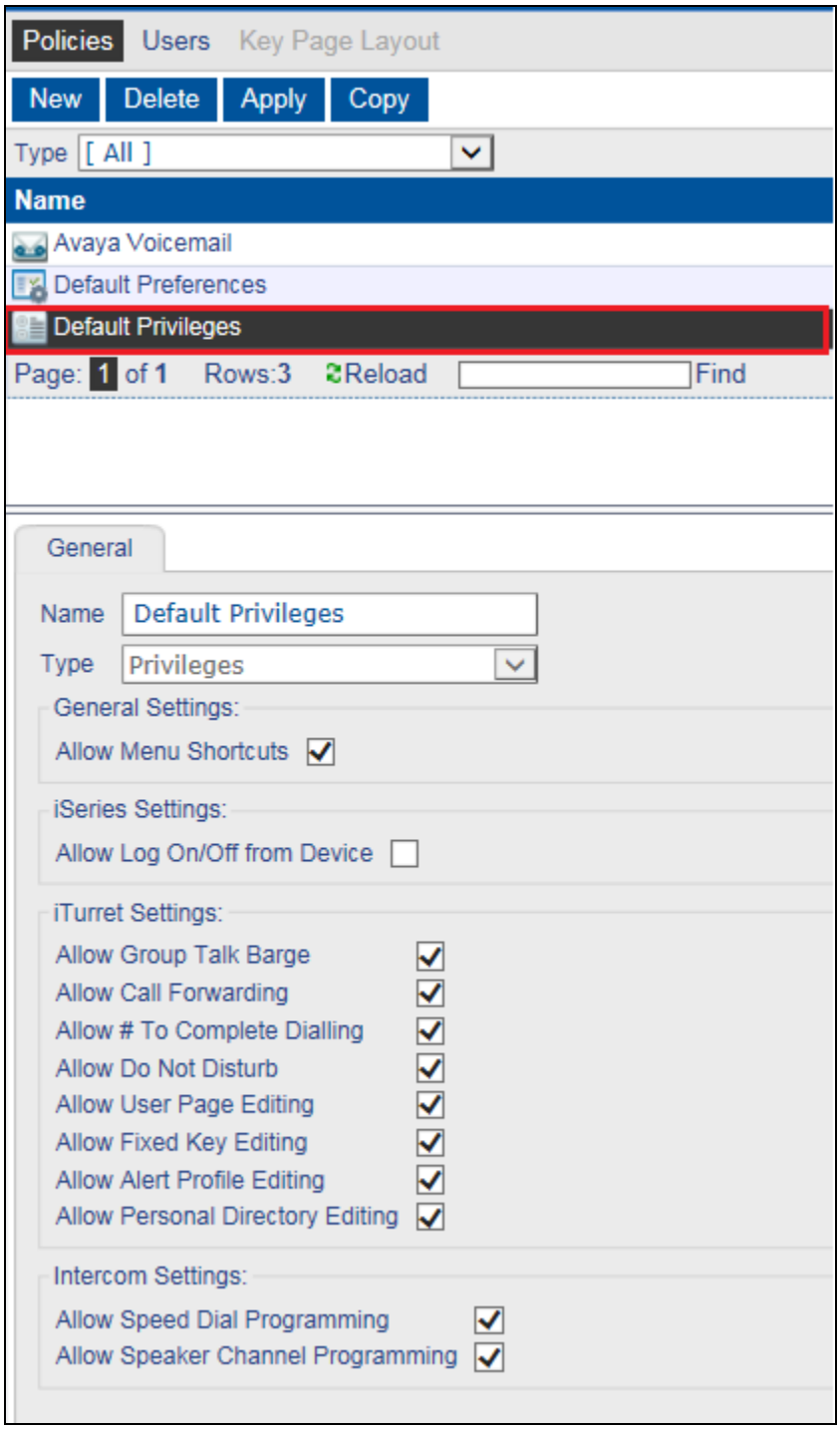

**Note**: A default call region is available and can be used for a single site setup. Refer to the *Speakerbus iManager Administrator`s Guide* for further configuration information.

## 7.5. Creating/Verifying User policies

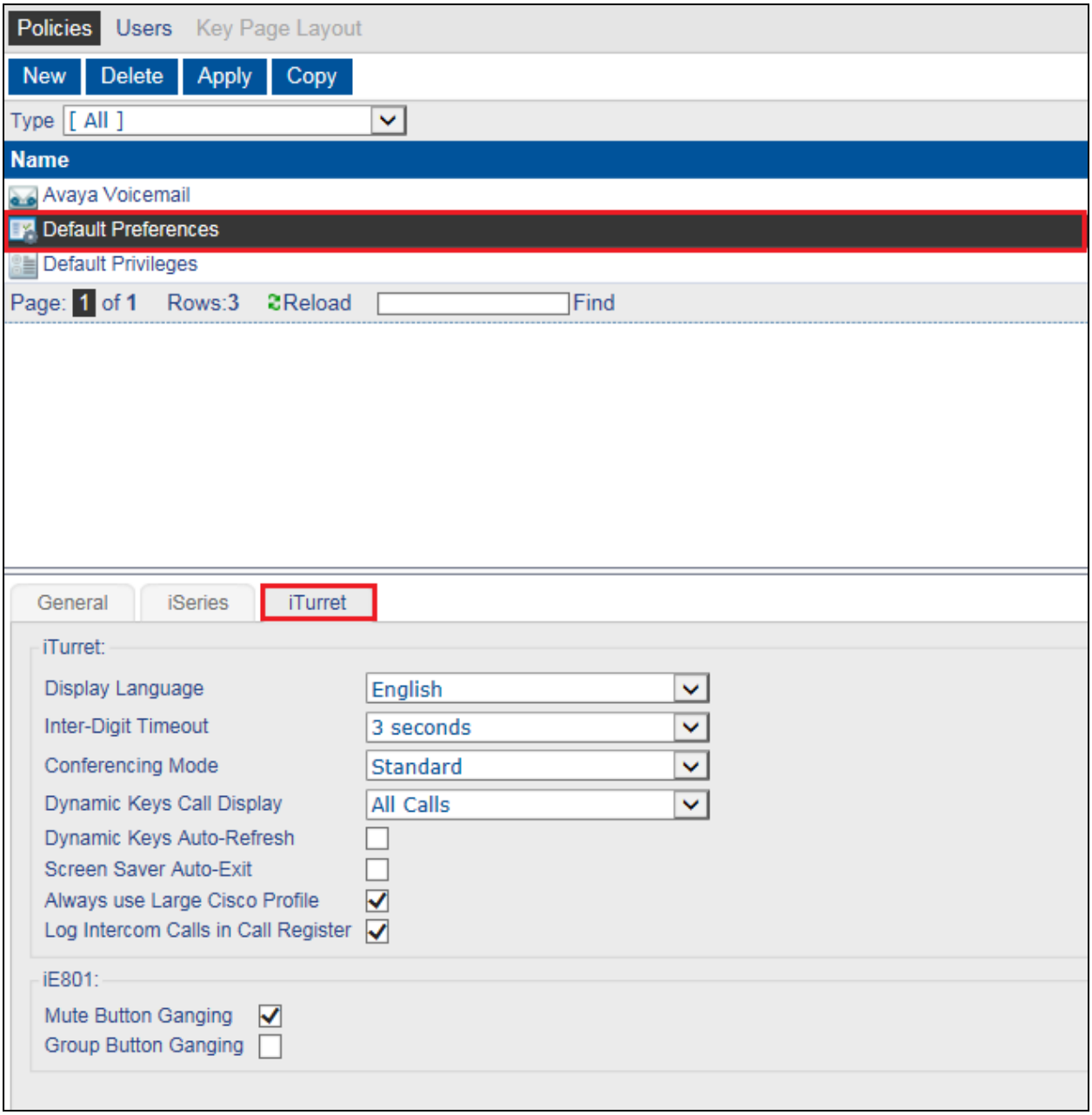
Select **Users → Policies** in the left pane (not shown) and click on **NEW** (not shown). Enter an identifying **Name**, in the **Type** dropdown box select **Voicemail,** and enter a valid address for the voicemail server**,** in this case a pre-configured hunt group number for voicemail access is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



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

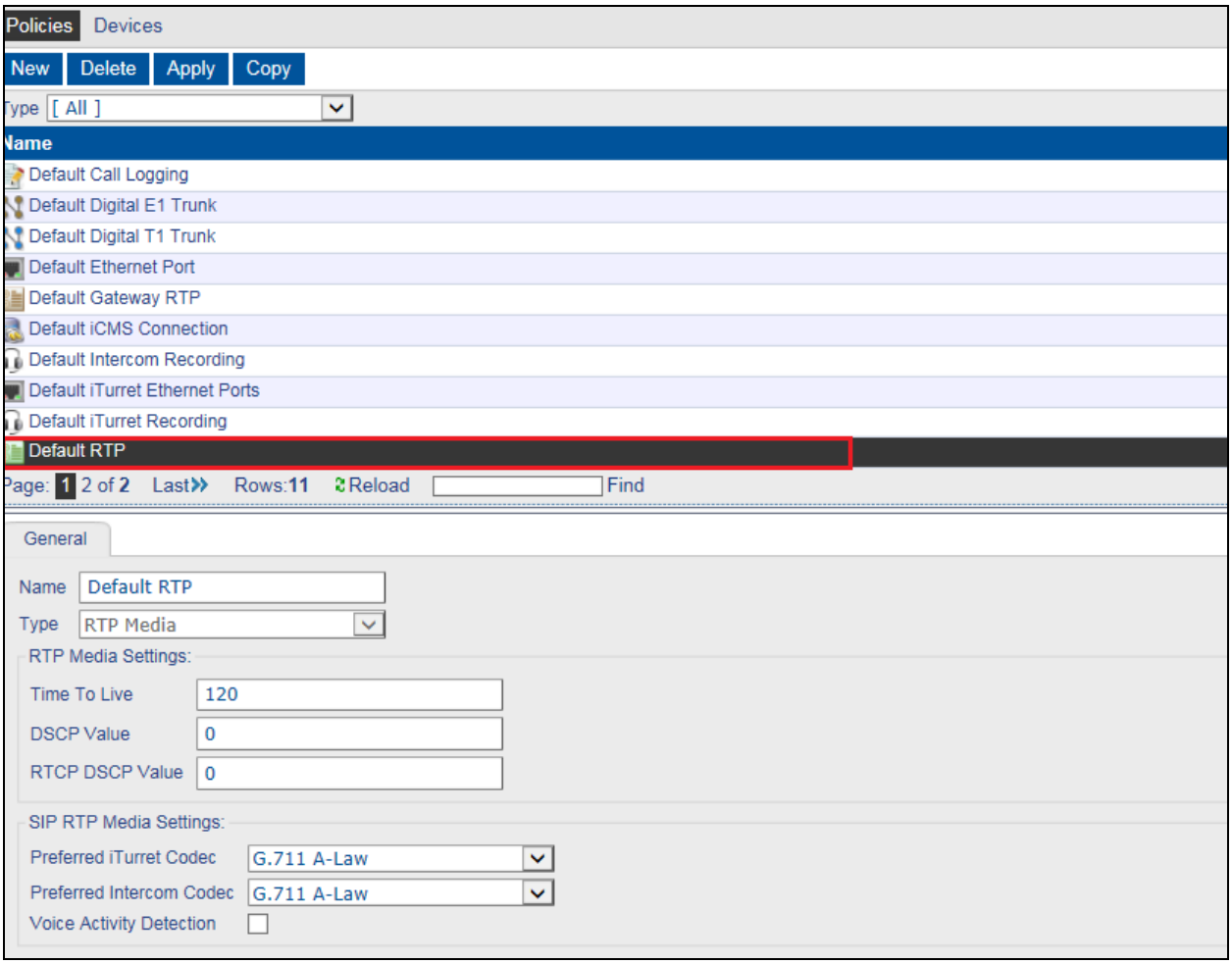


Select **Users → Policies** in the left pane (not shown) Select the **Default Preferences** policy, click the **iTurret** tab and review the default settings (no changes should be needed to this, however it`s referred to later in these Application Notes).

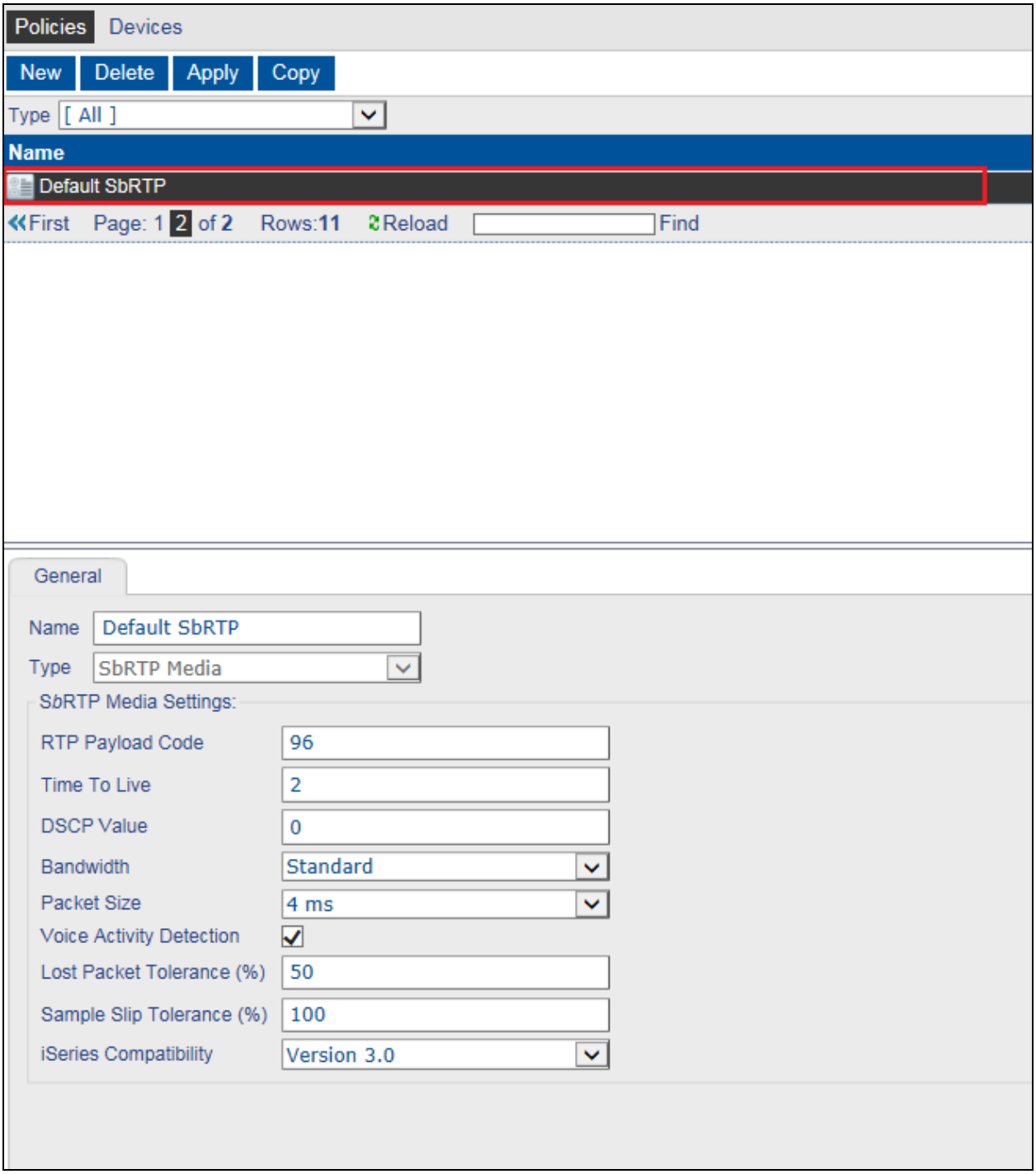


## 7.6. Creating/Verifying Device Policies

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

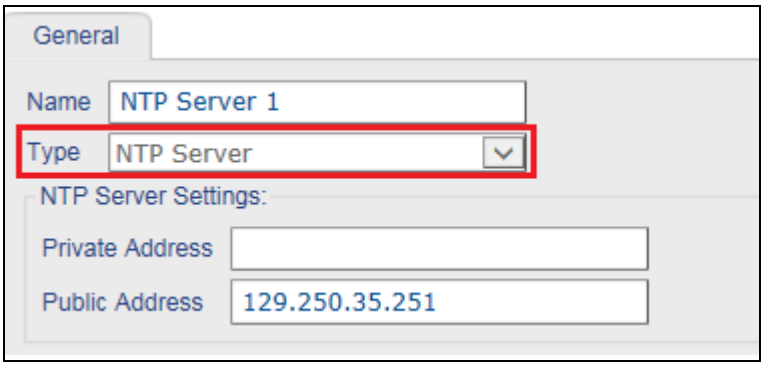


Select **Devices → Policies** in the left pane (not shown). Select and view the **Default SbRTP** policy (no changes should be needed to this, however it`s referred to later in these Application Notes).

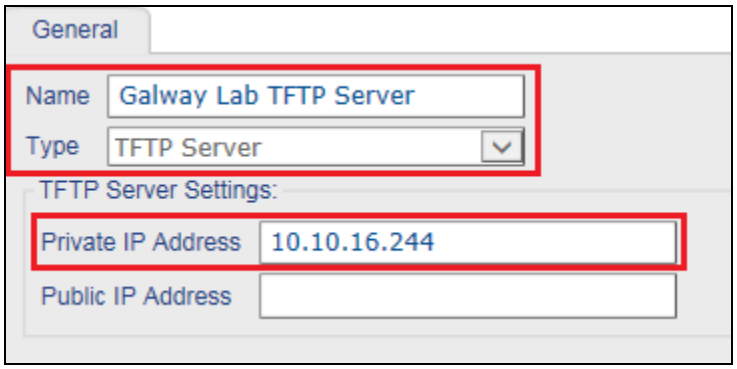


## 7.7. Create Network Services

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

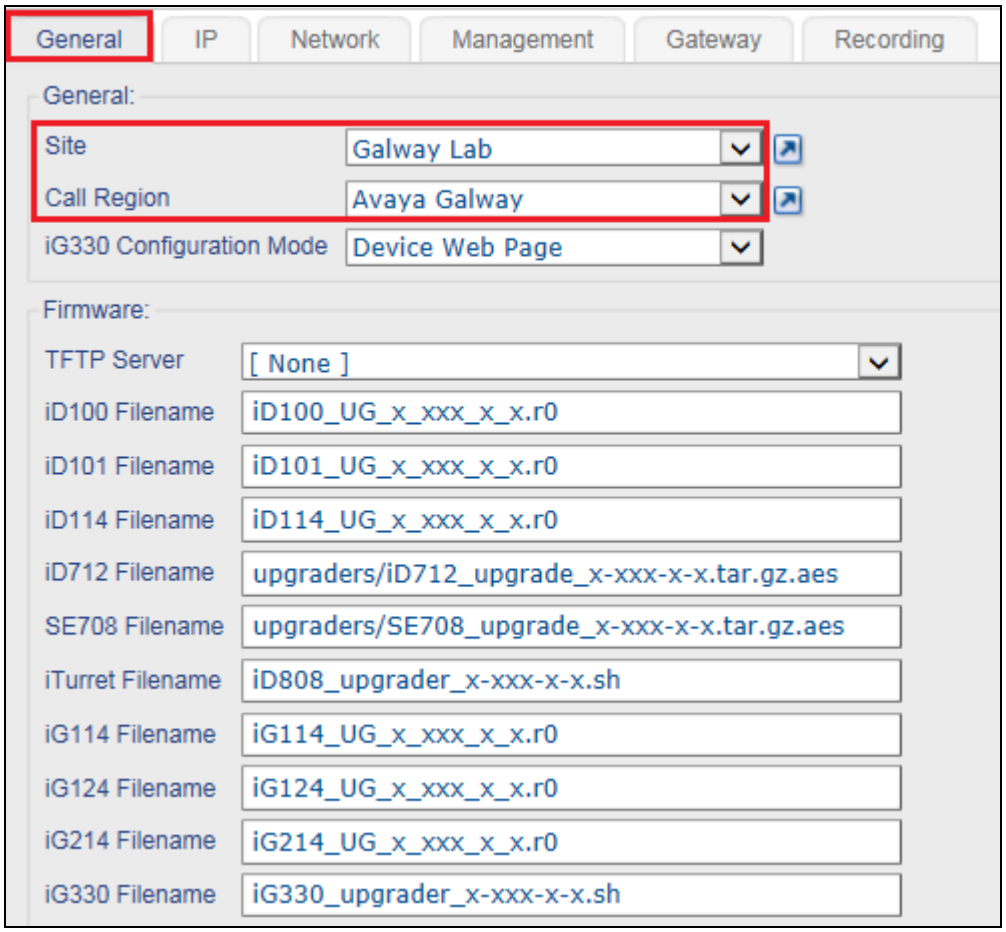



Select **Network → Network Services** in the left pane (not shown), click on **NEW** (not shown), enter a descriptive **Name**, in the **Type** dropdown list select **TFTP Server**, and enter a valid address for a TFTP server if available**.** Press **OK** once completed**,** as shown below.

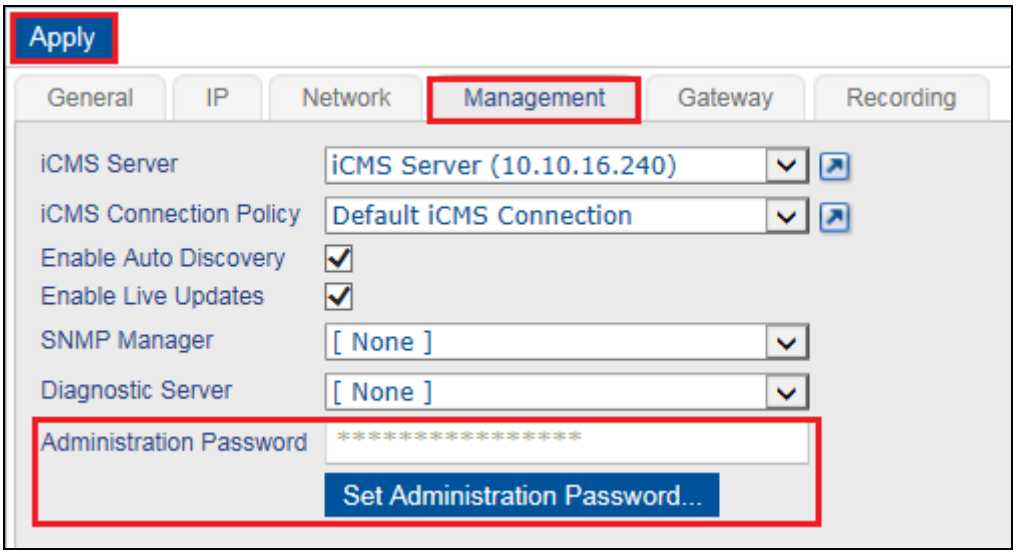


## 7.8. Confirm Defaults

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

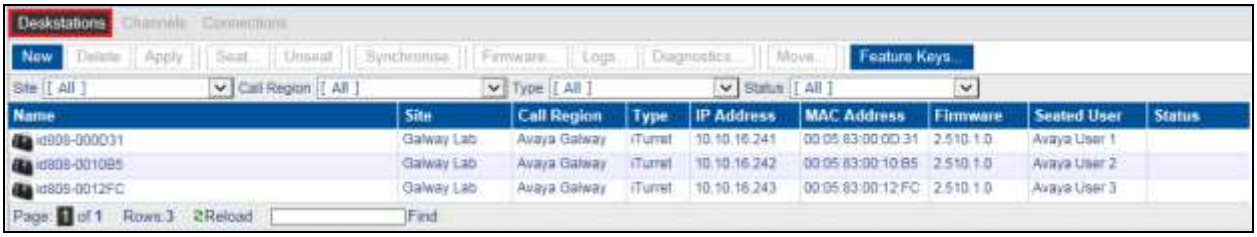


Under the **Management** tab, set the **Administration Password** and confirm as per below. Click **Apply** when completed.

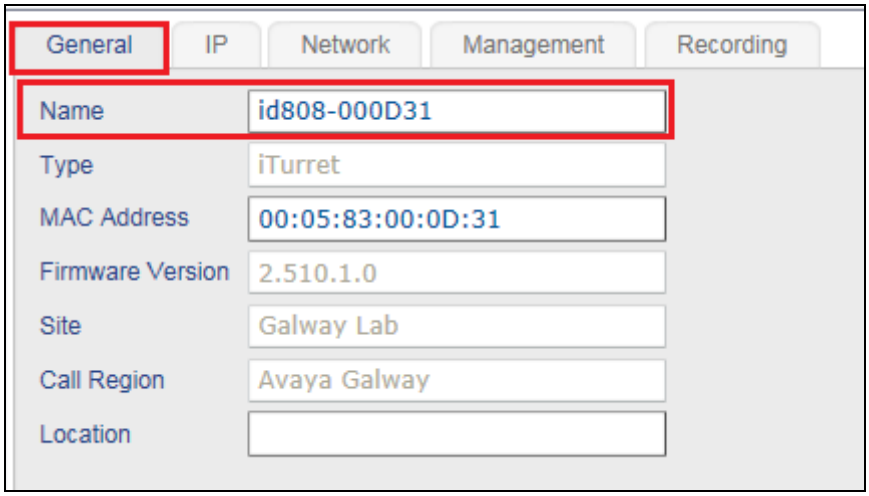



## 7.9. Create iTurret Deskstations

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

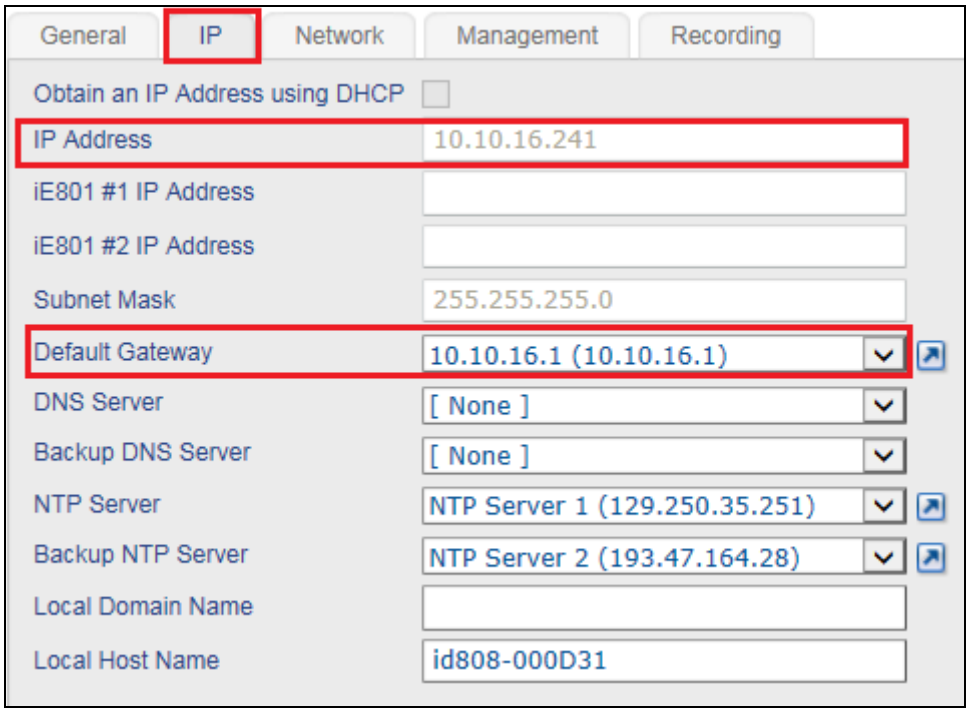


Select the iTurret Deskstation and under the **General** tab enter an identifying **Name**.



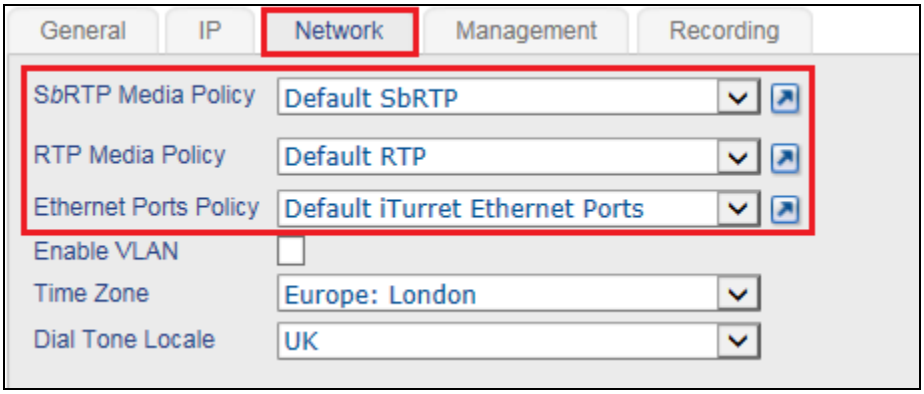

Click the **IP** tab and enter the **IP address** of the iTurret and the **Default Gateway**.

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



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

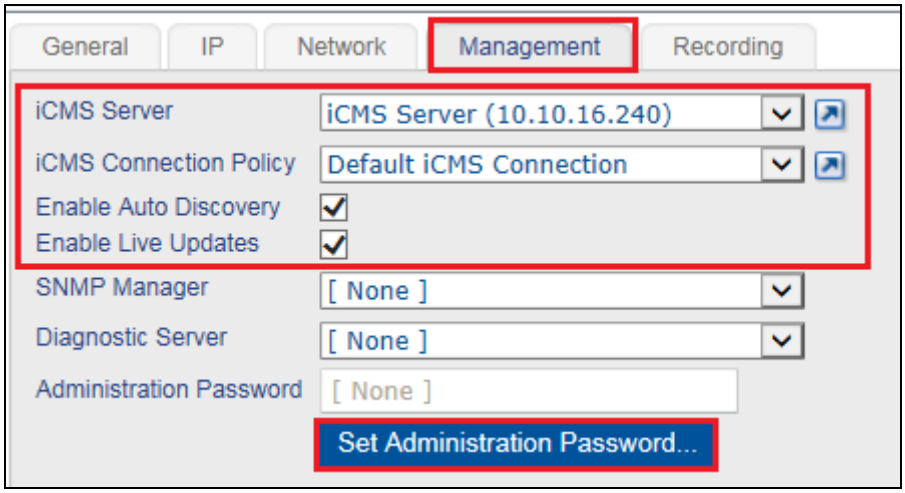
- **SbRTP Media Policy** is set to **Default SbRTP**
- **RTP Media Policy** is set to **Default RTP** (use the link to go to the policy to change the audio codec used, default is G.711 A-law)
- **Ethernet Ports Policy** is set to **Default iTurret Ethernet Ports**



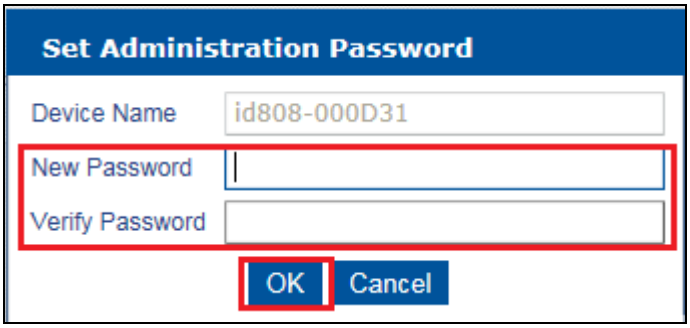

In the **Management** tab, verify or configure the following:

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

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



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



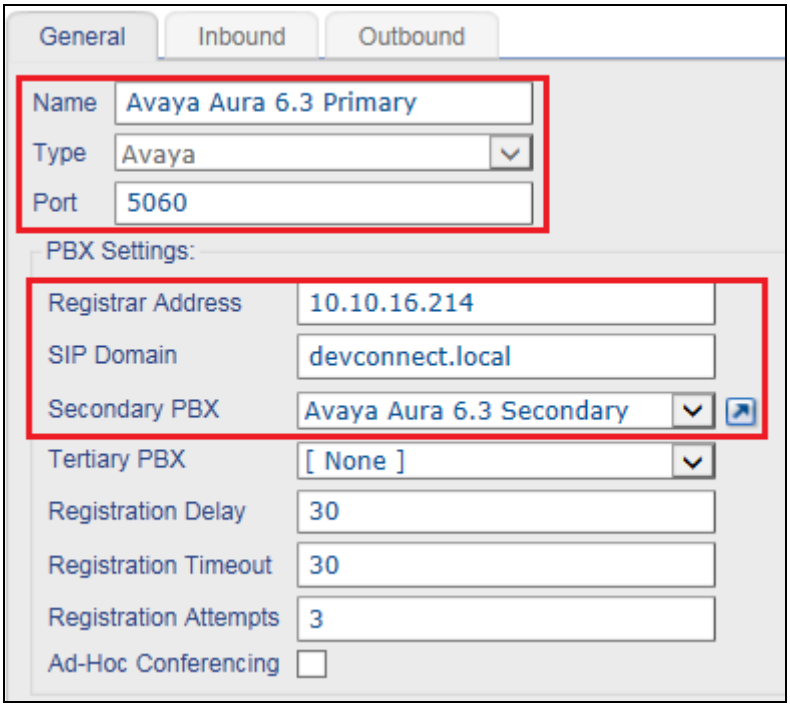
## 7.10. Create PBX (SIP Server)

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

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

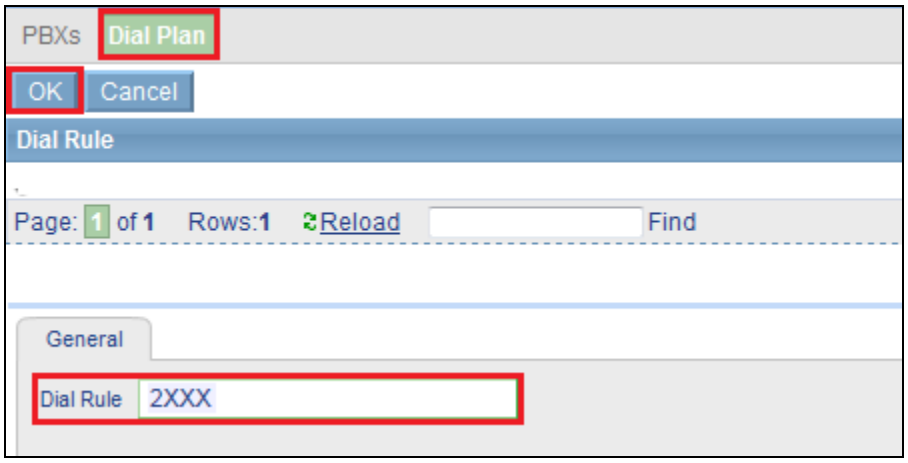
**Note 1**: A server locater record (SRV) for the registrar address and SIP domain may be created on DNS if the registrar address is set to devconnect.local, in the example below it will not be required. Refer to the *Speakerbus iManager Administrator`s Guide* for the correct configuration of DNS.
**Note 2**: If using failover, then a second PBX will be created and added to the **Secondary PBX** dropdown box.

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



## 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.



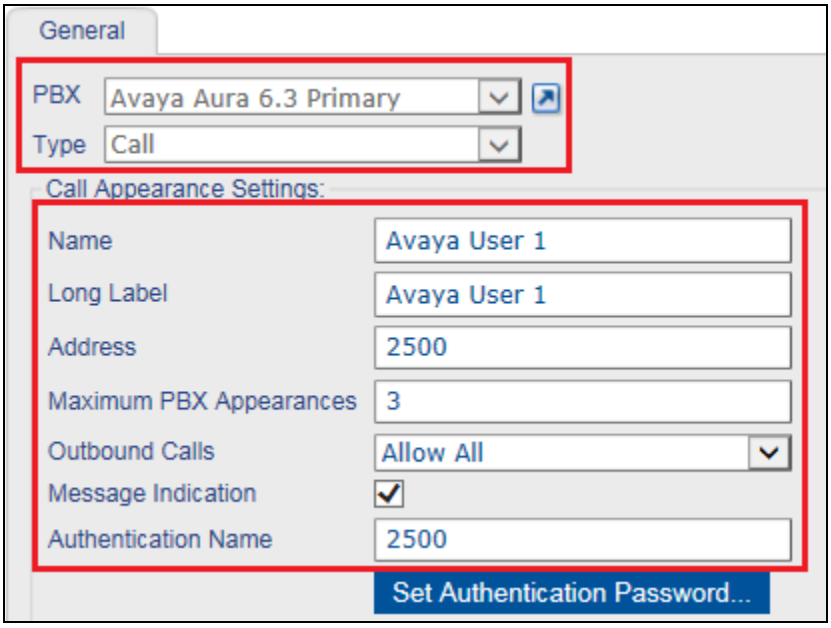

Repeat this for all valid extension formats.

## 7.12. Create Call and Handset Appearances

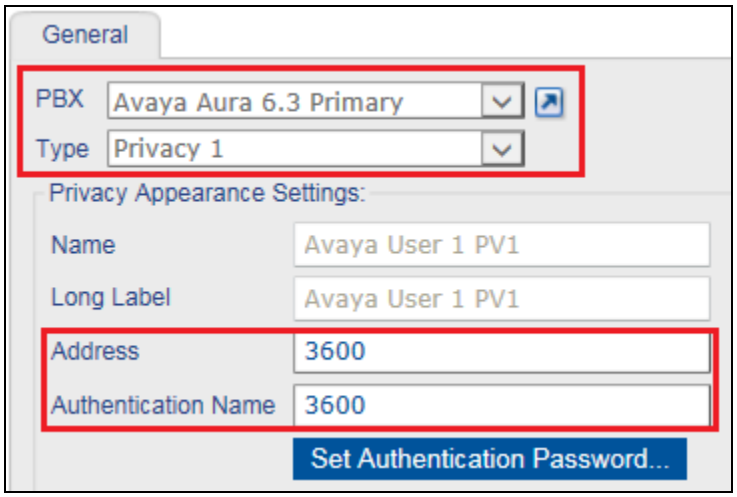
Three call appearances must be created for each iTurret device. One is for the main appearance, and one for each of the privacy appearances (handset 1 and handset 2). As previously explained, three extensions are configured in System Manager for this purpose.

To create the main appearance, click **Call Servers →PBX Appearances** in the left pane (not shown), click on **NEW** (not shown) select the PBX created in **Section 7.10** (in this case **Avaya 6.3 Primary**), then select the **Type** of appearance to be created (**Call** in this case) (not shown) and configure as follows under the **General** tab:

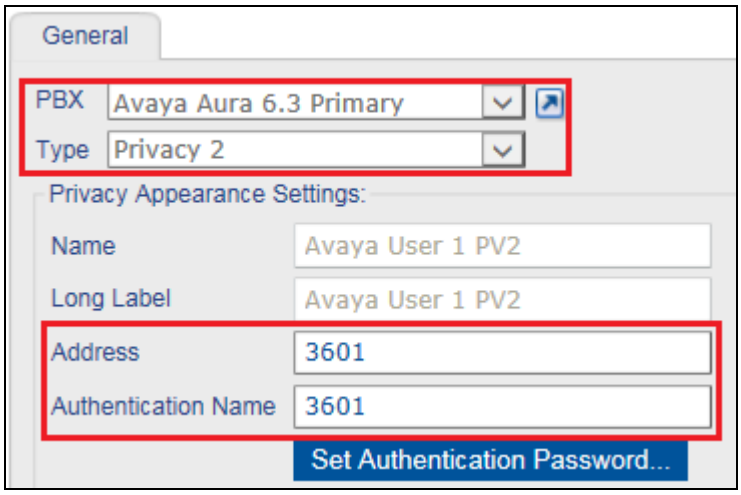
- Provide a descriptive name for the appearance in the **Name** field, such as the extension or user's name.
- Set the **Long Label** field to the label that will be displayed for the call appearance button on the iTurret deskstation. The **Address** field should also be set to the appearance extension.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



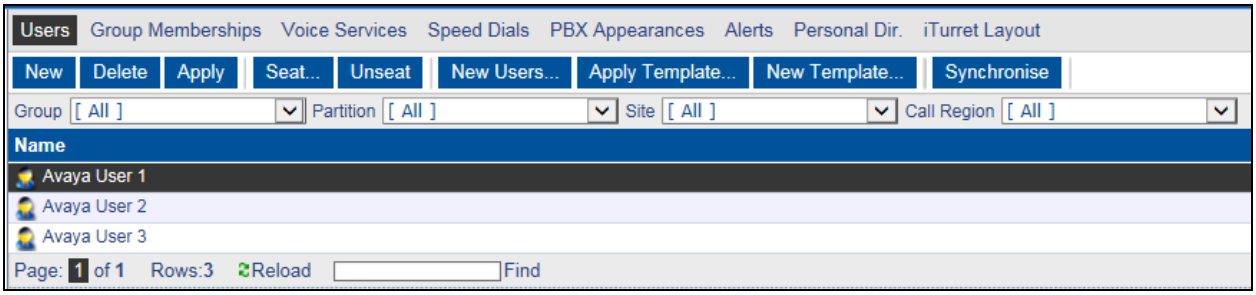
Repeat the procedure for the two corresponding privacy appearances. Click the **New** button to add another appearance. In the **General** tab select the **PBX** created in **Section 7.10**, set the **Type** field to **Privacy 1** and complete the **Address, Authentication Name** and **Authentication Password** fields. The last two fields should be identical to the setup in System Manager for registration to occur. Press **OK** (not shown) to commit the created appearance.




Repeat the above procedure to add the Privacy 2 appearance.

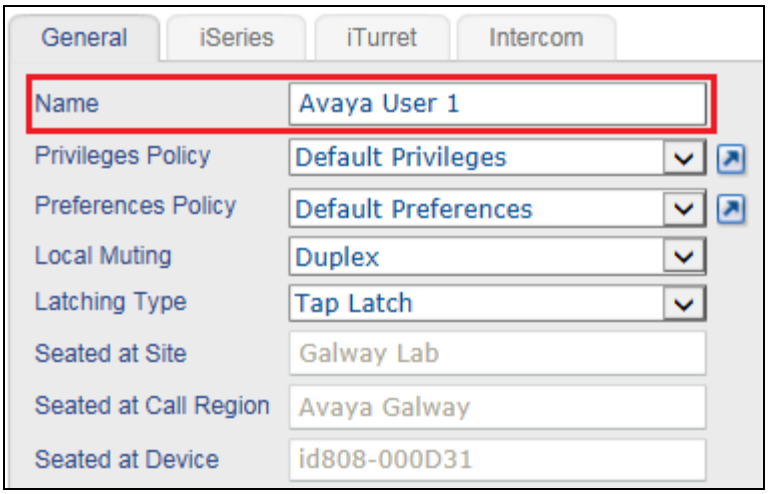


Repeat the above procedures for adding the Main and Privacy appearances for each iTurret.




## 7.13. Create Users

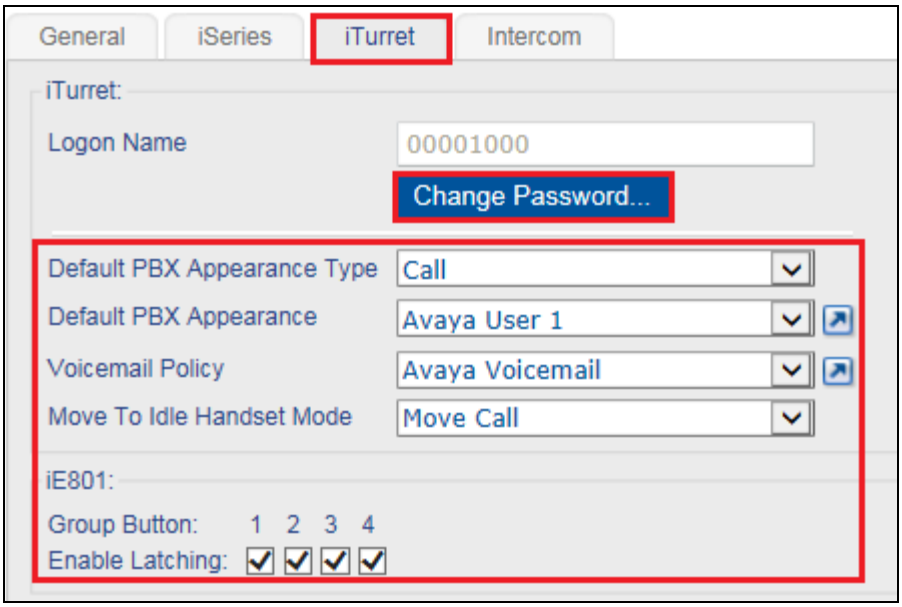
Select **Users →Users** in the left pane (not shown), click on **NEW** (not shown), within the **General** tab fill in a descriptive **name** for the user, leave the **privilege** and **preference policies** at the defaults along with **local muting**:



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

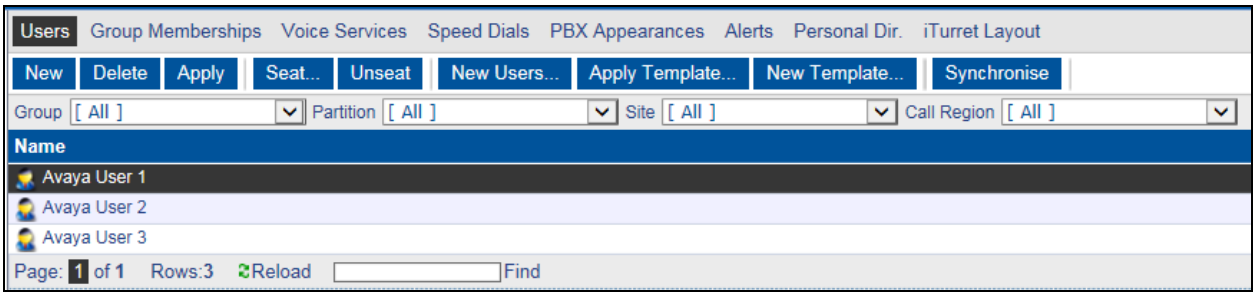
- **Voicemail Policy** — Select the voicemail policy as configured in **Section 7.5**.
- **Move to Idle Handset Mode** — Select **Move Call** from the drop down list
- **Enable Latching** — Tick **Group Button 1, 2,3** and **4**

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

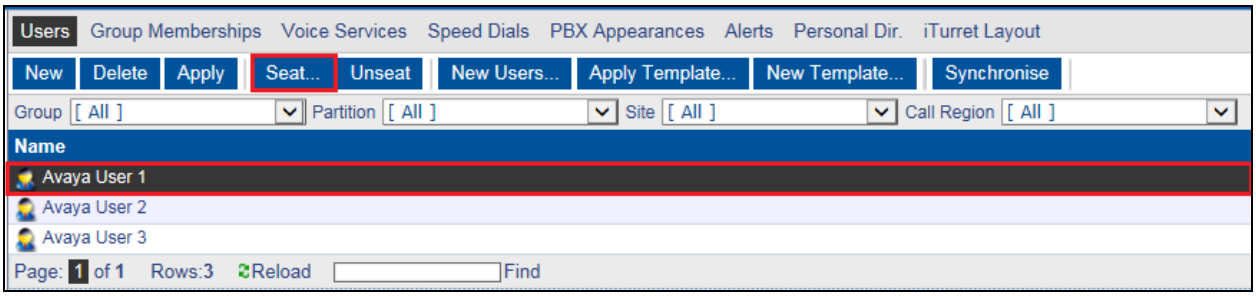



Repeat the previous steps to add more users.

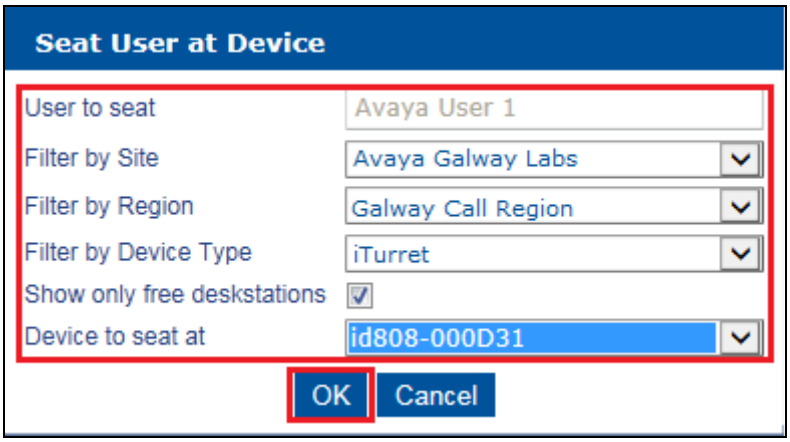
Once you have added the users, you can set up the PBX appearances for these users and then add them as Defaults PBX Appearance, see subsequent sections for further details.



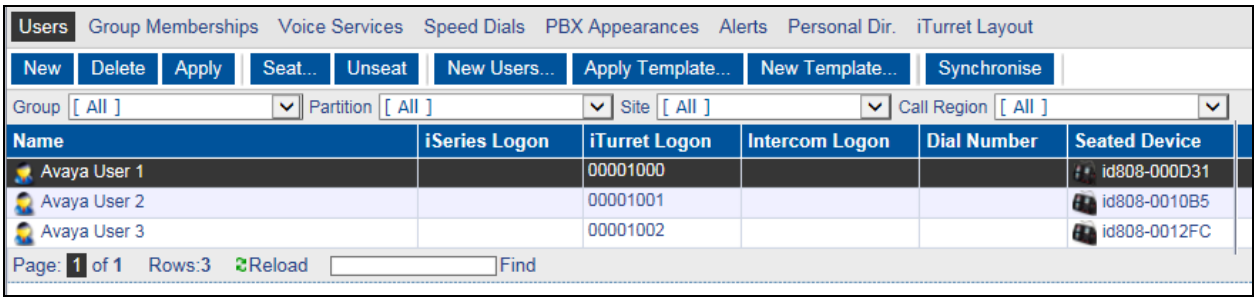
After a user has been created, that user can then be seated on an iTurret deskstation. Select the user to be seated and click **Seat** from the bar as shown below.




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

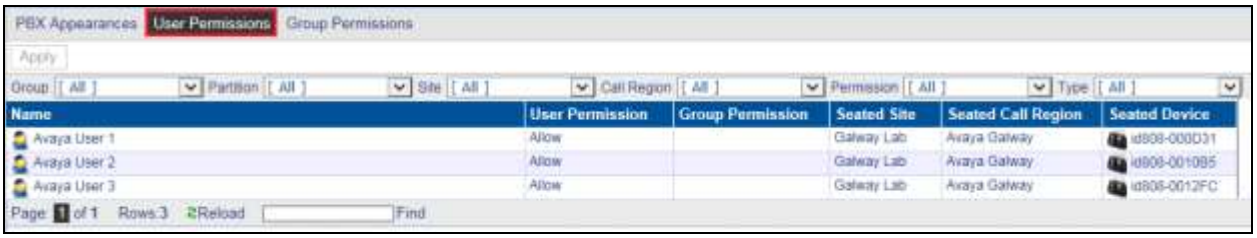


The user has been successfully seated as indicated by the iTurret deskstation in the **Seated Device** column on the following page. Repeat this process for seating all other users.

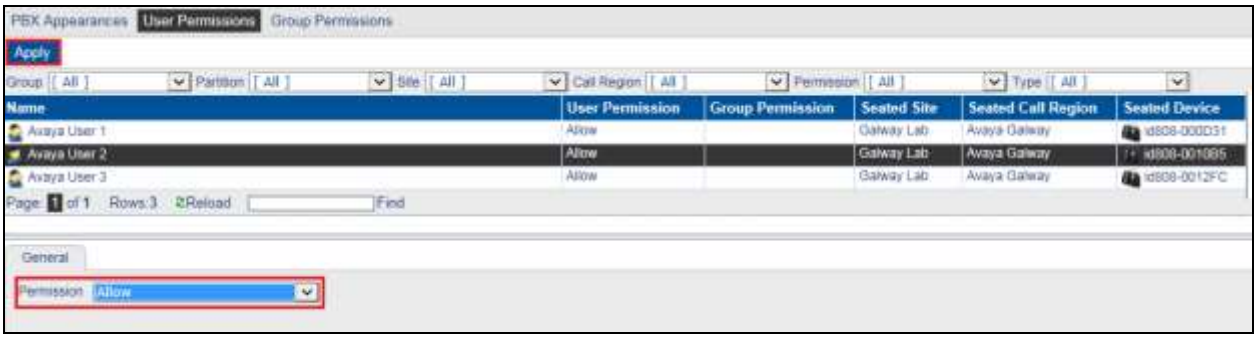



## 7.14. Assign User Permissions

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.

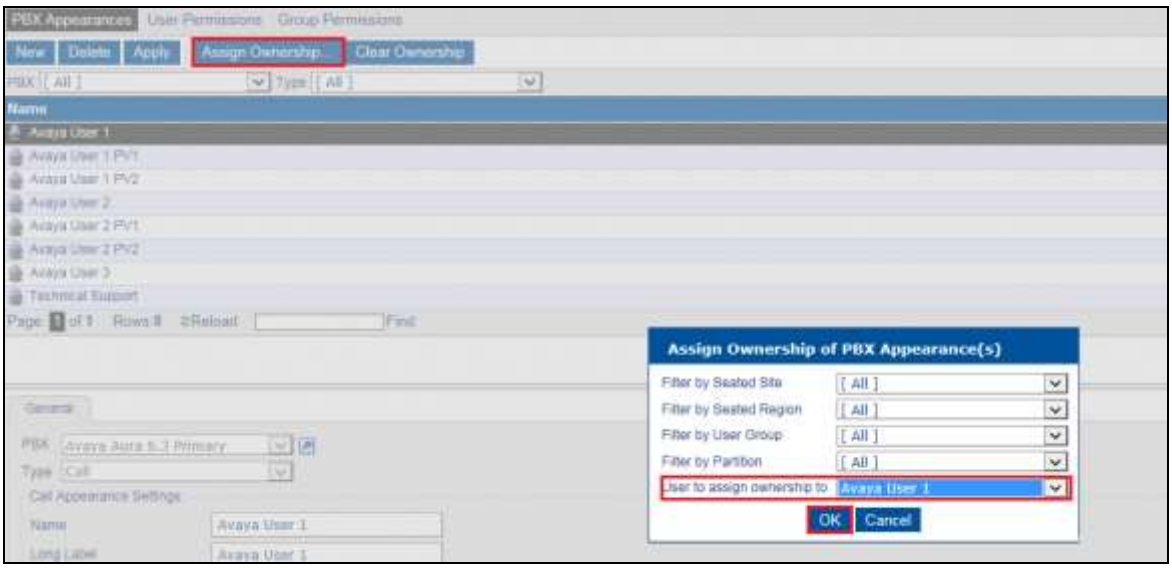



Select the user to give permissions to and select **Allow** from the **Permissions** drop down list and click **Apply**.



## 7.15. Assign Ownership

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

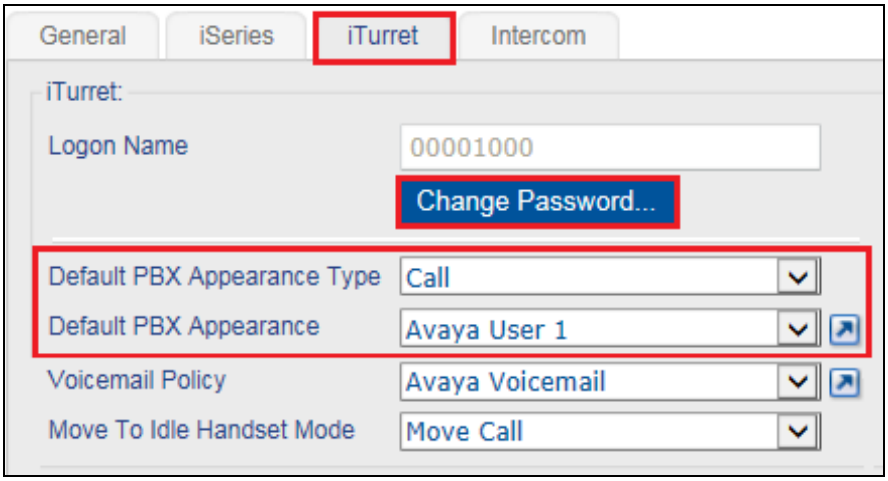



## 7.16. Set Default Appearance

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

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

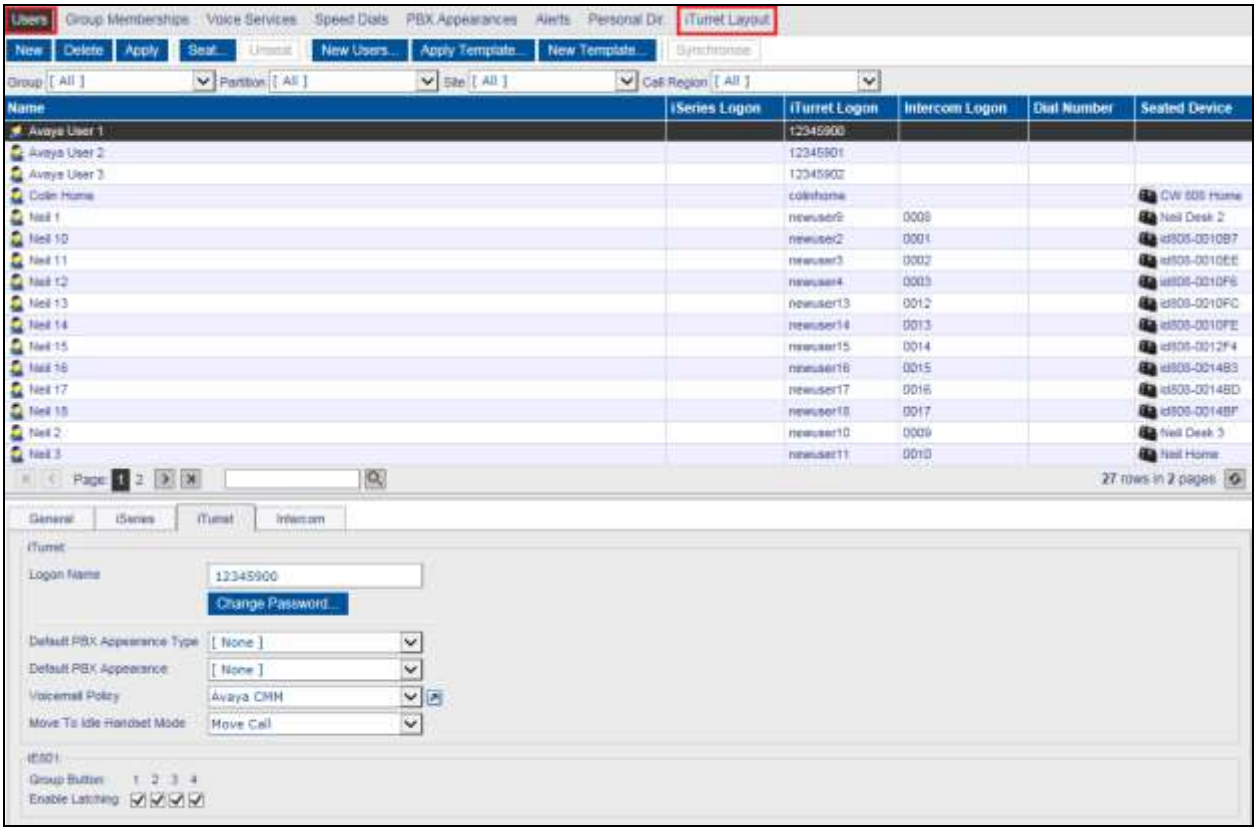
Click **APPLY** (not shown) once completed.



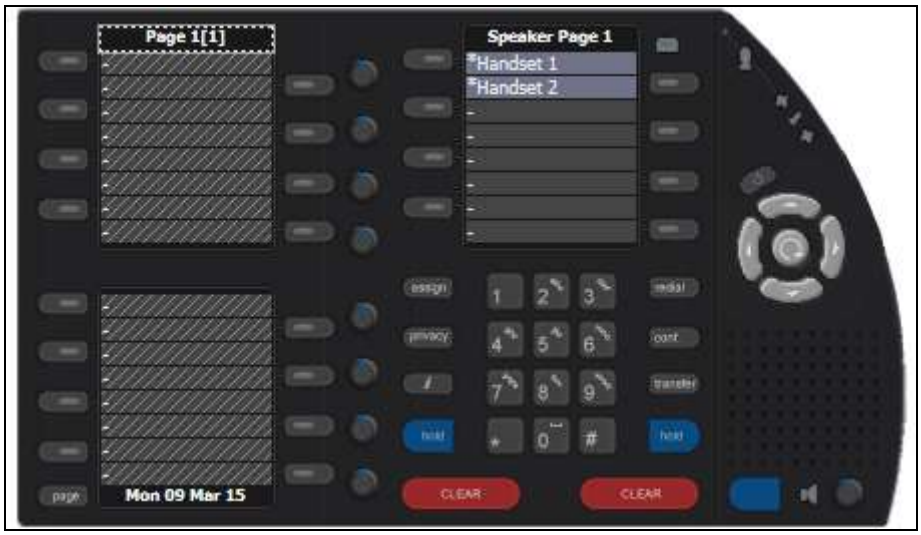
## 7.17. Program iTurret Layout Profiles

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

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



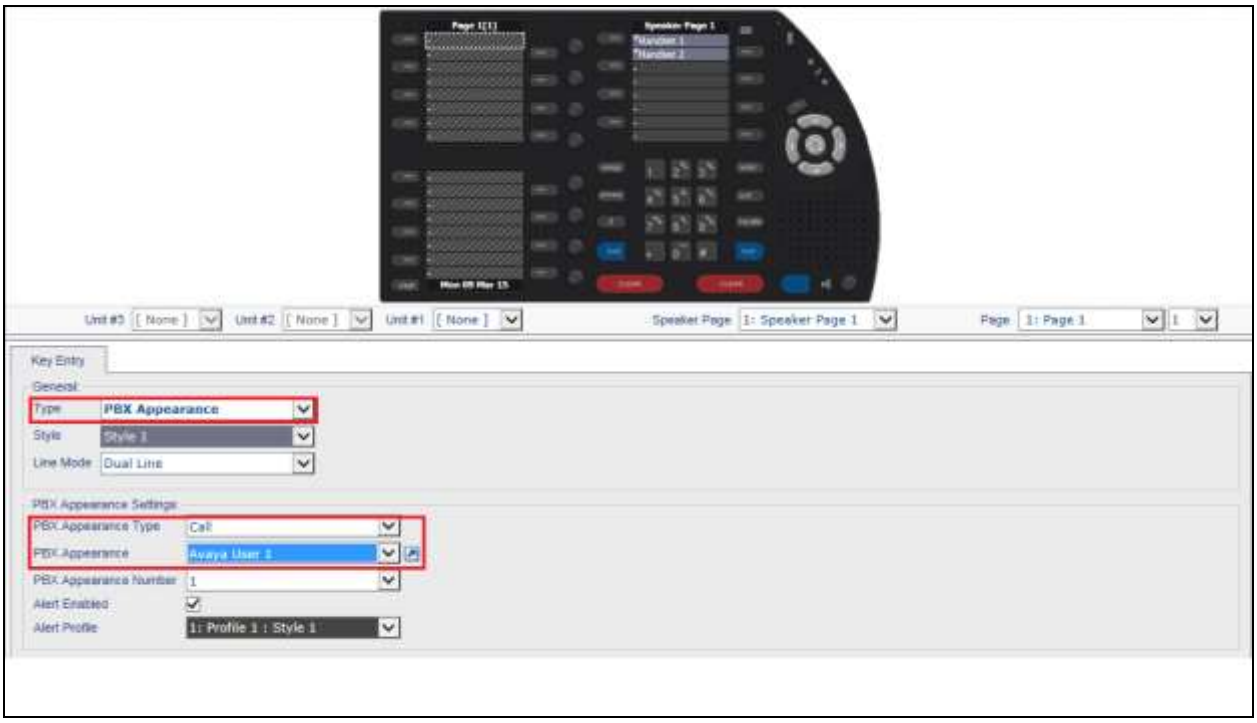
When selected you will see the following layout for a blank iTurret profile with ***Handset 1** and ***Handset 2** configured.



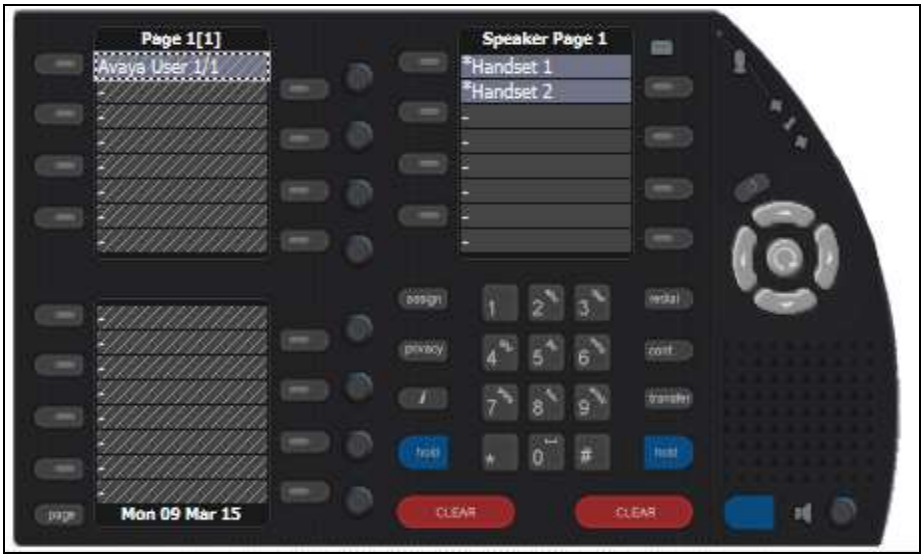

To add the keys for the call appearances, select a key (with hatching) and enter the following:

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

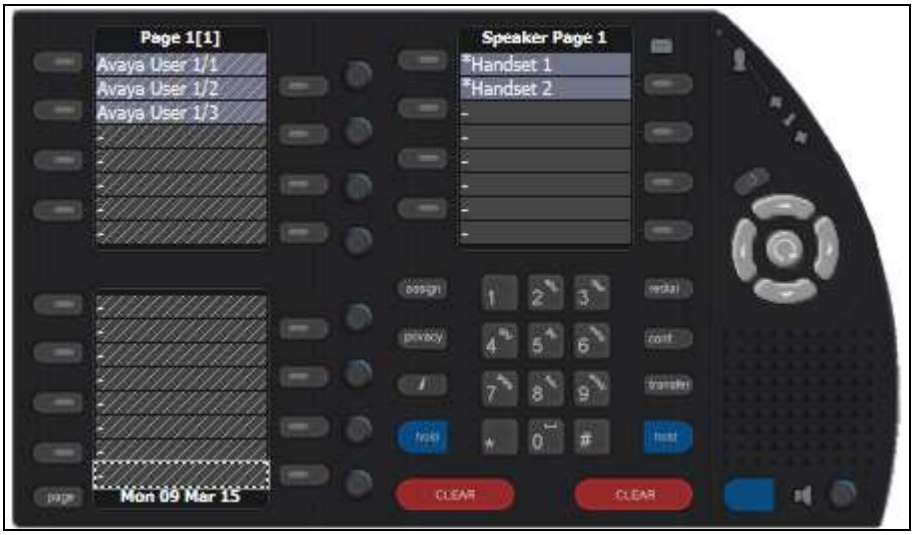
Click the **OK** button (not shown).



Once done the layout will look as follows.




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



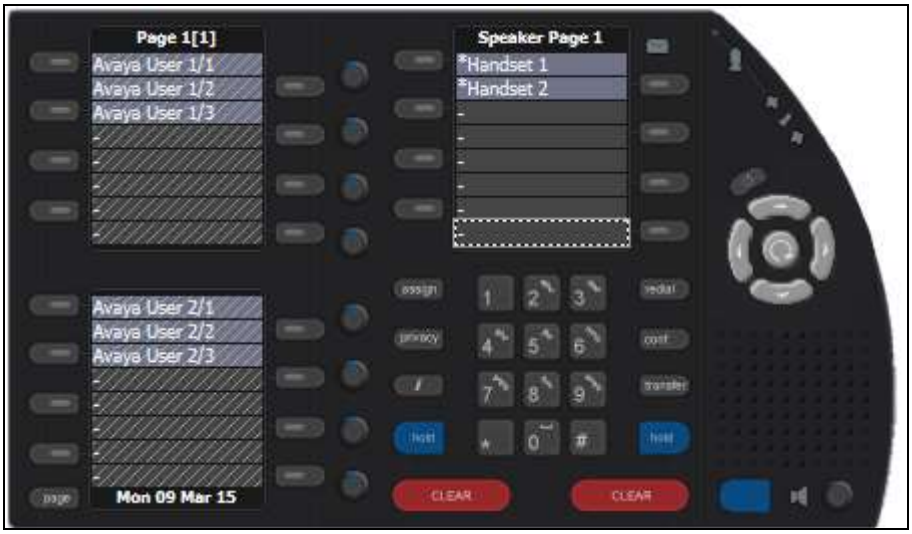
### 7.17.1. Add bridged appearances

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

- **Type** — Select **PBX Appearance** from the drop down box
- **PBX Appearance Type** — Select **Call**, from the drop down box
- **PBX Appearance** — Select the call appearance you have permissions to, but isn`t owned by this user (thus, it`s a bridged appearance)

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

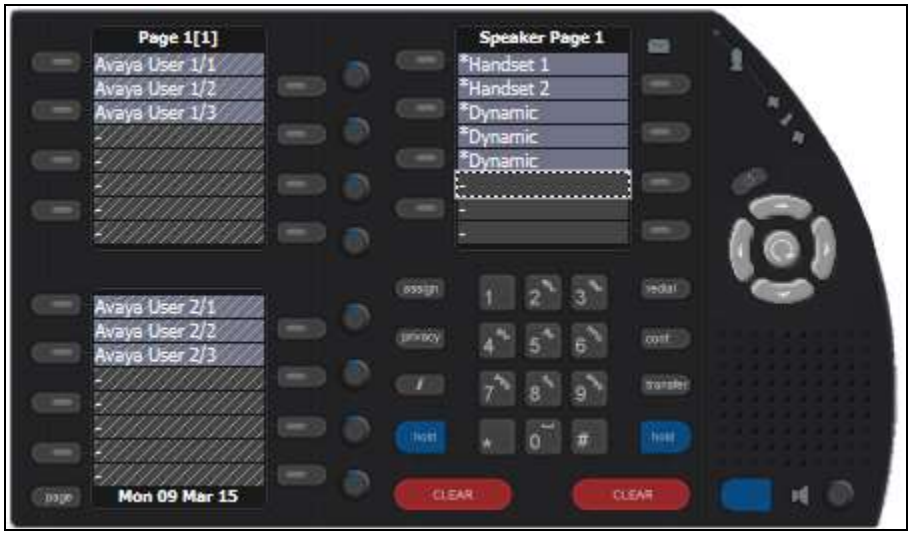
The example below shows Avaya User 2 three times.



### 7.17.2. Add dynamic keys

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

The example below shows the three dynamic keys added.

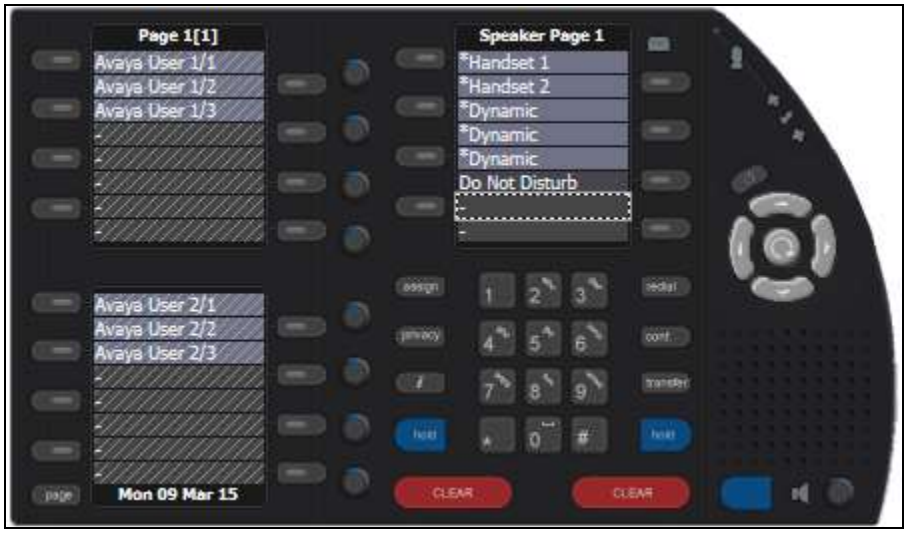


### 7.17.3. Add Do Not Disturb key

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

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

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

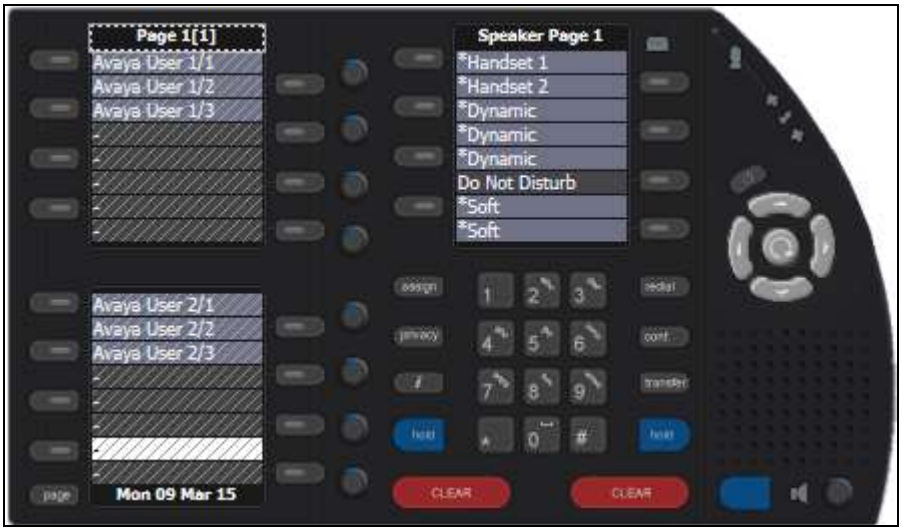


### 7.17.4. Add soft function keys

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

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

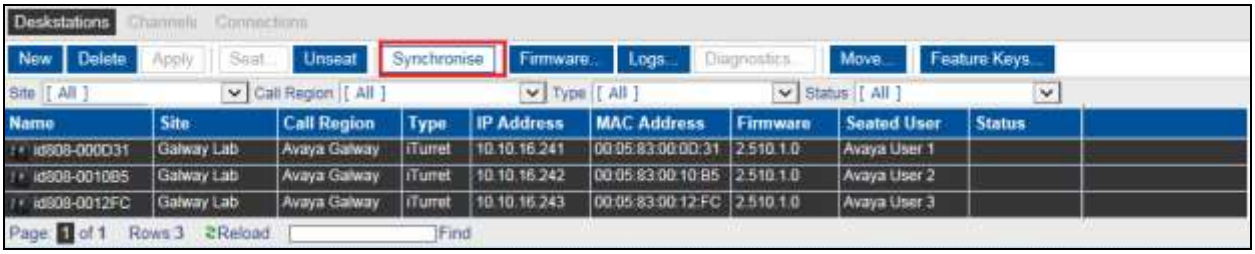
Click the **OK** button. Repeat this step two times. Once done the layout will look as below.




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

## 7.18. Synchronise Deskstations

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



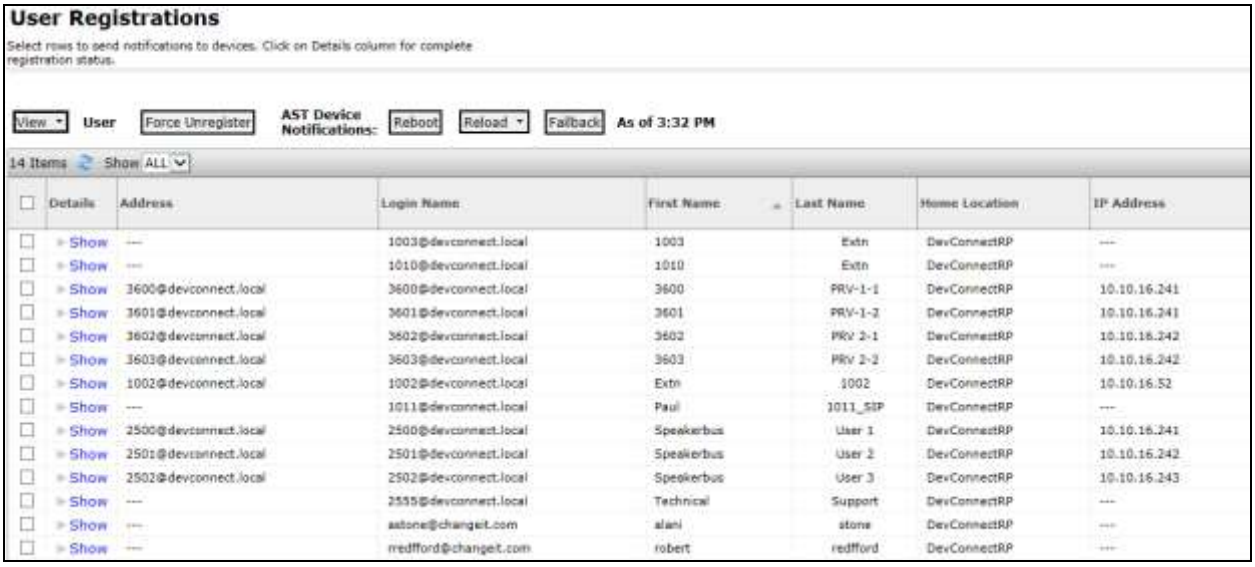

**Note**: Any changes you make to the profile within iManager will be updated on the iTurret device after **OK** or **Apply** is pressed. However, some changes will require a synchronization. Refer to the *Speakerbus iManager Administrator`s Guide* for more details.

# 8. Verification Steps

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

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

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



**User Registrations**

Select rows to send notifications to devices. Click on Details column for complete registration status.

View User Force Unregister AST Device Notifications: Reboot Reload Failback As of 3:32 PM

14 Items Show ALL

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

## 8.2. Verify iTurret status

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

# 9. Conclusion

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

# 10. Additional References

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


*[1] Administering Avaya Aura® Communication Manager, Release 6.3, June 2014, Document Number 03-300509, Issue 10..*

*[2] Avaya Aura® Communication Manager Feature Description and Implementation, Release 6.3, December 2014, Document Number 555-245-205, Issue 14.0.*

*[3] Administering Avaya Aura® Session Manager, Release 6.3, Issue 7 September 2014*

*[4] Administering Avaya Aura® System Manager, Release 6.3, Issue 5, October, 2014*

*[5] Speakerbus Administrator's Guide iManager PN AGiCMS V2.51, Revision 19, June 2014*


Product Documentation for Speakerbus can be requested from info@speakerbus.com

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.