Avaya Solution & Interoperability Test Lab

Application Notes for Speakerbus iD808 *i*turret with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

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

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

1. Introduction

These Application Notes describe the steps required to connect Speakerbus iD808 *i* turrets to a SIP infrastructure consisting of Avaya Aura® 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 in the *i* turret. In this configuration, the Off-PBX Stations (OPS) feature set is extended from Avaya Aura® Communication Manager to the Speakerbus iD808 *i* turret, providing the iTurret deskstation with enhanced calling features. The configuration steps described are also applicable to other Linux-based Avaya Servers and Media Gateways running Avaya Aura® Communication Manager.

The following table provides a summary of the supported features available on *i* turret with the Avaya SIP offer. Some features are supported locally in *i* turret, while others are only available with Avaya Aura® Communication Manager and Avaya Aura® 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 *i* turret using OPS.

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

FEATURE	Supported		COMMENTS
	Locally at the Phone	With Avaya SIP Offer	
Basic Calling Features			
Extension to Extension Call	Yes	Yes	
Basic Call to legacy phones	No	Yes	
Speed Dial Buttons	Yes	Yes	
Message Waiting Support	Yes	Yes	
SIPPING-19 Features			
Call Hold	Yes	Yes	
Consultation Hold	Yes	Yes	
Unattended Transfer	Yes	Yes	
Attended Transfer	Yes	Yes	
Call Forward All	Yes	Yes	Local menu option on *i* turret and FNU
Call Forward Busy/No Answer	Yes	Yes	Local menu option on *i* turret and FNU
Call Forward Cancel	Yes	Yes	Local menu option on *i* turret 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 Pick-Up	No	Yes	Via OPS FNE
Drop Last Added Party	No	Yes	Via OPS FNE
Exclusion/Privacy	Yes	Yes	Local hard key on *i* turret and FNU
Last Number Dialed	Yes	Yes	Via OPS FNE
Priority Call	No	Yes	Via OPS FNE, *i* turret does not support distinctive ring indication
Send All Calls	No	Yes	Via OPS FNE
Send All Calls Cancel	No	Yes	Via OPS FNE
Transfer to Voice Mail	No	Yes	Via OPS FNE
Whisper Page	No	Yes	Via OPS FNE

Table 1: SIP Features Table

2. General Test Approach and Test Results

To verify interoperability of Speakerbus iD808 *i* turret with Avaya Aura® Communication Manager and Avaya Aura® 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 *i* Turret, FNEs, and FNUs. The PBX features listed in **Section 1** were covered. Speakerbus iD808 *i* turret passed compliance testing.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of *i* turret with Session Manager
- Calls between *i* turret and Avaya SIP, H.323, and digital stations
- G.711and G729 codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus
- Proper operation of voicemail with message waiting indicators (MWI)
- PBX features including Multiple Call Appearances, Hold, Transfer, and Conference
- Extended telephony features using Communication Manager Feature Name Extensions (FNEs) such as, Conference On Answer, Call Park, Call Pickup and Automatic Redial. See **Table 1** for the complete list of features
- Exclusion/Privacy using the Exclusion FNU
- Call forwarding and Send All Calls using Call Forwarding and Send All Call FNU`s.
- Proper system recovery after an *i* turret restart and loss of IP connection

2.2. Test Results

During testing the Speakerbus iD808 i turret completed all scenarios with results in all cases as expected.

2.3. Support

For technical support of Speakerbus products contact the Speakerbus Service Desk:
Web: http://www.speakerbus.com
Email: info@speakerbus.com
Telephone: (646) 289-4700 in North America
+44 (0) 870 240 7252 in Europe
+65 6222 4577 in Asia

3. Reference Configuration

The configuration used as an example in these Application Notes is shown in **Figure 1**. The diagram illustrates an enterprise site with an Avaya SIP-based network, including a pair of Session Manager, System Manager, an Avaya S8800 Server with a G650 Media Gateway running Communication Manager, and Avaya IP endpoints. Avaya Modular Messaging provides voice mail service. The enterprise site also contains three iD808 *i* turret deskstations that register with Session Manager and are configured as OPS stations on Communication Manager. Communication Manager extends the telephony functionality that is supported by the SIP-based iD808 devices through the use of Feature Name Extensions (FNEs) and FNUs. The *i* cms server contains the *i* manager application for configuring the *i* turret deskstations.

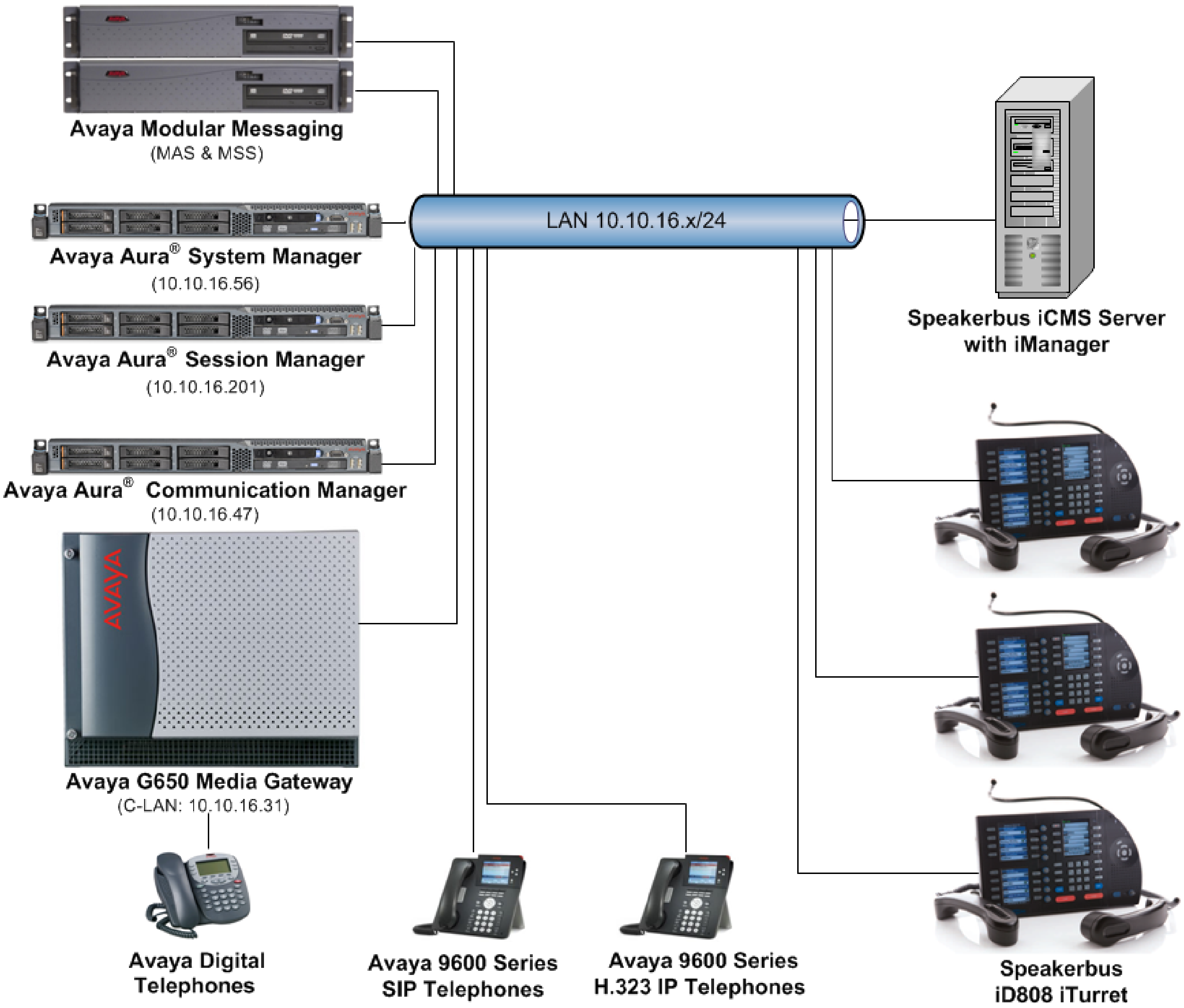


Figure 1: Speakerbus iD808 *i* turret with Avaya SIP Solution

4. Equipment and Software Validated

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

Hardware Component	Version
Avaya S8800 Server	Avaya Aura® Communication Manager 6.0 (R016x.00.0.345.0) with Service Pack 1 (Patch 18444)
Avaya G650 Media Gateway TN2602AP Media Processor	 HW08 FW057
Avaya S8800 Server	Avaya Aura® Session Manager 6.0 (Build 6.1.0.0.610023)
Avaya S8800 Server	Avaya Aura® System Manager 6.0 (Build 6.1.0.4.5072-6.1.4.113)
Avaya S3500 Servers Modular Messaging	Avaya Modular Messaging 5.2
Avaya 9600 Series IP Telephones	3.1 (H.323)
Avaya 9600 Series IP Telephones	2.6.4.0 (SIP)
Avaya Digital Telephones	--
Avaya Analog Telephones	--
Speakerbus iD808 *i* turret	1.30
Speakerbus *i* cms Server with *i* manager Administration on Windows 2003 Server	1.400.7.0

5. Configure Aura® Avaya Communication Manager

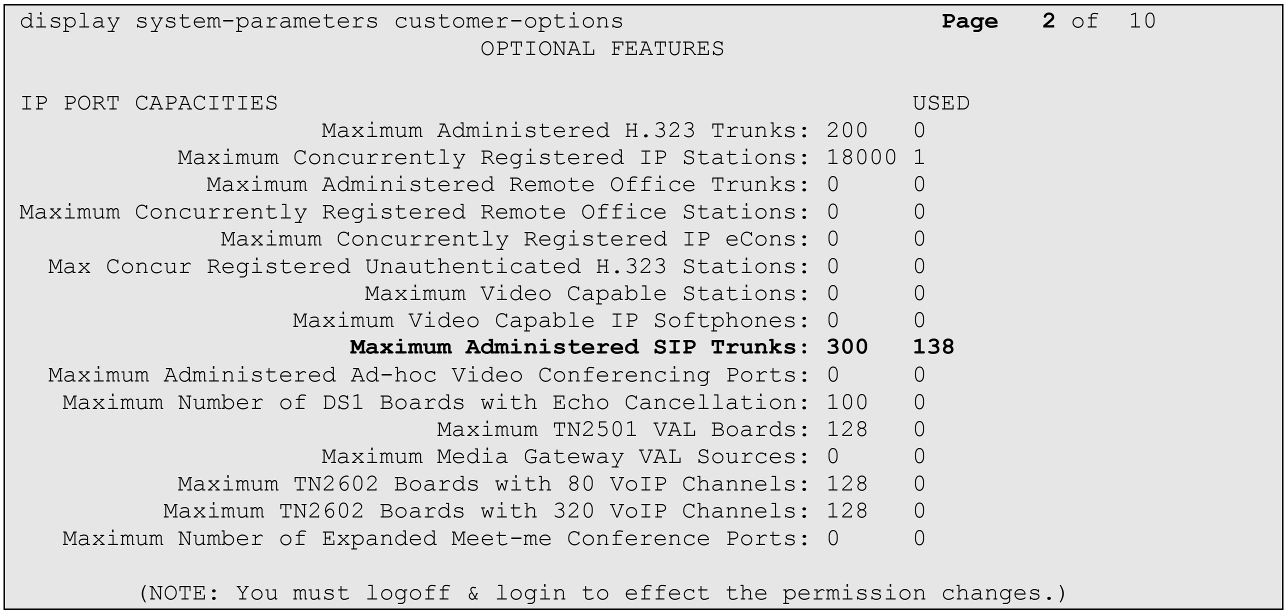
This section describes the steps for configuring the iD808 *i* turret as an Off-PBX Station (OPS), administering support for the OPS features indicated in **Table 1**, and configuring a SIP trunk between Communication Manager and Session Manager. Use the System Access Terminal (SAT) to configure Communication Manager. Log in with the appropriate credentials.

5.1. Verify System Capacity

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

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

     G3 Version: V15                            Software Package: Standard
       Location: 2                           RFA System ID (SID): 1
       Platform: 6                           RFA Module ID (MID): 1

                                                                USED
                                 Platform Maximum Ports: 48000 282
                                       Maximum Stations: 36000 48
                               Maximum XMOBILE Stations: 0     0
                     Maximum Off-PBX Telephones - EC500: 200   0
                     Maximum Off-PBX Telephones -   OPS: 200   18
                     Maximum Off-PBX Telephones - PBFMC: 0     0
                     Maximum Off-PBX Telephones - PVFMC: 0     0
                     Maximum Off-PBX Telephones - SCCAN: 0     0


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

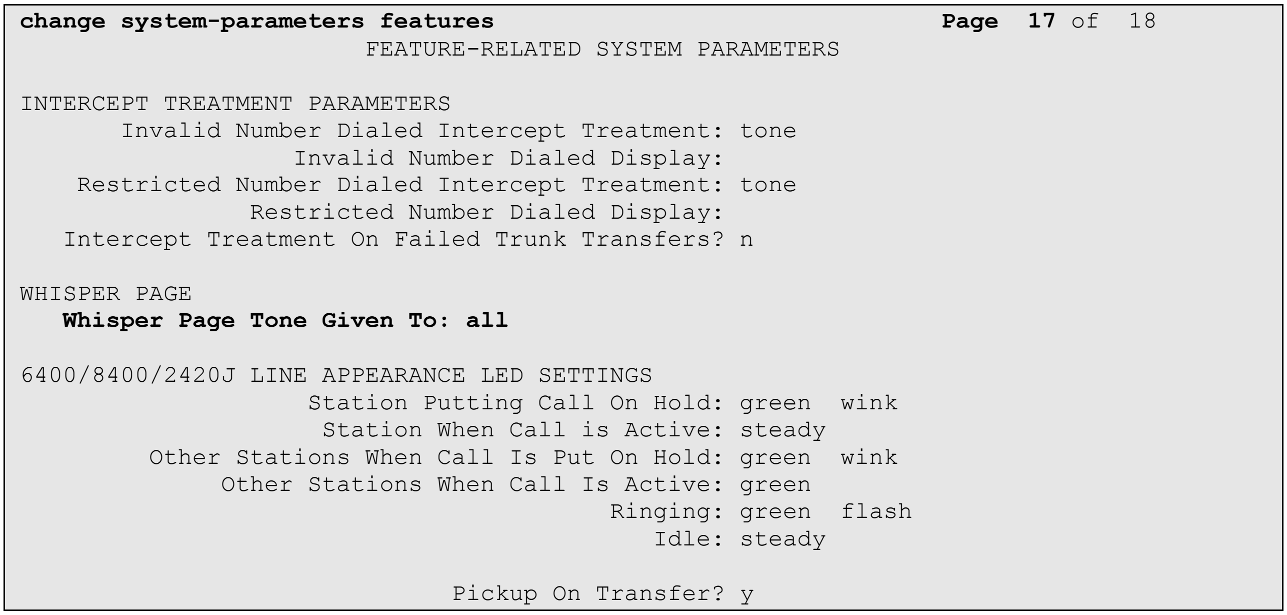
On **Page 2** of the **System-Parameters Customer-Options** form, verify that the number of **Maximum Administered SIP Trunks** supported by the system is sufficient.



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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 200    0
           Maximum Concurrently Registered IP Stations: 18000 1
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                        Maximum Video Capable Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 300   138
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 100   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0

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

5.2. Define System Features

Use the **change system-parameters features** command to administer system wide features for SIP endpoints. Those related to features listed in **Table 1** are shown in bold. These are all standard Communication Manager features that are also available to OPS stations. On **Page 17,** set 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
```

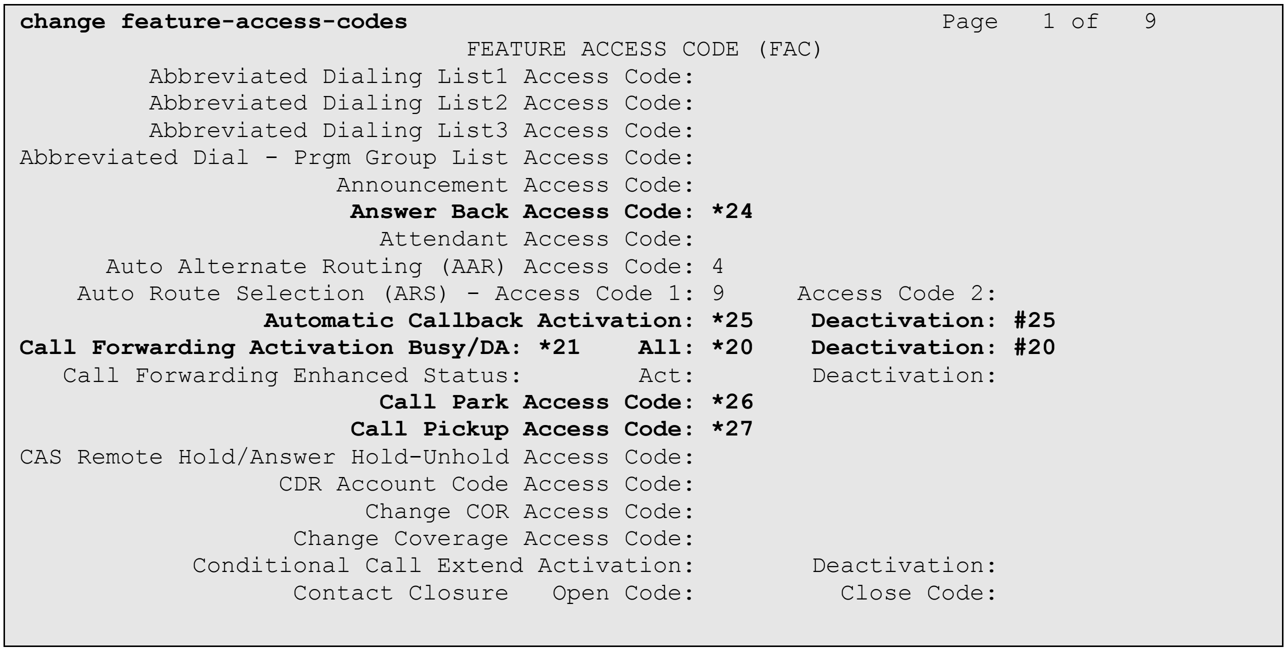
5.3. Define the Dial Plan

Use the **change dialplan analysis** command to define the dial plan used in the system. This includes all telephone extensions, OPS Feature Name Extensions (FNEs), and Feature Access Codes (FACs). To define the FNEs for the OPS features listed in **Table 1**, a Feature Access Code (FAC) must also be specified for the corresponding feature. In the sample configuration, telephone extensions are four digits long and begin with **1**, FNEs are also four digits beginning with **1**, and the FACs have formats as indicated with a **Call Type** of **fac**.

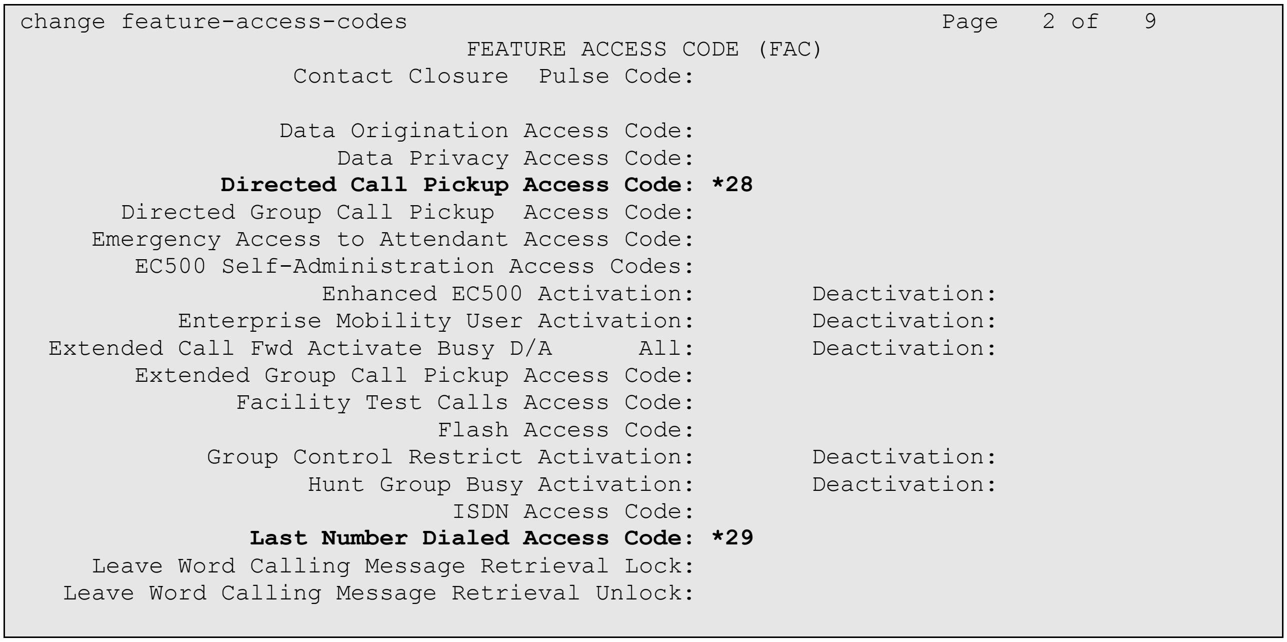
```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all           Percent Full:    1

       Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
       String   Length Type    String   Length Type     String   Length Type
     0            1    ext    7           4    ext
     1            4    ext    88          4    ext
     2            4    udp    89          4    ext
     3005         8    udp    9           1    fac
     3015         9    udp    *           3    fac
     31           4    udp    #           3    fac
     33           4    udp
     37           4    udp
     38           5    aar
     4            1    fac
     5            3    dac
     6            3    fac
     61           4    ext
     66           4    ext
     663          4    ext
```

5.4. Define Feature Access Codes (FACs)

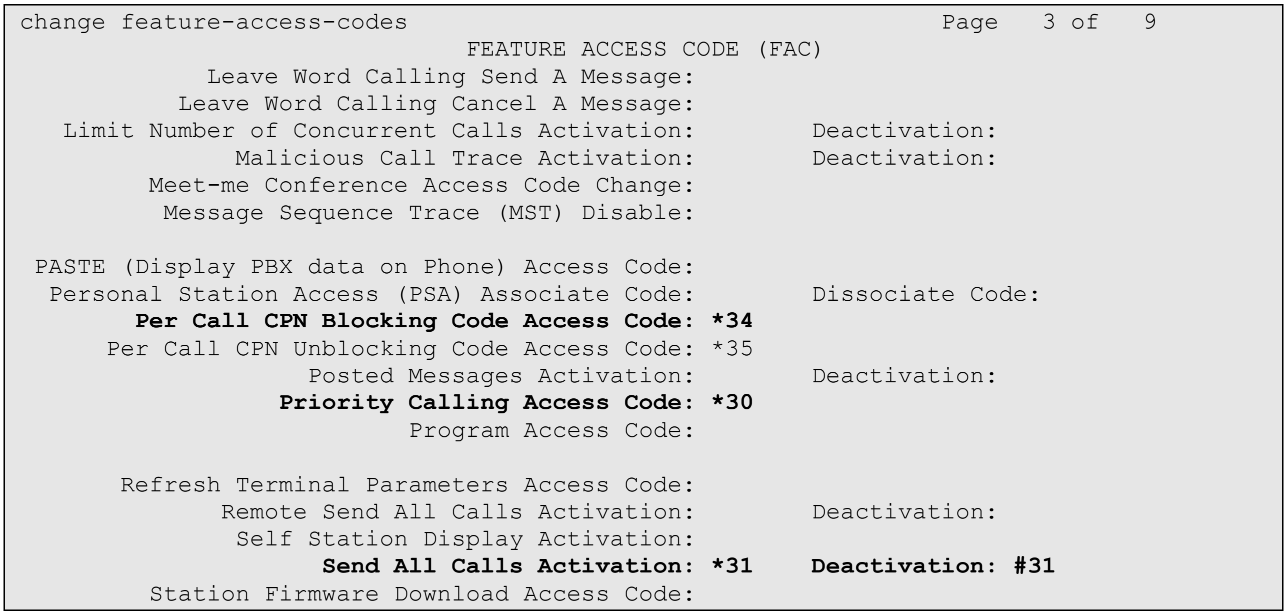
A FAC (feature access code) should be defined for each feature that will be used via the OPS FNEs. Use **change feature-access-codes** to define the required access codes. The FACs used in the sample configuration are shown in bold.



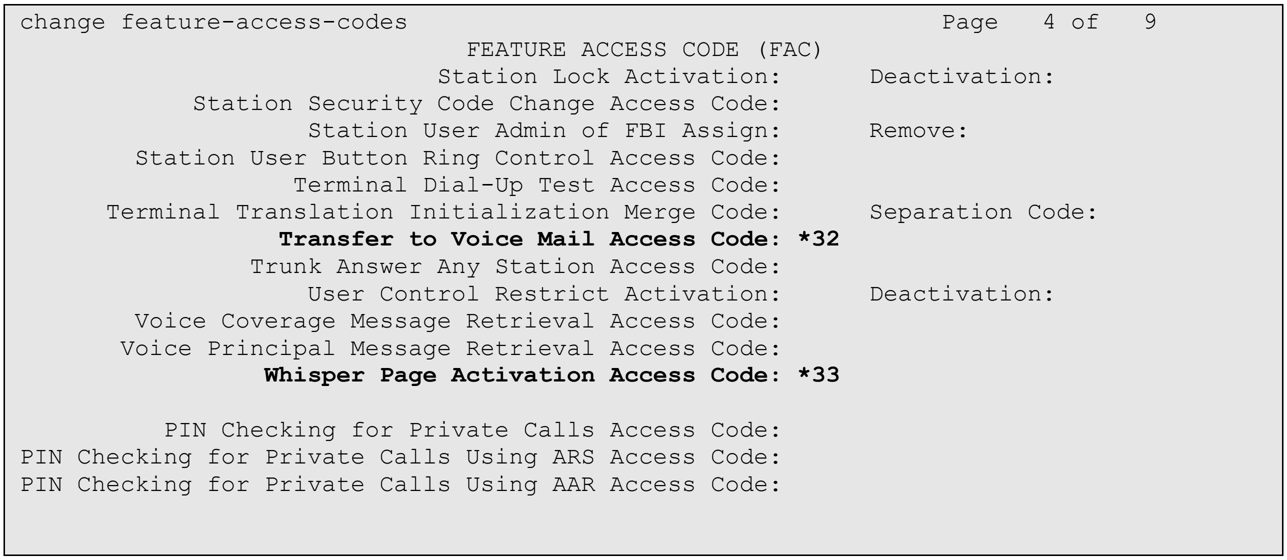
```
change feature-access-codes                                     Page   1 of   9
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial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



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

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



```
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:      Separation Code:
                  Transfer to Voice Mail Access Code: *32
                Trunk Answer Any Station Access Code:
                    User Control Restrict Activation:      Deactivation:
        Voice Coverage Message Retrieval Access Code:
       Voice Principal Message Retrieval Access Code:
                 Whisper Page Activation Access Code: *33

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

5.5. Define Feature Name Extensions (FNEs)

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

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

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

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

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

5.6. Configure Class of Service (COS)

Use the **change cos** command to set the appropriate service permissions to support OPS features (shown in bold). For the sample configuration a COS of **1** was used. Priority call indication (e.g., distinctive ring) is not supported on the *i* turret when using the Priority FNE. However, the iD808 does support a distinctive-ring/alerting mechanism locally on the turret, not covered in testing.

```
change cos                                                     Page   1 of   2

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

5.7. Configure Class of Restriction (COR)

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

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

               COR Number: 1
          COR Description: Default

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

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

5.8. Add Coverage Path

Use the **add coverage path n** command where **n** is the number of the coverage path to be added. Configure **Point 1** in the coverage path to one used to the voice messaging hunt group, which is group **h89** in the sample configuration. The default values shown for **Busy**, **Don't Answer**, and **DND/SAC/Goto Cover** can be used for the **Coverage Criteria**.

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

                   Coverage Path Number: 89
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA

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

COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h89           Rng:    Point2:
  Point3:                       Point4:
  Point5:                       Point6:
```

5.9. Add Stations

The Speakerbus iD808 *i* turret requires up to three stations for each device. Unlike previous versions of Session Manager the Station Features and button assignments can be added using the Endpoint Editor in System Manager. This method was used in this test configuration and procedure can be found in **Section 6.9**

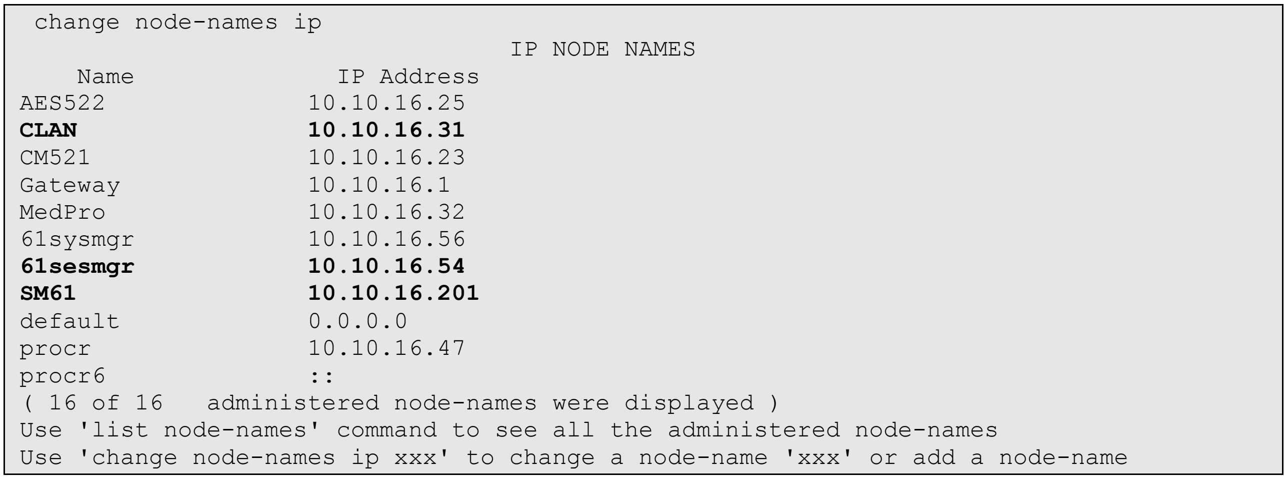
5.10. Verify Off PBX Station Mapping

Use the **display off-pbx-telephone station-mapping** command to verify that SIP Endpoints added to Session Manager in **section 6.9** have been administered in Communication Manager. The example below shows that **Station Extension 1310** uses the **Application OPS.**

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

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 1310             OPS          -      1310             aar        1
```

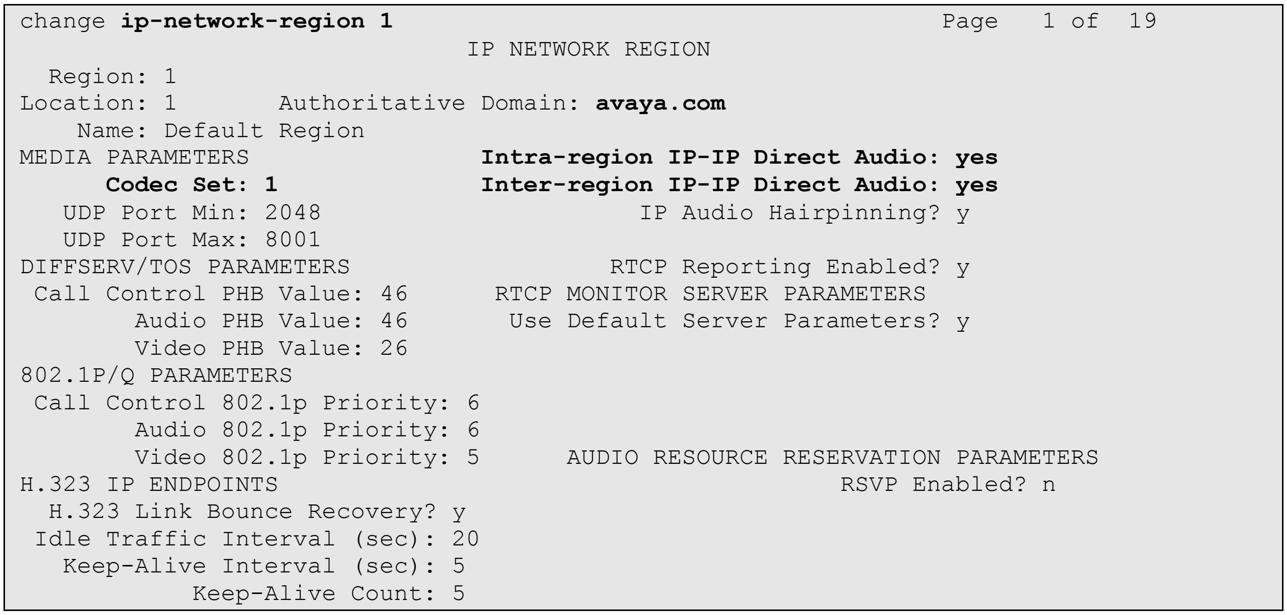
5.11. Configure SIP Trunk

In the **IP Node Names** form, assign an IP address and host name for the C-LAN board in the Avaya G650 Media Gateway and the Session Manager IP address. The host names will be used throughout the other configuration screens of Communication Manager.



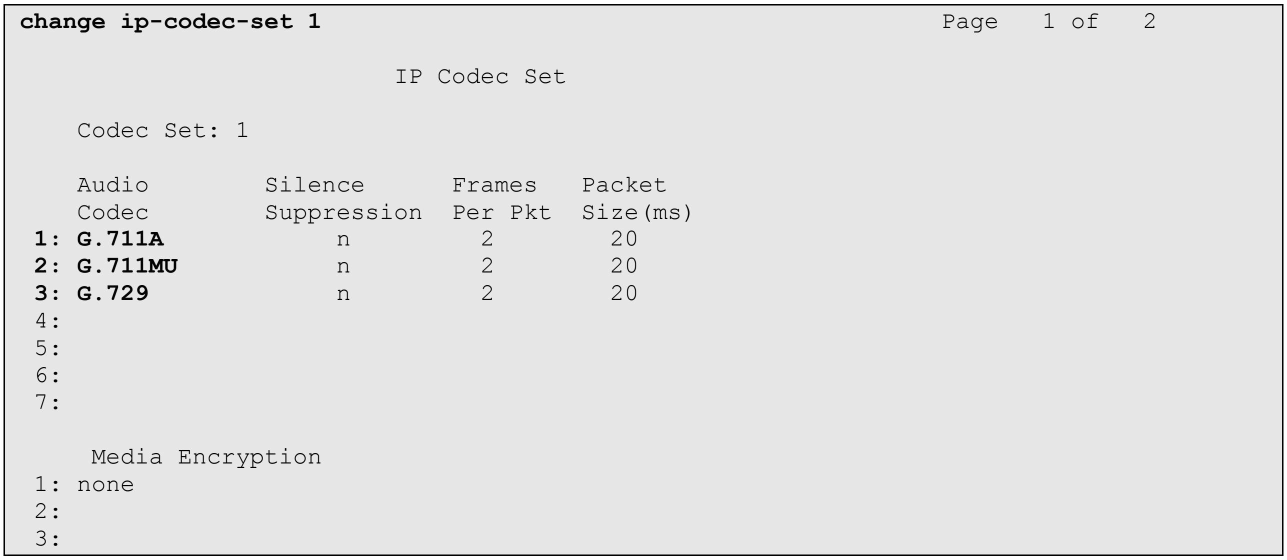
```
 change node-names ip
                                 IP NODE NAMES
    Name              IP Address
AES522              10.10.16.25
CLAN                10.10.16.31
CM521               10.10.16.23
Gateway             10.10.16.1
MedPro              10.10.16.32
61sysmgr            10.10.16.56
61sesmgr            10.10.16.54
SM61                10.10.16.201
default             0.0.0.0
procr               10.10.16.47
procr6              ::
( 16 of 16   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**. By default, **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G650 Media Gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session Manager as **ip-network region 1** is specified in the SIP signaling group.



```
change ip-network-region 1                                  Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Default Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 8001
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

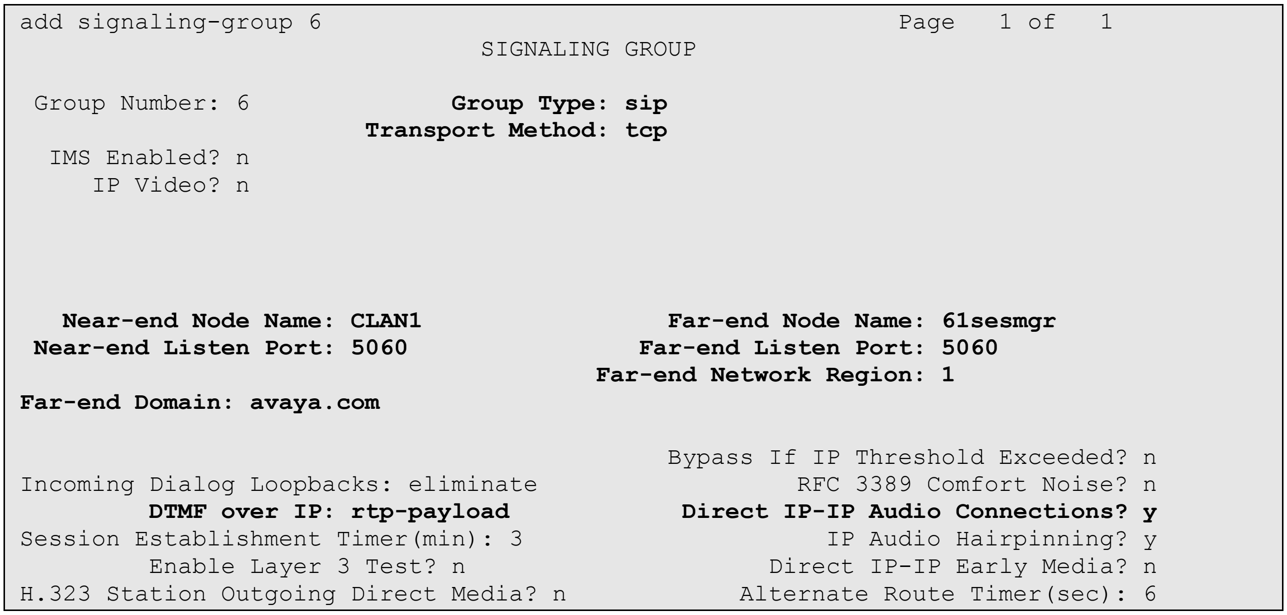
In the **IP Codec Set** form, select the audio codec's supported for calls routed over the SIP trunk to *i* turret deskstations. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), **G.711MU** (mu-law) and **G.729**, which are supported by the iD808 deskstations.



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

                          IP Codec Set

    Codec Set: 1

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

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

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown as follows:

- Set the **Group Type** field to **sip**
- Set the **Transport Method** to the desired transport method; **tcp** (transport control protocol) or tls (Transport Layer Security). **Note:** For transparency, tcp was used during this compliance test but the recommended method is tls
- Specify the node names for the C-LAN board in the G650 Media Gateway and the active Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above
- Ensure that the recommended port value of **5060** for tcp is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields **Note**: If tls is used then the recommended port value is 5061
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is **avaya.com**. This domain is specified in the Uniform Resource Identifier (URI) of the “SIP To Address” in the INVITE message. Mis-configuring this field may prevent calls from being successfully established to other SIP endpoints or to the PSTN
- If calls to/from SIP endpoints are to be shuffled, then the **Direct IP-IP Audio Connections** field must be set to **y**
- The **DTMF over IP** field should be set to the default value of **rtp-payload**. Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used



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

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




   Near-end Node Name: CLAN1                 Far-end Node Name: 61sesmgr
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1
Far-end Domain: avaya.com

                                             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? y
         Enable Layer 3 Test? n                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

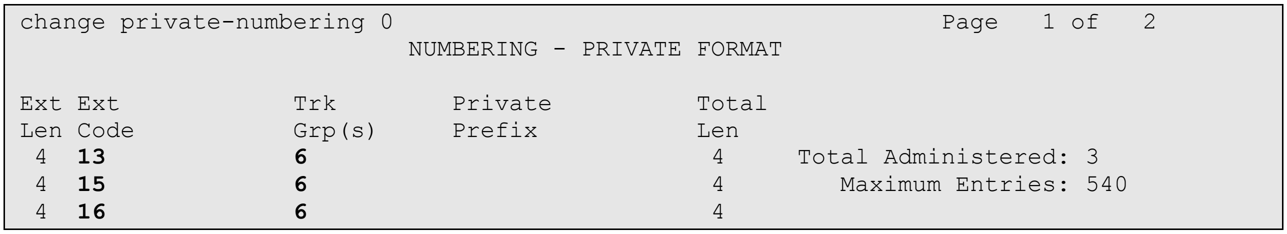
Configure the **Trunk Group** form as shown below. This trunk group is used for calls to *i* turret deskstations. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager. Set the **Service Type** field to **tie**, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

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

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

                                                       Signaling Group: 6
                                                     Number of Members: 30
```

On **Page 3** of the trunk group form, set the **Numbering Format** field to **private.** This field specifies the format of the calling party number sent to the far-end.

```
add trunk-group 6                                                    Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y

                     Numbering Format: private
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? y
                                               Replace Unavailable Numbers? y

 Show ANSWERED BY on Display? y
```

Configure the **Private Numbering** form to send the calling party number to the far-end. Add entries so that local stations with a 4-digit extension beginning with **13, 15 and 16** and whose calls are routed over SIP trunk group **6** have the number sent to the far-end for display purposes.



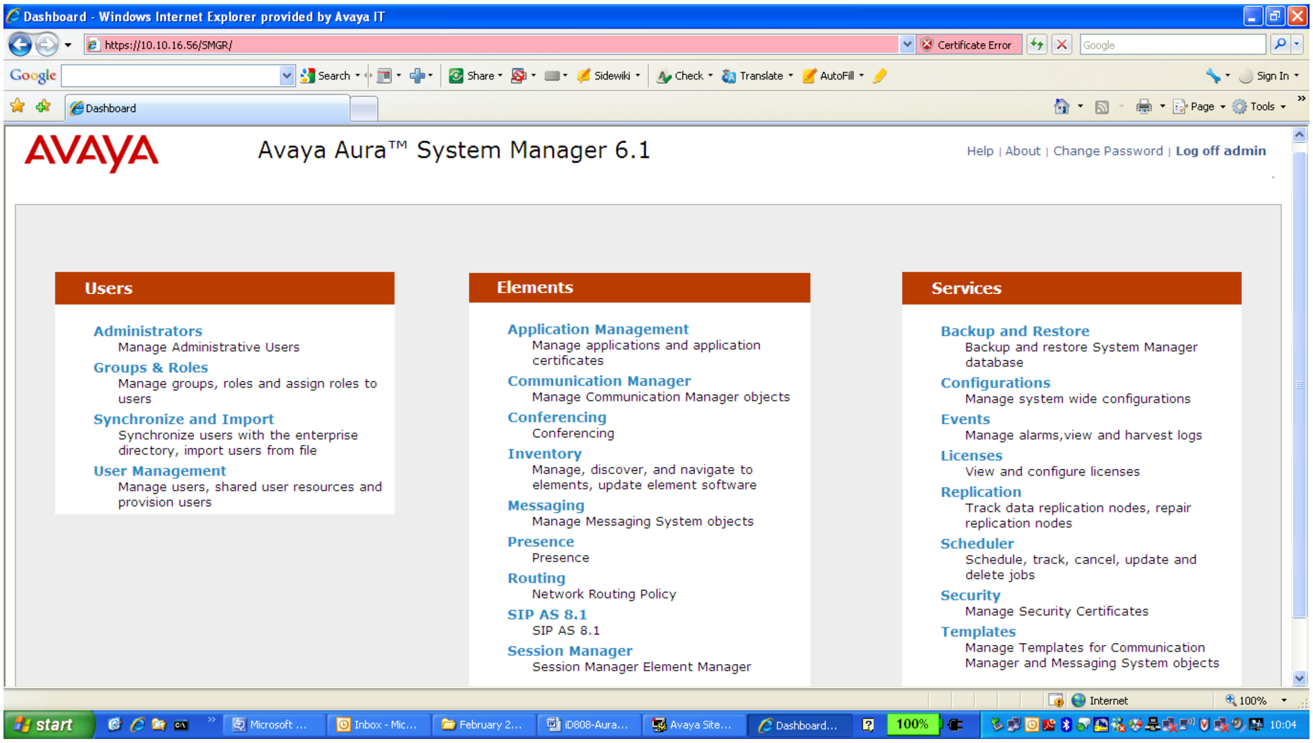
```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 4  13               6                            4     Total Administered: 3
 4  15               6                            4        Maximum Entries: 540
 4  16               6                            4
```

6. Configure Avaya Aura® Session Manager

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

6.1. Logging into Avaya Aura® System Manager

To access the administration web interface, enter **https://<ip-addr>/SMGR** as the URL in an Internet browser. Where <ip-addr> is the IP address of smgr on System Platform. Log in with the appropriate credentials. The main screen is displayed, as shown below.



AVAYA Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Users

- **Administrators** – Manage Administrative Users
- **Groups & Roles** – Manage groups, roles and assign roles to users
- **Synchronize and Import** – Synchronize users with the enterprise directory, import users from file
- **User Management** – Manage users, shared user resources and provision users

Elements

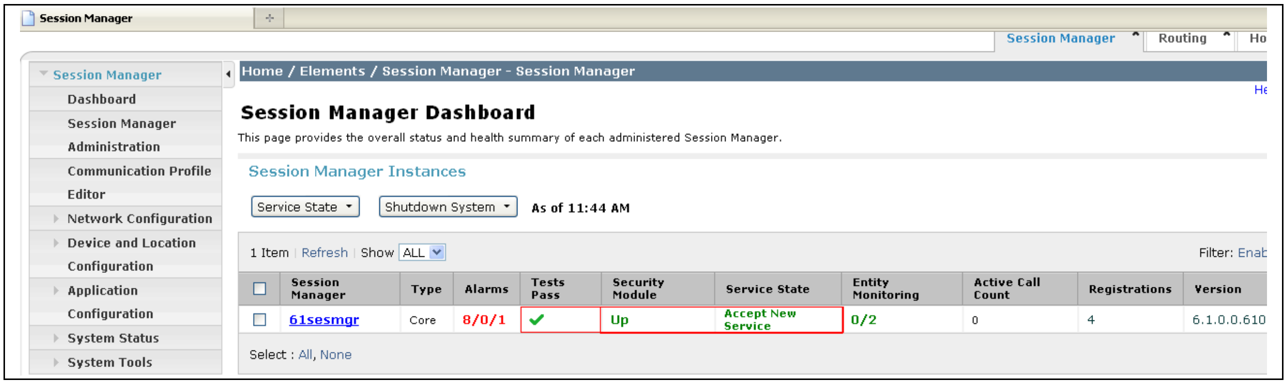
- **Application Management** – Manage applications and application certificates
- **Communication Manager** – Manage Communication Manager objects
- **Conferencing** – Conferencing
- **Inventory** – Manage, discover, and navigate to elements, update element software
- **Messaging** – Manage Messaging System objects
- **Presence** – Presence
- **Routing** – Network Routing Policy
- **SIP AS 8.1** – SIP AS 8.1
- **Session Manager** – Session Manager Element Manager

Services

- **Backup and Restore** – Backup and restore System Manager database
- **Configurations** – Manage system wide configurations
- **Events** – Manage alarms,view and harvest logs
- **Licenses** – View and configure licenses
- **Replication** – Track data replication nodes, repair replication nodes
- **Scheduler** – Schedule, track, cancel, update and delete jobs
- **Security** – Manage Security Certificates
- **Templates** – Manage Templates for Communication Manager and Messaging System objects

6.2. Verify System Properties

From the Dashboard of the web interface, choose **Session Manager** from the **Elements** section. Verify that a green tick shows under **Tests Passed**, **Security Module** is **Up** and **Service State** is set to **Accept New Service**.



Home / Elements / Session Manager - Session Manager

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

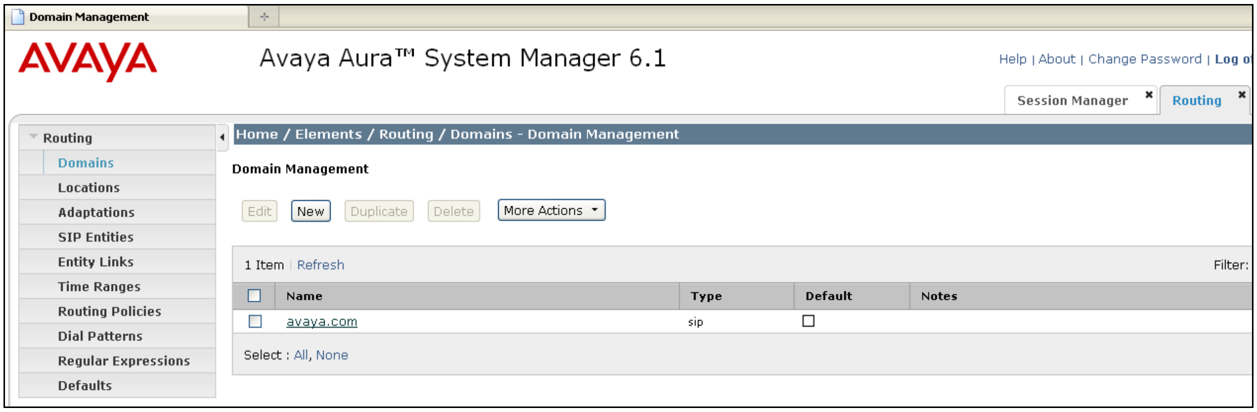
As of 11:44 AM

1 Item | Refresh | Show ALL

□	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
□	61sesmgr	Core	8/0/1	✓	Up	Accept New Service	0/2	0	4	6.1.0.0.610

Select : All, None

Next, go to **Routing** in the **Elements** section of the Dashboard and select **Domains** and check the domain administered.



Home / Elements / Routing / Domains - Domain Management

Domain Management

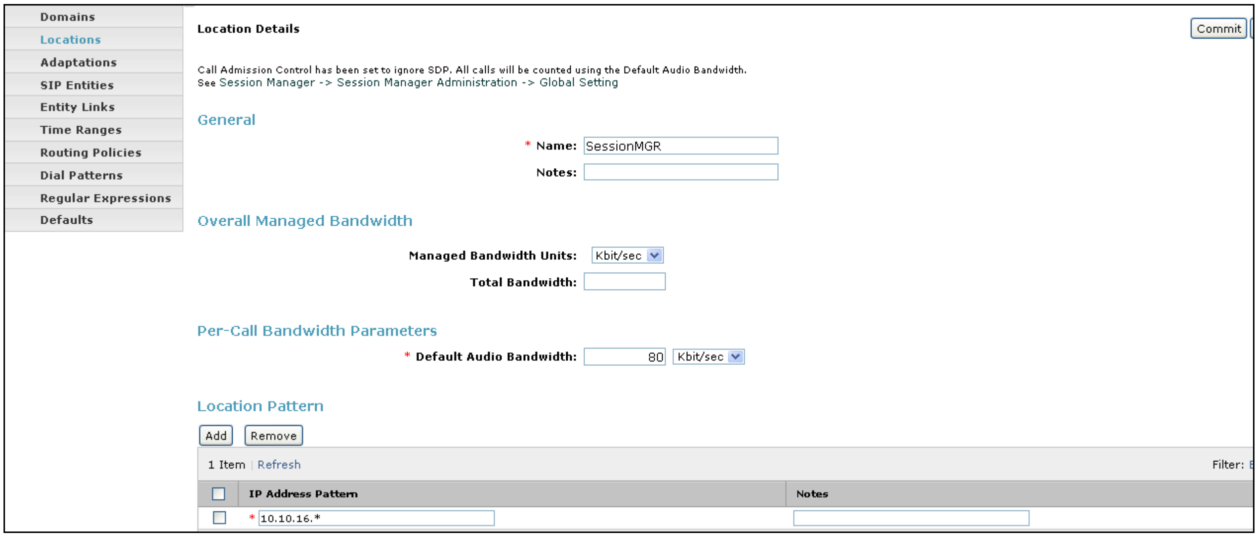
1 Item | Refresh

□	Name	Type	Default	Notes
□	avaya.com	sip	□	

Select : All, None

6.3. Add Location

Select **Routing** from the **Elements** section of the Dashboard and choose **Locations.** Click on the **New** button (not shown) and add a **Name** and specify the subnet in the format shown in the **IP Addresses Pattern** field under **Location Pattern**. Click on the **Commit** button to save.



Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name: SessionMGR

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

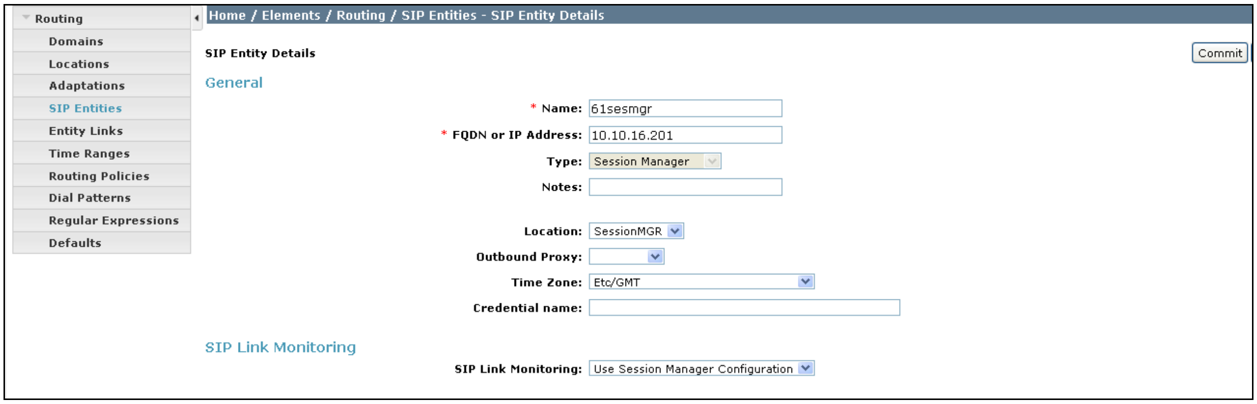
* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

□	IP Address Pattern	Notes
□	* 10.10.16.*	

6.4. Create a SIP entity

From the **Elements** section (not shown) of the Dashboard choose **Routing**. From the left-hand side menu choose **SIP Entities**. Click on the **New** and enter the information required and location as the Session Manager instance created.



Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: 61sesmgr

* FQDN or IP Address: 10.10.16.201

Type: Session Manager

Notes:

Location: SessionMGR

Outbound Proxy:

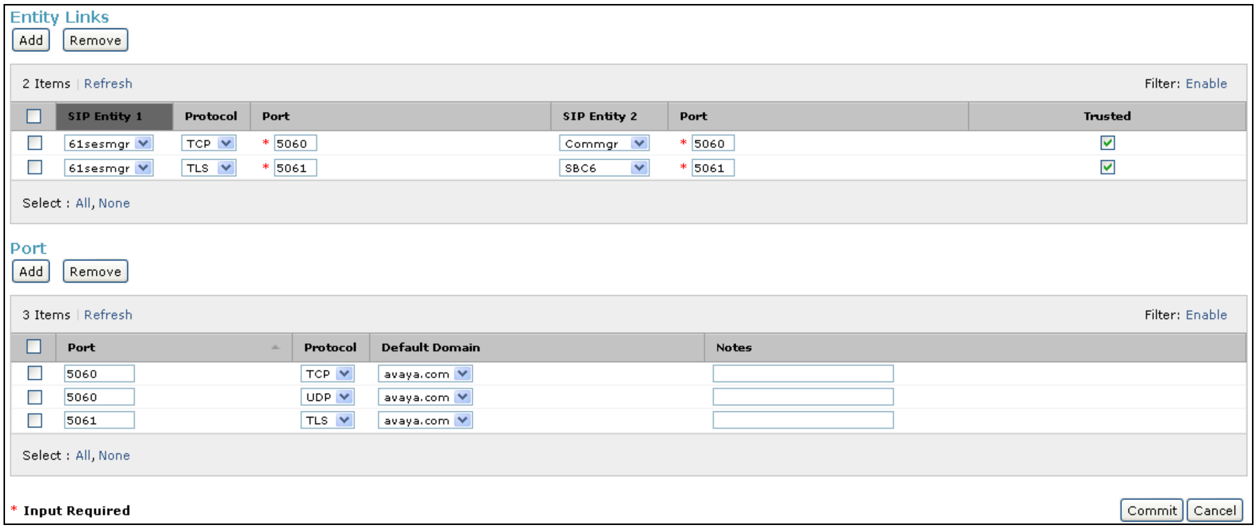
Time Zone: Etc/GMT

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Add the **Protocol** and **Port** information to the port section shown below. The entity link section will automatically populate after the link is added in **Section 6.5.** Click **Commit** to save the changes.



Entity Links

2 Items | Refresh

□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
□	61sesmgr	TCP	* 5060	Commgr	* 5060	☑
□	61sesmgr	TLS	* 5061	SBC6	* 5061	☑

Select : All, None

Port

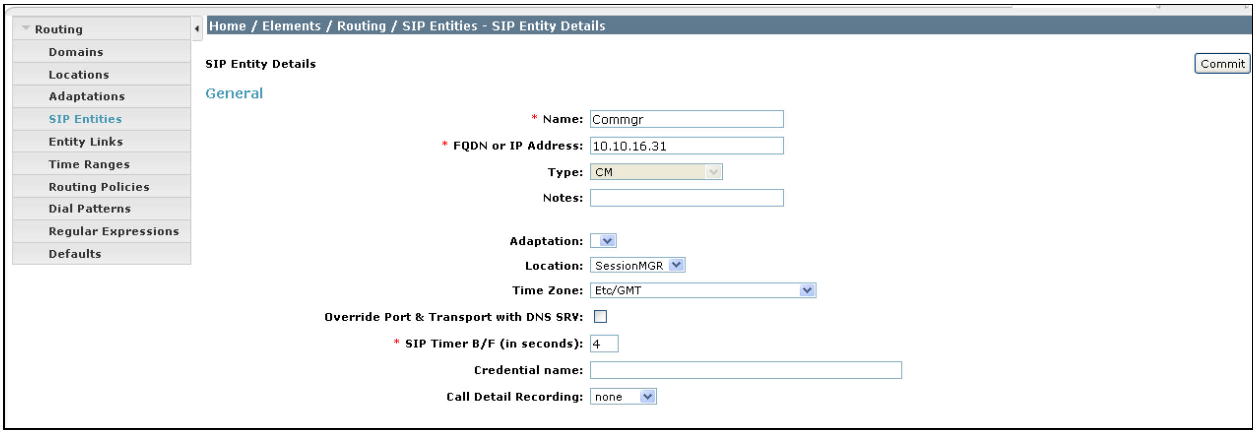
3 Items | Refresh

□	Port	Protocol	Default Domain	Notes
□	5060	TCP	avaya.com	
□	5060	UDP	avaya.com	
□	5061	TLS	avaya.com	

Select : All, None

* Input Required

Repeat this and add Communication Manager



SIP Entity Details

General

* Name: Commgr

* FQDN or IP Address: 10.10.16.31

Type: CM

Notes:

Adaptation:

Location: SessionMGR

Time Zone: Etc/GMT

Override Port & Transport with DNS SRV: □

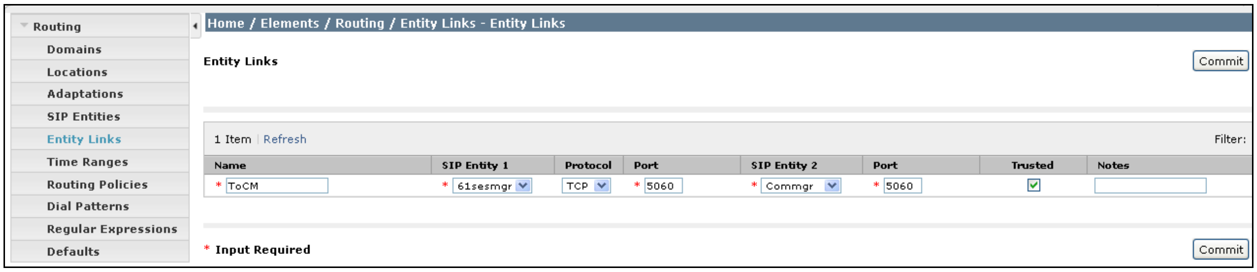
* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

6.5. Add an Entity link

From the Routing menu choose **Entity Links**, choose an appropriate name and then choose the entities added in **section 6.4,** the protocol you wish to use (TCP used in this example) and the port you wish to communication on. Click on the commit button to save.



Entity Links

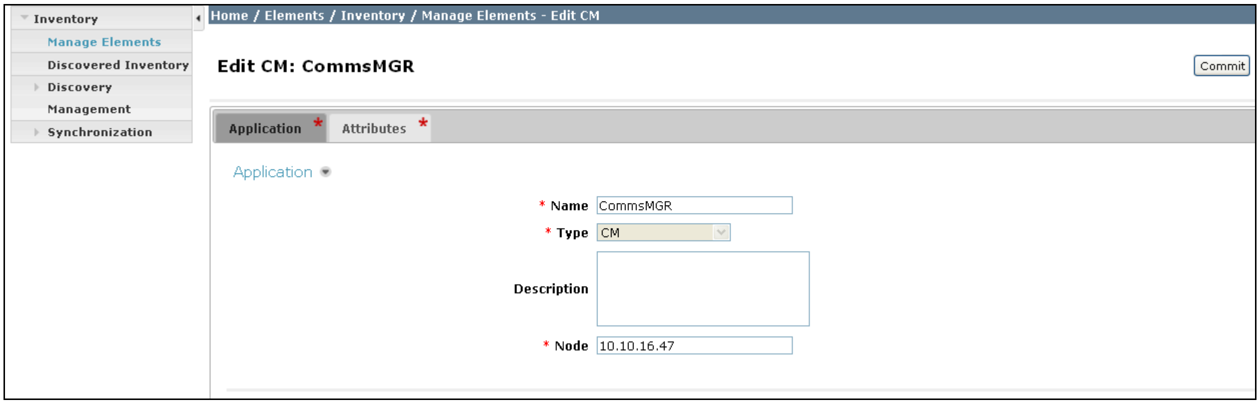
1 Item | Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ToCM	* 61sesmgr	TCP	* 5060	* Commgr	* 5060	☑	

* Input Required

6.6. Add Avaya Aura® Communication Manager Managed Element

From the **Elements** section of the Dashboard choose **Inventory** and then **Manage Elements**. Click the **New** button (not shown) and enter a valid name, set the **Type** field to **CM** and configure the SAT IP address in the **Node** field. Click on **Commit** to save.



Edit CM: CommsMGR

Application

* Name CommsMGR

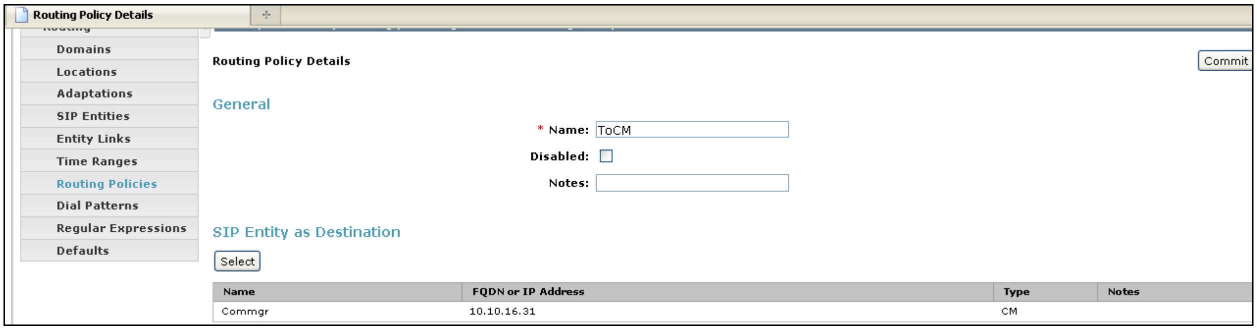
* Type CM

Description

* Node 10.10.16.47

6.7. Add Routing Policy

From the **Elements** section of the Dashboard choose **Routing** and then **Routing policy**. Click on the **New** button (not shown) and add a name for the policy. Select the Communication Manager entity as a Destination.



Routing Policy Details

General

* Name: ToCM

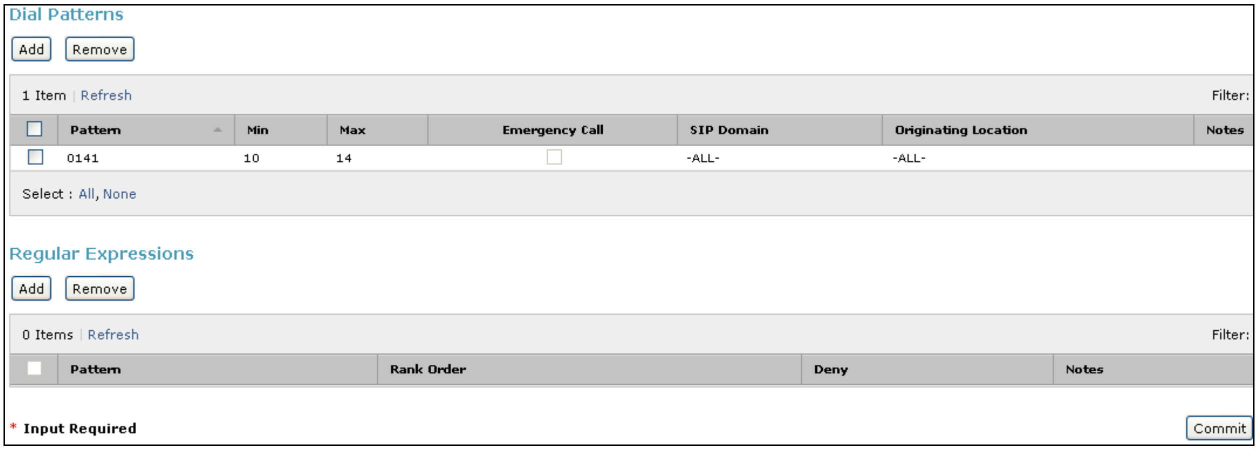
Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Commgr	10.10.16.31	CM	

Add dial patterns for non SIP stations and PSTN routing, and then click on the **Commit** button to save.



Dial Patterns

1 Item

□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
□	0141	10	14	□	-ALL-	-ALL-	

Regular Expressions

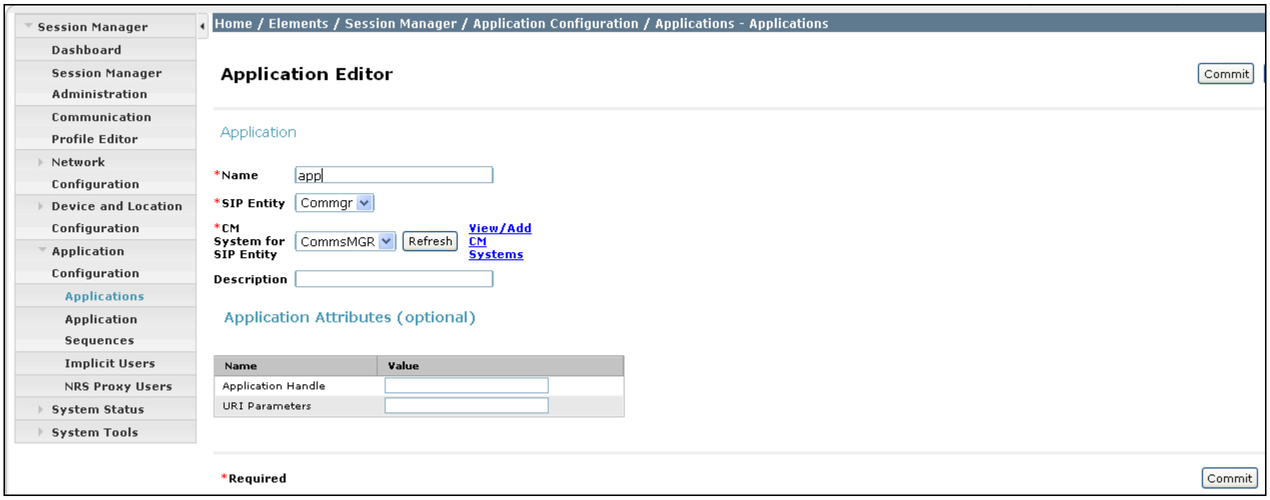
0 Items

□	Pattern	Rank Order	Deny	Notes

* Input Required

6.8. Add Application and Application Sequence

Select **Session Manager** from the **Elements** section of the Dashboard and choose **Application Configuration → Application.** Click on the **New** button (not shown) and enter the appropriate details as shown below. Click on the **Commit** button to save.



Home / Elements / Session Manager / Application Configuration / Applications - Applications

Application Editor

Application

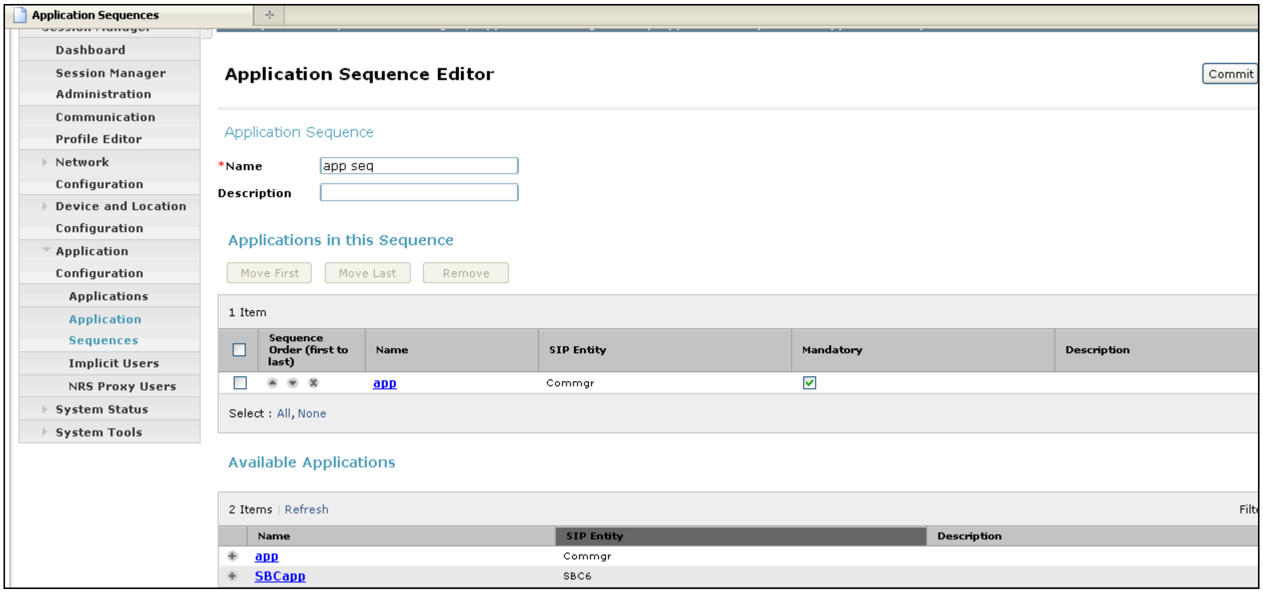
*Name	app
*SIP Entity	Commgr
*CM System for SIP Entity	CommsMGR
Description	

Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

*Required

Next, choose **Application Sequences** and click the **New** button (not shown). Add a name and select the available application to interact with the Communication Manager Entity. Click on the **Commit** button to save.



Application Sequence Editor

Application Sequence

*Name	app seq
Description	

Applications in this Sequence

1 Item

□	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
□		app	Commgr	☑	

Select : All, None

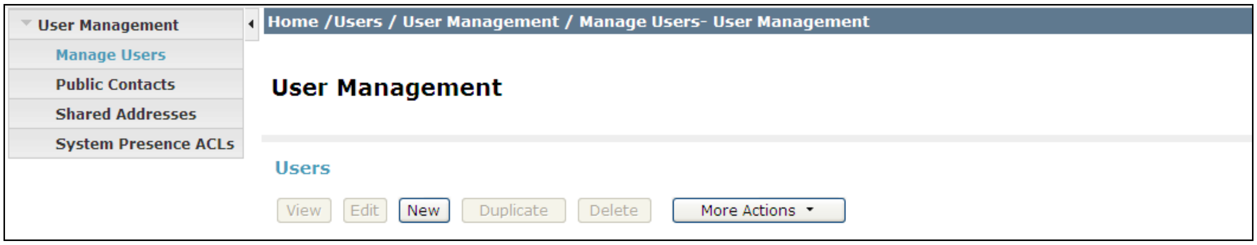
Available Applications

2 Items | Refresh

Name	SIP Entity	Description
app	Commgr	
SBCapp	SBC6	

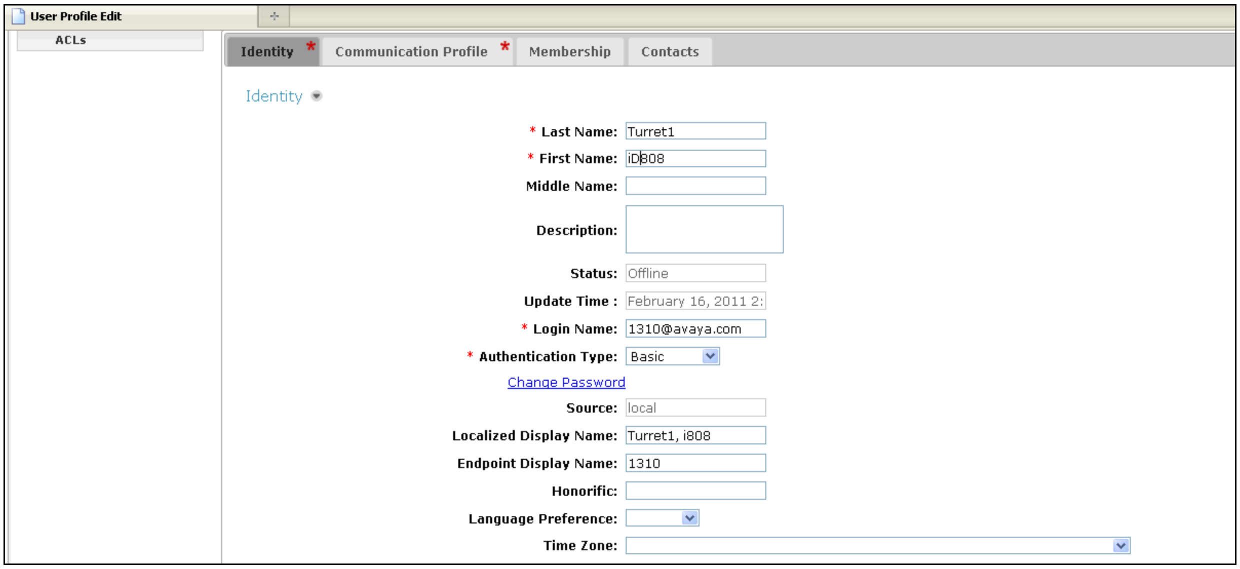
6.9. Add User

From the User section of the Dashboard choose **User Managerment** and then choose **Manage Users** from the menu. Click **New** to add a user.



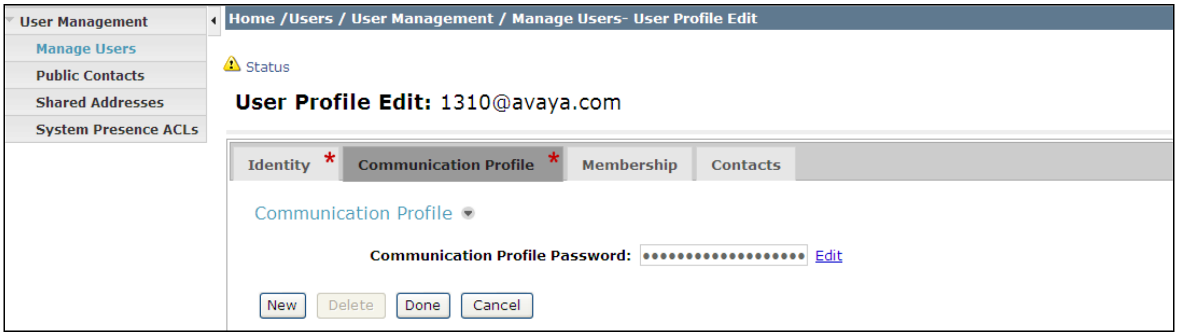
6.9.1. Add Primary iD808 Endpoint

Fill in the fields in the **Identity** tab and make sure that the **Login Name** is the fully qualified domain name and that the password is set (this is not the extension passcode).



* Last Name:	Turret1
* First Name:	iD808
Middle Name:	
Description:	
Status:	Offline
Update Time :	February 16, 2011 2:
* Login Name:	1310@avaya.com
* Authentication Type:	Basic
Source:	local
Localized Display Name:	Turret1, i808
Endpoint Display Name:	1310
Honorific:	
Language Preference:	
Time Zone:	

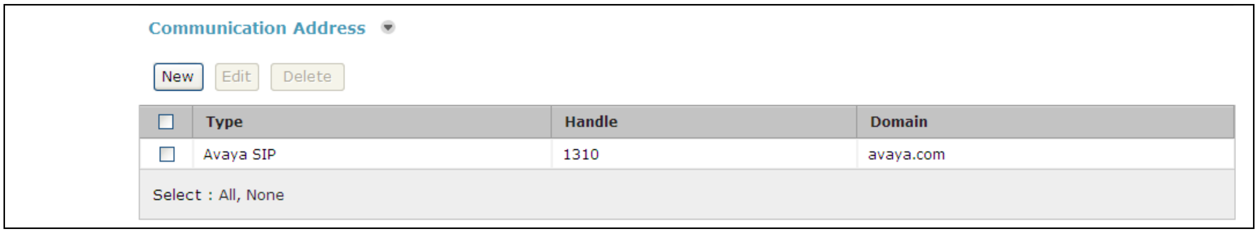
Next, choose the **Communication Profile** tab and enter the **Communication Profile Password** as the extension passcode to be used by the handset to register.



User Profile Edit: 1310@avaya.com

Communication Profile Password: ••••••••••••••••••••

Next, click **New** under **Communication Address** and specify the type, extension and domain. Click **Add** (not shown) to save this address.

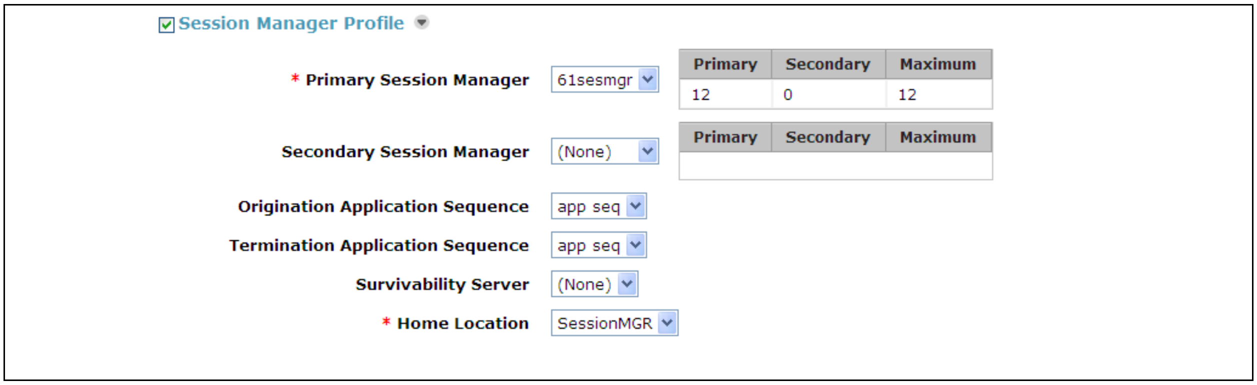


Communication Address

□	Type	Handle	Domain
□	Avaya SIP	1310	avaya.com

Select : All, None

Next, check the **Session Manager Profile** box and fill in the appropriate details.



☑ Session Manager Profile

* Primary Session Manager: 61sesmgr

Primary	Secondary	Maximum
12	0	12

Secondary Session Manager: (None)

Primary	Secondary	Maximum

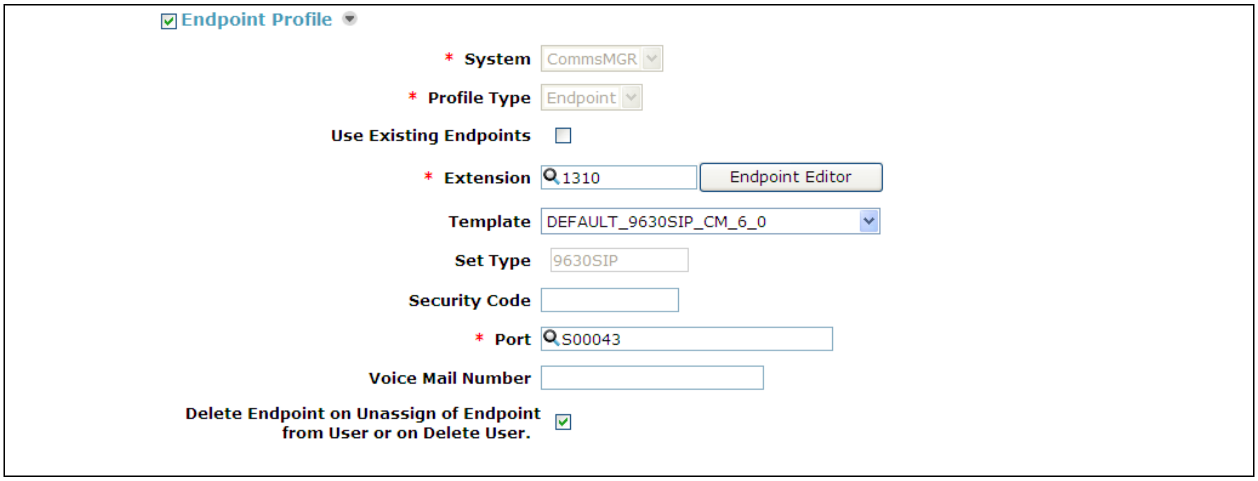
Origination Application Sequence: app seq

Termination Application Sequence: app seq

Survivability Server: (None)

* Home Location: SessionMGR

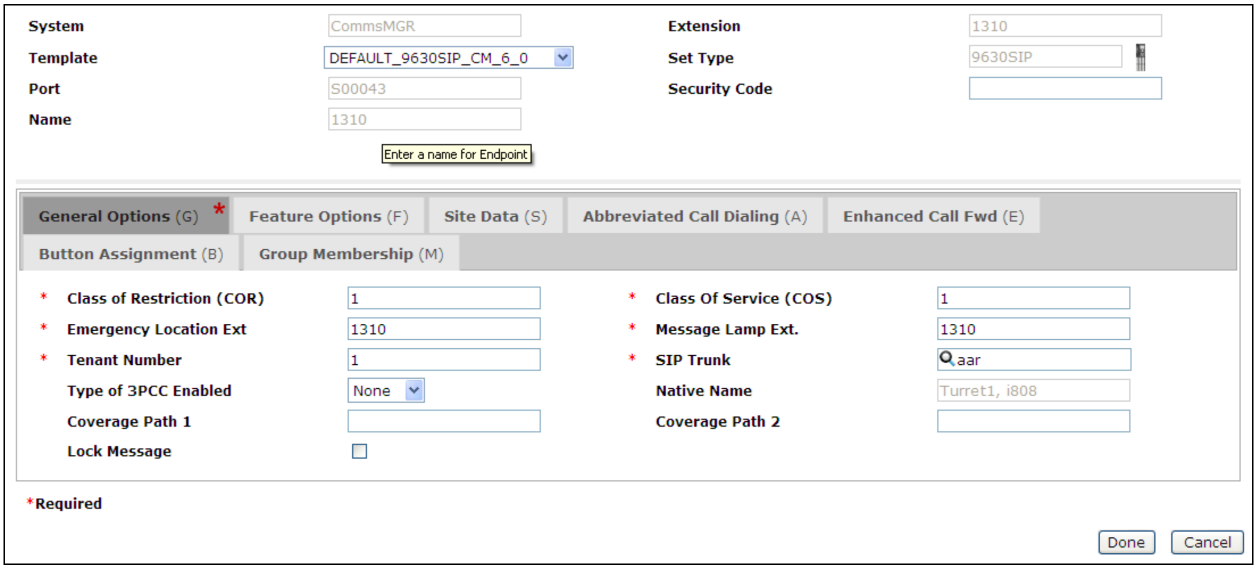
Next, check the **Endpoint Profile** box and fill in the appropriate details. Click on the **Endpoint Editor** button to administer station features and endpoint button assignments.



☑ Endpoint Profile

* System	CommsMGR
* Profile Type	Endpoint
Use Existing Endpoints	□
* Extension	1310
Template	DEFAULT_9630SIP_CM_6_0
Set Type	9630SIP
Security Code	
* Port	S00043
Voice Mail Number	
Delete Endpoint on Unassign of Endpoint from User or on Delete User.	☑

From the **General Options** Tab enter an appropriate **Class of Restriction**, **Class of Service**, **Emergency Location Extension**, **Message Lamp Extension**, **Tenant Number** and **SIP Trunk**. The values shown below are default values.



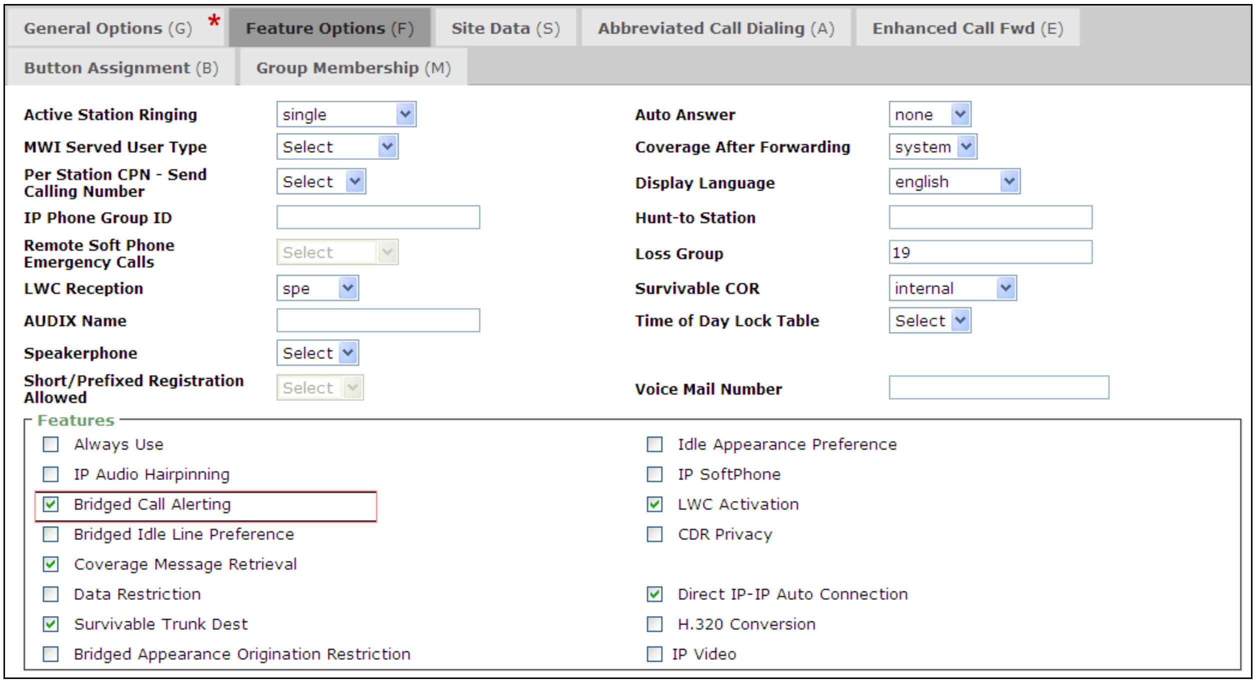
System	CommsMGR	Extension	1310
Template	DEFAULT_9630SIP_CM_6_0	Set Type	9630SIP
Port	S00043	Security Code	
Name	1310		

Enter a name for Endpoint

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	1310	* Message Lamp Ext.	1310
* Tenant Number	1	* SIP Trunk	aar
Type of 3PCC Enabled	None	Native Name	Turret1, i808
Coverage Path 1		Coverage Path 2	
Lock Message	□		

*Required

From the **Feature Options** tab, make sure **Bridged Call Alerting** is selected.

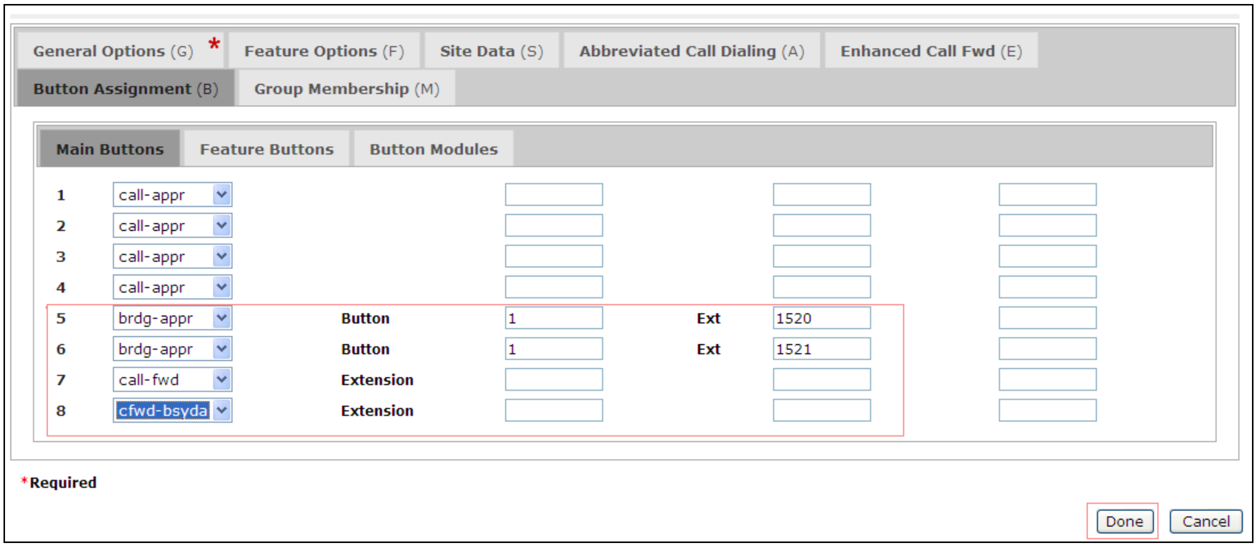


Active Station Ringing	single	Auto Answer	none
MWI Served User Type	Select	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	Select	Display Language	english
IP Phone Group ID		Hunt-to Station	
Remote Soft Phone Emergency Calls	Select	Loss Group	19
LWC Reception	spe	Survivable COR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

Features

□ Always Use	□ Idle Appearance Preference
□ IP Audio Hairpinning	□ IP SoftPhone
☑ Bridged Call Alerting	☑ LWC Activation
□ Bridged Idle Line Preference	□ CDR Privacy
☑ Coverage Message Retrieval	
□ Data Restriction	☑ Direct IP-IP Auto Connection
☑ Survivable Trunk Dest	□ H.320 Conversion
□ Bridged Appearance Origination Restriction	□ IP Video

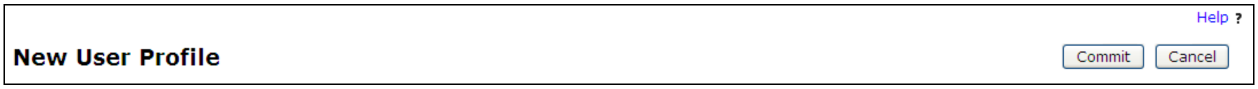
On the **Button Assignment** tab administer the **brdg-appr** buttons for the privacy extensions and the **call-fwd** and **cfwd-bsyda** buttons required. Click on the **Done** button to save changes.



1	call-appr					
2	call-appr					
3	call-appr					
4	call-appr					
5	brdg-appr	Button	1	Ext	1520	
6	brdg-appr	Button	1	Ext	1521	
7	call-fwd	Extension				
8	cfwd-bsyda	Extension				

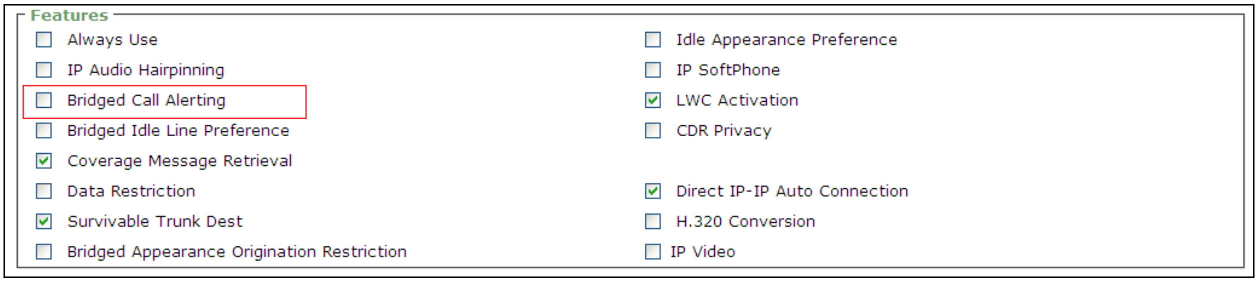
*Required

From the main user screen click on the **Commit** button to save.



6.9.2. Add Privacy Endpoints

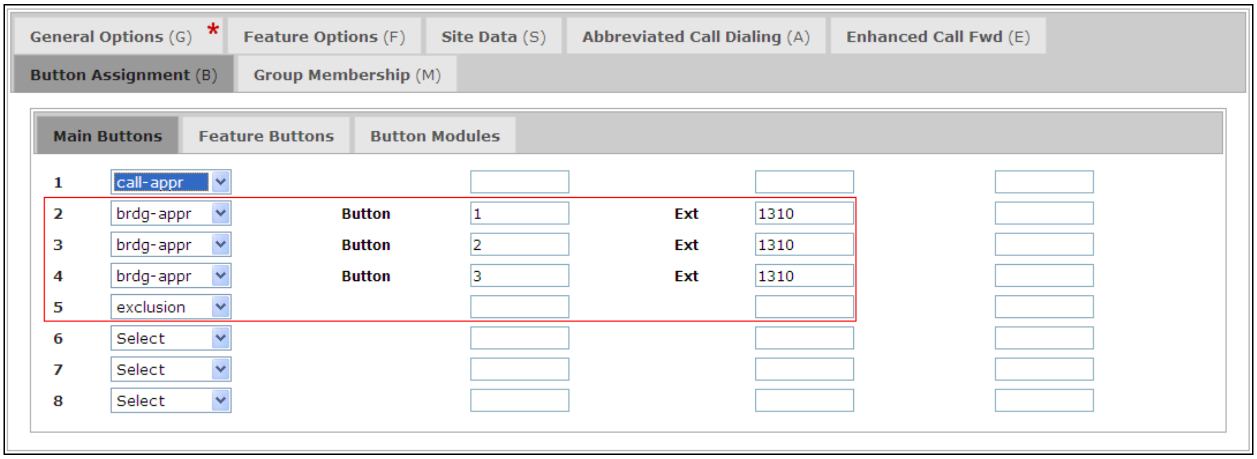
The privacy endpoints are added in the same way as the primary Endpoint. In the Endpoint Editor under the **Feature Options** tab, **Bridged Call Alerting** should not be selected.



Features

- □ Always Use
- □ IP Audio Hairpinning
- □ Bridged Call Alerting
- □ Bridged Idle Line Preference
- ☑ Coverage Message Retrieval
- □ Data Restriction
- ☑ Survivable Trunk Dest
- □ Bridged Appearance Origination Restriction
- □ Idle Appearance Preference
- □ IP SoftPhone
- ☑ LWC Activation
- □ CDR Privacy
- ☑ Direct IP-IP Auto Connection
- □ H.320 Conversion
- □ IP Video

Also, on the **Button assignments** tab, **brdg-appr** buttons must be added for the primary endpoint and an **exclusion** button to allow the Privacy feature. Clicking **Done** and **Commit** as in **Section 6.9.1** will save the endpoint.



1	call-appr					
2	brdg-appr	Button	1	Ext	1310	
3	brdg-appr	Button	2	Ext	1310	
4	brdg-appr	Button	3	Ext	1310	
5	exclusion					
6	Select					
7	Select					
8	Select					

7. Speakerbus iD808 *i* turret Configuration

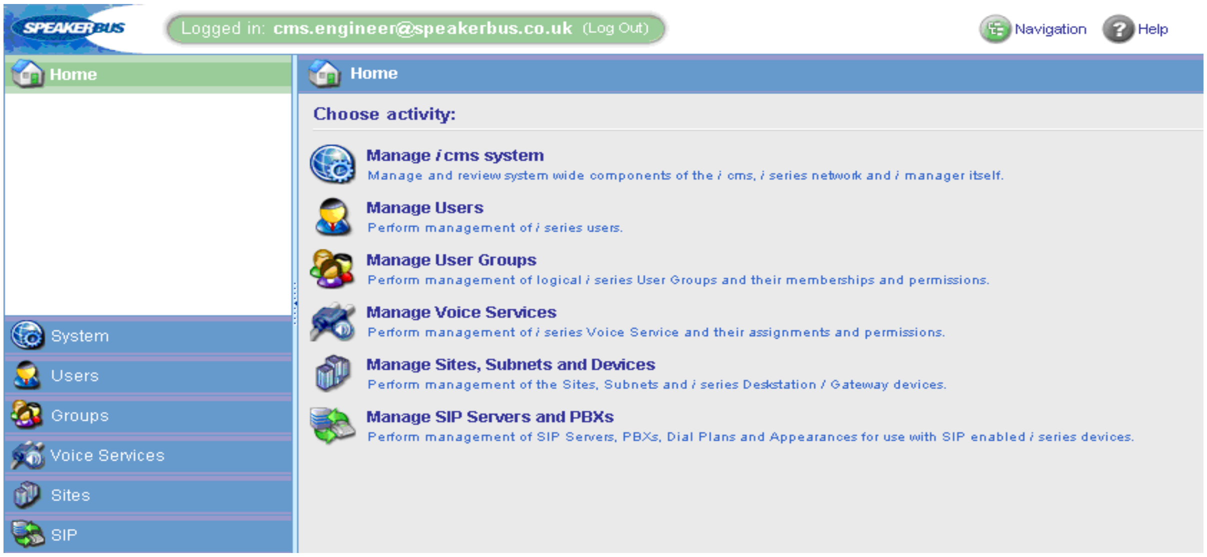
This section provides the procedure for configuring the Speakerbus iD808 *i* turret using *i* manager Administration. The *i* manager allows users to manage the iD808 *i* turret devices from a single workstation through a point-and-click interface using a web browser. The procedures for configuring an *i* turret fall into the following areas:

- Launch *i* manager
- Verify Product Key
- Create Site
- Create Subnet
- Create/Announce Deskstations
- Create PBX
- Create Dial Plan
- Create Appearances
- Create Users
- Create Groups
- Assign User Permissions
- Assign Ownership (of Appearances to Users)
- Assign Default Call Appearances
- Programming iD808 Deskstations (iD808 Layout)
- Assign Appearances to Deskstation Keys (iD808 Layout)
- Assign Bridged Call Appearances to Deskstations (iD808 Layout)
- Synchronize Deskstations/Live Updates
- Feature Name Extensions (FNEs)

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

7.1. Launch *i* manager

To access the *i* manager software interface, open a web browser and type the *i* manager web address, for example, http://10.10.16.50/imanager. Press the **Enter** key. In the *i* manager logon page, enter the appropriate credentials. The *i* manager home page is displayed as shown below.



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

Home

Choose activity:

Manage *i* cms system
Manage and review system wide components of the *i* cms, *i* series network and *i* manager itself.

Manage Users
Perform management of *i* series users.

Manage User Groups
Perform management of logical *i* series User Groups and their memberships and permissions.

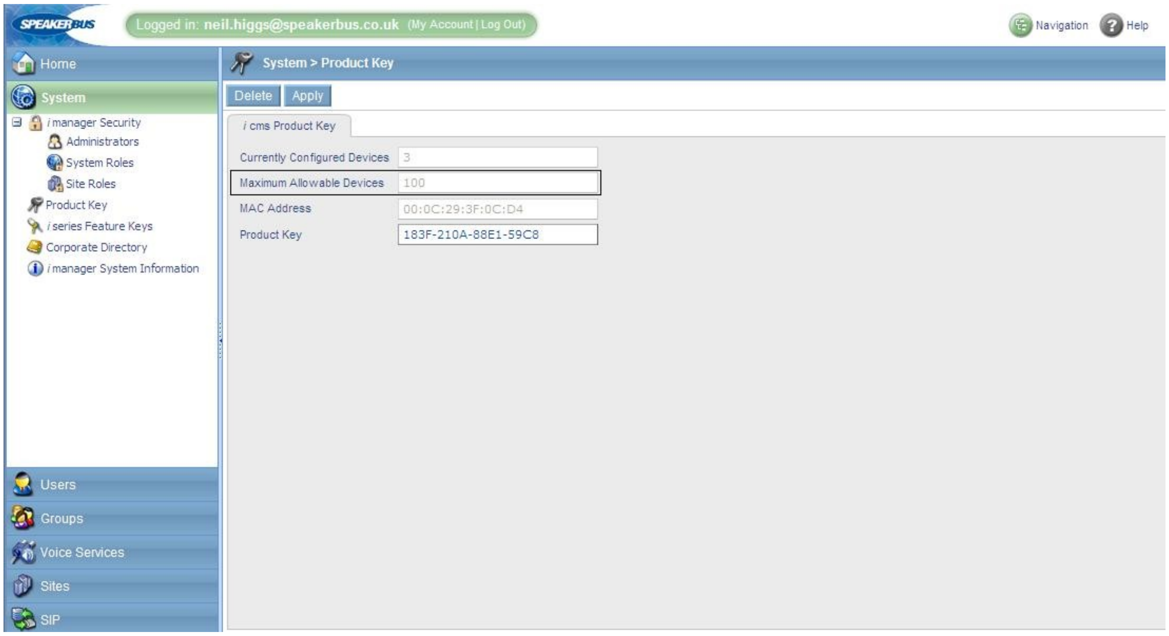
Manage Voice Services
Perform management of *i* series Voice Service and their assignments and permissions.

Manage Sites, Subnets and Devices
Perform management of the Sites, Subnets and *i* series Deskstation / Gateway devices.

Manage SIP Servers and PBXs
Perform management of SIP Servers, PBXs, Dial Plans and Appearances for use with SIP enabled *i* series devices.

7.2. Verify Product Key

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



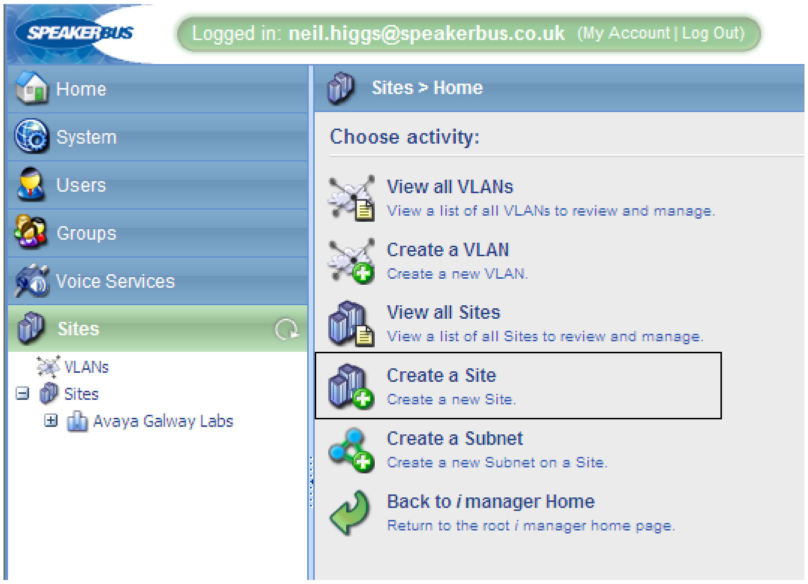
Logged in: neil.higgs@speakerbus.co.uk (My Account | Log Out)

System > Product Key

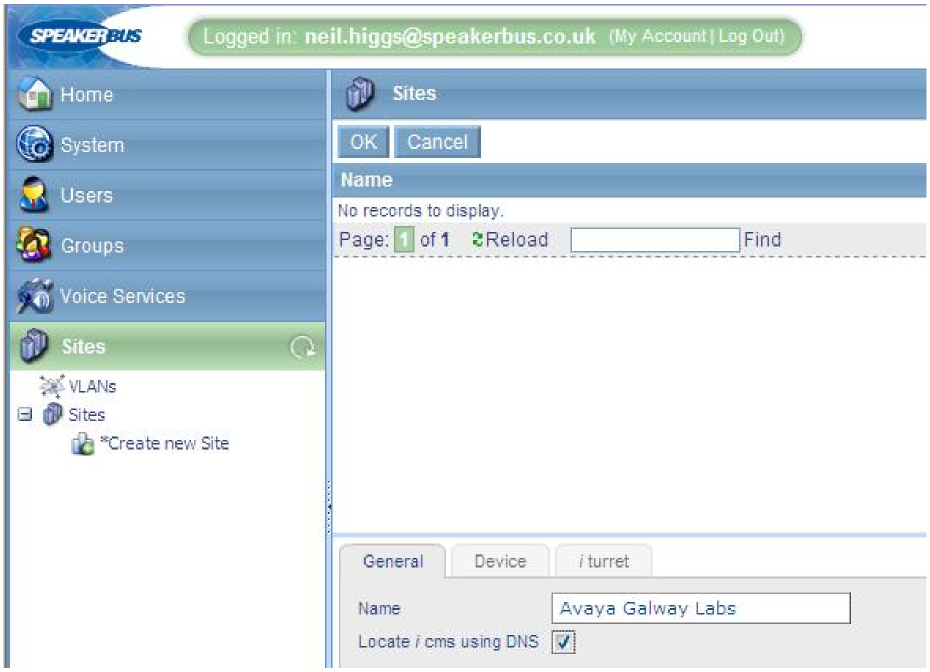
Currently Configured Devices: 3
Maximum Allowable Devices: 100
MAC Address: 00:0C:29:3F:0C:D4
Product Key: 183F-210A-88E1-59C8

7.3. Create Site

Configure a site representing the location where the Speakerbus turret devices are installed. Click **Sites** in the left pane, click on **Create a Site** in the right pane. The **Sites** page is displayed.



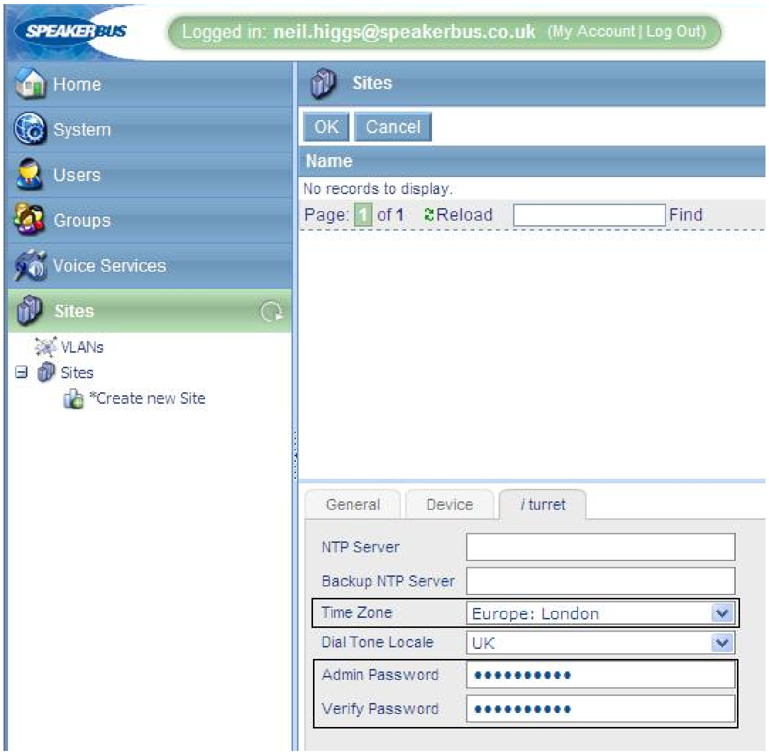
In the **General** tab of the **Sites** page, set the **Name** field to a descriptive name and select the **Locate *i* cms using DNS** checkbox. When this option is selected, *i* turret will use the DNS server to locate *i* cms server IP address. Refer to the *Speakerbus i manager Administrator`s Guide* for the correct configuration of DNS.



Name: Avaya Galway Labs

Locate *i* cms using DNS ☑

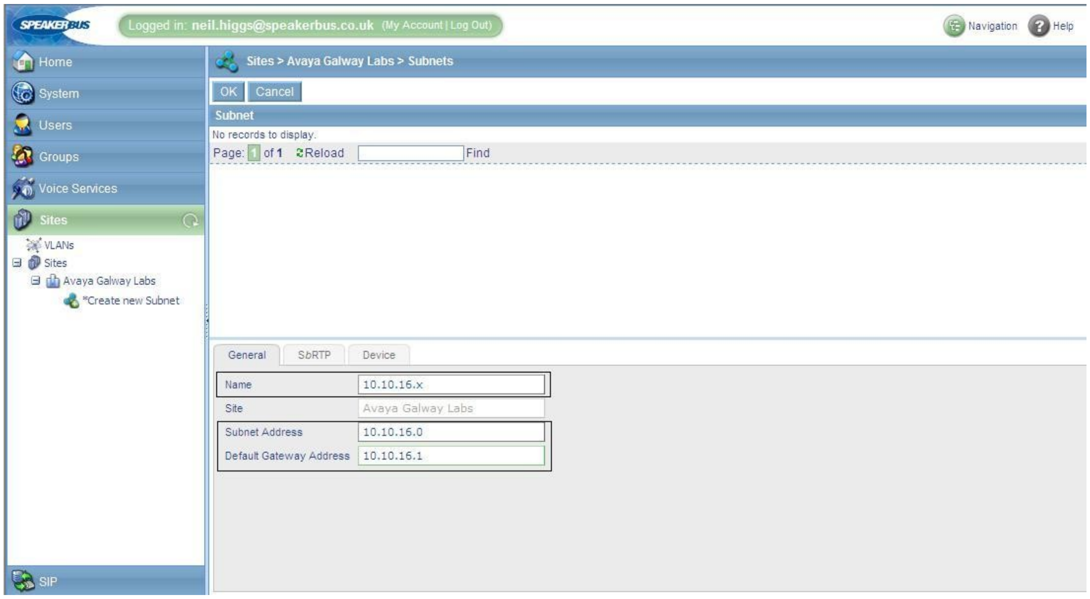
In the *i* turret tab, set the **NTP Time Zone** (network time protocol time zone) and configure the password for logging into the *i* turret deskstation by clicking the **Set Admin Password** button. The NTP Server field may be set to the IP address of the NTP server if one is used. Click **Apply.** The site will be now listed under **Sites**.



NTP Server	
Backup NTP Server	
Time Zone	Europe: London
Dial Tone Locale	UK
Admin Password	••••••••••
Verify Password	••••••••••

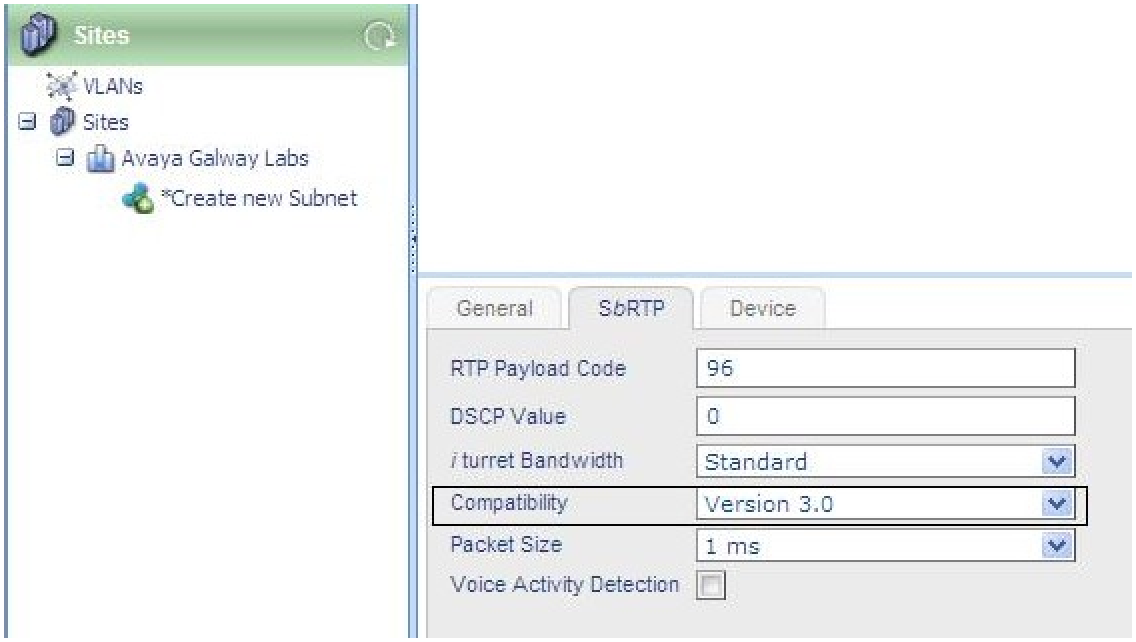
7.4. Create Subnet

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



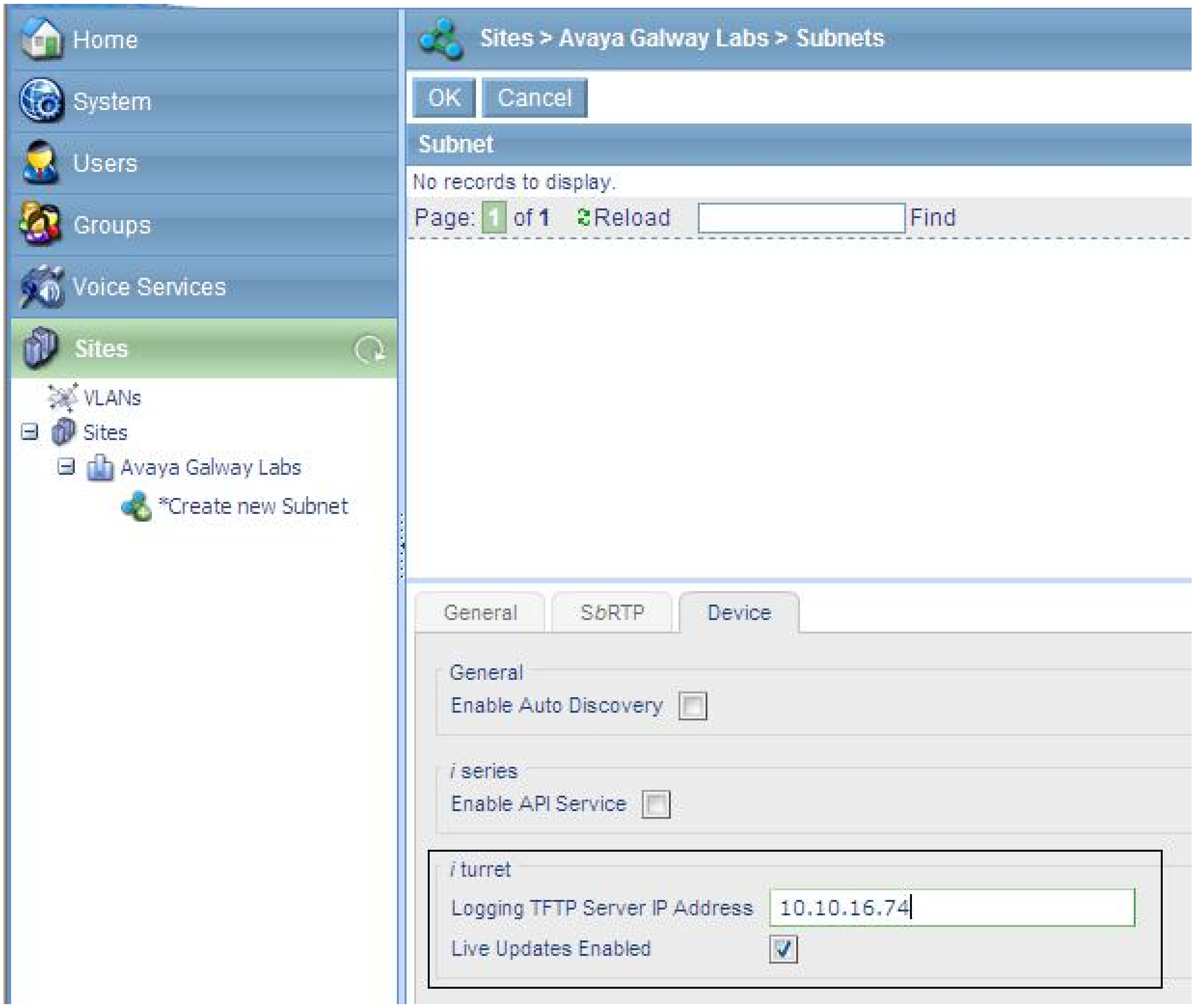
Name	10.10.16.x
Site	Avaya Galway Labs
Subnet Address	10.10.16.0
Default Gateway Address	10.10.16.1

In the **SbRTP** tab, set the **Compatibility** field to **Version 3.0**, leave everything else as default.



RTP Payload Code	96
DSCP Value	0
iTurret Bandwidth	Standard
Compatibility	Version 3.0
Packet Size	1 ms
Voice Activity Detection	☐

In the **Device** tab, set the *i* turret **Logging TFTP Server IP Address** and make sure the **Live Updates Enabled** tick box is checked (the later means that changes made in *i* cms will be sent automatically to the *i* turret without the need of synchronization). Click **OK**.



No records to display.

General

Enable Auto Discovery □

i series

Enable API Service □

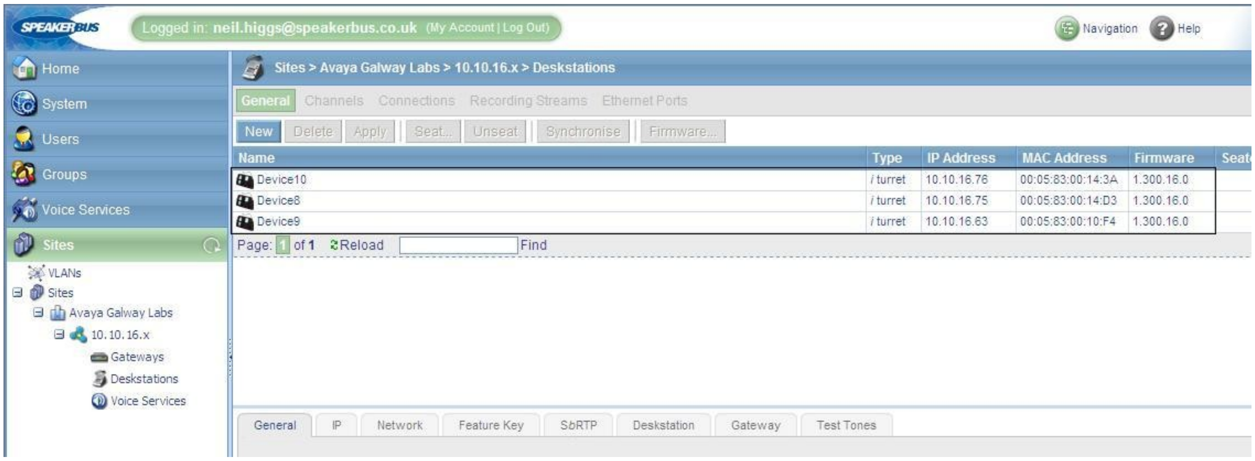
i turret

Logging TFTP Server IP Address 10.10.16.74

Live Updates Enabled ☑

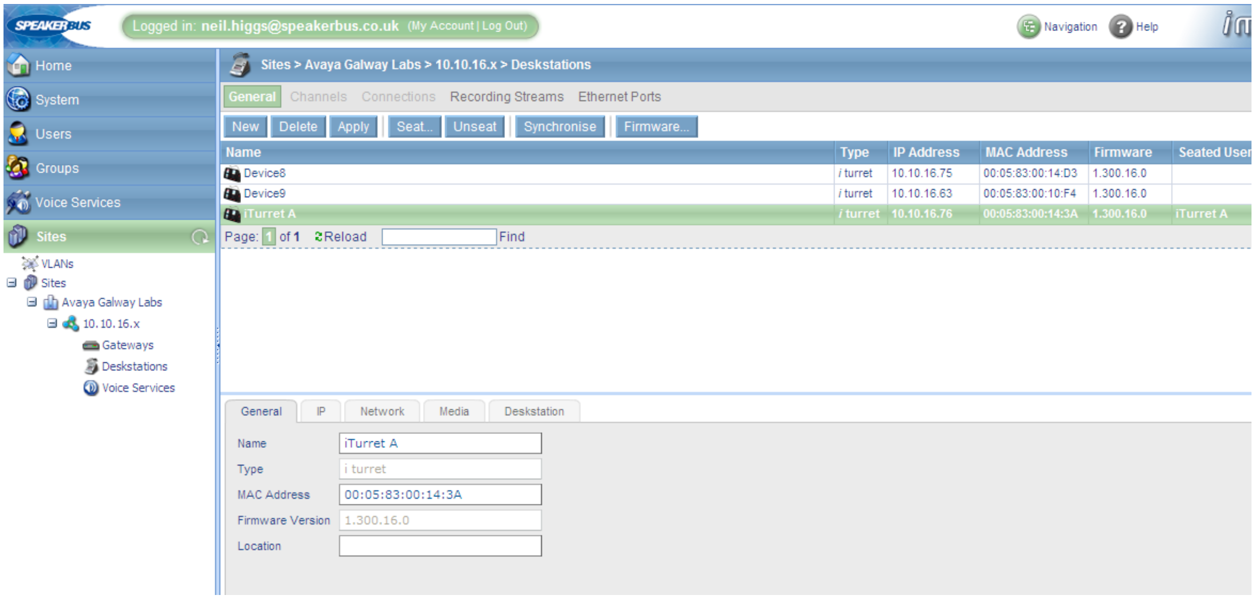
7.5. Create Deskstations

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



Name	Type	IP Address	MAC Address	Firmware	Seat
Device10	*i* turret	10.10.16.76	00:05:83:00:14:3A	1.300.16.0	
Device8	*i* turret	10.10.16.75	00:05:83:00:14:D3	1.300.16.0	
Device9	*i* turret	10.10.16.63	00:05:83:00:10:F4	1.300.16.0	

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

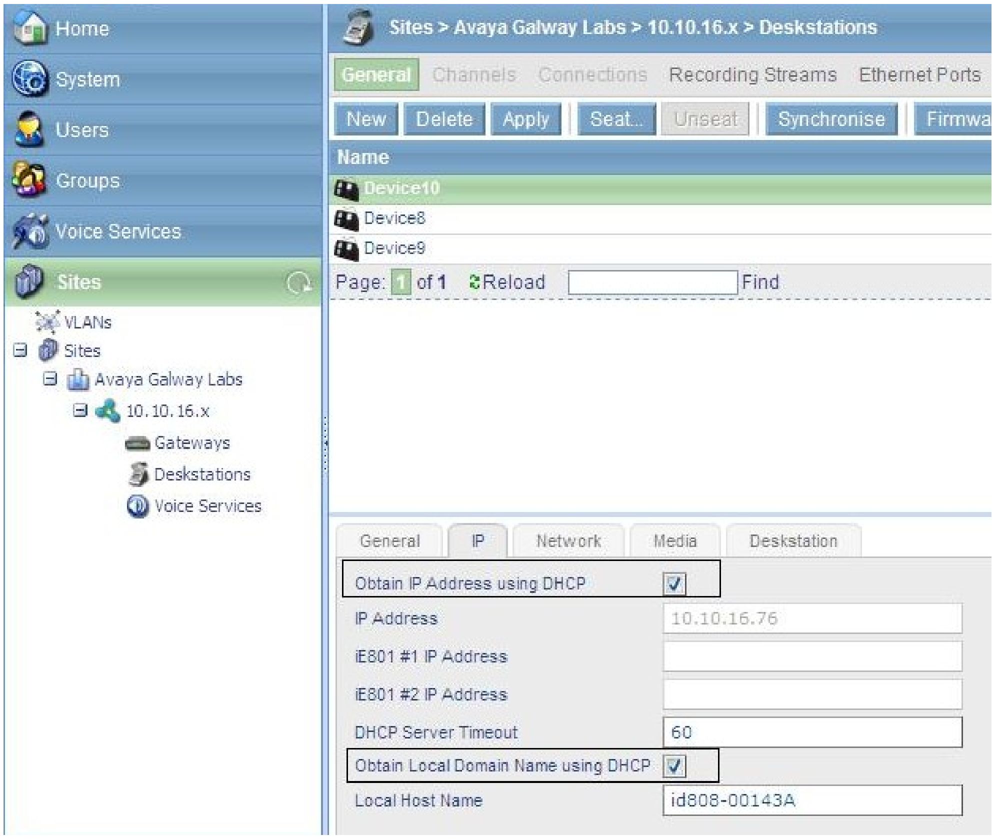


Name	Type	IP Address	MAC Address	Firmware	Seated User
Device8	*i* turret	10.10.16.75	00:05:83:00:14:D3	1.300.16.0	
Device9	*i* turret	10.10.16.63	00:05:83:00:10:F4	1.300.16.0	
iTurret A	*i* turret	10.10.16.76	00:05:83:00:14:3A	1.300.16.0	iTurret A

Page: 1 of 1 Reload Find

Name	iTurret A
Type	i turret
MAC Address	00:05:83:00:14:3A
Firmware Version	1.300.16.0
Location	

In the **IP** tab, verify that the **Obtain IP Address using DHCP** and the **Obtain local Domain Name using DHCP** tick boxes are checked (make sure you have a running DHCP and DNS Server on the network with relevant settings in both).

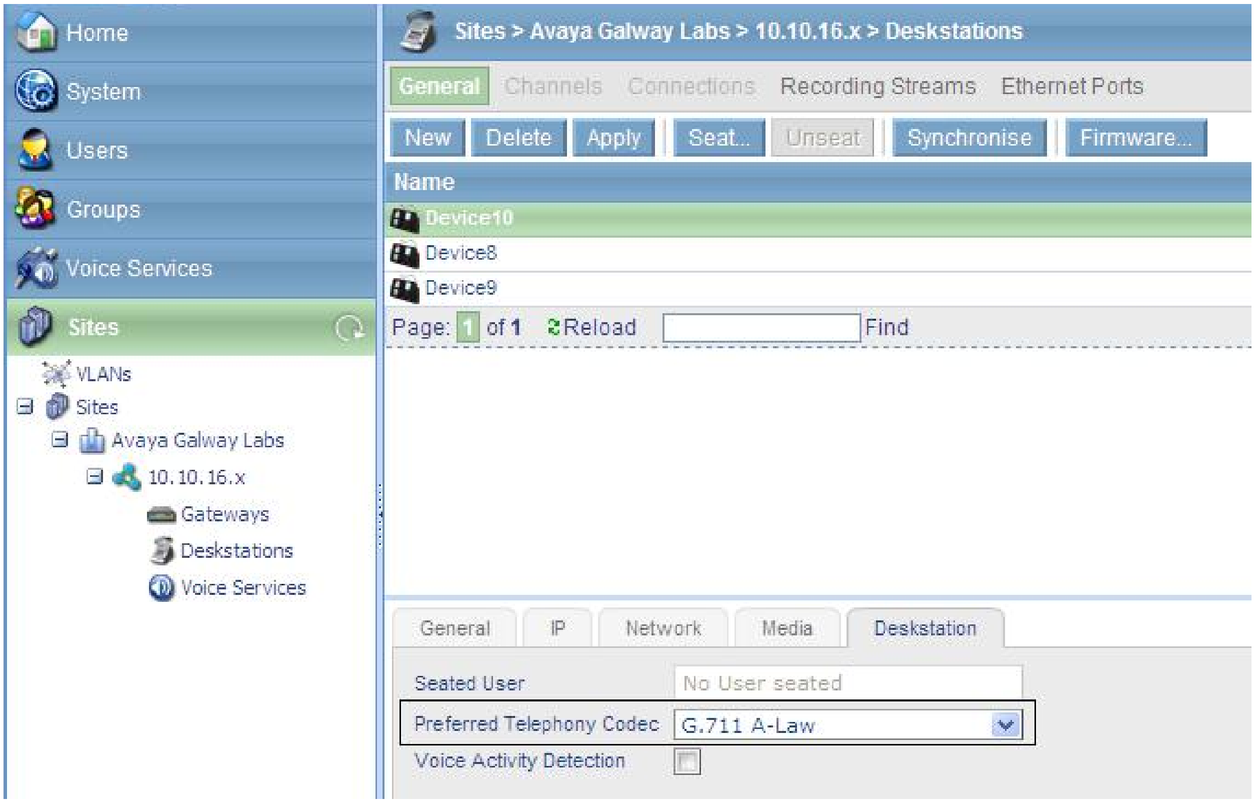


Name
Device10
Device8
Device9

Page: 1 of 1 Reload Find

Obtain IP Address using DHCP	☑
IP Address	10.10.16.76
iE801 #1 IP Address	
iE801 #2 IP Address	
DHCP Server Timeout	60
Obtain Local Domain Name using DHCP	☑
Local Host Name	id808-00143A

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



Seated User: No User seated

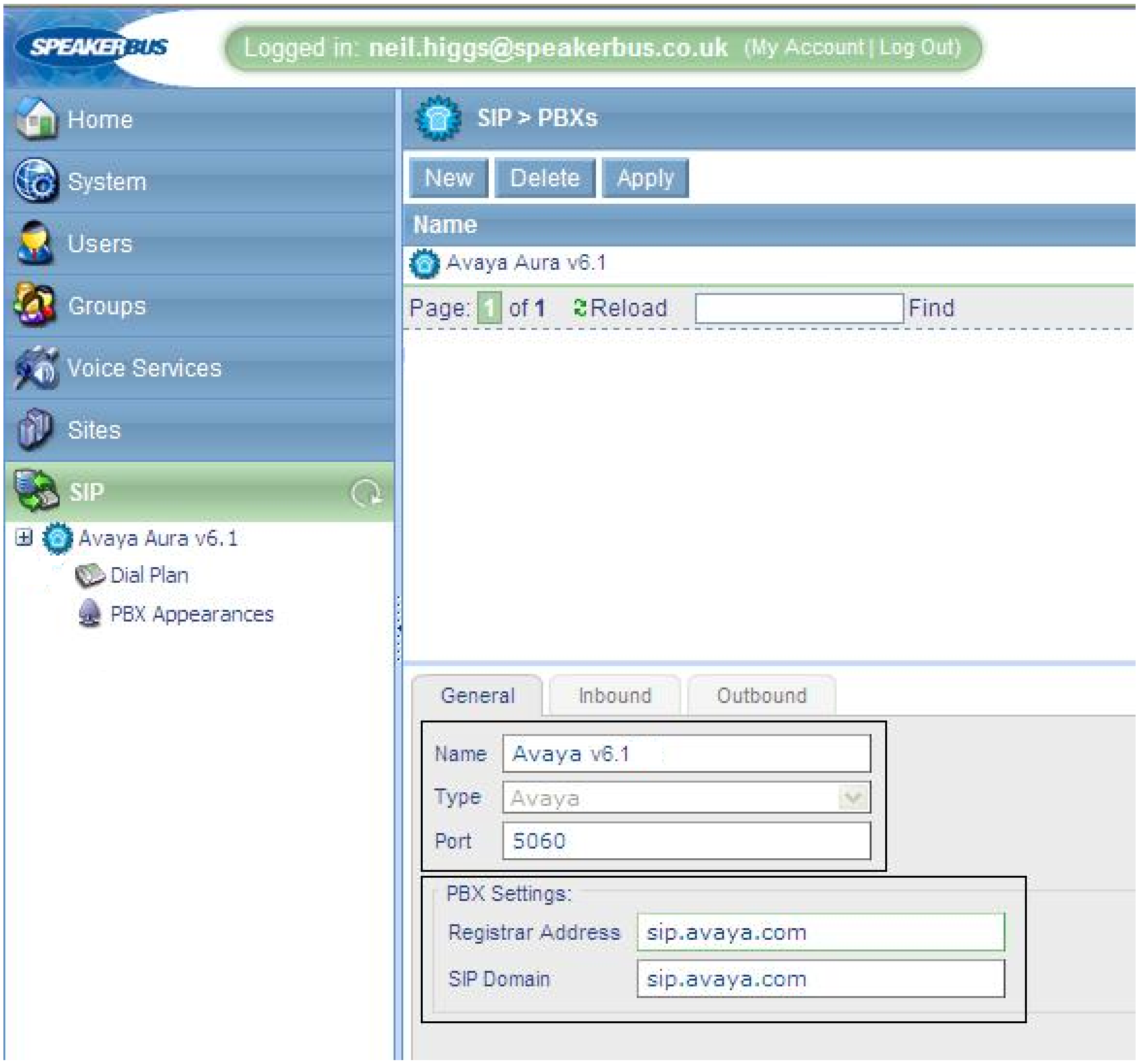
Preferred Telephony Codec: G.711 A-Law

Voice Activity Detection: □

7.6. Create SIP Server

To create a SIP Server, click **Create a new SIP Server** under the **SIP** directory in the left pane. Provide a descriptive name for the SIP server and select **AVAYA** from the **Type** dropdown box**.** In the **Registrar Address** and **SIP Domain** fields set to **sip.avaya.com**, in this configuration DNS resolves the domain name to 10.10.16.5, the Session Manager active IP address. After the SIP server is created, the **Port** field will be displayed on this page with the default value of 5060.

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



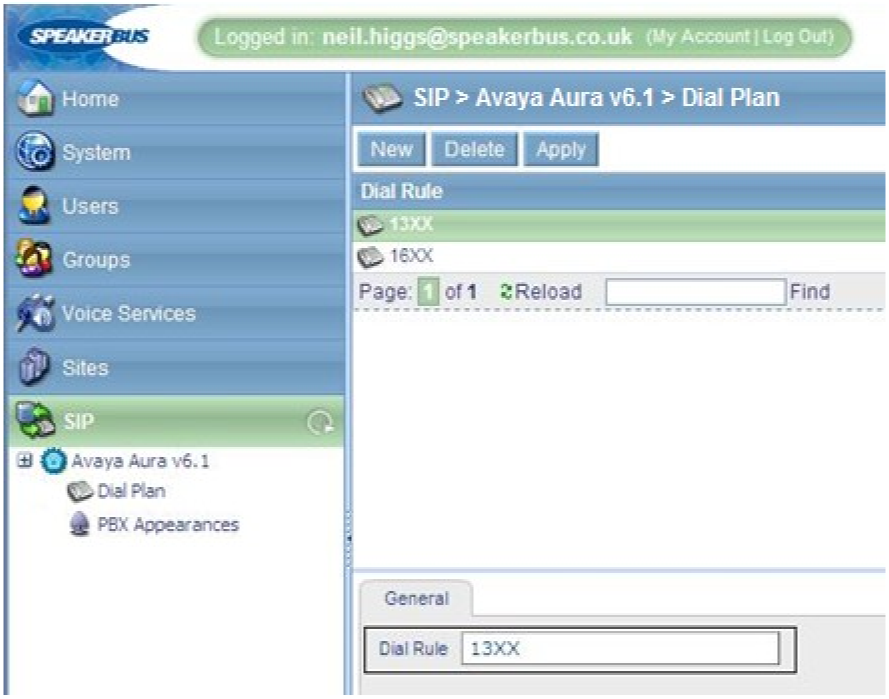
Name: Avaya v6.1
Type: Avaya
Port: 5060

PBX Settings:
Registrar Address: sip.avaya.com
SIP Domain: sip.avaya.com

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

7.7. Create Dial Plan

Under the **SIP** directory, click **Dial Plan** and then the **New** button to add a dial rule. Dial rules specify the valid digit formats that the *i* turret devices are allowed to dial, otherwise the user will have to press OK after entering the dial string on the *i* turret device. In this configuration, 4-digit extensions beginning with **13** were used to dial other *i* turret devices and Avaya telephones. A dial rule is also required for the voice mail pilot number which was a 4-digit extension beginning with **16**. The X's in the dial rule match any digit. Note that the **X** must be a capital letter. Click **OK**.



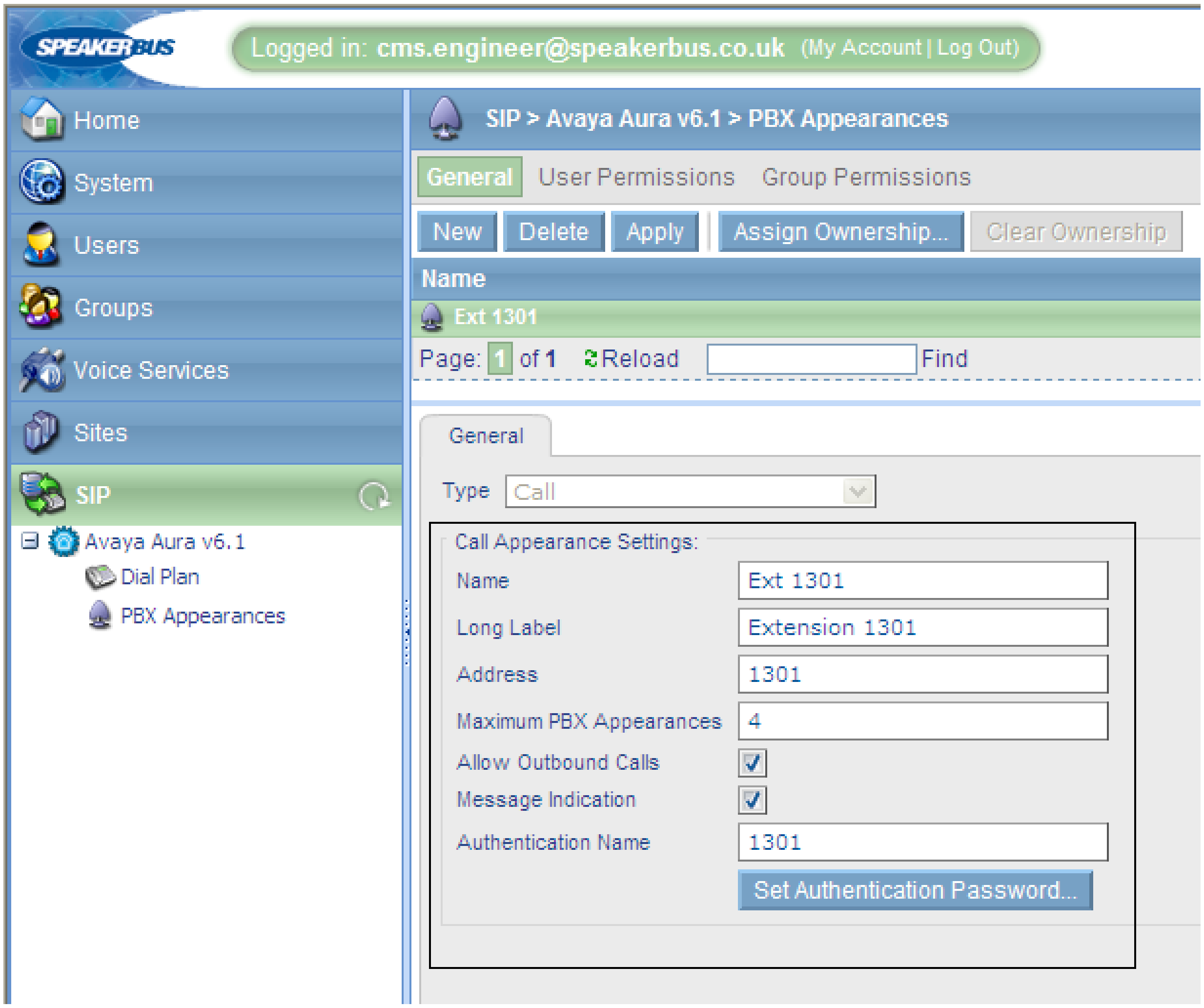
Dial Rule 13XX

Repeat this for all valid extension formats.

7.8. Create Call and Handset Appearances

Three call appearances need to be created for each *i* turret device, 1 for its main appearance, then one each for the privacy handset 1 and privacy handset 2. As previously mentioned, three extensions are also required on Communication Manager and Session manager. To create the main appearance, click **PBX Appearances** under the **Avaya** PBX. Click the **New** button, then select the **Type** of appearance you want to create (Call, Privacy 1 or Privacy 2).

In the **General** tab, provide a descriptive name for the appearance in the **Name** field, such as the extension or user's name. Set the **Long Label** field to the label that will be displayed for the call appearance button on the *i* turret deskstation. The **Address** field should also be set to the appearance extension. .



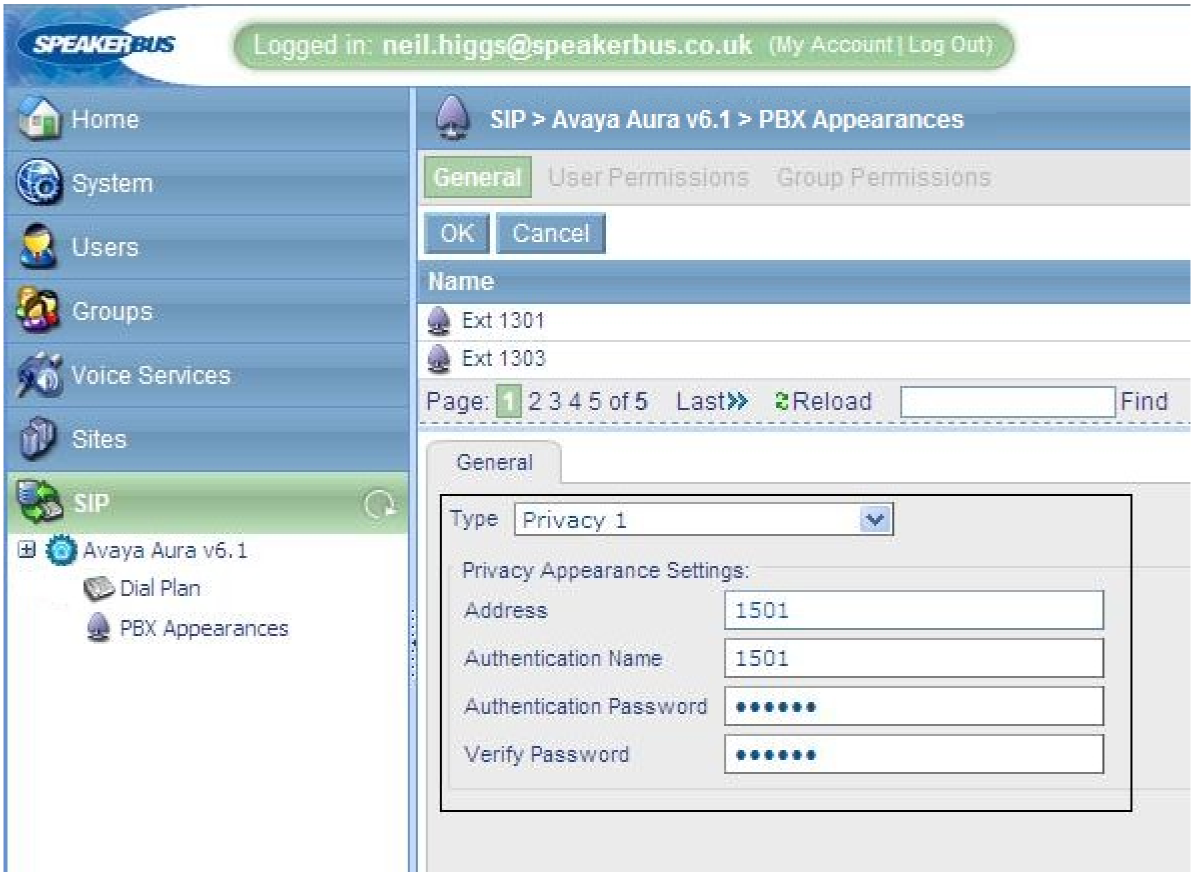
Type: Call

Call Appearance Settings:

Name	Ext 1301
Long Label	Extension 1301
Address	1301
Maximum PBX Appearances	4
Allow Outbound Calls	☑
Message Indication	☑
Authentication Name	1301

Set the **Maximum Appearances** field to the number of call appearances configured on the station in System Manager. See the button assignment section of the station in **Section 6.9.1** for details. The number of call appearance buttons dictates the number of calls on the system the user can have directed to them. When all of a user's call appearances are in-use (not idle) the user is considered busy and no further calls can be routed to them. Up to a maximum of 10 call appearances may be configured on Communication Manager for each *i* turret deskstation. Check the **Message Indication** checkbox for voice mail purposes. Check the **Allow Outbound Calls.** The **Authentication Name** and **Authentication Password** fields should be set to the extension and password, respectively, configured on Session Manager. These are the credentials that the *i* turret deskstation will use to authenticate and register with Session Manager. Use the default values for the other fields as shown below. Click **OK.**

Next, this procedure will be repeated for the two privacy appearances. Click the **New** button to add another appearance. In the **General** tab, set the **Type** field to **Privacy 1**. Then add in the **Address**, **Authentication Name** and **Authentication Password** fields. The later there fields should be identical to that set up in the System manager for registration to occur. Press **OK** to commit the created appearance.



Type: Privacy 1

Privacy Appearance Settings:

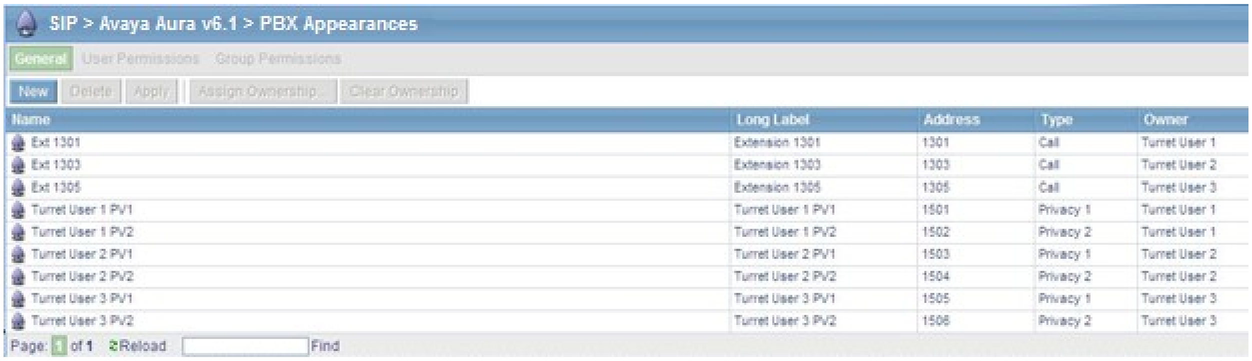
Address: 1501

Authentication Name: 1501

Authentication Password: ••••••

Verify Password: ••••••

Repeat the above procedure to add the Privacy 2 appearance. The call appearances for the previously configured *i* turret deskstations are listed below.

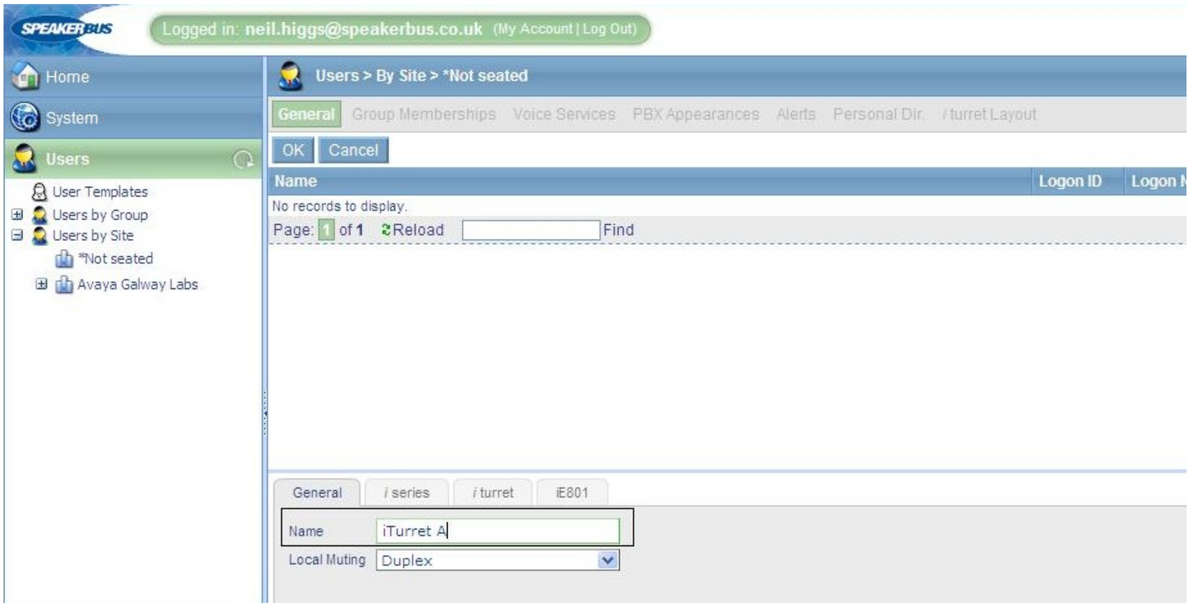

SIP > Avaya Aura v6.1 > PBX Appearances

Name	Long Label	Address	Type	Owner
Ext 1301	Extension 1301	1301	Call	Turret User 1
Ext 1303	Extension 1303	1303	Call	Turret User 2
Ext 1305	Extension 1305	1305	Call	Turret User 3
Turret User 1 PV1	Turret User 1 PV1	1501	Privacy 1	Turret User 1
Turret User 1 PV2	Turret User 1 PV2	1502	Privacy 2	Turret User 1
Turret User 2 PV1	Turret User 2 PV1	1503	Privacy 1	Turret User 2
Turret User 2 PV2	Turret User 2 PV2	1504	Privacy 2	Turret User 2
Turret User 3 PV1	Turret User 3 PV1	1505	Privacy 1	Turret User 3
Turret User 3 PV2	Turret User 3 PV2	1506	Privacy 2	Turret User 3

Repeat the above procedures for adding the Main and Privacy appearances for each *i* turret.

7.9. Create Users

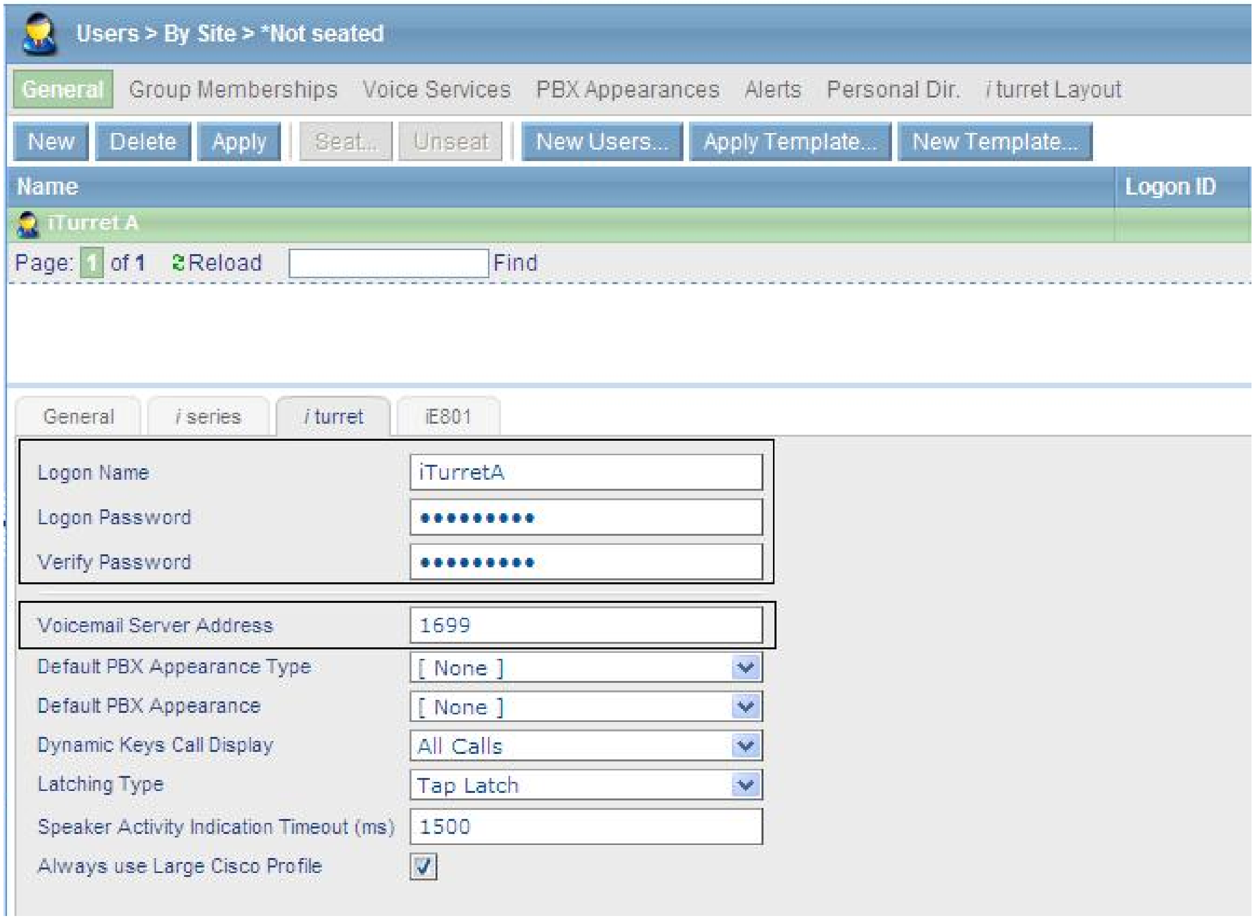
In the left panel click on **Users** and in the directory tree expand **User by Site**, click on **Avaya Galway Labs** followed by **New**. In the **General** tab, provide a descriptive name in the **Name** field. Then press **OK.**



Name: iTurret A

Local Muting: Duplex

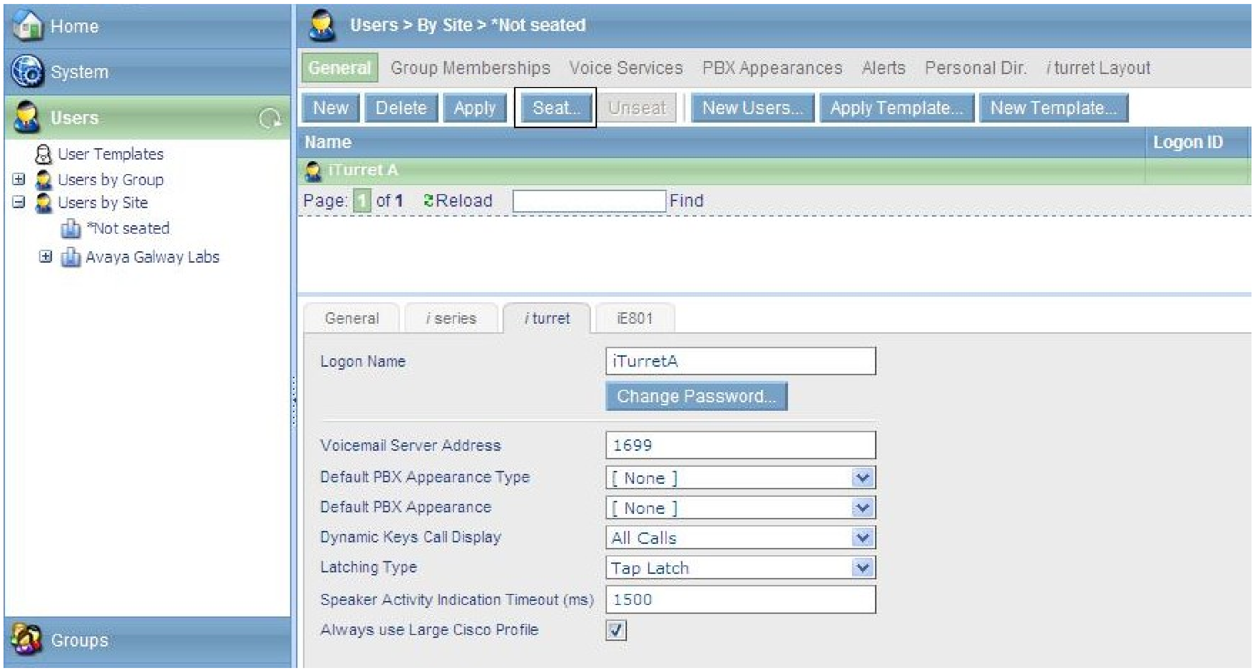
In the *i* turret tab, provide the logon credentials for the user to log into their *i* turret deskstation and enter the pilot number for Voicemail in the **Voicemail Server Address** field. This page will be revisited later in **Section 7.13** to configure the default call appearance for this deskstation. Click **Apply.**



Logon Name	iTurretA
Logon Password	••••••••••
Verify Password	••••••••••
Voicemail Server Address	1699
Default PBX Appearance Type	[None]
Default PBX Appearance	[None]
Dynamic Keys Call Display	All Calls
Latching Type	Tap Latch
Speaker Activity Indication Timeout (ms)	1500
Always use Large Cisco Profile	☑

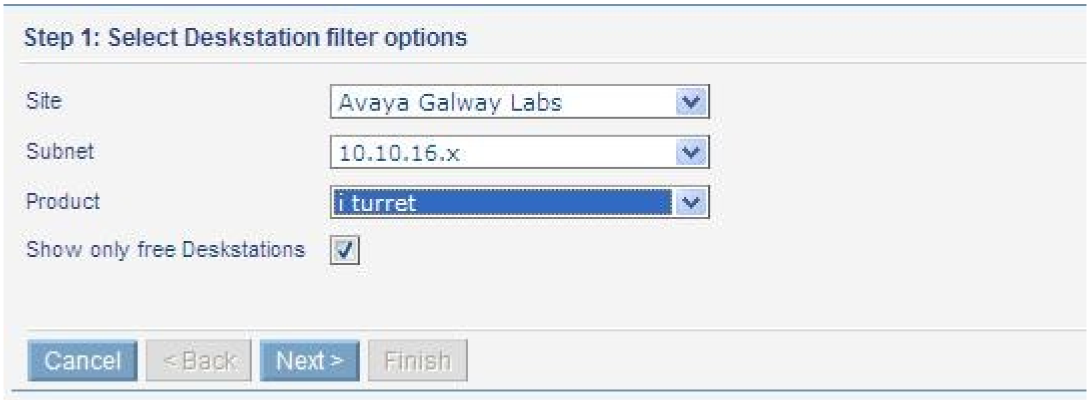
Repeat the previous procedure to add more users.

After a user has been created, the user needs to be **seated** on an *i* turret deskstation. In the left panel under the **Users** directory tree, click the ***Not seated** link under **Users by Site** to display the list of users. Select the user previously configured (i.e., iTurret A) and click on the **Seat…** button.



Logon Name	iTurretA
Voicemail Server Address	1699
Default PBX Appearance Type	[None]
Default PBX Appearance	[None]
Dynamic Keys Call Display	All Calls
Latching Type	Tap Latch
Speaker Activity Indication Timeout (ms)	1500
Always use Large Cisco Profile	☑

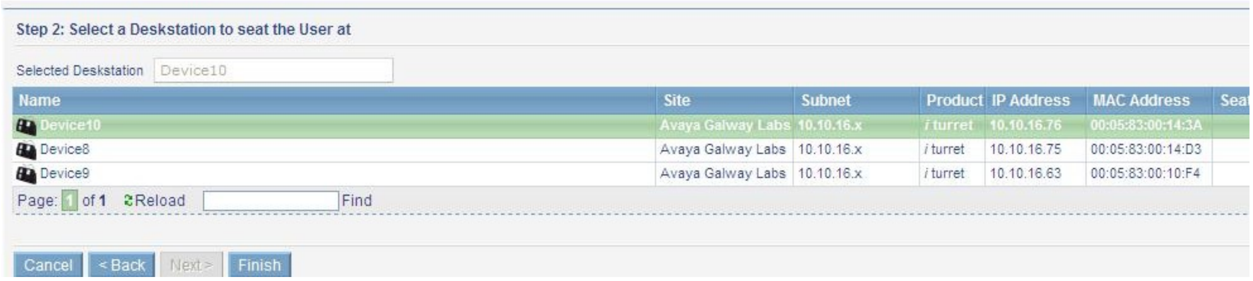
On the next page, filter options are presented. Filter deskstations in the **Avaya Galway Labs** site and in the **10.10.16.x** subnet as shown below. The user will be seated on an *i* turret deskstation with these properties. Click **Next**.



Step 1: Select Deskstation filter options

Site	Avaya Galway Labs
Subnet	10.10.16.x
Product	i turret
Show only free Deskstations	☑

In the resulting deskstation list, select the *i* turret deskstation where the selected user will be seated. In this example, the user will be seated on the **iTurret A** deskstation. Select **iTurret A** in the list and click **Finish**.



Step 2: Select a Deskstation to seat the User at

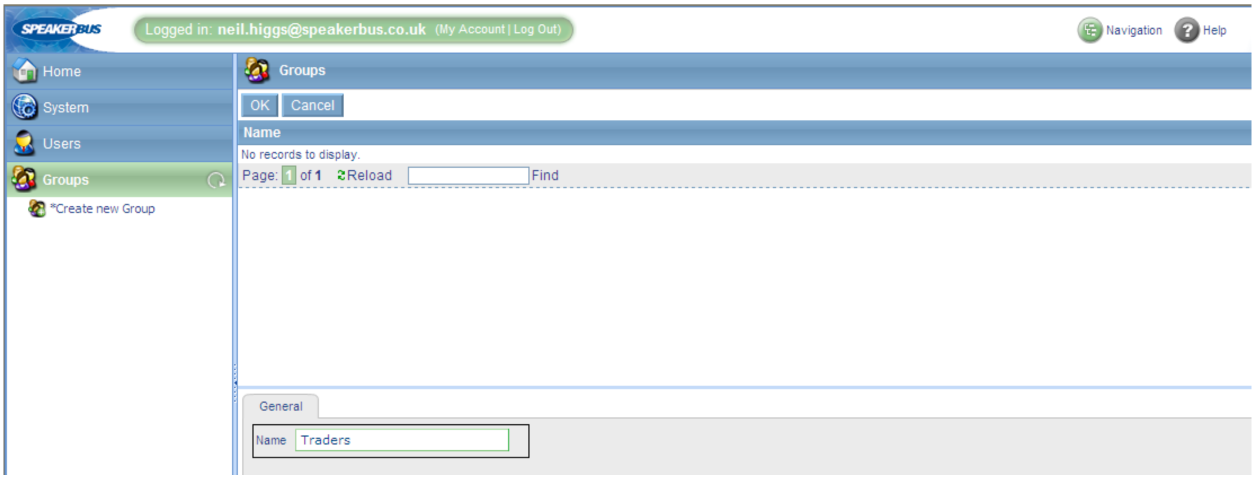
Selected Deskstation: Device10

Name	Site	Subnet	Product	IP Address	MAC Address	Seat
Device10	Avaya Galway Labs	10.10.16.x	*i* turret	10.10.16.76	00:05:83:00:14:3A	
Device8	Avaya Galway Labs	10.10.16.x	*i* turret	10.10.16.75	00:05:83:00:14:D3	
Device9	Avaya Galway Labs	10.10.16.x	*i* turret	10.10.16.63	00:05:83:00:10:F4	

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

7.10. Create Group

To create a group; in the left panel under the **Groups** directory tree click on **Create new Group**. In the **General** tab, provide a descriptive name in the **Name** field, such as **Traders**. Click **OK**. The **Traders** group has been successfully added.



Groups

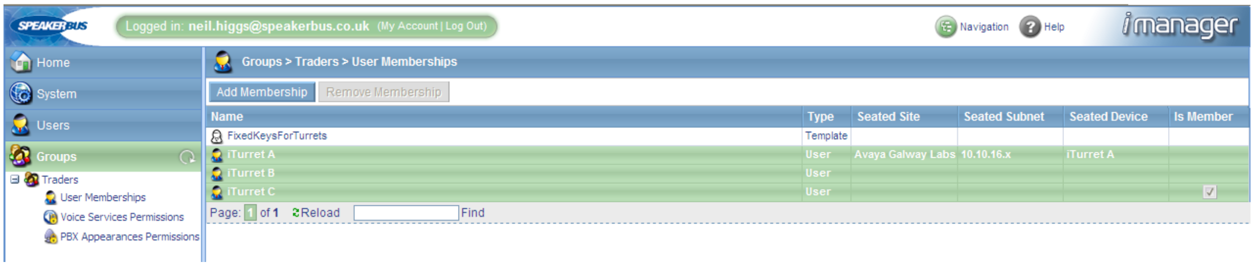
Name
No records to display.

Page: 1 of 1 Reload Find

General

Name: Traders

The user is now added to this new group. In the **Groups** directory tree, expand **Traders** and click on **User Memberships** in the left pane. A list of users is displayed. Select all the users to be added to the Traders group as shown below and then click **Add Membership**. The **Is Member** column will then indicate that the selected users are members of the Traders group (not shown). The **Is Member** column is not shown in the graphic!



Groups > Traders > User Memberships

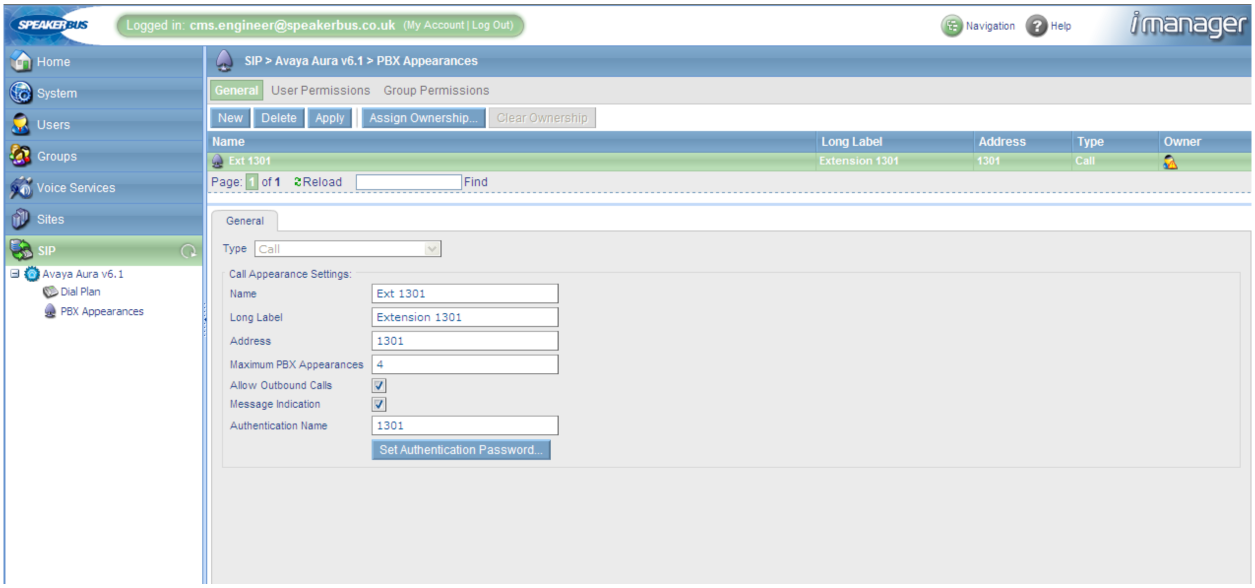
Name	Type	Seated Site	Seated Subnet	Seated Device	Is Member
FixedKeysForTurrets	Template				
iTurret A	User	Avaya Galway Labs	10.10.16.x	iTurret A	
iTurret B	User				
iTurret C	User				☑

Page: 1 of 1 Reload Find

SPEAKERBUS
Logged in: neil.higgs@speakerbus.co.uk (My Account | Log Out)
Navigation
Help
imanager
Home
System
Users
Groups
Traders
User Memberships
Voice Services Permissions
PBX Appearances Permissions
Add Membership
Remove Membership

7.11. Assign User Permissions

The next step will be to assign appearances permissions to users. In the left panel, expand **Avaya** and click on **PBX Appearances**. The list of appearances is displayed. Select the main call appearance for **iTurret A** (i.e., **1310**) and click **User Permissions**.



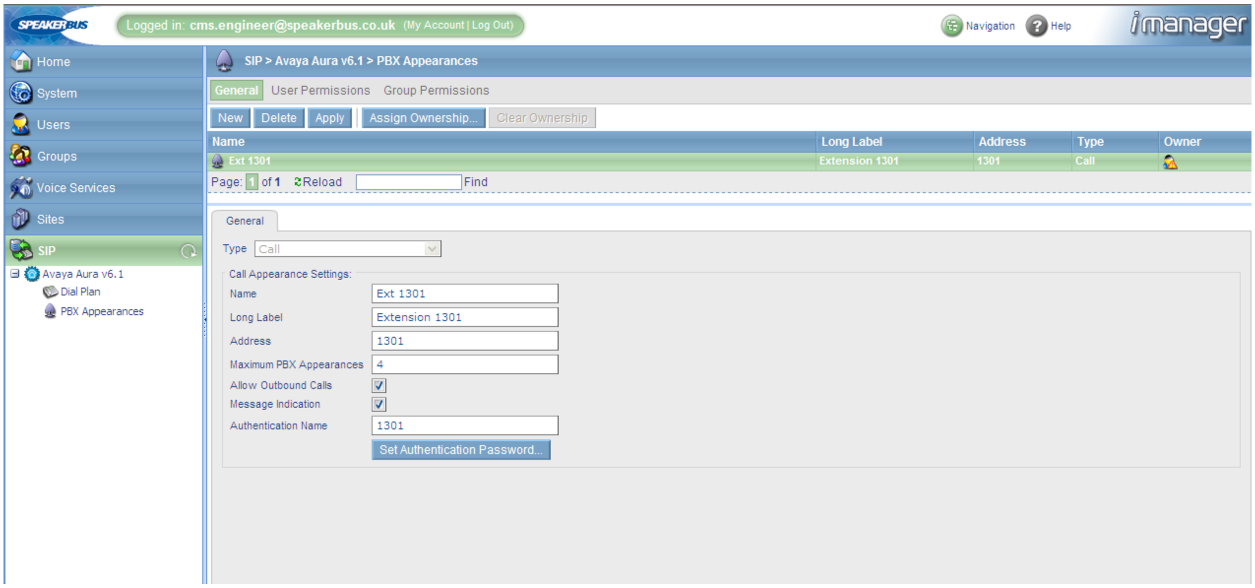
Name	Long Label	Address	Type	Owner
Ext 1301	Extension 1301	1301	Call	

Type: Call

Call Appearance Settings:

Name	Ext 1301
Long Label	Extension 1301
Address	1301
Maximum PBX Appearances	4
Allow Outbound Calls	☑
Message Indication	☑
Authentication Name	1301

On the resulting page select the user to which the appearance will be assigned. Set the **Permission** field to **Allow** as shown below. Click **Apply**. Assign the relevant Privacy 1 and Privacy 2 permissions to this user by repeating this procedure.


Name	Long Label	Address	Type	Owner
Ext 1301	Extension 1301	1301	Call	

Type: Call

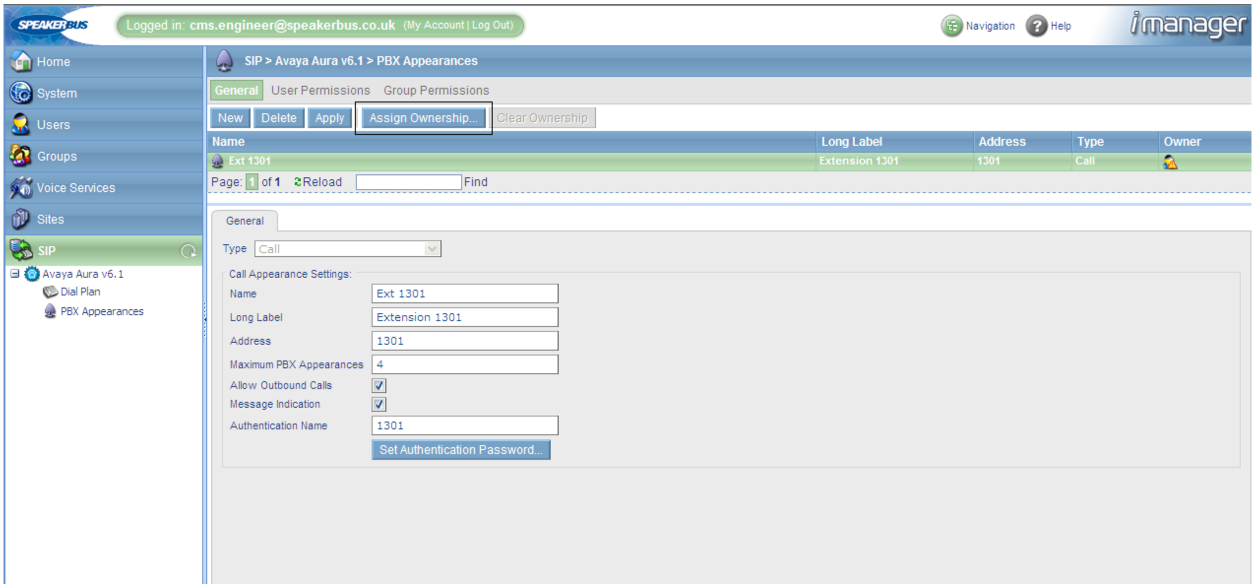
Call Appearance Settings:

Name	Ext 1301
Long Label	Extension 1301
Address	1301
Maximum PBX Appearances	4
Allow Outbound Calls	☑
Message Indication	☑
Authentication Name	1301

If other users require an appearance as a bridged line then those users must also have permissions to the appearance. For the compliance test, user **iTurretB** and **iTurretC** had a bridged line appearance for **iTurretA** (1301), so both users are assigned permissions for appearance 1301 as indicated by the **User Permission** column.

7.12. Assign Ownership

To assign ownership of the appearances to a user, in the left panel, expand **Avaya** and click on **PBX Appearances** to display the appearances list as shown below. In the **General** tab, select the main call appearance and click on the **Assign Ownership…** button.



Name	Long Label	Address	Type	Owner
Ext 1301	Extension 1301	1301	Call	

Type: Call

Call Appearance Settings:

Name: Ext 1301

Long Label: Extension 1301

Address: 1301

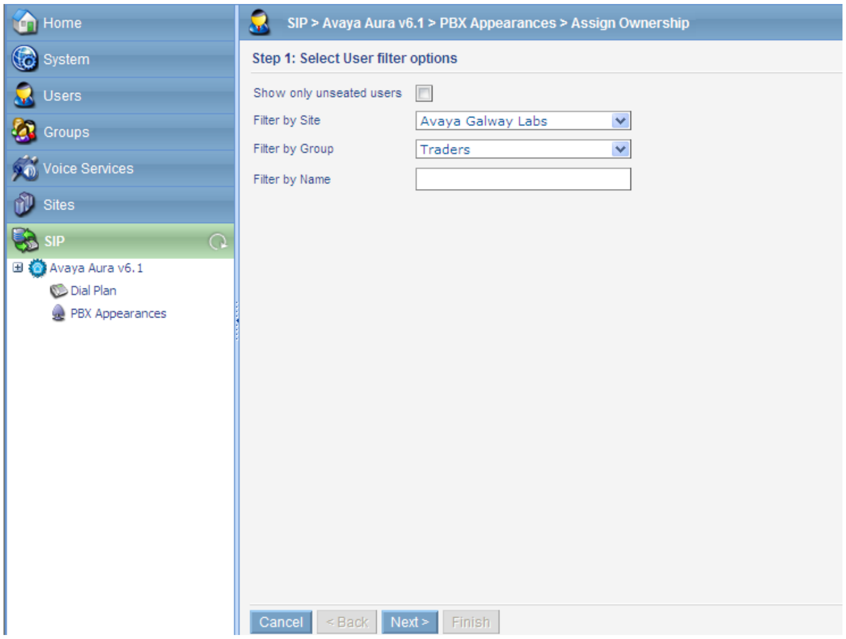
Maximum PBX Appearances: 4

Allow Outbound Calls: ☑

Message Indication: ☑

Authentication Name: 1301

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



SIP > Avaya Aura v6.1 > PBX Appearances > Assign Ownership

Step 1: Select User filter options

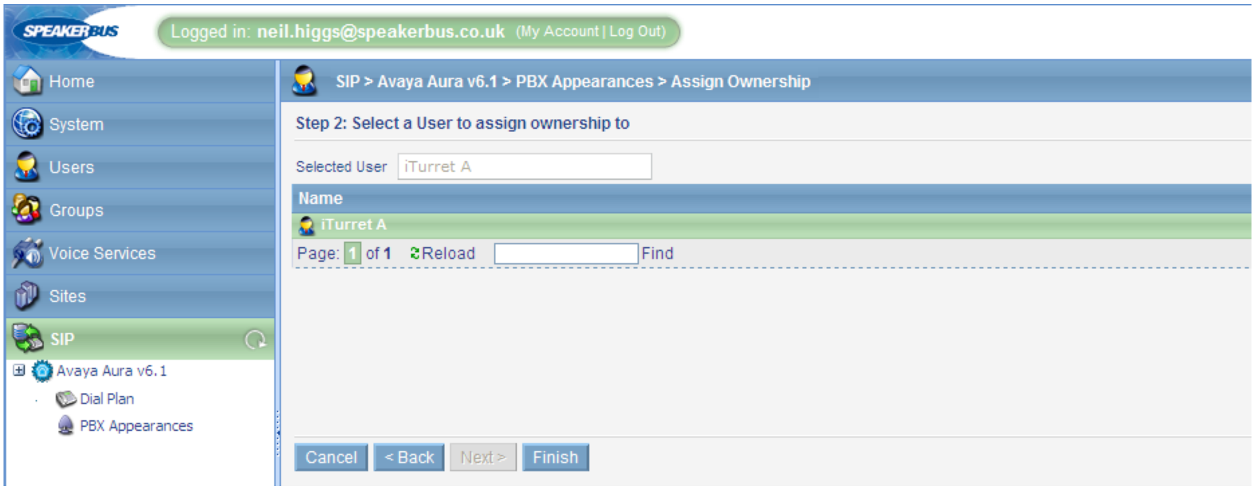
Show only unseated users □

Filter by Site: Avaya Galway Labs

Filter by Group: Traders

Filter by Name:

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



Logged in: neil.higgs@speakerbus.co.uk (My Account | Log Out)

SIP > Avaya Aura v6.1 > PBX Appearances > Assign Ownership

Step 2: Select a User to assign ownership to

Selected User: iTurret A

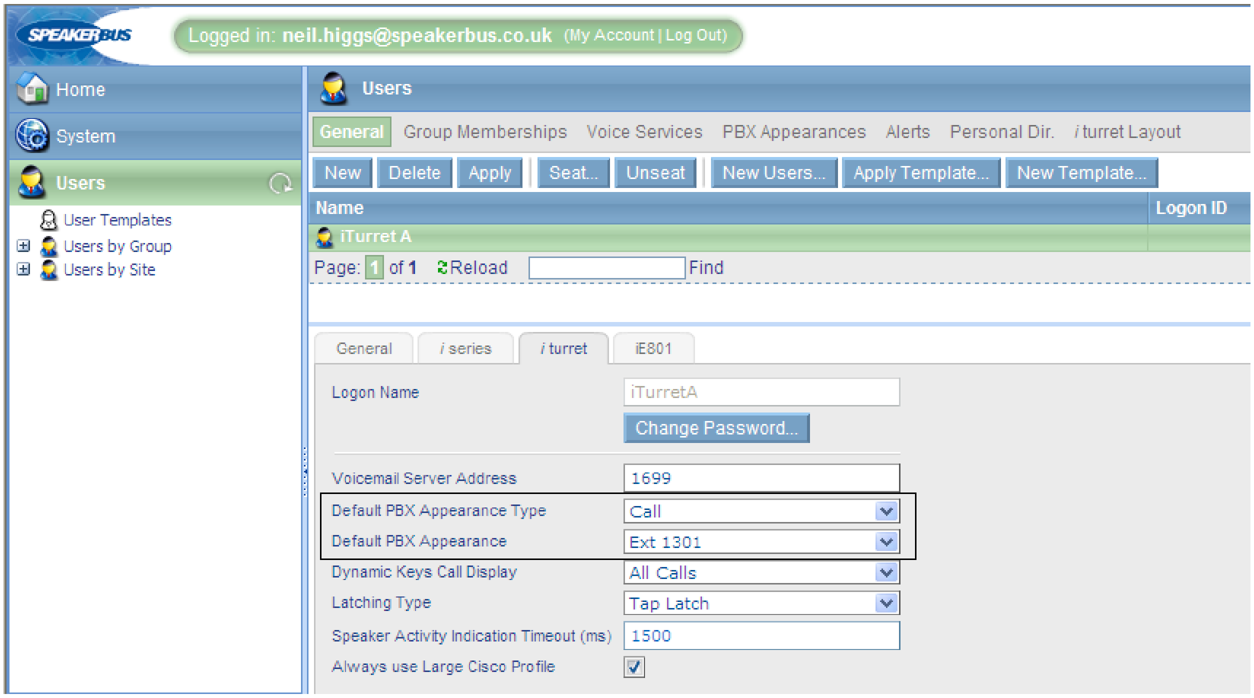
Name
iTurret A

Page: 1 of 1

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

7.13. Assign Default Call Appearance

In the **Users** directory tree, navigate to **Users by Site** → **Avaya Galway Labs** and click **10.10.16.x** link to display the users list. Set the **Default Appearance** field to the main call appearance (e.g., **1301**). Click **Apply**.



Logon Name: iTurretA

Voicemail Server Address: 1699

Default PBX Appearance Type: Call

Default PBX Appearance: Ext 1301

Dynamic Keys Call Display: All Calls

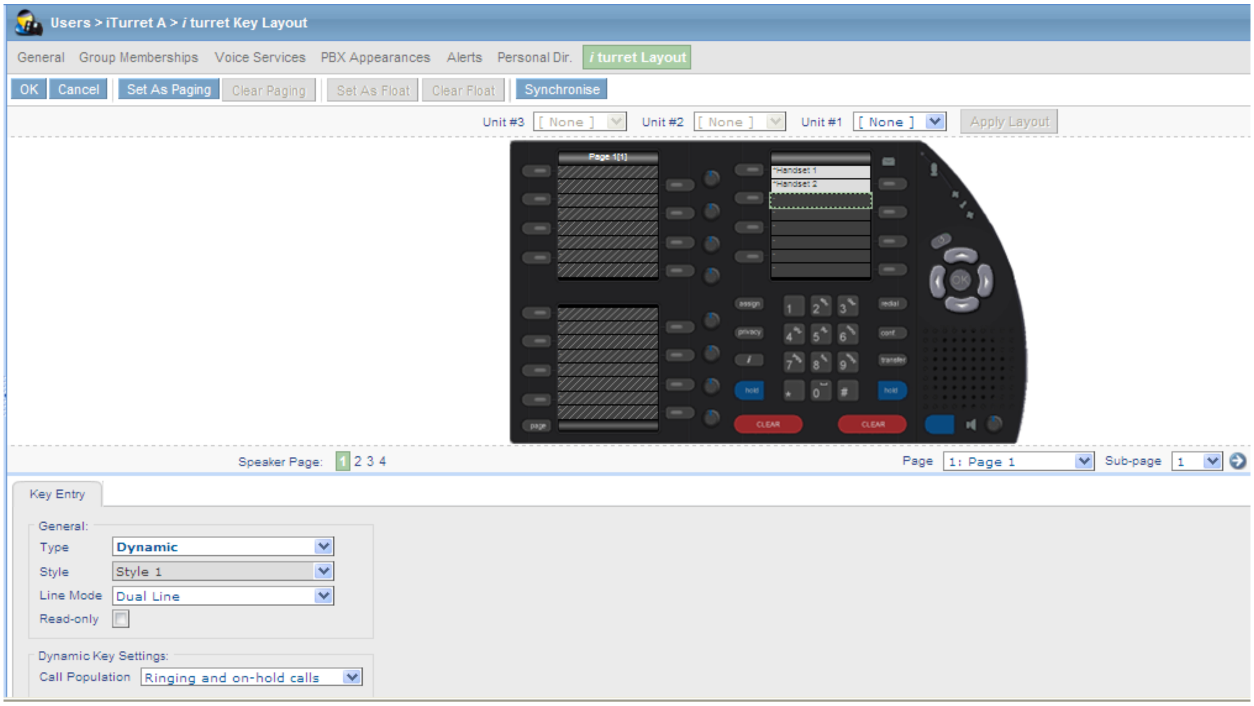
Latching Type: Tap Latch

Speaker Activity Indication Timeout (ms): 1500

Always use Large Cisco Profile: ☑

7.14. Programming *i turret* Desktations

This section describes how to create *i* turret deskstation keys. The following keys can be created using the *i* turret **layout** page: Dynamic, Appearance, Shortcut, Soft Function, and Speed Dial amongst others. In this configuration, each user will be configured with three Dynamic keys, two Soft Function keys, and one Shortcut key. Although the configuration may vary, this configuration is suitable for most users. In left panel under the **Users** directory tree, expand **Users by Site → Avaya Galway Labs** and click on **10.10.16.x** link to display a list of users. Select a user (e.g., **iTurret A**) and click *i* turret **Layout** to display the ***i*** turret key layout for this user. In the iTurret key layout, click on the key highlighted below Handset 2. In the Key Entry tab, set the **Type** field to **Dynamic**. Click **OK**.



Unit #3 [None] Unit #2 [None] Unit #1 [None]

Page 1: Page 1 Sub-page 1

General:

Type: Dynamic

Style: Style 1

Line Mode: Dual Line

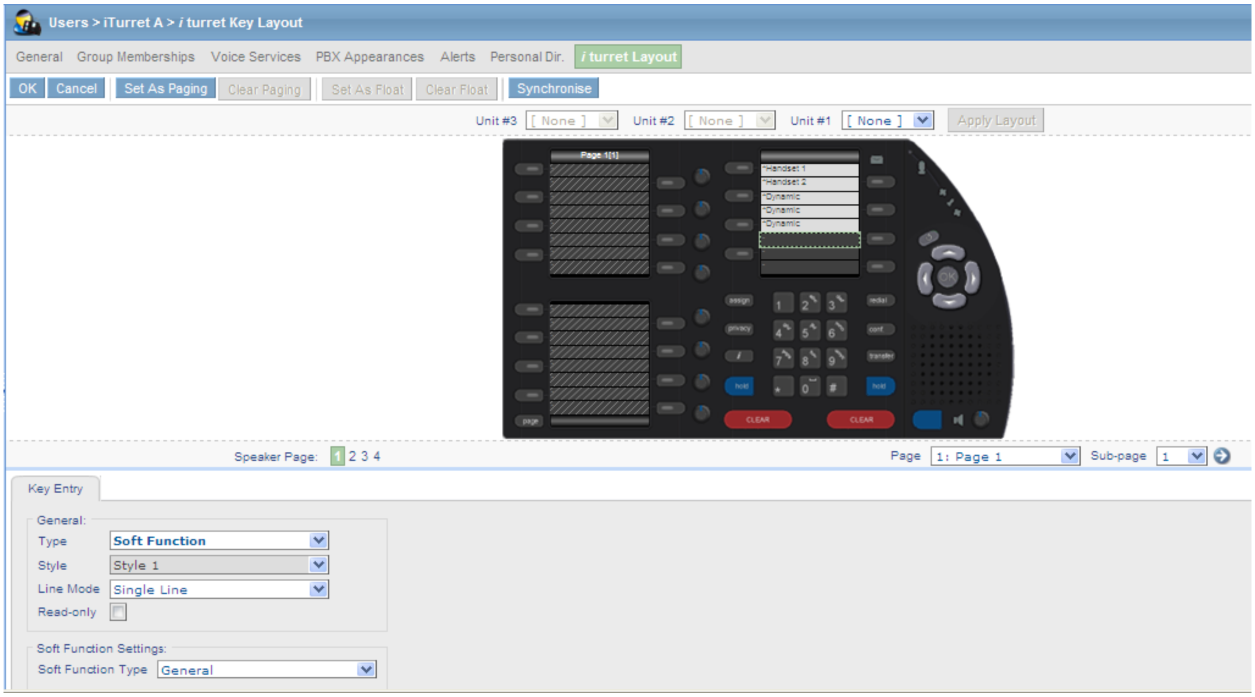
Read-only: ☐

Dynamic Key Settings:

Call Population: Ringing and on-hold calls

Three Dynamic keys will be added so repeat this step for the next two keys.

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



General:

Type: Soft Function

Style: Style 1

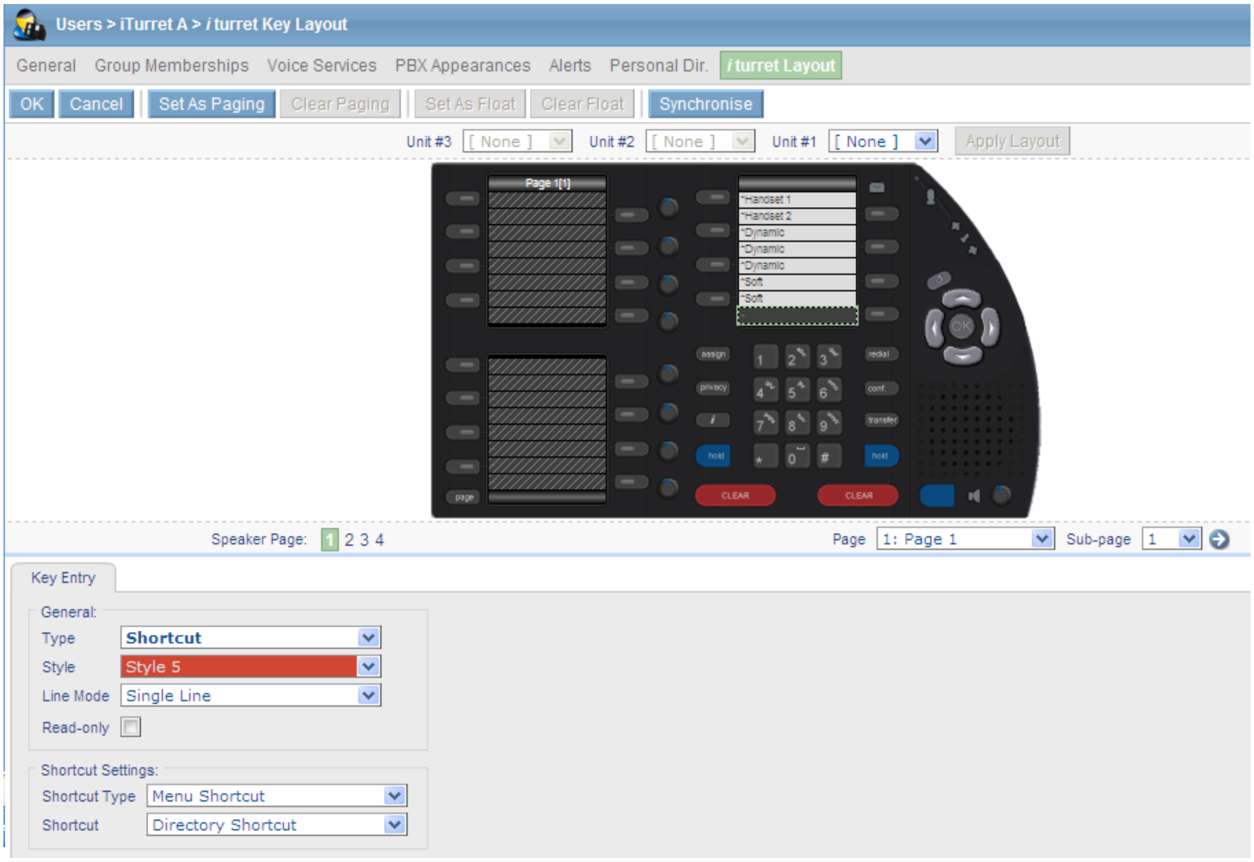
Line Mode: Single Line

Read-only: □

Soft Function Settings:

Soft Function Type: General

Finally, add a Shortcut key under the last Soft Function key. In the **Key Entry** tab, set the **Type** field to **Shortcut**. Set the **Shortcut type** field to **Menu Shortcut**. Set the **Shortcut** field to **Directory Shortcut**. Click **OK**.



Unit #3 [None] Unit #2 [None] Unit #1 [None]

Page 1: Page 1 Sub-page 1

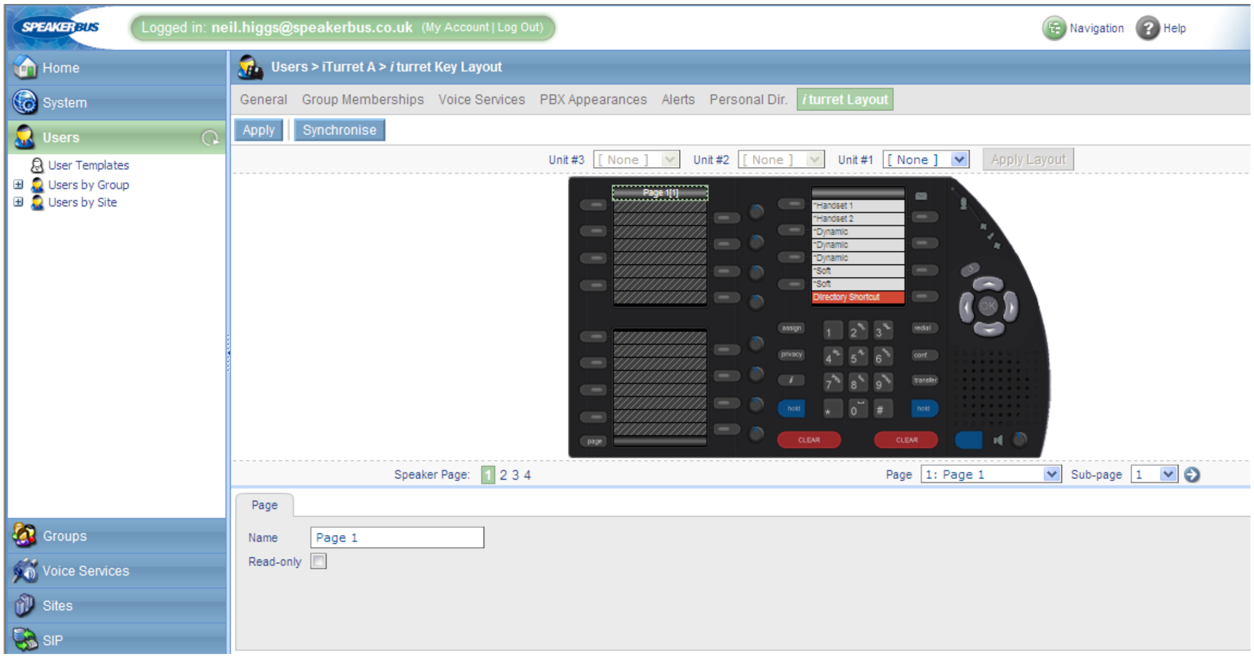
General:

Type	Shortcut
Style	Style 5
Line Mode	Single Line
Read-only	□

Shortcut Settings:

Shortcut Type	Menu Shortcut
Shortcut	Directory Shortcut

After all of the iD808 keys have been created on the deskstation, the ***i* turret layout** will appear as shown below.



Unit #3 [None] Unit #2 [None] Unit #1 [None]

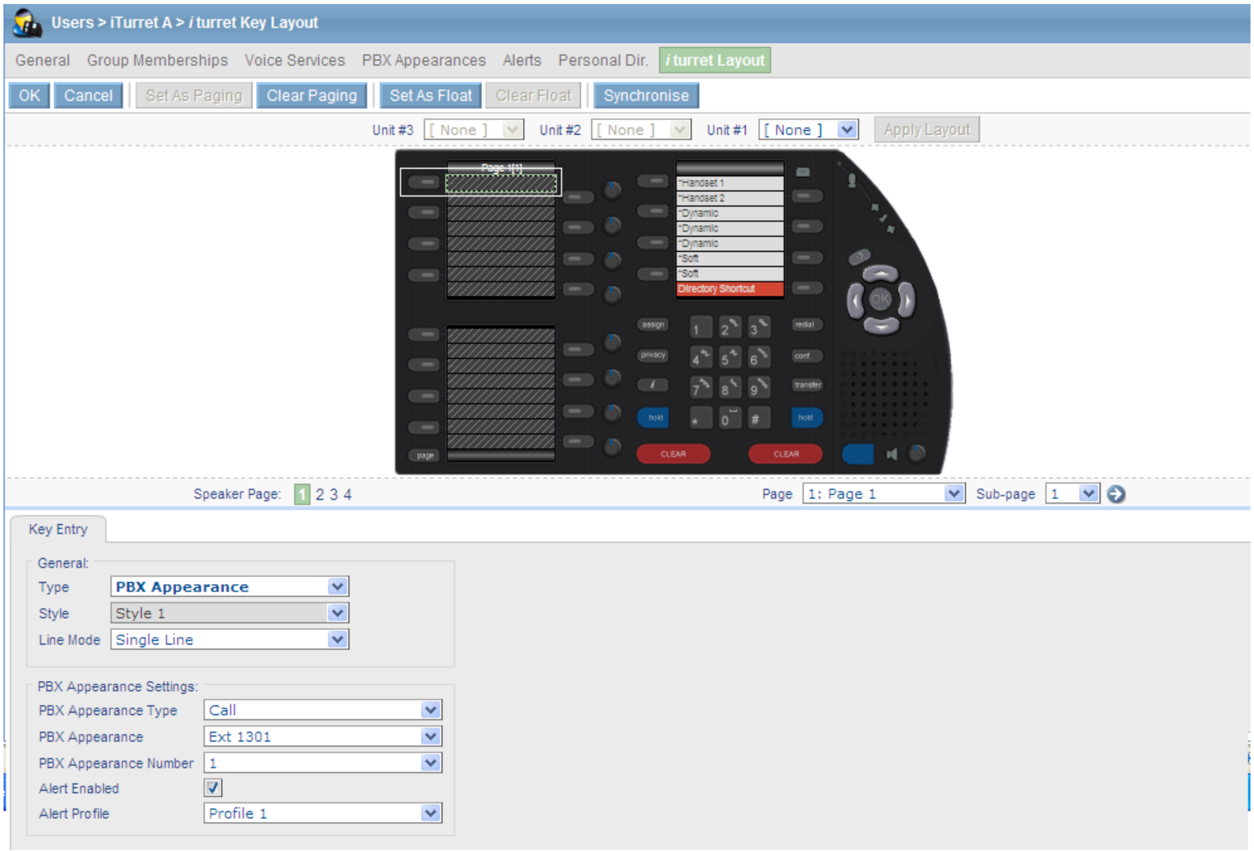
Page 1: Page 1 Sub-page 1

Name Page 1

Read-only □

7.15. Assigning Appearances to Deskstation Keys

In the *i* turret key layout page, go to **Page 1** of the deskstation by setting the **Page** field to **1** in the **Page** tab and clicking the arrow key to the right. Select the next available key as highlighted by the white box below. The next three keys on this page will be assigned to call appearances. In the **Key Entry** tab, set the **Type** field to **PBX Appearance**. Under the **PBX Appearance Settings**, select the **PBX Appearance Type** (Call in this case), **PBX Appearance** (Ext 1301 in this case), **PBX Appearance Number** (1 in this case) and check **Alert Enabled** and leave Profile 1 as default for **Alert Profile**. Click **OK**. Repeat this procedure to add the next two call appearances.



Unit #3 [None] Unit #2 [None] Unit #1 [None]

Speaker Page: 1 2 3 4

Page 1: Page 1 Sub-page 1

General:

Type: PBX Appearance

Style: Style 1

Line Mode: Single Line

PBX Appearance Settings:

PBX Appearance Type: Call

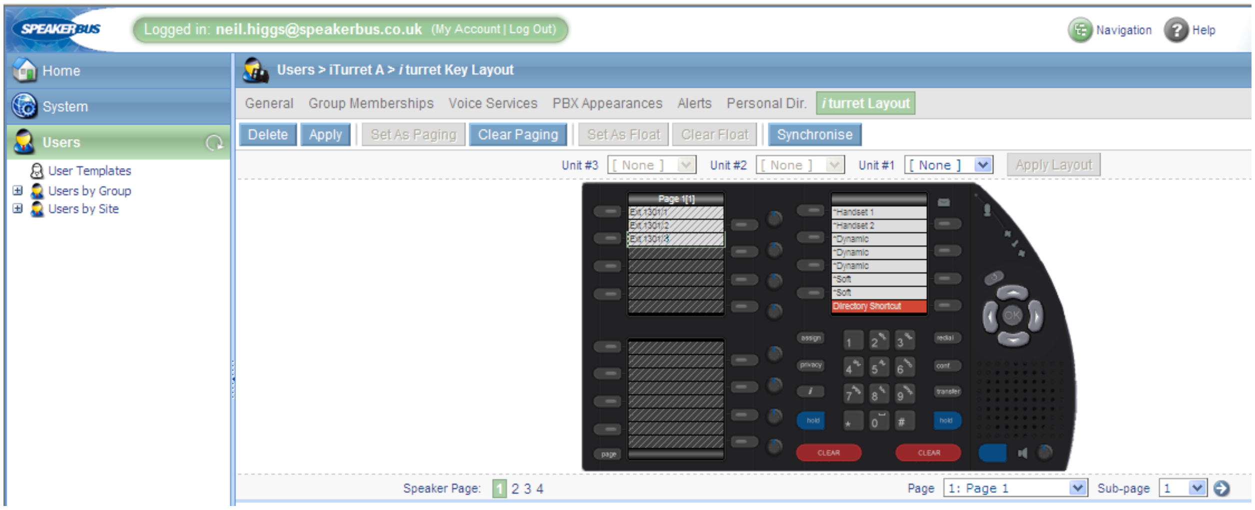
PBX Appearance: Ext 1301

PBX Appearance Number: 1

Alert Enabled: ☑

Alert Profile: Profile 1

Once the three call appearances have been added, the *i* turret layout will appear as follows.



Unit #3 [None] Unit #2 [None] Unit #1 [None]

Ext 1301/1
Ext 1301/2
Ext 1301/3

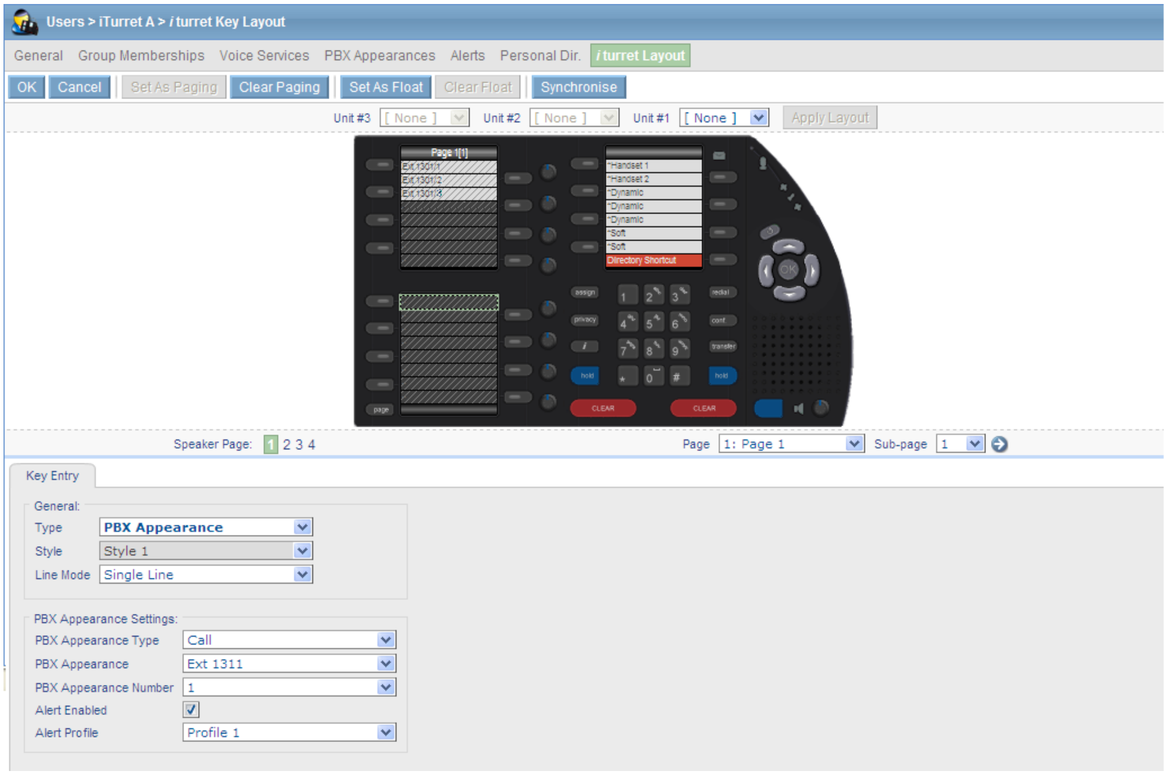
*Handset 1
*Handset 2
*Dynamic
*Dynamic
*Dynamic
*Soft
*Soft
Directory Shortcut

Page 1: Page 1 Sub-page 1

7.16. Assign a Bridge Call Appearance to Deskstation

In the *i* turret key layout page, go to **Page 1** of the deskstation by setting the **Page** field to **1** in the **Page** tab and clicking the arrow key to the right. Select the next available key in the lower section of page one. The next three keys on this page will be assigned to bridge call appearances. In the **Key Entry** tab, set the **Type** field to **PBX Appearance**. Under the **PBX Appearance Settings**, select the **PBX Appearance Type** (Call in this case), **PBX Appearance** (Ext 1311 in this case), **PBX Appearance Number** (1 in this case) and check **Alert Enabled** and leave Profile 1 as default for **Alert Profile**. Click **OK**.

Repeat this procedure to add the next two bridge call appearances.



Unit #3 [None] Unit #2 [None] Unit #1 [None]

Speaker Page: 1 2 3 4

Page 1: Page 1 Sub-page 1

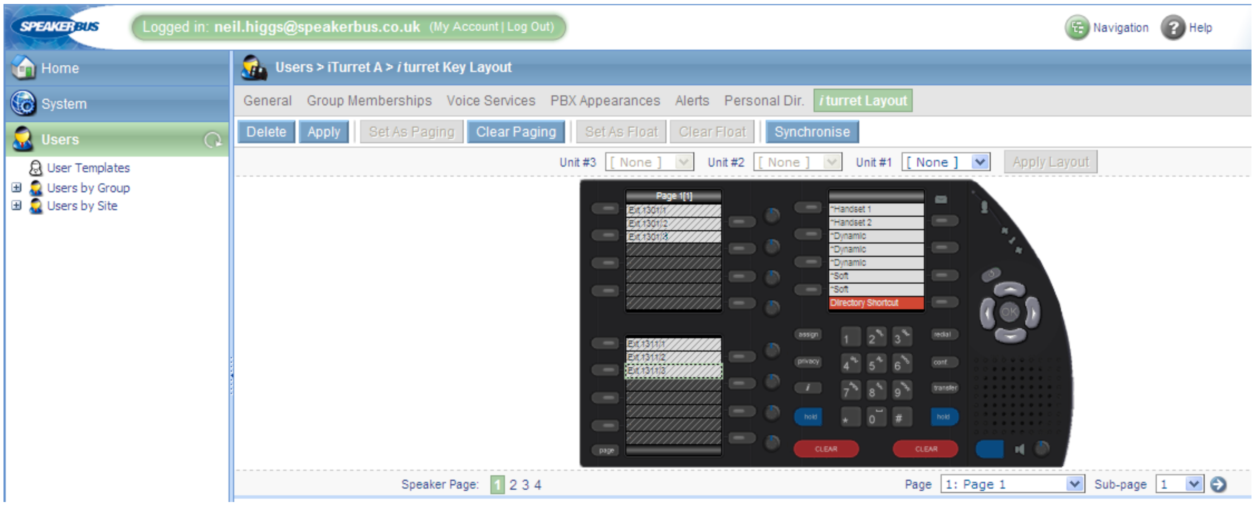
General:

Type	PBX Appearance
Style	Style 1
Line Mode	Single Line

PBX Appearance Settings:

PBX Appearance Type	Call
PBX Appearance	Ext 1311
PBX Appearance Number	1
Alert Enabled	☑
Alert Profile	Profile 1

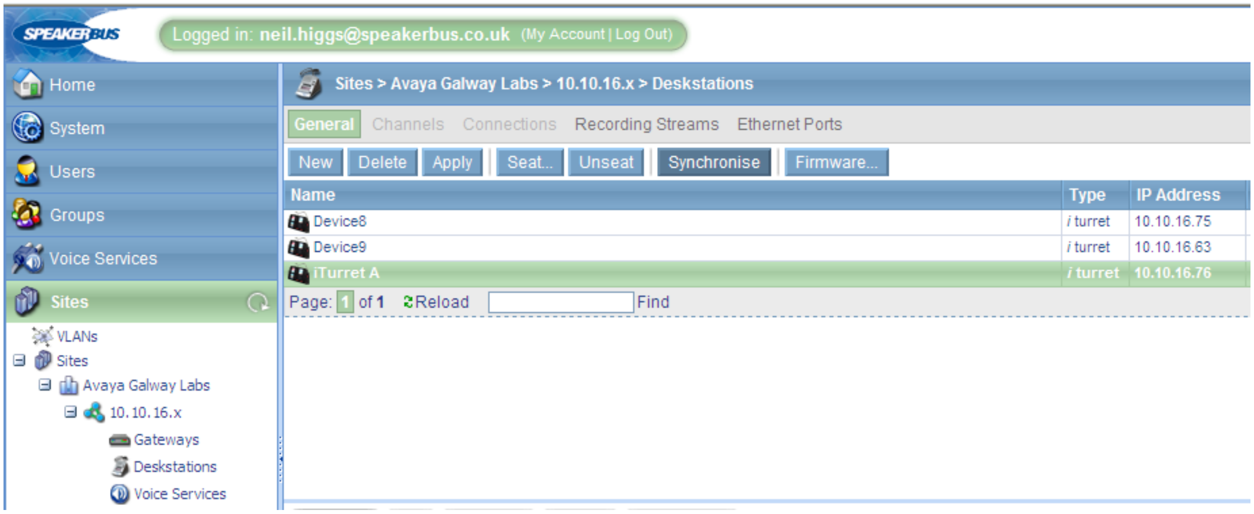
Once the three bridge call appearances have been added, the *i* turret layout will appear as follows.



7.17. Synchronise Deskstations

With Live updates enabled, see **Section 7.4** to confirm you have enabled this as default. Any changes you make to the profile within icms will be updated on the device after **OK** or **Apply** is pressed (any changes to site and subnet details will need a synchronization)
To synchronise a Turret device, under the **Sites** directory tree, expand **Avaya Galway Labs → 10.10.16.x** and click on **Deskstations** to display the deskstation list. Select the desired deskstations and click the **Synchronise** button. The *i* turret deskstation 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, *i* cms, and SIP registrar status should be green.

Note: Executing a synchronisation will cause active calls on the deskstation being synchronised to drop.



Name	Type	IP Address
Device8	*i* turret	10.10.16.75
Device9	*i* turret	10.10.16.63
iTurret A	*i* turret	10.10.16.76

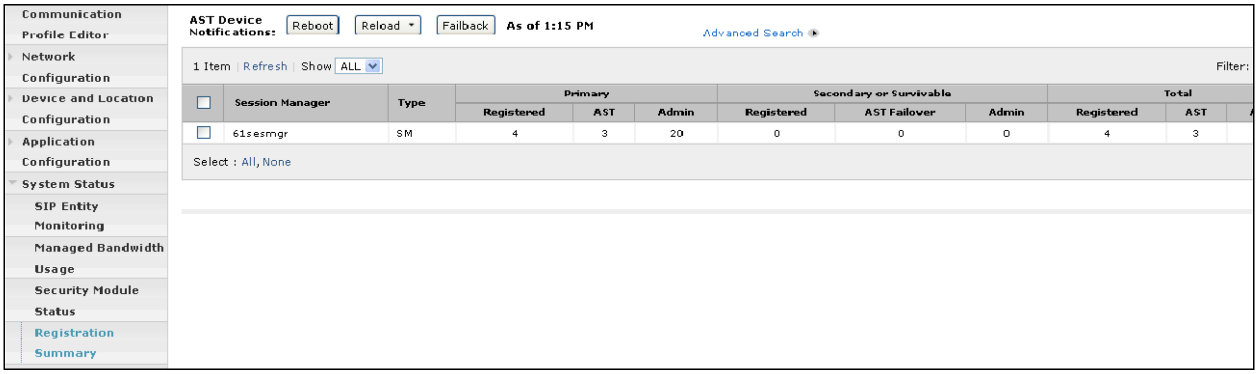
7.18. Feature Name Extensions (FNEs)

FNEs can be accessed by dialing the appropriate number via the dial pad. It is also possible to create FNEs as speed dials by defining the FNE in the corporate or personal directory within *iCMS*. Please refer **[5]** to Speakerbus documentation for further details.

8. Verification Steps

All features shown in **Table 1** were tested using the sample configuration. The following steps can be used to verify and/or troubleshoot installations in the field.

1. On the Speakerbus iD808 *i* turret, verify that the status icons are green. These status icons indicate whether *i* turret is connected to the network, *i* cms server, and SIP registrar (i.e., Avaya Aura® Session Manager). Refer to [5] for more details.
2. Verify that the iD808 deskstations have successfully registered with Session Manager, from the Dashoard select Session manager from the Elements section and choose **System Status** → **Registration Summary** this will display a summary of registered user's on Session Manager as shown below.



□	Session Manager	Type	Primary			Secondary or Survivable			Total	
			Registered	AST	Admin	Registered	AST Failover	Admin	Registered	AST
□	61sesmgr	SM	4	3	20	0	0	0	4	3

3. Verify basic feature set administration by making calls from one *i* turret to another *i* turret and phones. Test supported features according to **Table 1** and feature deployment plans at the site.
4. Verify extended OPS features by dialing the Feature Name Extensions and listening for the confirmation tones.
5. Call an *i* turret that currently has no voice messages, and leave a message. Verify that the message waiting indicator illuminates on the called *i* turret. Call the voice messaging system from *i* turret and use the voice messaging menus to retrieve and delete the voice message, verifying that DTMF is interpreted correctly by the system, and that the message waiting indicator extinguishes.

9. Conclusion

These Application Notes have described the administration steps required to use Speakerbus iD808 *i* turret with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Both basic and extended feature sets were covered as shown in **Table 1**.

10. References

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

[1] *Administering Avaya Aura® Communication Manager*, 9th august 2010, Document Number 03-300509.

[2] *Avaya Extension to Cellular User Guide Avaya Aura® Communication Manager*, Nov 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® Session Manager*, 5th January 2011, Document Number 03-603473.

[5] *Speakerbus i manager 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.