



DevConnect Program

Application Notes for Speakerbus ARIA iDUCX virtual deskstation with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the steps required to connect Speakerbus ARIA iDUCX virtual deskstation v4.1 to Avaya Aura® Session Manager R10.1 and Avaya Aura® Communication Manager R10.1 as a SIP user. Avaya Aura® Communication Manager features can be made available in addition to the standard features supported on the Speakerbus ARIA iDUCX virtual deskstation.

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

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

1. Introduction

These Application Notes describe the steps required to connect Speakerbus ARIA iDUCX virtual deskstation v4.1 to Avaya Aura® Session Manager R10.1 and Avaya Aura® Communication Manager R10.1 as a SIP user. Also described, is how Avaya Aura® Communication Manager features can be made available in addition to the standard features supported by Speakerbus ARIA iDUCX virtual deskstation. In this configuration, the Off-PBX Stations (OPS) feature set is extended from Avaya Aura® Communication Manager to the Speakerbus iDUCX virtual deskstation, providing the softphone with enhanced calling features.

The table below provides a summary of the supported features available on Speakerbus ARIA iDUCX virtual deskstation with the Avaya SIP offer. Some features are supported locally in Speakerbus ARIA iDUCX virtual deskstation, while others are only available with Communication Manager and 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 [5]. 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 Speakerbus ARIA iDUCX virtual deskstation using OPS.

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

FEATURE	SUPPORTED		COMMENTS
	Locally at the phone	With Avaya SIP Offer	
Basic Calling Features			
Extension to Extension Call	Yes	Yes	
Basic Call to legacy phones	No	Yes	
Speed Dial Buttons	Yes	Yes	
Message Waiting Support	Yes	Yes	

FEATURE	SUPPORTED		COMMENTS
	Locally at the phone	With Avaya SIP Offer	
SIPPING-19 Features			
Call Hold	Yes	Yes	
Consultation Hold	Yes	Yes	
Unattended Transfer	Yes	Yes	
Attended Transfer	Yes	Yes	
Call Forward All	Yes	Yes	Local menu option on ARIA iDUCX and FNU
Call Forward Busy/No answer	Yes	Yes	Local menu option on ARIA iDUCX and FNU
Call Forward Cancel	Yes	Yes	Local menu option on ARIA iDUCX and FNU
Find me	No	Yes	Via OPS Coverage Paths
Incoming call screening	No	Yes	Via OPS Class Of Restriction
Outgoing call screening	No	Yes	Via OPS Class Of Restriction
Call Park/Unpark	No	Yes	Via OPS FNE
Call Pickup	No	Yes	Via OPS FNE
Automatic Redial	No	Yes	Via OPS FNE
OPS – Selected Additional Station-Side Features			
Conference on answer	No	Yes	Via OPS FNE
Directed call pickup	No	Yes	Via OPS FNE
Drop last added party	No	Yes	Via OPS FNE
Exclusion/Privacy	Yes	Yes	Local hard key on ARIA iDUCX using FNU
Last number dialed	Yes	Yes	Via OPS FNE
Priority Call	No	Yes	Via OPS FNE, ARIA iDUCX doesn't support distinctive ring indication
Send All Calls	No	Yes	Via OPS FNE
Send All Calls Cancel	No	Yes	Via OPS FNE
Transfer to Voicemail	No	Yes	Via OPS FNE
Whisper Page	No	Yes	Via OPS FNE

Table 1

2. General Test Approach and Test Results

To verify interoperability of the Speakerbus ARIA iDUCX virtual deskstation with Communication Manager and Session Manager, calls were made between Speakerbus ARIA iDUCX virtual deskstation softphones and Avaya SIP, H.323 and Digital stations exercising common PBX features. The telephony features were activated and deactivated using buttons and menu options on Speakerbus ARIA iDUCX virtual deskstation, FNEs, and FNUs.

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

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/Smartphones that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/Smartphones for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Speakerbus ARIA iDUCX virtual deskstation did not include use of any specific encryption features as requested by Speakerbus.

Note: Compliance testing was carried out using both UDP and TCP as the transport for SIP signaling.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Registration of Speakerbus ARIA iDUCX virtual deskstation with Session Manager.
- Calls between Speakerbus ARIA iDUCX virtual deskstation and Avaya SIP, H.323, and digital stations with correct calling/called name presentation.
- Codec Support and Direct IP-IP Media (shuffling).
- Hold/Retrieve operations.
- Supervised and blind transfers.
- Conference.
- Bridged appearances.
- Barge in and Privacy.
- Voicemail and message waiting indicators (MWI).
- Extended telephony features using Communication Manager Feature Name Extensions (FNEs) shown in bold in **Table 1**.
- Call forwarding (busy and no-answer) and Send All Calls using Call Forwarding and Send All Call FNU's.
- Serviceability testing after a Speakerbus ARIA iDUCX virtual deskstation restart and loss of IP connection.

2.2. Test Results

All the test cases passed successfully.

2.3. Support

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

- Web: <http://www.speakerbus.com>
- Email: support@speakerbus.com
- Telephone: +1 (646) 289-4700 in North America
+44 (0) 870 240 7252 in Europe
+65 6590 9228 in Asia

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Manager, Session Manager along with a Media Gateway and a Media Server. System Manager was used to provision Communication Manager and Session Manager. Speakerbus ARIA iDUCX virtual deskstations were connected to the LAN and connect to Session Manager via the Speakerbus ICB server. SIP, Digital and H.323 telephones were used to place calls to and receive calls from the Speakerbus ARIA iDUCX virtual deskstation. Avaya Messaging was used to provide and test voicemail and message waiting facilities.

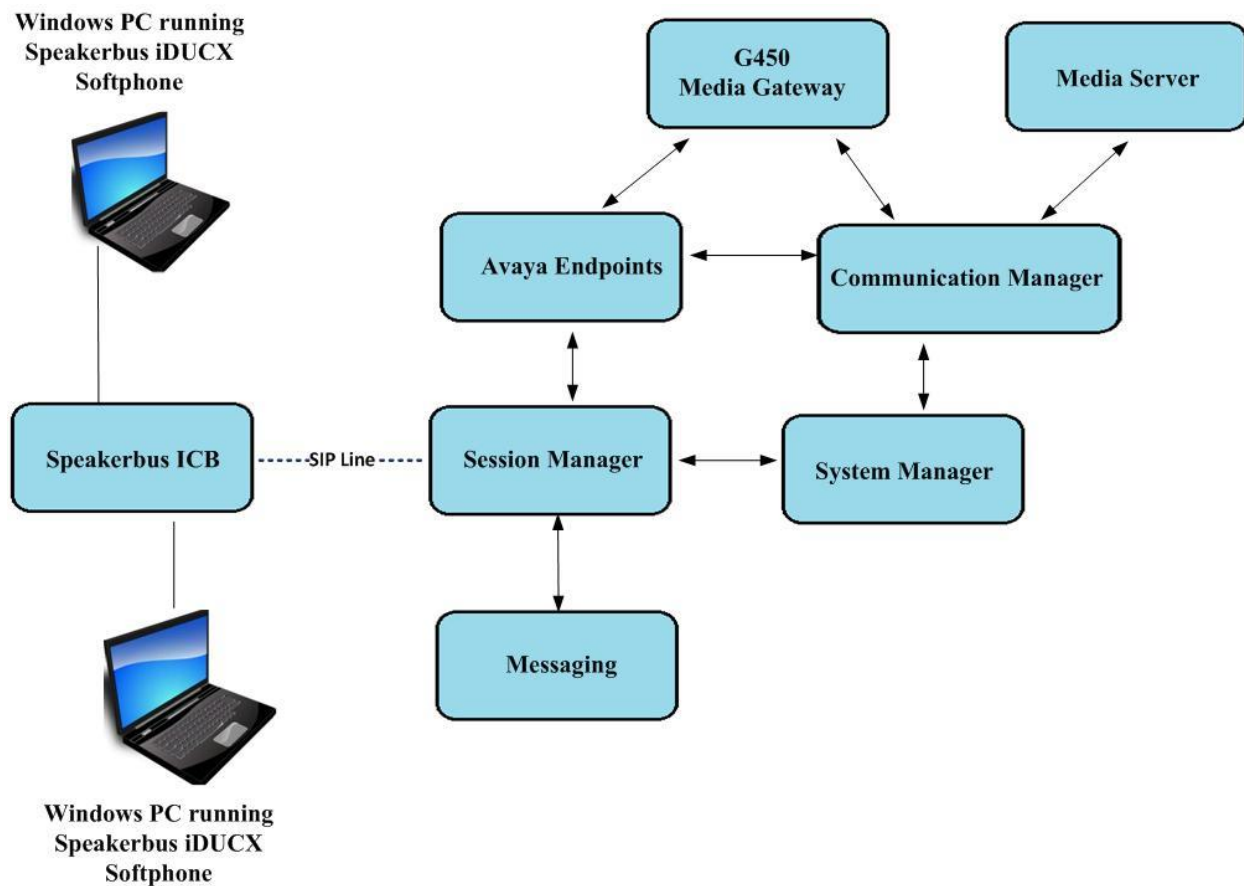


Figure 1: Avaya Aura® Communication Manager and Avaya Aura® Session Manager with the Speakerbus solution

4. Equipment and Software Validated

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

Avaya Equipment/Software	Release/Version
Avaya Aura® System Manager	10.1.2.0 Build no. 10.1.0.0.537353 Software update 10.1.2.0.0715476
Avaya Aura® Session Manager	10.1 Build No. – 10.1.2.0.1012016
Avaya Aura® Communication Manager	10.1.2.0 – FP2 Update 01.0.974.0-27783
Avaya Messaging	11.0 SP2 Build 11.0.0.324
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G450	42.7.0 /2
Avaya J100 Series (H323) Deskphone	6.8.5.3.2
Avaya J100 Series (SIP) Deskphone	4.0.14.0.7
Avaya 9404 Digital Deskphone	17.0
Speakerbus Equipment/Software	Release/Version
Speakerbus iCMS with iManager	V4.001.1.0
Speakerbus iCS Server	V3.200.4.0
Speakerbus iGS Server	V2.000.2.0
Speakerbus iCB Server	V2.100.5.0
Speakerbus iWS	V2.610.3.0
Speakerbus iDUCX Virtual Deskstation	V4.100.5.0

5. Configure Avaya Aura® Communication Manager

No specific changes were made on Communication Manager to facilitate the connection of the Speakerbus ARIA iDUCX virtual deskstation with Session Manager. The Speakerbus ARIA iDUCX virtual deskstation softphone utilizes some of the features provided by Communication Manager. These features along with the dial plan, SIP trunk and coverage path are displayed in this section to provide the reader with some helpful information on how Communication Manager was setup for compliance testing.

Every site will have a unique setup, the information contained in the System Parameters Features or the System Parameters Customer Options will be suited to that particular site. The information provided in this section serves to show how this system was setup during compliance testing and is not an instruction guide to setup the Communication Manager for Speakerbus ARIA iDUCX virtual deskstation to work. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

Configuration and verification operations on Communication Manager illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). Communication Manager information displayed in this section can be summarized as follows:

- System Parameters and Features.
- SIP Trunk.
- Call Routing for SIP Phones.
- Feature Access Codes (FACs).
- Feature Name Extensions (FNEs).
- Class of Service (COS).
- Class of Restriction (COR).
- Coverage Path.

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

5.1. Verify System Parameters and Features

Each Communication Manager system will have its own setup with different System Parameters and Features configured depending on the requirement of the customer. Here is a snapshot of some of these values that were configured on the DevConnect lab for compliance testing.

5.1.1. Verify System Parameters Customer Options

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 Speakerbus ARIA iDUCX virtual deskstation.

display system-parameters customer-options		Page	1 of 12
OPTIONAL FEATURES			
G3 Version: V18	Software Package: Enterprise		
Location: 2	System ID (SID): 1		
Platform: 28	Module ID (MID): 1		
		USED	
Platform Maximum Ports:	6400	82	
Maximum Stations:	2400	22	
Maximum XMOBILE Stations:	2400	0	
Maximum Off-PBX Telephones - EC500:	9600	0	
Maximum Off-PBX Telephones - OPS:	9600	18	
Maximum Off-PBX Telephones - PBFMC:	9600	0	
Maximum Off-PBX Telephones - PVFMC:	9600	0	
Maximum Off-PBX Telephones - SCCAN:	0	0	
Maximum Survivable Processors:	313	0	
(NOTE: You must logoff & login to effect the permission changes.)			

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

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	4000	0	
Maximum Concurrently Registered IP Stations:	1000	2	
Maximum Administered Remote Office Trunks:	4000	0	
Max Concurrently Registered Remote Office Stations:	1000	0	
Maximum Concurrently Registered IP eCons:	68	0	
Max Concur Reg Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	2400	0	
Maximum Video Capable IP Softphones:	1000	1	
Maximum Administered SIP Trunks:	4000	50	
Max Administered Ad-hoc Video Conferencing Ports:	4000	0	
Max Number of DS1 Boards with Echo Cancellation:	80	0	
(NOTE: You must logoff & login to effect the permission changes.)			

5.1.2. Define System Features

Use the **change system-parameters features** command to administer system wide features for SIP endpoints. Those related to features listed in **Section 1** are shown in bold. These are all standard Communication Manager features that are also available to OPS stations. On **Page 18**, set the **Whisper Page Tone Given To** field to **all**.

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

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

WHISPER PAGE
    Whisper Page Tone Given To: all

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

Pickup On Transfer? y
```

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

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

IP PARAMETERS
    Direct IP-IP Audio Connections? y          IP Audio Hairpinning? n
        Synchronization over IP? n    Allow SIP-H323 Video in SDES? y
    Initial INVITE with SDP for secure calls? y
        SIP Endpoint Managed Transfer? n

Expand ISDN Numbers to International for 1XCES? N

CALL PICKUP
    Maximum Number of Digits for Directed Group Call Pickup: 4
        Call Pickup on Intercom Calls? y          Call Pickup Alerting? y
    Temporary Bridged Appearance on Call Pickup? y          Directed Call Pickup? y
        Extended Group Call Pickup: simple
        Enhanced Call Pickup Alerting? n

    Call Pickup for Call to Coverage Answer Group? y
        Display Information With Bridged Call? n
    Keep Bridged Information on Multiline Displays During Calls? y
        PIN Checking for Private Calls? n
```

5.2. Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the **procr** and the Session Manager (**sm101x**). The host names will be displayed throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```
display node-names ip
                                IP NODE NAMES
      Name                      IP Address
IPOffice                      10.10.40.25
aes101x                       10.10.40.16
ams101x                       10.10.40.17
default                       0.0.0.0
g450                          10.10.40.15
procr                        10.10.40.13
procr6                        ::
sm101x                      10.10.40.12
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.1.1**. In this configuration, the domain name is **greanep.sil6.avaya.com**. 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.

```
display ip-network-region 1
                                IP NETWORK REGION
                                Page 1 of 20
      Region: 1
Location: 1      Authoritative Domain: greanep.sil6.avaya.com
      Name: Default region
MEDIA PARAMETERS
      Codec Set: 1
      UDP Port Min: 2048
      UDP Port Max: 3329
      Intra-region IP-IP Direct Audio: yes
      Inter-region IP-IP Direct Audio: yes
      IP Audio Hairpinning? y
DIFFSERV/TOS PARAMETERS
      Call Control PHB Value: 46
      Audio PHB Value: 46
      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 codecs supported by the Speakerbus ARIA iDUCX virtual deskstation. The Speakerbus ARIA iDUCX virtual deskstation currently supports G.711 only but these other codecs were added as default. 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), which is supported by Speakerbus ARIA iDUCX virtual deskstation. Note the **Media Encryption** includes a setting of **none** to allow for unencrypted media.

display ip-codec-set 1					Page 1 of 2	
IP MEDIA PARAMETERS						
Codec Set: 1						
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)			
1: G.711A	n	2	20			
2: G.711MU	n	2	20			
3: G.729A	n	2	20			
4:						
Media Encryption				Encrypted SRTCP: enforce-unenc-srtcp		
1: 1-srtp-aescm128-hmac80						
2: none						
3:						

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. The configuration of the Signaling group used to send calls from Communication Manager to Session Manager for SIP users is as follows.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the appropriate setting, in this case it was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the 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.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm101x**).
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- **Far-end Domain** was set to the domain used during compliance testing.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.

- The **Direct IP-IP Audio Connections** field is set to **y**.
- **Initial IP-IP Direct Media** is set to **n**.
- The default values for the other fields may be used.

change signaling-group 11		Page 1 of 2
SIGNALING GROUP		
Group Number: 11	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: sm101x	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: greaney.sil6.avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? Y	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

The Trunk Groups used to send calls between Communication Manager and Session Manager was setup as follows. 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 dial plan. 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.

change trunk-group 11		Page 1 of 5
TRUNK GROUP		
Group Number: 1	Group Type: sip	CDR Reports: y
Group Name: SIP Phones	COR: 1	TN: 1 TAC: *811
Direction: two-way	Outgoing Display? y	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: tie	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 11	
	Number of Members: 10	

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field was set to a value of **1200** to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away. This may be changed if required by Speakerbus.

change trunk-group 11	Page 2 of 5
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 1200	
Disconnect Supervision - In? y Out? y	
XOIP Treatment: auto	Delay Call Setup When Accessed Via IGAR? n

Settings on **Page 3** can be left as default. However, the **Numbering Format** in the example below is set to **private**.

change trunk-group 11	Page 3 of 5
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private
	UUI Treatment: shared
	Maximum Size of UUI Contents: 128
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Modify Tandem Calling Number: no
Send UCID? y	
Show ANSWERED BY on Display? y	
DSN Term? n	

Settings on **Page 4** are as follows.

display trunk-group 11	Page 4 of 5
SHARED UII FEATURE PRIORITIES	
ASAI: 1	
Universal Call ID (UCID): 2	
MULTI SITE ROUTING (MSR)	
In-VDN Time: 3	
VDN Name: 4	
Collected Digits: 5	
Other LAI Information: 6	
Held Call UCID: 7	
ECD UII: 8	

Settings on **Page 5** are as follows.

change trunk-group 11	Page 5 of 5
PROTOCOL VARIATIONS	
Mark Users as Phone? y	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: From	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

5.3. Configure Call Routing for SIP phones

For compliance testing all calls beginning with 31 with a total length of 4 digits were to be sent across the SIP trunk to Session Manager as all SIP phones begin with 31. Automatic Alternate Routing (aar) was used to route the calls.

5.3.1. Administer 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 **Section 5.5**, 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 **3**, FNEs are also four digits beginning with **1**, and the FACs have formats as indicated with a **Call Type** of **fac**, these begin with either a ***** or a **#** as shown in **Section 5.4**.

change dialplan analysis										Page 1 of 12	
DIAL PLAN ANALYSIS TABLE											
Location: all										Percent Full: 5	
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type			
1	4	udp									
2	4	udp									
3	4	ext									
5	4	udp									
6	4	ext									
8	1	fac									
9	1	fac									
*8	4	dac									
*	3	fac									
#	3	fac									

5.3.2. Administer Route Selection for SIP Phones

Use the **change aar analysis x** command to further configure the routing of the dialed digits. Calls to SIP phones begin with **31** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 11**, which contains the outbound SIP Trunk Group.

change aar analysis 3										Page 1 of 2	
AAR DIGIT ANALYSIS TABLE											
Location: all										Percent Full: 1	
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd				
	31	4	4	11	lev0		n				
	5	7	7	999	aar		n				
	666	4	4	66	aar		n				
	7	7	7	999	aar		n				
	8	7	7	999	aar		n				
	9	7	7	999	aar		n				
							n				
							n				

Use the **change route-pattern n** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 11** is used to route calls to trunk group (**Grp No**) **11**. This is the SIP Trunk configured in **Section 5.2**.

change route-pattern 11										Page 1 of 4		
Pattern Number: 1 Pattern Name: SIP Phones												
SCCAN? n Secure SIP? n												
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC				
No	Mrk	Lmt	List	Del	Digits	QSIG						
								Intw				
1:	11	0					n user					
2:									n user			
3:									n user			
4:									n user			
5:									n user			
BCC VALUE		TSC	CA-TSC	ITC BCIE Service/Feature PARM				No. Numbering		LAR		
0 1 2 M 4 W		Request						Dgts	Format			
1:	y y y y y n	n		unre					lev0-pvt	none		
2:	y y y y y n	n		rest						none		
3:	y y y y y n	n		rest						none		
4:	y y y y y n	n		rest						none		
5:	y y y y y n	n		rest						none		
6:	y y y y y n	n		rest						none		

5.4. Define Feature Access Codes (FACs)

A FAC (feature access code) should be defined for each feature that will be used via the OPS FNEs. These are the FAC's that were used during compliance testing, these will be configured differently for every site. The FACs used in the sample configuration are shown in bold.

change feature-access-codes										Page	1 of	12
FEATURE ACCESS CODE (FAC)												
Abbreviated Dialing List1 Access Code: *11												
Abbreviated Dialing List2 Access Code: *12												
Abbreviated Dialing List3 Access Code: *13												
Abbreviated Dial - Prgm Group List Access Code: *10												
Announcement Access Code: *27												
Answer Back Access Code: #02												
Attendant Access Code:												
Auto Alternate Routing (AAR) Access Code: 8												
Auto Route Selection (ARS) - Access Code 1: 9										Access Code 2:		
Automatic Callback Activation: *05										Deactivation: #05		
Call Forwarding Activation Busy/DA: *03 All: *04										Deactivation: #04		
Call Forwarding Enhanced Status: *73 Act: *74										Deactivation: #74		
Call Park Access Code: *02												
Call Pickup Access Code: *09												
CAS Remote Hold/Answer Hold-Unhold Access Code:												
CDR Account Code Access Code: *14												
Change COR Access Code:												
Change Coverage Access Code:												
Conditional Call Extend Activation:										Deactivation:		
Contact Closure Open Code:										Close Code:		

Some other Feature Access Codes used.

display feature-access-codes	Page 2 of 12
FEATURE ACCESS CODE (FAC)	
Contact Closure Pulse Code:	
Data Origination Access Code:	
Data Privacy Access Code:	
Directed Call Pickup Access Code: *29	
Directed Group Call Pickup Access Code:	
Emergency Access to Attendant Access Code:	
EC500 Self-Administration Access Codes:	*61 *62 *63 *64
Enhanced EC500 Activation:	*60 Deactivation: #60
Enterprise Mobility User Activation:	Deactivation:
Extended Call Fwd Activate Busy D/A All:	*06 Deactivation: #06
Extended Group Call Pickup Access Code:	
Facility Test Calls Access Code:	
Flash Access Code:	
Group Control Restrict Activation:	Deactivation:
Hunt Group Busy Activation:	*30 Deactivation: #30
ISDN Access Code:	
Last Number Dialed Access Code: *08	
Leave Word Calling Message Retrieval Lock:	
*15	
Leave Word Calling Message Retrieval Unlock:	
#15:	

display feature-access-codes	Page 3 of 12
FEATURE ACCESS CODE (FAC)	
Leave Word Calling Send A Message:	
*16	
Leave Word Calling Cancel A Message:	
#16	
Limit Number of Concurrent Calls Activation:	*18 Deactivation: #18
Malicious Call Trace Activation:	*17 Deactivation: #17
Meet-me Conference Access Code Change:	
Message Sequence Trace (MST) Disable:	
PASTE (Display PBX data on Phone) Access Code:	
*28	
Personal Station Access (PSA) Associate Code:	*20 Dissociate Code: #20
Per Call CPN Blocking Code Access Code: *24	
Per Call CPN Unblocking Code Access Code: #24	
Posted Messages Activation:	Deactivation:
Priority Calling Access Code:	*07
Program Access Code:	
*00	
Refresh Terminal Parameters Access Code:	
#28	
Remote Send All Calls Activation:	#11 Deactivation:
Self Station Display Activation:	
Send All Calls Activation: *01	
Deactivation: #01	
Station Firmware Download Access Code:	

5.5. Define Feature Name Extensions (FNEs)

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

```
display off-pbx-telephone feature-name-extensions set 1      Page 1 of 3

EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME
Set Name: PG

Active Appearance Select:
    Automatic Call Back: 1301
Automatic Call-Back Cancel: 1302
    Call Forward All:
Call Forward Busy/No Answer:
    Call Forward Cancel:
        Call Park: 1303
    Call Park Answer Back: 1304
    Call Pick-Up: 1309
    Calling Number Block:
    Calling Number Unblock:
    Conditional Call Extend Enable:
    Conditional Call Extend Disable:
    Conference Complete:
    Conference on Answer:
    Directed Call Pick-Up: 1310
    Drop Last Added Party:
```

```
display off-pbx-telephone feature-name-extensions set 1      Page 2 of 3

EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME

Exclusion (Toggle On/Off):
Extended Group Call Pickup:
    Held Appearance Select:
    Idle Appearance Select:
        Last Number Dialed: 1305
    Malicious Call Trace:
Malicious Call Trace Cancel:
    Off-Pbx Call Enable:
    Off-Pbx Call Disable:
    Priority Call:
    Recall:
        Send All Calls: 1306
    Send All Calls Cancel: 1307
    Transfer Complete:
    Transfer On Hang-Up:
    Transfer to Voice Mail:
    Whisper Page Activation: 1311
```

5.6. Configure Class of Service (COS)

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

display cos-group 1											Page 1 of 2					
CLASS OF SERVICE	COS Group: 1				COS Name: PG Default											
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Auto Callback	n	y	y	n	y	n	y	n	y	n	y	n	y	n	y	n
Call Fwd-All Calls	n	y	n	y	y	n	n	y	y	n	n	y	y	n	n	y
Data Privacy	n	y	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	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y
Call Forwarding Busy/DA	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Personal Station Access (PSA)	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Extended Forwarding All	n	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	n	n	n	n	n
QSIG Call Offer Originations	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
Contact Closure Activation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n

display cos-group 1																Page	2 of	2
	CLASS OF SERVICE																	
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
VIP Caller	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Masking CPN/Name Override	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Call Forwarding Enhanced	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y		
Priority Ip Video	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Ad-hoc Video Conferencing	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
MOC Control:	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Match BCA Display To Principal	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
DCC Activation/Deactivation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		
Bridging Exclusion Override	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n		

5.7. Configure Class of Restriction (COR)

The COR that was used during compliance testing is shown below. 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**.

display cor 1	Page 1 of 43
CLASS OF RESTRICTION	
COR Number: 1	
COR Description: PG Default	
FRL: 0	APLT? y
Can Be Service Observed? y	Calling Party Restriction: none
Can Be A Service Observer? y	Called Party Restriction: none
Time of Day Chart: 1	Forced Entry of Account Codes? n
Priority Queuing? n	Direct Agent Calling? n
Restriction Override: none	Facility Access Trunk Test? y
Restricted Call List? n	Can Change Coverage? n
Access to MCT? y	Fully Restricted Service? n
Group II Category For MFC: 7	Hear VDN of Origin Annc.? n
Send ANI for MFE? n	Add/Remove Agent Skills? y
MF ANI Prefix:	Automatic Charge Display? n
Hear System Music on Hold? y	PASTE (Display PBX Data on Phone)? n
Can Be Picked Up By Directed Call Pickup? y	
Can Use Directed Call Pickup? y	
Group Controlled Restriction: inactive	

5.8. Configure Coverage Path

The coverage path configuration is shown below. The default values shown for **Busy**, **Don't Answer**, and **DND/SAC/Goto Cover** can be used for the **Coverage Criteria**.

The coverage path setup used for compliance testing is illustrated below. Note the following:

Don't Answer is set to **y**: The coverage path will be used in the event the phone set is not answered.

Number of Rings is set to **3**: The coverage path will be used after 3 rings.

Point 1 is set to **h66**: Hunt Group 66 is utilised by this coverage path.

```
display coverage path 3
```

COVERAGE PATH			
Coverage Path Number: 3			
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: 3
All?	n	n	
DND/SAC/Goto Cover?	y	y	
Holiday Coverage?	n	n	
COVERAGE POINTS			
Terminate to Coverage Pts. with Bridged Appearances? n			
Point1: h66	Rng: 3	Point2:	
Point3:		Point4:	
Point5:		Point6:	

The hunt group used for compliance testing is shown below. Note that on **Page 1** the **Group Extension** is **6666**, which is used to dial for messaging and **Group Type** is set to **ucd-mia**.

```
display hunt-group 66
```

HUNT GROUP		Page	1 of 60
Group Number: 66	ACD? n		
Group Name: Messaging	Queue? n		
Group Extension: 6666	Vector? n		
Group Type: ucd-mia	Coverage Path: 1		
TN: 1	Night Service Destination:		
COR: 1	MM Early Answer? n		
Security Code:	Local Agent Preference? n		
ISDN/SIP Caller Display:			
SIP URI::			

On **Page 2 Message Center** is set to **sip-adjunct**.

display hunt-group 66

Page 2 of 60

HUNT GROUP

Message Center: sip-adjunct

Voice Mail Number	Voice Mail Handle	Routing Digits
6666	6666	(e.g., AAR/ARS Access Code) 8

6. Configure Avaya Aura® Session Manager

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

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

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

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

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

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

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

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:
Password:

Log On **Cancel** [Change Password](#)

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

Once logged in navigate to **Elements** and click on **Routing** highlighted below.

AVAYA
Aura® System Manager 10.1

Users Elements Services Widgets Shortcuts

Search admin

Disk Space Utilization

60
45
30
15
0

opk val enddata tmp

■ Critical ■ Warning

Alarms

■ Critical ■ Major ■ Indeterminate
■ Minor ■ Warning

0 0 0 14

Notifications (2)

- Your last successful login was on at April 14, 2022 1:36 PM from 192.168.40.240. [None...](#)
- No Session Manager emergency Dial Pattern routes are administered. [None...](#)

Application State

License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

Information

Elements	Count	Sync Status
Avaya Breeze	3	■
CM	1	■
Session Manager	1	■
System Manager	1	■
UCM Applications	8	■

Current Usage :

7/250000 USERS

1/50

Shortcuts

Drag shortcuts here

Avaya Breeze®

- Communication Manager
- Communication Server 1000
- Device Adapter
- Device Services
- IP Office
- Media Server
- Meeting Exchange
- Messaging
- Presence
- Routing**
- Session Manager
- Web Gateway

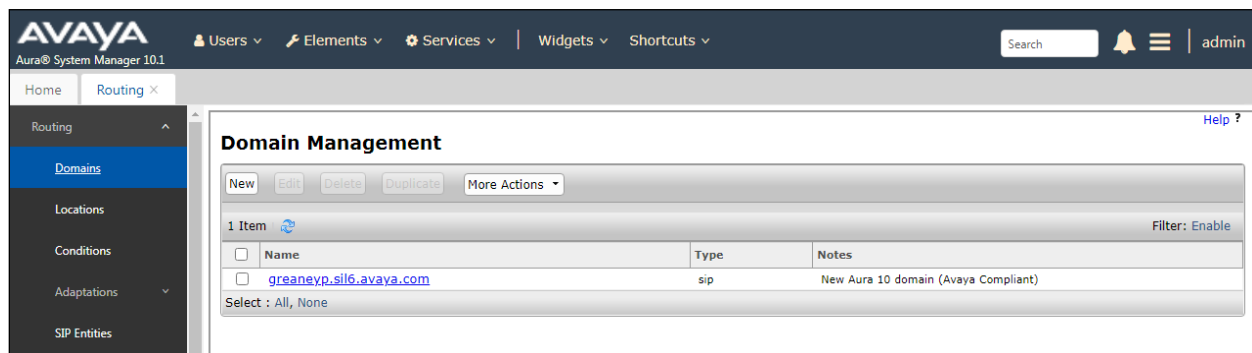
10.10.40.10 No successful backup taken for System Manager in the last 7 days.

6.1. Domains and Locations

Note: It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

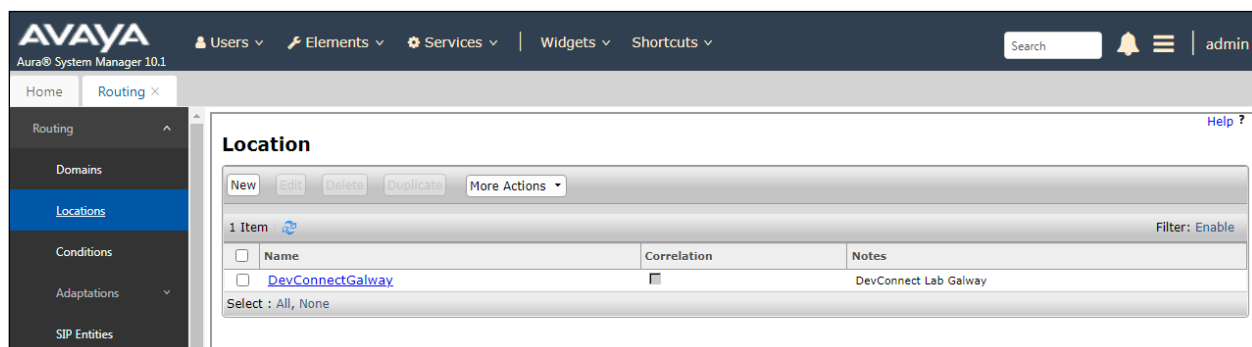
6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **greanep.sil6.avaya.com** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.



6.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectGalway** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.



6.2. Configure Ports for Speakerbus Registration

Each Session Manager Entity must be configured so that the Speakerbus ARIA iDUCX virtual deskstation can register to it using either TCP or UDP. From the web interface click **Routing** → **SIP Entities** → <Session Manager> (sm101x in the example below).

The screenshot shows the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and several menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar is located on the right. The left sidebar shows a navigation tree with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entities' and contains a table with 19 items. The table has columns for Name, FQDN or IP Address, and Type. The items listed are:

Name	FQDN or IP Address	Type
SBCE - InsideTrk - 158	10.10.40.158	SIP Trunk
SBCE - Loop -Voxtronic	10.10.40.158	SIP Trunk
sm101x	10.10.40.12	Session Manager
sm101xsec	10.10.40.22	Session Manager

Below the table, there is a 'Select : All, None' dropdown and a 'More Actions' button.

In the **Port** section, ensure that port **5060** of type **UDP** and **TCP** are added as shown below. This is the port the Speakerbus ARIA iDUCX virtual deskstation sends its SIP registration to. Select the appropriate SIP domain from the drop-down list and **Endpoint** is also ticked. Click **Commit** when done (not shown). Note that Avaya phones use **TLS** port **5061** which was also configured.

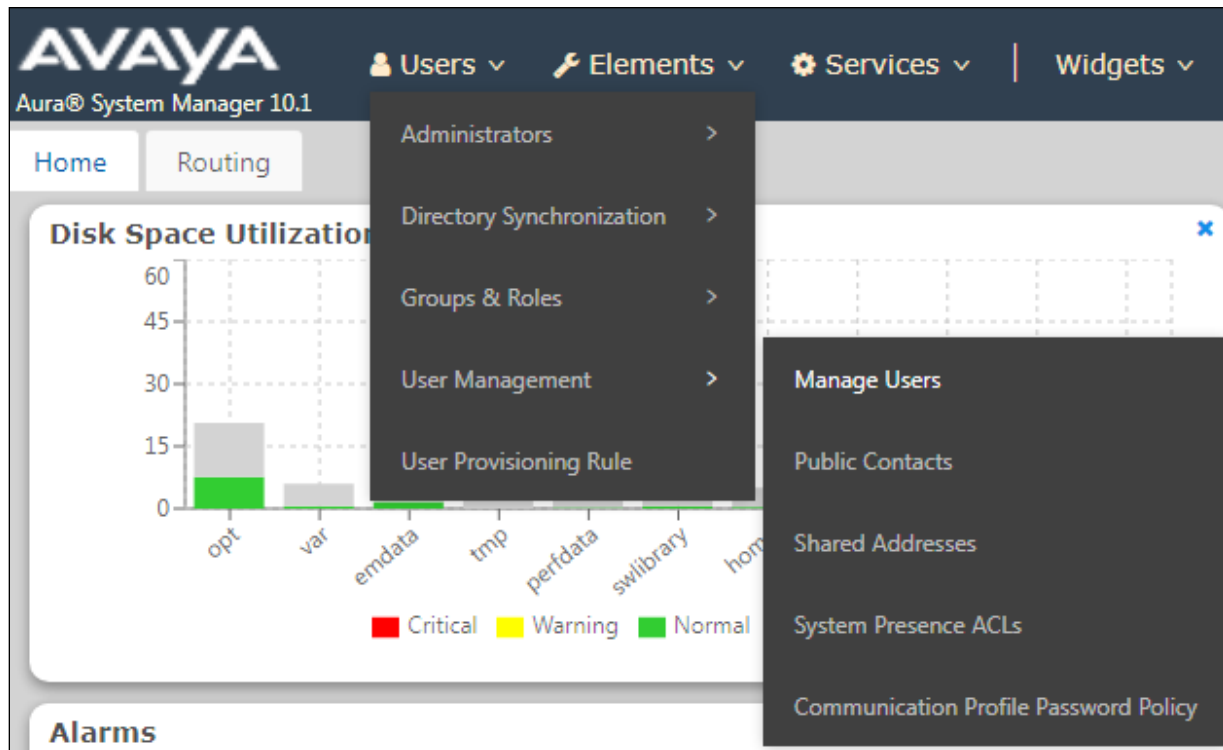
The screenshot shows the Avaya Aura System Manager 10.1 web interface, specifically the 'Failover Ports' and 'Listen Ports' configuration page. The left sidebar shows the navigation tree with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'Failover Ports' and contains two input fields for 'TCP Failover port' (5060) and 'TLS Failover port' (5061). Below this is the 'Listen Ports' section, which contains a table with 3 items. The table has columns for Listen Ports, Protocol, Default Domain, Endpoint, and Notes. The items listed are:

Listen Ports	Protocol	Default Domain	Endpoint	Notes
5060	TCP	greanep.sil6.avaya.com	<input checked="" type="checkbox"/>	
5060	UDP	greanep.sil6.avaya.com	<input checked="" type="checkbox"/>	
5061	TLS	greanep.sil6.avaya.com	<input checked="" type="checkbox"/>	

Below the table, there is a 'Select : All, None' dropdown and an 'Add' button. The 'SIP Responses to an OPTIONS Request' section is also visible at the bottom.

6.3. Add Primary Speakerbus ARIA iDUCX virtual deskstation User

A user must be added for each Speakerbus ARIA iDUCX virtual deskstation. Click **User Management** → **Manage Users**. Click on **New**, (not shown).



The Speakerbus ARIA iDUCX virtual deskstation uses ‘bridged appearance’ to enable calls to be presented and picked up at different Speakerbus ARIA iDUCX virtual deskstation. A site may have a group of say five Speakerbus ARIA iDUCX virtual deskstation all with each other’s extensions represented as bridged appearances so as each of them will display and can answer each other’s calls. This may be different on every site and in some cases perhaps only two out of the five may have bridged appearances there is no set rule on how the buttons should or would be configured.

What is shown in the next section is one iDUCX which has its own call appearance of 3181 and bridged appearances of extension 3182. It also has bridged appearances of 3191 and 3192 which are ‘Privacy’ extensions used specifically for making active calls private.

A user of a multi-appearance telephone can activate Privacy, a Manual Exclusion to keep the participants with appearance of the same extension from bridging on to an existing call. To use manual exclusion, the user presses the privacy button, either before the user places the call, or when the user is active on the call. If the user presses the privacy button while others are bridged onto the call, the system drops the other users. To turn off manual exclusion, the user presses the privacy button.

Note: The following screens display an existing user 3181, the screens will show an edited user instead of a new user but the information that is displayed is the very same as that required to add a new user.

From **Manager Users** section, click on **New** to add a new SIP user.

The screenshot shows the 'Manage Users' interface. At the top, there's a search bar and a table with columns: First Name, Surname, Display Name, Login Name, and SIP Handle. The table lists several users, including 'admin', 'J179', 'Paul', and 'J189'. A red box highlights the '+ New' button in the top toolbar. Below the table, there's a 'Total Users : 7' indicator and a '10 / page' dropdown.

Configure as following in the **Identity** tab.

- **First Name and Last Name** Enter an identifying name.
- **Login Name** Enter the extension number followed by the domain, in this case **3181@greaneyp.sil6.avaya.com**.
- **Time Zone** Enter the appropriate time zone.

The screenshot shows the 'User Profile | Edit | 3181@greaneyp.sil6.avaya.com' form. The 'Identity' tab is selected. The form contains several fields for user information, including 'Last Name', 'First Name', 'Login Name', 'Description', 'Password', 'Confirm Password', 'Endpoint Display Name', 'Language Preference', 'Employee ID', 'Last Name (in Latin alphabet characters)', 'First Name (in Latin alphabet characters)', 'Middle Name', 'Email Address', 'User Type', 'Localized Display Name', 'Title Of User', 'Time Zone', and 'Department'. The 'Last Name' field is filled with '3181'.

Click the **Communication Profile** tab and in the **Communication Profile Password** and **Confirm Password** fields, enter a numeric password. This will be used to register the iDUCX during login and adding into Speakerbus iCMS / imanager configuration in **Section 7.17**. Click **OK** to continue.

User Profile | Edit | 3181@greaney.sil6.avaya.com

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

Comm-Profile Password

Comm-Profile Password :

* Re-enter Comm-Profile Password :

Generate Comm-Profile Password

Cancel OK

Select **Communication Address** in the left window and click **New** in the main window.

User Profile | Edit | 3181@greaney.sil6.avaya.com

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

Edit + New Delete

	Type	Handle	Domain
--	------	--------	--------

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

The screenshot displays the Avaya DevConnect application interface. The main window has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' field and a 'PROFILE SET : Primary' section. Below this is a 'Communication Address' section with a 'PROFILES' list containing 'Session Manager Profile', 'Avaya Breeze® Profile', and 'CM Endpoint Profile'. A modal dialog titled 'Communication Address Add/Edit' is open in the foreground. It contains two main fields: '* Type:' with a dropdown menu set to 'Avaya SIP', and '*Fully Qualified Address:' which is split into two parts: a text box containing '3181' and a dropdown menu containing 'greaney.sil6.avaya...'. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

Ensure **Session Manager Profile** is checked and enter the **Primary Session Manager** details, enter the **Origination Sequence** and the **Termination Sequence**. Scroll down to complete the profile. Enter the **Home Location**, this should be the location configured in **Section Error! Reference source not found.** Click on Commit at the top of the page (not shown).

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

SIP Registration

* Primary Session Manager :

sm101x

Secondary Session Manager :

Start typing...

Survivability Server :

Start typing...

Max. Simultaneous Devices :

1

Block New Registration When Maximum Registrations Active?

☐

Application Sequences

Origination Sequence :

CM-APP-SEQ

Termination Sequence :

CM-APP-SEQ

Emergency Calling Application Sequences

Emergency Calling Origination Sequence :

Select

Emergency Calling Termination Sequence :

Select

Call Routing Settings

* Home Location :

DevConnectGalway



Conference Factory Set :

Select

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

- **System** Select the relevant Communication Manager SIP Entity from the drop-down list.
- **Profile Type** Select **Endpoint** from the drop-down list.
- **Extension** Enter the required extension number, in this case **3181**.
- **Template** Select **DEFAULT_9630SIP_CM_10_1** from the drop-down list.
- **Port** Enter **IP**.
- **Sip Trunk** This was set to **aar** for compliance testing.

Click on the Endpoint Editor icon, (this is next to the **Extension** number), to open the Communication Manger configuration for this extension. This will allow the buttons to be administered as well as changes to Class of Service and Class of Restriction and other features.

Identity	Communication Profile	Membership	Contacts
<p>Communication Profile Password</p> <p>PROFILE SET : Primary ▼</p> <p>Communication Address</p> <p>PROFILES</p> <p>Session Manager Profile <input checked="" type="checkbox"/></p> <p>Avaya Breeze® Profile <input type="checkbox"/></p> <p>CM Endpoint Profile <input checked="" type="checkbox"/></p>			
<p>* System: cm101x ▼</p> <p>Use Existing Endpoints: <input type="checkbox"/></p> <p>Template: 9630SIP_DEFAULT_CM_10_1 Q</p> <p>Security Code: Enter Security Code</p> <p>Voice Mail Number: 6668</p> <p>Calculate Route Pattern: <input type="checkbox"/></p> <p>SIP URI: Select ▼</p> <p>Delete on Unassign from User or on Delete User: <input checked="" type="checkbox"/></p> <p>Allow H.323 and SIP Endpoint Dual Registration: <input type="checkbox"/></p>		<p>* Profile Type: Endpoint ▼</p> <p>* Extension: 3181 </p> <p>* Set Type: 9630SIP</p> <p>Port: S000005 Q</p> <p>Preferred Handle: Select ▼</p> <p>Sip Trunk: aar</p> <p>Enhanced Callr-Info Display for 1-line phones: <input type="checkbox"/></p> <p>Override Endpoint Name and Localized Name: <input checked="" type="checkbox"/> </p>	

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

- **Class of Restriction (COR)** Enter the **COR** as configured in **Section 5.7**.
- **Emergency Location Ext** Enter **3181** (the extension for this user).
- **Tenant Number** Enter the appropriate **Tenant Number**.
- **SIP Trunk** Enter **aar**.
- **Class of Service (COS)** Enter the **COS** as configured in **Section 5.6**.
- **Message Lamp Ext.** Enter **3181** (the extension for this user).
- **Type of 3PCC Enabled** This was set to **Avaya** for compliance testing.
- **Coverage Path 1** This was set to the coverage path, as per **Section 5.8**.

System	cm101x	Extension	3181
Template	9630SIP_DEFAULT_CM_10_1	Set Type	9630SIP
Port	S000005	Security Code	
Name	3181, TurretOne		

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

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	3181	* Message Lamp Ext.	3181
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1	3	Coverage Path 2	
Lock Message	<input type="checkbox"/>	Localized Display Name	3181, TurretOne
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

SIP URI

Primary Session Manager

IPv4: 10.10.40.12 **IPv6:**

Secondary Session Manager

IPv4: **IPv6:**

Click on the **Feature Options** tab. The screen shot below shows the Feature Options that were used during compliance testing. Ensure that **Bridged Call Alerting** is ticked as shown below, the other features are ticked as default.

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)																						
Button Assignment (B)																										
Group Membership (M)																										
Active Station Ringing	single ▼		Auto Answer	none ▼																						
MWI Served User Type	None ▼		Coverage After Forwarding	system ▼																						
Per Station CPN - Send Calling Number	None ▼		Display Language	english ▼																						
IP Phone Group ID			Hunt-to Station																							
Remote Soft Phone Emergency Calls	as-on-local ▼		Loss Group	19																						
LWC Reception	spe ▼		Survivable COR	internal ▼																						
AUDIX Name	None ▼		Time of Day Lock Table	None ▼																						
Speakerphone	▼		Voice Mail Number	6668																						
Short/Prefixed Registration Allowed	default ▼		Music Source																							
EC500 State	enabled ▼																									
Bridging Tone for This Extension	no ▼																									
Features <table border="0"> <tr> <td><input type="checkbox"/> Always Use</td> <td><input type="checkbox"/> Idle Appearance Preference</td> </tr> <tr> <td><input type="checkbox"/> IP Audio Hairpinning</td> <td><input checked="" type="checkbox"/> IP SoftPhone</td> </tr> <tr> <td><input checked="" type="checkbox"/> Bridged Call Alerting</td> <td><input checked="" type="checkbox"/> LWC Activation</td> </tr> <tr> <td><input type="checkbox"/> Bridged Idle Line Preference</td> <td><input type="checkbox"/> CDR Privacy</td> </tr> <tr> <td><input checked="" type="checkbox"/> Coverage Message Retrieval</td> <td><input checked="" type="checkbox"/> Precedence Call Waiting</td> </tr> <tr> <td><input type="checkbox"/> Data Restriction</td> <td><input checked="" type="checkbox"/> Direct IP-IP Audio Connections</td> </tr> <tr> <td><input checked="" type="checkbox"/> Survivable Trunk Dest</td> <td><input type="checkbox"/> H.320 Conversion</td> </tr> <tr> <td><input type="checkbox"/> Bridged Appearance Origination Restriction</td> <td><input type="checkbox"/> IP Video Softphone</td> </tr> <tr> <td><input checked="" type="checkbox"/> Restrict Last Appearance</td> <td><input type="checkbox"/> Per Button Ring Control</td> </tr> <tr> <td><input type="checkbox"/> Turn on mute for remote off-hook attempt</td> <td></td> </tr> <tr> <td><input type="checkbox"/> IP Hoteling</td> <td></td> </tr> </table>					<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference	<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> IP SoftPhone	<input checked="" type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation	<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy	<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Precedence Call Waiting	<input type="checkbox"/> Data Restriction	<input checked="" type="checkbox"/> Direct IP-IP Audio Connections	<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> H.320 Conversion	<input type="checkbox"/> Bridged Appearance Origination Restriction	<input type="checkbox"/> IP Video Softphone	<input checked="" type="checkbox"/> Restrict Last Appearance	<input type="checkbox"/> Per Button Ring Control	<input type="checkbox"/> Turn on mute for remote off-hook attempt		<input type="checkbox"/> IP Hoteling	
<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference																									
<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> IP SoftPhone																									
<input checked="" type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation																									
<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy																									
<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Precedence Call Waiting																									
<input type="checkbox"/> Data Restriction	<input checked="" type="checkbox"/> Direct IP-IP Audio Connections																									
<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> H.320 Conversion																									
<input type="checkbox"/> Bridged Appearance Origination Restriction	<input type="checkbox"/> IP Video Softphone																									
<input checked="" type="checkbox"/> Restrict Last Appearance	<input type="checkbox"/> Per Button Ring Control																									
<input type="checkbox"/> Turn on mute for remote off-hook attempt																										
<input type="checkbox"/> IP Hoteling																										

Click on the **Button Assignments tab (Main Buttons)** and configure Buttons **1, 2** and **3** as **call-appr**. For compliance testing bridged appearances were configured to test ‘Barge In’ on buttons 4, 5 and 6. ‘Privacy’ buttons **7, 8** and **9** were set to extension **3191** and **Feature Buttons 10, 11** and **12** were set to **3192**.

System	cm101x	Extension	3181
Template	9630SIP_DEFAULT_CM_10_1	Set Type	9630SIP
Port	S000005	Security Code	
Name	3181, TurretOne		

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

Main Buttons		Feature Buttons	Button Modules	Phone View
1	call-appr			
2	call-appr			
3	call-appr			
4	brdg-appr	Button	1	Ext 3182
5	brdg-appr	Button	2	Ext 3182
6	brdg-appr	Button	3	Ext 3182
7	brdg-appr	Button	1	Ext 3191
8	brdg-appr	Button	2	Ext 3191

Click on **Feature Buttons** and configure as per screen shot below. There were two SIP Users configured as 'Privacy Users' these were extensions **3191** and **3192**. To allow this user (3181) use Privacy, the privacy extension must be added as bridged appearances on this user's buttons as shown below. Buttons **10**, **11** and **12** were set to extension **3192**. Other features such as Call Forward and Call Forward Busy Deactivated as well as Exclusion are also added as buttons as shown. Click **Done** when all the configuration has been set correctly (not shown).

Button Assignment (B)		Group Membership (M)					
<div> Main Buttons Feature Buttons Button Modules Phone View </div>							
9	brdg-appr ▼	Button	3	Ext	3191	Ring	
10	brdg-appr ▼	Button	1	Ext	3192	Ring	
11	brdg-appr ▼	Button	2	Ext	3192	Ring	
12	brdg-appr ▼	Button	3	Ext	3192	Ring	
13	None ▼						
14	None ▼						
15	None ▼						
16	None ▼						
17	None ▼						
18	None ▼						
19	None ▼						
20	None ▼						
21	None ▼						
22	call-fwd ▼	Extension					
23	cfwd-busyda ▼	Extension					
24	exclusion ▼						

Click on **Commit** at the top of the screen to save the new user.

User Profile | Edit | 3181@greaney.sil6.avaya.com

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

* System :

cm101x

* Profile Type :

Endpoint

Use Existing Endpoints :

* Extension :

3181

Template :

9630SIP_DEFAULT_CM_10

* Set Type :

9630SIP

Security Code :

Enter Security Code

Port :

S000005

Voice Mail Number :

6668

Preferred Handle :

Select

Calculate Route Pattern :

Sip Trunk :

aar

SIP URI :

Select

Enhanced Callr-Info Display for 1-line phones :

Delete on Unassign from User or on Delete User :

Override Endpoint Name and Localized Name :

Allow H.323 and SIP Endpoint Dual Registration :

6.4. Configure Privacy Users

Privacy users are configured on System Manager as bridged appearances on the primary user. Add a 'Privacy User' in the same way as the primary user was configured in **Section 6.3**. Two privacy users 3191 and 3192 were created to be used by the primary user 3181. Following the same procedure as **Section 6.3**, under the **Identity** tab, enter a suitable **Name** and **Time Zone**.

Identity	Communication Profile	Membership	Contacts
Basic Info			
Address	User Provisioning Rule: <input type="text"/>		
LocalizedName			
	* Last Name: <input type="text" value="3191"/>	Last Name (in Latin alphabet characters): <input type="text" value="3191"/>	
	* First Name: <input type="text" value="PrivacyOne"/>	First Name (in Latin alphabet characters): <input type="text" value="PrivacyOne"/>	
	* Login Name: <input type="text" value="3191@greanelyp.sil6.ava"/>	Middle Name: <input type="text" value="Middle Name Of User"/>	
	Description: <input type="text" value="Bridged Appearance"/>	Email Address: <input type="text" value="Email Address Of User"/>	
	Password: <input type="text"/>	User Type: <input type="text" value="Basic"/>	
	Confirm Password: <input type="text"/>	Localized Display Name: <input type="text" value="3191, PrivacyOne"/>	
	Endpoint Display Name: <input type="text" value="3191, PrivacyOne"/>	Title Of User: <input type="text" value="Title Of User"/>	
	Language Preference: <input type="text" value="English (United Stat..."/>	Time Zone: <input type="text" value="(+1:0)GMT : Dublin,..."/>	
	Employee ID: <input type="text" value="Employee Id Of User"/>	Department: <input type="text" value="Department Of User"/>	

A **Communication Profile** and **Session Manager Profile** are added as per **Section 6.3**, (not shown here). Click on **CM Endpoint Profile** and enter the same **Template** information, that being **9630SIP_DEFAULT_CM_10_1**. Enter the appropriate **Extension** number (**3191**) and click on the “configure extension” icon, next to the Extension number.

User Profile | Edit | 3191@greaney.sil6.avaya.com Commit & Continue Commit Cancel

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

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile ☒


Avaya Breeze® Profile ☐

CM Endpoint Profile ☒

* System: cm101x

* Profile Type: Endpoint

Use Existing Endpoints: ☐

* Extension: 3191 

Template: 9630SIP_DEFAULT_C

* Set Type: 9630SIP

Security Code: Enter Security Code

Port: S000010

Voice Mail Number: 6668


Preferred Handle: Select

Calculate Route Pattern: ☐

SIP URI: Select

Enhanced Callr-Info Display for 1-line phones: ☐

Delete on Unassign from User or on Delete User: ☒

Override Endpoint Name and Localized Name: ☒ 

Allow H.323 and SIP Endpoint Dual Registration: ☐

The same **COR** and **COS** that were selected for the primary user in **Section 6.3** can be used for this privacy user and again **Type of 3PCC Enabled** is set to **Avaya**.

General Options (G) **Feature Options (F)** **Site Data (S)** **Abbreviated Call Dialing (A)** **Enhanced Call Fwd (E)**

Button Assignment (B) **Group Membership (M)**

* Class of Restriction (COR) 1

* Emergency Location Ext 3191

* Tenant Number 1

* SIP Trunk aar

Coverage Path 1 3

Lock Message ☐

Multibyte Language Not Applicable

* Class Of Service (COS) 1

* Message Lamp Ext. 3191

Type of 3PCC Enabled Avaya

Coverage Path 2

Localized Display Name 3191, PrivacyOne

Enable Reachability for Station Domain Control system

Click on the **Feature Options** tab. The screen shot below shows the Feature Options that were used during compliance testing. Ensure that **Bridged Call Alerting** is ticked as shown below, the other features are ticked as default.

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
Button Assignment (B)		Group Membership (M)		
Active Station Ringing single ▼	Auto Answer none ▼			
MWI Served User Type None ▼	Coverage After Forwarding system ▼			
Per Station CPN - Send Calling Number None ▼	Display Language english ▼			
IP Phone Group ID <input type="text"/>	Hunt-to Station <input type="text"/>			
Remote Soft Phone Emergency Calls as-on-local ▼	Loss Group 19			
LWC Reception spe ▼	Survivable COR internal ▼			
AUDIX Name None ▼	Time of Day Lock Table None ▼			
Speakerphone <input type="text"/>	Voice Mail Number 6668			
Short/Prefixed Registration Allowed default ▼	Music Source <input type="text"/>			
EC500 State enabled ▼				
Bridging Tone for This Extension no ▼				
Features				
<div> <input type="checkbox"/> Always Use <input type="checkbox"/> Idle Appearance Preference </div> <div> <input type="checkbox"/> IP Audio Hairpinning <input type="checkbox"/> IP SoftPhone </div> <div> <input checked="" type="checkbox"/> Bridged Call Alerting <input checked="" type="checkbox"/> LWC Activation </div> <div> <input type="checkbox"/> Bridged Idle Line Preference <input type="checkbox"/> CDR Privacy </div> <div> <input checked="" type="checkbox"/> Coverage Message Retrieval <input checked="" type="checkbox"/> Precedence Call Waiting </div> <div> <input type="checkbox"/> Data Restriction <input checked="" type="checkbox"/> Direct IP-IP Audio Connections </div> <div> <input checked="" type="checkbox"/> Survivable Trunk Dest <input type="checkbox"/> H.320 Conversion </div> <div> <input type="checkbox"/> Bridged Appearance Origination Restriction <input type="checkbox"/> IP Video </div> <div> <input checked="" type="checkbox"/> Restrict Last Appearance <input type="checkbox"/> Per Button Ring Control </div> <div> <input type="checkbox"/> Turn on mute for remote off-hook attempt </div> <div> <input type="checkbox"/> IP Hoteling </div>				

Click on the **Button Assignments tab (Main buttons)** and configure Buttons **1, 2** and **3** as **call-appr**. For compliance testing, buttons **4, 5** and **6** were configured as **brdg-appr** to extension **3181** (Primary iDUCX User).

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)		Enhanced Call Fwd (E)	
Button Assignment (B)		Group Membership (M)							
Main Buttons		Feature Buttons		Button Modules		Phone View			
1	call-appr ▼								
2	call-appr ▼								
3	call-appr ▼								
4	brdg-appr ▼	Button	1	Ext	3181				
5	brdg-appr ▼	Button	2	Ext	3181				
6	brdg-appr ▼	Button	3	Ext	3181				
7	None ▼								
8	None ▼								

Click on the **Feature Buttons** tab and ensure that Exclusion is set on one of the buttons, in this case **Button 24** was configured as **exclusion**.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)		Enhanced Call Fwd (E)	
Button Assignment (B)		Group Membership (M)							
Main Buttons		Feature Buttons		Button Modules		Phone View			
9	None ▼								
10	None ▼								
11	None ▼								
12	None ▼								
13	None ▼								
14	None ▼								
15	None ▼								
16	None ▼								
17	None ▼								
18	None ▼								
19	None ▼								
20	None ▼								
21	None ▼								
22	None ▼								
23	None ▼								
24	exclusion ▼								

7. Speakerbus ARIA iDUCX Virtual Deskstation Configuration

This section provides the procedure for configuring the Speakerbus ARIA iDUCX virtual deskstation via the iManager Centralised Management System (iCMS). The iCMS comprises of three components, the iManager web portal application, the iCMS communication service and the iCMS database. The iManager web portal application consists of a series of configuration web pages that allow administrators to manage the Speakerbus ARIA iDUCX virtual deskstation.

The procedure for configuring an iDUCX falls into the following areas.

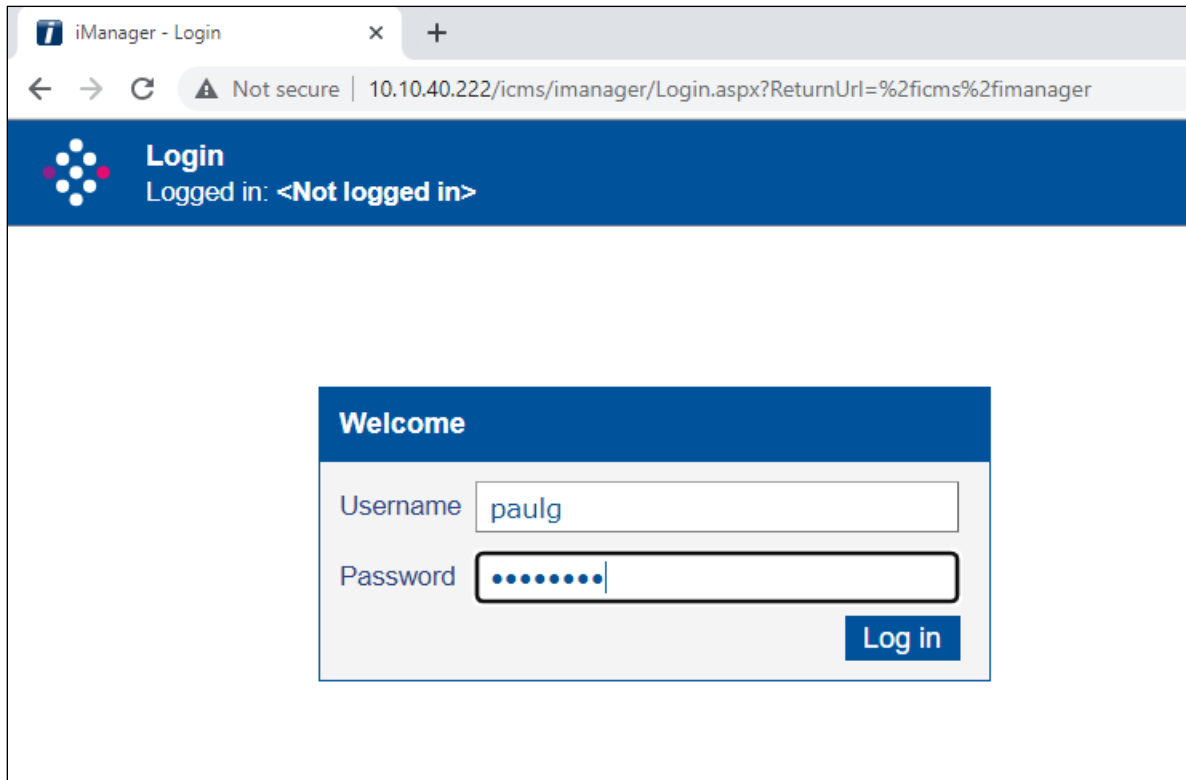
- Launch iManager Web Portal
- Create/Verify User Policies
- Create/Verify Device Policies
- Create Network Services (including iGS Server)
- Create Site and Call Region
- Assign iGS to Call Region
- Create CloudBase Collection
- Check Device Defaults
- Announce iCB Server
- Set up iDUCX devices
- Observe iDUCX
- Create Users
- Create Speakerbus iCS PBX (SIP Server)
- Assign iCS into a Call Region
- Create Avaya PBX (SIP Server)
- Create Dial Plan
- Create Call and Privacy Appearances
- Assign User Permissions
- Assign Ownership (of Appearances to Users)
- Assign Default Call Appearances
- Synchronize Deskstations

Note 1: The Speakerbus iCS, iGS and iCB are separate products which should be installed, and relevant IP addresses known before doing any of the configuration in the next sections. Refer to Speakerbus support for assistance.

Note 2: This section displays some the configuration screens that may have already been configured.

7.1. Launch iManager Web Portal

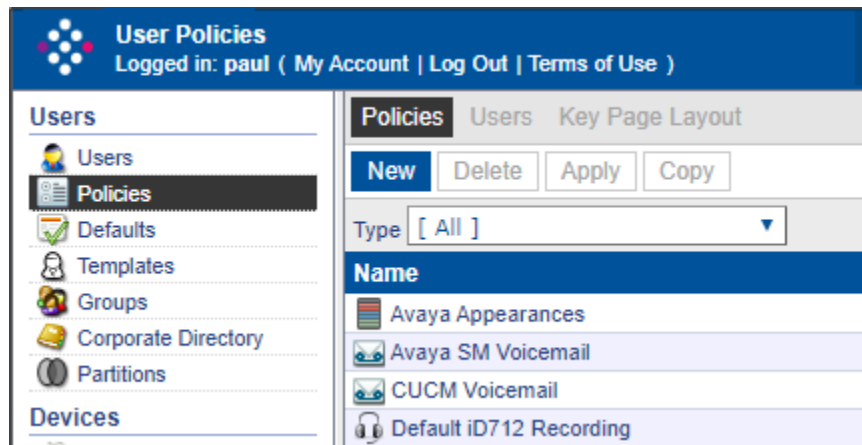
To access the iManager software interface, open a web browser and type the iManager web address, `http://<ServerIP>/icms/imanager`. (**Note:** If using an older version of icms / imanager, the URL is amended to `http://<ServerIP> /imanager`). Enter the appropriate credentials and click **Log in**.



The screenshot shows a web browser window titled "iManager - Login". The address bar displays "Not secure | 10.10.40.222/icms/imanager/Login.aspx?ReturnUrl=%2ficms%2fimanager". The page has a blue header with the iManager logo (a cluster of dots) and the text "Login" and "Logged in: <Not logged in>". Below the header is a "Welcome" section with a light blue background. It contains two input fields: "Username" with the value "paulg" and "Password" with masked characters (dots). A blue "Log in" button is positioned to the right of the password field.

7.2. Creating/Verifying User Policies

Select **Users** → **Policies** in the left pane and click on **New**.



Enter an identifying **Name**, in the **Type** dropdown box select **Voicemail**, and enter a valid address for the voicemail server, in this case a pre-configured hunt group number for voicemail access is used. Click **OK** once completed (not shown).

The screenshot shows the 'General' settings form for a new policy. It has a 'Name' field containing 'Avaya SM Voicemail' and a 'Type' dropdown menu set to 'Voicemail'. Below these is a section titled 'Voicemail Settings:' which contains an 'Address' field with the value '6666'.

Select **Users** → **Policies** in the left pane. Select and view the **Default Privileges** policy, (no changes to this should be required, however, it is referred to later in these Application Notes).

User Policies
Logged in: paul (My Account | Log Out | Terms of Use)

Users
Users
Policies
Defaults
Templates
Groups
Corporate Directory
Partitions

Devices
Deskstations
Gateways
CloudBase
Policies
Defaults

Call Servers
PBXs
PBX Appearances
Policies

Network
Sites
Call Regions
Voice Services
Network Services

Security
Administrators
Roles
API Accounts

System
Preferences
Audit Log
Reports
System
Licensing
Debugging

Policies Users Key Page Layout
New Delete Apply Copy
Type [All]
Name
Avaya Appearances
Avaya SM Voicemail
CUCM Voicemail
Default iD712 Recording
Default iDUCX Recording
Default iTurret Recording
Default Preferences
Default Privileges
Default SE708 Recording
iCS Appearances
No recording
No recording (aria)
Voice Services
Page: 1
General iTurret
Allow Group Talk Barge ☒
Allow Call Forwarding ☒
Allow # To Complete Dialling ☒
Allow Do Not Disturb ☒
Allow User Page Editing ☒
Allow Fixed Key Editing ☒
Allow Alert Profile Editing ☒
Allow Personal Directory Editing ☒
Allow CTI ☒
Allow SIPTAPI ☒
Allow Recording Tone Control ☒

Select **Users** → **Policies** in the left pane. Select the **Default Preferences** policy, click the **iTurret** tab and review the default settings (no changes should be needed to these; however, they are referred to later in these Application Notes).

The screenshot displays the Avaya DevConnect User Policies management interface. The left-hand navigation pane shows a tree structure with categories: Users, Policies (selected), Defaults, Templates, Groups, Corporate Directory, Partitions, and Account Mappings. Under the Policies category, sub-items include Deskstations, Gateways, CloudBase, Policies, and Defaults. The main content area is titled 'User Policies' and shows a list of policies. The 'Default Preferences' policy is selected, and the 'iTurret' tab is active. The settings are organized into two columns: 'General' and 'iE801'. The 'General' column includes settings for Display Language (English), Time Display Format (12 Hour), Conferencing Mode (Standard), Dynamic Keys Call Display (All Calls), Dynamic Keys Auto-Refresh (unchecked), Log Intercom Calls in Call Register (checked), MWI For Missed Calls (unchecked), Fast flash LED for unanswered calls (0 seconds), Alternate flash LED for on-hold calls (0 seconds), Speaker Playback Duration ([Off]), UI Mode (Standard), and Appearance Label Format (Appearance Line suffix: /I). The 'iE801' column includes settings for Mute Button Ganging (checked), Group Button Ganging (unchecked), Caller ID (Remote Party Name, P-Asserted Identity, and From Display Name all checked), and Screen Saver settings (Screen Saver Auto-Exit, Screen Saver Timeout, and Screen Saver Day / Night Mode all unchecked).

7.3. Creating/Verifying Device Policies

Select **Devices** → **Policies** in the left pane. Select the **Default RTP Media & SIP** policy, if leaving the SIP signaling protocol setting at default UDP, then no changes should be needed to these; however, they are referred to later in these Application Notes. If using TCP, then untick the “Allow UDP SIP Signaling” flag and press OK (not shown).

Device Policies
Logged in: paulg (My Account | Log Out | Terms of Use)
TRIAL LICENCE: 33 DAYS LEFT

Users
Users
Policies
Defaults
Templates
Groups
Corporate Directory
Partitions
Account Mappings

Devices
Deskstations
Gateways
CloudBase
Policies
Defaults

Call Servers
PBXs
PBX Appearances
Policies

Network
Sites
Call Regions
Voice Services
Network Services

Security
Administrators
Roles
API Accounts

System

Policies Devices Collections Servers

New Delete Apply Copy

Type [All]

Name	Type
Default MAC Address Range	MAC Address Range
Default RTP Media & SIP	RTP Media & SIP
Default SbRTP	SbRTP Media

Page: 1 2 3 4 5

General

Name: Default RTP Media & SIP

Type: RTP Media & SIP

RTP Media Settings:

Time To Live: 120

DSCP Value: 0

RTCP DSCP Value: 0

SIP RTP Media Settings:

Preferred Codec: G.711 A-Law

Preferred Intercom Codec: G.711 A-Law

Voice Activity Detection: ☐

AYRE Codec: 16KHZ PCM

AYRE Voice Activity Detection: ☐

SIP Signalling Settings:

Allow UDP SIP Signaling: ☒

Staying on **Policies**, select and view the **Default SbRTP** policy (no changes should be needed to these; however, they are referred to later in these Application Notes).

The screenshot displays the 'Policies' tab in the Avaya DevConnect interface. At the top, there are tabs for 'Policies', 'Devices', and 'Collections'. Below these are buttons for 'New', 'Delete', 'Apply', and 'Copy'. A 'Type' dropdown menu is set to '[All]'. A list of policies is shown, with 'Default SbRTP' highlighted. Below the list, a pagination bar shows 'Page: 1 2' with navigation arrows. The 'Default SbRTP' policy configuration is shown in the 'General' tab. The 'Name' field is 'Default SbRTP' and the 'Type' is 'SbRTP Media'. The 'SbRTP Media Settings' section includes the following fields:

Setting	Value
RTP Payload Code	96
Time To Live	1
DSCP Value	0
Bandwidth	Standard
Packet Size	4 ms
Voice Activity Detection	<input checked="" type="checkbox"/>
Lost Packet Tolerance (%)	50
Sample Slip Tolerance (%)	100
iSeries Compatibility	Version 3.0
SbRTP Inactivity Timeout	500 ms
RTCP Keep Alive	<input type="checkbox"/>

7.4. Creating Network Services

A network service is an addressable entity that a device uses to contact the relevant service when and where required. Defining network services here merely defines the network service configuration, it does not cause it to be used by any devices. Network services can be assigned to devices via the device configuration or via a policy, depending on the network service type. Confirm that CMS comms and seen in the list view with the correct details.

Note: Refer to the *Speakerbus iManager Administrator's Guide*.

To create an NTP Server, select **Network** → **Network Services** in the left pane, click **New** and select NTP Server from the dropdown menu (not shown).

Complete the following fields.

- **Name** Enter a descriptive name for the site.
- **Private Address** Enter the IP address of the NTP server.

The screenshot displays the Avaya iManager Network Services configuration page. The top header shows the user is logged in as 'paulg' and has a trial license for 33 days left. The left sidebar contains navigation menus for Users, Devices, Call Servers, and Network. The main content area shows a list of network services with columns for Type, Private Address, and Public Address. Below the list is a pagination control showing 'Page: 1'. The configuration form for the selected 'NTP Server' is visible, showing fields for Name (NTP Galway), Type (NTP Server), and NTP Server Settings (Private Address: 10.10.40.5, Public Address, IPv6 Address).

Type	Private Address	Public Address
iGS Server	10.10.40.216	
iWS Server	10.10.40.222	
NTP Server	10.1.1.9	
NTP Server	10.10.40.5	
iCMS Communications Server	10.10.40.222	

Page: 1

General

Name: NTP Galway

Type: NTP Server

NTP Server Settings:

Private Address: 10.10.40.5

Public Address:

IPv6 Address:

To create an iGS Server, select **Network** → **Network Services** in the left pane, click **New** and select **iGS Server** from the dropdown menu (not shown). Complete the following fields.

- **Name** Enter a descriptive name for the site.
- **Private Address** Enter the ip address of the iGS server.

Note: Refer to the *Speakerbus iManager Administrator's Guide*.

Click **OK** once completed.

The screenshot shows the iManager Administrator's Guide interface. The left pane contains a navigation tree with the following sections:

- Users**
 - Users
 - Policies
 - Defaults
 - Templates
 - Groups
 - Corporate Directory
 - Partitions
 - Account Mappings
- Devices**
 - Desktops
 - Gateways
 - CloudBase
 - Policies
 - Defaults
- Call Servers**
 - PBXs
 - PBX Appearances
 - Policies
- Network**
 - Sites
 - Call Regions
 - Voice Services
 - Network Services**
- Security**
 - Administrators
 - Roles

The main pane displays the **Network Services** configuration page. It includes a table of existing iGS Servers and a form for creating a new one.

Type	Private Address	Public Address
iGS Server	10.10.40.216	
iWS Server	10.10.40.222	
NTP Server	10.1.1.9	
NTP Server	10.10.40.5	
iCMS Communications Server	10.10.40.222	

The form for creating a new iGS Server includes the following fields:

- Name:** iGS
- Type:** iGS Server
- iGS Server Settings:**
 - Authentication Name:** MG-1
 - Change Password...** (button)
 - Private Address:** 10.10.40.216
 - Public Address:** (empty field)
 - IPv6 Address:** (empty field)

To create an iWS Server, select **Network** → **Network Services** in the left pane, click **New** and select **iWS Server** from the dropdown menu (not shown). Complete the following fields.

- **Name** Enter a descriptive name for the site.
- **Private Address** Enter the ip address of the iWS server.

Note: Refer to the *Speakerbus iManager Administrator's Guide*.

Click **OK** once completed.

For configuration of Voice Recording for the deskstation / user. Refer to the *Speakerbus iManager Administrator's Guide*.

Network Services
Devices
Call Regions
Collections

New
Delete
Apply

Type [All]
Status [All]

Type	Private Address	Public Address
iGS Server	10.10.40.216	
iWS Server	10.10.40.222	
NTP Server	10.1.1.9	
NTP Server	10.10.40.5	
iCMS Communications Server	10.10.40.222	

Page: 1

General

Name
iWS

Type
iWS Server

iWS Server Settings

Private Address
10.10.40.222

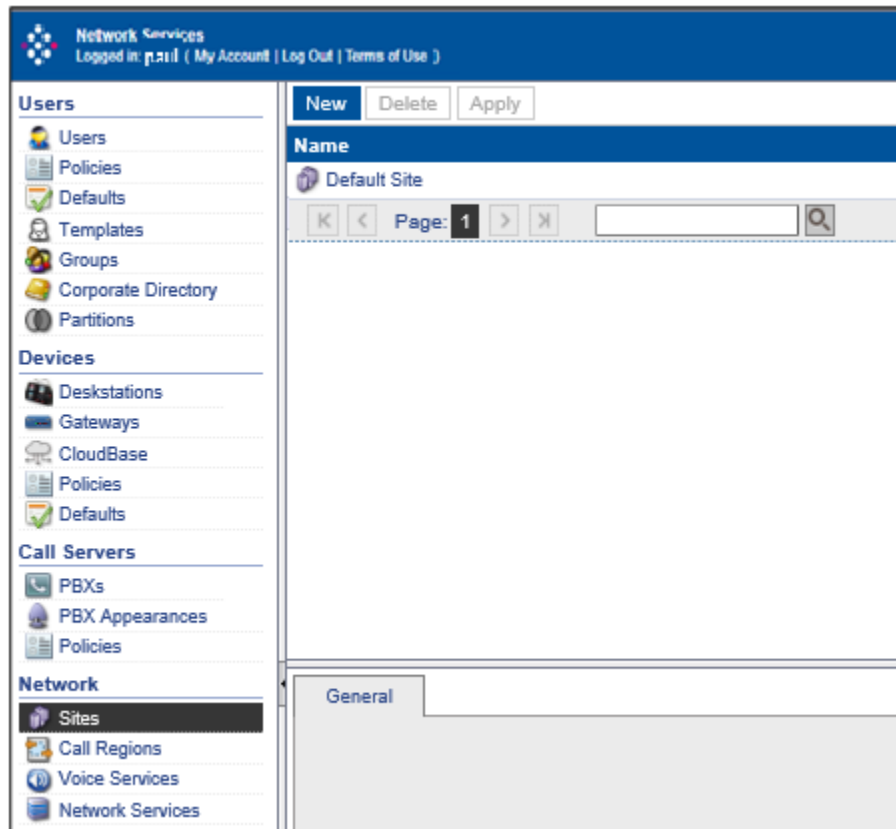
Public Address

IPv6 Address

7.5. Creating Site and Call Region

A site represents the location where the Speakerbus iSeries equipment is installed. To create a Site, select **Network** → **Sites** in the left pane, click **New**.

Note 1: A **Default Site** is available and can be used if required.



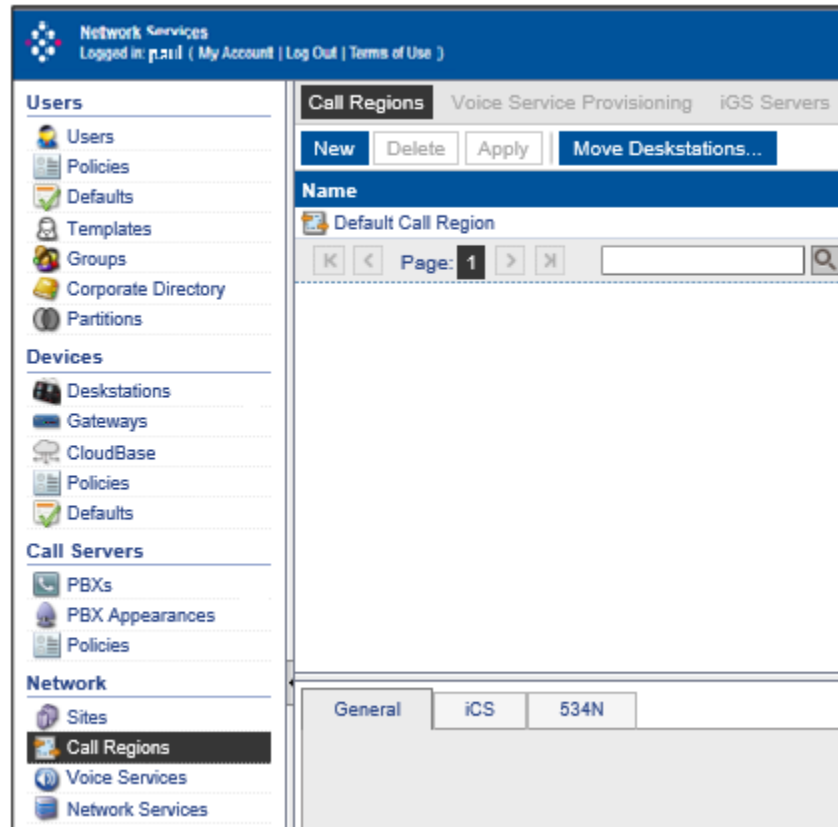
Complete the following fields (not shown).

- **Name** Enter a descriptive name for the site.
- **Remote Site** Leave unticked for most cases.

Click OK once completed.

A call region represents part of an organization's network over which all devices associated with the call region can communicate call audio and call signaling. To create a Call Region, select **Network** → **Call Region** in the left pane, click **New**.

Note 2: A **Default Call Region** is available and can be used if required.



Complete the following fields (not shown):

- **Name** Enter a descriptive name for the call region.
- **Partition Checking** Leave unticked for most cases.
- **Priority for P2P** Leave unticked for most cases.
- **IGMP Auto-leave** Leave unticked for most cases.
- **DMVS Intercom Calls** Leave unticked for most cases.

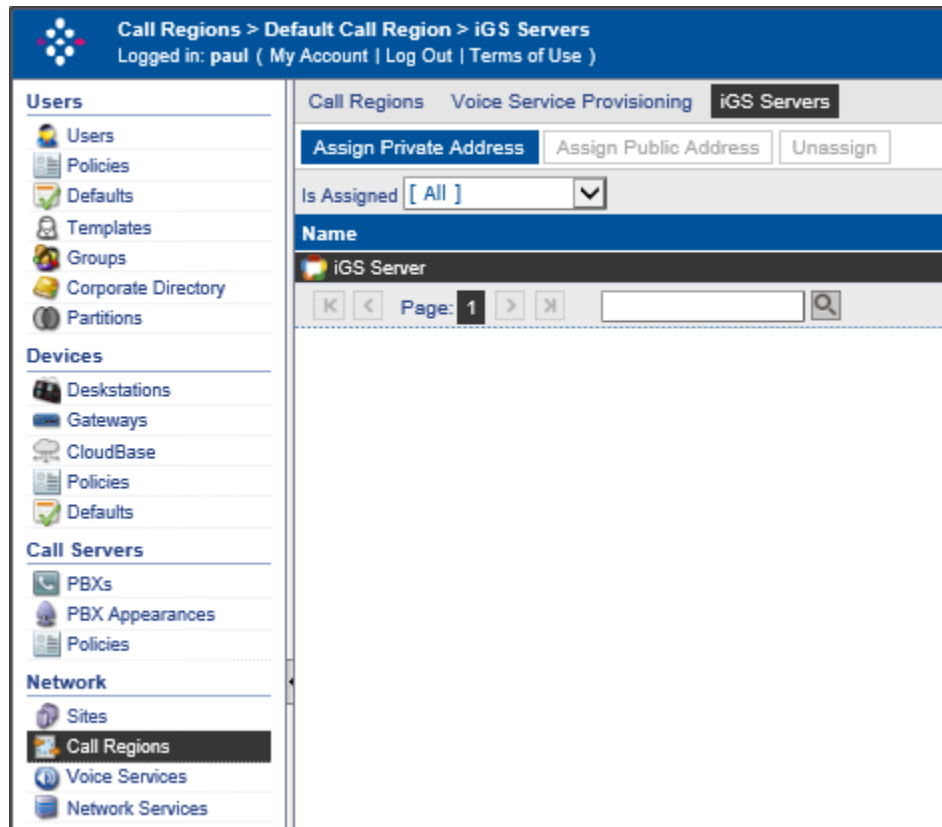
Note: Refer to the *Speakerbus iManager Administrator's Guide*.

Click OK once completed.

7.6. Assign iGS Server to a Call Region

iGS Servers are used to support connections between the ARIA deskstation and ARIA session controllers (either hosted on iTurret devices or CloudBase Servers (iCB`s)).

To create a Site, select **Network** → **Call Regions** in the left pane, select the Call Region already created (or the default) and select **Call Regions** in the top bar (as seen below).

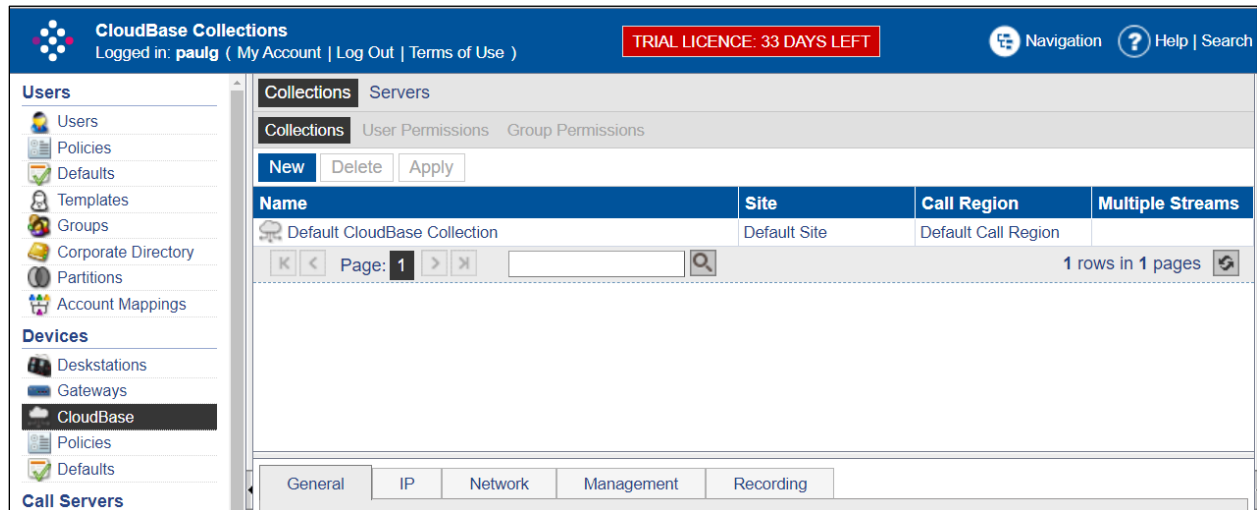


Select the iGS Server in the list and click **Assign Private Address**, to assign the iGS to the Call Region.

Note: Refer to the *Speakerbus iManager Administrator`s Guide*.

7.7. Create CloudBase Collection

Collections provide a way to group CloudBase servers (iCB) together to form resilience and capacity within the CloudBase network. All CloudBase servers (and the iDUCX devices running on those servers) inherit settings from their associated collection. Select **Device** → **CloudBase** in the left pane, click **New**.



Confirm the following fields are set.

General Tab

- Name Enter a descriptive name for the call region.
- Site Set with what created in **Section 7.5**.
- Call Region Set with what created in **Section 7.5**.

IP Tab

- NTP Server Set with what created in **Section 7.4**.

Network Tab

- SbRTP Media Policy is set to Default SbRTP.
- RTP Media Policy is set to Default RTP Media & SIP (use the link to go to the policy to change the audio codec used, default is G.711 A-law).
- Ethernet Ports Policy is set to Default Ethernet Ports.
- Time zone is set to the relevant time zone.

Management Tab

- iCMS Communication Policy is set to the default.
- iCMS Communication Server is set to Auto-Locate iCMS if using DHCP / DNS.
- Enable Live Updates is ticked.

Note: Refer to the *Speakerbus iManager Administrator's Guide*.
Click **Apply** once completed.

7.8. Check Device Defaults

The default configuration is used when a new device is created either from an auto-announce or from iManager. Select **Device** → **Defaults** in the left pane.

The screenshot shows the 'Device Defaults' configuration interface. The left sidebar contains a navigation menu with categories like 'Users', 'Policies', 'Defaults', 'Templates', 'Groups', 'Corporate Directory', 'Partitions', 'Account Mappings', 'Devices', 'Deskstations', 'Gateways', 'CloudBase', 'Policies', 'Defaults', and 'Call Servers'. The 'Defaults' option under 'Devices' is selected. The main content area has an 'Apply' button at the top and several tabs: 'General', 'CloudBase', 'IP', 'Network', 'Management', 'Deskstation', 'Gateway', and 'Recording'. The 'General' tab is currently selected. It contains three dropdown menus: 'Site' (set to 'Default Site'), 'Call Region' (set to 'Default Call Region'), and 'IG330 Configuration Mode' (set to 'Device Web Page'). Below these is a 'Firmware' section with a table of filenames. The table has columns for 'Type', 'Enabled', 'Filename', and 'File Server'. The rows are for iD100, iD101, and iD114. All 'Enabled' checkboxes are unchecked, and all 'File Server' dropdowns are set to '[None]'.

Type	Enabled	Filename	File Server
iD100	<input type="checkbox"/>	iD100_UG_x_xxx_x_x.r0	[None]
iD101	<input type="checkbox"/>	iD101_UG_x_xxx_x_x.r0	[None]
iD114	<input type="checkbox"/>	iD114_UG_x_xxx_x_x.r0	[None]

Confirm the following fields are set.

General Tab

- Site Set with what created in **Section 7.5**.
- Call Region Set with what created in **Section 7.5**.

CloudBase Tab

- CloudBase Collection Set with what created in **Section 7.7**.
- Starting iDUCX MAC Address Set this with the MAC Address for the first iDUCX.

IP Tab

- NTP Server Set with what created in **Section 7.4**.

Network Tab

- SbRTP Media Policy is set to Default SbRTP.
- RTP Media Policy is set to Default RTP Media & SIP (use the link to go to the policy to change the audio codec used, default is G.711 A-law).
- Ethernet Ports Policy is set to Default Ethernet Ports.
- Time zone is set to the relevant time zone.

Management Tab

- iCMS Communication Policy is set to the default.
- iCMS Communication Server is set to Auto-Locate iCMS if using DHCP / DNS.
- Enable Live Updates should be ticked.

Note: Refer to the *Speakerbus iManager Administrator's Guide*.
Click **Apply** once completed.

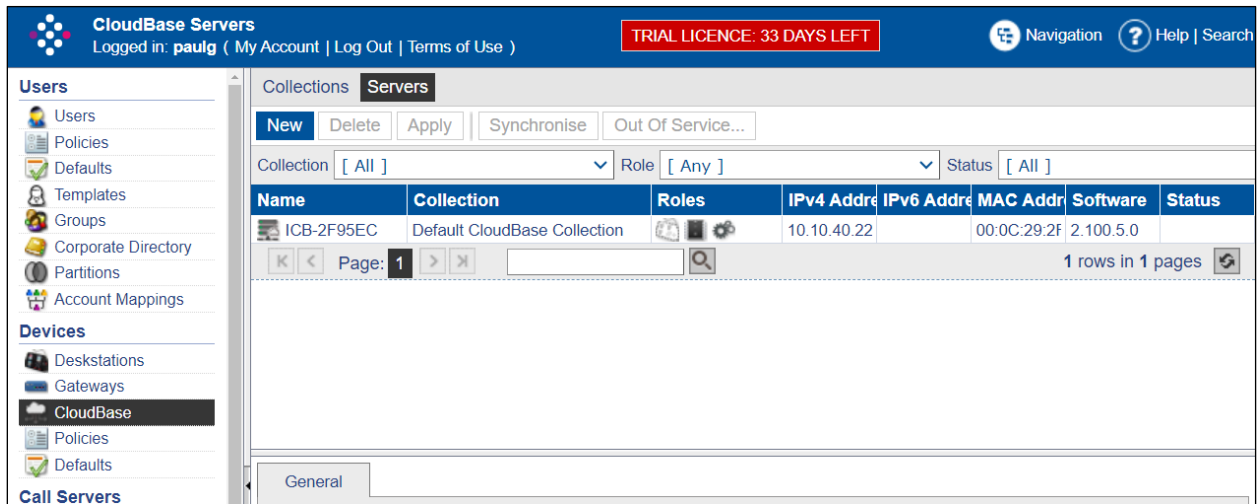
7.9. Announce iCB Server

A CloudBase server (iCB) is the host for one or more iDUCX deskstation devices. The iCB server(s) will automatically announce to the iCMS server if the appropriate **DHCP** record are created prior to the iCB server(s) being powered up.

Confirm the iCB server you have installed and powered up is visible in the list by going to **Devices → Cloudbase → Servers**. Verify the following:

- The iCB server has announced into the correct CloudBase Collection.
- It has the correct ip address (confirm via SSH connection onto the iCB Server).
- It has the correct MAC address of the server (confirm via SSH connection onto the iCB Server).
- It has the correct Software version (confirm via SSH connection onto the iCB Server).

Note: Later three items above are not in the screenshot below.



The screenshot shows the CloudBase Servers management interface. The top navigation bar includes the CloudBase logo, user information (Logged in: paulg), a trial license warning (TRIAL LICENCE: 33 DAYS LEFT), and navigation/help links. The left sidebar contains a tree view with categories: Users, Devices, and Call Servers. The 'Servers' tab is selected in the main content area. Below the tab, there are filters for Collection (All), Role (Any), and Status (All). A table lists the servers, with one entry visible: ICB-2F95EC, belonging to the Default CloudBase Collection, with IP address 10.10.40.22 and MAC address 00:0C:29:2F. The table also shows columns for Roles, IPv6 Address, and Software version. The bottom of the interface shows a 'General' tab and a 'Page: 1' indicator.

Name	Collection	Roles	IPv4 Address	IPv6 Address	MAC Address	Software	Status
ICB-2F95EC	Default CloudBase Collection		10.10.40.22		00:0C:29:2F	2.100.5.0	

7.10. Set up iDUCX Devices under the iCB Server

To create a number of iDUCX devices, go to **Devices → Cloudbase → Servers**, select the iCB server in the list (as seen in below).

General Tab

- Device Server Role Ticked (provides the ability to add the iDUCX count)
- DSP Server Role Ticked (provides the ability for iDUCX to support audio)
- Codec Server Role Ticked (provides the ability for iDUCX to support complex codecs)

Once the above are ticked, three more tabs will show called Device Server, DSP Server and Codec Server.

The screenshot displays the 'CloudBase Servers' management console. The left sidebar contains navigation menus for Users, Devices, Call Servers, Network, Security, and System. The main area shows the 'Servers' collection with a table listing servers. The selected server, 'ICB-2F95EC', is shown in detail under the 'General' tab. The configuration includes fields for Name, Collection, MAC Address, IPv4 Address, IPv6 Address, Software Version, Site, and Call Region. The 'Device Server Role', 'DSP Server Role', and 'Codec Server Role' are all checked. The 'iCMS Communications' section shows the 'Last Contacted Server' and 'Last in Contact' details.

CloudBase Servers
Logged in: paulg (My Account | Log Out | Terms of Use)
TRIAL LICENCE: 33 DAYS LEFT

Users
Users
Policies
Defaults
Templates
Groups
Corporate Directory
Partitions
Account Mappings

Devices
Deskstations
Gateways
CloudBase
Policies
Defaults

Call Servers
PBXs
PBX Appearances
Policies

Network
Sites
Call Regions
Voice Services
Network Services

Security
Administrators
Roles
API Accounts

System

Collections Servers
New Delete Apply Synchronise Out Of Service...
Collection [All] Role [Any] Status []

Name	Collection	Roles	IPv4 Address	IPv6 Address	MAC Address
ICB-2F95EC	Default CloudBase Coll		10.10.40.226		00:0C:29:2F:95:EC

Page: 1

General Device Server DSP Server Codec Server

General:

Name: ICB-2F95EC
Collection: Default CloudBase Collection
MAC Address: 00:0C:29:2F:95:EC
Device Server Role: ☒
DSP Server Role: ☒
Codec Server Role: ☒
IPv4 Address: 10.10.40.226
IPv6 Address:
Software Version: 2.100.5.0
Site: Default Site
Call Region: Default Call Region

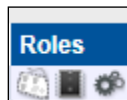
iCMS Communications:

Last Contacted Server: WIN-N7IVMBL3M1E
Last in Contact: 21/06/2023 12:03:35

Select **Device Server** tab. Set **Device Count** to the required number of IDUCX (refer to Speakerbus documentation for correct count values).

General	Device Server	DSP Server	Codec Server
Device Count <input type="text" value="2"/>			
Primary DSP Server [Auto-Locate] ▼			
Backup DSP Server [Auto-Locate] ▼			

Once this is complete the three Roles icons on the main list should appear below.



The following under the Status column should also be observed, this means the iCB is out of sync and needs to sync. Do this by clicking the **Synchronise** button.



Note: Refer to the *Speakerbus iManager Administrator's Guide*.

Click APPLY once completed.

7.11. Observe iCB Server and iDUCX Virtual Deskstation

The iCB Server should register using the CloudBase settings (which have been set up in the preceding sections above). To view the settings, select **Devices** → **Cloudbase** in the left pane. In the **Network** tab, verify the following are configured.

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

The screenshot displays the Avaya CloudBase Collections web interface. The top header shows the user is logged in as 'paulg' and has a trial license with 33 days left. The left sidebar contains navigation menus for Users, Devices, Call Servers, and Network. The 'CloudBase' option under the Devices menu is selected. The main content area shows the 'Collections' tab with a table listing the 'Default CloudBase Collection'. Below the table, the 'Network' tab is active, displaying configuration settings for the selected collection.

Name	Site
Default CloudBase Collection	Default Site

Page: 1

General	IP	Network	Management	Recording
SbRTP Media Policy: Default SbRTP				
RTP Media Policy: Avaya TCP RTP Media & SIP				
VLAN: [None]				
Time Zone: Europe: London				
Dial Tone Locale: UK				

Click on the **Devices → Deskstations**, select the iDUCX required. Under the **General** tab, ensure that the appropriate **CloudBase Collection** is chosen, this should be that shown on the previous page.

The screenshot displays the Avaya Deskstations management console. The left sidebar contains navigation menus for Users, Devices, Call Servers, Network, Security, and System. The main area shows a table of deskstations with columns for Name, Site, Call Region, Type, IP Address, MAC Address, Firmware, Seated User, and Status. The device 'iducx-FF0100' is selected, and its configuration details are shown in the 'General' tab.

Name	Site	Call Region	Type	IP Address	MAC Address	Firmware	Seated User	Status
id808-00F4EF	Default Site	Default Call F	iTurret	10.10.40.207	00:05:83:00:F	4.100.5.0	Avaya User 3	
id808-00F4F1	Default Site	Default Call F	iTurret	10.10.40.213	00:05:83:00:F	4.100.5.0		
id808-00F515	Default Site	Default Call F	iTurret	10.10.40.186	00:05:83:00:F	4.100.5.0		
iducx-FF0100	Default Site	Default Call F	iDUCX	10.10.40.223	02:05:83:FF:01:00	4.100.5.0		
iducx-FF0101	Default Site	Default Call F	iDUCX	10.10.40.197	02:05:83:FF:01:00	4.100.5.0		

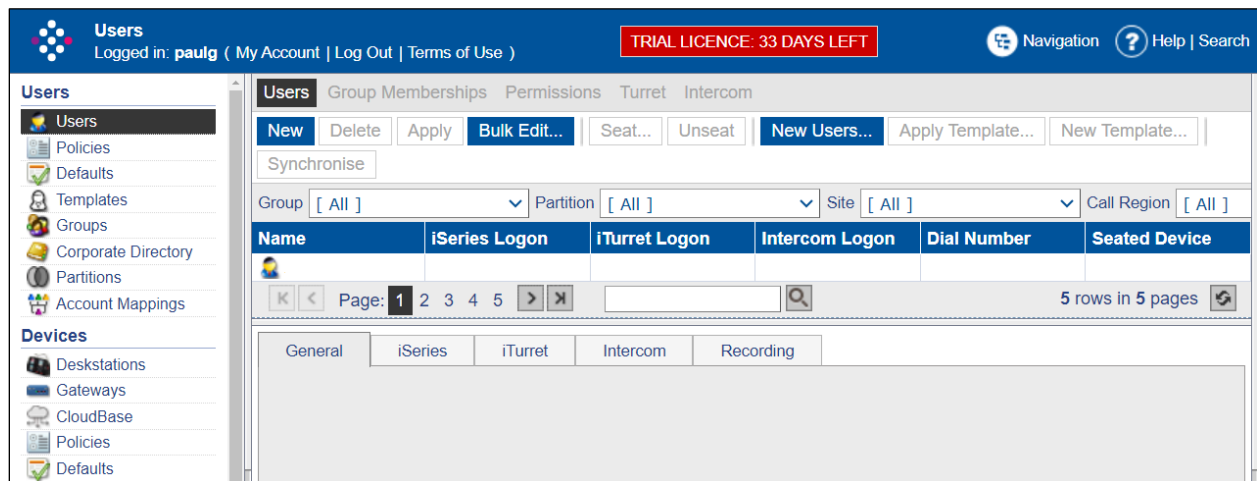
Configuration details for the selected device (iducx-FF0100):

- Name: iducx-FF0100
- Type: iDUCX
- MAC Address: 02:05:83:FF:01:00
- Firmware Version: 4.100.5.0
- Site: Default Site
- Call Region: Default Call Region
- CloudBase Collection: Default CloudBase Collection
- CloudBase Server: ICB-2F95EC
- Additional Info #1:
- Additional Info #2:

Seating Information: Seated User: No seated user

7.12. Create Users

To create a User, select **Users** → **Users**, click **New**.



Confirm the following fields are set.

General Tab

- **Name** Enter a descriptive name for the call region.
- **Privileges Policy** This should be set to the default in **Section 7.2**.
- **Preferences Policy** This should be set to the default in **Section 7.2**.

iTurret Tab

- **Logon Name** Enter a relevant logon name (8 – 16 characters in length).
- **Logon Password** Enter a relevant logon password.
- **Verify Password** Enter a relevant logon password (should match above).
- **Voicemail Policy** This should be set to the policy in **Section 7.2**.
- **All other areas can be left at defaults** (refer to the *Speakerbus iManager Administrator's Guide*).

Note: Refer to the *Speakerbus iManager Administrator's Guide*.

Click OK once completed.

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

- **Voicemail Policy** Select the voicemail policy as configured in **Section 7.2**.
- **Move to Idle Handset Mode** Select **Move Call** from the drop-down list.
- **Enable Latching** Tick **Group Button 1, 2, 3 and 4**.

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

General	iSeries	iTurret	Intercom	Recording															
<div> <div> iTurret: Logon Name <input type="text" value="avayauser1"/> <input type="button" value="Change Password..."/> Voicemail Policy <input type="text" value="Galway Voicemail"/> </div> <div> Group Talk Settings: <table> <thead> <tr> <th></th> <th>ARIA/AYRE Label</th> <th>Latched</th> </tr> </thead> <tbody> <tr> <td>Group 1</td> <td><input type="text" value="Group Talk 1"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Group 2</td> <td><input type="text" value="Group Talk 2"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Group 3</td> <td><input type="text" value="Group Talk 3"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Group 4</td> <td><input type="text" value="Group Talk 4"/></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table> </div> </div>						ARIA/AYRE Label	Latched	Group 1	<input type="text" value="Group Talk 1"/>	<input checked="" type="checkbox"/>	Group 2	<input type="text" value="Group Talk 2"/>	<input checked="" type="checkbox"/>	Group 3	<input type="text" value="Group Talk 3"/>	<input checked="" type="checkbox"/>	Group 4	<input type="text" value="Group Talk 4"/>	<input checked="" type="checkbox"/>
	ARIA/AYRE Label	Latched																	
Group 1	<input type="text" value="Group Talk 1"/>	<input checked="" type="checkbox"/>																	
Group 2	<input type="text" value="Group Talk 2"/>	<input checked="" type="checkbox"/>																	
Group 3	<input type="text" value="Group Talk 3"/>	<input checked="" type="checkbox"/>																	
Group 4	<input type="text" value="Group Talk 4"/>	<input checked="" type="checkbox"/>																	
<div> Preferences: Move To Idle Handset <input type="text" value="Move Call"/> Auto Hold/Clear <input type="text" value="Off"/> Answer On Idle Handset <input type="text" value="Off"/> Handset Privacy Default <input type="text" value="Off"/> Double-Tap Speaker To Handset <input checked="" type="checkbox"/> Auto-Hide Menu <input type="checkbox"/> Enable Key Press Tones <input type="checkbox"/> Enable Loud Listen Mode <input type="checkbox"/> Intercom Audio Device <input type="text" value="Handset"/> </div>																			

Repeat the previous steps to add more users.

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

Users	Group Memberships	Voice Services	Speed Dials	PBX Appearances	Alerts	Personal Dir.	iTurret Layout
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Apply"/> <input type="button" value="Seat..."/> <input type="button" value="Unseat"/> <input type="button" value="New Users..."/> <input type="button" value="Apply Template..."/> <input type="button" value="New Template..."/> <input type="button" value="Synchronise"/>							
Group <input type="text" value="[All]"/> Partition <input type="text" value="[All]"/> Site <input type="text" value="[All]"/> Call Region <input type="text" value="[All]"/>							
Name <div> <input checked="" type="checkbox"/> Avaya User 1 <input type="checkbox"/> Avaya User 2 <input type="checkbox"/> Avaya User 3 </div>							
Page: 1 of 1 Rows: 3 <input type="button" value="Reload"/> <input type="text" value="Find"/>							

7.13. Create iCS PBX (SIP Server)

To create a PBX, select **Call Servers** → **PBXs**, click **New**.

The screenshot shows the Avaya iManager web interface for configuring PBXs. The top navigation bar includes the 'PBXs' title, a user login 'paulg', and a 'TRIAL LICENCE: 33 DAYS LEFT' warning. The left sidebar contains a tree view with categories: Users (Users, Policies, Defaults, Templates, Groups, Corporate Directory, Partitions, Account Mappings), Devices (Deskstations, Gateways, CloudBase, Policies, Defaults), and Call Servers (PBXs, PBX Appearances, Policies). The 'PBXs' option under 'Call Servers' is selected. The main content area has a sub-header with 'PBXs', 'Dial Plan', 'SIP Trunk', and 'RTP Connections'. Below this is a row of action buttons: 'New', 'Delete', 'Apply', 'Export', 'Synchronise', 'Out Of Service...', and 'Create SIP Trunks...'. A table with the following headers is displayed: 'Name', 'Type', 'Address', 'IPv6 Address', and 'Node #1 Address'. Below the table, a 'General' tab is active, showing a large, empty text area for configuration details.

Complete the following fields (not shown):

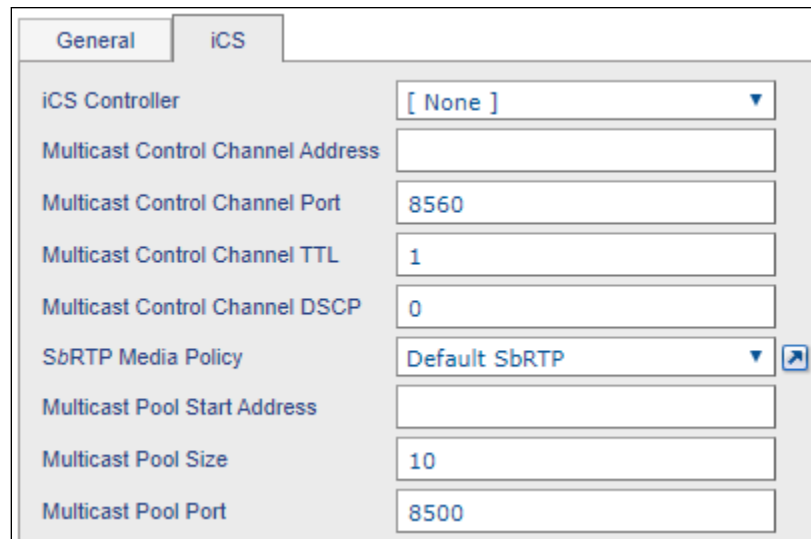
- **Name** Enter a descriptive name for the SIP/PBX server.
- **Type** Select **Speakerbus** from the dropdown list.
- **Port** Enter **5060**.
- **Resilience Mode** **Refer to the Speakerbus iManager Administrator's guide for further details**
- **Registrar Address** Enter the IP address of the Primary Session Manager.
- **RTP Media & SIP Policy** **Set with the default which is set for UDP and G.711 A-law (this will be changed if running in TCP mode see section 7.xx)**
- **iCMS Communications Server** Enter the appropriate server from the dropdown list.
- **NTP Server** Enter the appropriate server from the dropdown list.

Note: Refer to the *Speakerbus iManager Administrator's Guide*.

Click OK once completed.

7.14. Assign iCS to Call Region

To assign an iCS server into the created Call Region (from **Section 7.5**), select **Network → Call Regions** (not shown), select the Call Region to be used and select the **iCS** tab.



The screenshot shows the 'iCS' configuration tab. It contains the following fields and values:

Field	Value
iCS Controller	[None]
Multicast Control Channel Address	
Multicast Control Channel Port	8560
Multicast Control Channel TTL	1
Multicast Control Channel DSCP	0
SbRTP Media Policy	Default SbRTP
Multicast Pool Start Address	
Multicast Pool Size	10
Multicast Pool Port	8500

Complete the following fields:

- **iCS Controller** Set this with the iCS created in **Section 7.13**.
- **Multicast Control Channel Address** Set this with a valid multicast address.
- **Multicast Control Channel TTL** Change this value to higher than 1 if traversing multiple network nodes.
- **SbRTP Media Policy** This should be set with **Default SbRTP**.
- **Multicast Pool Start Address** Set this with the multicast start address within the range for the MCC Address above.

Note: Refer to the *Speakerbus iManager Administrator's Guide*.

Click **APPLY** once completed.

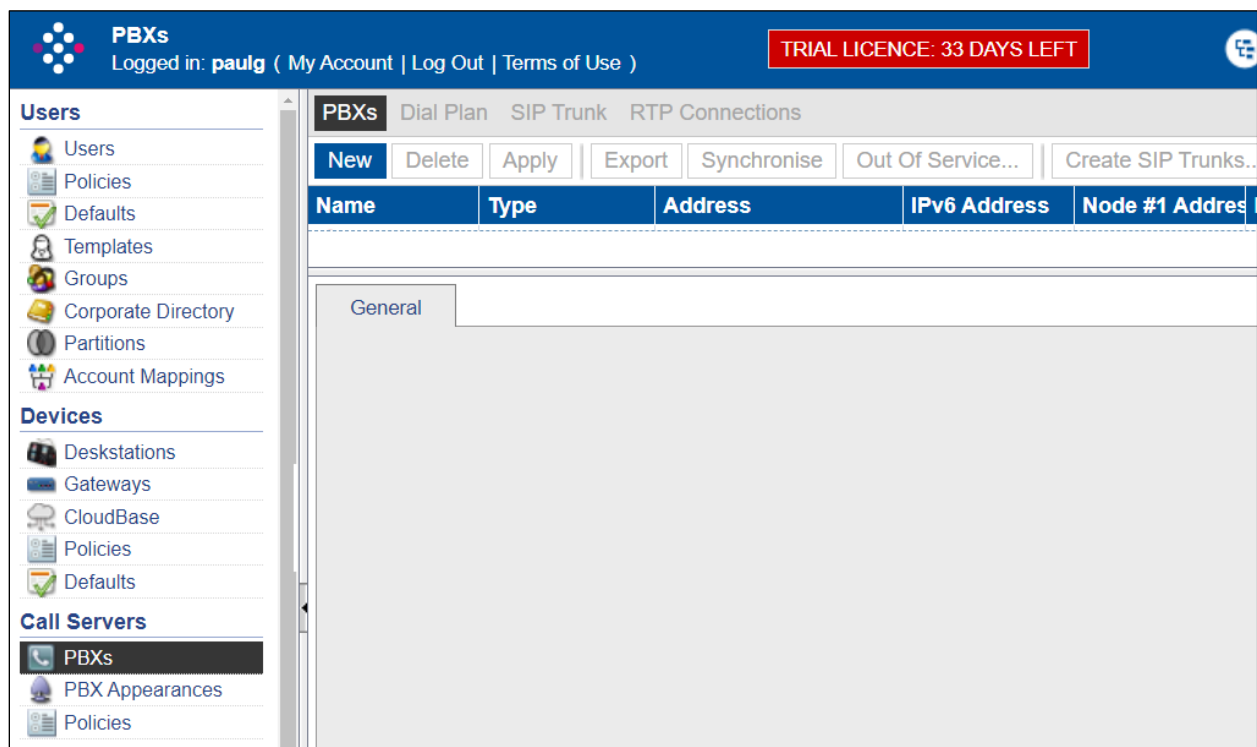
The iCS Server that was added to the above Call Region will now go out of sync, this can be left to auto-sync or can be manually synchronized as follows. Navigate to **Call Servers → PBXs**, then select the iCS server(s) and click the **Synchronise** button (not shown).

Once the profile has been sent to the Speakerbus iCS Server, navigate onto the server by clicking the ip address link seen in section 7.13, this takes you onto the server, login (ask for details of login and password), then press install configuration and follow prompts.

Note: Refer to the relevant *Speakerbus Administrator's Guide*.

7.15. Create Avaya PBX (SIP Server)

To create a PBX, select **Call Servers** → **PBXs**, click **New**.



Complete the following fields (shown on next page):

- **Name** Enter a descriptive name for the SIP/PBX server.
- **Type** Select **Avaya** from the dropdown list.
- **Port** Enter **5060**.
- **Registrar Address** Enter the IP address of the Primary Session Manager.
- **SIP Domain** Enter the appropriate SIP Domain.
- **SIP Signaling Protocol** This can be set to **UDP** or **TCP**.

Note 1: A server locator record (SRV) for the registrar address and SIP domain may be created on DNS if the registrar address is set to **greanep.sil6.avaya.com**, in the example below it will not be required. Refer to the *Speakerbus iManager Administrator's Guide* for the correct configuration of DNS.

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

General	Inbound	Outbound
General:		
Name	Avaya Aura 10.2	
Type	Avaya	
Port	5060	
Avaya PBX Settings:		
Registrar Address	10.10.40.12	
Registrar IPv6 Address		
SIP Domain	greanep.sil6.avaya.com	
SIP Signalling Protocol	UDP	
Secondary PBX	[None]	
Tertiary PBX	[None]	
Registration Delay (s)	30	
Registration Timeout (s)	30	
Registration Attempts	3	
Ad-Hoc Conferencing	<input type="checkbox"/>	

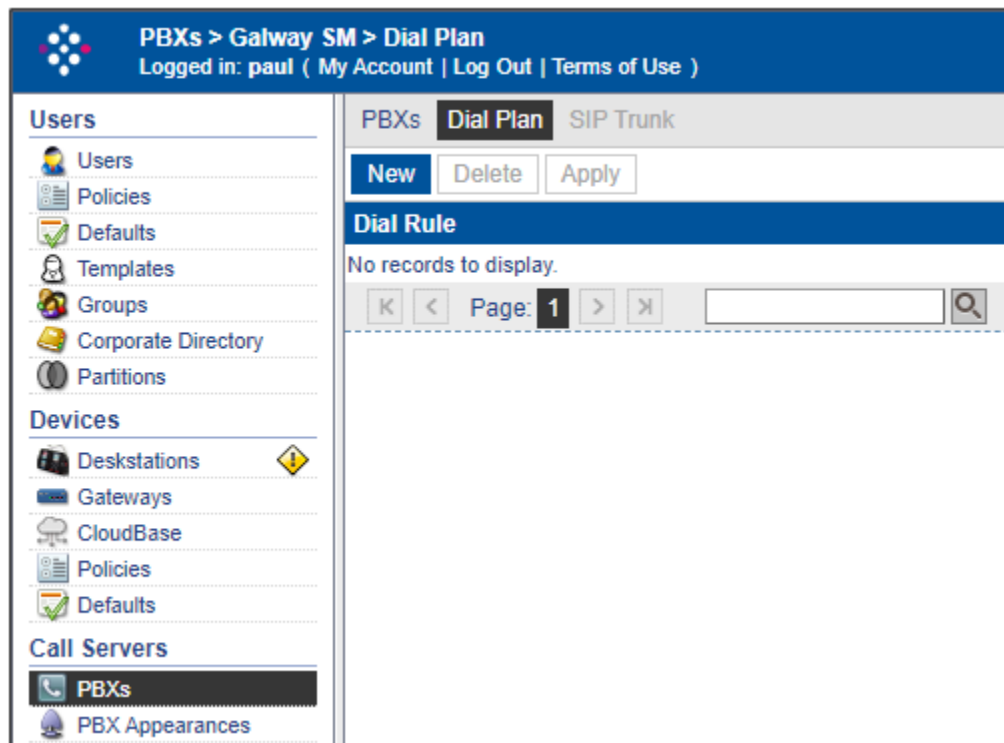
The **Outbound** and **Inbound** tabs are left with their default values, Click **OK** (not shown).

General	Inbound	Outbound
Internal:		
Length	4	
Prefix		
Local:		
Length	4	
Prefix		
National:		
Length	10	
Prefix		
International:		
Prefix		

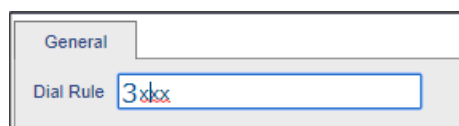
General	Inbound	Outbound
Internal:		
Length	4	
Prefix		
Local:		
Length	6	
Prefix		
National:		
Length	11	
Prefix		
International:		
Access Code	00	
Prefix		

7.16. Create Dial Plan

To create a PBX specific dial plan, select **Call Servers** → **PBXs**, select the **Dial Plan** tab, click **New**.



Under the **General** tab fill in the **Dial Rule**. Press **OK** when completed.



Repeat this for all valid extension formats.

7.17. Create Call and Privacy Appearances

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

7.17.1. Create Call Appearances

To create the main appearance, click **Call Servers** → **PBX Appearances** in the left pane, click on **New**.

The screenshot shows the 'PBX Appearances' management page. The left sidebar contains a navigation tree with categories: Users, Devices, Call Servers, and Network. Under 'Call Servers', 'PBX Appearances' is selected. The main content area has tabs for 'PBX Appearances', 'User Permissions', and 'Group Permissions'. Below the tabs are buttons for 'New', 'Delete', 'Apply', 'Assign Ownership...', and 'Clear Ownership'. There are also dropdown menus for 'PBX' (set to '[All]') and 'Type' (set to '[All]'). A table lists the appearances, with 'Speakerbus User 1' highlighted. The table has a 'Name' header. At the bottom, there is a pagination bar showing 'Page: 1' and a search icon.

Name
Matt Cheattle
Neil Higgs
Paul Greaney
Russell McLean
Speakerbus User PV1
Speakerbus User PV1
Speakerbus User PV2
Speakerbus User PV2
Speakerbus User 1
Speakerbus User 2
Speakerbus User 3
Speakerbus User 4
Speakerbus User 5
Tim Game

Select the PBX created in **Section 7.5** (in this case **Avaya Aura 10.2**), then select the **Type** of appearance to be created (which is **Call** in this case) and configure the following under the **General** tab:

- Provide a descriptive name for the appearance in the **Name** field, such as the extension or user's name.
- Set the **Long Label** field to the label that will be displayed for the call appearance button on the iDUCX deskstation. The **Address** field should also be set to the appearance extension.
- Set the **Maximum Appearance** field to the number of call appearances configured on the station in System Manager (the number of call appearance buttons dictates the number of calls on the system the user can have directed to them). When all of the call appearances are not idle the user is considered busy, and no further calls can be routed to them. Up to a maximum of 10 call appearances may be configured on Communication Manager for each iDUCX deskstation.
- Check the **Message Indication** checkbox for voice mail purposes and the **Allow Outbound Calls**.
- The **Authentication Name** and **Authentication Password** fields should be set to the extension and password configured on System Manager in **Section 6.3**. These are the credentials that the Speakerbus ARIA iDUCX virtual deskstation will use to authenticate and register with Session Manager. Use the default values for the other fields. Click **OK** (not shown).

The screenshot shows a configuration window with a 'General' tab. At the top, there are two dropdown menus: 'PBX' set to 'Avaya Aura 10.2' and 'Type' set to 'Call'. Below these is a section titled 'Call Appearance Settings:' containing several fields: 'Name' (Avaya User 1), 'Long Label' (Avaya User 1), 'Address' (3181), 'Maximum PBX Appearances' (3), 'Outbound Calls' (Allow All), 'Message Indication' (checked checkbox), and 'Authentication Name' (3181). At the bottom right of this section is a blue button labeled 'Change PBX Authentication Password...'.

7.17.2. Create Privacy Appearances

Repeat the procedure in 7.17.1 for the two corresponding privacy appearances. Click the **New** button to add another appearance. In the **General** tab select the **PBX** created in **Section 7.5**, set the **Type** field to **Privacy 1** and complete the **Address**, **Authentication Name** and **Authentication Password** fields. The last two fields should be identical to the setup in System Manager for registration to occur. Press **OK** (not shown) to commit the created appearance.

The screenshot shows the Avaya System Manager interface. On the left is a navigation pane with categories: Users, Devices, Call Servers, and Network. The 'PBX Appearances' link under 'Call Servers' is selected. The main area displays a table of PBX Appearances and a 'General' tab for editing a new appearance.

Name	PBX	Long Label	Address	Type	Owner
Avaya User 1 PV1	Avaya Aura 10.2	Avaya User 1 PV1	3191	Privacy 1	Avaya User 1
Avaya User 1 PV2	Avaya Aura 10.2	Avaya User 1 PV2	3192	Privacy 2	Avaya User 1
Avaya User 2	Avaya Aura 10.2	Avaya User 2	3182	Call	Avaya User 2
Avaya User 3	Avaya Aura 10.2	Avaya User 3	3183	Call	Avaya User 3

Page: 1 2 8 rows in 2 pages

General

PBX: Avaya Aura 10.2

Type: Privacy 1

Privacy Appearance Settings:

Name: Avaya User 1 PV1

Long Label: Avaya User 1 PV1

Address: 3191

Authentication Name: 3191

Change PBX Authentication Password...

Similar details for the second privacy user.

This screenshot is similar to the previous one, but it shows the configuration for 'Privacy 2'.

Name	PBX	Long Label	Address	Type	Owner
Avaya User 1 PV1	Avaya Aura 10.2	Avaya User 1 PV1	3191	Privacy 1	Avaya User 1
Avaya User 1 PV2	Avaya Aura 10.2	Avaya User 1 PV2	3192	Privacy 2	Avaya User 1
Avaya User 2	Avaya Aura 10.2	Avaya User 2	3182	Call	Avaya User 2
Avaya User 3	Avaya Aura 10.2	Avaya User 3	3183	Call	Avaya User 3

Page: 1 2 8 rows in 2 pages

General

PBX: Avaya Aura 10.2

Type: Privacy 2

Privacy Appearance Settings:

Name: Avaya User 1 PV2

Long Label: Avaya User 1 PV2

Address: 3192

Authentication Name: 3192

Change PBX Authentication Password...

7.18. Assign User Permissions

Appearance permissions must be assigned to the created users. Select **Call Servers** → **PBX Appearances** in the left pane, select the **Call Appearance** from the list, and select the **User Permissions** tab at the top of the page.

Name	User Permission	Group Permission	Seated Site	Seated Call Region	Seated Device	In Use
Avaya User 1	Allow					
Avaya User 2	Use group	Deny				
Avaya User 3	Use group	Deny	Default Site	Default Call Region	id808-00F4EF	
Trial User 1	Use group	Deny				
Trial User 2	Use group	Deny				

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

Name	User Permission	Group Permission	Seated Site	Seated Call Region	Seated Device	In Use
Avaya User	Use group	Deny				
Avaya User 1	Allow		Default Site	Default Call Region	iducx-FF0100	
Avaya User 2	Allow					
Avaya User 3	Use group	Deny	Default Site	Default Call Region	id808-00F4EF	
Trial User 1	Use group	Deny				
Trial User 2	Use group	Deny				

7.19. Assign Ownership

Appearance ownership must be assigned to a user as it enables the Speakerbus ARIA iDUCX virtual deskstation to distinguish between the owner of the call or appearance as opposed to someone who is bridged on to that appearance. Select **Call Servers** → **PBX Appearances** in the left pane. Select the appropriate user in the main window and click on the **Assign Ownership** button.

The screenshot shows the Avaya DevConnect interface. On the left is a navigation pane with categories: Users, Devices, Call Servers, Network, and Security. Under 'Call Servers', 'PBX Appearances' is selected. The main window has tabs for 'PBX Appearances', 'User Permissions', and 'Group Permissions'. The 'PBX Appearances' tab is active, showing a table of appearances and a 'General' settings panel for the selected 'Avaya User 1'.

Table: PBX Appearances

Name	PBX	Long Label	Address	Type	Owner
6000	Speakerbus iCS	6000	6000	Call	Trial User 1
6001	Speakerbus iCS	6001	6001	Call	Trial User 2
6002	Speakerbus iCS	6002	6002	Call	
Avaya User 1	Avaya Aura 10.2	Avaya User 1	3181	Call	Avaya User 1
Avaya User 1 PV1	Avaya Aura 10.2	Avaya User 1 PV1	3191	Privacy 1	Avaya User 1

General Settings for Avaya User 1:

- PBX: Avaya Aura 10.2
- Type: Call
- Call Appearance Settings:
 - Name: Avaya User 1
 - Long Label: Avaya User 1
 - Address: 3181
 - Maximum PBX Appearances: 3
 - Outbound Calls: Allow All
 - Message Indication: ☒
 - Authentication Name: 3181

[Change PBX Authentication Password...](#)

Filter accordingly and select the user from the **User to assign ownership to** drop down list. Click **OK**.

The screenshot shows the 'PBX Appearances' management interface. At the top, there are tabs for 'PBX Appearances', 'User Permissions', and 'Group Permissions'. Below the tabs are buttons for 'New', 'Delete', 'Apply', 'Assign Ownership...', and 'Clear Ownership'. There are also dropdown menus for 'PBX' (set to '[All]') and 'Type' (set to '[All]').

Name	PBX	Long Label	Address	Type
6000	Speakerbus iCS	6000	6000	Call
6001	Speakerbus iCS	6001	6001	Call
6002	Speakerbus iCS	6002	6002	Call
Avaya User 1	Avaya Aura 10.2	Avaya User 1	3181	Call
Avaya User 1				Privacy 1

The 'Assign Ownership of PBX Appearance(s)' dialog box is open, showing the following options:

- Filter by Seated Site: [All]
- Filter by Seated Region: [All]
- Filter by User Group: [All]
- Filter by Partition: [All]
- User to assign ownership to: Avaya User 1

At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

7.20. Set Default Appearance

Select **Users** → **Users** in the left pane.

Name	iSeries Logon	iTurret Logon	Intercom Logon	Dial Number	Seated Device
Avaya User 1		avayauser1			
Avaya User 2		avayauser2			
Avaya User 3		avayauser3			id808-00F4EF
Trial User 1		trialuser1			
Trial User 2		trialuser2			

Within the **General** tab fill in the following:

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

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

Name	iSeries Logon	iTurret Logon	Intercom Logon	Dial Number	Seated Device
Avaya User 1		avayauser1			
Avaya User 2		avayauser2			

General	iSeries	iTurret	Intercom	Recording
General:				
Name	Avaya User 1			
Privileges Policy	Default Privileges			
Preferences Policy	Default Preferences			
Default PBX Appearance Type	Call			
Default PBX Appearance	Avaya User 1			
Quiet Office	Disabled			
Handset Push Button Mode	Push to mute			
Cisco Device Name Prefix				
Additional Info #1				
Additional Info #2				
iCS Registration Name	MASTER-1			
Change iCS Registration Password...				

Speaker Channel Settings:	
Latching Type	Tap Latch
Local Dipping	Duplex
Local Dipping Level Reduction	Mute
Audio Restore Delay (s)	0
Paired User	[None]

7.21. Program ARIA Touch Layout Profiles

The programming of the ARIA Touch can be carried out by Speakerbus or Avaya engineer. For information on the types of tiles available and administration of the ARIA Touch tile layouts, refer to the Speakerbus iManager Administrator's Guide.

To add the above appearances to the tiles layout, go to the user and select the Turret, as per the screenshot below.

The screenshot shows the Avaya iManager Users page. The user is logged in as 'paulg'. The page has a navigation bar with 'Users', 'Group Memberships', 'Permissions', 'Turret' (highlighted), and 'Intercom'. Below the navigation bar, there are tabs for 'New', 'Delete', 'Apply', 'Bulk Edit...', 'Seat...', 'Unseat', 'New Users...', 'Apply Template...', and 'New Template...'. A table lists users with columns: Name, iSeries Logon, iTurret Logon, Intercom Logon, and Dial Number. The table contains five rows: Avaya User 1, Avaya User 2, Avaya User 3, Trial User 1, and Trial User 2. The 'iTurret Logon' column shows 'avayauser1', 'avayauser2', 'avayauser3', 'trialuser1', and 'trialuser2' respectively. The 'Page' indicator shows 'Page: 1'.

Click on **Tile Layout** and add the appropriate tiles.

The screenshot shows the Avaya iManager Users > Avaya User 1 > Tile Layout page. The user is logged in as 'paulg'. The page has a navigation bar with 'Users', 'Group Memberships', 'Permissions', 'Turret' (highlighted), and 'Intercom'. Below the navigation bar, there are tabs for 'Key Layout', 'Tile Layout' (highlighted), 'PBX Appearance Ownership', 'Personal Directory', and 'Alerts'. The 'Apply' button is visible. The 'Mode' is set to 'Page Edit'. The 'Page' indicator shows 'Page 1: Page 1'. The page displays a list of tiles with radio buttons and 'New' buttons. The tiles are: Speed Dial, PBX Appearance, Voice Service Appearance, Virtual Private Wire, Call Activity, Intercom Appearance, Soft Group Talk, Speaker Channel, and Handset. The 'Handset' tile is selected. The 'Page' indicator shows 'Page 1: Page 1'. The 'Speaker Page Naming Policy' is set to '[None]'. The 'Speaker Page' indicator shows 'Speaker Page 1: Speaker Page 1'. The 'Page' indicator shows 'Page 1: Page 1'. The 'Page Name' is 'Page 1'. The 'Read-only' checkbox is unchecked.

7.22. Synchronise Deskstations

Any changes made to the profile within iManager will be updated on the iDUCX device after **OK** or **Apply** is pressed. However, some changes will require a synchronization to push the new configuration to the iDUCX without disruption to the user. Select **Devices** → **Deskstations** and select the desired deskstations. Click the **Synchronise** button.

The screenshot displays the iManager web interface for managing Deskstations. The left sidebar contains navigation menus for Users, Devices, Call Servers, Network, and Security. The main content area shows a table of deskstations with columns for Name, Site, Call Region, Type, IP Address, MAC Address, Firmware, Seated User, and Status. Below the table, there are tabs for General, IP, Network, Management, and Recording. The General tab is active, showing fields for Name, Type, MAC Address, Firmware Version, Site, Call Region, CloudBase Collection, CloudBase Server, and Additional Info #1 and #2. A Seating Information section on the right shows the Seated User as 'No seated user'.

Name	Site	Call Region	Type	IP Address	MAC Address	Firmware	Seated User	Status
id808-00F	Default Site	Default Call R	iTurret	10.10.40.207	00:05:83:00:F4:EF	4.100.5.0	Avaya User 3	
id808-00F	Default Site	Default Call R	iTurret	10.10.40.213	00:05:83:00:F4:F1	4.100.5.0		
id808-00F	Default Site	Default Call R	iTurret	10.10.40.186	00:05:83:00:F5:15	4.100.5.0		
iducx-FF0100	Default Site	Default Call R	iDUCX	10.10.40.223	02:05:83:FF:01:00	4.100.5.0		

Page: 1 2 5 rows in 2 pages

General IP Network Management Recording

General:

Name: iducx-FF0100

Type: iDUCX

MAC Address: 02:05:83:FF:01:00

Firmware Version: 4.100.5.0

Site: Default Site

Call Region: Default Call Region

CloudBase Collection: Default CloudBase Collection

CloudBase Server: ICB-2F95EC

Additional Info #1:

Additional Info #2:

Seating Information:

Seated User: No seated user

7.23. Changing to TCP SIP signaling

As Speakerbus now supports both UDP and TCP at the deskstation for SIP signaling, this section details how to change the signaling protocol for the endpoint and iCS servers (Avaya PBX has already been provided in **Section 7.15**).

Navigate to **Devices > Policies** and select the relevant RTP Media & SIP policy outlined in section 7.3 and untick the “**Allow UDP SIP Signaling**” tick box, then press **OK**.

A resync of the iCB server will need to be performed.

The screenshot shows the iManager web interface for configuring Device Policies. The left sidebar contains a navigation tree with categories: Users, Devices, Call Servers, Network, and Security. The 'Policies' option under 'Devices' is selected. The main content area shows the configuration for a policy named 'Default RTP Media & SIP'. The 'General' tab is active, displaying various settings:

- Name:** Default RTP Media & SIP
- Type:** RTP Media & SIP
- RTP Media Settings:**
 - Time To Live: 120
 - DSCP Value: 0
 - RTCP DSCP Value: 0
- SIP RTP Media Settings:**
 - Preferred Codec: G.711 A-Law
 - Preferred Intercom Codec: G.711 A-Law
 - Voice Activity Detection: ☐
 - AYRE Codec: 16KHZ PCM
 - AYRE Voice Activity Detection: ☐
- SIP Signalling Settings:**
 - Allow UDP SIP Signaling: ☐ (This checkbox is currently unchecked, indicating TCP signaling is selected.)
 - DSCP Value: 0

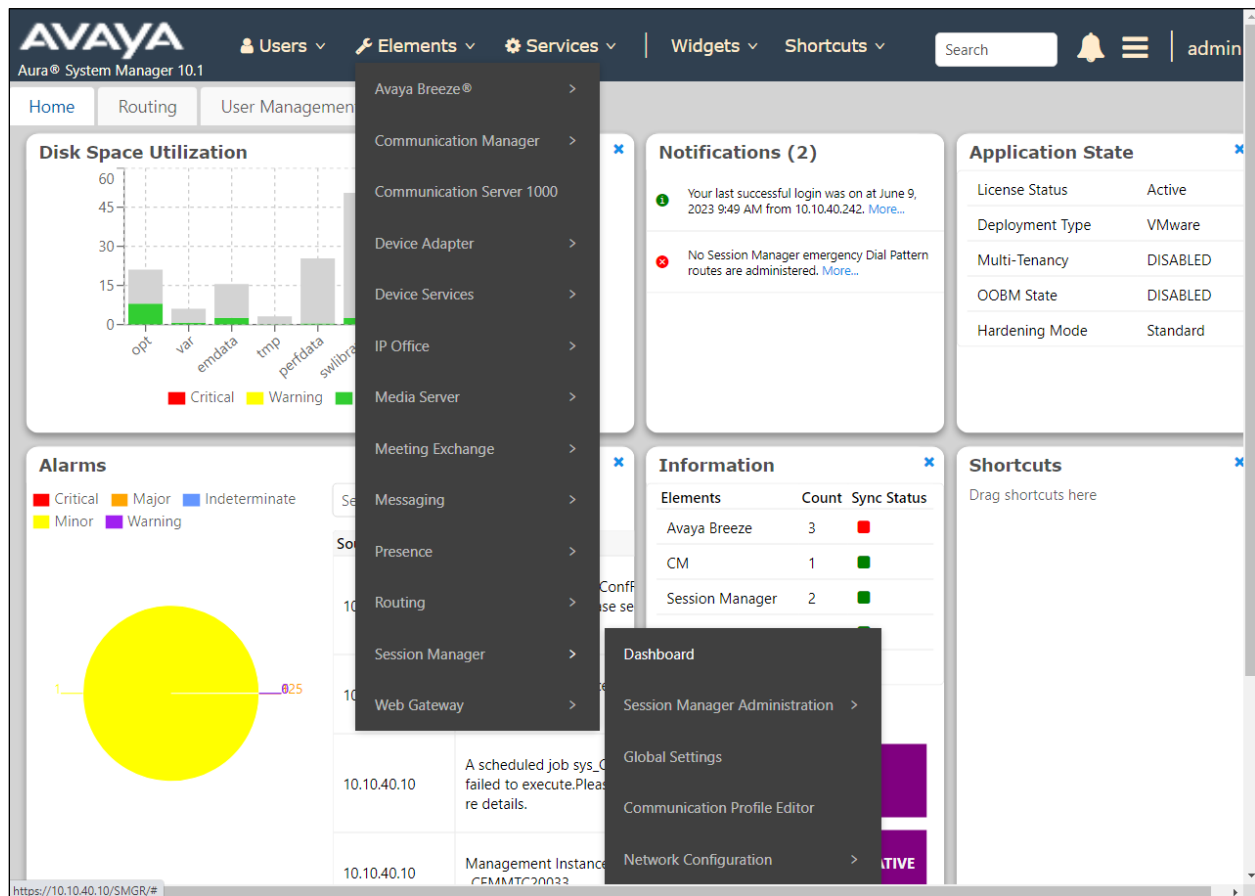
The top of the interface shows the user is logged in as 'neith' and provides links for My Account, Log Out, and Terms of Use. The iManager logo is in the top right corner.

8. Verification Steps

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

8.1. Verify Speakerbus ARIA iDUCX virtual deskstation registration with Avaya Aura® Session Manager

To verify that the Speakerbus ARIA iDUCX virtual deskstation have successfully registered with Session Manager, from the System Manager Web interface, click on **Elements** → **Session Manager**.



From the left window, click on **System Status → User Registrations**. This will display a summary of registered stations on each Session Manager as shown below. Note that **3181**, **3191** and **3192** are all registered which is a good indication that this iDUX/ARIA is registered correctly with Session Manager.

User Registrations

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

Customize

View Default Export Force Unregister AST Device Notifications: Reboot Reload Failback As of 11:54 AM

19 Items Show 15 Filter: Enable

<input type="checkbox"/>	Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control
<input type="checkbox"/>	► Show	3192@greanep.sil6.avaya.com	BridgedTwo	3192	---	10.10.40.223	fixed	<input type="checkbox"/>
<input type="checkbox"/>	► Show	3191@greanep.sil6.avaya.com	PrivacyOne	3191	---	10.10.40.223	fixed	<input type="checkbox"/>
<input type="checkbox"/>	► Show	3183@greanep.sil6.avaya.com	TurretThree	3183	---	10.10.40.207	fixed	<input type="checkbox"/>
<input type="checkbox"/>	► Show	3181@greanep.sil6.avaya.com	TurretOne	3181	---	10.10.40.223	fixed	<input type="checkbox"/>
<input type="checkbox"/>	► Show	3101@greanep.sil6.avaya.com	Agent One	Workspaces	DevConnectGalway	10.10.40.187	fixed	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	AAFD - one	SIP	---	---	fixed	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	AAFD - two	SIP	---	---	fixed	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	Workplace	Windows	---	---	fixed	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	Vantage01	K175	---	---	fixed	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	Third Party	SIP Phone	---	---	fixed	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	LifeX	3141	---	---	fixed	<input type="checkbox"/>

8.2. Verify Speakerbus ARIA iDUCX virtual deskstation status

Open a URL to the ICMS server for example [https://\[ip of iWS\]/ARIATouch/Login](https://[ip of iWS]/ARIATouch/Login). Enter the appropriate credentials and click on **SIGN IN**.

ARIA Touch Deskstation

Speakerbus

SIGN IN WITH SPEAKERBUS

avayauser1

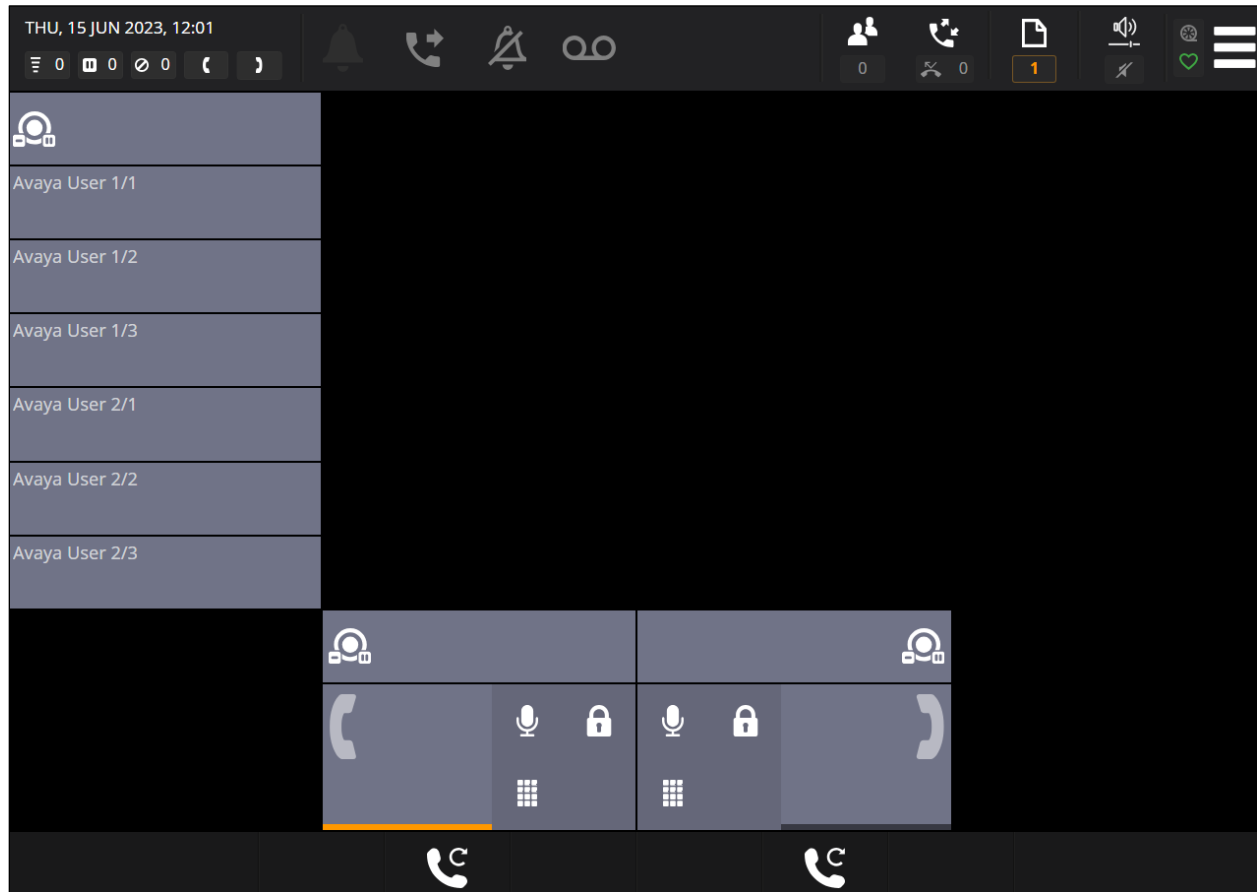
Default CloudBase Collection

SIGN IN

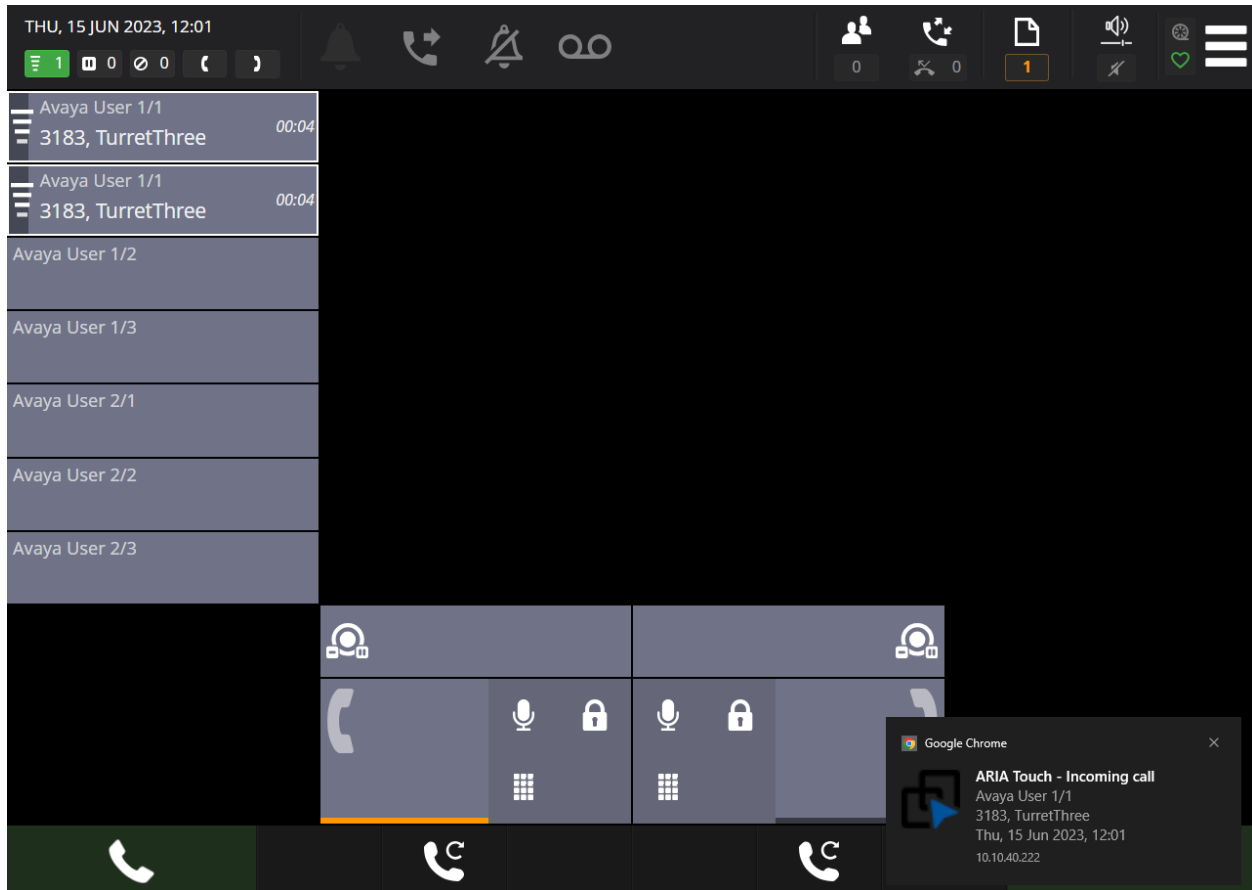
ARIA SHOULD NOT BE USED FOR EMERGENCY CALLS. THE LOCATION MAY BE INCORRECTLY REPORTED TO THE OPERATOR.

Copyright © Speakerbus Technology Ltd. All Rights Reserved. v2.610.3.0

The user is presented with the following screen, displaying the virtual turret.



A call was made from extension **3183** to this extension **3181** and the incoming call is shown on the buttons along the left side of the screen as well as a popup message from **Chrome** indicating that there is an incoming call. The call can be answered by clicking on one of the buttons on the left side.



Once the call is answered, the buttons along to bottom can be used to place the call on hold, transfer the call, or conference in another person.



9. Conclusion

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

10. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1.
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1.
- [4] *Administering Avaya Aura® System Manager*, Release 10.1.
- [5] *Speakerbus iCMS Administrators Guide v4.0 R46*
- [6] *Speakerbus Aria Touch User Guide R5*

Additional product documentation for Speakerbus can be requested from info@speakerbus.com

©2023 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.