



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

---

# **Application Notes for Bose ControlSpace EX-1280C Conferencing Processor with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required to integrate the Bose ControlSpace EX-1280C with Avaya Aura ® Communication Manager and Avaya Aura® Session Manager. The ControlSpace EX-1280C conferencing processor registered with Avaya Aura® Session Manager via SIP.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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 configuration steps required to integrate Bose ControlSpace EX-1280C conferencing processor with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The ControlSpace EX-1280C conferencing processor registered with Session Manager via SIP.

## 2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between the ControlSpace EX-1280C, Avaya H.323, SIP, Digital, Analog telephones, and the PSTN, and exercising basic telephony features, such as inbound, outbound call, DTMF and mute from the Avaya IP phones.

The serviceability testing focused on verifying that the ControlSpace EX-1280C would come back into service after re-connecting the Ethernet cable or rebooting the ControlSpace EX-1280C.

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 recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note 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 this Application Note, the interface between Avaya systems and the ControlSpace EX-1280C did not include use of any specific encryption features.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

## 2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of ControlSpace EX-1280C with Session Manager.
- Inbound and outbound calls between ControlSpace EX-1280C and Avaya SIP and H.323 telephones with Direct IP Media (Shuffling) enabled.
- Inbound and outbound calls between the ControlSpace EX-1280C and the PSTN.
- G.711 codec support.
- Proper recognition of DTMF tones.
- Basic telephony features, including hold, mute, redial, transfer, and 3-way conference, initiated from the Avaya IP phone.
- Proper system recovery after a restart of the ControlSpace EX-1280C and loss of IP connectivity.

## 2.2. Test Results

All test cases passed with the following observation(s):

- The ControlSpace EX-1280C conferencing processor does not support codec G.729. It supports G.711, G.722, and G.726.

## 2.3. Support

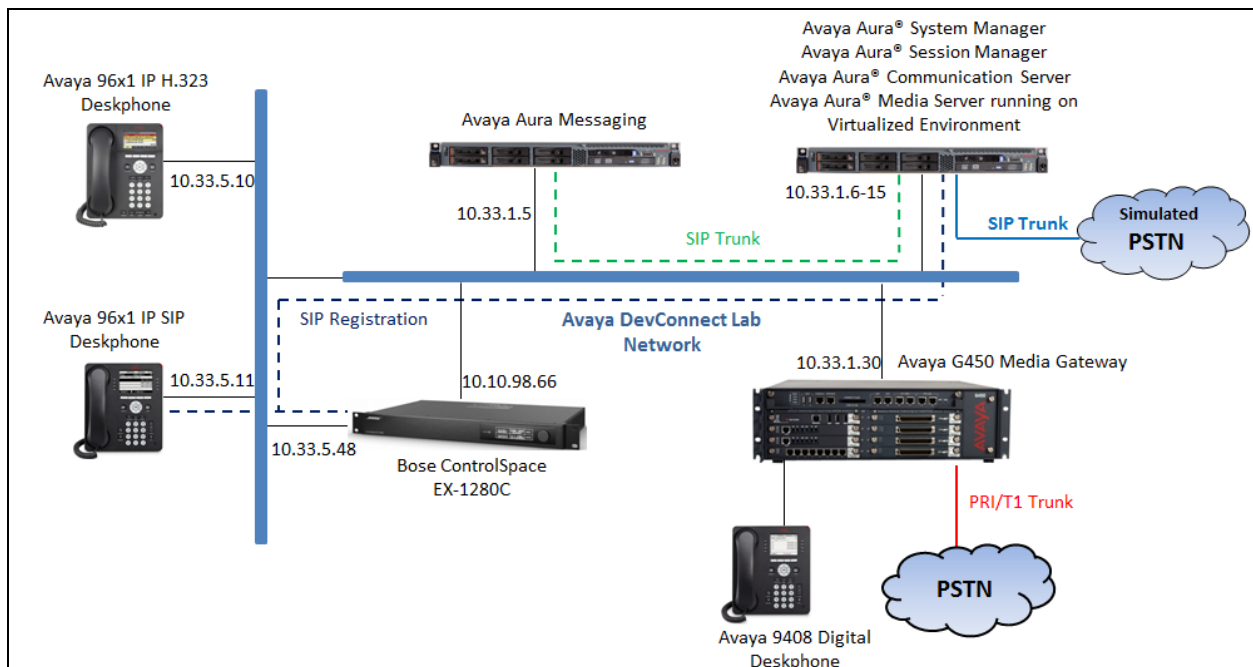
For technical support and information on Bose ControlSpace EX-1280C, contact Bose support at:

- Tel: 1-800-994-BOSE
- Website: [https://pro.bose.com/en\\_us/support.html](https://pro.bose.com/en_us/support.html)

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration with an Avaya SIP-based network that includes the following products:

- Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Aura® Media Server running on Virtualized environment.
- Avaya Aura Messaging has SIP trunk connected to Session Manager and used as Voicemail system for the endpoint.
- Avaya G450 Media Gateway registers to Communication Manager and has PRI trunk to simulated PSTN.
- Session Manager has SIP trunk to simulated PSTN.
- Avaya 96x1 H323 and SIP Deskphones were used to place and receive call to/from EX-1280C VOIP station.
- Bose ControlSpace EX-1280C registered with Avaya Aura® Session Manager.



**Figure 1: Avaya SIP Network with Bose ControlSpace EX-1280C**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtualized Environment	R017x.01.0.532.0 7.1.1.0.0.532.23985
Avaya Aura® System Manager running on Virtualized Environment	7.1.1.0.046931
Avaya Aura® Session Manager running on Virtualized Environment	7.1.1.0.711008
Avaya Aura® Media Server running on Virtualized Environment	7.8.0.333
Avaya Aura Messaging	7.0
Avaya G450 Media Gateway	38.20.1
Avaya 96x1 IP Deskphones	6.65 (H323) 7.1.1 (SIP)
Bose EX-1280C Conferencing Processor Bose ConstrolSpace Desgin	V1.17.0 V5.0.0.936

## 5. Configure Avaya Aura® Communication Manager

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

- Verify System Capacity
- Administer IP Node Names
- Administer Codecs
- Administer IP Network Region
- Administer Signaling Group
- Administer Trunk Group
- Administer Private Numbering
- Administer Outbound Routing

### 5.1. Verify System Capacity

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

display system-parameters customer-options		Page	1 of 10
OPTIONAL FEATURES			
G3 Version: V16	Software Package: Enterprise		
Location: 2	System ID (SID): 1		
Platform: 28	Module ID (MID): 1		
		USED	
Platform Maximum Ports:		65000	290
Maximum Stations:		41000	44
Maximum XMOBILE Stations:		41000	0
Maximum Off-PBX Telephones - EC500:		41000	0
<b>Maximum Off-PBX Telephones - OPS:</b>		<b>41000</b>	<b>14</b>
Maximum Off-PBX Telephones - PBFMC:		41000	0
Maximum Off-PBX Telephones - PVFMC:		41000	0
Maximum Off-PBX Telephones - SCCAN:		41000	0
Maximum Survivable Processors:		313	0
(NOTE: You must logoff & login to effect the permission changes.)			

On **Page 2** of the **system-parameters customer-options form**, verify that the number of **Maximum Administered SIP Trunks** supported by the system is sufficient.

display system-parameters customer-options	Page	2 of
10		
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	16
Maximum Concurrently Registered IP Stations:	18000	2
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	1
Maximum Video Capable IP Softphones:	18000	4
<b>Maximum Administered SIP Trunks:</b>	<b>24000</b>	<b>180</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	0
Maximum Media Gateway VAL Sources:	250	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0
(NOTE: You must logoff & login to effect the permission changes.)		

## 5.2. Administer IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the server running Communication Manager (**procr**) and for Session Manager (**interopASM**). These node names will be needed for defining the service provider signaling group in **Section 5.5**.

change node-names ip	Page	1 of	2
IP NODE NAMES			
Name	IP Address		
AMS1	10.33.1.30		
default	0.0.0.0		
<b>interopASM</b>	<b>10.33.1.12</b>		
<b>procr</b>	<b>10.33.1.6</b>		

### 5.3. Administer Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the local and remote sites. For the compliance test, codec G.711MU and G.729 was configured using ip-codec-set 1. Please note that the EX-1280C don't support codec G.729 as noted in **Section 2.2**. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference, the Media Encryption section was configured to use for Avaya endpoints, the EX-1280C station is not using the Media Encryption. Default values can be used for all other fields.

change ip-codec-set 1				Page	1 of	2
IP MEDIA PARAMETERS						
Codec Set: 1						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size (ms)			
1: G.711MU	n	2	20			
2: G.729	n	2	20			
3:	2	20				
4:						
5:						
6:						
7:						
Media Encryption				Encrypted SRTCP: enforce-unenc-srtcp		
1:	1-srtp-aescm128-hmac80					
2:	2-srtp-aescm128-hmac32					
3:	none					
4:						
5:						



## 5.4. Administer IP Network Region

For the compliance test, IP network region 1 was chosen. Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the local site. In this configuration, the domain name is **bvwddev.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field. This is optional.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.3**.
- Retain default values for all other fields.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1              NR Group: 1
Location: 1           Authoritative Domain: bvwddev.com
Name: Loc-1           Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
                      Codec Set: 1          Inter-region IP-IP Direct Audio: yes
                      UDP Port Min: 2048    IP Audio Hairpinning? n
                      UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
```

On **Page 4**, define the IP codec set to be used for traffic between various regions. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) **1**. Default values may be used for all other fields. In the case of the compliance test, only one IP network region was used, so no inter-region settings were required and therefore only codec set 1 is used.

```
change ip-network-region 1                                     Page 4 of 20

Source Region: 1      Inter Network Region Connection Management
dst codec direct      WAN-BW-limits  Video      Intervening
rgn set  WAN  Units    Total Norm  Prio Shr Regions  Dyn A G C
1  1          NoLimit          n      t          CAC R L e
2  2          NoLimit          n      t          CAC R L e
```

## 5.5. Administer Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by SIP trunks. This signaling group is used for inbound and outbound calls between the Communication Manager and Session Manager. For the compliance test, signaling group 1 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- The compliance test was conducted with the **Transport Method** set to “tls”. The transport method specified here is used between Communication Manager and Session Manager. Whatever protocol is used here, it must also be used on the Session Manager entity link defined in **Section 6.5**.
- Set the **Peer Detection Enabled** field to “y”. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to “procr”. This node name maps to the IP address of the Communication Manager as defined in **Section 5.2**.
- Set the **Far-end Node Name** to “InteropASM”. This node name maps to the IP address of Session Manager as defined in **Section 5.2**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a default well-known port value. (For TLS the well-known port value is 5061).
- Set the **Far-end Network Region** to the IP network region defined for the local site in **Section 5.4**.
- Set the **Far-end Domain** to the domain of the local site.
- Set **Direct IP-IP Audio Connections** to “y”. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to “rtp-payload”. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Retain default values for all other fields.

change signaling-group 1	SIGNALING GROUP	Page 1 of 3
Group Number: 1	Group Type: sip	
IMS Enabled? n	<b>Transport Method: tls</b>	
Q-SIP? n		
IP Video? n		Enforce SIPS URI for SRTP? n
Peer Detection Enabled? n	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		
<b>Near-end Node Name: procr</b>	<b>Far-end Node Name: interopASM</b>	
<b>Near-end Listen Port: 5061</b>	<b>Far-end Listen Port: 5061</b>	
	<b>Far-end Network Region: 1</b>	
<b>Far-end Domain: bvwdev.com</b>		
	Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n	
<b>DTMF over IP: rtp-payload</b>	<b>Direct IP-IP Audio Connections? y</b>	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

## 5.6. Administer Trunk Group

Use the “add trunk-group” command to create a trunk group for the signaling group created in **Section 5.5**. For the compliance test, trunk group 1 was configured using the parameters highlighted below.

- Set the **Group Type** field to “sip”.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to “tie”.
- Set **Member Assignment Method** to “auto”.
- Set the **Signaling Group** to the signaling group shown in **Section 5.5**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Retain default values for all other fields.

add trunk-group 1		Page 1 of 22	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: Private Trunk	COR: 1	TN: 1	TAC: #01
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0	Auth Code? n		
Service Type: tie	Member Assignment Method: auto		
		Signaling Group: 1	
		Number of Members: 14	

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. The **Numbering Format** was set to “private” and the **Numbering Format** in the route pattern was set to “lev0-pvt” (see **Section 5.8**).

add trunk-group 1		Page 3 of 22	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Suppress # Outpulsing? n	Numbering Format: private		
	UI Treatment: shared		
	Maximum Size of UI Contents: 128		
	Replace Restricted Numbers? y		
	Replace Unavailable Numbers? y		
	Hold/Unhold Notifications? y		
	Modify Tandem Calling Number: no		
Send UCID? y			

## 5.7. Administer Private Numbering

Private numbering defines the calling party number to be sent to the far-end. Use the **change private-numbering** command to create an entry that will be used by the trunk group defined in **Section 5.6**. In the example shown below, all calls originating from a 4-digit extension beginning with “3” and routed across trunk group 1 are sent with a 4-digit calling number.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	3	1		4	
4					
				Total Administered: 5	
				Maximum Entries: 540	

## 5.8. Administer Outbound Routing

In these Application Notes, the Automatic Alternate Routing (AAR) feature is used to route outbound calls via the SIP trunk to the SIP endpoint. In the sample configuration, the dial prefix “34” is used as the Dialed String. This common configuration is illustrated below with little elaboration. Use the “change dialplan analysis” command to define a dialed string beginning with 34 of length 4 as extension (ext).

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	
34	4	ext							

The route pattern defines which trunk group will be used for an outgoing call and performs any necessary digit manipulation. Use the “change route-pattern” command to configure the parameters for the local site route pattern in the following manner. The example below shows the values used for route pattern 1 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP trunk. For the compliance test, trunk group **1** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** “lev0-pvt”. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form in **Section 5.6** for full details.
- Retain default values for all other fields.

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

Use the “change aar analysis” command to create an entry in the AAR Digit Analysis Table for this purpose. The example below shows entries created for the local site “aar analysis 3”. The highlighted entry specifies that 4 digit dial string 3 was to use route pattern 1 to route calls to the SIP endpoint via Session Manager.

change aar analysis 3										Page 1 of 2	
AAR DIGIT ANALYSIS TABLE											
Location: all										Percent Full: 2	
Dialed		Total		Route		Call		Node		ANI	
String		Min Max		Pattern		Type		Num		Reqd	
3		4 4		1		lev0		n			

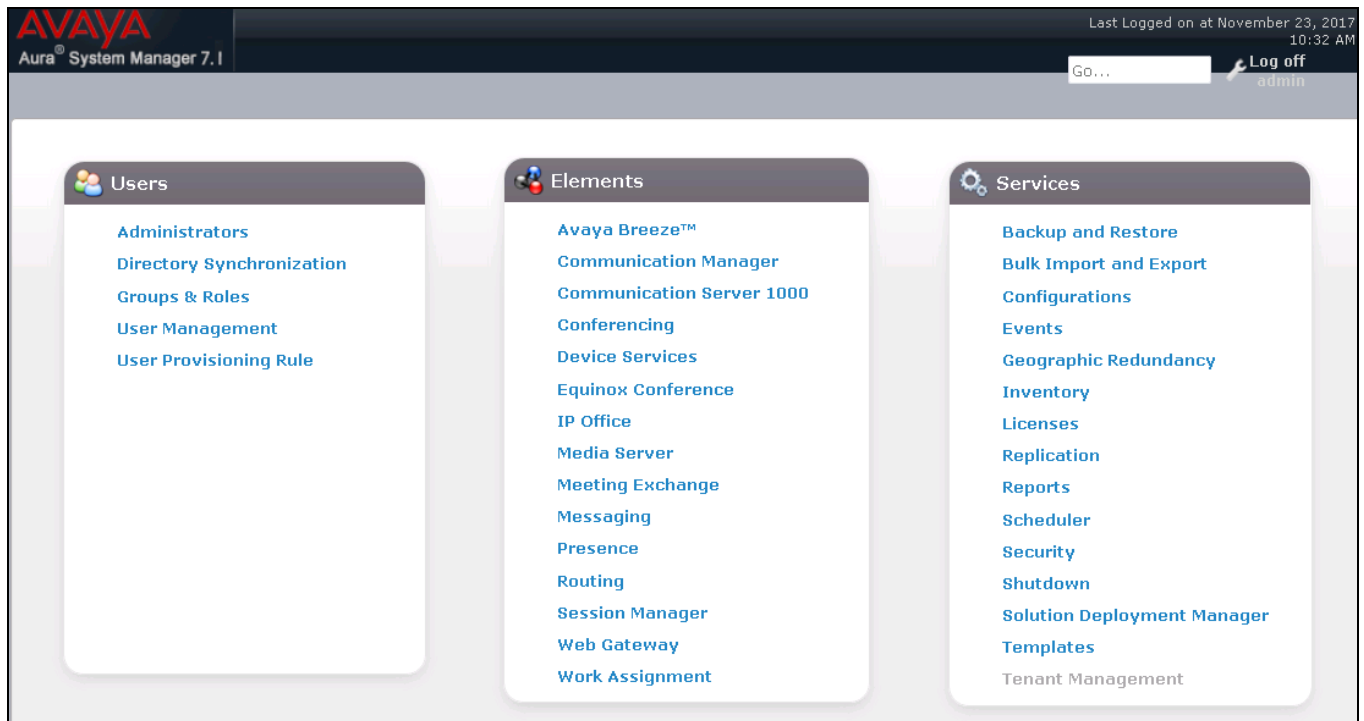
## 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain
- Location
- SIP Entities
- Entity Links
- Routing Policies
- Dial Patterns

For detail configuration details of the Session Manager refer to **Section 10**.

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log on** (not shown). The following page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration.



Clicking the **Elements** → **Routing** link, displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. At the top, the header includes the Avaya logo, the text 'Aura System Manager 7.1', and a 'Last Logged on at November 23, 2017 10:32 AM' timestamp. A search bar with 'Go...' and a 'Log off' button are also present. Below the header, a breadcrumb trail shows 'Home / Elements / Routing'. The left-hand navigation pane is expanded to show the 'Routing' section, which includes links for Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Introduction to Network Routing Policy' and contains the following text:

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc. The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
  - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
  - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)



## 6.1. Specify SIP Domain

Create a SIP Domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the domain (**bvwdev.com**) as defined in **Section 5.4**. Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.0**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name** – Enter the domain name.
- **Type** – Select “sip” from the pull-down menu.
- **Notes** – Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the added domain.

AVAYA  
Aura® System Manager 7.1

Last Logged on at November 1, 2018 10:00 AM

Go... Log out

Home Routing

Home / Elements / Routing / Domains

**Domain Management** [Help ?](#)

1 Item [Refresh](#) Filter: [Enable](#)

Name	Type	Notes
* bvwdev.com	sip	SIP Domain

## 6.2. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **BvwDevSIL**, which includes all equipment at the enterprise including Communication Manager and Session Manager.

To add a Location, navigate to **Routing → Locations** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name** – Enter a descriptive name for the Location.
- **Notes** – Add a brief description (optional).

The screenshot shows the 'Location Details' form in the 'Routing > Locations' section. The left-hand navigation pane is expanded to 'Locations'. The main content area has a breadcrumb trail 'Home / Elements / Routing / Locations' and a title bar 'Location Details' with 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields: 'Name' (required, value: BvwDevSIL), 'Notes' (empty), 'Dial Plan Transparency in Survivable Mode' (Enabled: ☐), and 'Listed Directory Number' (empty). The left-hand navigation pane lists: Routing, Domains, Locations (selected), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults.

Scroll down to the **Location Pattern** section. Click **Add** and enter the following values.

- **IP Address Pattern** – Add all IP address patterns used to identify the location.
- **Notes** – Add a brief description (optional).

Click **Commit** to save.

The screenshot shows the 'Location Pattern' section. It has 'Add' and 'Remove' buttons. Below them is a table with 1 item. The table has columns for 'IP Address Pattern' and 'Notes'. The first row shows the pattern '\* 10.33.1.\*' and the note 'Net 10.33.1.0 for Aura System'. At the bottom, there is a 'Select' dropdown with options 'All' and 'None'.

IP Address Pattern	Notes
* 10.33.1.*	Net 10.33.1.0 for Aura System

### 6.3. Add SIP Entity

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.0**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name** – Enter a descriptive name.
- **FQDN or IP Address** – Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type** – Enter “Session Manager” for Session Manager or “CM” for Communication Manager.
- **Adaptation** – This field is only present if Type is not set to Session Manager. If applicable, select the appropriate Adaptation name. During compliance testing no adaptation rule was used.
- **Location** – Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location “BvwDevSIL” created in **Section 6.2**.
- **Time Zone** – Select the time zone where the server is located.

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left-hand navigation pane is expanded to show the 'Routing' section, with 'SIP Entities' selected. The main content area displays the 'SIP Entity Details' form. The form has a 'General' tab selected. The fields and their values are as follows:

- Name:** ASM70A
- FQDN or IP Address:** 10.33.1.12
- Type:** Session Manager
- Notes:** (empty)
- Location:** BvwDevSIL
- Outbound Proxy:** (empty)
- Time Zone:** America/Toronto
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- SIP Link Monitoring:** Use Session Manager Configuration

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP Entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port** – Port number on which Session Manager can listen for SIP requests.
- **Protocol** – Transport protocol to be used with this port.
- **Default Domain** – The default domain associated with this port.
- **Endpoint** – Checked the checkbox to indicate the specific ports used for SIP endpoint.

**Listen Ports**

Add Remove

6 Items Filter: Enable

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	bvwdev.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	bvwdev.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	bvwdev.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5062	TLS	bvwdev.com	<input type="checkbox"/>	
<input type="checkbox"/>	5067	TLS	bvwdev.com	<input type="checkbox"/>	
<input type="checkbox"/>	5080	TCP	bvwdev.com	<input type="checkbox"/>	

Select : All, None

The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager; this requires the creation of a SIP Entity for Communication Manager for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of Communication Manager. The **Location** field is set to **BewDevSIL** which is the Location defined for the subnet where Communication Manager resides. See **Section 6.2**.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top header includes the Avaya logo, the text "Aura® System Manager 7.1", and a "Last Logged on at November" status. A navigation bar shows "Home" and "Routing" tabs. A left sidebar lists various configuration categories: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "SIP Entity Details" with a "General" sub-tab. The breadcrumb path is "Home / Elements / Routing / SIP Entities". The form contains the following fields: "Name" (ACM-Trunk1-Private), "FQDN or IP Address" (10.33.1.6), "Type" (CM), "Notes" (Private SIP trunk for SIP phone), "Adaptation" (empty), "Location" (BvwDevSIL), "Time Zone" (America/Toronto), "SIP Timer B/F (in seconds)" (4), "Minimum TLS Version" (Use Global Setting), "Credential name" (empty), "Securable" (checkbox), and "Call Detail Recording" (both). "Commit" and "Cancel" buttons are located at the top right of the form area.

SIP Entity Details	
General	
* Name:	ACM-Trunk1-Private
* FQDN or IP Address:	10.33.1.6
Type:	CM
Notes:	Private SIP trunk for SIP phone
Adaptation:	
Location:	BvwDevSIL
Time Zone:	America/Toronto
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	<input type="checkbox"/>
Call Detail Recording:	both

## 6.4. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. The Entity Link was created to Communication Manager, to add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.0**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name** – Enter a descriptive name.
- **SIP Entity 1** – Select the Session Manager SIP Entity.
- **Protocol** – Select the transport protocol used for this link. This must match the protocol used in the Communication Manager signaling group in **Section 5.5**.
- **Port** – Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager Entity Link, this must match the one defined on the Communication Manager signaling group in **Section 5.5**.
- **SIP Entity 2** – Select the name of the other system. For the Communication Manager Entity Link, select the Communication Manager SIP Entity defined in **Section 6.3**.
- **Port** – Port number on which the other system receives SIP requests from Session Manager. For the Communication Manager Entity Link, this must match the one defined on the Communication Manager signaling group in **Section 5.5**.
- **Connection Policy** – Select trusted from pull-down menu.

Click **Commit** to save. The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group configuration in **Section 5.5**.

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

Help ?

1 Item Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2
* ASM70_ACM_Trunk1_5	* ASM70A	TLS	* 5061	* ACM-Trunk1-Private

Select : All, None

## 6.5. Add Routing Policies

Routing Policy describes the conditions under which calls will be routed to the SIP Entities specified in **Section 6.3**. Routing Policy must be added for Communication Manager. To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.0**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- Name – Enter a descriptive name.
- Notes – Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP Entity to which this Routing Policy applies and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screen shows the Routing Policy for Communication Manager.

Home / Elements / Routing / Routing Policies

Routing Policy Details

CommitCancel

General

\* Name: To-CM-Trunk1

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM-Trunk1-Private	10.33.1.6	CM	Private SIP trunk for SIP phone

Time of Day

AddRemoveView Gaps/Overlaps

1 Item 

Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

## 6.6. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were needed to route calls from Communication Manager to the SIP endpoint and vice versa. Dial Patterns define which Route Policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a Dial Pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane (**Section 6.0**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Pattern** – Enter a dial string that will be matched against the Request-URI of the call.
- **Min** – Enter a minimum length used in the match criteria.
- **Max** – Enter a maximum length used in the match criteria.
- **SIP Domain** – Enter the destination domain used in the match criteria.
- **Notes** – Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**. Default values can be used for the remaining fields. Click **Commit** to save.

The first example shows the pattern (4 digits) that begins with “34” and has a destination domain of “bvwddev.com” from “All” location use route policy “ACM-Trunk1-Private”.



## Dial Pattern Details

### General

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

### Originating Locations and Routing Policies

2 Items

Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-CM-Trunk1	0	<input type="checkbox"/>	ACM-Trunk1-Private	

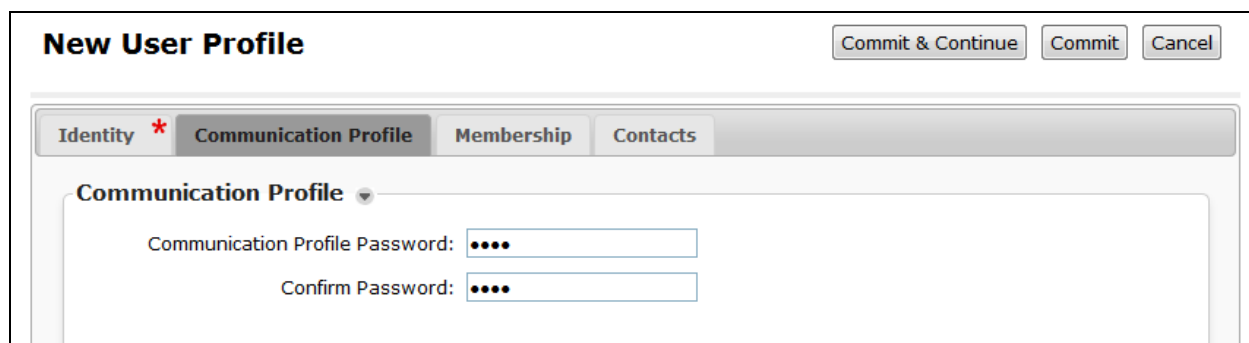
## 6.7. Add a SIP User

A SIP user must be added for EX-1280C VoIP station. Click **User Management** → **Manage Users** → **New** (not shown) and configure the following in the **Identity** tab.

- **First Name** – Enter an identifying name
- **Last Name** – Enter an identifying name
- **Login Name** – Enter the extension number followed by the domain, in this case [3409@bvwddev.com](mailto:3409@bvwddev.com)
- **Password** – Enter a password for the login above
- **Confirm Password** – Enter the confirm password

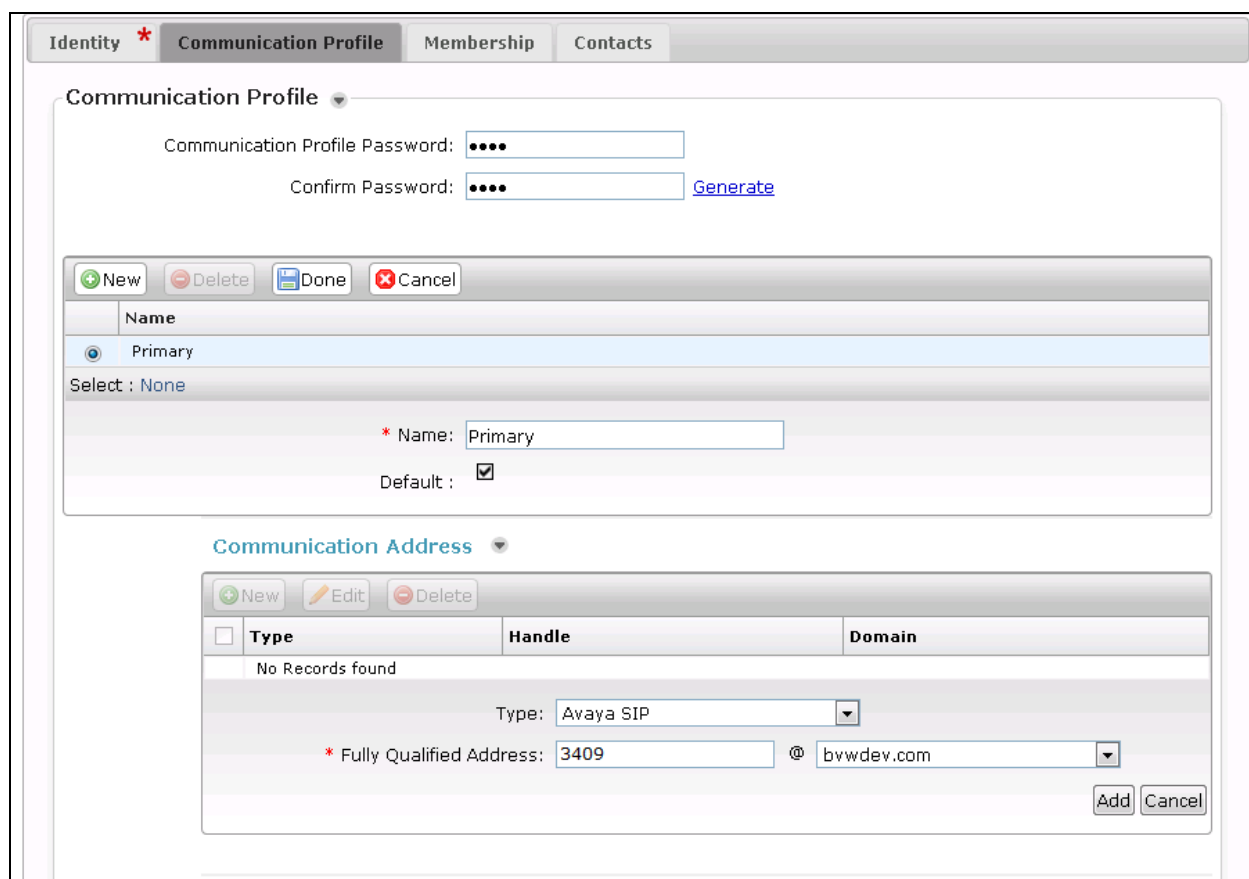
The screenshot shows a web interface for creating a new user profile. The breadcrumb trail at the top is 'Home / Users / User Management / Manage Users'. The page title is 'New User Profile'. There are three buttons at the top right: 'Commit & Continue', 'Commit', and 'Cancel'. Below the title is a tabbed interface with four tabs: 'Identity' (selected and marked with a red asterisk), 'Communication Profile', 'Membership', and 'Contacts'. Under the 'Identity' tab, there is a 'User Provisioning Rule' dropdown menu. Below that is the 'Identity' section, which contains several input fields: 'Last Name' (with a red asterisk) containing 'SIP', 'Last Name (Latin Translation)' containing 'SIP', 'First Name' (with a red asterisk) containing '3409', 'First Name (Latin Translation)' containing '3409', 'Middle Name' (empty), 'Description' (empty text area), 'Login Name' (with a red asterisk) containing '3409@bvwddev.com', 'Email Address' (empty), 'User Type' dropdown menu set to 'Basic', 'Password' (empty), and 'Confirm Password' (empty).

Click the **Communication Profile** tab and in the **Communication Profile Password** and **Confirm Password** fields, enter a numeric password. This will be used to register the EX-1280C VoIP station.



The screenshot shows the 'New User Profile' form with the 'Communication Profile' tab selected. The 'Identity' tab is marked with a red asterisk. The 'Communication Profile' section contains two password fields: 'Communication Profile Password' and 'Confirm Password', both masked with four dots. At the top right, there are three buttons: 'Commit & Continue', 'Commit', and 'Cancel'.

In the **Communication Address** section select **New**; for **Type** select **Avaya SIP** from the drop down list. In the **Fully Qualified Address** field enter the extension number and select the appropriate Domain from the drop down list, in this case the SIP domain is “bvwddev.com”. Click **Add** when done.



The screenshot shows the 'Communication Address' section of the 'New User Profile' form. The 'Communication Profile' section is visible above, with password fields and a 'Generate' link. Below it, there is a 'Communication Address' section with a 'New' button and a table. The table has columns for 'Type', 'Handle', and 'Domain'. A 'Primary' address is listed with 'Name: Primary' and 'Default: [checked]'. Below the table, there is a form to add a new address. The 'Type' is set to 'Avaya SIP'. The 'Fully Qualified Address' field contains '3409' and the 'Domain' is set to 'bvwddev.com'. There are 'Add' and 'Cancel' buttons at the bottom right of the form.

Type	Handle	Domain
Primary		

No Records found

Type: Avaya SIP

\* Fully Qualified Address: 3409 @ bvwddev.com

Add Cancel

Select the check box for **Session Manager Profile** and configure the **Primary Session Manager, Origination Sequence, Termination Sequence** and **Home Location**, from the respective drop down lists.

☒ **Session Manager Profile** ▼

**SIP Registration**

\* Primary Session Manager

QASM70A

Primary	Secondary	Maximum
13	0	13

Secondary Session Manager

Q

Survivability Server

Q

Max. Simultaneous Devices

1 ▼

Block New Registration  
When Maximum Registrations  
Active?

☐

**Application Sequences**

Origination Sequence

SEQ\_InteropCM70 ▼

Termination Sequence

SEQ\_InteropCM70 ▼

**Call Routing Settings**

\* Home Location

BvwDevSIL ▼

Conference Factory Set

(None) ▼


**Call History Settings**

Enable Centralized Call  
History?

☐

Select the check box for **CM Endpoint Profile** and configure as follows:

- **System** – Select the relevant Communication Manager Element from the drop down list
- **Profile Type** – Select “Endpoint” from the drop down list
- **Extension** – Enter the required extension number, in this case “3409”
- **Template** – Select “9641SIP\_DEFAULT\_CM\_7\_1” from the drop down list
- **Port** – The “IP” is auto filled out by the system

 **CM Endpoint Profile**

\* System

interopcm

\* Profile Type

Endpoint

Use Existing Endpoints ☐

\* Extension

3409

Endpoint Editor

\* Template

9641SIP\_DEFAULT\_CM\_7\_1

Set Type 9641SIP

Security Code

Port IP

Voice Mail Number

Preferred Handle (None)

Calculate Route Pattern ☐

Sip Trunk aar

Enhanced Callr-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User ☒

Override Endpoint Name and Localized Name ☒

Allow H.323 and SIP Endpoint Dual Registration ☐

Continuing from above, click on **Endpoint Editor**. Click on the **Feature Options** tab, the screen shot below shows the Feature options that were used during compliance testing.

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
<div> <div>Button Assignment (B)</div> <div>Profile Settings (P)</div> <div>Group Membership (M)</div> </div>				
<b>Active Station Ringing</b> <b>MWI Served User Type</b> <b>Per Station CPN - Send Calling Number</b> <b>IP Phone Group ID</b> <b>Remote Soft Phone Emergency Calls</b> <b>LWC Reception</b> <b>AUDIX Name</b> <b>EC500 State</b> <b>Short/Prefixed Registration Allowed</b> <b>Music Source</b>	<div>single</div> <div>None</div> <div>None</div> <div></div> <div>as-on-local</div> <div>spe</div> <div>None</div> <div>enabled</div> <div>default</div> <div></div>	<b>Auto Answer</b> <b>Coverage After Forwarding</b> <b>Display Language</b> <b>Hunt-to Station</b> <b>Loss Group</b> <b>Survivable CDR</b> <b>Time of Day Lock Table</b> <b>Voice Mail Number</b>	<div>none</div> <div></div> <div>english</div> <div></div> <div>19</div> <div>internal</div> <div>None</div> <div></div>	
<b>Features</b> <div> <div> <input type="checkbox"/> Always Use  <input type="checkbox"/> IP Audio Hairpinning  <input type="checkbox"/> Bridged Call Alerting  <input type="checkbox"/> Bridged Idle Line Preference  <input checked="" type="checkbox"/> Coverage Message Retrieval  <input type="checkbox"/> Data Restriction  <input checked="" type="checkbox"/> Survivable Trunk Dest  <input type="checkbox"/> Bridged Appearance Origination Restriction  <input checked="" type="checkbox"/> Restrict Last Appearance </div> <div> <input type="checkbox"/> Idle Appearance Preference  <input type="checkbox"/> IP SoftPhone  <input checked="" type="checkbox"/> LWC Activation  <input type="checkbox"/> CDR Privacy  <input checked="" type="checkbox"/> Precedence Call Waiting  <input checked="" type="checkbox"/> Direct IP-IP Audio Connections  <input type="checkbox"/> H.320 Conversion  <input type="checkbox"/> IP Video  <input type="checkbox"/> Per Button Ring Control </div> </div>				

Repeat the procedure in this section to create another SIP account 3408 for the second account of Bose EX-1280C.

## 7. Configure Bose ControlSpace EX-1280C

This section covers the configuration of the Bose ControlSpace EX-1280C. The following procedures are covered:

1. Launching the Web Administration Interface
2. Accounts Configuration
3. Audio Configuration
4. ControlSpace Designer Configuration

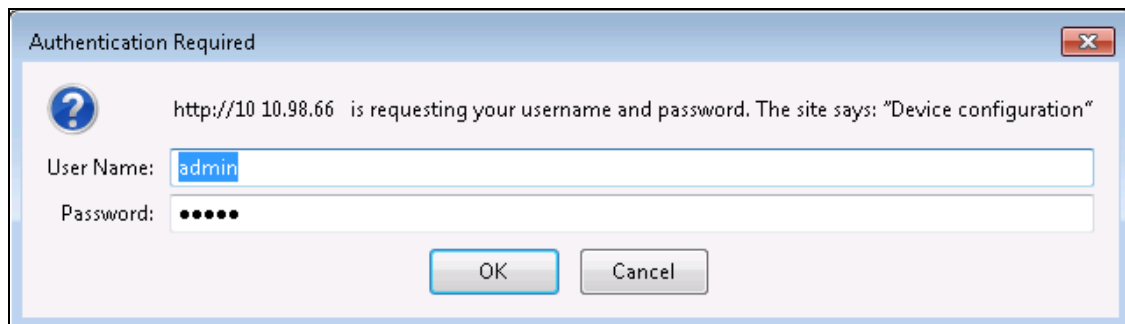
For more information on configuring other features of the ControlSpace EX-1280C, refer to [5], [6], [7], [8].

### 7.1. Launching the Web Administration Interface

The IP address of ControlSpace EX-1280C can be configured manually by using the button in the front, for the compliance test the ControlSpace EX-1280C conferencing processor is connected to network using the ControlSpace port and the VoIP port is used to register the EX-1280C to Session Manager via SIP. To launch the web administration, enter the IP address configured in the ControlSpace port with the following default values:

- **IP Address:** 10.10.98.86
- **Username:** admin
- **Password:** admin

Log in with the appropriate credentials above.



## 7.2. Accounts Configuration

To modify the **Accounts** configuration of the ControlSpace EX-1280C, navigate to the **Accounts** page. There are two accounts (2 VoIP lines), enter the SIP accounts 3408 and 3409 configured in **Section 6.7** as shown in the screenshot below. The **Domain** field is set to the signaling IP address of Session Manager and **Register with domain** is checked.

The screenshot displays the 'Accounts' configuration page for the ControlSpace EX-1280C. The page has a dark header with navigation tabs: Calls, Accounts, Audio, Network, System, Management, and License. The 'Accounts' tab is selected. Below the header, the title 'Accounts' is followed by the instruction 'Add an account to connect to a PBX.' The page shows two accounts, 3408 and 3409, each with a 'General' tab selected. For each account, there are 'Account Actions' (Disable, Register, Unregister) and a form with fields for Account Name, Display Name, Username/Number, Domain, and a checkbox for 'Register with domain'. The 'Domain' field is set to '10.33.1.12' and the 'Register with domain' checkbox is checked. The 'Password' field is masked with dots. The 'Unregister' button is highlighted in yellow for both accounts.

Account ID	Account Name	Display Name	Username/Number	Domain	Register with domain	Password
3408	3408	3408	3408	10.33.1.12	<input checked="" type="checkbox"/>	.....
3409	3409	3409	3409	10.33.1.12	<input checked="" type="checkbox"/>	.....



### 7.3. Audio Configuration

Navigate to **Audio** to configure the Audio setting of the ControlSpace EX-1280C. The selected codecs are moved to **Preferred** column by selecting the available codec in the **Available** column and click on **Enable >>** button. In the compliance test, the codec G.711uLaw is selected as first choice.

**Audio**  
Choose preferred codecs.

**Codec Selection**  
Choose Preferred Codecs

Available	Preferred
G.711 uLaw	G.711 uLaw
G.711 aLaw	G.711 aLaw
G.726 (16kbps)	G.726 fixed payload
G.726 (24kbps)	G.722 HD
G.726 fixed payload	
G.726 (40kbps)	
G.722 HD	
DVI4 Narrowband	
DVI4 HD	
DVI4 Ultra HD	
Linear PCM	
Linear PCM HD	
Linear PCM Ultra HD	
Linear PCM CD Audio	
Linear PCM (little endian)	

**Enable >>** **<< Disable** **Move Up** **Move Down**

**Codec Last Used**

RX G.711 uLaw

TX G.711 uLaw

**Jitter Buffer**

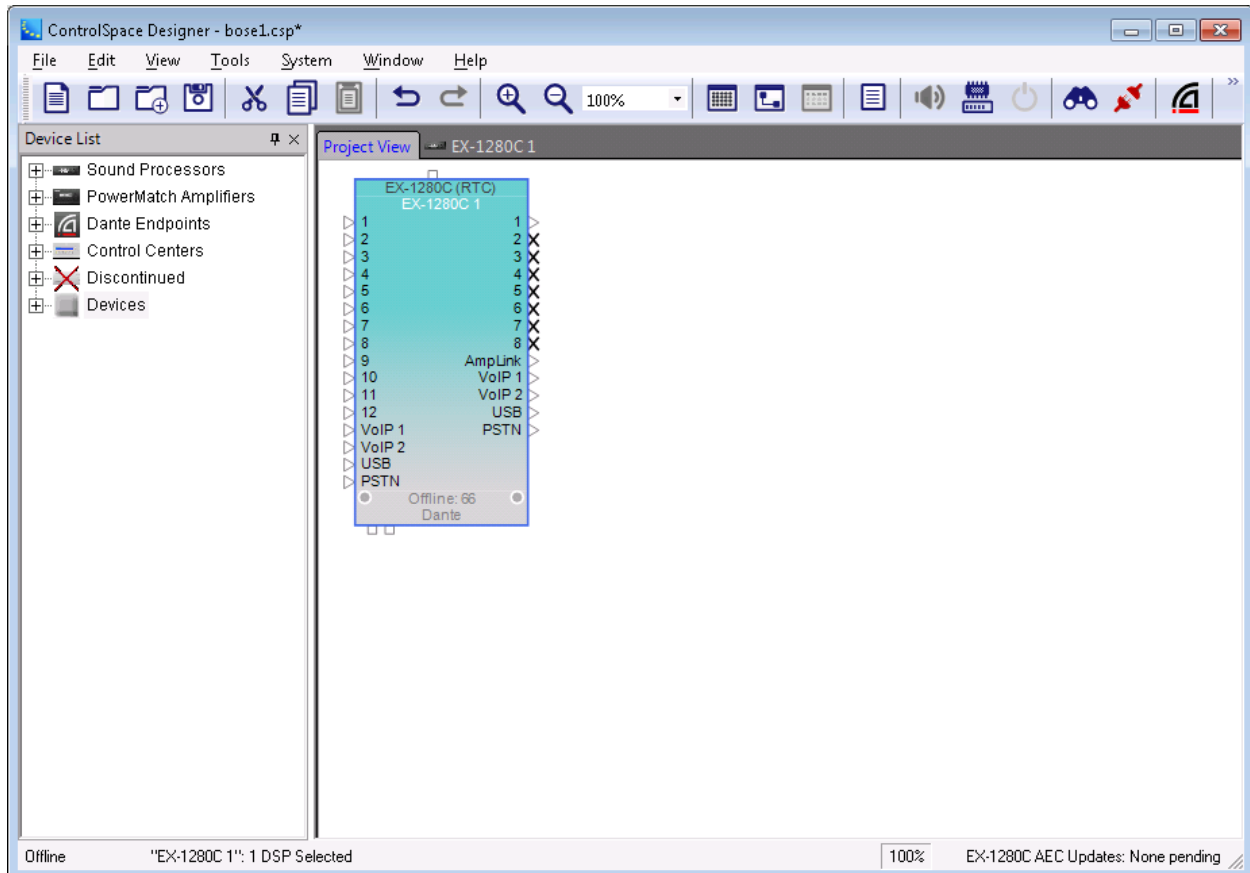
**Depth**

Target Depth 90 ms

Critical Depth 250 ms

## 7.4. ControlSpace Designer Configuration

The ControlSpace Designer (CSD) software is used to control and configure the EX-1280C conferencing processor. Install the CSD software on a PC which locates in the same network with the EX-1280C. From the PC where the CSD software installed, launch the CSD software, the ControlSpace Designer window is displayed as below.



From the menu, navigate to **System → Hardware Manager**. The **Hardware Manager** window is displayed as below.


- **Current Project Settings** section – make sure the correct information of network is displayed if is not, click on the **Change** button to update the network parameter.
- **Host Network Interface** – select the name of Ethernet card of the PC which the CSD software installed, in this case the **Card Name** is “To Lab Network” and its IP address and network mask are auto populated in the **IP address** and **Subnet Mask** fields.
- **Device List – Networking Settings** tab – if the **Hardware Manager** is able to detect the EX-1280C conferencing processor it will list the device under **Device List** window.

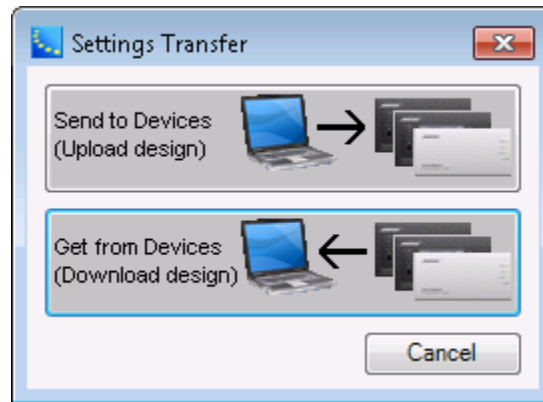
Select the EX-1280C in the **Device List** tab, the **Device Update** section is displayed in the bottom of the window with all networking information currently configured in the EX-1280C as shown in the screenshot below. If all information is correct, close the **Hardware Manager** window by clicking on the X red button in the top right corner.

The screenshot shows the **Hardware Manager** window with the following sections:

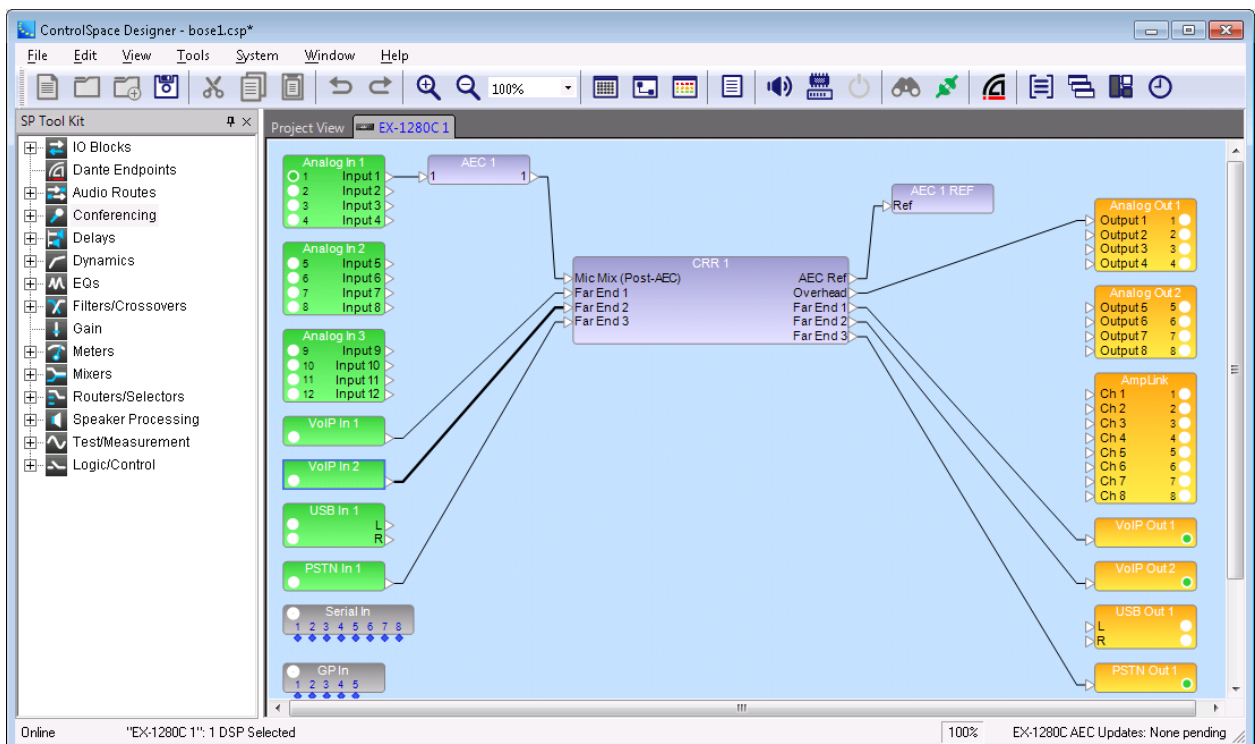
- Current Project Settings:**
  - Network Address: 10.10.98.64
  - Subnet Mask: 255.255.255.224
  - Gateway Address: 10.10.98.65
  - Change** button
- Host Network Interface:**
  - Card Name: To Lab Network (dropdown)
  - IP Address: 10.10.98.86
  - Subnet Mask: 255.255.255.224
- Device List:**
  - Network Settings | Serial Port Settings | Firmware Update | AEC Update | EQ Update | Dante Update | **Discover Devices**

Device Name	IP Address	Type	MAC Address	Subnet Mask	Gateway	DHCP	Status
<input checked="" type="checkbox"/> EX-1280C 1	10.10.98.66	EX-1280C	2C-41-A1-05-69-DE	255.255.255.224	192.168.0.1		
- Device Update:**
  - Device Name: EX-1280C 1
  - MAC Address: 2C - 41 - A1 - 05 - 69 - DE
  - ☐ Enable Front Panel Ethernet
  - Network Connection:**
    - ☐ DHCP ☒ Static IP
    - Current IP Address: 10 . 10 . 98 . 66
    - New IP Address: 10 . 10 . 98 . 66
  - VoIP:**
    - ☒ DHCP ☐ Static IP **VoIP Setup**
    - IP Address: 10 . 33 . 5 . 48
    - Subnet Mask: 255 . 255 . 255 . 0
    - Gateway: 10 . 33 . 5 . 1
    - VLAN: 0 **Update VoIP**

On the main menu of CDS window, click on **Go Online** icon  the **Setting Transfer** window is displayed as shown below. Select the **Send to Devices (Upload design)** option to send the configuration to the EX-1280C. Note that this option needs to be selected when the networking information is updated on the EX-1280C.



The CSD software now connects successfully to the EX-1280C and the **Online** status is shown in the left bottom of the window.



## 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of the Bose ControlSpace EX-1280C conferencing processor with Session Manager.

- Verify the status of Account 1 and Account 2 should change to **Registered** as shown below in the web administration interface.

### Status

**3408**  
User: 3408@10.33.1.12  
Status: Registered

**3409**  
User: 3409@10.33.1.12  
Status: Registered

**System**  
IP: 10.33.5.48 (DHCP)  
MAC Address: 2c:41:a1:05:69:df  
System time:  
2018-01-11 11:58:16  
Uptime: 8d 1h 53m 17s

- From the **System Manager** homepage, navigate to **Home → Elements → Session Manager → System Status → User Registrations** to check the user 3409 and 3408 are registered with the IP address of EX-1280C.

Home / Elements / Session Manager / System Status / User Registrations

Help ?

### User Registrations

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

View ▾ Default Export Force Unregister

AST Device Notifications: Reboot Reload ▾ Failback As of 4:50 PM

Advanced Search ▾

13 Items Show All ▾ Filter: Enable

<input type="checkbox"/>	Details	Address ▾	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
<input type="checkbox"/>	▼ Hide	3409@bywdev.com	3409	SIP	IP-Phone-Loc	---	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

User Registration Device Simultaneous History

Registration Address

3409@bywdev.com

IP Address

10.33.5.48:5060

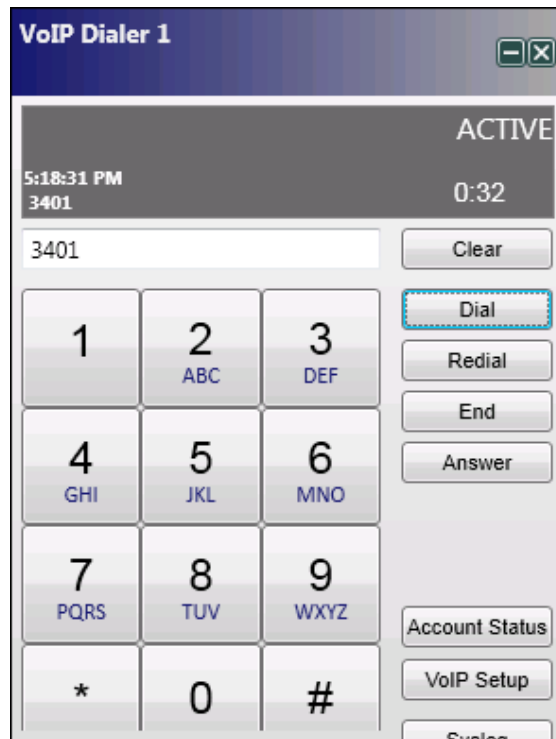
Actual Location

IP-Phone-Loc

Active Controller

---

- Use the VoIP Dialer 1 window from the CSD to place and receive outgoing and incoming calls from the Account 1. Check audio path between Avaya endpoint and EX-1280C, make sure it has two-way speech path with clear audio.



## 9. Conclusion

These Application Notes have described the administration steps required to integrate Bose ControlSpace EX-1280C conferencing processor with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Bose ControlSpace EX-1280C conferencing processor successfully registered with Avaya Aura® Session Manager and basic telephony features were verified. All test cases passed with observations noted in **Section 2.2**.

## 10. Additional References

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

- [1] Administering Avaya Aura® Communication Manager, Release 7.1, August 2017, Document Number 03-300509, Issue 1.
- [2] Avaya Aura® Communication Manager Feature Description and Implementation, Release 7.1, August 2017, Document Number 555-245-205, Issue 1.
- [3] Administering Avaya Aura® Session Manager, Release 7.1, Issue 1 August 2017
- [4] Administering Avaya Aura® System Manager, Release 7.1, Issue 1, August, 2017

The following Bose ControlSpace EX-1280C documentations

- [5] VoIP Server setup document-mods\_by\_DA.pdf
- [6] VoIP\_usage-from\_helpfile.pdf
- [7] Embedded Web Pages\_v2.pdf
- [8] tds\_ControlSpace\_EX\_1280C.pdf

---

**©2018 Avaya Inc. All Rights Reserved.**

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

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