



Avaya Solution & Interoperability Test Lab

Application Notes for Poly Studio X30/X50/X70 Video Bar and Poly G7500 Modular Video Conferencing System with Avaya Meetings Server – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Poly Studio X30/X50/X70 Video Bar 4.0.2 and Poly G7500 Modular Video Conferencing System 4.0.2 with Avaya Meetings Server 9.1.14. Poly Studio X30/X50/X70 are video endpoints that provide an all-in-one video bar, including camera, speaker, and microphones, for small, medium, and large rooms. Poly G7500 Modular Video Conferencing System is a flexible solution that allows connecting various cameras, microphones, and 3rd party components for customizing a conference room. Poly video endpoints support registration via SIP and H.323, simultaneously. Poly video endpoints can register to Avaya Aura® Session Manager through Avaya Session Border Controller as SIP endpoints whether they are connected to the enterprise network or the Internet. When Poly video endpoints are connected to the Internet, they register as SIP remote workers. In addition, Poly video endpoints can register directly to the internal H.323 gatekeeper in Avaya Meetings Server. Poly video endpoints can then join meetings on Avaya Meetings Server or establish point-to-point calls to other Poly and Avaya video endpoints using SIP or H.323.

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.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing.....	6
2.2.	Test Results	7
2.3.	Support	8
3.	Reference Configuration.....	9
4.	Equipment and Software Validated	10
5.	Configure Avaya Aura® Communication Manager.....	11
5.1.	Administer IP Node Names.....	11
5.2.	Administer IP Codec Set.....	12
5.3.	Administer IP Network Region.....	13
5.4.	Administer SIP Trunk to Session Manager.....	14
5.5.	AAR Call Routing.....	16
6.	Configure Avaya Aura® Session Manager	17
6.1.	Launch System Manager.....	17
6.2.	Add SIP Entities and Entity Links	18
6.2.1.	Communication Manager SIP Entity and Entity Link.....	18
6.2.2.	SBC SIP Entity and Entity Link	20
6.3.	Add Routing Policies	22
6.4.	Add Dial Patterns	23
6.5.	Set Network Transport Protocol for Studio X30/X70 and G7500	24
6.6.	Administer SIP User.....	25
6.6.1.	Identity	25
6.6.2.	Communication Profile	26
6.6.3.	Communication Address.....	26
6.6.4.	Session Manager Profile	27
6.6.5.	CM Endpoint Profile.....	28
7.	Configure Avaya Meetings Server.....	29
7.1.	Access Meetings Management Administrator Portal.....	29
7.2.	Configure H.323 Gatekeeper.....	30
7.3.	Configure Advanced Parameters.....	31
7.4.	Configure SIP Trunk to SBC	33
7.5.	Configure Corporate Address Book.....	35
7.6.	Configure Endpoints	36
7.6.1.	Configure H.323 Endpoint.....	37
7.6.2.	Configure SIP Endpoint.....	38
7.7.	Configure Virtual Rooms	39
8.	Configure Avaya Session Border Controller	42
8.1.	Launch SBC Web Interface.....	42
8.2.	Administer Server Interworking Profile.....	44
8.3.	Administer SIP Server.....	46
8.4.	Administer Routing Profile	48
8.5.	Administer Application Rule	49
8.6.	Administer Media Rule	50

8.7.	Administer End Point Policy Group.....	52
8.8.	Administer Media Interfaces	53
8.9.	Administer Signaling Interfaces.....	54
8.10.	Administer End Point Flows.....	55
8.10.1.	Subscriber Flows.....	55
8.10.2.	Server Flows	57
8.11.	Administer Application Relay for LDAP	62
9.	Configure Poly Studio X30 Video Bar	65
9.1.	Access Studio X30 Web Interface	65
9.2.	Administer Provider	66
9.3.	Administer H.323 Settings	67
9.4.	Administer SIP Settings	68
9.5.	Administer Call Settings	70
9.6.	Administer Dialing Options	71
9.7.	Administer Directory Servers.....	72
9.8.	Install Certificate	73
10.	Verification Steps.....	74
11.	Conclusion	82
12.	Additional References.....	82

1. Introduction

These Application Notes describe the configuration steps required to integrate Poly Studio X30/X50/X70 Video Bar 4.0.2 and Poly G7500 Modular Video Conferencing System 4.0.2 with Avaya Meetings Server 9.1.14. Poly Studio X30/X50/X70 are video endpoints that provide an all-in-one video bar, including camera, speaker, and microphones, for small, medium, and large rooms. Poly G7500 Modular Video Conferencing System is a flexible solution that allows connecting various cameras, microphones, and 3rd party components for customizing a conference room. Poly video endpoints support registration via SIP and H.323, simultaneously. Poly video endpoints can register to Avaya Aura® Session Manager through Avaya Session Border Controller (SBC) as SIP endpoints whether they are connected to the enterprise network or the Internet. When Poly video endpoints are connected to the Internet, they register as SIP remote workers. In addition, Poly video endpoints can register directly to the internal H.323 gatekeeper in Avaya Meetings Server. Poly video endpoints can then join meetings on Avaya Meetings Server or establish point-to-point calls to other Poly and Avaya video endpoints using SIP or H.323.

Avaya Meetings Server was deployed in an Over-The-Top environment and was integrated with Avaya Session Border Controller. All SIP calls to Avaya Meetings Server were routed through Avaya Session Border Controller. For H.323 calls, Poly video endpoints communicated directly with Avaya Meetings Server.

As mentioned above, these Application Notes cover three different configurations:

- Poly video endpoints registered to Session Manager through Session Border Controller as SIP endpoints while connected within the enterprise network,
- Poly video endpoints registered to Session Manager through Session Border Controller as SIP remote workers while connected to the Internet, and
- Poly video endpoints registered directly to the internal H.323 gatekeeper in the Meetings Management server of Meetings Server.

When Poly video endpoints are registered to Session Manager through Session Border Controller as SIP endpoints, they join meetings and establish point-to-point calls using the SIP interface. In this configuration, the H.323 interface on the Poly video endpoint is disabled. Typically, when a SIP endpoint is connected within the enterprise network, it would register directly to Session Manager without going through Session Border Controller. However, routing calls through Session Border Controller was required to work around SIP SDP errors encountered during testing mentioned in **Section 2.2**.

When Poly video endpoints register directly to Meetings Management via H.323, they join meetings and establish point-to-point calls to other Poly video endpoints registered to Meetings Management using H.323. In this configuration, the Poly video endpoints also registered to Session Manager through Session Border Controller via SIP. That is, simultaneous, dual registration was supported. The SIP interface was used for point-to-point calls to Avaya endpoints registered to Session Manager via SIP or Communication Manager via H.323. Poly

video endpoints were configured to attempt calls using H.323, and if that fails, attempt the call using SIP. Refer to **Section 9.6** for configuring dialing options.

For the compliance test, the Poly Studio X30/X70 and Poly G7500 were used for testing and will be referred to as Poly video endpoints in these Application Notes. They all provide the same SIP stack and web interface, so these Application Notes apply to all of them. In these Application Notes, the configuration for the Poly Studio X30 is shown, but also apply to the aforementioned Poly video endpoints.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on Poly video endpoints joining meetings on Meetings Server with various Avaya endpoints and web clients and verifying audio, video, voice-activated video switching, and content sharing using SIP and H.323.

The serviceability testing focused on verifying that Poly video endpoints return to service after a restart and re-establishing network connectivity.

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 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, Poly Studio X30/X70 Video Bar, and Poly G7500 Modular Video Conferencing System used TLS/SRTP encryption features for SIP calls. For H.323 calls, encryption features were not used. In addition, a non-secure connection to the LDAP server was used when searching the corporate address book on Avaya Meetings Server.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Poly video endpoints joining meetings from within the enterprise or connected to Internet using SIP with Direct Media (shuffling) enabled and disabled.
- Poly video endpoints joining meetings while registered to Meetings Server via H.323.
- Poly video endpoints joining meetings with audio/video and audio only.
- Poly video endpoints joining meeting with the following endpoint types:
 - Avaya Workplace Client for Windows using SIP and WebRTC
 - Avaya Vantage using SIP and WebRTC
 - Avaya Meetings for Web using WebRTC
 - Avaya J100 Series SIP Phone
 - Avaya 96x1 Series H.323 Deskphone
 - Poly Studio X30/X70 Video Bar and Poly G7500 Modular Video Conferencing System
- Poly video endpoints viewing the current speaker based on voice-activate switching and receiving video from other meeting participants.
- Web collaboration/content sharing from other meeting participants and verifying that shared content can be viewed by Poly video endpoints.
- A second video source (e.g., Windows PC) connected via HDMI to Poly video endpoints may be used to share content. Poly video endpoints can select the camera (i.e., video source 1) or the second video source to share content. Moderator can set the Poly video endpoint as lecturer to prevent the main video source viewed by other participants from changing.
- Using the built-in LDAP server in Meetings Management to provide its endpoint list as the corporate address book. Poly video endpoints can connect to the LDAP server using a non-secure connection with user credentials or anonymously, search for contact information of endpoints, and add them to Favorites. Poly video endpoints can then call endpoints using the LDAP search results.
- Poly video endpoints joining meeting with PIN protection. For SIP call, DTMF using RFC2833 was used. For H.323 calls, out-of-band DTMF via H.245 was used.
- Poly video endpoints muting audio and video.
- Meeting moderator muting the audio, video, and speaker on Poly video endpoints.
- Poly video endpoints being promoted to lecturer.
- Poly video endpoints disconnecting from meeting by either hanging up, being removed from meeting by moderator, or terminating a meeting.
- Poly video endpoints being added to meeting by a participant, such as Workplace, Vantage, or Meetings for Web.
- Poly video endpoints joining meeting by receiving a dial-out call from Meetings Server when the moderator starts a meeting. Poly video endpoints received dial out call via H.323 or SIP.
- Poly video endpoints establishing point-to-point calls with other Poly video endpoints registered to Meetings Server via H.323.
- Poly video endpoints establishing point-to-point calls with other Avaya endpoints registered to Session Manager via SIP.

- Long duration meetings.
- TLS transport for SIP signaling using a secure PFS cipher.
- SRTP for Poly video endpoints registered as SIP endpoints.
- Support of G.711, G.729, and G.722 codecs.
- Proper system recovery after a restart of Poly video endpoints and loss of IP network connectivity.

2.2. Test Results

All test cases passed with the following observations:

- Poly video endpoints do not support WebRTC with Meetings Server.
- Poly video endpoints must register to Session Manager through SBC whether connected to the enterprise network or the Internet. Video calls are not supported when Poly video endpoints are registered directly to Session Manager due to SIP SDP errors that prevent video calls from being established. The SIP SDP errors also impact audio call transfers to Poly video endpoints. The workaround is to register Poly video endpoints within the enterprise network to Session Manager through a private interface on SBC to bypass the SIP SDP errors. The SBC configuration is similar to the SBC remote worker configuration.
- Point-to-point video calls between Poly video endpoints and Avaya video endpoints, such as Vantage failed because of SIP SDP errors.
- Audio and video mute status is not synchronized between Poly video endpoints and Meetings Management, including Meetings Dashboard and the participant list. The exception was when Poly video endpoints joined meeting using H.323 and muted the audio via the TC8 Touch Controller or web interface
- Meetings Management cannot upgrade the Poly video endpoints because Meetings Management does not currently support the Poly REST API.
- Poly video endpoints were able to share content by connecting a second HDMI video source with content, such as a PC. From the TC8 Touch Controller, the video source could be selected (i.e., either the camera or second video source with content). In this mode, the Poly video endpoint would not have the floor – the video of the current speaker could override the shared content from the Poly video endpoint. However, the Poly video endpoint could be promoted to lecturer to prevent the video from switching, but the participants would be in listen only mode.
- If BFCP is enabled in the media rule on SBC, Poly video endpoints halt video and join meeting with audio only – no video in either direction. The workaround is to disable BFCP in the media rule on SBC. Refer to **Section 8.6** for disabling BFCP.
- Initial IP-IP Direct Media, which allows Early Media between SIP endpoints before call is established, must be disabled on Communication Manager as shown in **Section 5.4**. This option is disabled in the signaling group of the SIP trunk between Communication Manager and Session Manager.
- Poly video endpoints cannot connect to the built-in LDAP server on Meetings Management via a secure connection using SSL. The workaround is to use a non-secure connection.

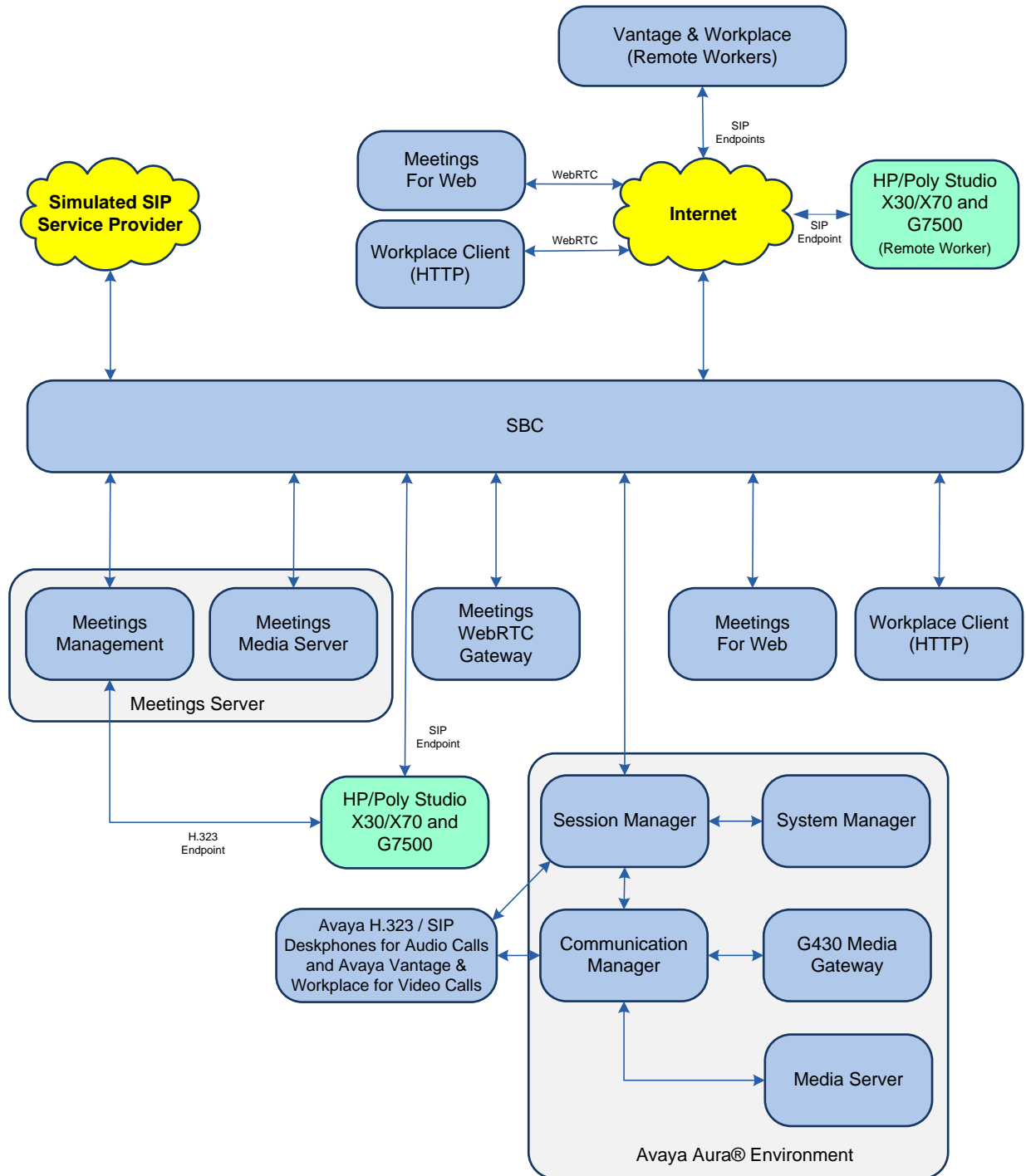
- When Poly video endpoints join a PIN-protected meeting using H.323, set the **addDTMFsInSimAltCaps** parameter to *1* in Meetings Media Server so that Poly video endpoints send PIN via out-of-band DTMF using H.245 as described in **Section 7.3**; otherwise, PIN authentication would fail.

2.3. Support

For support on Poly X30/X50/X70 Video Bar and G7500 Modular Video Conferencing System, visit the Poly support portal at <https://www.poly.com/us/en/support>.

3. Reference Configuration

The test configuration is shown below. Studio X30/X70 and G7500 register to Session Manager through SBC whether located within enterprise network or the Internet. All SIP calls with Meetings Server, including SIP signaling and media, flow through SBC. Poly video endpoints also register directly to the internal H.323 gatekeeper in Meetings Management. Various Avaya endpoints and web clients were used to join meeting with Poly video endpoints.



4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Meetings Server	9.1.14
Avaya Session Border Controller	10.1.1.0-35-21872
Avaya Vantage	3.1.1.2.0009
Avaya Workplace Client for Windows	3.33.0.96 (SIP)
Avaya 96x1 Series IP Deskphones	6.8.5.4.10 (H.323)
Avaya J100 Series IP Phones	4.1.1.0.7 (SIP)
Avaya Aura® Communication Manager	10.1.3.0.0-FP3
Avaya G430 Media Gateway	FW 42.2.0
Avaya Aura® Media Server	10.1.0.125
Avaya Aura® System Manager	10.1.3.0 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.3.0.0-0715713 Feature Pack 3
Avaya Aura® Session Manager	10.1.3.0.1013007
Poly Studio X30 Video Bar with TC8 Touch Controller	4.0.2-384012
Poly Studio X70 Video Bar with TC8 Touch Controller	4.0.2-384012
Poly G7500 Modular Video Conferencing System with TC8 Touch Controller	4.0.2-384012

5. Configure Avaya Aura® Communication Manager

This section covers the Communication Manager configuration related to IP codec set, IP network region, and SIP trunk group and routing to Session Manager, focusing on settings that would impact SIP signaling and media for calls between Meetings Server and Poly video endpoints using SIP. Note that the SIP station configuration for Poly video endpoints are configured through Avaya Aura® System Manager in **Section 6.6**. The System Access Terminal (SAT) was used to configure Communication Manager.

5.1. Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
default	0.0.0.0	
devcon-aes	10.64.102.119	
devcon-ams	10.64.102.118	
devcon-sm	10.64.102.117	
procr	10.64.102.115	
procr6	::	
(6 of 6 administered node-names were displayed)		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

5.2. Administer IP Codec Set

In the **IP Codec Set** form, specify the audio codec supported for calls routed over the SIP trunk to Poly video endpoints and Meetings Server. The form is accessed via the **change ip-codec-set** command. Poly video endpoints were tested using G.722, G.729 and G.711 codecs. G.722 is supported with Media Server.

To enable SRTP when Poly video endpoints are registered as a remote worker, **Media Encryption** should include *1-srtp-aescm128-hmac80* and **Encrypted SRTCP** should be left at the default value of *best-effort*.

change 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.722-64K		2	20
2: G.729A	n	2	20
3: G.711MU	n	2	20
4:			
5:			
6:			

Media Encryption

Encrypted SRTCP: best-effort

1: 1-srtp-aescm128-hmac80

2: 2-srtp-aescm128-hmac32

3: none

4:

5:

On **Page 2**, enable **Allow Direct-IP Multimedia** and set **Maximum Call rate for Direct-IP Multimedia** and **Maximum Call Rate for Priority Direct-IP Multimedia** to *4096 Kbits* as shown below to support video calls.

change ip-codec-set 1 Page 2 of 2

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? y

Maximum Call Rate for Direct-IP Multimedia: 4096:Kbits

Maximum Call Rate for Priority Direct-IP Multimedia: 4096:Kbits

	Mode	Redun- dancy	Packet Size (ms)
FAX	relay	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

Media Connection IP Address Type Preferences

1: IPv4

2:

5.3. Administer IP Network Region

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. **IP-IP Direct Audio** (shuffling) may be enabled to relinquish media resources in the Media Gateway or Media Server on the private side of SBC. The **IP Codec Set** should be set to the one configured in **Section 5.2** for calls routed over the SIP trunk to Session Manager.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1	NR Group: 1	
Location: 1	Authoritative Domain: avaya.com	
Name: SIP Enterprise	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: 50999		
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		

5.4. Administer SIP Trunk to Session Manager

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

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Set **IP Video** to *y* to support video calls.
- Specify Communication Manager (*procr*) and the Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **Direct IP-IP Audio Connections** field was enabled to allow shuffling for calls routed over the associated SIP trunk group.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.
- Disable **Initial IP-IP Direct Media**, which is not supported by Poly video endpoints.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

add signaling-group 10		Page 1 of 2
SIGNALING GROUP		
Group Number: 10	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? y	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
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: devcon-sm	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
Far-end Network Region: 1		
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to/from Poly video endpoints, Workplace, Vantage, Avaya SIP deskphones, and Meetings Server. Set the **Group Type** field to *sip*, 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. Configure the other fields in bold and accept the default values for the remaining fields.

add trunk-group 10		Page 1 of 5	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: To devcon-sm	COR: 1	TN: 1	TAC: 1010
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 10		
	Number of Members: 10		

Page 5 of the SIP trunk group was configured as follows.

add trunk-group 10		Page 5 of 5	
PROTOCOL VARIATIONS			
Mark Users as Phone? n			
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n			
Send Transferring Party Information? n			
Network Call Redirection? 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			
Resend Display UPDATE Once on Receipt of 481 Response? n			
Identity for Calling Party Display: P-Asserted-Identity			
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			

5.5. AAR Call Routing

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and enter add an entry that routes digits beginning with “78” and “79” to route pattern 10 as shown below. SIP endpoints have 5-digit extensions beginning with 78 and virtual rooms in Meetings Server have 5-digit extensions beginning with 79.

change aar analysis 78							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
	Dialed String	Total		Route	Call	Node	ANI
		Min	Max	Pattern	Type	Num	Reqd
78		5	5	10	lev0		n
79		5	5	10	lev0		n

Configure a preference in **Route Pattern** 10 to route calls over SIP trunk group 10 as shown below.

change route-pattern 10										Page 1 of 3
Pattern Number: 10										Pattern Name: To devcon-sm
SCCAN? n										Secure SIP? n
										Used for SIP stations? n
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted			
No			Mrk	Lmt	List	Del	Digits	DCS/	IXC	
								QSIG		
								Intw		
1:	10	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
		0 1 2 M 4 W		Request				PARM	Sub	Numbering
								Dgts	Format	LAR
1:	y	y	y	y	y	n	n	rest	unk-unk	none
2:	y	y	y	y	y	n	n	rest		none

6. Configure Avaya Aura® Session Manager

This section covers the configuration of Session Manager, including setting the transport protocol and port for SIP endpoints registered to Session Manager and adding a SIP user for Poly video endpoints.

6.1. Launch System Manager

Access the System Manager web interface by using the URL **https://<ip-address>** in an Internet browser window, where <ip-address> is the System Manager IP address. Log in using the appropriate credentials.

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.

User ID:

Password:

[Change Password](#)

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

6.2. Add SIP Entities and Entity Links

This section covers the SIP trunk configuration for Communication Manager and SBC. In this configuration, two SIP Entities were added for Communication Manager and SBC. The configuration of the Entity Links is also covered.

6.2.1. Communication Manager SIP Entity and Entity Link

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **Elements** → **Routing** → **SIP Entities** from the top menu, followed by **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., procr) on Communication Manager.
- **Type:** Select *CM*.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

Default values can be used for the remaining fields.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and various menu items: Users, Elements, Services, Widgets, Shortcuts, a search bar, a notification bell, and an 'admin' user profile. Below the navigation bar, the 'Routing' tab is selected in the breadcrumb trail. The left sidebar contains a list of navigation items: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions. The main content area displays the 'SIP Entity Details' form. The form has a 'General' tab selected. Fields include: Name (devcon-cm), FQDN or IP Address (10.64.102.115), Type (CM), Notes (Communication Manager), Adaptation (dropdown), Location (Thornton), Time Zone (America/New_York), SIP Timer B/F (4), Minimum TLS Version (Use Global Setting), Credential name (empty), Securable (checkbox), and Call Detail Recording (none). Buttons for 'Commit' and 'Cancel' are in the top right corner of the form area.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name (e.g., *devcon-sm*).
- **Protocol:** Set to *TLS*. TCP may also be used between Communication Manager and Session Manager.
- **Port:** Set to appropriate TLS port (e.g., *5061*).
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** Set to appropriate TLS port (e.g., *5061*).
- **Connection Policy:** Set to *trusted*.

Entity Links

Override Port & Transport with DNS SRV: ☐

Add		Remove							
1 Item								Filter: Enable	
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	
<input type="checkbox"/>	* devcon-cm Link	devcon-sm	TLS	* 5061	devcon-cm	* 5061	trusted	<input type="checkbox"/>	

Select : All, None

6.2.2. SBC SIP Entity and Entity Link

A SIP Entity must be added for SBC. To add a SIP Entity, select **Elements** → **Routing** → **SIP Entities** from the top menu, followed by **New** in the subsequent screen (not shown) to add a new SIP entity for SBC.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the SBC internal interface.
- **Type:** Select *SIP Trunk*.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and various menu items: Users, Elements, Services, Widgets, Shortcuts, a search bar, a notification bell, and a user profile labeled 'admin'. Below this, a secondary navigation bar shows 'Home' and 'Routing'. The left sidebar is expanded, showing 'Routing' with a sub-menu where 'SIP Entities' is highlighted. The main content area is titled 'SIP Entity Details' and features a 'General' tab. The form contains the following fields and values:

- Name:** devcon-sbce
- FQDN or IP Address:** 10.64.102.106
- Type:** SIP Trunk
- Notes:** SBCE
- Adaptation:** (empty dropdown)
- Location:** Thornton-SBC
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** egress

At the top right of the form, there are 'Commit' and 'Cancel' buttons. A 'Help ?' link is also visible in the top right corner of the main content area.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name (e.g., *devcon-sm*).
- **Protocol:** Set to *TLS*. TCP may also be used between Session Manager and SBC.
- **Port:** Set to appropriate TLS port (e.g., *5061*).
- **SIP Entity 2:** The SBC entity name from this section.
- **Port:** Set to appropriate TLS port (e.g., *5061*).
- **Connection Policy:** Set to *trusted*.

Entity Links

Override Port & Transport with DNS SRV: ☐

Add		Remove							
1 Item								Filter: Enable	
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	
<input type="checkbox"/>	* devcon-sbce Link	devcon-sm	TLS	* 5061	devcon-sbce	* 5061	trusted	<input type="checkbox"/>	

Select : All, None

6.3. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.2**. A routing policy was added for SBC to route outgoing calls to Meetings Server. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, "Aura® System Manager 10.1", and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled "admin" are on the right. The left sidebar shows a tree view with "Routing" selected, and sub-items: Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, and Routing Policies (highlighted in blue).

The main content area is titled "Routing Policy Details" and contains a "Commit" button and a "Cancel" button. The form is divided into two sections:

- General**: Contains fields for "Name" (devcon-sbce Policy), "Disabled" (checkbox), "Retries" (0), and "Notes" (empty text area).
- SIP Entity as Destination**: Contains a "Select" button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
devcon-sbce	10.64.102.106	SIP Trunk	

Below the table, the text "Time of Day" is partially visible.

6.4. Add Dial Patterns

Dial patterns are defined to direct calls to the appropriate SIP Entity. In the sample configuration, 5-digit extensions for meetings IDs beginning with 792 were routed to Meetings Server through SBC.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **SIP Domain:** SIP domain of dial pattern.
- **Notes:** Comment on purpose of dial pattern (optional).

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definition for routing calls to Meetings Server.

Dial Pattern Details

General

* Pattern: 792

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Meetings Virtual Rooms

Originating Locations and Routing Policies

Add Remove

1 Item 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-		devcon-sbce Policy	0	<input type="checkbox"/>	devcon-sbce	

Select : All, None

6.5. Set Network Transport Protocol for Studio X30/X70 and G7500

Set the transport protocol used by Poly video endpoints. From the System Manager **Home** screen, select **Elements** → **Routing** → **SIP Entities** and edit the SIP Entity for Session Manager shown below.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The 'General' tab contains the following fields: Name (devcon-sm), IP Address (10.64.102.117), SIP FQDN (empty), Type (Session Manager), Notes (empty), Location (Thornton), Outbound Proxy (empty), Time Zone (America/New_York), Minimum TLS Version (Use Global Setting), and Credential name (empty). There are 'Commit' and 'Cancel' buttons at the top right. Below the 'General' tab is a 'Monitoring' section with two dropdown menus: 'SIP Link Monitoring' (Use Session Manager Configuration) and 'CRLF Keep Alive Monitoring' (Use Session Manager Configuration).

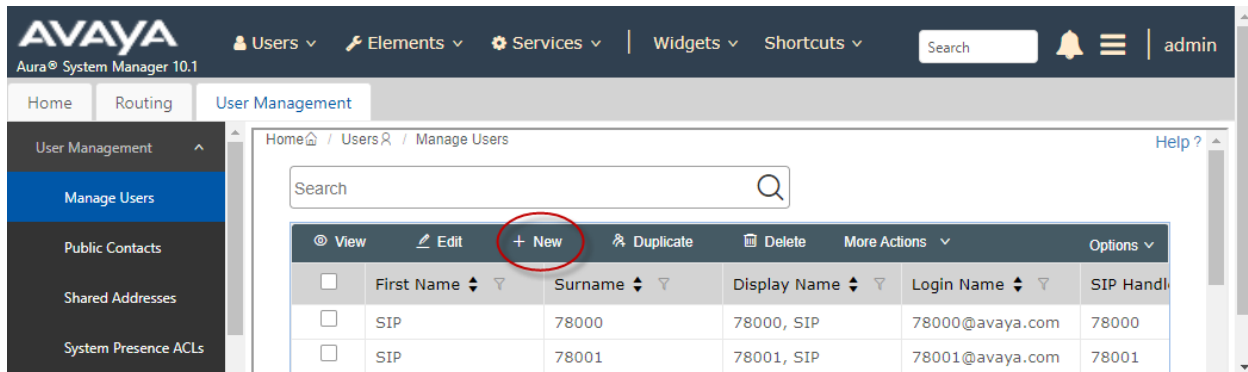
Scroll down to the **Listen Ports** section and verify that the transport network protocol used by Poly video endpoints is specified in the list below. For the compliance test, TLS network transport was used.

Listen Ports

Add Remove					
3 Items					
Filter: Enable					
<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	avaya.com	<input checked="" type="checkbox"/>	
Select : All, None					

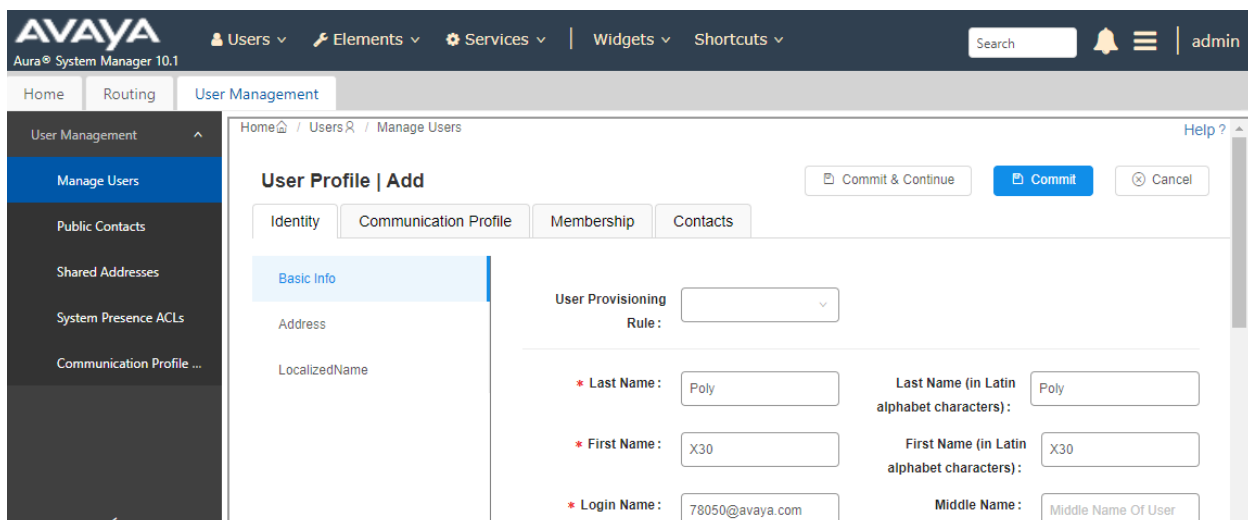
6.6. Administer SIP User

In the System Manager **Home** screen (not shown), select **Users** → **User Management** → **Manage Users** to display the **User Management** screen below. Select a SIP user and click **New** to add a SIP user.



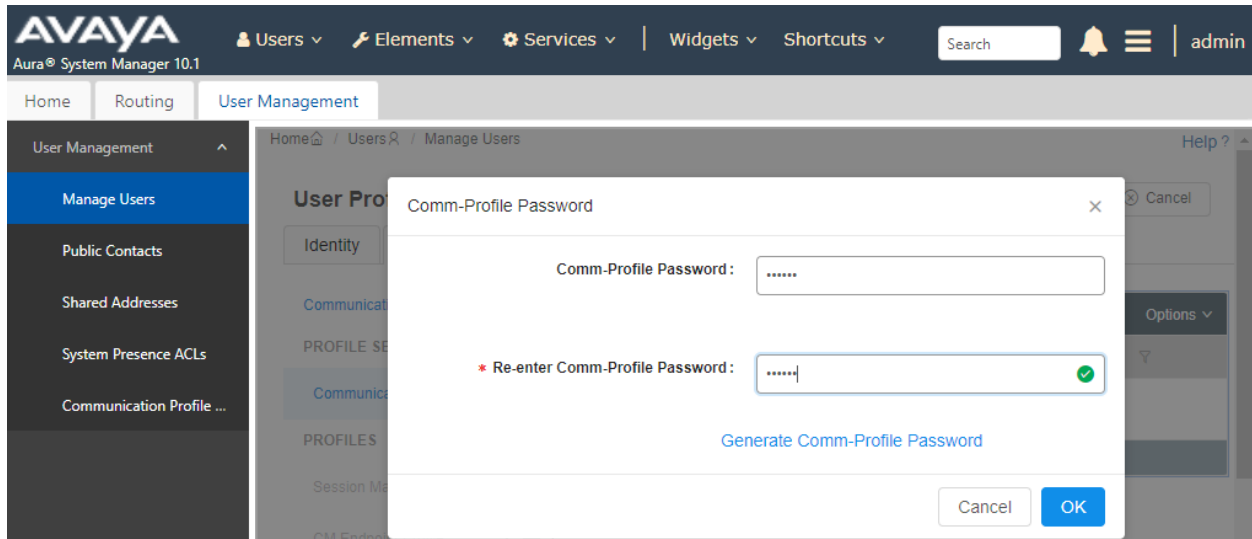
6.6.1. Identity

The **Add User Profile** screen is displayed. Select the **Identity** tab. The desired **Last Name** and **First Name** is configured. The **Login Name** is configured in the format of `<ext>@<domain>`, where `<ext>` is the desired Studio X30 SIP extension and `<domain>` is the SIP domain name. Retain the default values in the remaining fields.



6.6.2. Communication Profile

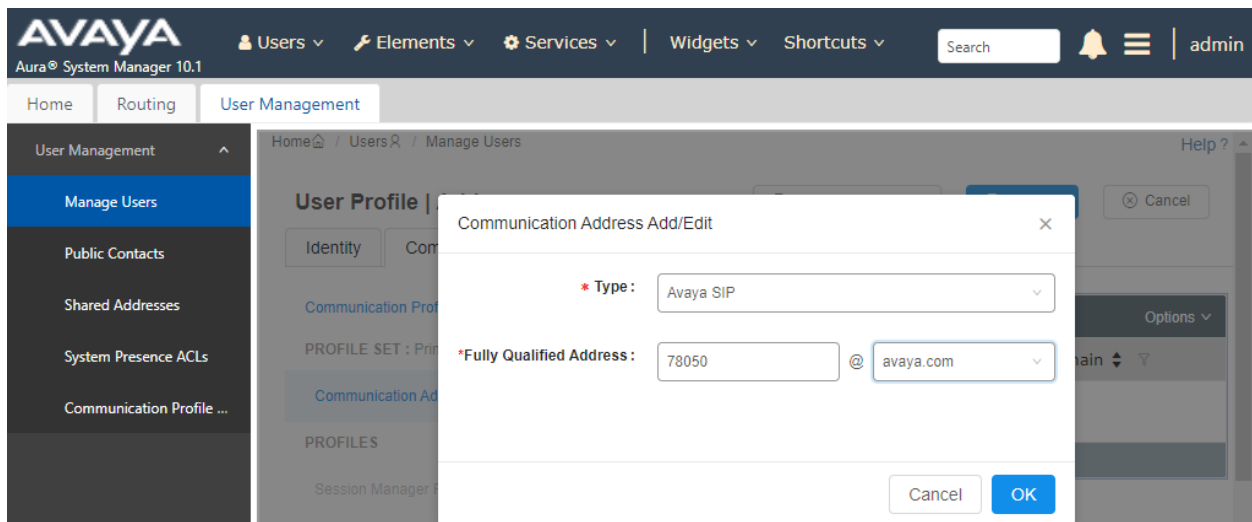
Select the **Communication Profile** tab. Next, click on **Communication Profile Password**. For **Comm-Profile Password** and **Re-enter Comm-Profile Password**, enter the desired password for the SIP user required for registration. Click **OK**.



The screenshot shows the Avaya Aura System Manager 10.1 interface. The 'User Management' tab is selected, and the 'Manage Users' sub-tab is active. A dialog box titled 'Comm-Profile Password' is open, prompting the user to enter a password for the communication profile. The dialog includes fields for 'Comm-Profile Password' and 'Re-enter Comm-Profile Password', both masked with dots. A green checkmark is visible next to the 'Re-enter' field, indicating the passwords match. There is a 'Generate Comm-Profile Password' link and 'Cancel' and 'OK' buttons at the bottom.

6.6.3. Communication Address

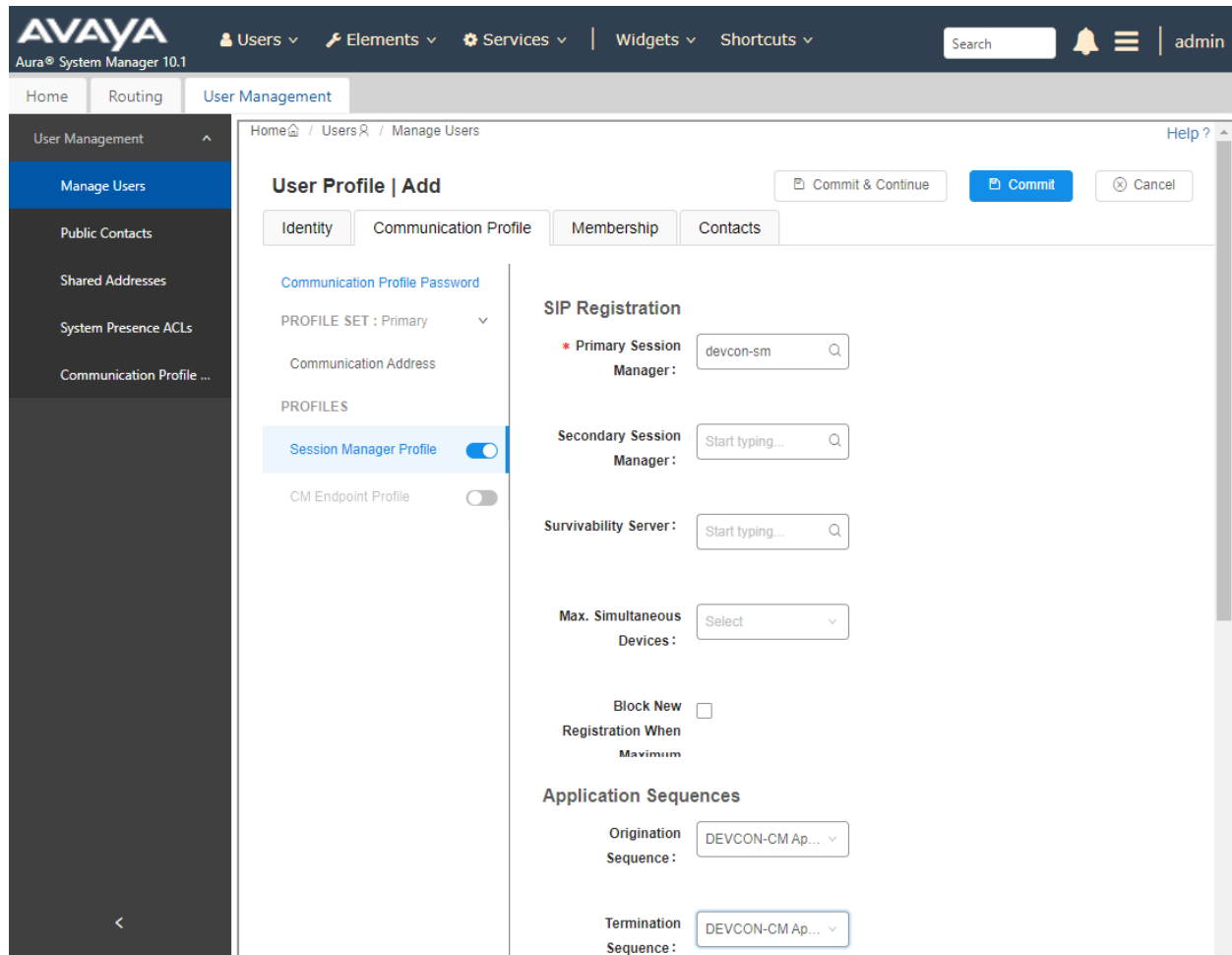
Click on **Communication Address** and then click **New** to add a new entry. The **Communication Address Add/Edit** dialog box is displayed as shown below. Set **Type** to *Avaya SIP*. For **Fully Qualified Address**, enter the SIP user extension (e.g., 78050) and domain name (e.g., *avaya.com*). Click **OK**.



The screenshot shows the Avaya Aura System Manager 10.1 interface. The 'User Management' tab is selected, and the 'Manage Users' sub-tab is active. A dialog box titled 'Communication Address Add/Edit' is open, prompting the user to add or edit a communication address. The dialog includes a 'Type' dropdown menu set to 'Avaya SIP' and a 'Fully Qualified Address' field with a text input for the extension (78050) and a dropdown for the domain (avaya.com). There are 'Cancel' and 'OK' buttons at the bottom.

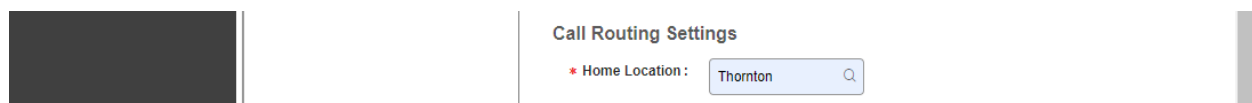
6.6.4. Session Manager Profile

Click on toggle button by **Session Manager Profile**. For **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence**, and **Home Location**, select the values corresponding to the applicable Session Manager and Communication Manager. Retain the default values in the remaining fields.



The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 10.1', and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows the 'User Management' section with options like Manage Users, Public Contacts, Shared Addresses, System Presence ACLs, and Communication Profile. The main content area is titled 'User Profile | Add' and contains several tabs: Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section with a dropdown for 'PROFILE SET : Primary' and a 'Communication Address' field. Below this is a 'PROFILES' section with a 'Session Manager Profile' toggle (turned on) and a 'CM Endpoint Profile' toggle (turned off). The 'SIP Registration' section includes fields for 'Primary Session Manager' (devcon-sm), 'Secondary Session Manager' (Start typing...), and 'Survivability Server' (Start typing...). There is also a 'Max. Simultaneous Devices' dropdown (Set) and a 'Block New Registration When Maximum' checkbox. The 'Application Sequences' section includes 'Origination Sequence' (DEVCON-CM Ap...) and 'Termination Sequence' (DEVCON-CM Ap...). At the bottom, the 'Call Routing Settings' section shows 'Home Location' (Thornton).

Scroll down to the **Call Routing Settings** section to configure the **Home Location**.



This screenshot shows a close-up of the 'Call Routing Settings' section. It features a single field labeled 'Home Location' with the value 'Thornton' entered and a search icon to its right.

6.6.5. CM Endpoint Profile

Click on **CM Endpoint Profile**. For **System**, select the value corresponding to the applicable Communication Manager. For **Extension**, enter the SIP user extension (e.g., 78050). For **Template**, 9641SIP_DEFAULT_CM_8_1 was selected.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and tabs for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile icon are also present. The left sidebar shows a hierarchy: 'User Management' > 'Manage Users' > 'Public Contacts' > 'Shared Addresses' > 'System Presence ACLs' > 'Communication Profile ...'. The main content area is titled 'User Profile | Add' and features tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active. The form includes the following fields and options:

- Communication Profile Password:** PROFILE SET : Primary (dropdown), Communication Address, PROFILES (Session Manager Profile and CM Endpoint Profile, both with toggle switches).
- * System:** devcon-cm (dropdown).
- * Profile Type:** Endpoint (dropdown).
- Use Existing Endpoints:** ☐.
- * Extension:** 78050 (text input with a search icon).
- * Template:** 9641SIP_DEFAULT_CM_8_1 (dropdown with a search icon).
- * Set Type:** 9641SIP (text input).
- Security Code:** Enter Security Code (text input).
- Port:** IP (dropdown with a search icon).
- Voice Mail Number:** (text input).
- Preferred Handle:** Select (dropdown).
- Calculate Route Pattern:** ☐.
- SIP URI:** Select (dropdown).
- Sip Trunk:** aar (text input).
- Delete on Unassign from User or on Delete:** ☒.
- Override Endpoint Name and Localized Name:** ☒.
- Allow H.323 and SIP Endpoint Dual Registration:** ☐.

Buttons at the top right include 'Commit & Continue', 'Commit', and 'Cancel'. A 'Help ?' link is located in the top right corner of the main content area.

7. Configure Avaya Meetings Server

This section covers the configuration of an endpoint for Poly video endpoints with the default maximum bandwidth and inviting Poly video endpoints to a meeting using dial out from a virtual room. The configuration is performed via the Meetings Management Administration Portal. A virtual room is assigned a Meeting ID and can be used for instant meetings. However, scheduled meetings are also supported, but not covered in these Application Notes.

Note: It is assumed that the integration of Meetings Media Server, Meeting WebRTC Gateway, and SBC have already been configured.

7.1. Access Meetings Management Administrator Portal

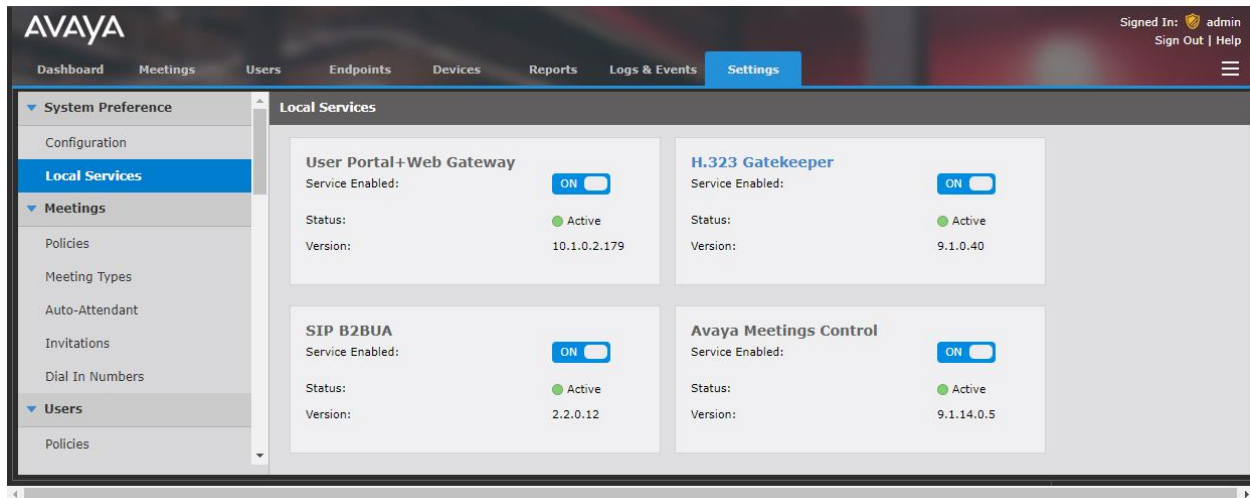
Log into the Meetings Management administrator portal by using the URL **Error! Hyperlink reference not valid.** in an Internet browser, where *<hostname>* is the Meetings Management server hostname or FQDN. The login screen below is displayed. Log in with the appropriate credentials.



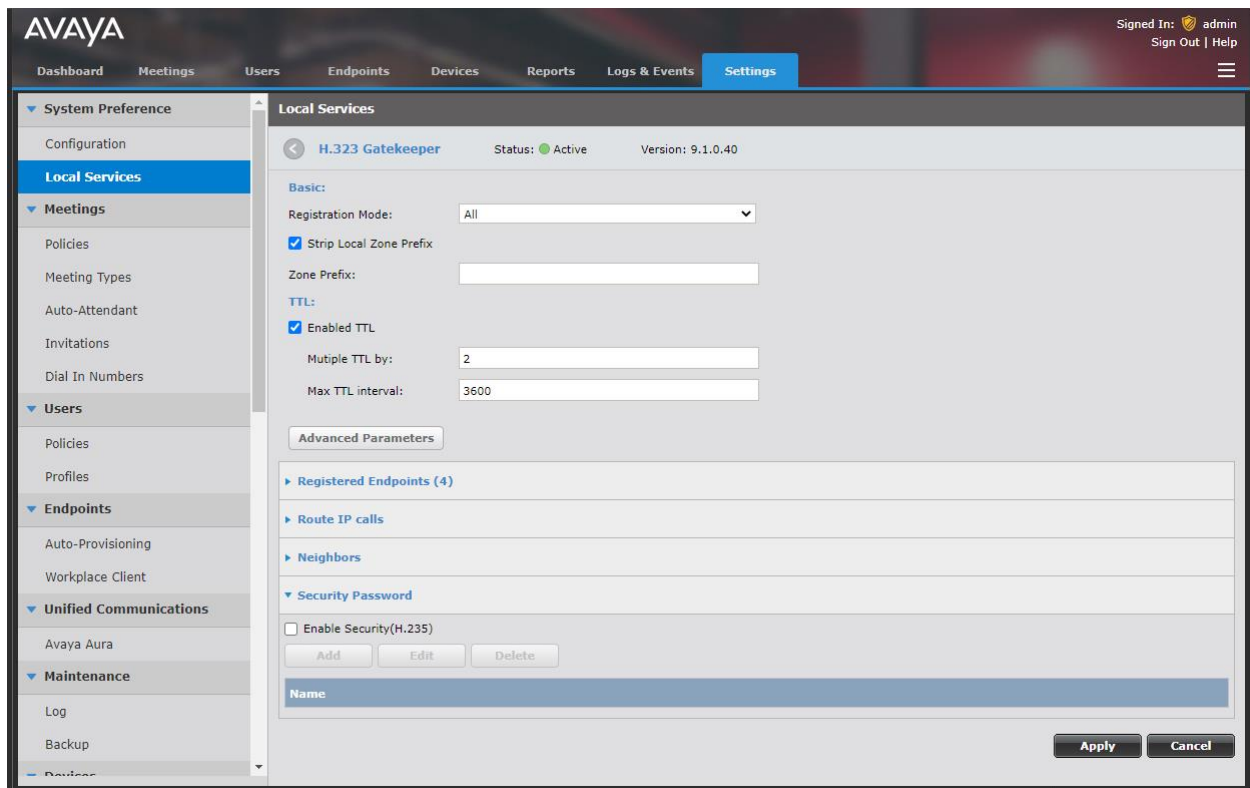
The image shows the login interface for the Avaya Meetings Management Administration portal. The background is dark with a blurred image of a person. The title 'Avaya Meetings Management Administration' is centered at the top in a light blue font. Below it, a subtitle reads 'Sign in to configure and manage your videoconferencing deployment.' in a smaller, lighter font. There are two white input fields: 'Username' and 'Password'. Below the 'Username' field is a checkbox labeled 'Keep me signed in'. To the right of the checkbox is a 'Sign In' button. Below the 'Sign In' button is a link that says 'Forgot Password?'. At the bottom of the screen, a copyright notice reads '© 2022 Avaya Inc. All Rights Reserved.'

7.2. Configure H.323 Gatekeeper

Navigate to **Settings** → **Local Services** and click on **H.323 Gatekeeper** to configure the internal H.323 gatekeeper in Meetings Management.



In this configuration, no **Zone Prefix** was used. To require authentication (optional), enable **Security (H.235)** and configure a **Name** and **Password** in the **Security Password** section. This should match the H.323 settings for Poly video endpoints in **Section 9.3**. In this configuration, **Security Password** was disabled.



7.3. Configure Advanced Parameters

When Poly video endpoints join a PIN-protected meeting using H.323, the **addDTMFsInSimAltCaps** parameter must be set to *1* in Meetings Media Server so that Poly video endpoints send PIN via out-of-band DTMF using H.245. Navigate to **Devices** and click on the Meetings Media Server. Next, select the **Configuration** tab and click on **Advanced Parameters**.

The screenshot shows the Avaya Meetings Media Server configuration interface. The top navigation bar includes 'Dashboard', 'Meetings', 'Users', 'Endpoints', 'Devices' (selected), 'Reports', 'Logs & Events', and 'Settings'. The user is signed in as 'admin'. The left sidebar shows a tree view of devices, with 'Media & Signaling' selected. The main content area is titled 'Avaya Meetings Media Server: devcon-amms' and has tabs for 'Info', 'Configuration' (selected), 'Certificate', 'Licensing', 'Alarms', 'Events', and 'Access'. The 'Configuration' tab is divided into several sections: 'Basic Settings' (Name: devcon-amms, Location: Home, Service FQDN: devcon-amms.avaya.com, Public URL branch: meetings.avaya.com/wcs1, In Maintenance: unchecked, Secure Connection: checked, Master Media Server for Cascading: checked), 'H.323 Settings' (Required Gatekeeper: LocalAppServer (127.0.0.1), Current Gatekeeper: 10.64.102.140), 'SIP Settings' (SIP Proxy Server: 10.64.102.140, Transport Type: TLS, Turn/Stun Server: None), 'NTP Settings' (NTP Server: 128.138.141.172, Time Zone: GMT-07:00 Mountain Standard Time), 'Network Settings' (DNS Server 1: 10.64.102.114, DNS Server 2: , DNS Search List: avaya.com), and 'IP Address' (IP Address: 10.64.102.141, Subnet Mask: 255.255.255.0, Default Gateway: 10.64.102.1, Local FQDN: devcon-amms.avaya.com). At the bottom of the configuration area is an 'Advanced Parameters' button. The bottom right of the interface has 'Apply' and 'Cancel' buttons.

In **Advanced Parameters**, set the **addDTMFsInSimAltCaps** parameter to *1* as shown below.

The screenshot shows the 'Advanced Parameters' dialog box. The 'ID' field is set to 'adddtmfinsimaltcaps' with a red asterisk indicating it is required. The 'Name' field is 'NULL', 'Parameter' is empty, and 'Value' is '1'. The 'Description' field contains the text: 'Add DTMFs in SimAltCaps and to the H323 caps (forced). Values limit: [0-Disable/1-Enable]'. There are 'Get', 'Apply', 'Clear', and 'Close' buttons. Below the form is a table of other parameters.

Name	Value	Edit
Video Base Port	12000	
Audio Base Port	16384	
H323 RAS port number	1719	
H323 SIG port number	1720	
Registration mode	MCU	
SIP support video fast update	1	
SIP BFCP base port	3400	
No Self-See		
Enable DTMF conference control	1	
Register conference ID	1	
Participants join conference policy	All	

7.4. Configure SIP Trunk to SBC

To add a SIP trunk for inbound and outbound calls to/from Meetings Server, navigate to **Devices** → **Media & Signaling** → **SIP Servers** in the left pane and click **Add**.

The screenshot displays the Avaya Management System (AMS) interface. The top navigation bar includes the Avaya logo and tabs for Dashboard, Meetings, Users, Endpoints, **Devices**, Reports, Logs & Events, and Settings. The user is logged in as 'admin' with options to Sign Out or Help.

The left sidebar shows a tree view of the system configuration. Under 'Devices by Type', the 'Media & Signaling' section is expanded, showing 'Media Servers', 'Gateways', 'H.323 Gatekeepers', and 'H.323 Edge Servers'. The 'SIP Servers' option is selected and highlighted in blue.

The main content area is titled 'SIP Servers (1)' and contains a table with the following data:

	Name	Model	IP Address	SIP Domain	Location
<input type="checkbox"/>	SBCE Dial Out	Avaya Aura	10.64.102.230	avaya.com	Home

At the top of the main content area, there are 'Add' and 'Delete' buttons, and a search bar with the placeholder text 'Search'.

In the **SIP Server** configuration, configure the following fields:

- Name: Provide a descriptive name (e.g., *SBCE Dial Out*).
- IP Address/FQDN: Specify an internal SBC IP address (e.g., *10.64.102.230*).
- Port: Specify port *5061*.
- Transport Type: Select *TLS*.
- Model: Select *Avaya Aura*.
- Location: Select *Home*.
- SIP Domain: Specify SIP domain (e.g., *avaya.com*).

The SIP trunk uses TLS. In this configuration, a TLS certificate signed by the System Manager certificate authority was used. The signing and import of the TLS certificate are not shown in these Application Notes.

The screenshot shows the Avaya System Manager interface. The top navigation bar includes 'Dashboard', 'Meetings', 'Users', 'Endpoints', 'Devices' (selected), 'Reports', 'Logs & Events', and 'Settings'. The user is logged in as 'admin'. The left sidebar shows a tree view with 'Devices by Location' (All, Home) and 'Devices by Type' (Management & Directory, Media & Signaling). The main content area is titled 'Modify SIP Server' and contains a 'Basic Settings' section. The fields are: Name (SBCE Dial Out), IP Address/FQDN (10.64.102.230), Port (5061), Transport Type (TLS), Model (Avaya Aura), Location (Home), and SIP Domain (avaya.com). There are 'OK' and 'Cancel' buttons at the bottom right.

7.5. Configure Corporate Address Book

The built-in LDAP server in Meetings Management may be used to allow endpoints to search the corporate address book, which includes the entries in the endpoint list configured in **Section 7.6**. Navigate to **Settings → Address Book → Corporate Address Book** and configure the following fields:

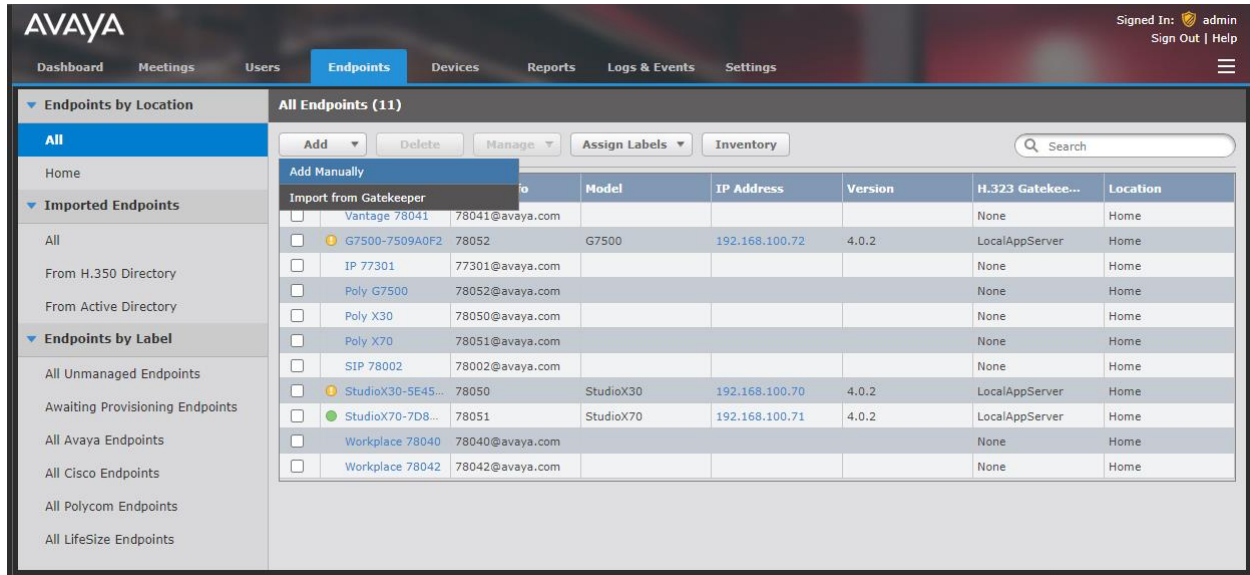
- **Enable Corporate Address Book:** Enable this option.
- **Listening Port:** Accept the default port 389 for non-secure LDAP connection.
- **LDAP Distinguished Name (DN) Suffix:** Select *None*. When none is used, the Base DN in **Section 9.7** should be set to *ou=users*.
- **Allow Anonymous Login:** Enable this option if anonymous LDAP connections are allowed.

The screenshot shows the Avaya Meetings Management interface. The left sidebar contains a navigation menu with categories: HTTP Protocol, Servers, Alarm, Address Book, Advanced, and Topology. The 'Address Book' category is expanded, and 'Corporate Address Book' is selected. The main panel displays the configuration for the Corporate Address Book. The 'Enable Corporate Address Book' checkbox is checked. The 'Listening Port' is set to 389, and the 'Listening Port for secure connection using SSL' is set to 636. The 'LDAP Distinguished Name (DN) Suffix' is set to 'None'. The 'Allow Anonymous Login' checkbox is unchecked, and the 'Enforce secure connection using TLS' checkbox is also unchecked. Below the configuration fields is an 'Events' table showing a list of search and bind requests. The table has columns for Event Name, Time, User Name, host, and Duration. The 'Apply' button is located at the bottom right of the configuration panel.

Event Name	Time	User Name	host	Duration
Search Request	08/23/2023 11:51	test1	192.168.100.71:53584	0.0
Bind Request	08/23/2023 11:51	test1	192.168.100.71:53584	0.0
Search Request	08/23/2023 11:47	test1	10.64.102.230:30325	0.0
Bind Request	08/23/2023 11:47	test1	10.64.102.230:30325	0.0
Search Request	08/23/2023 11:30	test1	10.64.102.230:28643	0.0
Bind Request	08/23/2023 11:30	test1	10.64.102.230:28643	0.0
Search Request	08/23/2023 10:51	test1	192.168.100.71:53334	0.0
Bind Request	08/23/2023 10:51	test1	192.168.100.71:53334	0.0
Search Request	08/23/2023 10:47	test1	10.64.102.230:22054	0.0

7.6. Configure Endpoints

This section covers the configuration of H.323 and SIP endpoints. To add an endpoint, select the **Endpoints** tab, then click **Add** button and select the **Add Manually** option as shown below. Alternatively, H.323 endpoints may be imported from the internal H.323 gatekeeper.



The screenshot shows the Avaya DevConnect Application interface. The top navigation bar includes tabs for Dashboard, Meetings, Users, Endpoints, Devices, Reports, Logs & Events, and Settings. The 'Endpoints' tab is selected. On the left, there is a sidebar with 'Endpoints by Location' and 'Endpoints by Label' sections. The main area displays 'All Endpoints (11)' with a table of endpoints. The 'Add' button is highlighted, and the 'Add Manually' option is selected in the dropdown menu.

Name	Model	IP Address	Version	H.323 Gatekeeper	Location
Vantage 78041	78041@avaya.com			None	Home
G7500-7509A0F2	78052	192.168.100.72	4.0.2	LocalAppServer	Home
IP 77301	77301@avaya.com			None	Home
Poly G7500	78052@avaya.com			None	Home
Poly X30	78050@avaya.com			None	Home
Poly X70	78051@avaya.com			None	Home
SIP 78002	78002@avaya.com			None	Home
StudioX30-5E45...	78050	192.168.100.70	4.0.2	LocalAppServer	Home
StudioX70-7D8...	78051	192.168.100.71	4.0.2	LocalAppServer	Home
Workplace 78040	78040@avaya.com			None	Home
Workplace 78042	78042@avaya.com			None	Home

7.6.1. Configure H.323 Endpoint

Poly video endpoints cannot be managed by Meetings Management (e.g., upgrade endpoint) so only basic endpoint dialing information is required to call and invite endpoint to meetings. In the **Add Endpoint** screen, configure the following fields:

- **Name:** Type the name to identify the endpoint (e.g., *StudioX30-5E45C2FC*).
- **Description:** Provide a description for the endpoint (optional).
- **Type:** Select *Single Codec Endpoint* as the model of endpoint.
- **Protocol:** Select *IP (H.323)* from the list.
- **E.164/IP Address:** Specify the H.323 extension (e.g., *78050*).
- **Registered To:** Select *LocalAppServer (127.0.0.1)*.
- **Location:** Select the location of the endpoint from the list (e.g., *Home*).
- **Max Bandwidth:** Define the default maximum bandwidth for the endpoint (e.g., *4096 Kbps*).
- **Visible in the directory of other endpoints:** Enable this option to include this endpoint in LDAP search results.
- **Manage (upgrade and configure) this endpoint:** Disable this option since the Poly video endpoint cannot currently be managed by Meetings Management.

The screenshot shows the Avaya Meetings Management interface. The top navigation bar includes 'Dashboard', 'Meetings', 'Users', 'Endpoints' (selected), 'Devices', 'Reports', 'Logs & Events', and 'Settings'. The user is signed in as 'admin'. The left sidebar shows a tree view with 'Endpoints by Location' (All, Home) and 'Endpoints by Label' (All Unmanaged Endpoints, Awaiting Provisioning Endpoints, All Avaya Endpoints, All Cisco Endpoints, All Polycom Endpoints, All LifeSize Endpoints). The main panel is titled 'Endpoint: StudioX30-5E45C2FC' and contains the following fields:

- Name: StudioX30-5E45C2FC
- Description: (empty)
- Type: Single Codec Endpoint
- Protocol: IP (H.323)
- E.164/IP Address: 78050
- Registered To: LocalAppServer (127.0.0.1)
- Location: Home
- Max Bandwidth: 4096 (Kbps)

Below the fields are four checkboxes:

- ☒ Visible in the directory of other endpoints (H.323-enabled endpoints, desktop and mobile)
- ☐ VIP Endpoint (experience will not be downgraded during call)
- ☒ Enable Gallery Layouts (recommended for single monitor endpoints)
- ☐ Manage (upgrade and configure) this endpoint

At the bottom right are 'OK' and 'Cancel' buttons.

7.6.2. Configure SIP Endpoint

Poly video endpoints cannot be managed by Meetings Management (e.g., upgrade endpoint) so only basic endpoint dialing information is required to call and invite endpoint to meetings. In the **Add Endpoint** screen, configure the following fields:

- **Name:** Type the name to identify the endpoint (e.g., *Poly X30*).
- **Description:** Provide a description for the endpoint (optional).
- **Type:** Select *Single Codec Endpoint* as the model of endpoint.
- **Protocol:** Select *IP (SIP)* from the list.
- **SIP URI:** Provide the endpoint identifier followed by the SIP server domain name (e.g., 78050@avaya.com).
- **Location:** Select the location of the endpoint from the list (e.g., *Home*).
- **Max Bandwidth:** Define the default maximum bandwidth for the endpoint (e.g., *2048 Kbps*).
- **Visible in the directory of other endpoints:** Enable this option to include this endpoint in LDAP search results.
- **Manage (upgrade and configure) this endpoint:** Disable this option since the Poly video endpoint cannot currently be managed by Meetings Management.

The screenshot displays the 'Add Endpoint' configuration window in the Avaya Meetings Management application. The sidebar on the left shows the 'Endpoints' section selected, with sub-options like 'All', 'Home', 'Imported Endpoints', and 'Endpoints by Label'. The main form area contains the following fields and options:

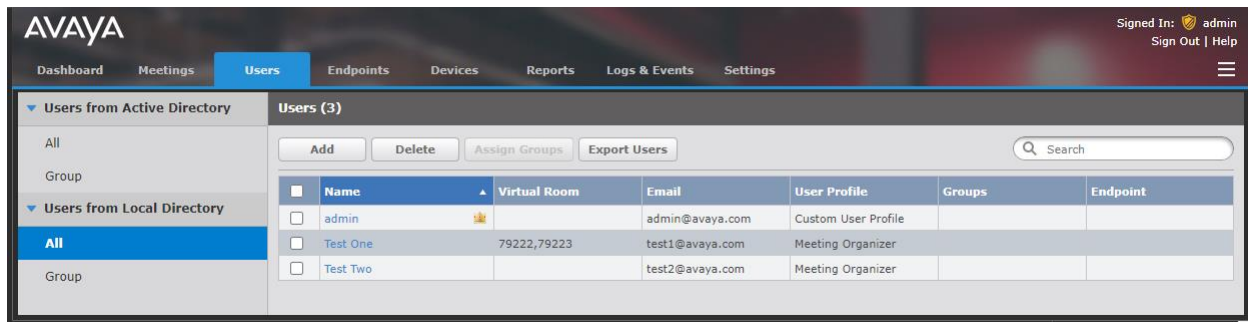
- Name:** Text input field containing 'Poly X30'.
- Description:** Text input field (empty).
- Type:** Dropdown menu set to 'Single Codec Endpoint'.
- Protocol:** Dropdown menu set to 'IP (SIP)'.
- SIP URI:** Text input field containing '78050@avaya.com'.
- Location:** Dropdown menu set to 'Home'.
- Max Bandwidth:** Dropdown menu set to '2048' (Kbps).
- Visible in the directory of other endpoints (H.350-enabled endpoints, desktop and mobile):** Checked checkbox.
- VIP Endpoint (experience will not be downgraded during call):** Unchecked checkbox.
- Manage (upgrade and configure) this endpoint:** Unchecked checkbox.

At the bottom right of the form are 'OK' and 'Cancel' buttons.

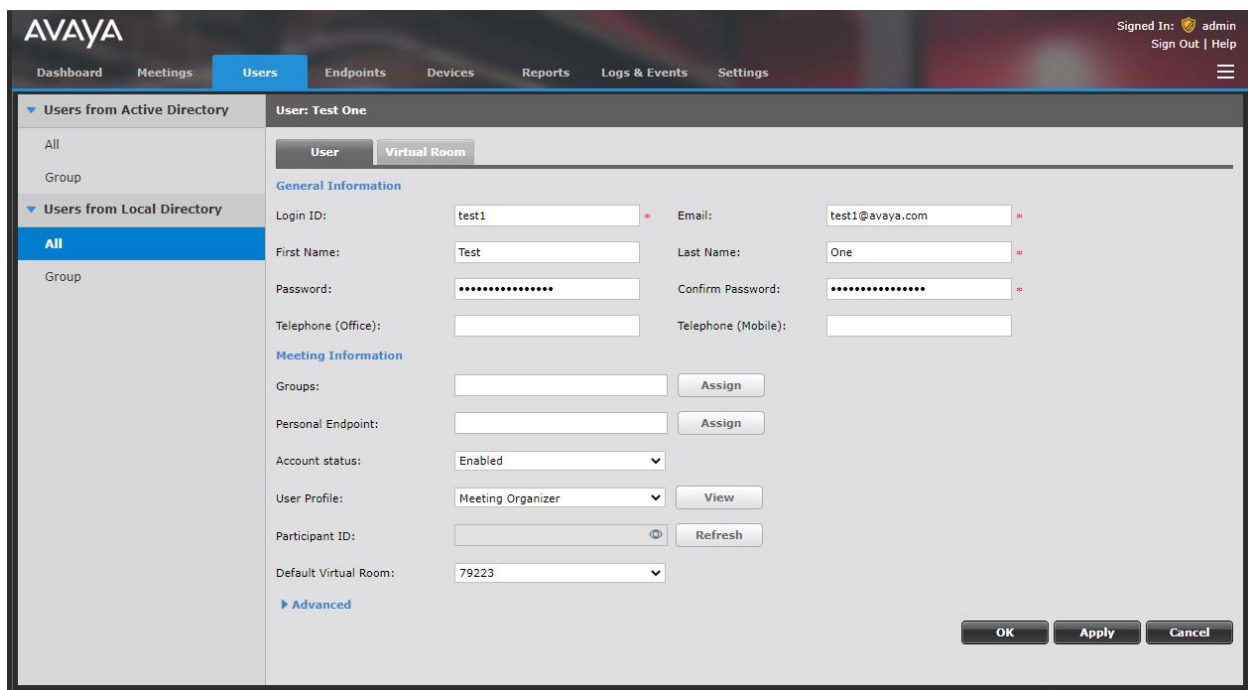
7.7. Configure Virtual Rooms

A virtual room is an online space used to connect multiple participants in a video conference. In addition to hosting video conferences, virtual rooms can offer features, such as protecting meetings with a PIN and dialing out to endpoints when the moderator joins a meeting.

Virtual rooms are assigned to a user. To create or assign a virtual room to a user, select the **Users** tab, and then click on an existing user or click **Add** to create one.



The configuration of an existing user is shown below. Next, select the **Virtual Room** tab.



In the **Virtual Room** tab, set the **Select** field to the appropriate virtual room number to modify an existing one or *Create New Virtual Room* to create a new virtual room. Configure **Virtual Room Number**, **Virtual Room Name**, and **Meeting Type** as shown below. Enable **Protect meeting with a PIN** and specify the **PIN**, if desired. Other fields may be left at default values. Scroll down to the bottom of the screen to the **Select Participants** button.

AVAYA

Dashboard Meetings **Users** Endpoints Devices Reports Logs & Events Settings

▼ Users from Active Directory

All

Group

▼ Users from Local Directory

All

Group

User: Test One

User Virtual Room

Select: 79222

Virtual Room Number: 79222 *

Virtual Room Name: Test Virtual Room *

Description:

Meeting Type: 71 - Default Service

Maximum Room Endpoints: 250

Maximum Participants: 250

Moderator PIN:

☐ Protect meeting with a PIN:

☒ Use permanent PIN:

☐ Use one-time PIN for each meeting

☐ Protect meeting with participant ID

Advanced

Audio prompts for Guest User: English (U.S.)

Meeting invitation language: English (U.K.)

Preferred dial-in number location: All Locations

Max Participants to play the entry/exit tone: 6

Max Participants to play the entry/exit name announcement: 20

Entry Announcement: Tone

Exit Announcement: Tone

☒ Allow instant meetings

☒ Allow requests to join locked meetings

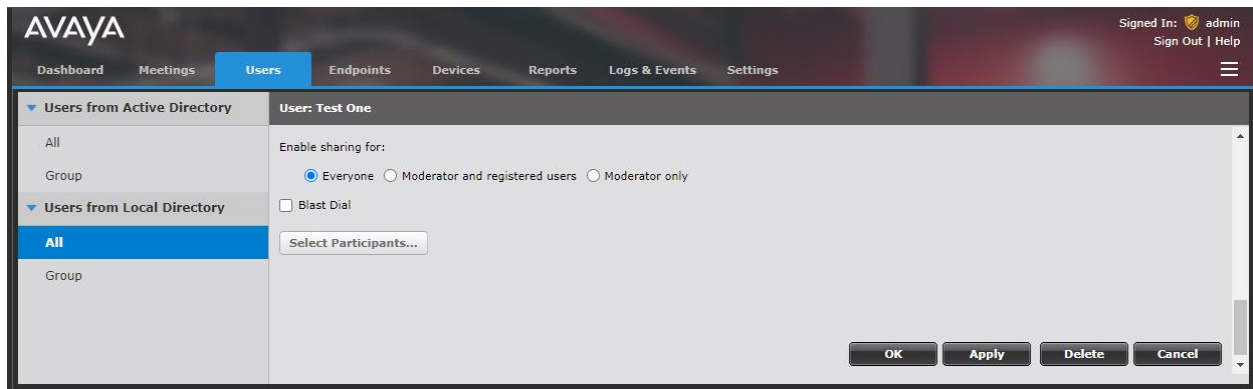
☐ Place participants in a 'waiting room' until the moderator joins the meeting

☐ Terminate meeting after the last moderator leaves

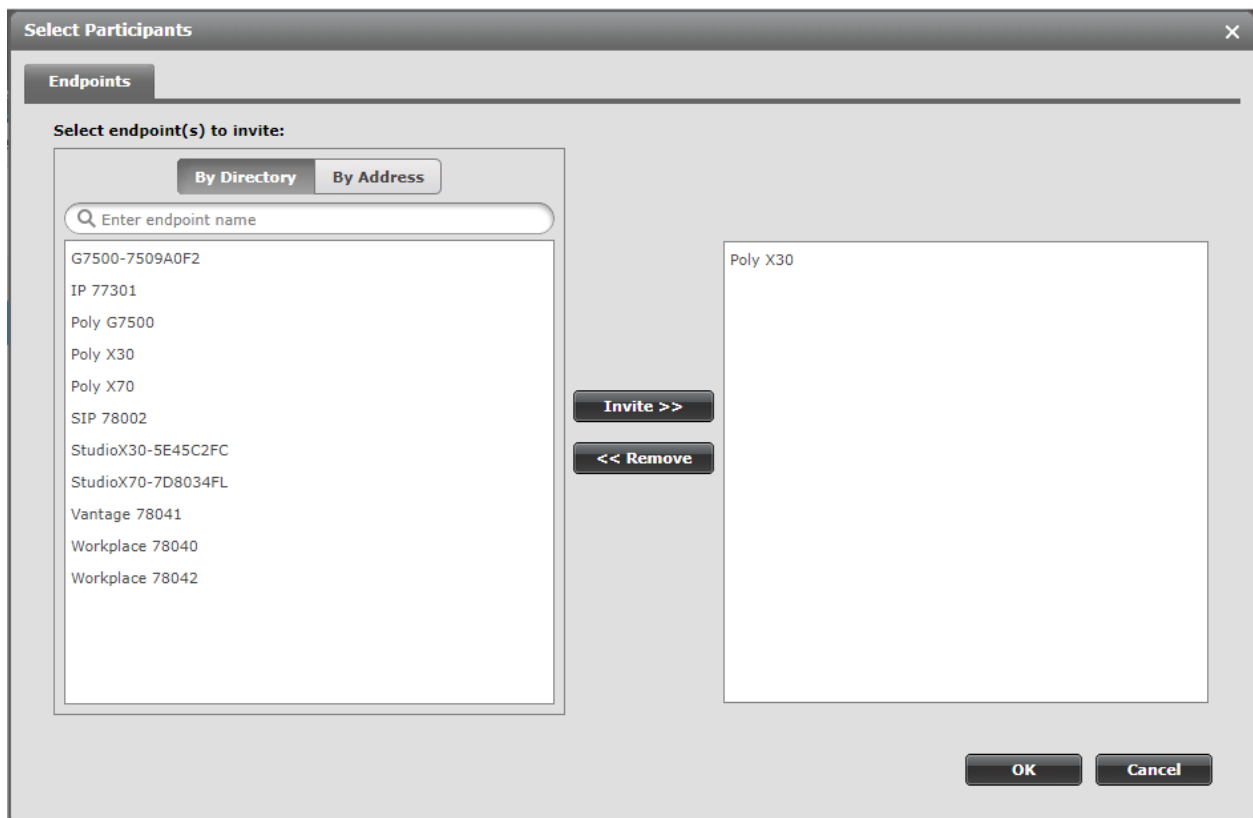
Enable sharing for:

☒ Everyone ☐ Moderator and registered users ☐ Moderator only

Click **Select Participants** button to select the endpoints that should receive a dial out call when the moderator starts the meeting.



In **Select Participants**, select the Poly video endpoint (e.g., *Poly X30*) added in **Section 7.6.1** and/or **7.6.2**. When the moderator starts the meeting, the Poly video endpoint will be invited via a dial out call.



8. Configure Avaya Session Border Controller

SBC is part of the Meetings Server Over-The-Top deployment. This section covers the SBC configuration required for the Meetings Server integration, including the SIP trunks and routing to Meetings Server.

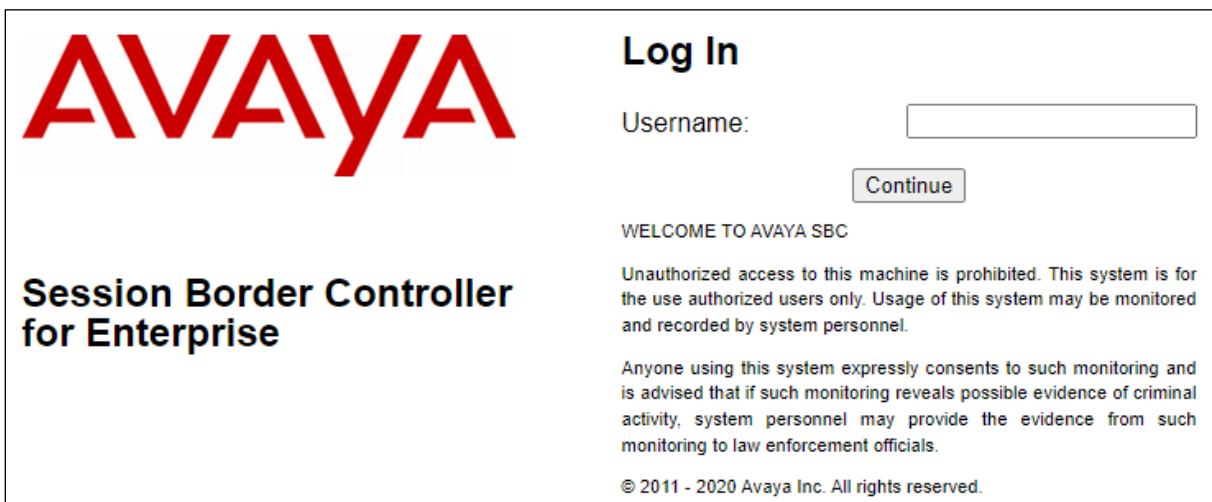
Note: For this solution, SBC provided connectivity to Meetings Server and Session Manager. In addition, it supported registering Avaya and Poly video endpoints to Session Manager through SBC. These Application Notes will focus on the Meetings Server integration. It is assumed that the SIP trunk and routing to Session Manager, URL rewriting using reverse proxy, and WebRTC support are already in place and will not be covered in these Application Notes.

This section covers the following SBC configuration:

- Launch SBC Web Interface
- Administer Server Interworking Profile
- Administer SIP Server
- Administer Routing Profile
- Administer Application Rule
- Administer Media Rule
- Administer End Point Policy Group
- Administer Media Interfaces
- Administer Signaling Interfaces
- Administer End Point Flows
- Administer Application Relay for LDAP

8.1. Launch SBC Web Interface

Access the SBC EMS web interface by using the URL **https://<ip-address>/sbc** in an Internet browser window, where <ip-address> is the IP address of the SBC management interface. The screen below is displayed. Log in using the appropriate credentials.



The image shows the Avaya Session Border Controller (SBC) web interface login page. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, there is a "Log In" section with a "Username:" label and a text input field. Below the input field is a "Continue" button. Further down, there is a "WELCOME TO AVAYA SBC" message, followed by a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." Below this is a consent statement: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 2020 Avaya Inc. All rights reserved." is visible.

After logging in, the Dashboard will appear as shown below. SBC configuration screens are accessed by navigating the menu tree in the left pane. Select **Device** → **SBCE** from the top menu.

Device: EMS ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice Management▸ System Administration▸ TemplatesBackup/Restore▸ Monitoring & Logging

Dashboard

Information		
System Time	02:06:47 PM EDT	Refresh
Version	10.1.1.0-35-21872	
GUI Version	10.1.1.0-21872	
Build Date	Mon Apr 18 07:57:04 UTC 2022	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	08/11/2023 12:21:11 EDT	
Failed Login Attempts	0	

Active Alarms (past 24 hours)	
None found.	

Incidents (past 24 hours)	
SBCE: unable to get local issuer certificate	
SBCE: unable to get local issuer certificate	
SBCE: Heartbeat Successful, Server is UP	
SBCE: unable to get local issuer certificate	
SBCE: unable to get local issuer certificate	

Add

Notes
No notes found.

Installed Devices

EMS

SBCE

JAO; Reviewed:
SPOC 9/8/2023

Avaya DevConnect Application Notes
©2023 Avaya LLC. All Rights Reserved.

43 of 83
Poly-AMS

8.2. Administer Server Interworking Profile

A **Server Interworking Profile** defines a set of parameters that aid in the interworking between SBC and connected server (e.g., Meetings Server). The Meetings Server interworking profile was cloned from the pre-existing **avaya-ru** profile and is shown below. The **General** tab below shows the default settings.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▾ Configuration Profiles
 Domain DoS
 Server Interworking
 Media Forking
 Routing
 Topology Hiding
 Signaling Manipulation
 URI Groups
 SNMP Traps
 Time of Day Rules
 FGDN Groups
 Reverse Proxy Policy
 URN Profile
 Recording Profile
 H248 Profile
 IP/URI Blocklist Profile
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Interworking Profiles: Meetings

Add

Interworking Profiles

cs2100

avaya-ru

Avaya-SM

PSTN-SIP

Meetings

Meetings

Rename Clone Delete

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation Advanced

General

Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

JAO; Reviewed:
SPOC 9/8/2023

Avaya DevConnect Application Notes
©2023 Avaya LLC. All Rights Reserved.

44 of 83
Poly-AMS

Select the **Advanced** tab and configure as shown below. Disable **Has Remote SBC**.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

Server

Interworking

Media Forking

Routing

Topology Hiding

Signaling

Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy

Policy

URN Profile

Recording Profile

Interworking Profiles: Meetings

Add

RenameCloneDelete

Click here to add a description.

Interworking Profiles

cs2100

avaya-ru

Avaya-SM

PSTN-SIP

Meetings

DTMF

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

Record RoutesBoth Sides

Include End Point IP for Context LookupYes

ExtensionsAvaya

Diversion ManipulationNo

Has Remote SBCNo

Route Response on Via PortNo

Relay INVITE Replace for SIPRECNo

MOBX Re-INVITE HandlingNo

NATing for 301/302 RedirectionYes

DTMF

DTMF SupportNone

Edit

8.3. Administer SIP Server

A **SIP Server** definition is required for each server connected to SBC. Add a **SIP Server** for Meetings Server, specifically the Meetings Management server.

The **General** tab of the Meetings Management SIP server was configured as shown below. The IP address (e.g., *10.64.102.140*) and Port *5061* were used. TLS transport was used for the Meetings Management SIP trunk. It is assumed that the **TLS Client Profile** for the SBC internal A1 interface to which Meetings Management was connected has already been configured and is not shown in these Application Notes.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesSIP ServersH248 ServersLDAPRADIUSDomain PoliciesTLS ManagementNetwork & FlowsDMZ ServicesMonitoring & Logging

SIP Servers: MeetingsM

AddRenameCloneDelete

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Server TypeTrunk Server

TLS Client ProfilesbceInternalA1

DNS Query TypeNONE/A

IP Address / FQDNPortTransport

10.64.102.1405061TLS

Edit

JAO; Reviewed:
SPOC 9/8/2023

Avaya DevConnect Application Notes
©2023 Avaya LLC. All Rights Reserved.

46 of 83
Poly-AMS

The **Heartbeat** tab was configured as shown below. This allows SBC to send SIP OPTIONS to Meetings Management.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesSIP ServersH248 ServersLDAPRADIUSDomain PoliciesTLS ManagementNetwork & FlowsDMZ ServicesMonitoring & Logging

SIP Servers: MeetingsMAddRenameCloneDelete

Server ProfilesPSTN-SIPPhone-SBC-PU...Phone-SBC-PU...Session ManagerVoIPSPMeetingsMMeetingsWebGW

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Enable Heartbeat☒

MethodOPTIONS

Frequency30 seconds

From URIdevcon-sbce@10.64.102.231

To URImeetings@10.64.102.140

Edit

The **Advanced** tab was configured as shown below. **Grooming** was enabled and the **Interworking Profile** was set to the one configured in **Section 8.2**. All other tabs were left with their default values.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesSIP ServersH248 ServersLDAPRADIUSDomain PoliciesTLS ManagementNetwork & FlowsDMZ ServicesMonitoring & Logging

SIP Servers: MeetingsMAddRenameCloneDelete

Server ProfilesPSTN-SIPPhone-SBC-PU...Phone-SBC-PU...Session ManagerVoIPSPMeetingsMMeetingsWebGW

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Enable DoS Protection☐

Enable Grooming☒

Interworking ProfileMeetings

Signaling Manipulation ScriptNone

Securable☐

Enable FGDN☐

Tolerant☐

URI GroupNone

NG911 Support☐

Edit

JAO; Reviewed:
SPOC 9/8/2023

Avaya DevConnect Application Notes
©2023 Avaya LLC. All Rights Reserved.

47 of 83
Poly-AMS

8.4. Administer Routing Profile

A **Routing Profile** is used to specify the next-hop for a SIP message. A routing profile is applied only after traffic has matched a **Server Flow** defined in **Section 8.10.2**. The IP addresses and ports defined here will be used as destination addresses for signaling. Create a routing profile for Meetings Management as shown below.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy

Policy

Routing Profiles: Meetings

Add

RenameCloneDelete

Click here to add a description.

Routing Profile

Update PriorityAdd

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1		default	Priority	10.64.102.140:5061	TLS	EditDelete

8.5. Administer Application Rule

An **Application Rule** specifies whether audio and video traffic are allowed to enter the enterprise network and originate from within the enterprise network. In addition, an application rule specifies the maximum number of concurrent voice and video sessions that can be processed. To add or modify an application rule, navigate to **Domain Policies → Application Rules** in the left pane. In the center pane, select an existing application rule (e.g., *Meetings-AR*) or add a new one. If a different application rule is used for routing calls through Session Manager, then that application rule should be modified as shown below.

The application rule used to support audio and video calls to Meetings Server is shown below. In this example, 200 concurrent incoming and outgoing audio and video calls are supported.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▾ Domain Policies

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

Charging Rules

End Point Policy Groups

Session Policies

Application Rules: Meetings-AR

Add

Rename

Clone

Delete

Click here to add a description.

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	200
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	200

Miscellaneous

CDR SupportOff

RTCP Keep-AliveNo

Edit

JAO; Reviewed:
SPOC 9/8/2023

Avaya DevConnect Application Notes
©2023 Avaya LLC. All Rights Reserved.

49 of 83
Poly-AMS

8.6. Administer Media Rule

A **Media Rule** defines the processing to be applied to the selected media. A media rule is one component of the larger **End Point Policy Group** defined in **Section 8.7**, which is applied to **Server Flows** in **Section 8.10.2**.

To add or modify a media rule, navigate to **Domain Policies** → **Media Rules** in the left pane. In the center pane, select an existing media rule (e.g., *Meetings-MR*) or add a new one. The **Encryption** tab displays the audio and video encryption being used as shown below.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo.

The left sidebar contains a navigation menu with the following items:

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
 - Application Rules
 - Border Rules
 - Media Rules**
 - Security Rules
 - Signaling Rules
 - Charging Rules
 - End Point Policy Groups
 - Session Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

The main content area is titled 'Media Rules: Meetings-MR'. It features an 'Add' button and a list of media rules: default-low-med, default-low-m..., default-high, default-high-enc, avaya-low-me..., RTP-SRTP, RTP-SRTP-P..., and **Meetings-MR**. The 'Meetings-MR' rule is selected, and its configuration is displayed in the center pane.

The configuration for 'Meetings-MR' is shown in the 'Encryption' tab. It includes sections for Audio Encryption, Video Encryption, and Miscellaneous. The 'Encryption' tab is active, and the 'Audio Encryption' section is expanded.

Audio Encryption Configuration:

Property	Value
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 SRTP_AES_CM_128_HMAC_SHA1_32 RTP
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption Configuration:

Property	Value
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 SRTP_AES_CM_128_HMAC_SHA1_32 RTP
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous Configuration:

Property	Value
Capability Negotiation	<input checked="" type="checkbox"/>

The 'Edit' button is located at the bottom right of the configuration pane.

As mentioned in **Section 2.2**, BFCP must be disabled in the media rule so that Poly video endpoints can join meetings using video. If BFCP is enabled, Poly video endpoints would halt video and join the meeting as audio only.

Select the **Advanced** tab and verify that **BFCP Enabled** is unchecked and **FECC Enabled** is checked.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

- Application Rules
- Border Rules
- Media Rules**
- Security Rules
- Signaling Rules
- Charging Rules
- End Point Policy Groups
- Session Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Media Rules: Meetings-MR

Add

Media Rules

default-low-med

default-low-m...

default-high

default-high-enc

avaya-low-me...

RTP-SRTP

RTP-SRTP-P...

Meetings-MR

Rename

Clone

Delete

Click here to add a description.

Encryption

Codec Prioritization

Advanced

QoS

Silencing

Silencing Enabled ☐

Binary Floor Control Protocol

BFCP Enabled ☐

Far End Camera Control

FECC Enabled ☒

Real Time Text

RTT Enabled ☐

ANAT

ANAT Enabled ☐

Media Line Compliance

Media Line Compliance Enabled ☐

Interactive Connectivity Establishment

ICE Gateway Support ☐

Port Change on New Offer

Audio Port Change on New Offer Enabled ☐

Video Port Change on New Offer Enabled ☐

Edit

8.7. Administer End Point Policy Group

An **Endpoint Policy Group** is a set of policies that will be applied to traffic between the SBC and an endpoint (connected server), such as Meetings Server.

The application and media rules configured above are assigned to an **End Point Policy Group** configuration as shown below. The **End Point Policy Group** is applied to the traffic as part of the **Server Flows** defined in **Section Error! Reference source not found.**

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

Charging Rules

End Point Policy Groups

Session Policies

▸ TLS Management

▸ Network & Flows

Policy Groups: Meetings

Add

Policy Groups

default-low

default-low-enc

default-med

default-med-enc

default-high

default-high-enc

avaya-def-low-enc

avaya-def-high-sub...

avaya-def-high-server

RTP-SRTP

RTP-SRTP-PCIPAL

Meetings

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	Meetings-AR	default	Meetings-MR	default-low	default	None	Off	Edit

8.8. Administer Media Interfaces

A **Media Interface** defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of SBC. Media Interfaces need to be defined for each SIP server to send and receive media.

Navigate to **Networks & Flows → Media Interface** to define a new **Media Interface**. During the compliance test, the following interfaces were defined. For security reasons, public IP addresses have been redacted. The media interfaces used for this solution are listed below.

- **MeetingsMedia:** Interface used by Meetings Management for calls with Session Manager.
- **PrivateMedia:** Interface used by Session Manager for calls with Meetings Management.
- **PublicMediaRW:** Interface used by remote workers for media.
- **PrivateMediaRW:** Interface used by Session Manager for calls with Poly video endpoints and Poly video endpoints within the enterprise network.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 Advanced Options
▸ DMZ Services
▸ Monitoring & Logging

Media Interface

Media Interface

Add

Name	Media IP Network	Port Range	TLS Profile	Buffer Size [KB]	
PublicMedia	10.64.101.101 Public-B1 (B1, VLAN 0)	35000 - 40000	None	500	Edit Delete
PublicMediaB2	[REDACTED] Public-B2 (B2, VLAN 0)	35000 - 40000	None	500	Edit Delete
PublicMediaRW	10.64.101.102 Public-B1 (B1, VLAN 0)	50000 - 55000	sbceExternalB1	500	Edit Delete
MeetingsMedia	10.64.102.230 Private-A1 (A1, VLAN 0)	35000 - 40000	sbceInternalA1	500	Edit Delete
PrivateMediaRW	10.64.102.108 Private-A1 (A1, VLAN 0)	35000 - 40000	None	500	Edit Delete
PrivateMedia	10.64.102.106 Private-A1 (A1, VLAN 0)	35000 - 40000	None	500	Edit Delete
MedTunExt	[REDACTED] Public-B2 (B2, VLAN 0)	35000 - 40000	sbceExternalB2-Media	500	Edit Delete
MedTunInt	10.64.102.231 Private-A1 (A1, VLAN 0)	35000 - 40000	sbceInternalA1	500	Edit Delete

8.9. Administer Signaling Interfaces

A **Signaling Interface** defines an IP address, protocols and listen ports that SBC can use for signaling. Create a signaling interface for both the internal and external sides of SBC. Signaling Interface needs to be defined for each SIP server to send and receive SIP signaling messages.

Navigate to **Networks & Flows → Signaling Interface** to define a new **Signaling Interface**. During the compliance test, the following interfaces were defined. For security reasons, public IP addresses have been redacted. The signaling interfaces used for this solution are listed below.

- **MeetingsSignaling:** Interface used by Meetings Management for calls with Session Manager.
- **PrivateSignaling:** Interface used by Session Manager for calls with Meetings Management.
- **PublicSignalingRW:** Interface used by remote workers for SIP signaling.
- **PrivateSignalingRW:** Interface used by Session Manager for calls with remote Workers and Poly video endpoints within the enterprise network.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 Advanced Options
▸ DMZ Services
▸ Monitoring & Logging

Signaling Interface

Signaling Interface

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
PublicSignaling	10.64.101.101 Public-B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete
PublicSignalingRW	10.64.101.102 Public-B1 (B1, VLAN 0)	---	---	5061	sbceExternalB1	Edit Delete
ServiceProvider	[REDACTED] Public-B2 (B2, VLAN 0)	5060	5060	---	None	Edit Delete
MeetingsSignaling	10.64.102.230 Private-A1 (A1, VLAN 0)	---	---	5061	sbceInternalA1	Edit Delete
PrivateSignalingRW	10.64.102.108 Private-A1 (A1, VLAN 0)	---	---	5061	sbceInternalA1	Edit Delete
SigTunInt	10.64.102.231 Private-A1 (A1, VLAN 0)	---	---	5061	sbceInternalA1	Edit Delete
PublicSignalingB2	[REDACTED] Public-B2 (B2, VLAN 0)	---	5062	5061	sbceExternalB2	Edit Delete
PrivateSignaling	10.64.102.106 Private-A1 (A1, VLAN 0)	5060	5060	5061	sbceInternalA1	Edit Delete

8.10. Administer End Point Flows

End Point Flows are used to determine the endpoints (connected servers) involved in a call in order to apply the appropriate policies. When a packet arrives at SBC, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles that control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In this configuration, the endpoints are Meetings Server, Session Manager, and remote workers. This section covers the **End Point Flows** for Meetings Management, Session Manager, and remote workers.

8.10.1. Subscriber Flows

Navigate to **Network & Flows → End Point Flows** and select the **Subscriber Flows** tab. The **Subscriber Flow** used for remote workers is shown below. A subscriber flow is required for Poly video endpoints that register to Session Manager through SBC as remote workers. If Poly video endpoints are located within the enterprise network, the **Subscriber Flow** would use an internal SBC interface for the **Signaling Interface** (not shown).

Device: SBCE ▼ Alarms Incidents Status ▼ Logs ▼ Diagnostics Users Settings ▼ Help ▼ Log Out

Session Border Controller for Enterprise

AVAYA

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
 - System Parameters
 - Configuration Profiles
 - Services
 - Domain Policies
 - TLS Management
- Network & Flows
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows**
 - Session Flows
 - Advanced Options
- DMZ Services
- Monitoring & Logging

End Point Flows

Subscriber Flows Server Flows

Add

Modifications made to an End-Point Flow will only take effect on new registrations or re-registrations.

Hover over a row to see its description.

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group	
1	Remote Worker	*	*	*	RTP-SRTP	View Clone Edit Delete

The subscriber flow for remote worker is shown below. Note that the **Signaling Interface** and **Media Interface** specify an external SBC interface. In this configuration, the remote workers used TLS and SRTP.

If Poly video endpoints are located within the enterprise network, the **Signaling Interface** and **Media Interface** would specify an internal SBC interface.

View Flow: Remote Worker

X

Criteria

Flow Name	Remote Worker
URI Group	*
User Agent	*
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	PublicSignalingRW

Optional Settings

TLS Client Profile	sbceExternalB1
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	*
Media Interface	PublicMediaRW
Secondary Media Interface	None
End Point Policy Group	RTP-SRTP
Routing Profile	Session Manager
Presence Server Address	---
FQDN Support	<input type="checkbox"/>
IP / URI Blocklist Profile	None / Disabled

8.10.2. Server Flows

Navigate to **Network & Flows** → **End Point Flows** and select the **Server Flows** tab. The Meetings Management and Session Manager **Server Flows** used in the compliance test are shown below. The following subsections will review the settings for each server flow.

The relevant Meetings Management Server Flow is shown below.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 Advanced Options
▸ DMZ Services
▸ Monitoring & Logging

End Point Flows

Subscriber Flows Server Flows

Add

Modifications made to a Server Flow will only take effect on new sessions.

Hover over a row to see its description.

SIP Server: MeetingsM
Update

Priority	Flow Name	URI Group	Received Interface	Signalling Interface	End Point Policy Group	Routing Profile	
1	Meetings Mgmt (B2BUA)	*	SigTunInt	SigTunInt	Meetings	default	View Clone Edit Delete
2	Meetings to SM	*	PrivateSignaling	MeetingsSignaling	Meetings	Session Manager	View Clone Edit Delete

SIP Server: MeetingsWebGW

Priority	Flow Name	URI Group	Received Interface	Signalling Interface	End Point Policy Group	Routing Profile	
1	Meetings Web Gateway	*	SigTunInt	SigTunInt	Meetings	default	View Clone Edit Delete

JAO; Reviewed:
SPOC 9/8/2023

Avaya DevConnect Application Notes
©2023 Avaya LLC. All Rights Reserved.

57 of 83
Poly-AMS

The following server flow is for calls between Meetings Management and Session Manager.

Edit Flow: Meetings to SM X

Flow Name	<input type="text" value="Meetings to SM"/>
SIP Server Profile	<input type="text" value="MeetingsM"/> ▼
URI Group	<input type="text" value="*"/> ▼
Transport	<input type="text" value="*"/> ▼
Remote Subnet	<input type="text" value="*"/>
Received Interface	<input type="text" value="PrivateSignaling"/> ▼
Signaling Interface	<input type="text" value="MeetingsSignaling"/> ▼
Media Interface	<input type="text" value="MeetingsMedia"/> ▼
Secondary Media Interface	<input type="text" value="None"/> ▼
End Point Policy Group	<input type="text" value="Meetings"/> ▼
Routing Profile	<input type="text" value="Session Manager"/> ▼
Topology Hiding Profile	<input type="text" value="None"/> ▼
Signaling Manipulation Script	<input type="text" value="None"/> ▼
Remote Branch Office	<input type="text" value="Any"/> ▼
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	<input type="text"/>

Finish

For the compliance test, two server flows were created for Session Manager: one for calls with Meetings Management and one for calls with remote workers.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for Enterprise

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services▸ Domain Policies▸ TLS Management▸ Network & FlowsNetwork ManagementMedia InterfaceSignaling InterfaceEnd Point Flows

End Point Flows

Subscriber FlowsServer Flows

SIP Server: Session Manager

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Meetings	*	MeetingsSignaling	PrivateSignaling	Meetings	Meetings	View Clone Edit Delete
2	Session Manager Flow	*	PublicSignaling	PrivateSignaling	RTP-SRTP	PSTN-SIP	View Clone Edit Delete
3	Remote Worker Flow	*	PublicSignalingRW	PrivateSignalingRW	RTP-SRTP	default	View Clone Edit Delete

The following server flow is for calls between Session Manager and Meetings Management.

Edit Flow: Meetings X

Flow Name	<input type="text" value="Meetings"/>
SIP Server Profile	<input type="text" value="Session Manager"/>
URI Group	<input type="text" value="*/"/>
Transport	<input type="text" value="*/"/>
Remote Subnet	<input type="text" value="*/"/>
Received Interface	<input type="text" value="MeetingsSignaling"/>
Signaling Interface	<input type="text" value="PrivateSignaling"/>
Media Interface	<input type="text" value="PrivateMedia"/>
Secondary Media Interface	<input type="text" value="None"/>
End Point Policy Group	<input type="text" value="Meetings"/>
Routing Profile	<input type="text" value="Meetings"/>
Topology Hiding Profile	<input type="text" value="Session Manager"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Remote Branch Office	<input type="text" value="Any"/>
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	<input type="text"/>

The following server flow is for calls between Session Manager and remote workers.

Edit Flow: Remote Worker Flow X

Flow Name	Remote Worker Flow
SIP Server Profile	Session Manager ▼
URI Group	* ▼
Transport	* ▼
Remote Subnet	*
Received Interface	PublicSignalingRW ▼
Signaling Interface	PrivateSignalingRW ▼
Media Interface	PrivateMediaRW ▼
Secondary Media Interface	None ▼
End Point Policy Group	RTP-SRTP ▼
Routing Profile	default ▼
Topology Hiding Profile	Session Manager ▼
Signaling Manipulation Script	None ▼
Remote Branch Office	Any ▼
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Finish

8.11. Administer Application Relay for LDAP

An **Application Relay** is required to support LDAP requests from Poly video endpoints. Navigate to **DMZ Services** → **Relay** and select the **Application Relay** tab. **Add** to create an LDAP application relay.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
▸ DMZ Services
 Relay
 Firewall
 TURN/STUN
 PPM Mapping
▸ Monitoring & Logging

Relay Services: SBCE

Application Relay Reverse Proxy XMPP H248 Relay

Add

Name	Type	Remote IP/FQDN:Port	Remote Transport	Listen IP:Port Network	Listen Transport	Connect IP Network	
Remote-Worker-RTCP	RTCP	10.64.102.113:5005	UDP	10.64.101.102:5005 Public-B1 (B1, VLAN 0)	UDP	10.64.102.108 Private-A1 (A1, VLAN 0)	View Edit Delete
Meetings LDAP	LDAP	10.64.102.140:389	TCP	10.64.101.102:389 Public-B1 (B1, VLAN 0)	TCP	10.64.102.230 Private-A1 (A1, VLAN 0)	View Edit Delete

For the LDAP Application Relay, configure the following fields:

- **Name:** Specify a name for the application relay (e.g., *Meetings LDAP*).
- **Service Type:** Select *LDAP*.
- **Remote IP/FQDN:** Specify the Meetings Management IP address (e.g., *10.64.102.140*).
- **Remote Port:** Specify port 389 for non-secure connection to LDAP server.
- **Remote Transport:** Set to *TCP*.
- **Listen IP:** Specify the external SBC interface for remote workers and the internal SBC interface for Poly video endpoints located within the enterprise.
- **Listen Port:** Specify port 389 for non-secure LDAP connection from Poly video endpoints.
- **Connect IP:** Specify the internal SBC interface used to connect to the LDAP server.
- **Listen Transport:** Set to *TCP*.

Edit Application Relay
X

General Configuration

Name

Meetings LDAP

Service Type

LDAP ▾

Remote Configuration

Remote IP/FQDN

10.64.102.140

Remote Port

389

Remote Transport

TCP ▾

Device Configuration

Listen IP

Public-B1 (B1, VLAN 0) ▾

10.64.101.102 ▾

Listen Port

389

Connect IP

Private-A1 (A1, VLAN 0) ▾

10.64.102.230 ▾

Listen Transport

TCP ▾

Additional Configuration

Whitelist Flows

☐

Use Relay Actors

☐

Options

Use Ctrl+Click to select or deselect multiple items.

RTCP Monitoring

End-to-End Rewrite

Hop-by-Hop Traceroute

Bridging

Finish

9. Configure Poly Studio X30 Video Bar


This section covers the configuration of Studio X30 to register directly Session Manager from within the enterprise or to Session Manager through SBC as a remote worker. This configuration requires following steps:

- Access Studio X30 Web Interface
- Administer Provider
- Administer SIP Settings
- Administer Call Settings
- Administer Dialing Options
- Administer Directory Servers
- Install Certificate

Note: This section covers the Studio X30 configuration, but also applies to Studio X70 and G7500.

9.1. Access Studio X30 Web Interface

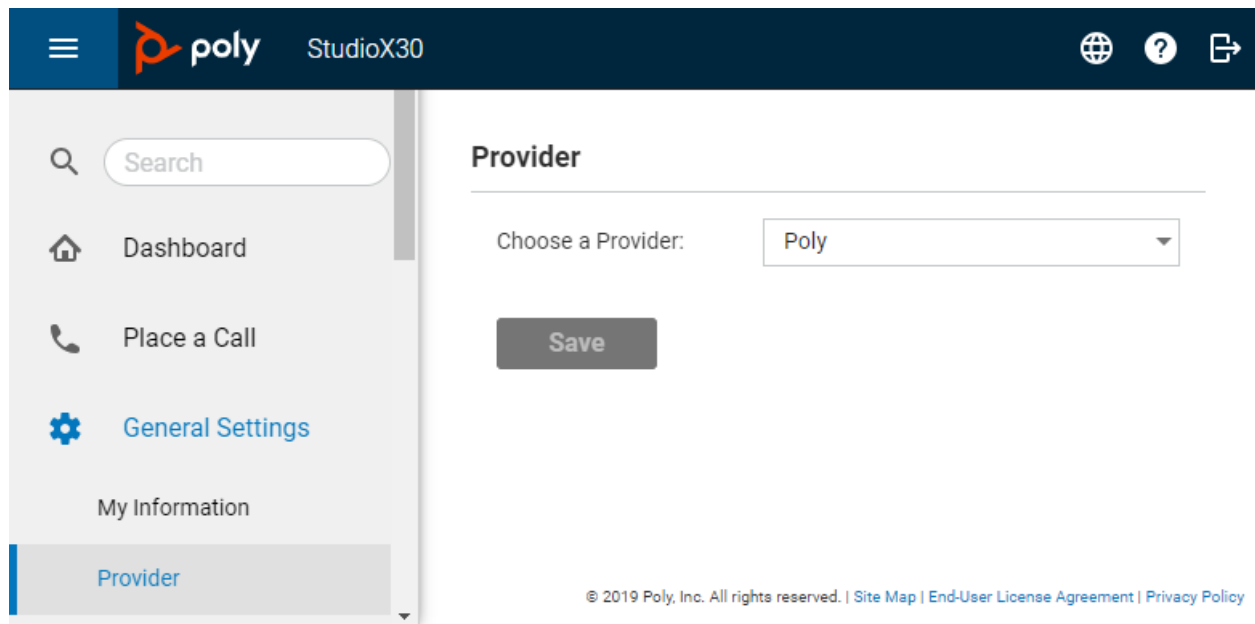
Access the Studio X30 web interface by using the URL `https://<ip-address>` in a web browser, where `<ip-address>` is the Studio X30 IP address. Log in using the appropriate credentials.



The screenshot shows the Poly StudioX30 Sign In web interface. At the top is the Poly logo, followed by the text "StudioX30" and "Sign In". Below this is a language selection dropdown menu currently set to "American English". There are two input fields for "User Name" and "Password". A large grey "Sign In" button is positioned below the input fields. At the bottom, there is a copyright notice "© 2019 Poly, Inc. All rights reserved." and two links: "End-User License Agreement" and "Privacy Policy".

9.2. Administer Provider

Navigate to **General Settings** → **Provider** in the left pane and verify *Poly* is set as the provider as shown below.



The screenshot displays the Poly StudioX30 Admin interface. The top navigation bar is dark blue with the Poly logo, the text 'StudioX30', and icons for a globe, help, and share. The left sidebar is light gray and contains a search bar and several menu items: 'Dashboard', 'Place a Call', 'General Settings' (highlighted with a blue gear icon), 'My Information', and 'Provider' (highlighted with a blue bar). The main content area is white and titled 'Provider'. It features a label 'Choose a Provider:' next to a dropdown menu that currently shows 'Poly'. Below the dropdown is a dark gray 'Save' button. At the bottom of the page, there is a copyright notice: '© 2019 Poly, Inc. All rights reserved. | [Site Map](#) | [End-User License Agreement](#) | [Privacy Policy](#)'.

9.3. Administer H.323 Settings

This section covers the H.323 configuration for Studio X30 to register with the internal H.323 gatekeeper in Meetings Management. If H.323 is not required, this section could be skipped and the reader may proceed to the next section to configure the SIP interface. Navigate to **Call Configuration → H.323** and configure the following fields:

- **Enable H.323:** Enable this option to allow Studio X30 to make and receive H.323 calls.
- **H.323 Name:** Specify a descriptive name (e.g., *StudioX30-5E45C2FC*).
- **H.323 Extension (E.164):** Specify the H.323 extension (e.g., *78050*).
- **Use Gatekeeper:** Select *Specify*.
- **Require Authentication:** Enable this option if authentication is required. If enabled, the **User Name** and **Password** must be specified and should match the **Security Password** configuration in Meetings Server as shown in **Section 7.2**.
- **Primary Gatekeeper IP Address:** Specify IP address of internal H.323 gatekeeper in Meetings Management (e.g., *10.64.102.140*).

Note: In this configuration, the H.323 interface was used to join meetings and establish point-to-point calls with other Poly video endpoints registered to the internal H.323 gatekeeper in Meetings Management. To establish calls with other Avaya SIP endpoints registered to Session Manager, the SIP interface was used. The SIP interface is configured in the next section.

The screenshot shows the StudioX30 web interface for H.323 configuration. The top navigation bar includes the Poly logo, 'StudioX30', and icons for help, search, and share. A left sidebar contains a search bar and a menu with options: Dashboard, Place a Call, General Settings, Network, Call Configuration (highlighted), Call Settings, Dialing Preference, Recent Calls, H.323 (highlighted), and SIP. The main content area is titled 'H.323' and contains the following configuration fields:

Enable IP H.323:	<input checked="" type="checkbox"/>
Registration Status:	Registered
H.323 Name:	StudioX30-5E45C2FC
H.323 Extension (E.164):	78050
Use Gatekeeper:	Specify
Require Authentication:	<input type="checkbox"/>
Current Gatekeeper IP Address:	10.64.102.140:1719
Primary Gatekeeper IP Address:	10.64.102.140

A 'Save' button is located at the bottom of the configuration fields. At the bottom right of the page, there is a copyright notice: '© 2019 Poly, Inc. All rights reserved. | Site Map | End-User License Agreement | Privacy Policy'.

9.4. Administer SIP Settings

This section covers the SIP configuration so that Studio X30 can register to Session Manager through SBC as a SIP endpoint. In this configuration, the SIP interface is *required* to establish calls with other Avaya SIP endpoints registered to Session Manager. Navigate to **Call Configuration → SIP** and configure the following fields:

- **Enable SIP:** Enable this option to allow Studio X30 to make and receive SIP calls.
- **SIP Server Configuration:** Select *Specify*.
- **Transport Protocol:** Select *TLS* to allow secure SIP signaling.
- **Sign-in Address:** Specify SIP extension (e.g., 78050) assigned to Studio X30 on Session Manager.
- **User Name:** Specify SIP extension used to register with Session Manager.
- **Password:** Specify password used for SIP registration.
- **Registrar Server:** Specify IP address of the external interface on SBC to register as a remote worker or specify the IP address of the internal interface on SBC to register to Session Manager through SBC, if Studio X30 is located within the enterprise network. *For this solution, the Poly video endpoints should not register directly to Session Manager.*

9.5. Administer Call Settings

Navigate to **Call Configuration** → **Call Settings** to configure the **Require AES Encryption for Calls** field. Set this field to *When Available* so that Poly video endpoints can join meetings using H.323 without SRTP. If a Poly video endpoint uses SIP to join a meeting, the call could still be established using SRTP. This field may also be set to *Required for All Calls* if only SIP calls are established with Poly video endpoints, which would enforce SRTP for media.

Call Settings

Maximum Time in Call:	8 Hours
Auto Answer Point-to-Point Call:	No
Auto-Merge Incoming Call to Current Call:	No
Display Icons in a Call:	<input checked="" type="checkbox"/>
Display System Name Instead of SIP Address:	<input type="checkbox"/>
Display Status Info When Sharing Full Screen Content	<input checked="" type="checkbox"/>
Preferred 'Place a Call' Navigation:	Keypad
Require AES Encryption for Calls:	When Available

© 2019 Poly, Inc. All rights reserved. | [Site Map](#) | [End-User License Agreement](#) | [Privacy Policy](#)

9.6. Administer Dialing Options

Navigate to **Call Configuration → Dialing Preference** to configure the following fields:

- **Enable Audio-Only Calls:** Select this checkbox to allow audio-only calls on the TC8 touch controller.
- **Video Dialing Order Preference 1:** Specify *IP-H.323* so that video calls would first be attempted using H.323.
- **Video Dialing Order Preference 2:** Specify *SIP* so that video calls would be attempted using SIP, if H.323 failed.
- **Audio Dialing Order Preference 1:** Specify *IP-H.323* so that audio calls would first be attempted using H.323.
- **Audio Dialing Order Preference 2:** Specify *SIP* so that audio calls would be attempted using SIP, if H.323 failed.
- **Preferred Speed for Placed Calls:** Specify the desired bandwidth for placed calls. If video freezes during a call, try lowering the speed (e.g., 2048).

The screenshot shows the Poly StudioX30 web interface. The top navigation bar includes the Poly logo, 'StudioX30', and icons for help, search, and share. The left sidebar contains a search bar and a list of navigation items: Dashboard, Place a Call, General Settings, Network, Call Configuration (highlighted), Call Settings, Dialing Preference (highlighted), Recent Calls, H.323, SIP, Audio / Video, and Security. The main content area is titled 'Dialing Preference' and is divided into two sections: 'Dialing Options' and 'Preferred Speeds'.

Dialing Options

Scalable Video Coding Preference (H.264):	AVC Only
Enable H.239:	<input checked="" type="checkbox"/>
Enable Audio-Only Calls:	<input checked="" type="checkbox"/>
Call Type Order:	Video
Video Dialing Order Preference 1:	IP H.323
Video Dialing Order Preference 2:	SIP
Audio Dialing Order Preference 1:	H.323
Audio Dialing Order Preference 2:	SIP

Preferred Speeds

Preferred Speed for Placed Calls:	2048
Maximum Speed for Received Calls:	6144

© 2019 Poly, Inc. All rights reserved. | [Site Map](#) | [End-User License Agreement](#) | [Privacy Policy](#)

9.7. Administer Directory Servers

A directory server must be configured for Poly video endpoints to connect to the built-in LDAP server in Meetings Management to allow searches in the corporate address book. Navigate to **Servers → Directory Servers** to configure the following fields:

- **Server Type:** Set to *LDAP*.
- **Server Address:** Set to internal or external SBC IP address depending on whether the Poly video endpoint is connected to the enterprise network or Internet.
- **Server Port:** Set to port 389 for non-secure LDAP connection.
- **Base DN (Distinguished Name):** Set to *ou=users* if **LDAP Distinguished Name (DN) Suffix** is set to *none* in **Section 7.5**.
- **Authentication:** Set to *Basic* to require authentication. Set to *Anonymous*, if authentication is not required and allowed on Meetings Management in **Section 7.5**.
- **Bind DN (Distinguished Name):** Specify name of user account if authentication is required.
- **Password:** Specify password of user account if authentication is required.

The screenshot displays the Poly StudioX30 web interface. The top navigation bar includes the Poly logo, 'StudioX30', and icons for help, search, and settings. A left sidebar contains a search bar and a list of navigation items: Dashboard, Place a Call, General Settings, Network, Call Configuration, Audio / Video, Security, Servers (highlighted), Calendaring Service, Directory Servers (highlighted), and Provisioning Server. The main content area is titled 'Directory Servers' and contains the following configuration fields:

- Server Type: LDAP (dropdown)
- Registration Status: Registered
- Server Address: 10.64.101.102
- Server Port: 389
- Base DN (Distinguished Name): ou=users
- Multitiered Directory Default Group DN: (empty)
- Use SSL (Secure Socket Layer): ☐
- Authentication Type: Basic (dropdown)
- Bind DN (Distinguished Name): test1
- Password: (masked with dots)

A 'Save' button is located at the bottom left of the configuration area. At the bottom right, a footer contains the copyright notice: '© 2019 Poly, Inc. All rights reserved. | Site Map | End-User License Agreement | Privacy Policy'.

9.8. Install Certificate

Navigate to **Security** → **Certificates** to install certificates. To support TLS, click on **Install Certificate** to import the TLS certificate from Avaya Aura® System Manager, the certificate authority. This certificate is used for Session Manager and SBC. When done, the user-installed certificates are listed and can be viewed.

The screenshot displays the Poly StudioX30 interface for managing certificates. The left sidebar shows the navigation menu with 'Security' and 'Certificates' highlighted. The main content area is titled 'Certificates' and includes tabs for 'StudioX30' and 'Poly TC8'. Under 'Certificate Options', there are settings for 'Maximum Peer Certificate Chain Depth' (set to 3), 'Always Validate Peer Certificates From Server' (unchecked), 'Always Validate Peer Certificates From Browser' (unchecked), and 'Disable Preinstalled Certificates' (unchecked). The 'New Certificates' section has a button 'Create Certificate Signing Request (CSR)'. The 'Installed Certificates' section shows a table with one certificate entry.

Issued To	Issued By	Expiration Date	Type	Action
System Manager CA	System Manager CA	Jun 24 02:29:23 2029 GMT	ca,server,client	View Delete

Below the table, there is a pagination control showing '1 - 1 of 1' and navigation arrows. An 'Install Certificate' button is located at the bottom of the 'Installed Certificates' section.

© 2019 Poly, Inc. All rights reserved. | [Site Map](#) | [End-User License Agreement](#) | [Privacy Policy](#)

10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, Meetings Server, SBC, and Poly video endpoints.

1. Verify Poly video endpoints have successfully registered with internal H.323 gatekeeper in Meetings Management. Navigate to **Settings** → **Local Services** → **H.323 Gatekeeper** and verify that the Poly video endpoints are listed under **Registered Endpoints**.

AVAYA Signed In: admin Sign Out | Help

Dashboard Meetings Users Endpoints Devices Reports Logs & Events **Settings**

Local Services

H.323 Gatekeeper Status: Active Version: 9.1.0.40

Basic:

Registration Mode: All

☒ Strip Local Zone Prefix

Zone Prefix:

TTL:

☒ Enabled TTL

Multiple TTL by: 2

Max TTL interval: 3600

Advanced Parameters

Registered Endpoints (4)

Name	Number	Registration IP
StudioX30-5E45C2FC	78050	192.168.100.70
G7500-7509A0F2	78052	192.168.100.72
StudioX70-7D8034FL	78051	192.168.100.71
Avaya Conferencing MCU-010064102141	71	10.64.102.141

Route IP calls

Neighbors

Security Password

Apply Cancel

- Alternatively, verify the H.323 registration status in the Poly web interface. Navigate to **Call Configuration → H.323** and verify the **Registration Status** is *Registered*.

The screenshot shows the Poly StudioX30 web interface. The left sidebar contains navigation options: Dashboard, Place a Call, General Settings, Network, Call Configuration (highlighted), Call Settings, Dialing Preference, Recent Calls, H.323, and SIP. The main content area is titled 'H.323' and contains the following configuration fields:

- Enable IP H.323: ☒
- Registration Status: Registered
- H.323 Name: StudioX30-5E45C2FC
- H.323 Extension (E.164): 78050
- Use Gatekeeper: Specify
- Require Authentication: ☐
- Current Gatekeeper IP Address: 10.64.102.140:1719
- Primary Gatekeeper IP Address: 10.64.102.140

A 'Save' button is located at the bottom of the configuration area. The footer indicates '© 2019 Poly, Inc. All rights reserved. | Site Map | End-User License Agreement | Privacy Policy'.

- Verify Poly video endpoints have successfully registered with Session Manager. In System Manager, navigate to **Elements → Session Manager → System Status → User Registrations** to check the registration status.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains navigation options: Session Manager, Dashboard, Session Manager..., Global Settings, Communication Prof..., Network Configur..., Device and Locati..., Application Conf..., and System Status. The main content area is titled 'User Registrations' and contains a table of user registration data.

25 Items Show 15 Filter: Enable

	Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered					
											Prim	Sec	3rd	4th	Surv	Visiting
<input type="checkbox"/>	Show	78002@avaya.com	SIP	78002	---	10.64.102.108	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	SIP	78300	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	78050@avaya.com	Poly	78050	---	10.64.102.108	fixed	<input type="checkbox"/>	1/3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	78030@avaya.com	Agent	78030	---	192.168.100.49	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Since Poly video endpoints register to Session Manager through SBC, SBC would also provide a registration status, which could be viewed by navigating to **Status → User Registrations** as shown below.

Device: SBCE ▾ Help

User Registrations

AVAYA

Displaying entries 1 to 2 of 2.

AOR	SIP Instance	SBC Device	SM Address	Registration State
Contains ▾	Contains ▾	Contains ▾	Contains ▾	Contains ▾
78002@avaya.com	c81fead0d23d	SBCE	10.64.102.117(PRIMARY)	REGISTERED(ACTIVE)
78050@10.64.101.102	89b7f09f39f3	SBCE	10.64.102.117(NONE)	REGISTERED

5. Alternatively, the registration status may be verified in the Poly web interface. Navigate to **Call Configuration → SIP** and verify that **Registration Status** is *Registered*.

poly StudioX30

Search

- Dashboard
- Place a Call
- General Settings
- Network
- Call Configuration**
 - Call Settings
 - Dialing Preference
 - Recent Calls
 - H.323
 - SIP**
- Audio / Video
- Security

SIP

Enable SIP: ☒

Registration Status: Registered

SIP Server Configuration: Specify ▾

Transport Protocol: TLS ▾

Force Connection Reuse: ☐

BFCP transport preference: Prefer UDP ▾

Sign-in Address: 78050

User Name: 78050

Password:

Registrar Server: 10.64.101.102

Proxy Server:

Registrar Server Type: Standard SIP ▾

Enable AS-SIP: ☐

6. To verify the status of the SIP trunk between SBC and Meetings Management, navigate to **Status** → **Server Status** and verify the SIP trunk is *UP* as shown below.

Device: SBCE ▾

Help

Status


AVAYA

Server Status




MeetingsM	10.64.102.140	10.64.102.140	5061	TLS	UP	UNKNOWN	08/23/2023 12:55:00 EDT
-----------	---------------	---------------	------	-----	----	---------	-------------------------


7. Verify the status of the LDAP connection in the Poly web interface. Navigate to **Servers** → **Directory Servers** and verify the **Registration Status** is *Registered*.

≡

 poly

StudioX30



 Search

Dashboard

Place a Call

General Settings

Network

Call Configuration

Audio / Video

Security

Servers

Calendaring Service

Directory Servers

Provisioning Server

Directory Servers

Server Type:

LDAP ▾

Registration Status:

Registered

Server Address:

10.64.101.102

Server Port:

389

Base DN (Distinguished Name):

ou=users

Multitiered Directory Default Group DN:

Use SSL (Secure Socket Layer):

☐

Authentication Type:

Basic ▾

Bind DN (Distinguished Name):

test1

Password:

Save

© 2019 Poly, Inc. All rights reserved. | [Site Map](#) | [End-User License Agreement](#) | [Privacy Policy](#)

8. Perform a LDAP search for endpoints by name from the TC8 Touch Controller or Poly web interface and verify that Meetings Management receives the LDAP requests under **Events** as shown below.

The screenshot shows the Avaya Meetings Management interface. The left sidebar contains navigation options: HTTP Protocol, Servers, Alarm, Address Book, Advanced, Customization, CDR Settings, Branding, Topology, Locations, and IP Topology. The 'Address Book' section is expanded, showing 'Corporate Address Book' and 'Advanced'. The 'Corporate Address Book' configuration includes options to enable the address book, set listening ports (389 and 636), and select LDAP Distinguished Name (DN) suffixes (None, Organization, Domain Name). Below the configuration is an 'Events' table showing LDAP search and bind requests.

Event Name	Time	User Name	host	Duration
Search Request	08/23/2023 11:51	test1	192.168.100.71:53584	0.0
Bind Request	08/23/2023 11:51	test1	192.168.100.71:53584	0.0
Search Request	08/23/2023 11:47	test1	10.64.102.230:30325	0.0
Bind Request	08/23/2023 11:47	test1	10.64.102.230:30325	0.0
Search Request	08/23/2023 11:30	test1	10.64.102.230:28643	0.0
Bind Request	08/23/2023 11:30	test1	10.64.102.230:28643	0.0
Search Request	08/23/2023 10:51	test1	192.168.100.71:53334	0.0
Bind Request	08/23/2023 10:51	test1	192.168.100.71:53334	0.0
Search Request	08/23/2023 10:47	test1	10.64.102.230:22054	0.0

Also, verify that Poly video endpoints display search results on TC8 Touch Controller or web interface (shown below), a call can be placed by clicking on an entry in the search results, and a search result entry can be added to Favorites.

The screenshot shows the Poly StudioX30 web interface. The left sidebar contains navigation options: Search, Dashboard, Place a Call, General Settings, Network, Call Configuration, Audio / Video, Security, Servers, and Diagnostics. The main area displays a 'Place a Call' section with tabs for Dial, Contacts, Favorites, and Recent. A search bar is present, and the results show a list of endpoints: Poly G7500, Poly X30, and Poly X70. The Poly G7500 entry is highlighted with a star icon.

9. Join a meeting from a Poly video endpoint using the Meeting ID. Verify Poly video endpoint joins the meeting and receives audio and video from other participants. In the Meetings Management Administrator Portal, navigate to **Dashboard** and click on the active Meeting ID.

The screenshot shows the Avaya Meetings Management Administrator Portal Dashboard. The top navigation bar includes links for Dashboard, Meetings, Users, Endpoints, Devices, Reports, Logs & Events, and Settings. The user is signed in as 'admin'. The main content area is divided into two sections: 'Calls and Meetings in Progress' and 'System Information'. The 'Calls and Meetings in Progress' section shows 1 Meeting and 3 Participants. The 'System Information' section displays server details such as Server Edition (Enterprise), Software Version (9.1.14.0.17), and Up Time (5 days 3 hours 41 minutes). A 'Device Usage' section shows the usage of 'devcon-amms' (50%) and 'devcon-amms-web' (0%).

Verify Poly video endpoint is in the participant list and expand the entry to view call details, which should include the codecs, frame rate, and bandwidth.

The screenshot shows the Avaya Meetings Management Administrator Portal with the 'Participants' tab selected. The 'Participants (3)' section lists three participants: Vantage 78041 (Avaya Vantage), John Smith (Web Client), and Poly X30 (null). The Poly X30 (null) participant is expanded, showing detailed call information. The 'Sending' section displays 'Video: H264 HP (HD1080p) 30 fps / 1.9 Mbps', 'Audio: G711U 64 Kbps', and 'Data: N/A'. The 'Receiving' section displays the same information. The 'Host Avaya Meetings Media Server: ...' and 'Connect Time: 13:47:28 17-07-2023 -0600' are also visible. At the bottom, the 'Meeting Ends: 00:24:24' and 'Bandwidth: 4096 Kbps' are displayed.

10. H.323 call statistics can also be viewed from the Poly web interface. Navigate to **Active Call**, and then click on **Call Statistics**.

The screenshot displays the Poly StudioX30 web interface. The top navigation bar includes the Poly logo, 'StudioX30', a green status bar with a phone icon and '00:00:29', and icons for globe, help, and share. The left sidebar contains a search bar and a list of navigation items: Dashboard, Place a Call, Active Call, General Settings, Network, Call Configuration, Audio / Video, Security, Servers, Diagnostics (highlighted in blue), Remote Monitoring, Video Capture, and Call Statistics (highlighted in blue). The main content area is titled 'Call Statistics' and shows 'Participants (1)'. A card for 'Test Virtual Room (79222)' displays call details: Participant Name, Participant Number, Participant System, Call Type, Call Speed, and AES Encryption. Below this is a table of streams.

Streams	Format	Rate Used	Packet Loss
AUDIO TX G.722.1C	---	48	0%
AUDIO RX G.722.1C	---	48	0%
VIDEO TX H.264-HP	1080p	2011	0%
VIDEO RX H.264-HP	1080p	1996	0%

© 2019 Poly, Inc. All rights reserved. | [Site Map](#) | [End-User License Agreement](#) | [Privacy Policy](#)

11. SIP call statistics can also be viewed from the Poly web interface. Navigate to **Active Call**, and then click on **Call Statistics**.

The screenshot displays the Poly StudioX30 web interface. The top header bar includes the Poly logo, 'StudioX30', a green status bar with a phone icon and '00:00:37', and icons for globe, help, and share. The left sidebar contains a search bar and navigation links: Dashboard, Place a Call, Active Call, General Settings, Network, Call Configuration, Audio / Video, Security, Servers, and Diagnostics (highlighted in blue). Below the sidebar is a 'Remote Monitoring' link. The main content area is titled 'Call Statistics' and shows 'Participants (1)'. A card for participant '79222' is displayed, with a 'Details' link and an upward arrow. The card contains the following information:

- Participant Name: 79222
- Participant Number: 79222
- Participant System: RADVision Vialp MCU 9.1.1 RVID53416241474658415f
- Call Type: SIP
- Call Speed: 2048
- AES Encryption: AES-128 / TLS/SDS

Below this information is a table with four columns: Streams, Format, Rate Used, and Packet Loss. The table lists four streams:

Streams	Format	Rate Used	Packet Loss
AUDIO TX G.711U	---	64	0%
AUDIO RX G.711U	---	64	0%
VIDEO TX H.264-HP	1080p	1927	0%
VIDEO RX H.264-HP	1080p	1971	0%

11. Conclusion

These Application Notes describe the configuration steps required to integrate Poly Studio X30/X70 Video Bar and G7500 Modular Video Conferencing System with Avaya Meetings Server and Avaya Session Border Controller. Poly video endpoints registered to Avaya Aura® Session Manager through Avaya Session Border Controller whether located within the enterprise network or the Internet. Poly video endpoints were able to join meetings and establish point-to-point calls using H.323 or SIP, perform LDAP searches, and use TLS/SRTP for SIP calls. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

12. Additional References

This section references the Avaya documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, June 2023, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 11, July 2023, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023, available at <http://support.avaya.com>.
- [4] *Administering Avaya Meetings Management*, Release 9.1.14, Issue 2, June 2023, available at <http://support.avaya.com>.
- [5] *Administering Avaya Session Border Controller*, Release 10.1.x, Issue 3, June 2023, available at <http://support.avaya.com>.

©2023 Avaya LLC All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.