



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Poly Studio X30/X50/X70 Video Bar and Poly G7500 Modular Video Conferencing System with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller – 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 Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, and Avaya Session Border Controller 10.1. 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 cameras, microphones, and 3<sup>rd</sup> party components for customizing a conference room. Poly video endpoints 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. Poly video endpoints can then establish point-to-point audio and video calls with other Avaya endpoints.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

# 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 Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, and Avaya Session Border Controller 10.1. 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 cameras, microphones, and 3<sup>rd</sup> party components for customizing a conference room. Poly video endpoints 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. Poly video endpoints can then establish point-to-point audio and video calls with other Avaya endpoints.

These Application Notes will focus on the remote worker configuration on SBC, but the configuration for registering Poly video endpoints within the enterprise network is similar, except that Poly video endpoints will communicate with SBC via a private interface instead of a public interface.

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 the configuration also applies to the other Poly video endpoints.

## 2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing point-to-point audio and video calls between the Poly video endpoints, Avaya Workplace Client for Windows, Avaya Vantage, Avaya SIP / H.323 IP Deskphones, and the PSTN. Telephony features, such as hold/resume, audio and video mute, call transfer, add party, call forward, and coverage, were also tested.

The serviceability testing focused on verifying that the Poly video endpoints came back into service after restoring the network connection or a reboot.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya

products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with this Application Note, the interface between Avaya systems, Poly Studio X30/X70 Video Bar, and Poly G7500 Modular Video Conferencing System used TLS/SRTP encryption features.

## 2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of Poly video endpoints with Session Manager through SBC. Poly video endpoints within the enterprise network connect to SBC over a private interface, whereas a remote worker on the Internet connect to SBC over a public interface. Refer to **Section 2.2** for more details.
- Audio and video calls between Poly video endpoints, Avaya Workplace, Avaya Vantage, Avaya H.323/SIP deskphones, and the PSTN with Direct IP Media (Shuffling) enabled and disabled. Shuffling allows IP endpoints to send audio RTP packets directly to each other without using media resources on the Avaya Media Gateway or Avaya Aura® Media Server.
- TLS transport using a secure PFS cipher of TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384.
- Support of G.711 and G.729 codecs.
- Proper recognition of DTMF tones using RFC2833.
- Basic telephony features, such as hold/resume, transfer, and conference from Avaya endpoints, and audio/video mute, add party, coverage, multiple calls, and long duration calls.
- Audio conference from Avaya deskphone.
- Audio and video mute from Poly.
- Extended telephony features using Communication Manager FACs for Call Forward, Call Park/Unpark, and Call Pickup.
- Proper system recovery after restoring network connectivity or restarting the Poly video endpoints.

## 2.2. Test Results

Testing of Poly video endpoints as remote workers passed with the following observations.

- 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.

- Video call transfers are not supported. Transferring a video call with a Poly video endpoint to Workplace results in an audio only call, no video. Transferring a video call to a Poly video endpoint causes the call to drop.
- Workplace or Vantage may have to “start video” if a call is originally established as an audio only call. However, starting video on Workplace or Vantage causes audio from Poly to be lost (i.e., one-way audio) for about a minute. Afterwards, audio is restored.
- When Poly video endpoints add a party to an existing audio or video call, the party is added as audio only.
- Poly video endpoints do not support call transfer, hold/resume, or voicemail coverage.
- Poly video endpoints do not send MAC address during SIP registration. E911 solutions may use the MAC address of SIP endpoints to provide location information when an emergency call is made.
- If frozen video is experienced on calls between the Poly video endpoints and Workplace/Vantage, lower the bandwidth/speed of the video call as shown in **Section 8.5**.

## 2.3. Support

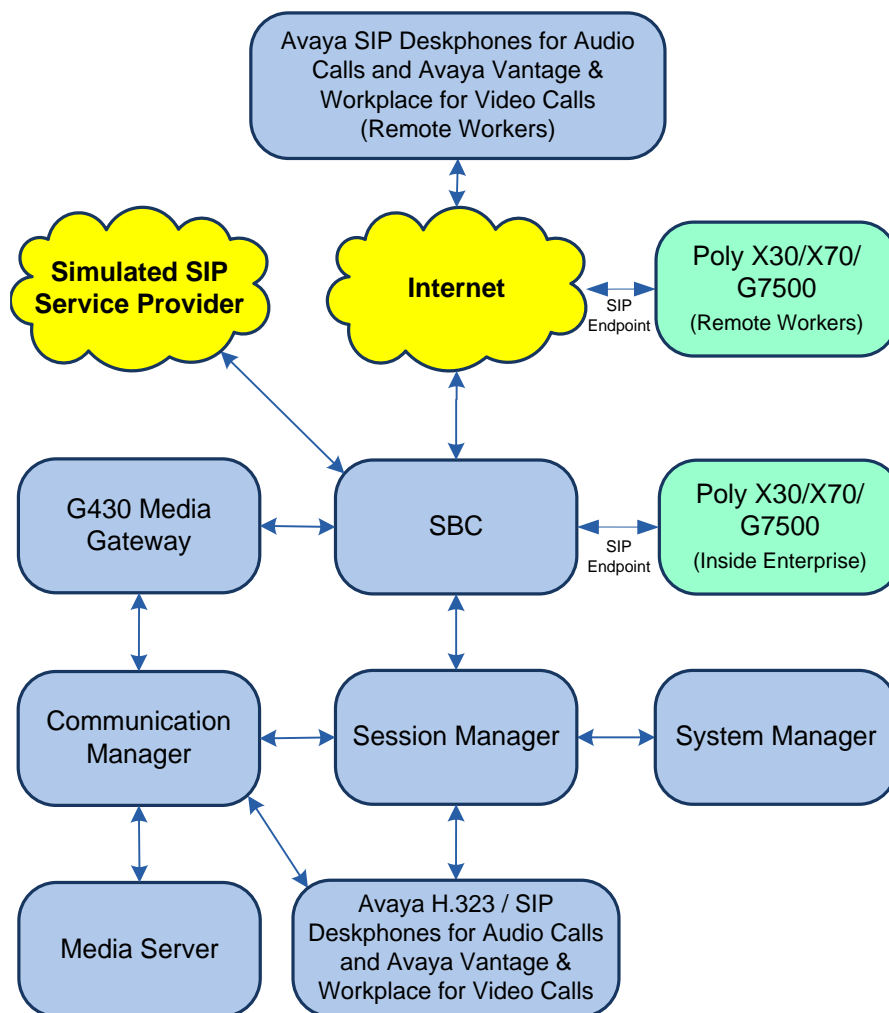
For support on Poly X30/X50/X70 Video Bar and G7500 Modular Video Conferencing System, visit the Poly support portal at <https://www.poly.com/us/en/support>.

### 3. Reference Configuration

The configuration used for the compliance test is shown below. Studio X30/X70 and G7500 registered to Session Manager through SBC while connected within the enterprise network or connected to the Internet and registered as remote workers. The configuration included:

- Avaya Aura® Communication Manager with an Avaya G430 Media Gateway.
- Media resources in the Avaya G430 Media Gateway and Avaya Aura® Media Server.
- Avaya Aura® Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP endpoints, including the Poly video endpoints.
- Avaya Aura® System Manager used to configure Session Manager.
- Avaya Session Border Controller to provide connectivity to a simulated SIP service provider and to register the Poly video endpoints to Session Manager.
- Avaya Workplace, Avaya Vantage, and Avaya H.323 and SIP deskphones.
- Poly Studio X30/X70 Video Bar and Poly G7500 Modular Video Conferencing System.

Poly video endpoints registered to Session Manager as SIP endpoints and were configured as Off-PBX Stations (OPS) on Communication Manager.



## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	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
Avaya Vantage	3.1.1.2.0009
Avaya Workplace Client for Windows	3.33.0.96
Avaya Session Border Controller	10.1.1.0-35-21872
Avaya 96x1 Series IP Deskphones	6.8.5.4.10 (H.323)
Avaya J100 Series IP Phones	4.1.1.0.7 (SIP)
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 network region, IP codec set, and SIP trunk group to Session Manager, focusing on settings that would impact SIP signaling and media to Poly video endpoints. Note that the SIP station configuration for Poly video endpoints are configured through Avaya Aura® System Manager in **Section 6.3**.

Use the System Access Terminal (SAT) to configure Communication Manager and log in with appropriate credentials.

### 5.1. Verify License

Using the SAT, verify that the Off-PBX Telephones (OPS) option is enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

```

display system-parameters customer-options
                                OPTIONAL FEATURES

G3 Version: V20                  Software Package: Enterprise
Location: 2                      System ID (SID): 1
Platform: 28                    Module ID (MID): 1

                                USED
Platform Maximum Ports: 48000    152
Maximum Stations: 36000         37
Maximum XMOBILE Stations: 36000    0
Maximum Off-PBX Telephones - EC500: 41000    0
Maximum Off-PBX Telephones - OPS: 41000    25
Maximum Off-PBX Telephones - PBFMC: 41000    0
Maximum Off-PBX Telephones - PVFMC: 41000    0
Maximum Off-PBX Telephones - SCCAN: 0        0
Maximum Survivable Processors: 313        0

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

```

## 5.2. 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	
<b>devcon-sm</b>	<b>10.64.102.117</b>	
<b>procr</b>	<b>10.64.102.115</b>	
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		

### 5.3. Administer IP Codec Set

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

To enable SRTP, **Media Encryption** was set to *1-srtp-aescm128-hmac80* and **Encrypted SRTCP** was left at the default value of *best-effort*.

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

                                IP MEDIA PARAMETERS

Codec Set: 1

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

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

Media Connection IP Address Type Preferences
1: IPv4
2:
```

## 5.4. 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*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow RTP to be sent directly between IP endpoints or between Communication Manager and SBC without using media resources in the Avaya Aura® Media Servers after the call is established. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 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		

## 5.5. 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 the PSTN. 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	<b>Group Type: sip</b>	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			
<b>Service Type: tie</b>	Auth Code? n		
	Member Assignment Method: auto		
	<b>Signaling Group: 10</b>		
	<b>Number of Members: 10</b>		

**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			

## 5.6. 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” to route pattern 10 as shown below.

change aar analysis 78							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed String	Total Min	Max	Route Pattern	Call Type	Node Num	ANI Req'd	
78	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 No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted
			Mrk	Lmt	List	Del	Digits
1: 10	0						
2:							
3:							
4:							
5:							
6:							
BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM Sub
0	1	2	M	4	W	Request	Dgts
1: y	y	y	y	y	n	n	rest
2: y	y	y	y	y	n	n	rest
DCS/	IXC						
QSIG							
Intw							
n	user						
n	user						
n	user						
n	user						
n	user						
Numbering	LAR						
Format							
unk-unk	none						
none							

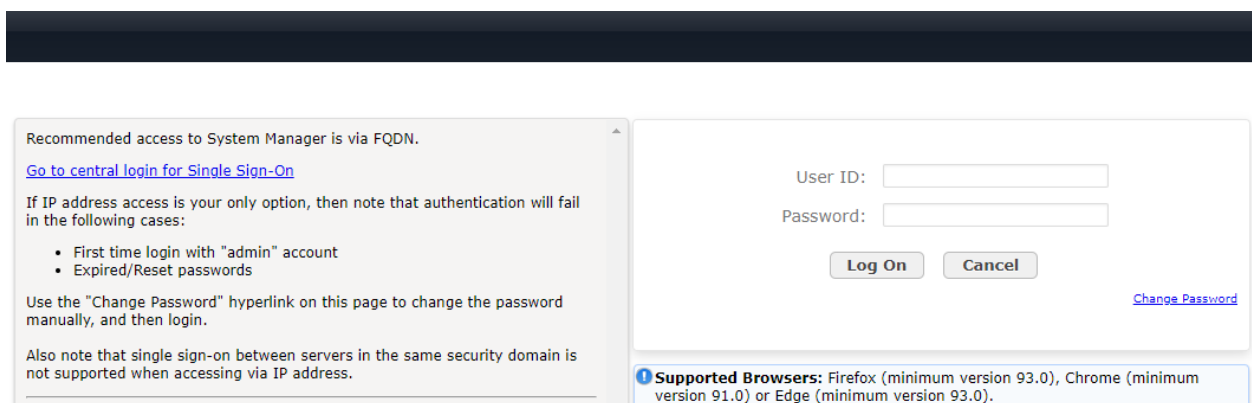
## 6. Configure Avaya Aura® Session Manager

This section covers the configuration of a SIP user in Session Manager for Poly video endpoints. Poly video endpoints register to Session Manager through SBC.

**Note:** It is assumed that basic configuration of Session Manager has already been performed, including the SIP trunk to Communication Manager and SBC. This section will focus on the configuration of 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 IP address of the System Manager server. 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. Set Network Transport Protocol

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 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 'admin' are also present. The left sidebar shows a tree view with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains two sections: 'General' and 'Monitoring'. The 'General' section includes fields for Name (devcon-sm), IP Address (10.64.102.117), SIP FQDN, Type (Session Manager), Notes, Location (Thornton), Outbound Proxy, Time Zone (America/New\_York), Minimum TLS Version (Use Global Setting), and Credential name. The 'Monitoring' section includes SIP Link Monitoring and CRLF Keep Alive Monitoring, both set to 'Use Session Manager Configuration'. Buttons for 'Commit' and 'Cancel' are in the top right.

Field	Value
Name	devcon-sm
IP Address	10.64.102.117
SIP FQDN	
Type	Session Manager
Notes	
Location	Thornton
Outbound Proxy	
Time Zone	America/New_York
Minimum TLS Version	Use Global Setting
Credential name	
SIP Link Monitoring	Use Session Manager Configuration
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, the solution used TLS network transport.

**Listen Ports**

Add Remove

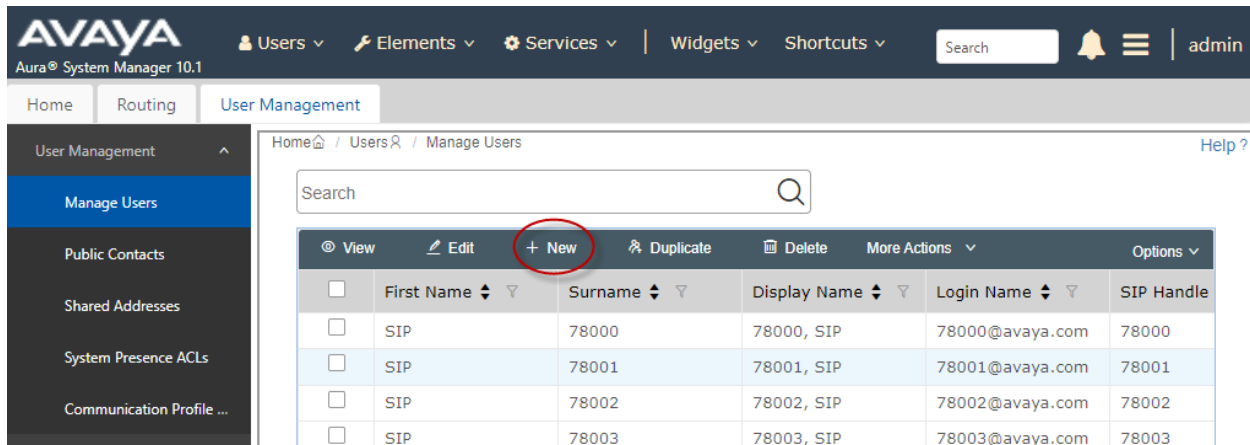
3 Items Filter: Enable

<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

## 6.3. Administer SIP User

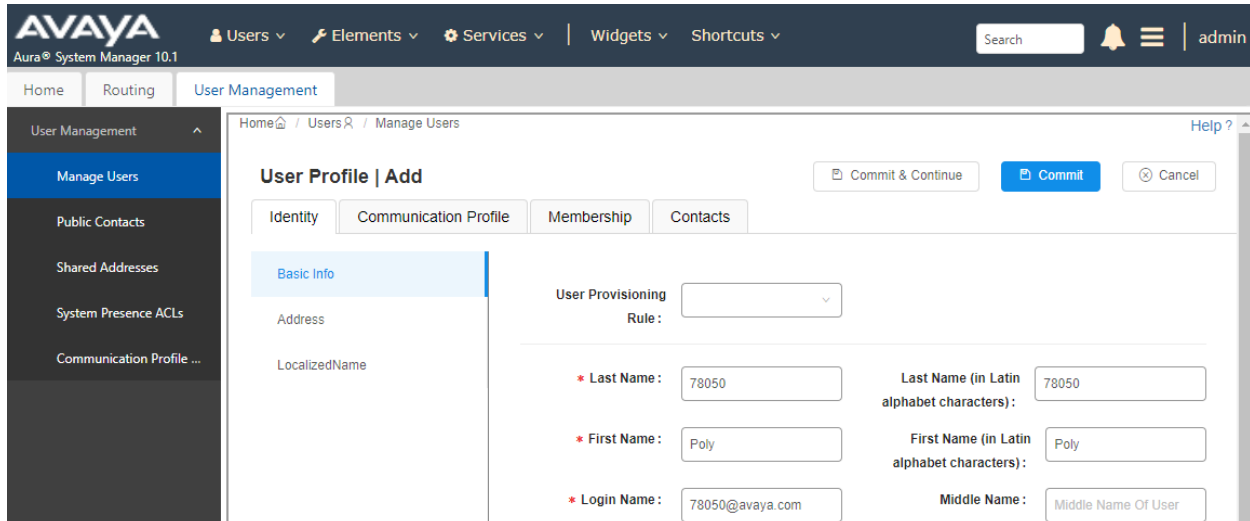
In the **Home** screen (not shown), select **Users** → **User Management** → **Manage Users** to display the **User Management** screen below. Click **New** to add a user.



	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	78000	78000, SIP	78000@avaya.com	78000
<input type="checkbox"/>	SIP	78001	78001, SIP	78001@avaya.com	78001
<input type="checkbox"/>	SIP	78002	78002, SIP	78002@avaya.com	78002
<input type="checkbox"/>	SIP	78003	78003, SIP	78003@avaya.com	78003

### 6.3.1. Identity

The **New User Profile** screen is displayed. Enter desired **Last Name** and **First Name**. For **Login Name**, enter “<ext>@<domain>”, where “<ext>” is the desired Poly video endpoint SIP extension and “<domain>” is the applicable SIP domain name. Retain the default values in the remaining fields.



**User Profile | Add**

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Basic Info

Address

LocalizedName

User Provisioning Rule: [v]

\* Last Name: 78050 Last Name (in Latin alphabet characters): 78050

\* First Name: Poly First Name (in Latin alphabet characters): Poly

\* Login Name: 78050@avaya.com Middle Name: Middle Name Of User

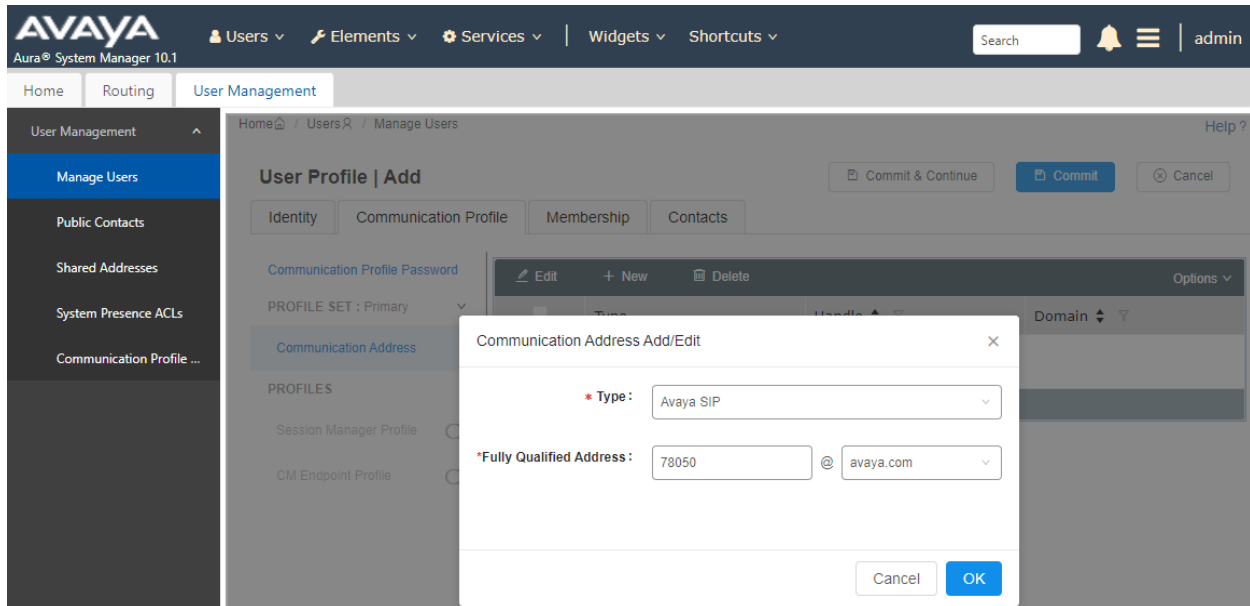
### 6.3.2. Communication Profile

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 to use for registration. Click **OK**.

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 'admin' are also visible. The left sidebar shows a tree view with 'User Management' expanded, containing 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profile ...'. The main content area is titled 'User Profile | Add' and has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section with 'Edit', 'New', and 'Delete' buttons. A modal window titled 'Comm-Profile Password' is open, featuring two password input fields: 'Comm-Profile Password' and 'Re-enter Comm-Profile Password'. The 'Re-enter' field has a green checkmark indicating a match. Below the fields is a 'Generate Comm-Profile Password' link and 'Cancel' and 'OK' buttons.

### 6.3.3. 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. For **Type**, select *Avaya SIP*. For **Fully Qualified Address**, enter the SIP user extension and select the domain name. For the compliance test, 5-digit SIP extensions starting with '78' were assigned to Poly video endpoints. Click **OK**.



### 6.3.4. 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 shows the 'User Profile | Add' page in the Avaya Aura System Manager 10.1 interface. The 'Session Manager Profile' toggle is turned on. The 'SIP Registration' section includes fields for Primary Session Manager (devcon-sm), Secondary Session Manager (Start typing...), and Survivability Server (Start typing...). The 'Application Sequences' section includes Origination Sequence (DEVCON-CM App S...) and Termination Sequence (DEVCON-CM App S...). The 'Call Routing Settings' section is partially visible at the bottom.

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

The screenshot shows the 'Call Routing Settings' section. The 'Home Location' field is set to 'Thornton'. The 'Conference Factory Set' field is set to 'Select'.

### 6.3.5. CM Endpoint Profile

Click on the toggle button by **CM Endpoint Profile**. For **System**, select the value corresponding to the applicable Communication Manager. For **Extension**, enter the SIP user extension from **Section 6.3.3**. For **Template**, select *9641SIP\_DEFAULT\_CM\_8\_1*. For **Port**, click and select *IP*. Retain the default values in the remaining fields.

The screenshot displays the Avaya Aura System Manager 10.1 interface for adding a new user profile. The left sidebar shows the navigation menu with 'User Management' expanded and 'Manage Users' selected. The main content area is titled 'User Profile | Add' and includes tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section on the left and a main configuration area on the right. The main configuration area includes fields for 'System' (devcon-cm), 'Profile Type' (Endpoint), 'Extension' (78050), 'Set Type' (9641SIP), 'Template' (9641SIP\_DEFAULT\_CM\_8\_1), 'Security Code' (Enter Security Code), 'Port' (IP), 'Voice Mail Number', 'Preferred Handle' (Select), 'Sip Trunk' (aar), 'Calculate Route Pattern' (Calculate Route Pattern), 'SIP URI' (Select), 'Delete on Unassign from User or on Delete User' (checked), 'Override Endpoint Name and Localized Name' (checked), and 'Allow H.323 and SIP Endpoint Dual Registration' (unchecked). The 'CM Endpoint Profile' toggle is turned on.

Avaya Aura System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search 🔍 | admin

Home Routing User Management

User Management ▾

Manage Users

Public Contacts

Shared Addresses

System Presence ACLs

Communication Profile ...

Home / Users / Manage Users

Help ?

User Profile | Add

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary ▾

Communication Address

PROFILES

Session Manager Profile ☒

CM Endpoint Profile ☒

\* System : devcon-cm

\* Profile Type : Endpoint

Use Existing Endpoints: ☐

\* Extension : 78050

\* Template : 9641SIP\_DEFAULT\_CM\_8\_1

\* Set Type : 9641SIP

Security Code : Enter Security Code

Port : IP

Voice Mail Number :

Preferred Handle : Select

Calculate Route Pattern: ☐

Sip Trunk : aar

SIP URI : Select

Delete on Unassign from User or on Delete User: ☒

Override Endpoint Name and Localized Name: ☒

Allow H.323 and SIP Endpoint Dual Registration: ☐

## 7. Configure Avaya Session Border Controller

This section covers the **Subscriber Flows** required to register Poly video endpoints to Session Manager through SBC as remote workers. In addition, the **Application Rule** and **Media Rule** required to support video calls using SRTP are also covered. These rules are assigned to an **End Point Policy Group**, which in turn is assigned to **Server Flows**.

### 7.1. 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) login interface. 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, a text input field, and a "Continue" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, a disclaimer about unauthorized access, a consent statement, and a copyright notice for 2011-2020 Avaya Inc.

**AVAYA**

**Session Border Controller  
for Enterprise**

**Log In**

Username:

WELCOME TO AVAYA SBC

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.

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.

© 2011 - 2020 Avaya Inc. All rights reserved.

## 7.2. Add 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., *SM-AR*) or add a new one.

The application rule used to support audio and video calls to/from Poly video endpoints registered through SBC is shown below. In this example, 200 concurrent incoming and outgoing audio and video calls are supported.

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 lists the navigation menu, with 'Domain Policies' expanded and 'Application Rules' selected. The main content area is titled 'Application Rules: SM-AR' and features an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. Below this is a table with columns for Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The table lists 'Audio' and 'Video' with 'In' and 'Out' checkboxes checked and 'Maximum Concurrent Sessions' set to 200. A 'Miscellaneous' section below the table shows 'CDR Support' as 'Off' and 'RTCP Keep-Alive' as 'No'. An 'Edit' button is located at the bottom right of the table.

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 Support	Off
RTCP Keep-Alive	No

## 7.3. Modify Media Rule

Determine the media rule that is used for calls to Session Manager. The media rule is specified in the Server Flows configured under Session Manager. To modify a media rule, navigate to **Domain Policies** → **Media Rules** in the left pane. In the center pane, select the appropriate media rule (e.g., *RTP-SRTP*). The **Encryption** tab displays the audio and video encryption being used as shown below. For calls to Poly video endpoints, SBC used the first encryption format in the list.

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: RTP-SRTP". It features a list of media rules on the left, including "default-low-med", "default-low-m...", "default-high", "default-high-enc", "avaya-low-me...", "RTP-SRTP" (selected), "RTP-SRTP-P...", and "Meetings-MR". An "Add" button is located above the list.

The "RTP-SRTP" rule is selected, and the "Encryption" tab is active. The configuration details are as follows:

Audio Encryption	
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	
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	
Capability Negotiation	<input type="checkbox"/>

An "Edit" button is located at the bottom right of the configuration area.

The **Advanced** tab and verify that **BFCP Enabled** is unchecked.

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: RTP-SRTP

Add

Rename

Clone

Delete

Click here to add a description.

Encryption

Codec Prioritization

**Advanced**

QoS

Silencing

Silencing Enabled ☒

Timeout 60 second(s)

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 ☐

## 7.4. Administer End Point Policy Group

The application and media rules configured above are part of the **End Point Policy Group** configuration as shown below. The **End Point Policy Group** is assigned to a **End Point Flows** as shown in **Section 7.7**.

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**

Policy Groups: RTP-SRTP

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-s...

avaya-def-high-s...

RTP-SRTP

Rename

Clone

Delete

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	SM-AR	default	RTP-SRTP	default-low	default	None	Off	Edit

## 7.5. 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 to support remote workers. When Poly video endpoints are located within the enterprise network, media is exchanged via an internal SBC interface.

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.

- **PublicMediaRW:** Interface used by remote workers for media.
- **PrivateMediaRW:** Interface used by Communication Manager and media resources for exchanging media with remote workers.

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	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	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

## 7.6. 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 to support remote workers. When Poly video endpoints are located within the enterprise network, SIP signaling is exchanged via an internal SBC interface.

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.

- **PublicSignalingRW:** Interface used by remote workers for SIP signaling.
- **PrivateSignalingRW:** Interface used by Session Manager for SIP signaling with remote workers.

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	10.64.102.230 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	10.64.102.106 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

## 7.7. Administer End Point Flows

This section covers the **End Point Flows** to support remote workers. Similar configuration is required for Poly video endpoints located within the enterprise network (not shown).

### 7.7.1. 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 to 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 DashboardSoftware ManagementDevice ManagementBackup/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 FlowsServer 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	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

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

## 7.7.2. Server Flows

Navigate to **Network & Flows** → **End Point Flows** and select the **Server Flows** tab. The Session Manager **Server Flow** for remote workers 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**

End Point Flows

Subscriber Flows

Server 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	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>
2	Session Manager Flow	*	PublicSignaling	PrivateSignaling	RTP-SRTP	PSTN-SIP	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>
3	Remote Worker Flow	*	PublicSignalingRW	PrivateSignalingRW	RTP-SRTP	default	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

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. Configure Poly Studio X30 Video Bar

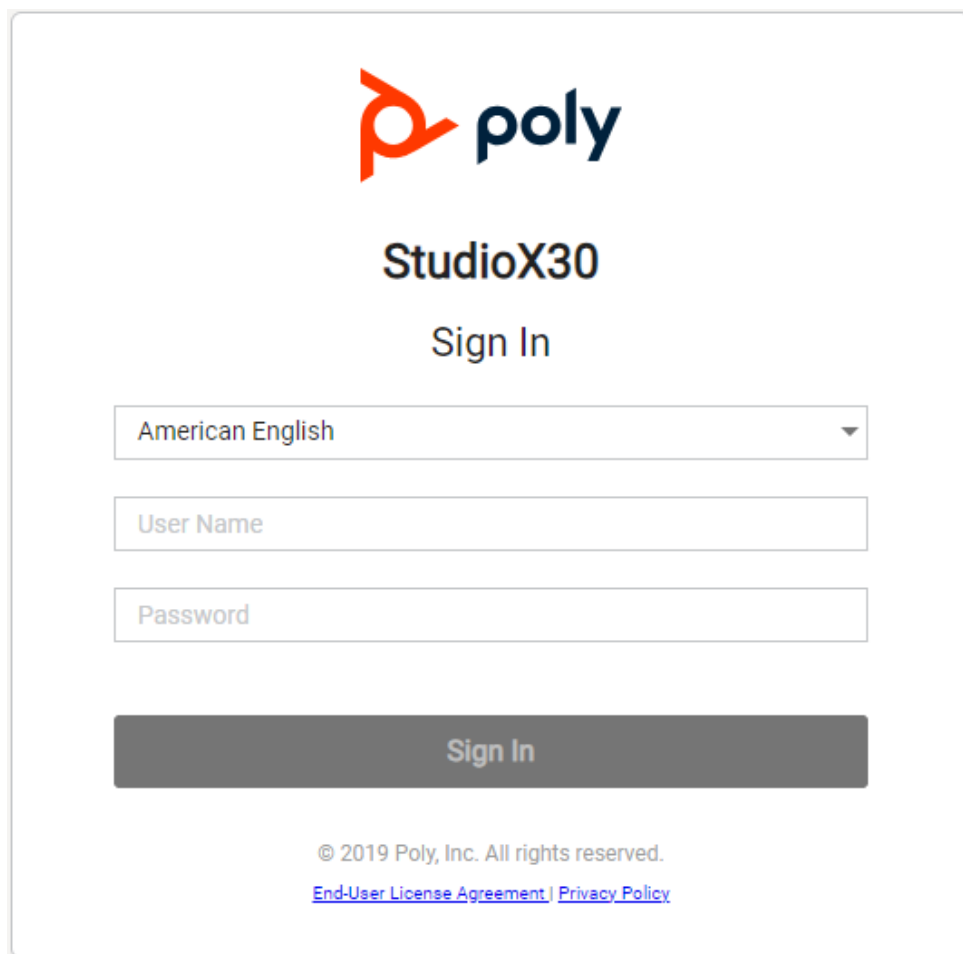
This section covers the configuration of Studio X30 to register to Session Manager through SBC as a remote worker. This configuration requires following steps:

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

**Note:** This section covers the Studio X30 configuration, but it also applies to Studio X70 and G7500 as the configuration screens are the same.

### 8.1. 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, consisting of an orange stylized 'P' and the word 'poly' in blue. Below the logo is the text 'StudioX30' in bold black, followed by 'Sign In' in a lighter gray. There is a language selection dropdown menu currently set to 'American English'. Below this are two input fields: 'User Name' and 'Password'. At the bottom of the form is a large gray 'Sign In' button. Below the button, the copyright notice '© 2019 Poly, Inc. All rights reserved.' is displayed, followed by two blue links: 'End-User License Agreement' and 'Privacy Policy'.

## 8.2. Set 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 user interface. The top header 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 this is a dark gray 'Save' button. At the bottom of the page, there is a footer with the text: '© 2019 Poly, Inc. All rights reserved. | [Site Map](#) | [End-User License Agreement](#) | [Privacy Policy](#)'.

## 8.3. Administer SIP Settings

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 SBC public IP address used for remote workers (e.g., 10.64.101.102) or specify the SBC private IP address, If Studio X30 is located within the enterprise network.

The screenshot shows the StudioX30 web interface for configuring SIP settings. The left sidebar contains navigation links: Dashboard, Place a Call, General Settings, Network, Call Configuration (highlighted), Call Settings, Dialing Preference, Recent Calls, H.323, SIP (highlighted), Audio / Video, Security, Servers, and Diagnostics. The main content area is titled 'SIP' and contains the following fields:

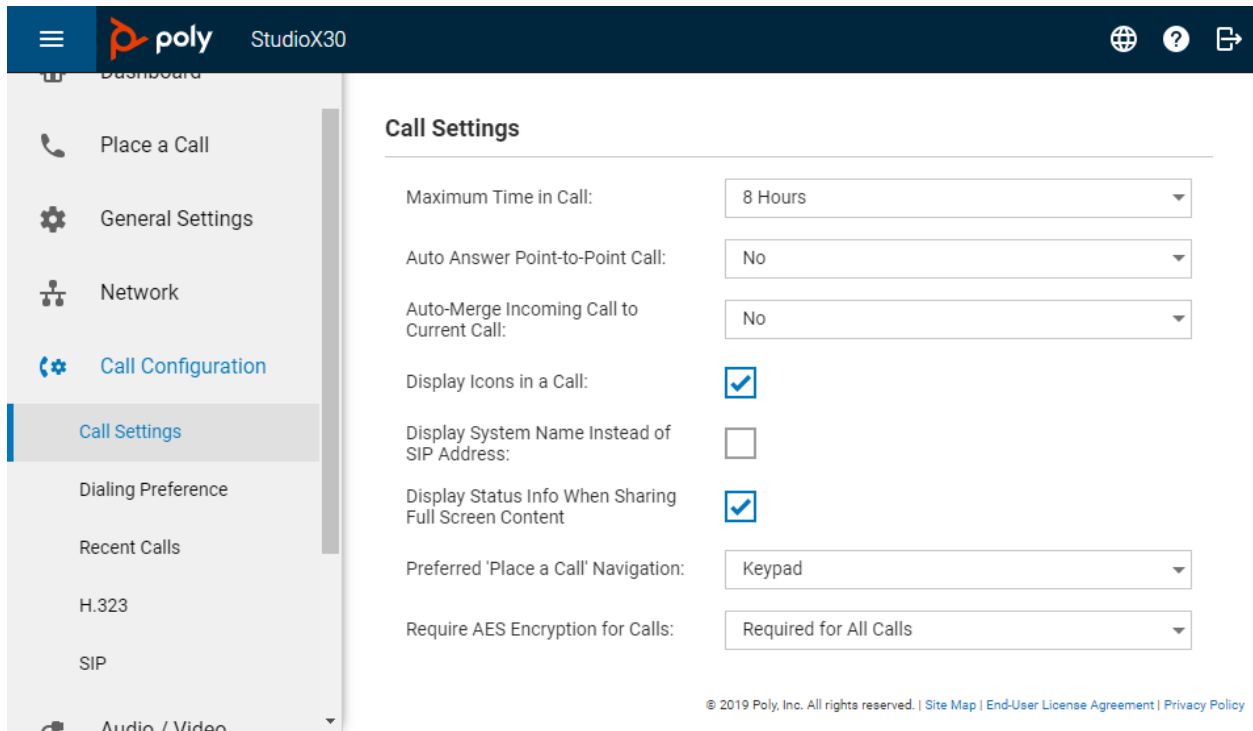
- Enable SIP: ☒
- Registration Status: Registered
- SIP Server Configuration: Specify (dropdown)
- Transport Protocol: TLS (dropdown)
- Force Connection Reuse: ☐
- BFCP transport preference: Prefer UDP (dropdown)
- Sign-in Address: 78050
- User Name: 78050
- Password: .....
- Registrar Server: 10.64.101.102
- Proxy Server: (empty field)
- Registrar Server Type: Standard SIP (dropdown)
- Enable AS-SIP: ☐

Below the SIP settings is the 'Adhoc Call Escalation' section, which includes the text: 'This feature will work when SIP is registered with Polycom DMA.' and a checkbox for 'Enable automatic call escalation of point to point calls to an external MCU:'. A 'Save' button is located at the bottom of the configuration area.

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

## 8.4. Administer Call Settings

Navigate to **Call Configuration** → **Call Settings** to configure the **Require AES Encryption for Calls** field. Set this field to *Required for All Calls* to enforce SRTP for audio and video calls.



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:	Required for All Calls

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

## 8.5. 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 *SIP* as the protocol used placing video calls.
- **Audio Dialing Order Preference 1:** Specify *SIP* as the protocol used placing audio calls.
- **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 global settings, help, and a share button. A 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, and SIP. 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:	<input type="text" value="SIP"/>
Audio Dialing Order Preference 1:	<input type="text" value="SIP"/>

Preferred Speeds	
Preferred Speed for Placed Calls:	<input type="text" value="2048"/>
Maximum Speed for Received Calls:	<input type="text" value="6144"/>

## 8.6. 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 SIP signaling with 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 contains navigation links: Dashboard, Place a Call, General Settings, Network, Call Configuration, Audio / Video, Security (selected), Access, Certificates (selected), Local Accounts, Global Security, Password Requirements, Security Code, and Security Banner. 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' (checkbox), 'Always Validate Peer Certificates From Browser' (checkbox), and 'Disable Preinstalled Certificates' (checkbox). The 'New Certificates' section has a button 'Create Certificate Signing Request (CSR)'. The 'Installed Certificates' section shows a table with one 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	<a href="#">View</a> <a href="#">Delete</a>

Below the table is a pagination control showing '5' items per page and '1 - 1 of 1' total items. An 'Install Certificate' button is located at the bottom left of the installed certificates section. The footer contains copyright information: '© 2019 Poly, Inc. All rights reserved. | Site Map | End-User License Agreement | Privacy Policy'.

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, SBC, and Studio X30.

1. Verify that Studio X30 has 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 top navigation bar includes links for Users, Elements, Services, Widgets, and Shortcuts. A search box and notification bell are also present. The left sidebar contains a menu with options like Dashboard, Session Manager, Global Settings, Communication Prof..., Network Configur..., Device and Locati..., and Application Confi....

### User Registrations

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

**Ast Device Notifications:**

- [View] [Default] [Export] [Force Unregister] [Reboot] [Reload] [Fallback]
- As of 1:21 PM
- [Advanced Search]

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"/>	(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"/>	(AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Since Studio X30 is registered as a remote worker, SBC would also provide a registration status, which could be viewed by Navigating to **Status → User Registrations** in the SBC EMS web interface as shown below.

Device: SBCE

Help

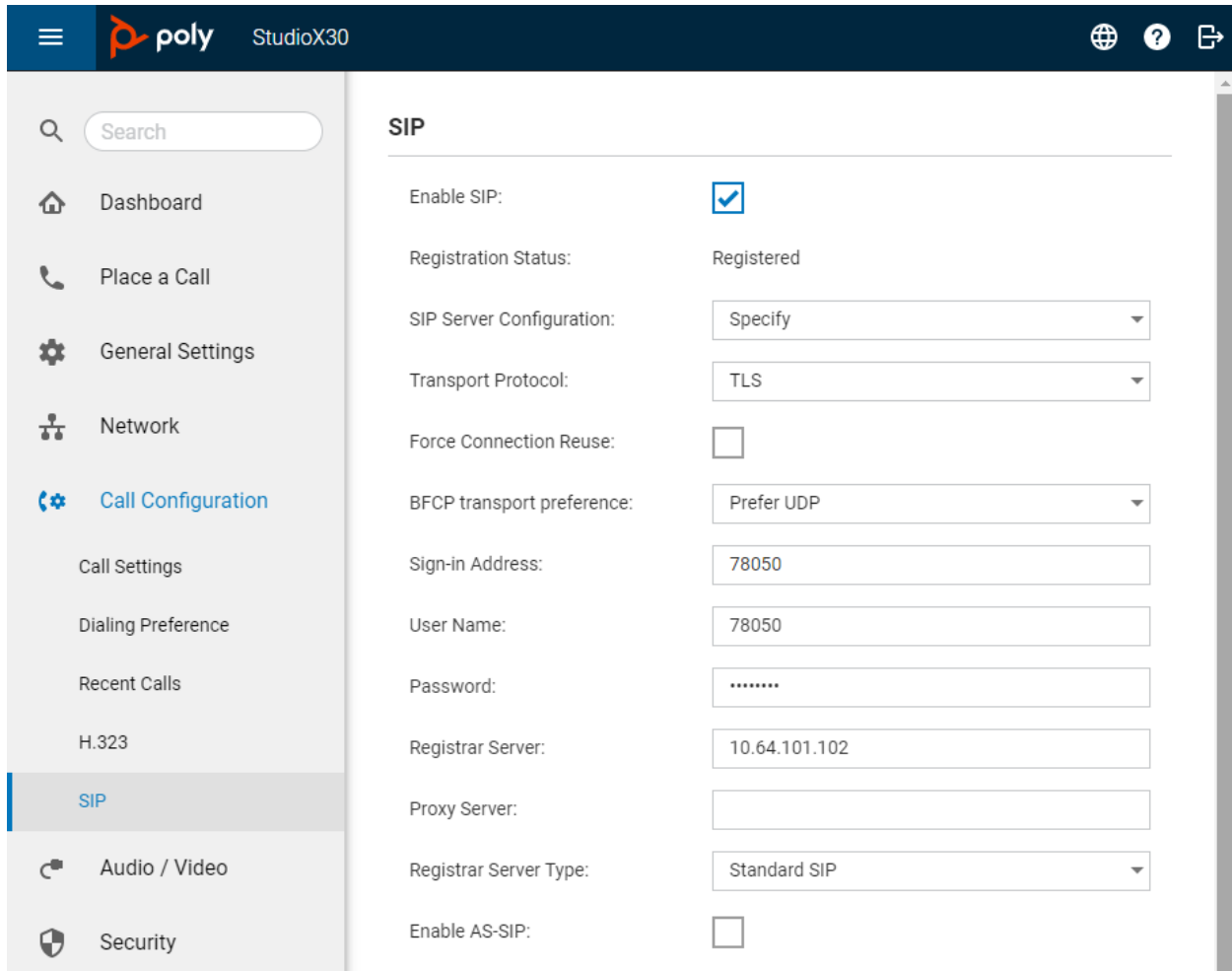
## User Registrations

AVAYA

Displaying entries 1 to 2 of 2.

AOR	SIP Instance	SBC Device	SM Address	Registration State
Contains <input type="text"/>	Contains <input type="text"/>	Contains <input type="text"/>	Contains <input type="text"/>	Contains <input type="text"/>
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

3. Alternatively, the registration status may be verified in the Studio X30 web interface. Navigate to **Call Configuration → SIP** and verify that **Registration Status** is *Registered*.



The screenshot displays the Studio X30 web interface. The top header bar includes the Poly logo, 'StudioX30' text, and icons for global settings, help, and sharing. 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, Recent Calls, H.323, SIP (highlighted), Audio / Video, and Security. The main content area is titled 'SIP' and contains the following configuration fields:

Field	Value
Enable SIP:	<input checked="" type="checkbox"/>
Registration Status:	Registered
SIP Server Configuration:	Specify
Transport Protocol:	TLS
Force Connection Reuse:	<input type="checkbox"/>
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:	<input type="checkbox"/>

4. Establish a video call with an Avaya video endpoint, such as Vantage. Verify there is two-way audio and video.

5. Call statistics for the active call can be viewed from the Studio X30 web interface. Navigate to **Active Call**, and then click on **Call Statistics**.

The screenshot displays the Studio X30 web interface. The top header bar includes the Poly logo, 'StudioX30', a green status bar with a phone icon and '00:00:43', 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 participant card for '78041' is displayed, showing details like Participant Name, Number, System, Call Type, Speed, and Encryption. Below this is a table of 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	1271	0%
VIDEO RX H.264-HP	1080p	1252	0%

## 10. 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 Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller. Poly video endpoints were able to register to Session Manager through SBC as remote workers and establish point-to-point audio and video calls to Avaya Workplace, Avaya Vantage, Avaya H.323 / SIP deskphones, and the PSTN. All feature and serviceability test cases were completed successfully with observations noted in **Section** □.

## 11. 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 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](mailto:devconnect@avaya.com).