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 3rd 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 3rd 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

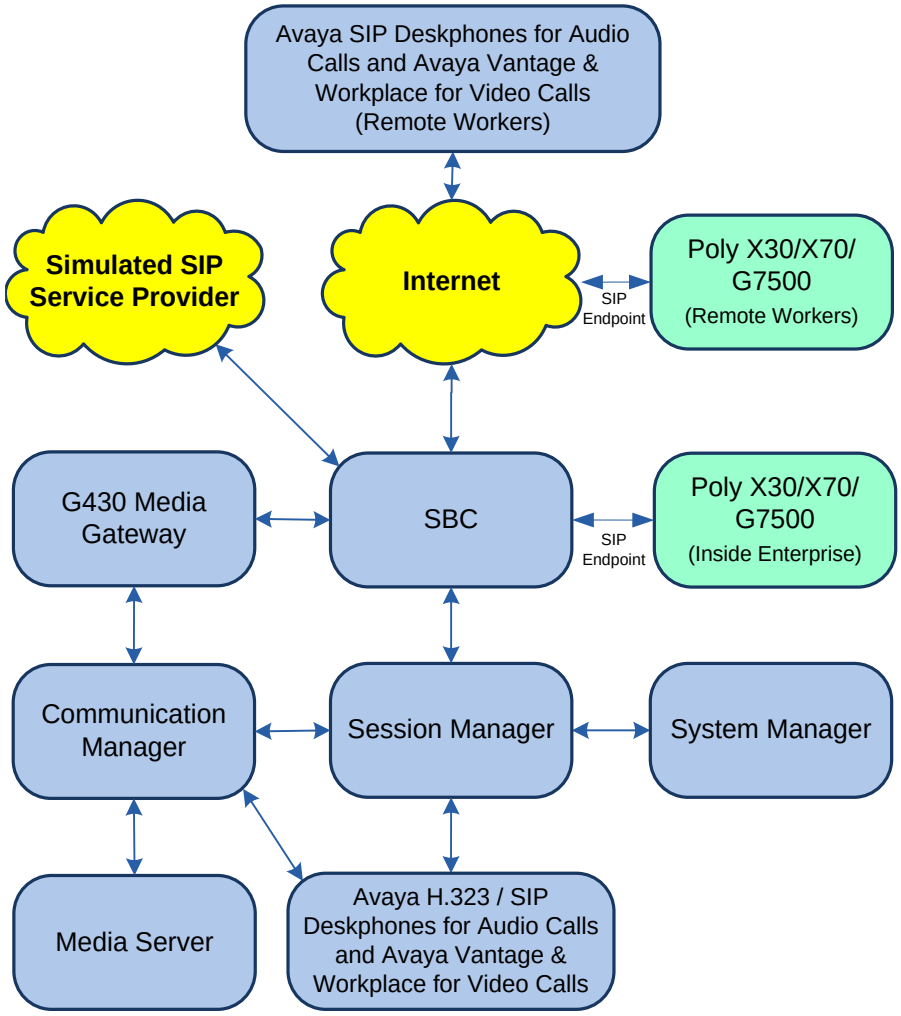
For support on Poly X30/X50/X70 Video Bar and G7500 Modular Video Conferencing System, visit the Poly support portal at https://www.poly.com/us/en/support.

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                    Page   1 of  12
                            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
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
```

5.3. 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

                                       Redun-                      Packet
                         Mode          dancy                       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:
```

5.4. 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
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y                 Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for 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                  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
```

5.6. 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           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    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 FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
    No          Mrk Lmt List Del  Digits                          QSIG
                              Dgts                                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 PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
 1: y y y y y n  n            rest                               unk-unk   none
 2: y y y y y n  n            rest                                         none
```

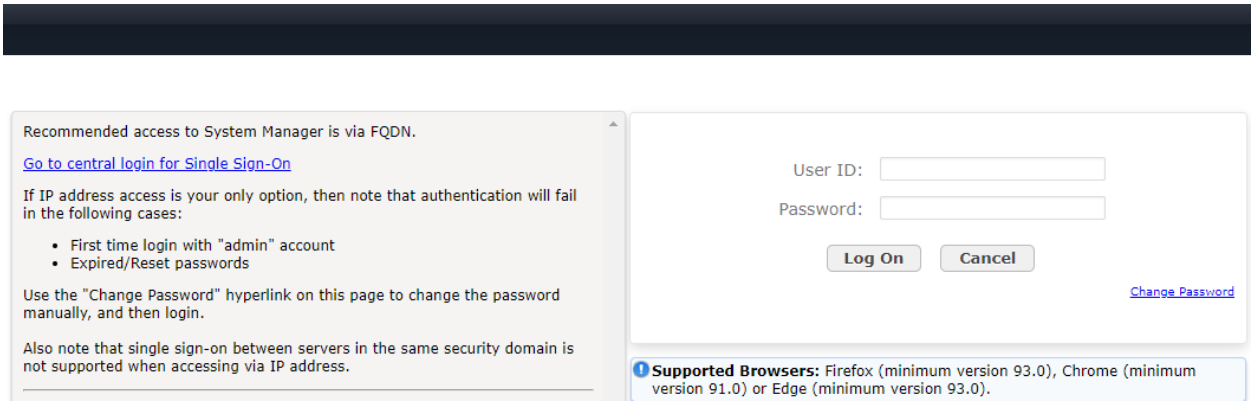
6. Configure Avaya Aura® Session Manager

This section covers the configuration of 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.

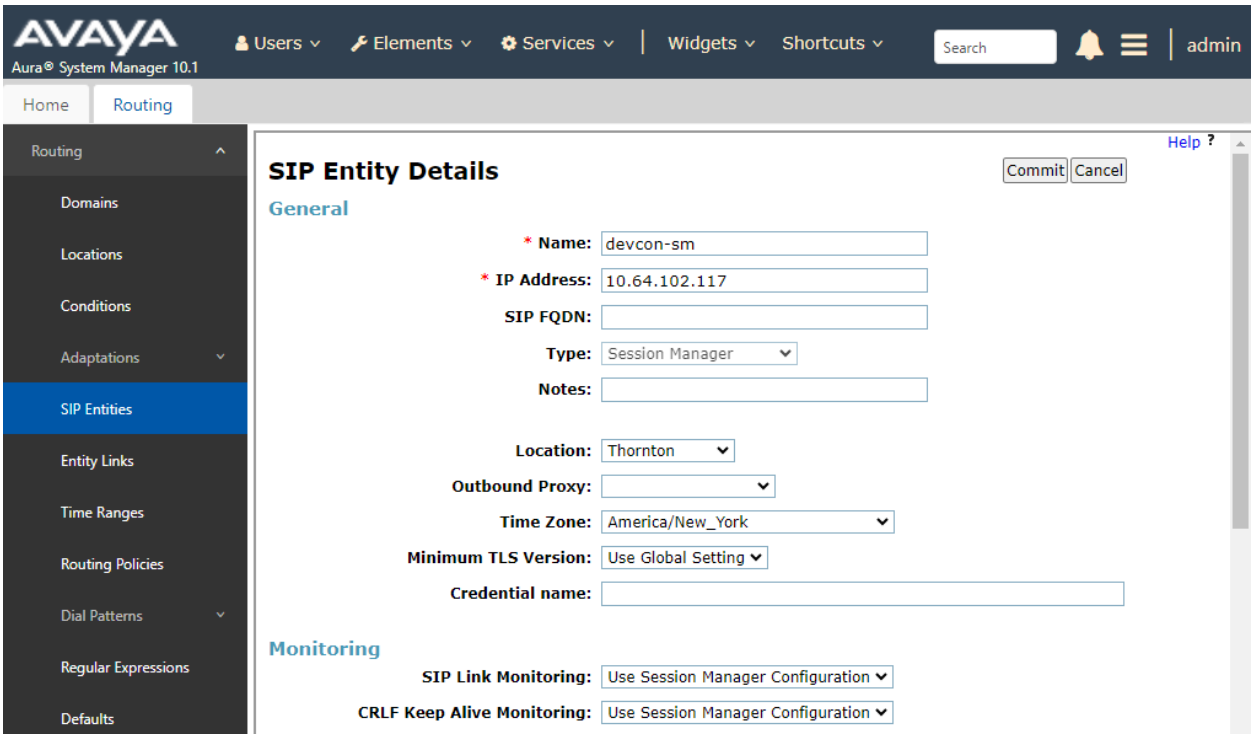
6.1. Launch System Manager

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.

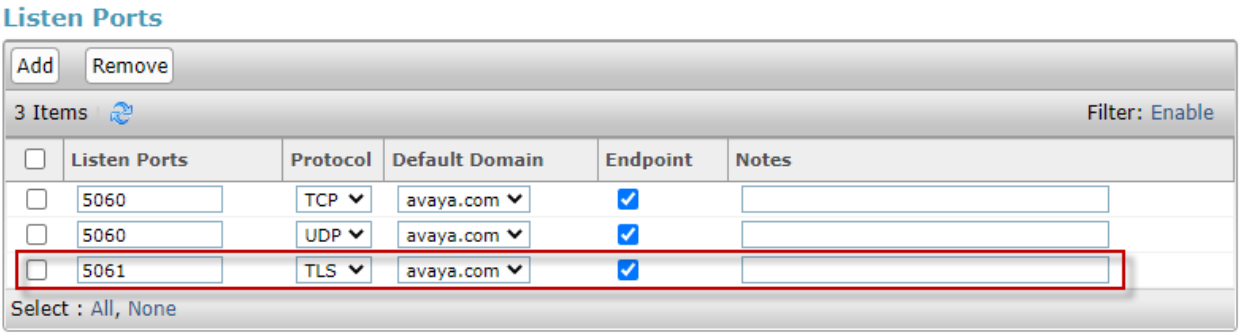


6.2. Set Network Transport Protocol

From the System Manager **Home** screen, select **Elements → Routing → SIP Entities** and edit the SIP Entity for Session Manager shown below.

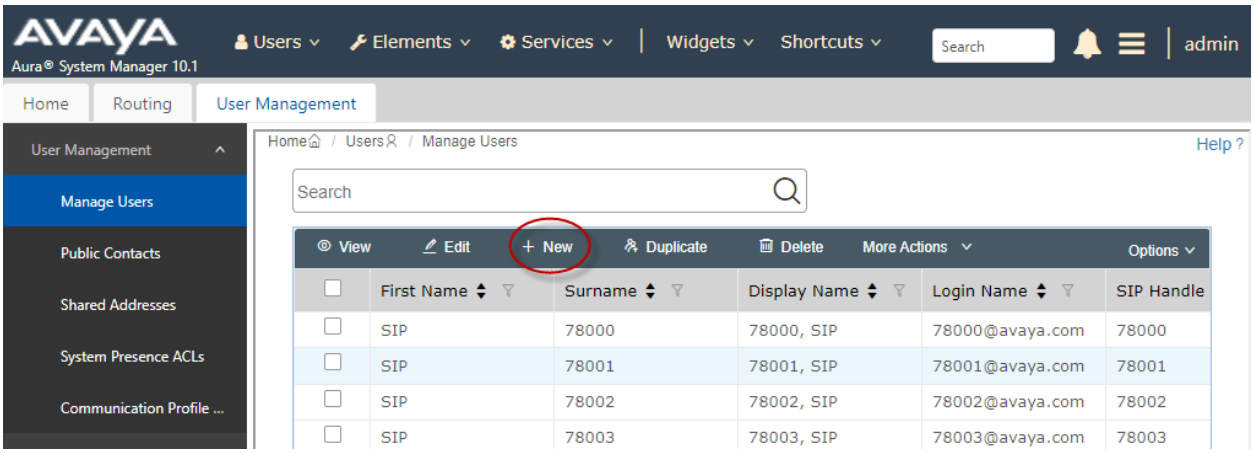


Scroll down to the **Listen Ports** section and verify that the transport network protocol used by Poly video endpoints is specified in the list below. For the compliance test, the solution used TLS network transport.



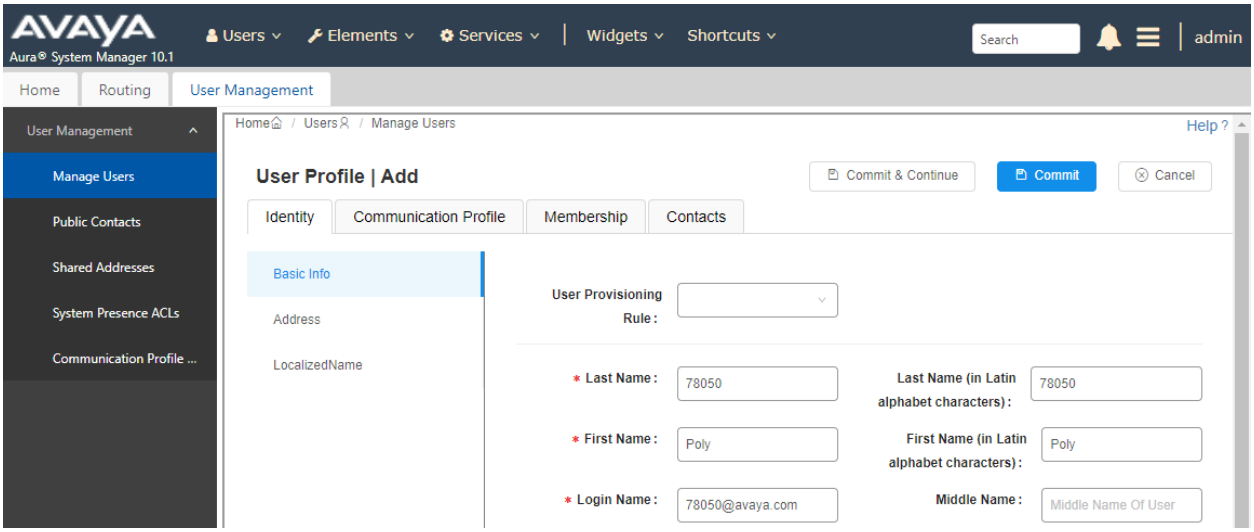
6.3. Administer SIP User

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.



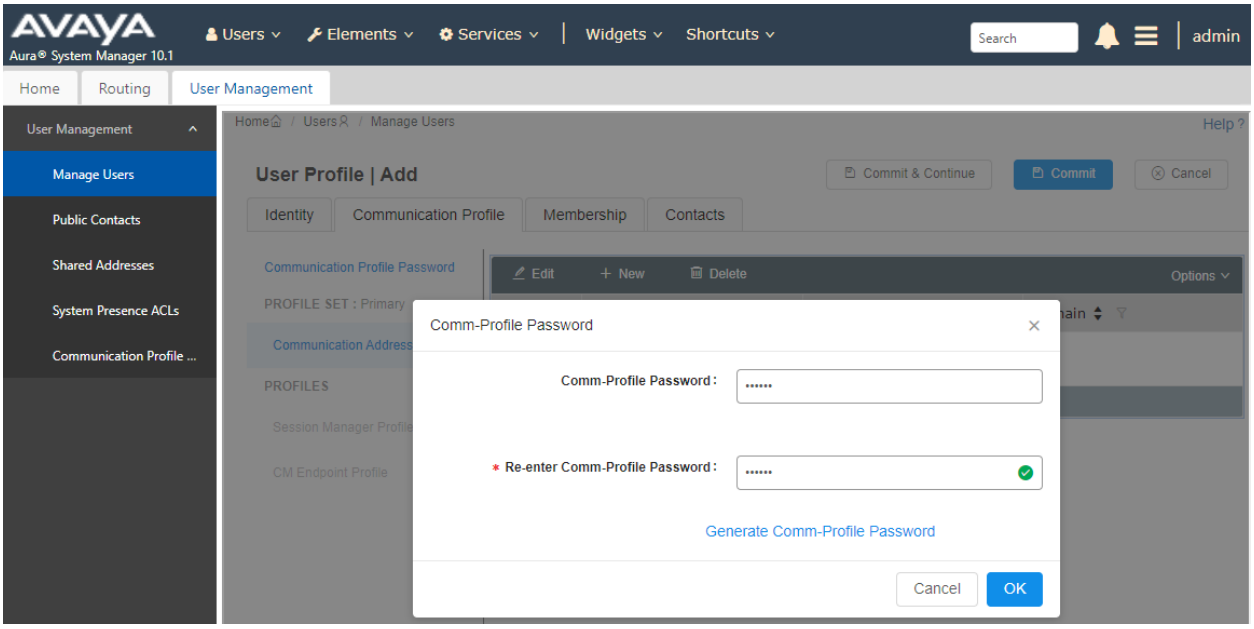
6.3.1. Identity

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.



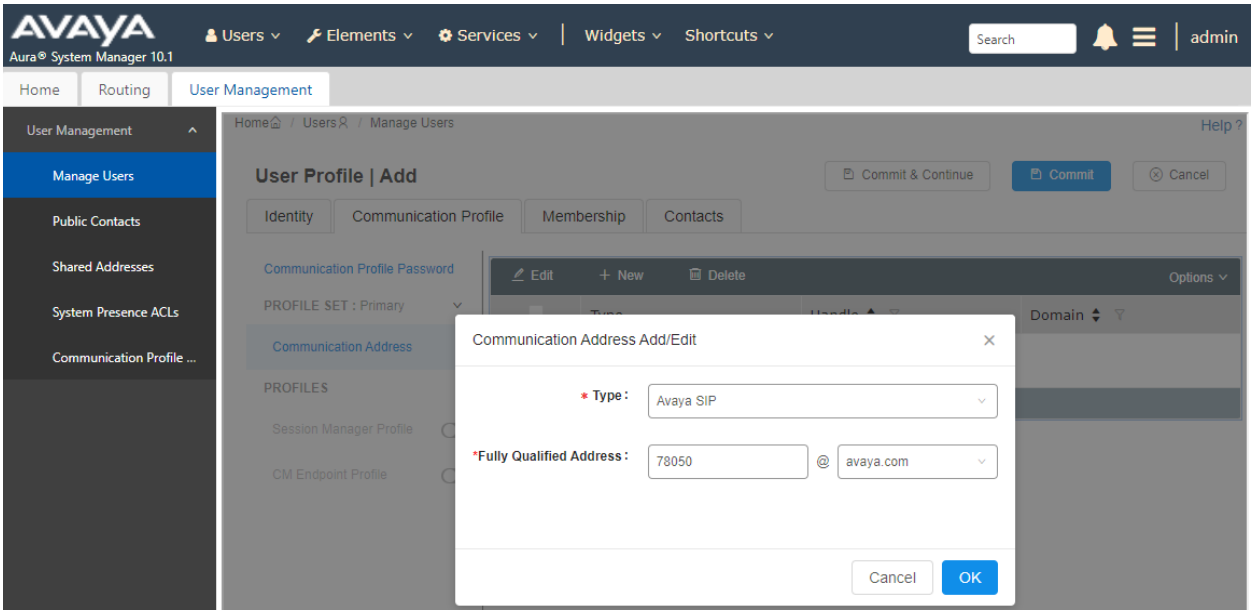
6.3.2. Communication Profile

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**.



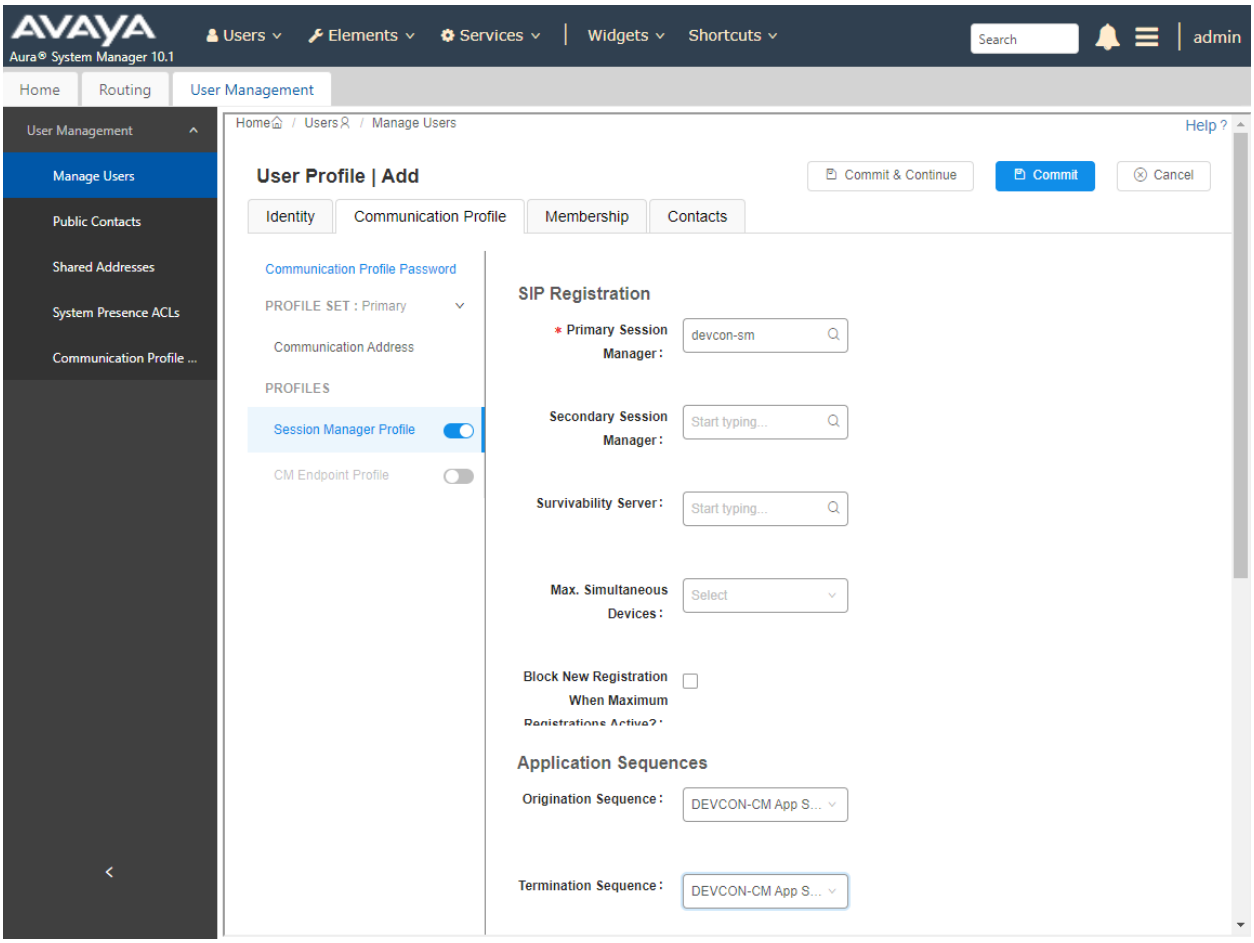
6.3.3. Communication Address

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**.

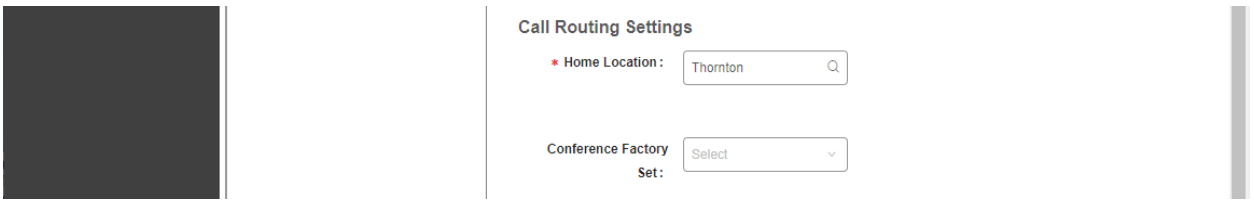


6.3.4. Session Manager Profile

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.

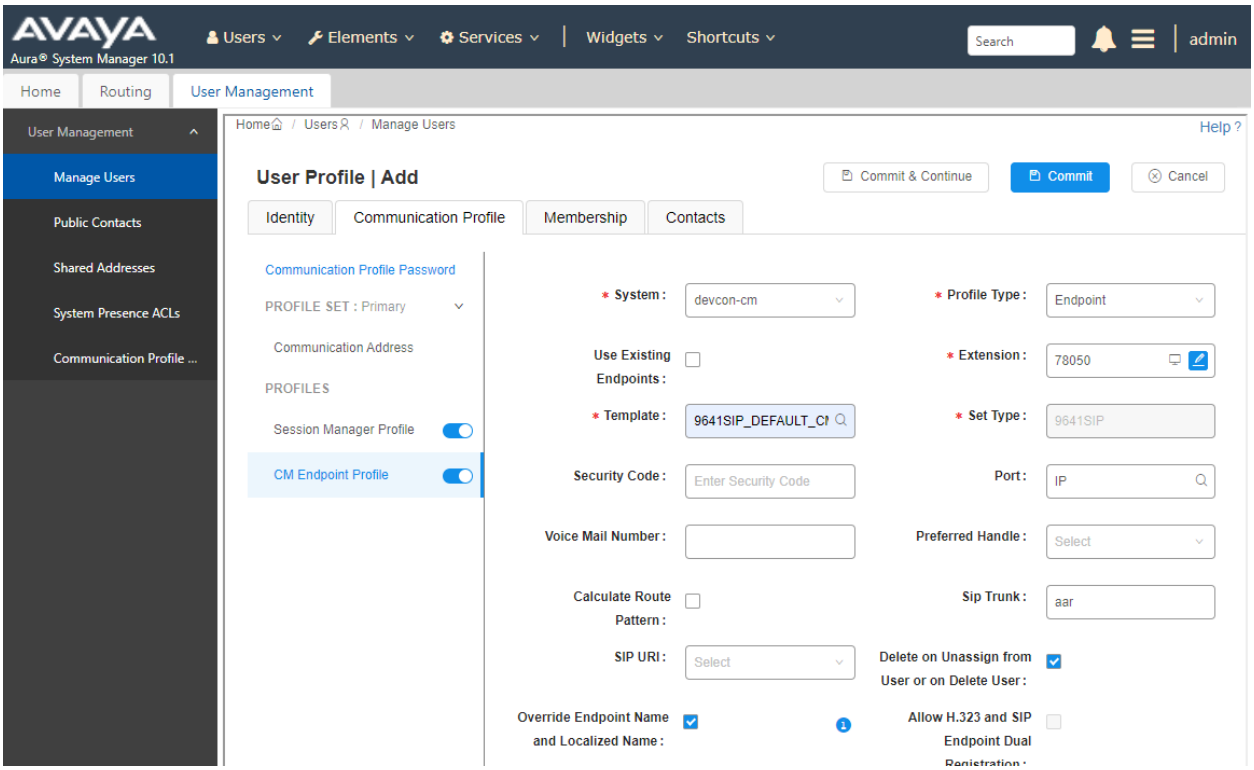


Scroll down to the **Call Routing Settings** section to configure the **Home Location**.



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.



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**.

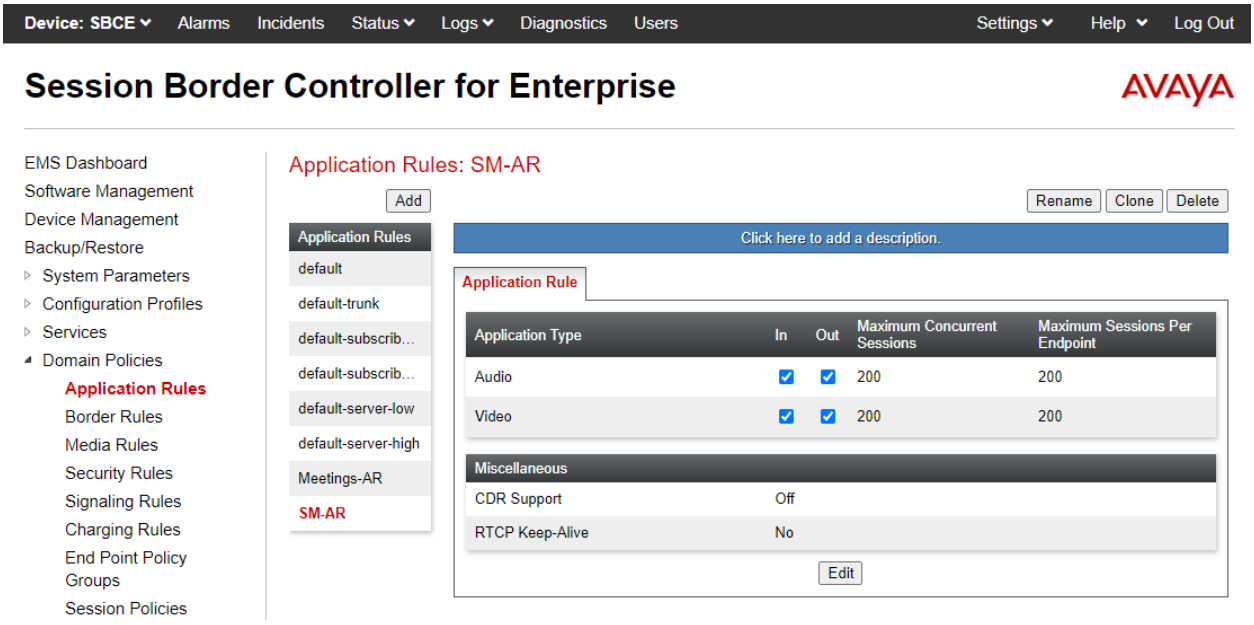
7.1. Launch SBC Web Interface

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.

7.2. Add Application Rule

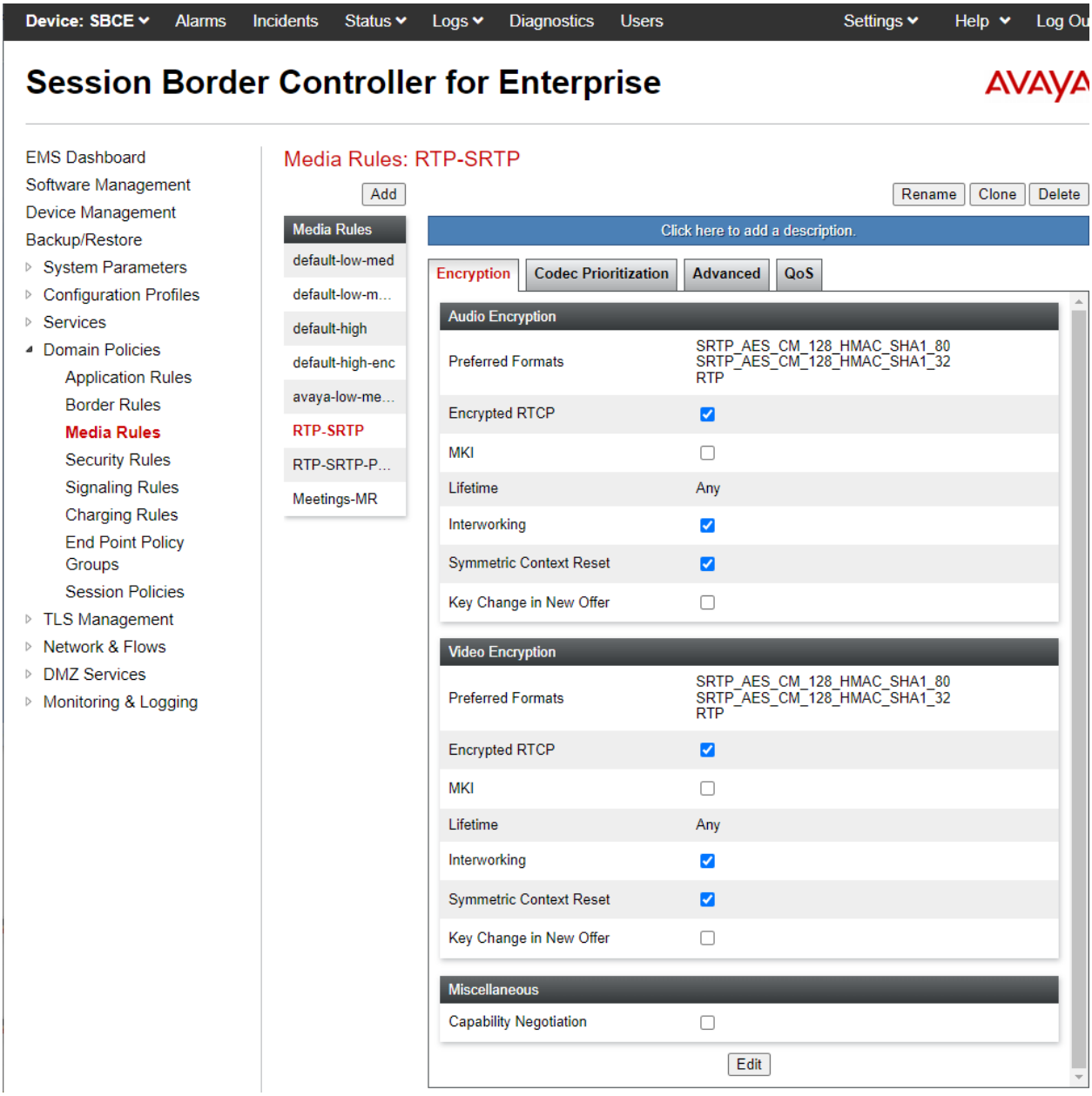
An Application Rule specifies whether audio and video traffic are allowed to enter the enterprise network and originate from within the enterprise network. In addition, an application rule specifies the maximum number of concurrent voice and video sessions that can be processed. To add or modify an application 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.

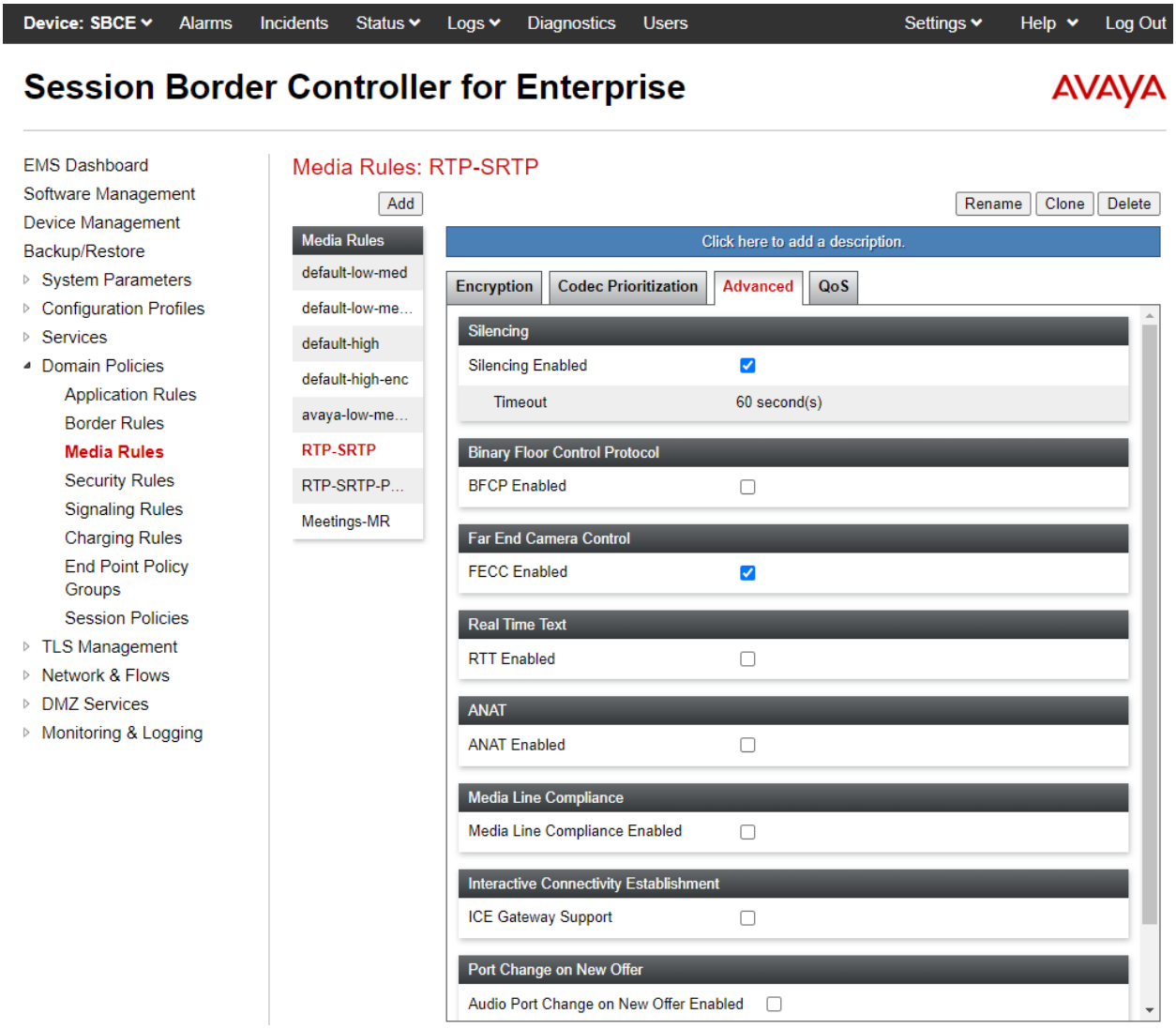


7.3. Modify Media Rule

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.

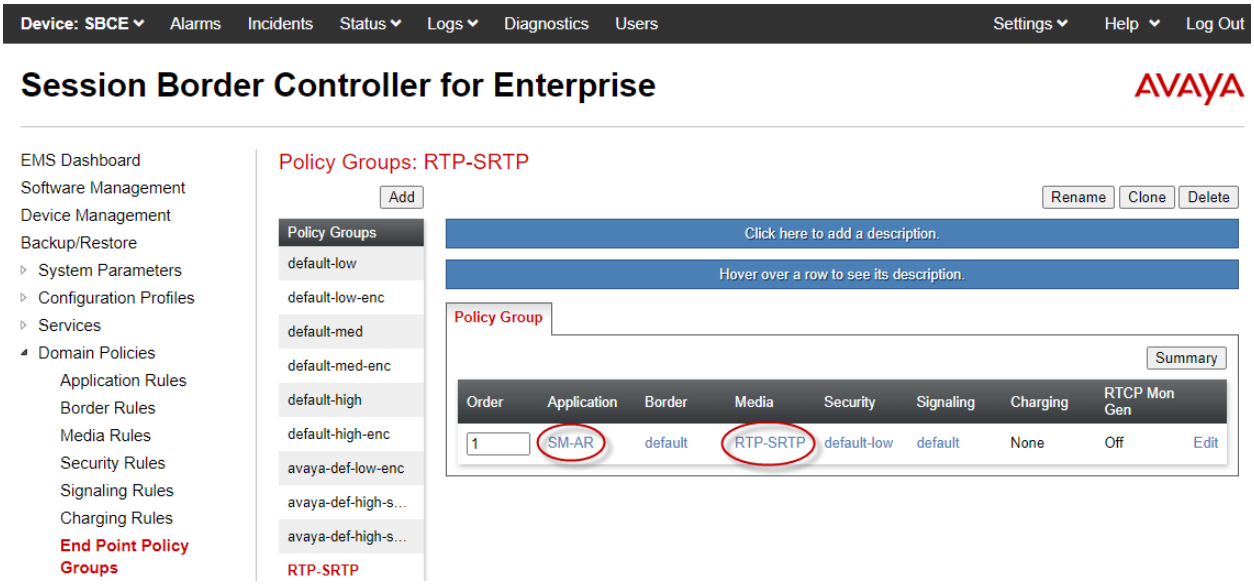


The **Advanced** tab and verify that **BFCP Enabled** is unchecked.



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**.

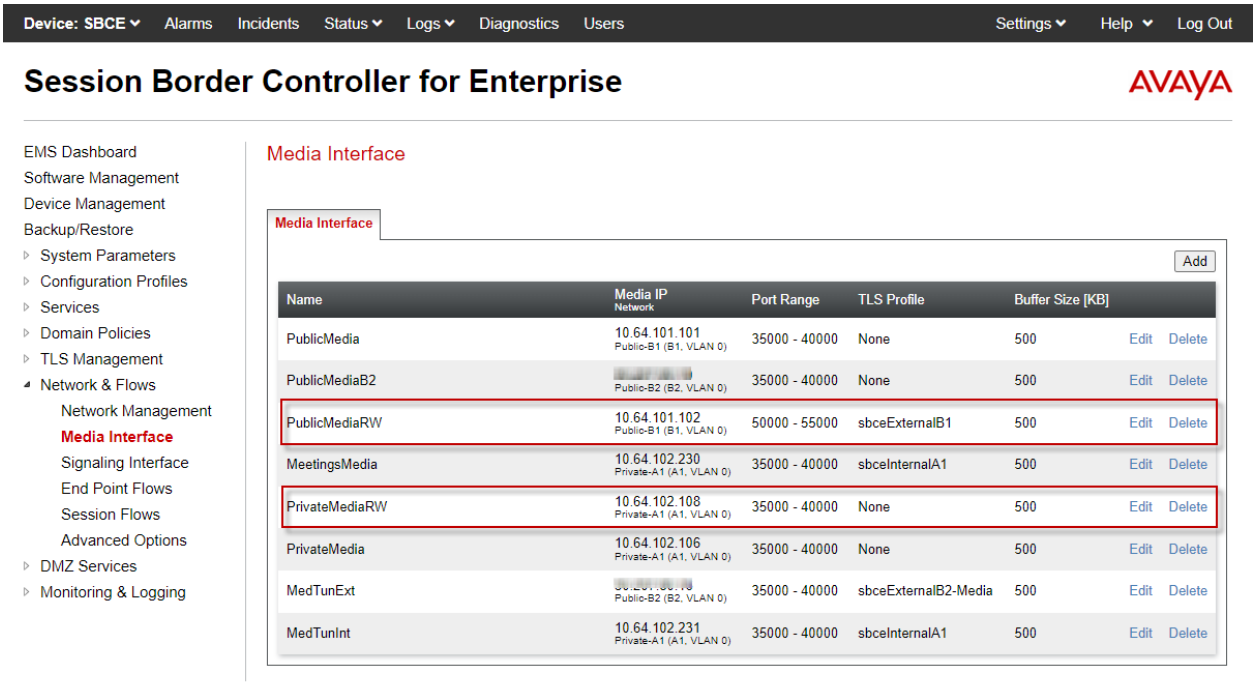


7.5. Administer Media Interfaces

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.

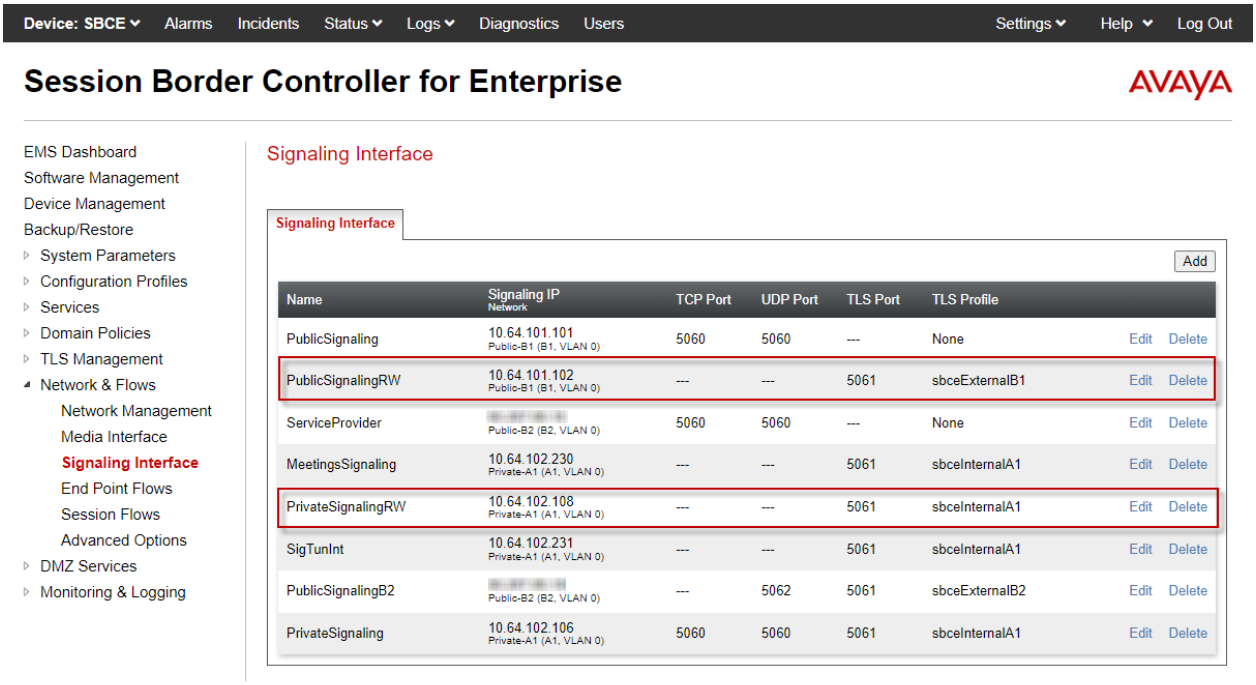


7.6. Administer Signaling Interfaces

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.

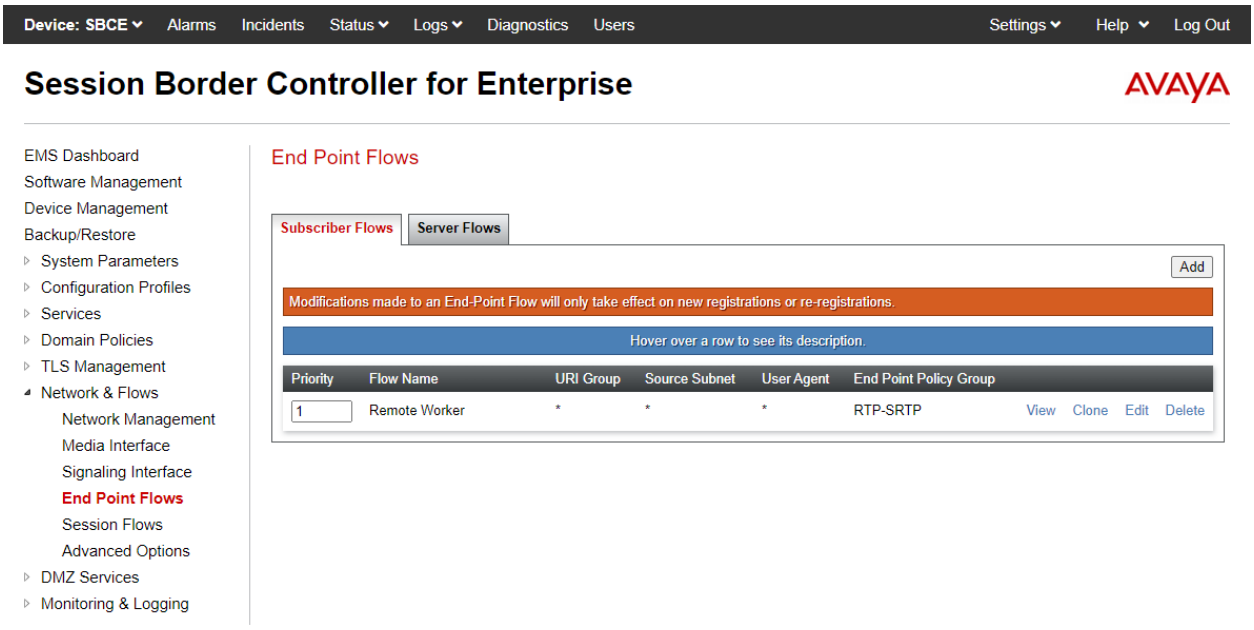


7.7. Administer End Point Flows

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).



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

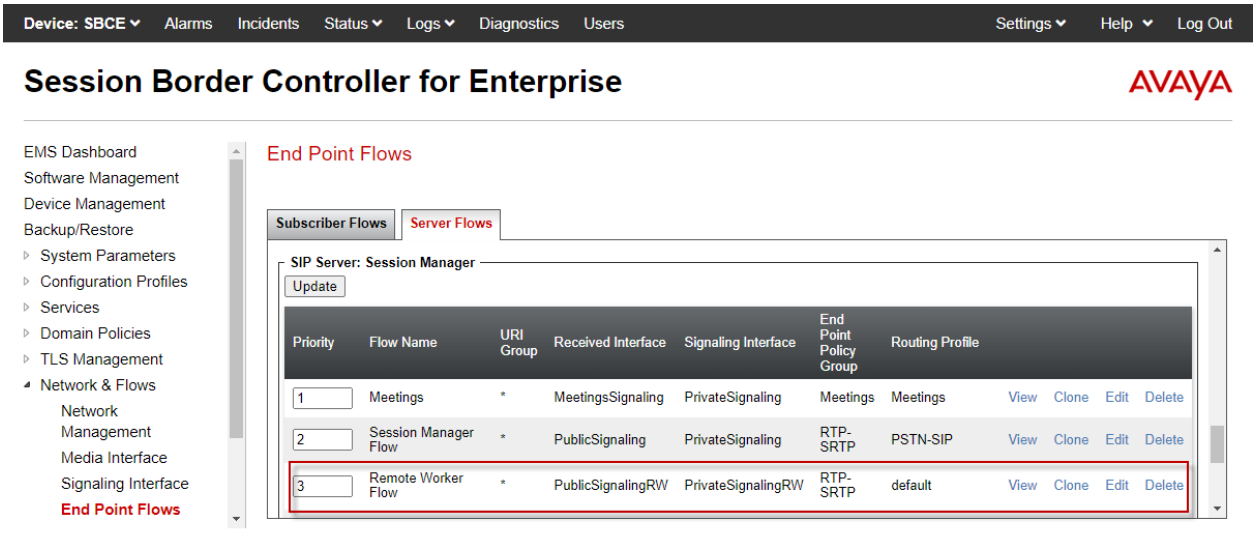
TLS Client Profile	sbceExternalB1
Signaling Manipulation Script	None

Profile

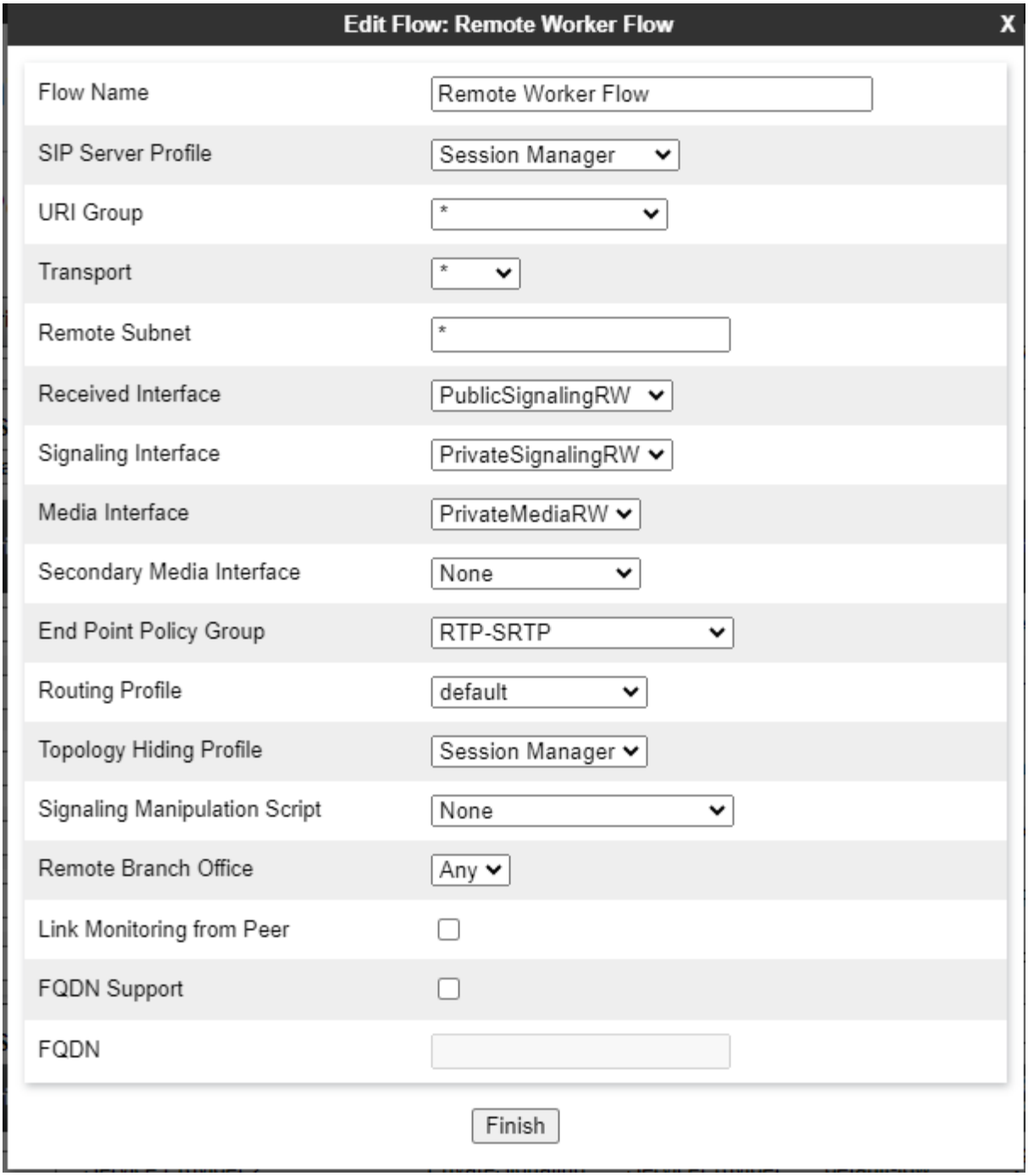
Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	*
Media Interface	PublicMediaRW
Secondary Media Interface	None
End Point Policy Group	RTP-SRTP
Routing Profile	Session Manager
Presence Server Address	---
FQDN Support	☐
IP / URI Blocklist Profile	None / Disabled

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.



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



8. Configure Poly Studio X30 Video Bar

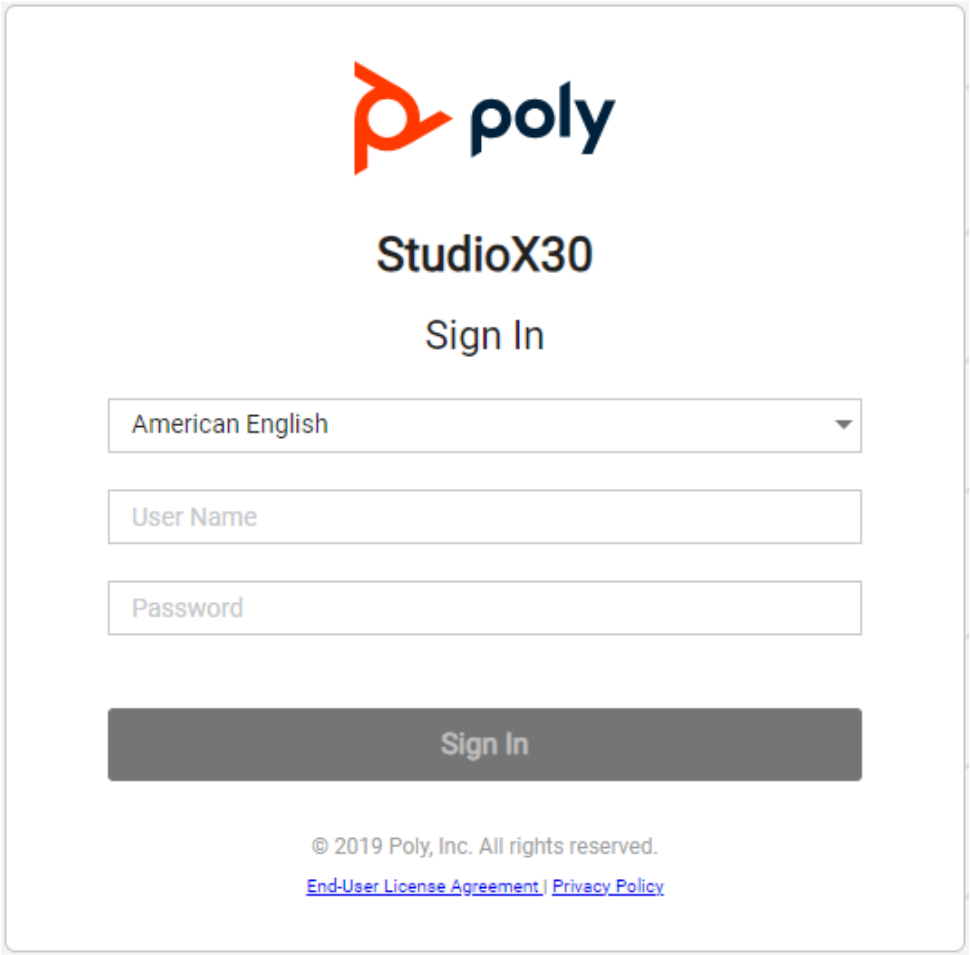
This section covers the configuration of Studio X30 to register to Session Manager through SBC as a remote worker. This configuration requires following steps:

- 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.

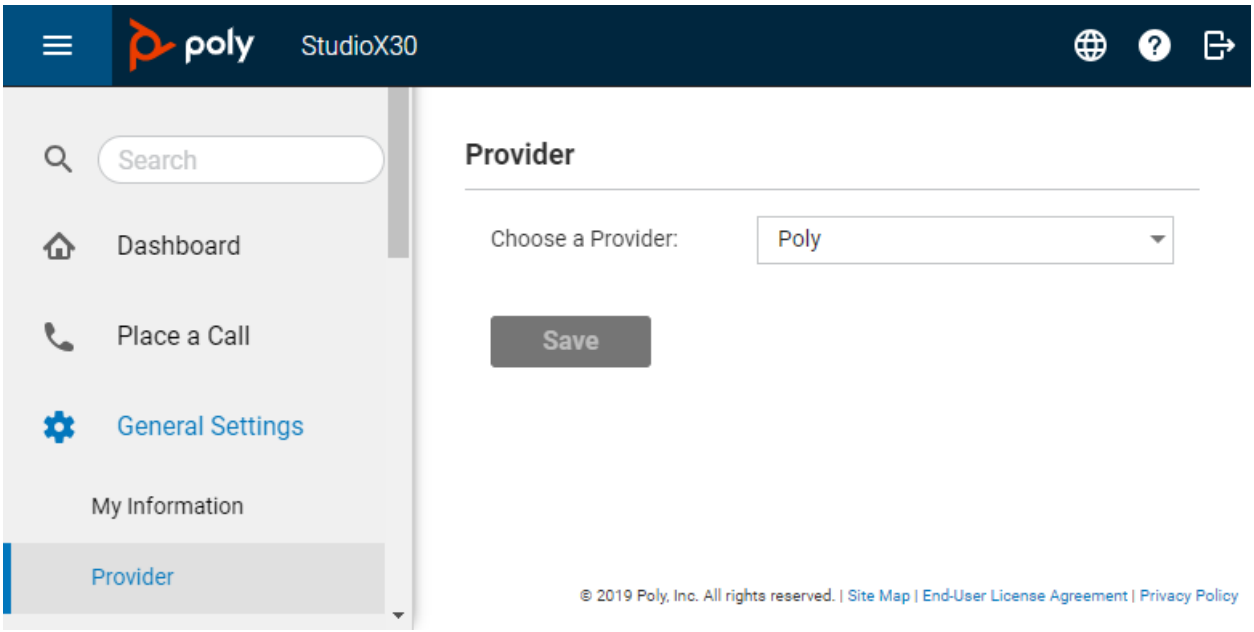
8.1. Access Studio X30 Web Interface

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.



8.2. Set Provider

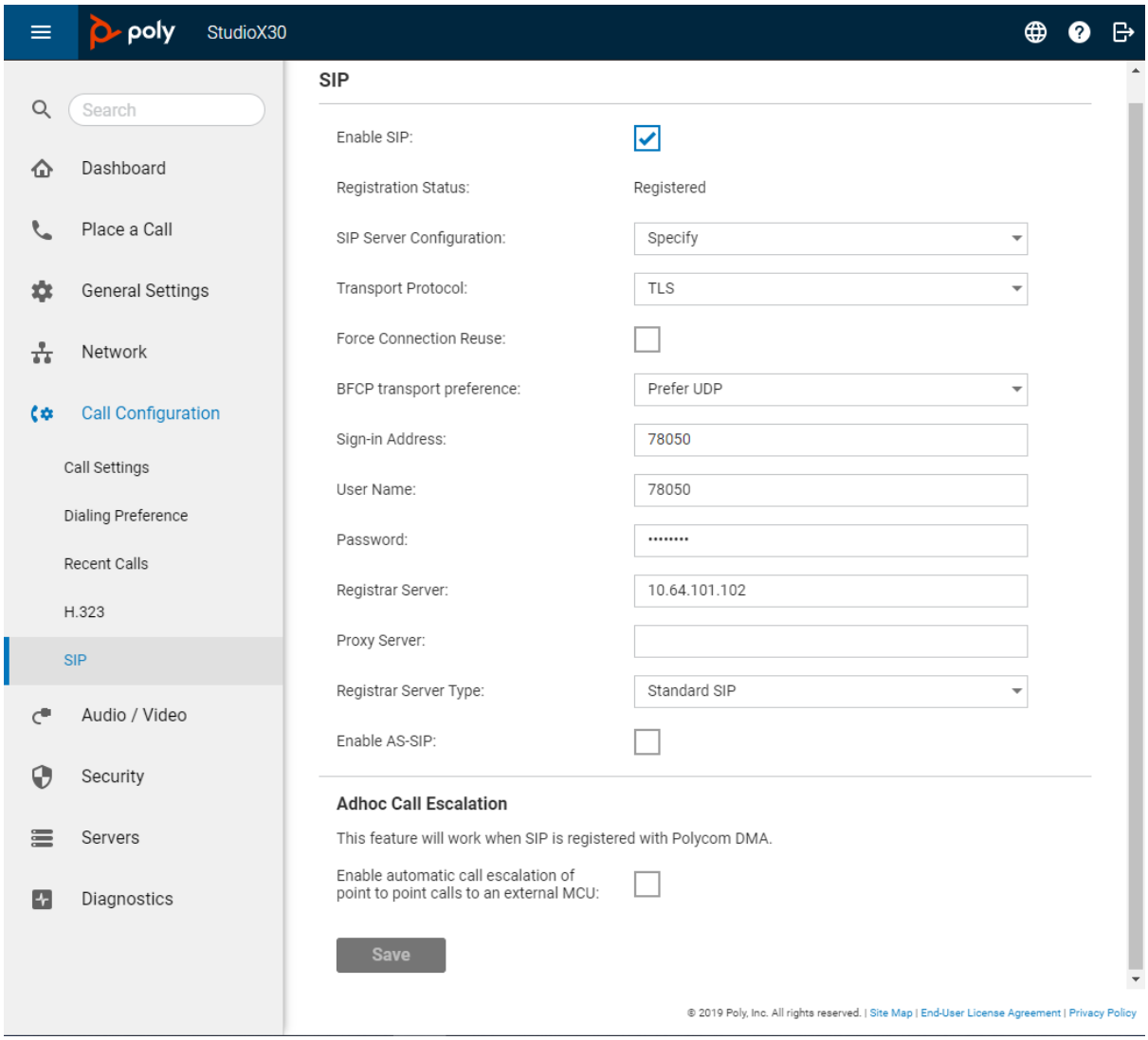
Navigate to **General Settings → Provider** in the left pane and verify *Poly* is set as the provider as shown below.



8.3. Administer SIP Settings

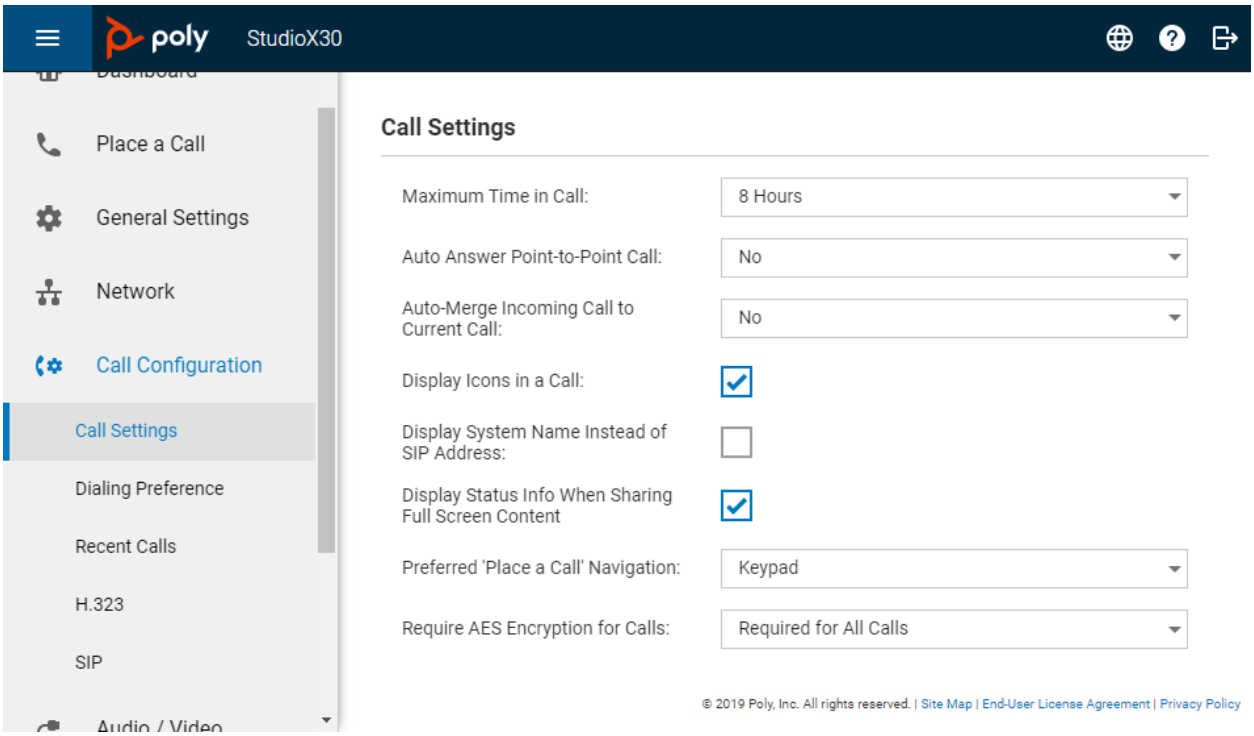
Navigate to **Call Configuration → SIP** and configure the following fields:

- **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 X30is located within the enterprise network.



8.4. Administer Call Settings

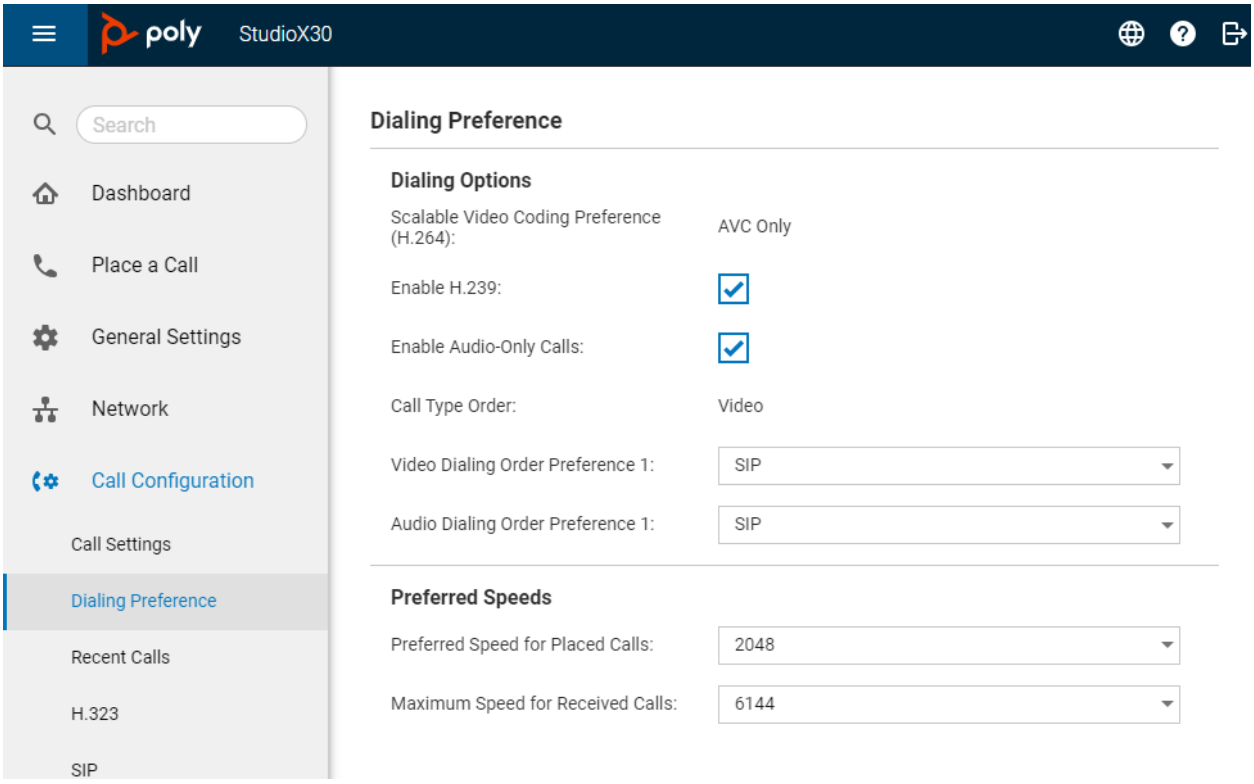
Navigate to **Call Configuration → Call Settings** to configure the **Require AES Encryption for Calls** field. Set this field to *Required for All Calls* to enforce SRTP for audio and video calls.



8.5. Administer Dialing Options

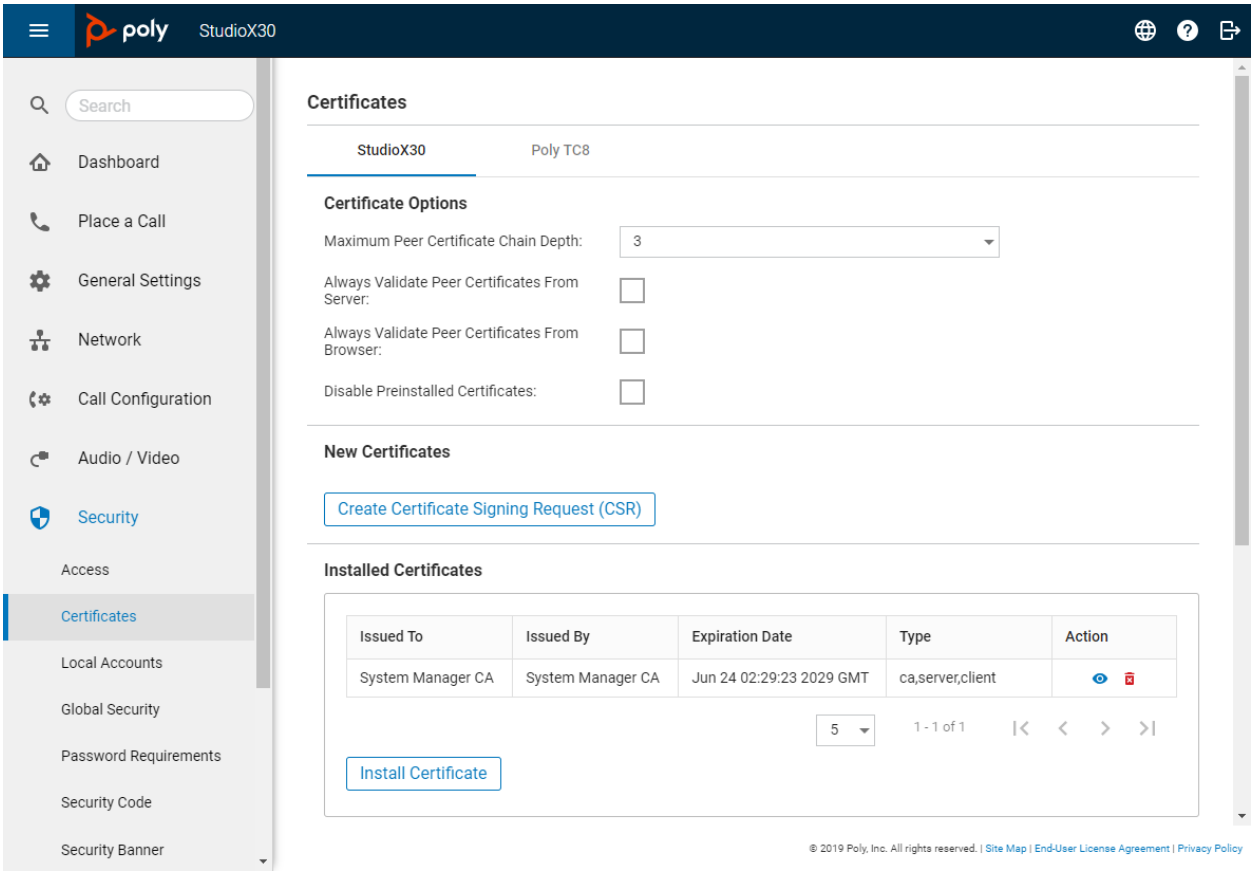
Navigate to **Call Configuration → Dialing Preference** to configure the following fields:

- **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*).



8.6. Install Certificate

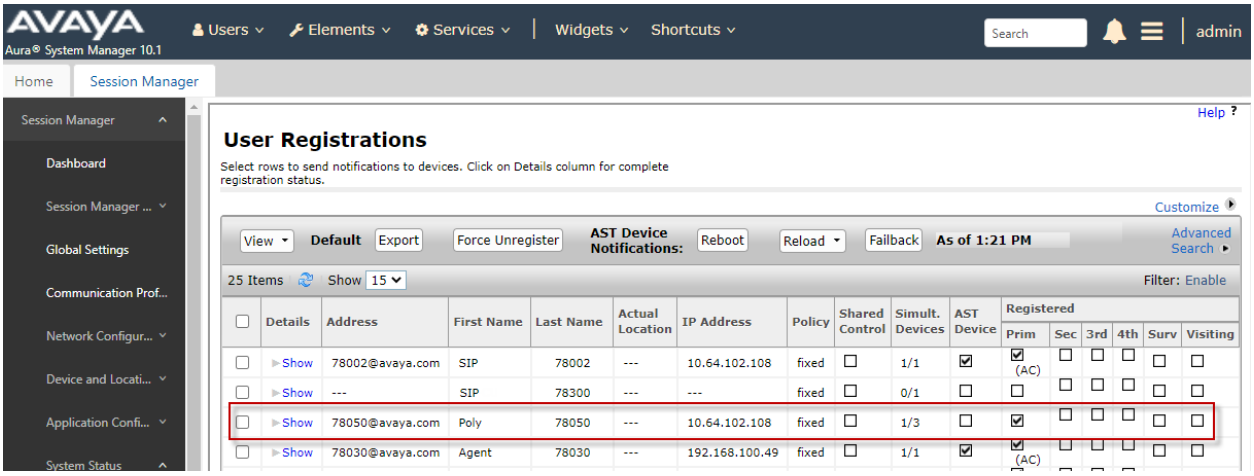
Navigate to **Security → Certificates** to install certificates. To support TLS, click on **Install Certificate** to import the TLS certificate from Avaya Aura® System Manager, the certificate authority. This certificate is used for SIP signaling with SBC. When done, the user-installed certificates are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



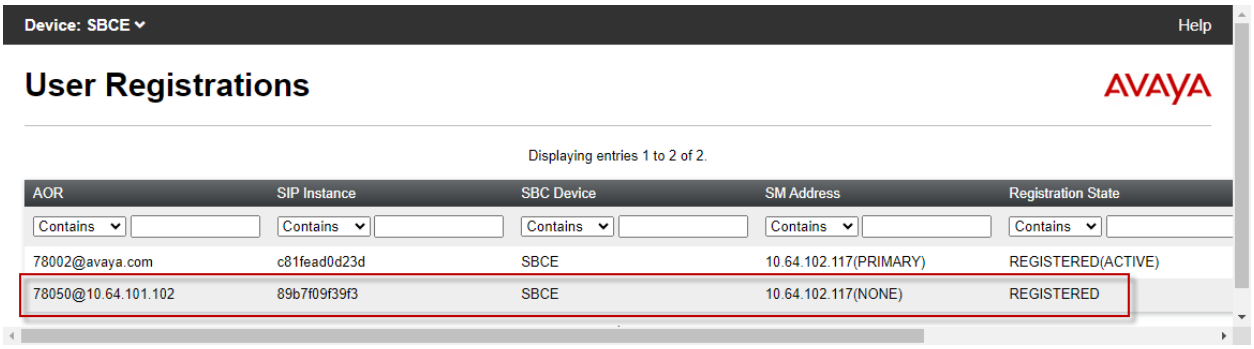
9. Verification Steps

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

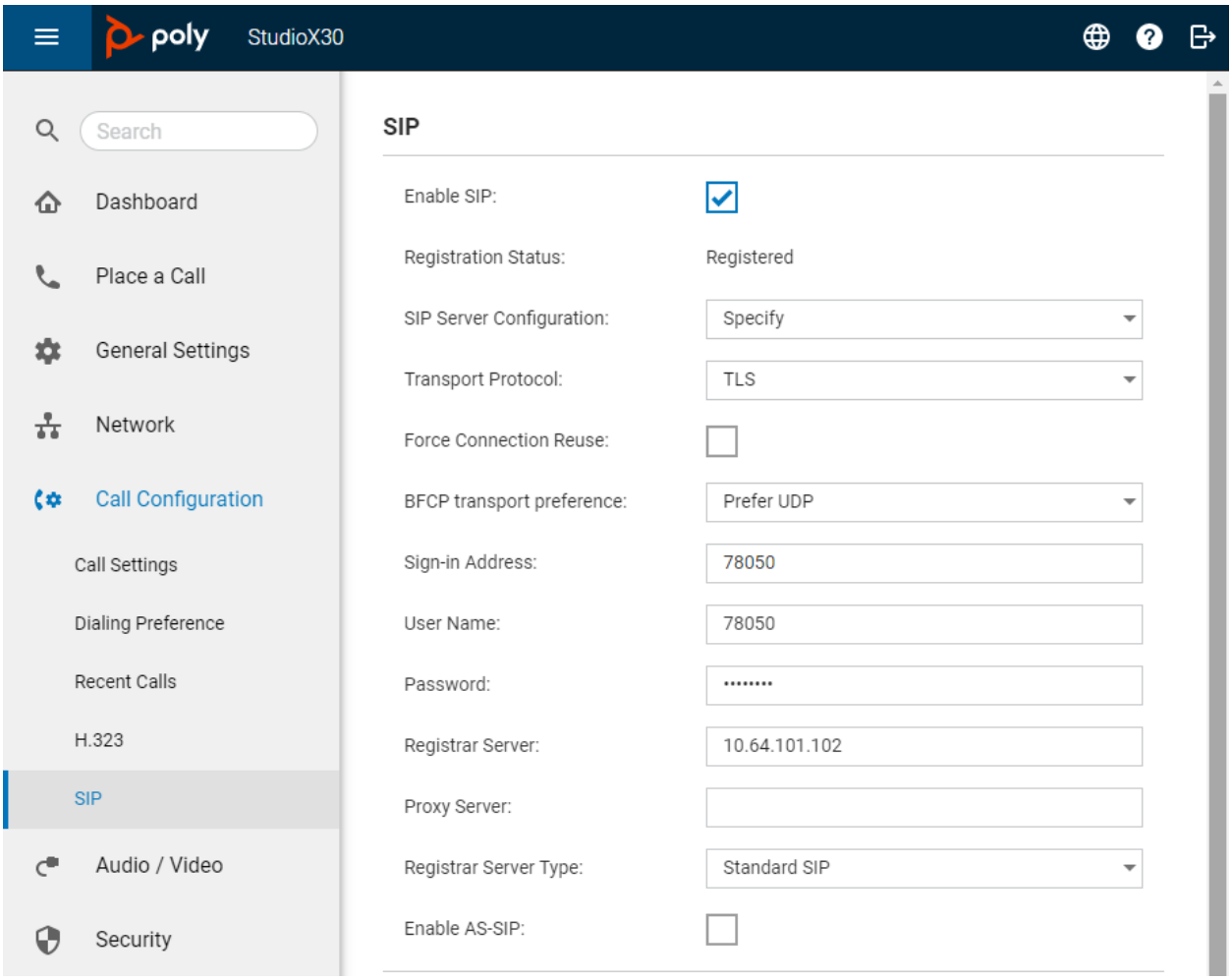
1. Verify that Studio X30 has successfully registered with Session Manager. In System Manager, navigate to **Elements → Session Manager → System Status → User Registrations** to check the registration status.



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.

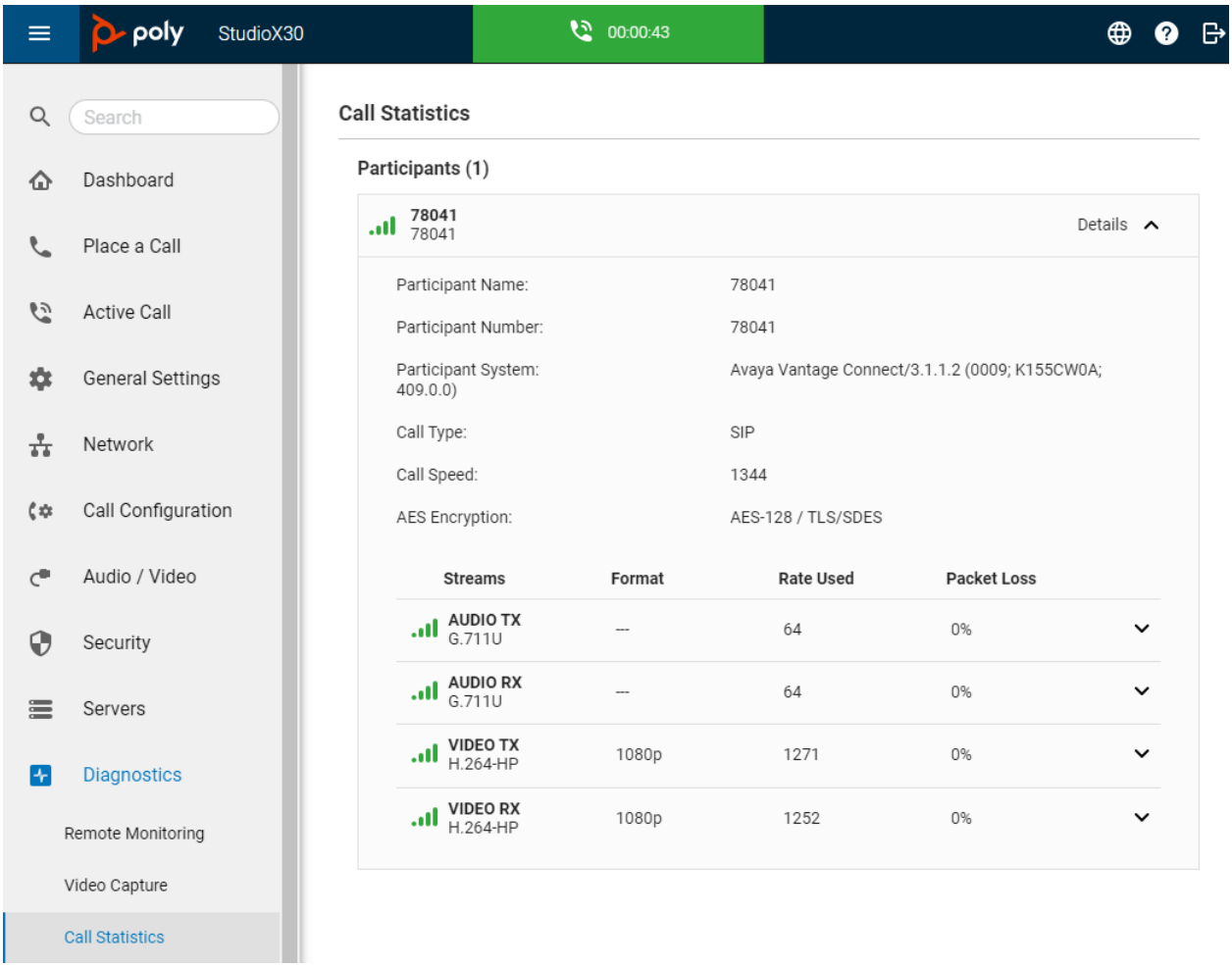


3. Alternatively, the registration status may be verified in the Studio X30 web interface. Navigate to **Call Configuration → SIP** and verify that **Registration Status** is *Registered*.



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**.



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.

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.