Avaya Solution & Interoperability Test Lab

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

Abstract

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

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

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

Table of Contents

1. Introduction

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

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

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

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

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

When Poly video endpoints register directly to Meetings Management via H.323, they join meetings and establish point-to-point calls to other Poly video endpoints registered to Meetings Management using H.323. In this configuration, the Poly video endpoints also registered to Session Manager through Session Border Controller via SIP. That is, simultaneous, dual registration was supported. The SIP interface was used for point-to-point calls to Avaya endpoints registered to Session Manager via SIP or Communication Manager via H.323. Poly video endpoints were configured to attempt calls using H.323, and if that fails, attempt the call using SIP. Refer to **Section 9.6** for configuring dialing options.

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

2. General Test Approach and Test Results

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

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

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

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

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

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

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

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

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

2.2. Test Results

All test cases passed with the following observations:

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

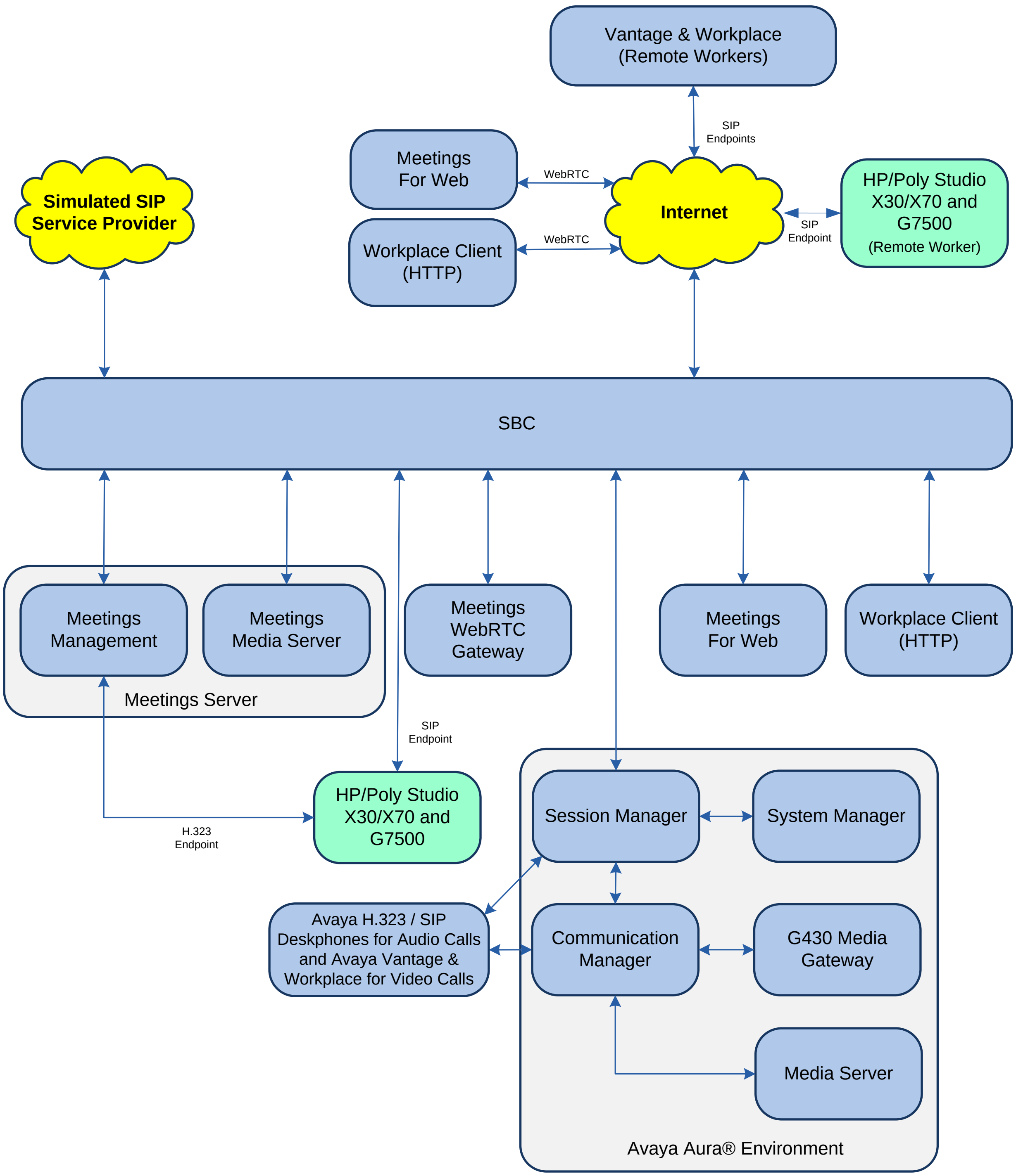
- When Poly video endpoints join a PIN-protected meeting using H.323, set the **addDTMFsInSimAltCaps** parameter to *1* in Meetings Media Server so that Poly video endpoints send PIN via out-of-band DTMF using H.245 as described in **Section 7.3**; otherwise, PIN authentication would fail.

2.3. Support

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

3. Reference Configuration

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



4. Equipment and Software Validated

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

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

5. Configure Avaya Aura® Communication Manager

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

5.1. Administer IP Node Names

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

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
devcon-aes          10.64.102.119
devcon-ams          10.64.102.118
devcon-sm           10.64.102.117
procr               10.64.102.115
procr6              ::

( 6  of 6    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.2. Administer IP Codec Set

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

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

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

                           IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.722-64K                    2        20
 2: G.729A           n           2        20
 3: G.711MU          n           2        20
 4:
 5:
 6:

     Media Encryption                   Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: none
 4:
 5:
```

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

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

                           IP MEDIA PARAMETERS

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

                                          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:
```

5.3. Administer IP Network Region

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

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: avaya.com
    Name: SIP Enterprise        Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 50999
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.4. Administer SIP Trunk to Session Manager

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

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

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

```
add signaling-group 10                                     Page   1 of   2
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y                                 Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                     Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                Far-end Node Name: devcon-sm
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1

Far-end Domain: avaya.com
                                             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 Meetings Server. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Configure the other fields in bold and accept the default values for the remaining fields.

```
add trunk-group 10                                                Page   1 of  5
                                TRUNK GROUP

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

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

```
add trunk-group 10                                                Page   5 of   5
                              PROTOCOL VARIATIONS

                                        Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
     Resend Display UPDATE Once on Receipt of 481 Response? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
          Enable Q-SIP? n
          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                              Request URI Contents: may-have-extra-digits
```

5.5. AAR Call Routing

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

```
change aar analysis 78                                        Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

          Dialed           Total     Route     Call    Node  ANI
          String          Min  Max  Pattern    Type    Num   Reqd
    78                    5    5     10        lev0          n
    79                    5    5     10        lev0          n
```

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

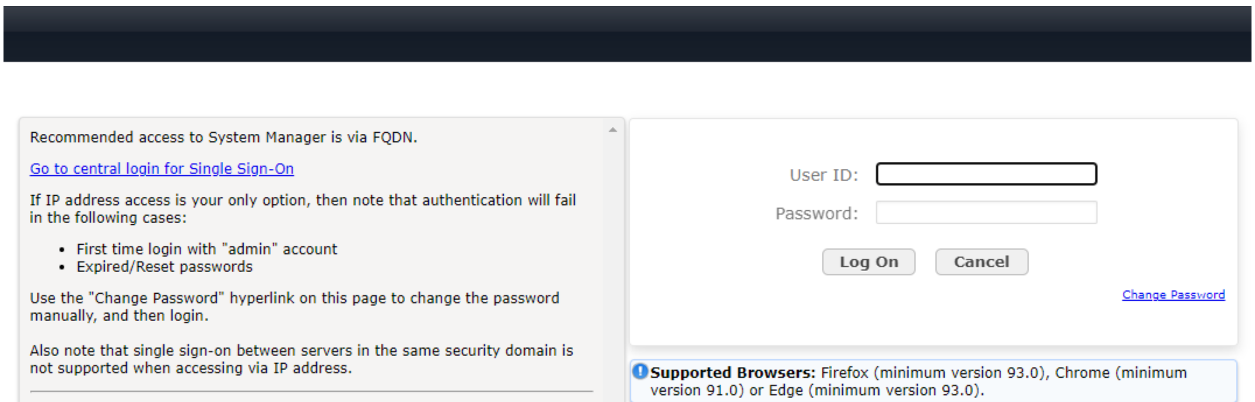
```
change route-pattern 10                                       Page   1 of   3
                    Pattern Number: 10     Pattern Name: To devcon-sm
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                           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 Session Manager, including setting the transport protocol and port for SIP endpoints registered to Session Manager and adding a SIP user for Poly video endpoints.

6.1. Launch System Manager

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



6.2. Add SIP Entities and Entity Links

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

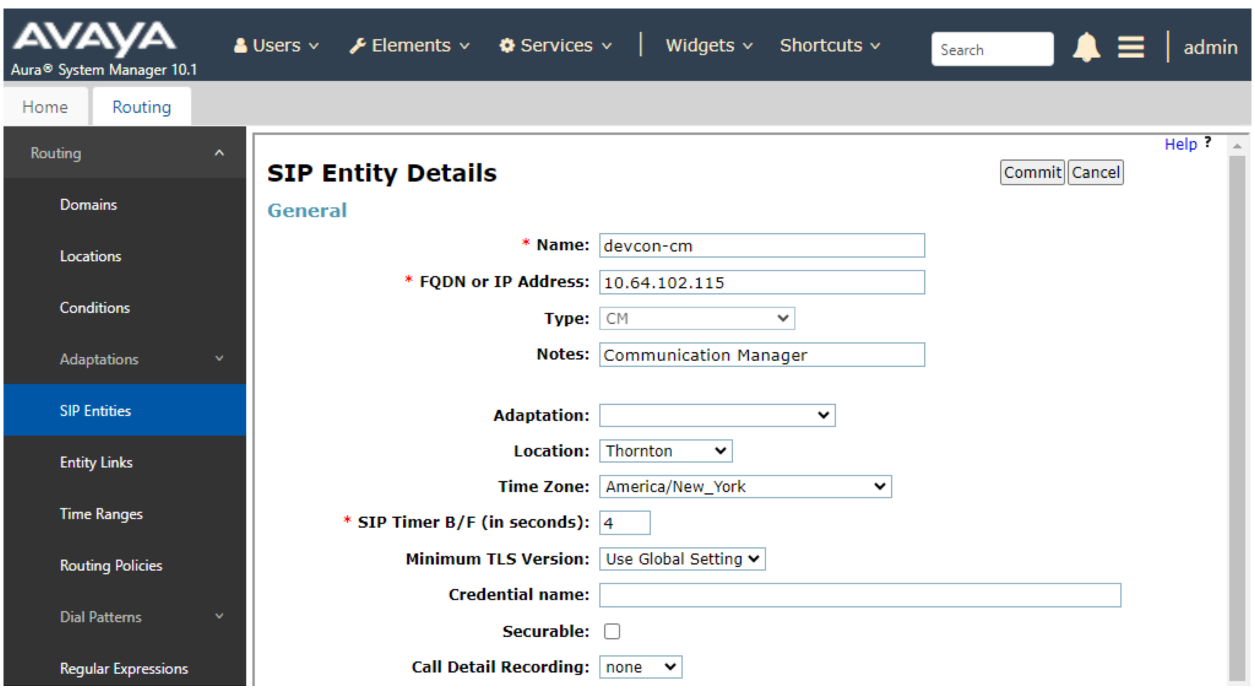
6.2.1. Communication Manager SIP Entity and Entity Link

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

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

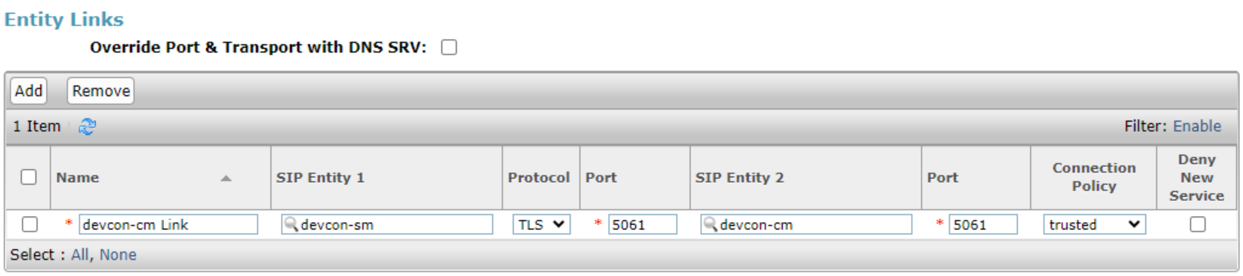
- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., procr) on Communication Manager.
- **Type:** Select *CM*.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

Default values can be used for the remaining fields.



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

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

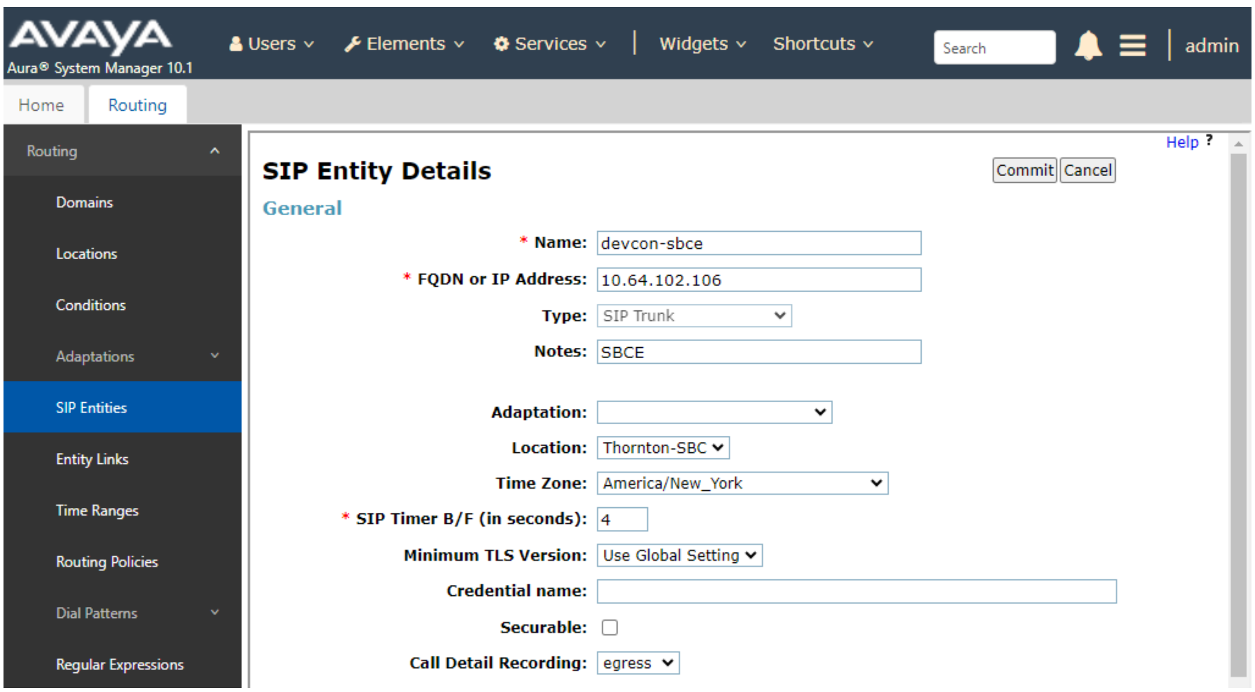


6.2.2. SBC SIP Entity and Entity Link

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

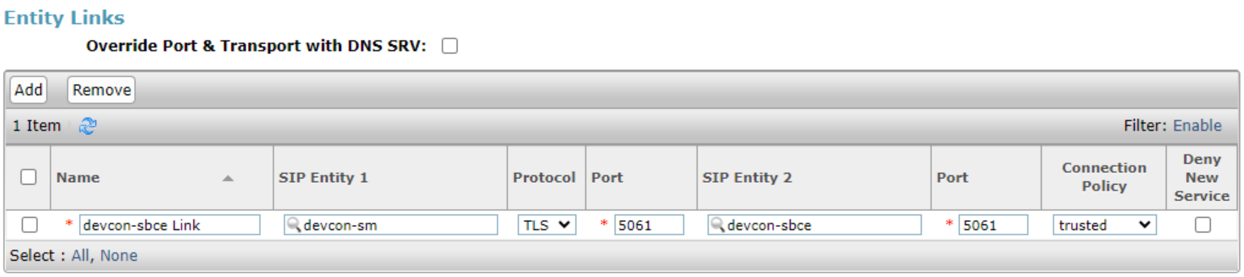
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

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



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

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



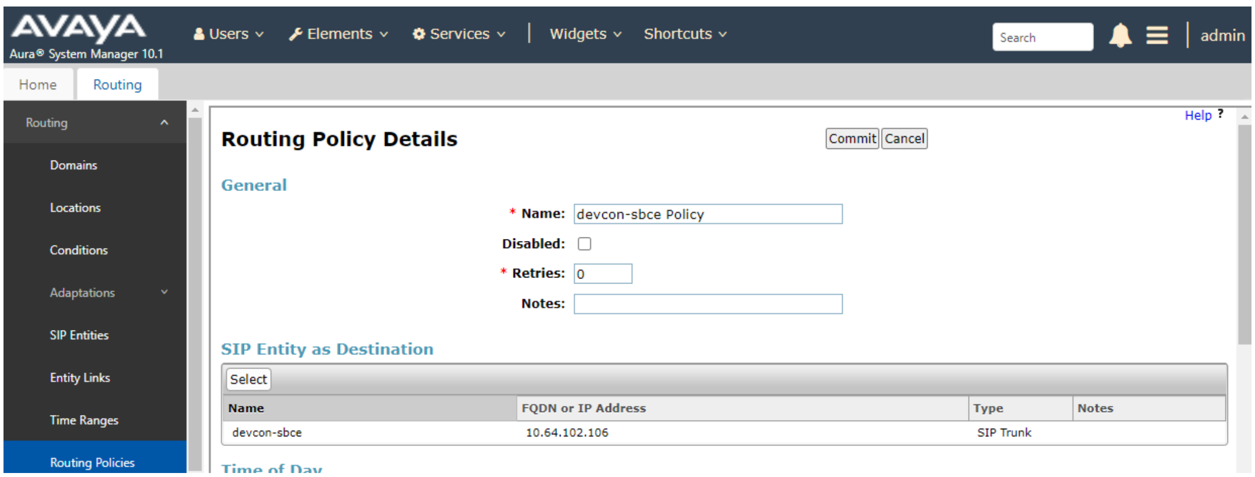
6.3. Add Routing Policies

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

Under *General*:
Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:
Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

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



6.4. Add Dial Patterns

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

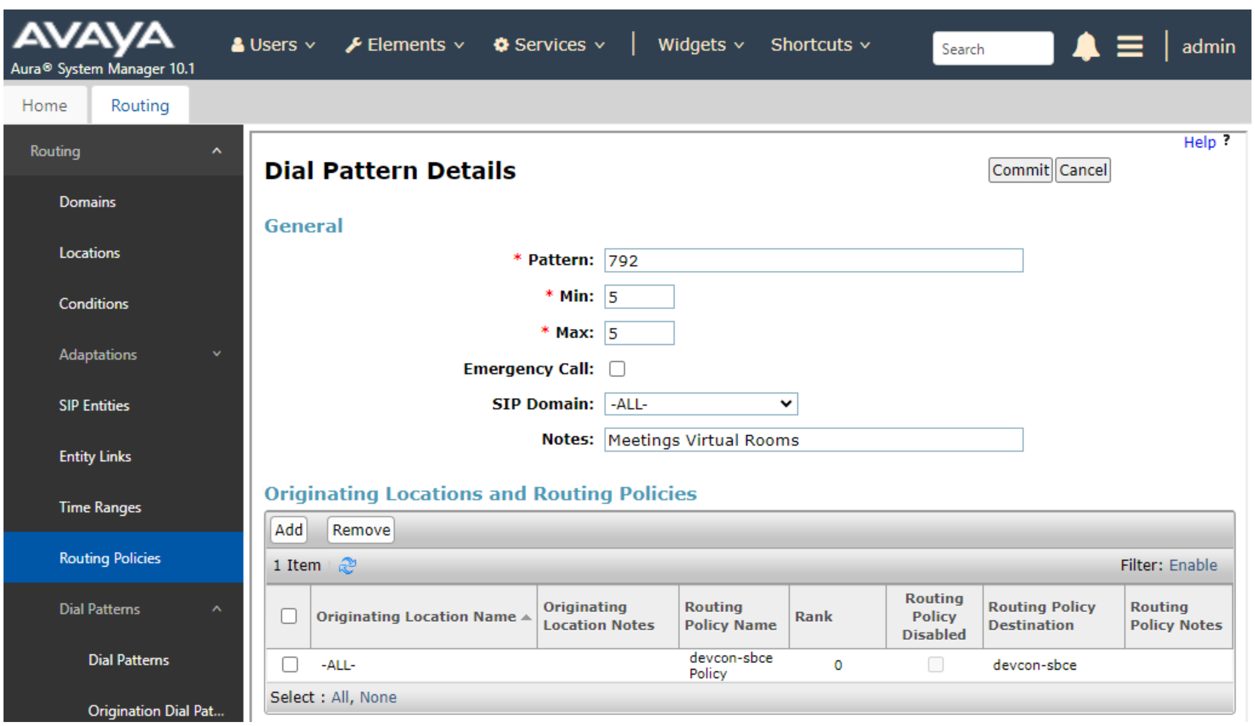
To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

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

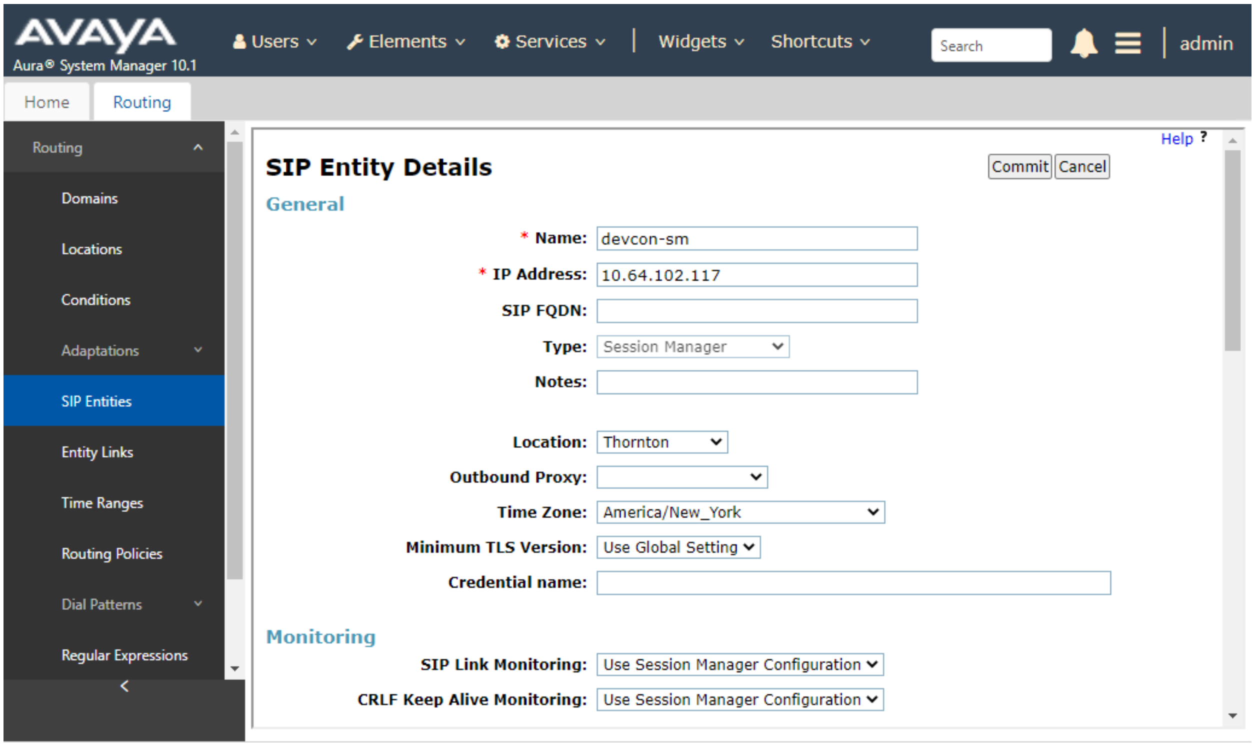
Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the appropriate location and routing policy from the list.

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

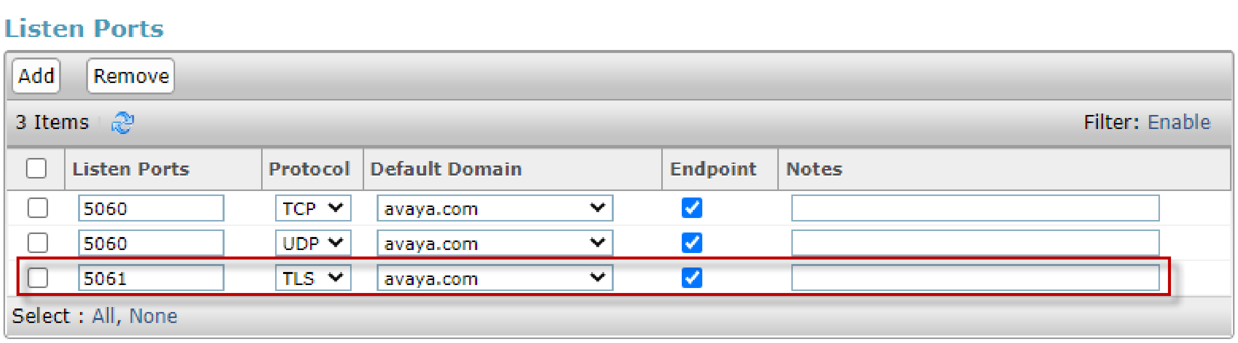


6.5. Set Network Transport Protocol for Studio X30/X70 and G7500

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

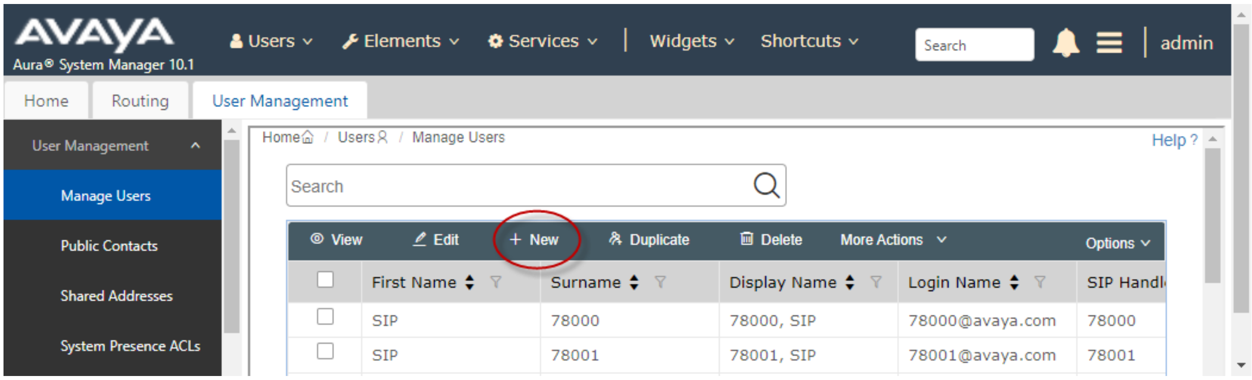


Scroll down to the **Listen Ports** section and verify that the transport network protocol used by Poly video endpoints is specified in the list below. For the compliance test, TLS network transport was used.



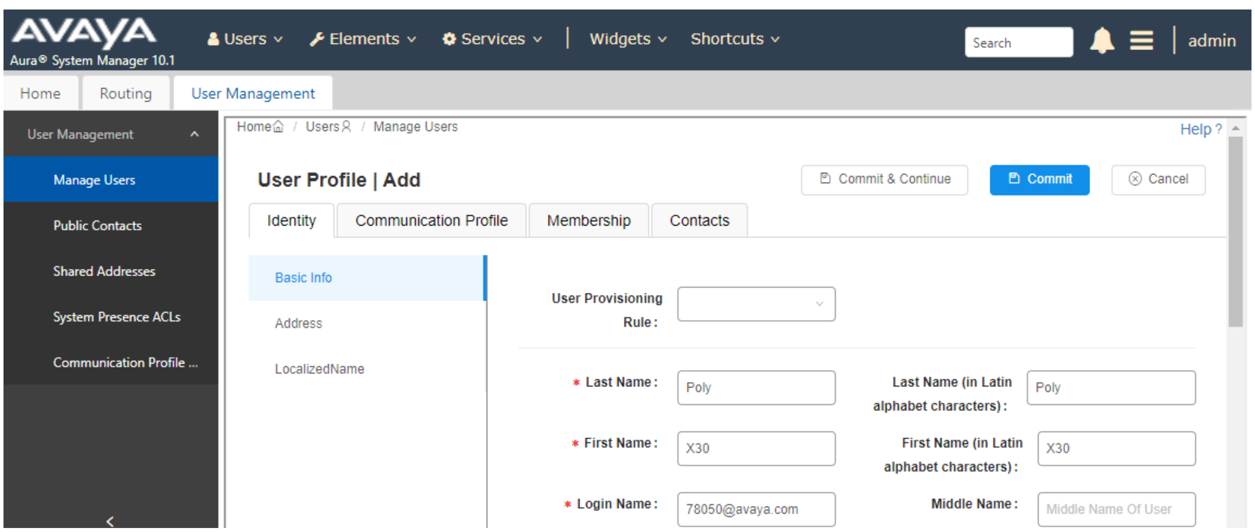
6.6. Administer SIP User

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



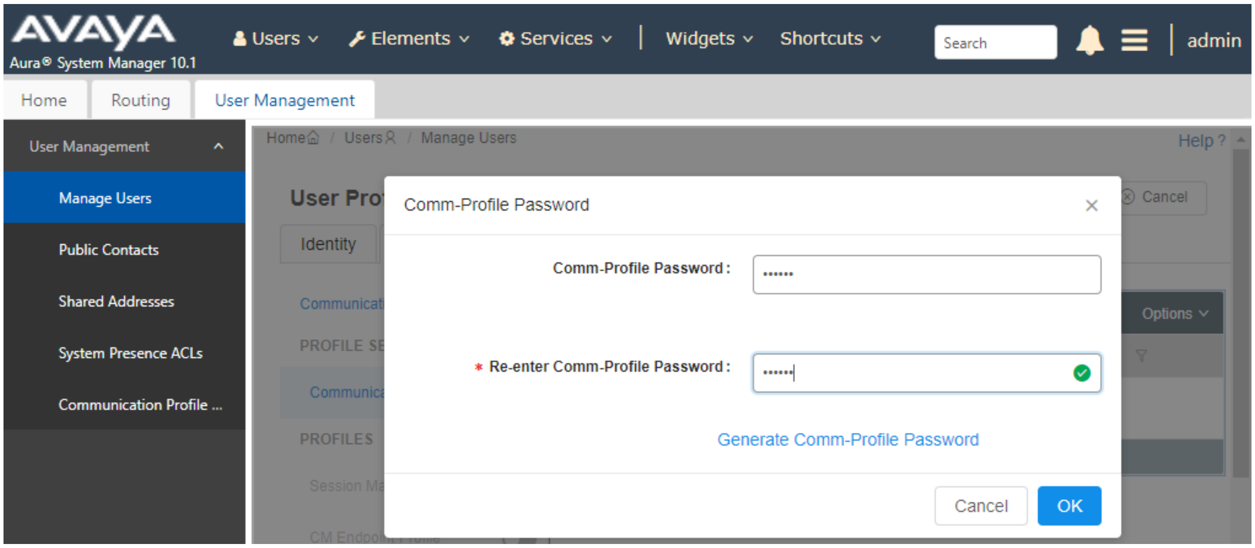
6.6.1. Identity

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



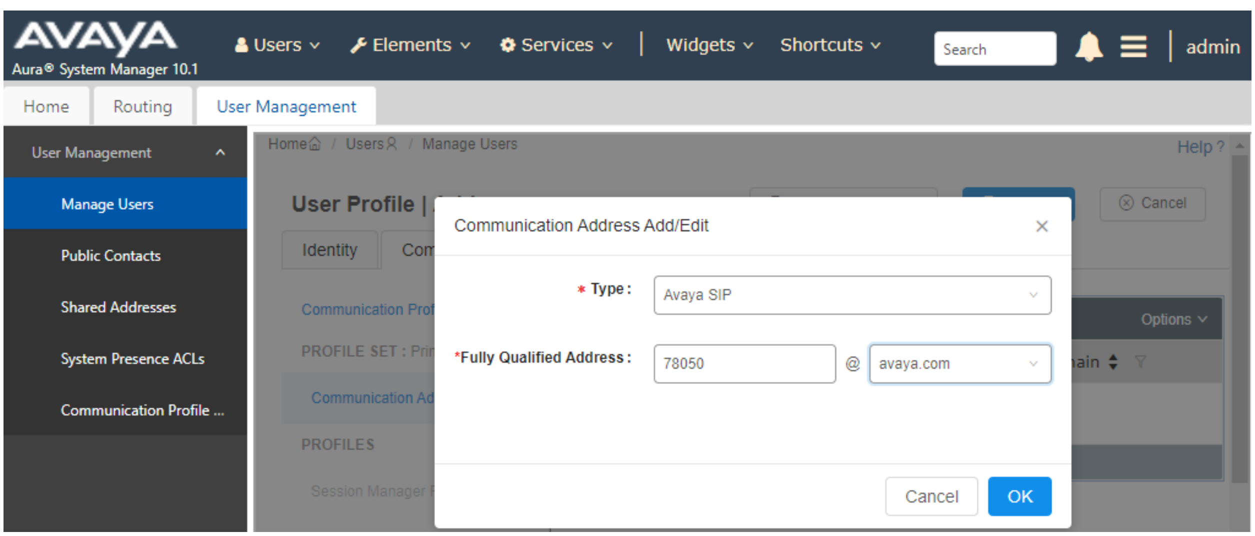
6.6.2. Communication Profile

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



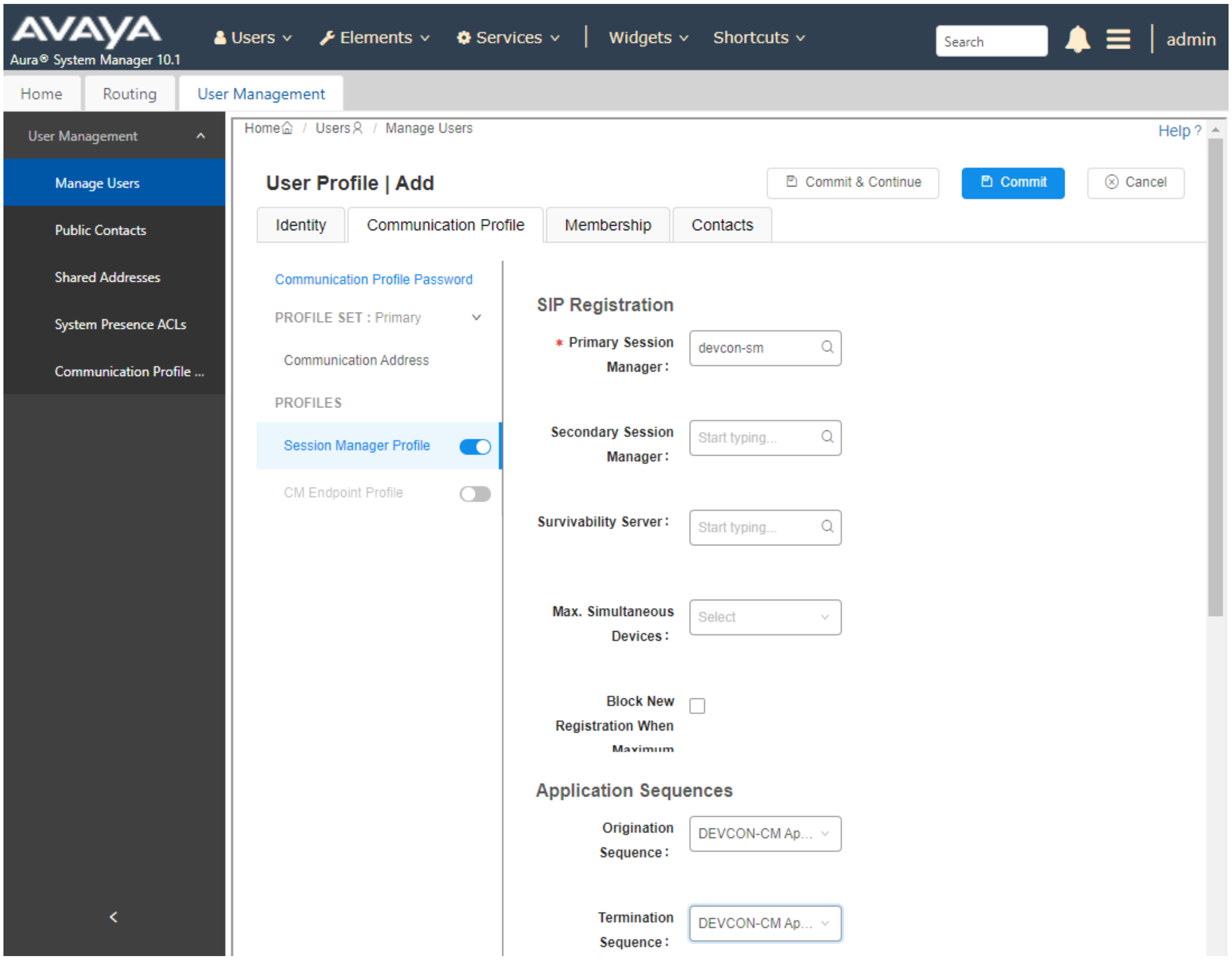
6.6.3. Communication Address

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

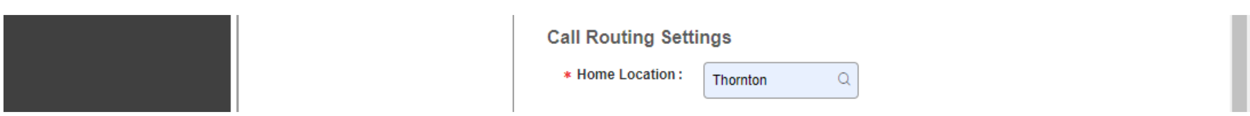


6.6.4. Session Manager Profile

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

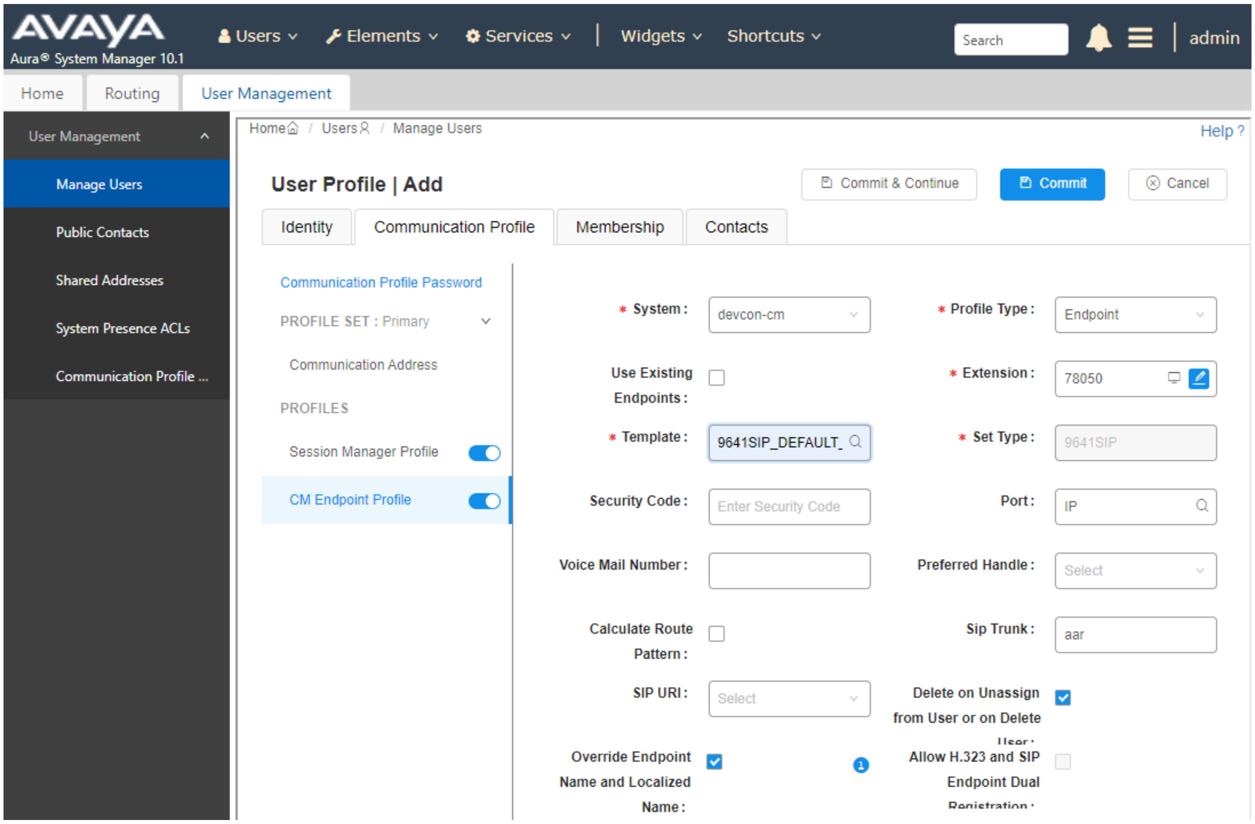


Scroll down to the **Call Routing Settings** section to configure the **Home Location**.



6.6.5. CM Endpoint Profile

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



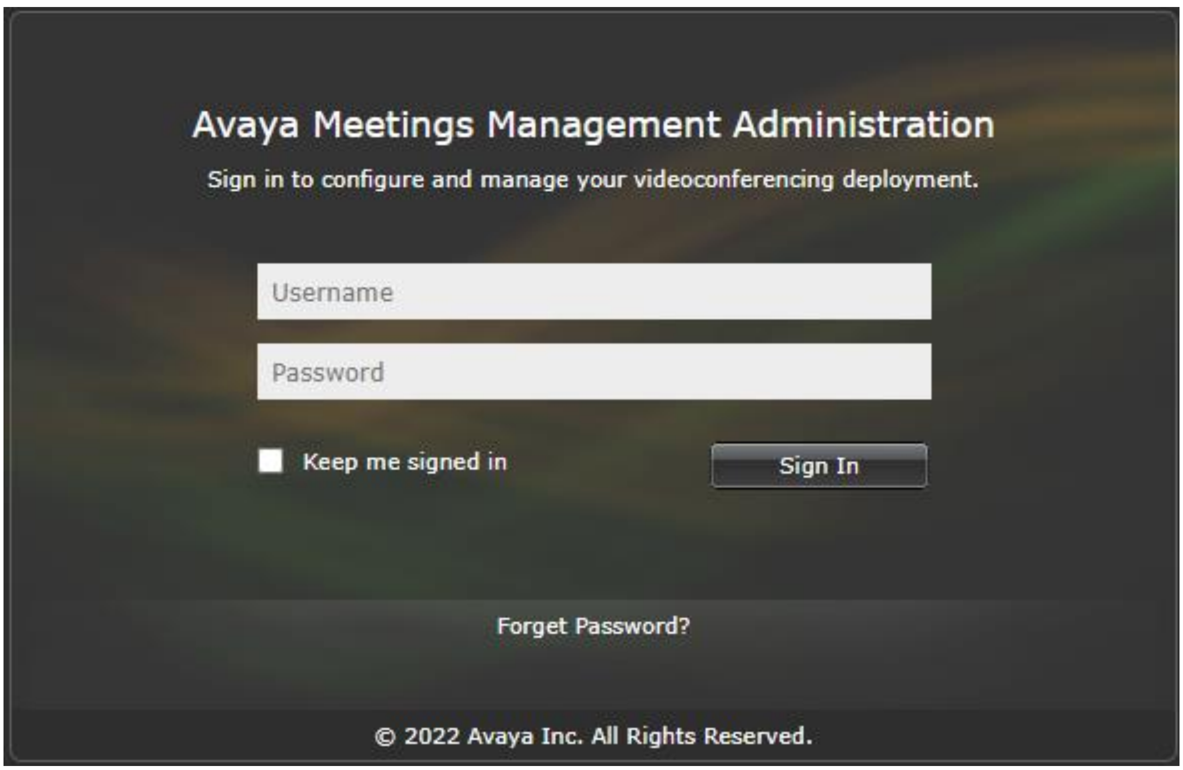
7. Configure Avaya Meetings Server

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

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

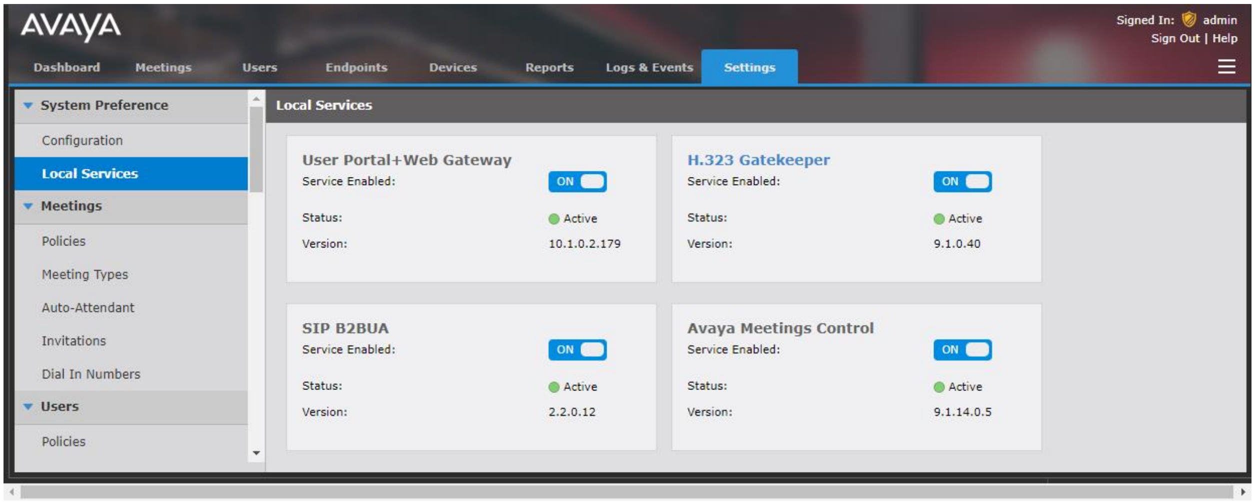
7.1. Access Meetings Management Administrator Portal

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

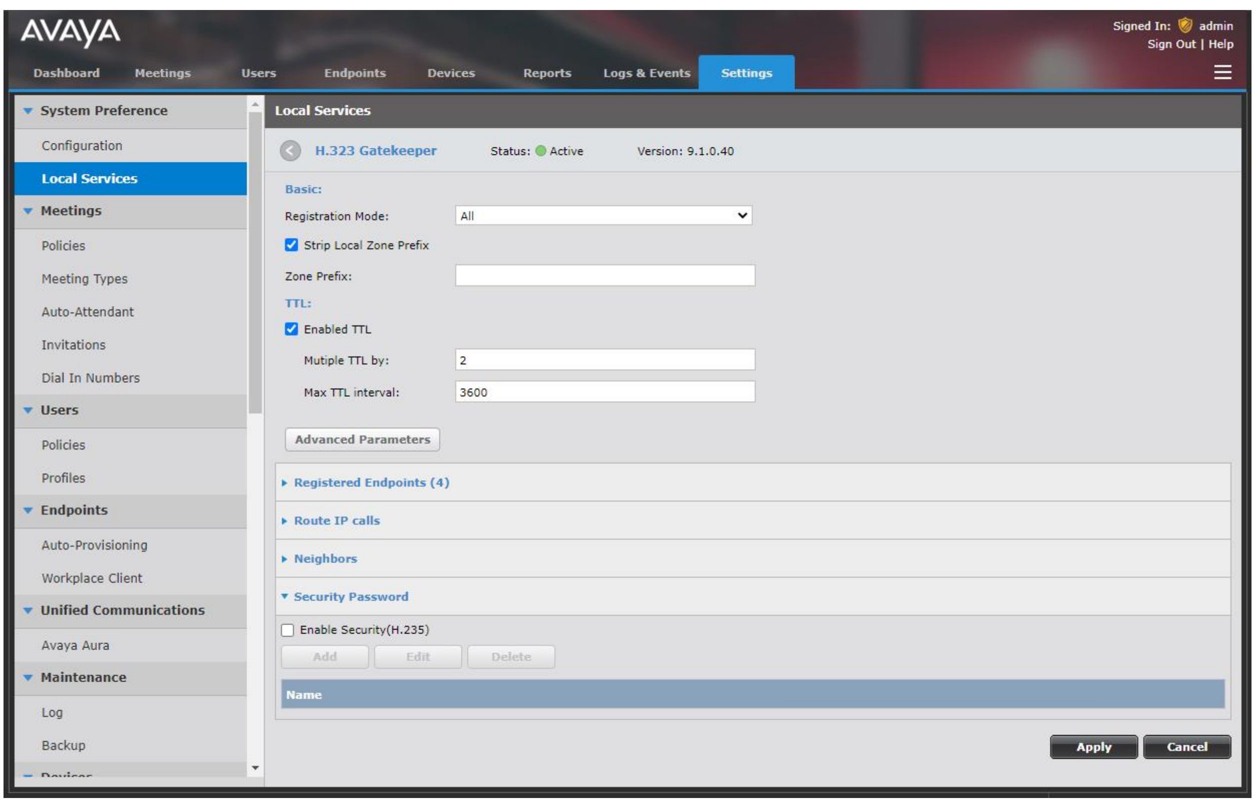


7.2. Configure H.323 Gatekeeper

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

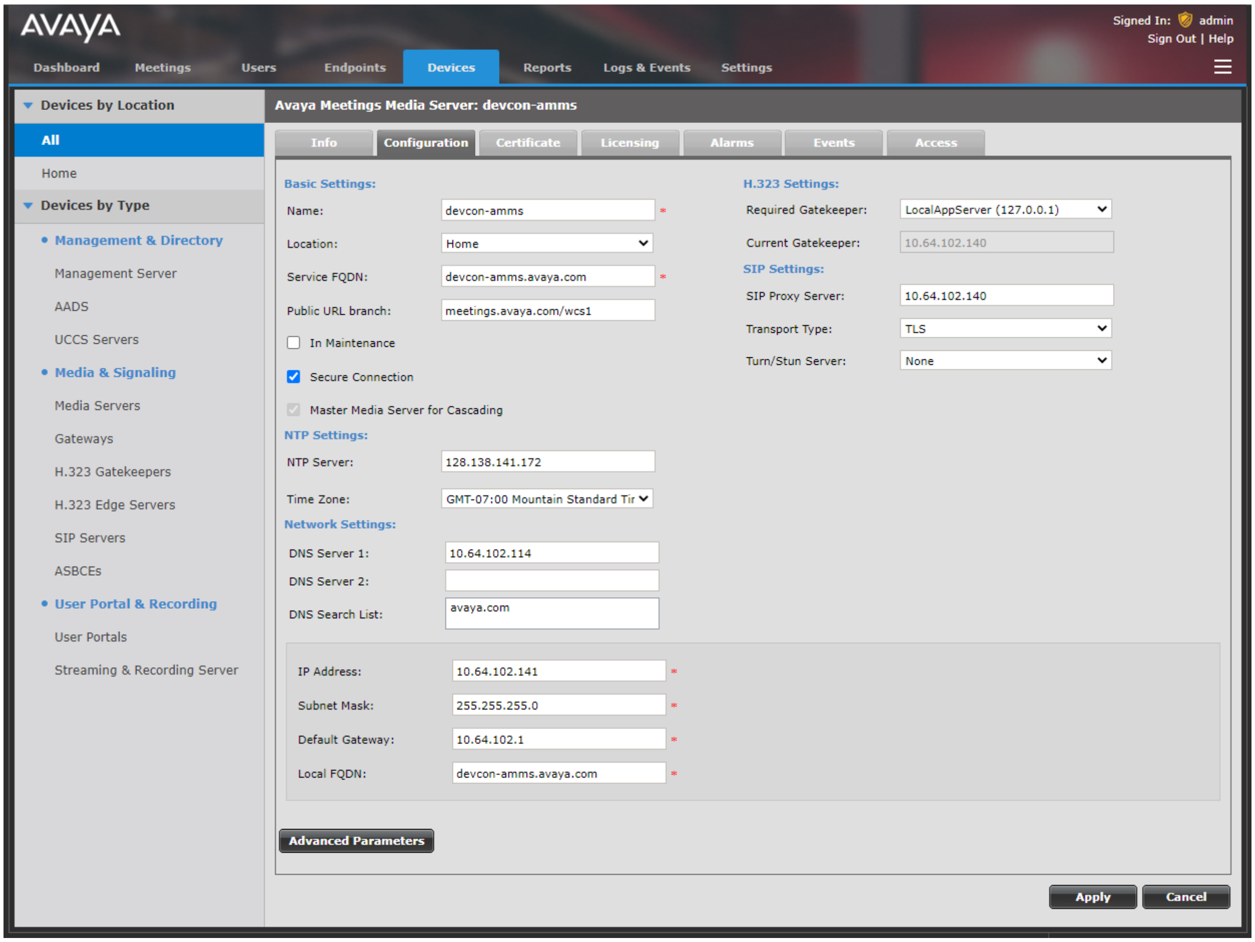


In this configuration, no **Zone Prefix** was used. To require authentication (optional), enable **Security (H.235)** and configure a **Name** and **Password** in the **Security Password** section. This should match the H.323 settings for Poly video endpoints in **Section 9.3**. In this configuration,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

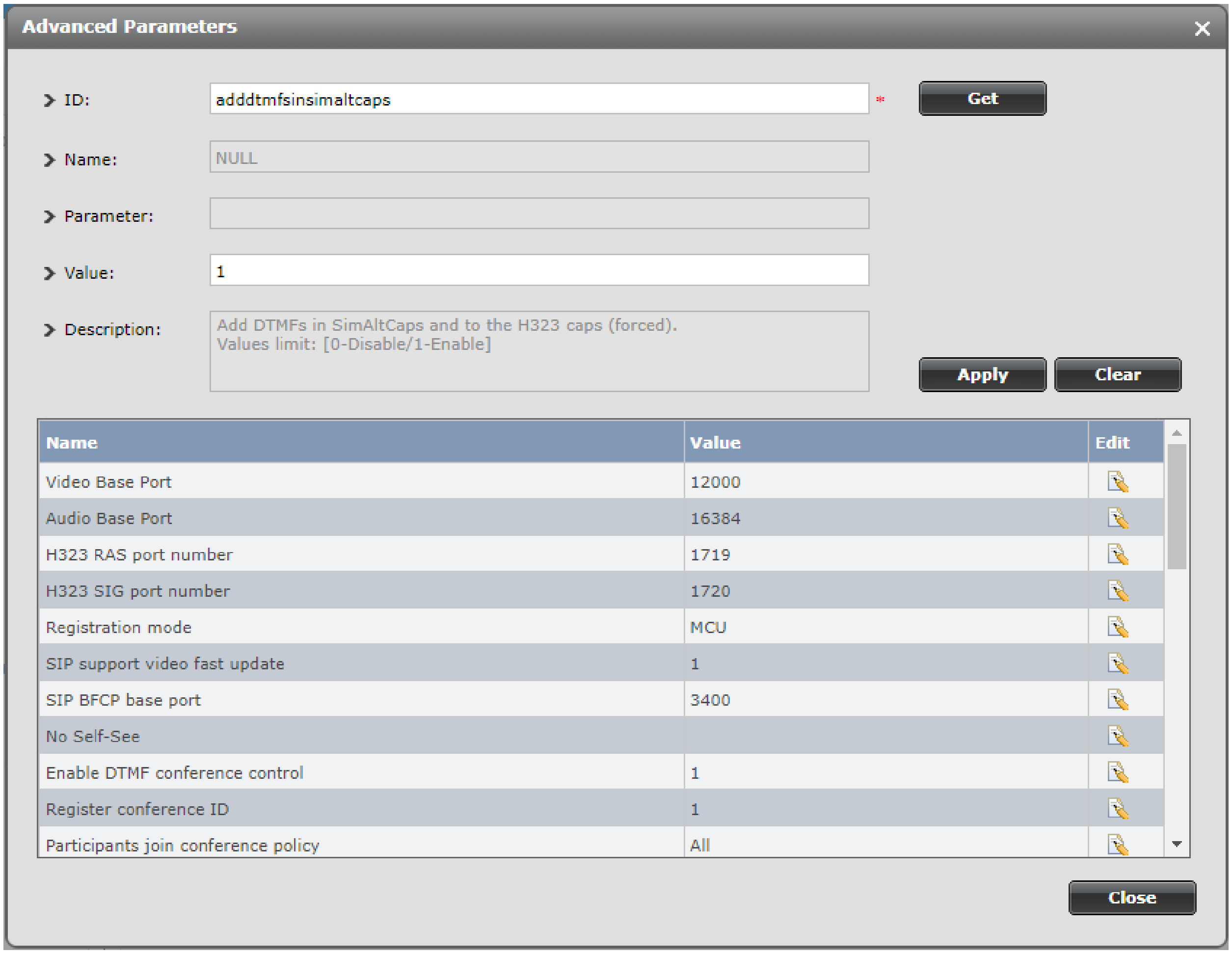


7.3. Configure Advanced Parameters

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

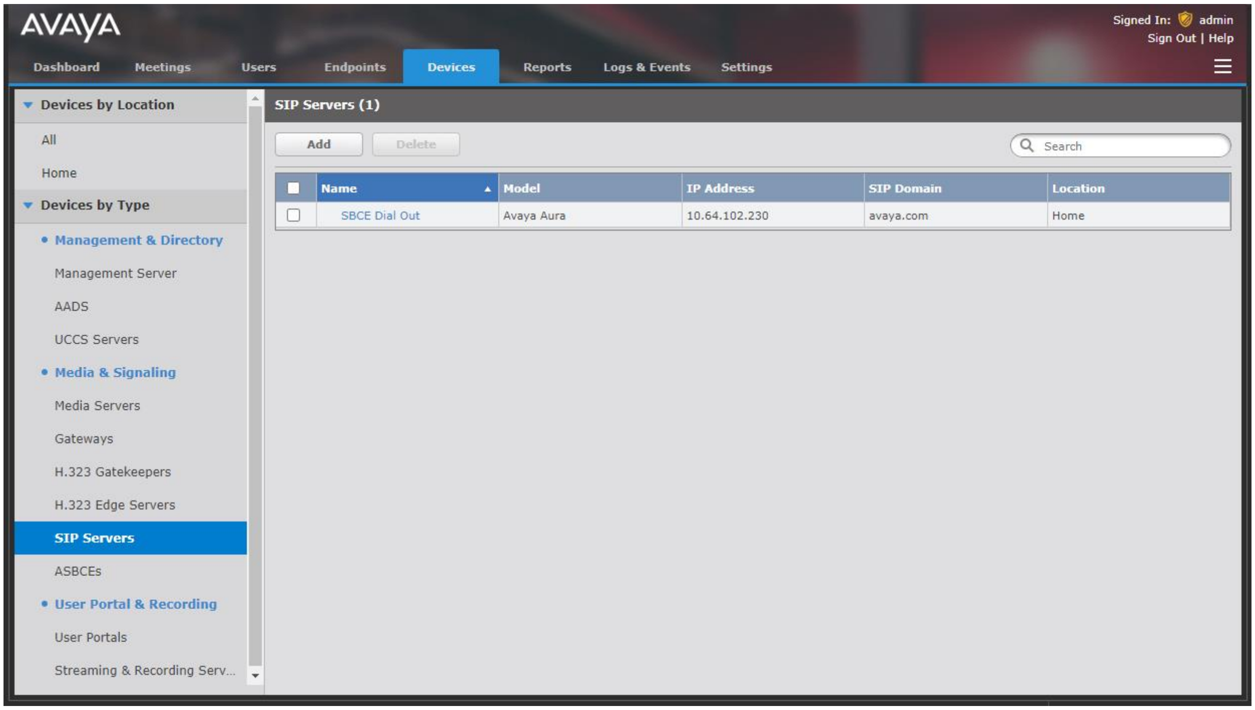


In **Advanced Parameters**, set the **addDTMFsInSimAltCaps** parameter to *1* as shown below.



7.4. Configure SIP Trunk to SBC

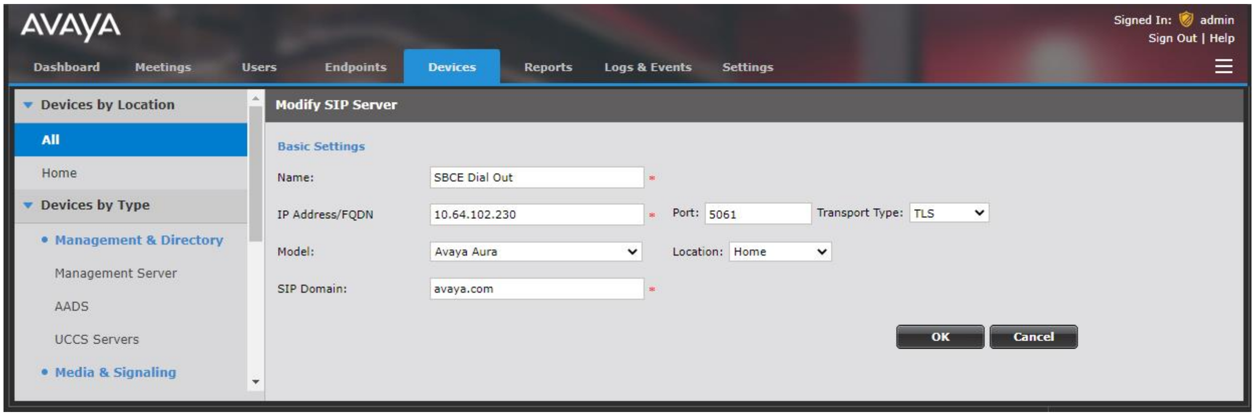
To add a SIP trunk for inbound and outbound calls to/from Meetings Server, navigate to **Devices → Media & Signaling → SIP Servers** in the left pane and click **Add**.



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

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

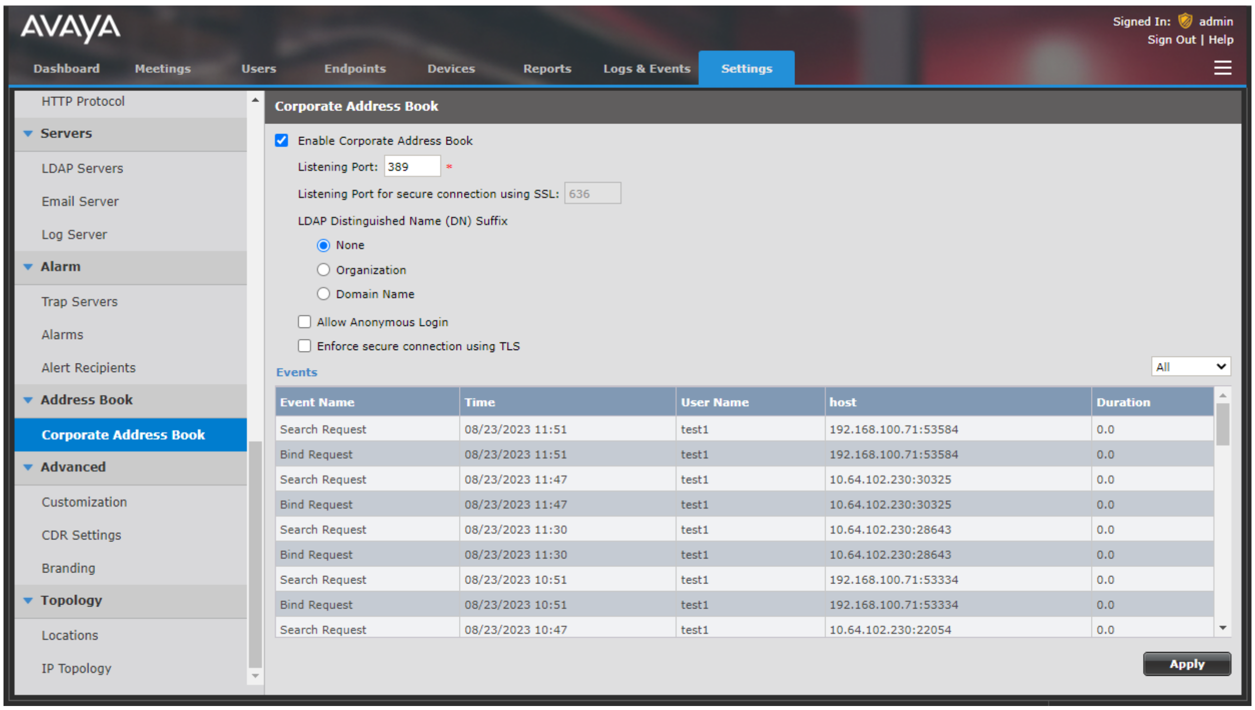
The SIP trunk uses TLS. In this configuration, a TLS certificate signed by the System Manager certificate authority was used. The signing and import of the TLS certificate are not shown in these Application Notes.



7.5. Configure Corporate Address Book

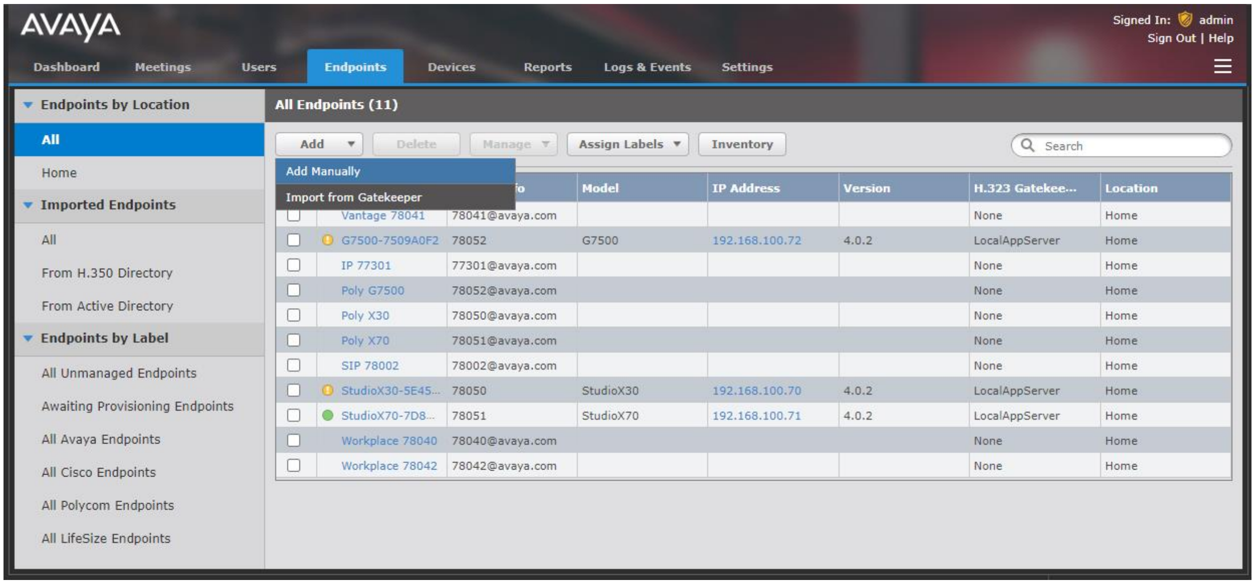
The built-in LDAP server in Meetings Management may be used to allow endpoints to search the corporate address book, which includes the entries in the endpoint list configured in **Section 7.6**. Navigate to **Settings → Address Book → Corporate Address Book** and configure the following fields:

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



7.6. Configure Endpoints

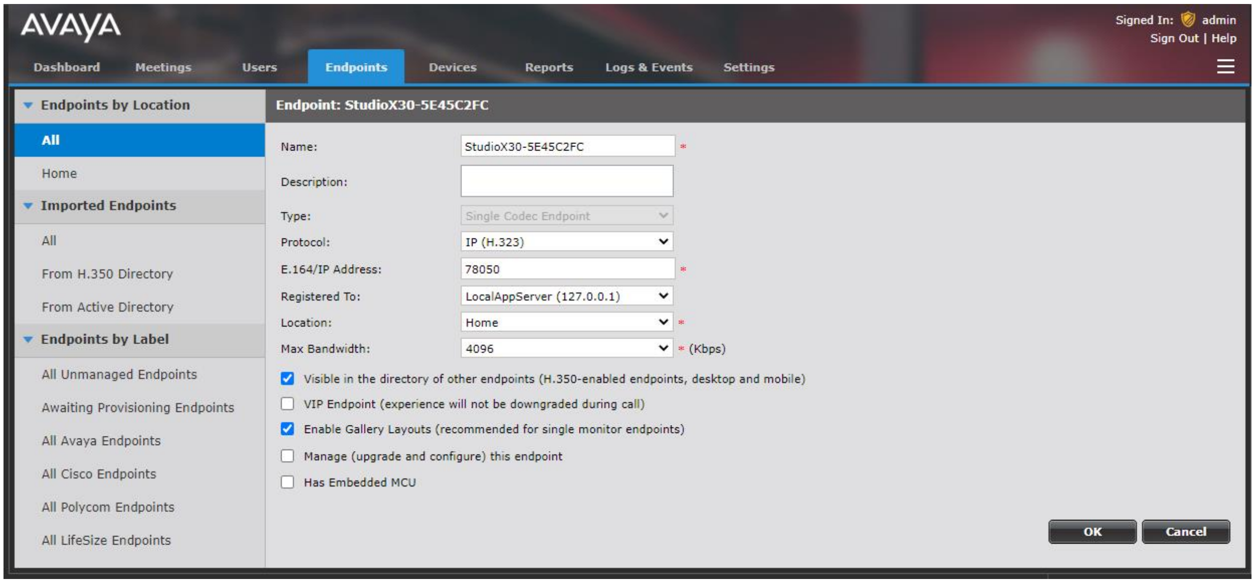
This section covers the configuration of H.323 and SIP endpoints. To add an endpoint, select the **Endpoints** tab, then click **Add** button and select the **Add Manually** option as shown below. Alternatively, H.323 endpoints may be imported from the internal H.323 gatekeeper.



7.6.1. Configure H.323 Endpoint

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

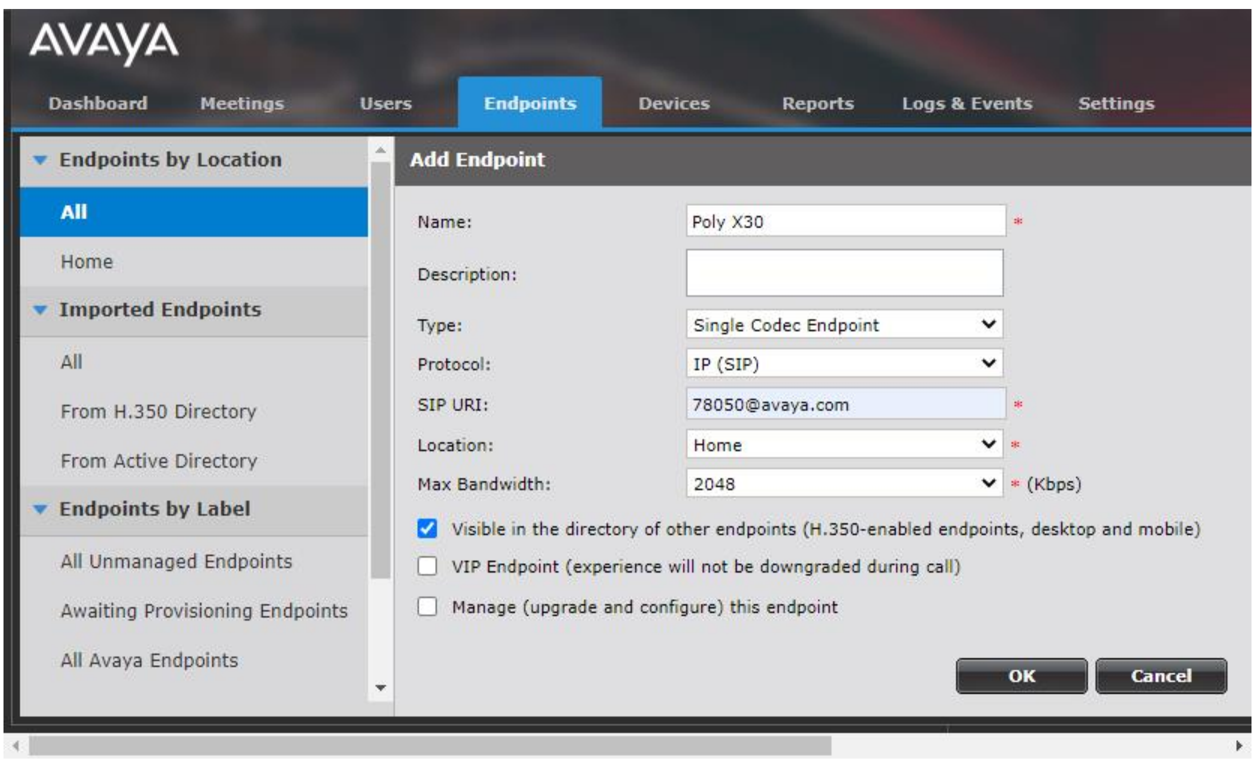
- **Name:** Type the name to identify the endpoint (e.g., *StudioX30-5E45C2FC*).
- **Description:** Provide a description for the endpoint (optional).
- **Type:** Select *Single Codec Endpoint* as the model of endpoint.
- **Protocol:** Select *IP (H.323)* from the list.
- **E.164/IP Address:** Specify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



7.6.2. Configure SIP Endpoint

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

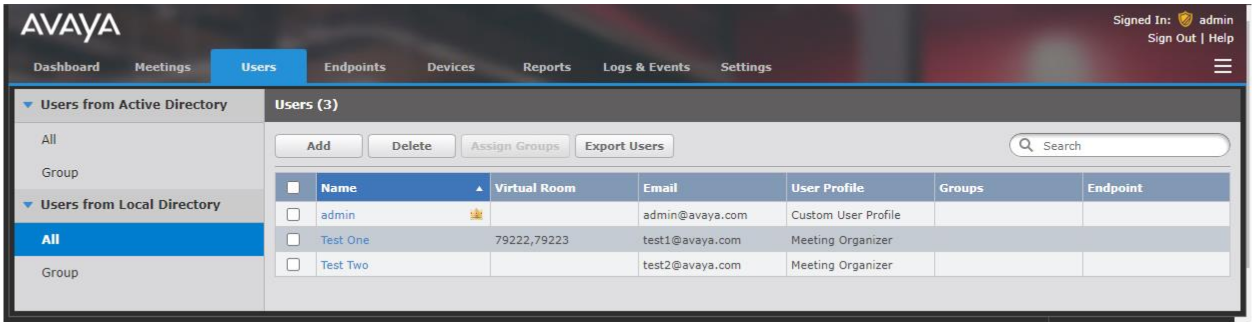
- **Name:** Type the name to identify the endpoint (e.g., *Poly X30*).
- **Description:** Provide a description for the endpoint (optional).
- **Type:** Select *Single Codec Endpoint* as the model of endpoint.
- **Protocol:** Select *IP (SIP)* from the list.
- **SIP URI:** Provide the endpoint identifier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



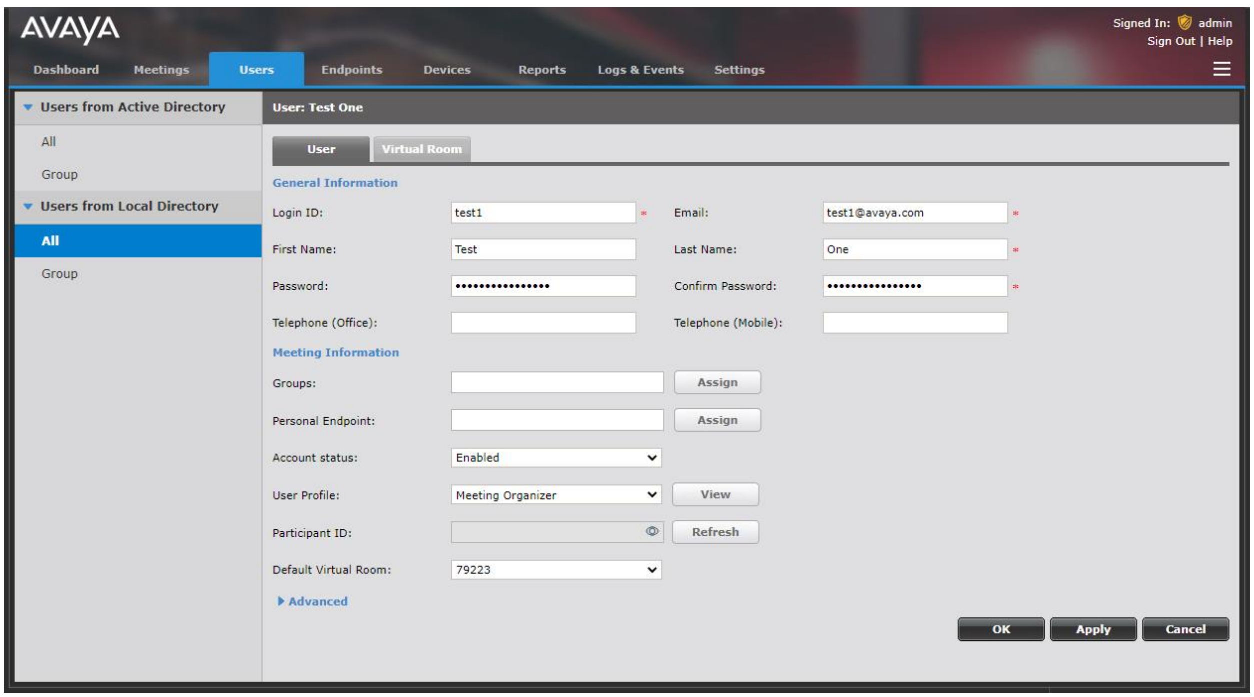
7.7. Configure Virtual Rooms

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

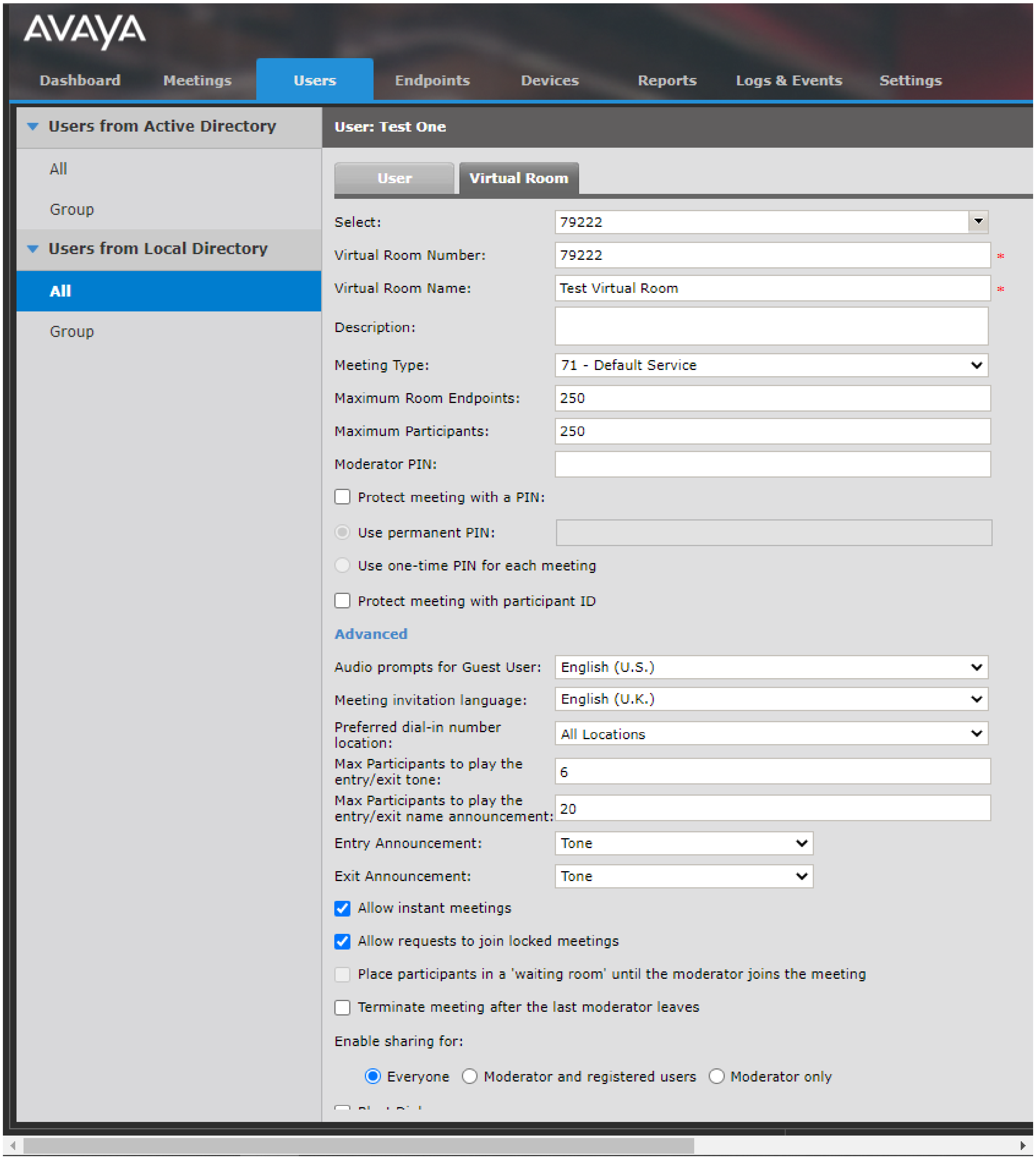
Virtual rooms are assigned to a user. To create or assign a virtual room to a user, select the **Users** tab, and then click on an existing user or click **Add** to create one.



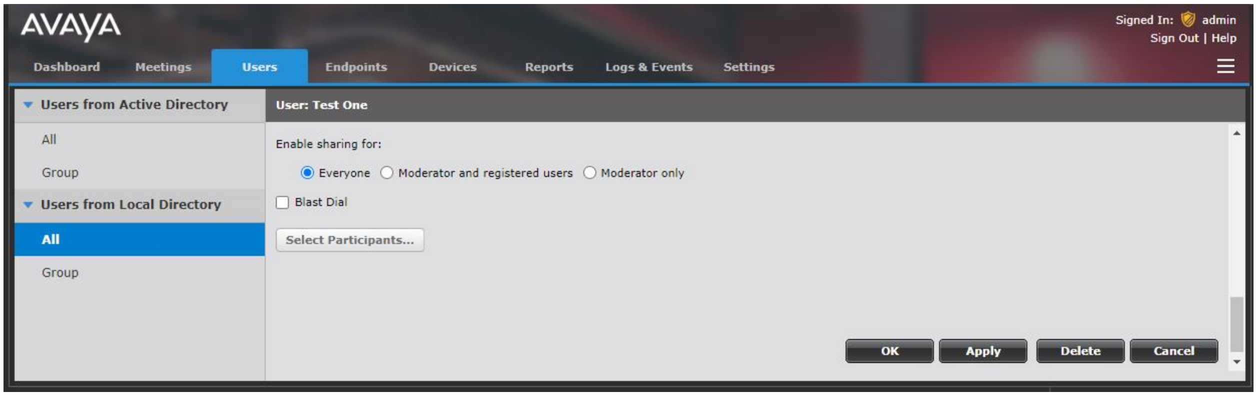
The configuration of an existing user is shown below. Next, select the **Virtual Room** tab.



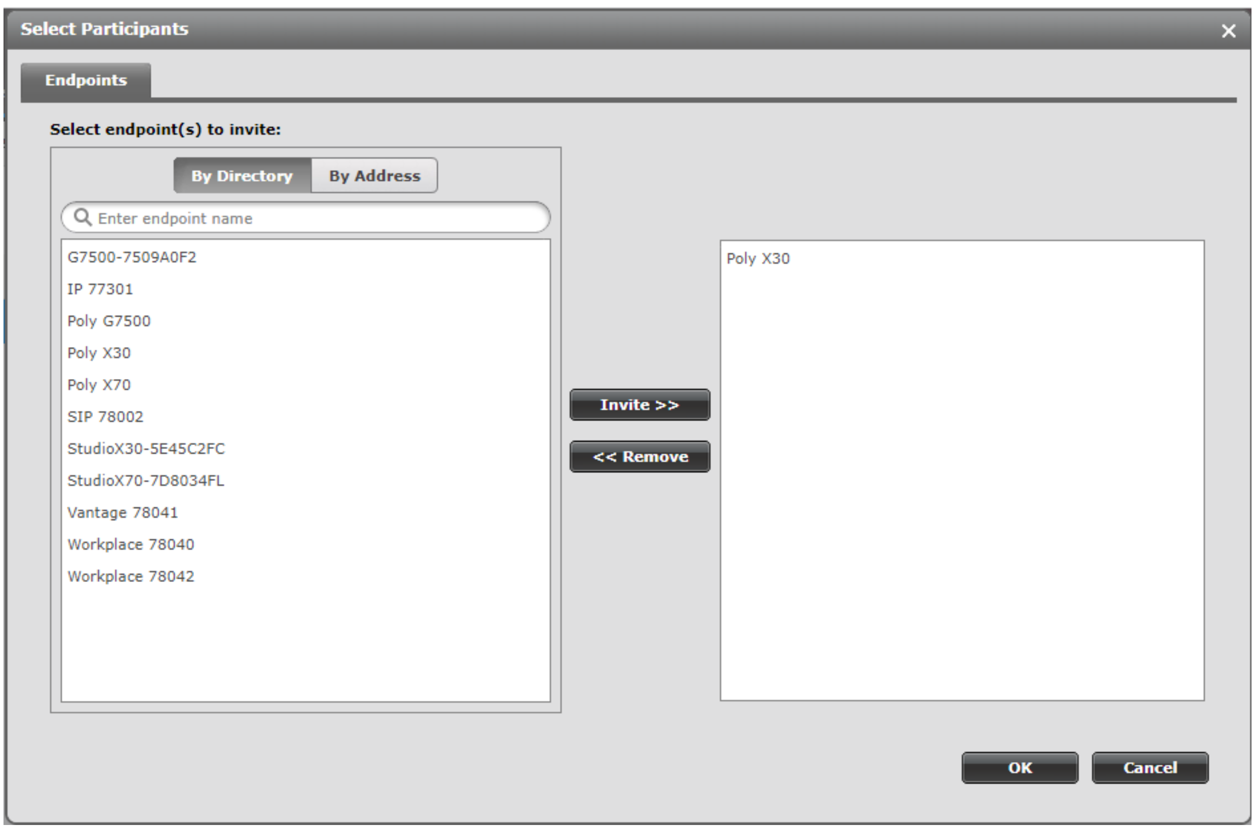
In the **Virtual Room** tab, set the **Select** field to the appropriate virtual room number to modify an existing one or Create *New Virtual Room* to create a new virtual room. Configure **Virtual Room Number**, **Virtual Room Name**, and **Meeting Type** as shown below. Enable **Protect meeting with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



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



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



8. Configure Avaya Session Border Controller

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

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

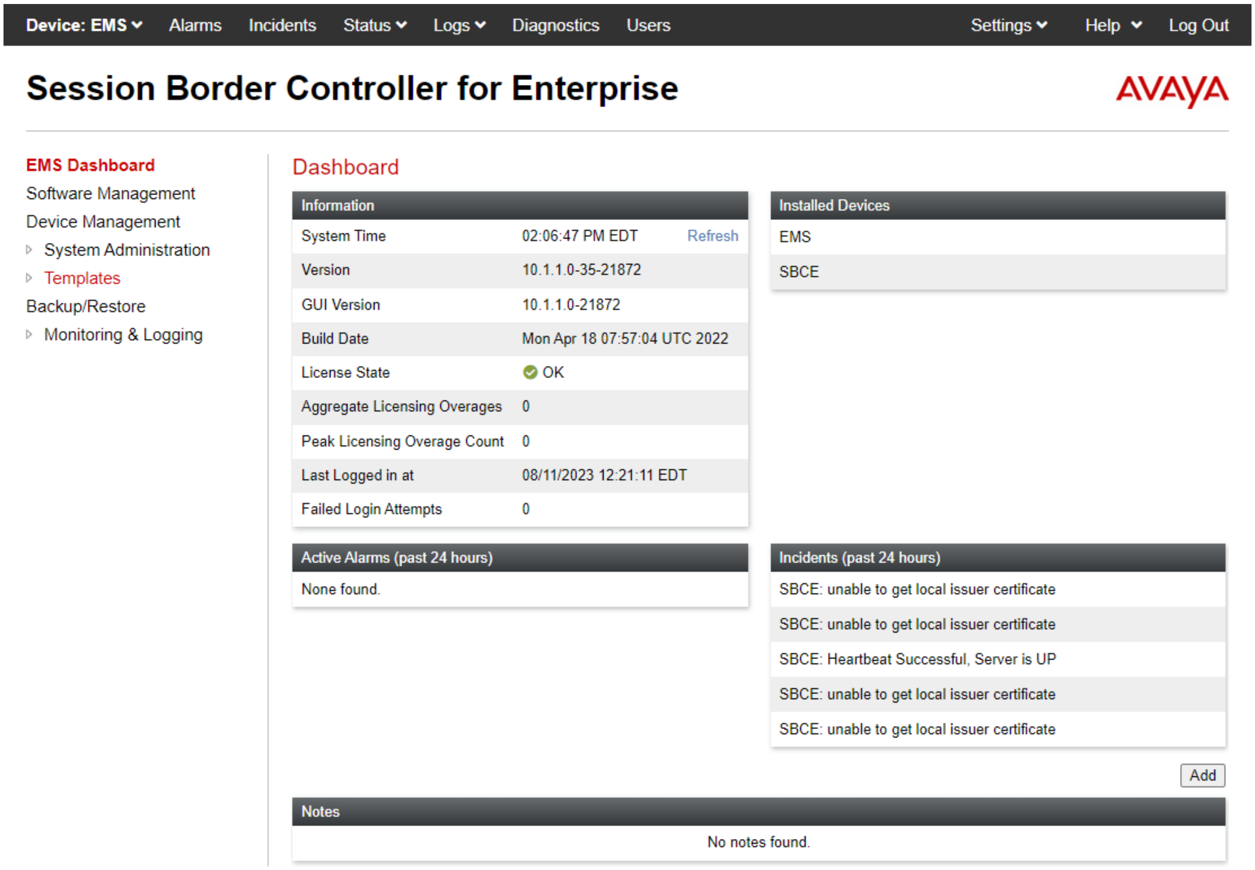
This section covers the following SBC configuration:

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

8.1. Launch SBC Web Interface

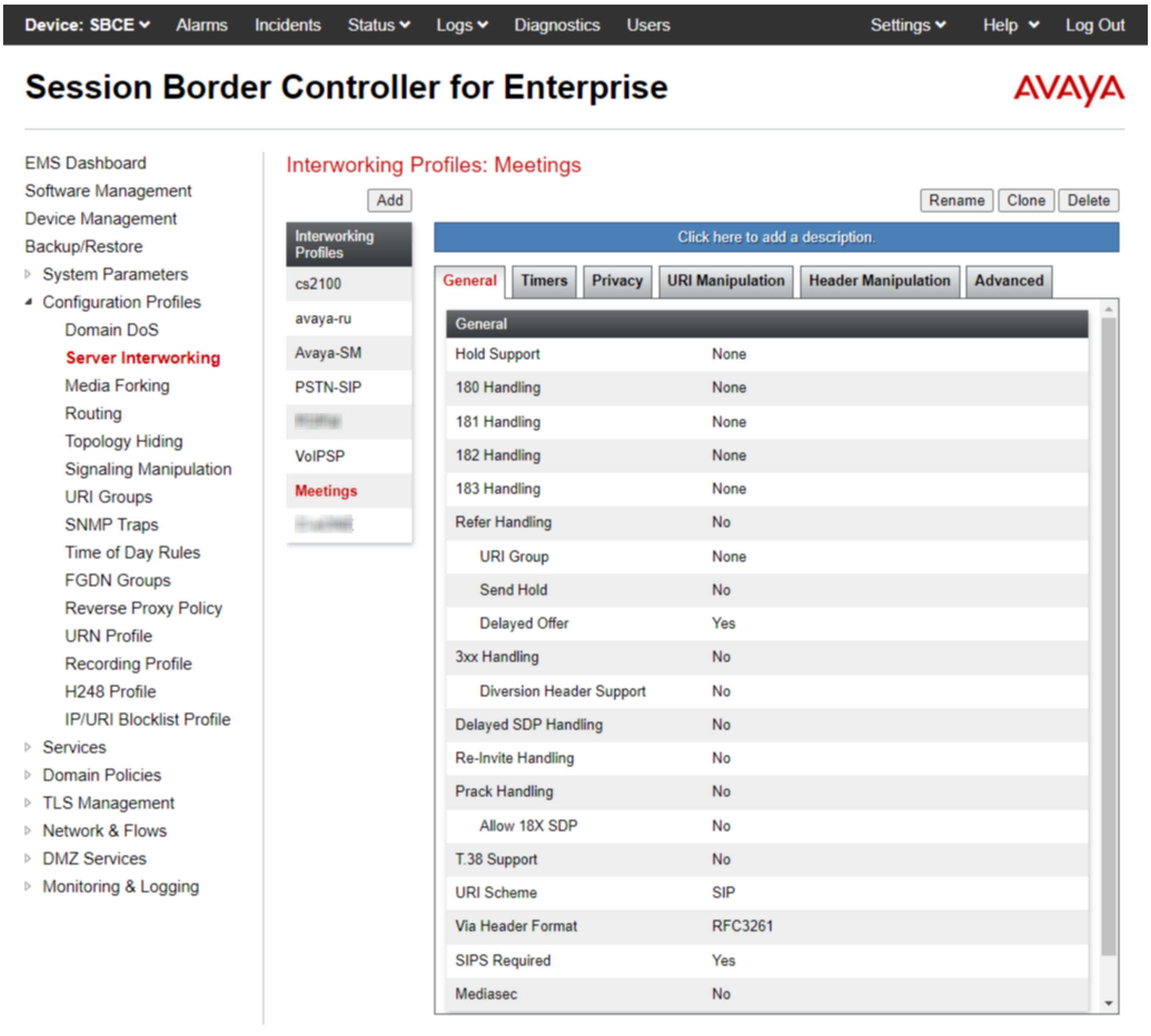
Access the SBC EMS web interface by using the URL **https://<*ip-address*>/sbc** in an Internet browser window, where **<*ip-address*>** is the IP address of the SBC management interface. The screen below is displayed. Log in using the appropriate credentials.

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

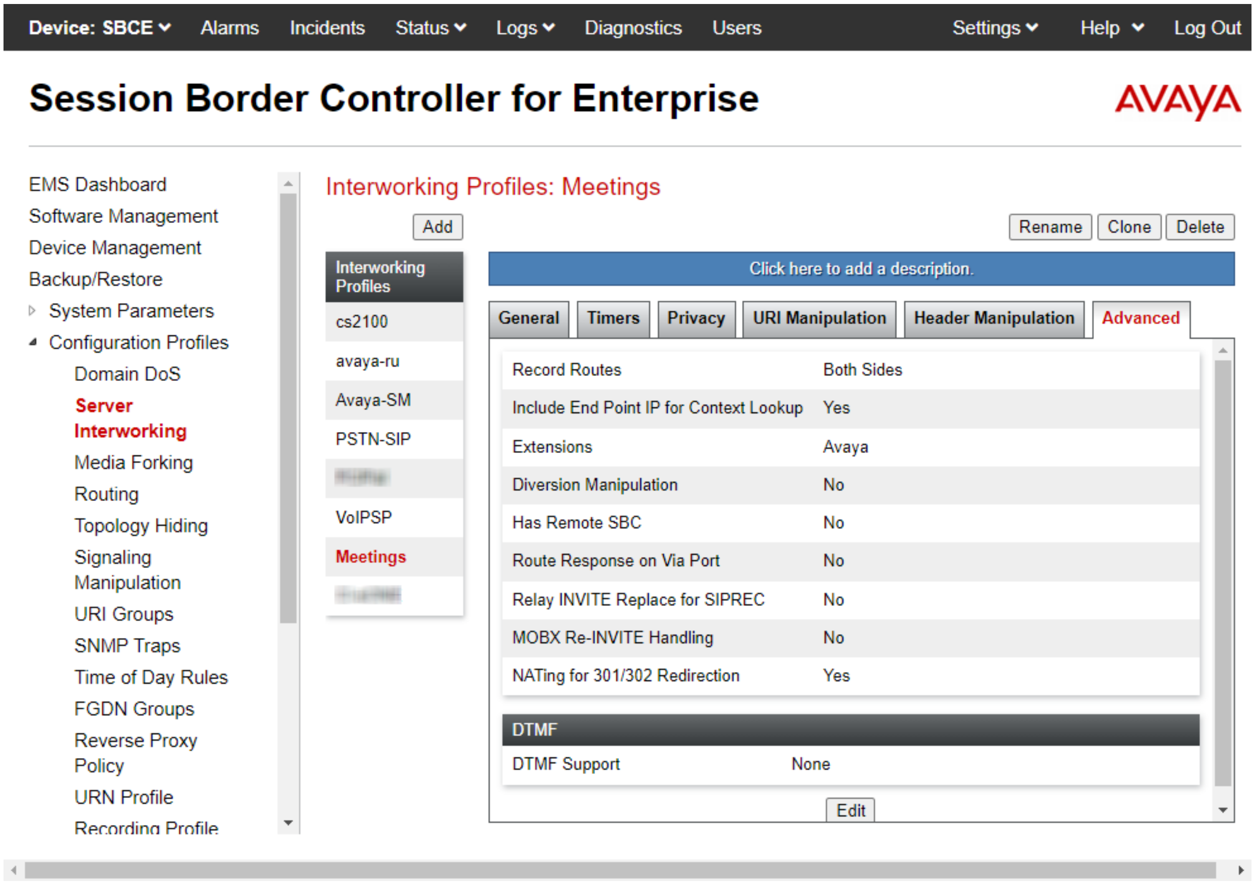


8.2. Administer Server Interworking Profile

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



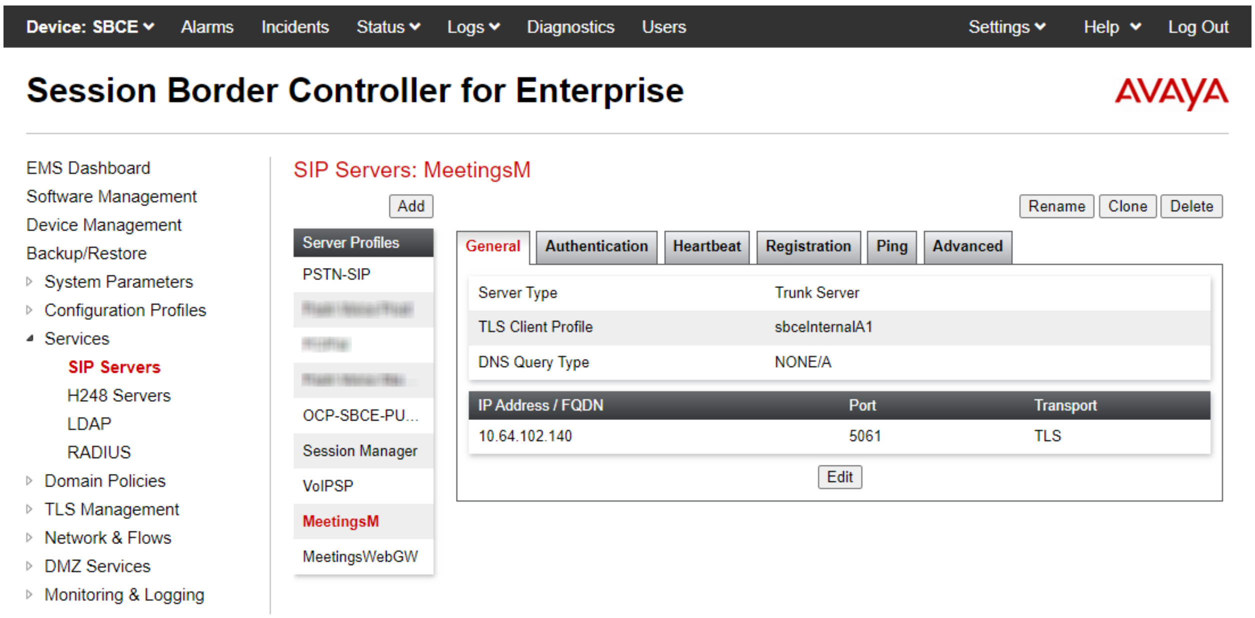
Select the **Advanced** tab and configure as shown below. Disable **Has Remote SBC**.



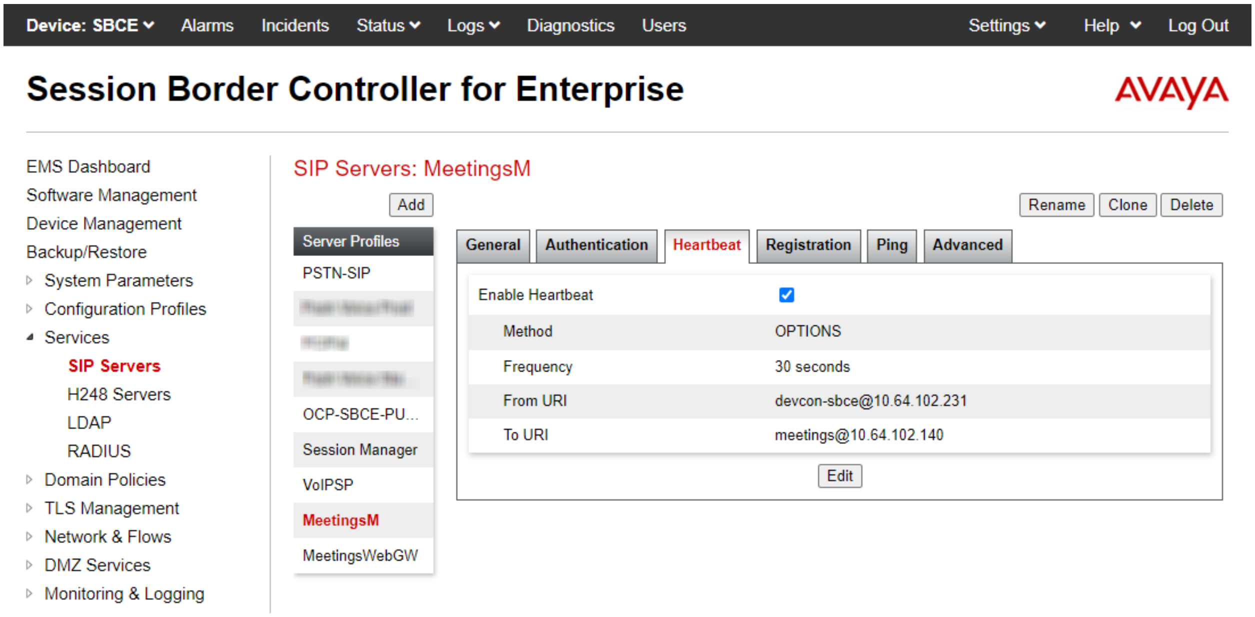
8.3. Administer SIP Server

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

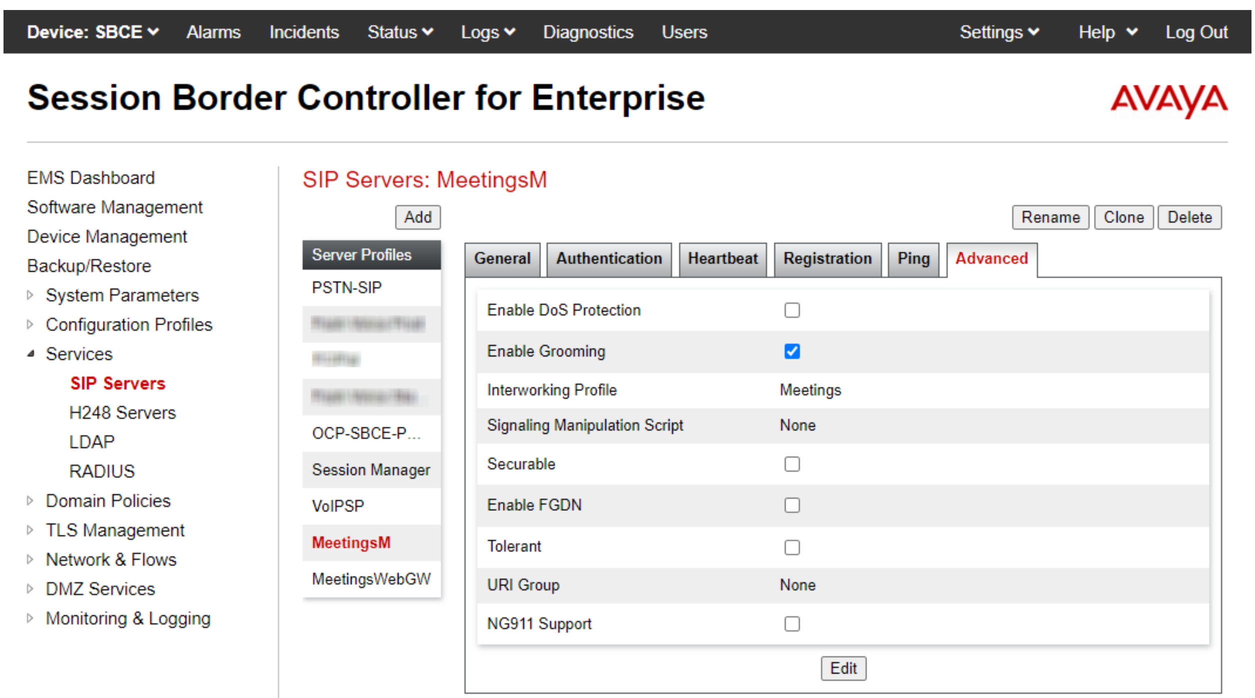
The **General** tab of the Meetings Management SIP server was configured as shown below. The IP address (e.g., *10.64.102.140*) and Port *5061* were used. TLS transport was used for the Meetings Management SIP trunk. It is assumed that the **TLS Client Profile** for the SBC internal A1 interface to which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



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

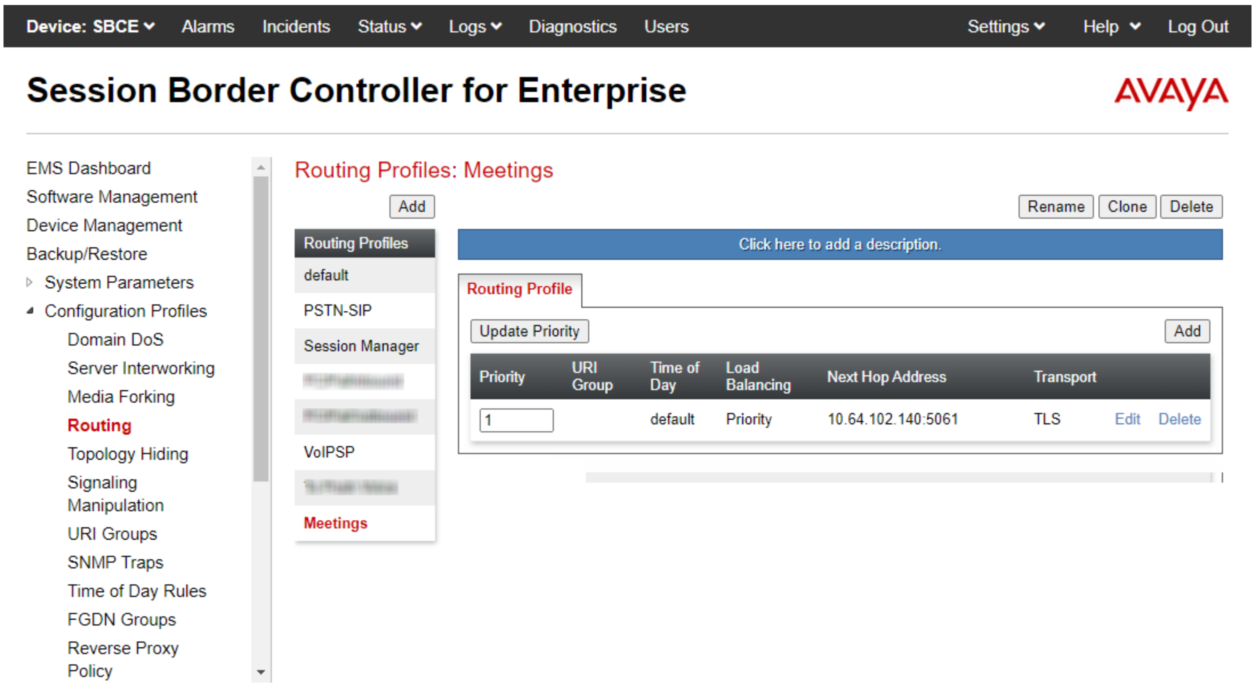


The **Advanced** tab was configured as shown below. **Grooming** was enabled and the **Interworking Profile** was set to the one configured in **Section 8.2**. All other tabs were left with their default values.



8.4. Administer Routing Profile

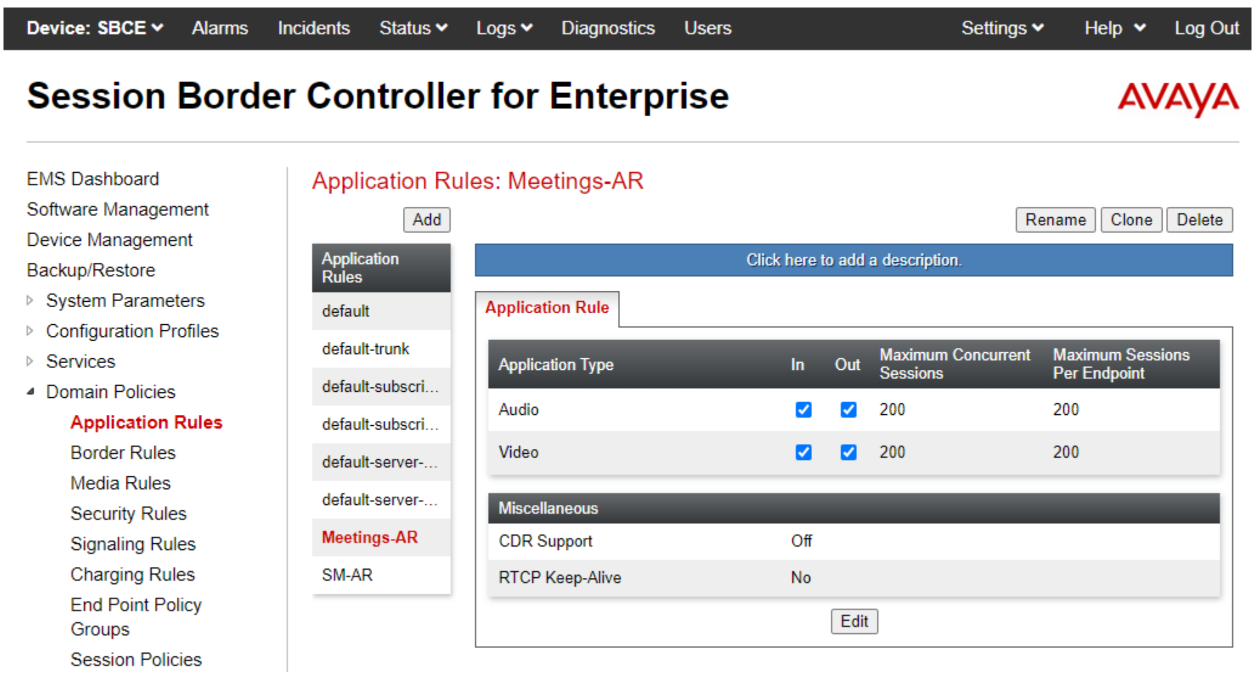
A **Routing Profile** is used to specify the next-hop for a SIP message. A routing profile is applied only after traffic has matched a **Server Flow** defined in **Section 8.10.2**. The IP addresses and ports defined here will be used as destination addresses for signaling. Create a routing profile for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



8.5. Administer Application Rule

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

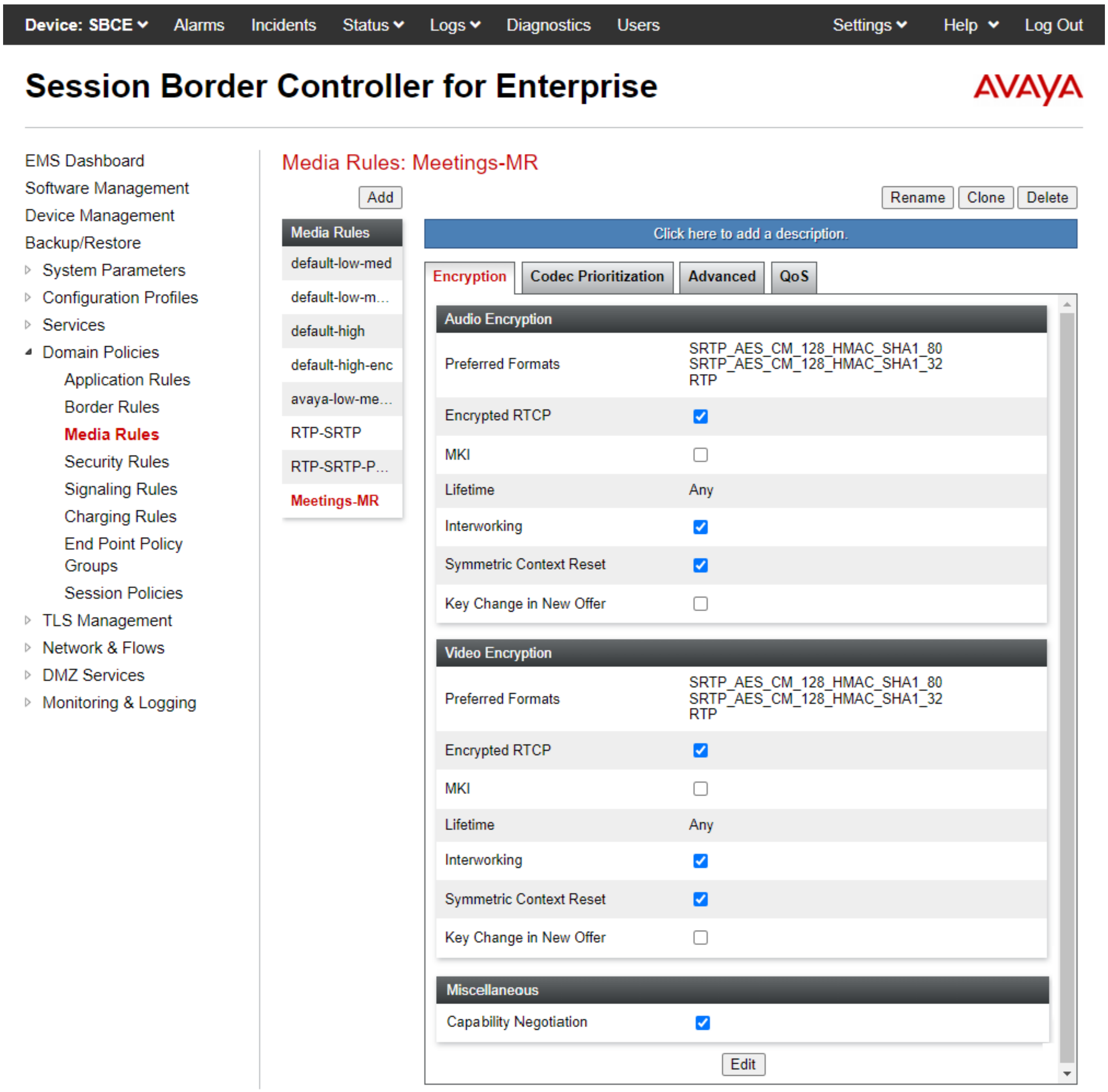
The application rule used to support audio and video calls to Meetings Server is shown below. In this example, 200 concurrent incoming and outgoing audio and video calls are supported.



8.6. Administer Media Rule

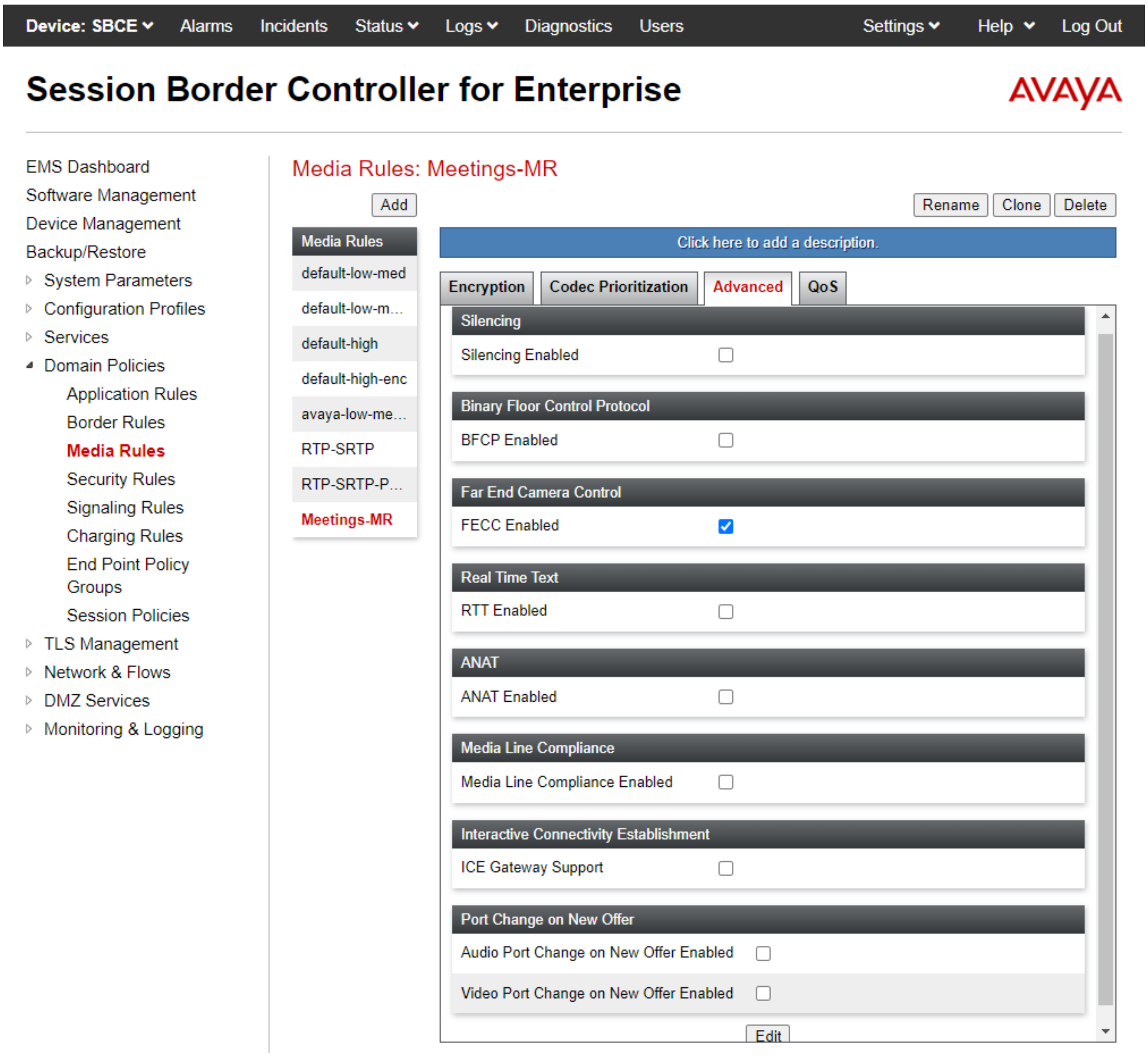
A **Media Rule** defines the processing to be applied to the selected media. A media rule is one component of the larger **End Point Policy Group** defined in **Section 8.7**, which is applied to **Server Flows** in **Section 8.10.2**.

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



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

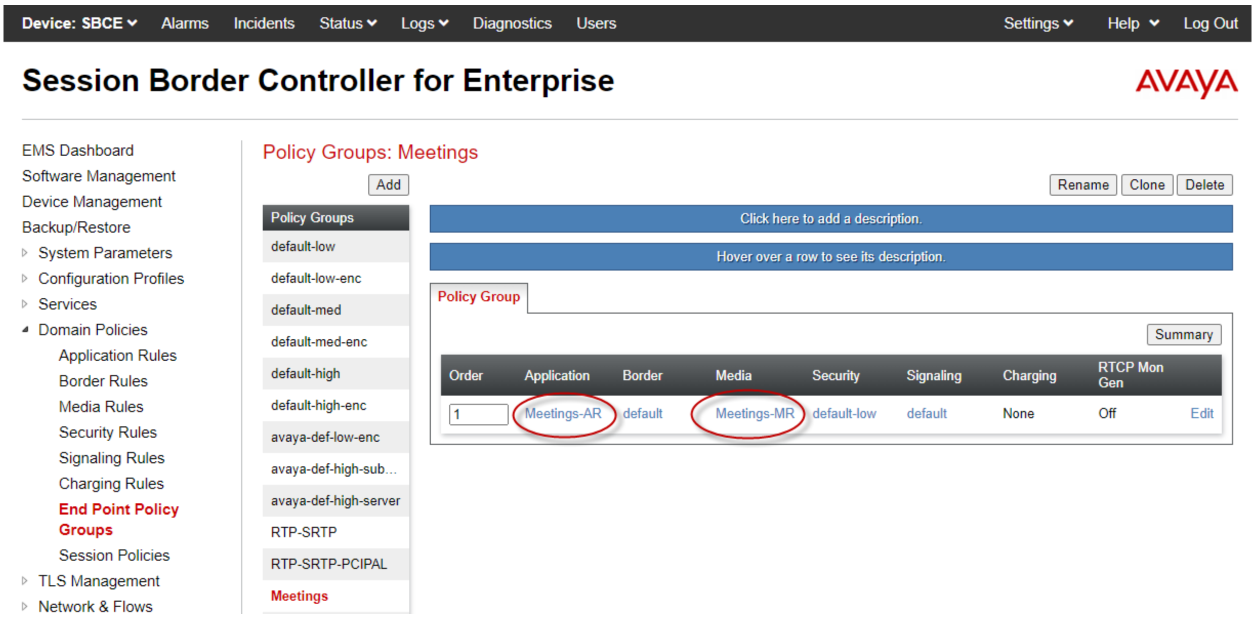
Select the **Advanced** tab and verify that **BFCP Enabled** is unchecked and **FECC Enabled** is checked.



8.7. Administer End Point Policy Group

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

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

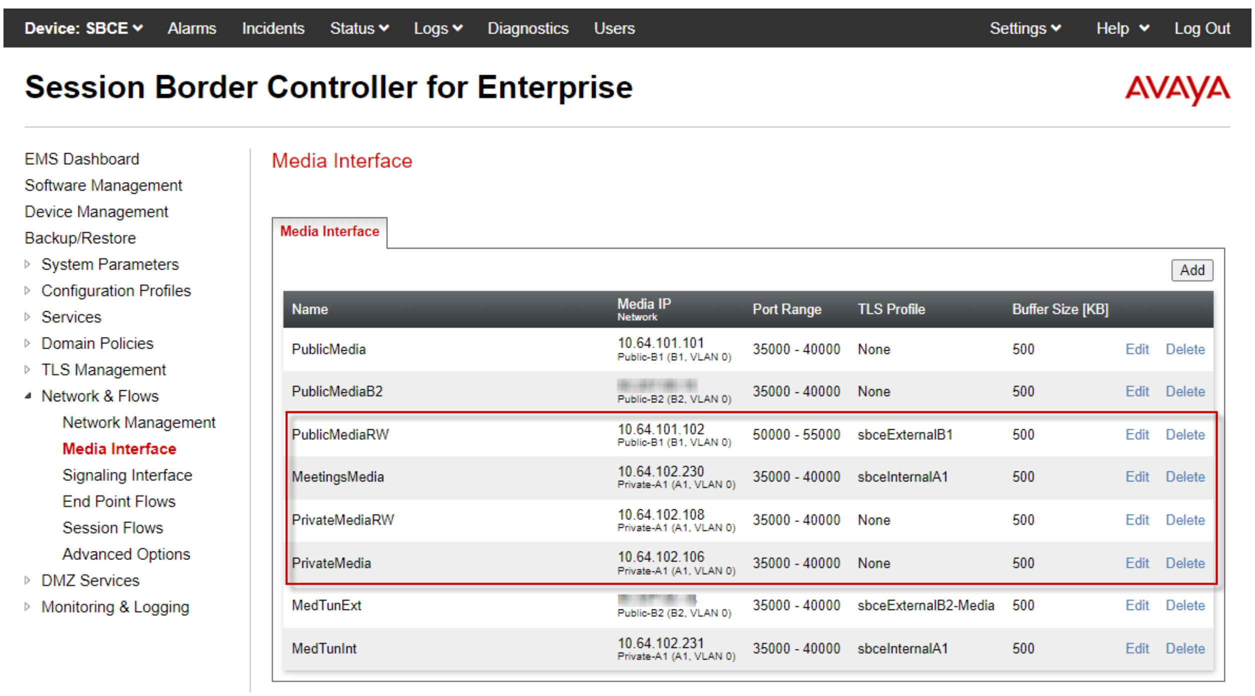


8.8. Administer Media Interfaces

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

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

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

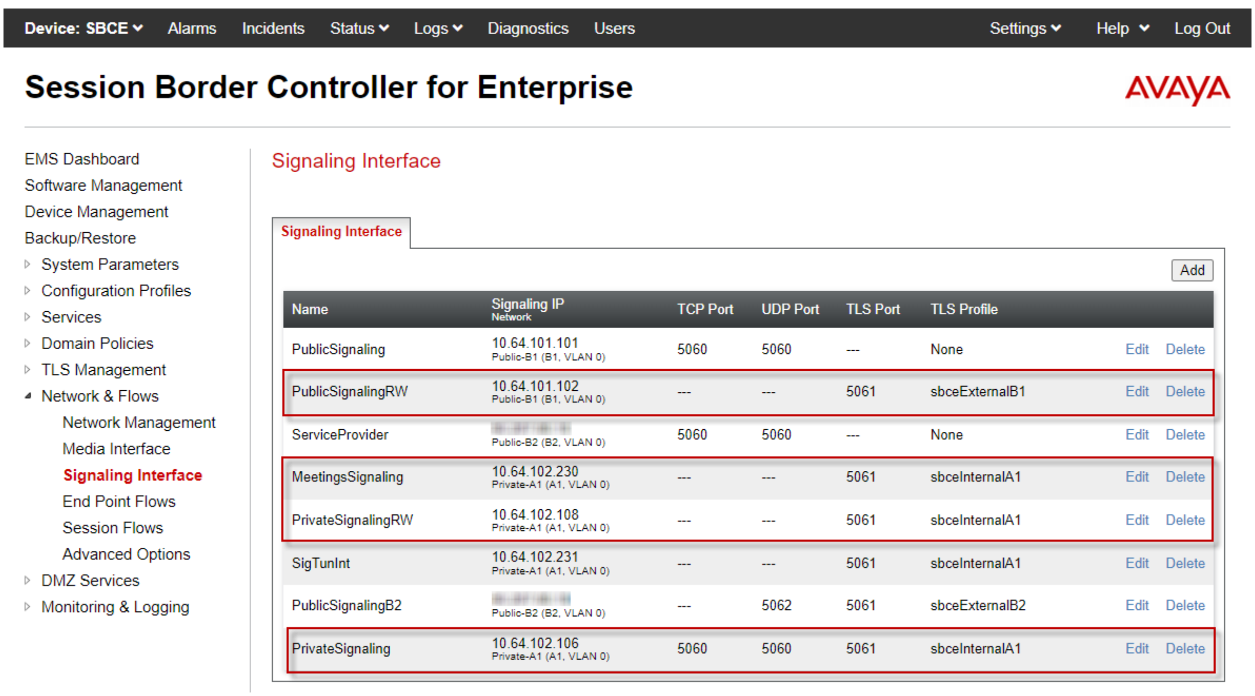


8.9. Administer Signaling Interfaces

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

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

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

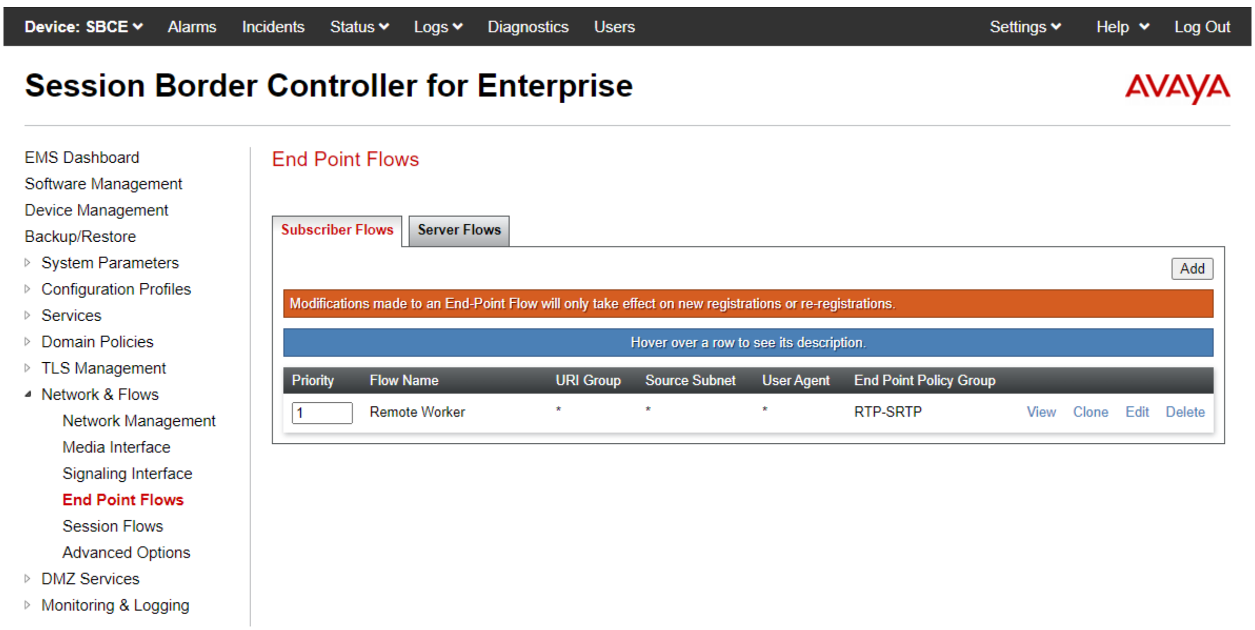


8.10. Administer End Point Flows

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

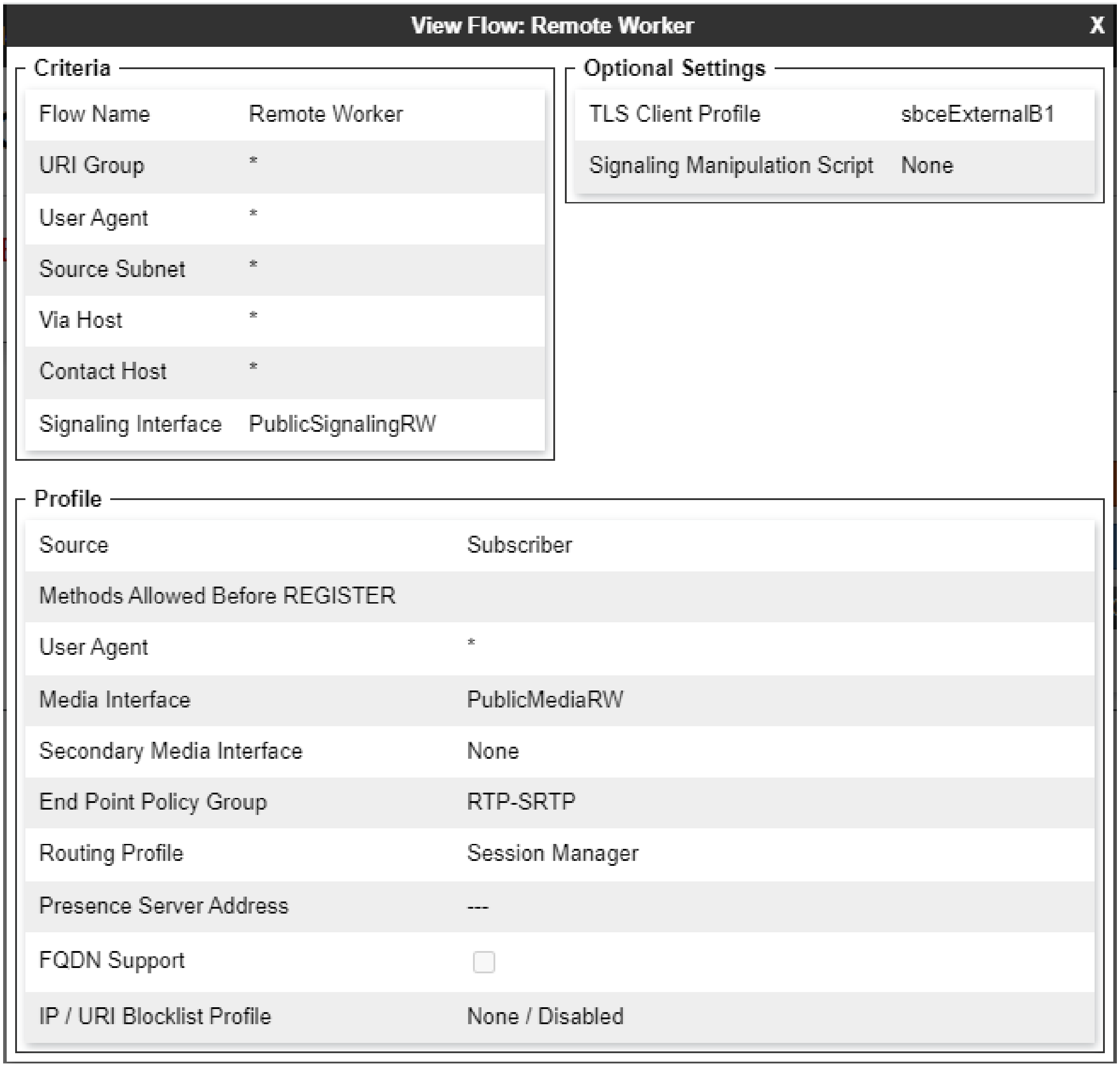
8.10.1. Subscriber Flows

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



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

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

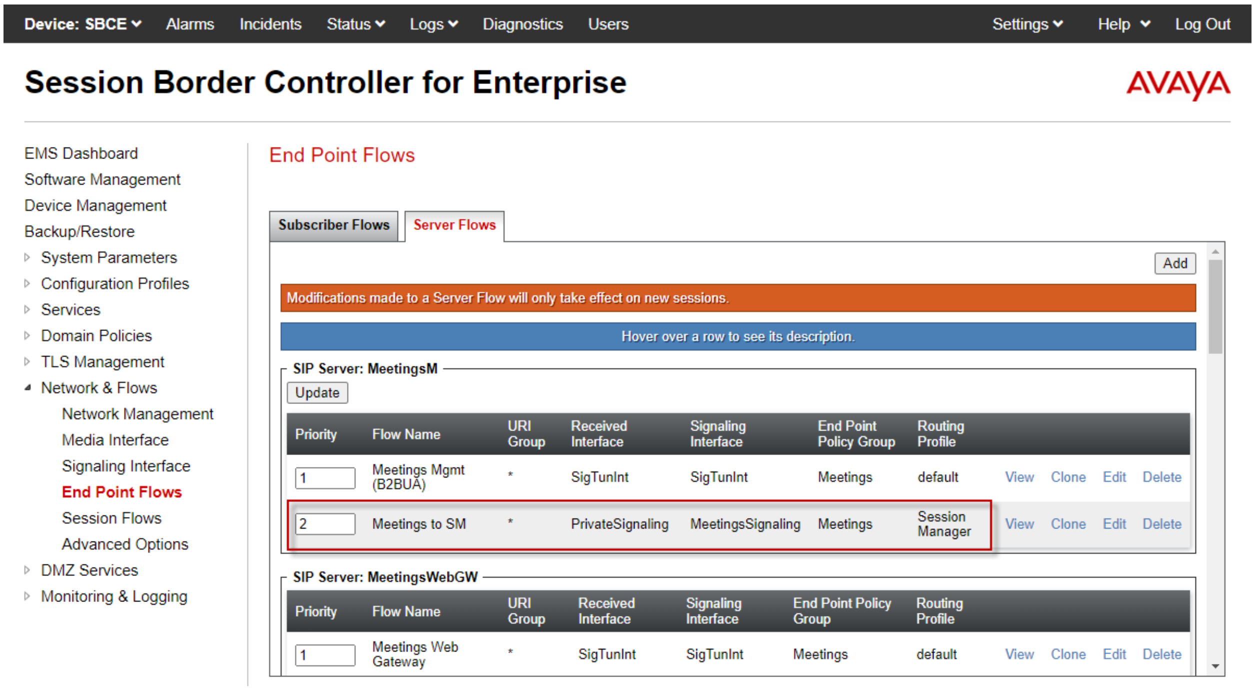
Profile

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

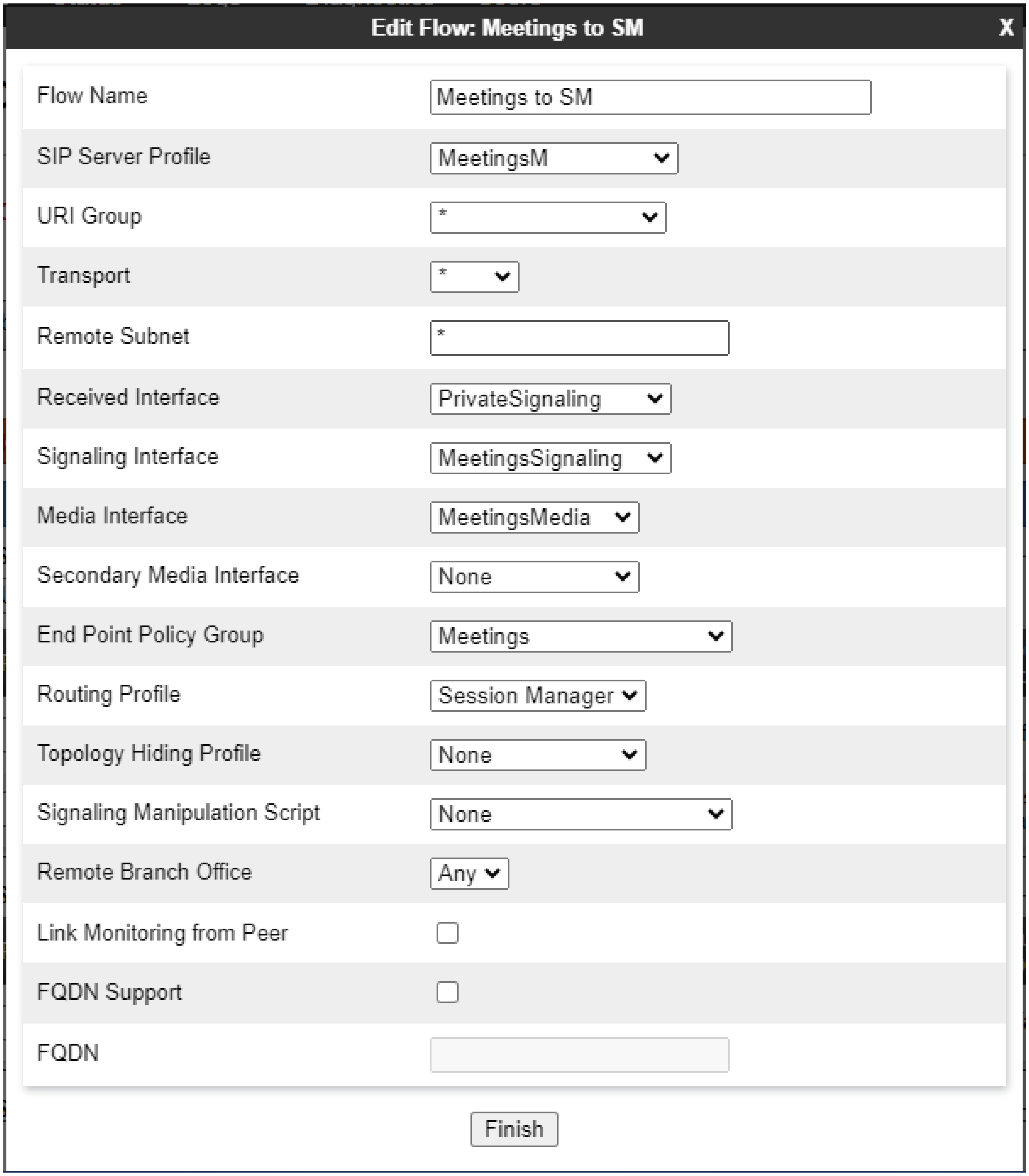
8.10.2. Server Flows

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

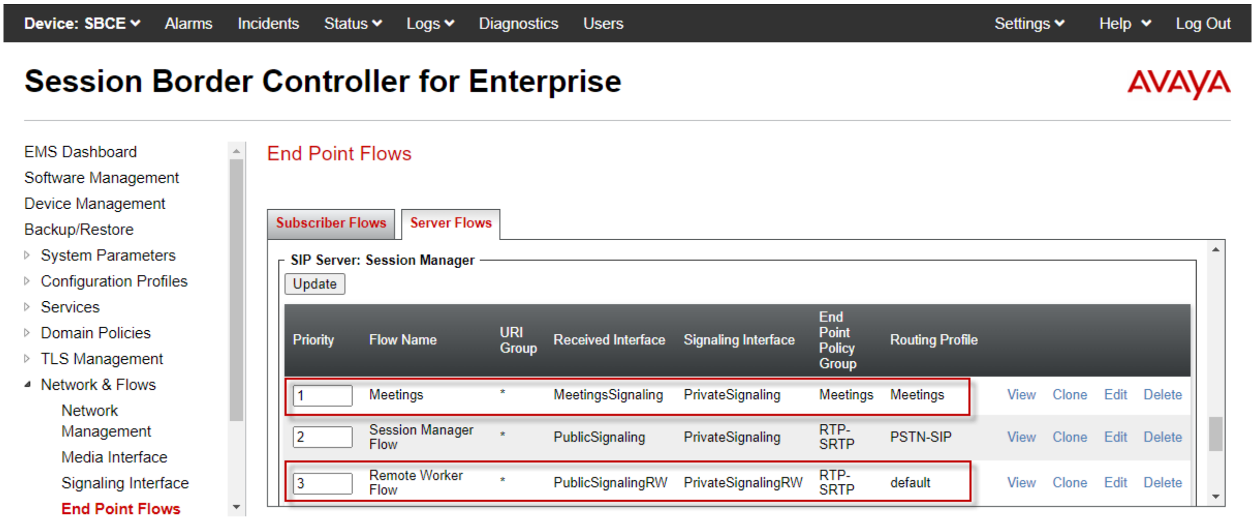
The relevant Meetings Management Server Flow is shown below.



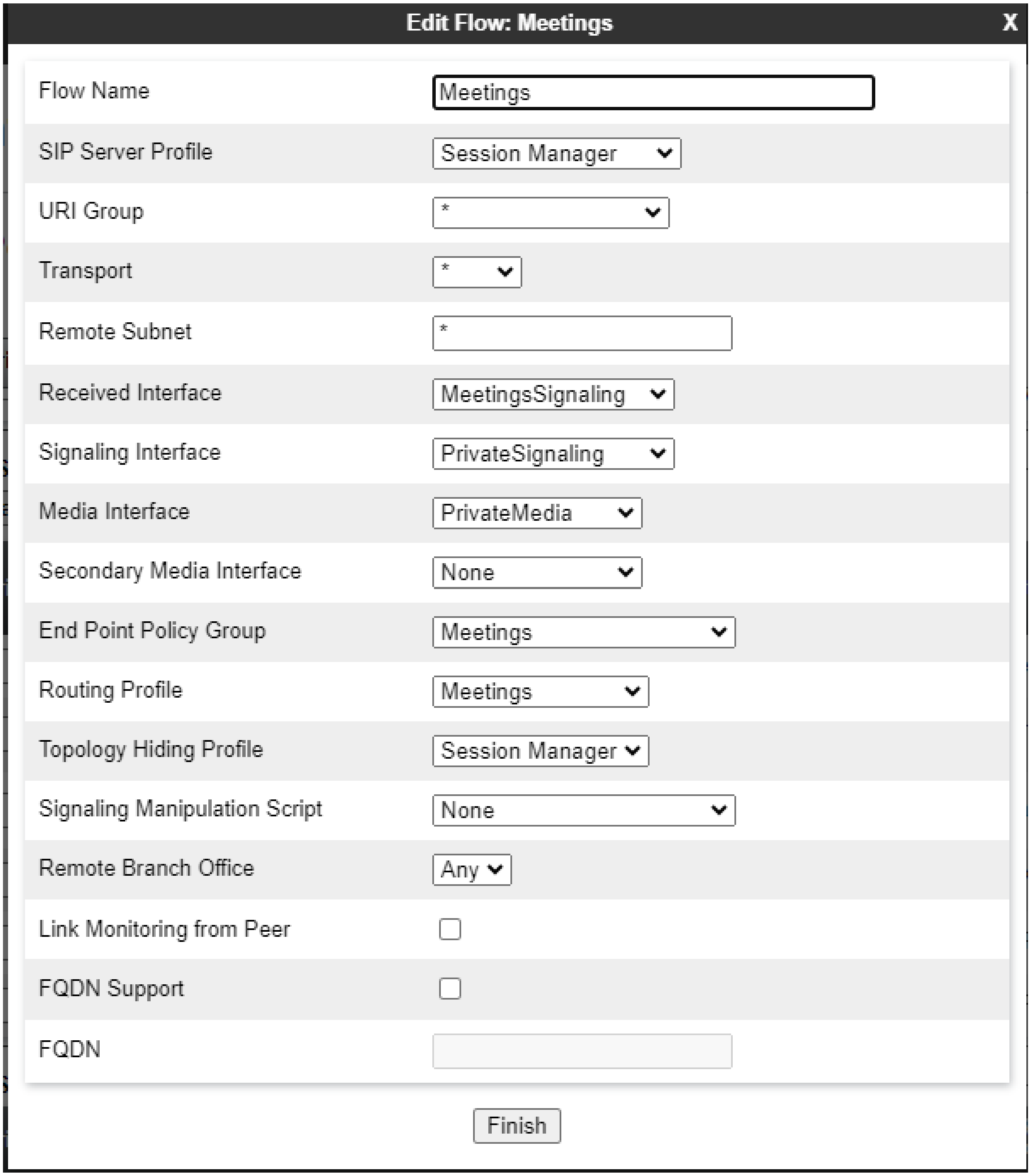
The following server flow is for calls between Meetings Management and Session Manager.



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



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

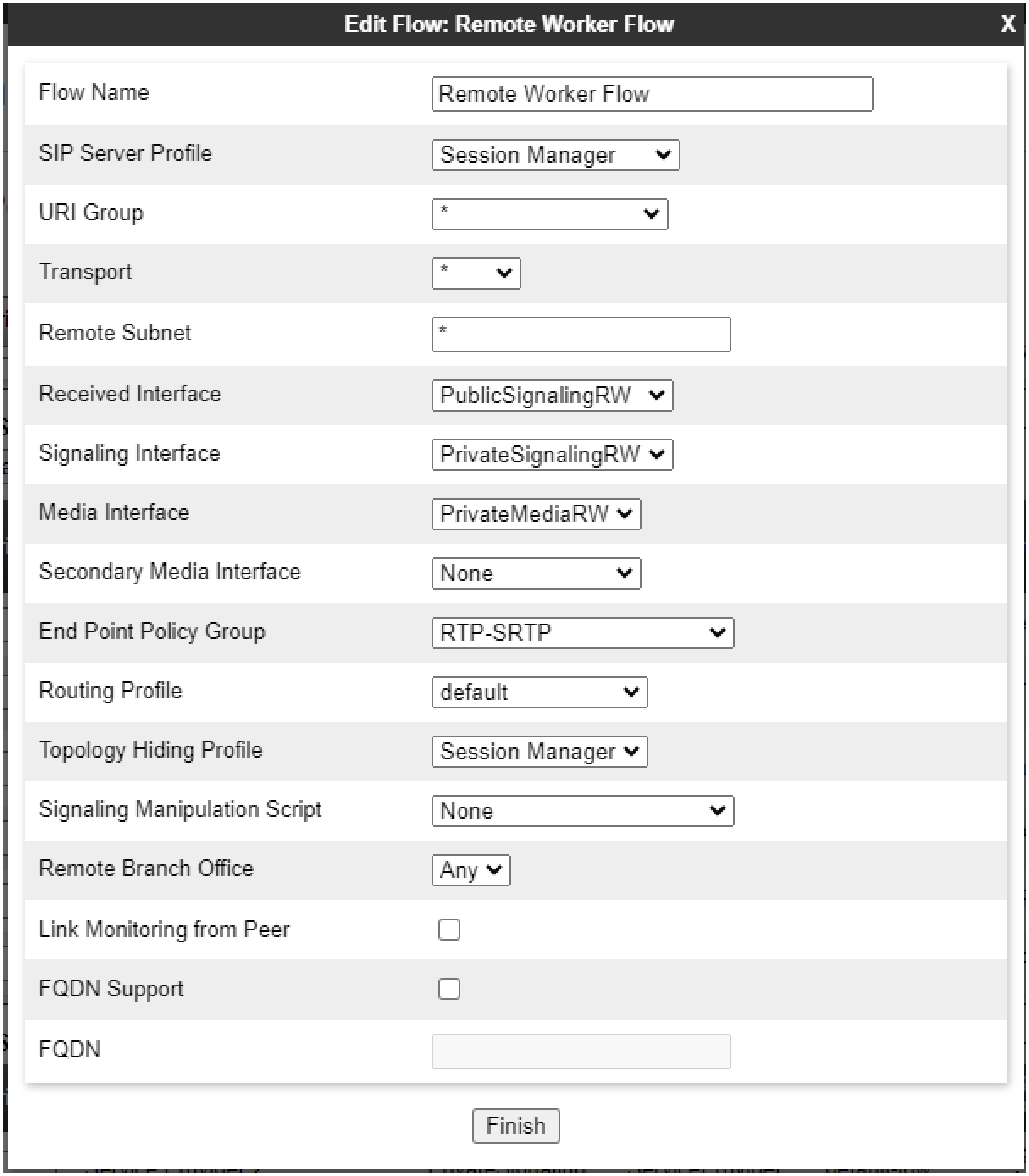


Edit Flow: Meetings

Flow Name	Meetings
SIP Server Profile	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	MeetingsSignaling
Signaling Interface	PrivateSignaling
Media Interface	PrivateMedia
Secondary Media Interface	None
End Point Policy Group	Meetings
Routing Profile	Meetings
Topology Hiding Profile	Session Manager
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☐
FQDN Support	☐
FQDN	

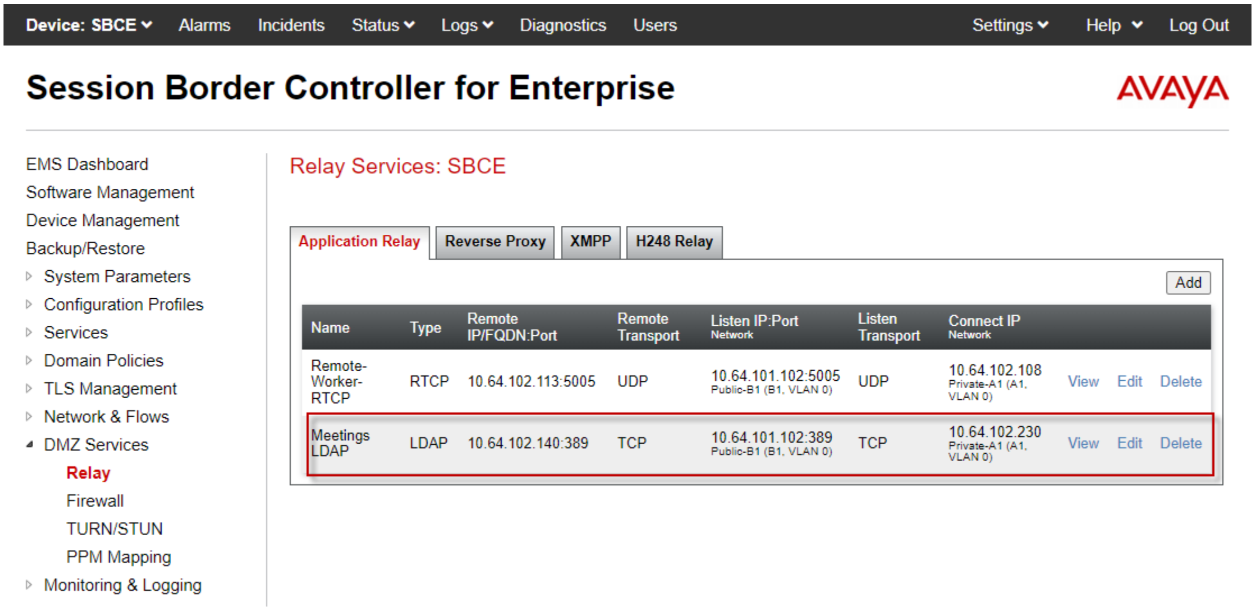
Finish

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



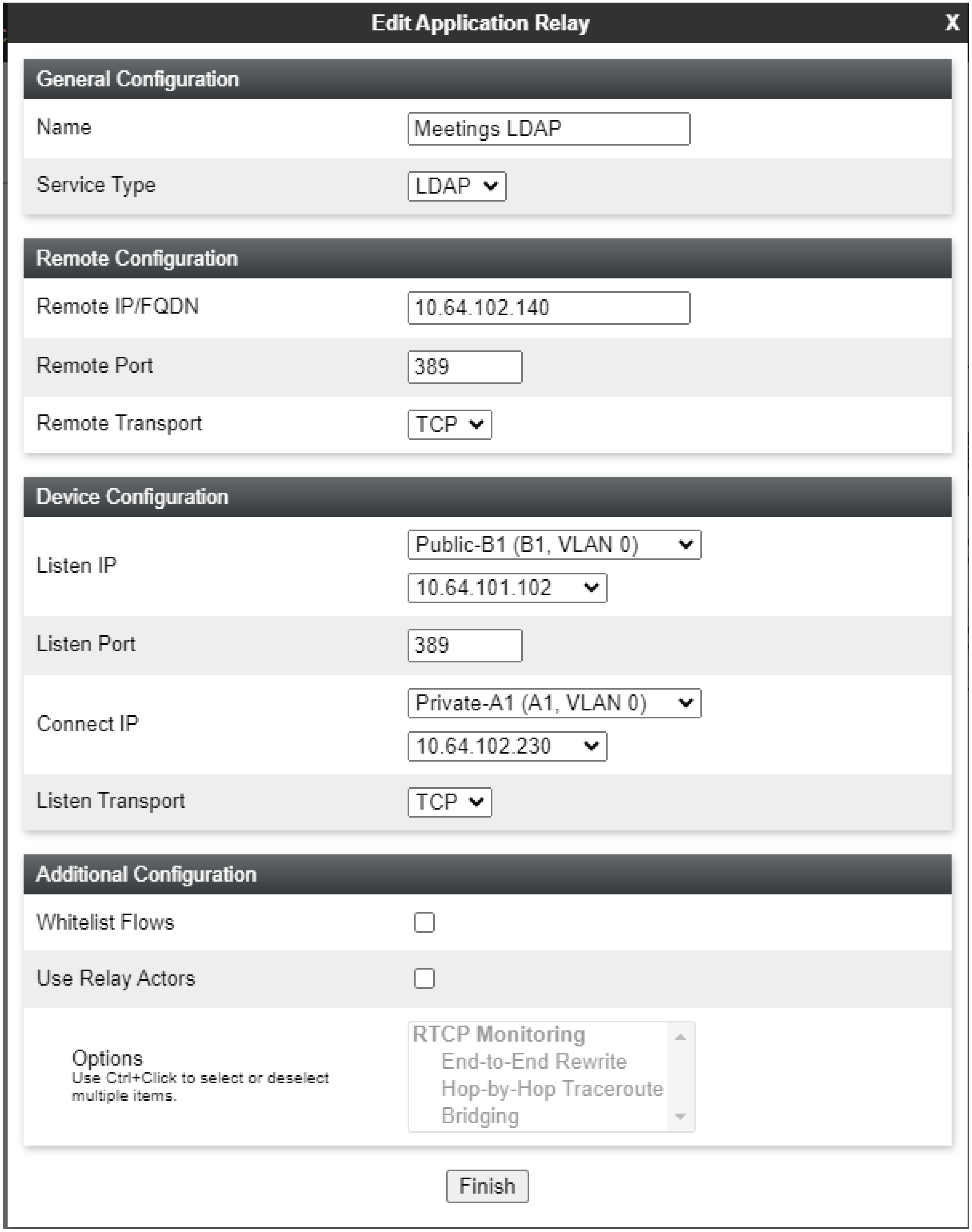
8.11. Administer Application Relay for LDAP

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



For the LDAP Application Relay, configure the following fields:

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


Edit Application Relay
X
General Configuration
Name
Meetings LDAP
Service Type
LDAP
Remote Configuration
Remote IP/FQDN
10.64.102.140
Remote Port
389
Remote Transport
TCP
Device Configuration
Listen IP
Public-B1 (B1, VLAN 0)
10.64.101.102
Listen Port
389
Connect IP
Private-A1 (A1, VLAN 0)
10.64.102.230
Listen Transport
TCP
Additional Configuration
Whitelist Flows
Use Relay Actors
Options
Use Ctrl+Click to select or deselect multiple items.
RTCP Monitoring
End-to-End Rewrite
Hop-by-Hop Traceroute
Bridging
Finish

9. Configure Poly Studio X30 Video Bar

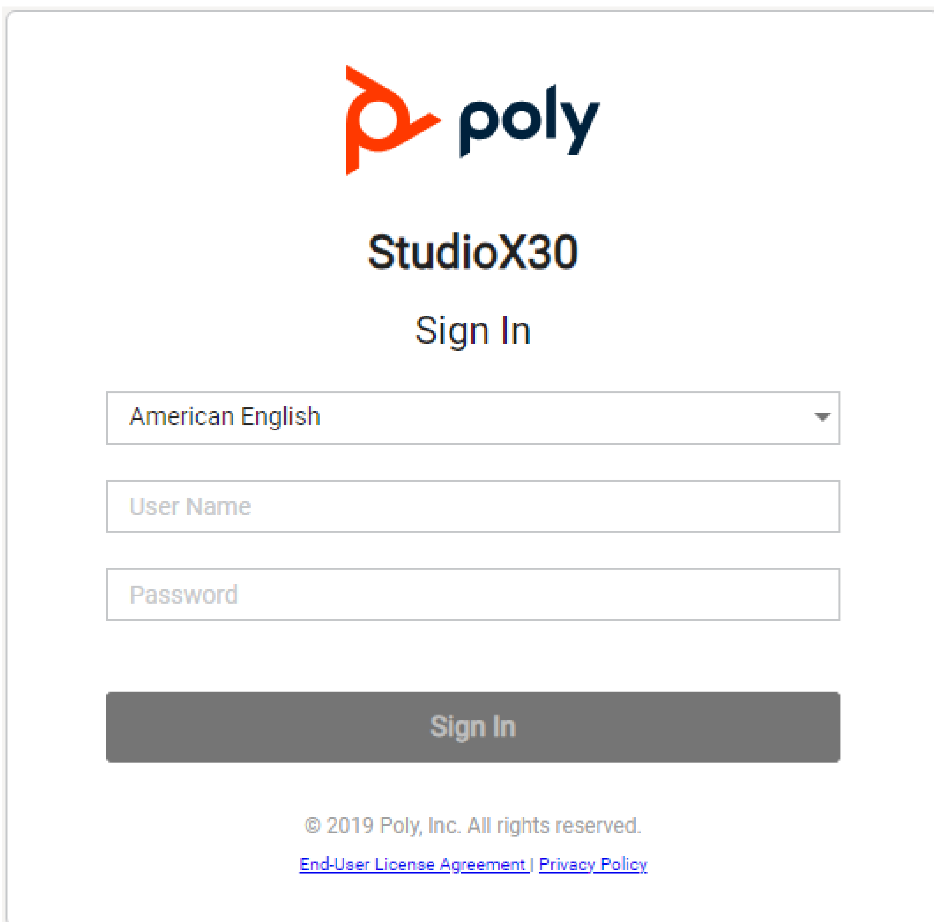
This section covers the configuration of Studio X30 to register directly Session Manager from within the enterprise or to Session Manager through SBC as a remote worker. This configuration requires following steps:

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

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

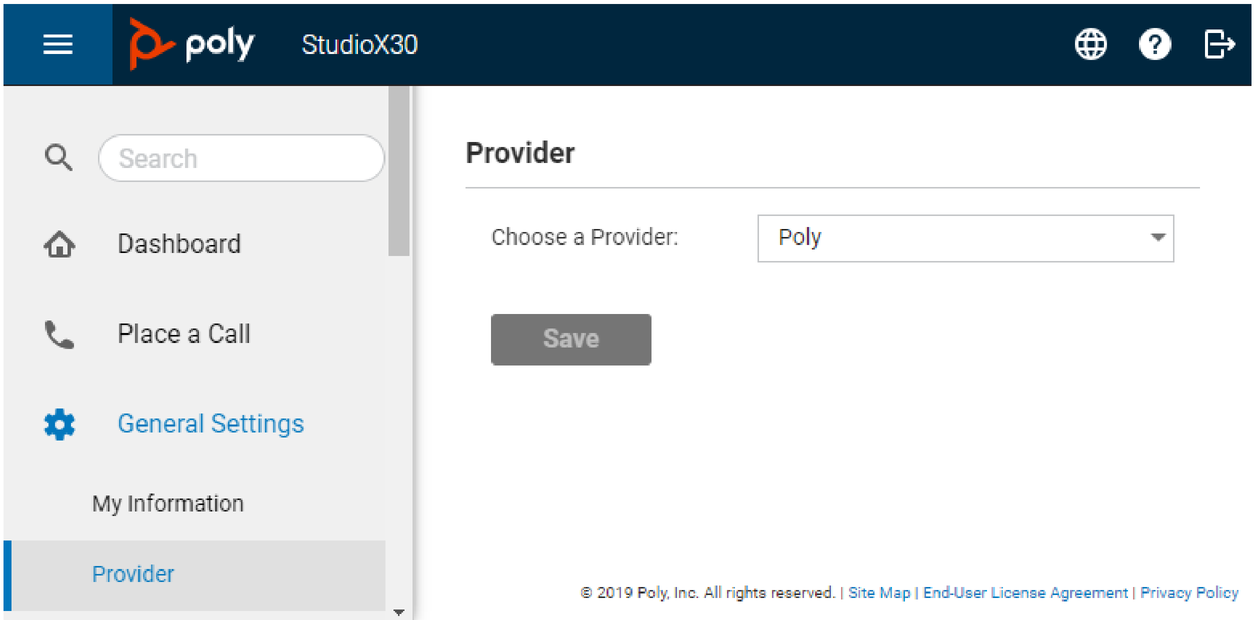
9.1. Access Studio X30 Web Interface

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



9.2. Administer Provider

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

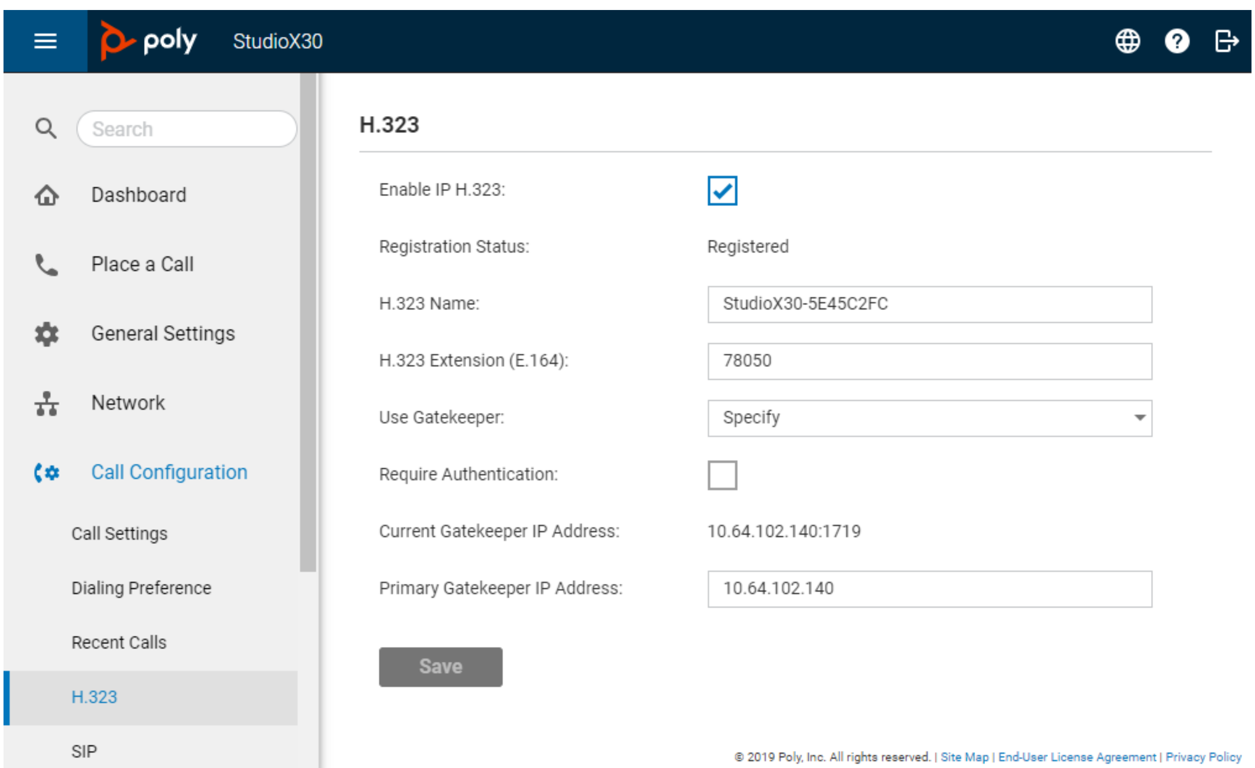


9.3. Administer H.323 Settings

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

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

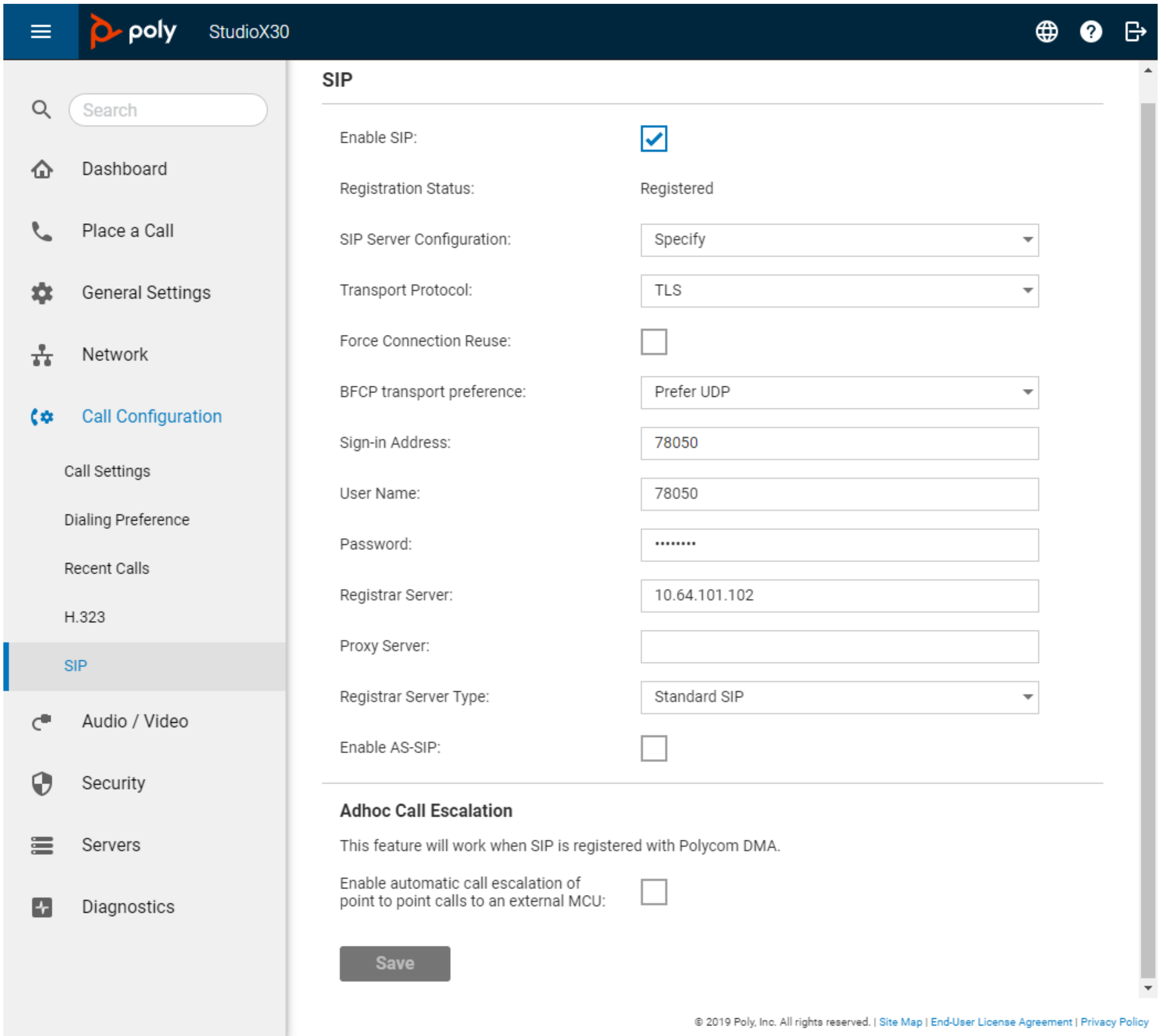
Note: In this configuration, the H.323 interface was used to join meetings and establish point-to-point calls with other Poly video endpoints registered to the internal H.323 gatekeeper in Meetings Management. To establish calls with other Avaya SIP endpoints registered to Session Manager, the SIP interface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



9.4. Administer SIP Settings

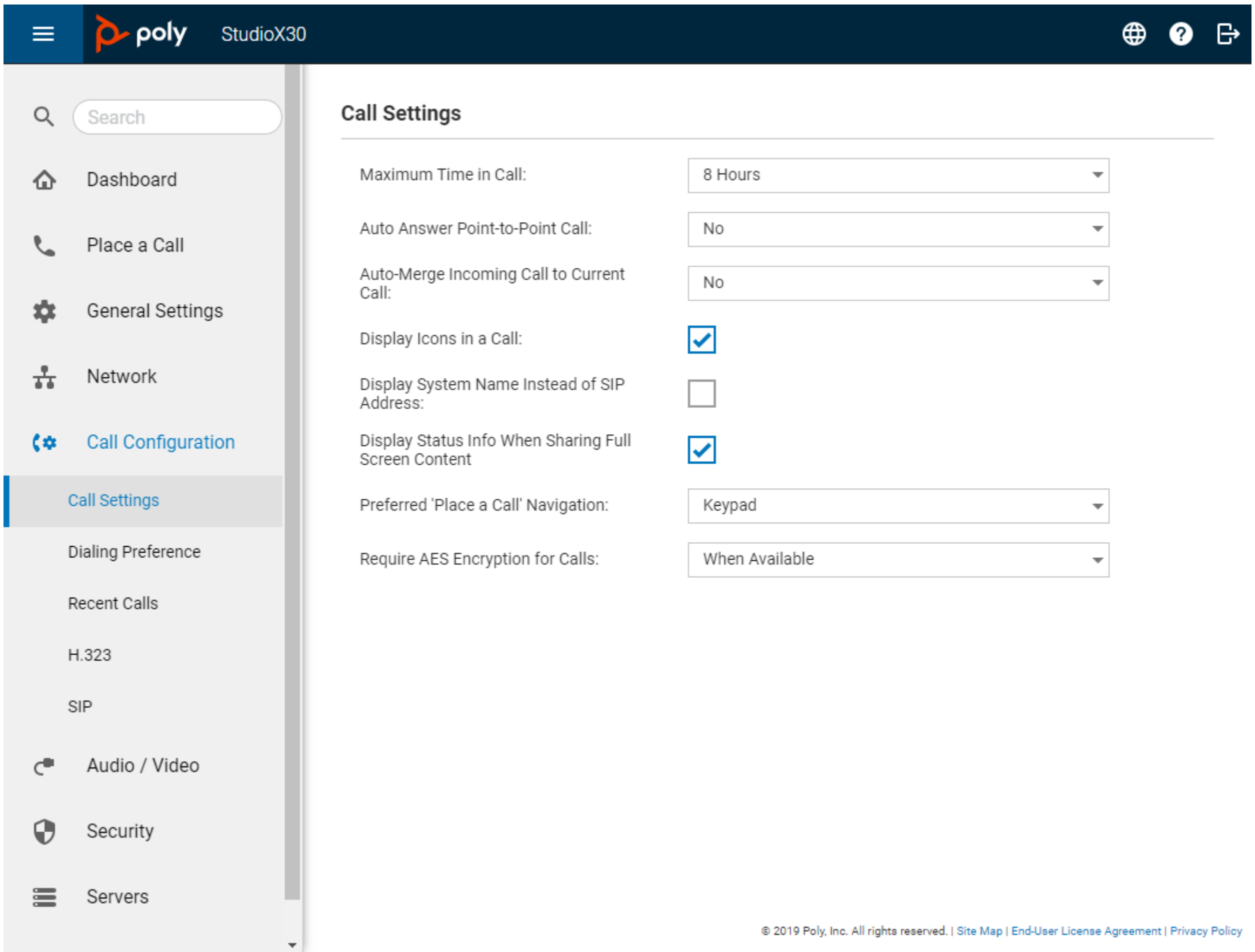
This section covers the SIP configuration so that Studio X30 can register to Session Manager through SBC as a SIP endpoint. In this configuration, the SIP interface is *required* to establish calls with other Avaya SIP endpoints registered to Session Manager. Navigate to **Call Configuration → SIP**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

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


poly
StudioX30
Search
Dashboard
Place a Call
General Settings
Network
Call Configuration
Call Settings
Dialing Preference
Recent Calls
H.323
SIP
Audio / Video
Security
Servers
Diagnostics
SIP
Enable SIP:
Registration Status:
Registered
SIP Server Configuration:
Specify
Transport Protocol:
TLS
Force Connection Reuse:
BFCP transport preference:
Prefer UDP
Sign-in Address:
78050
User Name:
78050
Password:
Registrar Server:
10.64.101.102
Proxy Server:
Registrar Server Type:
Standard SIP
Enable AS-SIP:
Adhoc Call Escalation
This feature will work when SIP is registered with Polycom DMA.
Enable automatic call escalation of point to point calls to an external MCU:
Save
© 2019 Poly, Inc. All rights reserved. | Site Map | End-User License Agreement | Privacy Policy

9.5. Administer Call Settings

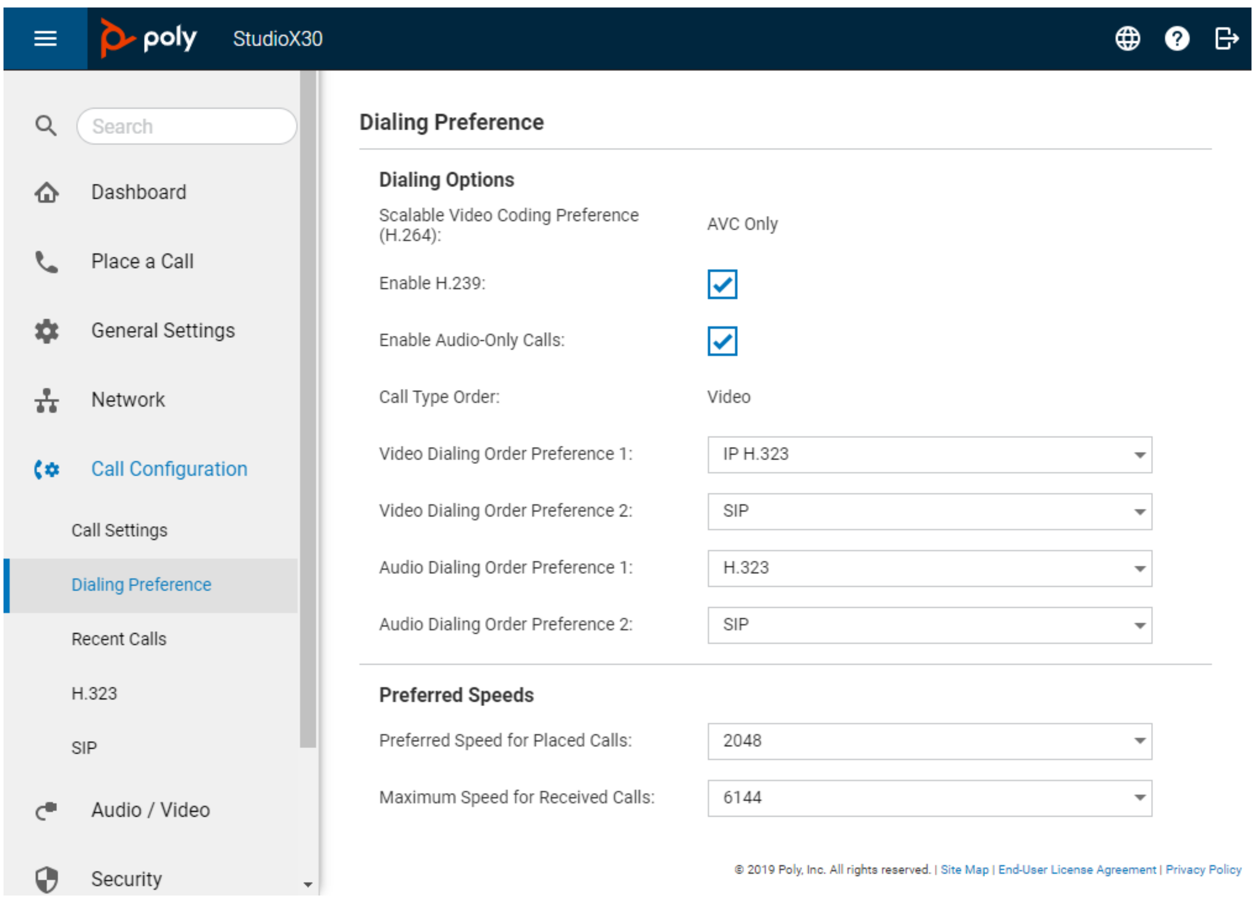
Navigate to **Call Configuration → Call Settings** to configure the **Require AES Encryption for Calls** field. Set this field to *When Available* so that Poly video endpoints can join meetings using H.323 without SRTP. If a Poly video endpoint uses SIP to join a meeting, the call could still be established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



9.6. Administer Dialing Options

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

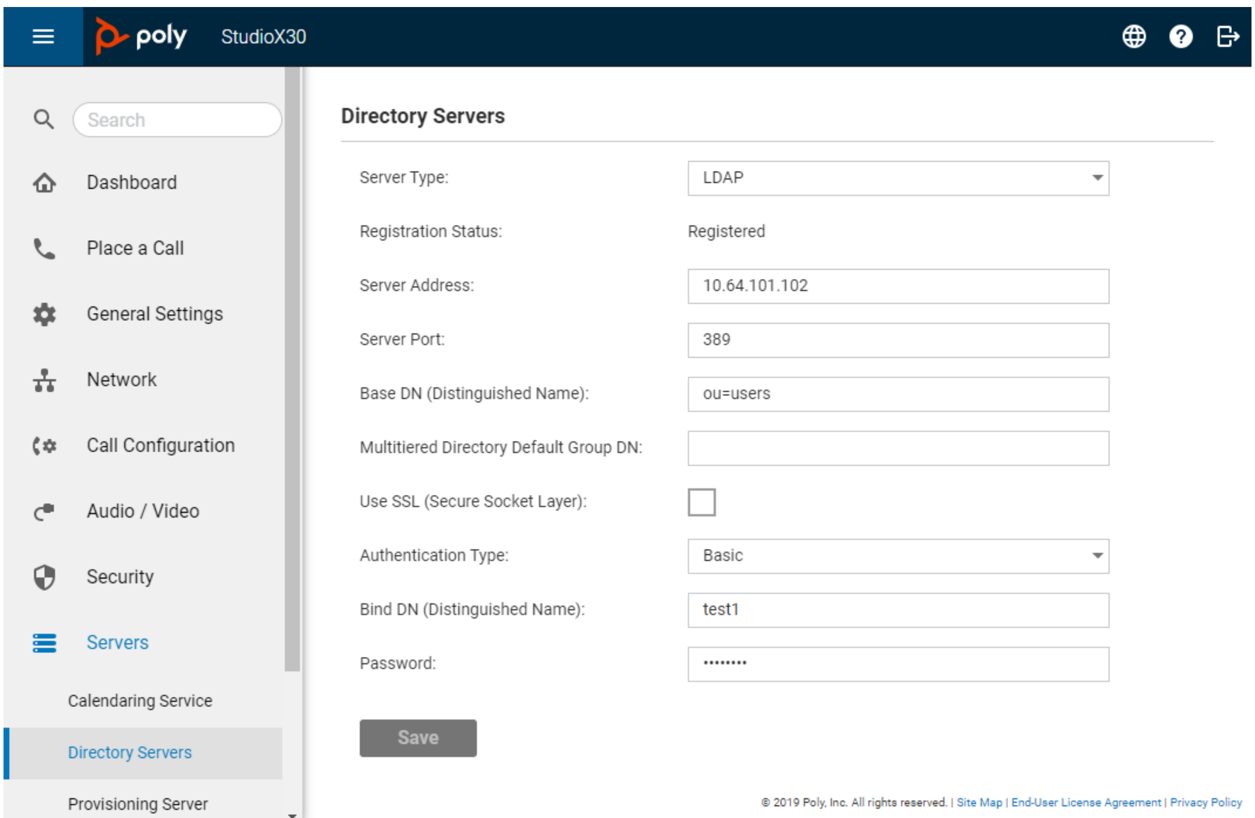
- **Enable Audio-Only Calls:** Select this checkbox to allow audio-only calls on the TC8 touch controller.
- **Video Dialing Order Preference 1:** Specify *IP-H.323* so that video calls would first be attempted using H.323.
- **Video Dialing Order Preference 2:** Specify *SIP* so that video calls would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



9.7. Administer Directory Servers

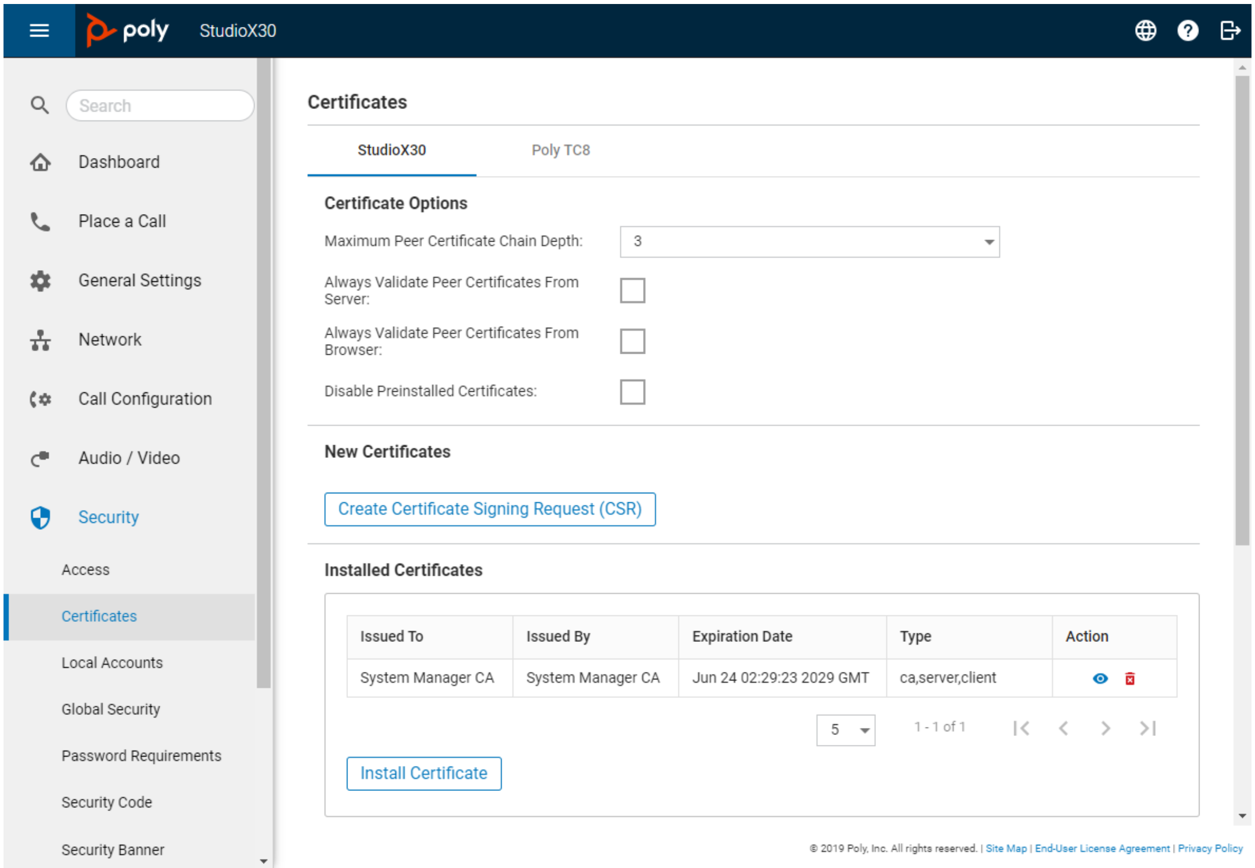
A directory server must be configured for Poly video endpoints to connect to the built-in LDAP server in Meetings Management to allow searches in the corporate address book. Navigate to **Servers → Directory Servers** to configure the following fields:

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



9.8. Install Certificate

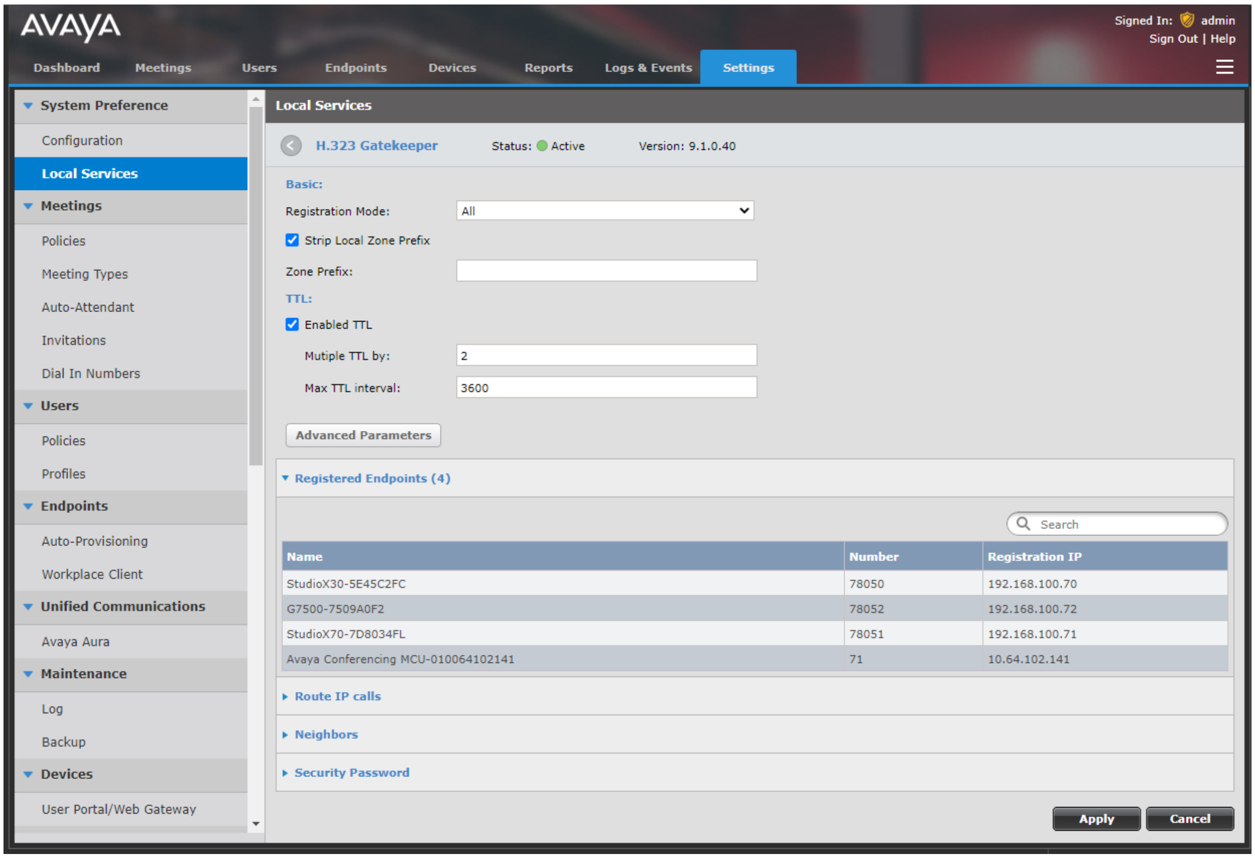
Navigate to **Security → Certificates** to install certificates. To support TLS, click on **Install Certificate** to import the TLS certificate from Avaya Aura® System Manager, the certificate authority. This certificate is used for Session Manager and SBC. When done, the user-installed certificates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



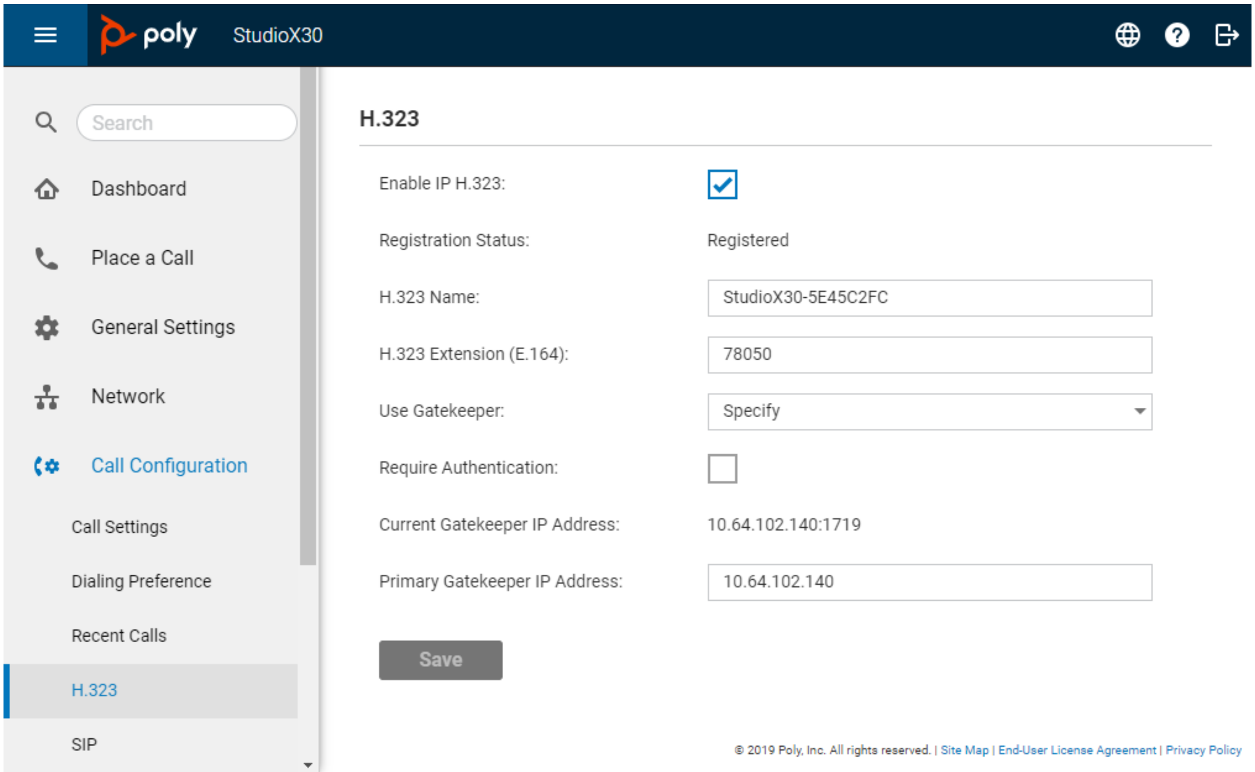
10. Verification Steps

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

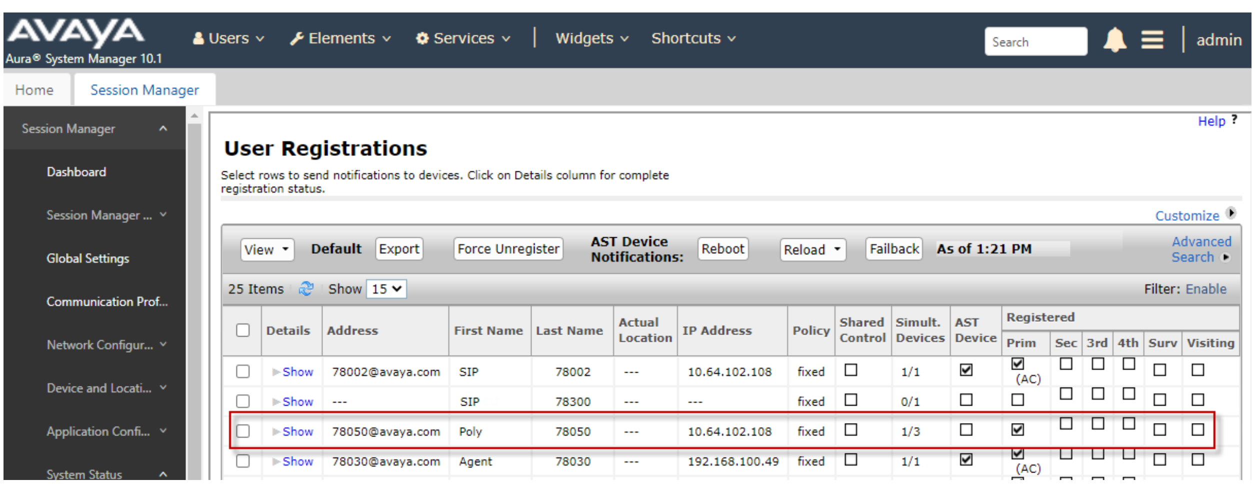
1. Verify Poly video endpoints have successfully registered with internal H.323 gatekeeper in Meetings Management. Navigate to **Settings → Local Services → H.323 Gatekeeper** and verify that the Poly video endpoints are listed under **Registered Endpoints**.



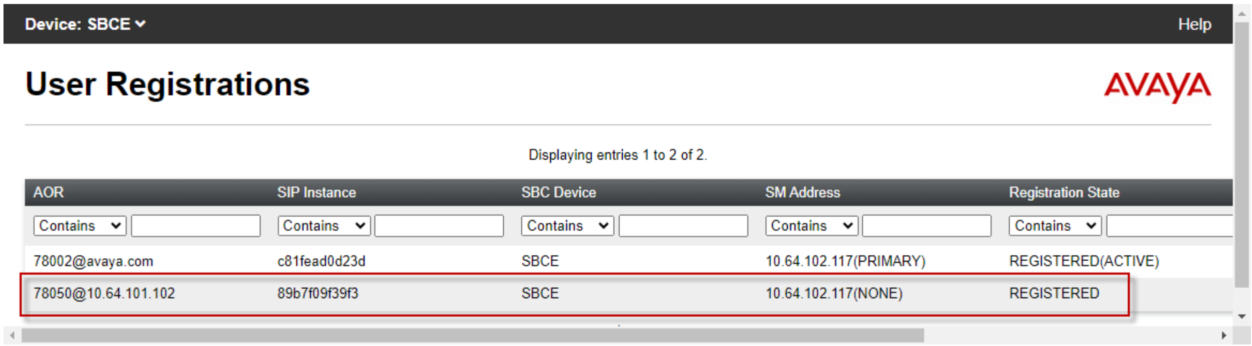
2. Alternatively, verify the H.323 registration status in the Poly web interface. Navigate to **Call Configuration → H.323** and verify the **Registration Status** is *Registered*.



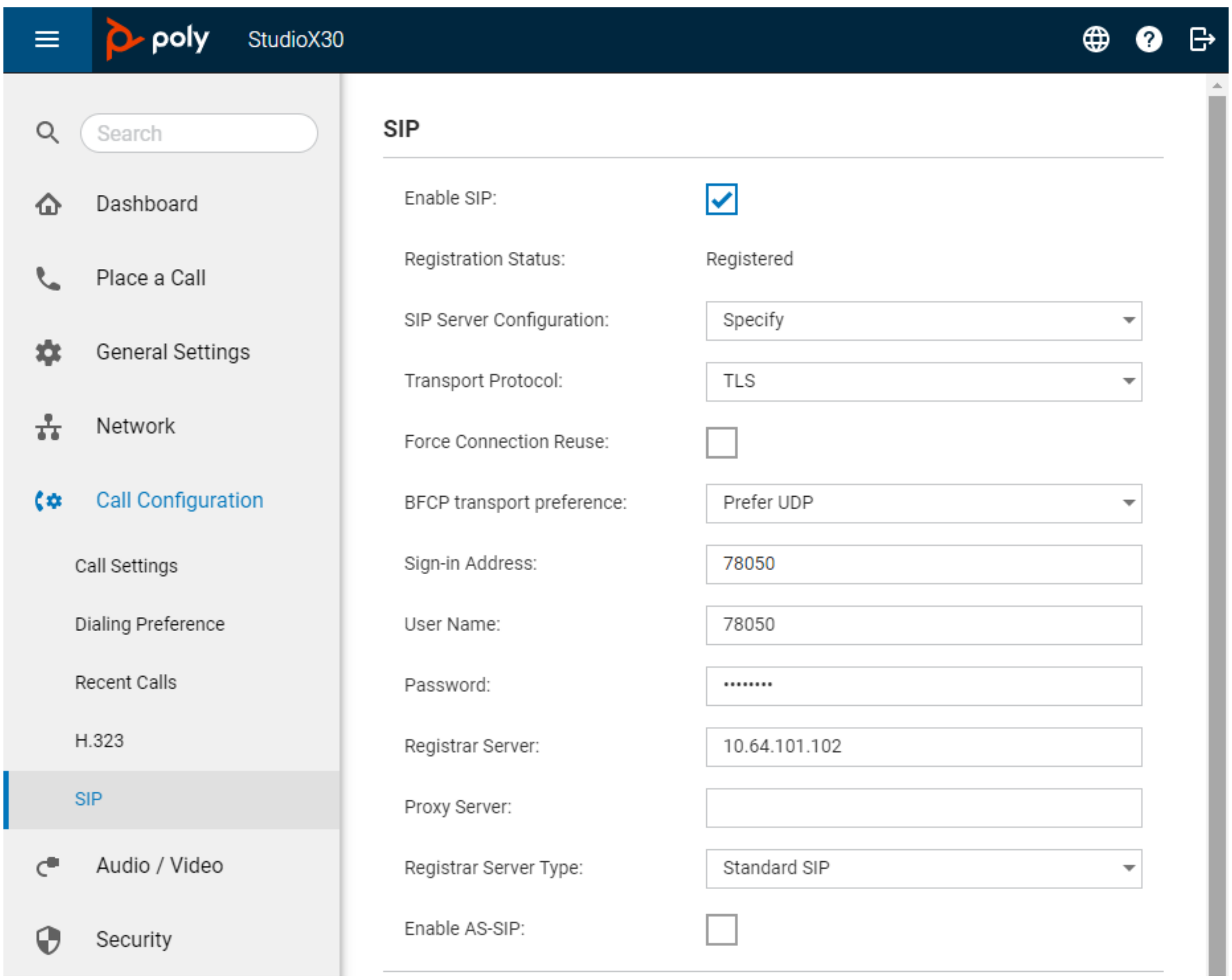
3. Verify Poly video endpoints have successfully registered with Session Manager. In System Manager, navigate to **Elements → Session Manager → System Status → User Registrations** to check the registration status.



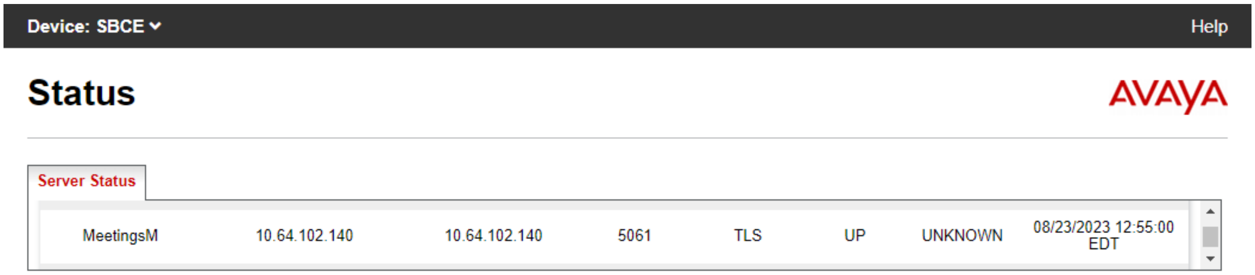
4. Since Poly video endpoints register to Session Manager through SBC, SBC would also provide a registration status, which could be viewed by navigating to **Status → User Registrations** as shown below.



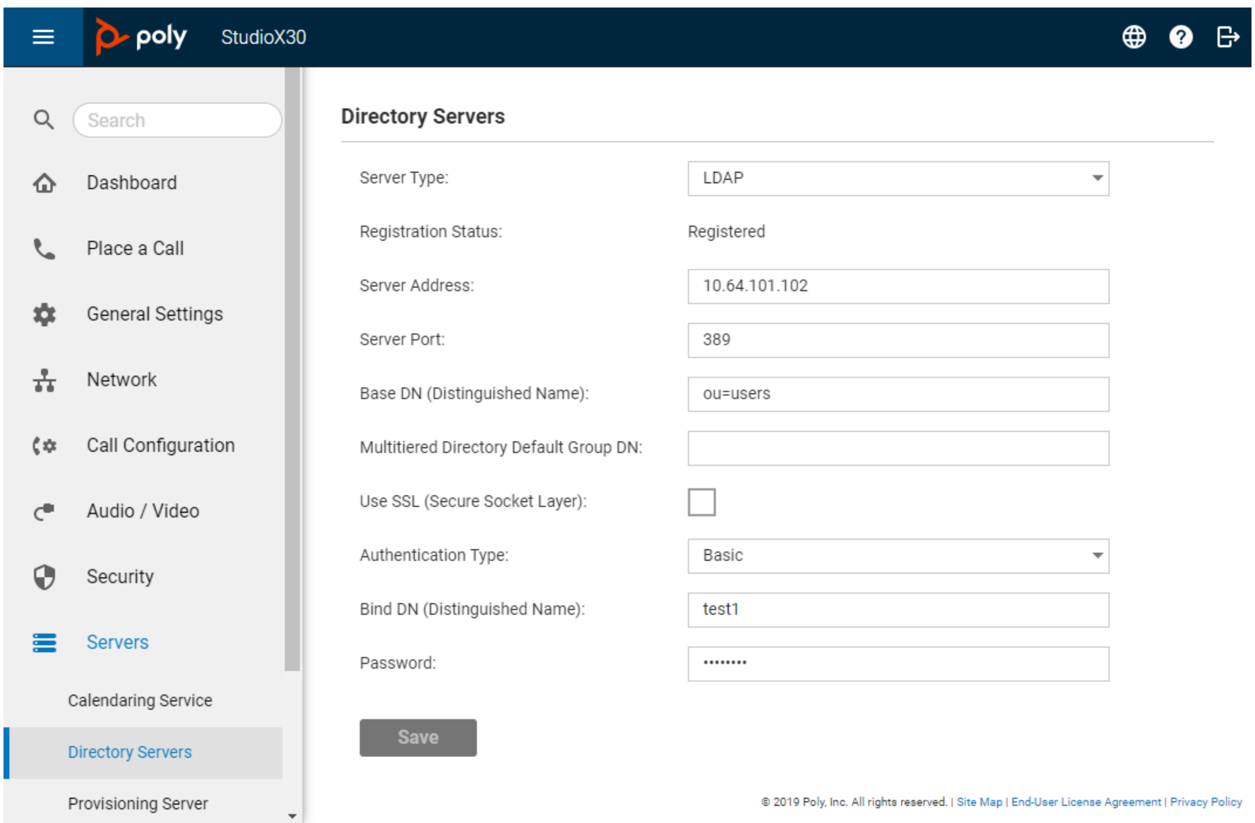
5. Alternatively, the registration status may be verified in the Poly web interface. Navigate to **Call Configuration → SIP** and verify that **Registration Status** is *Registered*.



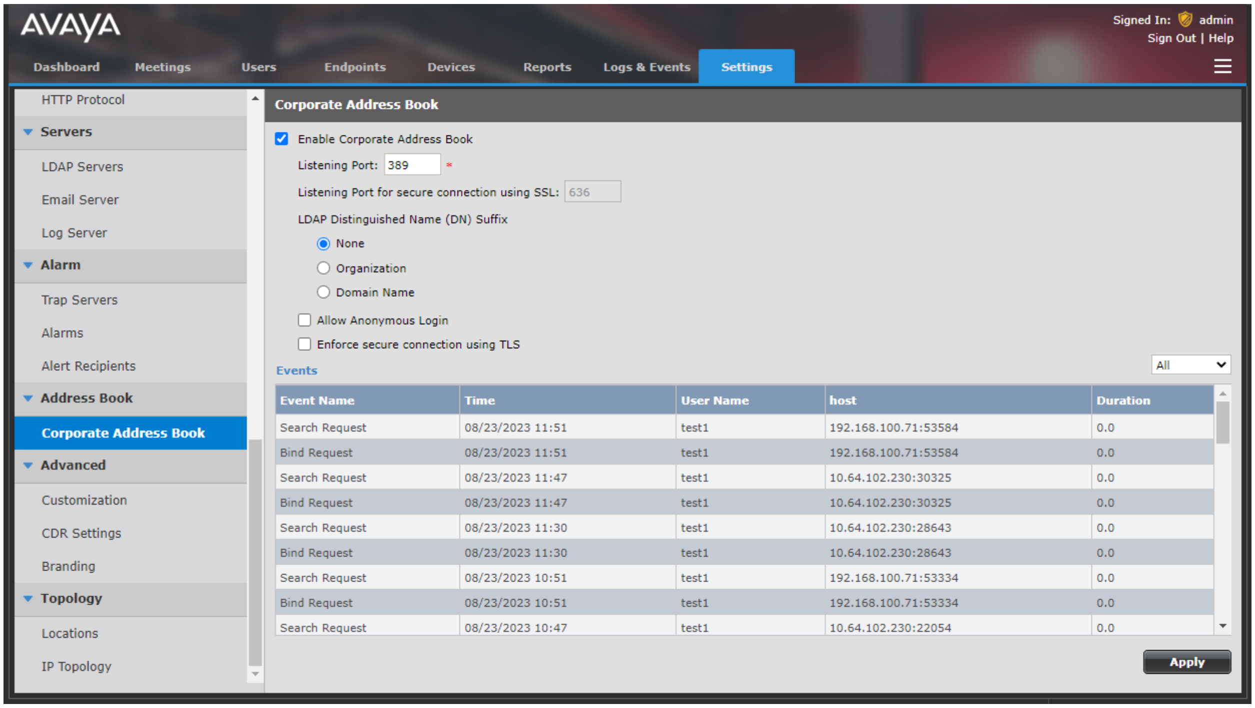
6. To verify the status of the SIP trunk between SBC and Meetings Management, navigate to **Status → Server Status** and verify the SIP trunk is *UP* as shown below.



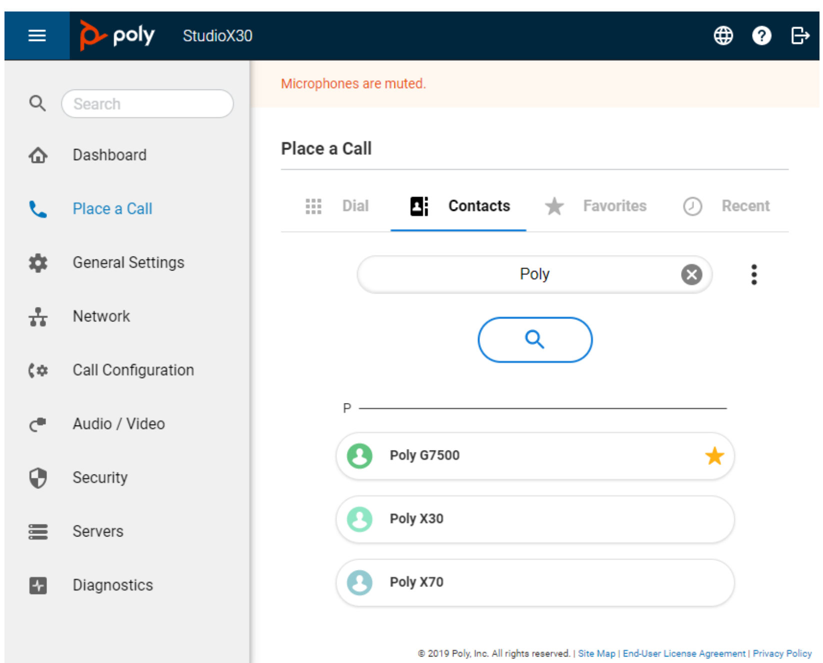
7. Verify the status of the LDAP connection in the Poly web interface. Navigate to **Servers → Directory Servers** and verify the **Registration Status** is *Registered*.



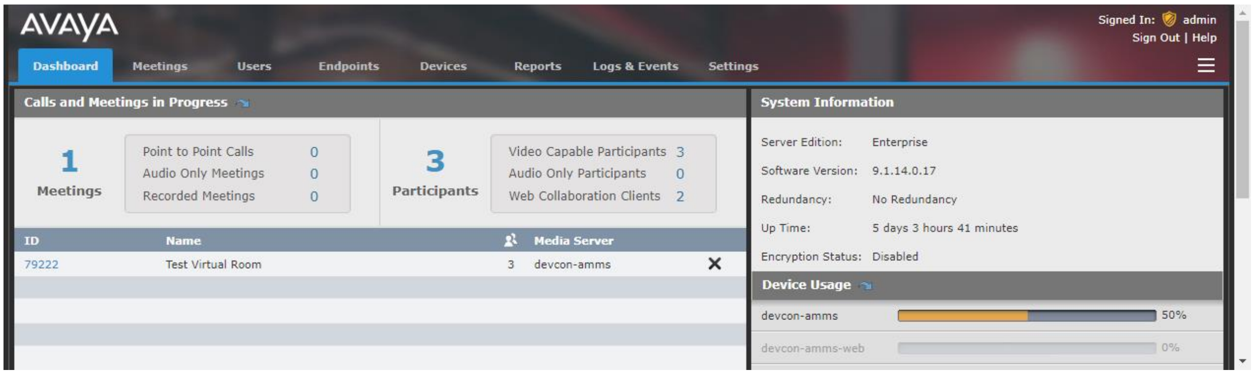
8. Perform a LDAP search for endpoints by name from the TC8 Touch Controller or Poly web interface and verify that Meetings Management receives the LDAP requests under **Events** as shown below.



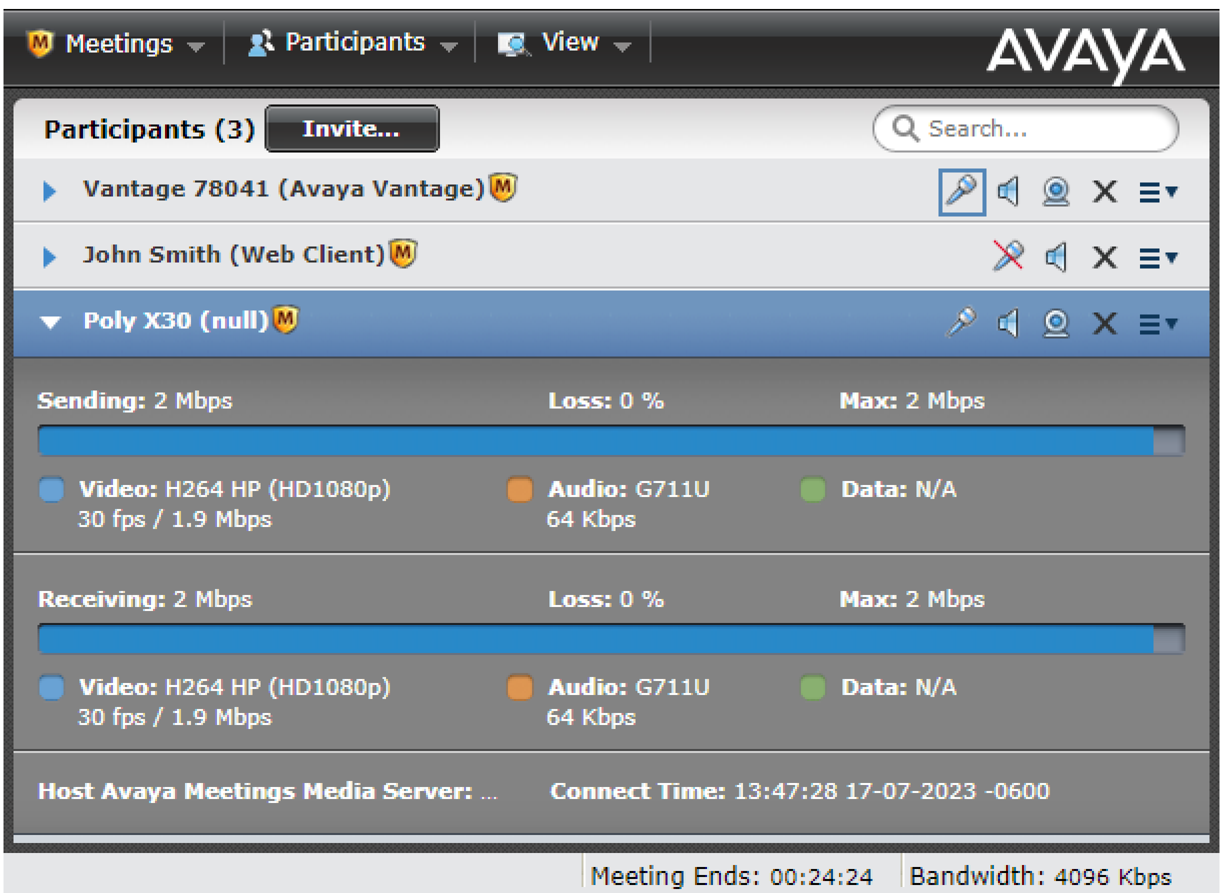
Also, verify that Poly video endpoints display search results on TC8 Touch Controller or web interface (shown below), a call can be placed by clicking on an entry in the search results, and a search result entry can be added to Favorites.



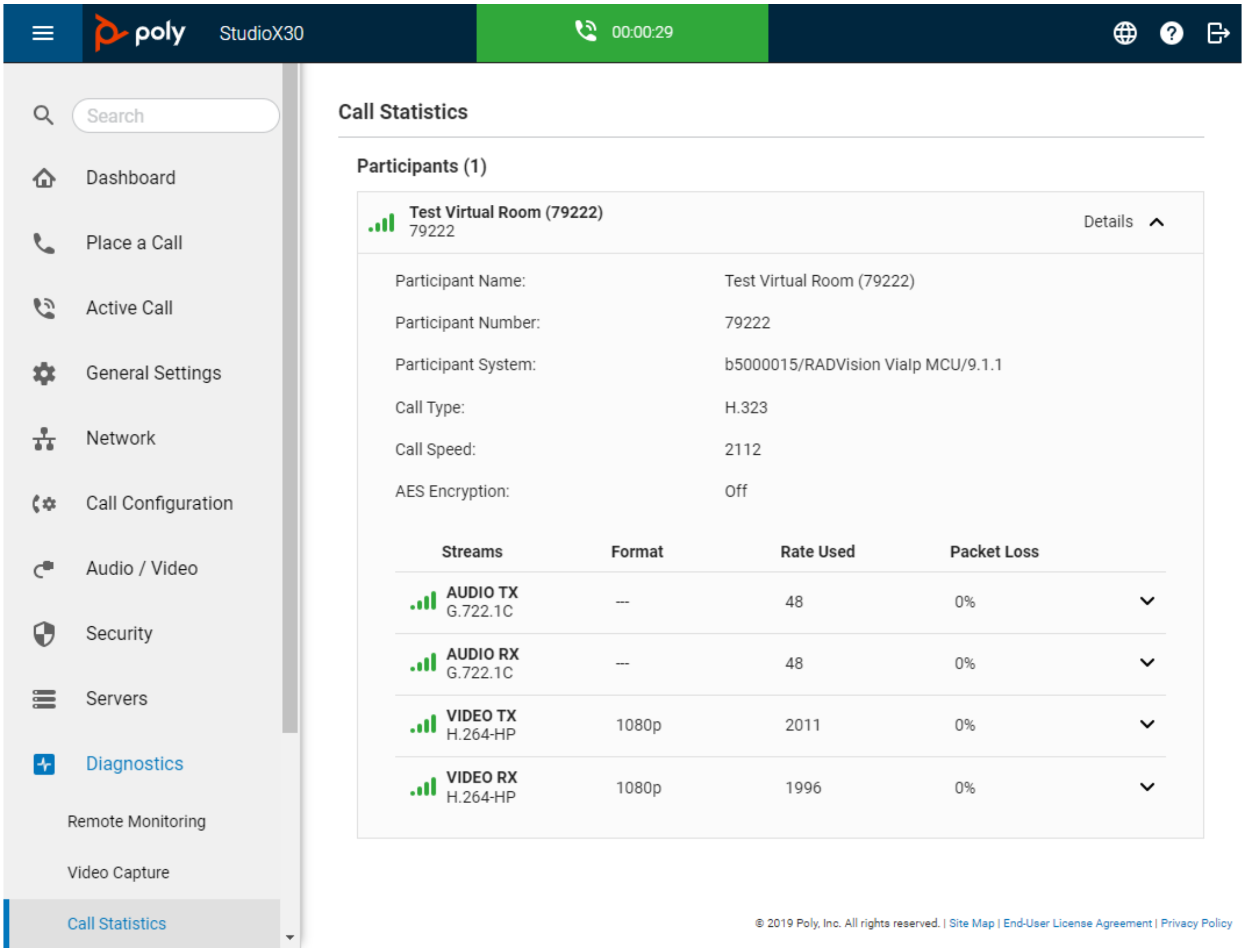
9. Join a meeting from a Poly video endpoint using the Meeting ID. Verify Poly video endpoint joins the meeting and receives audio and video from other participants. In the Meetings Management Administrator Portal, navigate to **Dashboard** and click on the active Meeting ID.



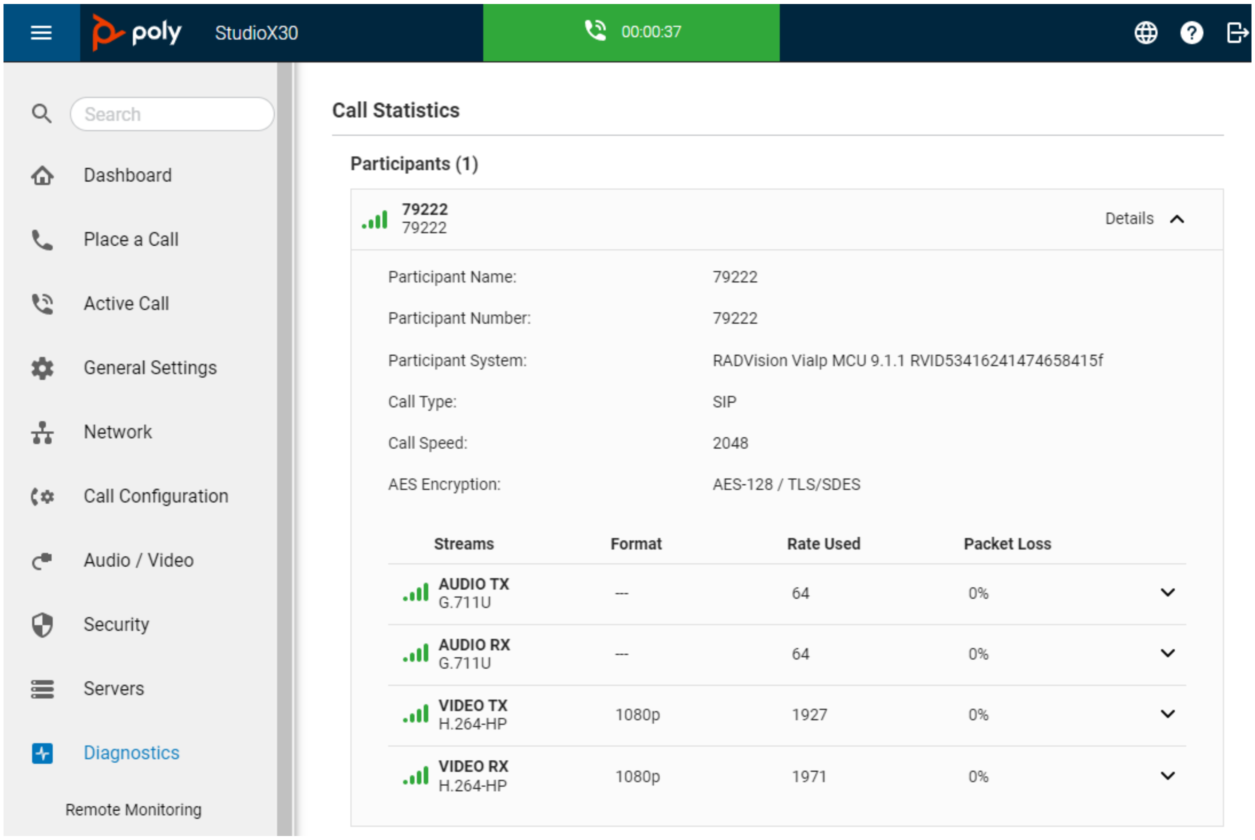
Verify Poly video endpoint is in the participant list and expand the entry to view call details, which should include the codecs, frame rate, and bandwidth.



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



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



11. Conclusion

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

12. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, June 2023, available at http://support.avaya.com.

[2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 11, July 2023, available at http://support.avaya.com.

[3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023, available at http://support.avaya.com.

[4] *Administering Avaya Meetings Management*, Release 9.1.14, Issue 2, June 2023, available at http://support.avaya.com.

[5] *Administering Avaya Session Border Controller*, Release 10.1.x, Issue 3, June 2023, available at http://support.avaya.com.

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.