Avaya Solution & Interoperability Test Lab

Application Notes for PCI Pal® Agent Assist with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate PCI Pal® Agent Assist 2022 with Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, and Avaya Session Border Controller for Enterprise 10.1. Avaya Session Border Controller for Enterprise routes calls between a contact center on Avaya Aura® Communication Manager and a VoIP Service Provider with calls routing through PCI Pal® Agent Assist. PCI Pal® Agent Assist is a hosted solution that allows contact centers to take card payments securely using DTMF capture technology while the contact center agent remains in the conversation with the customer. PCI Pal® Agent Assist integrates with Avaya Session Border Controller for Enterprise via a SIP trunk.

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.

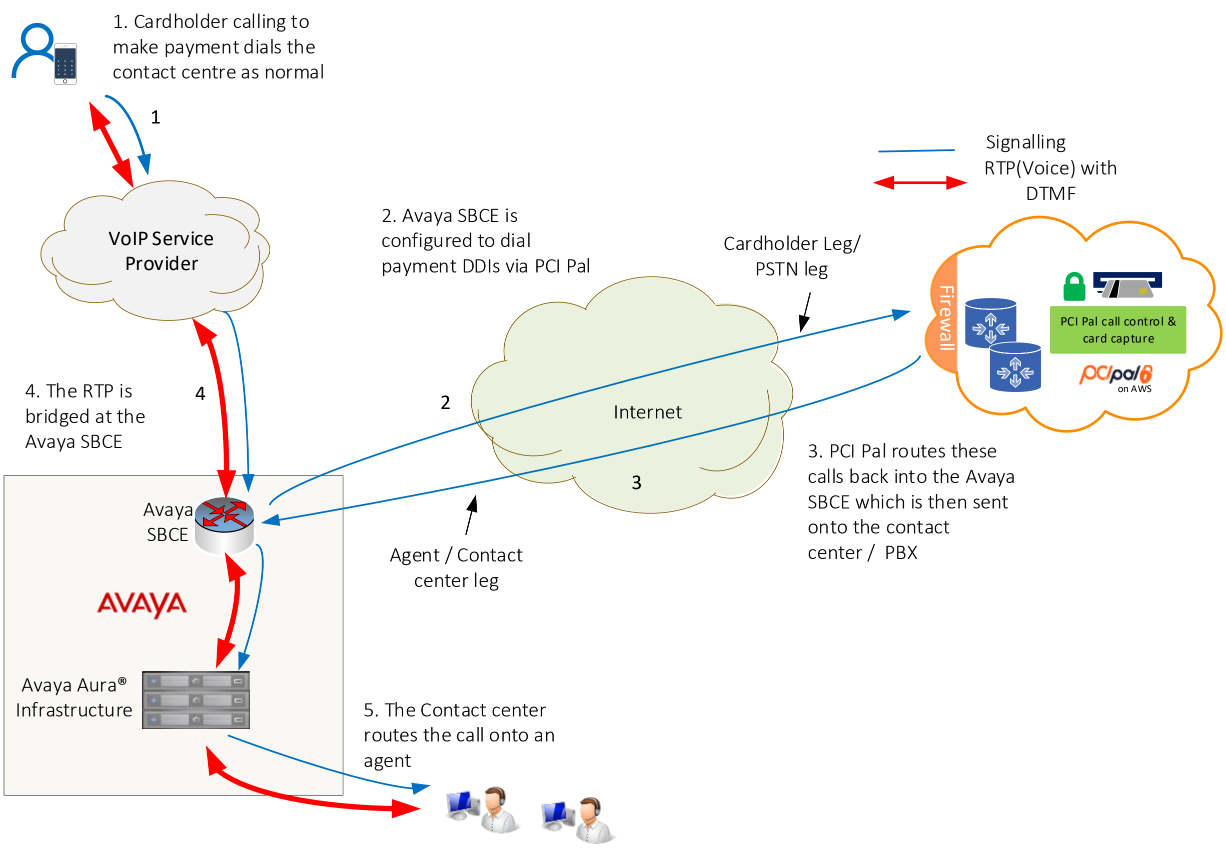
Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe the configuration steps required to integrate PCI Pal® Agent Assist with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise. Avaya Session Border Controller for Enterprise routes calls between a contact center on Avaya Aura® Communication Manager and a VoIP Service Provider with calls routing through PCI Pal® Agent Assist. PCI Pal Agent Assist is a hosted solution that allows contact centers to take card payments securely using DTMF capture technology while the contact center agent remains in the conversation with the customer. PCI Pal Agent Assist integrates with Avaya Session Border Controller for Enterprise (Avaya SBCE) via a SIP trunk.

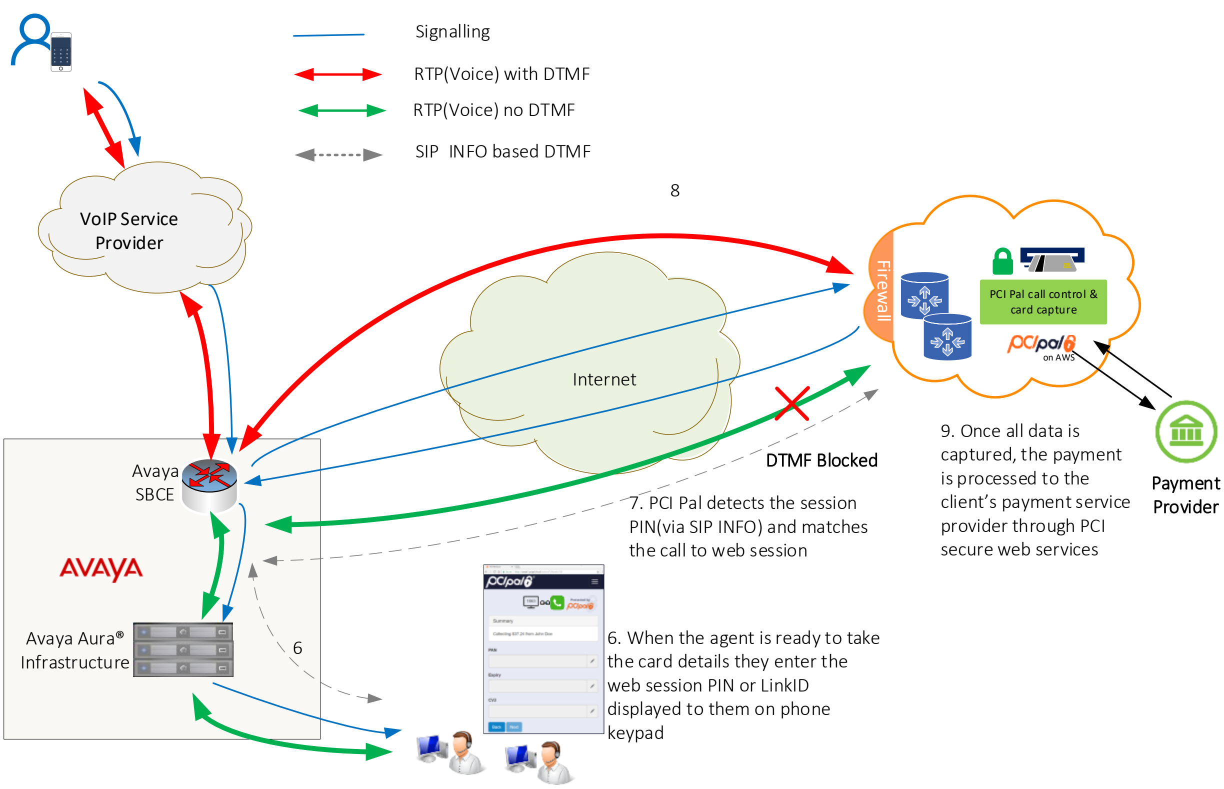
Calls between the Avaya Aura® environment and the VoIP Service Provider are generally routed via Avaya SBCE. Avaya SBCE routes such calls through PCI Pal Agent Assist. All inbound and outbound calls are routed (looped) via Avaya SBCE to PCI Pal Agent Assist. Initially, for a given call, only SIP signaling is looped via Avaya SBCE to PCI Pal Agent Assist, RTP still flows through Avaya SBCE.



Once the call is answered by a contact center agent, a 4-digit code (PIN or Link ID) provided by the PCI Pal Portal is entered by the contact center agent at the time of payment is required to secure the call. This code is sent to Avaya SBCE via DTMF using RFC2833. Avaya SBCE then converts the DTMF using RFC2833 to SIP INFO messages and sends them to PCI Pal Agent

Assist. RFC2833 tones are also sent in the RTP. Upon successful authentication, PCI Pal Agent Assist sends a re-INVITE to Avaya SBCE to redirect RTP using RFC2833 to PCI Pal Agent Assist. After the RTP has been successfully redirected, the call is considered secured. Once instructed, customer enters payment information via their telephone keypad. These DTMF digits are sent to Avaya SBCE and converted to SIP INFO. Both DTMF methods using RFC2833 and SIP INFO are sent to PCI Pal Agent Assist when the call is secured. For each DTMF digit, PCI Pal Agent Assist removes the SIP INFO, RFC2833, and in-band DTMF (if present) from the agent leg RTP, and replaces with mono tones (i.e., not the actual digits entered by customer) and sends them along with RTP. Mono tones are sent to agents for informational purposes only to inform them that the customer has entered digits.

After the payment has been successfully processed, PCI Pal Agent Assist redirects the RTP back to Avaya SBCE by sending re-INVITEs for both call legs.



2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between a customer, via the VoIP Service Provider, and agents in an Avaya contact center, and routing calls through PCI Pal Agent Assist. Agents then enter a PIN supplied by the PCI Pal Portal to secure the call and allow cardholder/payment information to be redirected to PCI Pal Agent Assist. Compliance testing also entailed verifying DTMF transmission in both directions by navigating the menu of an IVR application or voicemail system. In addition, agents exercised various telephony features before and after calls were secured and unsecured.

The serviceability test cases focused on failover scenarios where the primary PCI Pal Agent Assist was unavailable and the call had to route to the secondary PCI Pal Agent Assist or both PCI Pal Agent Assist were unavailable and the call had to be routed directly to Session Manager.

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 and PCI Pal Agent Assist utilized encryption capabilities of TLS/SRTP.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP trunk between SBCE and Agent Assist using TLS transport and verifying the exchange of SIP OPTIONS messages.
- Inbound and outbound PSTN call via a VoIP Service Provider routed through Agent Assist using TLS/SRTP with Direct IP Media (Shuffling) and Initial IP-IP Direct Media enabled or disabled.
- DTMF transmission using RFC2833 to SBCE.
- Conversion of RFC2833 to SIP INFO by SBCE and vice versa.
- DTMF transmission using RFC2833 and SIP INFO with Agent Assist.

- RTP redirection from SBCE to Agent Assist after call is secured and card payment info is being sent.
- Agent enters PIN using DTMF (telephone keypad) and PIN is sent to Agent Assist via SIP INFO. DTMF using RFC2833 is redirected from SBCE to Agent Assist to secure call. Payment info is sent only to Agent Assist (i.e., agent doesn't receive DTMF).
- Multiple payments processed by a single agent on one call.
- Multiple payments processed by multiple agents simultaneously.
- Inbound calls from VoIP Service Provider to IVR to verify successful navigation of menu using DTMF.
- Outbound calls that cover to voicemail to verify successful navigation of voicemail system using DTMF.
- G.711mu-law codec support.
- Telephony features, such as call hold/resume, call transfer, conference, call forwarding, call coverage, and queuing calls to split to ensure proper operation after call is secured and unsecured.
- Failover scenarios between primary and secondary Agent Assist when one is unavailable and routing calls directly to Session Manager when both Agent Assist aren't available.

2.2. Test Results

All test cases passed with the following observation:

- The call legs between (1) SBCE and Session Manager and (2) SBCE and Agent Assist must use different SRTP ciphers to trigger a change in SRTP encryption keys, which helps SBCE decrypt the DTMF signals. For example, one call leg may use srtp-aescm128-hmac80 while the other call leg may srtp-aescm128-hmac32. If the ciphers are the same for both call legs, the SIP INFO messages, which are supposed to deliver the DTMF digits (PIN) provided by the contact center agent to secure the call, may contain a blank Signal header instead of a DTMF digit. When this occurs the call cannot be secured.

2.3. Support

Technical support on PCI Pal Agent Assist can be obtained through the following:

- **Phone:** US: +1 866 645 2903 (Charlotte, NC)
UK: +44 207 030 3770 (London) or +44 330 131 0330 (Ipswich)
- **Web:** www.pcipal.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of redundant PCI Pal Agent Assist in an Avaya Aura® environment. All SIP calls between the VoIP Service Provider and the Avaya Aura® environment were routed from SBCE to PCI Pal Agent Assist, and then to Session Manager or VoIP Service Provider, depending on the call direction. The Avaya Aura® environment consisted of the following products:

- SBCE with SIP trunk connectivity to Session Manager, PCI Pal Agent Assist, and VoIP Service Provider.
- Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP endpoints.
- Media resources in Avaya G450 Media Gateway and Avaya Aura® Media Server.
- System Manager used to configure Session Manager.
- Experience Portal to provide access to IVR applications.
- Avaya 96x1 Series H.323 Deskphones and Avaya J100 Series SIP Phones.

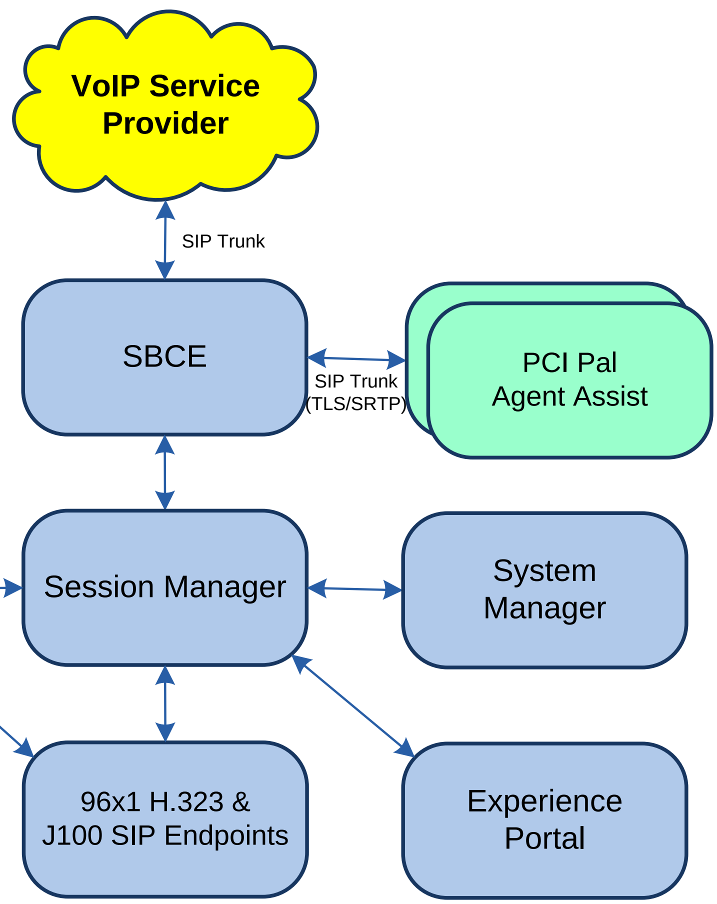


Figure 1: Avaya Aura® Environment with PCI Pal Agent Assist

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	10.1.0.1.0-SP1
Avaya G450 Media Gateway	FW 42.4.0
Avaya Aura® Media Server	v.10.1.0.77
Avaya Aura® System Manager	10.1.0.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.1.061394 Service Pack 1
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Aura® Experience Portal	8.1.1.0.0251
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya 96x1 Series IP Deskphones	6.8511 (H.323)
Avaya J100 Series IP Phones	4.0.10.3.2 (SIP)
PCI Pal® Agent Assist	2022.707.166.8421

5. Configure Avaya Aura® Communication Manager

For this solution, Communication Manager provides a contact center whose agents communicate with customers to collect payment information using Agent Assist. The configuration of the contact center, including agents, skill/hunt group, vectors, and VDNs are outside the scope of these Application Notes, but note that customer calls were placed to a VDN, which pointed to a vector that queued the call to a split/hunt group, and eventually routed the call to an available agent or queued the call. Customer calls were routed from the VoIP Service Provider to SBCE, SBCE looped the SIP signaling through Agent Assist, and then the call was routed to Session Manager and finally to Communication Manager. Outbound agent calls followed the same call path, but in reverse order.

This section covers the configuration steps required to establish a SIP trunk between Communication Manager and Session Manager and routing calls to/from the VoIP Service Provider. Communication Manager is configured through the System Access Terminal (SAT). The procedures include the following areas:

- Verify Licenses
- Administer IP Node Names
- Administer IP Codec Set
- Administer IP Network Region
- Administer SIP Trunk Group to Session Manager
- Administer Private Numbering
- Administer AAR Call Routing
- Administer Route Pattern
- Administer Incoming Call Treatment

5.1. Verify Licenses

Using the SAT, enter the **display system-parameters customer-options** command to verify there is sufficient capacity for SIP trunks on **Page 2**. The license file installed on the system controls these options. If there is insufficient capacity of SIP trunks or a required feature is not enabled, contact an authorized Avaya sales representative.

```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                          USED
                 Maximum Administered H.323 Trunks: 12000      0
       Maximum Concurrently Registered IP Stations:  2400      2
         Maximum Administered Remote Office Trunks: 12000      0
Max Concurrently Registered Remote Office Stations:  2400      0
          Maximum Concurrently Registered IP eCons:  128       0
     Max Concur Reg Unauthenticated H.323 Stations:   100      0
                    Maximum Video Capable Stations:  36000     2
               Maximum Video Capable IP Softphones:   2400     2
                   Maximum Administered SIP Trunks: 12000     20
  Max Administered Ad-hoc Video Conferencing Ports: 12000      0
   Max Number of DS1 Boards with Echo Cancellation: 688    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 to be used by Agent Assist. The form is accessed via the **change ip-codec-set 2** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, *G.711MU* was used. In addition, configure **Media Encryption** and **Encrypted SRTCP** as shown below.

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

                          IP MEDIA PARAMETERS
    Codec Set: 2

    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: none
 3:
 4:
 5:
```

5.4. Administer IP Network Region

In the **IP Network Region** form, specify the codec set to be used for Agent Assist and enable **IP-IP Direct Audio** (shuffling), if desired. Shuffling allows audio traffic to be sent directly between IP endpoints and SBCE without using media resources in the Avaya G450 Media Gateway or Avaya Aura® Media Server after call establishment. For this compliance test, shuffling was enabled. The **Authoritative Domain** for this configuration is *avaya.com*.

```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2       NR Group: 2
Location: 1       Authoritative Domain: avaya.com
    Name: To Avaya SBCE         Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
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*.
- Specify Communication Manager (*procr*) and the Session Manager (*devcon-sm*) 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 *5062* 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 **DTMF over IP** field should be set to the default value of *rtp-payload*.
- **Direct IP-IP Audio Connections** is enabled to allow shuffling for calls routed over the trunk group associated with this signaling group.
- **Initial IP-IP Direct Media** may be enabled or disabled.

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

```
add signaling-group 11                                     Page   1 of   2
                                SIGNALING GROUP

 Group Number: 11              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? n        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: 5062                Far-end Listen Port: 5062
                                        Far-end Network Region: 2

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? y
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 the VoIP Service Provider. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie* or *public-ntwk*, 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. Accept the default values for the remaining fields.

```
add trunk-group 11                                          Page   1 of   5
                                TRUNK GROUP

Group Number: 11                   Group Type: sip          CDR Reports: y
  Group Name: To SIP Service Provider     COR: 1        TN: 1        TAC: 1011
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 11
                                                     Number of Members: 10
```

On **Page 3** of the trunk group form, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number sent to the far-end.

```
add trunk-group 11                                          Page   3 of   5
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no
               Send UCID? n



 Show ANSWERED BY on Display? y
```

On **Page 5** of the trunk group form, the default settings were used as shown below.

```
add trunk-group 11                                            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. Administer Private Numbering

Configure the **Numbering – Private Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with '7' whose calls are routed over trunk group 11 have their extension converted to a 11-digit number.

```
change private-numbering 0                                       Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext                 Trk         Private          Total
Len Code                Grp(s)      Prefix           Len
 5  7                                                5  Total Administered: 2
 5  7                   11          173277           11    Maximum Entries: 540
```

5.7. Administer ARS Call Routing

Use the **change feature access code** command to define a feature access code for **Auto Route Selection (ARS)** per the dial plan**.** For the compliance test, *9* was used as the ARS Access Code.

```
change feature-access-codes                                    Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *11
                       Answer Back Access Code: *24

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *25    Deactivation: #25
Call Forwarding Activation Busy/DA: *21    All: *20    Deactivation: #20
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: *26
                       Call Pickup Access Code: *27
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code: *39
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

SIP calls destined for the VoIP Service Provider are routed through Session Manager over a SIP trunk via ARS call routing. Configure the ARS analysis form and add an entry that routes digits beginning with “1908” to route pattern 12 as shown below.

```
change ars analysis 19                                         Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    190                   11   11    4        fnpa         n
    1900                  11   11    deny     fnpa         n
    1900555               11   11    deny     fnpa         n
    1908                  11   11    12       fnpa         n
```

5.8. Administer Route Pattern

Configure a preference in **Route Pattern** 12 to route calls over SIP trunk group 11 as shown below.

```
change route-pattern 12                                         Page   1 of   4
                    Pattern Number: 12     Pattern Name: Twilio
    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: 11   0       1                                                      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
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

5.9. Administer Incoming Call Treatment

Incoming calls from the VoIP Service Provider use a DID number beginning with "+1720". Use the **change inc-call-handling-trmt trunk-group** command to convert the DID number to the VDN that routes calls to an agent in the contact center.

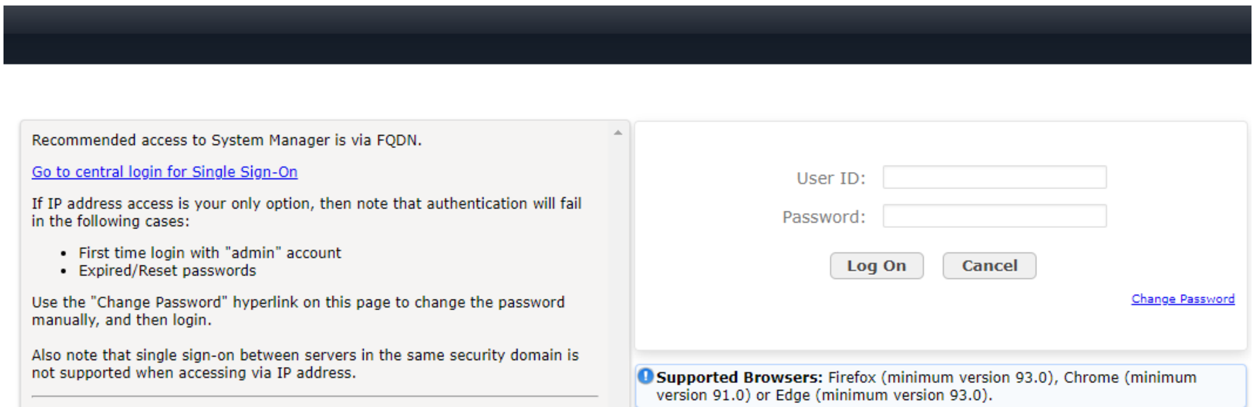
```
change inc-call-handling-trmt trunk-group 11                    Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature         Len      Digits
 public-ntwrk    12 +1720            all 77550
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedure includes adding the following items:

- Adaptation
- SIP Entities for Communication Manager and SBCE
- Entity Links, which defines the SIP trunk parameters used by Session Manager when routing calls to/from Communication Manager and SBCE
- Routing Policies and Dial Patterns
- Session Manager, corresponding to the Avaya Aura® Session Manager server to be managed by Avaya Aura® System Manager

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL **https://<*ip-address*>/SMGR**, where **<*ip-address*>** is the IP address of System Manager. Log in with the appropriate credentials.

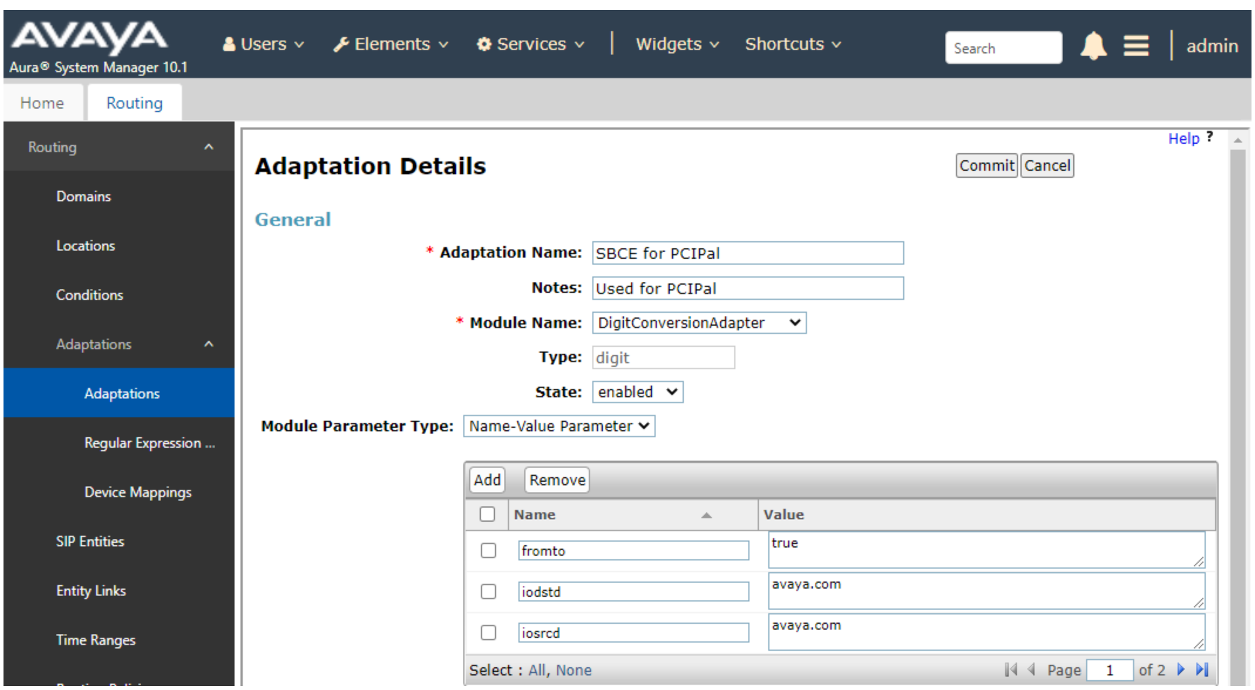


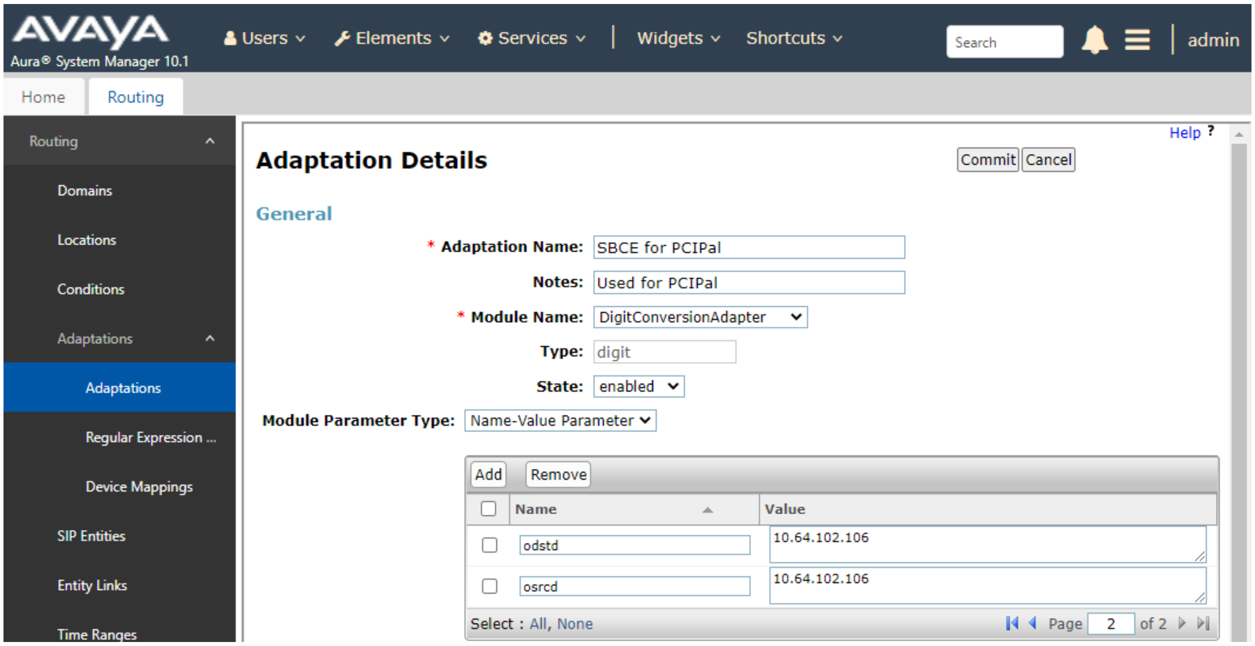
6.1. Add Adaptation

Session Manager can be configured with Adaptations that can modify SIP messages before or after routing decisions have been made; for example, replacing a domain name with a different value as shown in this section. Note that the following Adaptation replaces the domain in the To and From header to the IP address of the SBCE internal interface. This allows SBCE to identify calls that should route through Agent Assist (i.e., if domain matches SBCE internal interface, then route call through Agent Assist). Session Manager should route all other calls, which should not route through Agent Assist, to a different SBCE SIP entity without this Adaptation assigned to it.

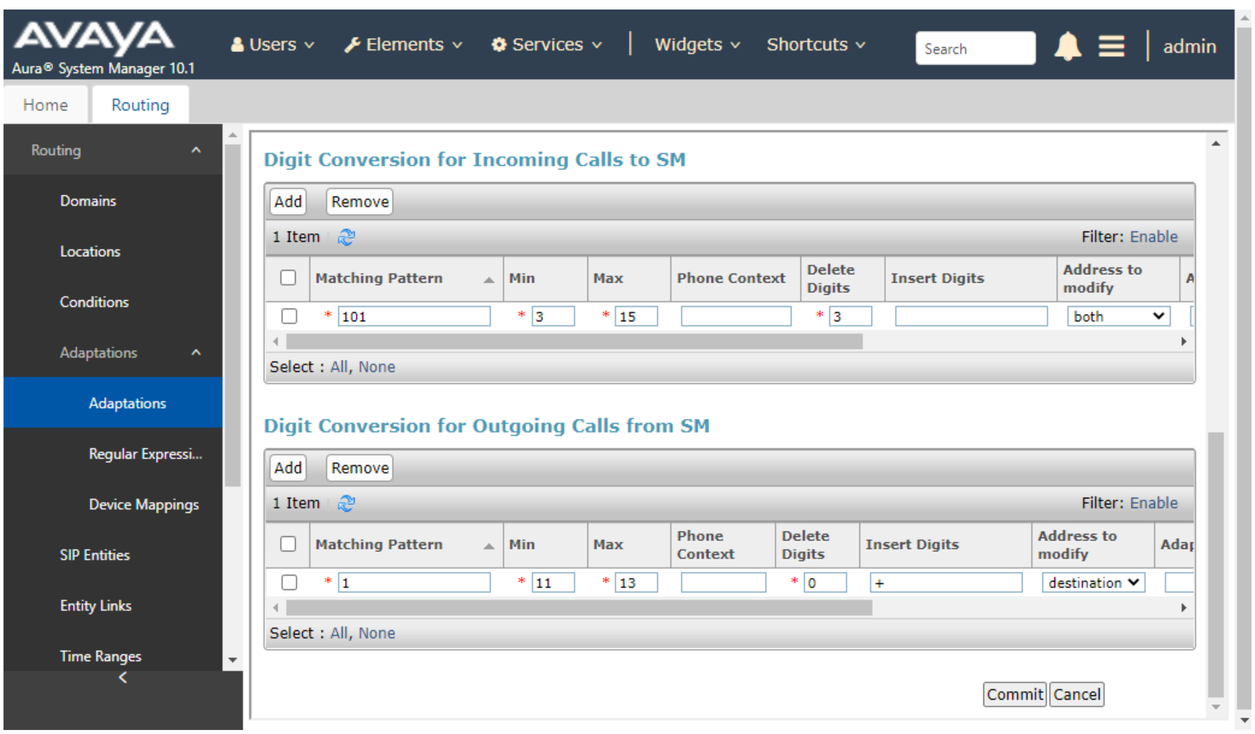
To create an **Adaptation** that will be applied to the SBCE SIP entity in **Section 6.2.2**, navigate to **Elements → Routing → Adaptations** and click on the **New** button (not shown). In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation Name:** Enter a descriptive name for the Adaptation (e.g., *SBCE for PCIPal*).
- **Module Name:** Select *DigitConversionAdapter*.
- **Module Parameter Type:** Select *Name-Value Parameter*. The section will expand with an area to enter **Name** and **Value** pairs. Click **Add**. Set **fromto** to *true* to allow the From and To headers to be modified. Set **iodstd** and **iosrcd** to *avaya.com* to replace the ingress domain name with *avaya.com*. Set **odstd** and **osrcd** to *10.64.102.106* to replace the egress domain name with the IP address of the SBCE interface connected to Session Manager.





For inbound calls from the VoIP Service Provider, Agent Assist will prepend *101* to the dialed number to steer the call towards Session Manager on SBCE. In this Adaptation, the 101 is removed as shown below. For outbound calls to the VoIP Service Provider a '+' is prepended to the dialed number as expected by the VoIP Service Provider.



6.2. Add SIP Entities

In the sample configuration, two SIP Entities were added for Communication Manager and SBCE. This section also covers the configuration of the Entity Links.

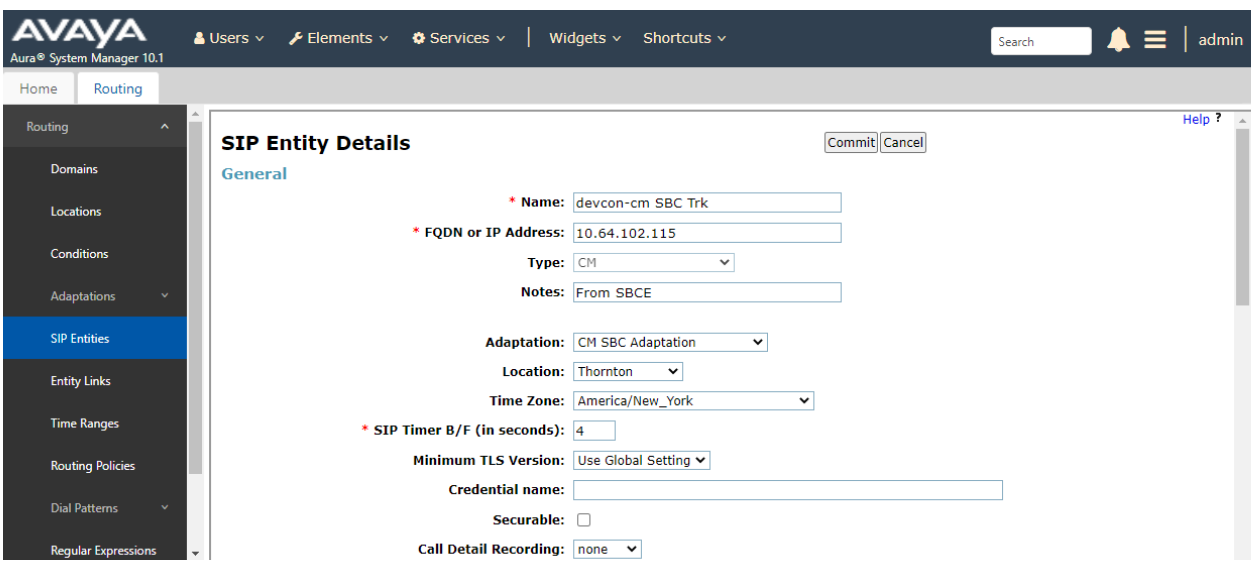
6.2.1. Avaya Aura® Communication Manager

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.

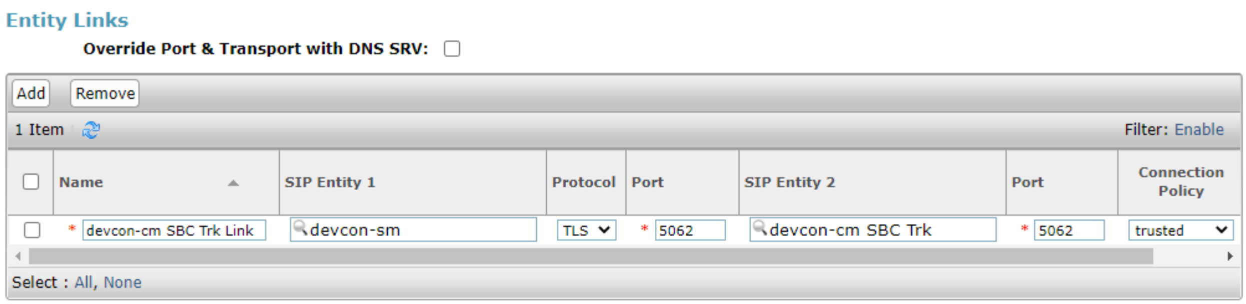
- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., procr) on Communication Manager.
- **Type:** Select *CM*.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

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-cm SBC Trk Link*).
- **Protocol:** Set to *TLS*.
- **Port:** Set to *5062*.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** Set to *5062*.
- **Connection Policy:** Set to *trusted*.

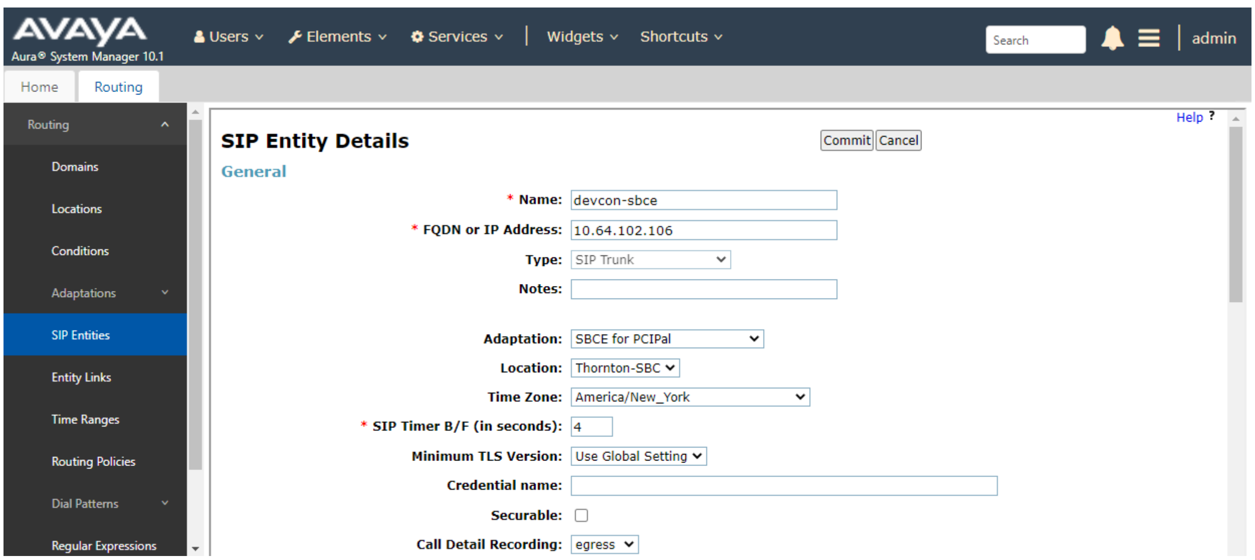


6.2.2. SIP Entity for SBCE

A SIP Entity must be added for SBCE. 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 SBCE.

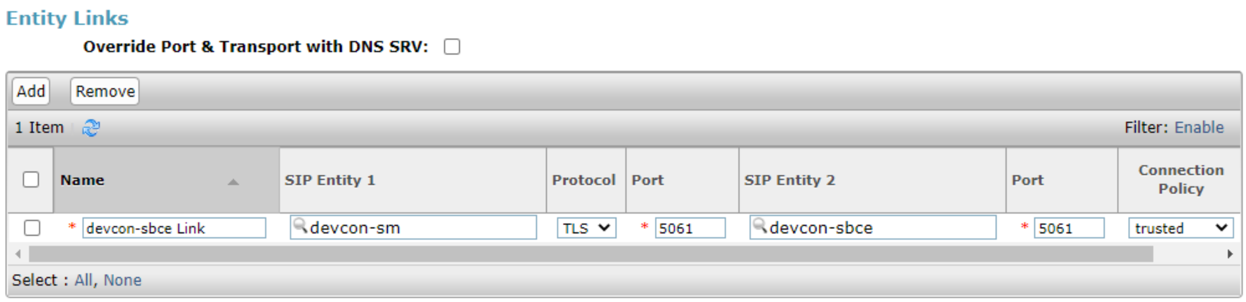
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the SBCE internal interface.
- **Type:** Select *SIP Trunk*.
- **Adaptation :** Select the Adaptation configured in **Section 6.1**.
- **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*.
- **Port:** Set to *5061*.
- **SIP Entity 2:** The SBCE entity name from this section.
- **Port:** Set to *5061*.
- **Connection Policy:** Set to *trusted*.



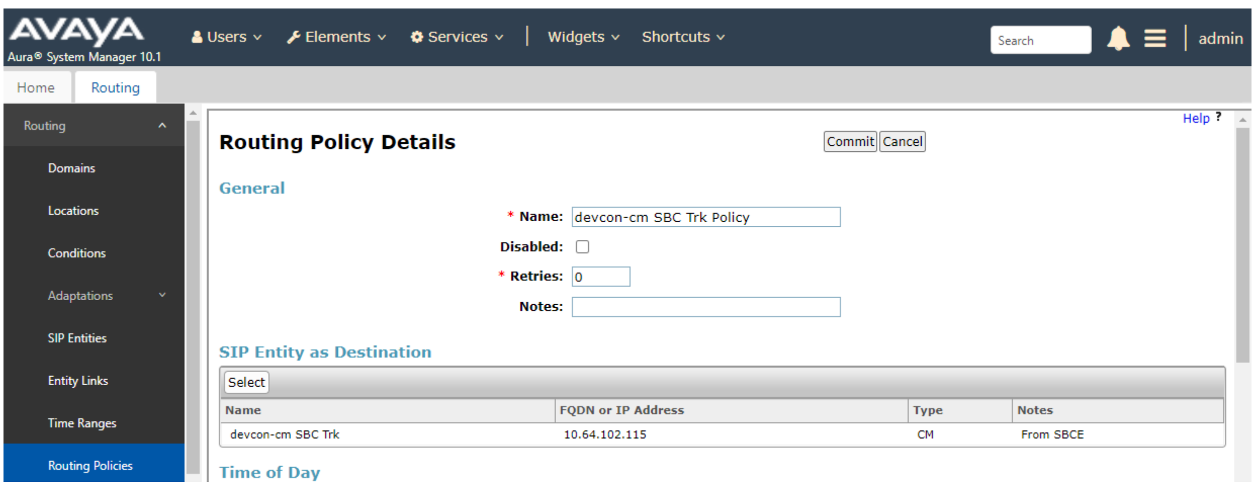
6.3. Add Routing Policies

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 Communication Manager to route incoming calls from the VoIP Service Provider. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

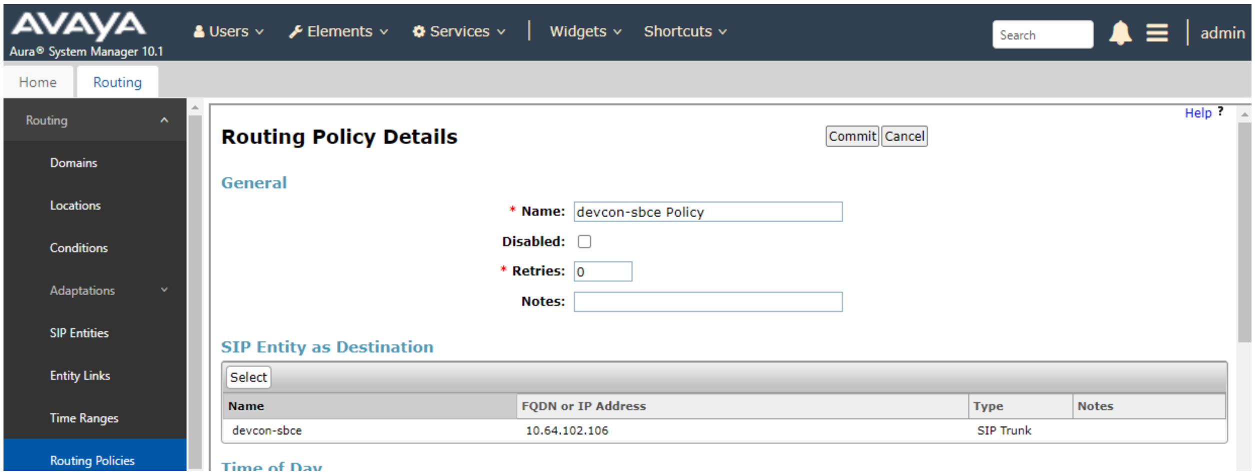
Under *General*:
Enter a descriptive name in **Name**.

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

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition. The following screen shows the Communication Manager Policy.



Another routing policy was added for SBCE, which routes outgoing calls to the VoIP Service Provider.



6.4. Add Dial Patterns

Dial patterns are defined to direct calls to the appropriate SIP Entity. In the sample configuration, numbers beginning with *+1* are routed to Communication Manager.

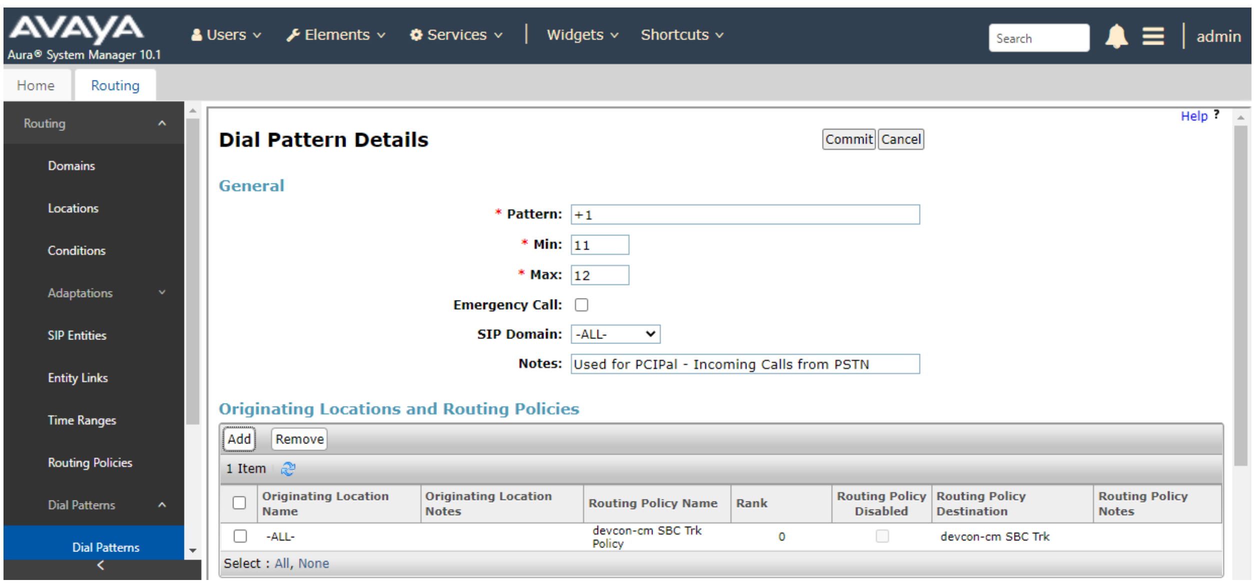
To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

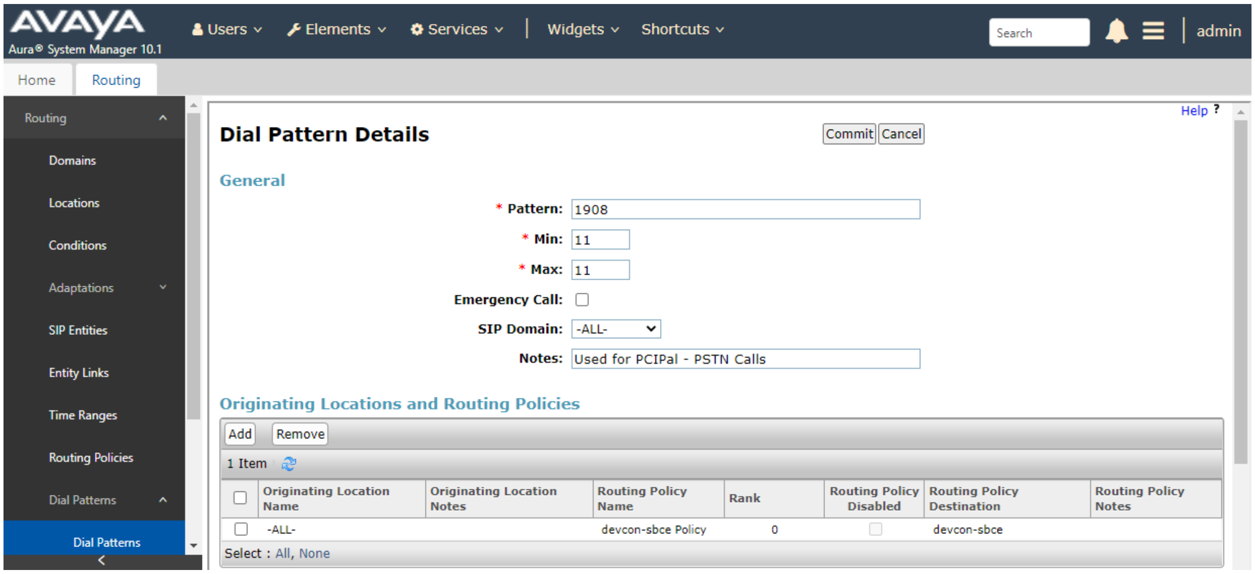
- **Pattern:** Dialed number or prefix.
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **SIP Domain:** SIP domain of dial pattern.
- **Notes:** Comment on purpose of dial pattern (optional).

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 Communication Manager.



A Dial Pattern was also created for 11-digit numbers beginning with *1908* that are routed to the SBCE as shown below.



6.5. Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

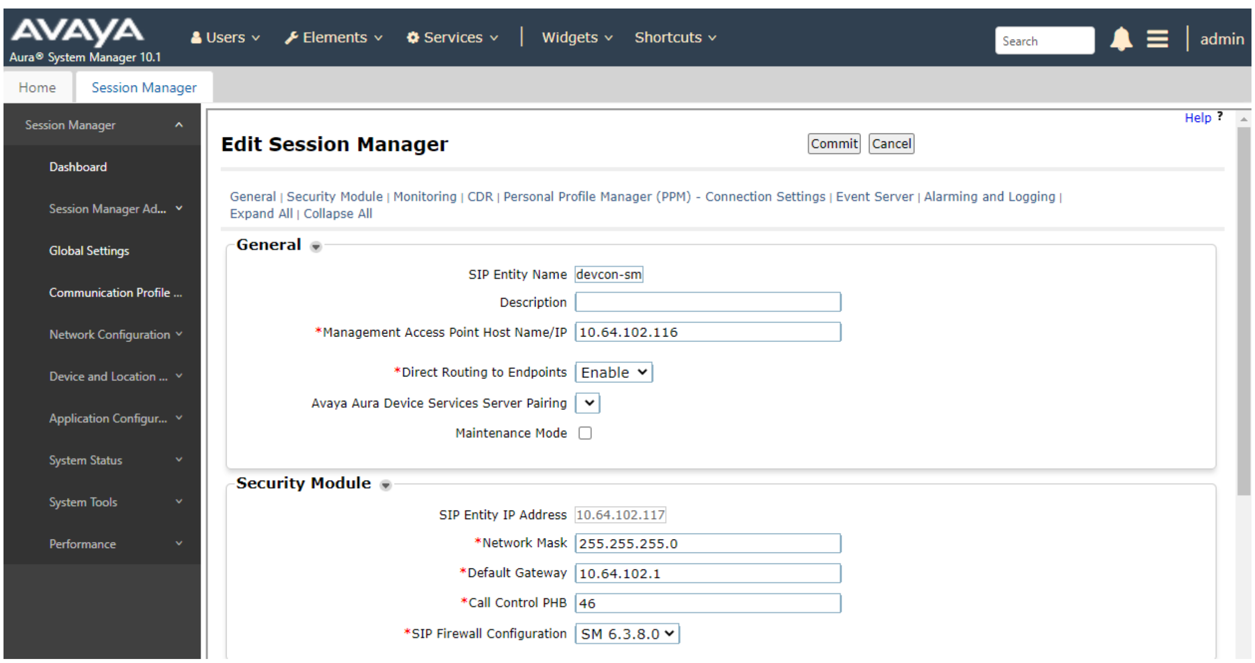
Under *General*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface

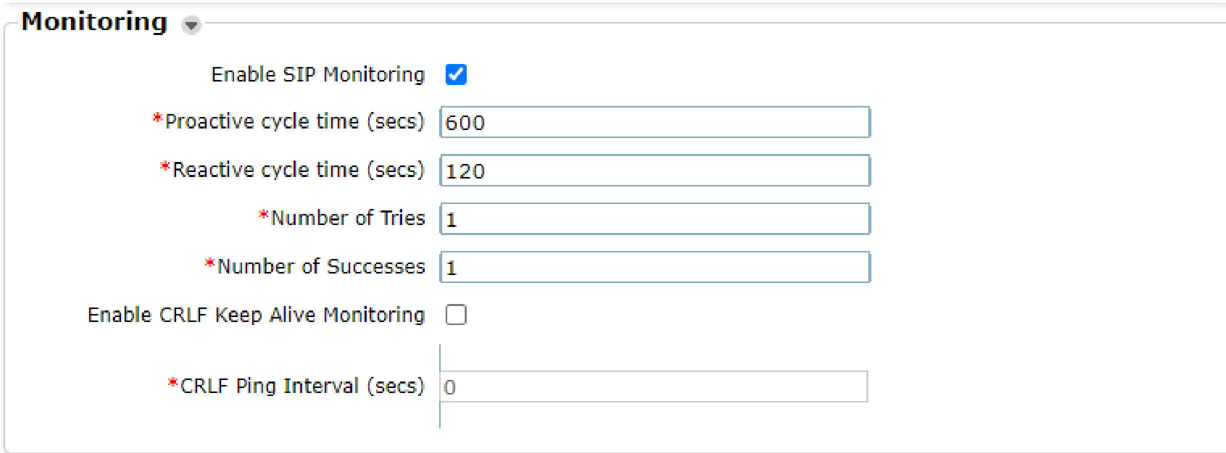
Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.



The following screen shows the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to SIP Entities, including SBCE. Use default values for the remaining fields. Click **Commit** to add this Session Manager. In the following configuration, Session Manager sends a SIP Options message every *600* secs. If there is no response, Session Manager will send a SIP Options message every *120* secs.



7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya SBCE. Avaya SBCE provides SIP connectivity to Session Manager, VoIP Service Provider, and PCI Pal Agent Assist.

This section covers the following SBCE configuration:

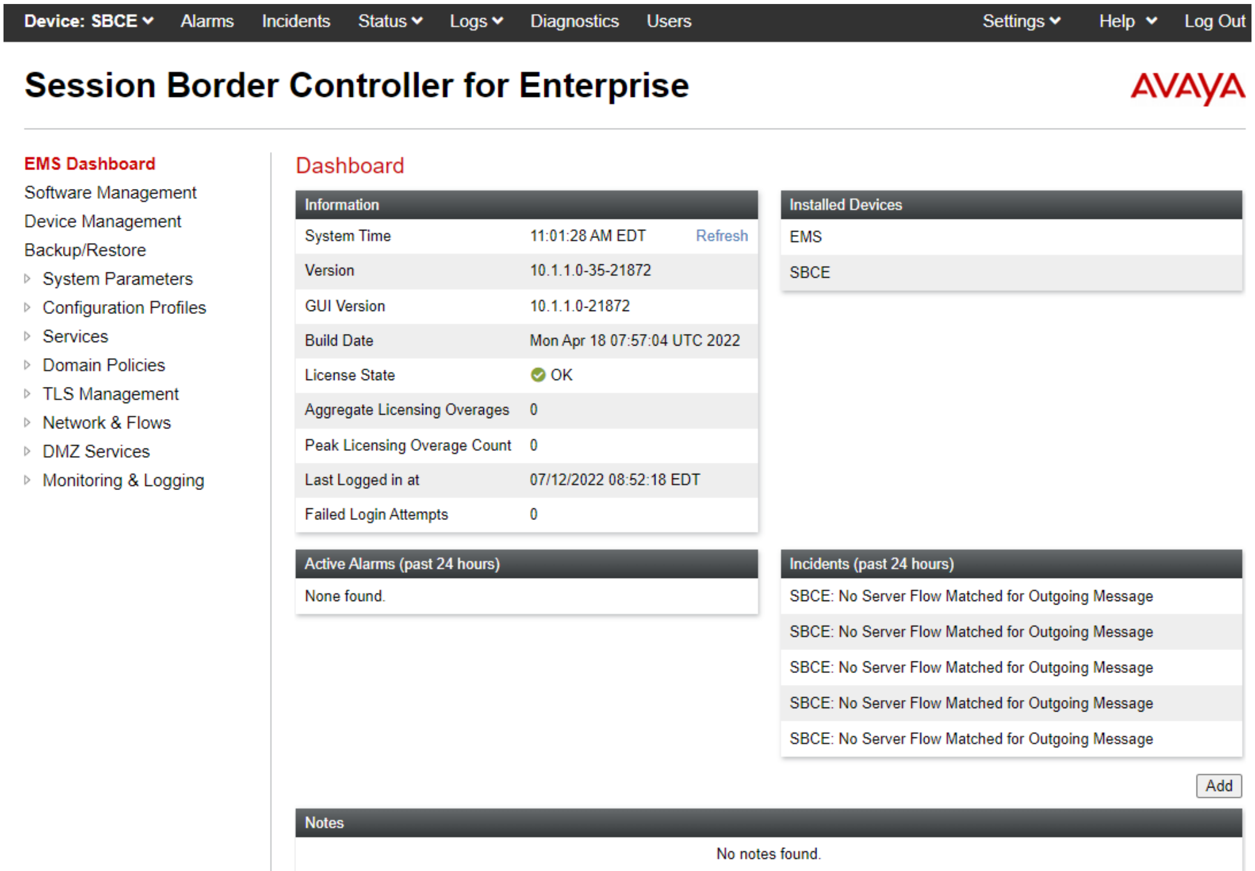
- Launch SBCE Web Interface
- Administer Server Interworking Profiles
- Administer SIP Servers
- Administer Routing Profiles
- Administer Signaling Manipulation Scripts
- Administer URI Groups
- Administer Media Rules
- Administer End Point Policy Groups
- Administer TLS Management
- Administer Media Interfaces
- Administer Signaling Interfaces
- Administer End Point Flows

Note: For security reasons, public IP addresses will be blacked out in these Application Notes.

7.1. Launch SBCE Web Interface

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

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

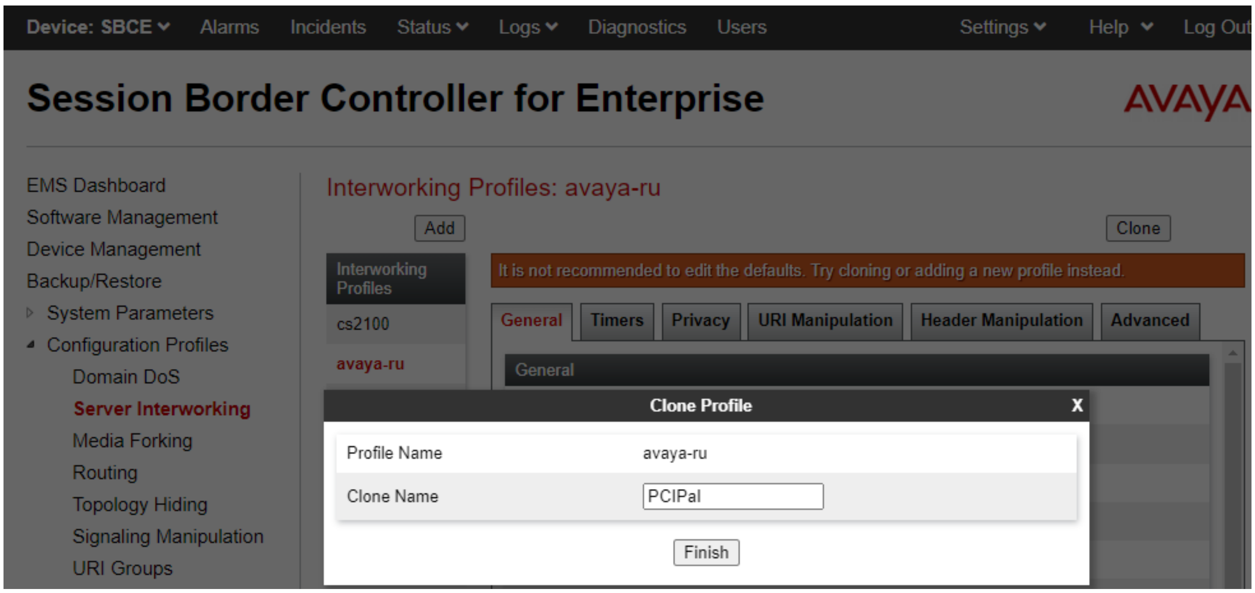


7.2. Administer Server Interworking Profiles

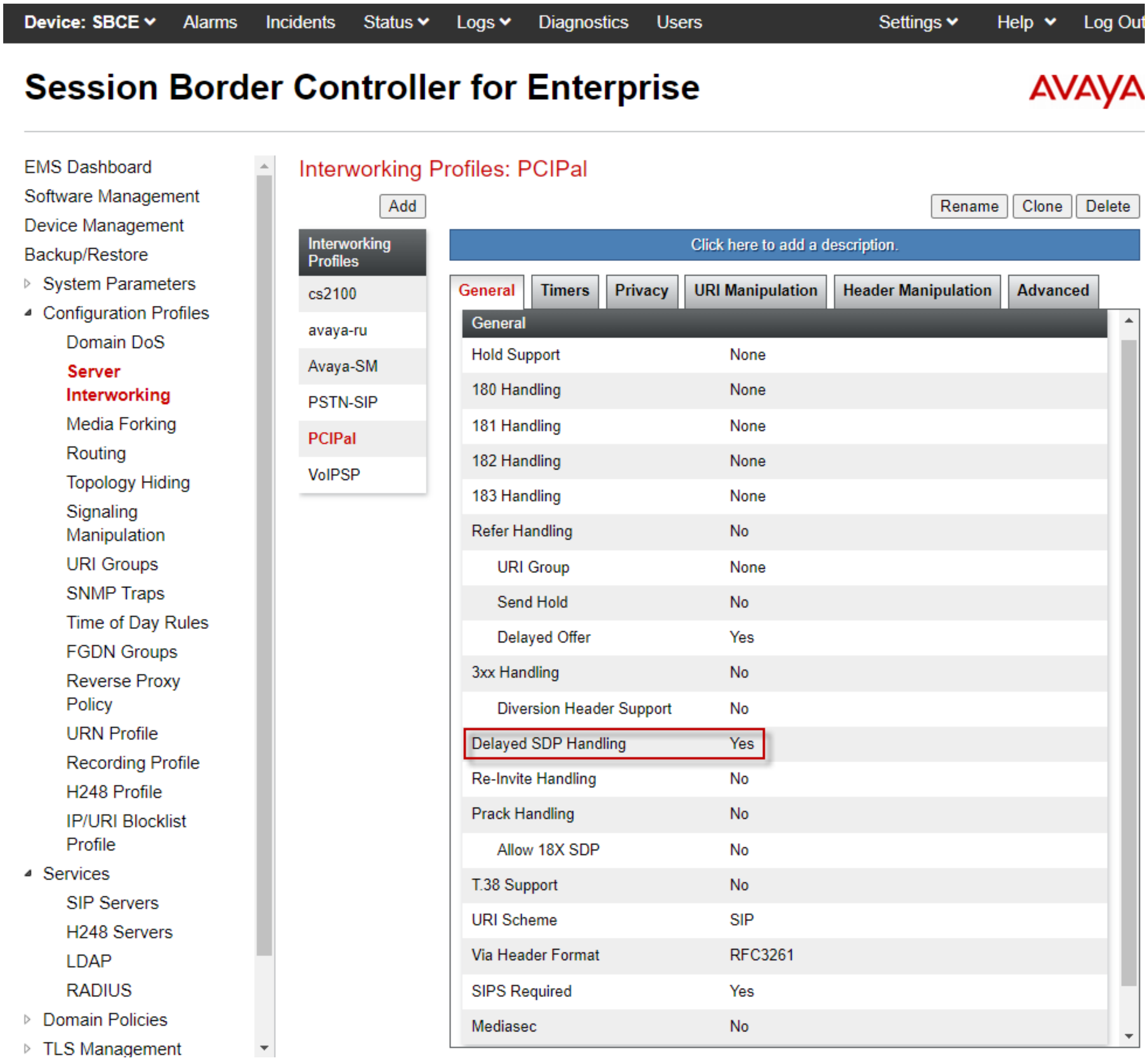
A server interworking profile defines a set of parameters that aid in interworking between the SBCE and a connected server. **Server Interworking** profiles were added for PCI Pal, Session Manager, and VoIP Service Provider.

7.2.1. Server Interworking Profile for PCI PAL Agent Assist

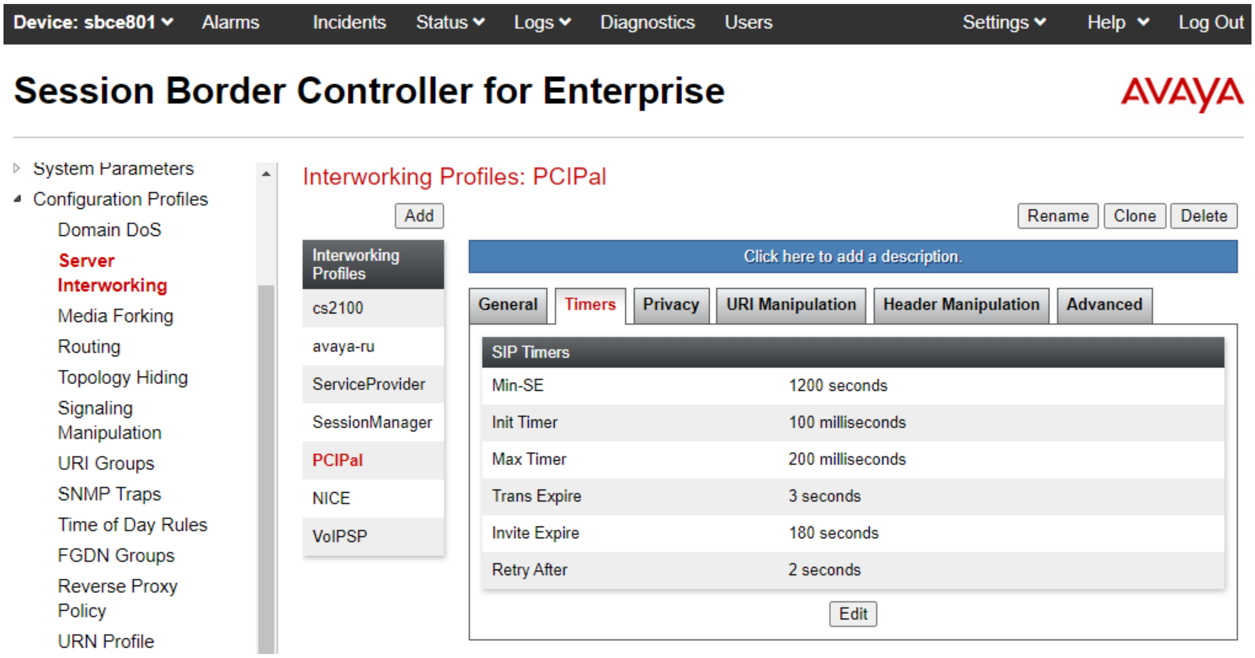
To create a new **Server Interworking** profile, select **Configuration Profiles → Server Interworking** from the left-hand menu. A new profile may be created by cloning an existing profile. Select the **avaya-ru** profile and click **Clone**. Type in a **Clone Name** for the PCI Pal profile. Select **Finish** once done.



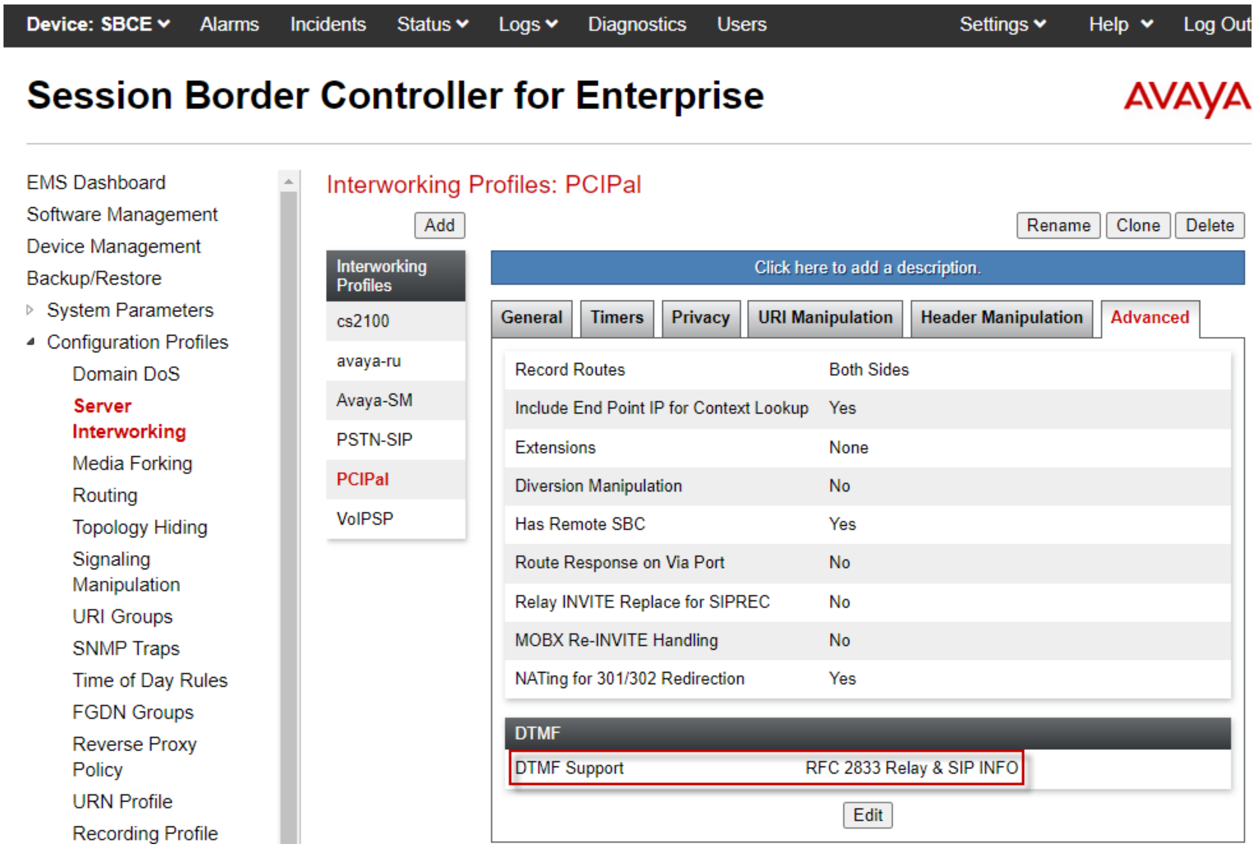
Once added, select the PCI Pal profile and select the **General** tab to modify it. Enable **Delayed SDP Handling**. When **Delayed SDP Handling** is enabled, SBCE will include SDP in a re-INVITE sent to Agent Assist. This is required because SBCE may receive a re-INVITE without SDP from Communication Manager to shuffle a call (i.e., Direct IP Media) or un-shuffle a call when a media resource is required to send a DTMF tone.



Select the **Timers** tab. For the compliance test, the following timers were configured.

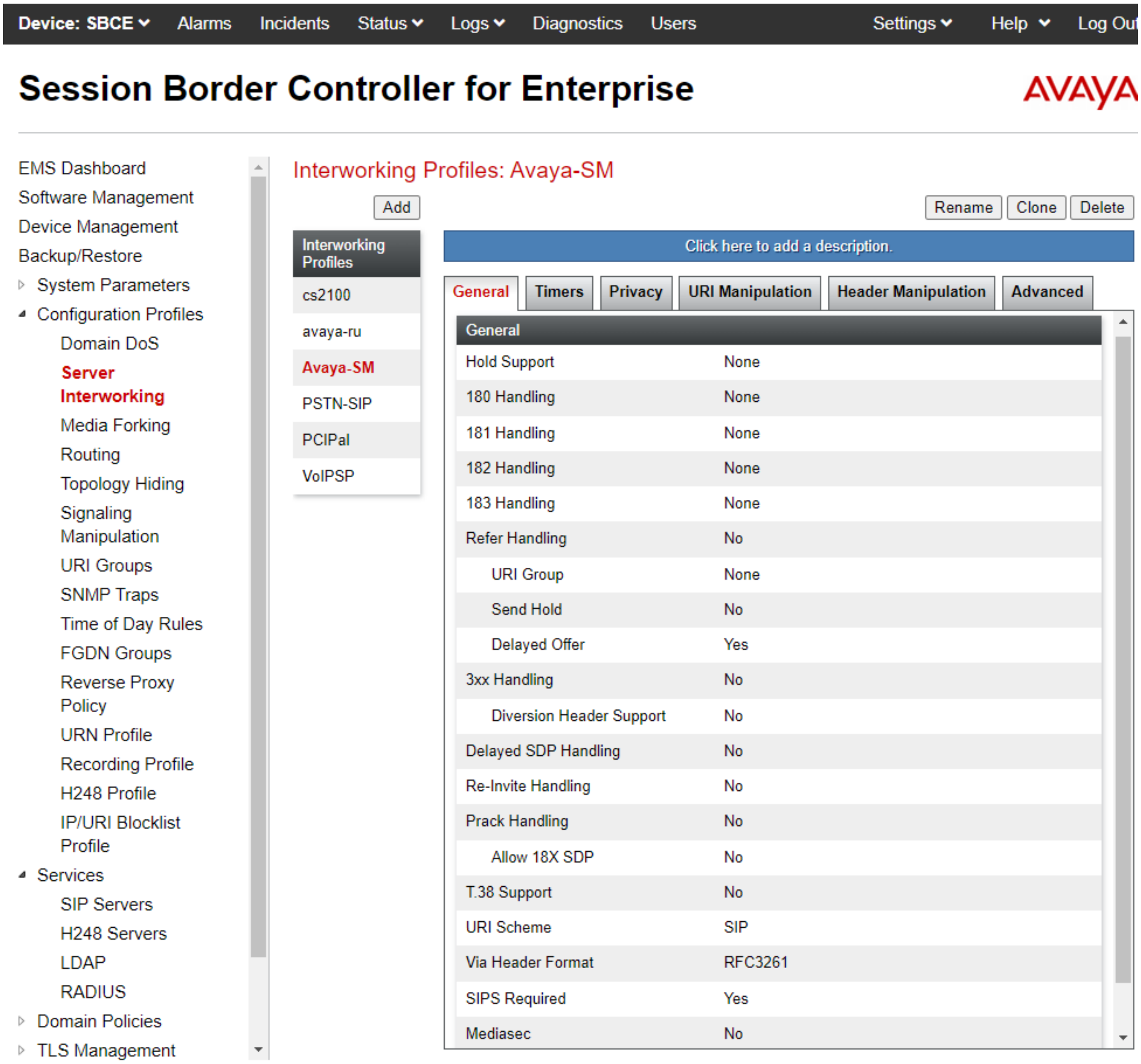


Select the **Advanced** tab and configure the fields as the screen capture below. Note that **DTMF Support** is set to *RFC 2833 Relay & SIP INFO***.** Agent Assist receives the PIN to secure the call using SIP INFO, and once the call is secured, card payment information is received using RFC2833.

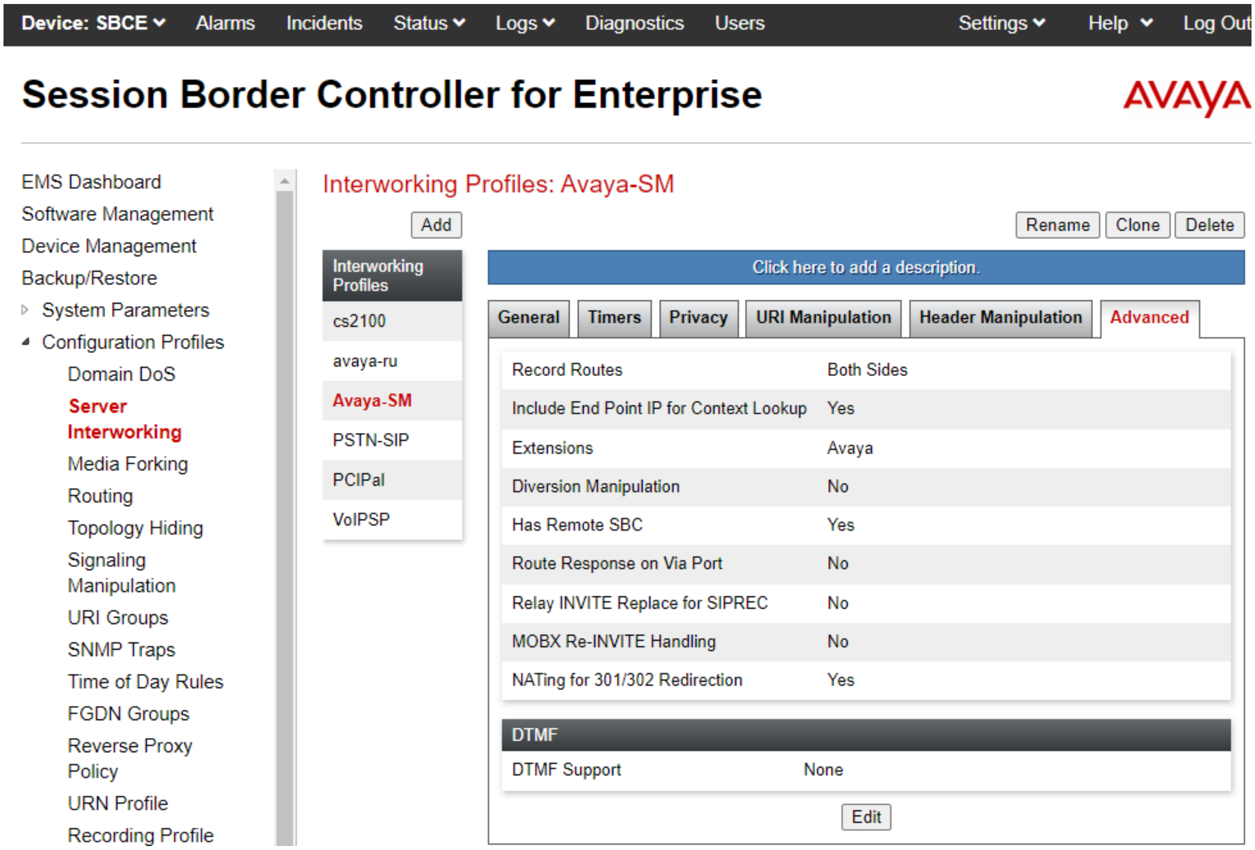


7.2.2. Server Interworking Profile for Session Manager

Session Manager profile was cloned from the same **avaya-ru** profile. The **General** tab below shows the default settings.

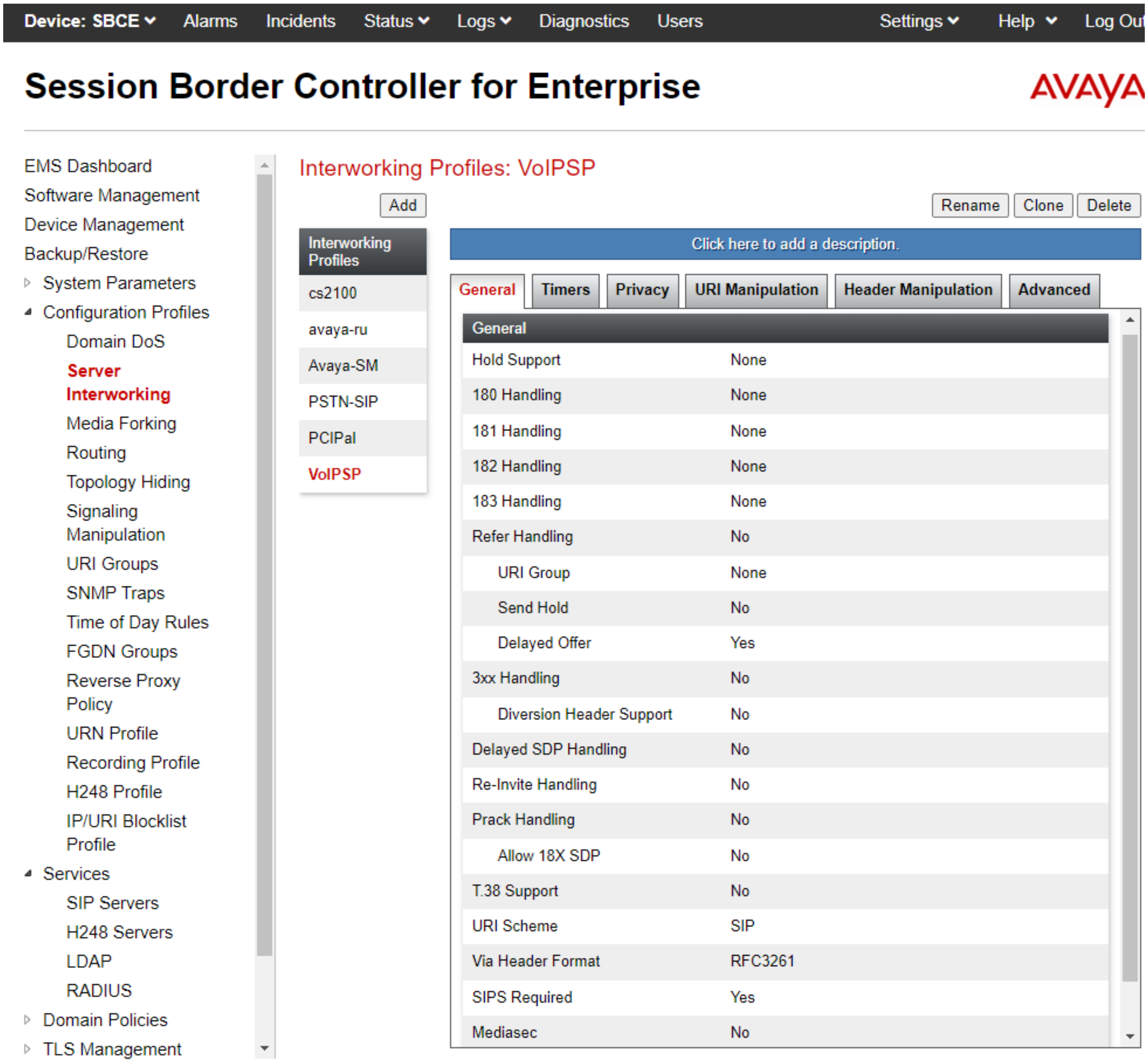


Select the **Advanced** tab and configure as shown in the screen capture below.

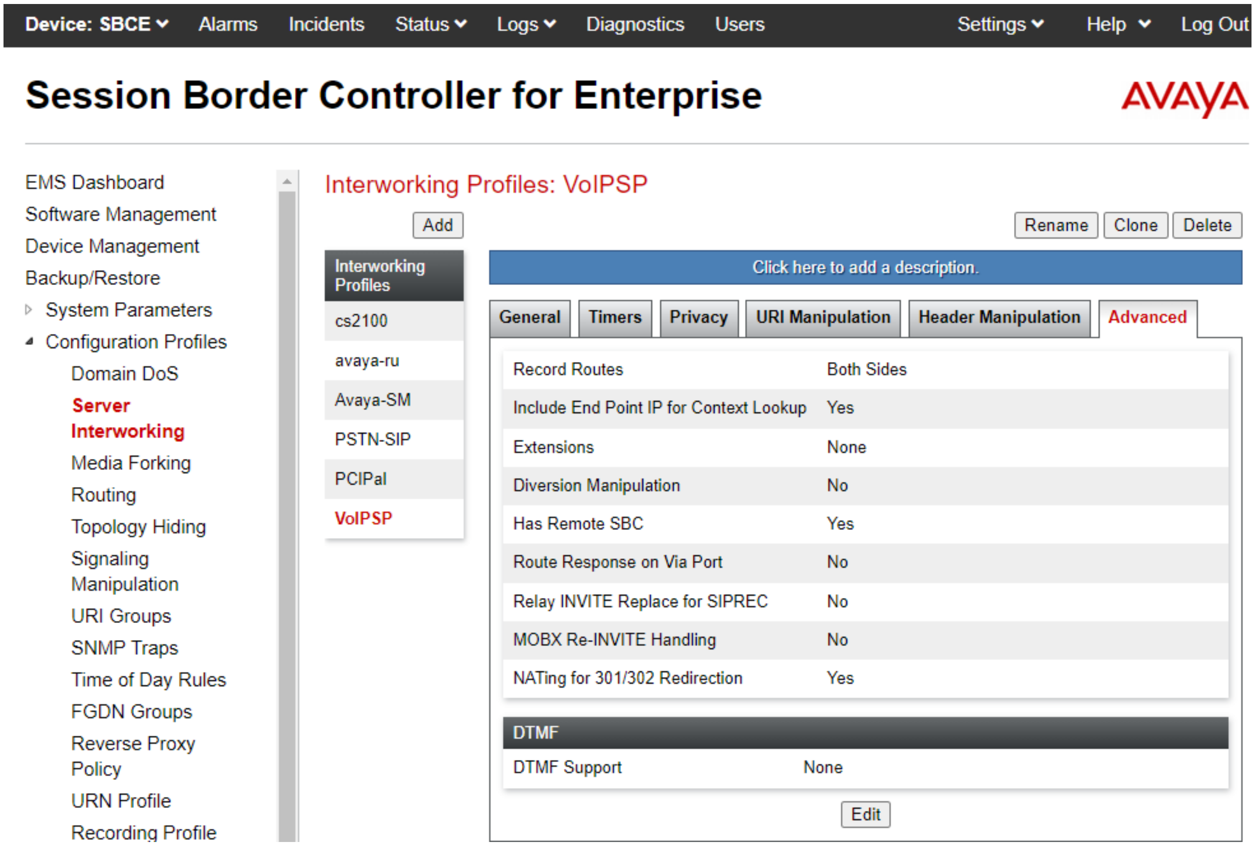


7.2.3. Server Interworking Profile for VoIP Service Provider

VoIP Service Provider profile was cloned from the same **avaya-ru** profile. The **General** tab below shows the default settings.



VoIP Service Provider profile was also cloned from the same **avaya-ru** profile. No changes were made to the cloned profile. The **Advanced** tab screen capture is shown below.



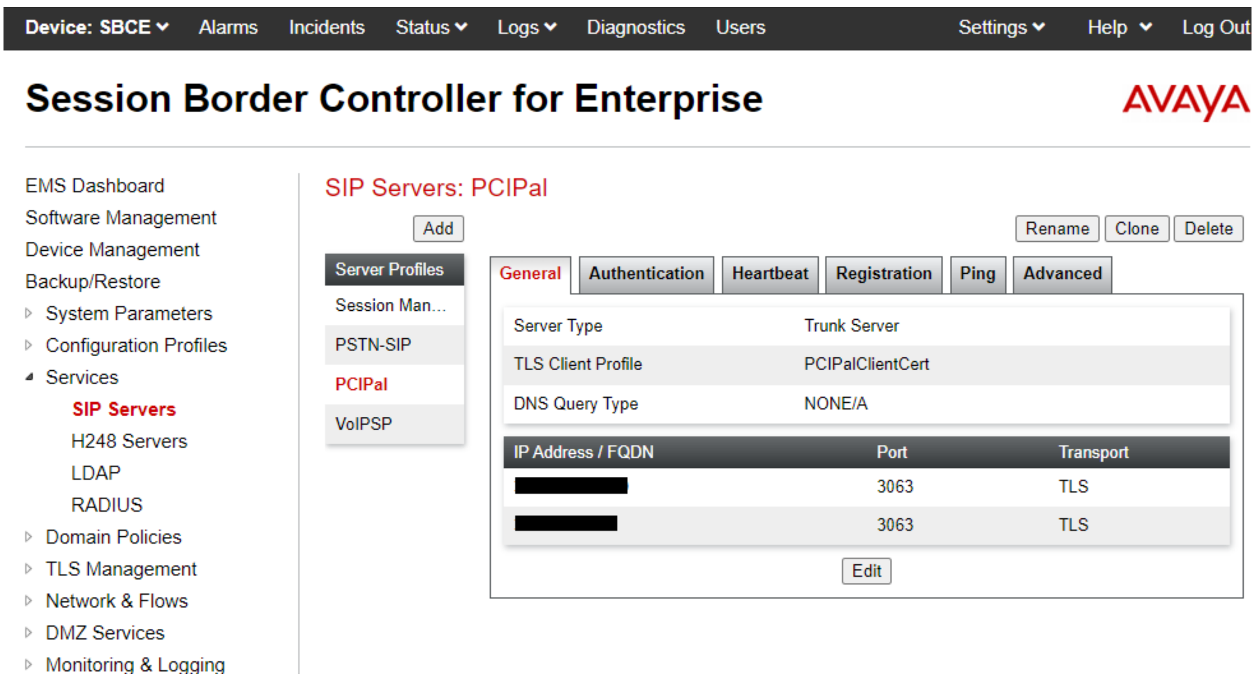
7.3. Administer SIP Servers

A SIP server definition is required for each server connected to SBCE. Add a **SIP Server** for Session Manager, PCI Pal Agent Assist, and VoIP Service Provider. TLS transport was used for the SIP trunks to Session Manager and PCI Pal Agent Assist.

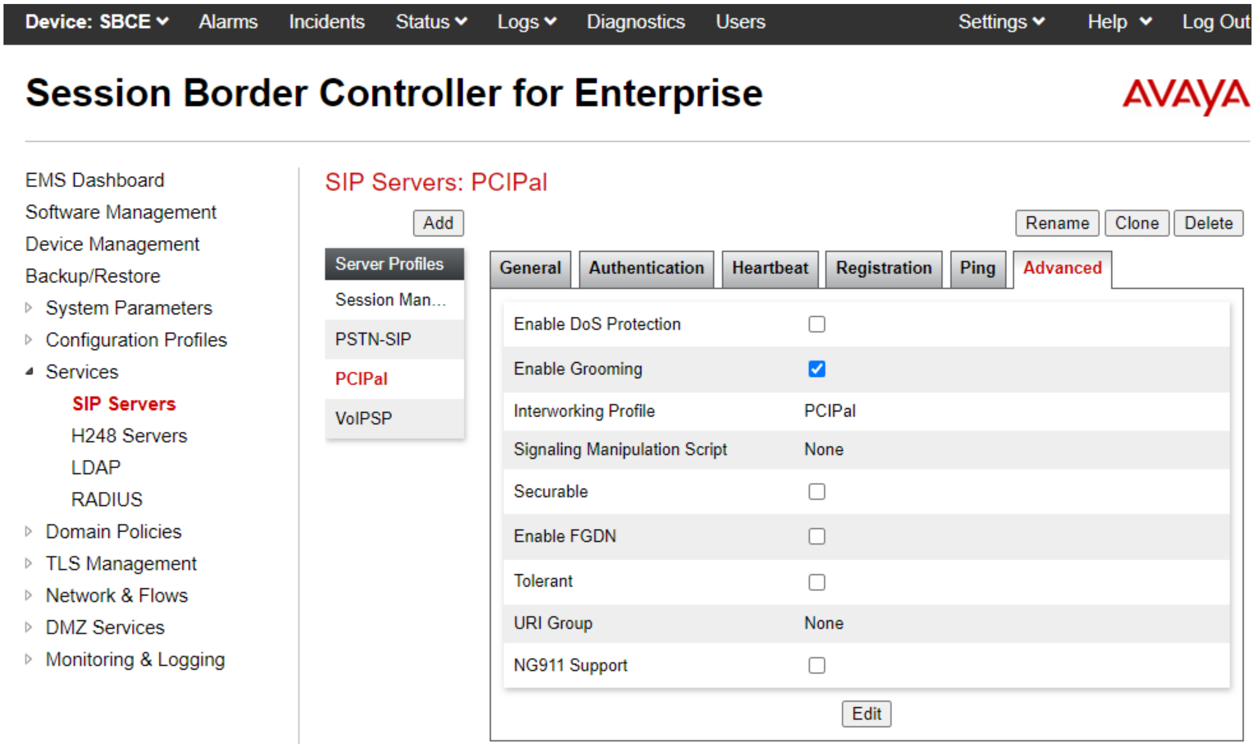
Note: TLS profiles were preconfigured for Session Manager and are not shown in these Application Notes. However, configuration of TLS profiles for PCI Pal Agent Assist are shown in **Section 7.9**.

7.3.1. SIP Server for PCI Pal Agent Assist

The **General** tab of the PCI Pal Agent Assist SIP Server was configured as shown below. TLS transport was used for the PCI Pal Agent Assist SIP trunk. The configuration of the **TLS Client Profile** is shown in **Section 7.9**. Note that a secondary PCI Pal Agent Assist was configured for redundancy and to test failover scenarios.

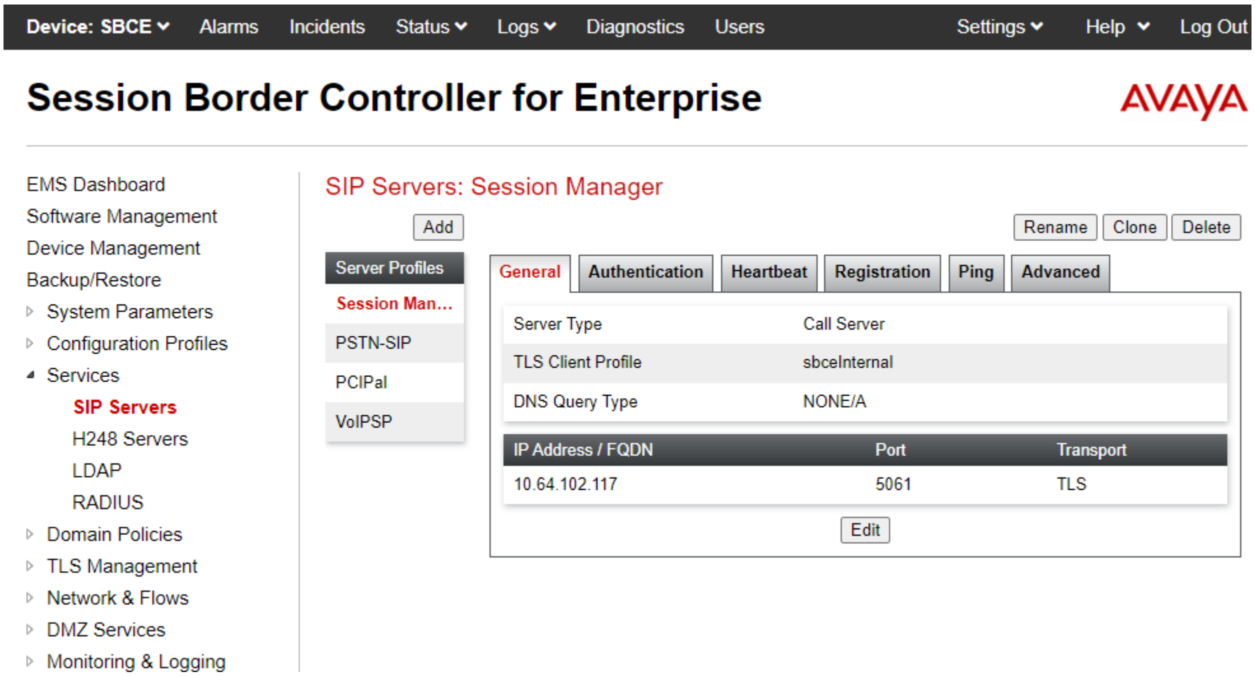


The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 7.2.1**. All other tabs were left with their default values.

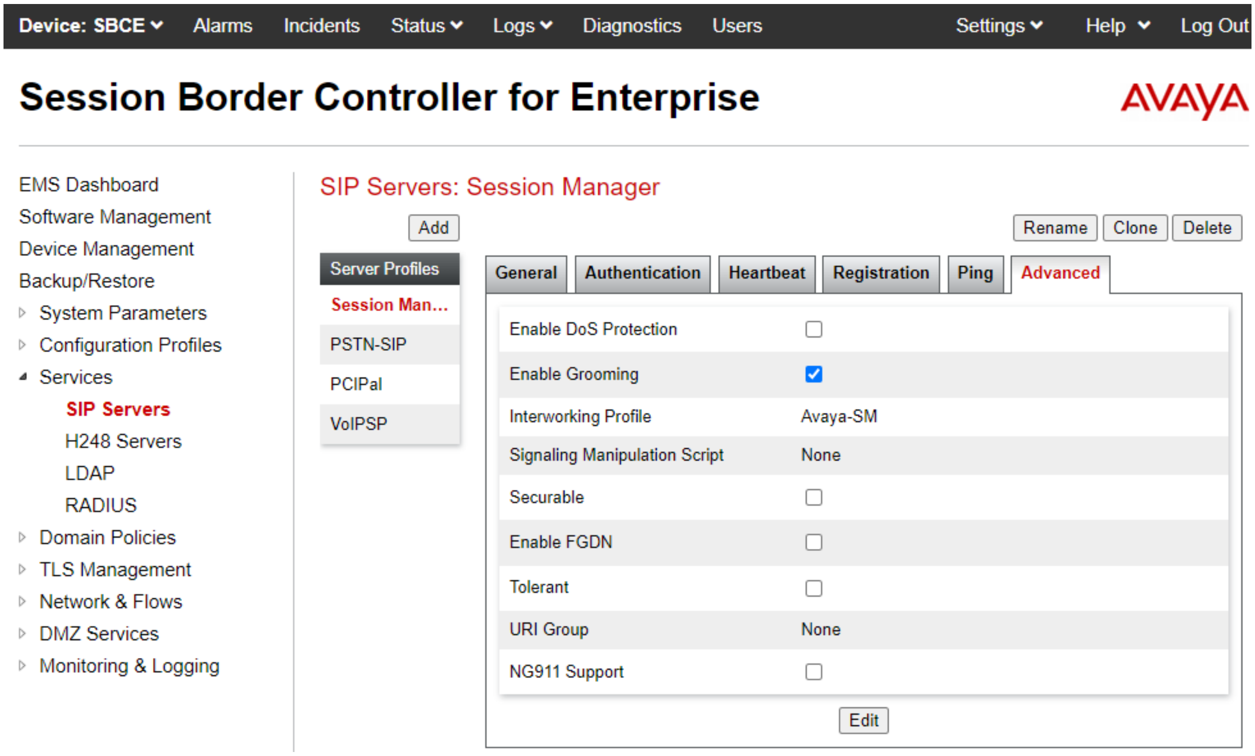


7.3.2. SIP Server for Session Manager

To define a SIP server, navigate to **Services** → **SIP Servers** from the left pane to display the existing SIP server profiles. Click **Add** to create a new SIP Server or select a pre-configured SIP server to view its settings. The **General** tab of the Session Manager SIP Server was configured as follows. TLS transport was used for the Session Manager SIP trunk.

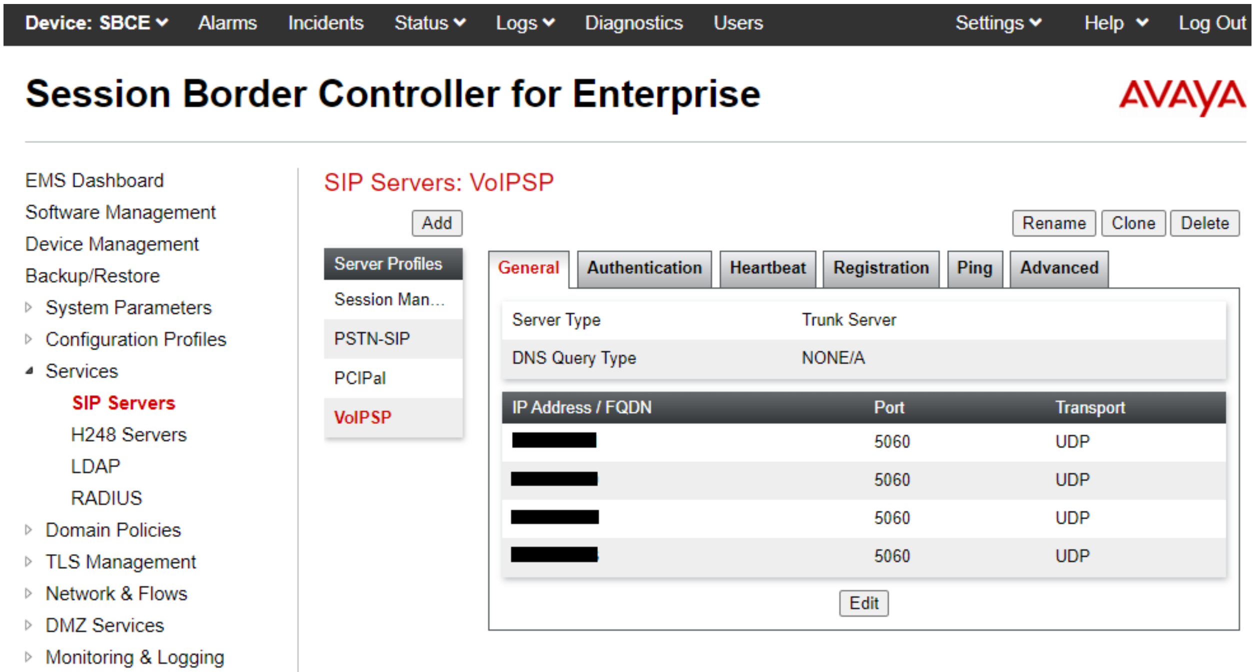


The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 7.2.2**. All other tabs were left with their default values.

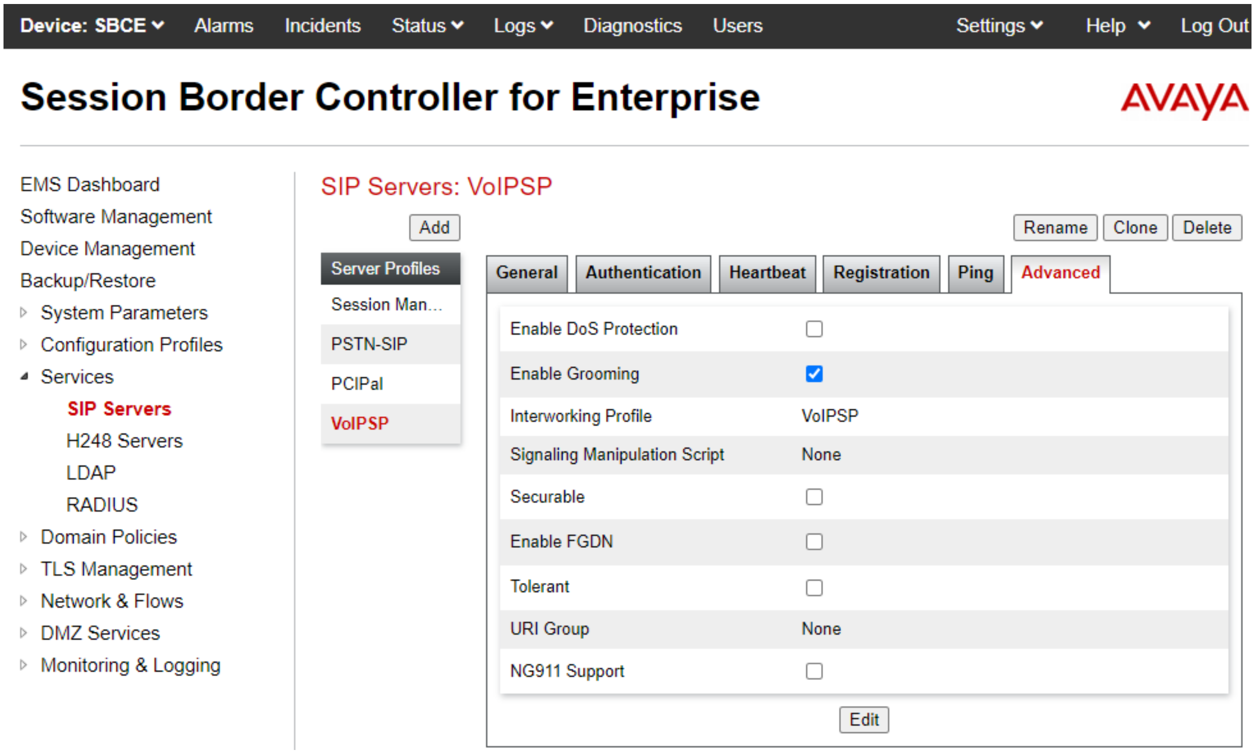


7.3.3. SIP Server for VoIP Service Provider

The **General** tab of the VoIP Service Provider SIP Server was configured as shown below. UDP transport was used for the VoIP Service Provider SIP trunk. The VoIP Service Provider was accessible via any one of four IP addresses.



The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 7.2.3**. All other tabs were left with their default values.

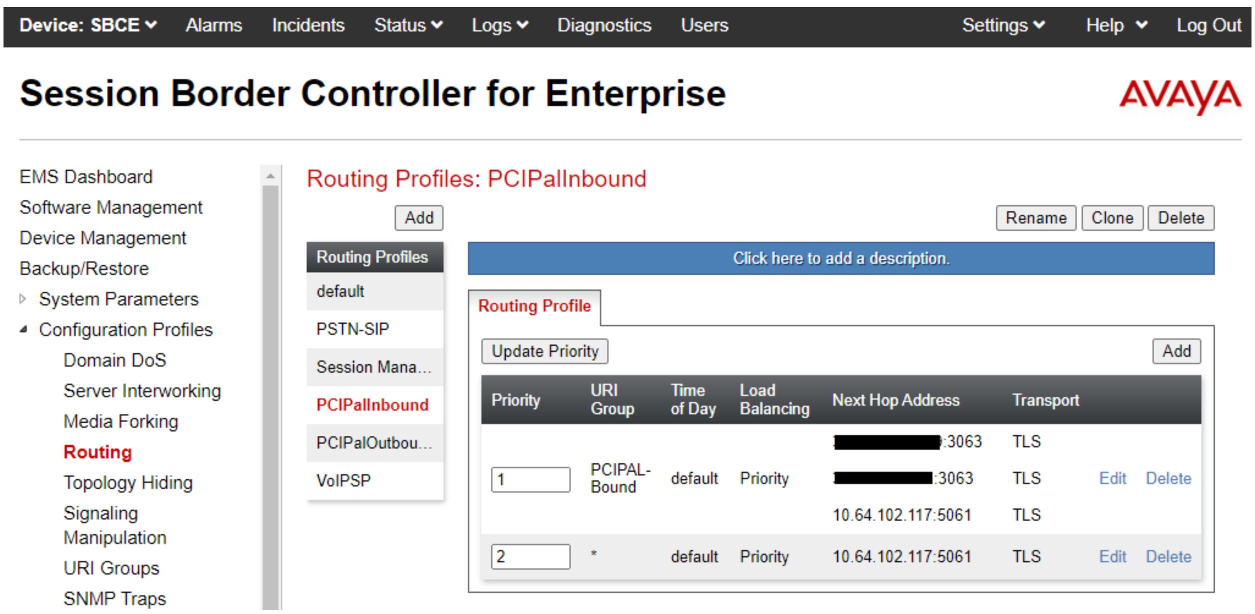


7.4. Administer Routing Profiles

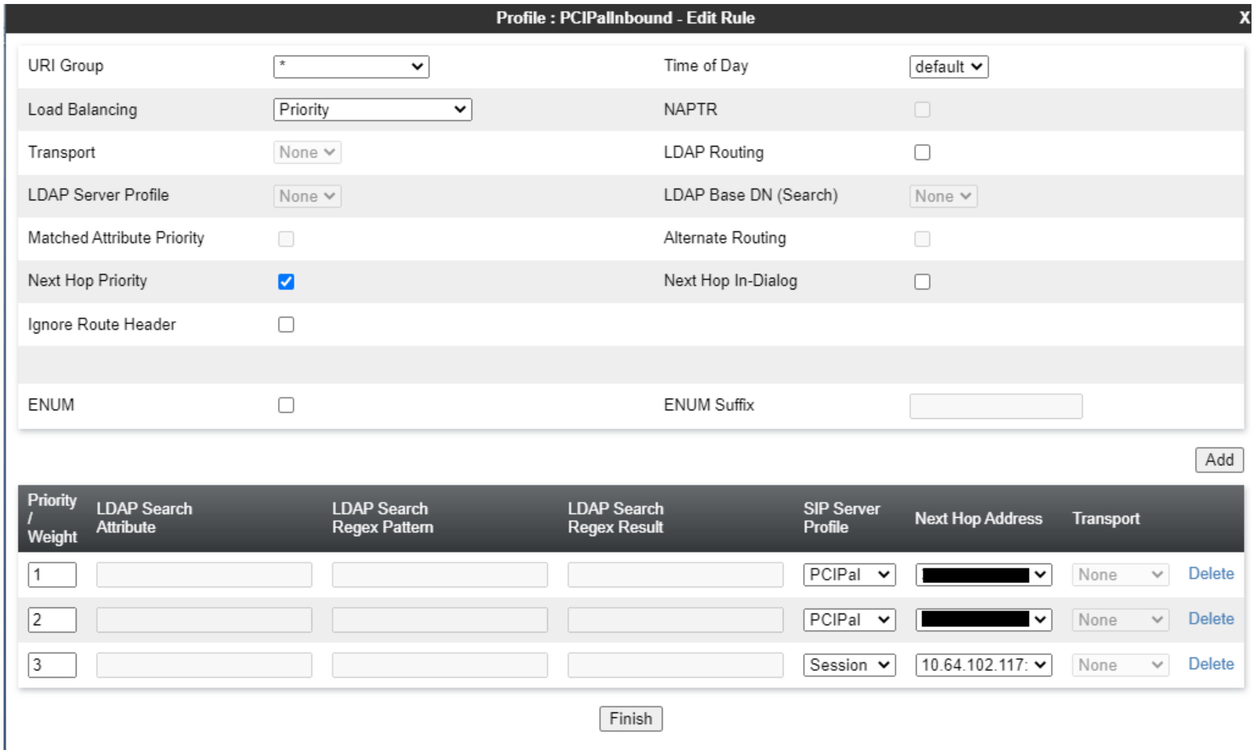
A routing profile is used to specify the next-hop for a SIP message. A routing profile is applied only after the traffic has matched an End Point Flow defined in **Section 7.12**. The IP addresses and ports defined here will be used as destination addresses for signaling. Create a routing profile for Session Manager, PCI Pal Agent Assist, and VoIP Service Provider.

7.4.1. Routing Profile for PCI Pal Agent Assist

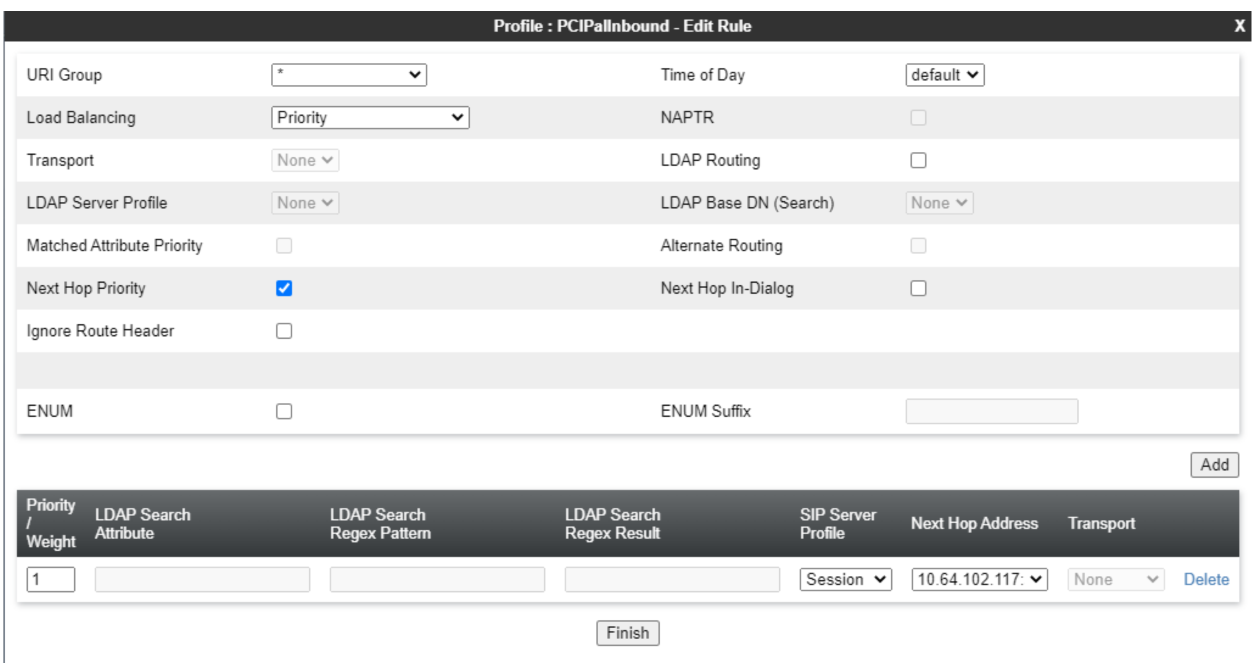
Two routing profiles were added for PCI Pal Agent Assist for inbound and outbound calls. The routing profile for inbound calls from the VoIP Service Provider to Session Manager is shown below. The routing profile was named *PCIPalInbound*. This routing profile contains two routing rules. The first routing rule with **Priority** of *1* is used to route calls through Agent Assist if the incoming number matches the URI Group *PCIPAL-Bound* configured in **Section 7.6**. The second routing rule with **Priority** of *2* is used to route all other calls directly to Session Manager – bypassing Agent Assist.



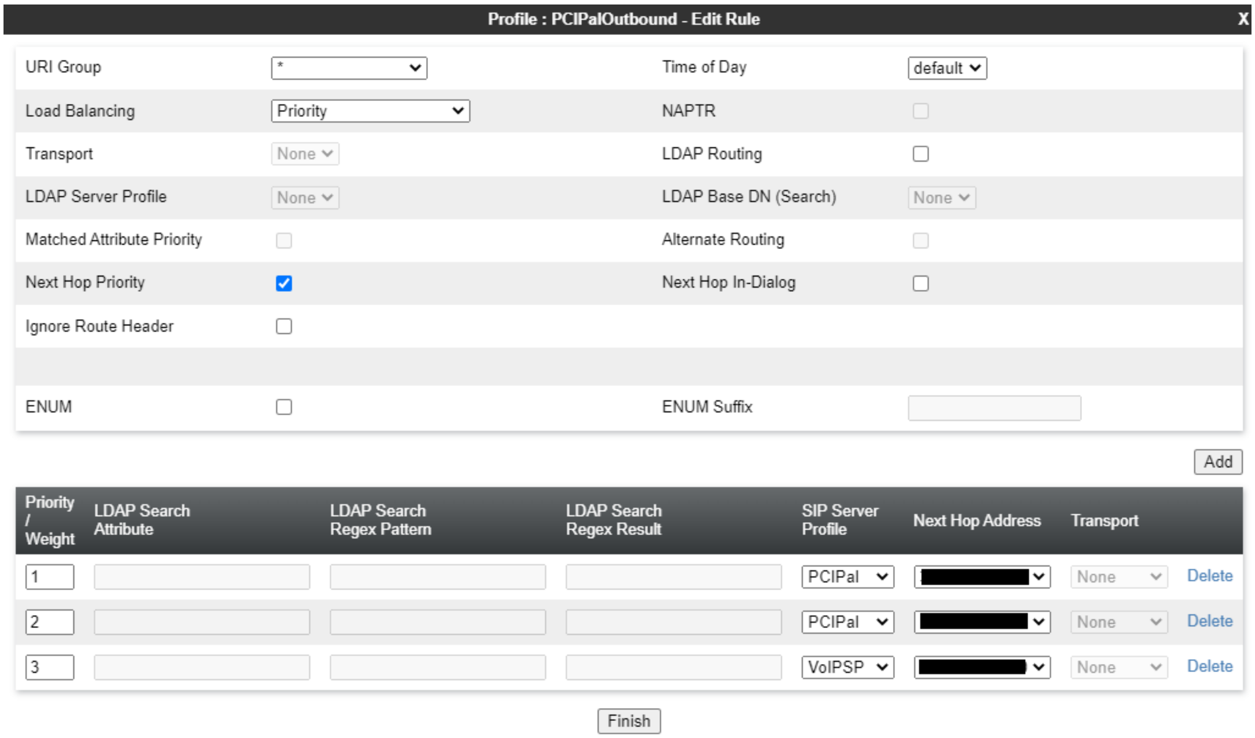
The first routing rule of Routing Profile *PCIPALInbound* is shown more detail below. It contains three routing preferences, the primary Agent Assist, the secondary Agent Assist, and Session Manager in that priority order.



The second routing rule of Routing Profile *PCIPALInbound* is shown more detail below. It contains Session Manager as the only routing preference.



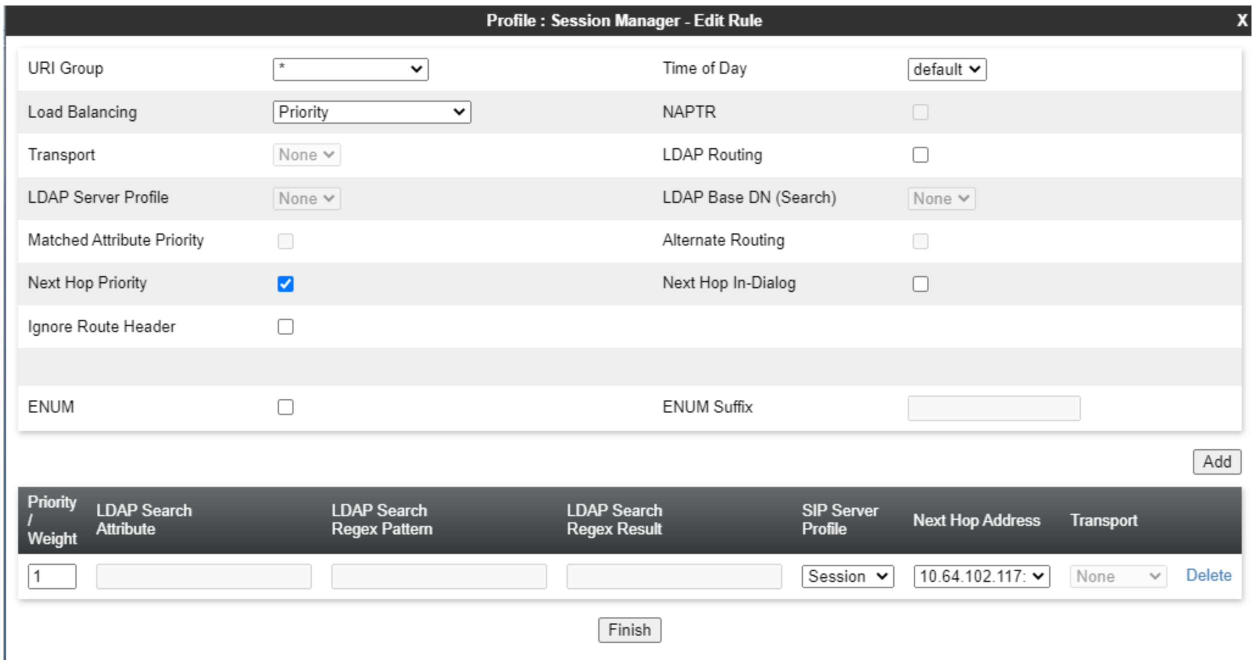
The routing profile for outbound calls from Session Manager to the VoIP Service Provider is shown below. The routing profile was named *PCIPalOutbound*. This routing profile contains three routing preferences, the primary Agent Assist, the secondary Agent Assist, and the VoIP Service Provider in that priority order.



7.4.2. Routing Profile for Session Manager

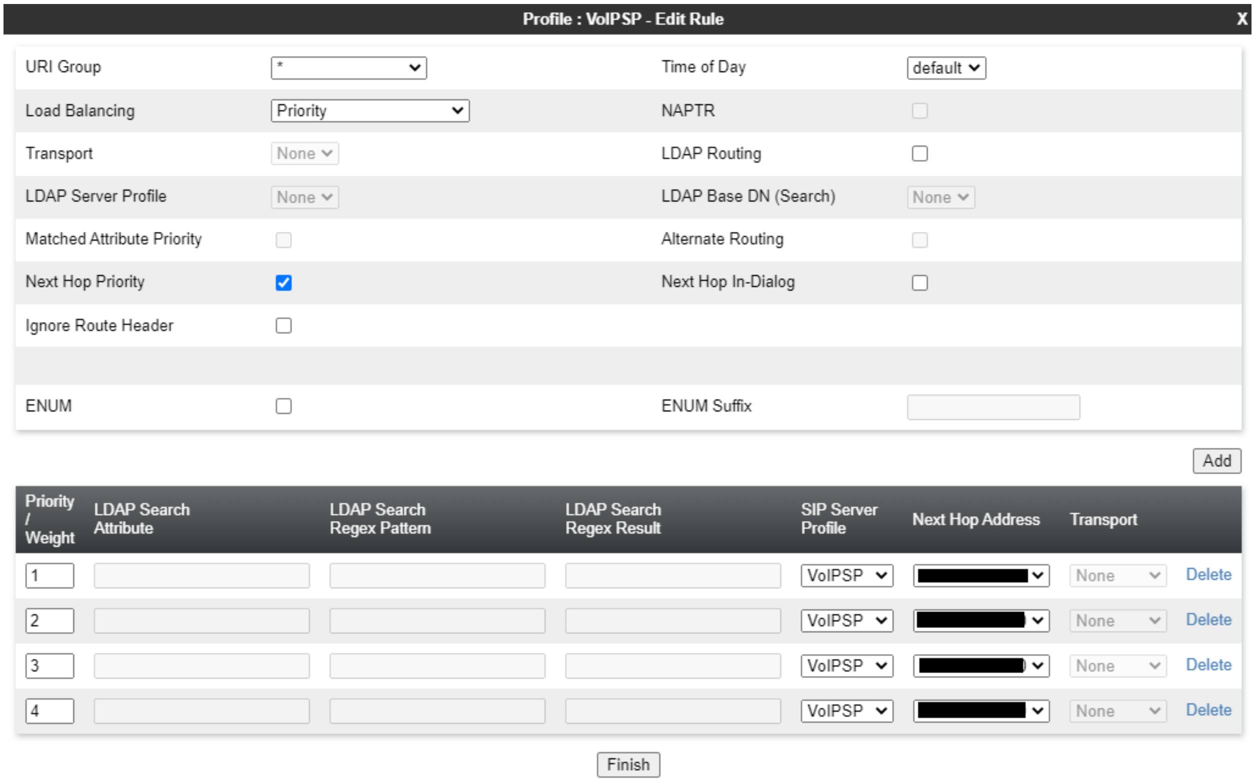
To create a new profile, navigate to **Configuration Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. To view the settings of an existing profile, select the profile from the center pane.

The routing profile for calls to Session Manager is shown below. The routing profile was named *Session Manager*. This routing profile contains the IP address of the signaling interface of Session Manager.



7.4.3. Routing Profile for VoIP Service Provider

The routing profile for calls to VoIP Service Provider is shown below. The routing profile was named *VoIPSP*. This routing profile contains the IP addresses for accessing the VoIP Service Provider.



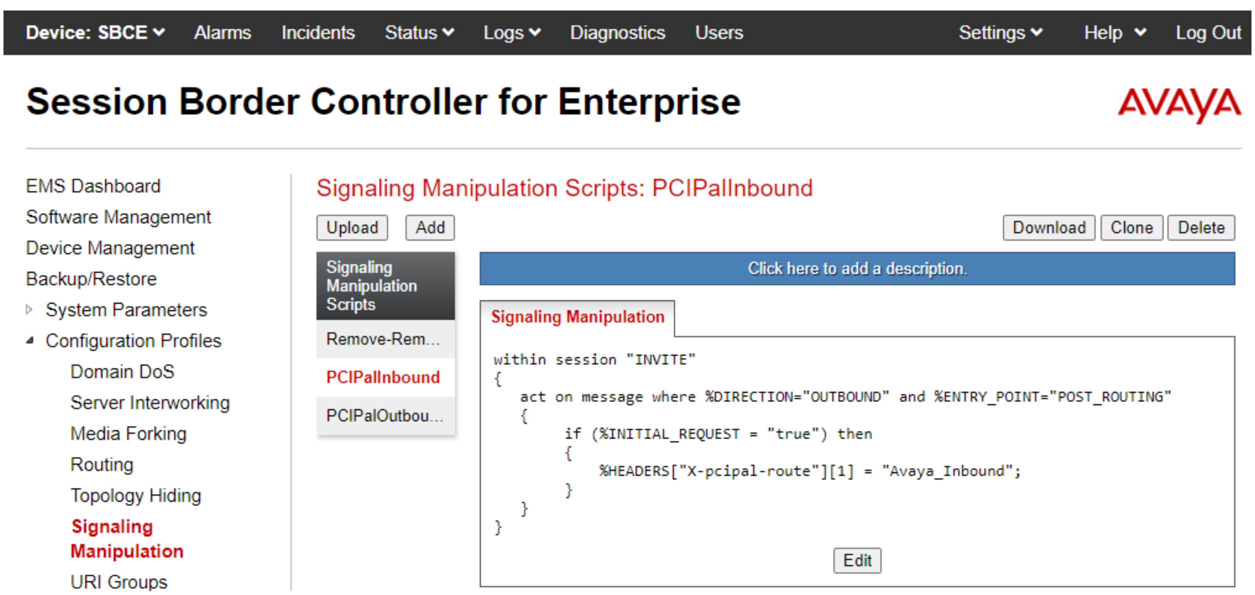
7.5. Administer Signaling Manipulation Scripts

Signaling manipulation scripts provide for the manipulation of SIP messages which cannot be done by another configuration within SBCE. Agent Assist required the signaling manipulation scripts in this section. It is applied to the End Point Flows in **Section 7.12**.

To create a script, navigate to **Configuration Profiles→ Signaling Manipulation** in the left pane. In the center pane, select **Add**. A script editor window (not shown) will appear in which the script can be entered line by line. The **Title** field at the top of the editor window (not shown) is where the script name is entered. Once complete, the script is displayed. To view an existing script, select the script from the list.

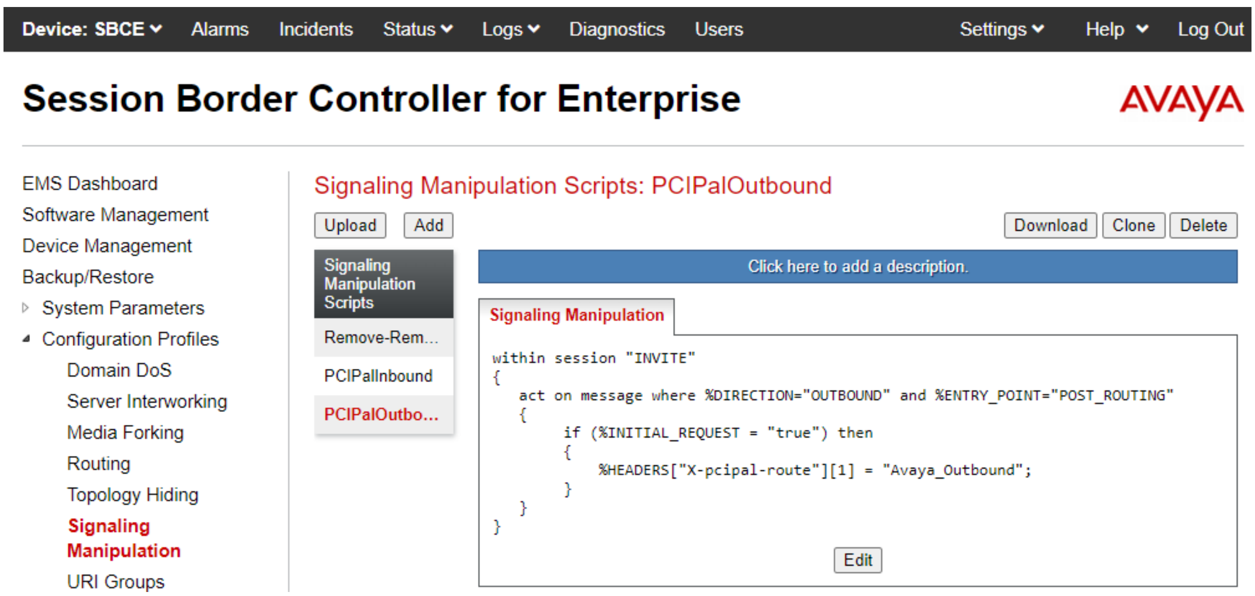
The following signaling manipulation script, named *PCIPalInbound*, inserts the **X-pcipal-route** header with a value of *Avaya_Inbound* in the SIP INVITE of an inbound call from the VoIP Service Provider.

```
within session "INVITE"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
        if (%INITIAL_REQUEST = "true" ) then
        {
            %HEADERS["X-pcipal-route"][1] ="Avaya_Inbound";
        }
  }
}
```



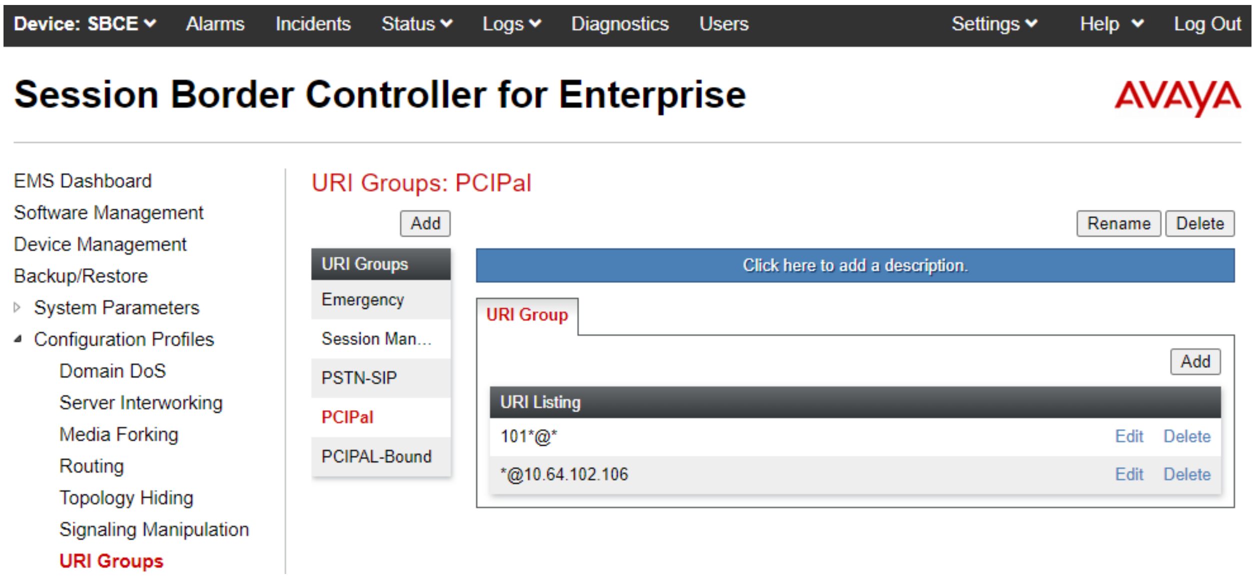
The following signaling manipulation script, named *PCIPalIOutbound*, inserts the **X-pcipal-route** header with a value on *Avaya_Outbound* in the SIP INVITE of an outbound call to the VoIP Service Provider.

```
within session "INVITE"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
        if (%INITIAL_REQUEST = "true" ) then
        {
            %HEADERS["X-pcipal-route"][1] ="Avaya_Outbound";
        }
  }
}
```

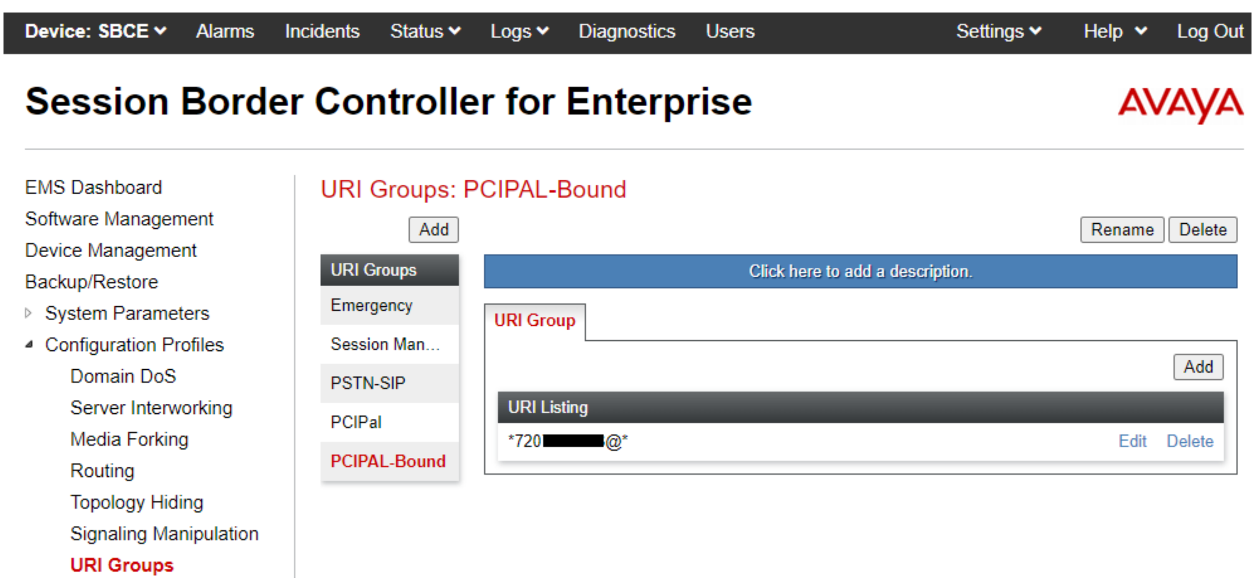


7.6. Administer URI Groups

A **URI Group** defines any number of logical URI groups consisting of each SIP subscriber location in the particular domain or group. For this solution, a **URI Group** named *PCIPal* that is assigned to the *OutboundPCIPal* endpoint flow configured in **Section 7.12.1**. In order for the SBCE to select the *OutboundPCIPal* endpoint flow, either (1) the domain in the From header must match *10.64.102.106*, which is the SIP IP Address of Session Manager, or (2) the user part of the From header must start with *101* and the domain in the From header must be the PCI Pal Agent Assist IP address or domain.



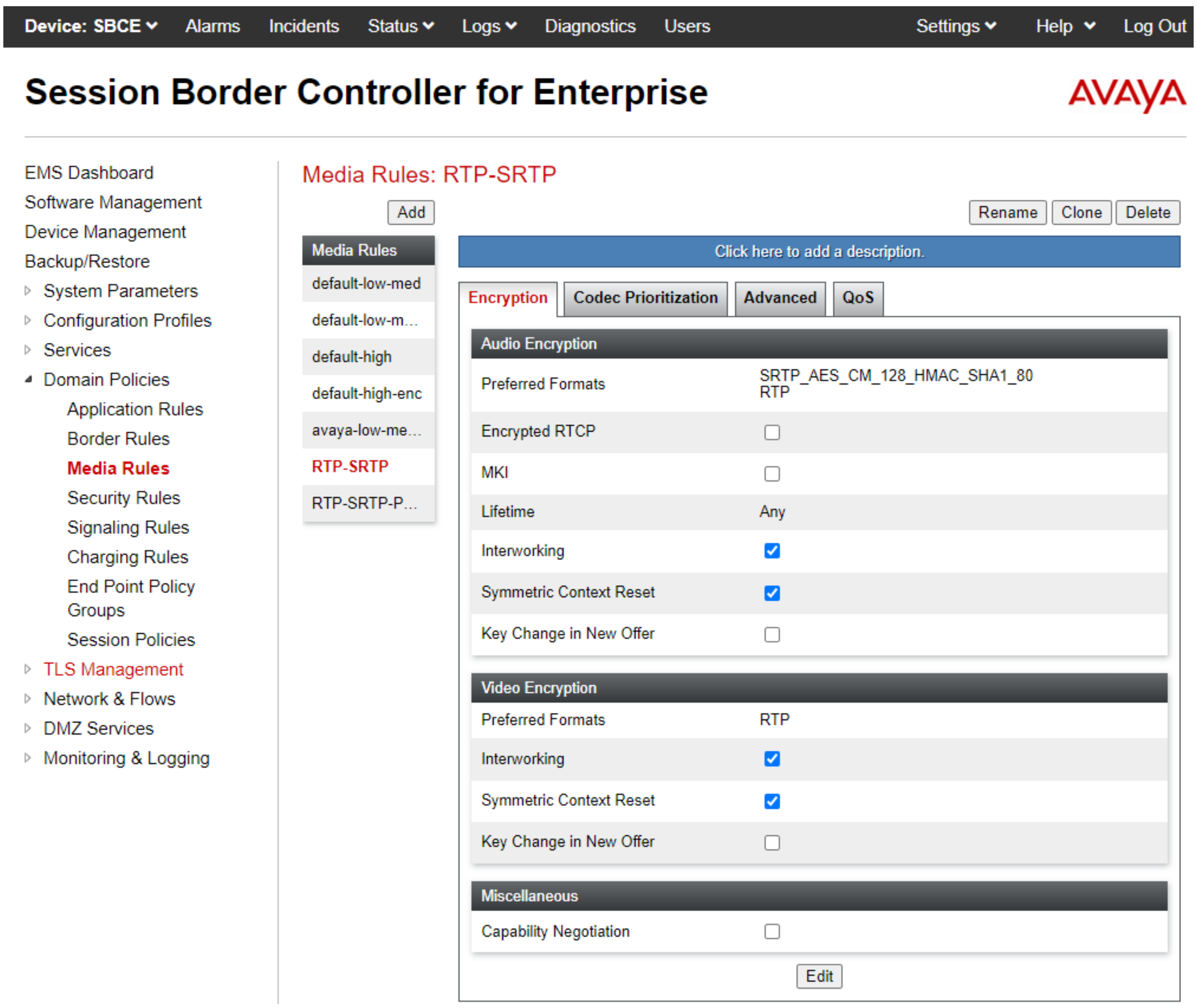
In addition, another URI Group, *PCIPAL-Bound*, may be added to specify which calls should be routed to Agent Assist based on the number in the To header. This URI group was assigned to the *PCIPALInbound* routing profile in **Section 7.4.1**.



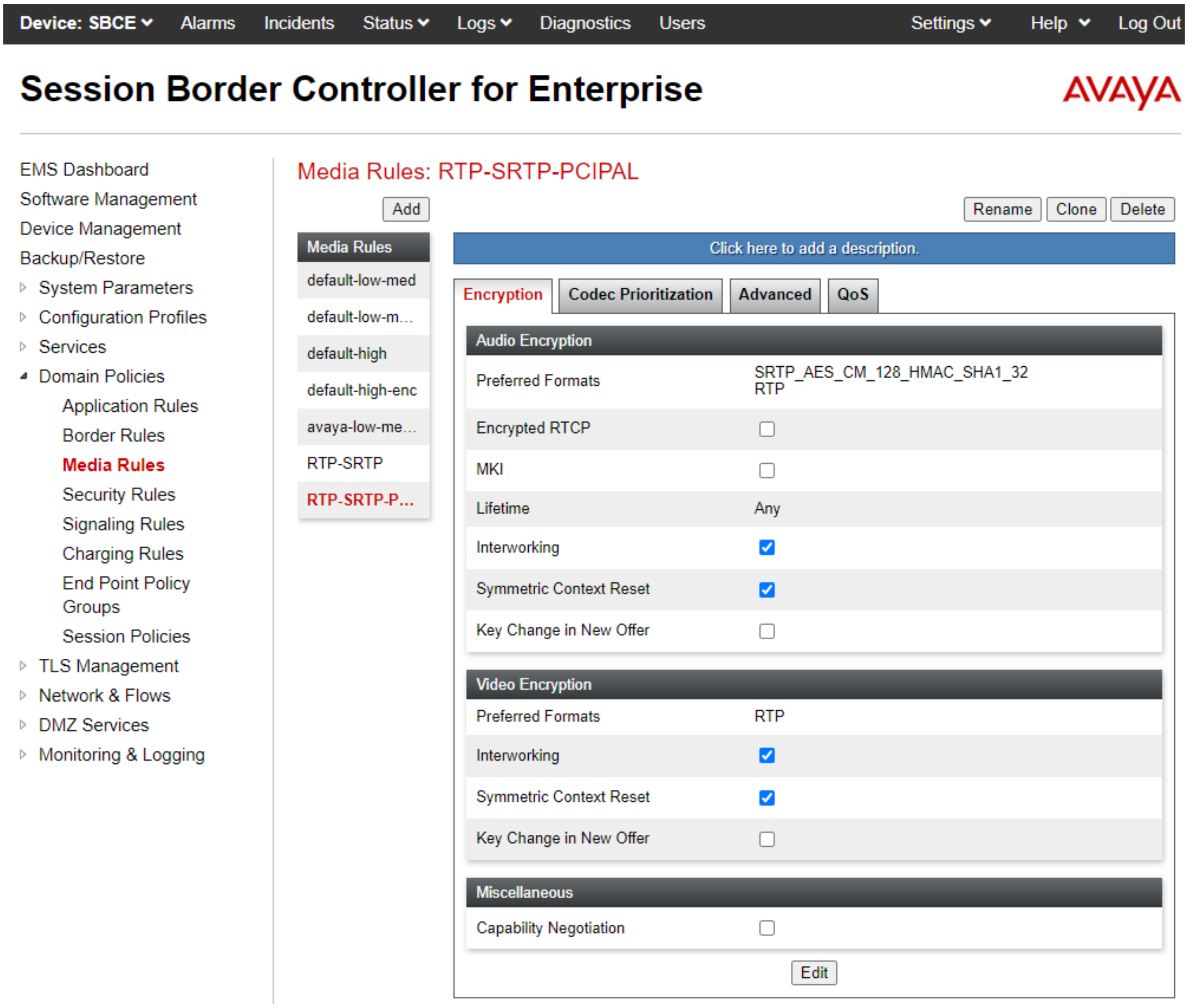
7.7. Administer Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 7.8**. For the compliance test, two new media rules were created, one for Session Manager and another one for Agent Assist. A pre-existing media rule, *default-low*, will be used for the VoIP Service Provider.

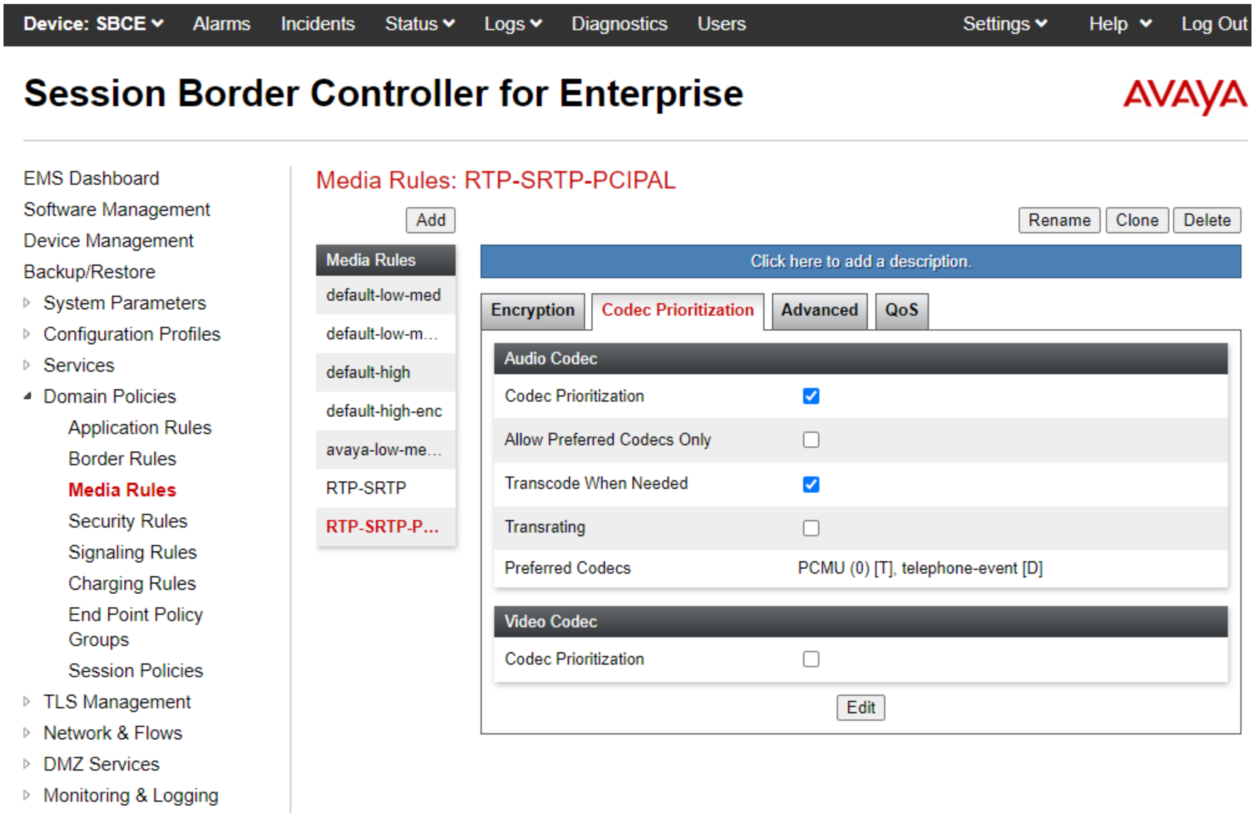
To view an existing rule, navigate to **Domain Policies → Media Rules** in the left pane. In the center pane, select the rule (e.g., *RTP-SRTP*) to be viewed. The content of the *RTP-SRTP* media rule, used for Session Manager, is described below. The **Encryption** tab was configured as shown below. It supports both SRTP and RTP. Note that the SRTP cipher is SRTP_AES_CM_128_HMAC_SHA1_80, which is different than the cipher used in the PCI Pal media rule. Refer to **Section 2.2** for the reason why they must be different.



The content of the *RTP-SRTP-PCIPAL* media rule, used for Agent Assist, is described below. The **Encryption** tab was configured as shown below. It supports both SRTP and RTP. Note that the SRTP cipher is SRTP_AES_CM_128_HMAC_SHA1_32, which is different than the cipher used in the Session Manager media rule. Refer to **Section 2.2** for the reason why they must be different.



The **Codec Prioritization** tab for the *RTP-SRTP-PCIPAL* media rule was configured as shown below.

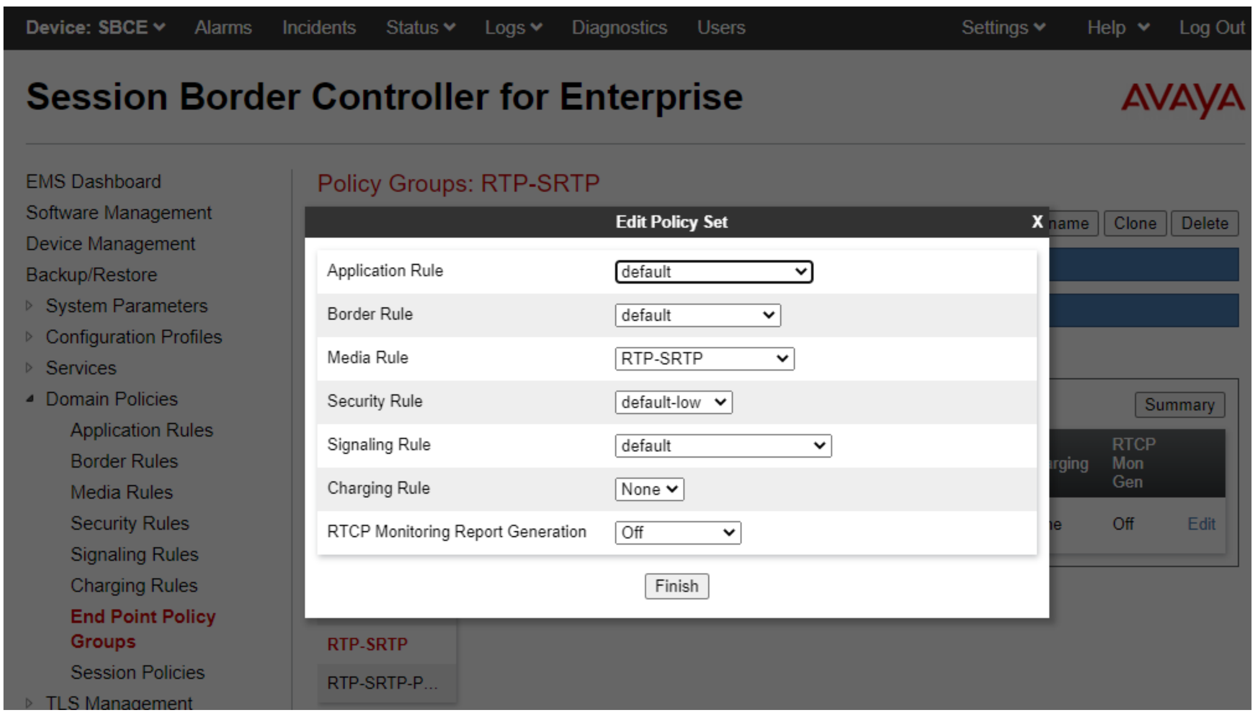


7.8. Administer End Point Policy Groups

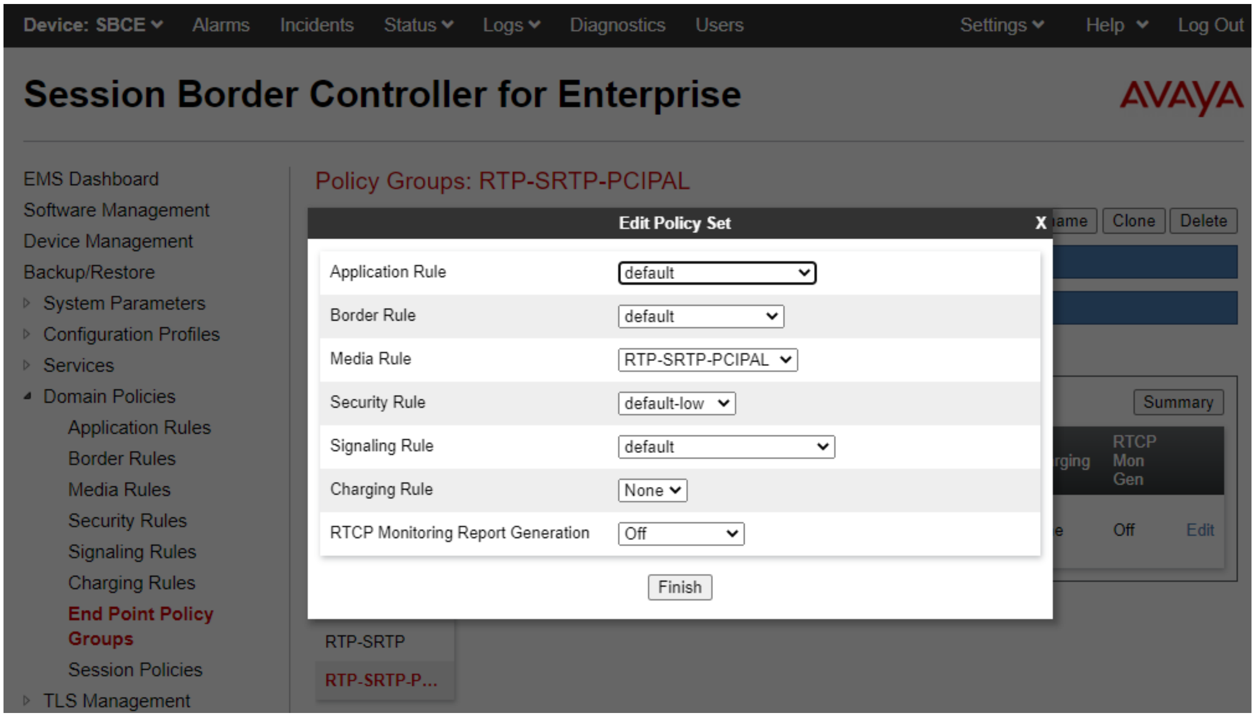
An endpoint policy group is a set of policies that will be applied to traffic between the SBCE and an endpoint (connected server). Two endpoint policy groups must be created for Session Manager and Agent Assist. The VoIP Service Provider will use a pre-existing endpoint policy group. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.12**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by the **Policy Group** window (not shown) to configure the group parameters. Once complete, the settings will be displayed. To view the settings of an existing group, select the group from the list. The settings will appear in the right pane.

The new endpoint policy group, named *RTP-SRTP*, is shown below and is assigned the *RTP-SRTP* media rule configured above. This endpoint policy group is used for Session Manager.



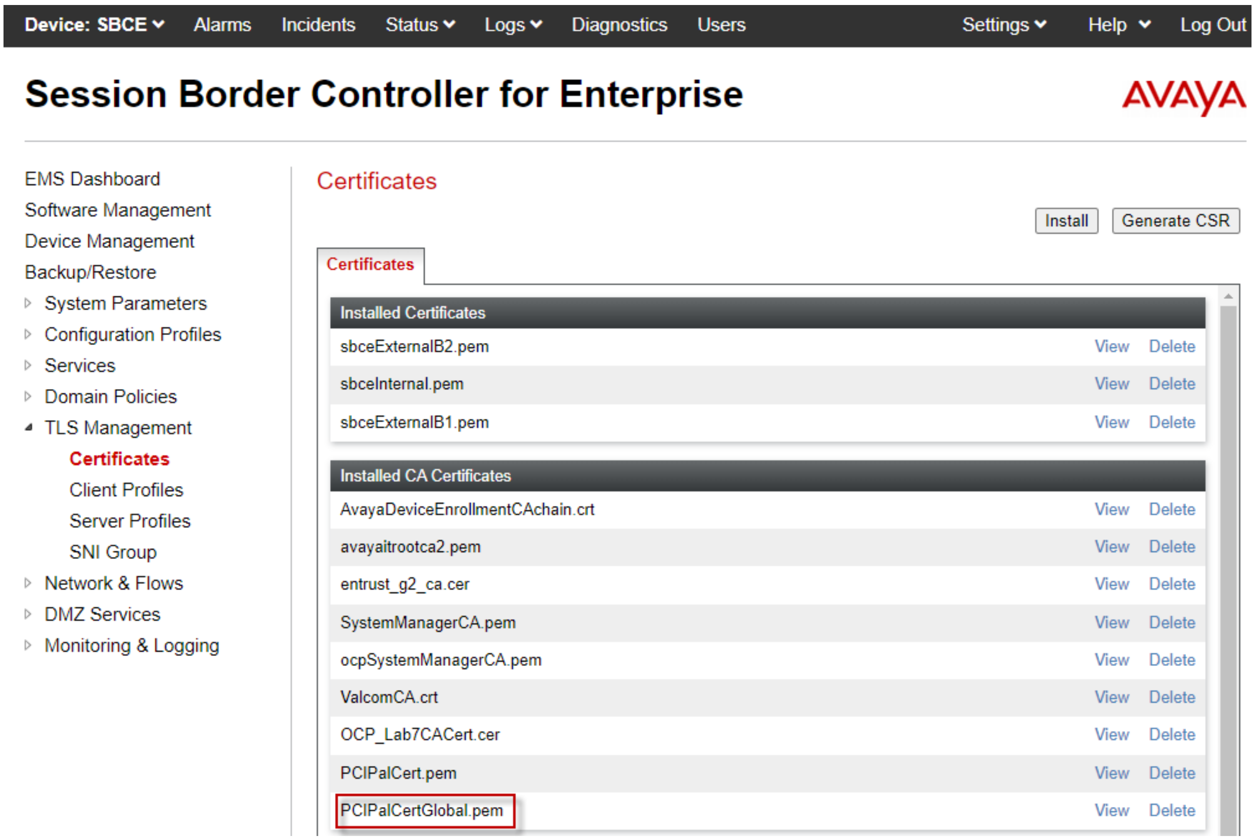
The new endpoint policy group, named *RTP-SRTP-PCIPAL*, is shown below and is assigned the *RTP-SRTP-PCIPAL* media rule configured above. This endpoint policy group is used for Agent Assist.



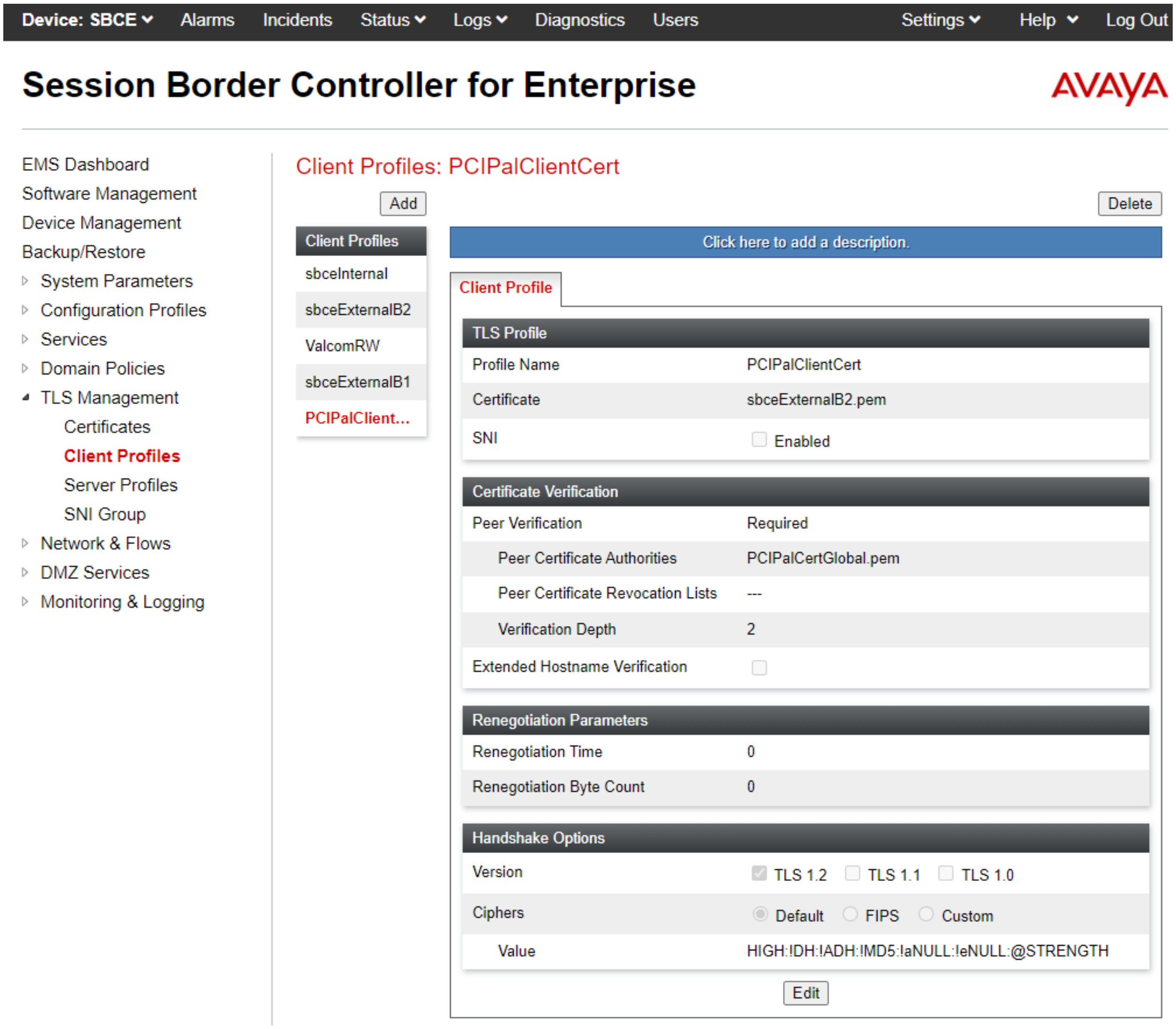
7.9. Administer TLS Management

This section covers installing the Agent Assist certificate, configuring the Agent Assist client profile, and configuring the server profile for the B2 public interface, which connects to Agent Assist, to set up secure communications using TLS. The TLS configuration for Session Manager is assumed to already be in place and is not shown in these Application Notes.

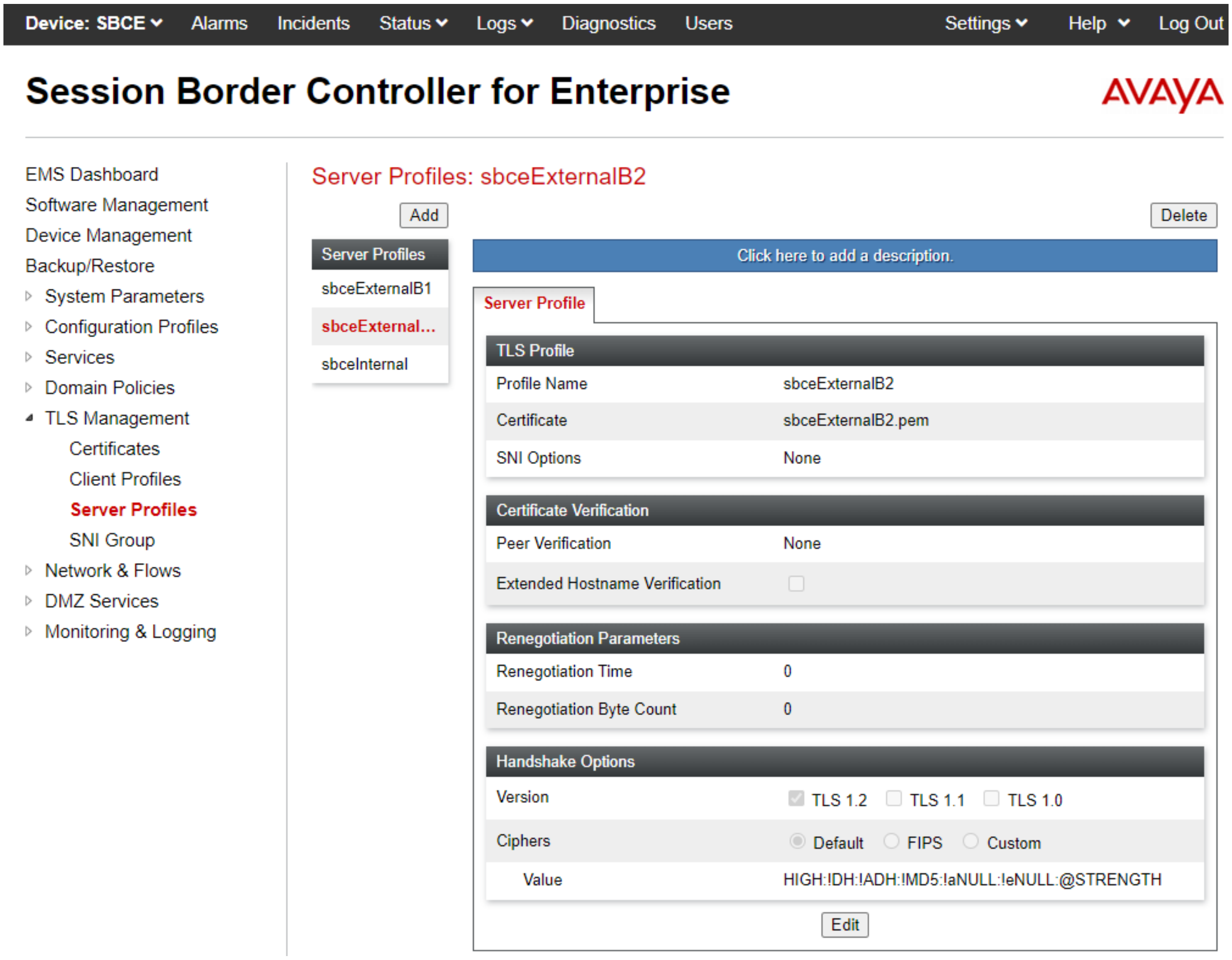
Navigate to **TLS Management → Certificates** and install the Agent Assist CA certificate. For the compliance test, the certificate was named *PCIPalCertGlobal.pem* as shown below.



Next, create a client profile for Agent Assist as shown below. The **Profile Name** was set to *PCIPalClientCert* and the certificate for B2 public interface was selected. **Peer Verification** was set to *Required* and the *PCIPalCertGlobal.pem* certificate was selected for **Peer Certificate Authorities**. The **Verification Depth** was set to *2* and the **Version** was set to *TLS 1.2*. This client profile was assigned to the Agent Assist SIP server in **Section 7.3.1**.



The following server profile is assigned to the B2 public interface covered in **Section 7.11**.

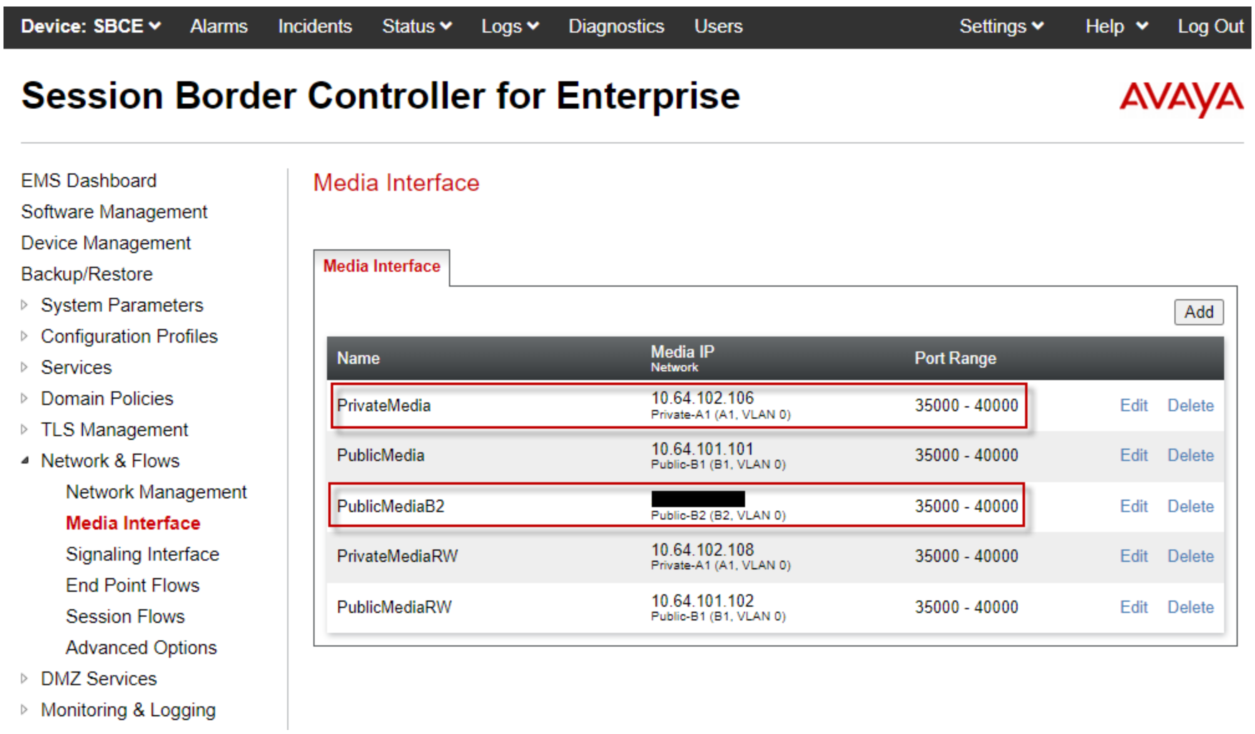


7.10. Administer Media Interfaces

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 the SBCE. Media Interface needs to be defined for each SIP server to send and receive media (RTP or SRTP).

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 blacked out. The media interfaces used for this solution are listed below.

- **PrivateMedia:** Interface used by Session Manager to send and receive media.
- **PublicMediaB2:** Interface used by Agent Assist and VoIP Service Provider to send and receive media.



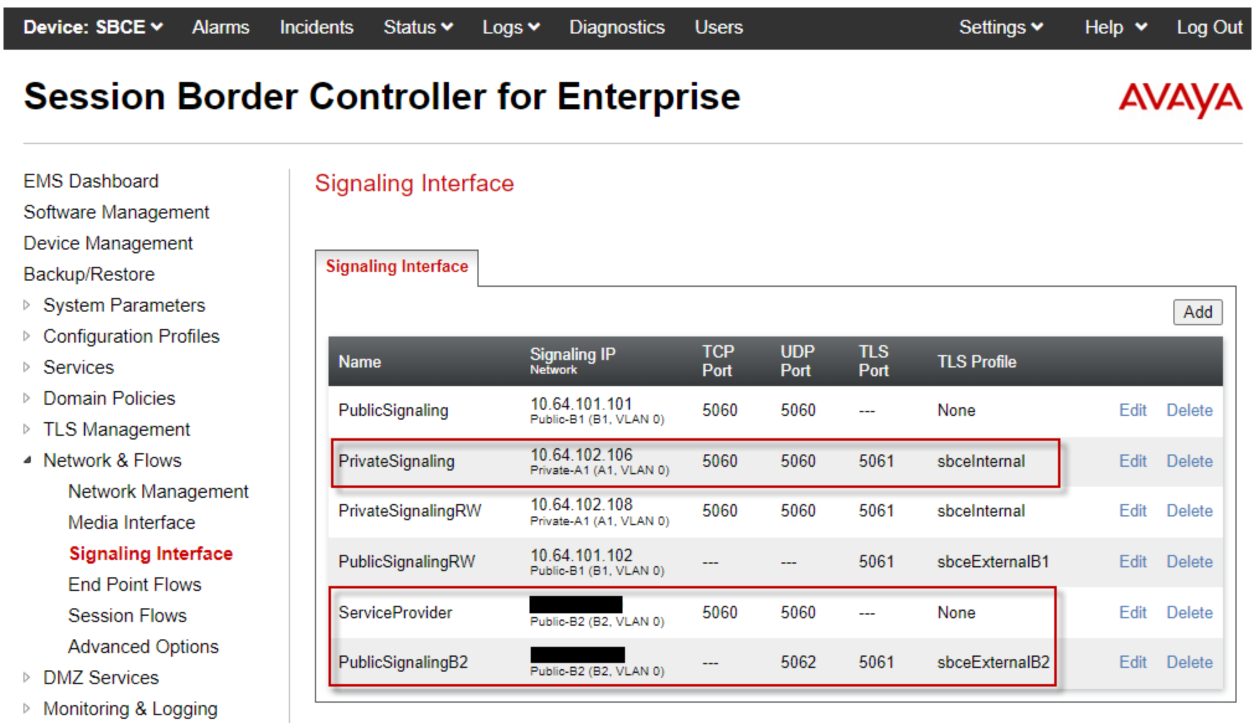
7.11. Administer Signaling Interfaces

A signaling interface defines an IP address, protocols and listen ports that the SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the SBCE. Signaling interface needs to be defined for each SIP server to send and receive media (RTP or SRTP).

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

- **PrivateSignaling:** Interface used by Session Manager to send and receive calls.
- **ServiceProvider:** Interface used by VoIP Service Provider to send and receive calls.
- **PublicSignalingB2:** Interface used by Agent Assist to send and receive calls.

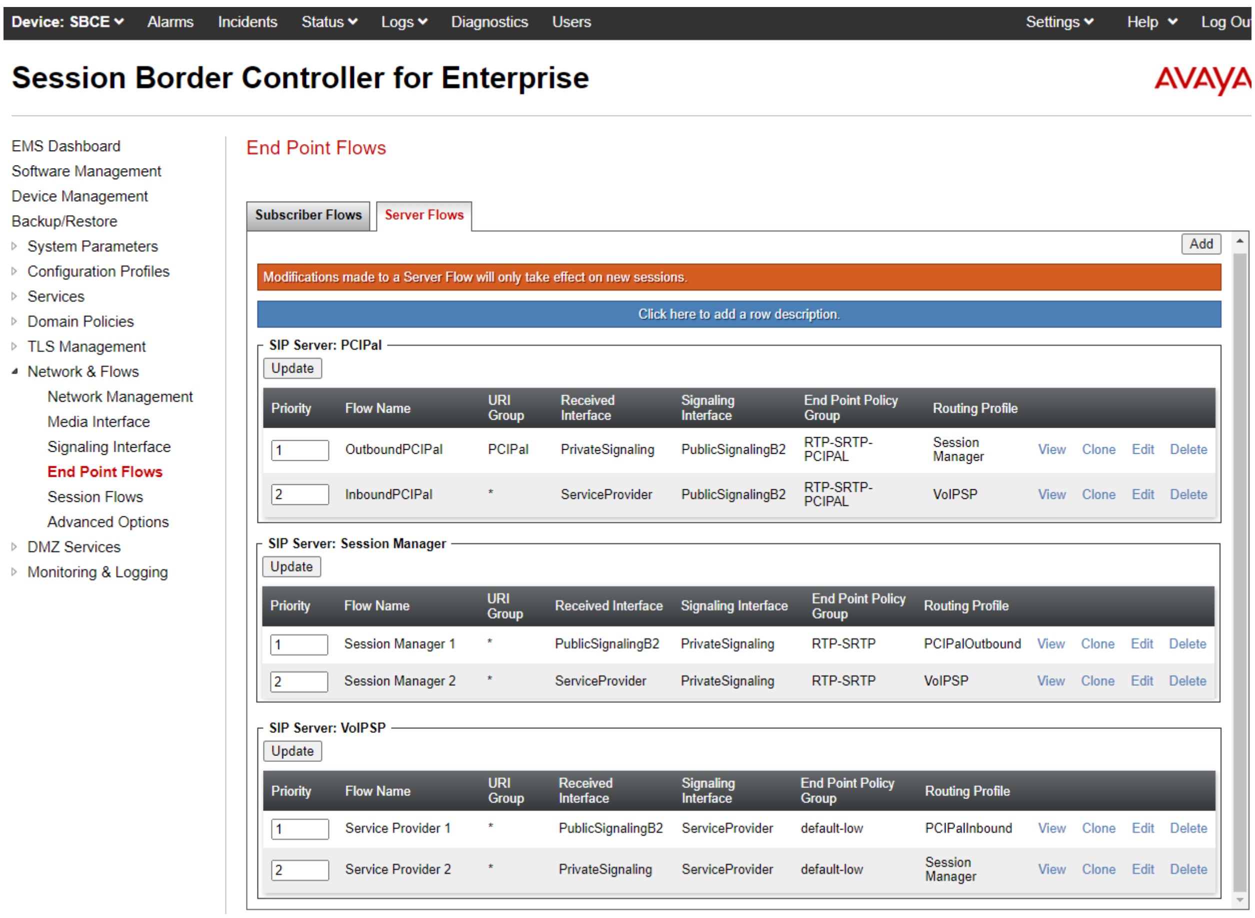
Note that PCI Pal and VoIP Service Provider use the same physical interface on SBCE.



7.12. Administer End Point Flows

Endpoint 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 the SBCE, 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 the case of the compliance test, the endpoints are Session Manager, Agent Assist, and the VoIP Service Provider.

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

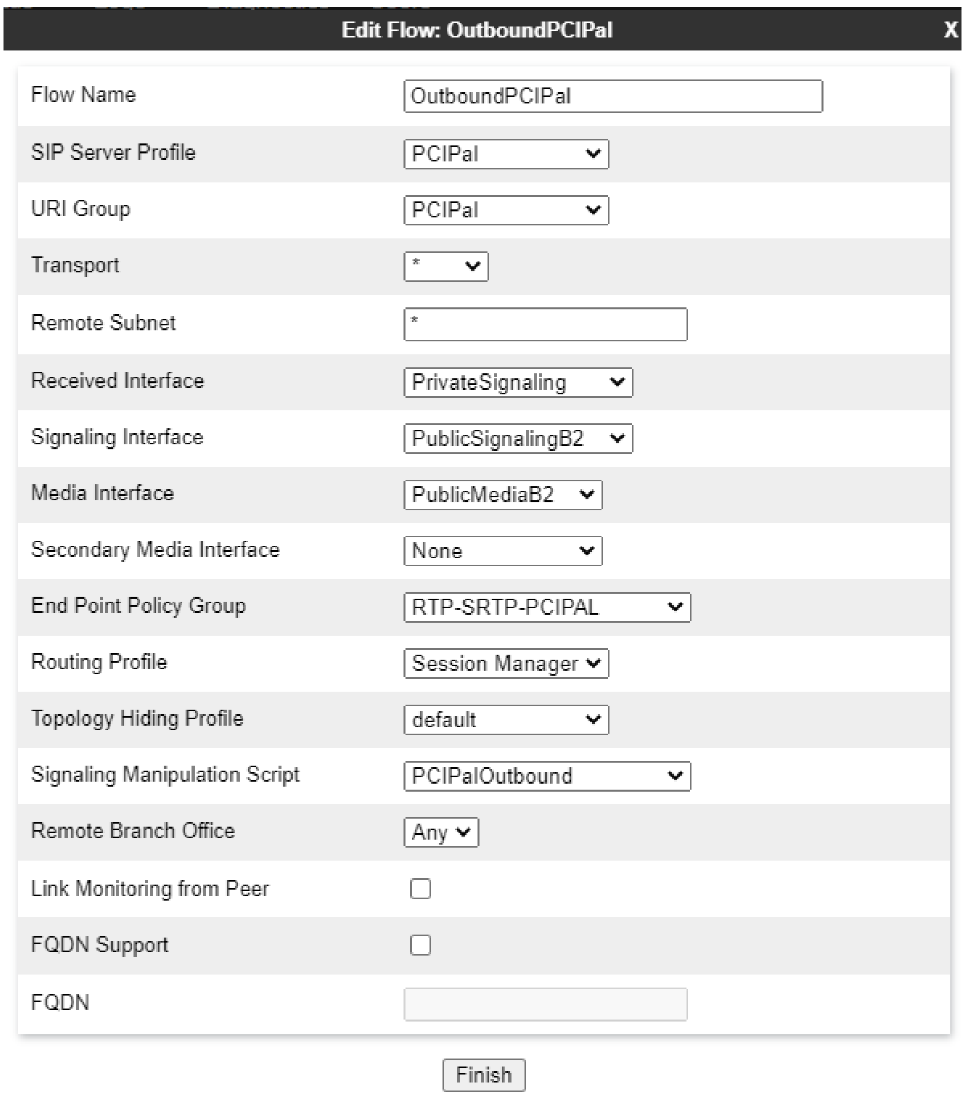


7.12.1. End Point Flows for PCI Pal Agent Assist

For the compliance test, two endpoint flows were created for PCI Pal Agent Assist.

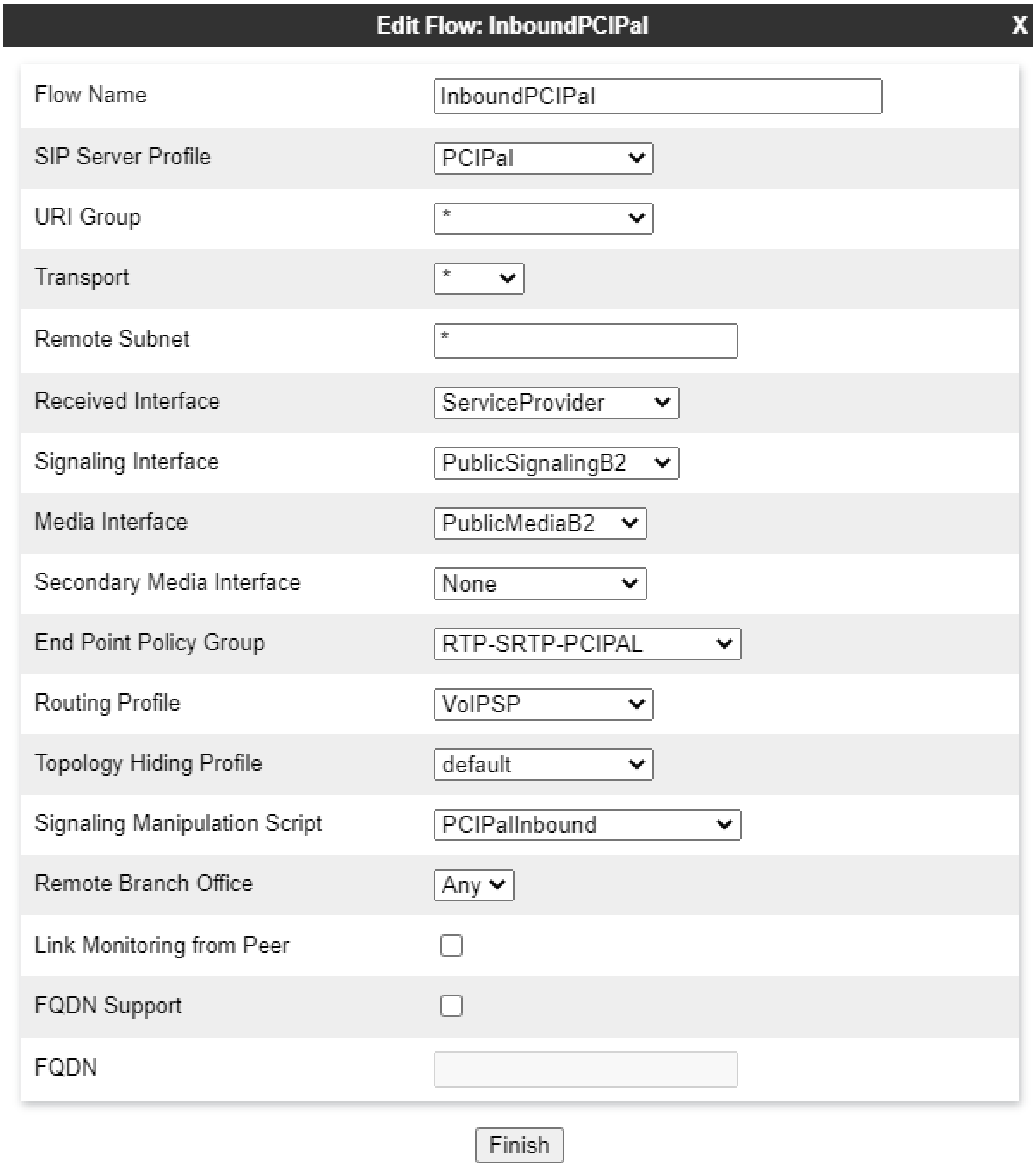
For inbound PSTN calls from the VoIP Service Provider, the *OutboundPCIPal* flow shown below is used as the source flow when SBCE receives a SIP INVITE from PCI Pal Agent Assist. This flow is used, because the URI Group matches the 101 prepended to the user part of the From header. The routing profile selects Session Manager as the destination endpoint.

For outbound PSTN calls from Session Manager, this flow is used as the destination flow when a SIP INVITE must be sent to PCI Pal Agent Assist. This flow is used, because URI Group matches the domain in the From header of the SIP INVITE, which contains the SBCE internal interface connected to Session Manager. The **Signaling Manipulation Script** adds a **X-pcipal-route** header with a value of *Avaya_Outbound* to the SIP INVITE sent to PCI Pal Agent Assist.



For inbound PSTN calls from the VoIP Service Provider, the *InboundPCIPal* flow shown below is used as the destination flow when a SIP INVITE must be sent to PCI Pal Agent Assist. The **Signaling Manipulation Script** adds a **X-pcipal-route** header with a value of *Avaya_Inbound* to the SIP INVITE sent to PCI Pal Agent Assist.

For outbound PSTN calls from Session Manager, this flow is used as the source flow when SBCE receives a SIP INVITE from PCI Pal Agent Assist. The routing profile selects the VoIP Service Provider as the destination endpoint.

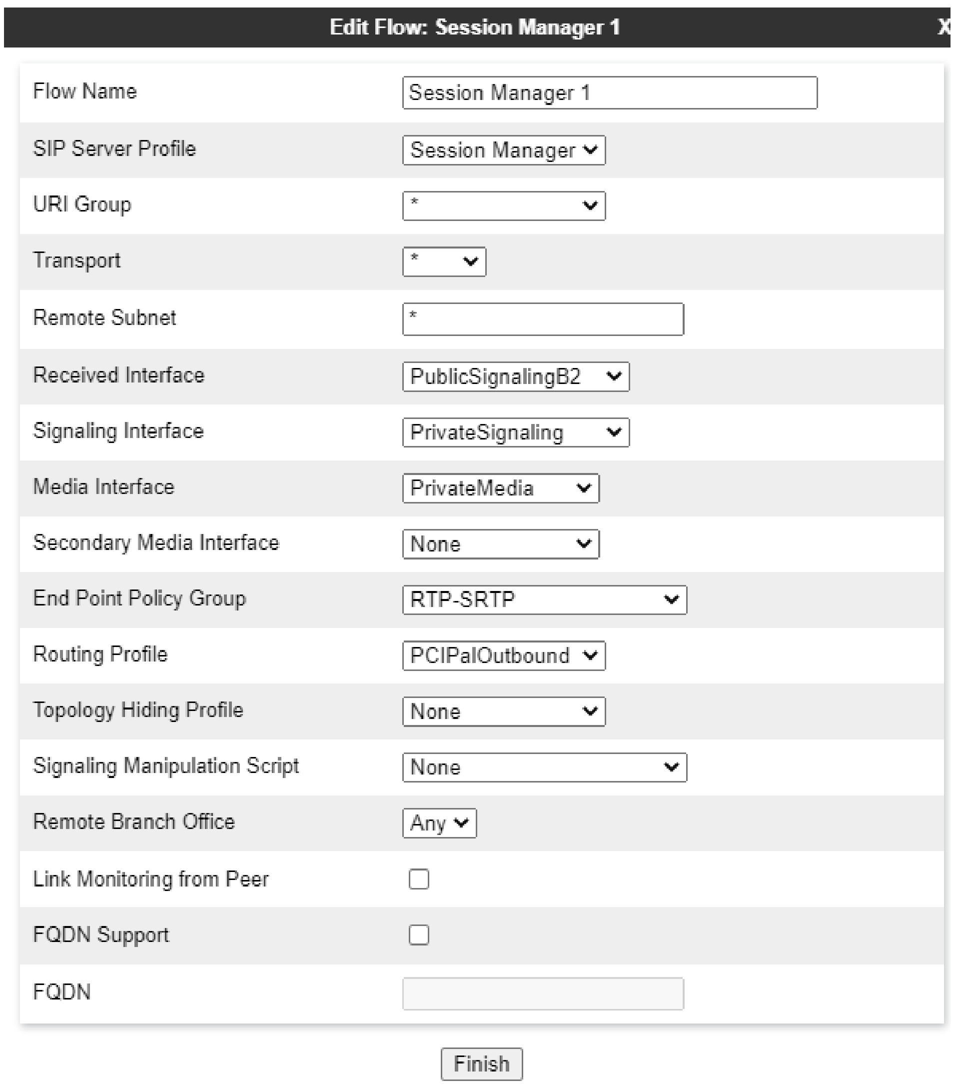


7.12.2. End Point Flows for Session Manager

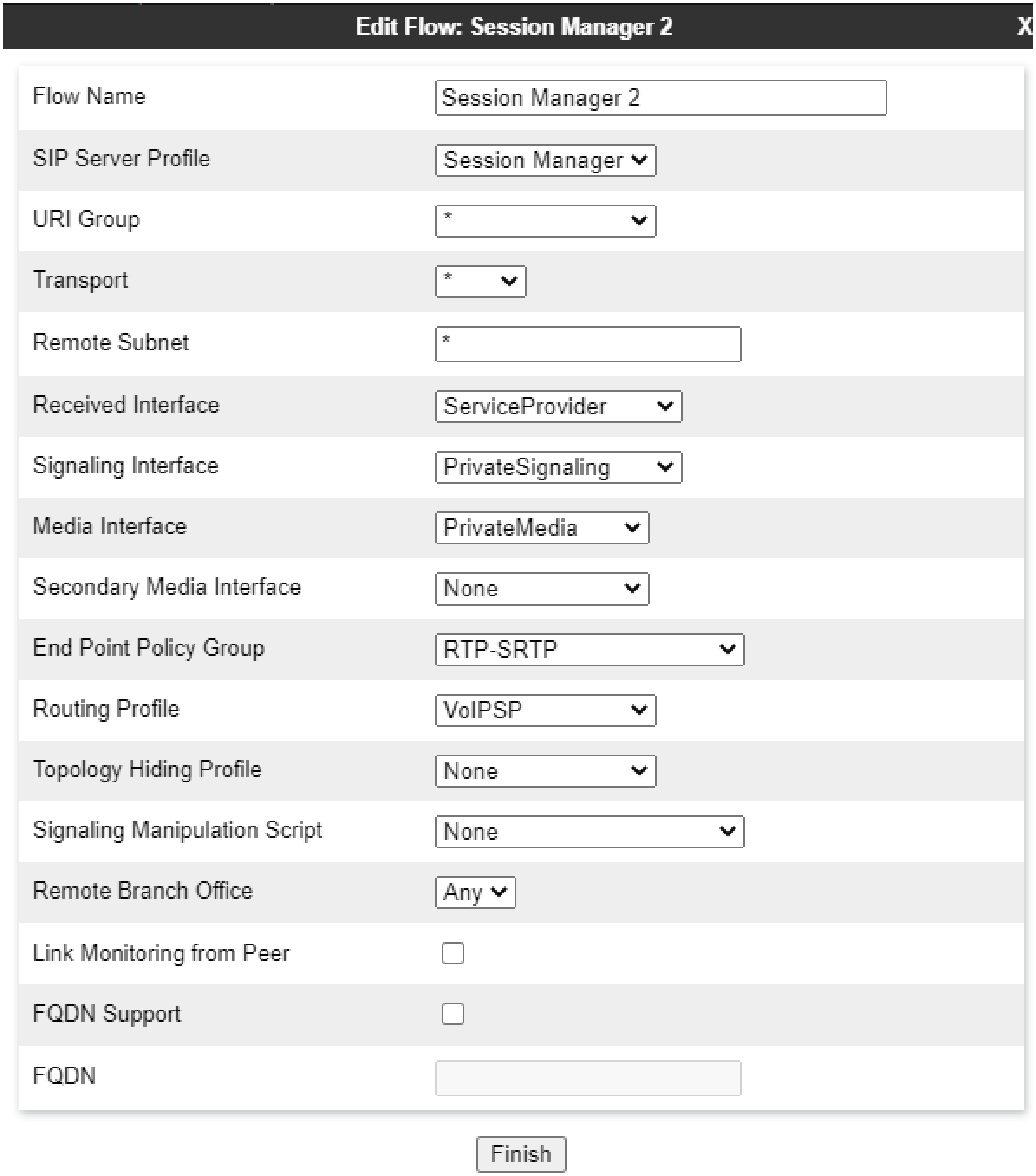
For the compliance test, two endpoint flows were created for Session Manager. If PCI Pal Agent Assist is available, the destination flow will be one of the PCI Pal flows in **Section 7.12.1**; otherwise, the destination flow will be one of the VoIP Service Provider flows in **Section 7.12.3**.

The *Session Manager 1* flow shown below is used as a source flow for outbound PSTN calls from Session Manager. The routing profile selects PCI Pal Agent Assist as the destination endpoint, if available; otherwise, the VoIP Service Provider is selected as the destination endpoint.

This flow is also used as a destination flow for inbound PSTN calls from the VoIP Service Provider.



The *Session Manager 2* flow shown below is used as the destination flow for inbound PSTN calls from the VoIP Service Provider when PCI Pal Agent Assist is not available.

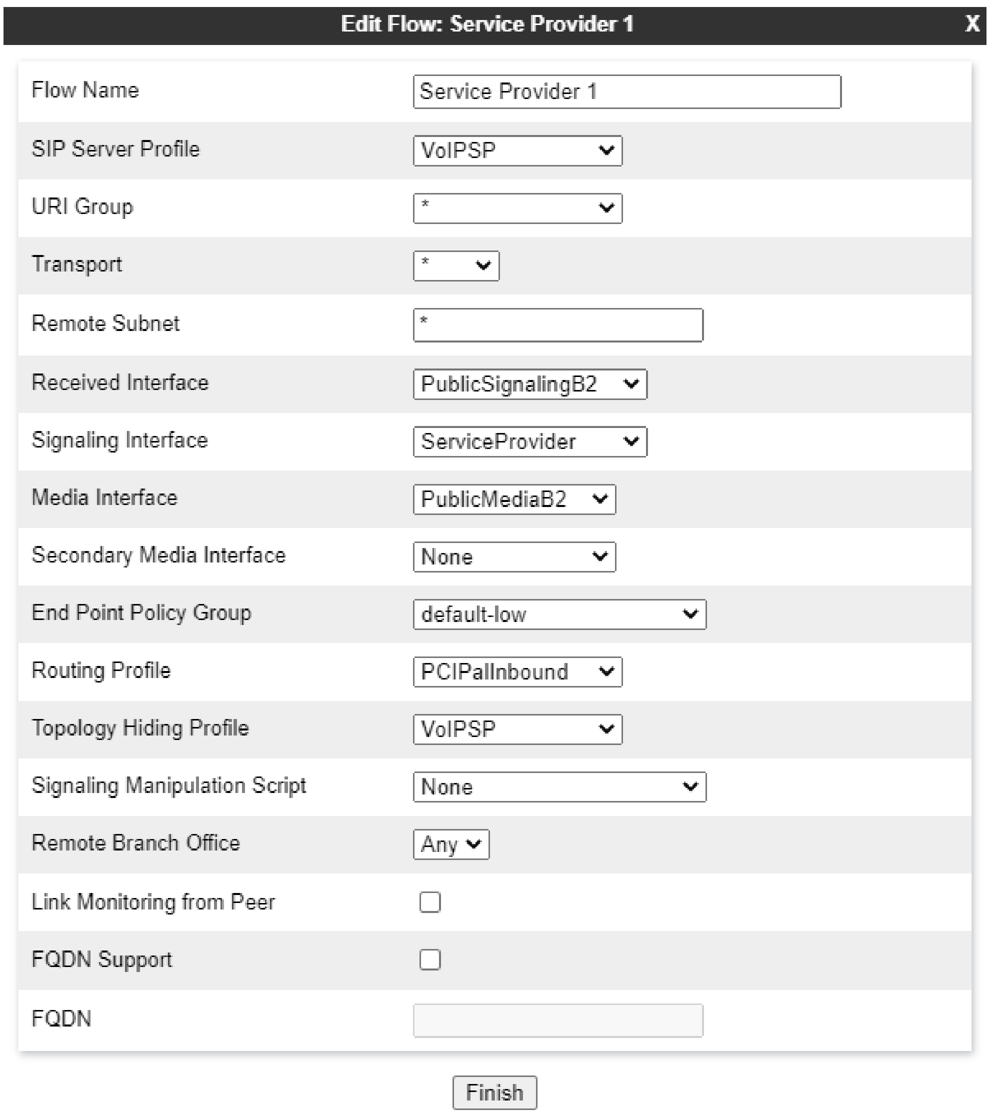


7.12.3. End Point Flows for VoIP Service Provider

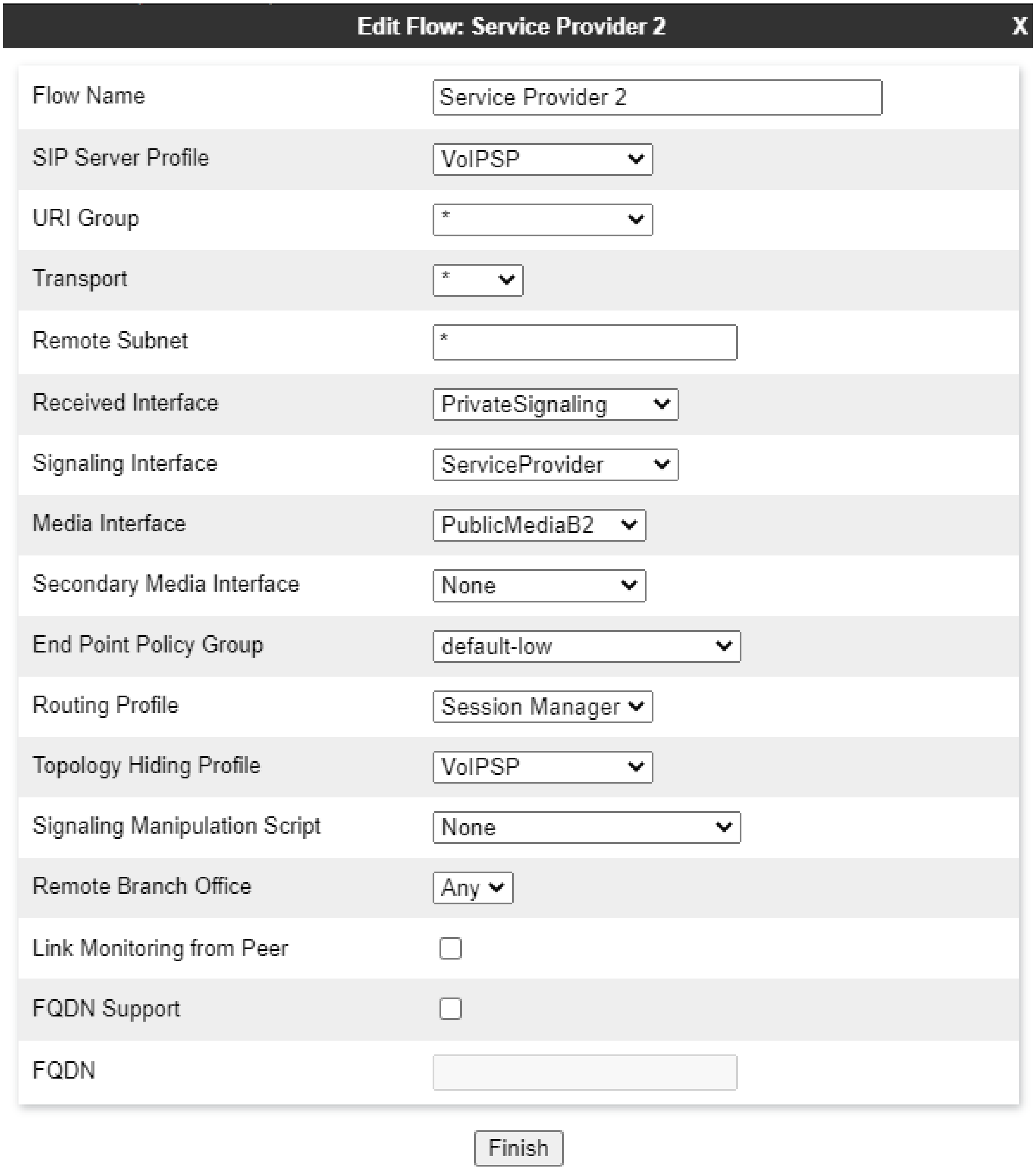
For the compliance test, two endpoint flows were created for VoIP Service Provider. If PCI Pal Agent Assist is available, the destination flow will be one of the PCI Pal flows in **Section 7.12.1**; otherwise, the destination flow will be one of the Session Manager flows in **Section 7.12.2**.

The *Service Provider 1* flow shown below is used as the source flow for inbound PSTN calls from the VoIP Service Provider. The routing profiles selects PCI Pal Agent Assist as the destination endpoint, if available; otherwise, Session Manager is selected as the destination endpoint.

This flow is also used as a destination flow for outbound PSTN calls from Session Manager. The Topology Hiding Profile is used for outbound PSTN calls to change the domain in the Request-URI and To header to the domain of the VoIP Service Provider.



The *Service Provider 2* flow shown below is used as the destination flow for outbound PSTN calls from Session Manager when PCI Pal Agent Assist is not available.



8. Configure PCI Pal Agent Assist

PCI Pal is responsible for the configuration PCI Pal Agent Assist.

PCI Pal will require that the customer provide the IP addresses and ports used to reach Avaya SBCE at the edge of the enterprise. In addition, TLS certificates must be exchanged.

PCI Pal will provide the IP addresses and ports of Agent Assist. This information is used to complete the SBCE configuration in the previous section.

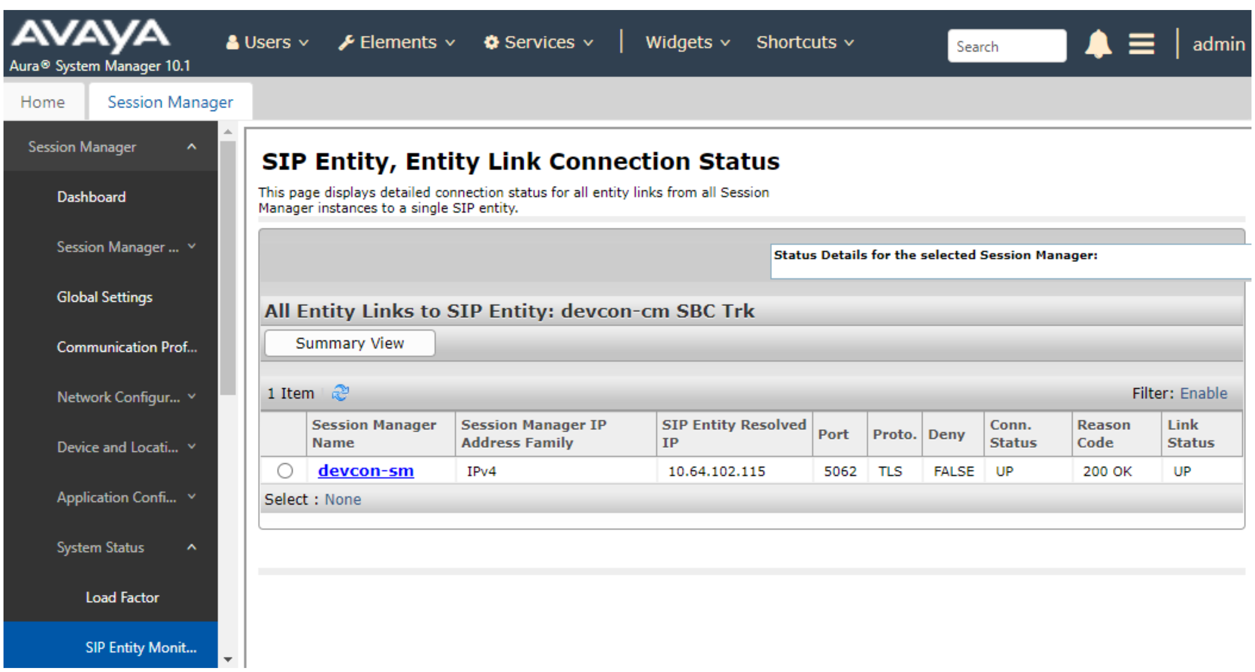
9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, SBCE, and PCI Pal Agent Assist.

1. From the System Manager home page (not shown), select **Elements → Session Manager** from the top menu to display the **Session Manager Dashboard** screen (not shown).

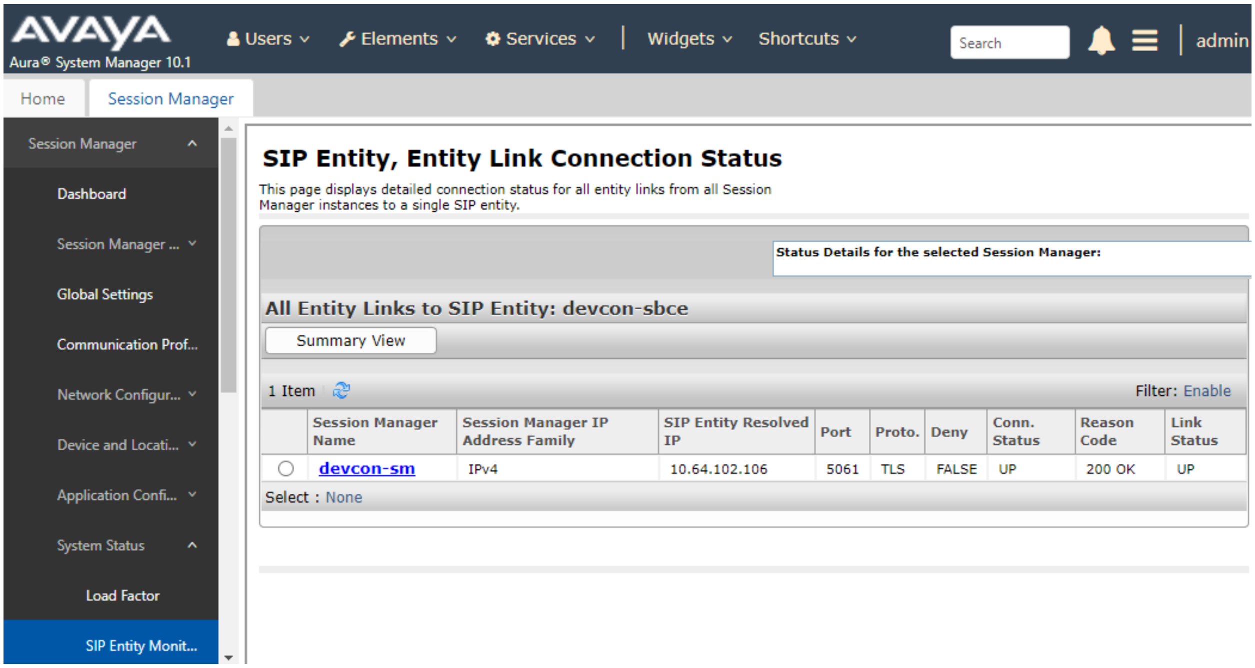
   Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the Communication Manager entity name from **Section 6.2.1**.

   The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn. Status** and **Link Status** are "UP", as shown below.



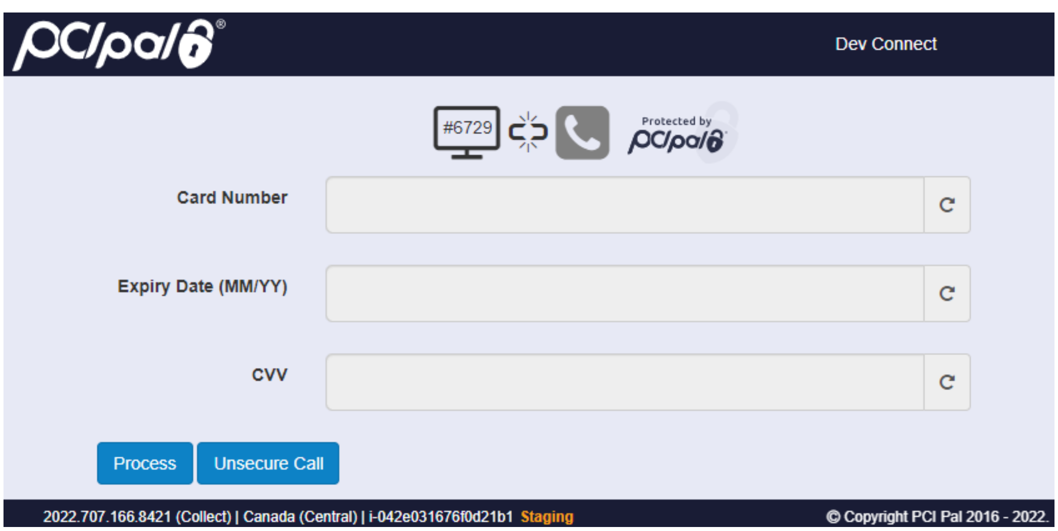
2. Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the SBCE entity name from **Section 6.2.2**.

   The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn. Status** and **Link Status** are "UP", as shown below.

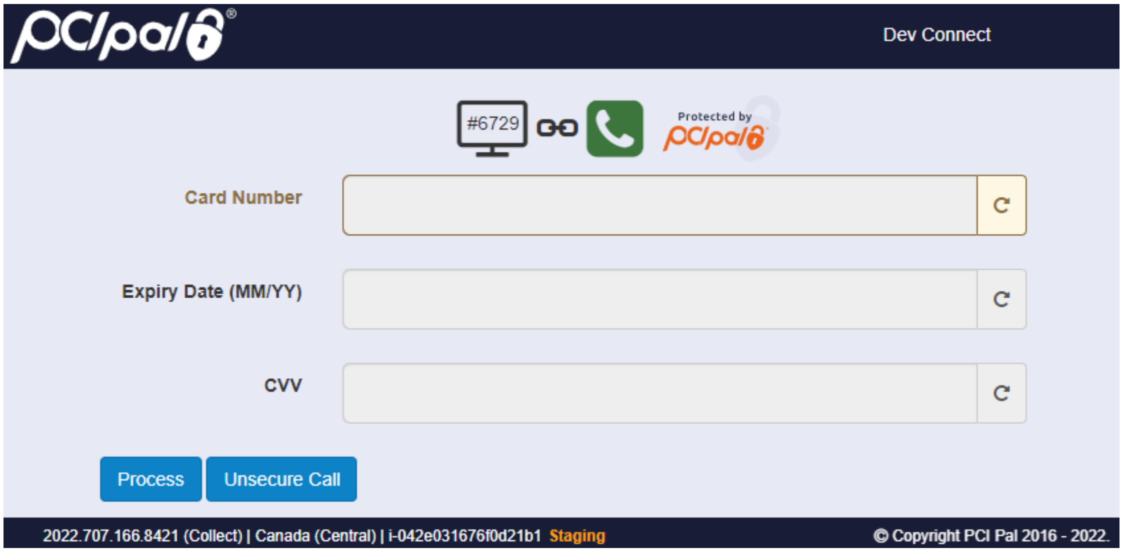


3. Place an incoming PSTN call from the VoIP Service Provider to an agent in the contact center. Verify the call is established with two-way audio.

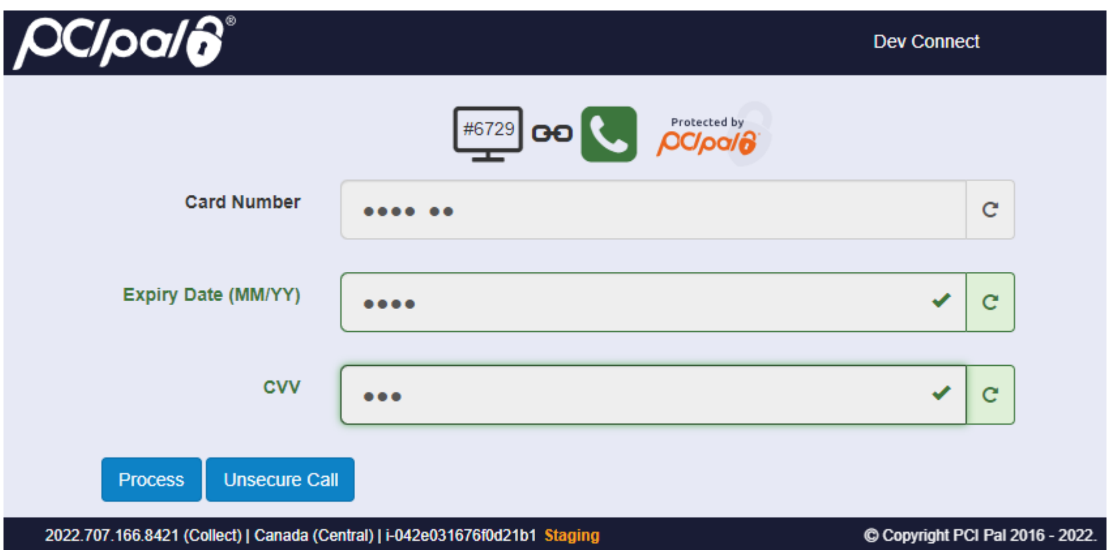
4. For the compliance test, a sample PCI Pal Portal was used to obtain a 4-digit code to secure the call. The PCI Pal Portal is displayed below.



5. Agent enters the 4-digit code via DTMF and the telephone icon in the PCI Pal Portal changes to green indicating the call is secured as shown below.



6. While the call is secured, customer sends payment information via DTMF using telephone keypad to PCI Pal Agent Assist. The fields in the PCI Pal Portal are populated with the customer information. The agent hears a mono tone for each DTMF digit sent indicating that the customer is entering data.



 Solution & Interoperability Test Lab Application Notes

10. Conclusion

These Application Notes have described the configuration steps required to integrate PCI Pal® Agent Assist with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise. Agents were able to secure customer calls so that card payment information could be sent via DTMF securely to PCI Pal Agent Assist. All test cases passed with an observation noted in **Section 2.2**.

11. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 1, December 2021, available at http://support.avaya.com.

[2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022, available at http://support.avaya.com.

[3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022, available at http://support.avaya.com.

[4] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1.x, Issue 1, December 2021, 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.