Avaya Solution & Interoperability Test Lab

Application Notes for VHT Mindful Callback 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 VHT Mindful Callback May 2021 Release with Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, and Avaya Session Border Controller for Enterprise 8.1. VHT Mindful Callback is a cloud-based, contact center solution that allows callers to hold for an agent or request a callback. Calls are routed between VHT Mindful Callback and an Avaya Call Center via Avaya Session Border Controller for Enterprise using SIP trunks.

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.

1. Introduction

These Application Notes describe the configuration steps required to integrate VHT Mindful Callback May 2021 Release with Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, and Avaya Session Border Controller for Enterprise 8.1. VHT Mindful Callback is a cloud-based, contact center solution that allows callers to hold for an agent or request a callback. Calls are routed between VHT Mindful Callback and an Avaya Call Center via Avaya Session Border Controller for Enterprise (Avaya SBCE) using SIP trunks. The VHT Mindful Callback SIP trunk was verified with both UDP/RTP and TLS/SRTP.

Callers initially make a call to an "Entry VDN" that essentially routes the call to VHT Mindful Callback. When VHT Mindful Callback answers the call, it provides the caller the option to hold for an agent or request a callback. Callers that decide to hold for an agent will be transferred by VHT Mindful Callback to an ACD queue on Avaya Aura® Communication Manager via the "Hold VDN." Callers that decide to be called back will be prompted for a callback number. VHT Mindful Callback tracks the caller position in the virtual queue. When it is time for the caller to be serviced from the virtual queue, VHT Mindful initiates the callback to the caller. When the callback is connected and accepted by the caller, VHT Mindful Callback then uses SIP to transfer the call to an ACD queue on Avaya Aura® Communication Manager via the "Callback VDN."

VHT Mindful Callback supports two call models for the callback flow, one uses a VHT Mindful Callback PSTN Gateway to call the customer, and the other is SIP Advanced, which uses the Avaya Aura® infrastructure to call the customer. Both call models were covered by the compliance test. VHT Mindful Callback PSTN Gateway calls the customer via the PSTN, without using the Avaya Aura® infrastructure, then once the customer has answered, VHT Mindful Callback calls the agent in the Avaya Call Center via Avaya SBCE. Once an agent has answered, VHT Mindful Callback bridges the customer and agent calls together.

The second call model, SIP Advanced, uses the Avaya Aura® infrastructure to place the call to the customer. When VHT Mindful Callback launches the callback, the customer is called by sending the SIP INVITE to Avaya SBCE, where it will either send the call request back out to the SIP service provider (or to Session Manager/Communication Manager where the call is routed out to the PSTN). Once the call is answered, VHT Mindful Callback initiates the agent call. For the compliance test, Avaya SBCE routed the customer call directly to the PSTN.

Alternatively, VHT Mindful Callback may be configured to place the callback to the agent first and then the customer.

2. General Test Approach and Test Results

The feature test cases were performed manually. Incoming customer calls from the PSTN were made to the entry VDN on Communication Manager, which collected User-to-User Information (UUI) and routed the call to VHT Mindful Callback. The test cases verified the ability of VHT Mindful Callback to transfer the customer to an agent or initiate a callback to the customer and connect them to an agent.

The UUI data test cases were performed by using vector variables to assign UUI data to inbound calls and verifying that it was delivered to VHT Mindful Callback by reviewing the SIP messages and checking the call details in the VHT Mindful Callback web interface.

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 VHT Mindful Callback utilized encryption capabilities of TLS/SRTP.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP trunk between VHT Mindful Callback and Avaya SBCE using UDP and TLS transport and verifying the exchange of SIP OPTIONS messages.
- Incoming and outgoing customer calls from VHT Mindful Callback to the SIP Service Provider, and vice versa, using UDP/RTP and TLS/SRTP and with Direct IP Media (Shuffling) enabled and disabled.
- G.711mu-law codec support.
- Incoming calls to VHT Mindful Callback and holding for an agent.
- Incoming calls to VHT Mindful Callback and requesting a callback.
- VHT Mindful Callback initiating a callback to the customer and then bridging the call to an agent. Also, verified callback to the "Agent First" and then to the customer.

- Verifying callback using VHT Mindful Callback PSTN Gateway and SIP Advanced as described in **Section 1**.
- Verified the exchange of UUI between VHT Mindful Callback and the Avaya Call Center.
- VHT Mindful Callback retry mechanism when callback fails due to ring no-answer, busy, customer rejecting callback, premature drop by customer, and customer abandoning call.

2.2. Test Results

All test cases passed.

2.3. Support

For technical support on VHT Mindful Callback, contact VHT Support Team through one of the following:

- **Phone:** + 1 (866) 670-2223 (USA)
  +44 (0)20 3633 4644 (EMEA)
  +1 330 670 2238 (International)
- **Website:** https://vhtcx.com/support/
- **Email:** support@vhctx.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of VHT Mindful Callback (cloud-hosted) with an Avaya Call Center. The Avaya Aura® environment consisted of the following products:

- SBCE with SIP trunk connectivity to VHT Mindful Callback, Session Manager, and SIP Service Provider.
- Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP telephones.
- Media resources in Avaya G450 Media Gateway and Avaya Aura® Media Server.
- Communication Manager with call center.
- System Manager used to configure Session Manager.
- Avaya 96x1 Series H.323 Deskphones and Avaya J100 Series SIP Deskphones.

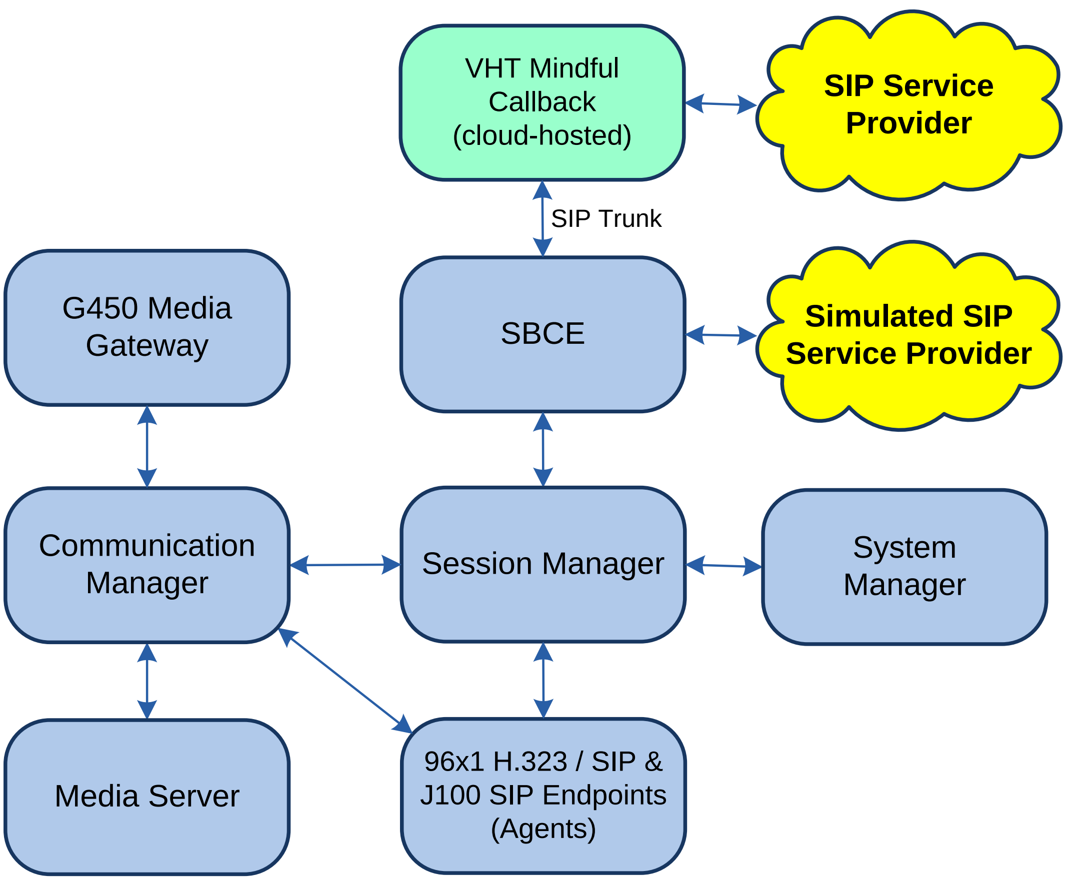


Figure 1: Avaya Aura® Environment with VHT Mindful Callback (Cloud-Hosted)

3.1. Call Flows

This section covers the relevant call flows for VHT Mindful Callback solution, including:

- Incoming Customer Calls
- Route to VHT Mindful Callback
- Hold for Agent
- Customer Callback

Refer to **Figure 1** to follow the call paths described in the following sections.

3.1.1. Incoming Customer Calls

Incoming customer calls arrived from the Simulated SIP Service Provider to an entry VDN on Communication Manager. This call flow was as follows:

Customer → Simulated SIP Service Provider → SBCE → Session Manager → Communication Manager (Entry VDN)

The entry VDN collected UUI and then routed the call to VHT Mindful Callback.

3.1.2. Route to VHT Mindful Callback

The entry VDN on Communication Manager routed the call to VHT Mindful Callback via the following call path:

Communication Manager → Session Manager → SBCE → VHT Mindful Callback

When VHT Mindful Callback answered the call, it provided the customer the options to hold for an agent or request a callback.

3.1.3. Hold for Agent

If the customer opts to hold for an agent, VHT Mindful Callback transferred the customer to the hold VDN, where the customer was placed in the ACD queue and eventually connected to an agent. The call path is as follows:

VHT Mindful Callback → SBCE → Session Manager → Communication Manager (Hold VDN)

3.1.4. Customer Callback

There are two call paths that the callback from VHT Mindful Callback could take depending on the call model being used, using a VHT Mindful Callback PSTN Gateway or SIP Advanced.

Note that the following sections describe the callback being made to the customer first and then the agent. However, VHT Mindful Callback could also be configured to place the callback to the agent first and then the customer. After both legs of the callback are made, VHT Mindful Callback bridges the two calls together.

3.1.4.1 VHT Mindful Callback PSTN Gateway

When using the VHT Mindful Callback PSTN Gateway, the callback to the customer followed this call path:

Customer Call
VHT Mindful Callback → SIP Service Provider → Customer

Agent Call
VHT Mindful Callback → SBCE → Session Manager → Communication Manager (Callback VDN)

3.1.4.2 SIP Advanced

When using SIP Advanced, the callback to the customer followed these call paths:

Customer Call
VHT Mindful Callback → SBCE → Simulated SIP Service Provider → Customer

Agent Call
VHT Mindful Callback → SBCE → Session Manager → Communication Manager (Callback VDN)

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	8.1.3.1.0-FP3SP1
Avaya G450 Media Gateway	FW 41.24.0
Avaya Aura® Media Server	v.8.0.2.138
Avaya Aura® System Manager	8.1.3.1 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.1.1012493 Service Pack 1
Avaya Aura® Session Manager	8.1.3.1.813113
Avaya Session Border Controller for Enterprise	8.1.2.0-31-19809 with Hotfix 2 (8.1.2.0-34-19941-hotfix-01222021)
Avaya 96x1 Series IP Deskphones	6.8502 (H.323)
Avaya J100 Series IP Deskphones	4.0.9.0.4 (SIP)
VHT Mindful Callback	May 2021 Release

5. Configure Avaya Aura® Communication Manager

This section provides the steps for configuring Communication Manager. It includes the SIP trunk between Communication Manager and Session Manager, call routing, and the sample vectors and VDNs used by the solution. Administration of Communication Manager was performed using the System Access Terminal (SAT). The procedures include the following areas:

- Administer IP Node Names
- Administer IP Codec Set
- Administer IP Network Region
- Administer SIP Trunk to Session Manager
- Administer Private Numbering
- Administer ARS Call Routing
- Administer Vectors and VDNs

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 to be used by the agents in the call center. 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, media encryption was enabled and G.711MU was used.

```
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:
```

5.3. Administer IP Network Region

In the **IP Network Region** form, specify the codec set to be used for VHT Mindful Callback and enable **IP-IP Direct Audio** (Shuffling), if desired. Shuffling allows audio traffic to be sent directly between IP endpoints 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: 1
Location: 1       Authoritative Domain: avaya.com
    Name:                       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
```

5.4. 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*.
- 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.

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? 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? 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 the VoIP Service Provider. Set the **Group Type** field to *sip*, set the **Service Type** field to *public-ntwrk*, 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   4
                                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*, **UUI Treatment** to *shared*, and **Maximum Size of UUI Contents** to *128*. 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**, set the **Telephone Event Payload Type** to *101* to avoid DTMF issues when a SIP agent attempts to accept a call prior to VHT Mindful Callback connecting the agent to the customer.

```
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
```

5.5. 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 10-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: 1
                                                          Maximum Entries: 540
```

5.6. 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  12
                               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: *81
                       Answer Back Access Code: *71
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *73    All: *74    Deactivation: *75
   Call Forwarding Enhanced Status:        Act: *84    Deactivation: *85
                         Call Park Access Code: *72
                       Call Pickup Access Code: *77
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

SIP calls to VHT Mindful Callback are routed through Session Manager over a SIP trunk via ARS call routing. Configure the ARS analysis form and add an entry that routes "19084605258" 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
    19084605258           11   11    11        fnpa         n
    19084957057           11   11    11        fnpa         n
    19086519420           11   11    11        fnpa         n
    191                   11   11     4        fnpa         n
    192                   11   11    deny      fnpa         n
    193                   11   11    deny      fnpa         n
```

Configure a preference in **Route Pattern** 11 to route calls over SIP trunk group 11 as shown below. This route pattern inserts a '+' to the dialed number as indicated by the 'p' in the **Inserted Digits** field.

```
change route-pattern 11                                         Page   1 of   4
                    Pattern Number: 11     Pattern Name: devcon-sm SBC
    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                p                                    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
```

5.7. Administer Vectors and VDNs

Administer three sets of vectors and VDNs shown below for routing of calls to Callback. Note that the VDN extensions and vector numbers can vary.

VDN	Vector	Purpose
77211	211	Entry vector & VDN called by customer. This vector collects UUI and routes calls to VHT Mindful Callback.
77212	212	Hold vector & VDN for queuing customer call to skill at medium priority
77213	213	Callback vector & VDN for queuing callback to skill at high priority

5.7.1. Entry Vector and VDN

Modify an available vector using the **change vector** command. The vector will be used to collect UUI and route the customer call to VHT Mindful Callback. Vector variables are configured via the **change variables** command (not shown).

Note that the vector **Number**, **Name**, **wait-time** and **route-to number** parameter settings may vary. Step 02 prompts the caller to enter 6 digits for UUI, and in step 03, stores the data in variable A (as configured in the Variables form not shown). Step 04 routes the call to VHT Mindful Callback. Note that the 9 prepended to number is the ARS feature access code. If the call to VHT Mindful Callback fails, step 06 routes the call to VDN 77212, the Hold VDN, where the customer is simply placed in the ACD queue.

```
display vector 211                                              Page   1 of   6
                                  CALL VECTOR

    Number: 211              Name: VHT Entry
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    0   secs hearing silence
02 collect      6    digits after announcement 70001    for none
03 set          A      = digits ADD   none
04 route-to     number 919084605258            cov n if unconditionally
05 wait-time    5   secs hearing ringback
06 route-to     number 77212                   cov n if unconditionally
07 wait-time    2   secs hearing silence
08 disconnect   after announcement none
09 stop
10
11
12

                       Press 'Esc f 6' for Vector Editing
```

Add a VDN using the **add vdn** command. Enter a descriptive **Name** and the vector number specified above for **Vector Number**. Retain the default values for all remaining fields.

```
add vdn 77211                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 77211
                                 Name*: Entry VDN
                           Destination: Vector Number        211
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none     Report Adjunct Calls as ACD*? n
```

5.7.2. Hold Vector and VDN

Modify an available vector to queue incoming calls to the ACD skill group at medium priority. Note that the vector **Number**, **Name**, **queue-to skill** and **wait-time** parameter settings may vary, and that *77* is the existing skill group number.

```
display vector 212                                             Page   1 of   6
                                  CALL VECTOR

    Number: 212              Name: VHT Hold
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 queue-to     skill 77   pri m
03 wait-time    30  secs hearing music
04 goto step    3             if unconditionally
05 disconnect   after announcement none
06 stop
07
08
09
10
11
12

                       Press 'Esc f 6' for Vector Editing
```

Add a VDN with an available extension as shown below. Enter a descriptive **Name** and the vector number specified above for **Vector Number**.

```
add vdn 77212                                               Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 77212
                                 Name*: Hold VDN
                           Destination: Vector Number        212
                     Attendant Vectoring? n
                    Meet-me Conferencing? n
                      Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none     Report Adjunct Calls as ACD*? n
```

5.7.3. Callback Vector and VDN

Modify an available vector to queue callback calls to the ACD skill group at high priority. Note that the vector **Number**, **Name**, **queue-to skill** and **wait-time** parameters may vary, and that *77* is the existing skill group number.

```
display vector 213                                              Page   1 of   6
                                  CALL VECTOR

    Number: 213              Name: VHT Callback
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 queue-to     skill 77   pri h
03 wait-time    30  secs hearing music
04 goto step    3             if unconditionally
05 disconnect   after announcement none
06 stop
07
08
09
10
11
12

                       Press 'Esc f 6' for Vector Editing
```

Add a VDN with an available extension as shown below. Enter a descriptive name for **Name**, and the vector number specified above for **Vector Number**.

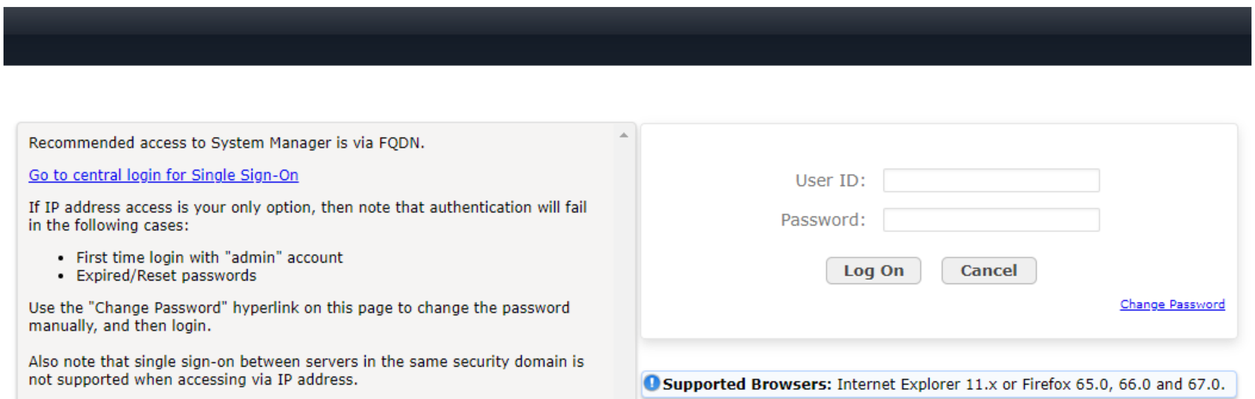
```
add vdn 77213                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 77213
                                 Name*: Callback VDN
                           Destination: Vector Number        213
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none     Report Adjunct Calls as ACD*? n
```

6. Configure Avaya Aura® Session Manager

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

- 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 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.

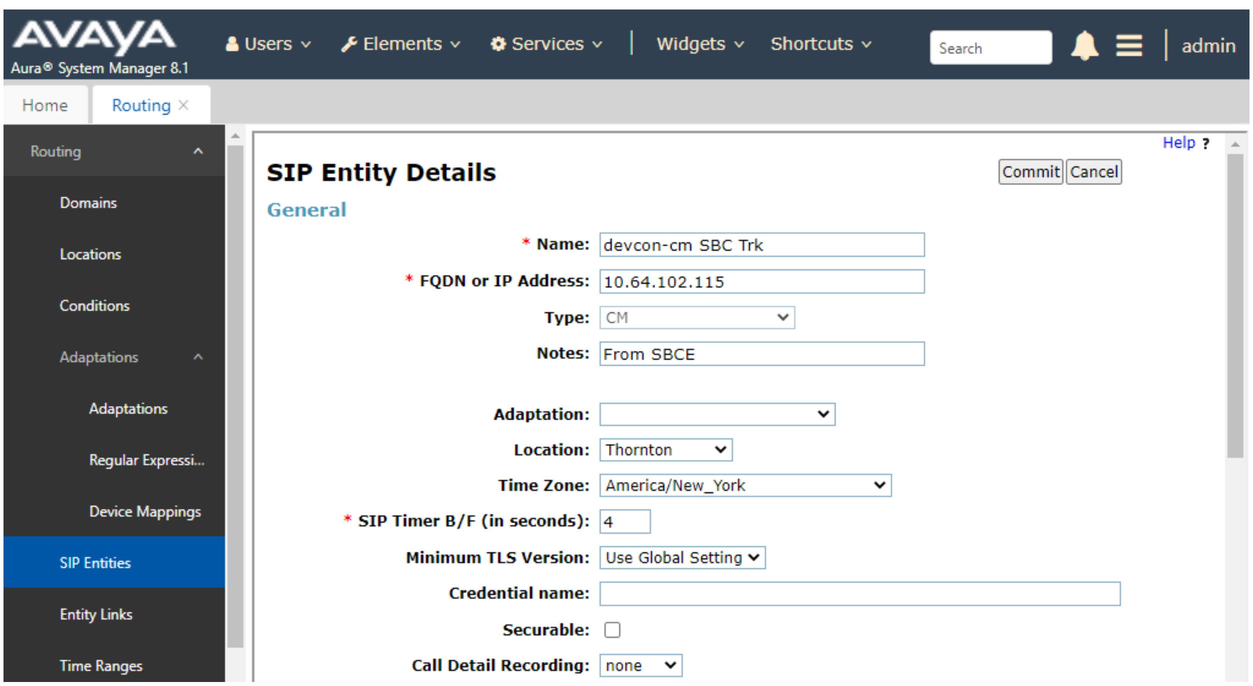
6.1.1. Avaya Aura® Communication Manager

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 Voice Spam Filter.

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

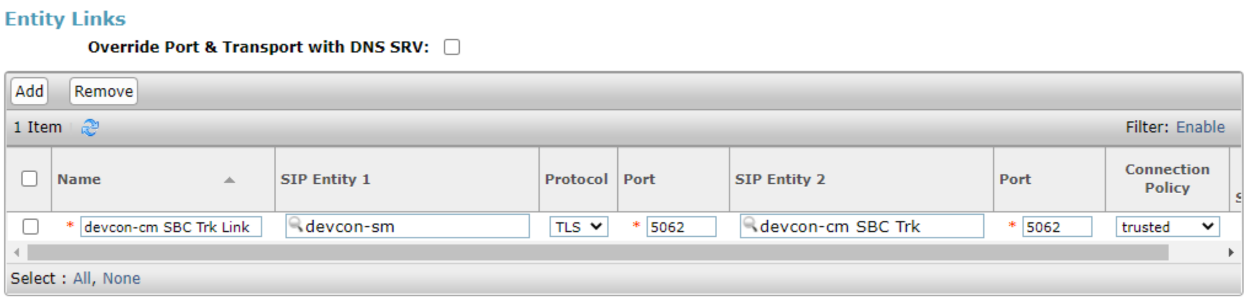
- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., procr) on the telephony system.
- **Type:** Select *CM*.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

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*.
- **Port:** Set to *5062*.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** Set to *5062*.
- **Connection Policy:** Set to *trusted*.

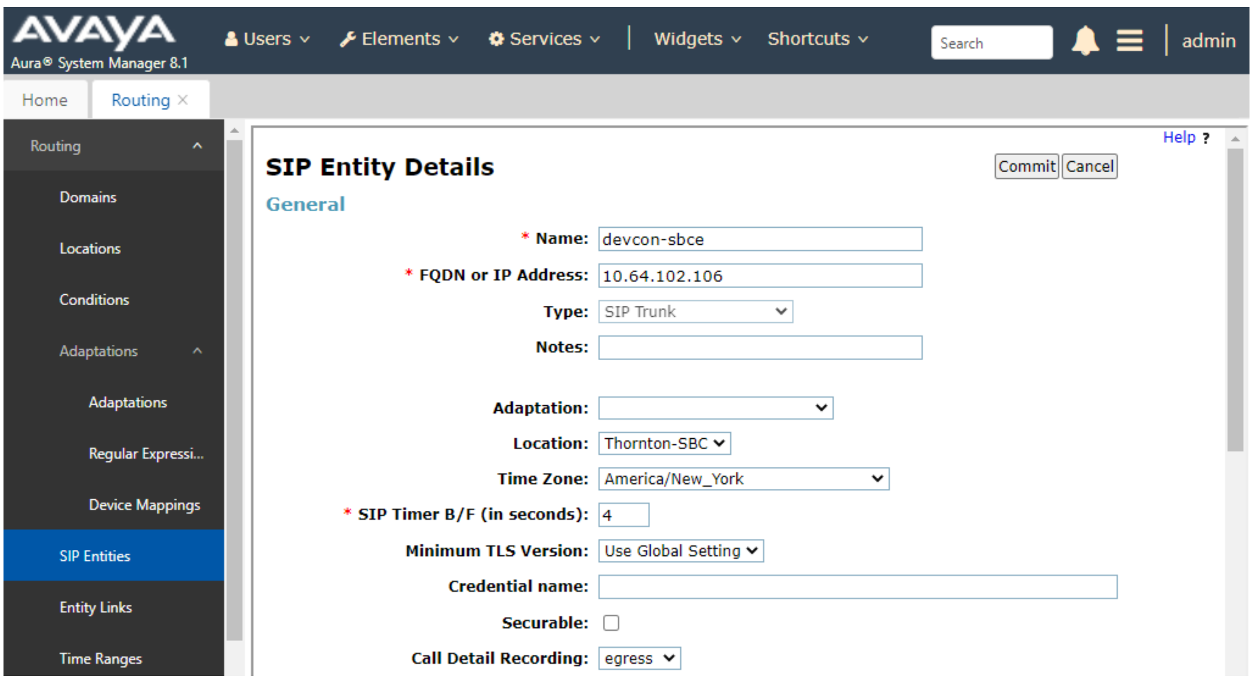


6.1.2. SIP Entity for SBCE

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.

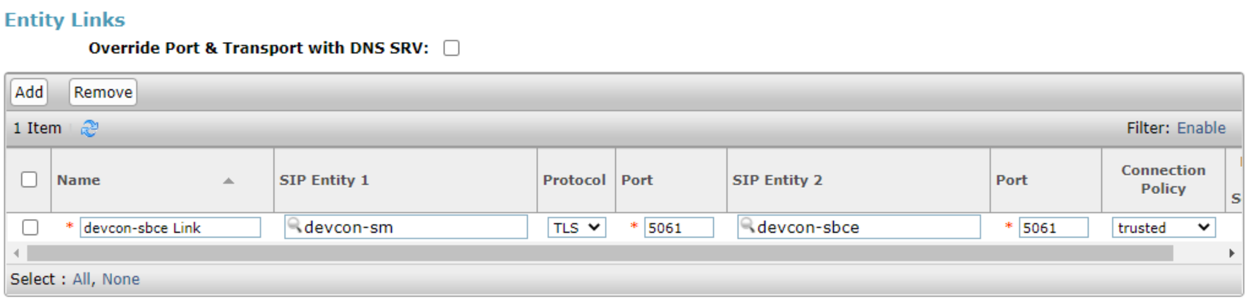
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the SBCE internal interface.
- **Type:** Select *SIP Trunk*.
- **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*.



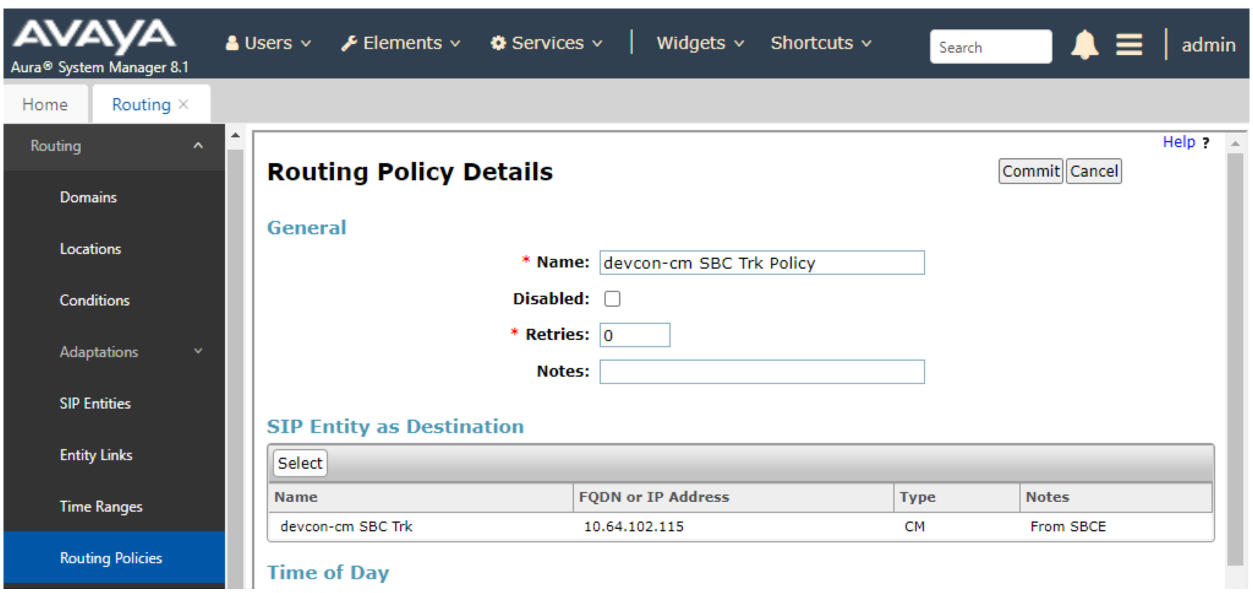
6.2. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.1**. A routing policy was added for Communication Manager to route incoming calls from VHT Mindful Callback or the SIP 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:

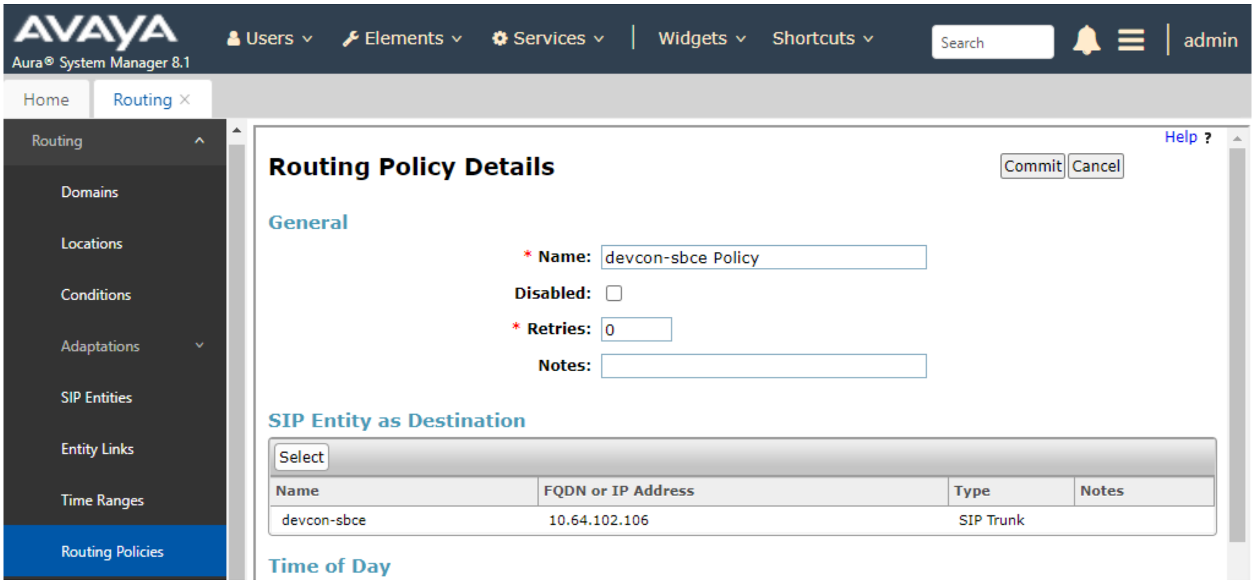
Under *General*:
Enter a descriptive name in **Name**.

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.



Another routing policy was added for SBCE, which routes outgoing calls to VHT Mindful Callback and the SIP Service Provider.



6.3. Add Dial Patterns

Dial patterns are defined to direct calls to the appropriate SIP Entity. In the sample configuration, 7-digit numbers beginning with *+1* are routed to Communication Manager.

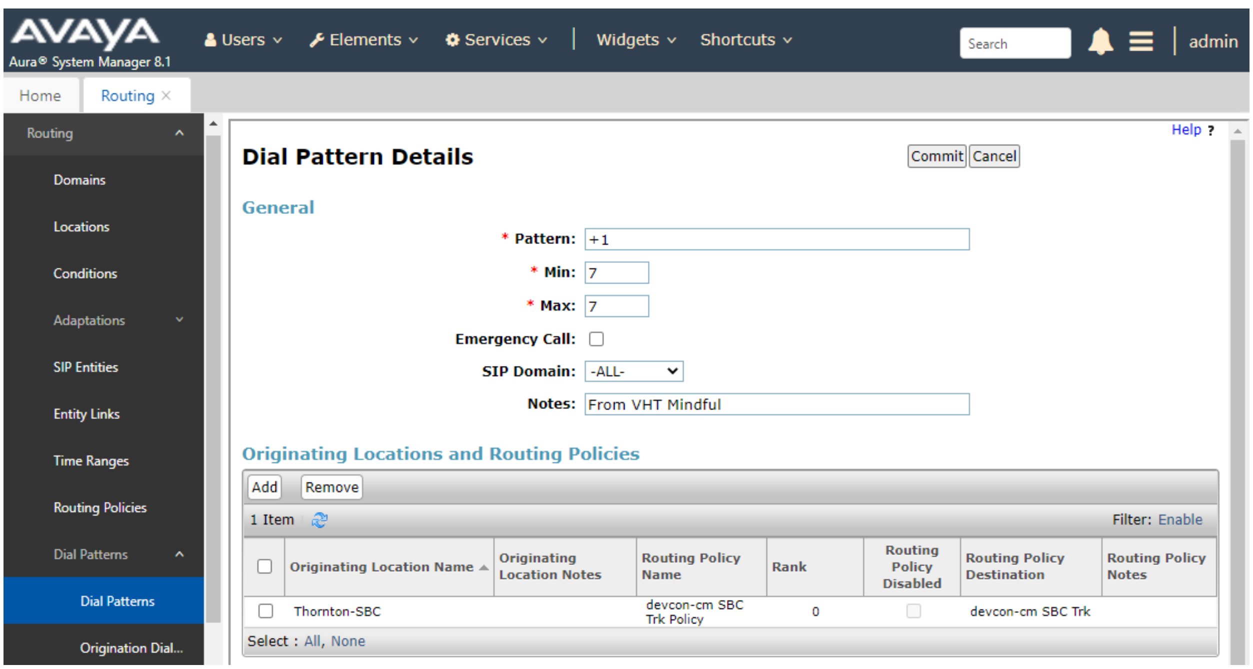
To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

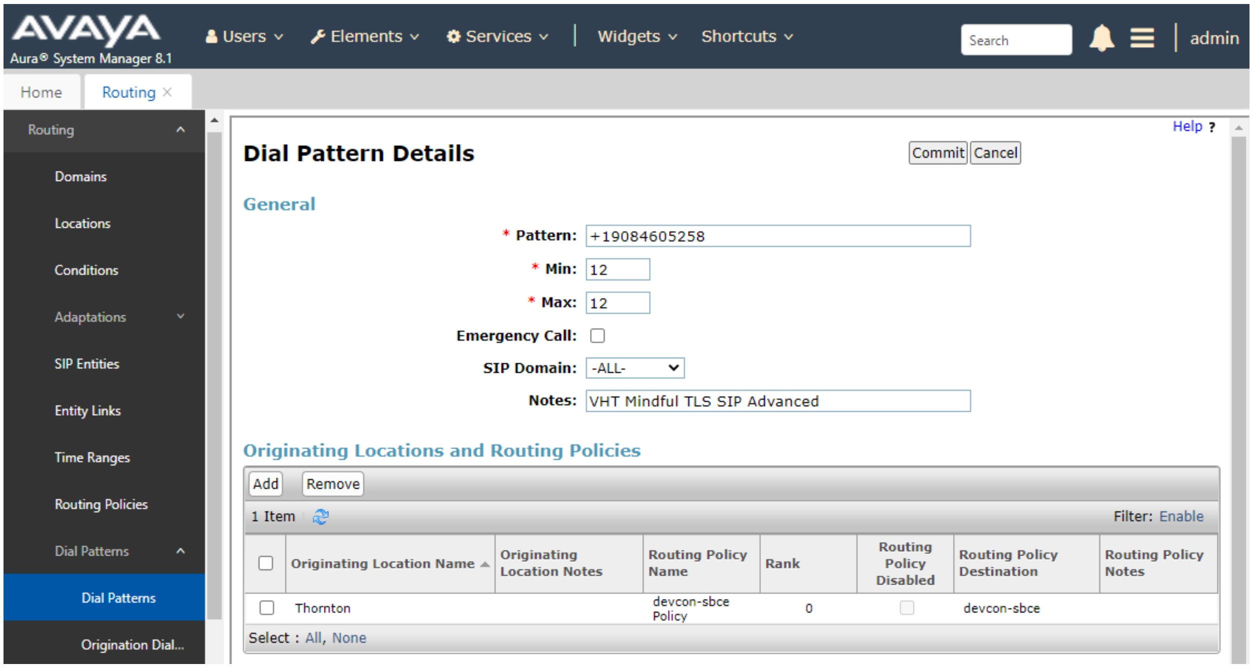
- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern (optional).

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 from VHT Mindful Callback to Communication Manager.



A Dial Pattern was also created for "+19084605258" that is used to route calls to VHT Mindful Callback via SBCE. Other call target numbers assigned to VHT Mindful Callback should be added as dial patterns.



6.4. 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:

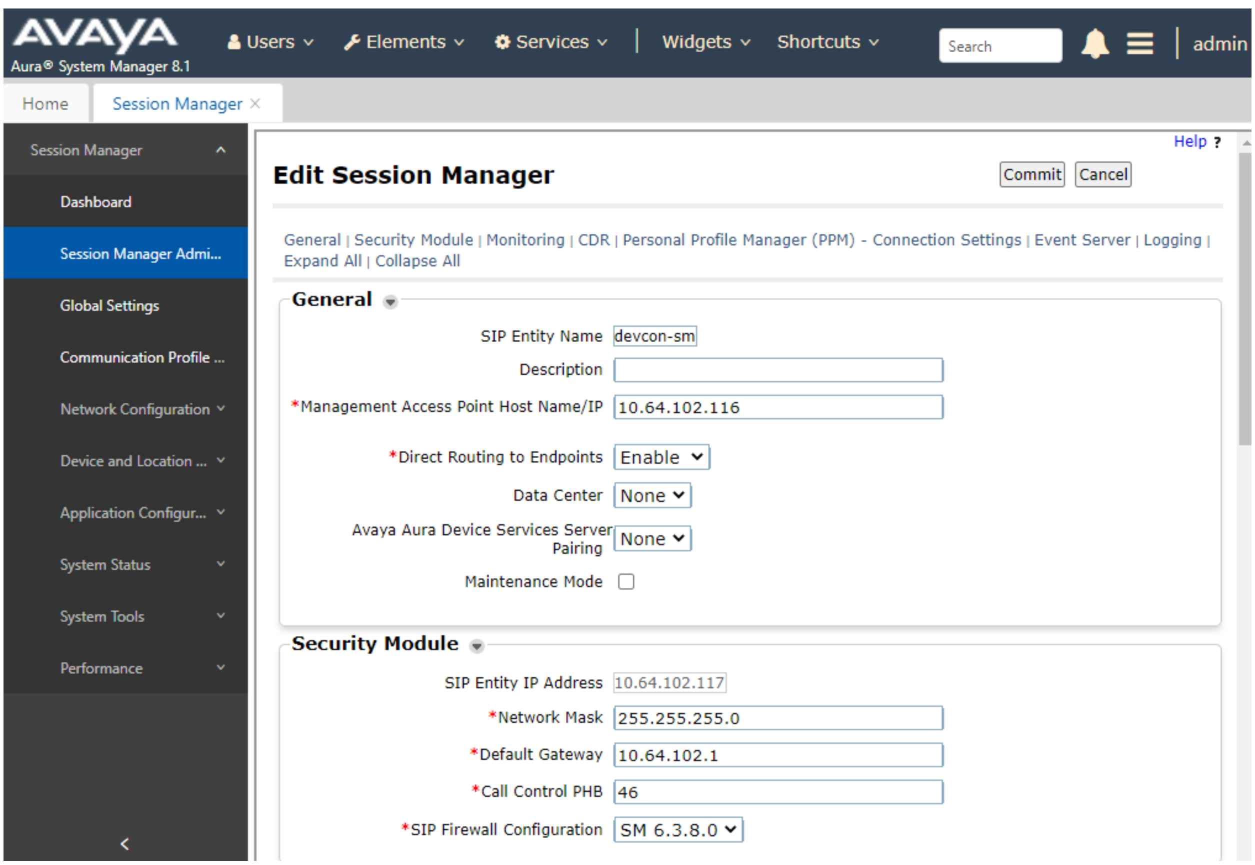
Under *General*:

- **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

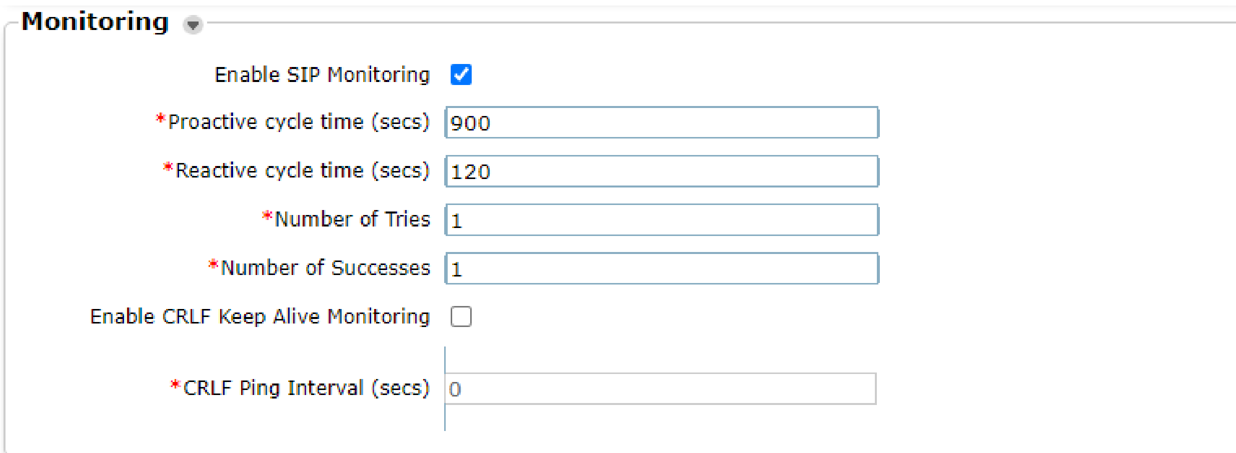
Under *Security Module*:

- **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 *900* 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, SIP Service Provider, and VHT Mindful Callback.

This section covers the following SBCE configuration:

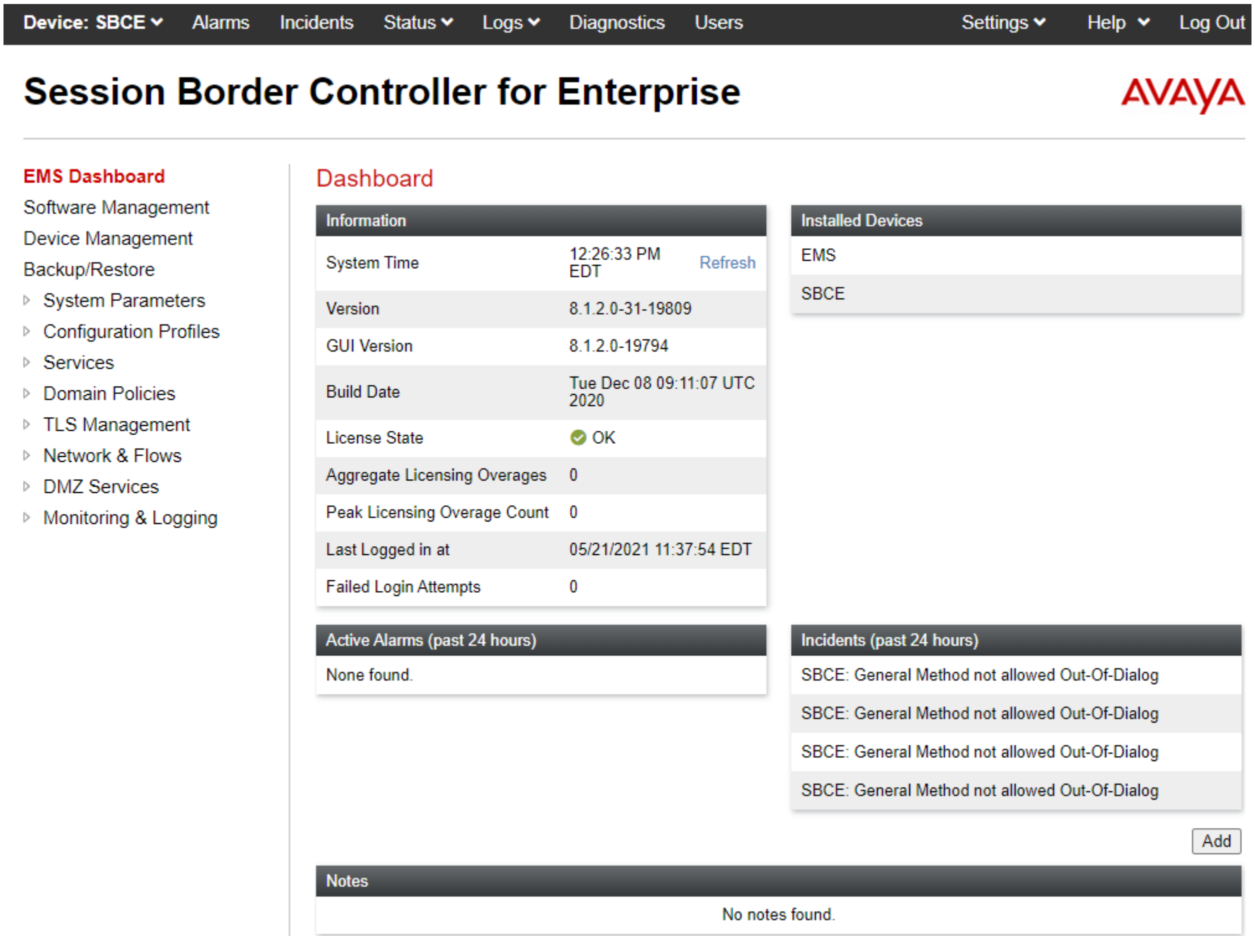
- Launch SBCE Web Interface
- Administer Server Interworking Profiles
- Administer SIP Servers
- Administer URI Groups
- Administer Routing Profiles
- Administer Topology Hiding
- Administer Media Rules
- Administer End Point Policy Groups
- Administer Media Interfaces
- Administer Signaling Interfaces
- 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.

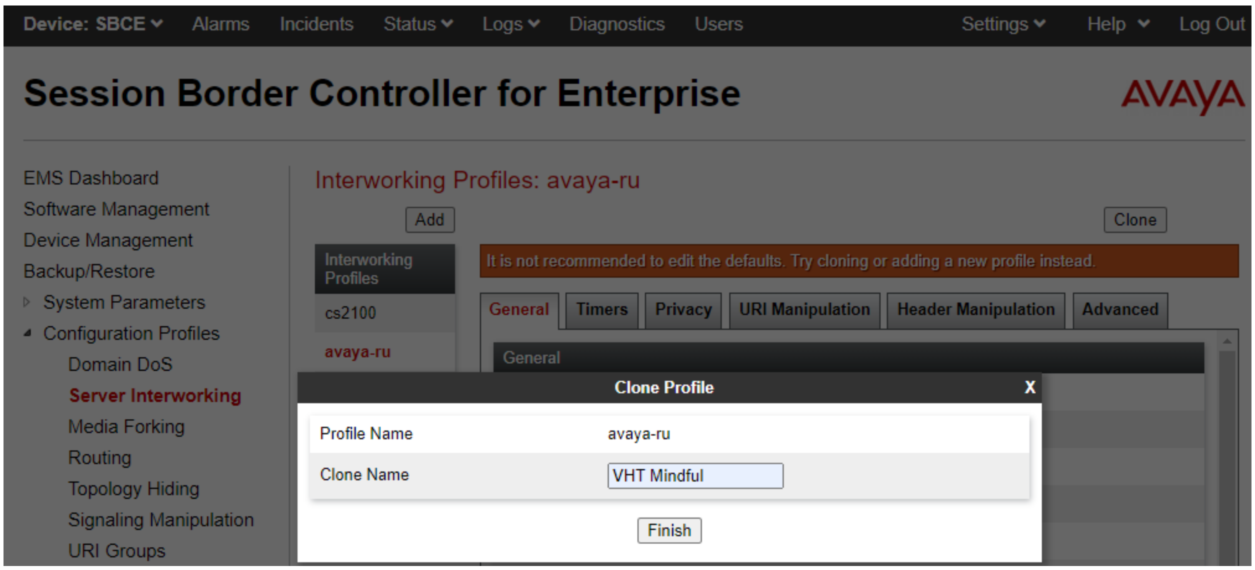


7.2. Administer Server Interworking Profiles

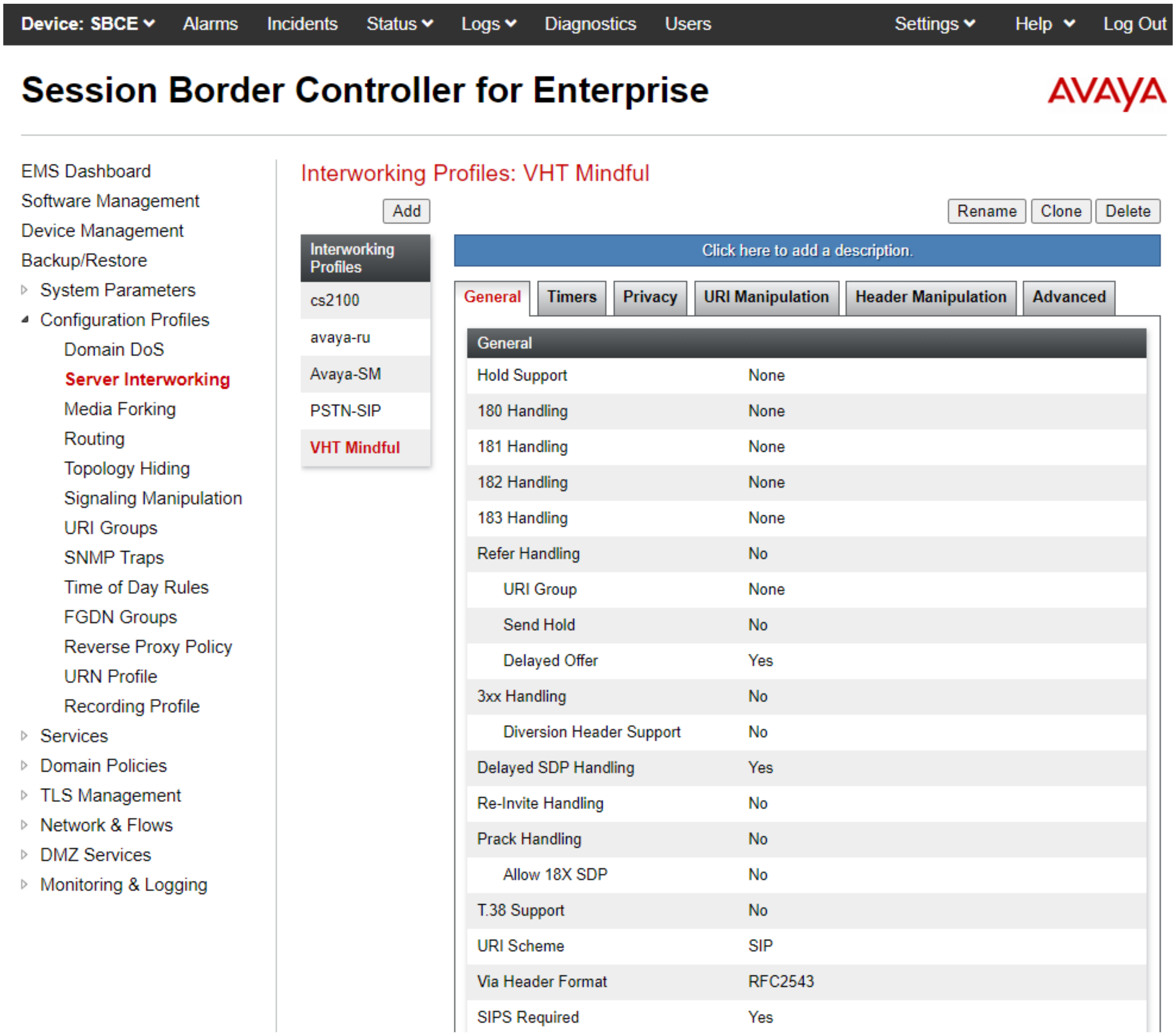
A server interworking profile defines a set of parameters that aid in interworking between the SBCE and a connected server. Add Interworking profile for VHT Mindful Callback, Session Manager, and SIP Service Provider.

7.2.1. Server Interworking Profile for VHT Mindful Callback

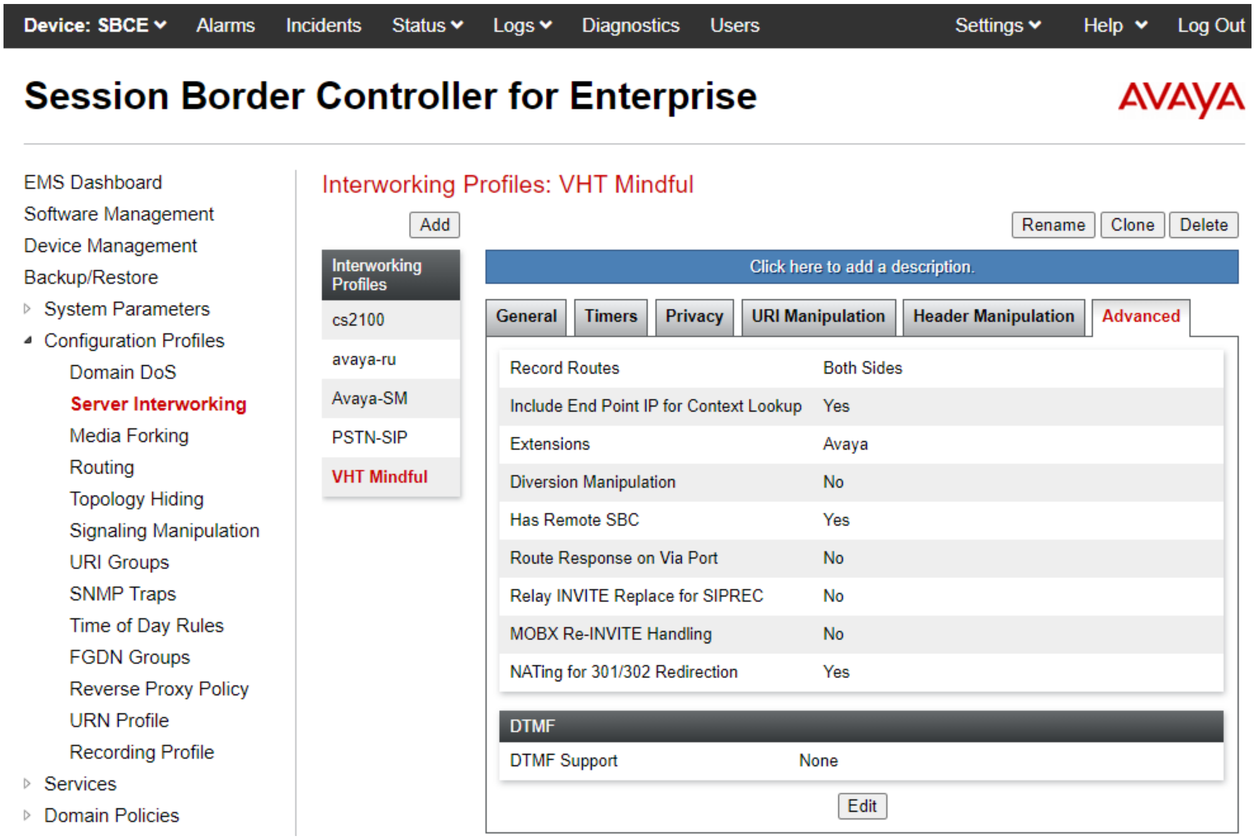
To create a new **Server Interworking** profile, select **Configuration Profiles → Server Interworking** from the left-hand menu. A new profile may be cloned from an existing profile. Select the **avaya-ru** profile and click **Clone**. Type in a **Clone Name** for VHT Mindful Callback. Select **Finish**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



Once added, select the VHT Mindful Callback profile and select the **General** tab and enable **Delayed SDP Handling**. This is required to work with agents using Avaya H.323 deskphones while Direct IP Media (i.e., shuffling) is enabled.



The **Advanced** tab was configured with the default settings.



7.2.2. Server Interworking Profile for Session Manager

Session Manager profile was cloned from the same **avaya-ru** profile.

7.2.3. Server Interworking Profile for SIP Service Provider

VoIP Service Provider profile was also cloned from the same **avaya-ru** profile.

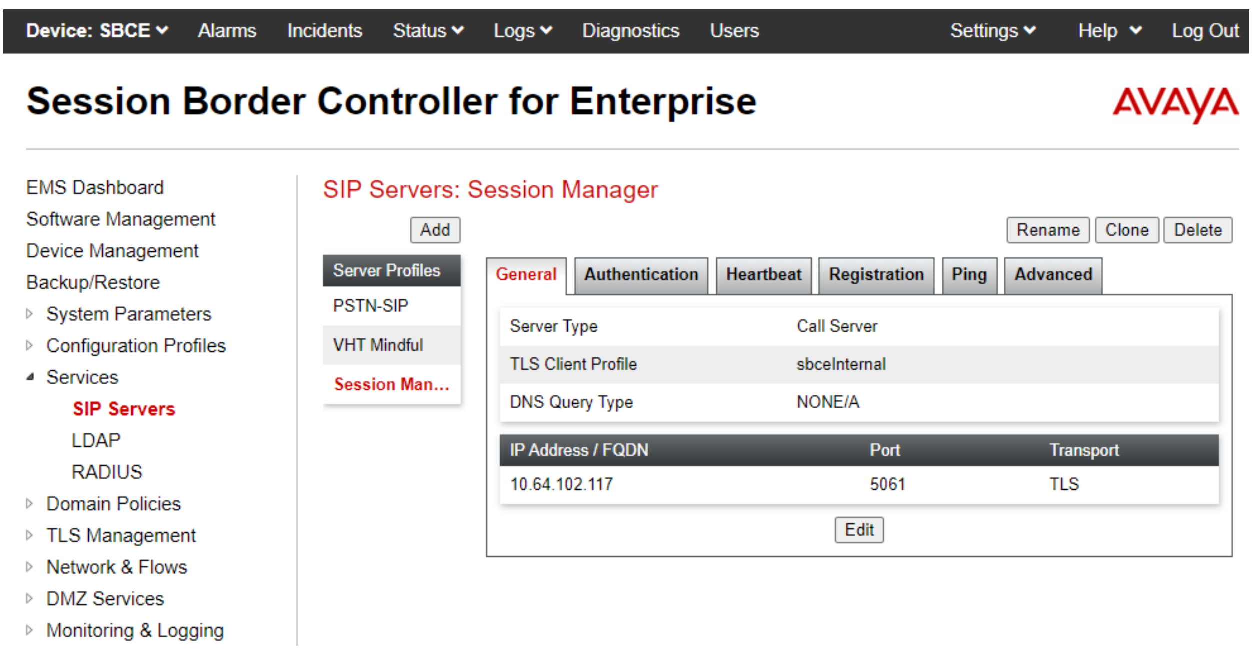
7.3. Administer SIP Servers

A SIP server definition is required for each server connected to SBCE. Add a **SIP Server** for Session Manager, VHT Mindful Callback, and SIP Service Provider. TLS transport was used for the SIP trunks to Session Manager and VHT Mindful Callback.

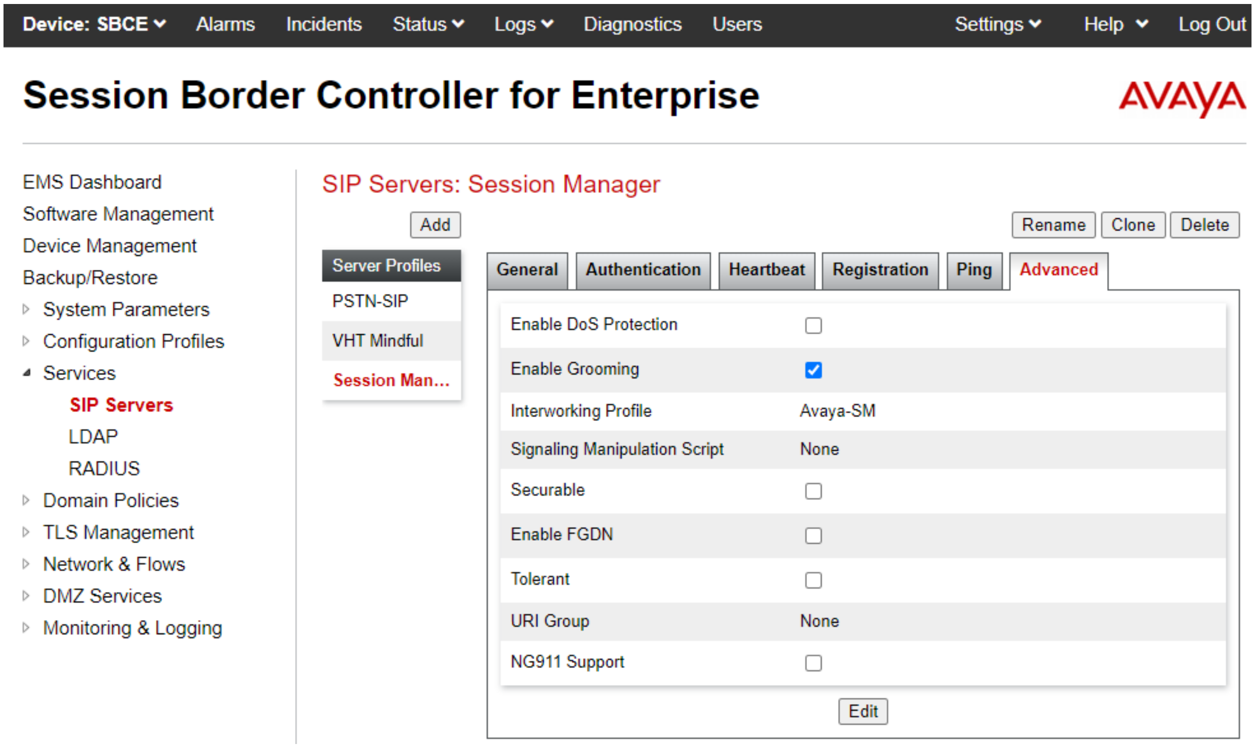
Note: TLS profiles were preconfigured and are not shown in these Application Notes. The TLS certificate used for the Session Manager SIP trunk was signed by System Manager. The TLS certificate used for the VHT Mindful Callback was provided by VHT.

7.3.1. 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.

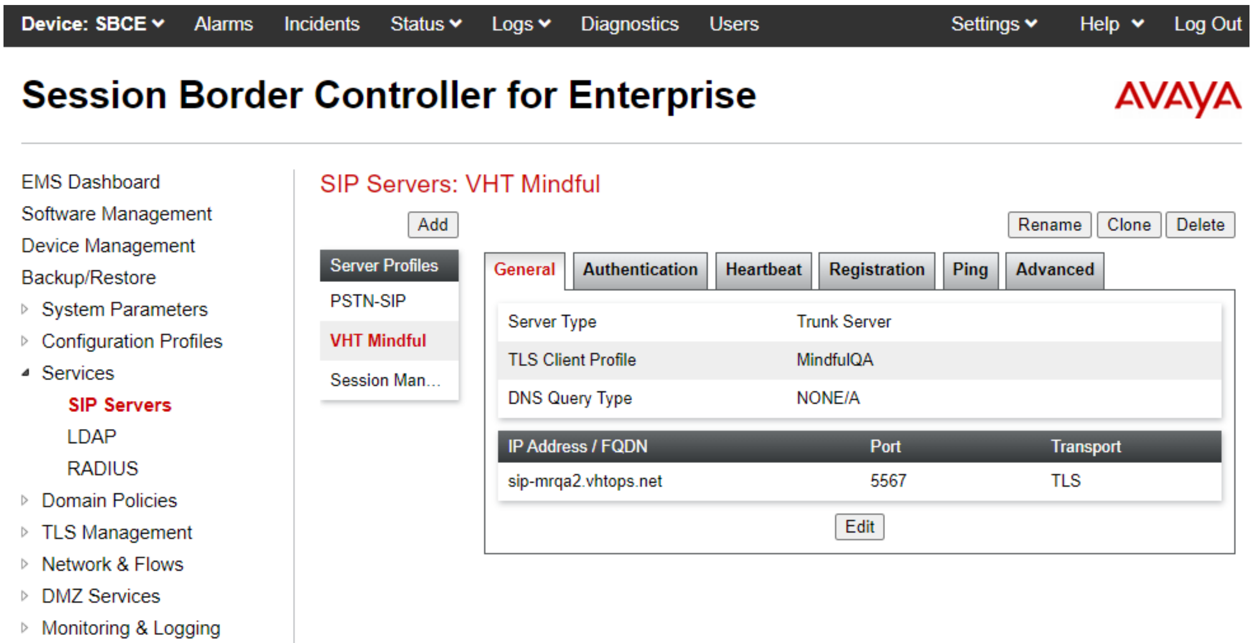


The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 7.2.2**. All other tabs were left with their default values.

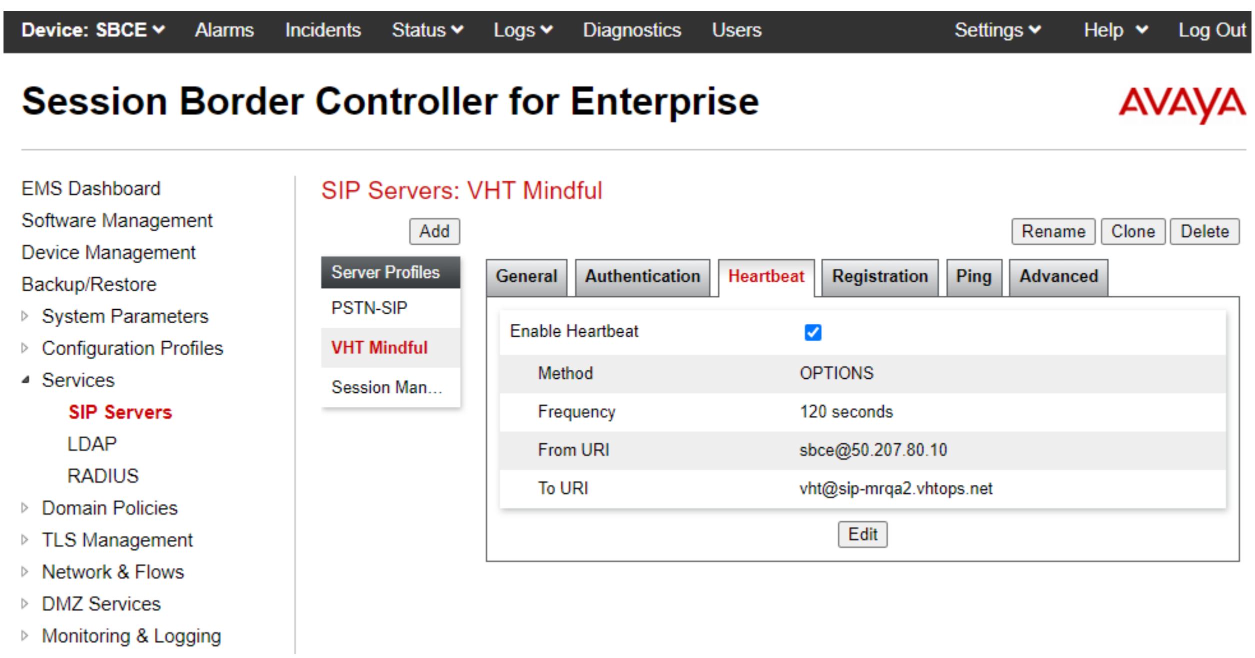


7.3.2. SIP Server for VHT Mindful Callback

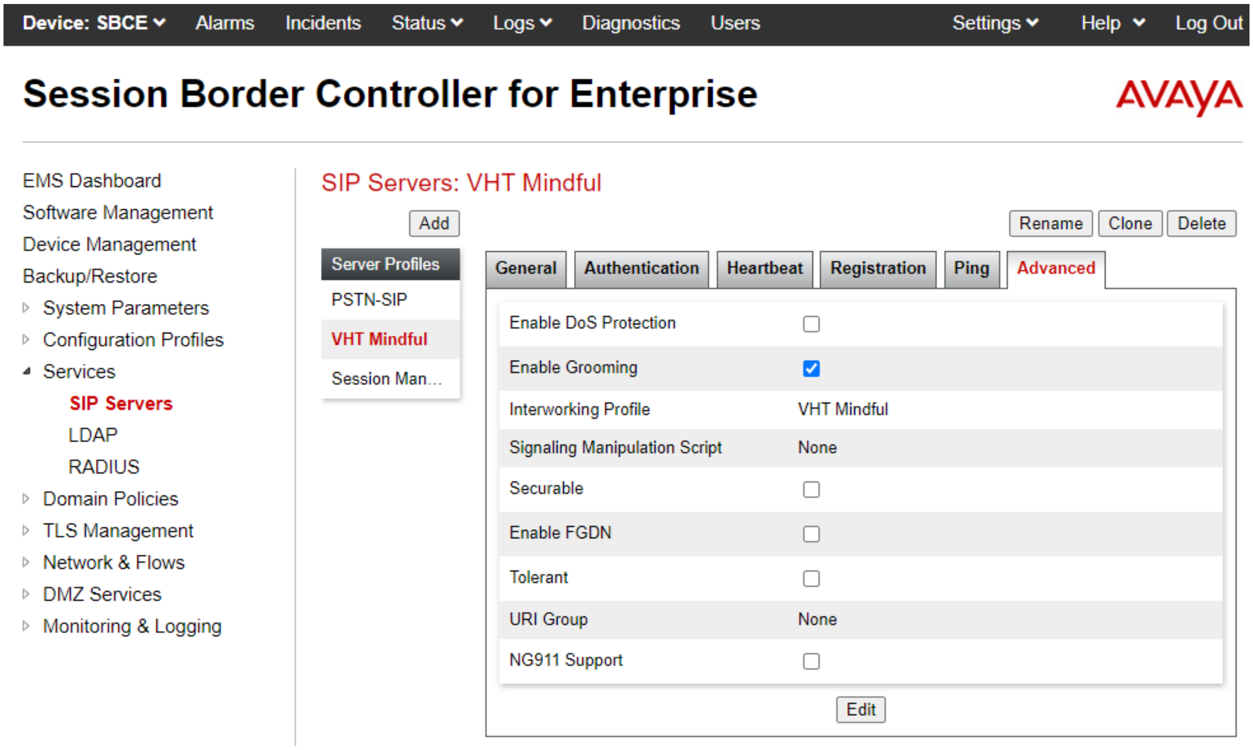
The **General** tab of the VHT Mindful Callback SIP Server was configured as shown below. TLS transport was used for the VHT Mindful Callback SIP trunk. The **TLS Client Profile** was installed under **TLS Management → Client Profiles** (not shown). The TLS certificate was provided by VHT.



The Heartbeat tab was configured as follows so that Avaya SBCE would send SIP OPTIONS to VHT Mindful Callback.

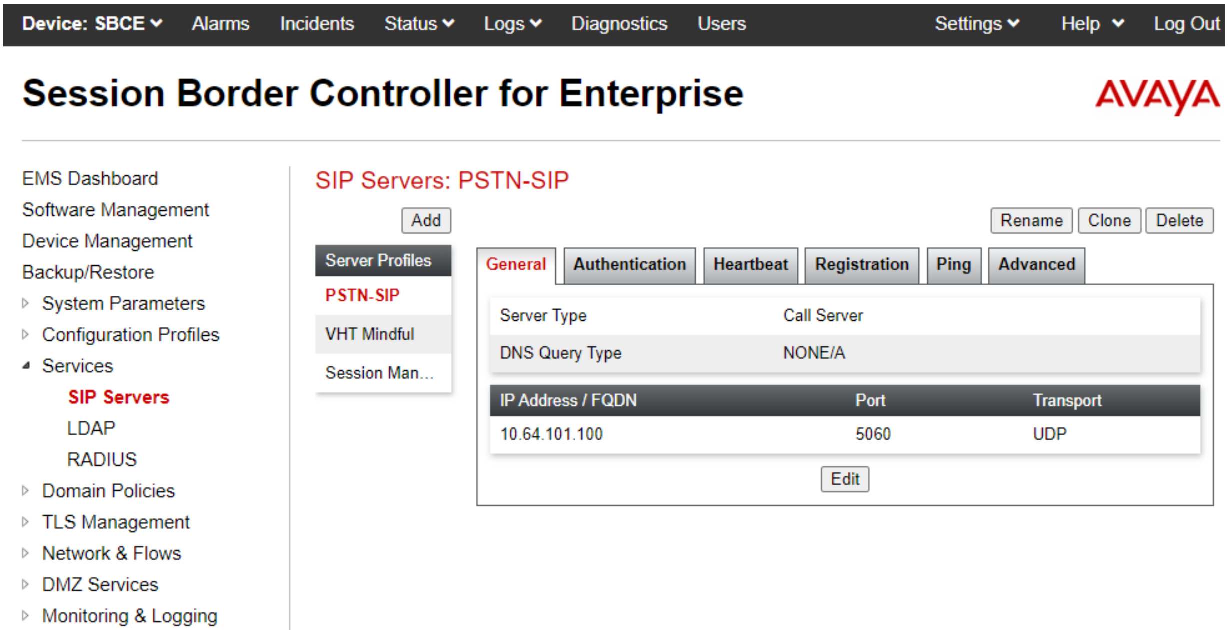


The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 7.2.1**. All other tabs were left with their default values.

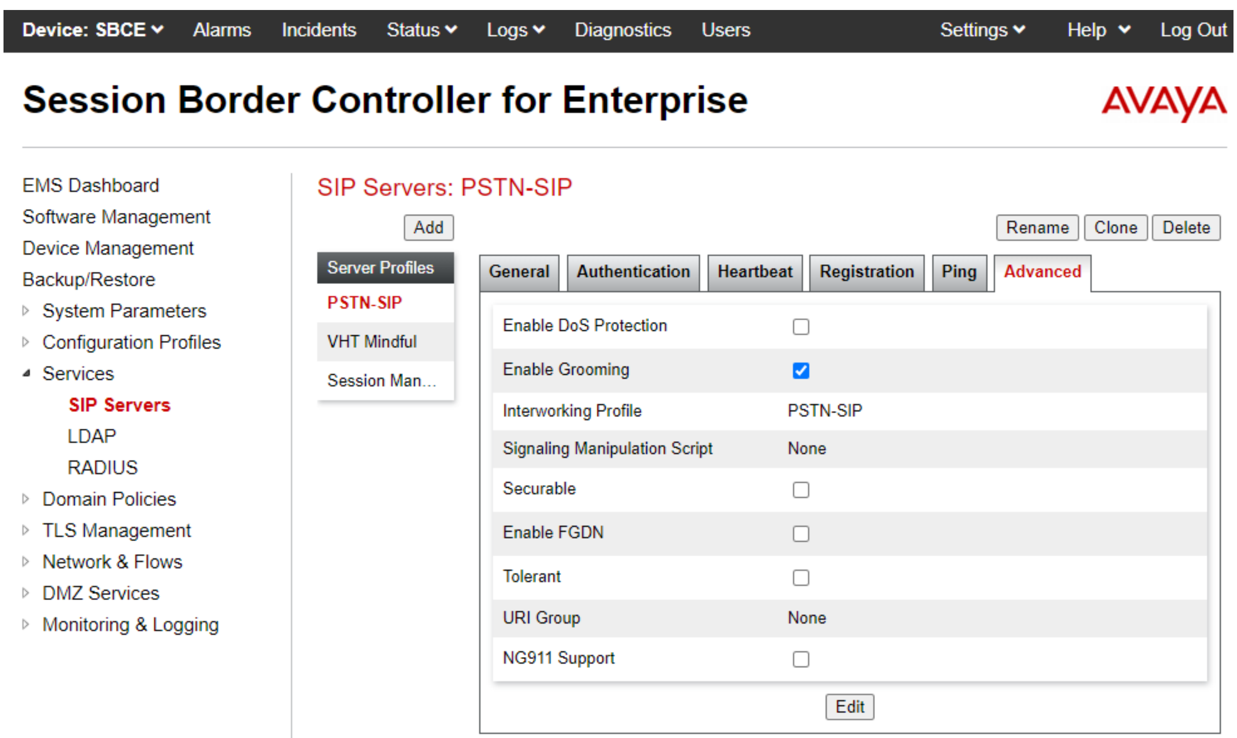


7.3.3. SIP Server for VoIP Service Provider

The **General** tab of the SIP Service Provider SIP Server was configured as shown below. UDP transport was used for the SIP Service Provider SIP trunk.



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.

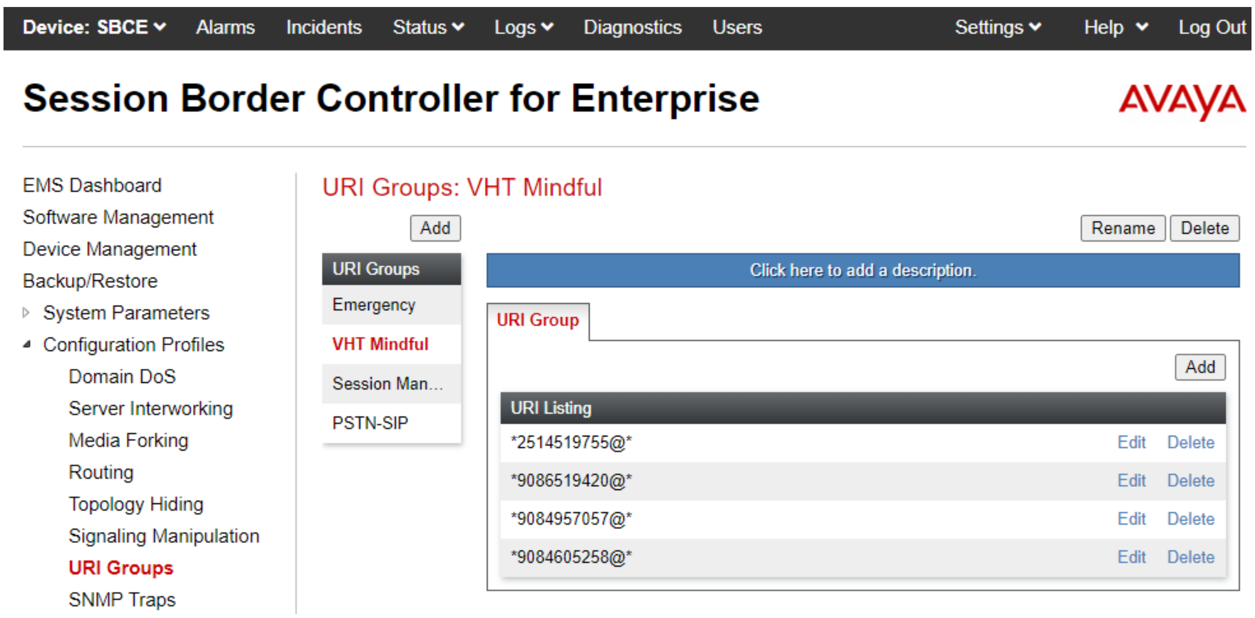


7.4. Administer URI Groups

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, three **URI Groups** were created that were associated with VHT Mindful Callback, Session Manager, and the SIP Service Provider. These **URI Groups** are assigned to **Routing Profiles** in **Section 7.5**. Avaya SBCE will select a particular route if a SIP URI entry in the URI group associated with a route matches the SIP URI in the To header of the SIP Invite.

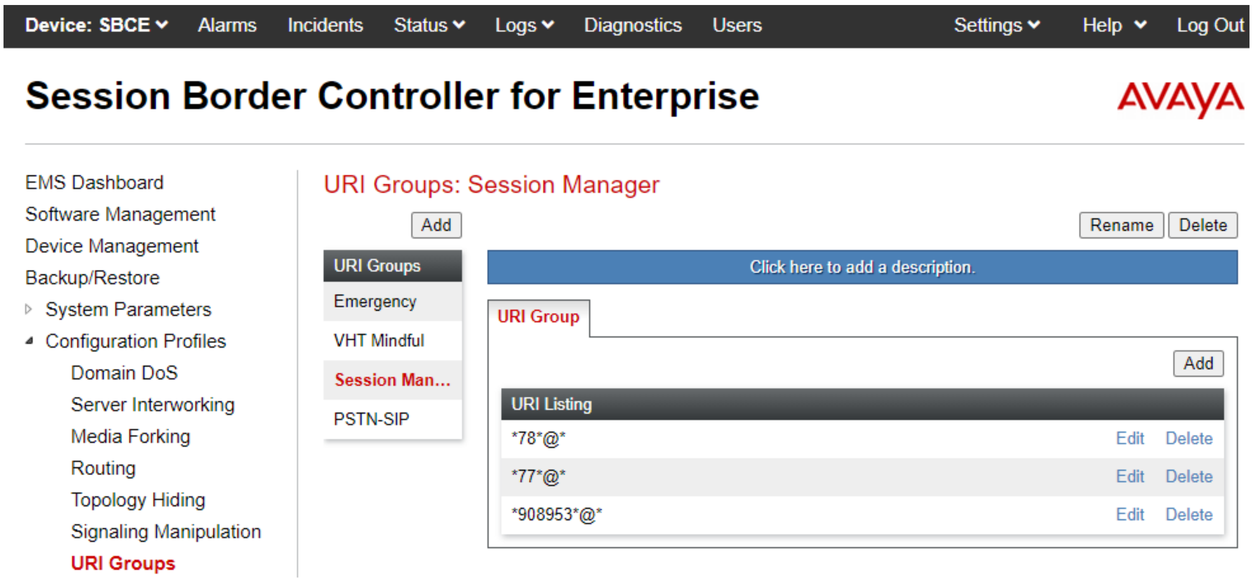
7.4.1. VHT Mindful Callback URI Group

The following URI Group is associated with VHT Mindful Callback. This URI Group covers SIP URIs that are routed to VHT Mindful Callback. These SIP URIs include call targets configured on VHT Mindful Callback.



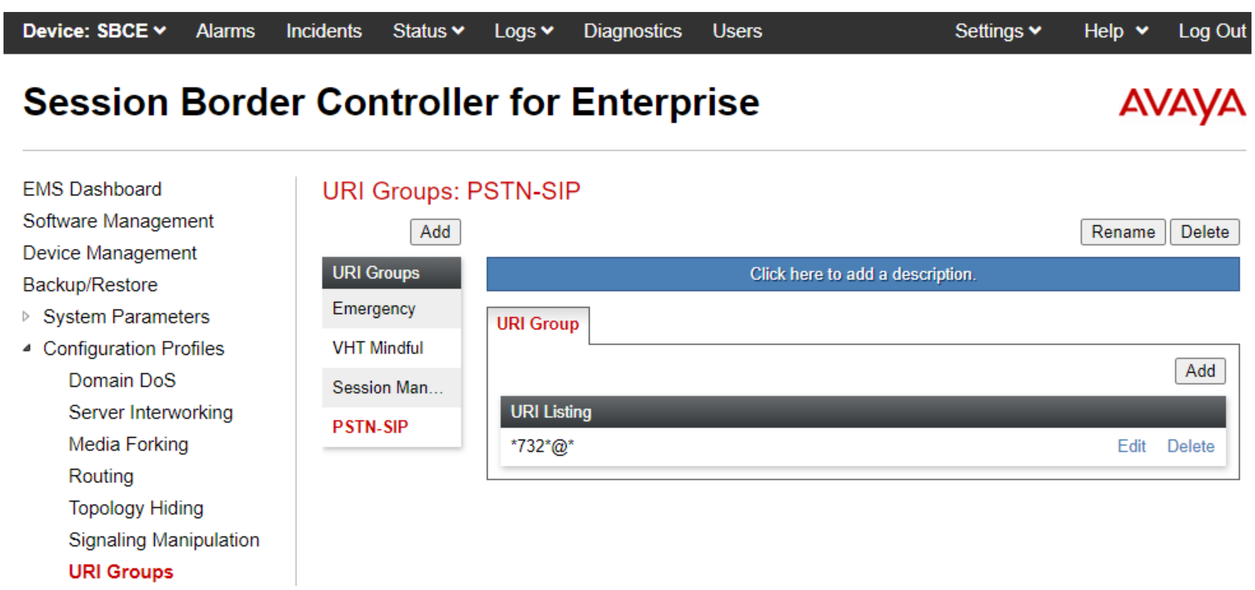
7.4.2. Session Manager URI Group

The following URI Group is associated with Session Manager. This URI Group covers SIP URIs that are routed to Session Manager. These SIP URIs include the VDN numbers, Communication Manager local extensions, and PSTN numbers that are routed via Communication Manager using SIP Advanced.



7.4.3. SIP Service Provider URI Group

The following URI Group is associated with the SIP Service Provider. This URI Group covers SIP URIs that are routed to the PSTN via the SIP Service Provider.



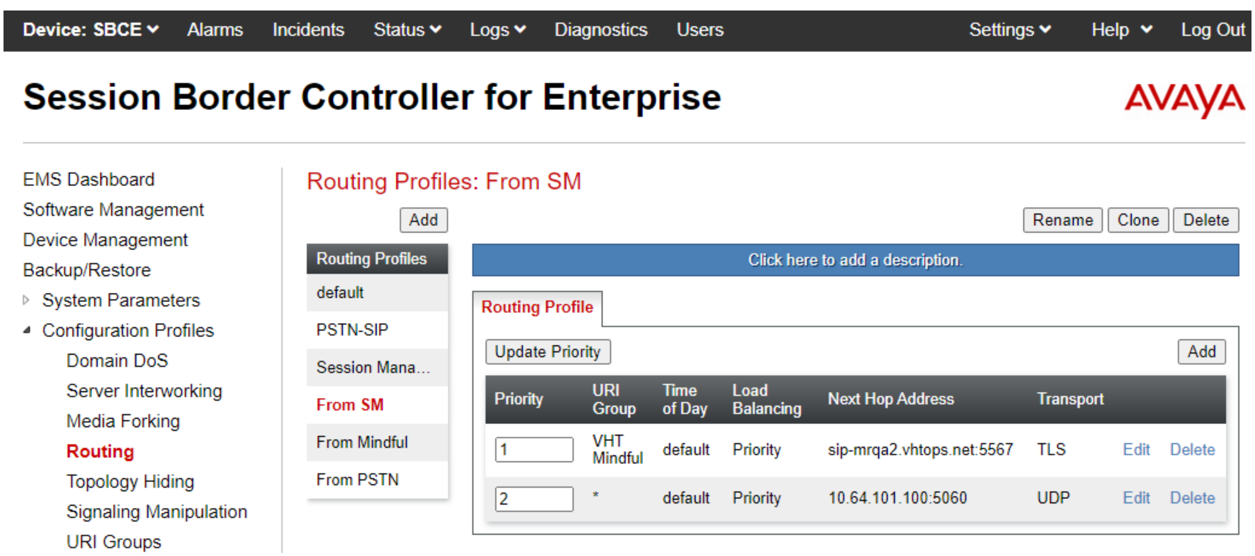
7.5. Administer Routing Profiles

A routing profile defines where traffic will be directed based on the contents of the Request-URI. A routing profile is applied only after the traffic has matched an End Point Flow defined in **Section 7.11**. The IP addresses and ports defined here will be used as destination addresses for signaling. Create a routing profile for Session Manager, VHT Mindful Callback, and SIP Service Provider.

7.5.1. Routing Profile used for Calls from Session Manager

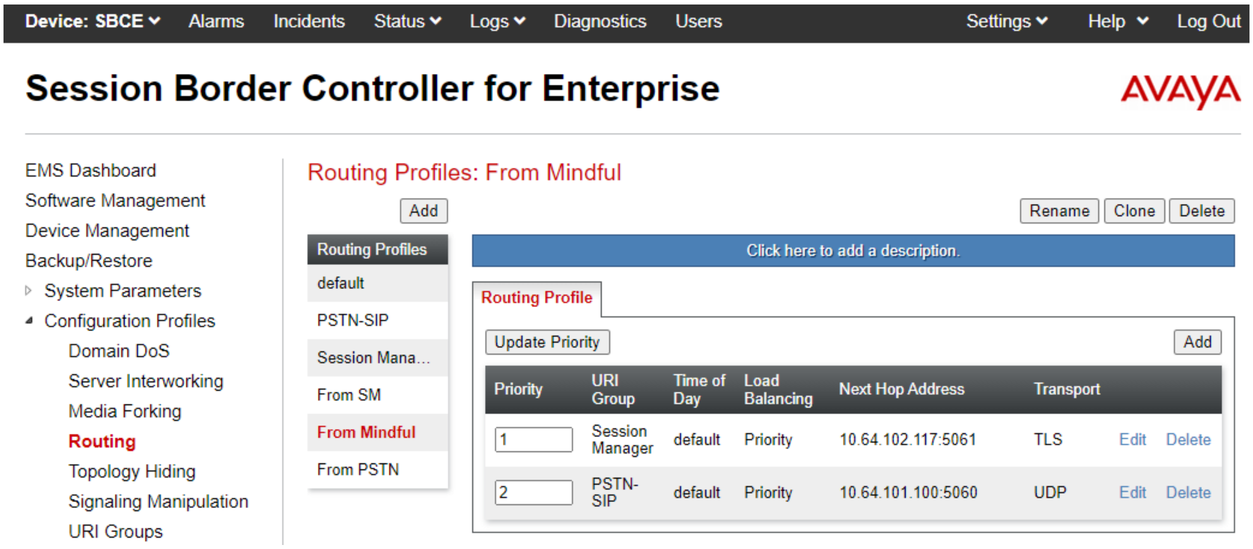
To create a new profile, navigate to **Configuration Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. To view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

The routing profile applied to calls from Session Manager is shown below. The routing profile was named *From SM*. This routing profile contains two routes, one to VHT Mindful Callback and another one to SIP Service Provider. If the SIP Invite matches the VHT Mindful URI Group, VHT Mindful Callback becomes the destination. If it doesn't match the URI group, the SIP Service Provider becomes the destination.



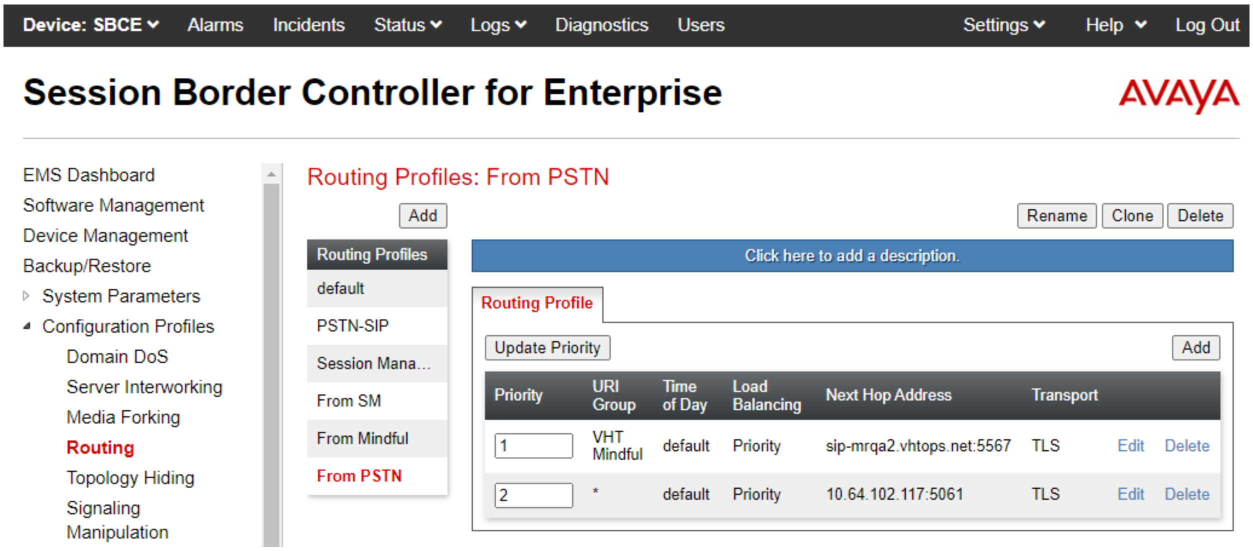
7.5.2. Routing Profile for Calls from VHT Mindful Callback

The routing profile applied to calls from Session Manager is shown below. The routing profile was named *From Mindful*. This routing profile contains two routes, one to Session Manager and another one to SIP Service Provider. If the SIP Invite matches the Session Manager URI Group, Session Manager becomes the destination. If it doesn't match the URI group, the SIP Service Provider becomes the destination.



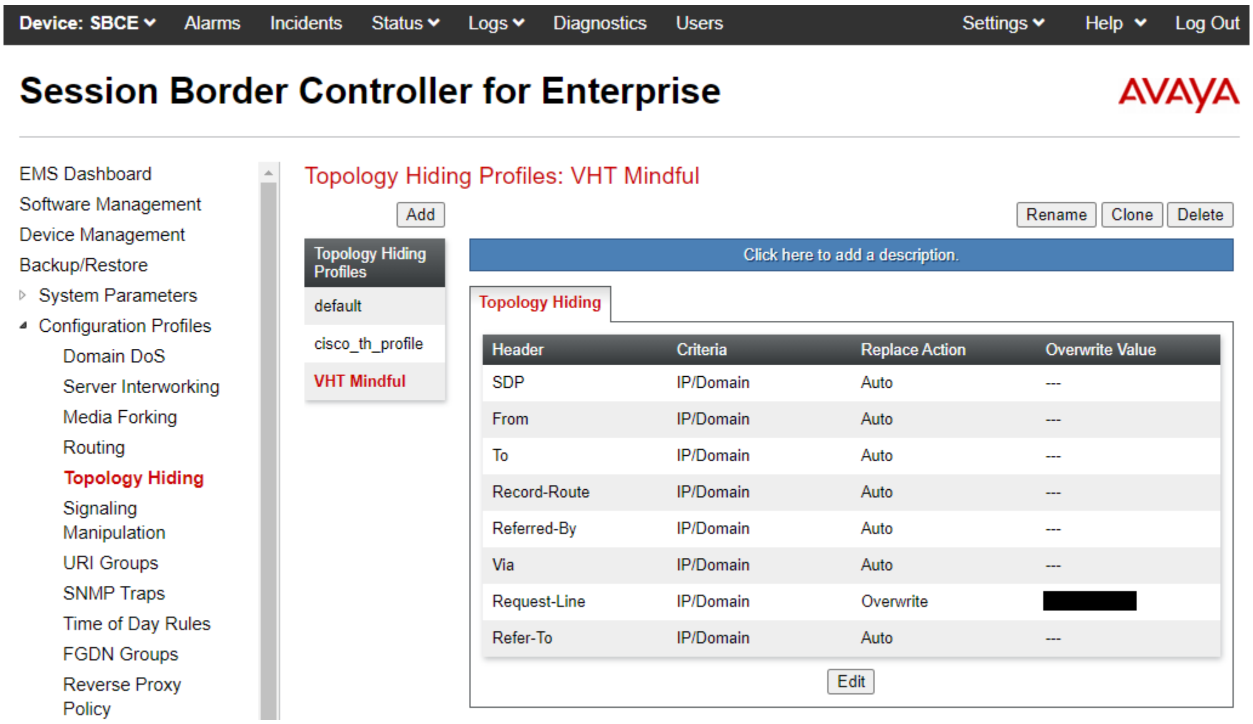
7.5.3. Routing Profile for Calls from SIP Service Provider

The routing profile applied to calls from the SIP Service Provider is shown below. The routing profile was named *From PSTN*. This routing profile contains two routes, one to VHT Mindful Callback and another one to Session Manager. If the SIP Invite matches the VHT Mindful Callback URI Group, VHT Mindful Callback becomes the destination. If it doesn't match the URI group, Session Manager becomes the destination.



7.6. Administer Topology Hiding

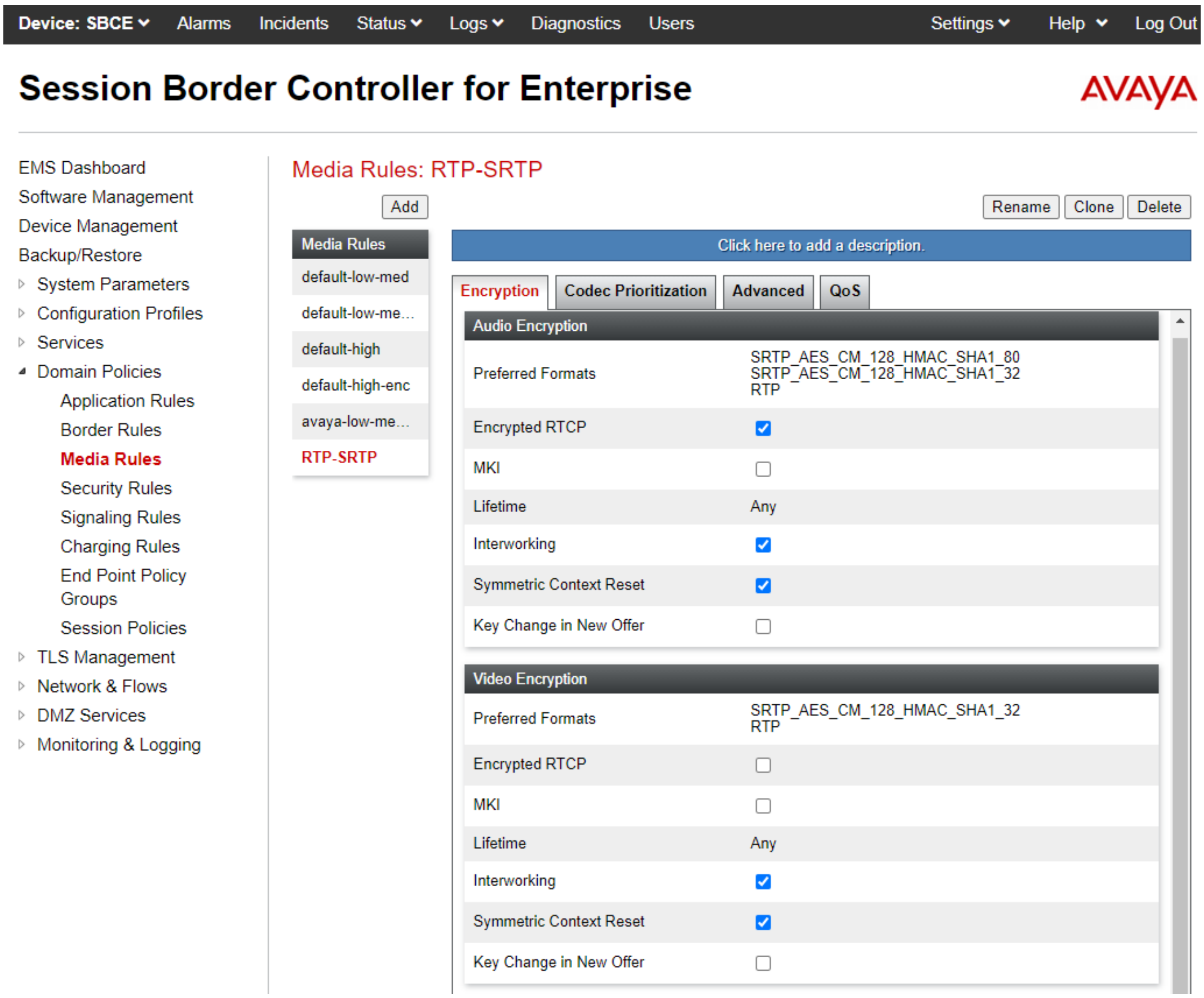
To create a new **Topology Hiding** profile, navigate to **Configuration Profiles → Topology Hiding** in the left pane. The default topology hiding profile may be cloned and named **VHT Mindful** as in the example below. The **Request-Line** should be modified to *overwrite* the IP address of the SBCE public interface connected to VHT Mindful Callback to the VHT Mindful Callback domain. This **Topology Hiding** profile will be assigned to the **Endpoint Flows** in **Section 7.11.1** associated with VHT Mindful Callback. This is required to prevent calls to VHT Mindful Callback from failing.



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, a new media rule was created to support RTP and SRTP.

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 contents of the *RTP-SRTP* media rule are described below. The **Encryption** tab was configured as shown below.

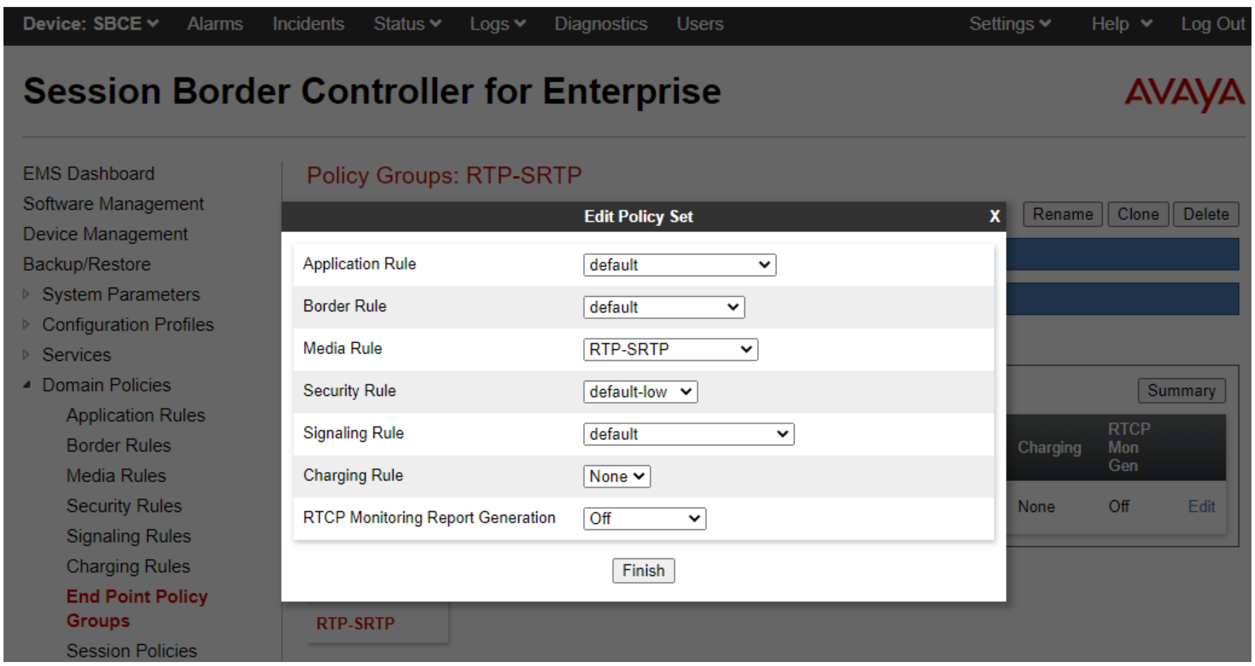


7.8. Administer End Point Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the SBCE and an endpoint (connected server). The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.11**.

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.

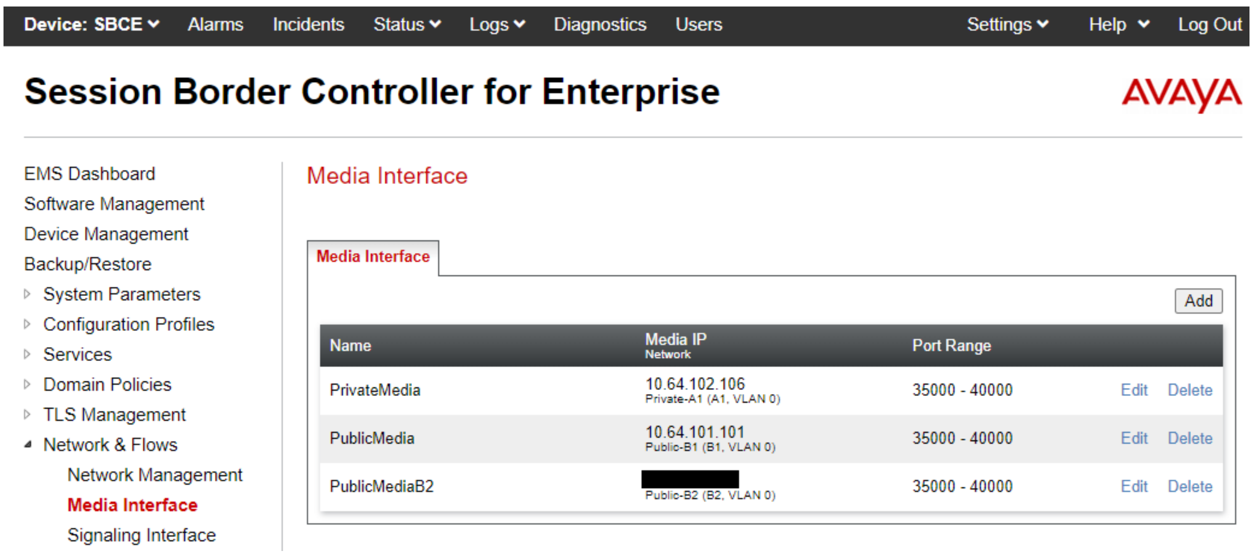


7.9. Administer Media Interfaces

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 Testing 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.
- **PublicMedia:** Interface used by SIP Service Provider to send and receive media.
- **PublicMediaB2:** Interface used VHT Mindful Callback to send and receive media.

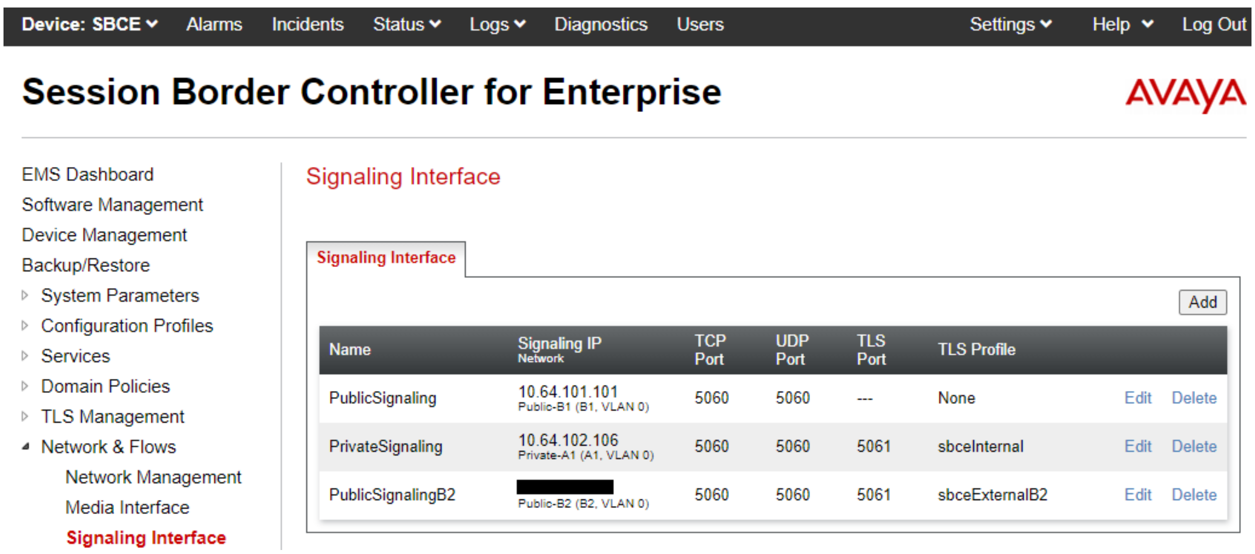


7.10. Administer Signaling Interfaces

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.

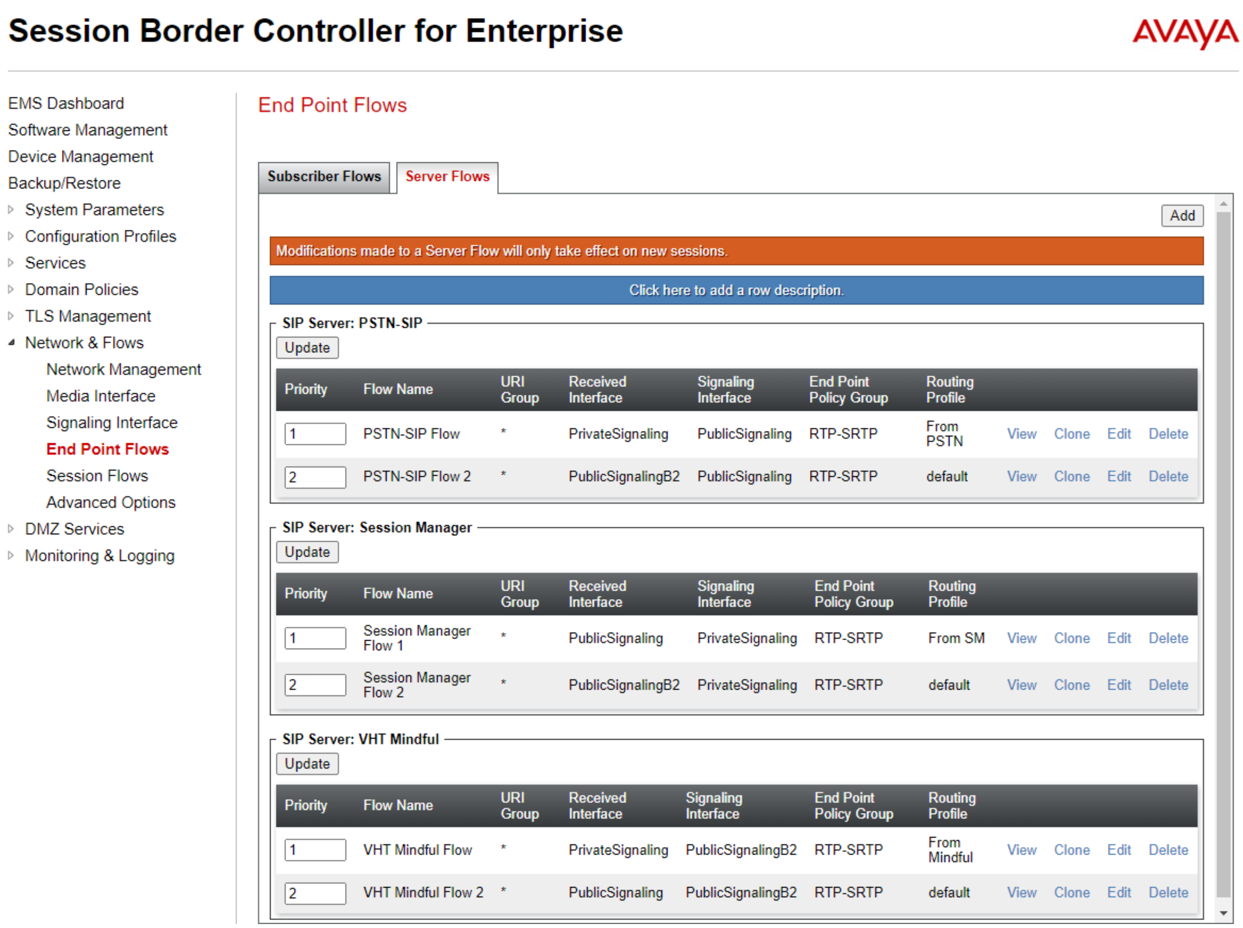
- **PrivateSignaling:** Interface used by Session Manager to send and receive calls.
- **PublicSignaling:** Interface used by SIP Service Provider to send and receive calls.
- **PublicSignalingB2:** Interface used by VHT Mindful Callback to send and receive calls.



7.11. 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, VHT Mindful Callback, and the SIP Service Provider.

Navigate to **Network & Flows → End Point 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.



Session Border Controller for Enterprise

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

End Point Flows

Subscriber Flows | Server Flows

Add

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

Click here to add a row description.

SIP Server: PSTN-SIP

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	PSTN-SIP Flow	*	PrivateSignaling	PublicSignaling	RTP-SRTP	From PSTN	View	Clone	Edit	Delete
2	PSTN-SIP Flow 2	*	PublicSignalingB2	PublicSignaling	RTP-SRTP	default	View	Clone	Edit	Delete

SIP Server: Session Manager

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Session Manager Flow 1	*	PublicSignaling	PrivateSignaling	RTP-SRTP	From SM	View	Clone	Edit	Delete
2	Session Manager Flow 2	*	PublicSignalingB2	PrivateSignaling	RTP-SRTP	default	View	Clone	Edit	Delete

SIP Server: VHT Mindful

Update

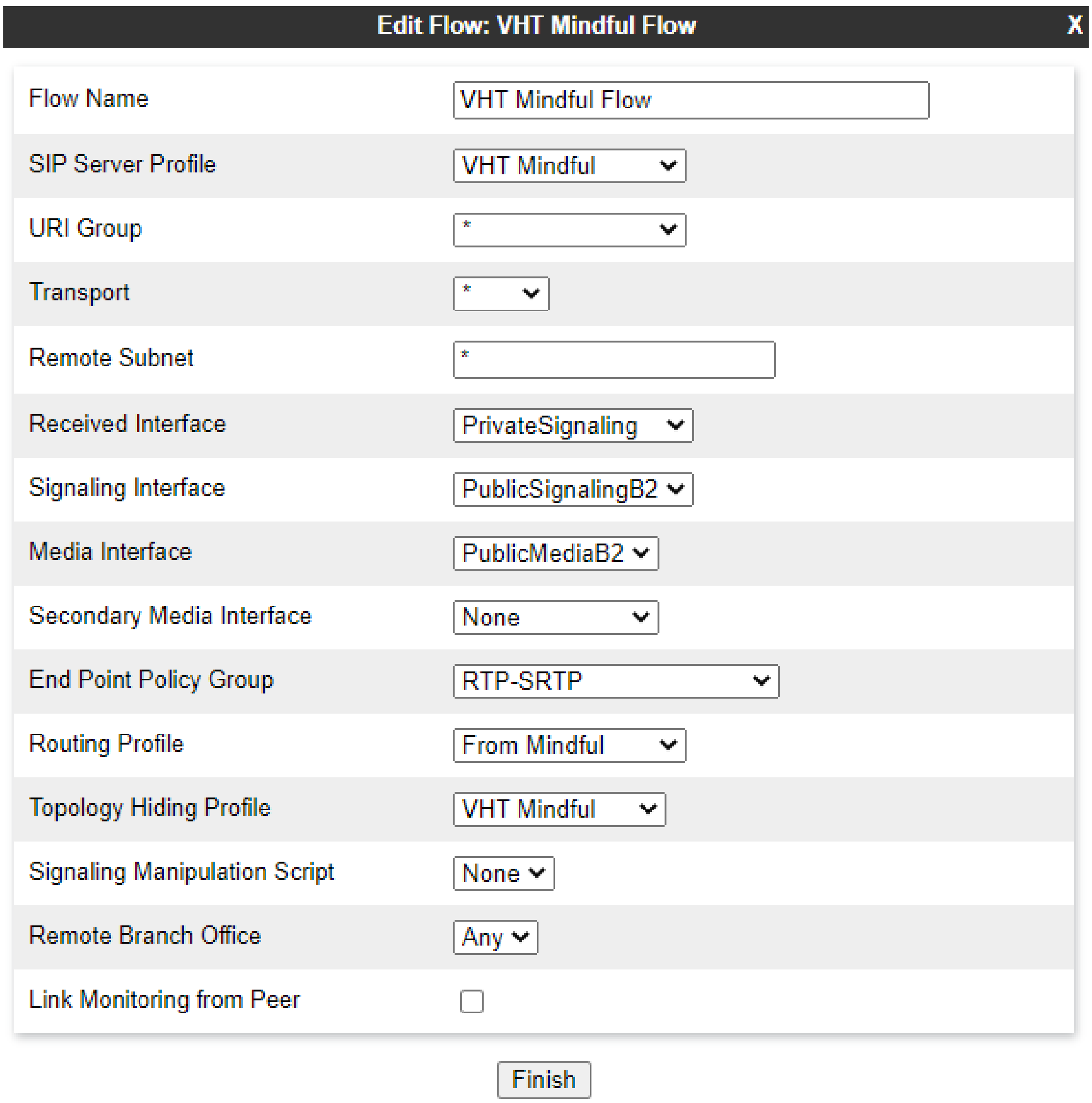
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	VHT Mindful Flow	*	PrivateSignaling	PublicSignalingB2	RTP-SRTP	From Mindful	View	Clone	Edit	Delete
2	VHT Mindful Flow 2	*	PublicSignaling	PublicSignalingB2	RTP-SRTP	default	View	Clone	Edit	Delete

7.11.1. End Point Flows – VHT Mindful Callback

For the compliance test, two endpoint flows were created for VHT Mindful Callback. All traffic from VHT Mindful Callback will match one of these flows as the source flow. The destination flow will either be a Session Manager flow or SIP Service Provider flow depending on whether the URI Group in the Routing Profile matches.

The *VHT Mindful Flow* shown below is used as the source flow when VHT Mindful Callback sends a SIP Invite to the SBCE. The routing profile selects either Session Manager or SIP Service Provider as the destination endpoint.

The **Topology Hiding Profile** is used to change the domain in the Request-URI and To header to the domain of VHT Mindful Callback.

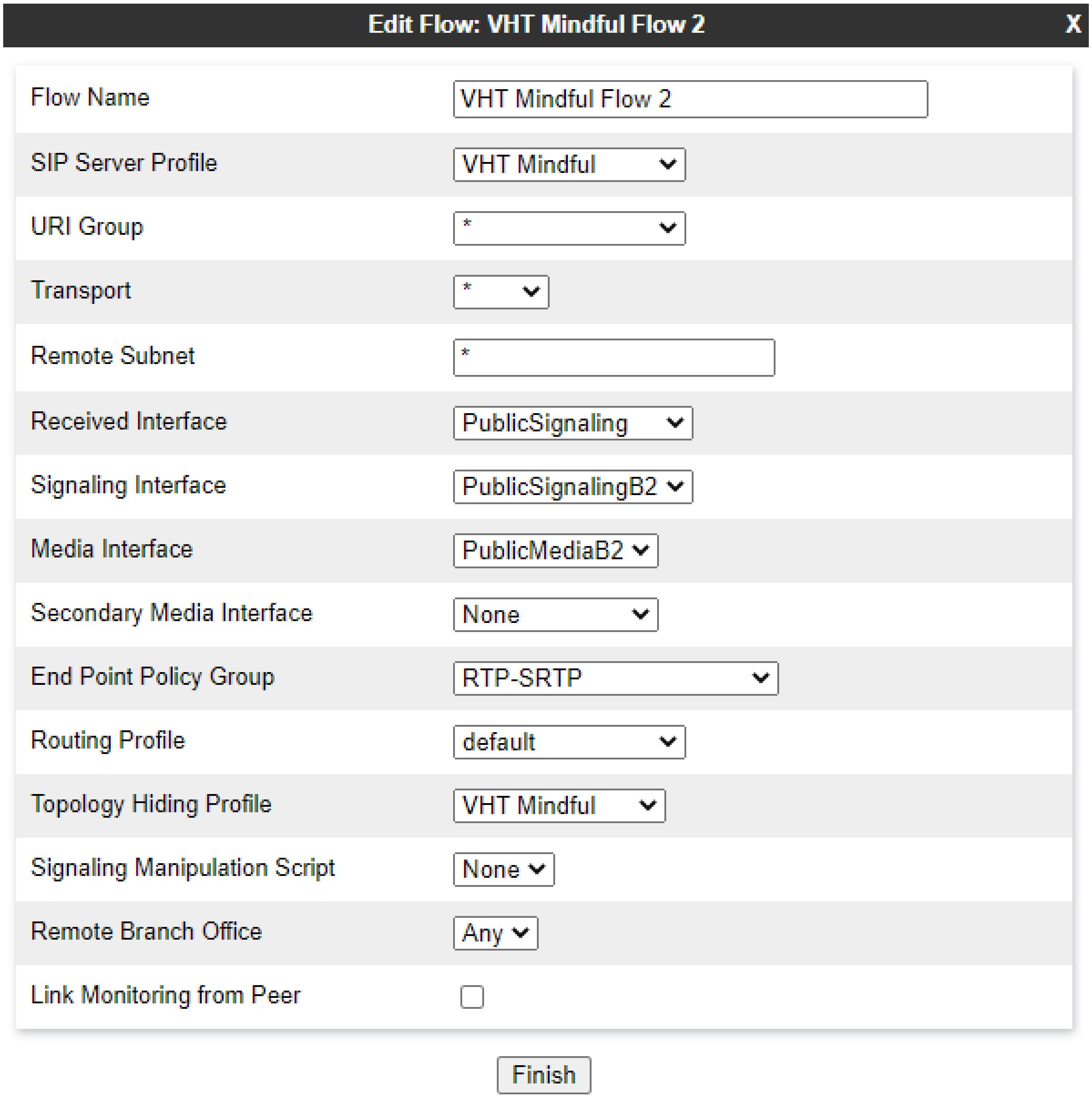


Edit Flow: VHT Mindful Flow

Flow Name	VHT Mindful Flow
SIP Server Profile	VHT Mindful
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	PrivateSignaling
Signaling Interface	PublicSignalingB2
Media Interface	PublicMediaB2
Secondary Media Interface	None
End Point Policy Group	RTP-SRTP
Routing Profile	From Mindful
Topology Hiding Profile	VHT Mindful
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	

Finish

The *VHT Mindful Flow 2* shown below is used as the destination flow for inbound calls from either Session Manager or the VoIP Service Provider.



Edit Flow: VHT Mindful Flow 2

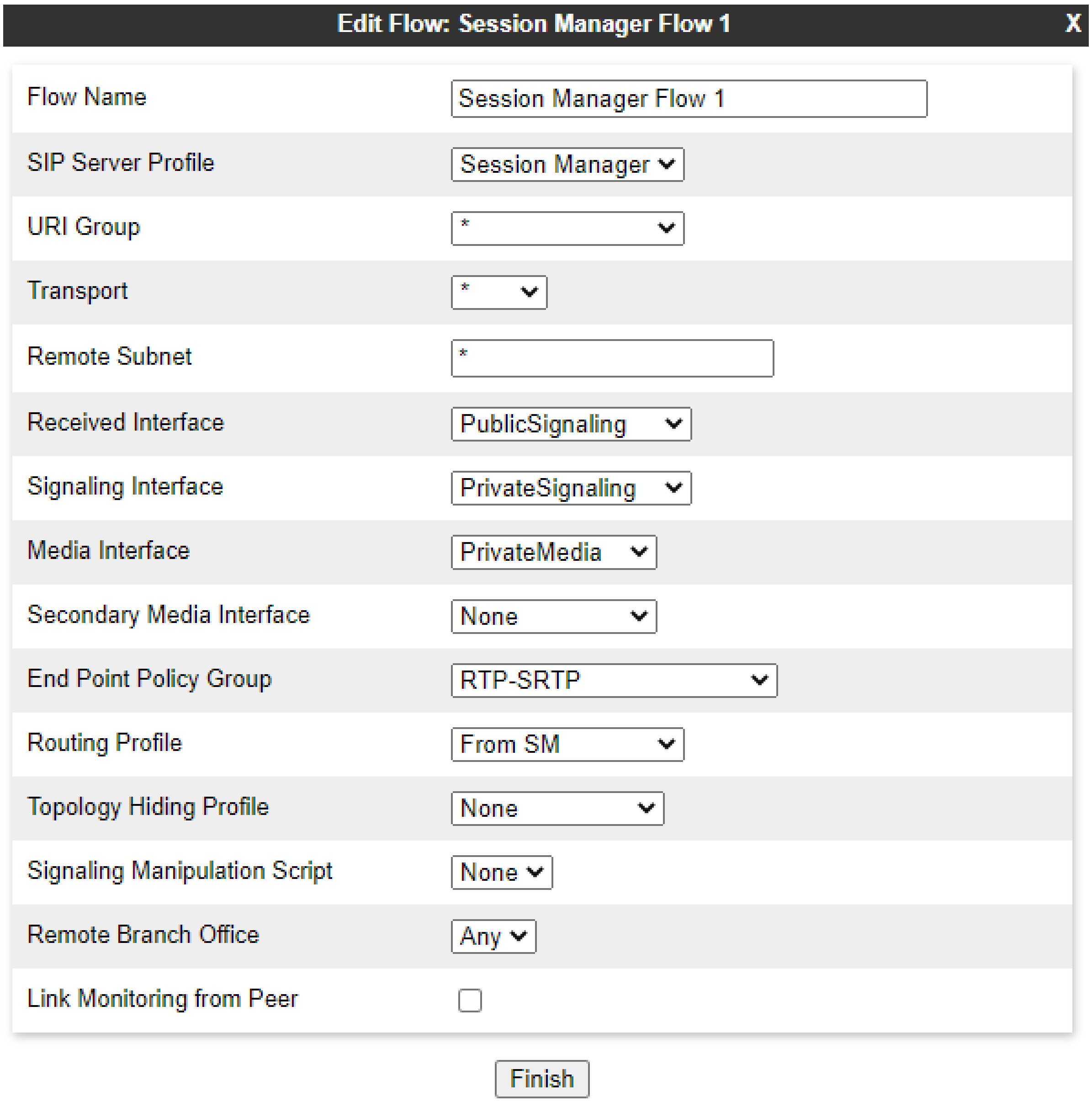
Flow Name	VHT Mindful Flow 2
SIP Server Profile	VHT Mindful
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	PublicSignaling
Signaling Interface	PublicSignalingB2
Media Interface	PublicMediaB2
Secondary Media Interface	None
End Point Policy Group	RTP-SRTP
Routing Profile	default
Topology Hiding Profile	VHT Mindful
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☐

Finish

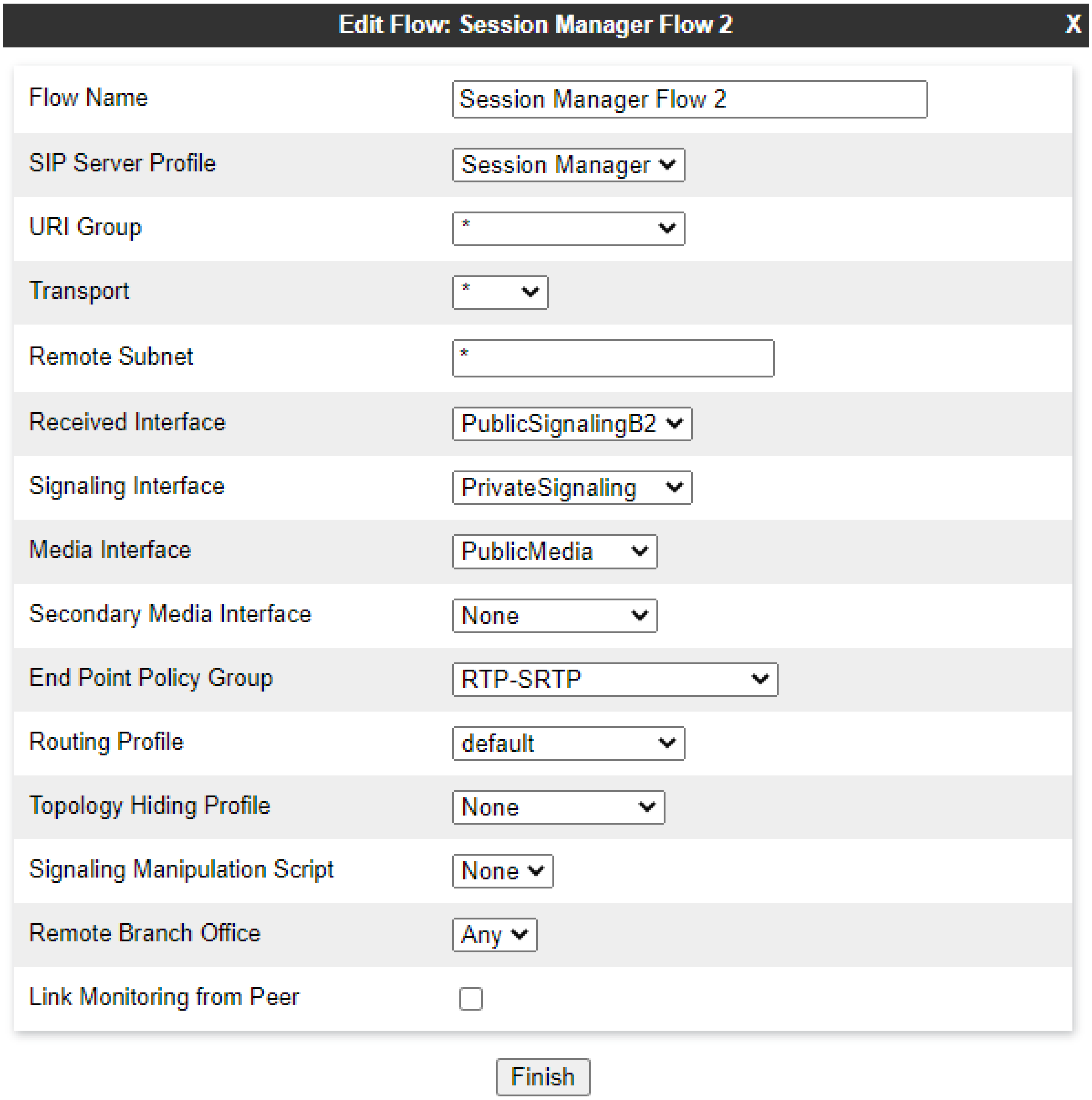
7.11.2. End Point Flows – Session Manager

For the compliance test, two endpoint flows were created for Session Manager. All traffic from Session Manager will match one of these flows as the source flow. The destination flow will either be a VHT Mindful Callback flow or SIP Service Provider flow depending on whether the URI Group in the Routing Profile matches.

The *Session Manager 1* flow shown below is used as a source flow for calls from Session Manager to either VHT Mindful Callback or the SIP Service Provider.



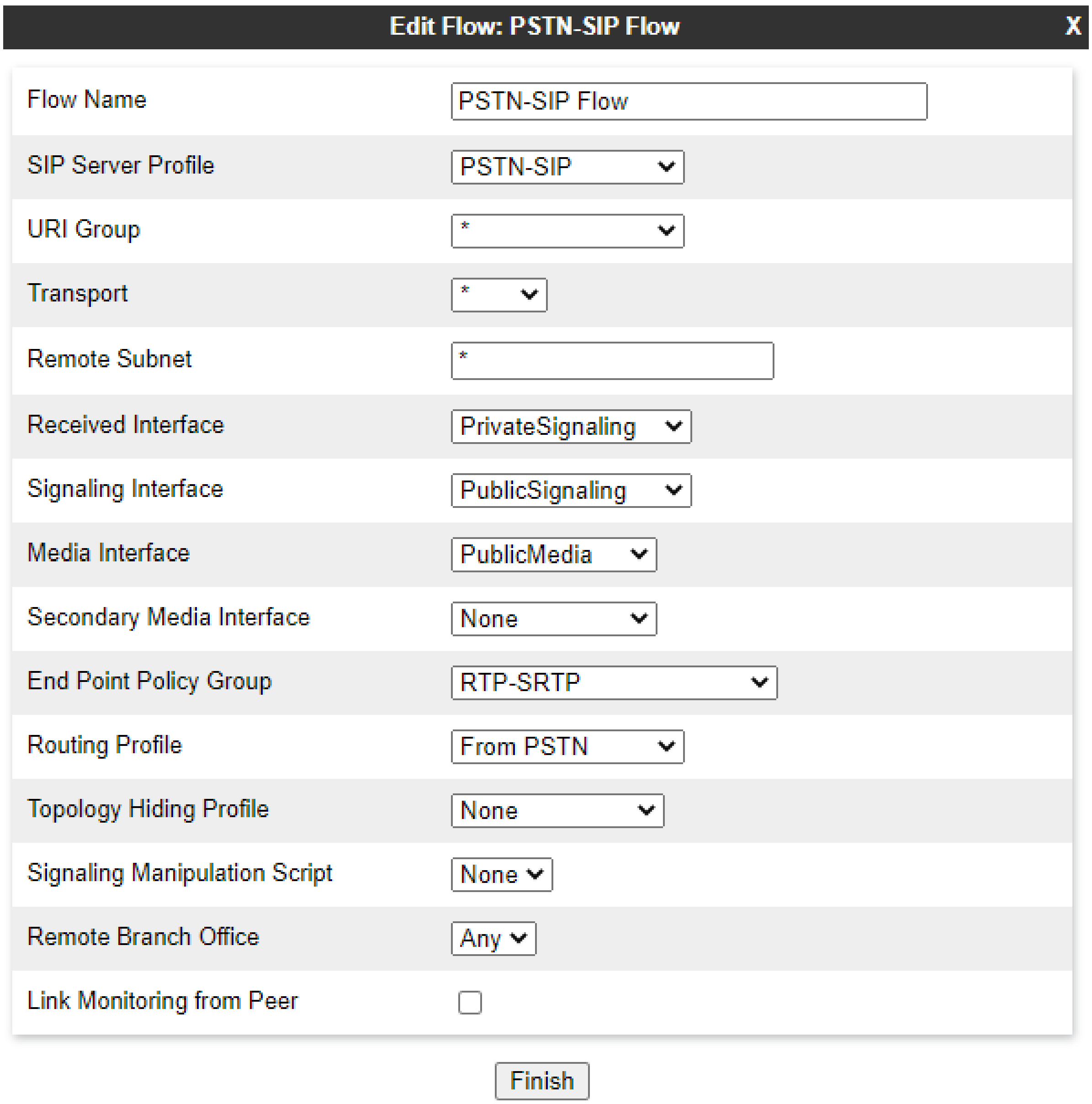
The *Session Manager 2* flow shown below is used as the destination flow for calls from VHT Mindful Callback or the SIP Service Provider.



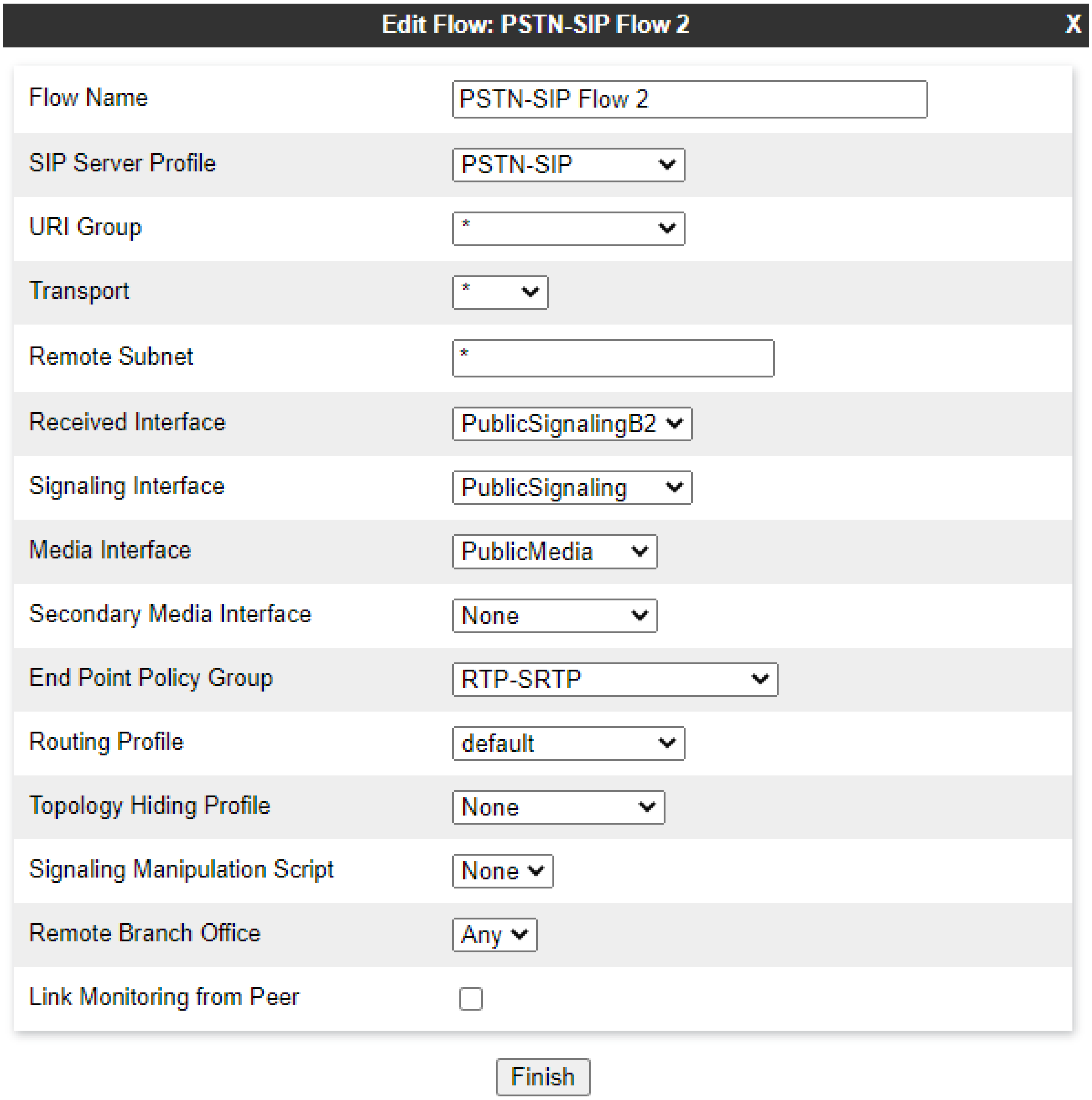
7.11.3. End Point Flows – VoIP Service Provider

For the compliance test, two endpoint flows were created for SIP Service Provider. All traffic from VoIP Service Provider will match one of these flows as the source flow. The destination flow will either be a VHT Mindful Callback flow or Session Manager flow depending on whether the URI Group in the Routing Profile matches.

The *PSTN-SIP Flow* shown below is used as the source flow for calls from the SIP Service Provider.



The *PSTN-SIP Flow 2* shown below is used as the destination flow for calls from VHT Mindful Callback or Session Manager.



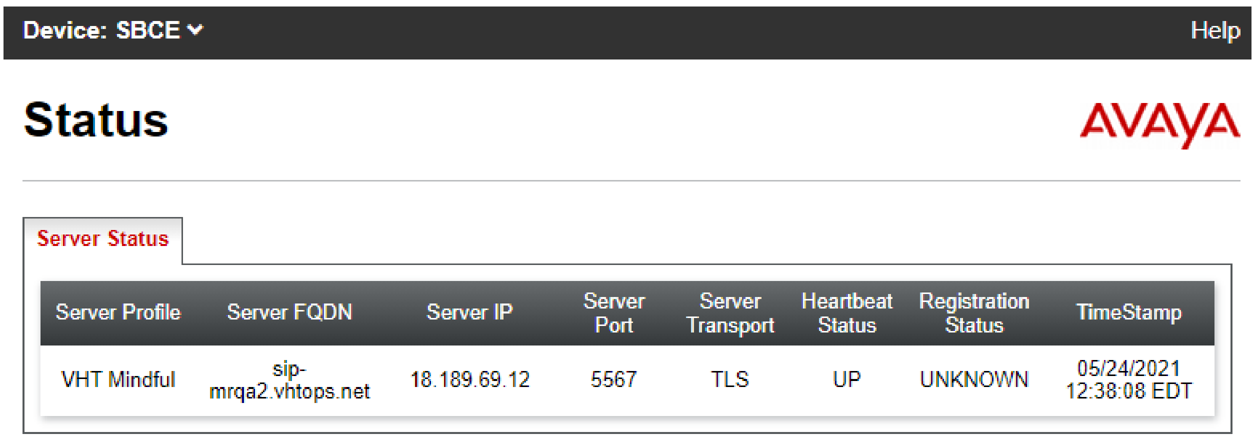
8. Configure VHT Mindful Callback

The VHT Support Team will perform the configuration of VHT Mindful Callback, including the Call Targets. To configure VHT Mindful Callback, the VDN numbers, SIP trunk transport/port, and the SBCE IP address are required. VHT Support should provide the call target number(s) so that call routing can be configured in the Avaya Aura® environment, including SBCE.

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, SBCE, and VHT Mindful Callback.

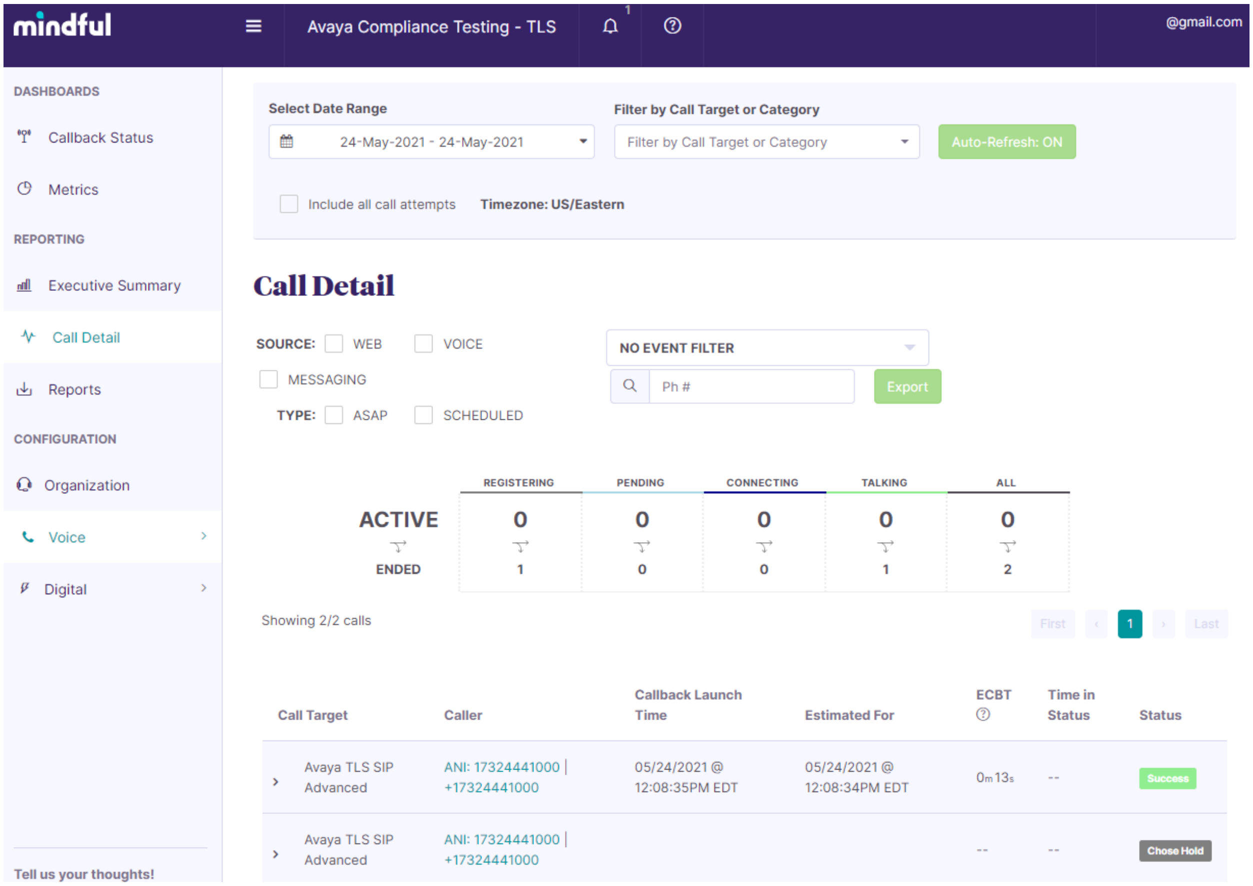
1. From SBCE, navigate to **Status → Server Status** to verify that the SIP trunk between SBCE and VHT Mindful Callback is *UP* as shown below.



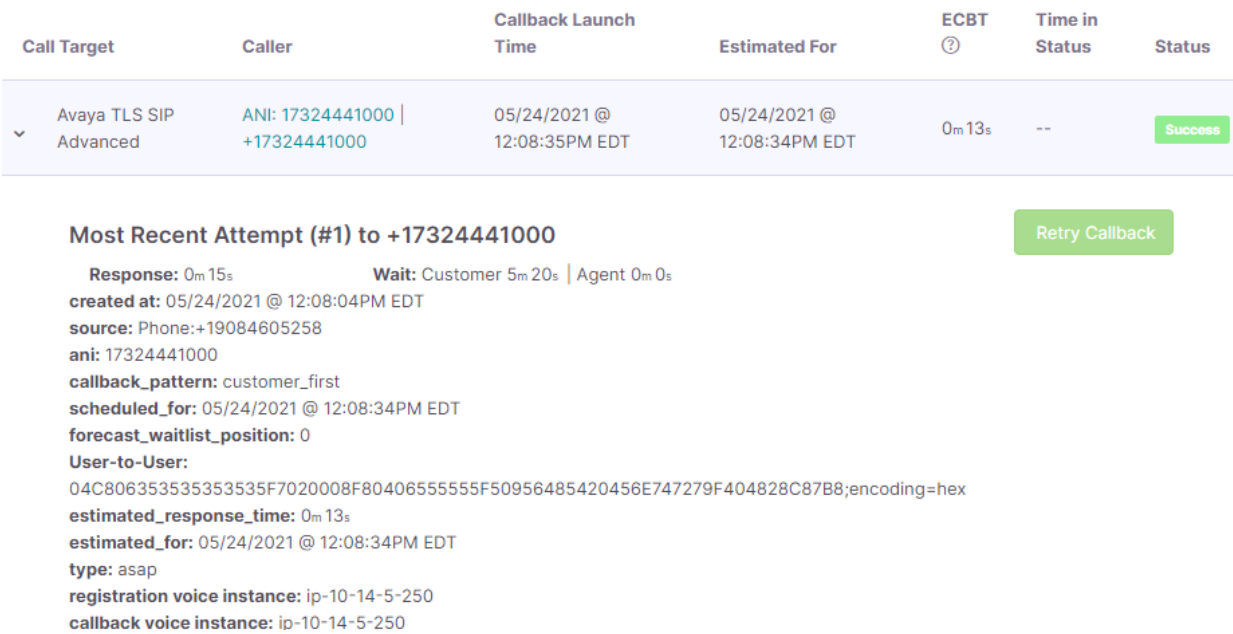
Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
VHT Mindful	sip-mrqa2.vhtops.net	18.189.69.12	5567	TLS	UP	UNKNOWN	05/24/2021 12:38:08 EDT

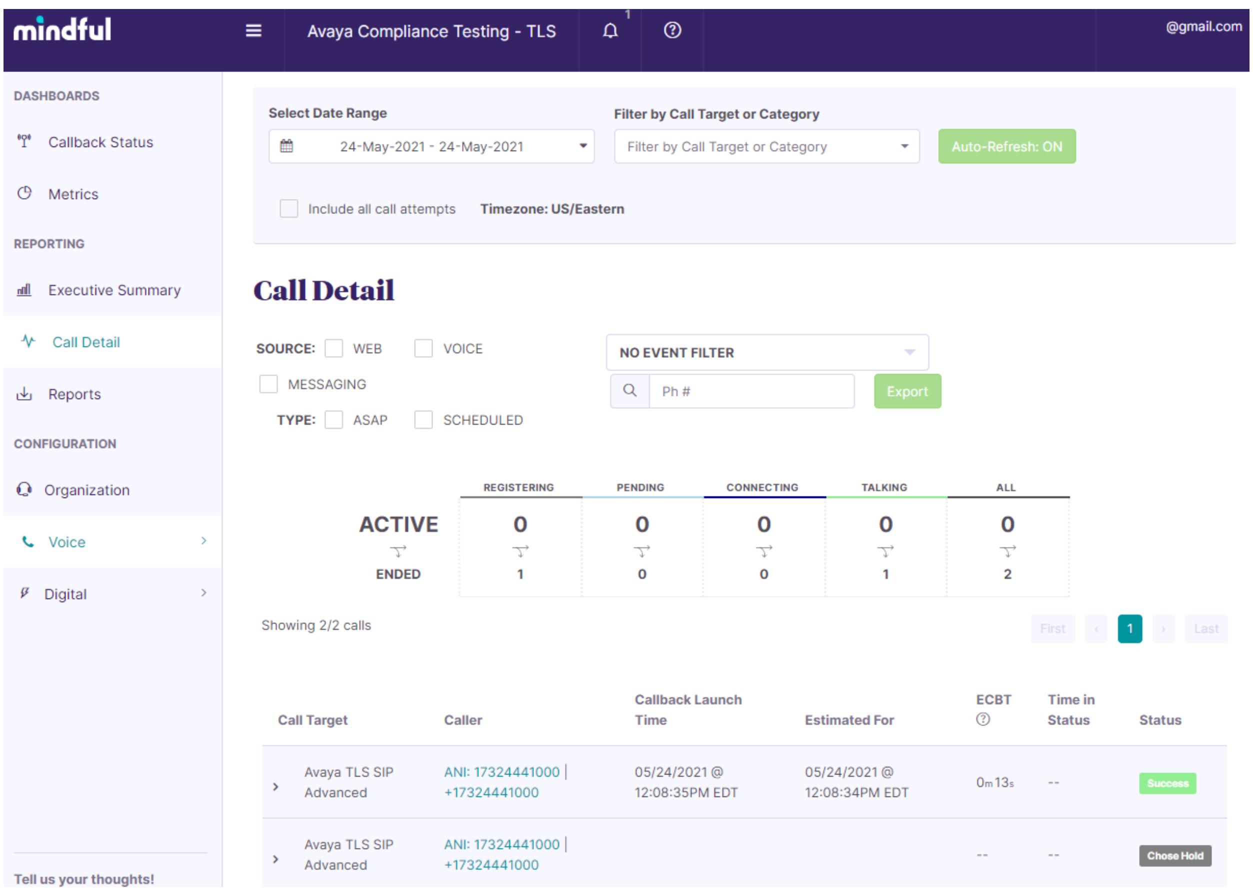
2. Place an incoming customer call to the entry VDN and verify the call is routed to VHT Mindful Callback and the greeting is heard. Request a callback.

3. Verify the customer receives the callback and accept the call. In the **Call Detail** screen in the VHT Mindful Callback web interface, the **Status** should be *Success* as shown below.



Expand the callback entry to view additional details, including the UUI received, the ANI for the callback, and the number of callback attempts.





4. Verify the agent receives the call and accept the call to be connected to the customer.

5. Finally, verify VHT Mindful Callback bridges the two calls together and the customer and agent are connected.

10. Conclusion

These Application Notes have described the configuration steps required to integrate VHT Mindful Callback with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise. Customer calls were able to enter UUI, and then hold for an agent or receive a callback. When the callback option was selected, VHT Mindful Callback was able to connect the customer and agent successfully. All test cases passed.

11. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 8, November 2020, available at http://support.avaya.com.

[2] *Administering Avaya Aura® System Manager for Release 8.1.x*, Release 8.1.x, Issue 8, November 2020, available at http://support.avaya.com.

[3] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 7, October 2020, available at http://support.avaya.com.

[4] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020, available at http://support.avaya.com.

[5] *VHT Mindful Callback – Avaya Aura 8 and Mindful Callback Integration Guide*, Updated May 4th, 2021, available at https://help.vhtcx.com (login required).

[6] *VHT Mindful Callback – Avaya UUI Routing with Mindful Callback*, Updated May 4th, 2021, available at https://help.vhtcx.com (login required).

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.