Avaya Solution & Interoperability Test Lab

Application Notes for configuring Frequentis AG 3020 LifeX with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning 3020 LifeX V3.5 from Frequentis to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 using Avaya Session Border Controller for Enterprise R8.1.2 to connect to an Oracle Session Border Controller provided by Frequentis.

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 for provisioning 3020 LifeX V3.5 from Frequentis to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 using Avaya Session Border Controller for Enterprise R8.1.2 to connect to an Oracle Session Border Controller provided by Frequentis.

The Frequentis 3020 LifeX (LifeX) is an Integrated Communication Control System that is used by emergency service customers for communicating between control rooms and the front line NHS Ambulance service responders and then from the same application using radio communication (TETRA digital radio or analogue PMR) to pass details to mobile resources.

As a radio dispatch deployment with basic PTN/PSTN the LifeX acts as an end Private Branch Exchange (PBX) and performs call prioritisation and distribution to LifeX operators as defined by the profile in which they have logged in to the LifeX application. In this type of configuration, the LifeX has one primary connection to the Avaya Solution, a SIP connection to Avaya Aura ® Session Manager. The LifeX supports basic call control including hold and transfer.

Some of the acronyms that will be used throughout this document are as follows.

- **UDP:** User Datagram Protocol (UDP) – a communications protocol that facilitates the exchange of messages between computing devices in a network. It's an alternative to the transmission control protocol (TCP).
- **TCP:** TCP/IP, in full Transmission Control Protocol/Internet Protocol, standard Internet communications protocols that allow digital computers to communicate over long distances.
- **TLS:** Transport Layer Security (TLS) is the successor protocol to SSL. TLS is an improved version of SSL. It works in much the same way as the SSL, using encryption to protect the transfer of data and information.
- **SIP:** Session Initiation Protocol and refers to a TCP/IP-based network protocol which can be used to establish and control communication connections of several subscribers. SIP is often used in Voice-over-IP telephony to establish the connection for telephone calls.
- **H.323:** H. 323 is an ITU Telecommunication Standardization Sector (ITU-T) recommendation that describes protocols for the provision of audio-visual (A/V) communication sessions on all packet networks. H. 323 is widely used in IP based videoconferencing, Voice over Internet Protocol (VoIP) and Internet telephony.
- **PSTN:** "Public Switched Telephone Network", and it refers to the world's oldest collection of interconnected communication solutions – both government, and commercially-owned. Some people also refer to this communications option as the "Plain Old Telephone Service", or POTS.
- **PBX:** Private Branch eXchange and has become a general term used to describe a business telephone system that offers multiple inbound and outbound lines, call routing, voicemail, and call management features.
- **CM:** Avaya Aura® Communication Manager.
- **SM:** Avaya Aura® Session Manager.

- **ASBCE**: Avaya Session Border Controller for Enterprise or Avaya SBCE.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of LifeX operators to make and receive calls to and from Communication Manager endpoints. Calls from a simulated PSTN were routed to Communication Manager endpoints and were then transferred to LifeX operators as well as routing PSTN calls directly to LifeX. The connection between LifeX and Session Manager is facilitated by a Session Border Controller on each side, this is outlined in **Section 3**.

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 the Avaya Session Border Controller for Enterprise and LifeX made use of a TLS connection, however the RTP between the Avaya SBCE and LifeX was not secure as requested by Frequentis.

2.1. Interoperability Compliance Testing

The compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP, H.323 and Digital endpoints.

- **Basic calls between Communication Manager and LifeX** – Test calls between the Avaya platform and the LifeX platform, these are basic calls that involve no transfers.
- **Hold/Transfer/Conference calls between Communication Manager and LifeX** – Test the hold and transfer functions to/from the LifeX platform.
- **Simulated PSTN calls to and from Life X** – Calls to and from LifeX from a simulated PSTN.
- **Test calls with CM Shuffling on and off** – Calls are made using a Direct Media path between Avaya endpoints and with the initial media path on the Media Server/Gateway that then shuffles off to the IP endpoints.
- **CODEC testing** – Testing using different codecs on Communication Manager.
- **DTMF** – Testing the DTMF using a voicemail system.

- **LifeX Features** – Calls were made to specific LifeX roles that utilized features on the LifeX platform.
- **Serviceability Tests** – Observations on call flow when a LAN failure occurs.

Note: Compliance testing does not include redundancy testing as standard. Where some LAN failures were simulated, and the results observed, there were no redundancy or failover tests performed.

2.2. Test Results

Tests were performed to verify interoperability between LifeX operators and Communication Manager endpoints. All test cases passed with the following observations noted.

1. The SIP trunk on Communication Manger was configured to use the From header for the Identity for Calling Party Display, see **Section 5.5**.
2. Topology Hiding was used to ensure that all calls to LifeX were in the format ext@domain, see **Section 7.10**.
3. When calling from Avaya H.323 endpoints the display shows information from the CONTACT header received from LifeX. Initially this was set by the Oracle SBC by overwriting the Contact Header and testing was carried out using this setup. This was then changed to have LifeX send out the "role number" in the Contact header and some regression testing was carried out successfully using that setup, thus eliminating the need for the Oracle SBC to make any changes to the Contact header.
4. When Avaya transfers LifeX caller to another Avaya phone the LifeX callers display is not updated with the new CLID info. Scenario – LifeX calls to CM1 and CM1 transfers LifeX to CM2. LifeX should show CM2 number on the display but continues to show CM1. SIP Updates are not supported in LifeX release 3.5 but will be supported in future releases.
5. When an Avaya user transfers LifeX caller back to another LifeX caller, the display on both LifeX callers should be updated to show each other's CLID on the display, however the CLID of the CM phone is displayed on both. SIP Updates are not supported in LifeX release 3.5 but will be supported in future releases.
6. There is no MOH or Announcement played to the Avaya party when the LifeX places the caller on hold. This only occurs when it is LifeX that initiates the original call. This will be configurable in future releases of LifeX.
7. G.722 or G723 codecs were not utilized between the Avaya and LifeX. G.711A, G.711U and G.729 are the only supported codecs on LifeX currently.

2.3. Support

Technical support for the Frequentis AG 3020 LifeX can be obtained as follows:

- Web: https://www.frequentis.com/en/contact-us

3. Reference Configuration

Figure 1 shows the setup for compliance testing Frequentis's LifeX with Communication Manager and Session Manager using SIP signalling over SIP trunks to pass calls from Communication Manager to the LifeX Operators. There are two Session Border controllers each side of the solution, these are designed as Firewalls and simply pass the SIP messages through them onto each relevant destination.

A VPN connection was established between the Session Border Controllers as they are on the edge of each platform. This VPN connection was to facilitate testing between labs in London and Galway but would not necessarily be part of a typical setup.

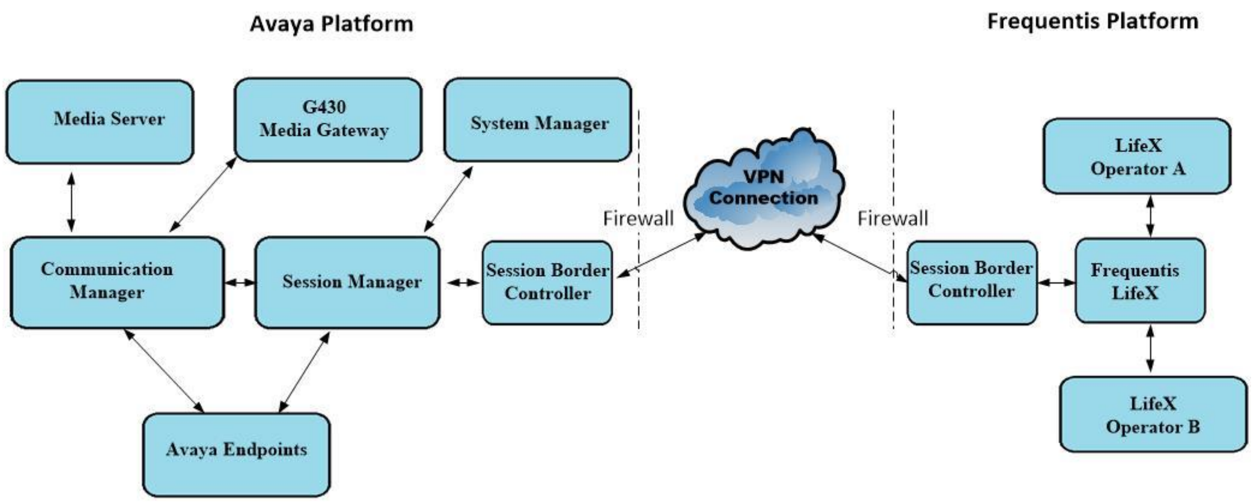


Figure 1: Connection of Frequentis LifeX with Avaya Aura® Communication Manager R8.1, Avaya Aura® Session Manager R8.1 and Avaya Session Border Controller for Enterprise R8.1.2

4. Equipment and Software Validated

The following equipment and software were used for the compliance test.

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	8.1.3.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.0.1011784 Feature Pack 3
Avaya Aura® Session Manager running on a virtual server	8.1.3 Build No. – 8.1.3.0.813014
Avaya Aura® Communication Manager running on a virtual server	8.1.3 – FP3 R018x.01.0.890.0 Update ID 01.0.890.0-26568
Avaya Session Border Controller for Enterprise	8.1.2.0-31-19809
Avaya Aura® Media Server	8.0.2.138
Avaya G450 Media Gateway	40.20.0/2
Avaya J179 H.323 Deskphone	6.8304
Avaya J189 SIP Deskphone	4.0.7.0.7
Avaya 9404 Digital Phone	2.00
Frequentis LifeX 3020 ORACLE Enterprise Session Border Controller	3.5.13.4 8.3.0

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing with SIP trunks in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 11** of these Application Notes.

The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options.
- System Features and Access Codes.
- Administer Dial Plan.
- Administer Route Selection for calls to LifeX.
- Configure SIP Trunk.

Note: The configuration of PSTN trunks and routes are outside the scope of these Application Notes.

5.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that **Maximum Administered SIP Trunks** has sufficient capacity. Calls that are transferred across the link between the two systems use two SIP trunks for the full duration of the call.

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

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 12000 250
           Maximum Concurrently Registered IP Stations: 18000 2
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 319
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
```

On **Page 4**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

```
display system-parameters customer-options                    Page   4 of  12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                      DCS (Basic)? y
```

On **Page 6**, ensure that **Uniform Dialing Plan** is set to **y**.

```
display system-parameters customer-options                    Page   6 of  12
                                OPTIONAL FEATURES

                Multinational Locations? n            Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n     Station as Virtual Extension? y
                     Multiple Locations? n
                                             System Management Data Transfer? n
          Personal Station Access (PSA)? y              Tenant Partitioning? y
                        PNC Duplication? n      Terminal Trans. Init. (TTI)? y
                   Port Network Support? y              Time of Day Routing? y
                        Posted Messages? y      TN2501 VAL Maximum Capacity? y
                                                       Uniform Dialing Plan? y
                     Private Networking? y     Usage Allocation Enhancements? y
```

5.2. System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **Page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 11** for supporting documentation.

```
display system-parameters features                            Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
              Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                      Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

             Music (or Silence) on Transferred Trunk Calls? no
                      DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                 Automatic Circuit Assurance (ACA) Enabled? n

             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **8** is used for AAR and **9** for ARS routing.

```
display feature-access-codes                                          Page   1 of  10
                               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:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *25    Deactivation: #25
```

5.3. Administer Dial Plan

It was decided for compliance testing that all calls beginning with 700x with a total length of 4 digits were to be sent across the SIP trunk to LifeX via Session Manager and ASBCE. In order to achieve this, automatic alternate routing (aar) would be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this.

Type **change dialplan analysis** in order to make changes to the dial plan. Ensure that **700** is added with a **Total Length** of **4** and a **Call Type** of **udp**.

```
change dialplan analysis                                           Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 2

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   4           4   udp
   5           5   udp
   6           4   ext
   700         4   udp
   9           1   fac
   *           3   fac
```

5.4. Administer Route Selection for calls to LifeX

As digits 7001 to 7009 (700x) were defined in the dial plan as udp (**Section 5.3**) use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **700x** that are **4** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

```
change uniform-dialplan 5                                            Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                    Insert              Node
  Pattern       Len Del       Digits      Net Conv Num
  700           4   0                     aar  n
                                               n
```

Use the **change aar analysis** x command to further configure the routing of the dialed digits. Calls to LifeX begin with **700x** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 12**, which contains the outbound SIP Trunk Group.

```
change aar analysis 7                                         Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

    Dialed                 Total      Route     Call   Node  ANI
    String                Min  Max  Pattern    Type   Num   Reqd
    700                   4    4     12        aar           n
```

Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Pattern Number 12** is used to route calls to trunk group **(Grp No) 12**, this is the SIP Trunk configured in **Section 5.5**. Other settings such as **FRL** and **Numbering Format** can be seen below.

```
change route-pattern 12                                        Page   1 of   4
                    Pattern Number: 12      Pattern Name: SIP-Trunk-Out
    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: 12  0                                                             n   user
 2:                                                                   n   user
 3:                                                                   n   user
 4:                                                                   n   user
 5:                                                                   n   user
 6:                                                                   n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            unre                               lev0-pvt  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
```

5.5. Configure SIP Trunk

In the Node Names IP form, note the IP Address of the **procr** and the Session Manager (**sm81vmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
AMS80vmpg           10.10.40.61
G450                10.10.40.14
IPOffice            10.10.40.25
NRS                 10.10.40.101
PGDECT              10.10.40.50
sm81vmpg            10.10.40.32
SM_Oceana           10.10.41.26
aes81vmpg           10.10.40.56
default             0.0.0.0
procr               10.10.40.37

( 16 of 18   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
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.1**. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

```
display ip-network-region 1                                         Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: devconnect.local
    Name: PG Default            Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 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            Keep-Alive Count: 5
```

In the **IP Media Parameters** form, select the audio codec's supported for calls routed over the SIP trunk to Communications Portal. The form is accessed via the **display ip-codec-set n** command or if a change were needed to be made type change ip-codec-set n. Note that IP codec set 1 was specified in IP Network Region 1 shown on the previous page. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), **G.711U** (mu-law), and **G.729** which are supported by LifeX.

Media Encryption is used on the Avaya sets where possible these use **srtp-aescm128-hmac80** media encryption. **None** is also present to facilitate any devices that do not support media encryption.

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

                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711A            n         2        20
 2: G.711U            n         2        20
 3: G.729             n         2        20
 4:
 5:
 6:
 7:

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
 4:
 5:
```

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

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method, for compliance testing this was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively.
- Set the **Near-end Node Name** to **procr**.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm81vmpg**).
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured previously**.** This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- Leave the **Far-end Domain** field blank to allow Communication Manager to accept any domain.
- The **Direct IP-IP Audio Connections** field is set to **y**. This is to turn ‘shuffling’ on.
- The default values for the other fields may be used.

Note: During Compliance testing a selection of complex calls including blind transfers were carried out with the **Initial IP-IP Direct Media** field is set to **y**. This was to ensure that no issues would arise with this set for early media.

```
change signaling-group 12                                       Page   1 of   3
                                SIGNALING GROUP

 Group Number: 12             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: sm81vmpg
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain:
                                             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
                                                  Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for all incoming and outgoing SIP calls to Session Manager SIP Entities including the Avaya SBCE. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie** (this may vary depending on the site in question). 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.

```
change trunk-group 12                                             Page   1 of   4
                                TRUNK GROUP

Group Number: 1                   Group Type: sip          CDR Reports: y
  Group Name: SIPTRUNK-OUT               COR: 1        TN: 1        TAC: *812
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 12
                                                    Number of Members: 10
```

On **Page 2** of the trunk-group form the following values were used for compliance testing.

```
change trunk-group 12                                             Page   2 of   4
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n




 Caller ID for Service Link Call to H.323 1xC: station-extension
```

On **Page 3** of the trunk-group form the following values were used for compliance testing. The **Numbering Format** was set to **private**.

```
change trunk-group 12                                           Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no





 Show ANSWERED BY on Display? y

 DSN Term? n
```

Settings on **Page 4** are as follows. **Send Transferring Party Information** is set to **y** and **Identity for Calling Party Display** is set to **From**. The other settings should be set as shown below.

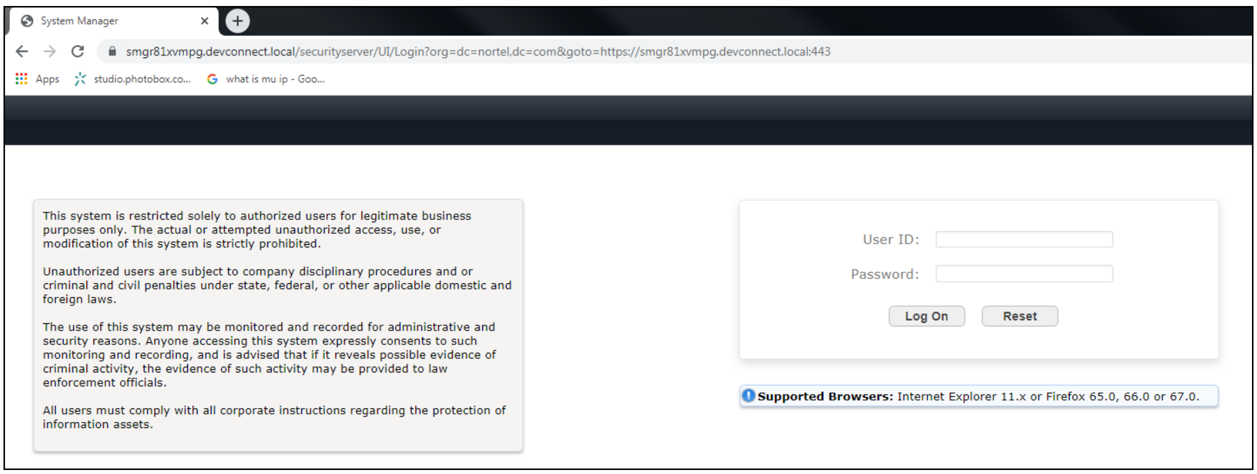
```
change trunk-group 12                                           Page   4 of   4
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? n
          Build Refer-To URI of REFER From Contact For NCR? 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: From
            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
```

6. Configure Avaya Aura® Session Manager

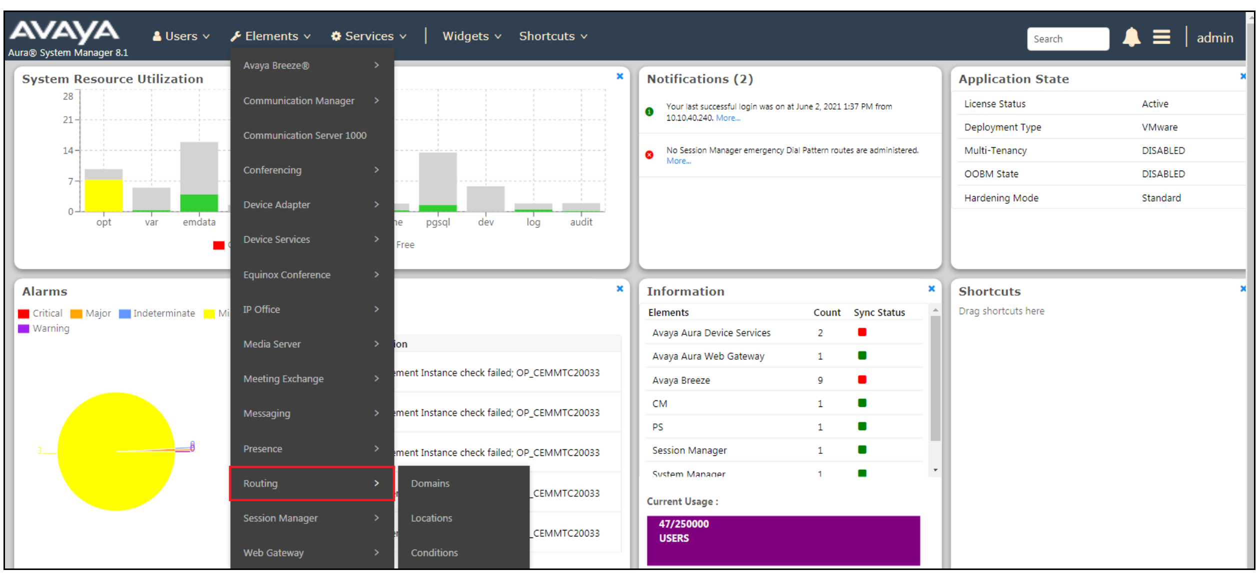
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Adding a SIP Entity for Avaya Session Border Controller for Enterprise
- Adding a Routing Policy for Avaya Session Border Controller for Enterprise
- Adding a Dial Pattern for Avaya Session Border Controller for Enterprise

To make changes on Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to https://<System Manager FQDN>/SMGR. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.



Once logged in navigate to **Elements** and click on **Routing**.

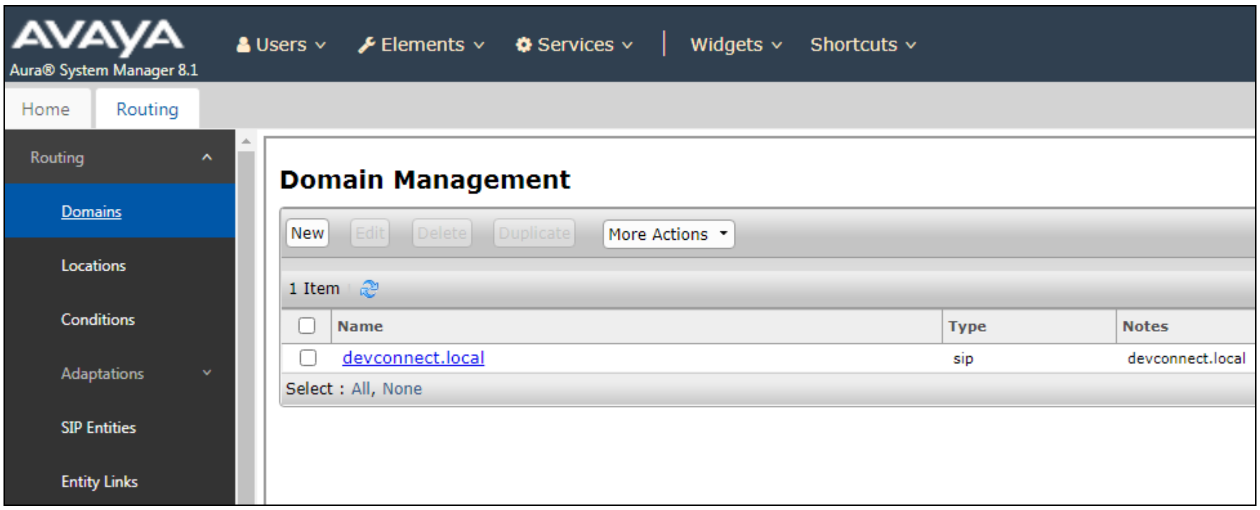


6.1. Domains and Locations

Note: It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

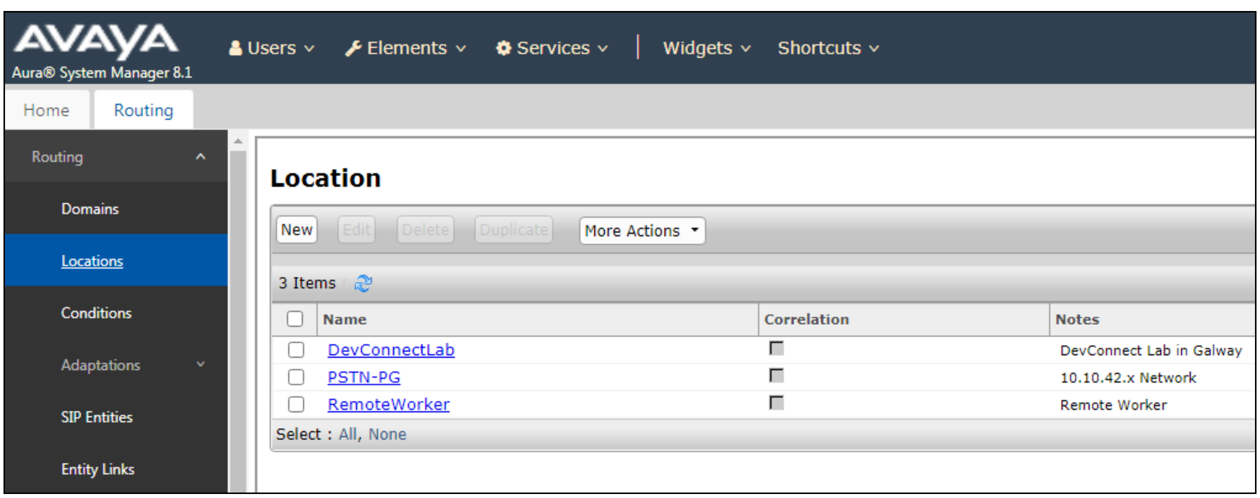
6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **devconnect.local** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.



6.1.2. Display the Location

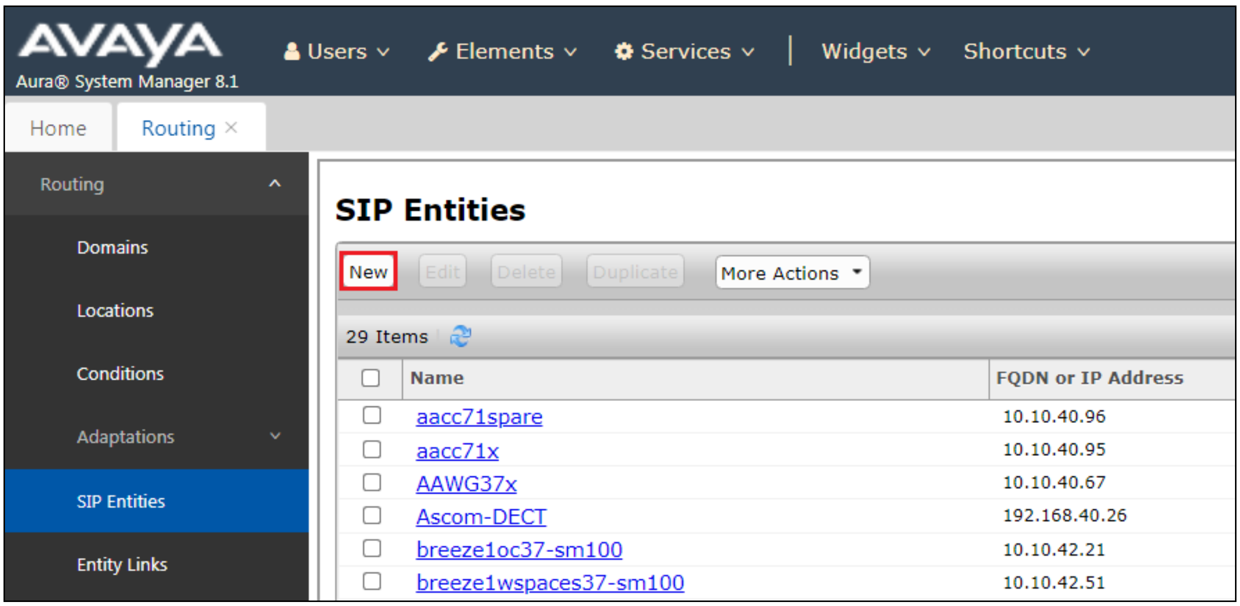
Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.



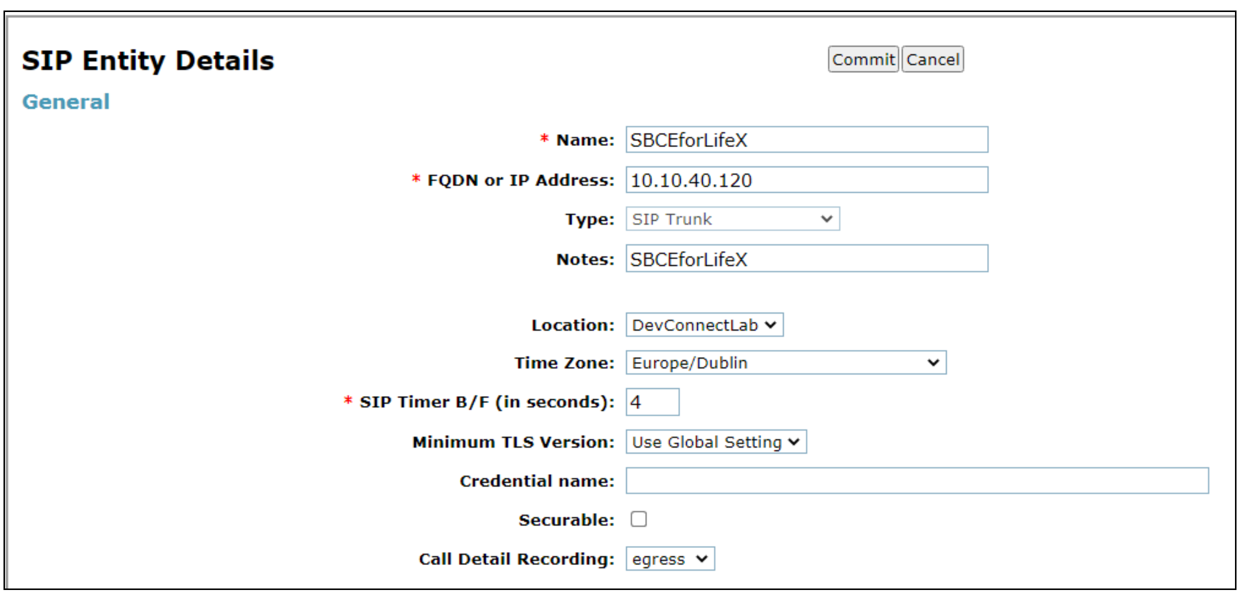
6.2. Adding a SIP Entity for Avaya Session Border Controller for Enterprise

Because the calls are routed to the Avaya Session Border Controller and then onto LifeX there is only a requirement to have the ASBCE added as a SIP Entity, all calls to LifeX will be routed to the ASBCE and the ASBCE is then configured to route the calls to LifeX.

Click on **SIP Entities** in the left column and select **New** in the right window.

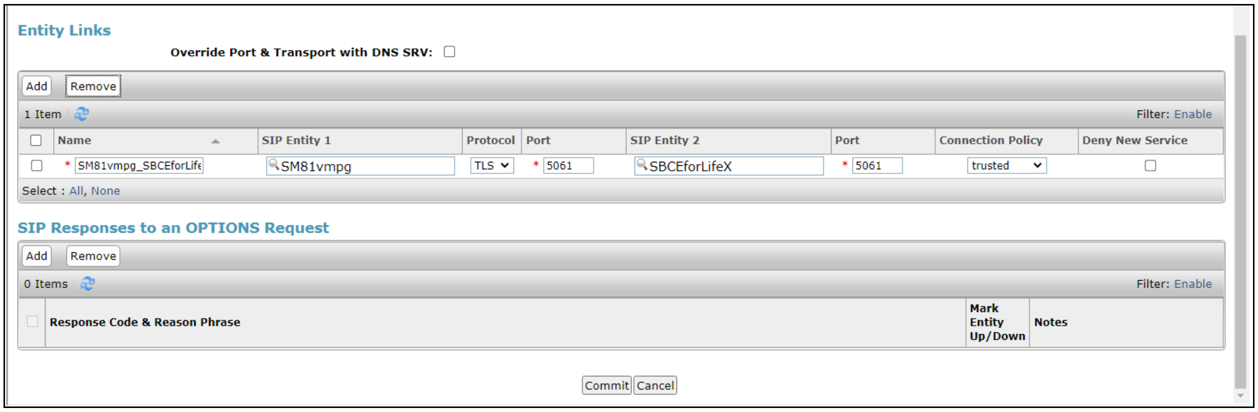


Enter a suitable **Name** for the SIP Entity, enter the **IP Address** of the ASBCE. Enter the correct **Time Zone** and **Location**. From this page, scroll down to add the appropriate Entity Link.



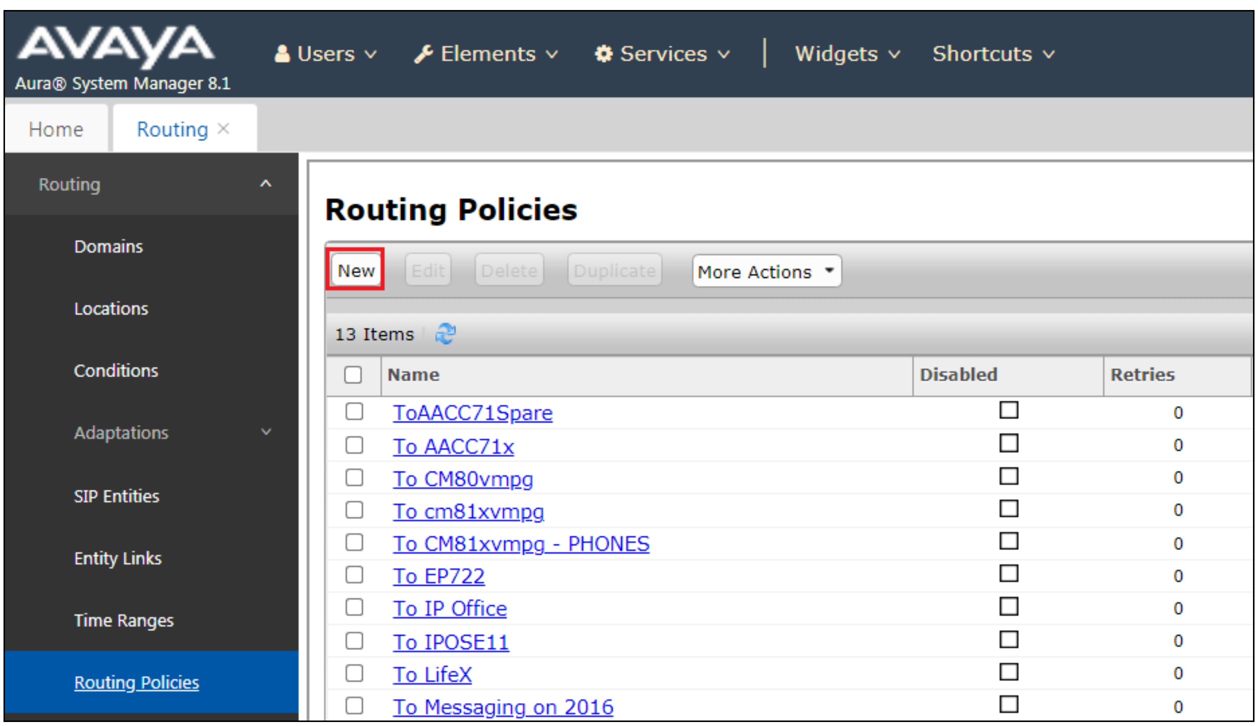
An Entity Link can be added from the SIP Entities page, as shown in the previous page, by scrolling down to **Entity Links**.

Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created ASBCE SIP Entity for **SIP Entity 2**. Ensure that **TLS** is selected for the **Protocol** and that **Port 5061** is used, this is to secure communications between Session Manager and the ASBCE. Click on **Commit** once finished to save the new Entity Link and SIP Entity.

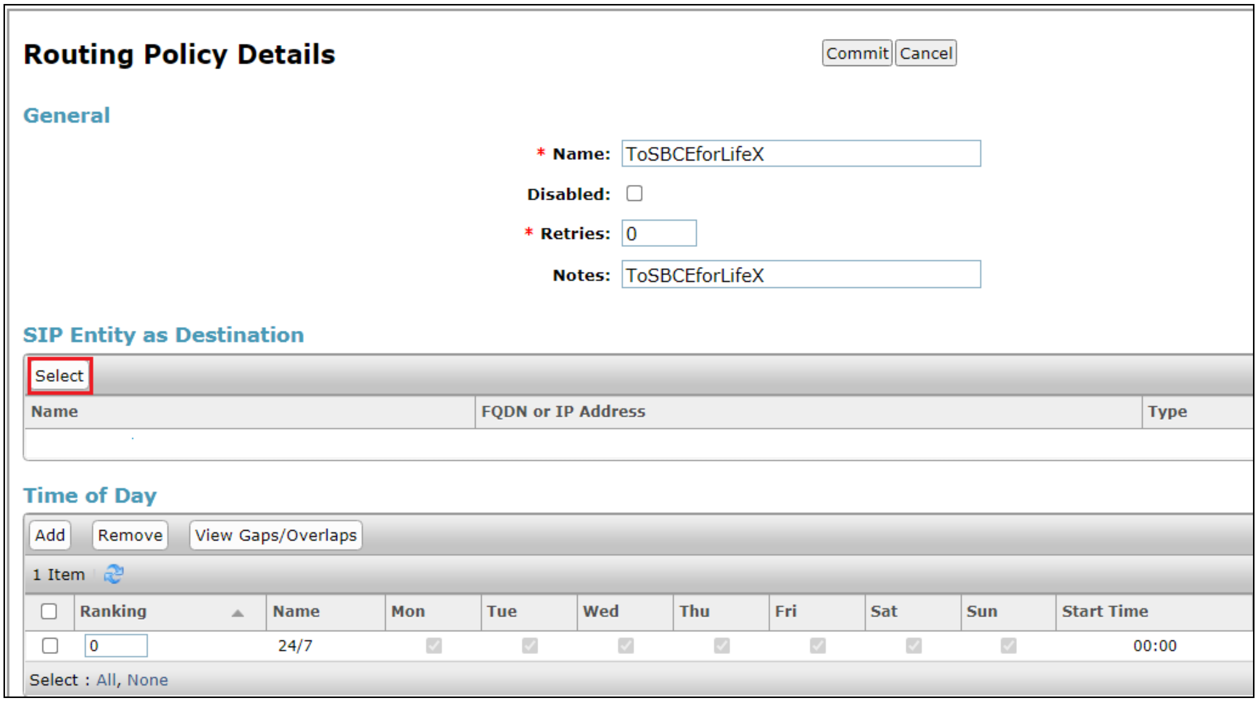


6.3. Adding a Routing Policy for Avaya Session Border Controller for Enterprise

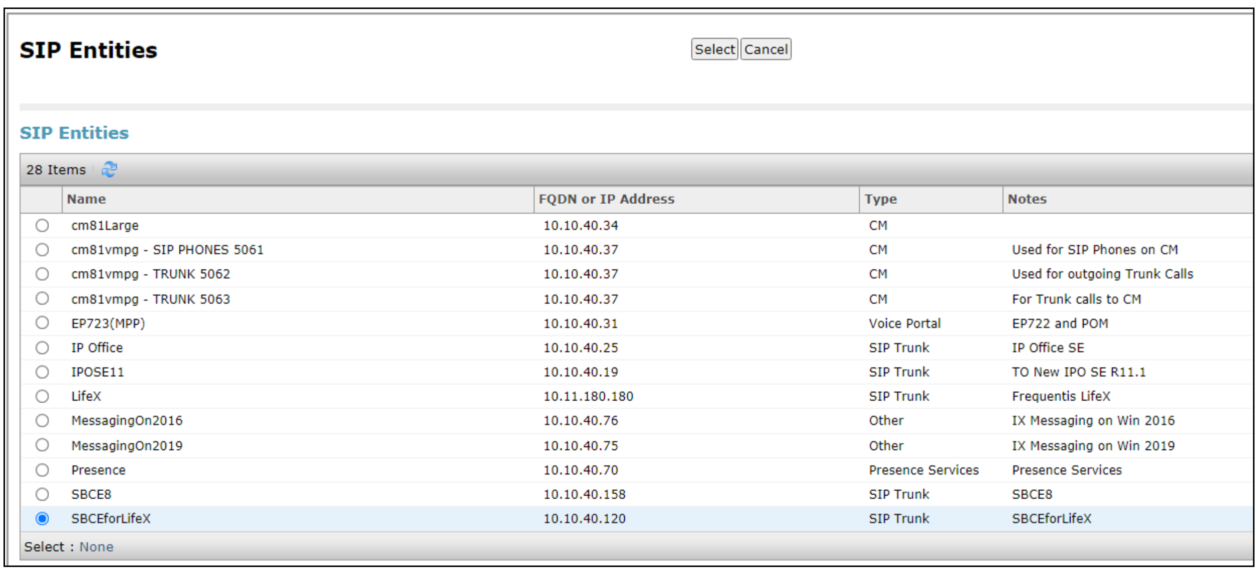
Click on **Routing Policies** in the left window and select **New** in the main window.



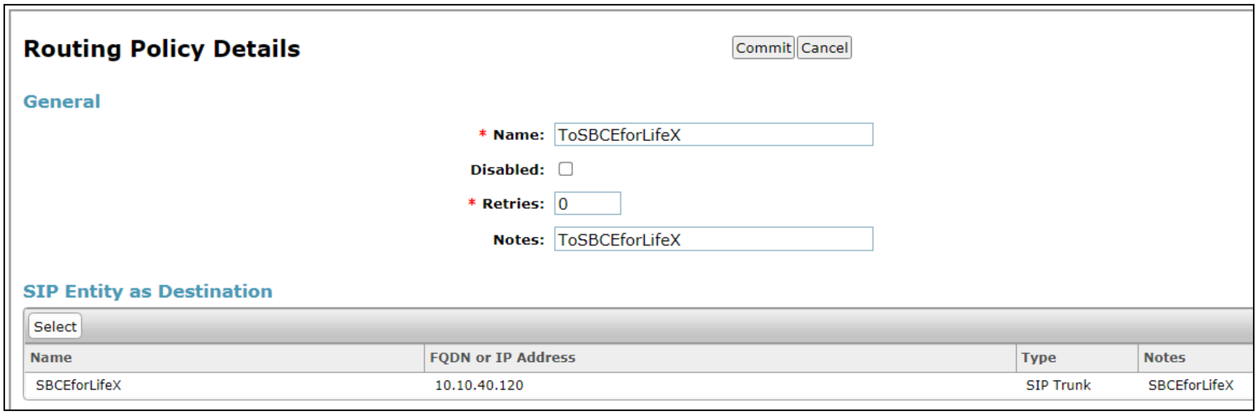
Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**.



Select the ASBCE SIP Entity (**SBCEforLifeX**) as shown below and click on **Select**.

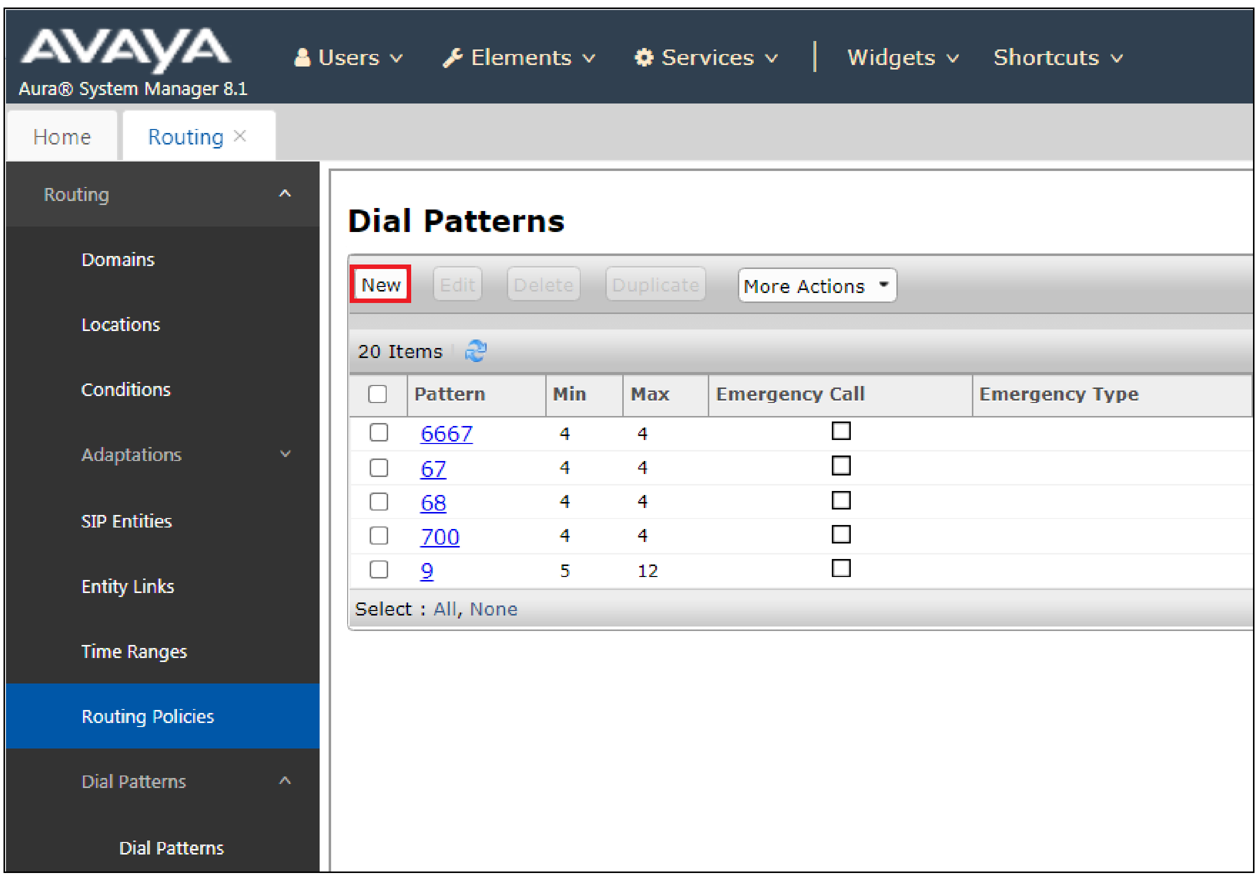


The selected destination is now shown, click on **Commit** to save this.

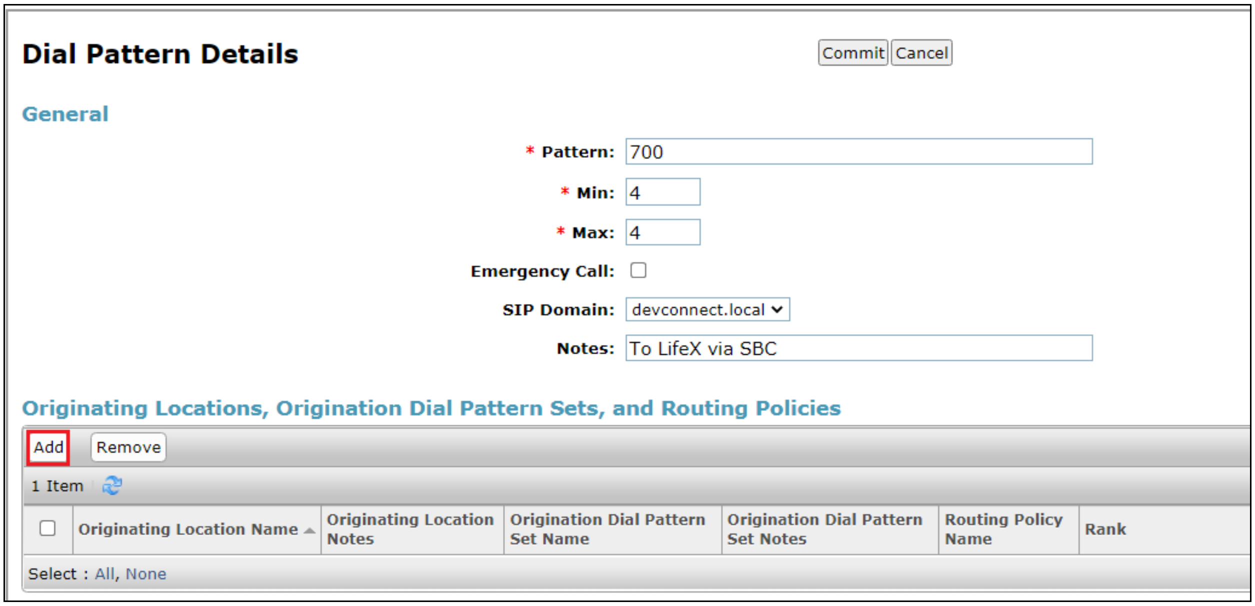


6.4. Adding a Dial Pattern for Avaya Session Border Controller for Enterprise

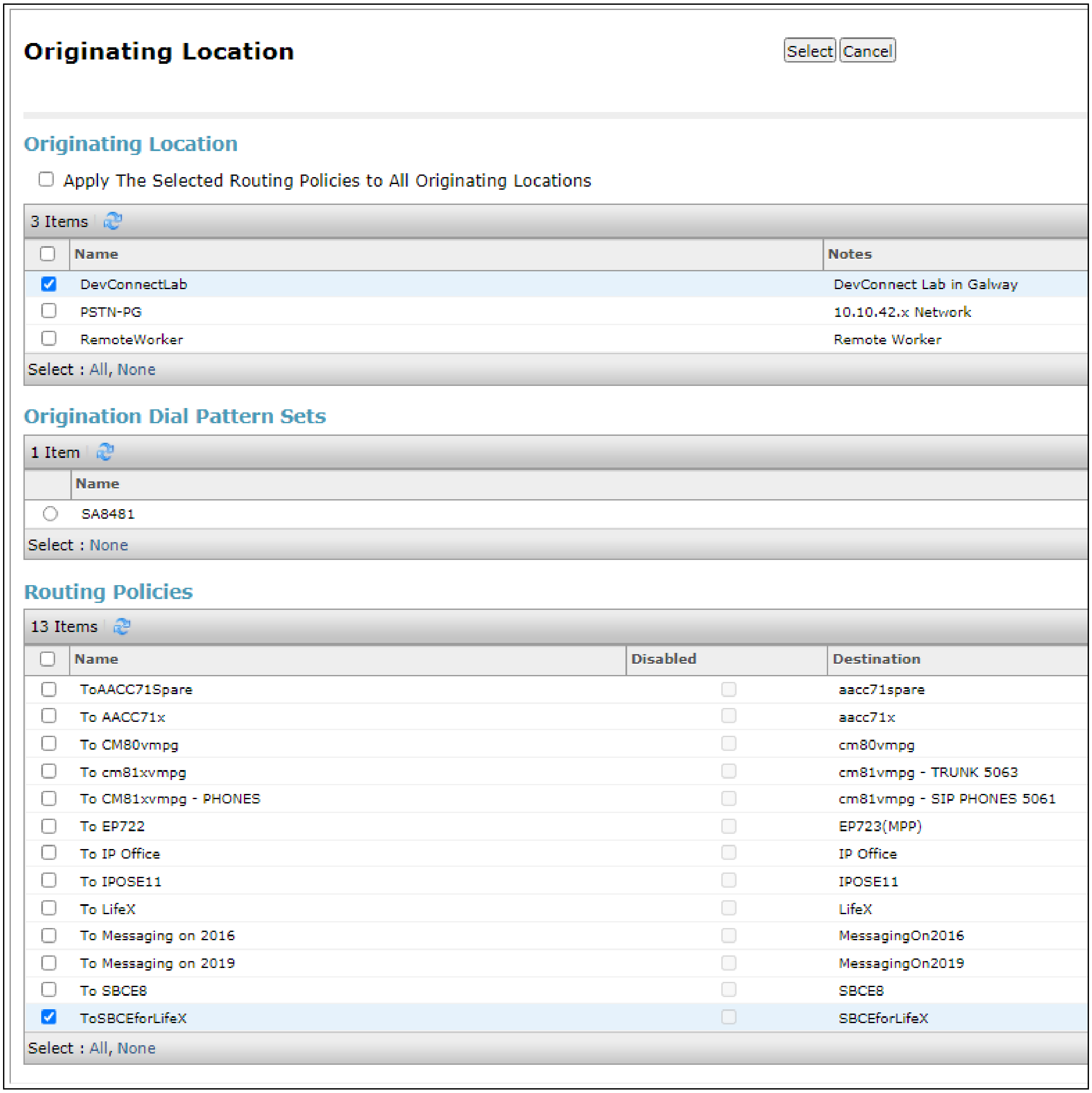
Select **Dial Patterns** in the left window and select **New** in the main window.



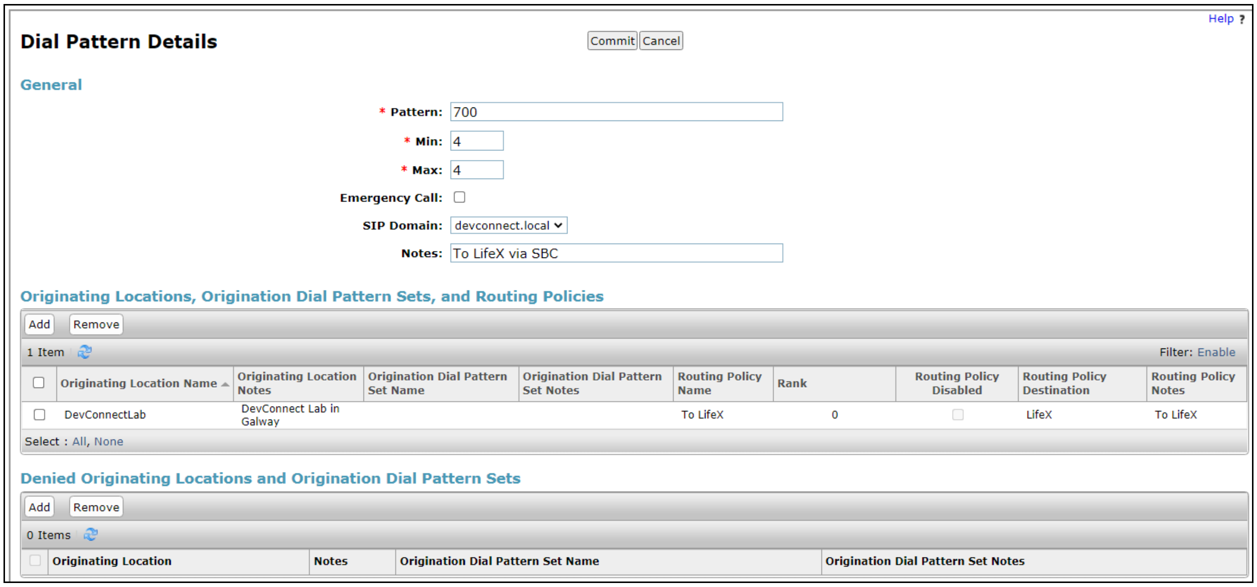
Enter the required digits for the Pattern, in the example below 700 is used, which means that 7000 – 7009 will use the Routing Policy that will be selected. **700** is entered as the **Pattern** and the **Min** and **Max** digit length of **4** is used thus giving 700x. Ensure that the correct domain is entered for **SIP Domain** in this example the domain created in **Section 6.1.1** is added. Click on **Add** under **Originating Locations, Origination Dial Pattern Sets, and Routing Policies** to select the Routing Policy.



Select the **Originating Location**, this will be the location added in **Section 6.1.2** select the newly created routing policy for the ASBCE (**ToSBCEforLifeX**).



With the Routing Policy selected click on **Commit** to finish adding the **Dial Pattern**.

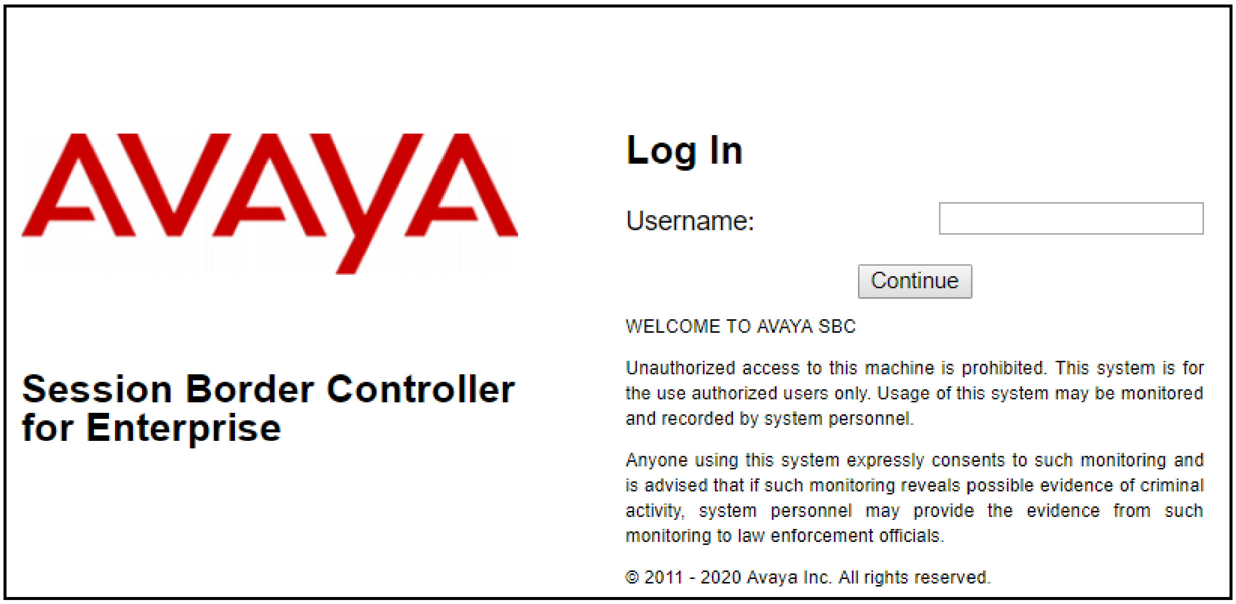


7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE, consult the Avaya SBCE documentation in the **Section 11**.

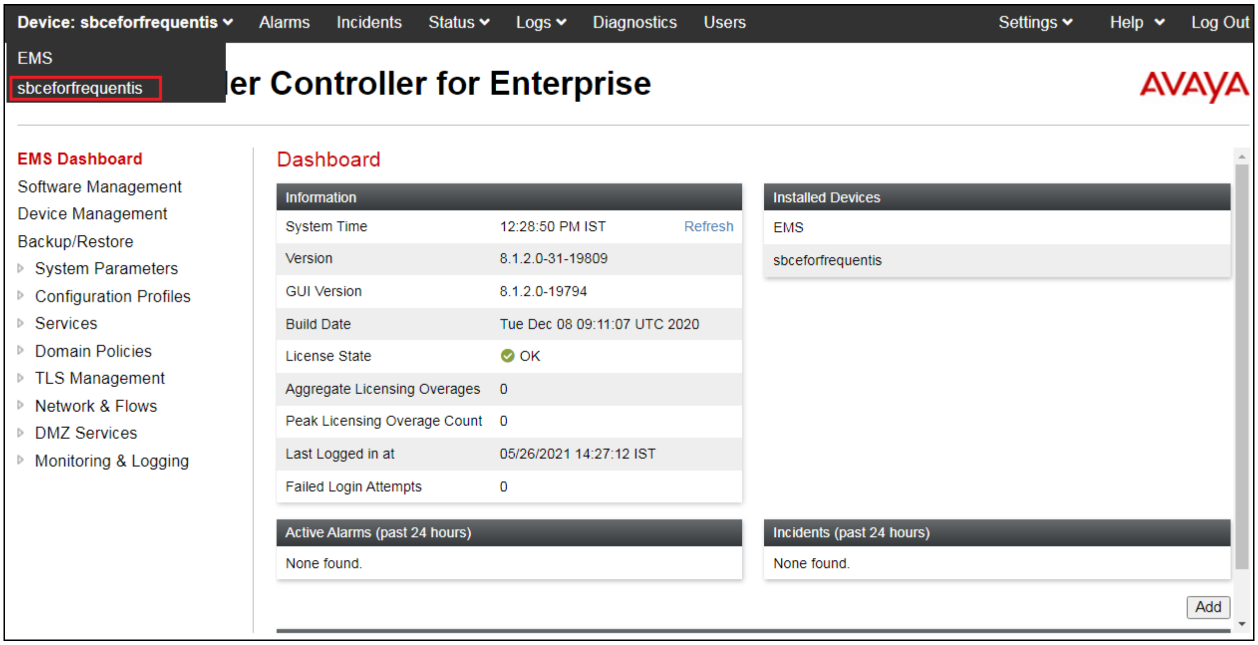
7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



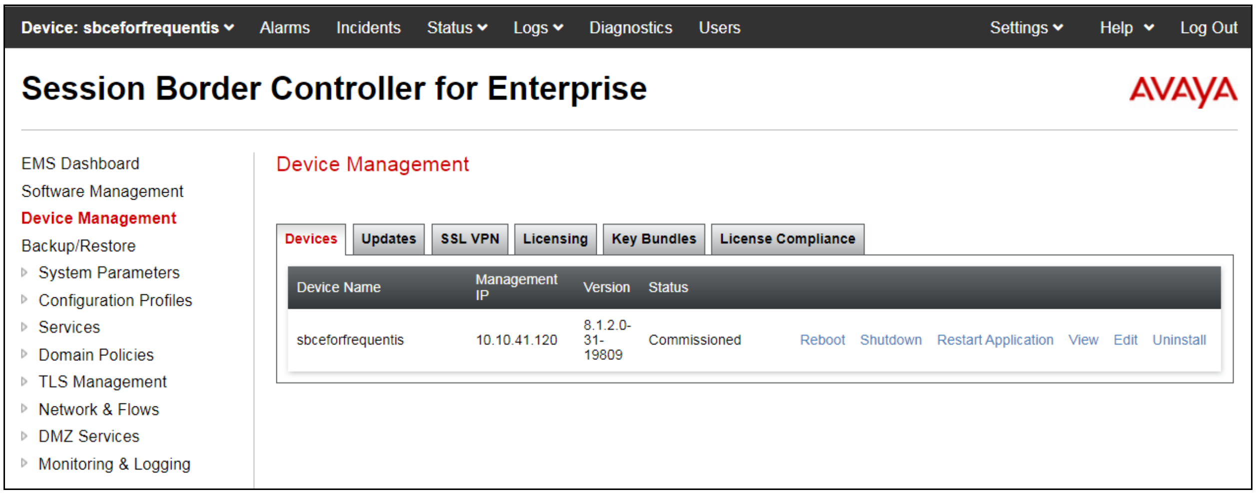
Once logged in, on the top left of the screen, under **Device:** select the device being managed, ***sbceforfrequentis*** in the sample configuration.

The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.



7.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named ***sbceforfrequentis*** is shown. The current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.

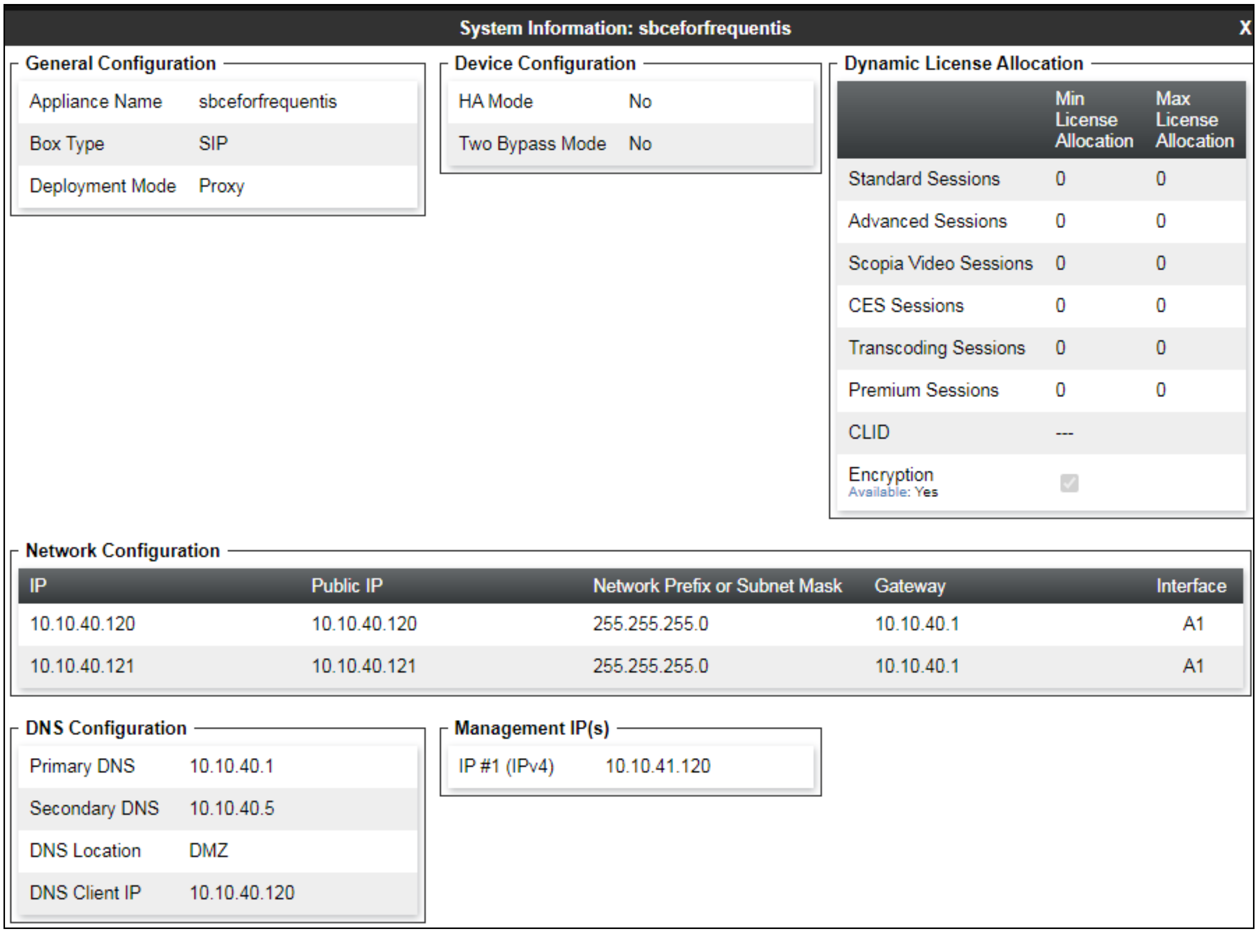


To view the network configuration assigned to the Avaya SBCE, click **View** on the screen shown above. The **System Information** window is displayed, containing the current device configuration and network settings.

The highlighted IP addresses in the **System Information** screen shown on the next page are the ones used for the SIP trunk to LifeX and are the ones relevant to these Application Notes. Other IP addresses me be assigned to other interfaces to support remote workers and other SIP trunks, and they are not discussed in this document.

The private interface of the Avaya SBCE (10.10.40.120) was used to connect to the enterprise network, the public interface of the Avaya SBCE (10.10.40.121) was used to connect to the LAN interface of the LifeX managed SBC (10.11.180.180). A VPN connection to the network connected to LifeX was used to facilitate compliance testing, see **Figure 1**. Note that Frequentis is responsible for the configuration of the Session Border Controller that we are connecting to from this Avaya SBCE.

On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.



7.3. TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

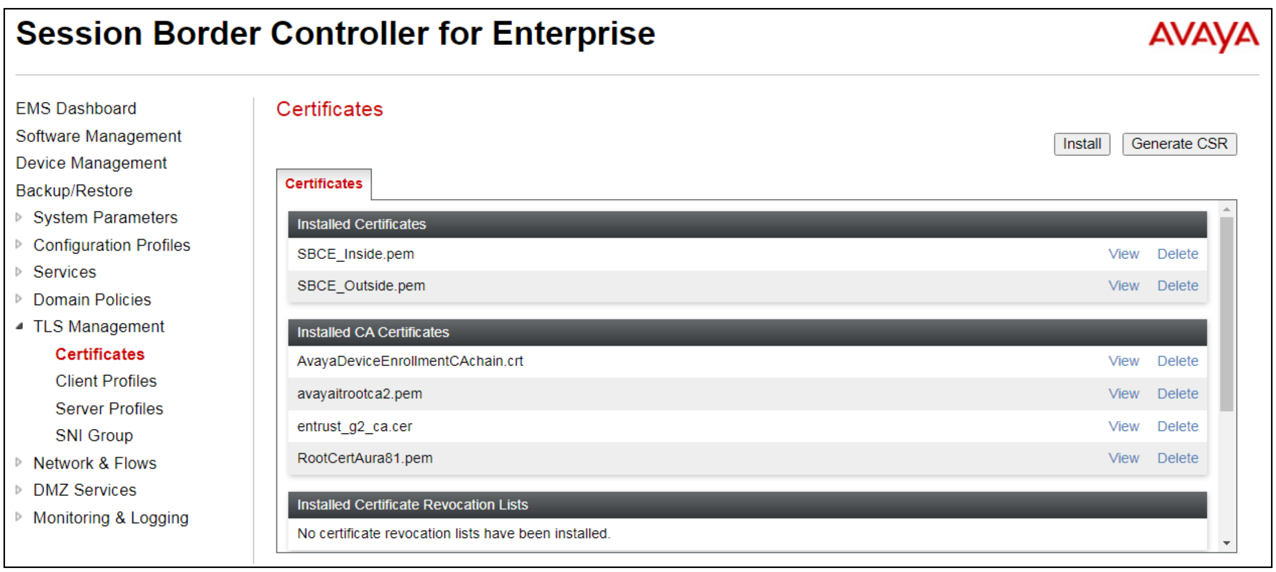
In the reference configuration, TLS transport is used for both the communication between Session Manager and Avaya SBCE and between the Avaya SBCE and LifeX. The following procedures show how to create the client and server profiles to support the TLS connection.

Note – Testing was done with System Manager signed identity certificates. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

7.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

Select **TLS Management → Certificates** from the left-hand menu. Verify the following:

- System Manager CA certificate is present in the **Installed CA Certificates** area.
- System Manager CA signed identity certificate is present in the **Installed Certificates** area.
- Private key associated with the identity certificate is present in the **Installed Keys** area, (not shown below but is visible after scrolling down the page).

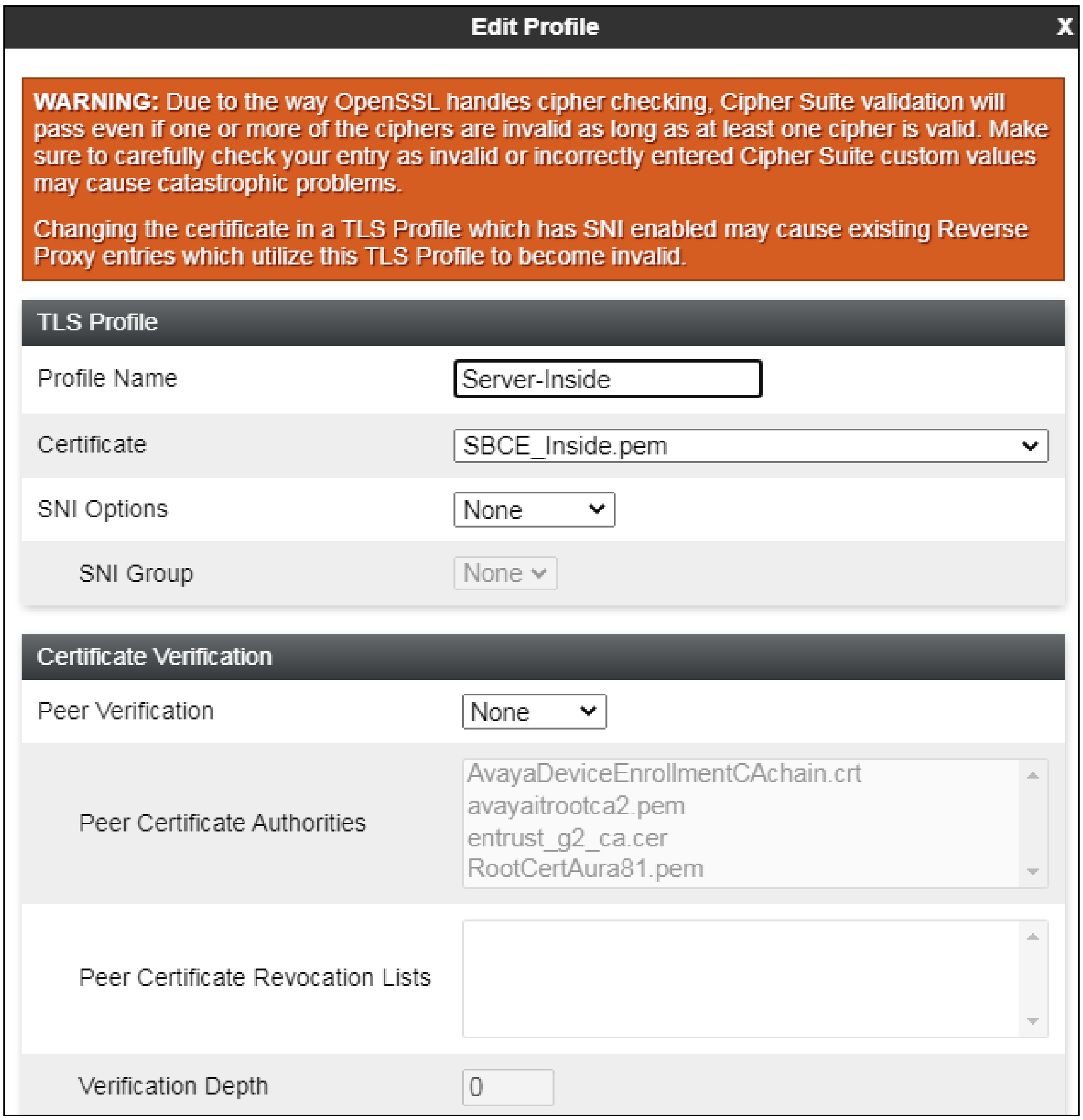


7.3.2. Server Profiles

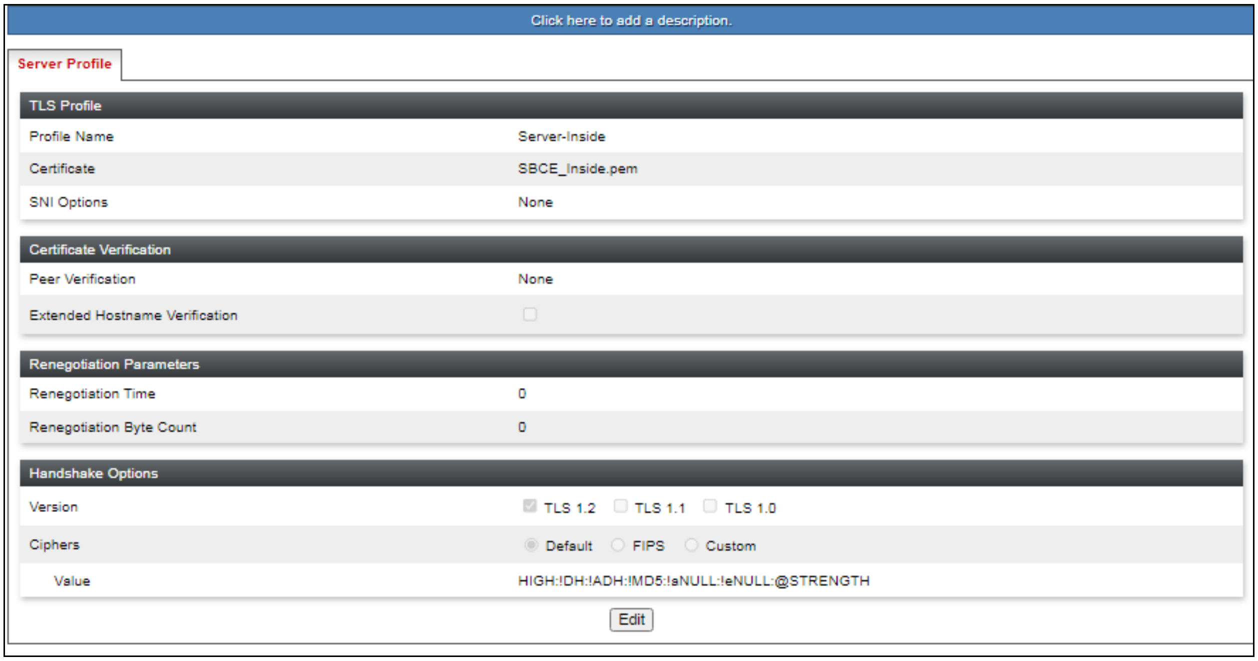
Select **TLS Management → Server Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **SBCE_inside.pem**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

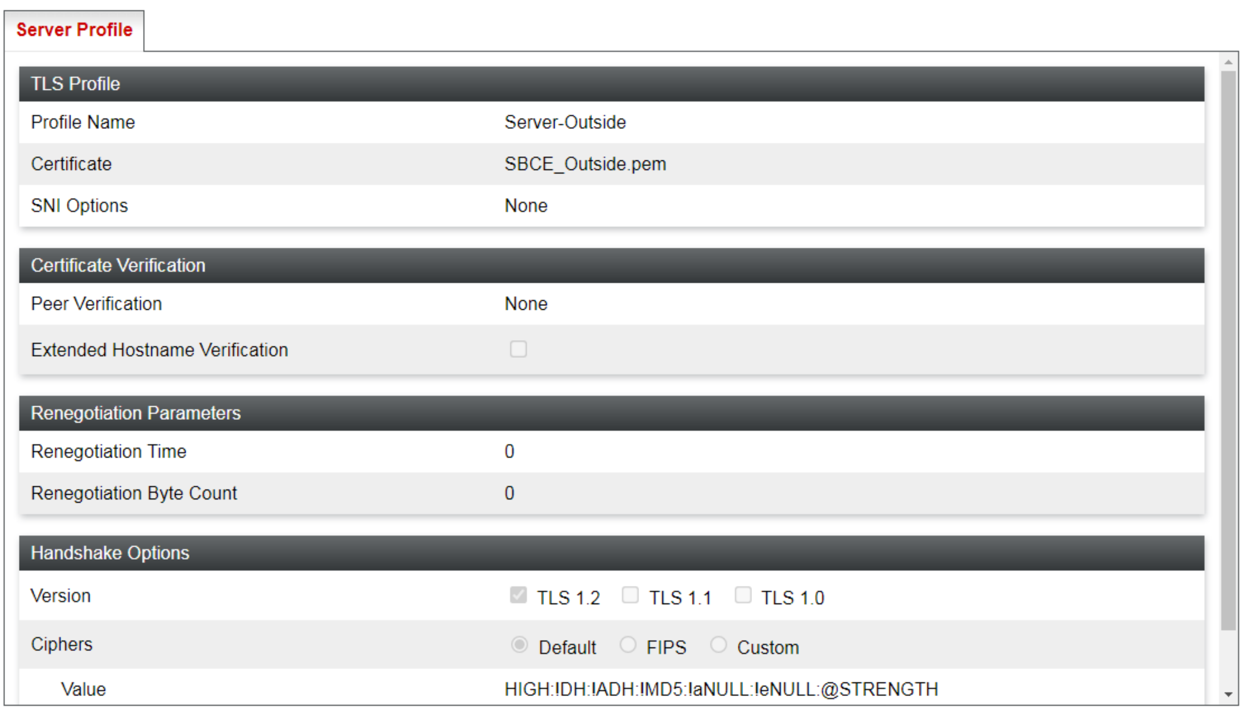
Accept default values for the next screen (not shown) and click **Finish**.



The following screen shows the completed TLS **Server Profile** form.



Below is the profile set for the outside server connection. It is very similar to that above just uses a different **Certificate** that contains the outside IP address instead of the inside or enterprise IP address.

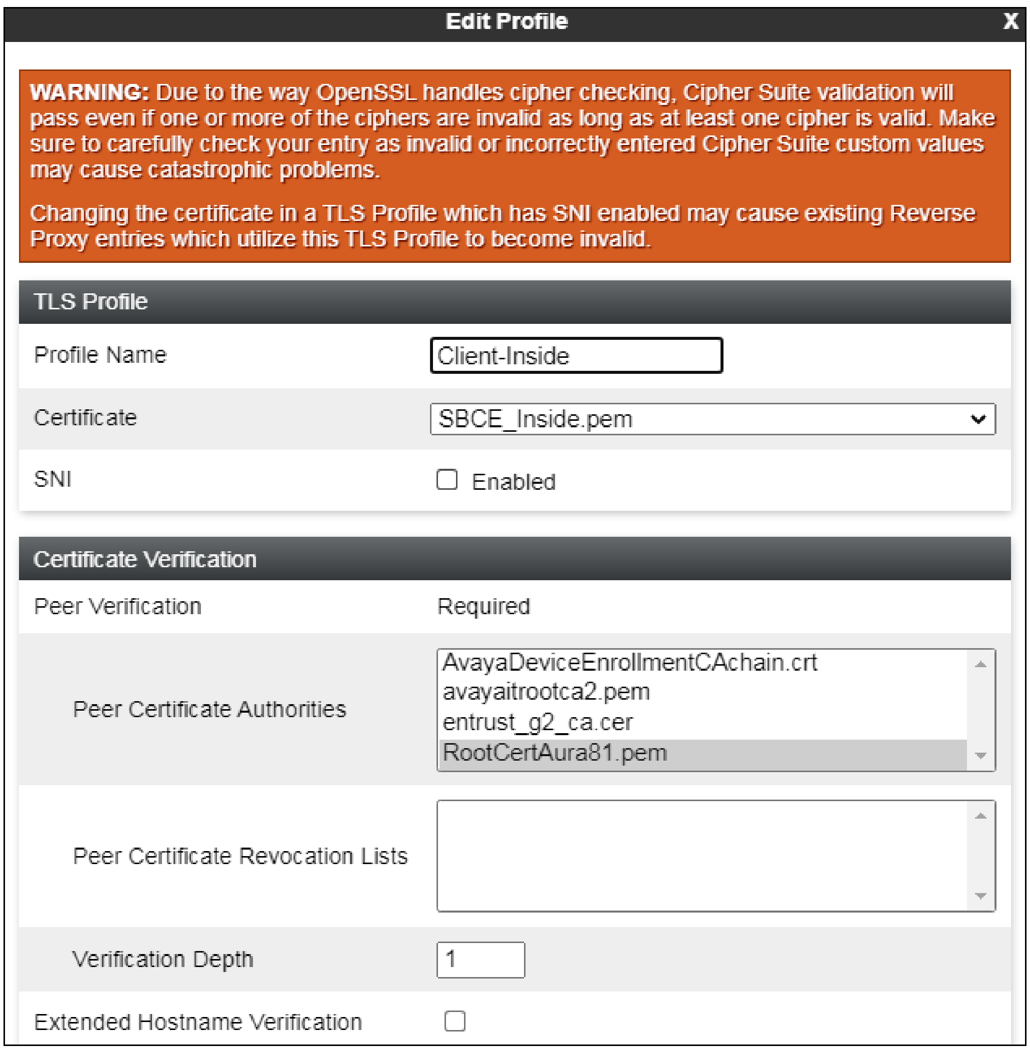


7.3.3. Client Profiles

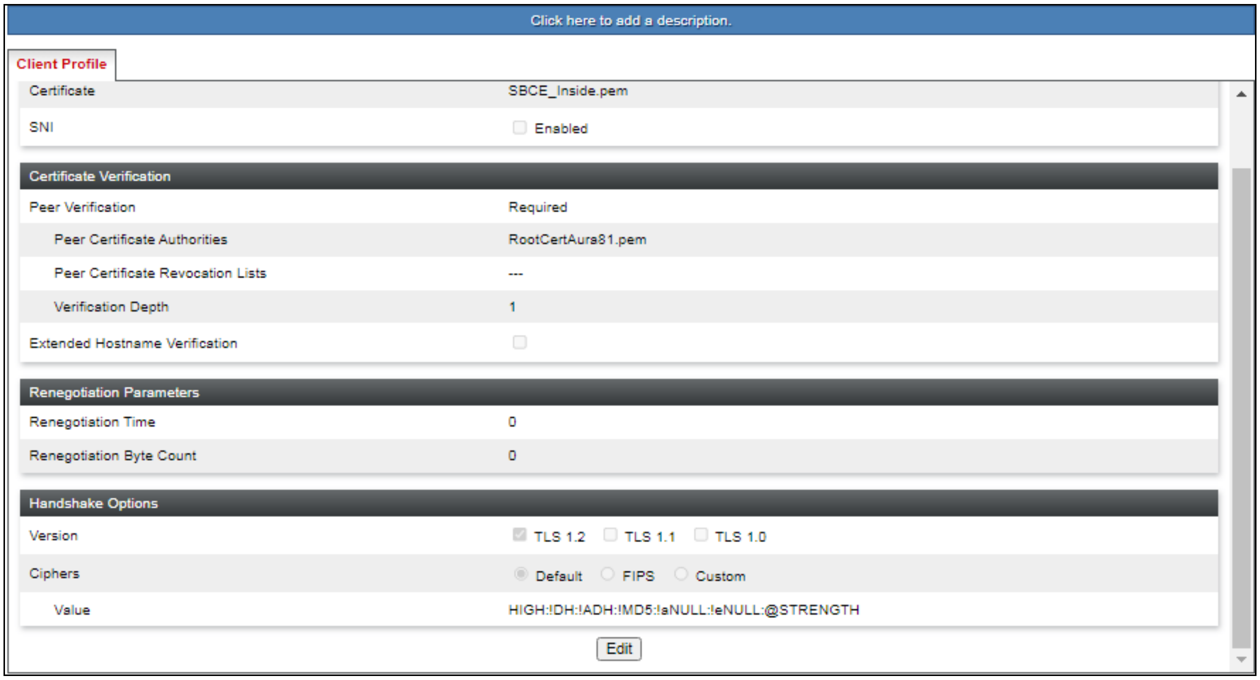
Select **TLS Management → Client Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **SBCE_Inside.pem**, from pull down menu.
- **Peer Verification** = **Required**.
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **RootCertAura81.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

Accept default values for the next screen (not shown) and click **Finish**.



The following screen shows the completed TLS **Client Profile** form:



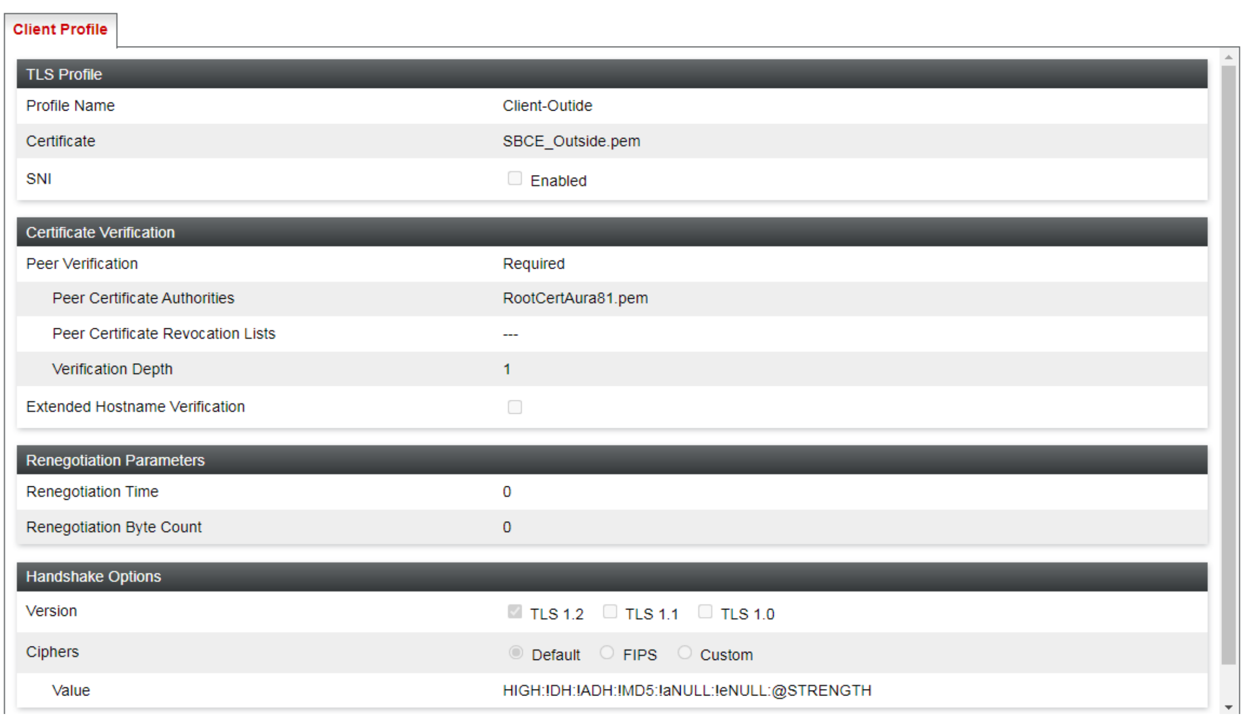
Click here to add a description.

Client Profile

Certificate	SBCE_Inside.pem
SNI	☐ Enabled
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	RootCertAura81.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	☐
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	☑ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
Ciphers	◉ Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

Below is the profile set for the outside client connection. It is very similar to that above just uses a different **Certificate** that contains the outside IP address instead of the inside or enterprise IP address.



Client Profile

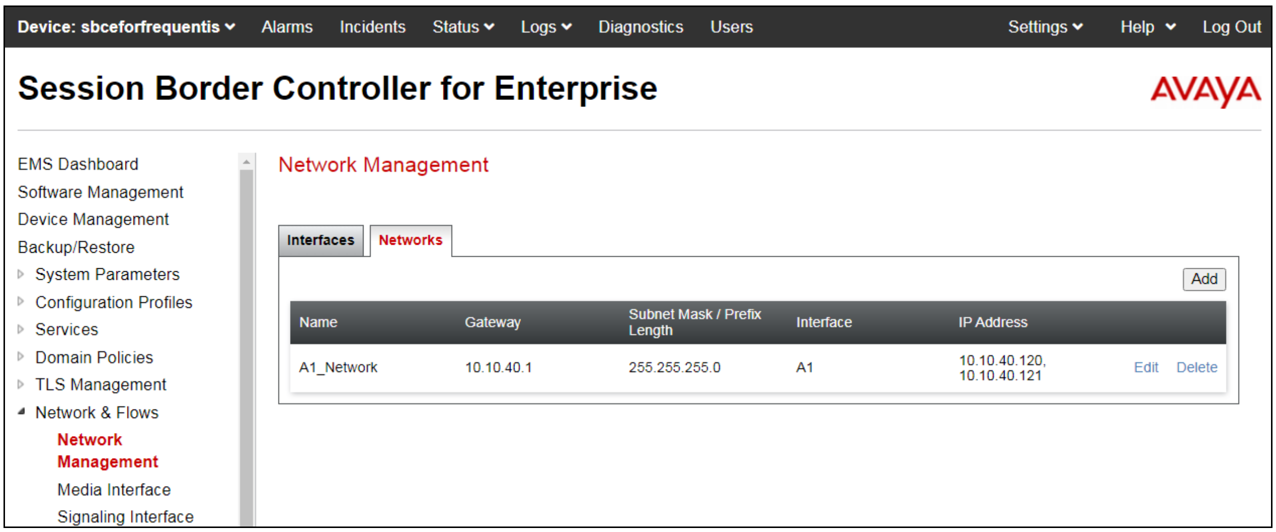
TLS Profile	
Profile Name	Client-Outide
Certificate	SBCE_Outside.pem
SNI	☐ Enabled
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	RootCertAura81.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	☐
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	☑ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
Ciphers	◉ Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

7.4. Network Management

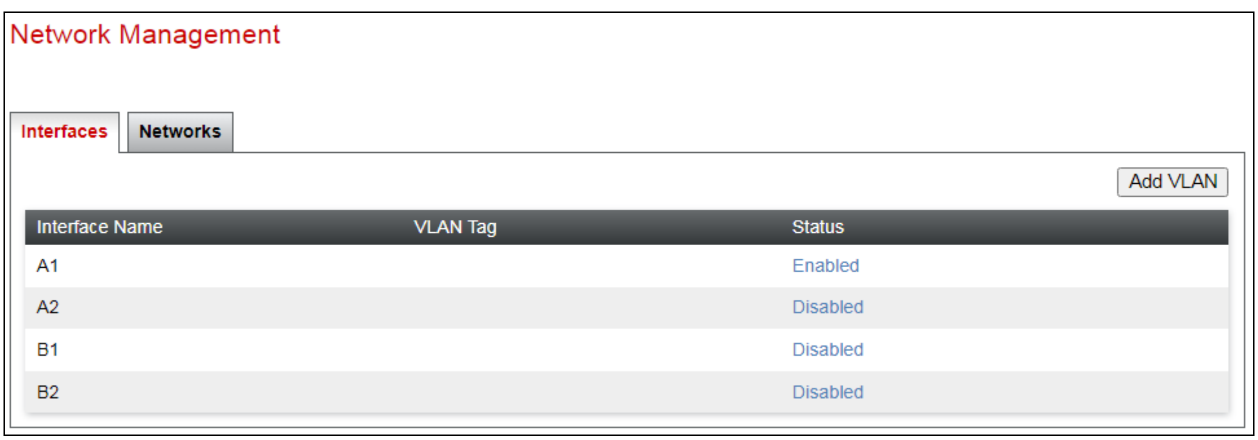
The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from the **Network & Flows** on the left-side menu. On the **Networks** tab, verify or enter the network information as needed.

The configuration used during the compliance test is displayed below, the IP addresses assigned to the private (***10.10.40.120***) and public (***10.10.40.121)*** sides are as shown.



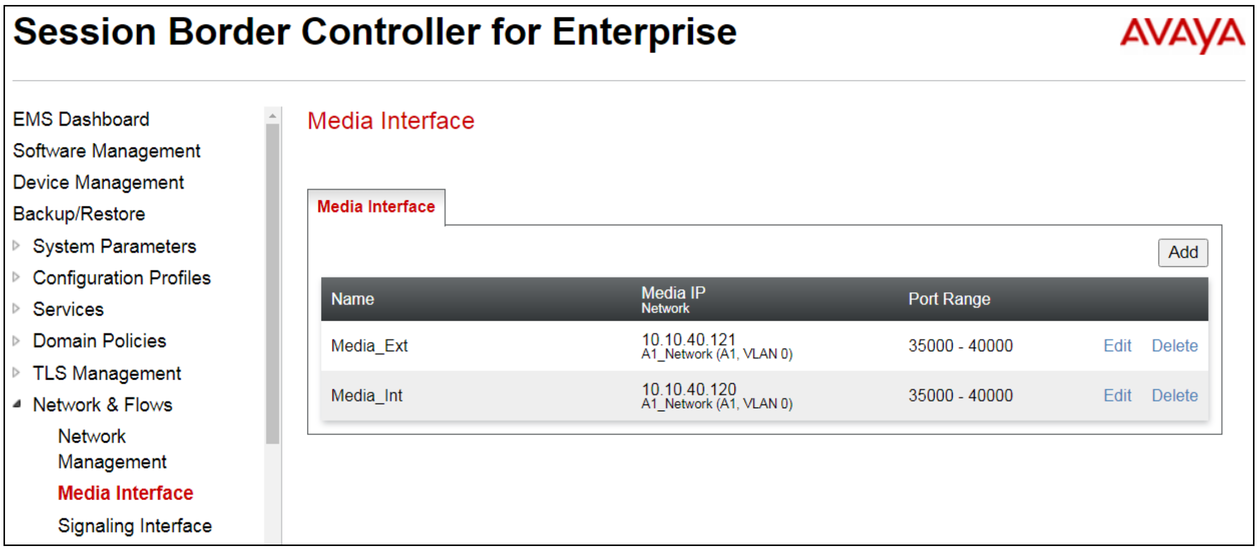
On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for the **A1** interface. Click the buttons under the **Status** column if necessary, to enable the interface.



7.5. Media Interfaces

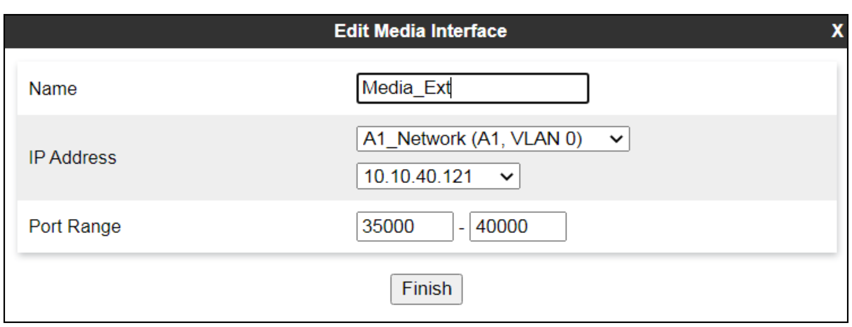
Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call Server or the trunk server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (the two configured Media Interfaces are already shown below).



The example below shows the external media interface, as shown in the screen above similar configurations are used for both internal and external interfaces. If a new media interface is to be added, these are the necessary steps to follow.

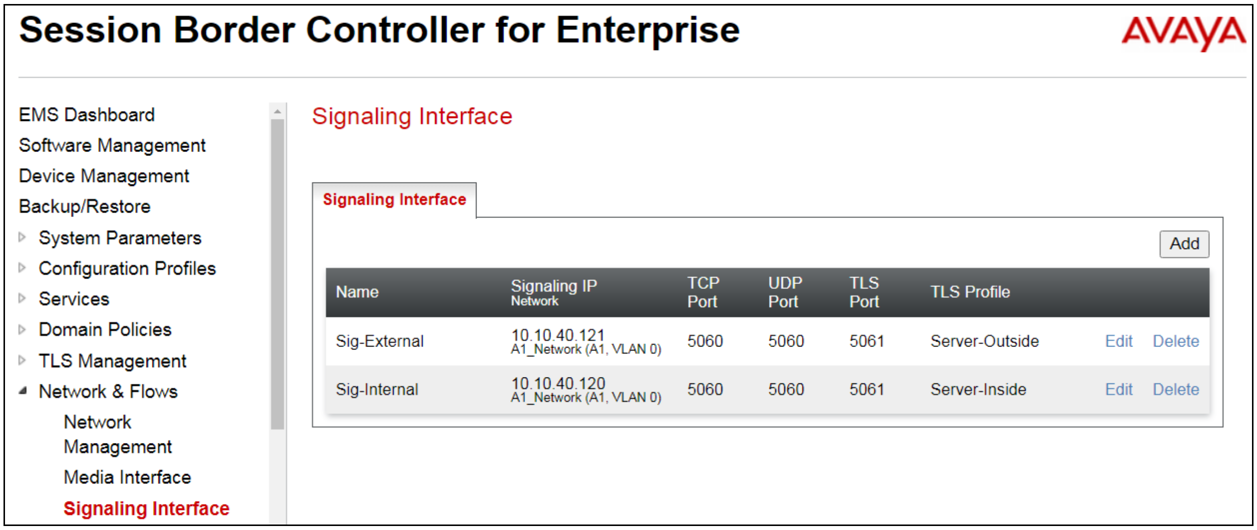
- On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface, in the example **Media_Ext** was used.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.



7.6. Signaling Interfaces

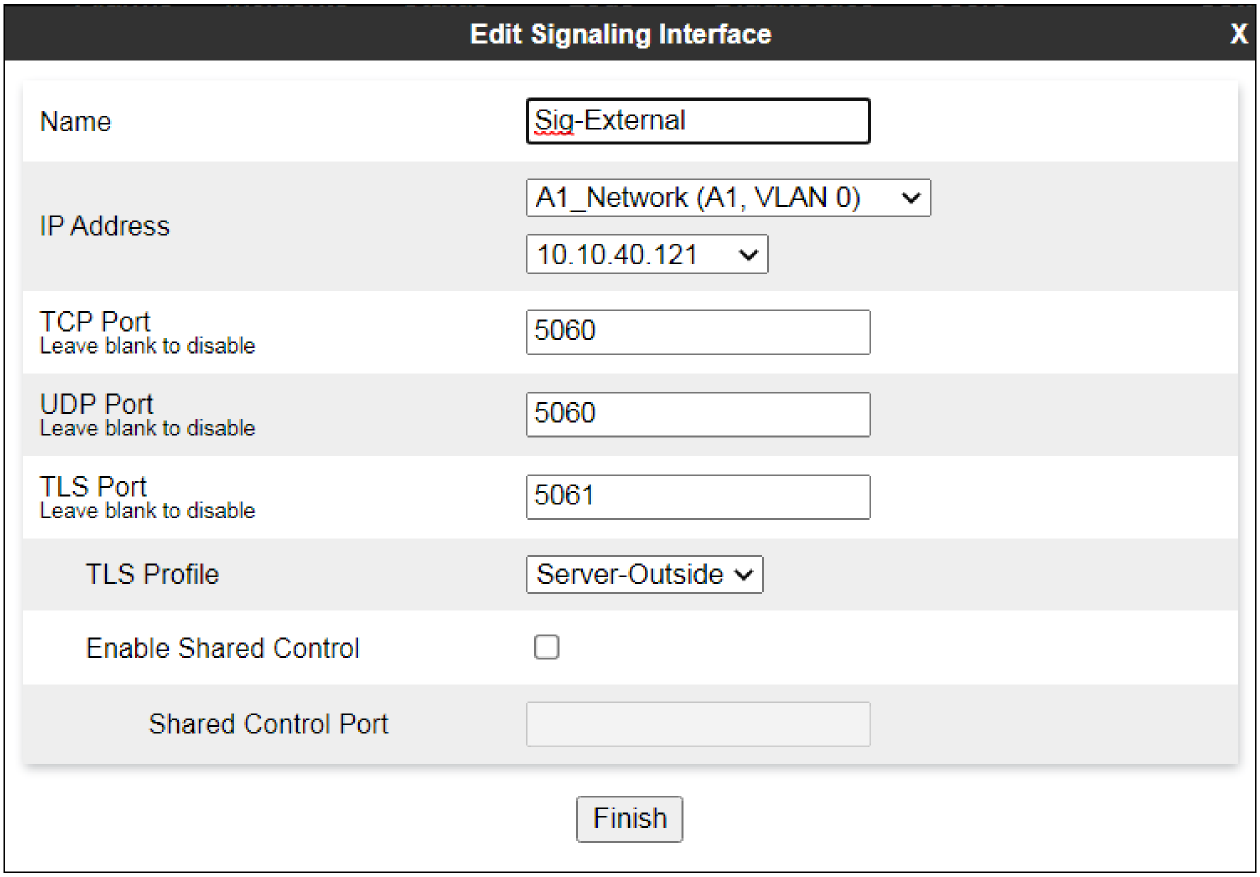
Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (the two configured Signaling Interfaces are already shown below).



The example on the next page shows the Signaling Interface that was used for the external connection to LifeX, a similar interface needs to be created for the connection to Session Manager. As shown above from the configured interfaces, there are different IP addresses used as well as different TLS Profiles. If a new interface is to be created, then click on Add from the screen above.

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface, in the example **Sig-External** was used.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.2**.
- Select a **TLS Profile** defined in **Section 7.3.2**.
- Click **Finish**.

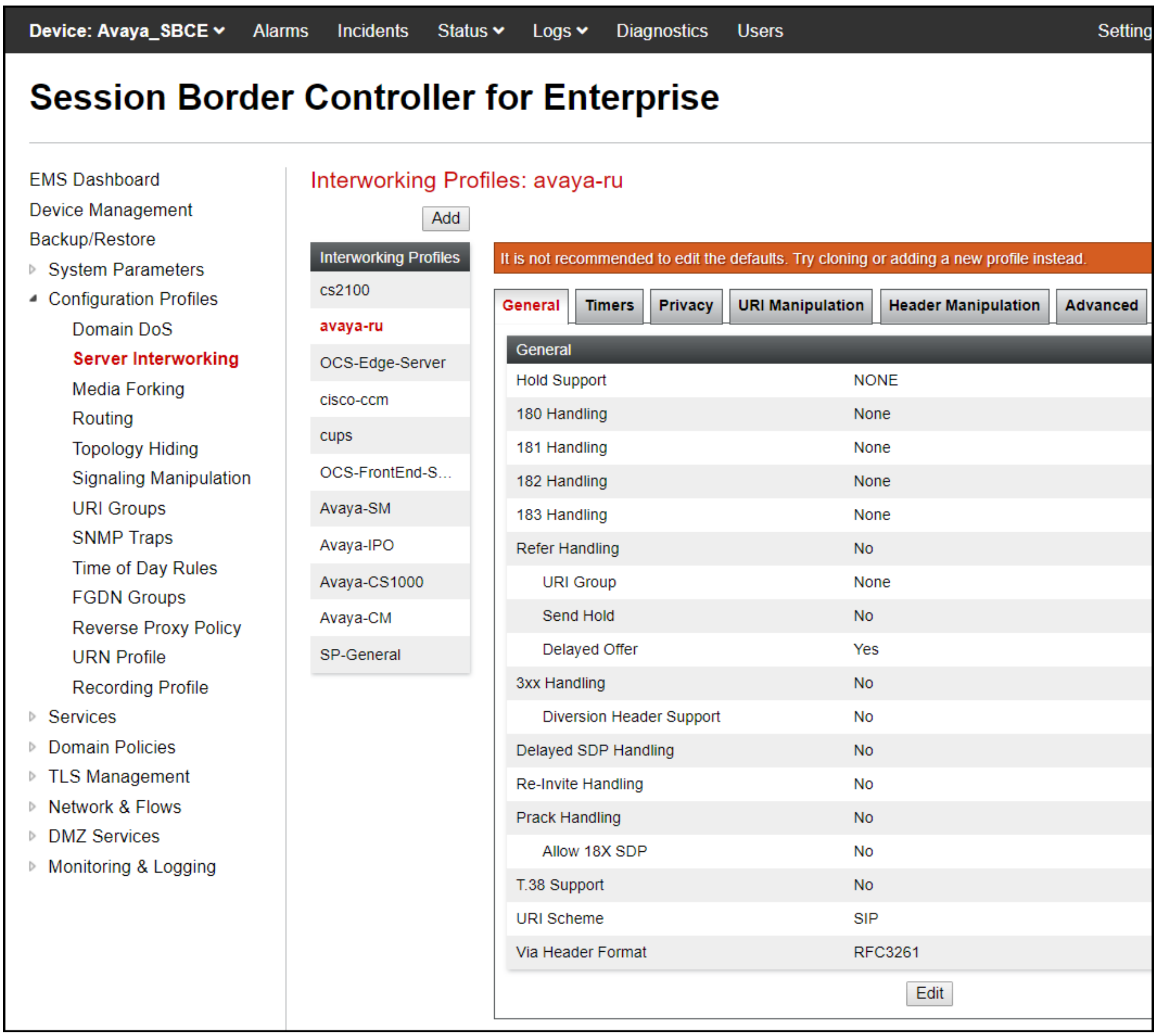

Edit Signaling Interface
X
Name
Sig-External
IP Address
A1_Network (A1, VLAN 0)
10.10.40.121
TCP Port
Leave blank to disable
5060
UDP Port
Leave blank to disable
5060
TLS Port
Leave blank to disable
5061
TLS Profile
Server-Outside
Enable Shared Control
Shared Control Port
Finish

7.7. Server Interworking

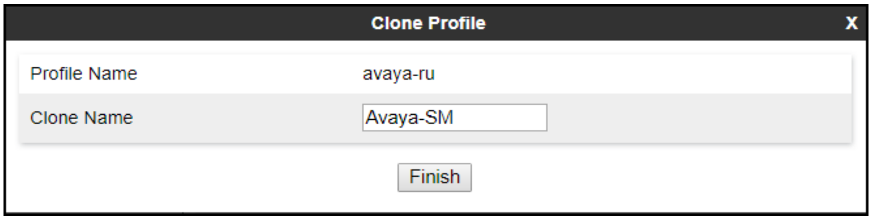
Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

7.7.1. Server Interworking Profile – Enterprise

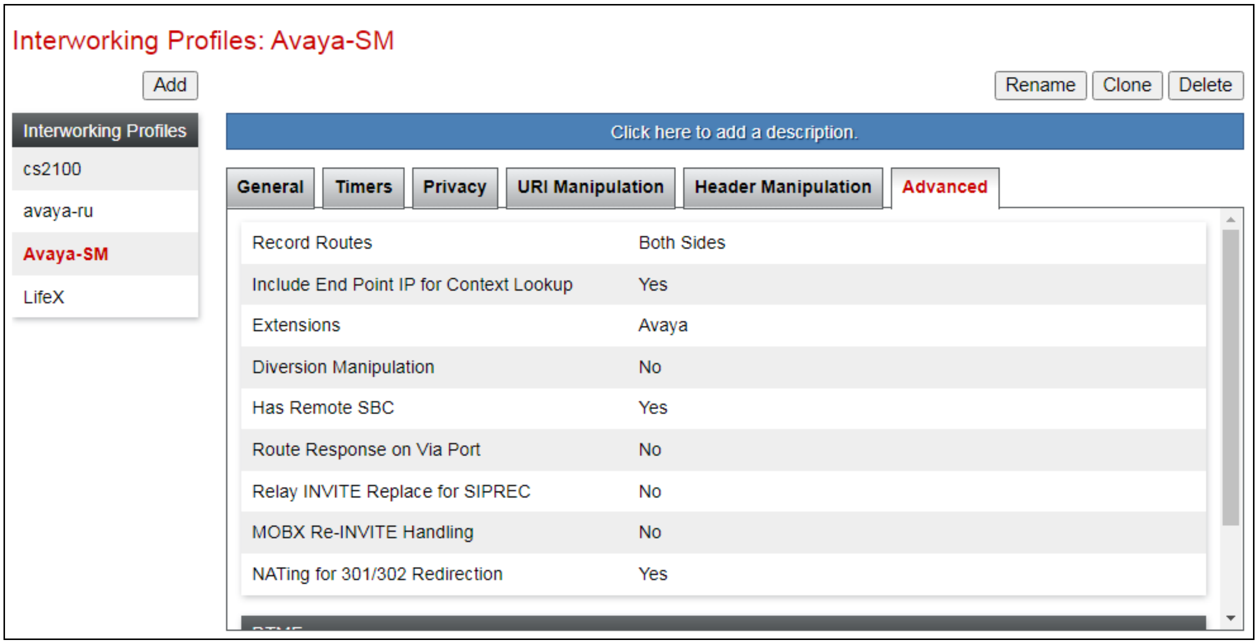
Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Configuration Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select ***avaya-ru*** from the list of pre-defined profiles. Click **Clone** (not shown).



Enter a descriptive name for the cloned profile and click **Finish**.

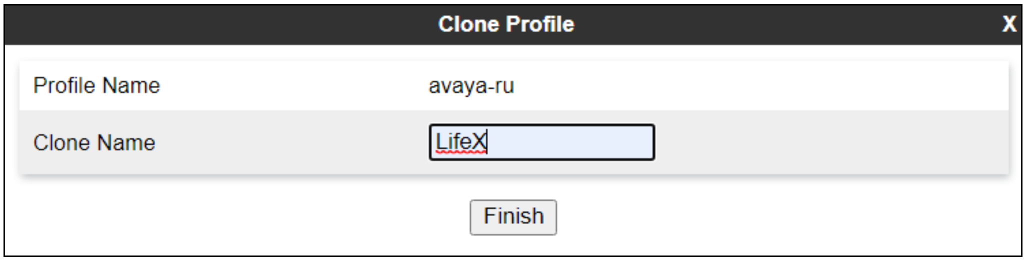


The **Advanced** tab settings are shown on the screen below:

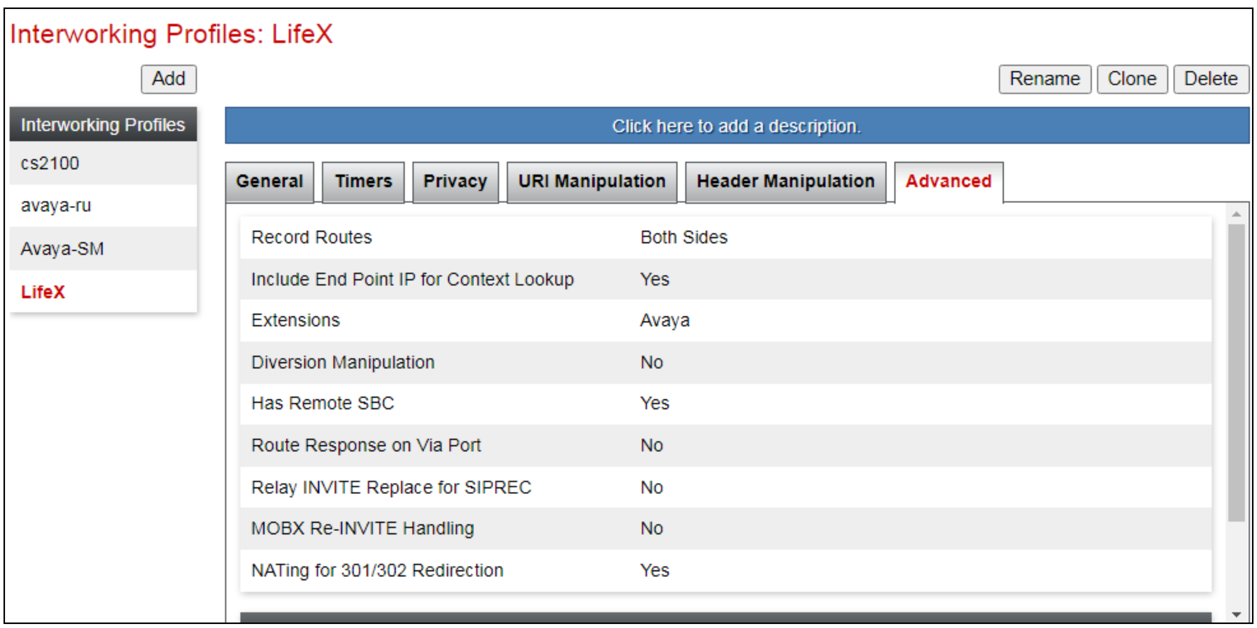


7.7.2. Server Interworking Profile – LifeX

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Configuration Profiles → Server Interworking** on the left navigation pane and click **Clone** (not shown). Enter a descriptive name for the new profile and click **Finish**.

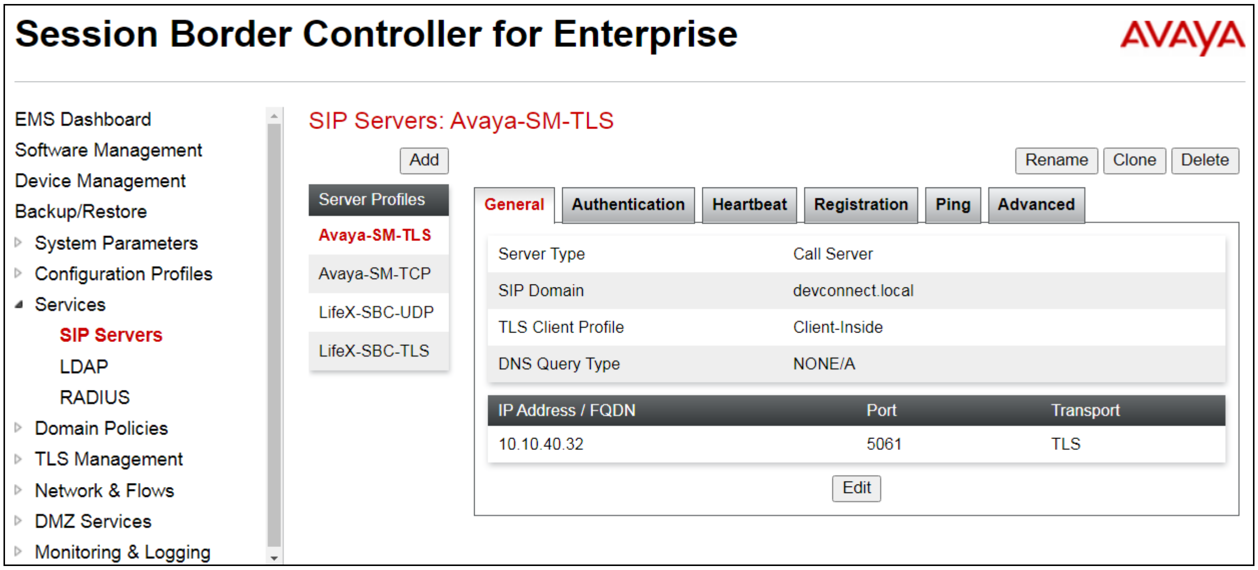


Again, the **Advanced** tab shows a similar setting to that of the Enterprise.



7.8. Server Configuration

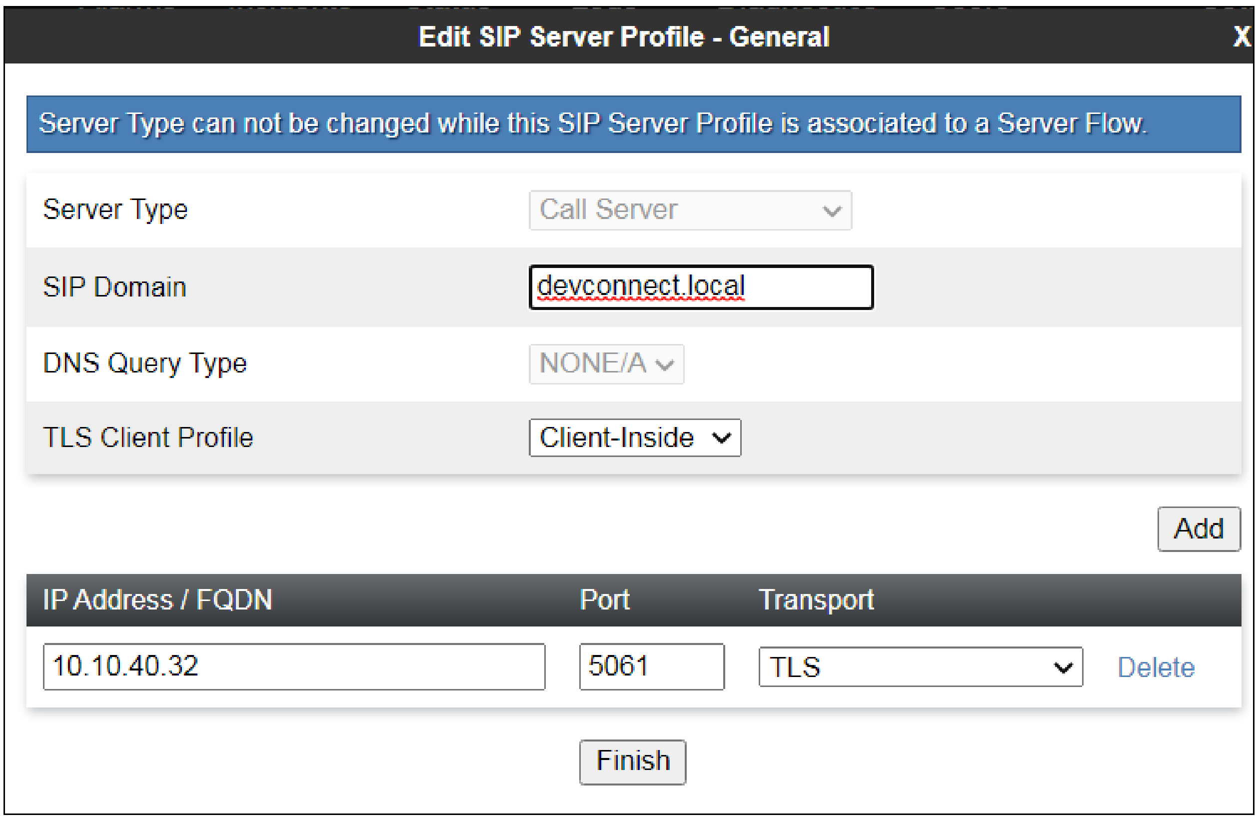
Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and LifeX (Trunk Server). Below shows some Server Profiles that were used during compliance testing, to add a new Server Profile, from the Services menu on the left-hand navigation pane, select **SIP Servers** and click the **Add**.



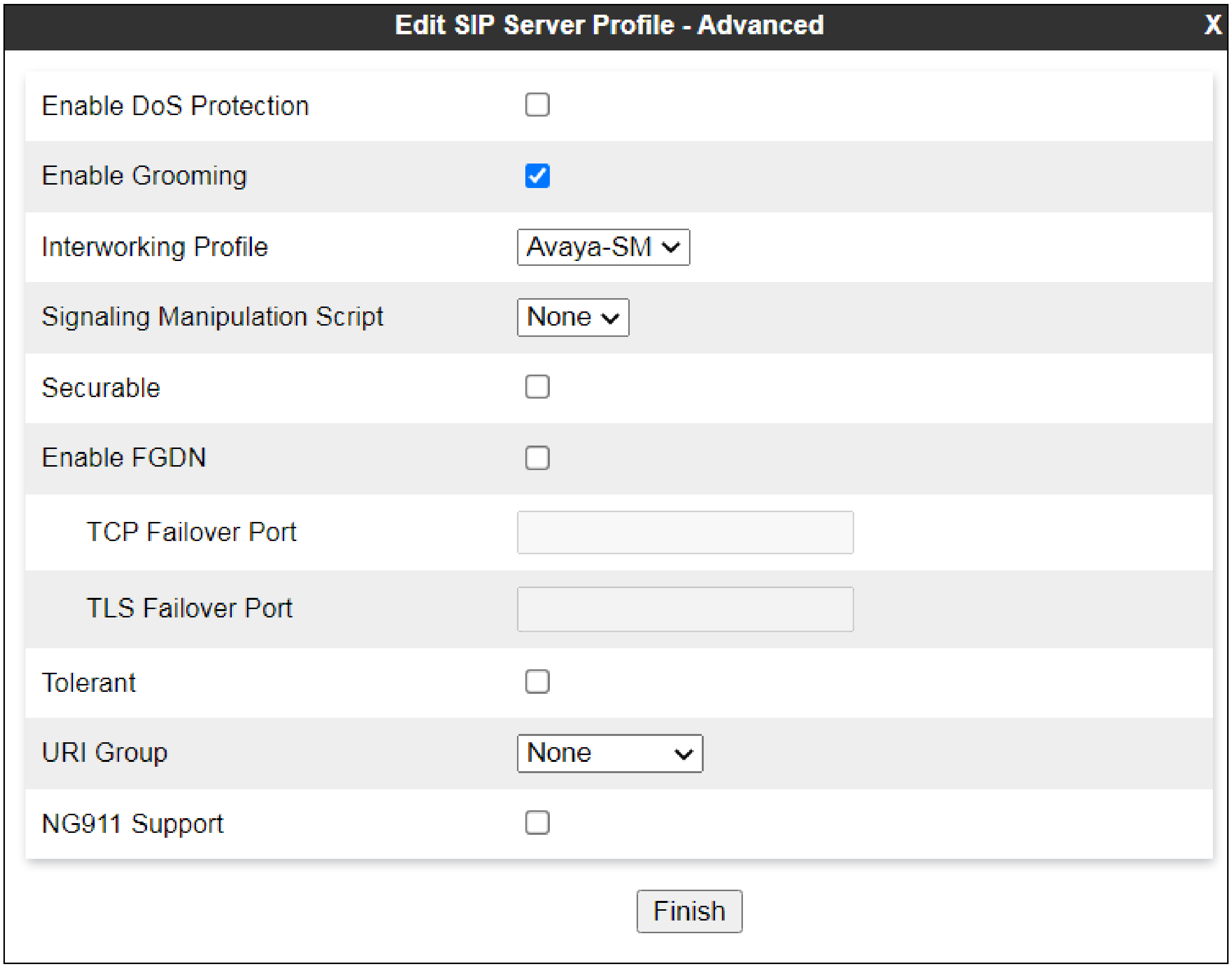
7.8.1. Server Configuration Profile – Enterprise

The following shows the Profile used to connect to Session Manager on the Enterprise side.

- On the **Edit SIP Server Profile – General** tab select **Call Server** from the drop-down menu under the **Server Type**.
- On the **IP Addresses / FQDN** field**,** enter the IP address of the Session Manager Security Module (**Section 5.5)**.
- Enter **5061** under **Port** and select **TLS** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 6.2**.
- Select a **TLS Client Profile** defined in **Section 7.3.3**.



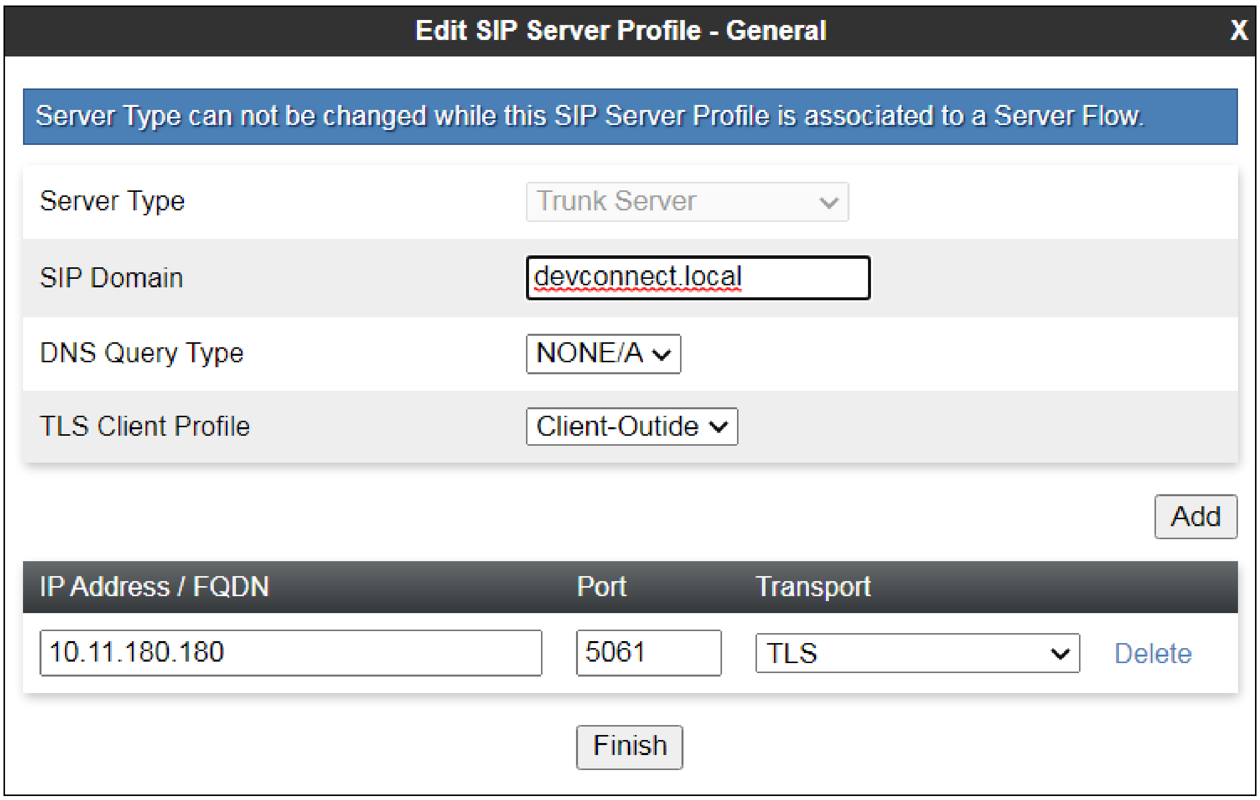
- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab:
  - Check **Enable Grooming**.
  - Select **Avaya-SM** from the **Interworking Profile** drop-down menu (**Section 7.7.1**).
- Click **Finish**.



7.8.2. Server Configuration Profile – Service Provider

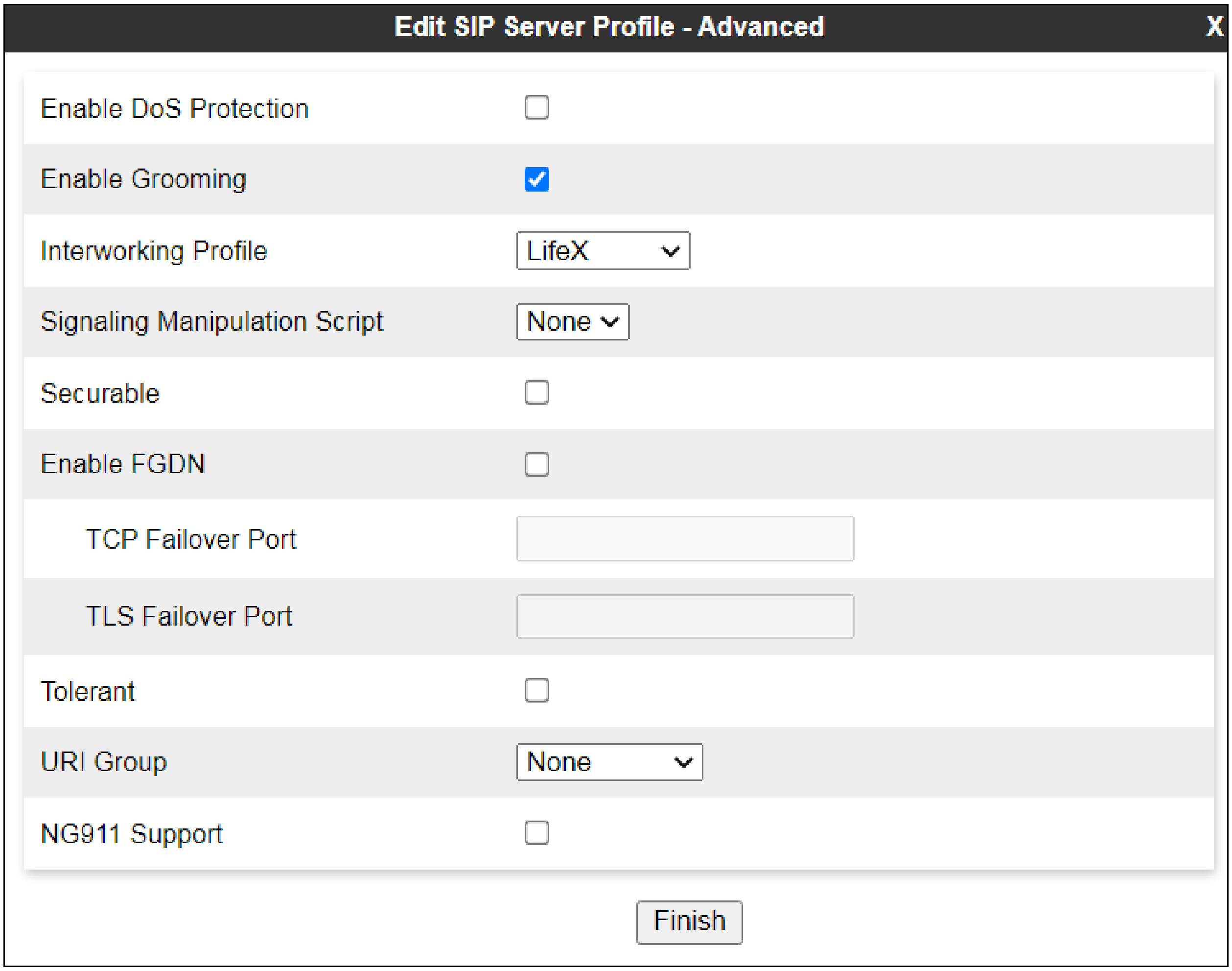
Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- On the **Edit Server Configuration Profile - General** Tab select **Trunk Server** from the drop-down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the LAN interface of the LifeX device to connect to (**10.11.180.180*)***.
- Select **TLS** for **Transport** and enter **5061** under **Port**.
- Click **Next** until the **Advanced** tab is reached (not shown).



On the **Add SIP Server Profile - Advanced** window:

- **Enable Grooming** (should be checked).
- Select **LifeX** from the **Interworking Profile** drop-down menu (**Section 7.7.2**).
- Click **Finish**.

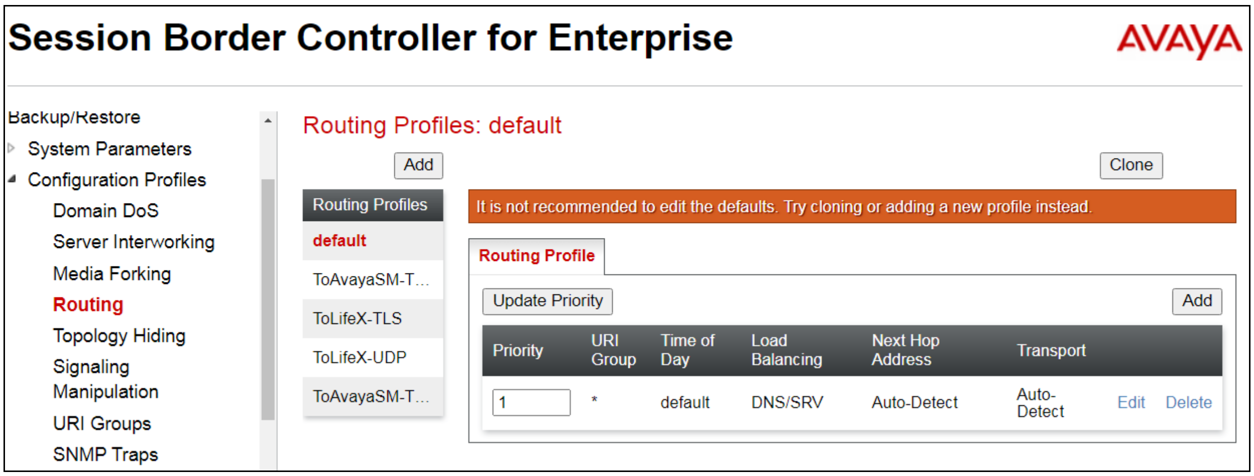


7.9. Routing

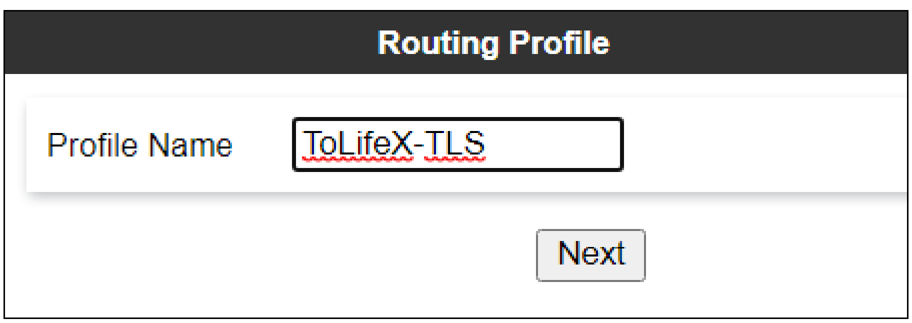
Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the LifeX SIP trunk.

7.9.1. Routing Profile – LifeX

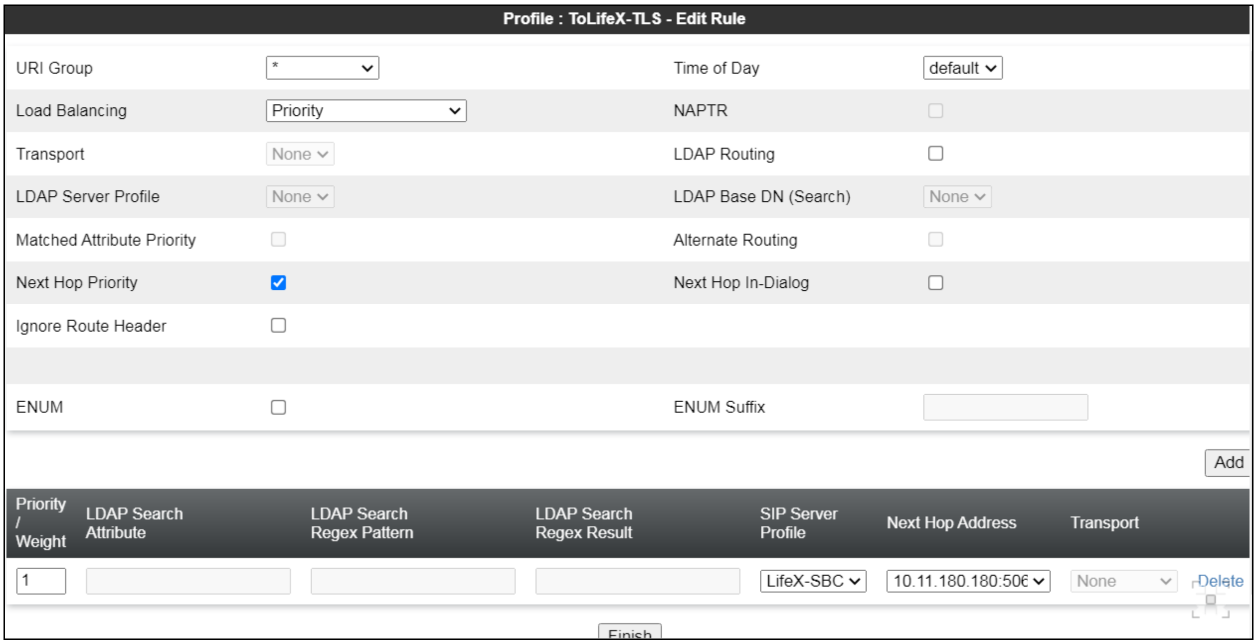
To create the outbound route, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add**.



Enter an appropriate **Profile Name** similar to the example below and click **Next**.

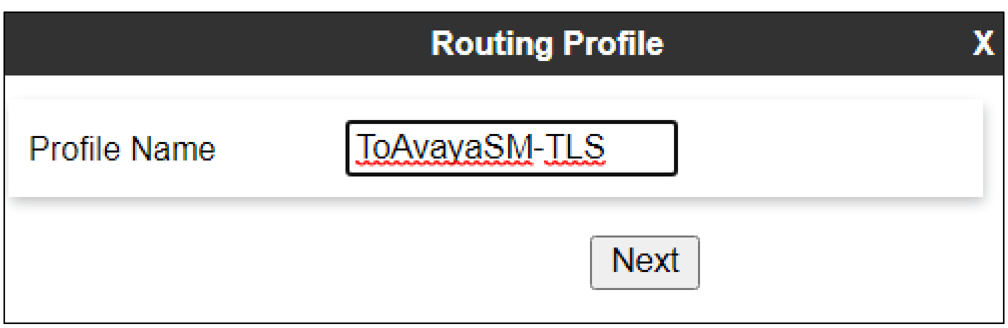


- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **SIP Server Profile**, select the SIP Server Profile for LifeX. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the LifeX Server Configuration Profile in **Section 7.8.2**.
- Defaults were used for all other parameters.
- Click **Finish**.

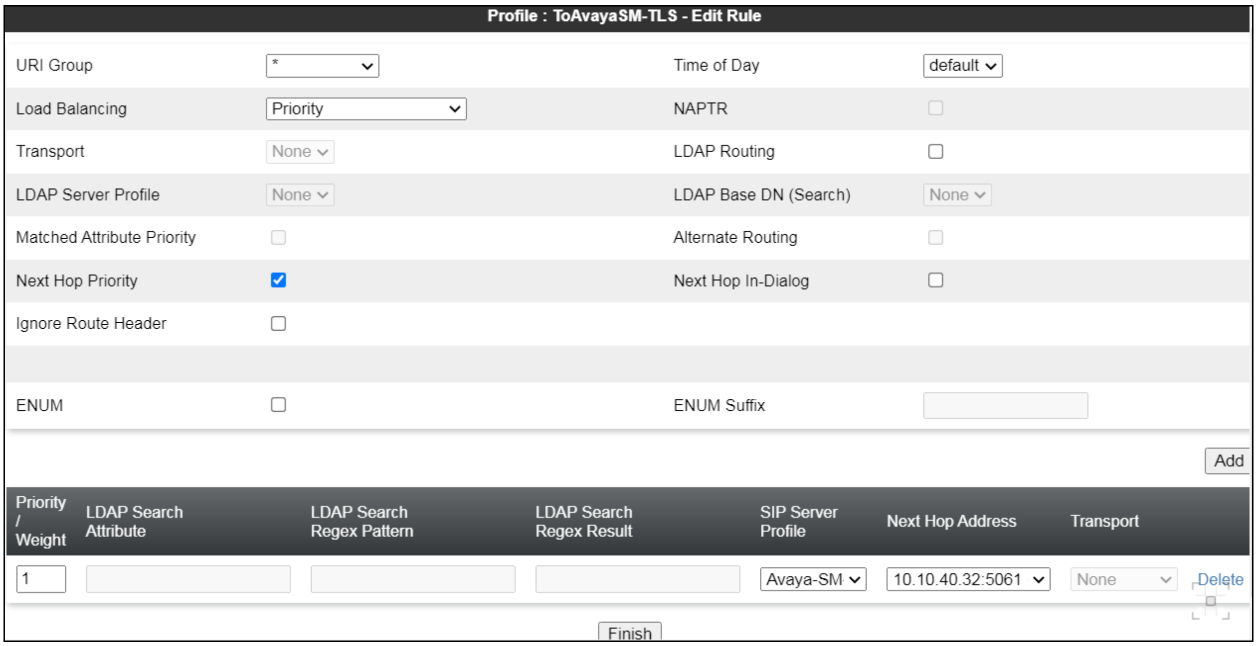


7.9.2. Routing Profile – Session Manager

Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the inbound route. Enter an appropriate **Profile Name** similar to the example below and click **Next**.



- Click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **SIP Server Profile**, select the Session Manager profile. The **Next Hop Address** is populated automatically with the IP address of Session Manager along with the port number defined in **Section 7.8.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



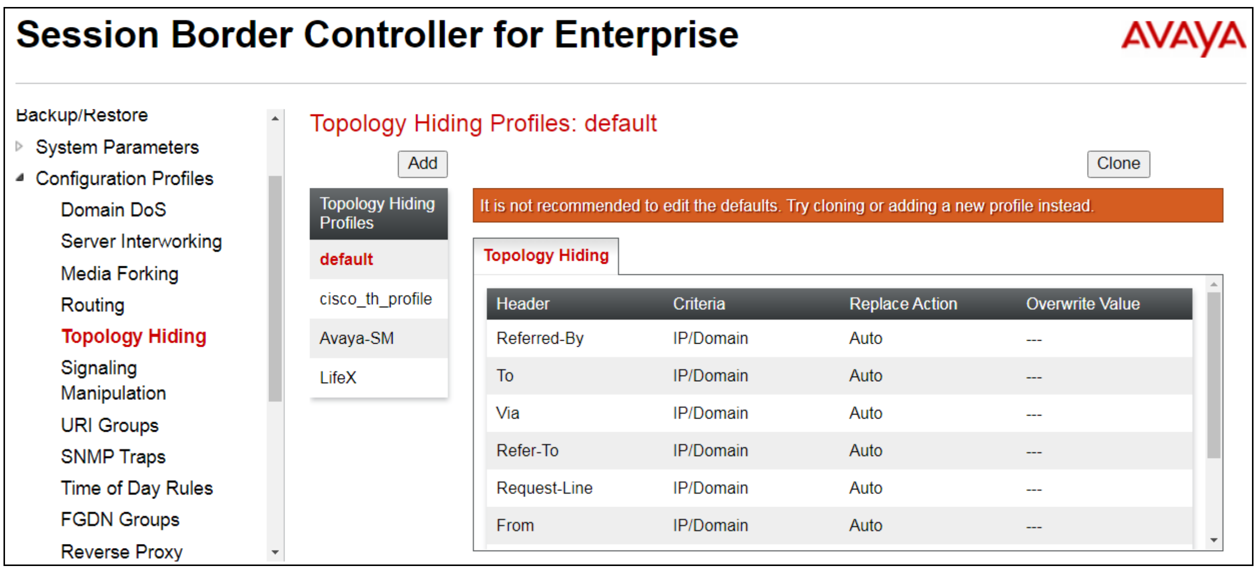
7.10. Topology Hiding

Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

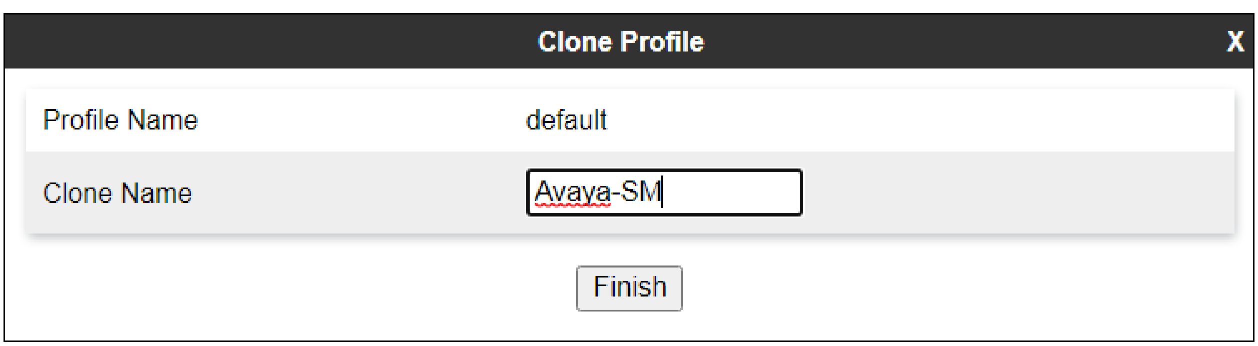
Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

7.10.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side, select ***default*** from the list of pre-defined profiles and click the **Clone** button.

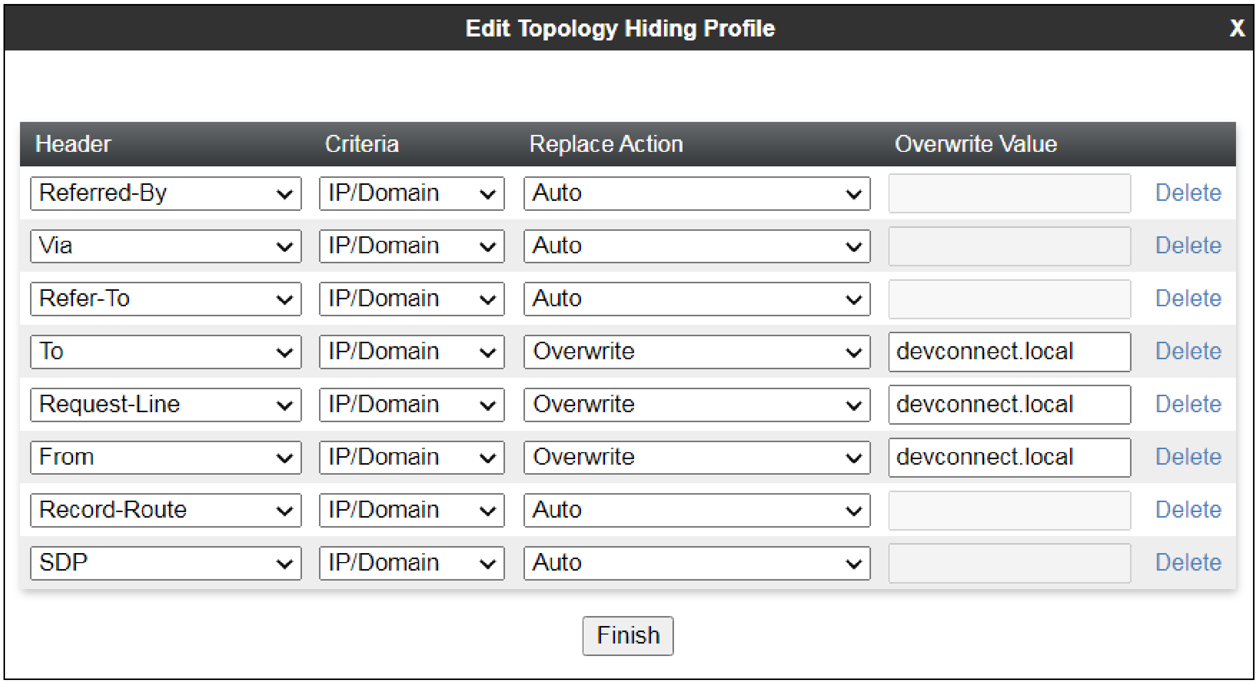


Enter a **Clone Name** such as the one shown below and click **Finish**.



On the newly cloned Avaya-SM profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **devconnect.local**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.1.1**.
- Default values were used for all other fields.
- Click **Finish**.



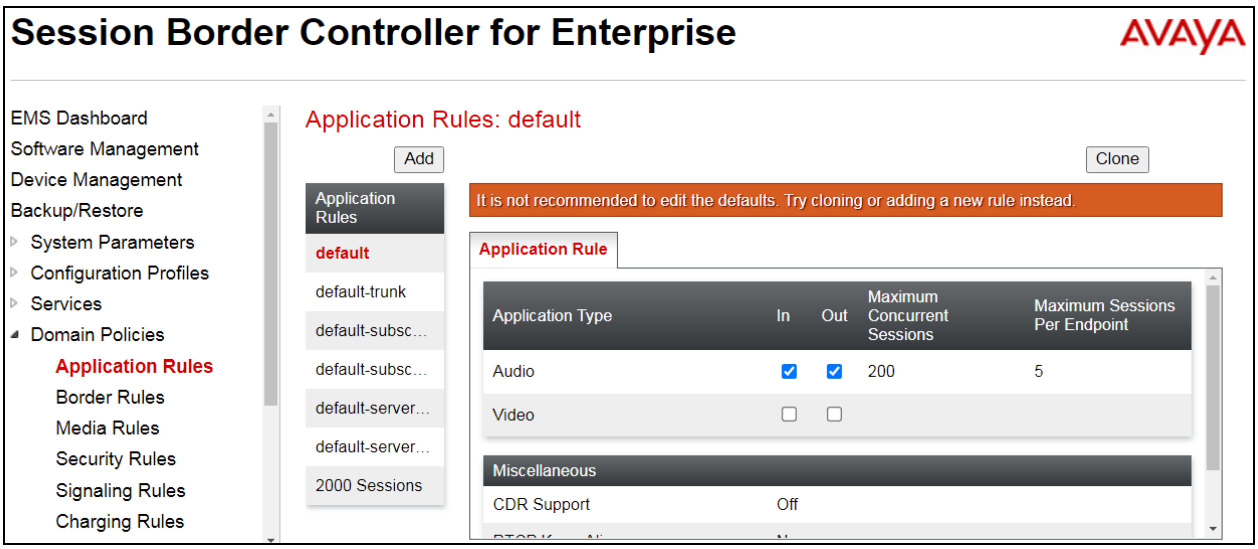
There was no requirement to any other Topology Hiding Profile.

7.11. Domain Policies

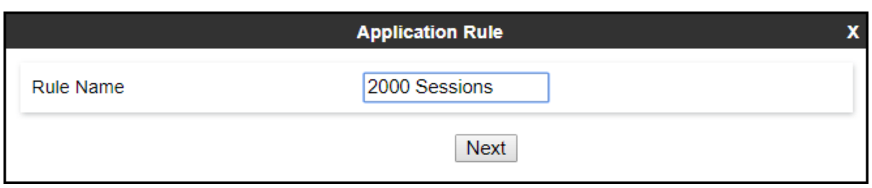
Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

7.11.1. Application Rules

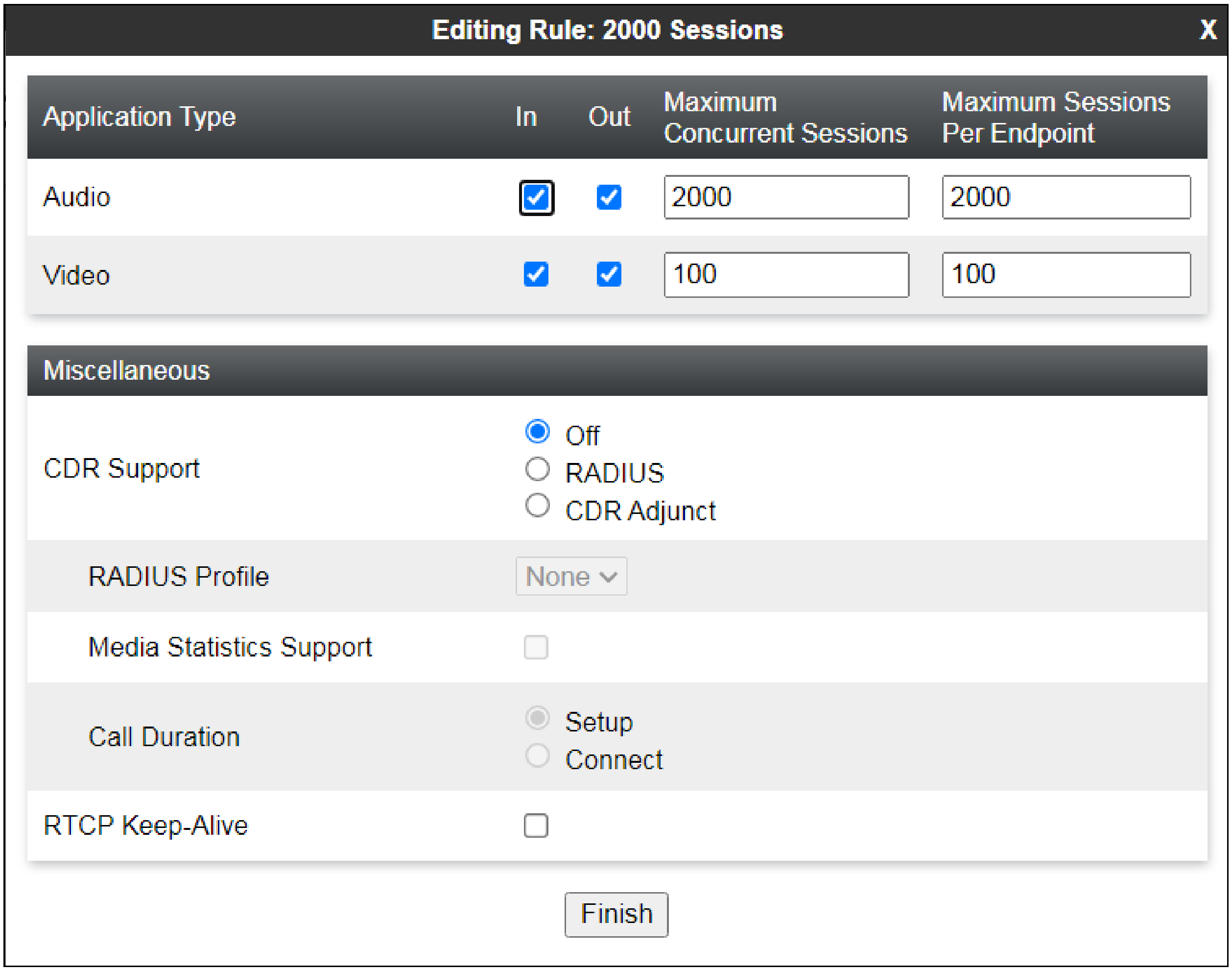
Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies → Application Rules**, click on the **Add** button to add a new rule.



Under **Rule Name** enter the name of the profile, e.g., **2000 Sessions** and click **Next**.



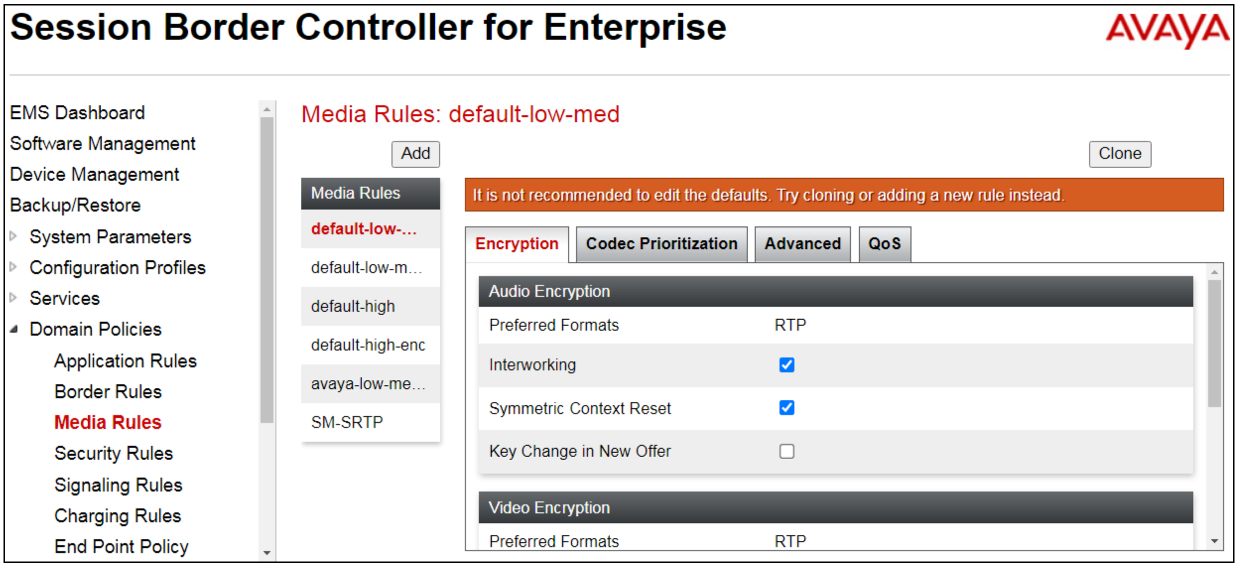
- Under **Audio** check ***In*** and ***Out*** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **2000** for Audio. Repeat for video if needed, the value of **100** for Video was used for the test.
- Click **Finish**.



7.11.2. Media Rules

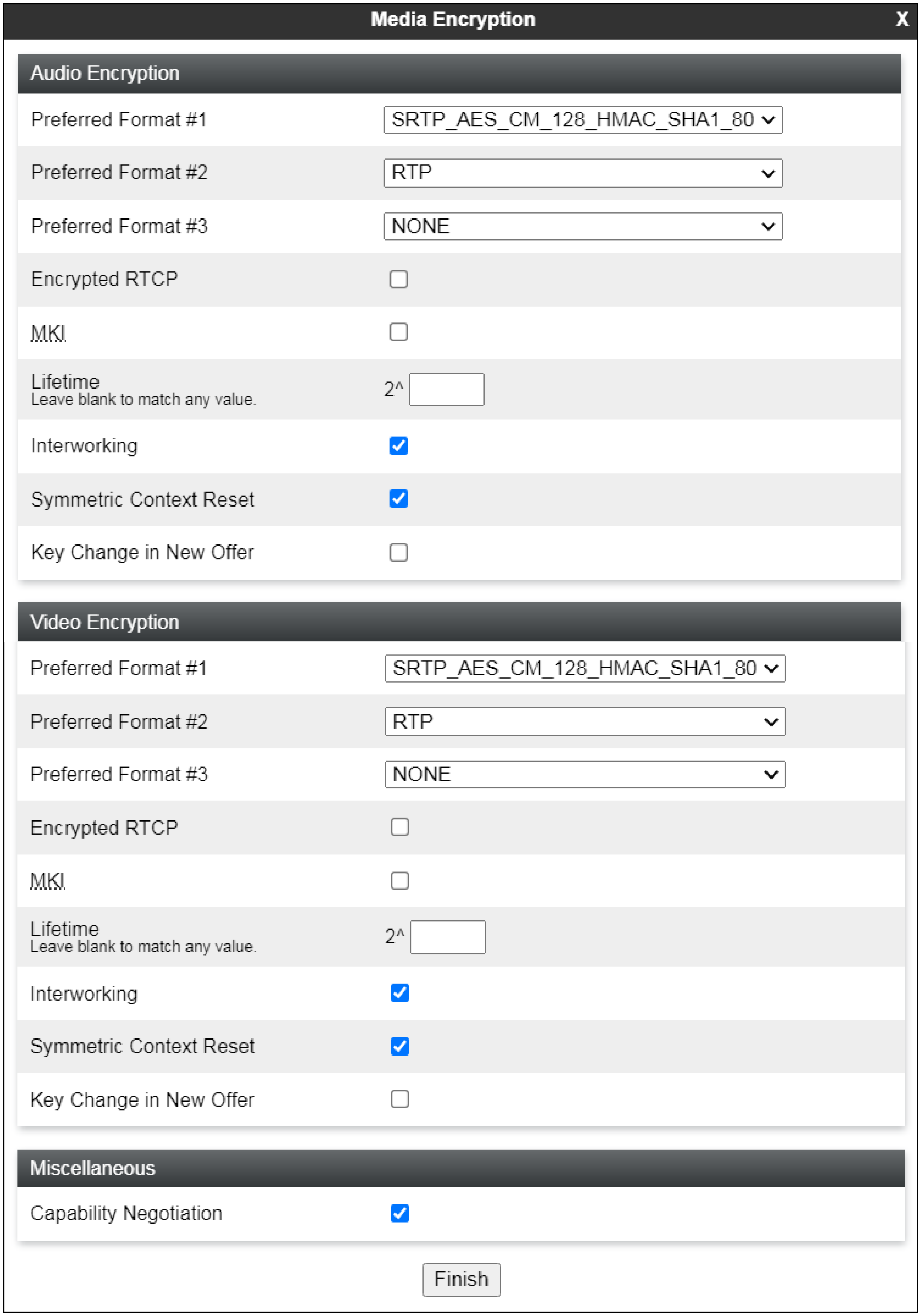
Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, one media rule (shown below) was created toward Session Manager and a default media rule was used toward LifeX.

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**. Click on the **Add** button to add a new media rule.

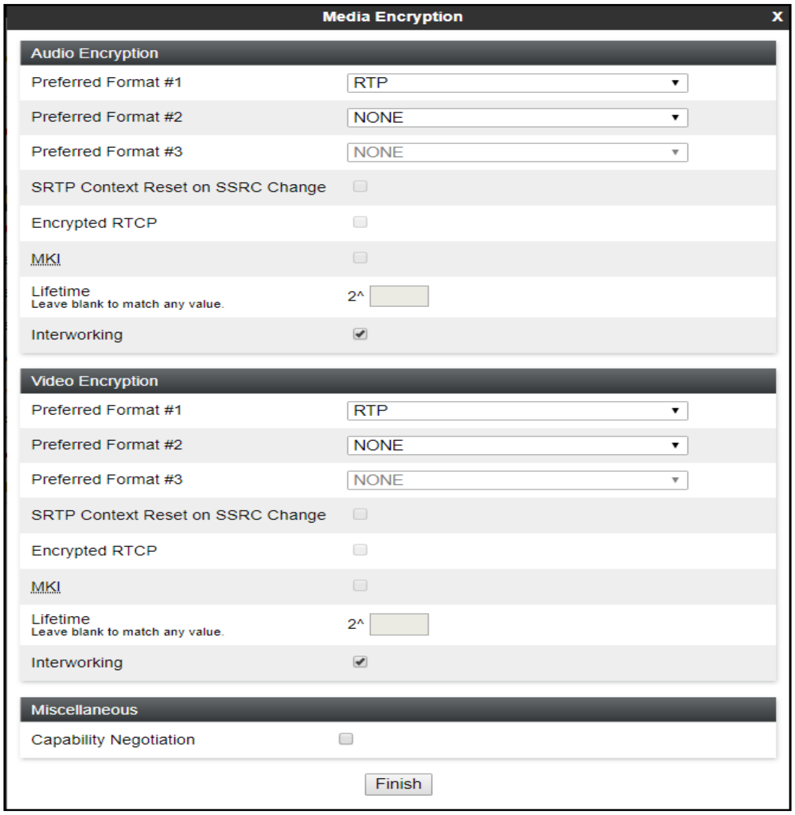


- Under **Rule Name** enter **SM_SRTP**.
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption, if needed.
- Under Miscellaneous verify that **Capability Negotiation** is checked.
- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish**.

(See next page)

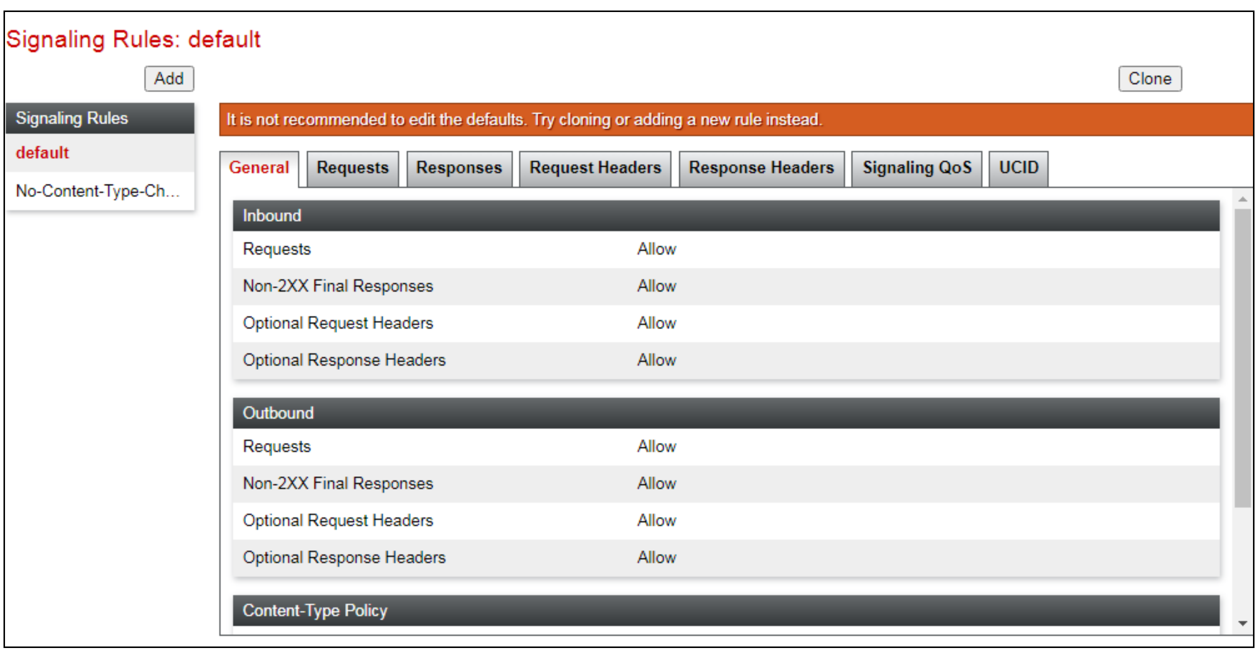

Media Encryption
X
Audio Encryption
Preferred Format #1
SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2
RTP
Preferred Format #3
NONE
Encrypted RTCP
MKI
Lifetime
Leave blank to match any value.
2^
Interworking
Symmetric Context Reset
Key Change in New Offer
Video Encryption
Preferred Format #1
SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2
RTP
Preferred Format #3
NONE
Encrypted RTCP
MKI
Lifetime
Leave blank to match any value.
2^
Interworking
Symmetric Context Reset
Key Change in New Offer
Miscellaneous
Capability Negotiation
Finish

For the compliance test, the **default-low-med** Media Rule was used in the LifeX direction.



7.11.3. Signaling Rules

For the compliance test, the **default** signaling rule was used.

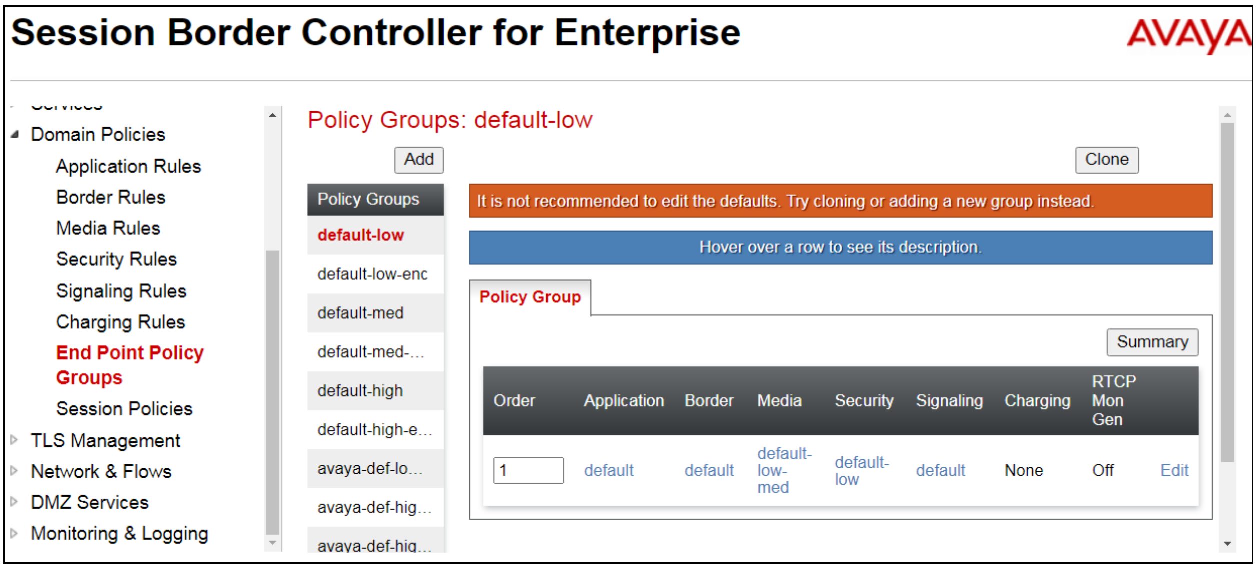


7.12. End Point Policy Groups

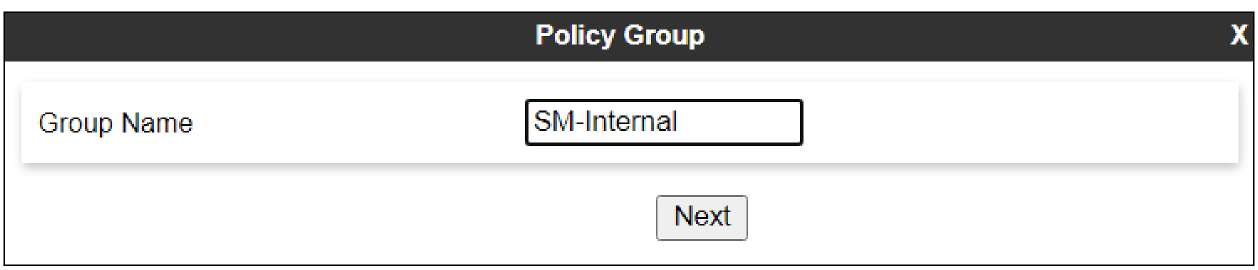
End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups.

7.12.1. End Point Policy Group – Enterprise

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add**.

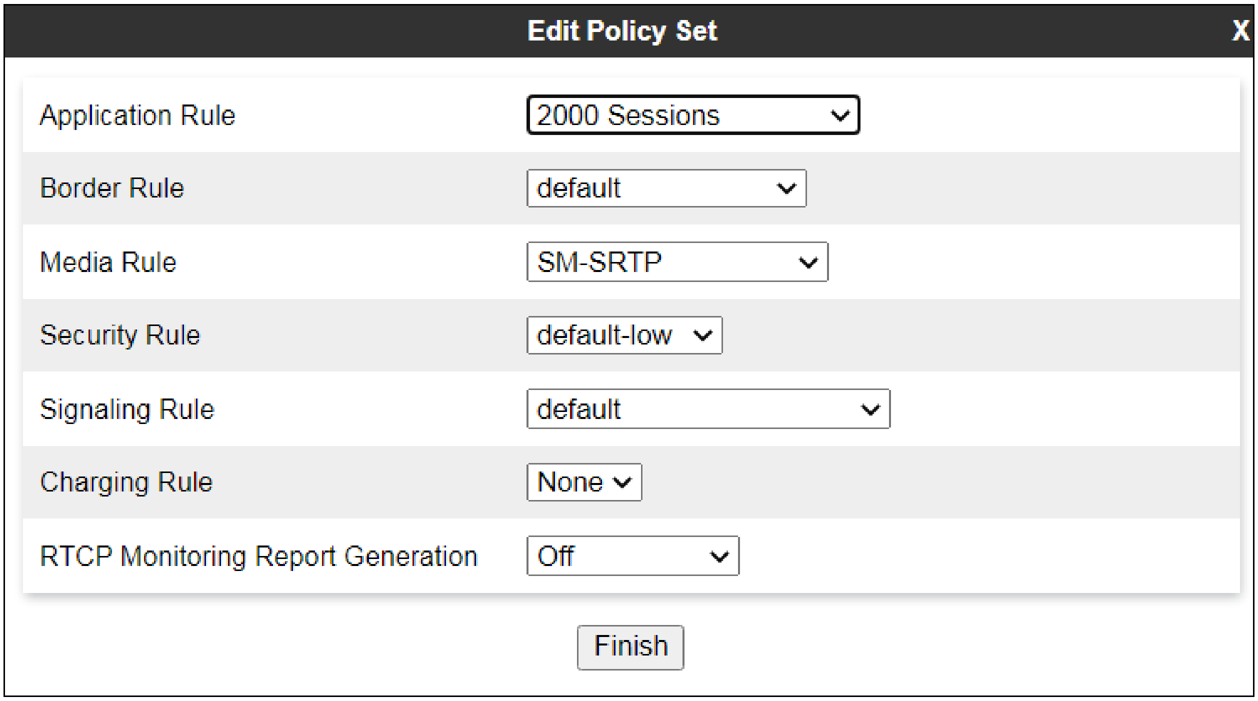


Enter an appropriate name in the **Group Name** field and click **Next**.



Under the **Policy Group** tab enter the following:

- **Application Rule: 2000 Sessions** (**Section 7.11.1**).
- **Border Rule: default**.
- **Media Rule: SM-SRTP** (**Section 7.11.2**).
- **Security Rule: default-low**.
- **Signaling Rule: default** (**Section 7.11.3**).
- Click **Finish**.

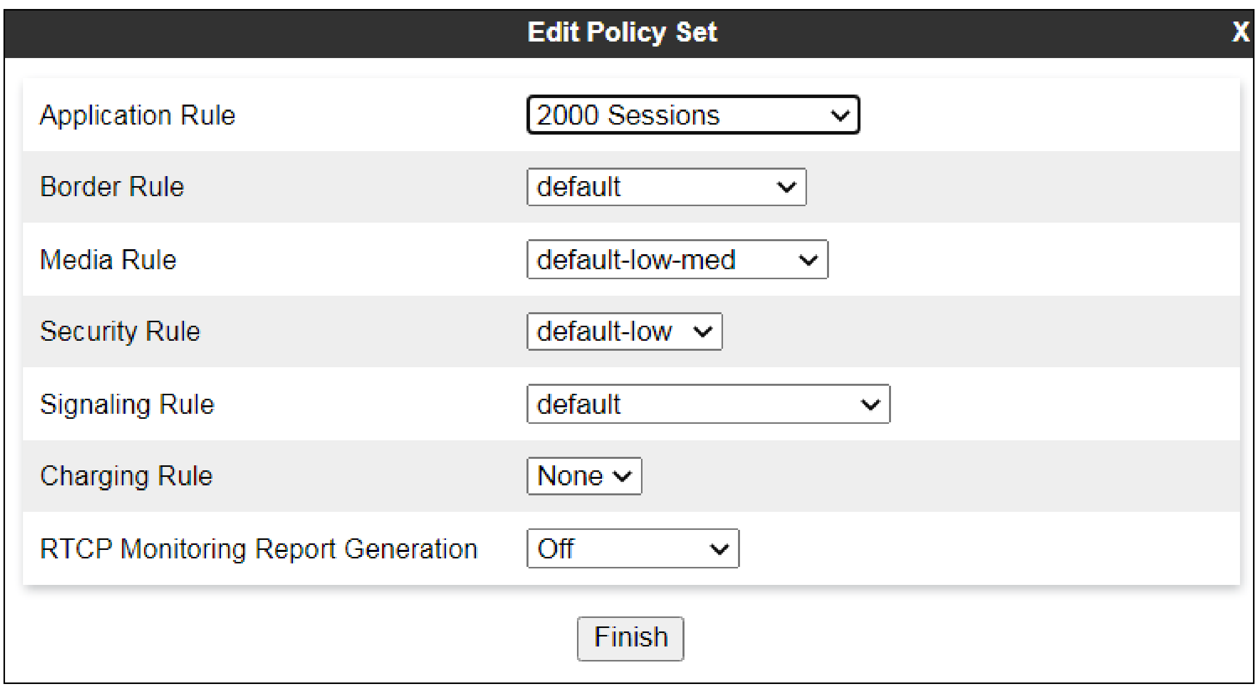


7.12.2. End Point Policy Group – Service Provider

To create an End Point Policy Group for the Service Provider, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add**. Enter an appropriate name in the **Group Name** field and click **Next**.

Under the **Policy Group** tab enter the following:

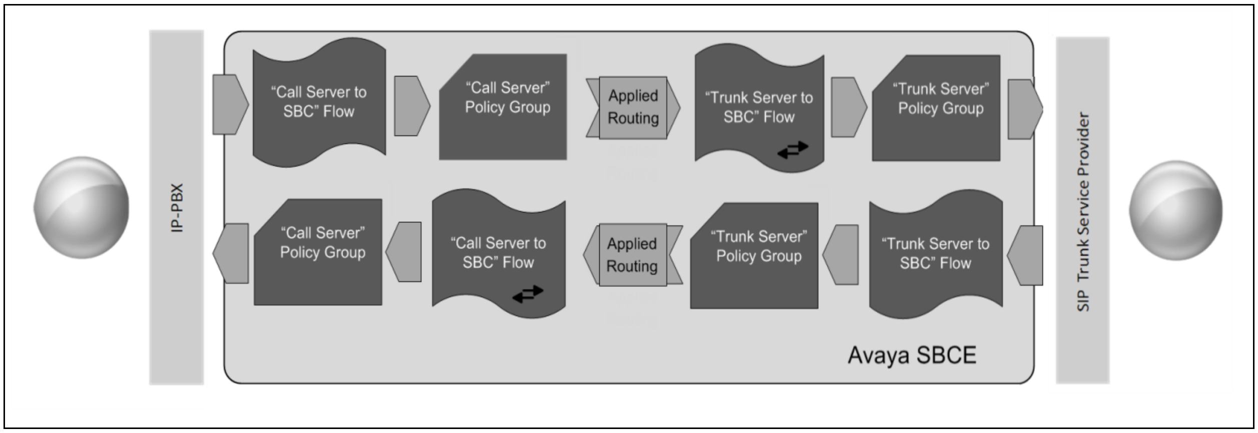
- **Application Rule: 2000 Sessions** (**Section 7.11.1**).
- **Border Rule: default**.
- **Media Rule: default-low-med** (**Section 7.11.2**).
- **Security Rule: default-low**.
- **Signaling Rule: default** (**Section 7.11.3**).
- Click **Finish**.



.

7.13. End Point Flows

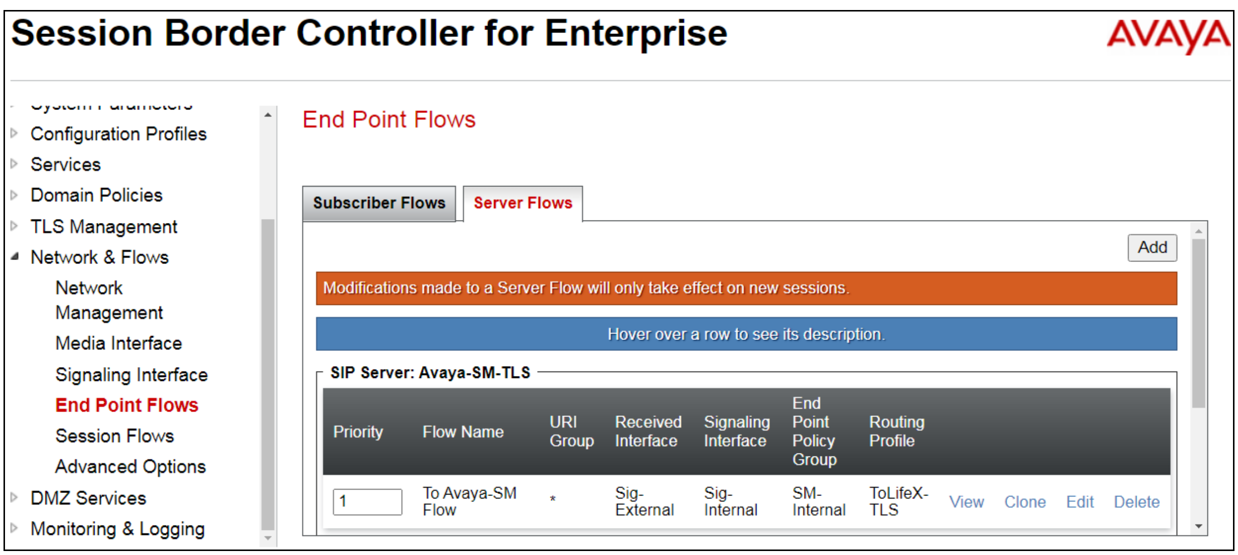
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP trunk call.



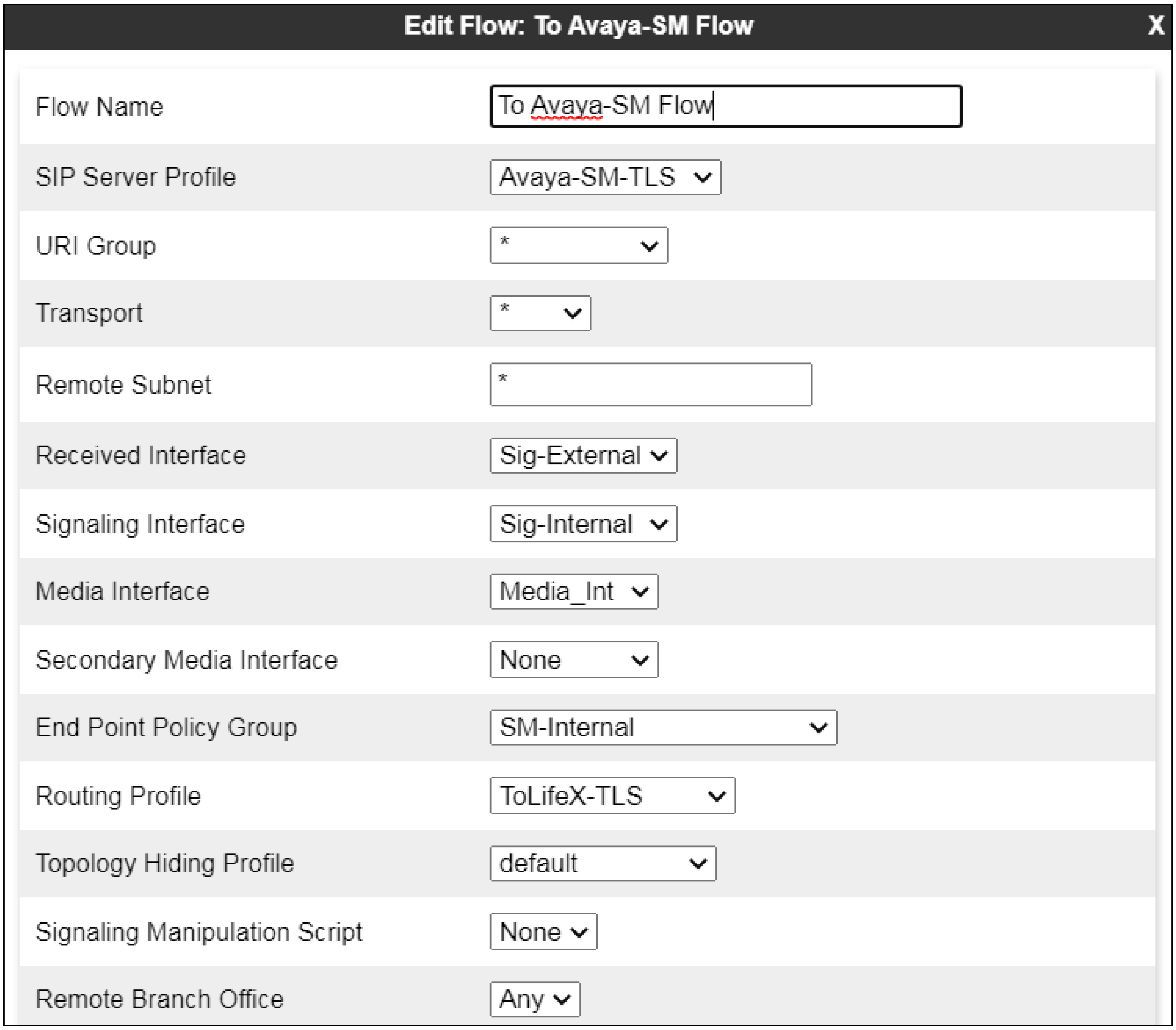
The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

7.13.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown).

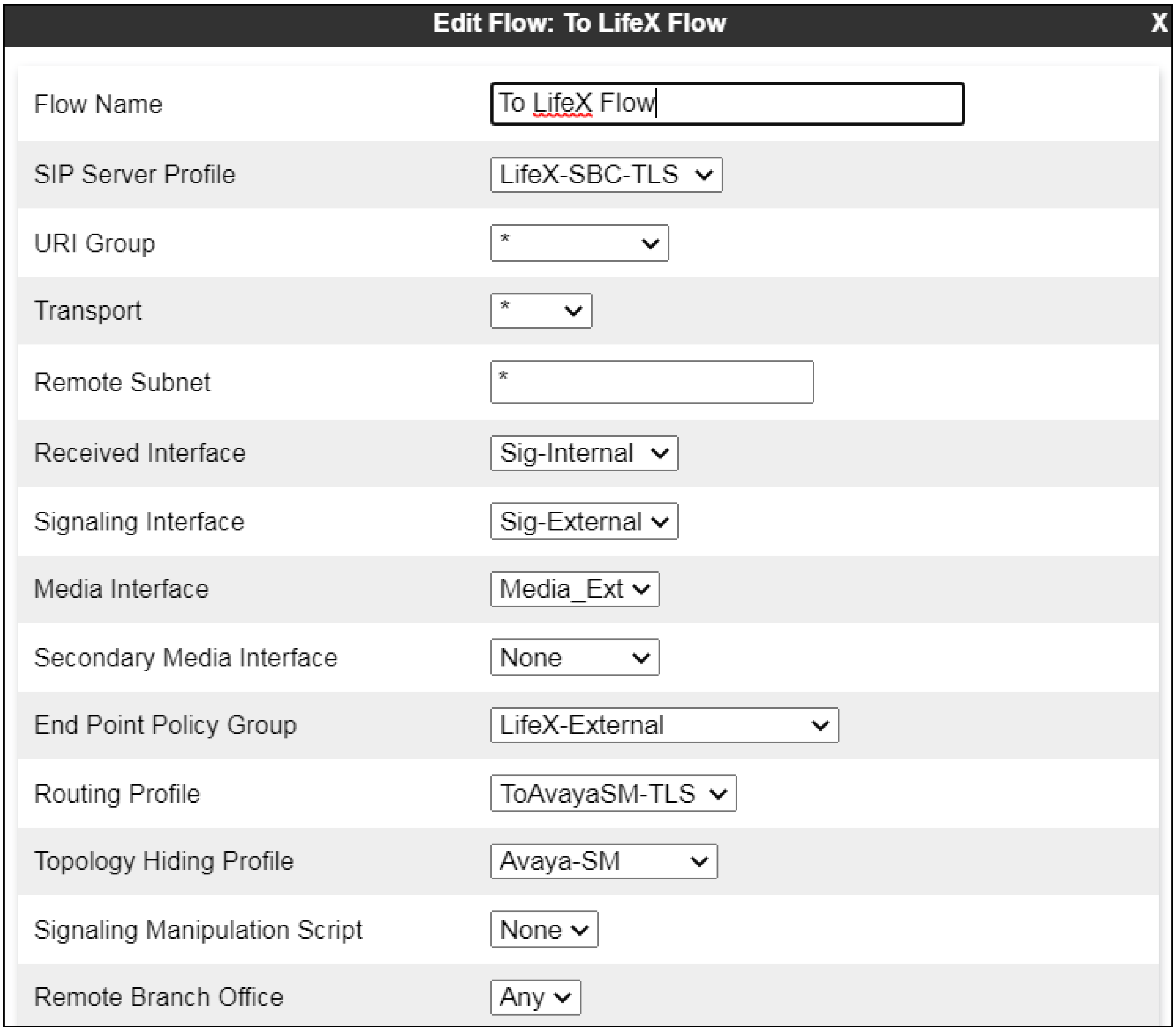


The screen below shows the flow named **To Avaya-SM Flow** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for LifeX in **Section7.9.1**, which is the reverse route of the flow. Click **Finish** (not shown).



7.13.2. End Point Flow – Service Provider

A second Server Flow with the name **To LifeX Flow** was similarly created in the LifeX direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 7.9.2**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Click **Finish** (not shown).



8. Configuration of Frequentis AG 3020 LifeX

This section describes the configuration of both the LifeX server and the Oracle Session Border Controller in order to connect to the Avaya Session Border Controller for Enterprise.

8.1. LifeX 3020

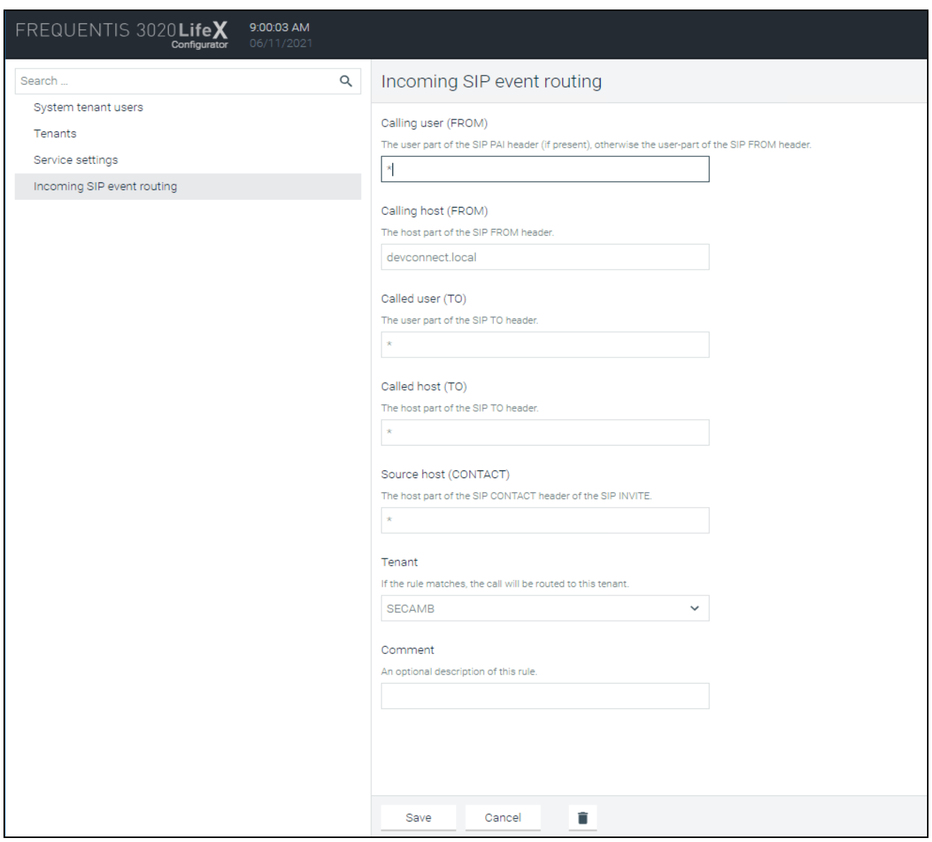
This section shows the steps necessary on the LifeX server to facilitate the connection to the Avaya Session Border Controller.

8.1.1. System Access

Access the LifeX Configurator by using a web browser and entering the URL https://<ip-address>/lifex-configurator/?tenant=<tenant name>, where <ip-address> is the IP address of web server belonging to each LX instance (DCA/DCB/RefSys…) and <tenant name> is shortcode of each tenant (SECAMB,NEAS…).

8.1.2. Incoming Calls Configuration

For incoming calls configuration, SYSTEM as <tenant name> was used. Navigate to section **Incoming SIP event routing** and click Create new incoming routing rule (not shown). Define to which Tenant, from all available tenants, incoming calls should be routed from specific Calling host, in this case devconnect.local.

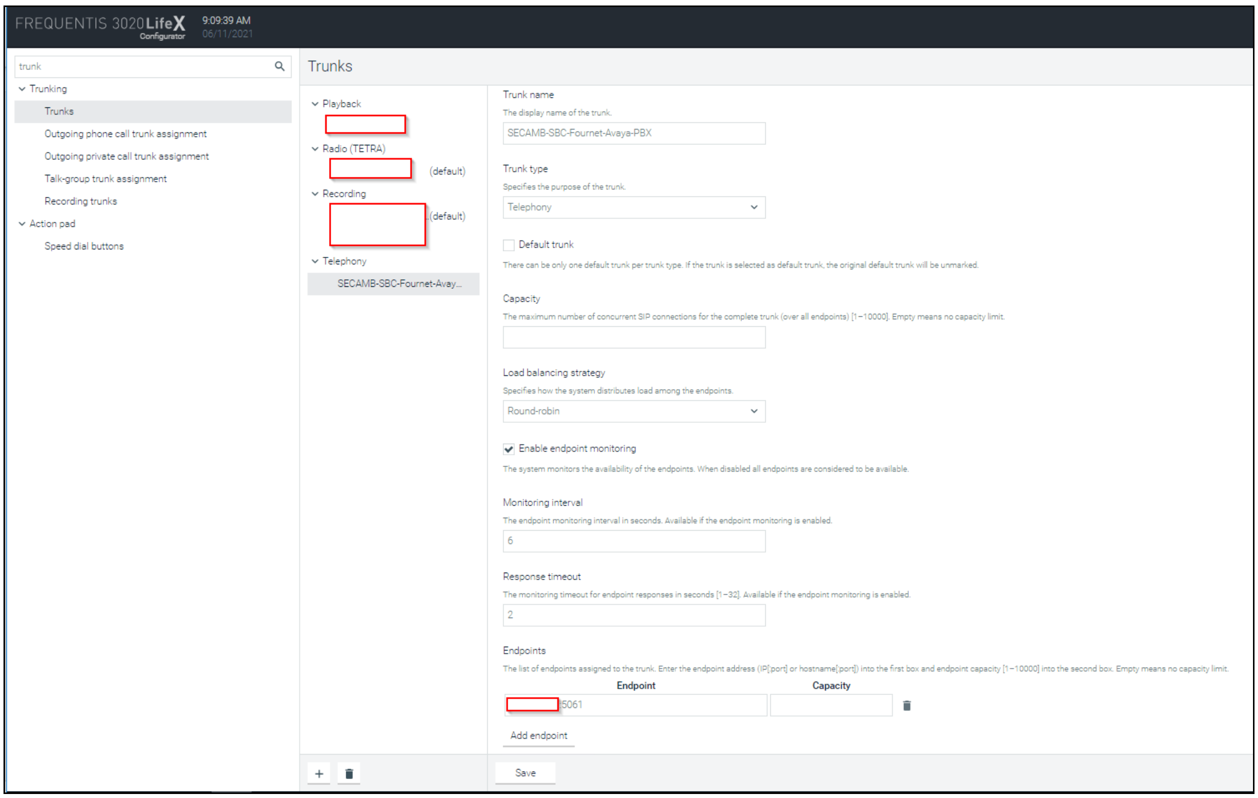


8.1.3. Outgoing Calls Configuration

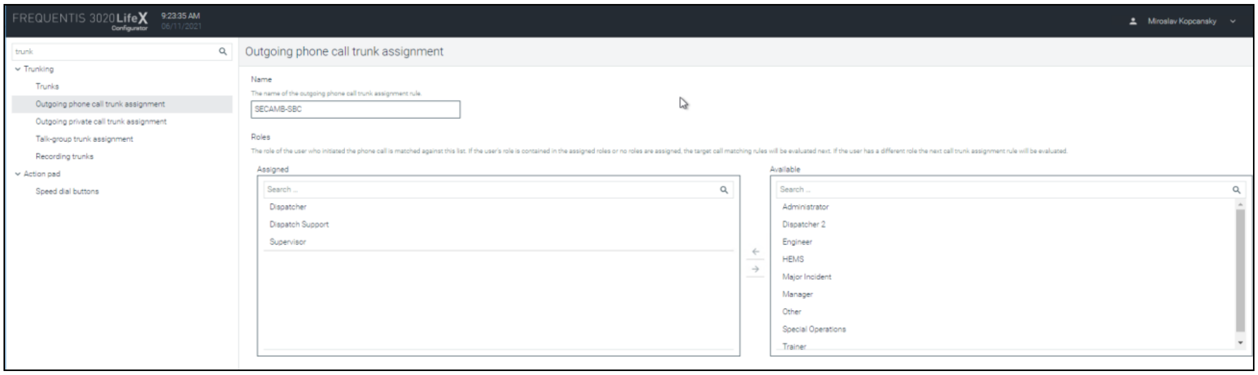
For outgoing calls configuration, specific site as <tenant name> was used, in this case SECAMB tenant was used.

First navigate to **Trunking →Trunks** in the left window and click create new trunk (there is a + on the button). Name the new trunk and select **Telephony** as **Trunk type**. **Enable endpoint monitoring** and set **Monitoring interval** and **Response timeout**. At the end configure endpoint in the format <ip-address>:5061, where <ip-address> is IP of SBC SIP interface INT_PHONE dedicated for media flow between LifeX and the Oracle SBC. Realm INT_PHONE is described in **Section 8.2**.

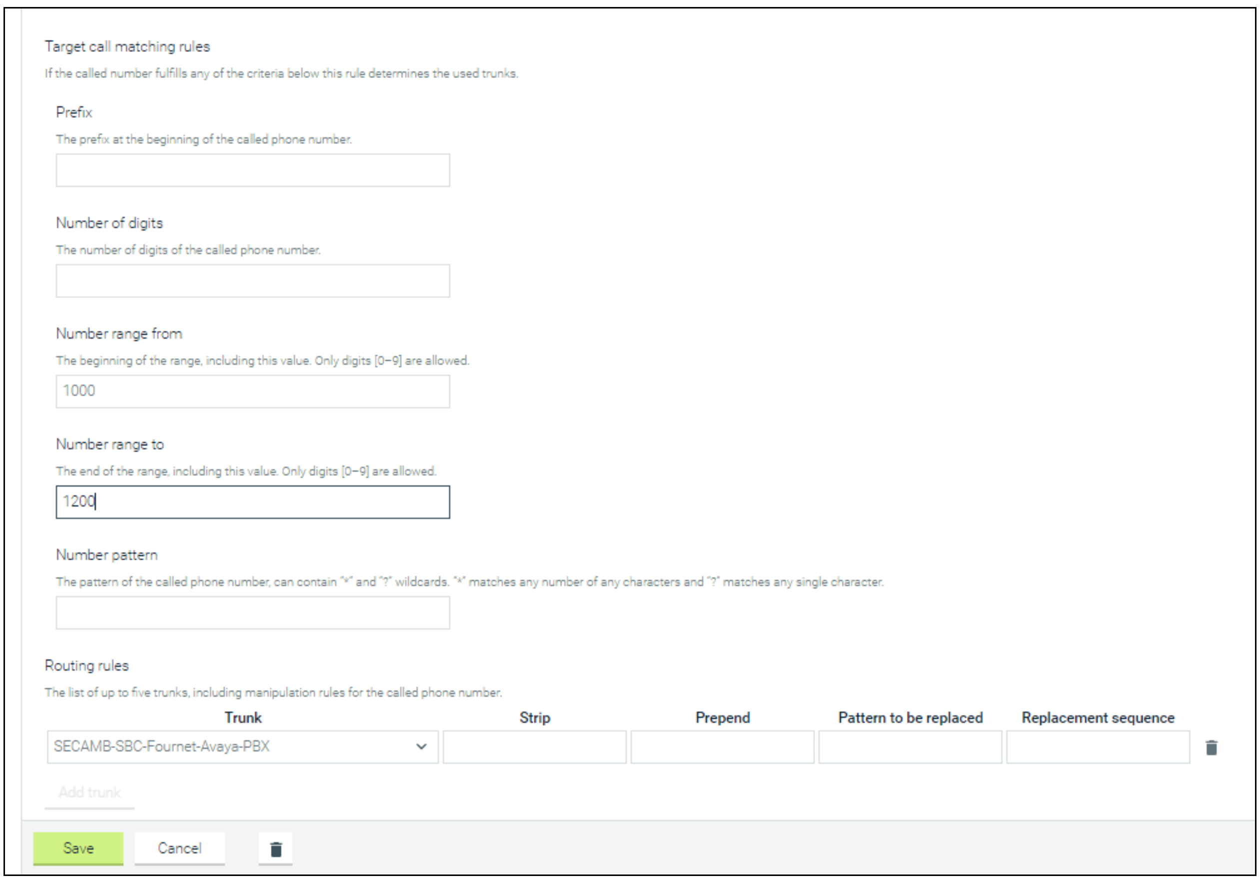
Note: Some sensitive information has been blocked out from some of the screen shots.



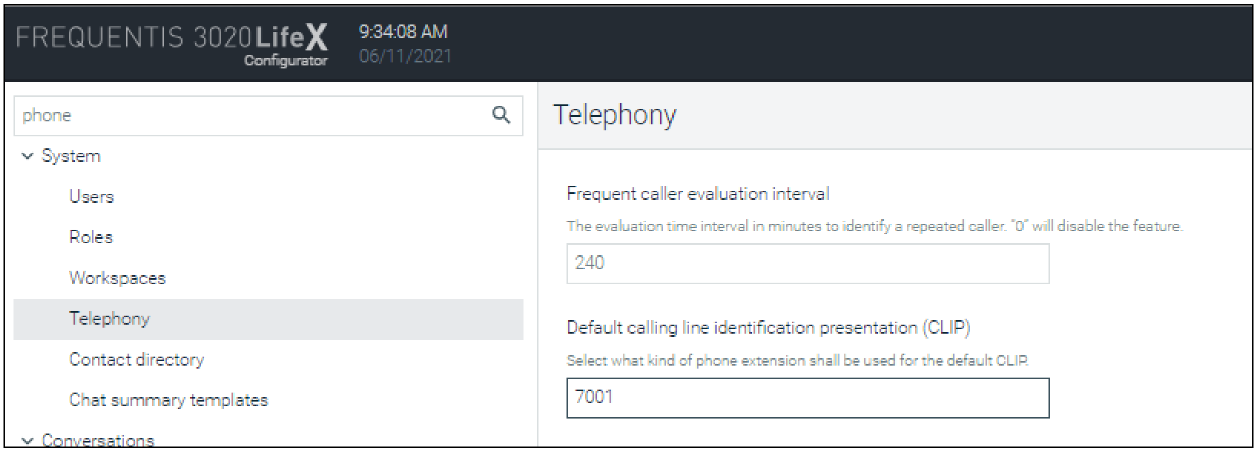
After trunk is created navigate to **Outgoing phone call trunk assignment** and click create new rule. **Name** the new rule and select to which LifeX Roles shoud be **Assigned**.



Scroll down to the bottom and select the telephony trunk that was created in the previous step from the **Trunk** drop down. A range of allowed phone numbers for outgoing phone calls is also defined. To have the possiblity of calling any number, leave **Number range from** and **Number range to** empty.



Default CLIP configuration is under the **System → Telephony** in the left window. Typically this would be the "main number" associated with the system.



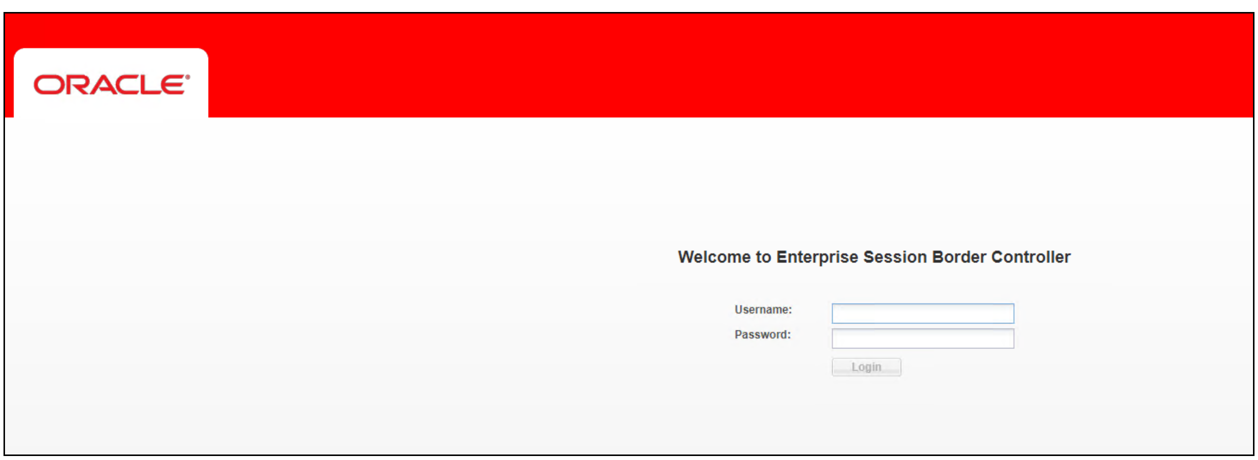
8.2. Oracle SBC-E

Frequentis use an SBC-E from Oracle as a SIP trunk between LifeX system and 3rd party sites. The reason is that Frequentis systems are more and more connected to customer equipment via IP (SIP trunks) instead of traditional legacy lines.

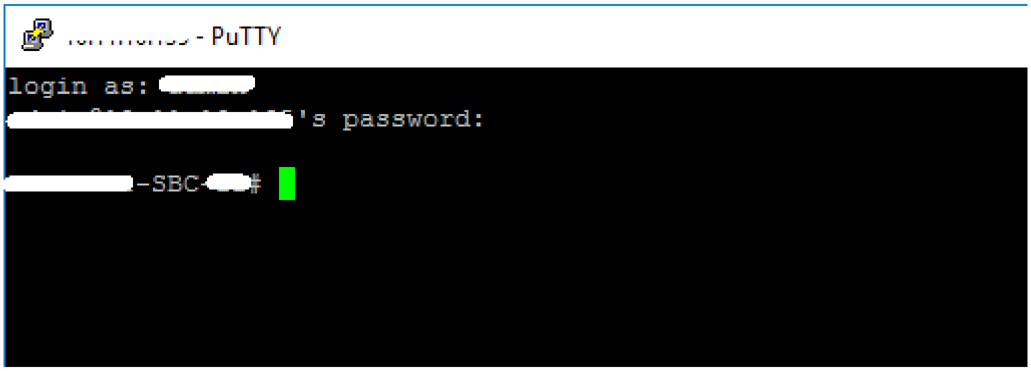
A **session border controller** (SBC) is a device regularly deployed in Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications.

8.2.1. System Access

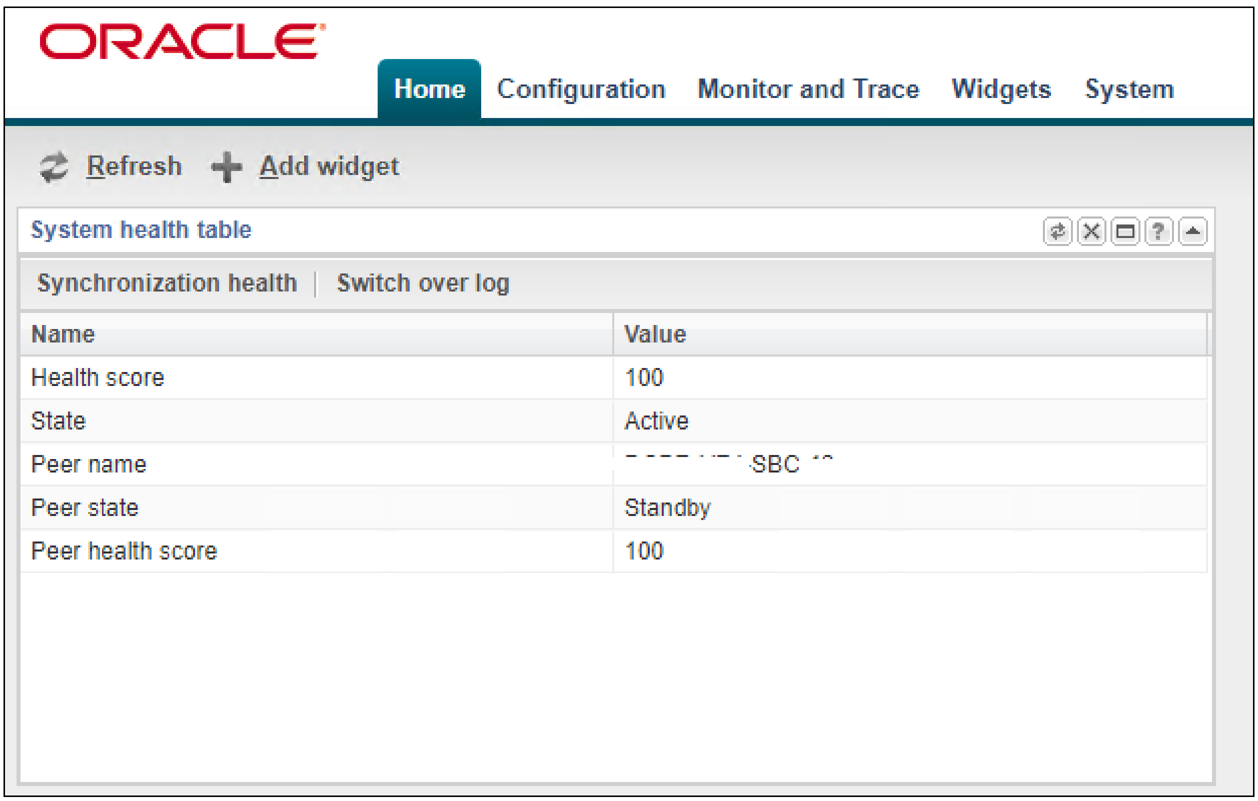
Access the Session Border Controller web management interface by using a web browser and entering the URL https://<ip-address>, where <ip-address> is the management IP address configured at installation. Also, the command line interface can be accessed using a ssh client i.e., "PuTTY". Log in using the appropriate credentials.



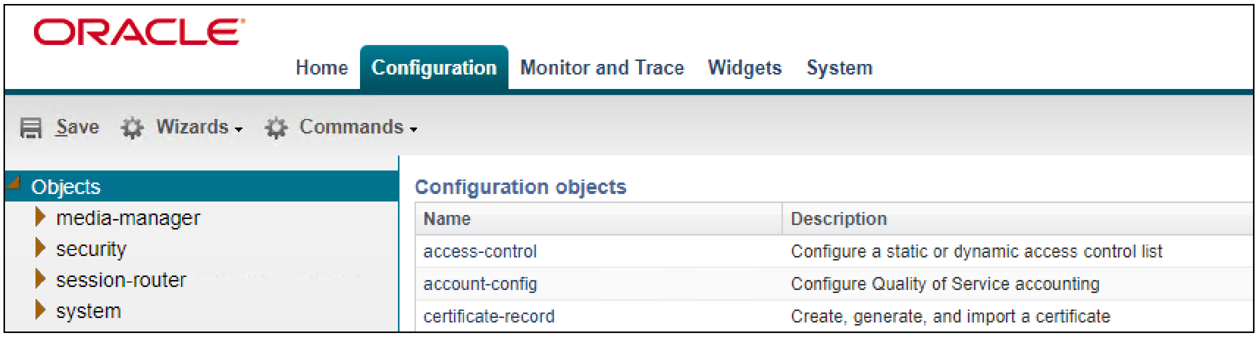
The screen shot below shows the interface using **PuTTY**.



Once logged in, on the top of the screen, 5 tabs shoud be visible. The **Home** tab is a dashboard where widgets can be added from **Wigets** tab.



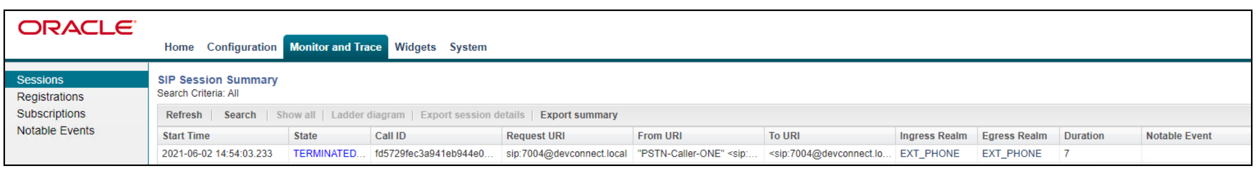
The **Configuration tab** provides a graphical display of the same objects and elements that can be accessed by CLI. Also, it provides some configuration Wizards and Commands.



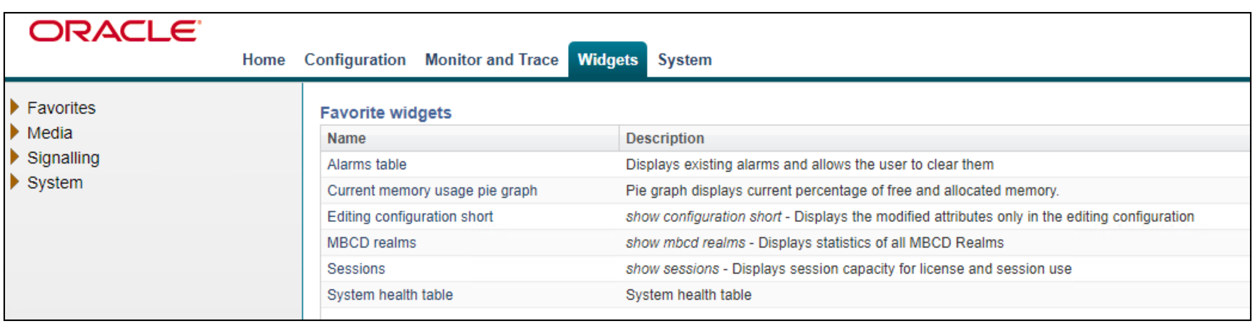
The **Monitor and Trace** tab displays the results of filtered SIP session data from the SBC. It supports the summary reports.

- **Sessions**
- **Registrations**
- **Subscriptions**
- **Notable Events**

Double-click on a line entry opens the Ladder Diagram window with session details, not shown here but described in the verification steps in **Section 9.4.2**.

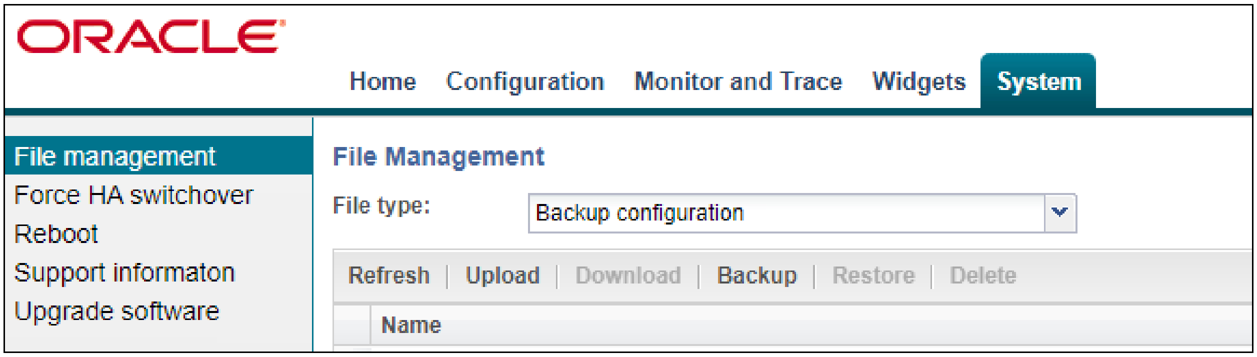


The **Widgets** tab contains a list of all available widgets that can be used to view system data and statistics. A **license** can be added here under **System → Licenses**.



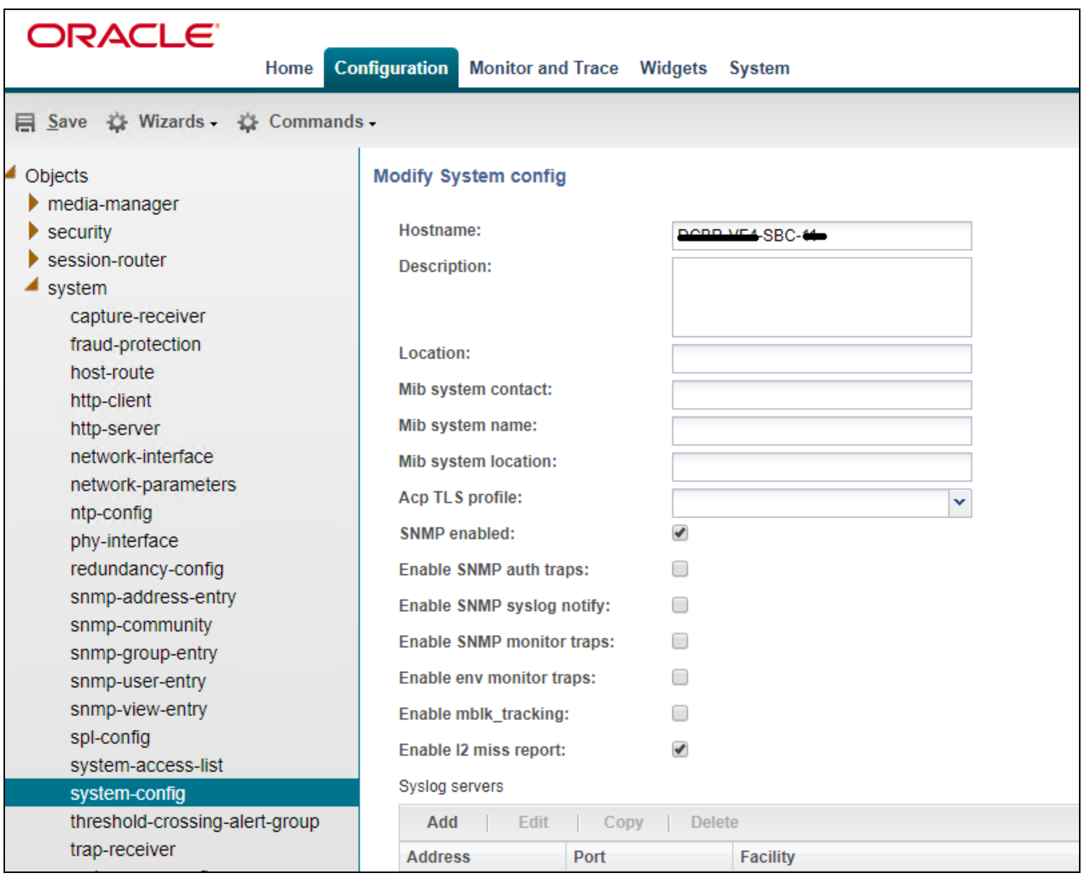
The System tab provides the following ways to manage files on the system.

- **File Management**
- **Force HA switchover**
- **Reboot**
- **Support Information**
- **Upgrade software**

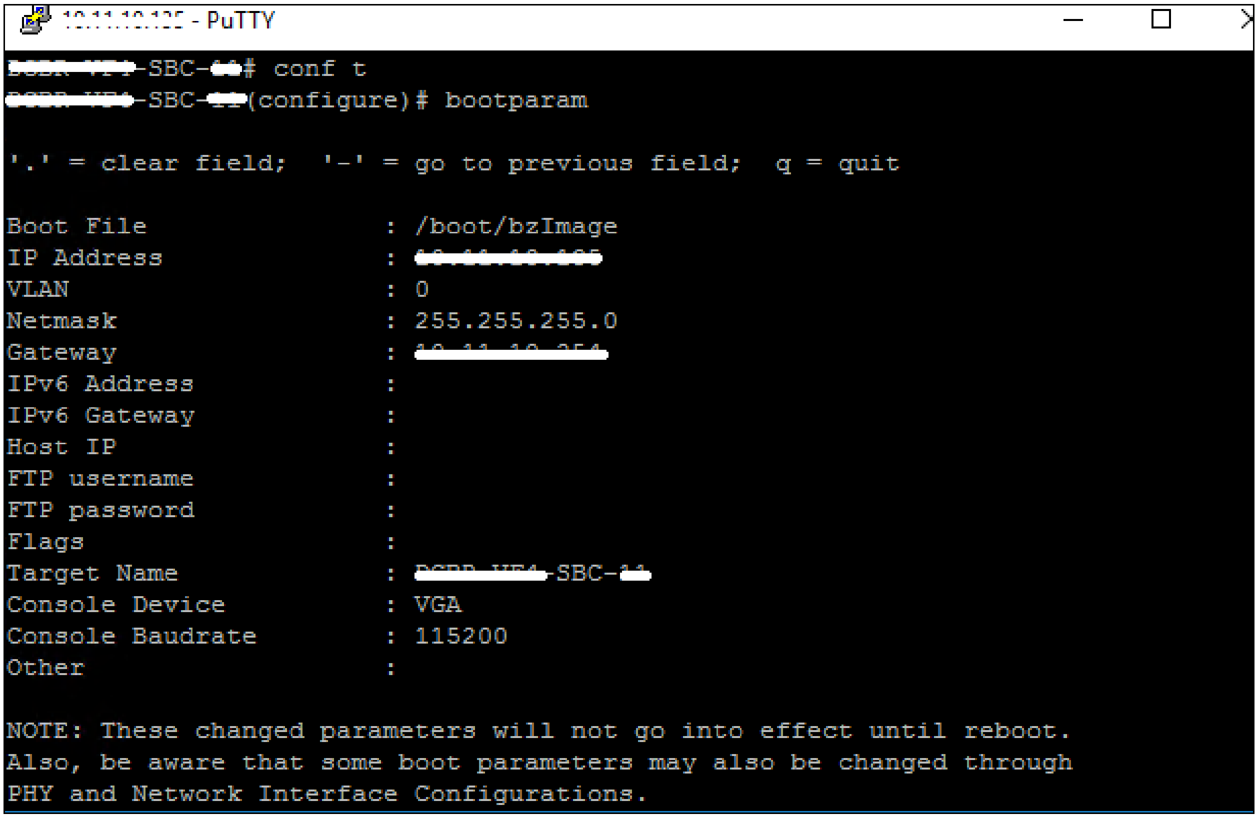


8.2.2. System configuration

The basic system configuration is configured under **Configuration→Objects→System**.



The management IP is set during the OVF deployment. This can be changed using the CLI command **bootparam**. It is interface **wancom0**.



```
[redacted] - PuTTY
[redacted]-SBC-[redacted]# conf t
[redacted]-SBC-[redacted](configure)# bootparam

'.' = clear field;  '-' = go to previous field;  q = quit

Boot File               : /boot/bzImage
IP Address              : [redacted]
VLAN                    : 0
Netmask                 : 255.255.255.0
Gateway                 : [redacted]
IPv6 Address            :
IPv6 Gateway            :
Host IP                 :
FTP username            :
FTP password            :
Flags                   :
Target Name             : [redacted]-SBC-[redacted]
Console Device          : VGA
Console Baudrate        : 115200
Other                   :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.
```

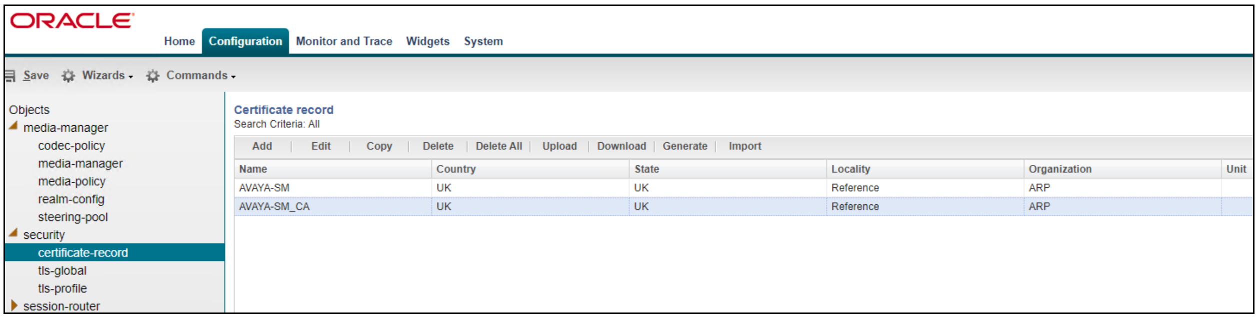
These commands can be run from the CLI command or, as displayed on the screen from the previous page, can be run from the GUI.

- **system-config**: set hostname and default gateway to be used.
- **snmp-community**: configure SNMP communities and IPs of monitoring servers (Zabbix).
- **redundancy-config**: a routing policy for SIP failover – primary and secondary node of HA cluster.
- **phy-interface**: add or edit interfaces for management and media.
  - **wancom1** is dedicated for HA failover - operational type Control
  - **INT** is dedicated for internal media flow - operational type Media
  - **EXT** is dedicated for external media flow - operational type Media
- **ntp-config**: clock sync.
- **network interface**: set IP for physical interface, public IP (EXT) 10.11.180.180 - 3rd party, private IP (INT) X.X.X.X – LifeX
- **host-route**: routing table; 3rd party route: destination networks →10.13.2.0/24; 10.13.4.0/24, Gateway 10.11.180.254

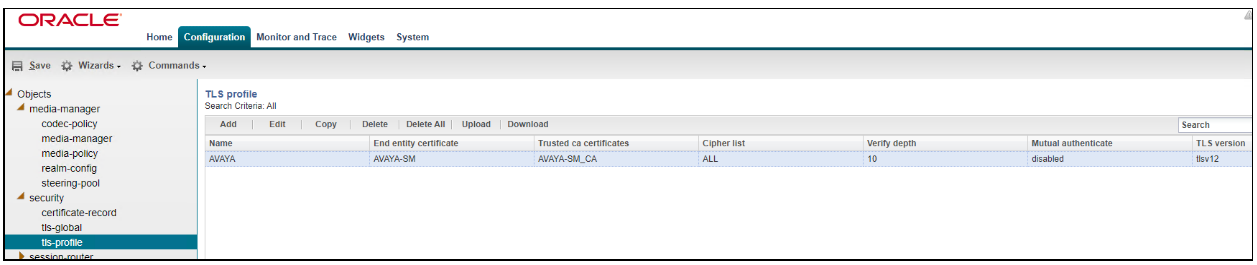
8.2.3. Security – TLS configuration

Frequentis use secured communications between LifeX and 3rd party vendors (PBX, VR) as standard practice. For this to happen, it is required to have configured a certificate record and imported a certificate issued by 3rd party.

To create a certificate record, navigate to **Configuration→Objects→security→certificate-records** in the left window. There are two records present, one for private certificate (signed a generated CSR of SBC-E by CA) and root certificate of Certification Authority (in this case it is the Avaya System Manager).



Create a TLS profile where both certificate records are used by clicking on **tls-profile** in the left window. How to apply this TLS profile is described in **Section 8.2.5**.

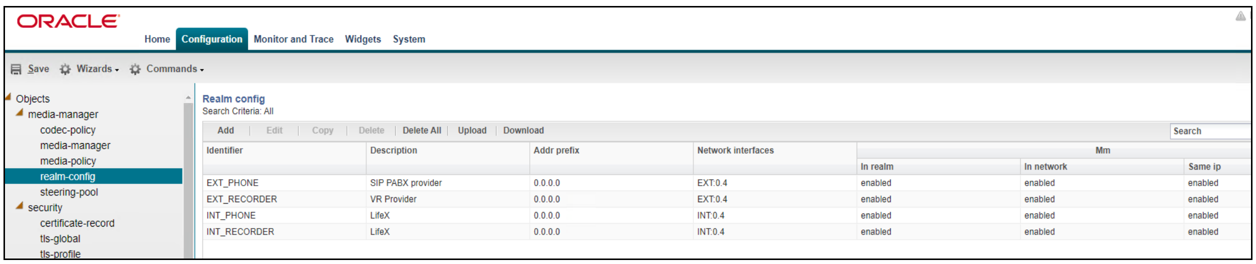


8.2.4. Media Manager – REALM Config

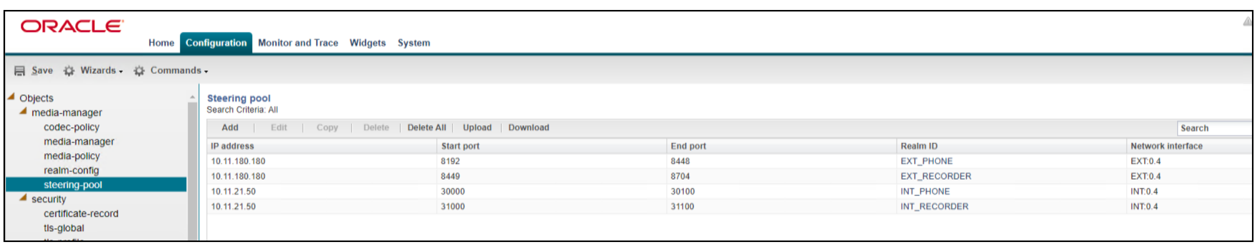
Realms are a logical distinction representing routes (or groups of routes) reachable by the SBC and what kinds of resources and special functions apply to those routes. A **REALM** must be seen as an "area" / "territory" / "region". It may include multiple session agents and / or SIP interfaces.

There are four realms created, two for LifeX (using the network interface for internal media flow described in **Section 8.2.2**) and two for 3rd Party (using the network interface for external media flow described in **Section 8.2.2**). All realms reference network interfaces on the SBC.

To create a new realm, navigate to **Configuration→Objects→media manager→realm-config** in the left window.



To define a set of ports that are used for steering media flows, click on **steering-pool**. A set for every realm is defined.



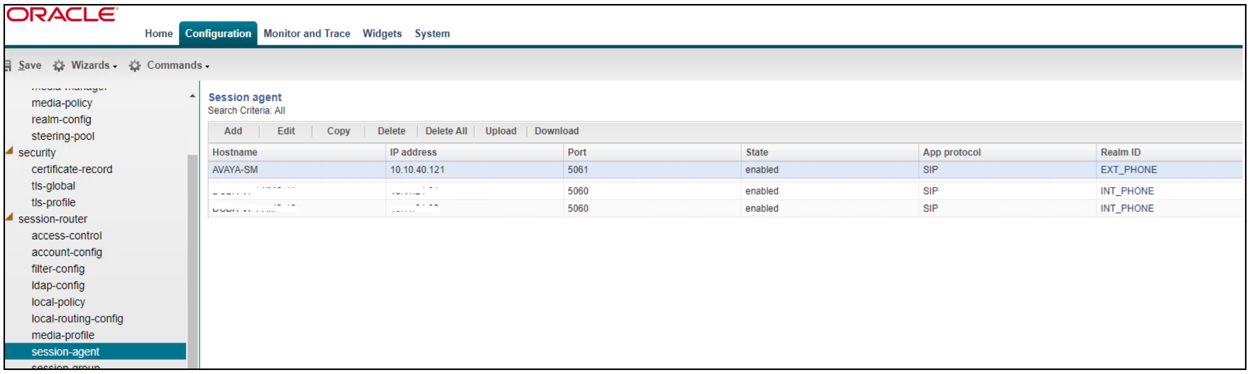
8.2.5. Session Router

Session Router provides high-performance SIP routing with scalable routing policies that increase overall network capacity and reduce cost. It plays a central role in Oracle's open session routing architecture and helps service providers build a scalable, next-generation signaling core for SIP-based services.

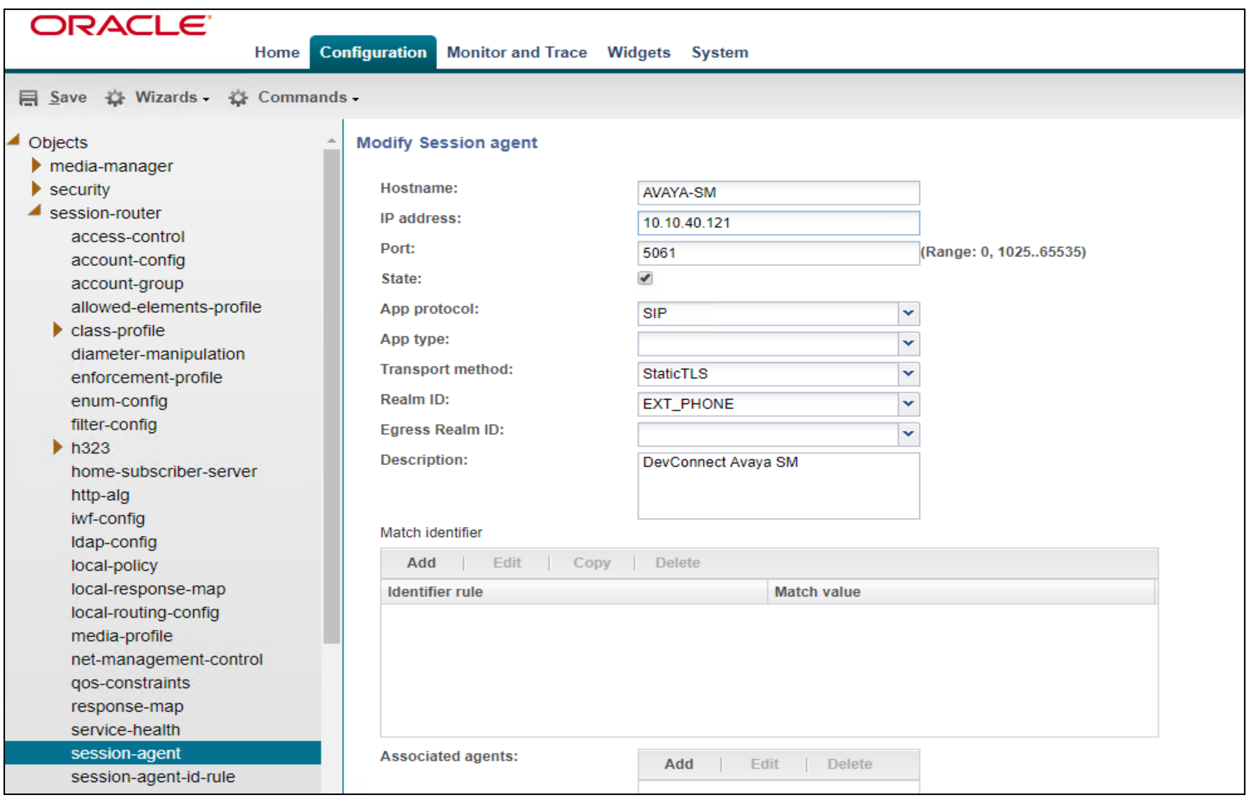
SIP agents are created to specify the IP addresses and ports in which the SBC-E will listen for signalling traffic in the connected networks. SIP agent defines a signaling endpoint.

To create a new Session agent, navigate to **Configuration→Objects→session-router→session-agent** in the left window.

Two session agents are created for the LifeX testing environment (two media servers working as HA failover cluster) with UDP/TPC transport method. Both of these have the **Realm ID** set to **INT_PHONE**, the **Port** is set to **5060**. There is one session agent for the Avaya SBCE with the **IP address** set to that of the Avaya SBCE. Clicking on this will open the window at the bottom of the screen where some further details can be observed.

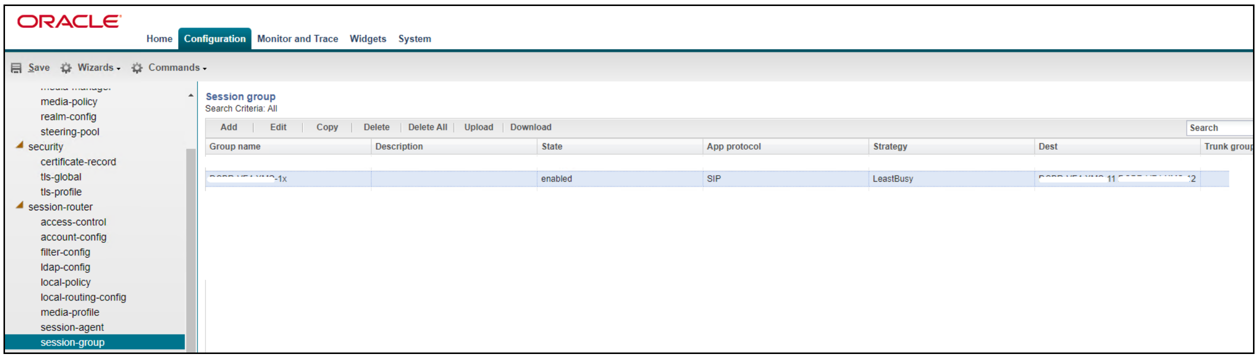


A suitable name if given for the Avaya SBCE with the **IP address** set to that of the Avaya SBC which is **10.10.10.121**, the **Realm ID** is set to **EXT_PHONE**, with the **Port** set to **5061**. The **Transport method** is set to **StaticTLS**.

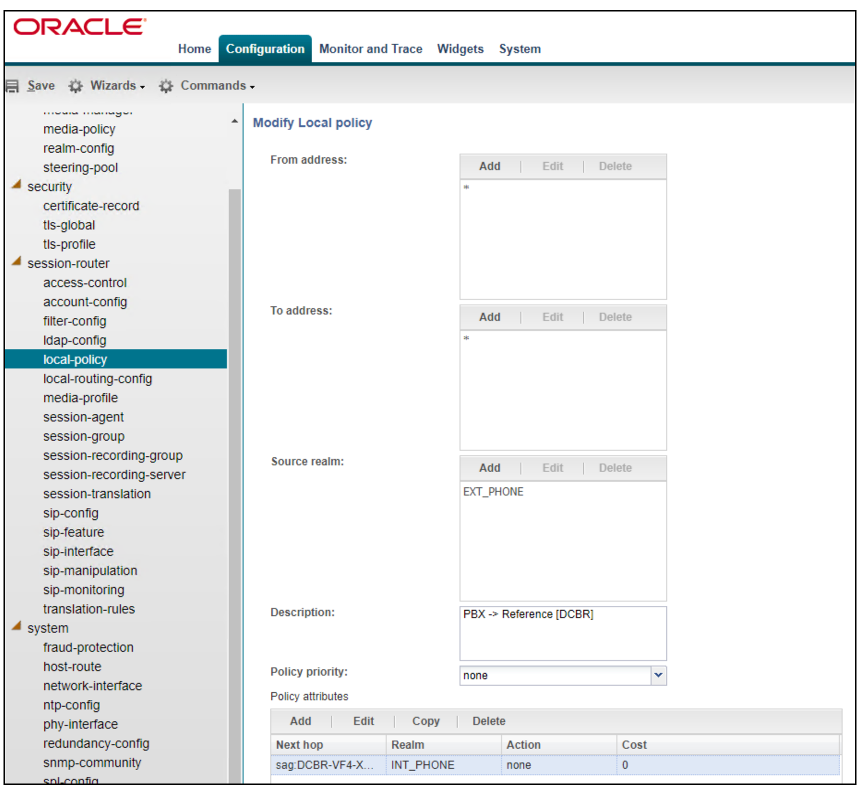


A **Session-group** includes the session agents of both media servers from the LifeX testing environment. Session agent group (SAG) contains individual session agents. Members of a SAG are logically equivalent (although they might vary in their individual constraints) and can be used interchangeably. An allocation strategy is applied to the SAG to allocate traffic across the group members. Session agent groups also assist in load balancing among session agents.

To add a new session group, navigate to **session-router→session-group** in the left window.



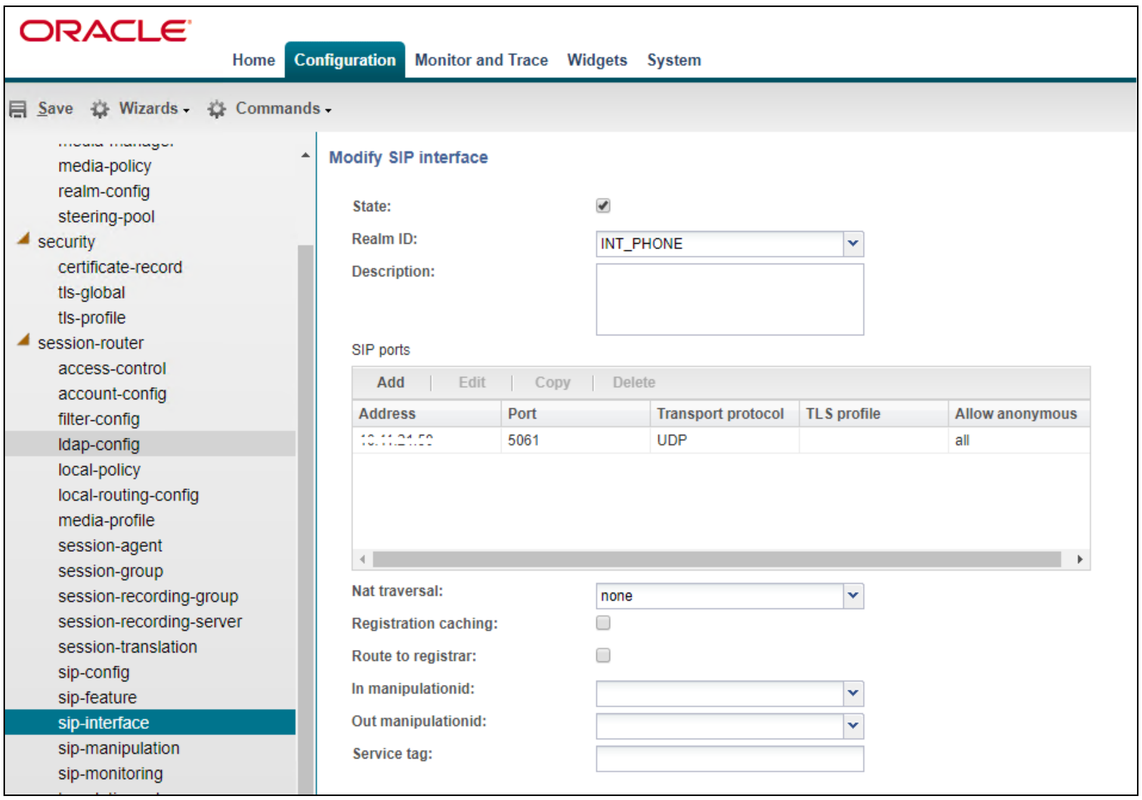
Local policy indicates where session request messages, such as SIP INVITES, are routed and/or forwarded. A local policy can be used to set a preference for selecting one route over another. For the Avaya Realm “EXT_PHONE”, there is set the policy to forward all calls from 3rd party to any number of LifeX Reference system – SAG group (cluster of media servers – Realm ID INT_PHONE) dedicated for LifeX testing environment.



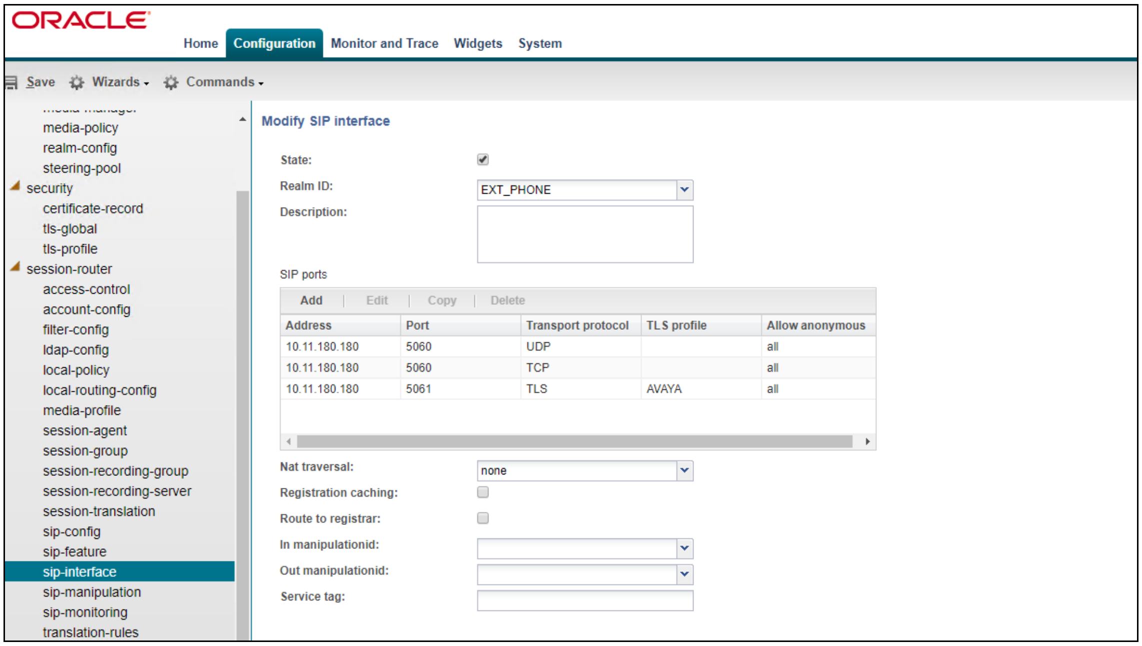
SIP interface defines the transport sockets (IP address and port) upon which the SBC receives and sends SIP messages. SIP interfaces support UDP/TCP/TLS/SCTP Stream Control Transmission Protocol (SCTP) transport, as well as multiple SIP ports. A SIP interface can be defined for each network or realm to which the SBC is connected.

Every SIP interface references a **Realm ID**, as shown below. In this case one SIP interface is used for internal SIP communication with LifeX and one SIP interface for external SIP communication with Avaya SBCE. These are added as TCP and TLS as described in **Section 8.2.3**.

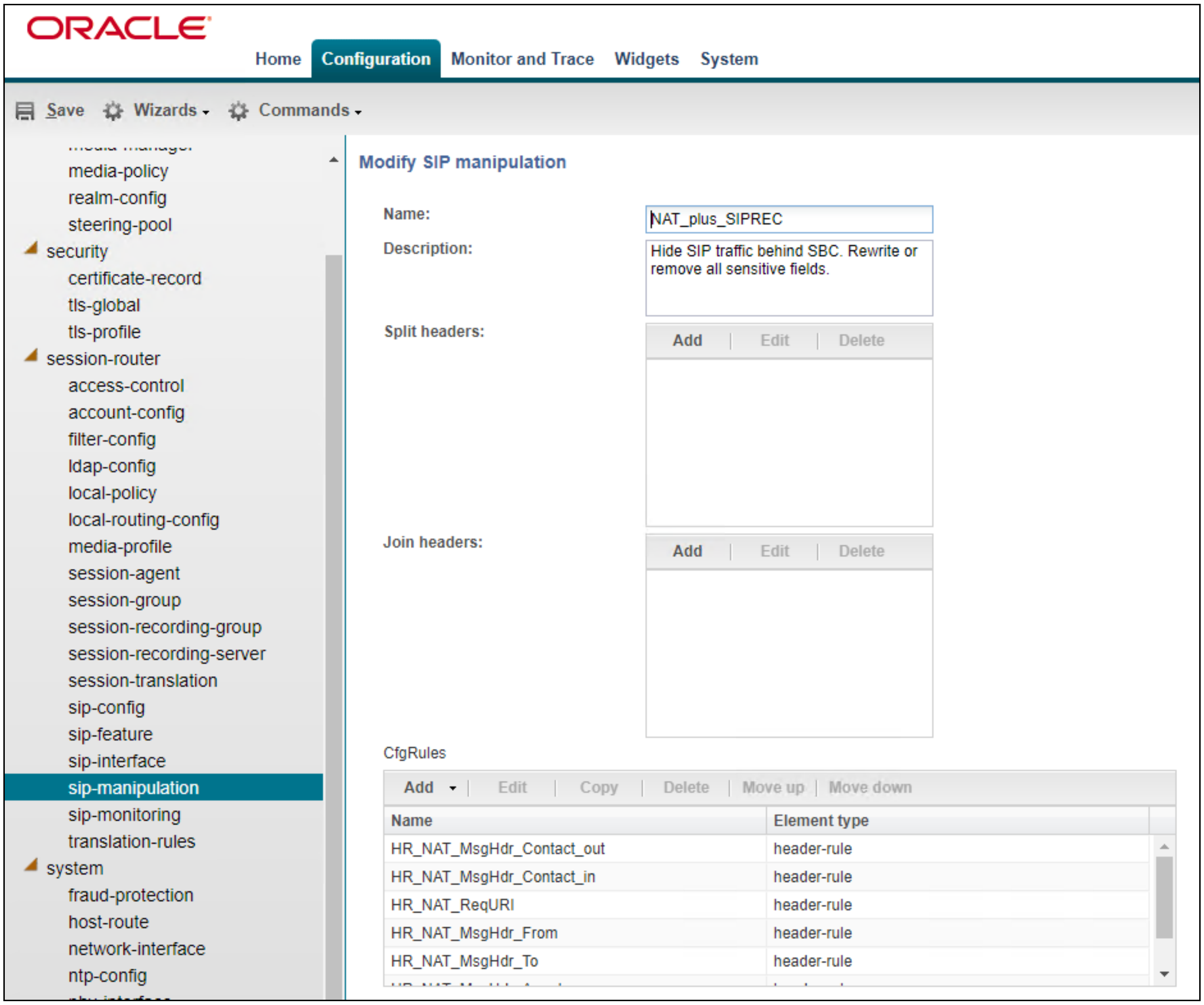
The **INT_PHONE** sip interface is shown below. Frequentis use port 5061 with UDP transport for communication between LifeX and the Oracle SBC.



The **EXT_PHONE** sip interface, which shows all three transport protocols configured for use.



SIP manipulation is confgured, as variances among SIP networks can degrade SIP services or disrupt SIP operations. To resolve these variances, Header Manipulation Rules (HMR) are giving network administrators the ability to control SIP traffic by manipulating SIP messages. The manipulation of SIP messages is carried out because of functionality, security and 3rd party requirements. Below is an example of the SIP manipulation used for compliance testing.

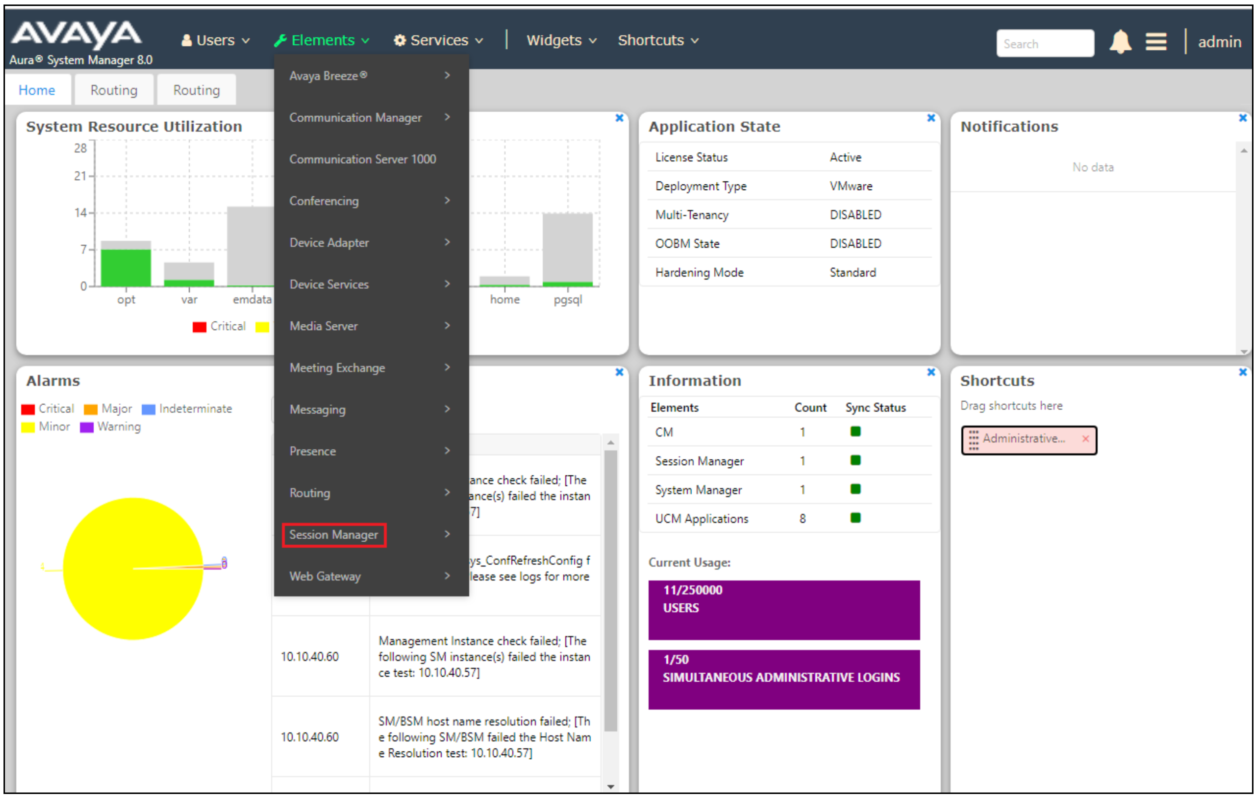


9. Verification Steps

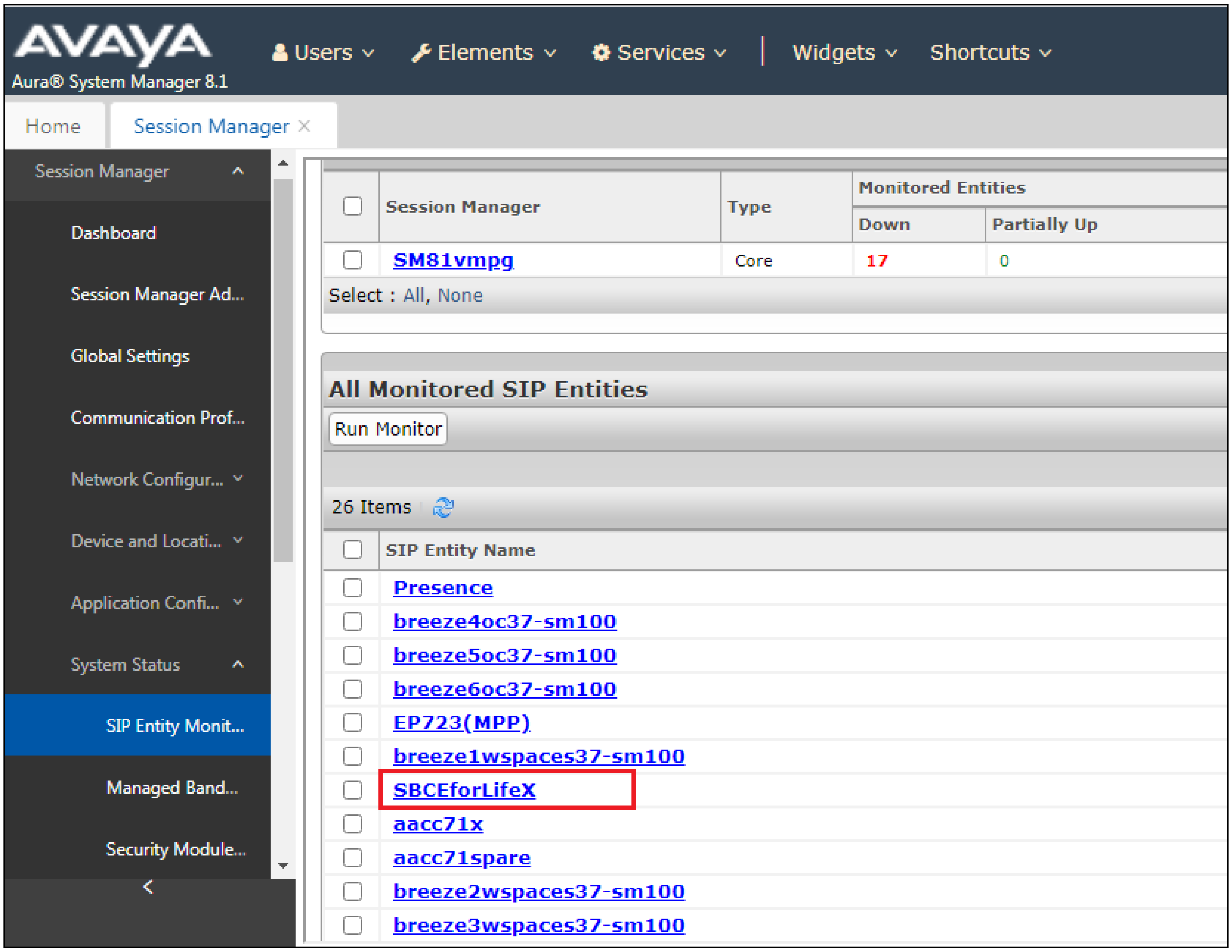
The following steps can be taken to ensure that connections between the Avaya platform and the Frequentis platform successfully in place.

9.1. Session Manager Registration

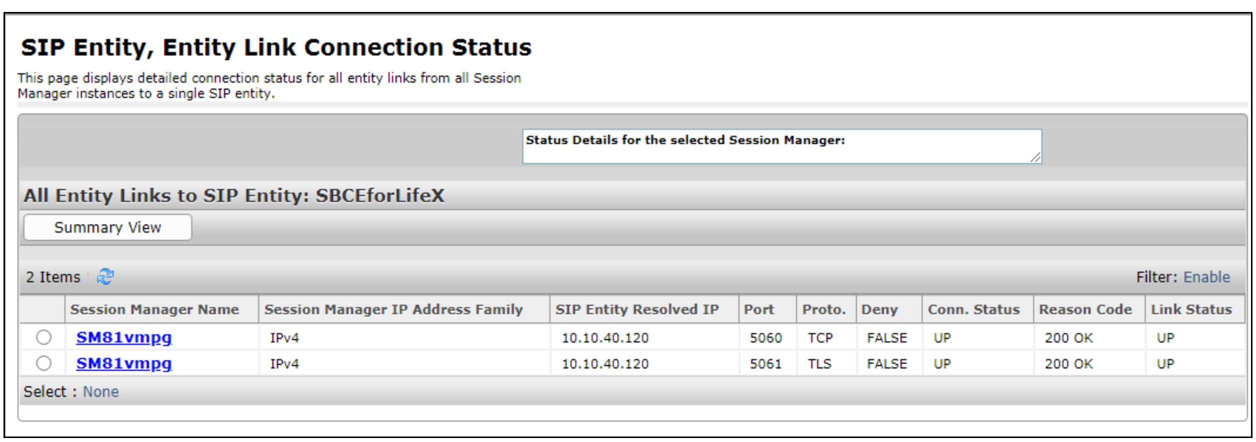
Log into System Manager as per **Section 6**. Navigate to **Elements** and click on **Session Manager**.



Select the Avaya SBCE SIP Entity.



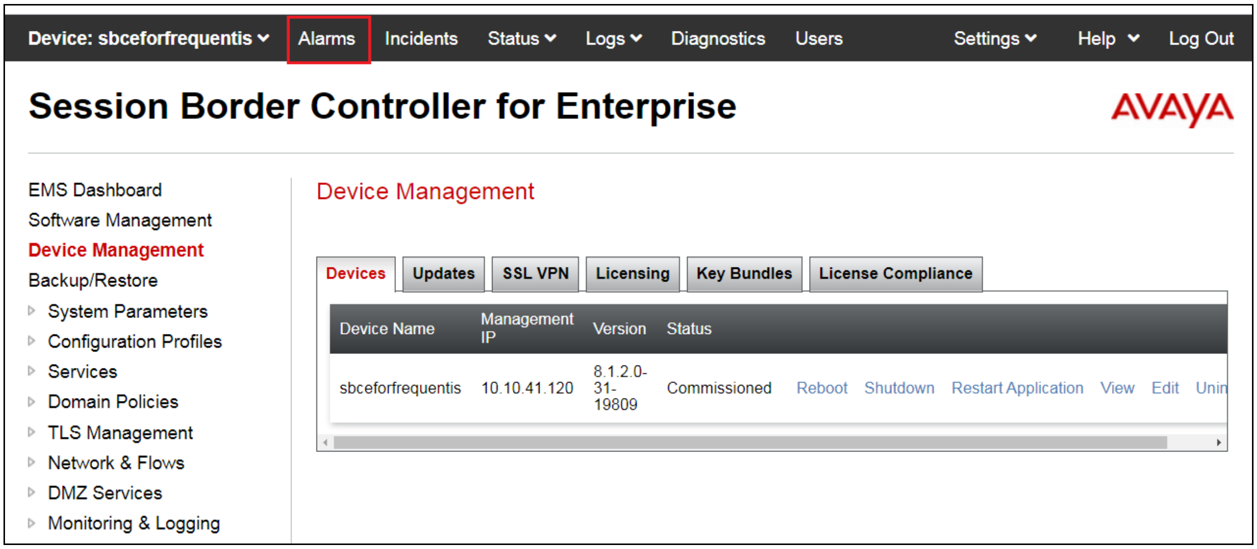
The SIP Entity should show as **UP** as it is shown below. The example below shows a connection for both TLS and TCP; however, the TLS connection was the only connection used during compliance testing.



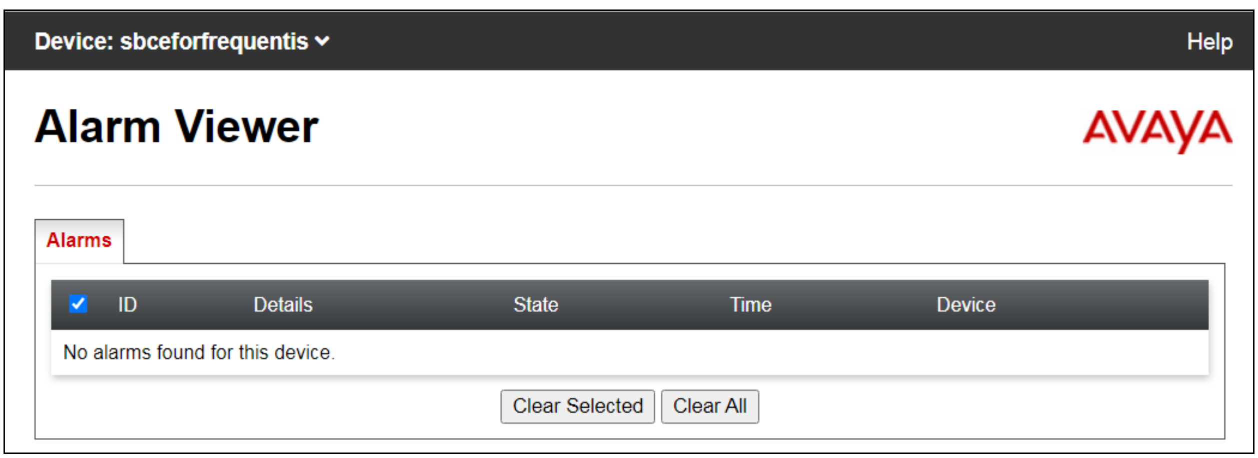
9.2. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

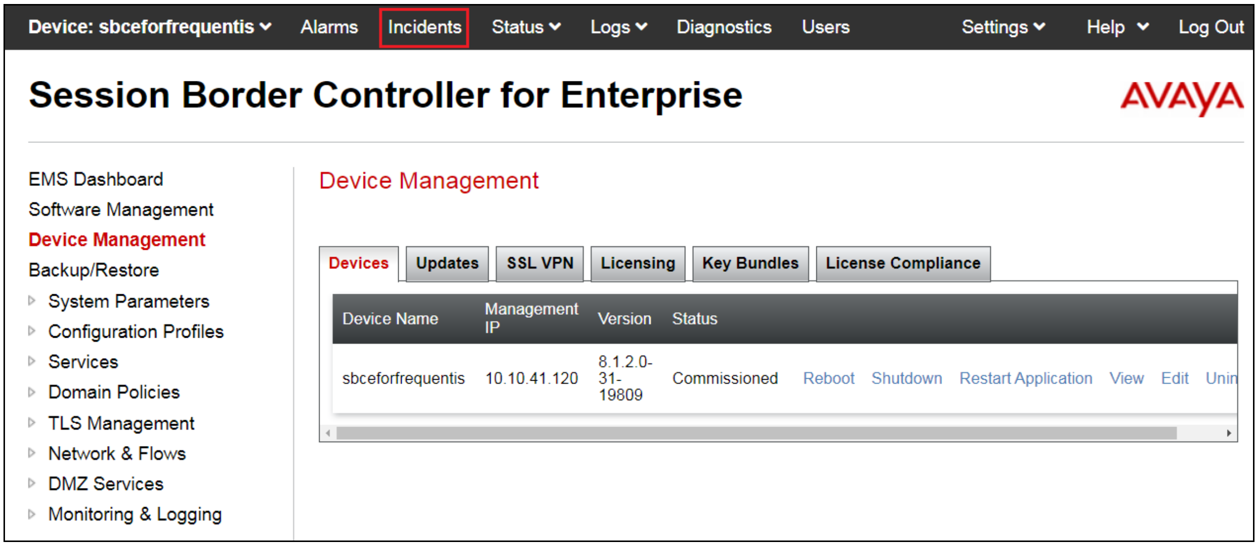
Alarms: This screen provides information about the health of the SBC.



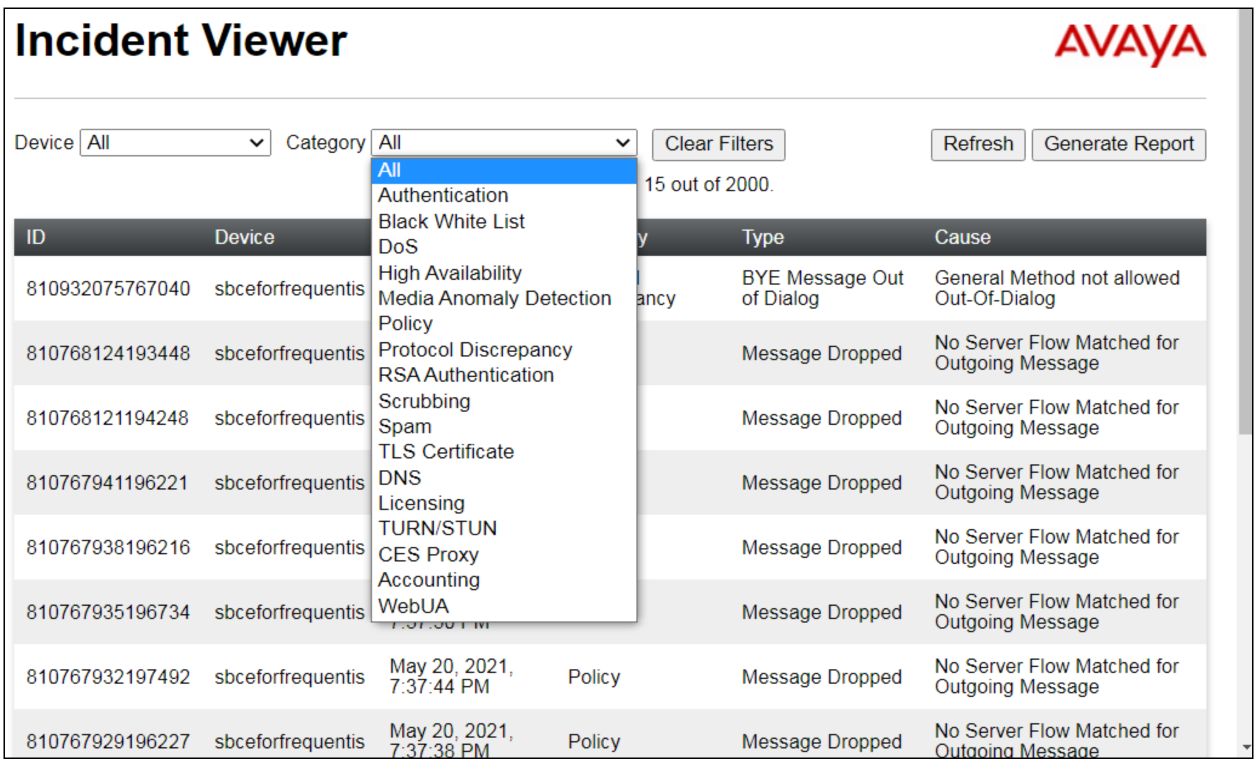
The following screen shows the **Alarm Viewer** page.



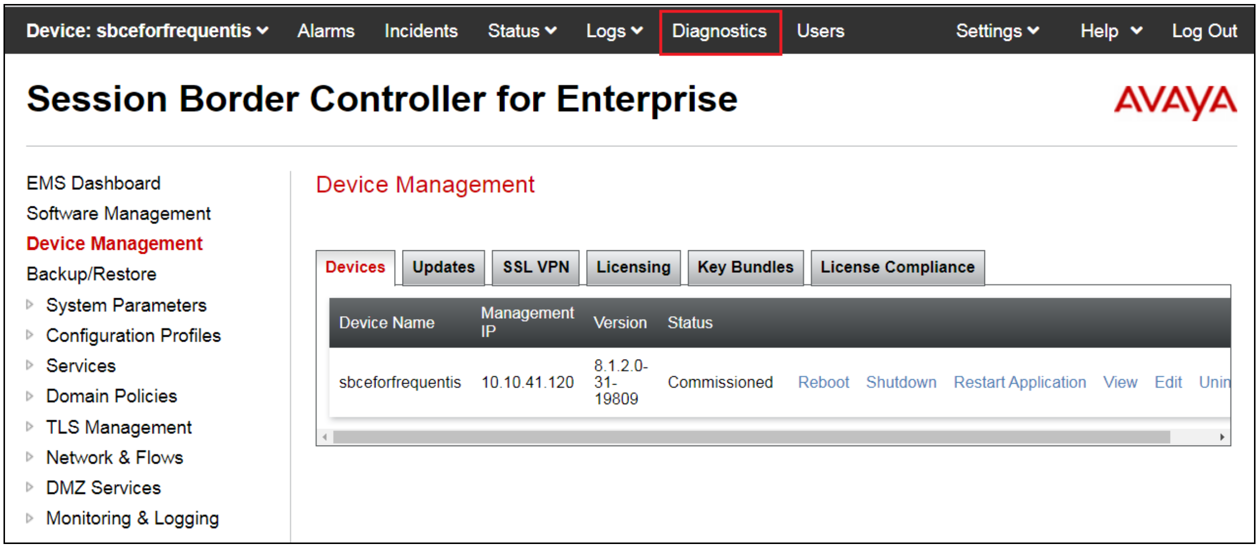
Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.



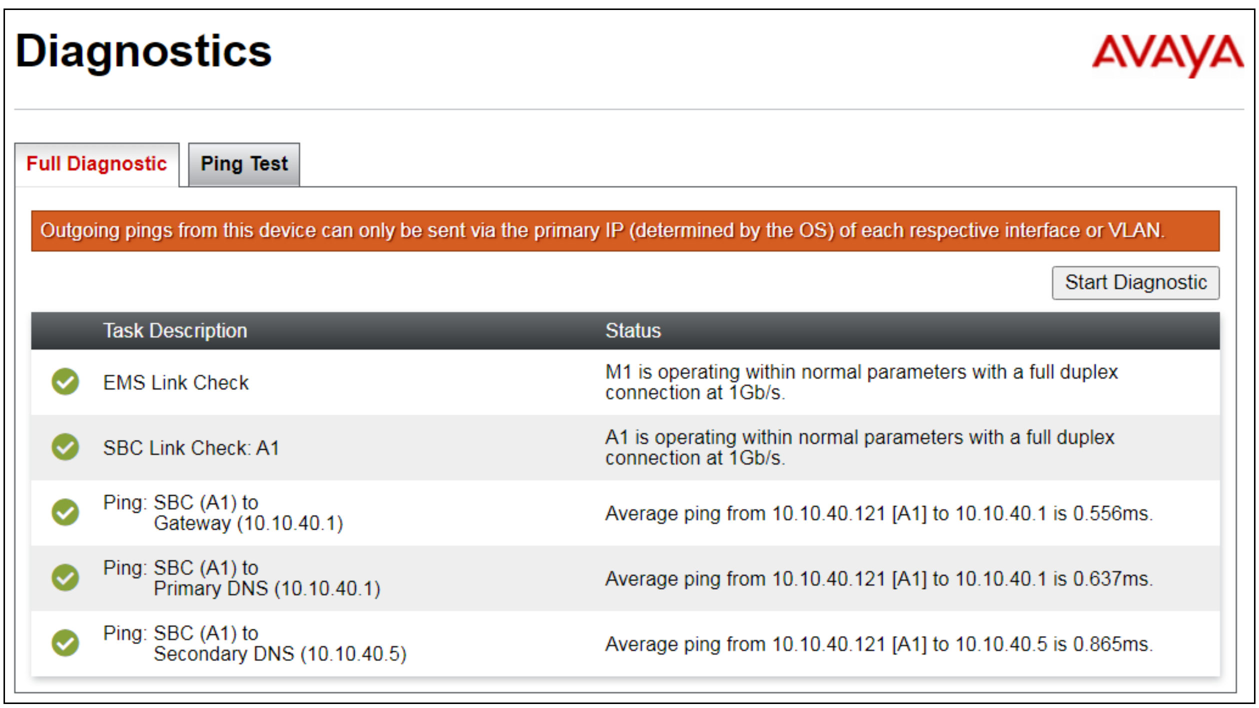
The following screen shows the **Incident Viewer** page. The incidents can be filtered as shown below. The example below also includes some old incidents that occurred during the setup phase.



Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

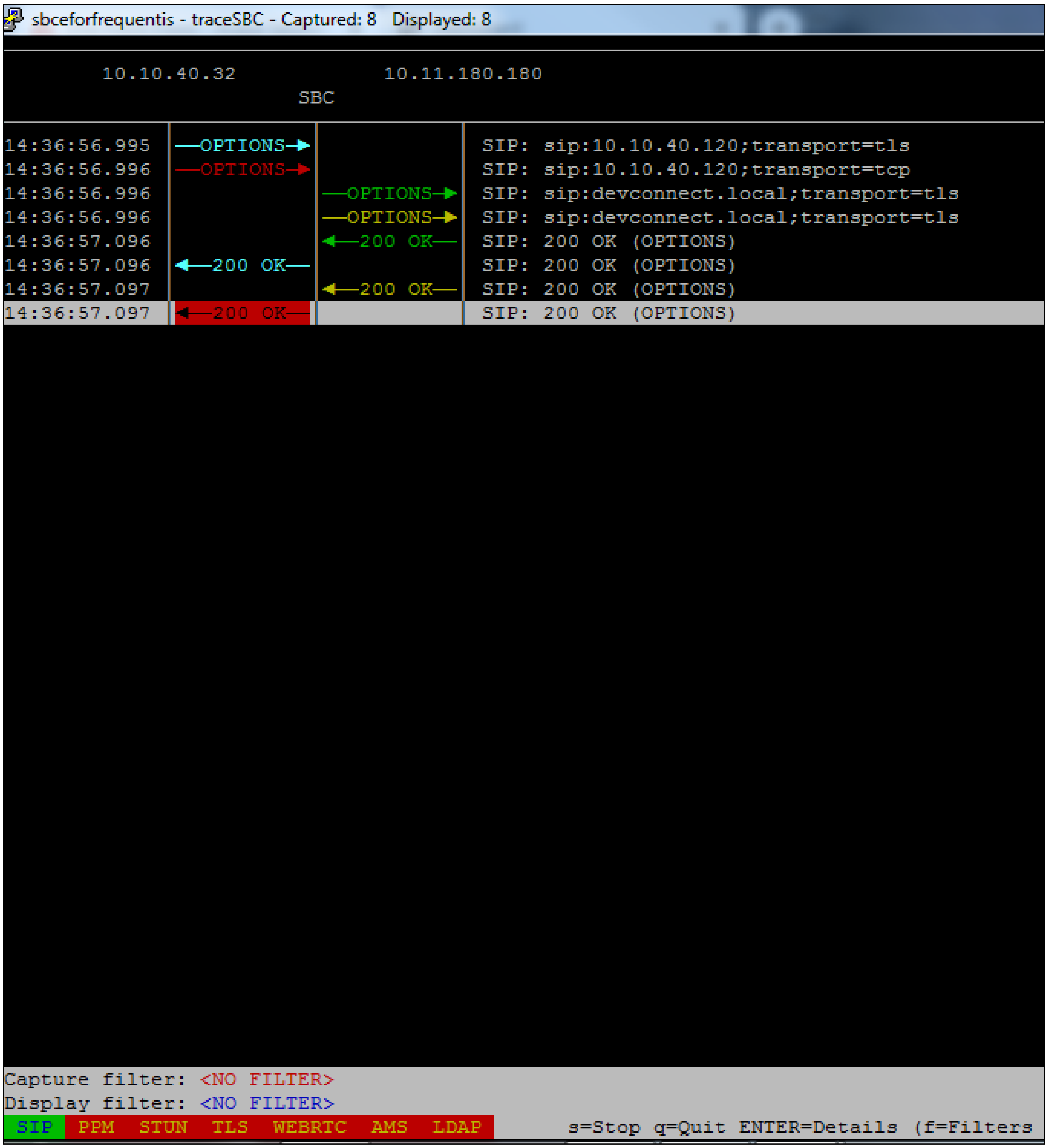


The following shows a **Full Diagnostic** test being performed.



9.3. Observe the connection using the Avaya Session Border Controller for Enterprise tracesbc tool

By opening PuTTY and connecting to the Avaya SBCE, a **traceSBC** tool can be run by typing in tracesbc, the following shows the **OPTIONS** and **200 OK** messaging being passed back and forth which signals that the devices are connected and sending/receiving SIP messages. When calls are made the SIP messaging can be analysed here also.



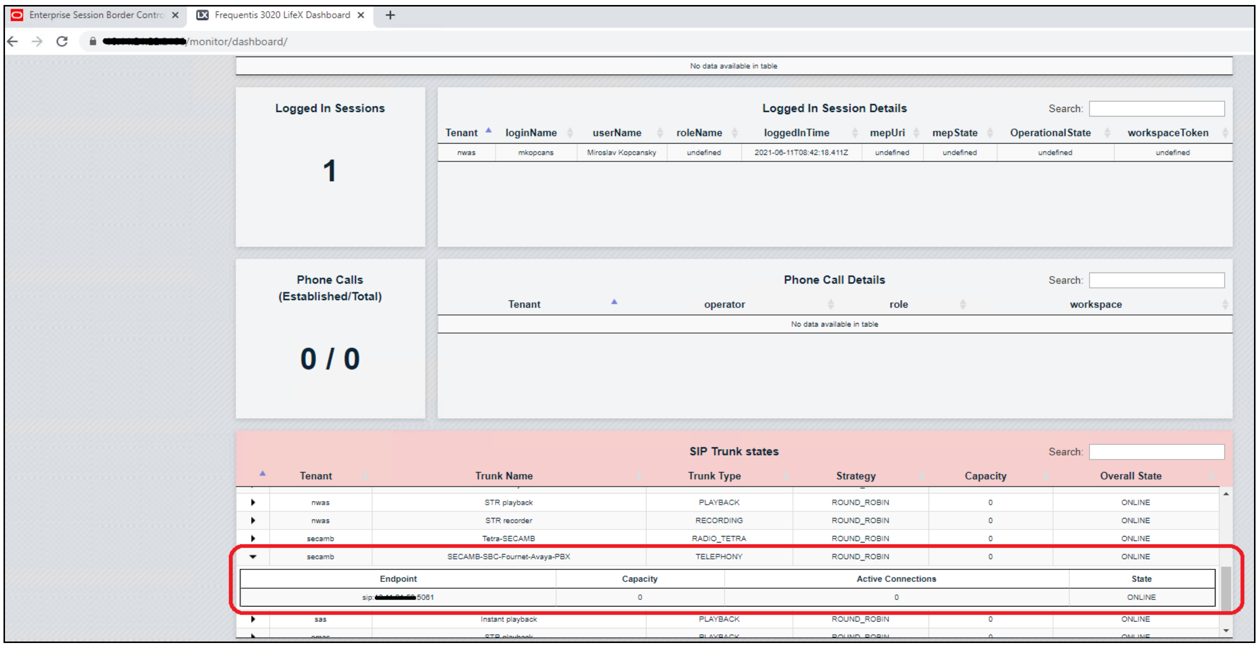
9.4. Verify LifeX 3020

This section shows the steps that can be taken to verify the connection from the LifeX side.

9.4.1. Frequentis LifeX

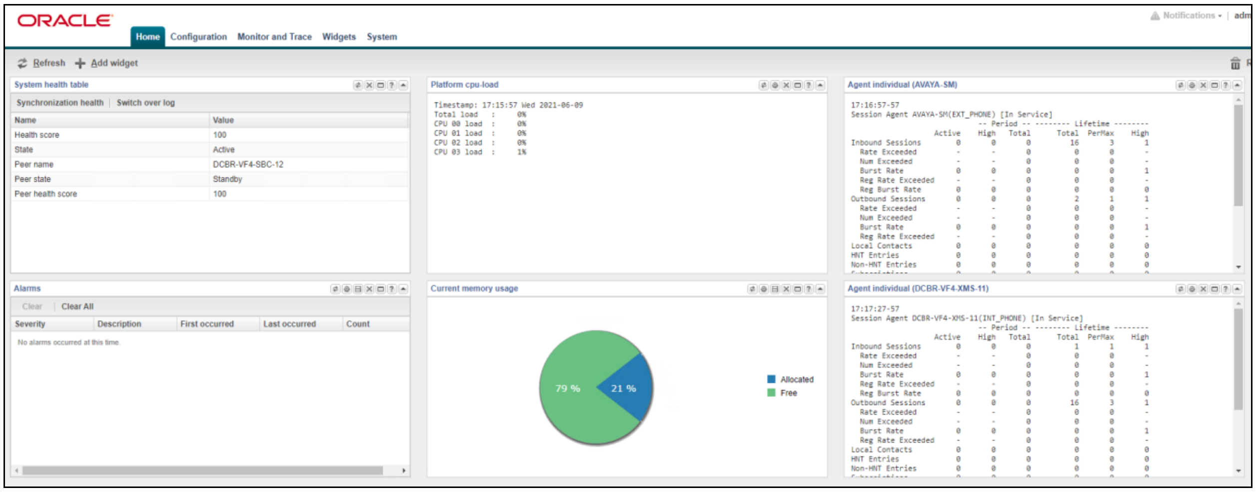
To verify a SIP trunk (**SBC**), access the LifeX dashboard webpage by using https://<IP_address>:<port>/**monitor/dashboard**/ where IP is the business main server of LifeX reference environment and port is the monitoring service running on it.

The overall status is either Online or Degraded and the **State** below shows **ONLINE**.

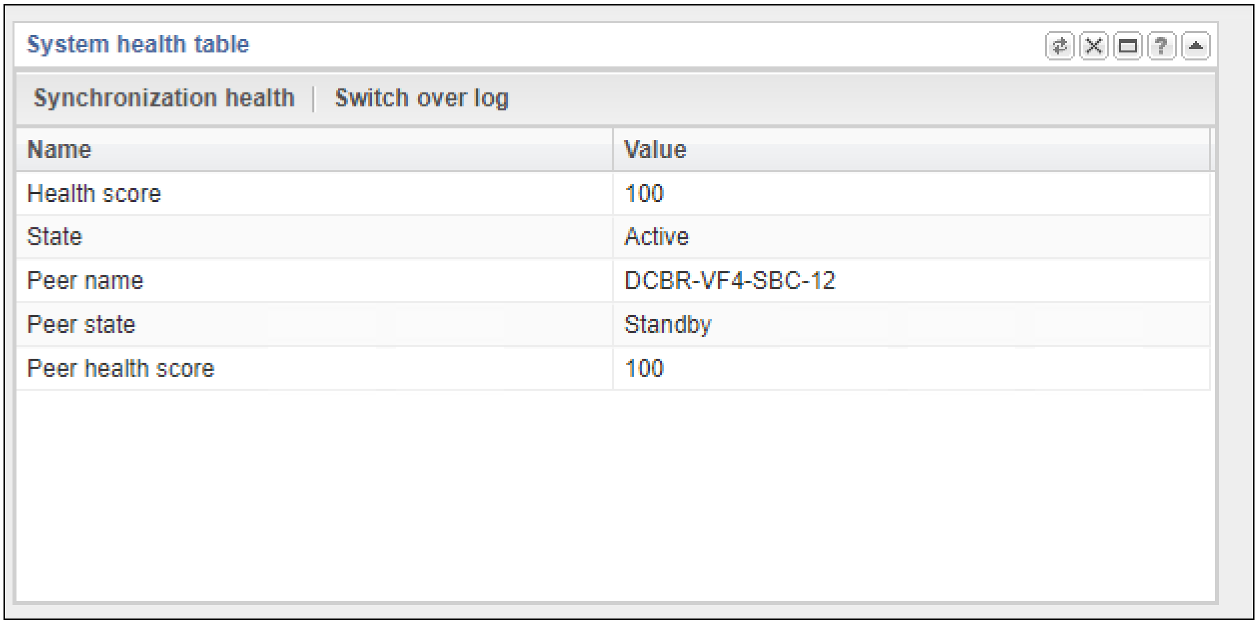


9.4.2. Frequentis Oracle SBC

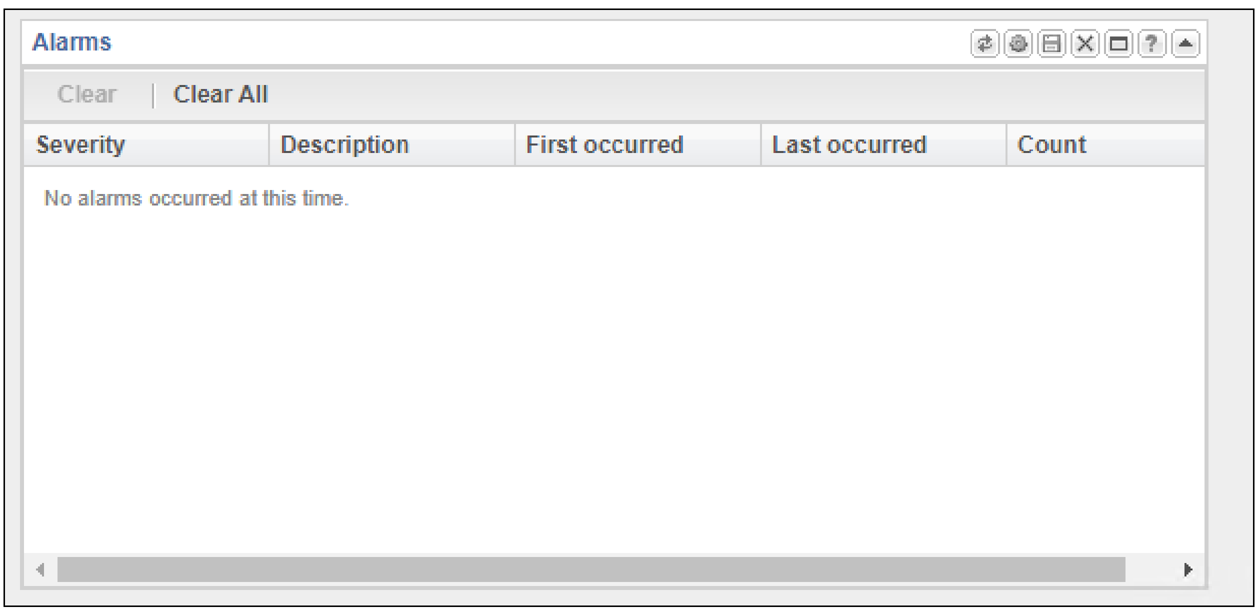
From the Oracle SBC, on the **Home** tab, widgets can be added dedicated for monitoring.



Some examples of these widgets include:
System health table – where the cluster health is observed.



Alarms – describes any issue or problem.



Platform cpu-load – shows the utilization of the CPU.

Platform cpu-load

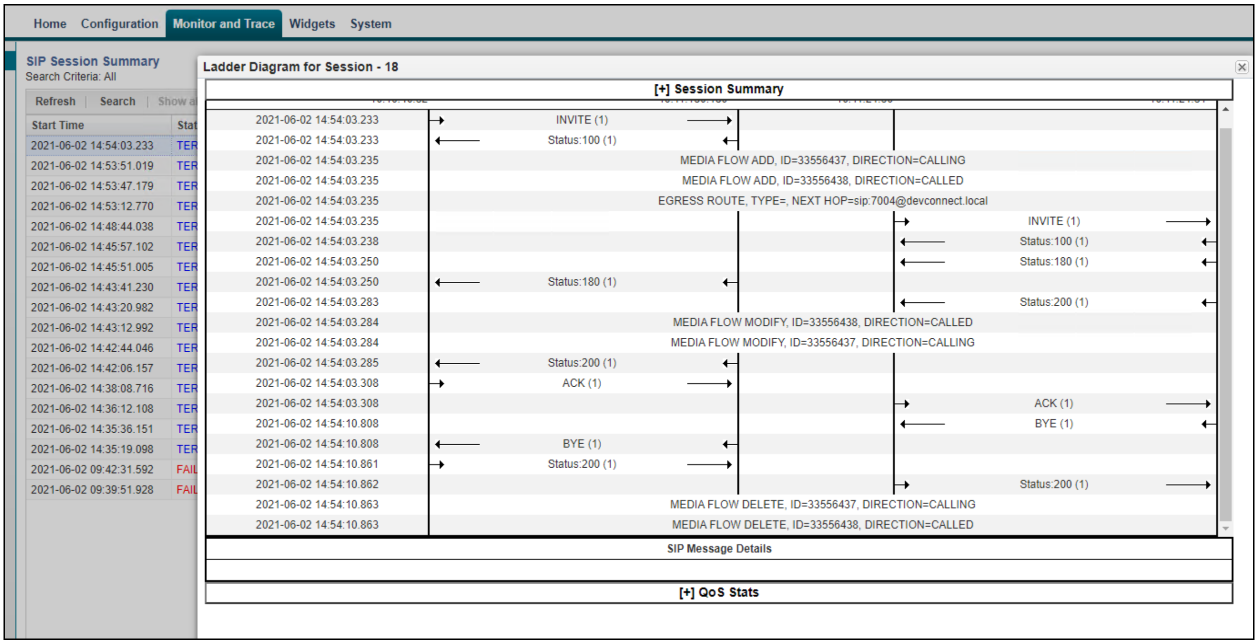
```
Timestamp: 17:15:57 Wed 2021-06-09
Total load  :      0%
CPU 00 load  :      0%
CPU 01 load  :      0%
CPU 02 load  :      0%
CPU 03 load  :      1%
```

Agent individual – monitors the SIP connection.

Agent individual (AVAYA-SM)

```
17:16:57-57
Session Agent AVAYA-SM(EXT_PHONE) [In Service]
                             -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Inbound Sessions        0       0       0         16       3       1
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0       0       0          0       0       1
  Reg Rate Exceeded     -       -       0          0       0       -
  Reg Burst Rate        0       0       0          0       0       0
Outbound Sessions       0       0       0          2       1       1
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0       0       0          0       0       1
  Reg Rate Exceeded     -       -       0          0       0       -
Local Contacts          0       0       0          0       0       0
HNT Entries             0       0       0          0       0       0
Non-HNT Entries         0       0       0          0       0       0
```

For troubleshooting of a potential failed SIP session, use **SIP Session Summary** from **Monitor and Trace**. Double-click on a session to open a diagram with useful information of the SIP flow.



10. Conclusion

These Application Notes describe the configuration steps required for Frequentis AG 3020 LifeX to successfully interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 utilizing the Avaya Session Border Controller for Enterprise R8.1.2. Please refer to **Section 2.2** for test results and observations.

11. Additional References

This section references the product documentation relevant to these Application Notes. Product documentation for Avaya products may be found at http://support.avaya.com.

[1] *Deploying Avaya Aura® Communication Manager* in a Virtualized Environment, Release 8.1.x, Issue 6, October 2020.
[2] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 7, October 2020.
[3] *Administering Avaya Aura® System Manager* for Release 8.1.x, Issue 8, November 2020.
[4] *Deploying Avaya Aura® System Manager* in a Virtualized Environment, Release 8.1.x, Issue 7, November 2020.
[5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager* in a Virtualized Environment, Release 8.1., Issue 4, October 2020.
[6] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 7, October 2020.
[7] *Deploying Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020.
[8] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020.
[9] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.x, Issue 11, October 2020.
[10] *Implementing and Administering Avaya Aura® Media Server*. Release 8.0.x, Issue 11, October 2020.
[11] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[12] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

Documentation for Frequentis products can be obtained from Frequentis as follows.

- Web: https://www.frequentis.com/en/contact-us

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.