Avaya Solution & Interoperability Test Lab

Application Notes for configuring Frequentis AG 3020 LifeX with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – 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 a direct connection to Avaya Aura® Session Manager R8.1.

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 a direct connection from Avaya Aura® Session Manager 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.

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 the Avaya platform uses a direct connection from Session Manager to a Session Border Controller provided by Frequentis, 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 Aura® Session Manager and LifeX made use of a TLS connection, however the RTP between the Avaya platform 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. An Adaptation was used to ensure that all calls to LifeX were in the format ext@domain, see **Section 6.2**.
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 is a Session Border controller on the Frequentis side of the solution, which connects directly to Session Manager on the Avaya side.

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.

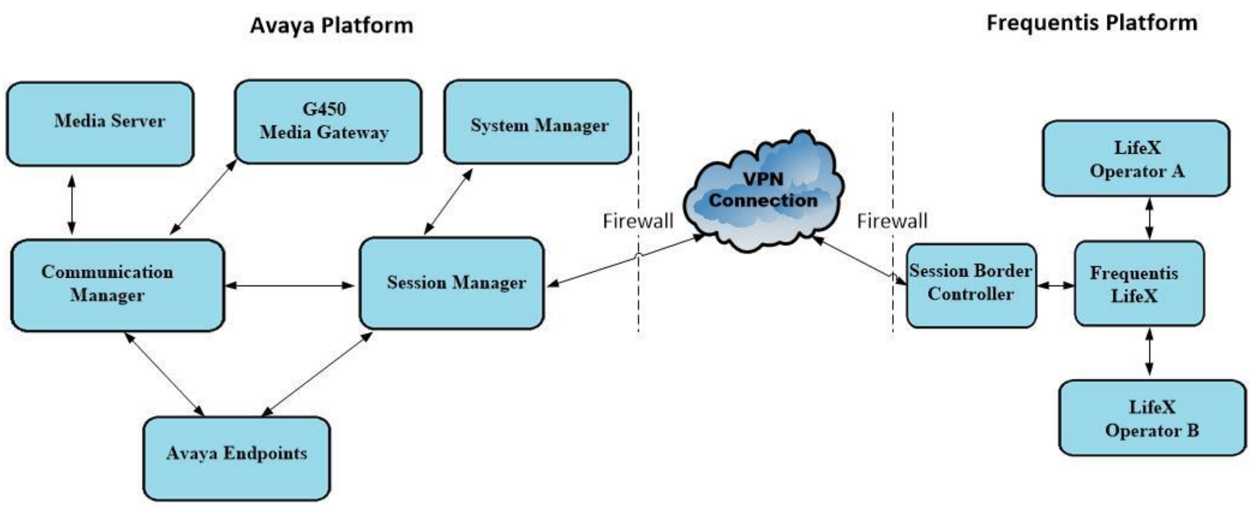


Figure 1: Connection of Frequentis LifeX with Avaya Aura® Communication Manager R8.1, Avaya Aura® Session Manager R8.1

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 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 10** 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 10** 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. 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 LifeX. 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 LifeX. 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.

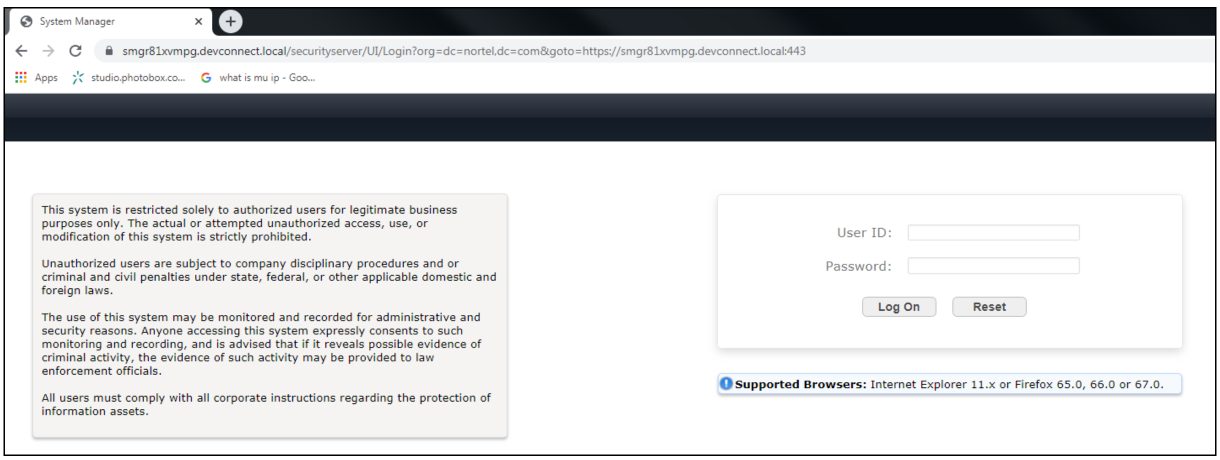
```
change trunk-group 12                                           Page   4 of   4
                              PROTOCOL VARIATIONS

                                       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

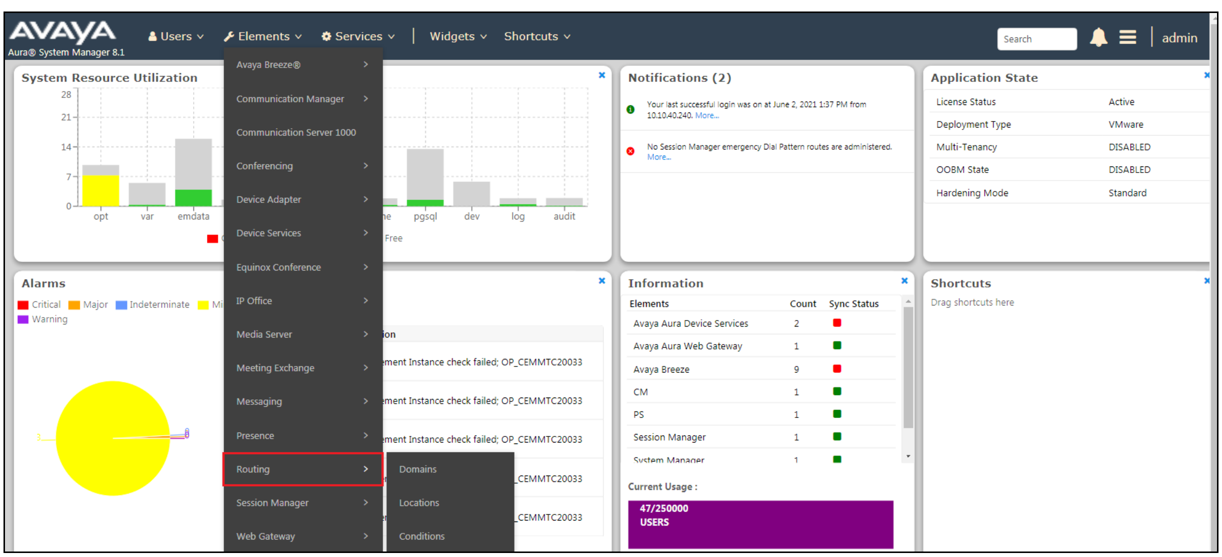
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Adding an Adaptation for LifeX
- Adding a SIP Entity for LifeX
- Adding a Routing Policy for LifeX
- Adding a Dial Pattern for lifeX

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**.

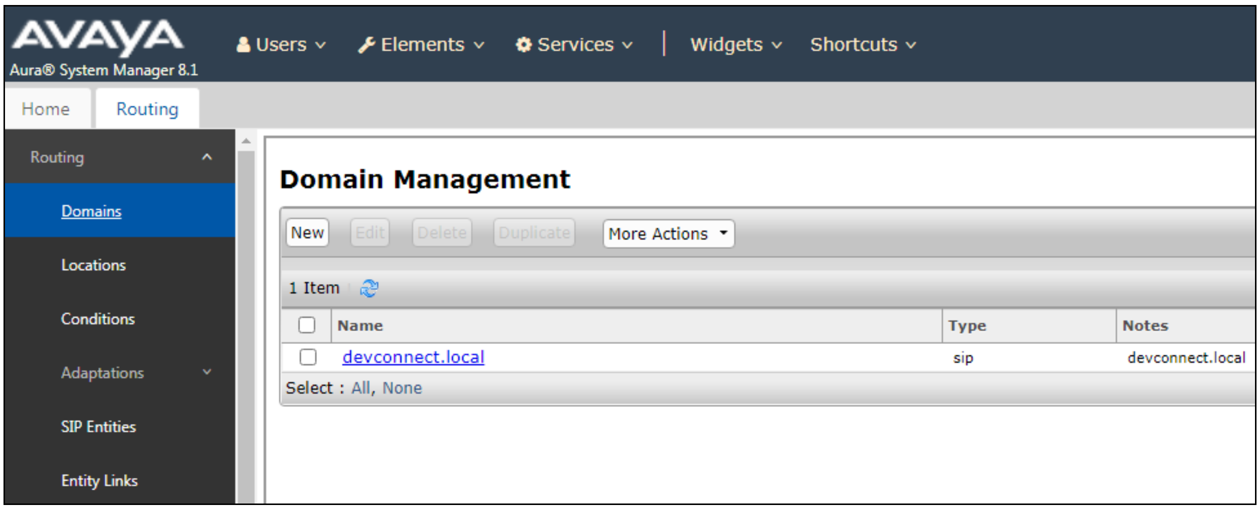


6.1. Domains and Locations

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.

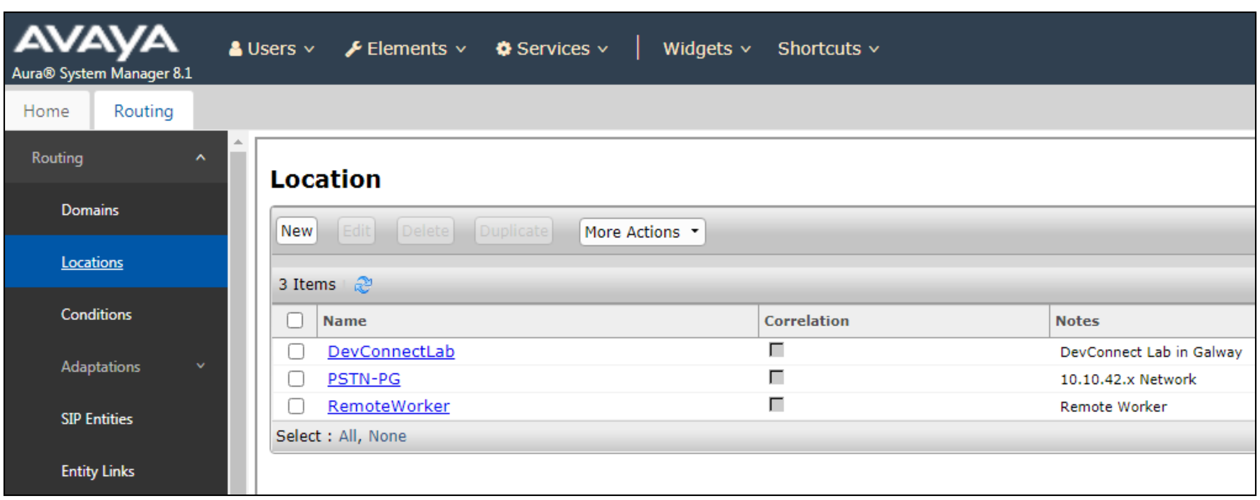
6.1.1. Display the Domain

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

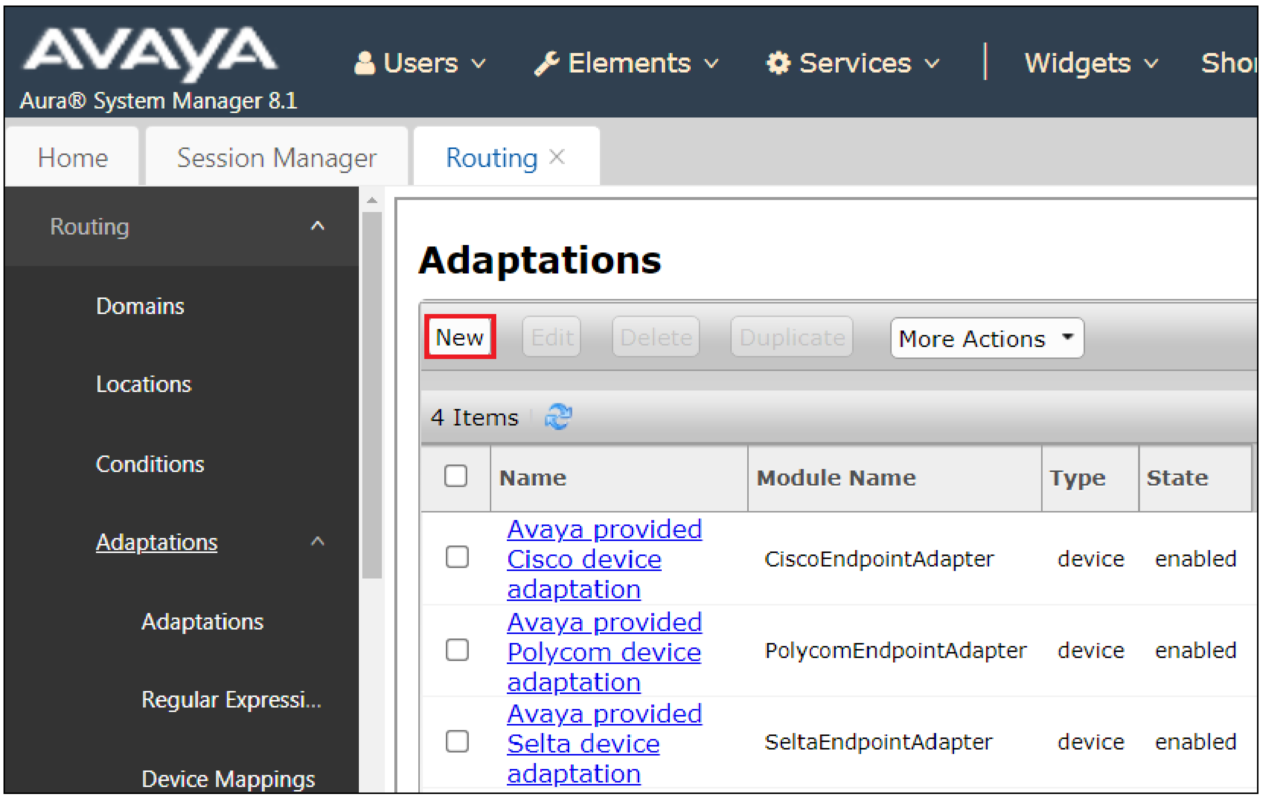
Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click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



6.2. Adding an Adaptation for Frequentis LifeX

An issue arose during testing when Avaya phones were forwarded back to LifeX operators. The calls were being declined by LifeX because the domain name was not present on the forwarded call, this is as per design from LifeX as this domain name should be present. Adding an Adaptation ensures that the domain name is always present on any and all outgoing calls to LifeX. Once the Adaptation is created, it is then associated with the LifeX SIP Entity created in **Section 6.3**.

From the left window navigate to **Routing** → **Adaptations** and from the main window click on **New**.

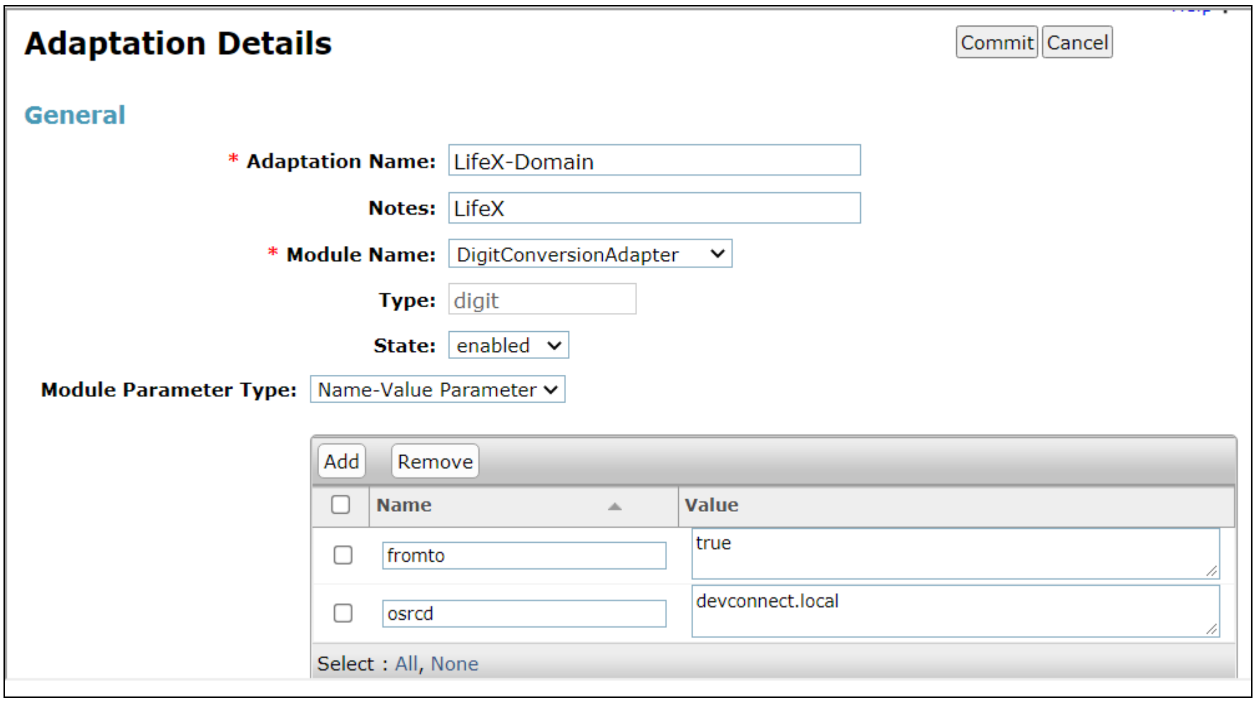


The following should be configured for this Adaptation.

- **Adaptation name**: Add a suitable name for this Adaptation.
- **Notes**: Enter something descriptive.
- **Module Name**: Select **DigitConversionAdapter** from the dropdown.
- **Type**: Should automatically select **digit.**
- **State**: Should be **enabled**.
- **Module Parameter Type**: Select **Name-Value Parameter** from the dropdown.

The following items will ensure that the correct domain name is sent out to LifeX on all outgoing calls to that SIP Entity.

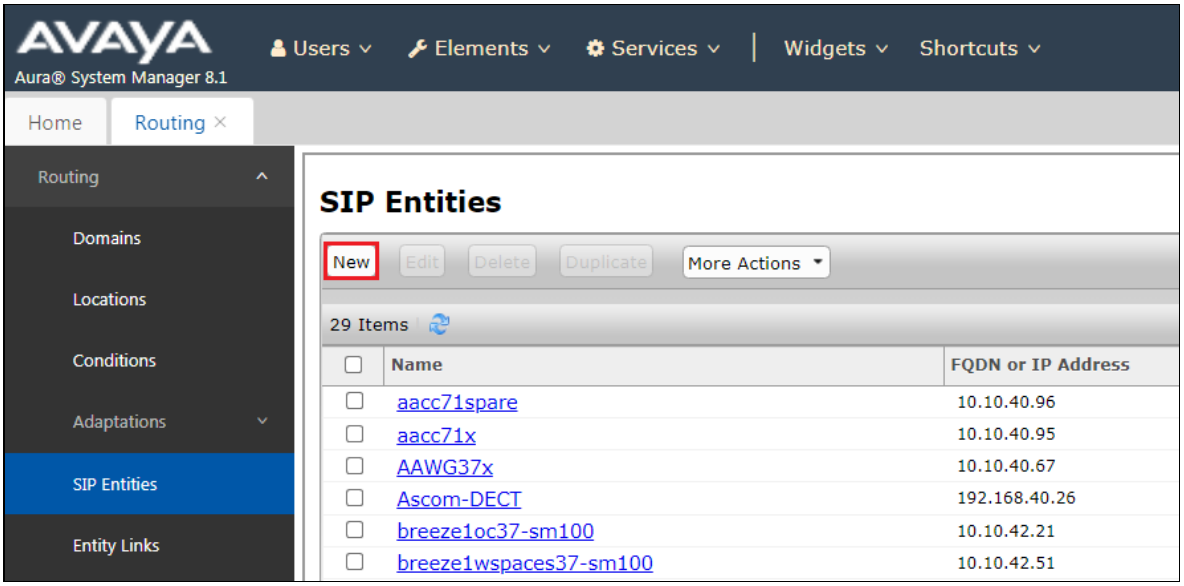
- **fromto** is set to **true**.
- **osrcd** is set to **devconnect.local** (which is the correct domain name in this case).



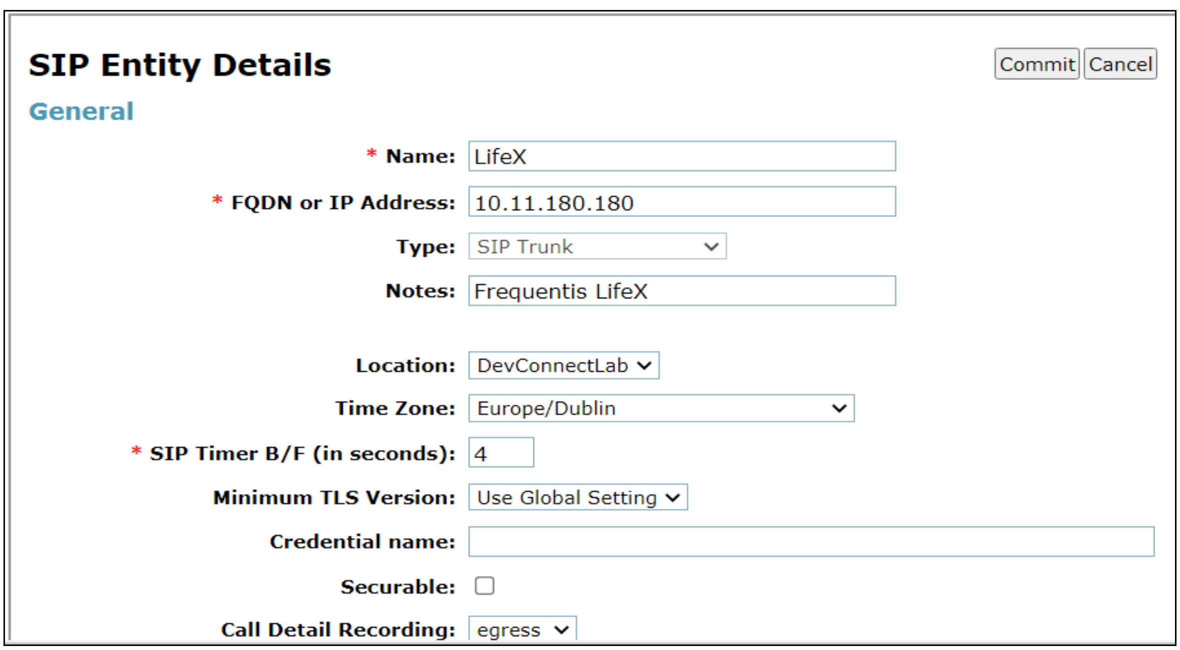
6.3. Adding a SIP Entity for Frequentis LifeX

Because the calls are routed to LifeX directly it must be added as a SIP Entity, the Adaptation from the previous page is also added.

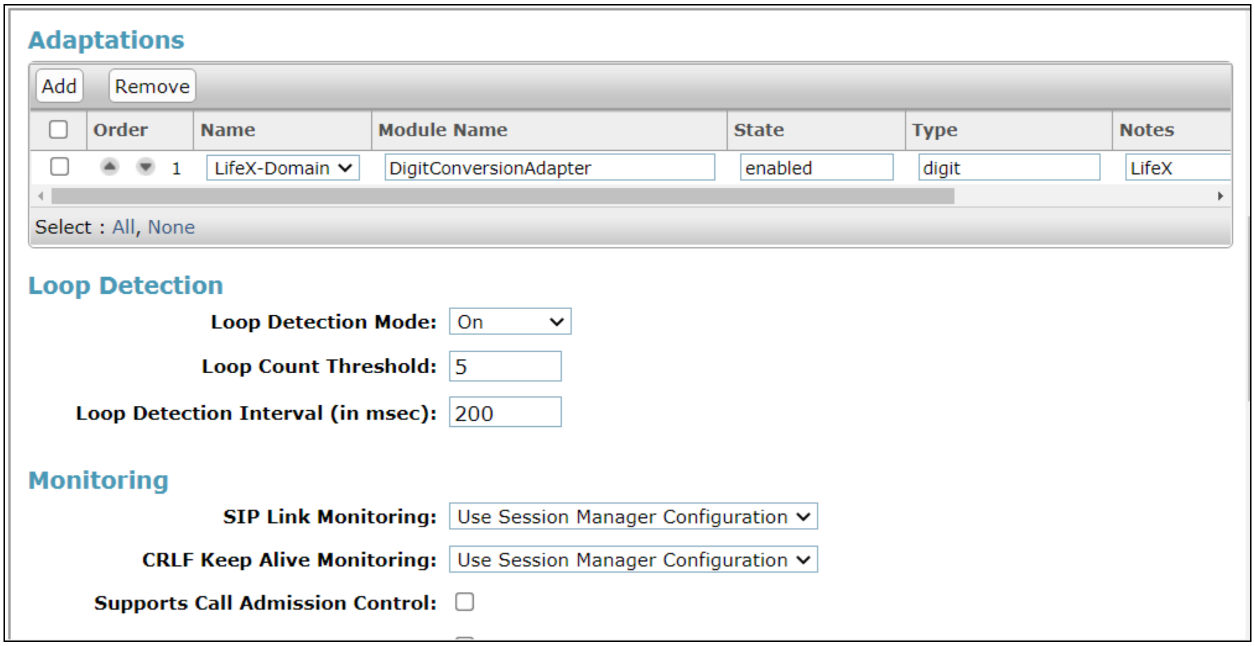
Click on **SIP Entities** in the left column and select **New** in the right window.



Enter a suitable **Name** for the SIP Entity, enter the **IP Address** of the device on the LifeX side that will make the connection, in this case this IP address is the address of the Oracle SBC. Enter the correct **Time Zone** and **Location**. From this page, scroll down to add the Adaptation.

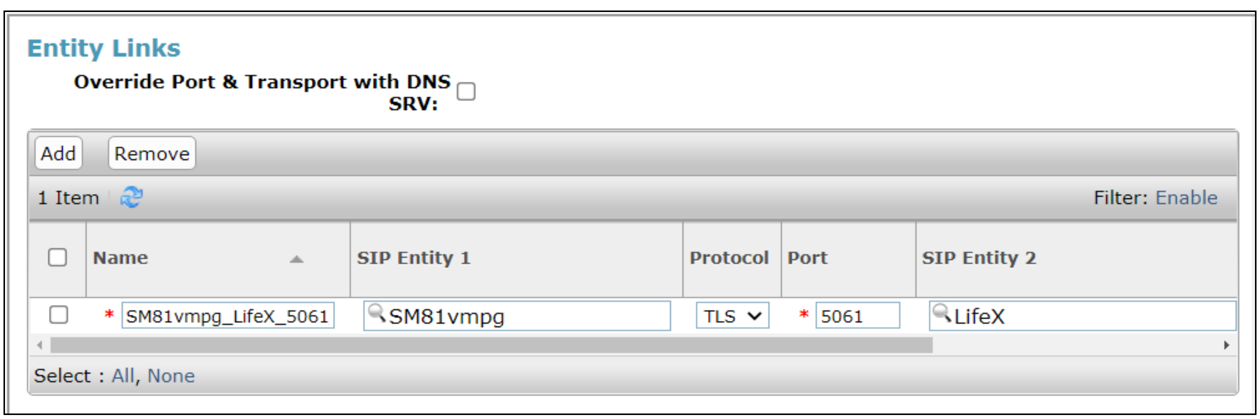


Scroll down to **Adaptations** and add the Adaptation that was created in **Section 6.2**.



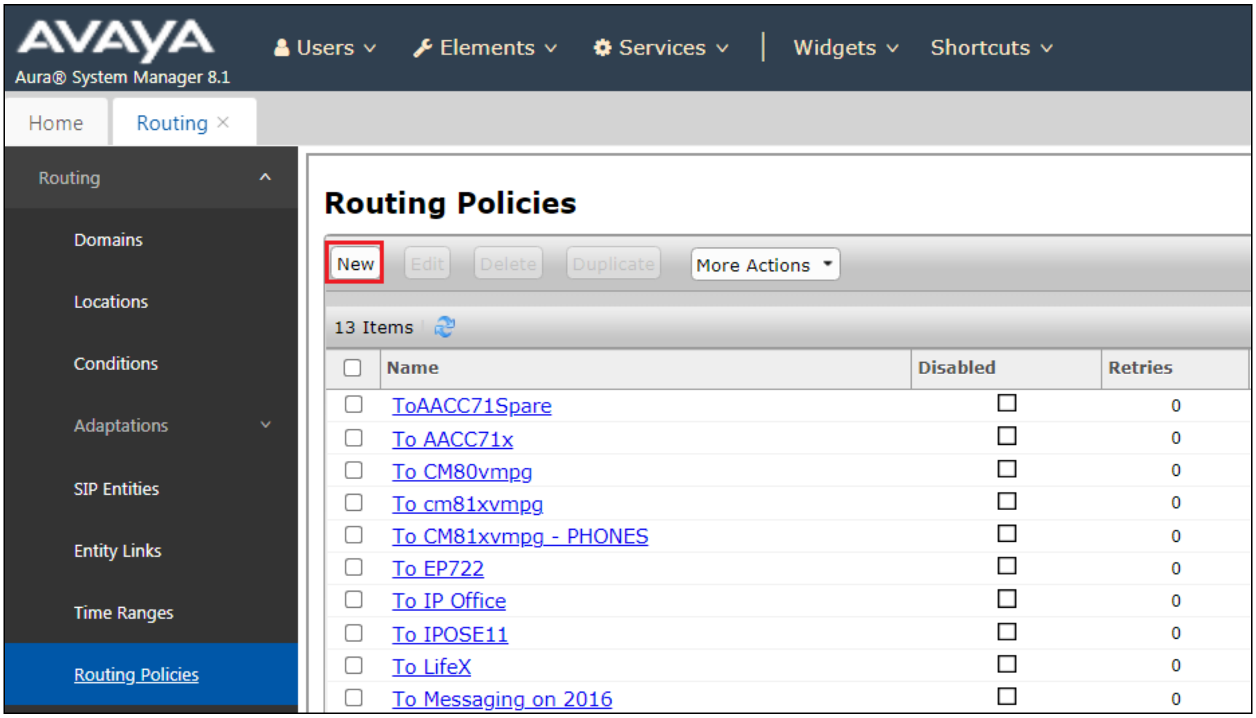
An Entity Link can be added from the same page, by scrolling down to **Entity Links**.

Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created LifeX 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 LifeX. Click on **Commit** once finished to save the new Entity Link and SIP Entity.

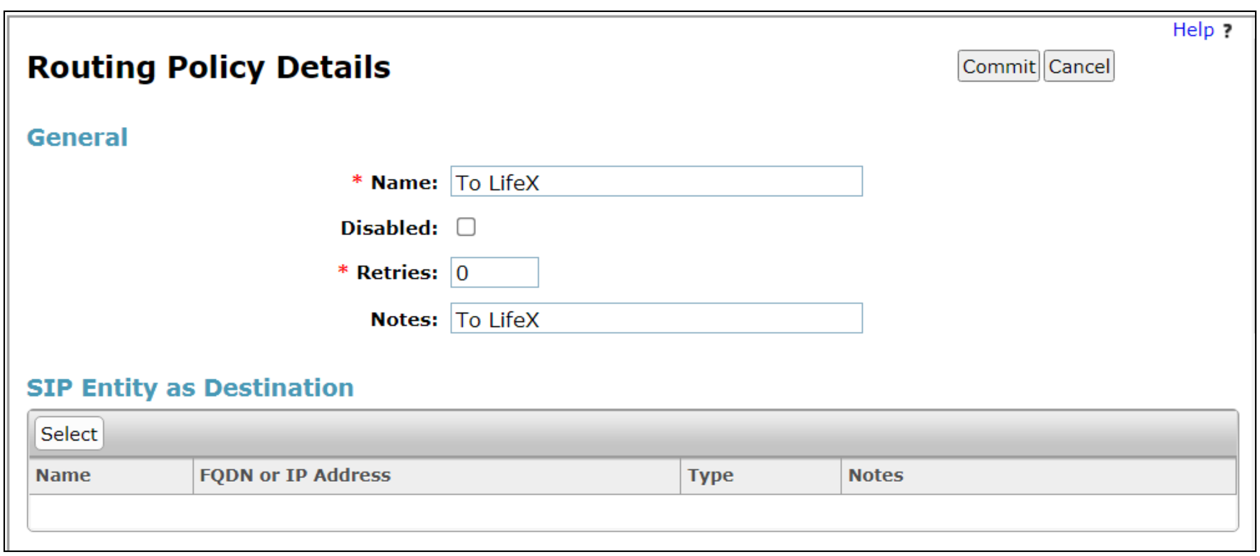


6.4. Adding a Routing Policy for Frequentis LifeX

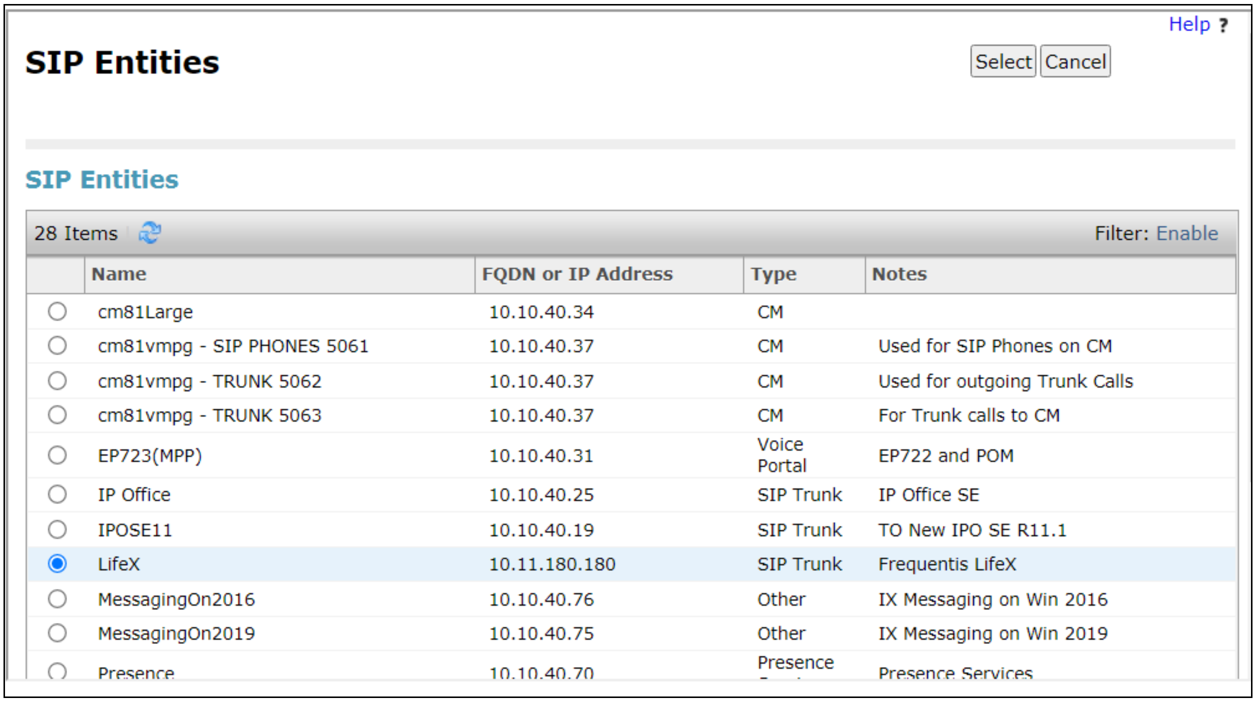
Click on **Routing Policies** in the left window and select **New** in the main window.



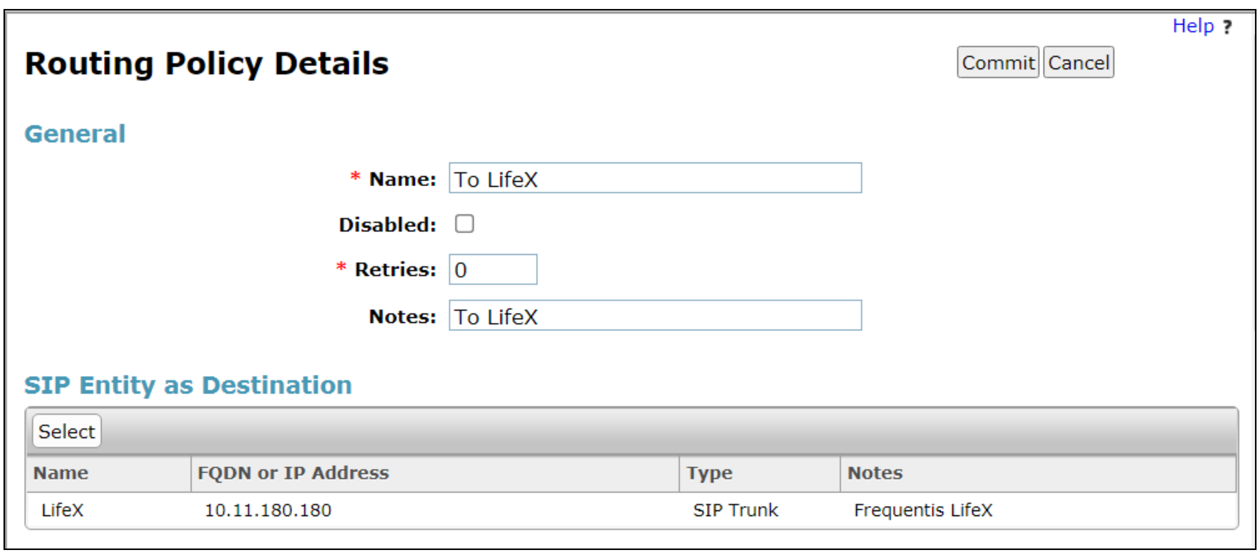
Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**.



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

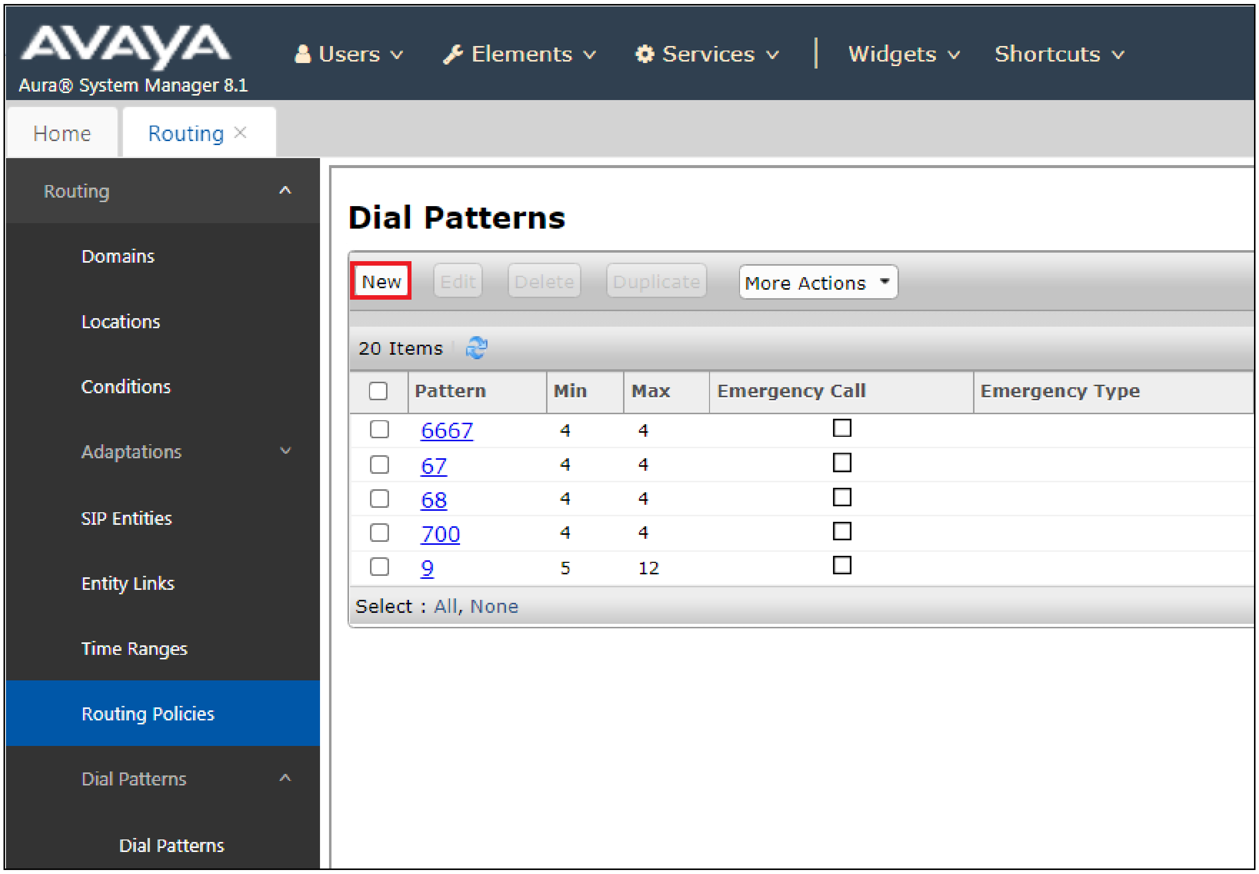


The selected destination is now shown, click on **Commit** to save this.

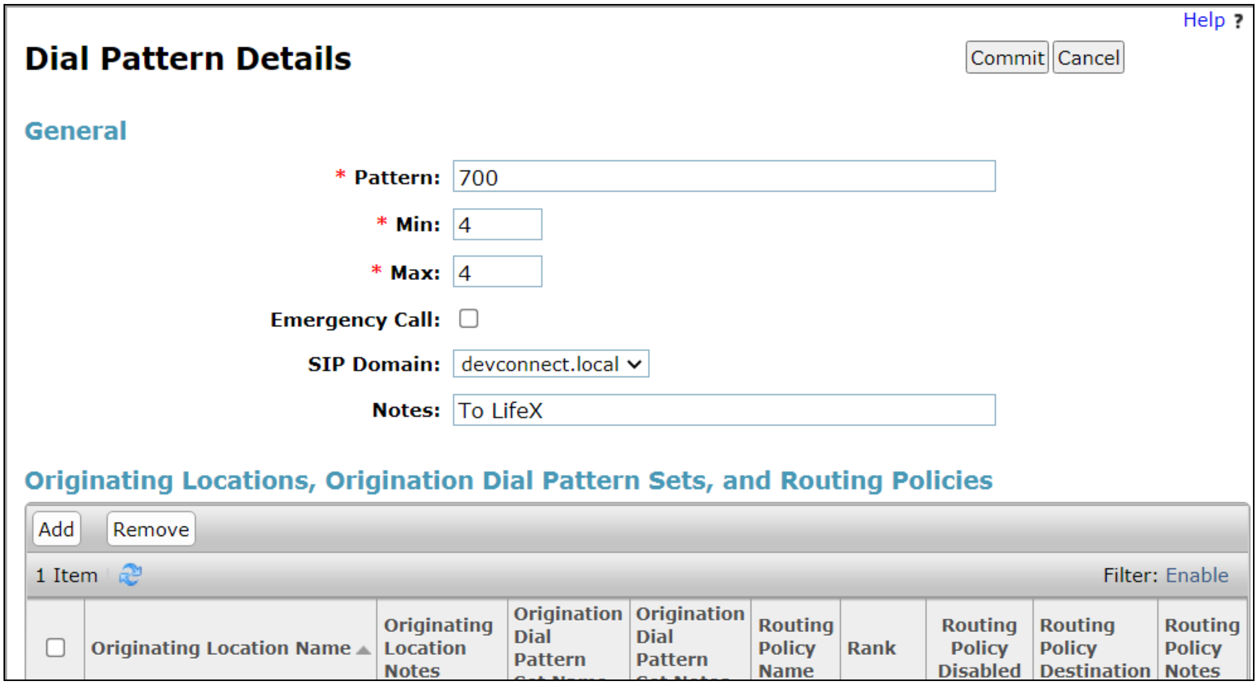


6.5. Adding a Dial Pattern for Frequentis LifeX

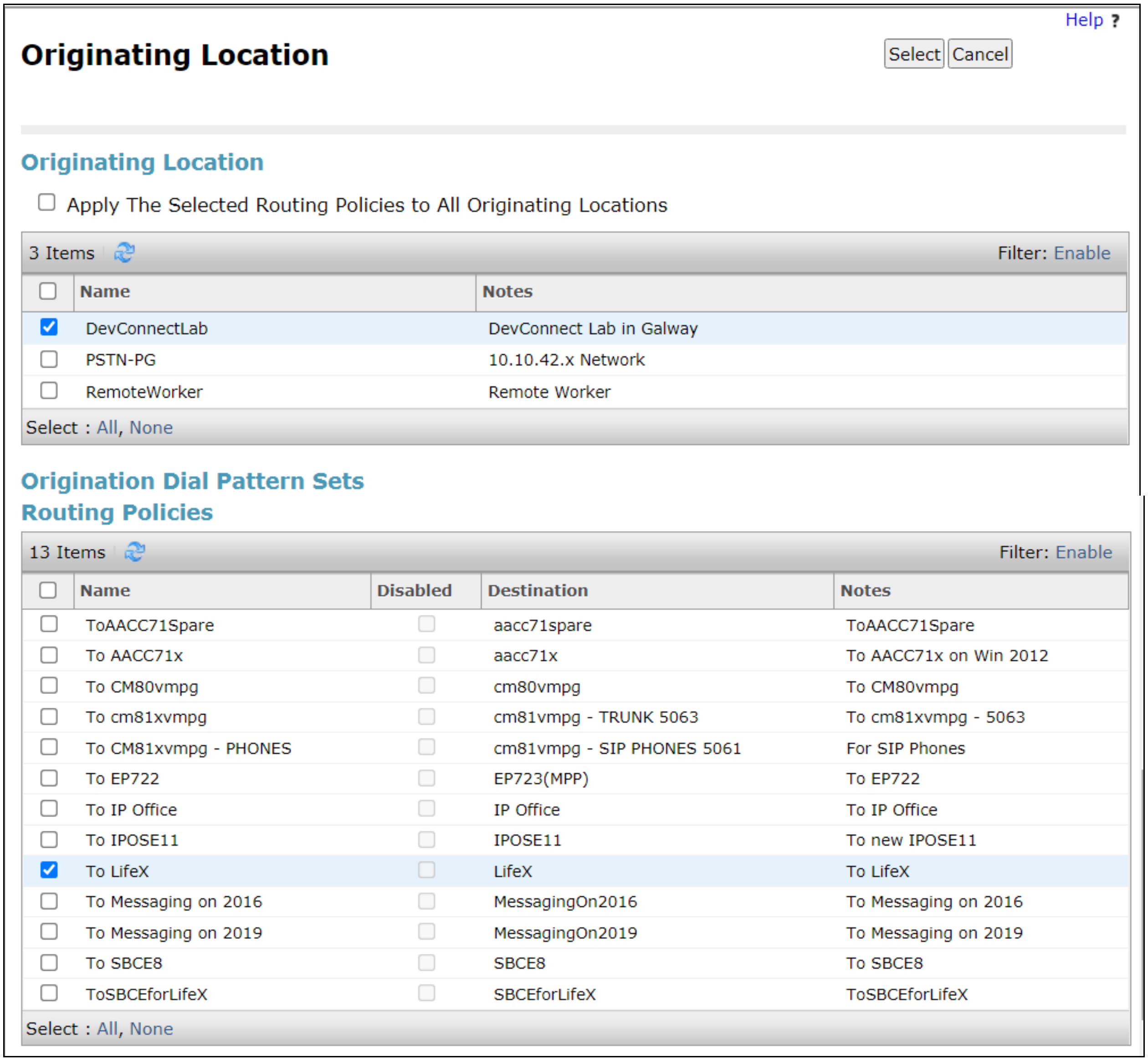
Select **Dial Patterns** in the left window and select **New** in the main window.



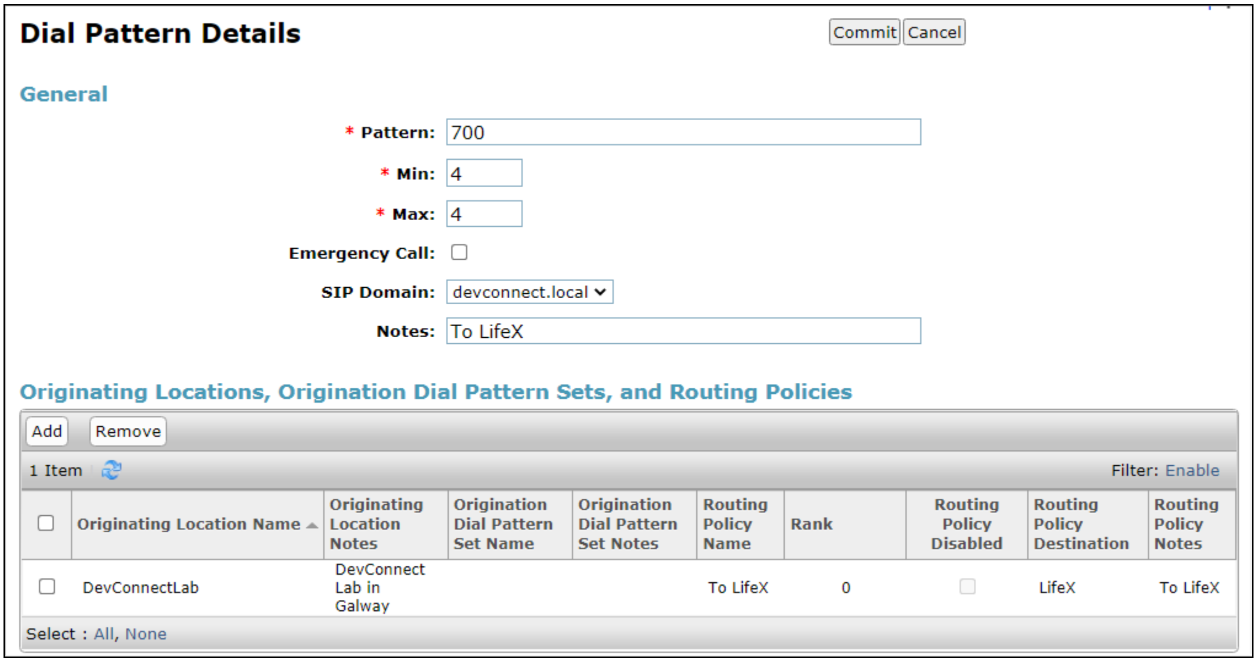
Enter the required digits for the Pattern, in the example below 700 is used, which means that 7000 – 7009 will use the Routing Policy that will be selected. **700** is entered as the **Pattern** and the **Min** and **Max** digit length of **4** is used thus giving 700x. Ensure that the correct domain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



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



7. 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 Avaya Aura® Session Manager directly.

7.1. LifeX 3020

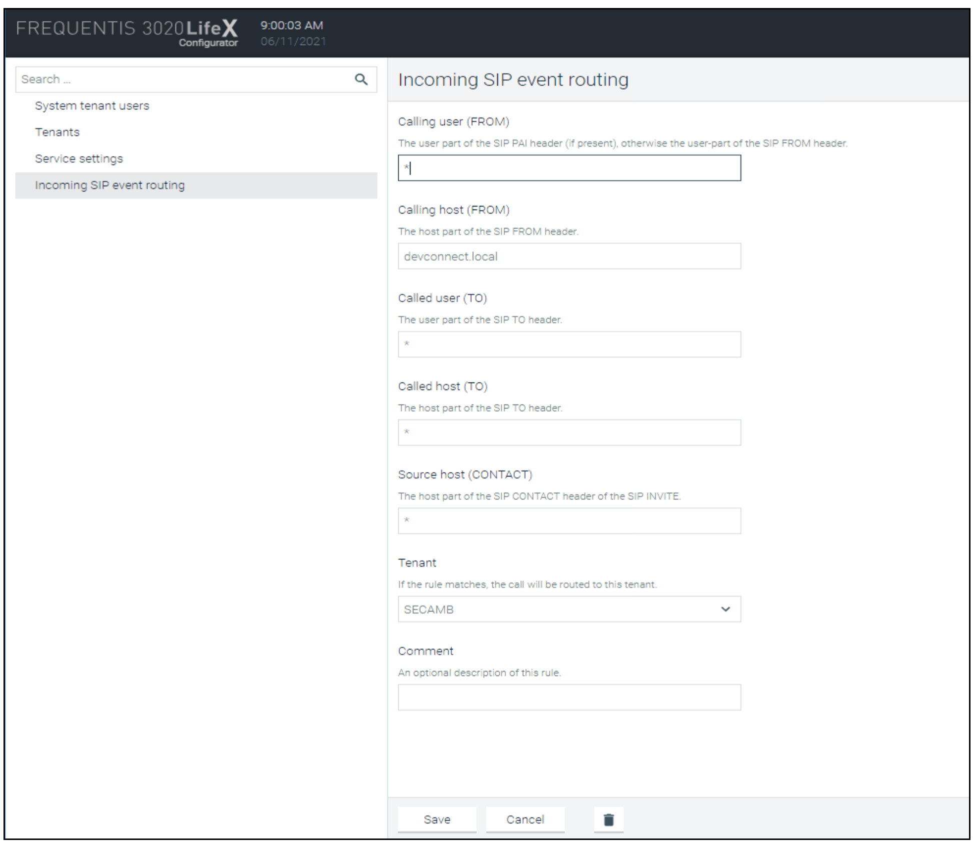
This section shows the steps necessary on the LifeX server to facilitate the connection to the Avaya Session Manager.

7.1.1. System Access

Access the LX 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…).

7.1.2. 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.

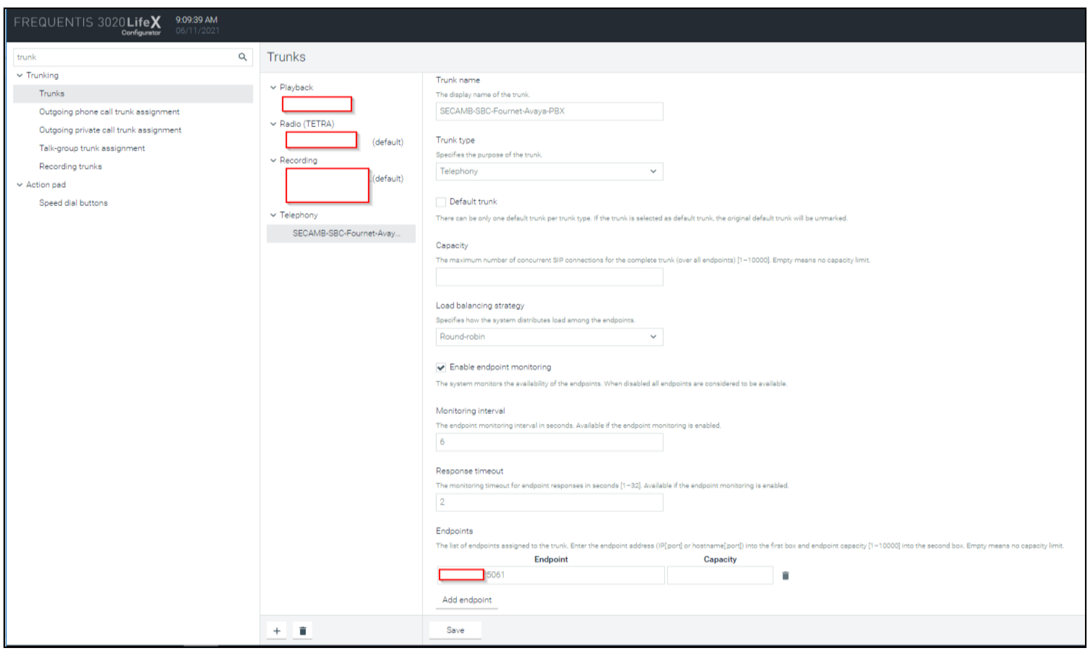


7.1.3. Outgoing calls configuration

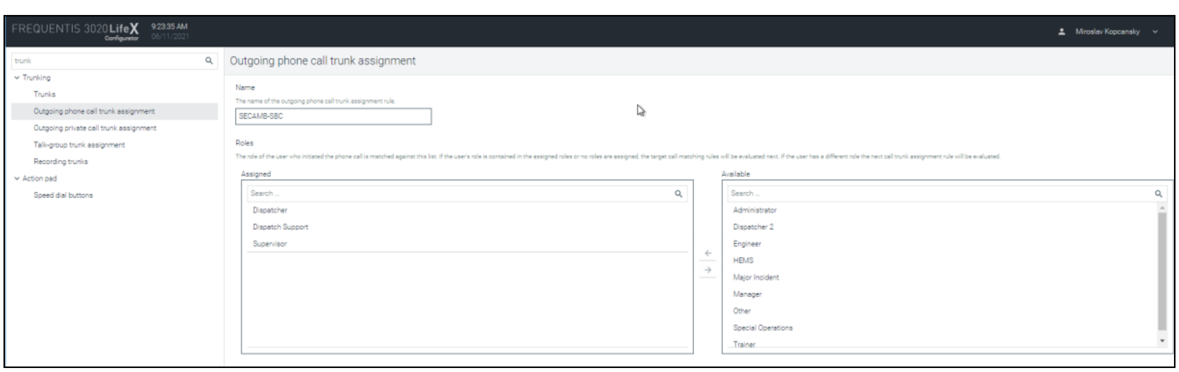
For outgoing calls configuration, specific site as <tenant name> was used, in this case SECAMB tenant was used.

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 7.2**.

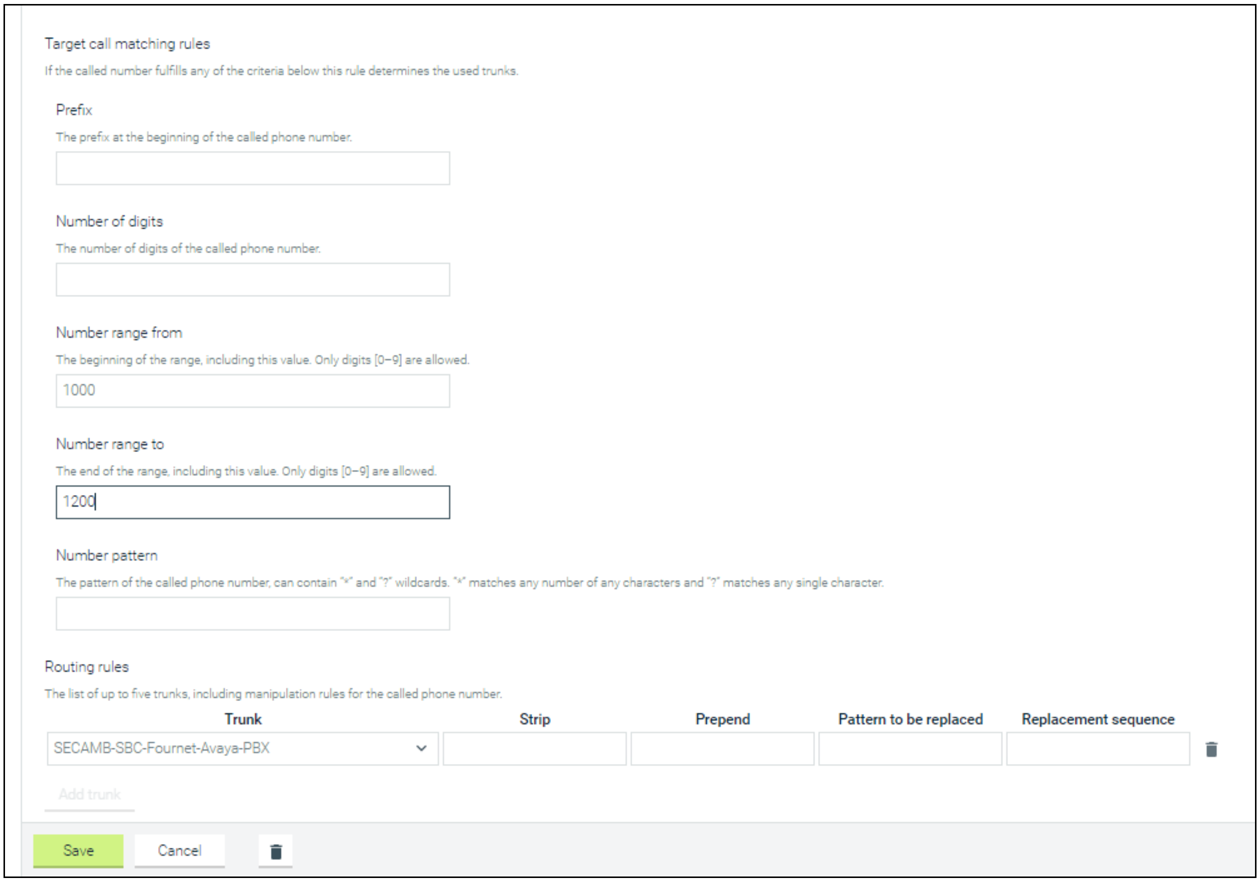
Note: Some sensitive information has been blocked out from some of the screen shots.



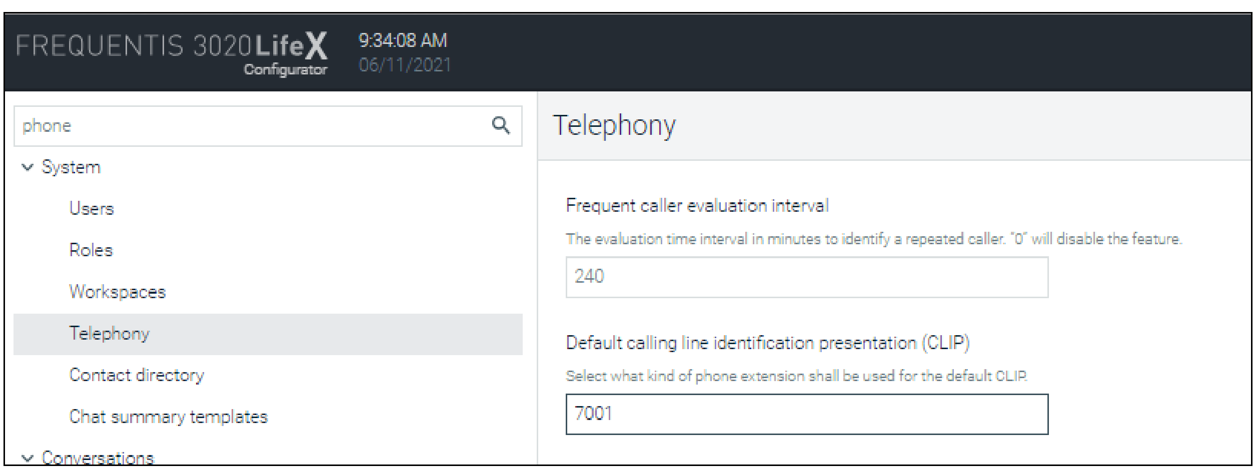
After trunk is created navigate to **Outgoing phone call trunk assignment** and click create new rule. **Name** the new rule and select to which LX Roles shoud be **Assigned**.



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.



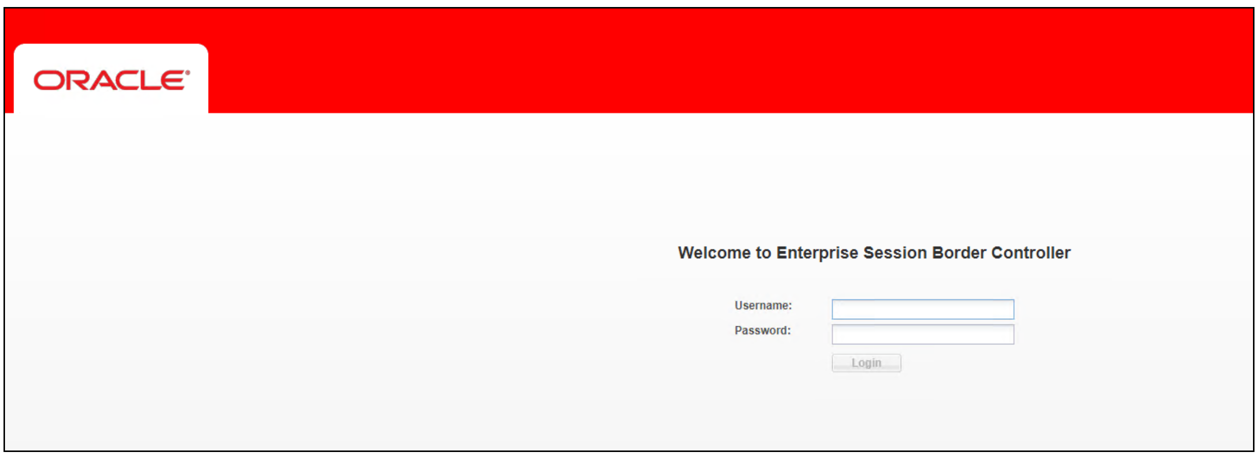
7.2. Oracle SBC-E

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.

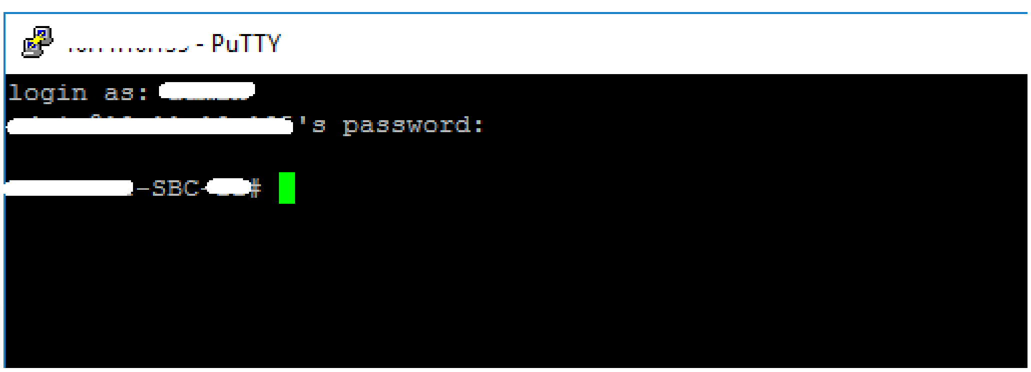
A **session border controller** (SBC) is a device regularly deployed in Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications.

7.2.1. System Access

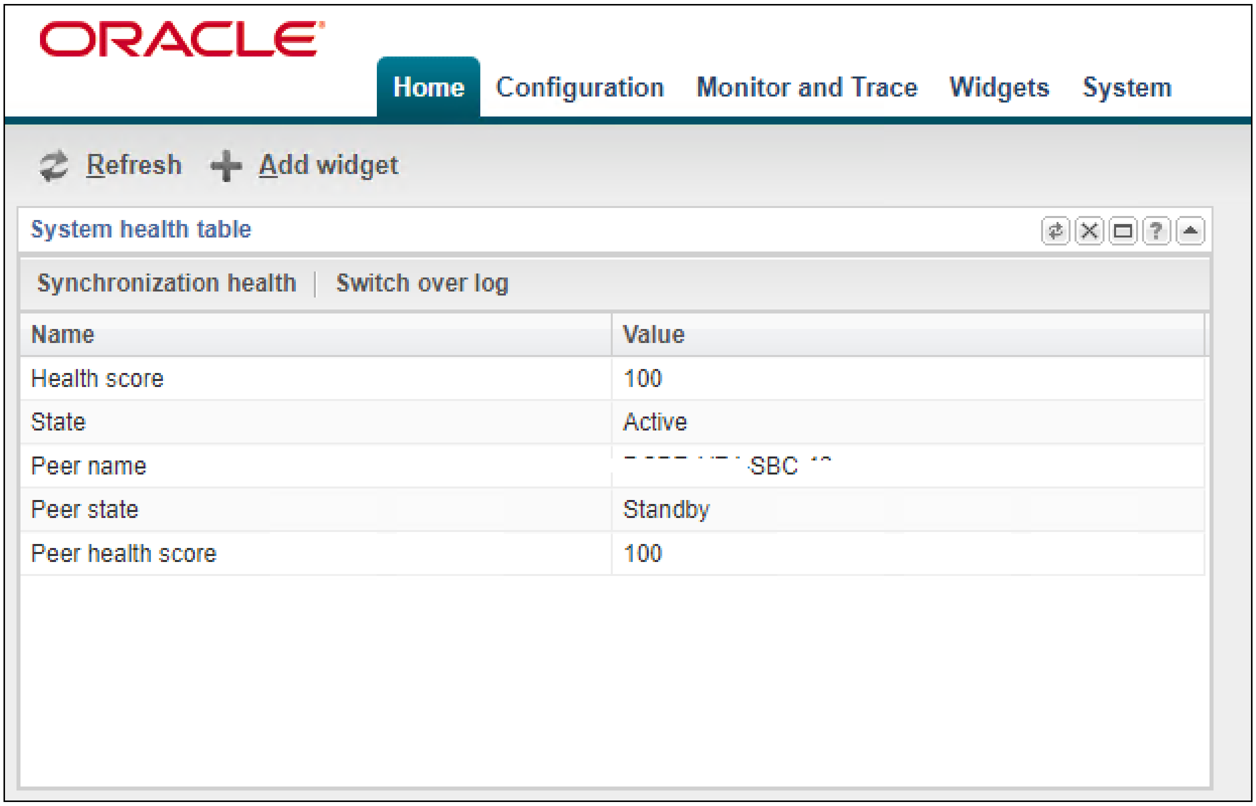
Access the Session Border Controller web management interface by using a web browser and entering the URL https://<ip-address>, where <ip-address> is the management IP address configured at installation. Also, the command line interface can be accessed using a ssh client i.e., “PuTTY”. Log in using the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



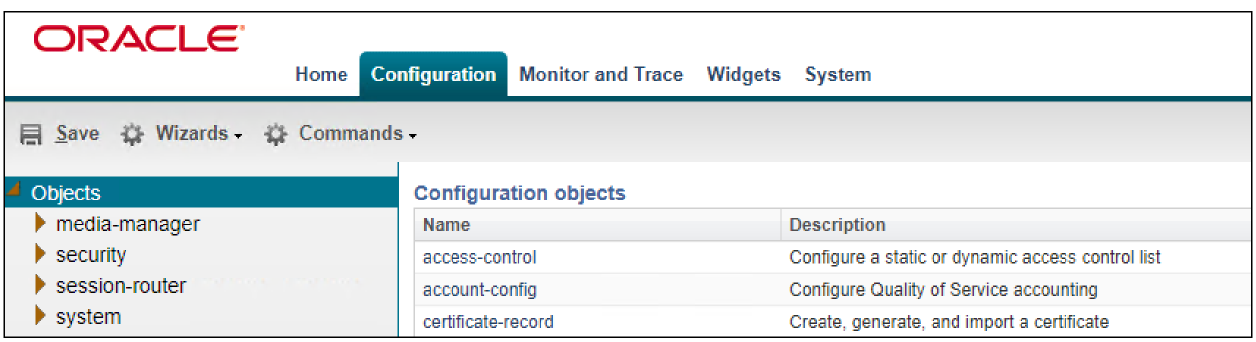
The screen shot below shows the interface using **PuTTY**.



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.



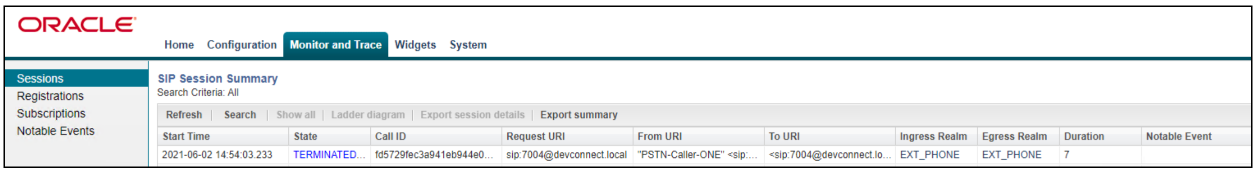
The **Configuration tab** provides a graphical display of the same objects and elements that can be accessed by CLI. Also, it provides some configuration Wizards and Commands.



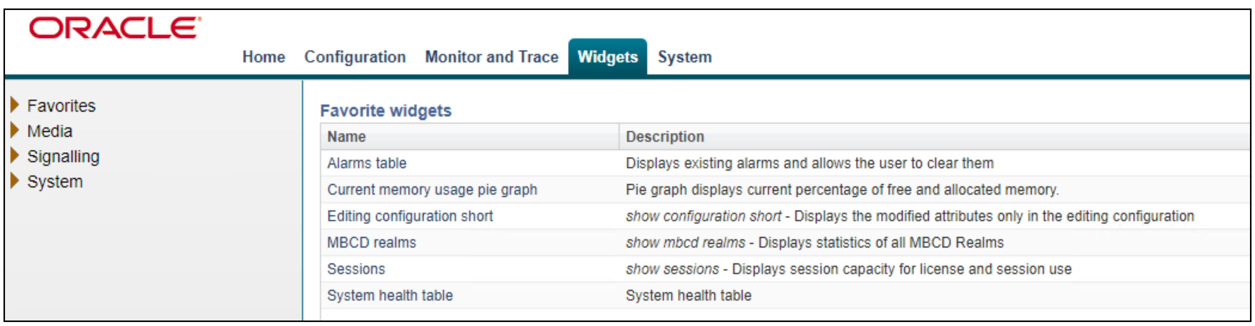
The **Monitor and Trace** tab displays the results of filtered SIP session data from the SBC. It supports the summary reports.

- **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 8.3.2**.

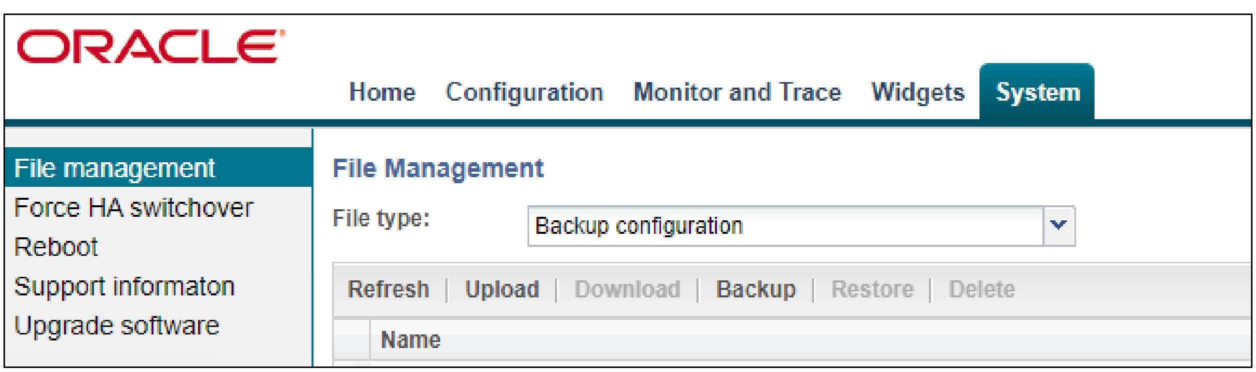


The **Widgets** tab contains a list of all available widgets that can be used to view system data and statistics. A **license** can be added here under **System → Licenses**.



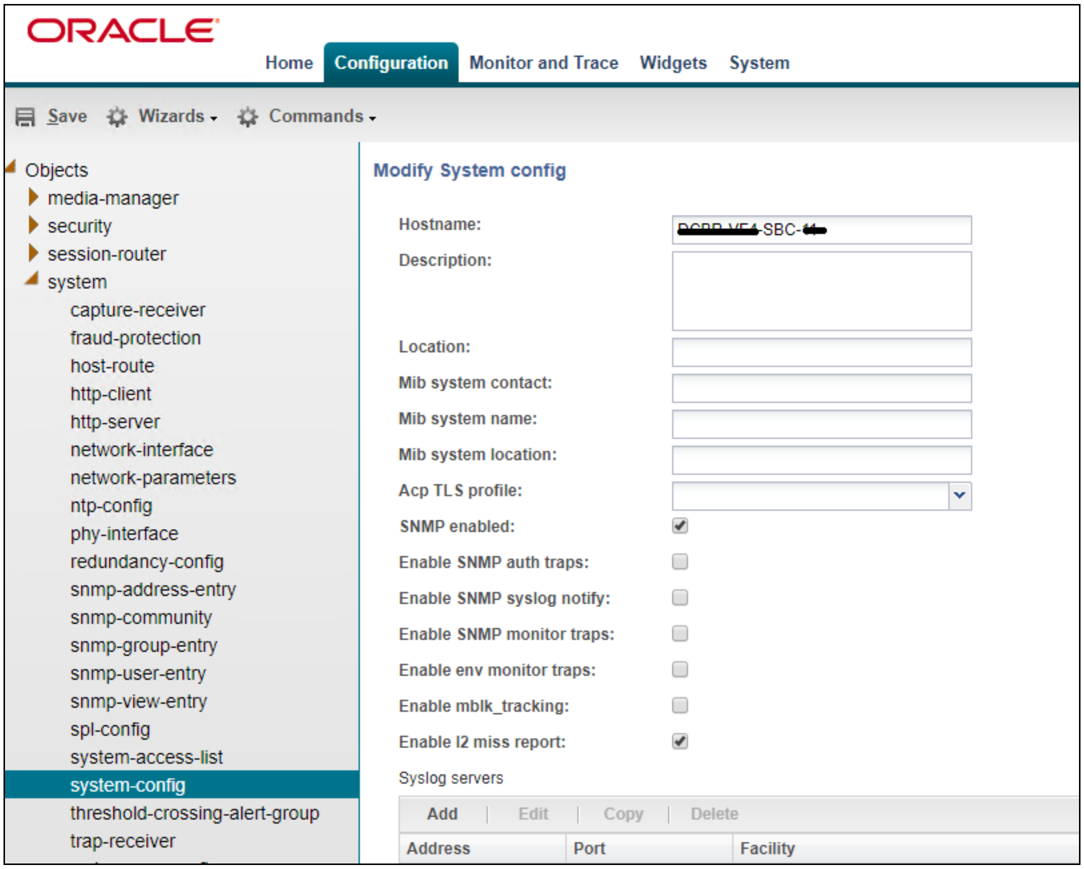
The System tab provides the following ways to manage files on the system.

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

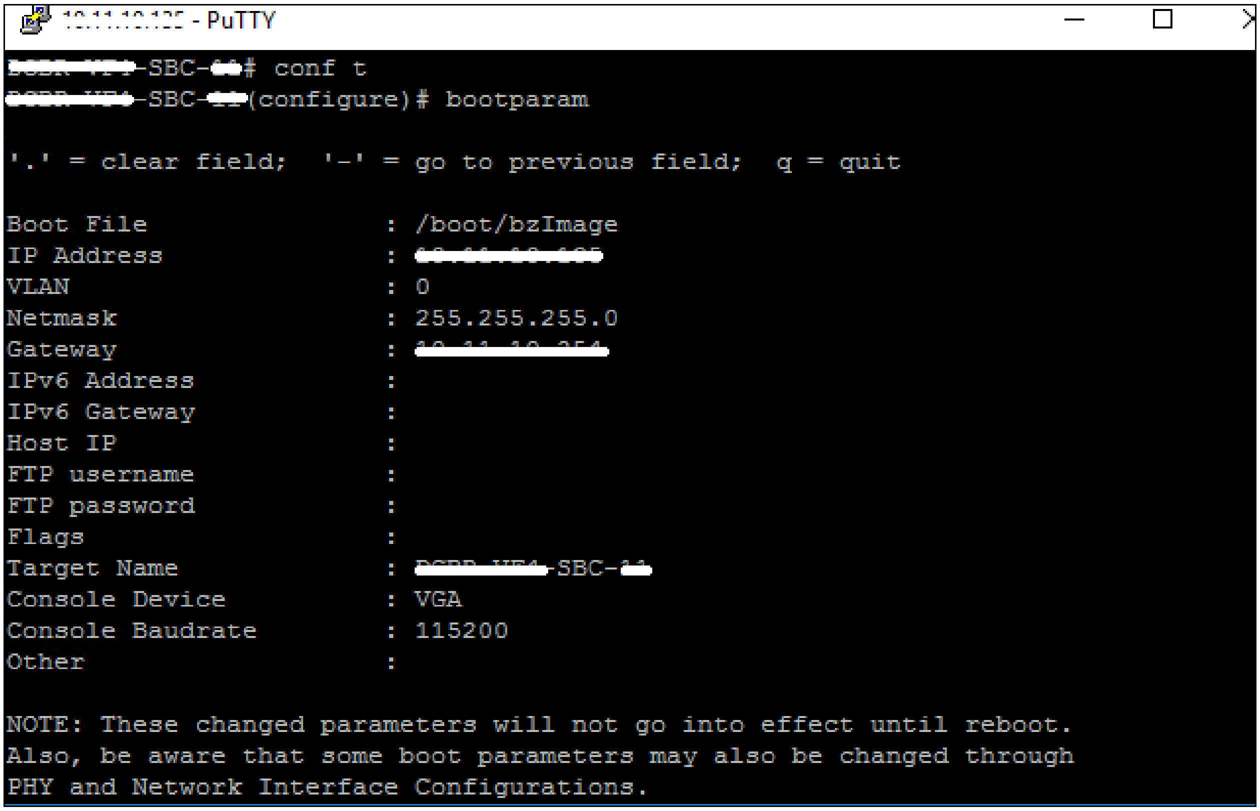


7.2.2. System configuration

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**.



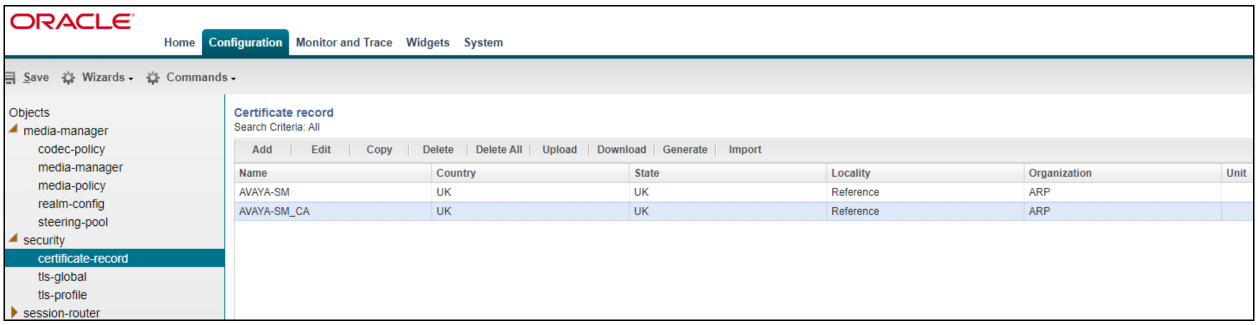
These commands can be run from the CLI command or, as displayed on the screen from the previous page, can be run from the GUI.

- **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

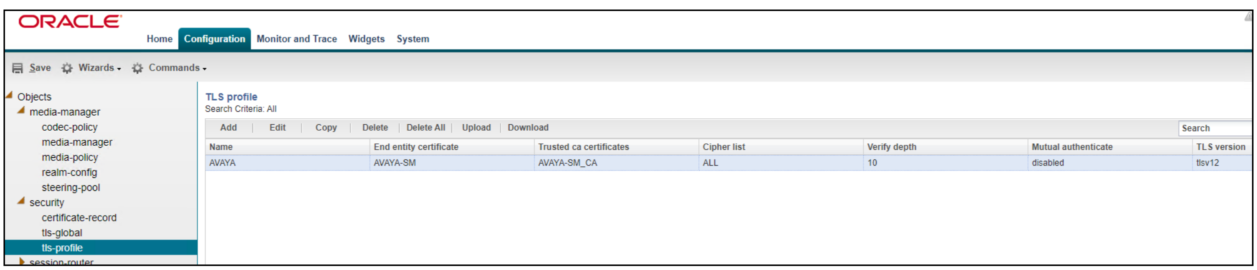
7.2.3. Security – TLS configuration

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 7.2.5**.

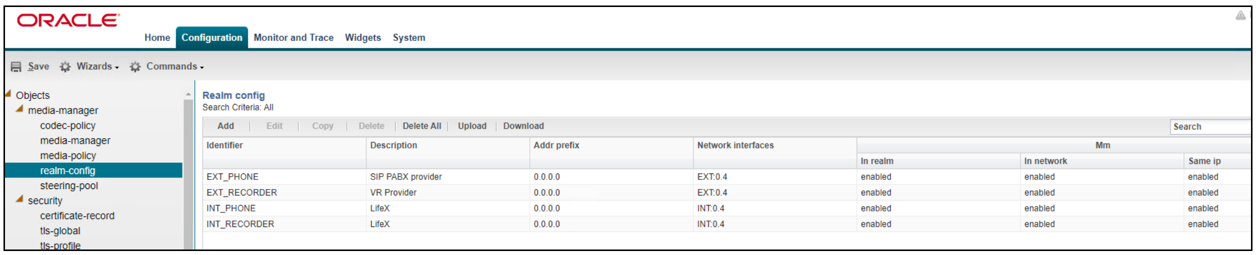


7.2.4. Media Manager – REALM Config

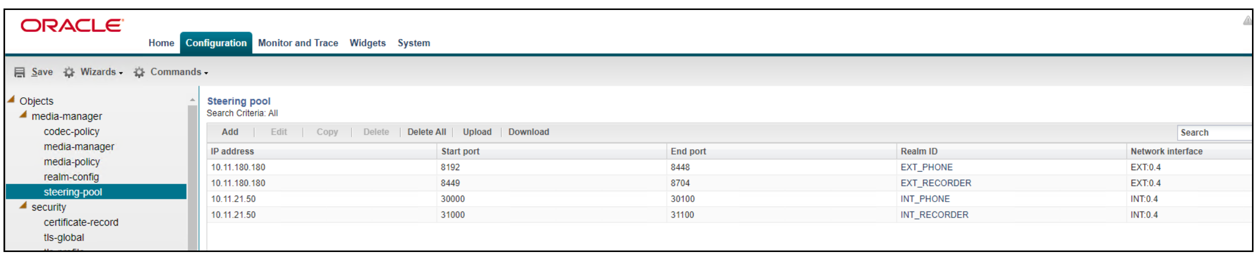
Realms are a logical distinction representing routes (or groups of routes) reachable by the SBC and what kinds of resources and special functions apply to those routes. A **REALM** must be seen as an “area” / “territory” / “region”. It may include multiple session agents and / or SIP interfaces.

There are four realms created, two for LifeX (using the network interface for internal media flow described in **Section 7.2.2.**) and two for 3rd Party (using the network interface for external media flow described in **Section 7.2.2.**). 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.



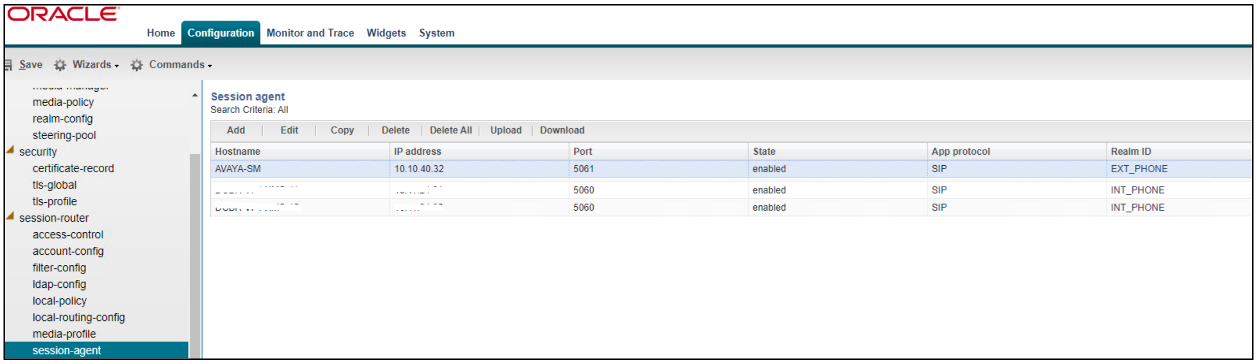
7.2.5. Session Router

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.

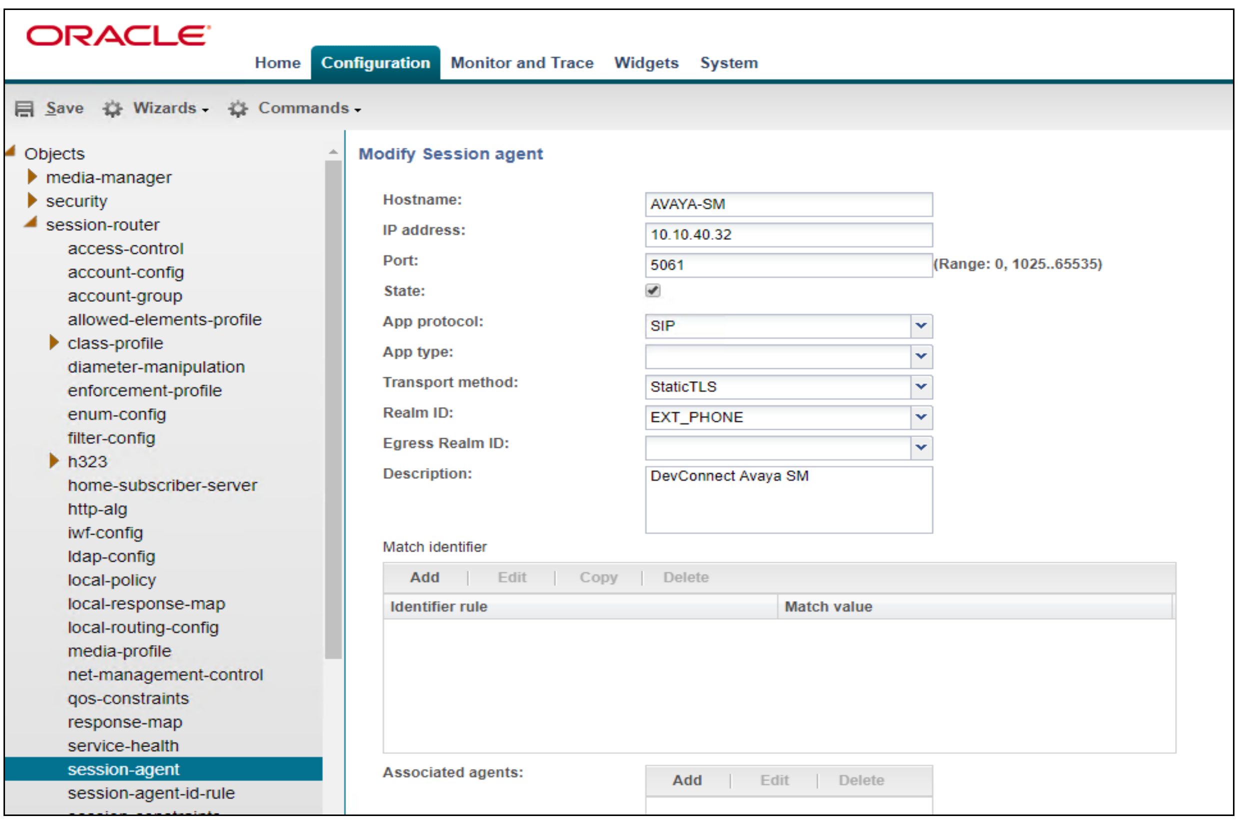
SIP agents are created to specify the IP addresses and ports in which the SBC-E will listen for signalling traffic in the connected networks. SIP agent defines a signalling endpoint.

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 Session Manager with the **IP address** set to that of the Session Manager. Clicking on this will open the window at the bottom of the screen where some further details can be observed.

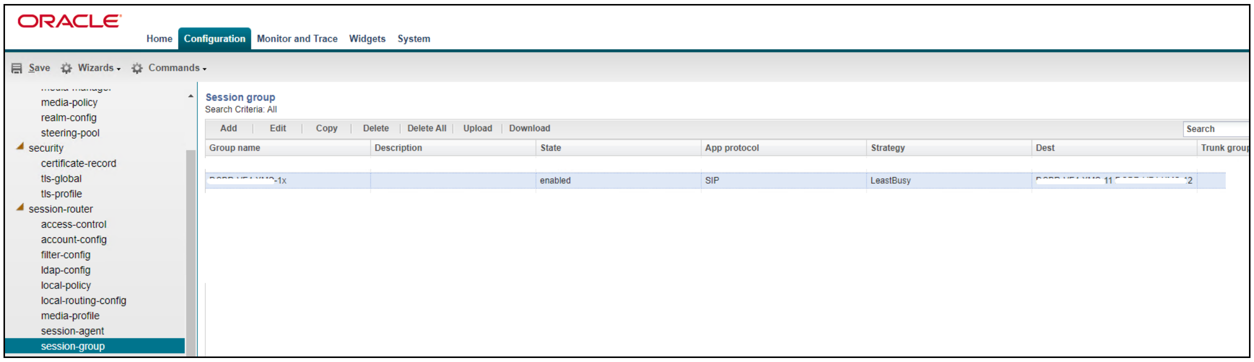


A suitable name if given for Session Manager with the **IP address** set to that of Session Manager which is **10.10.40.32**, the **Realm ID** is set to **EXT_PHONE**, with the **Port** set to **5061**. The **Transport method** is set to **StaticTLS**.

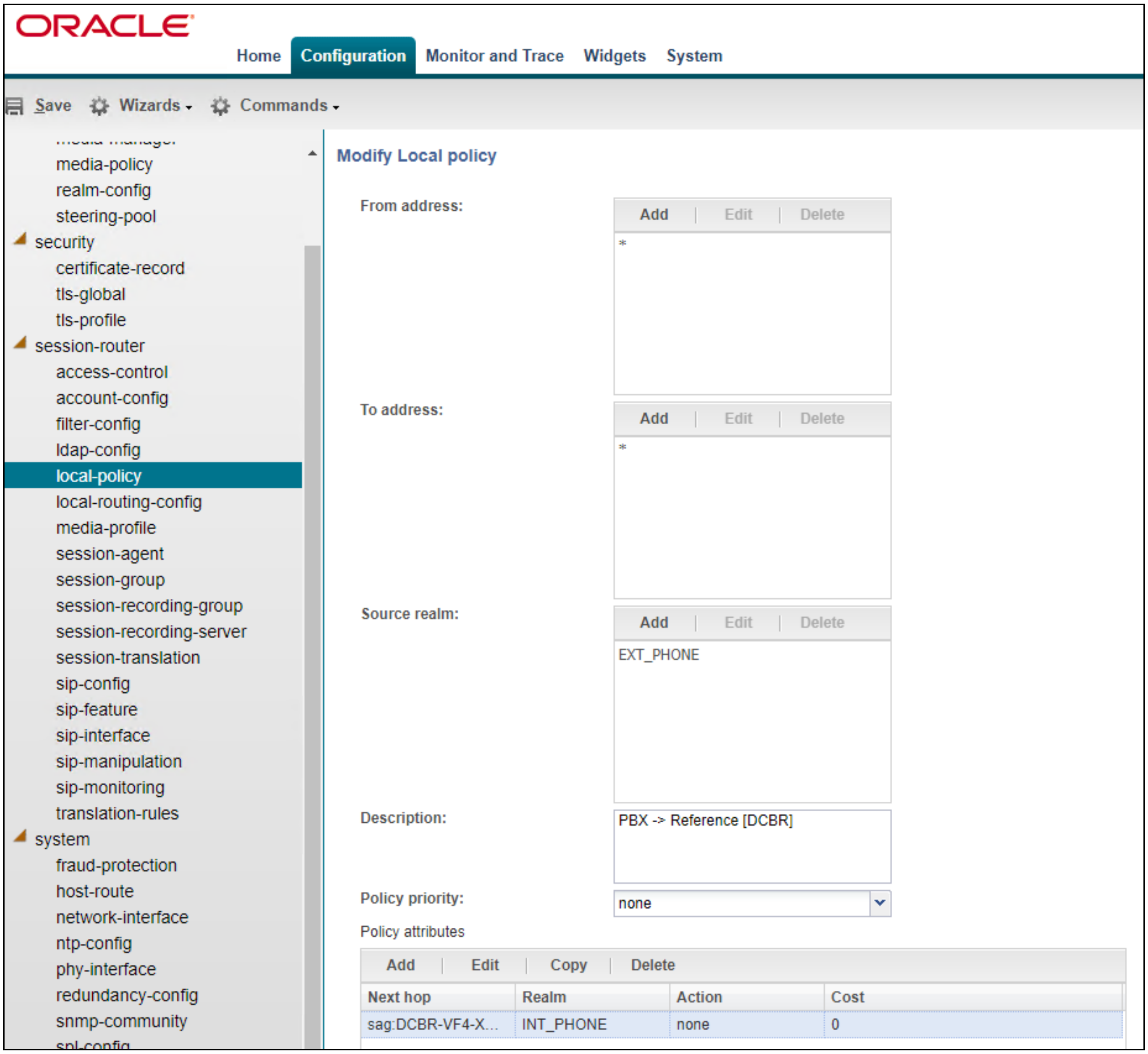


A **Session-group** includes the session agents of both media servers from the LifeX testing environment. Session agent group (SAG) contains individual session agents. Members of a SAG are logically equivalent (although they might vary in their individual constraints) and can be used interchangeably. 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 **Objects→session-router→session-group** in the left window.



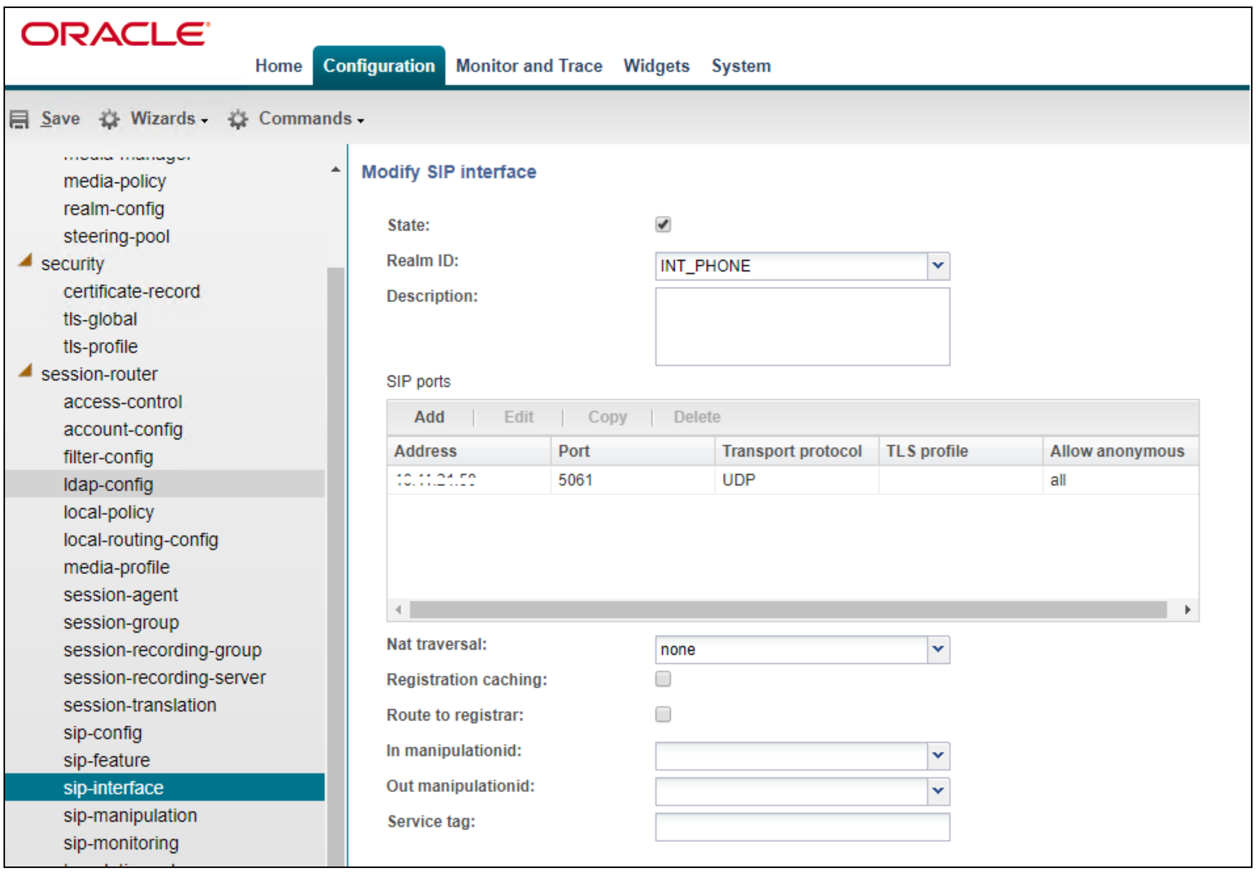
Local policy indicates where session request messages, such as SIP INVITES, are routed and/or forwarded. A local policy can be used to set a preference for selecting one route over another. For the Avaya Realm "EXT_PHONE", there is set the policy to forward all calls from 3rd party to any number of LifeX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



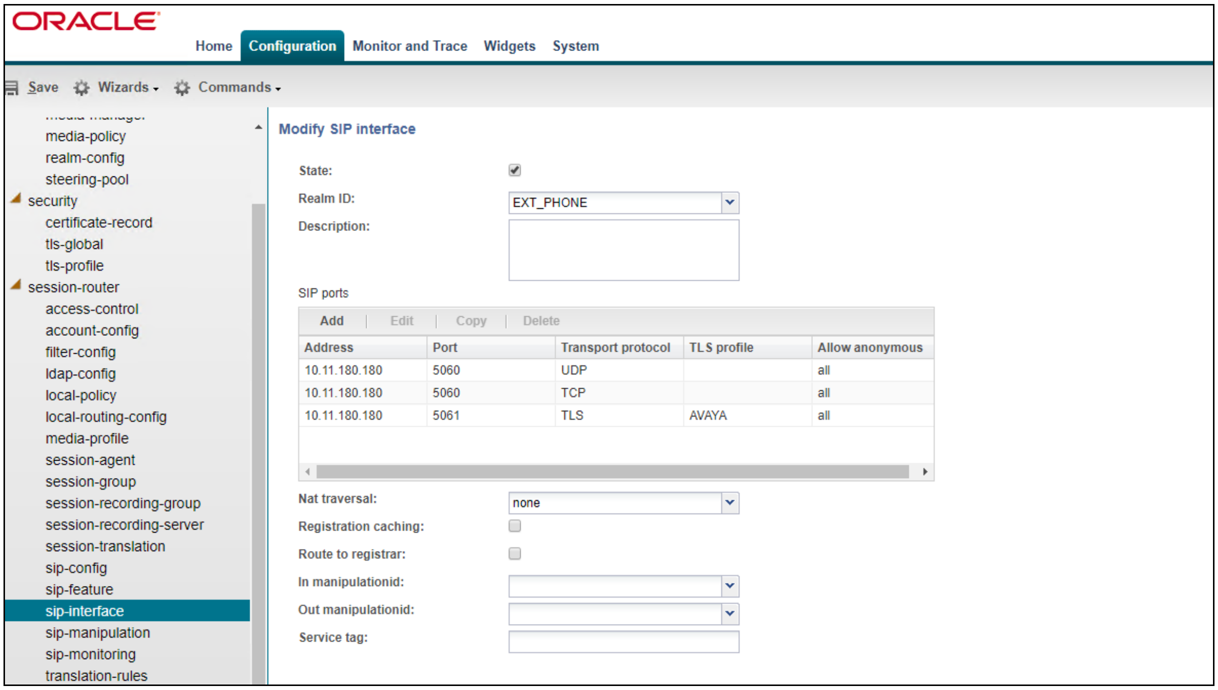
SIP interface defines the transport sockets (IP address and port) upon which the SBC receives and sends SIP messages. SIP interfaces support UDP/TCP/TLS/SCTP Stream Control Transmission Protocol (SCTP) transport, as well as multiple SIP ports. A SIP interface can be defined for each network or realm 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, in the case Session Manager. These are added as TCP and TLS as described in **Section 7.2.3**.

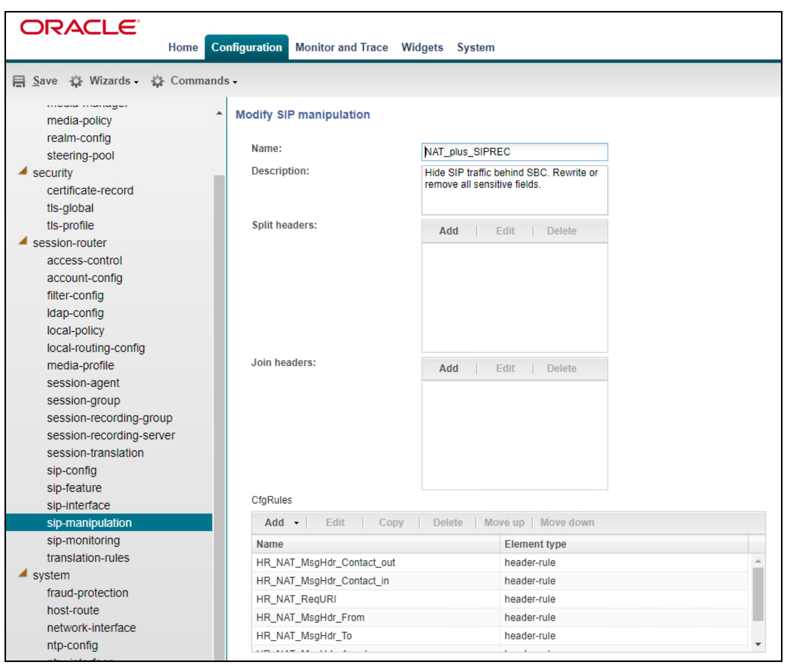
The **INT_PHONE** sip interface is shown below. Frequentis use port 5061 with UDP transport for communication between LifeX and the Oracle SBC.



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.

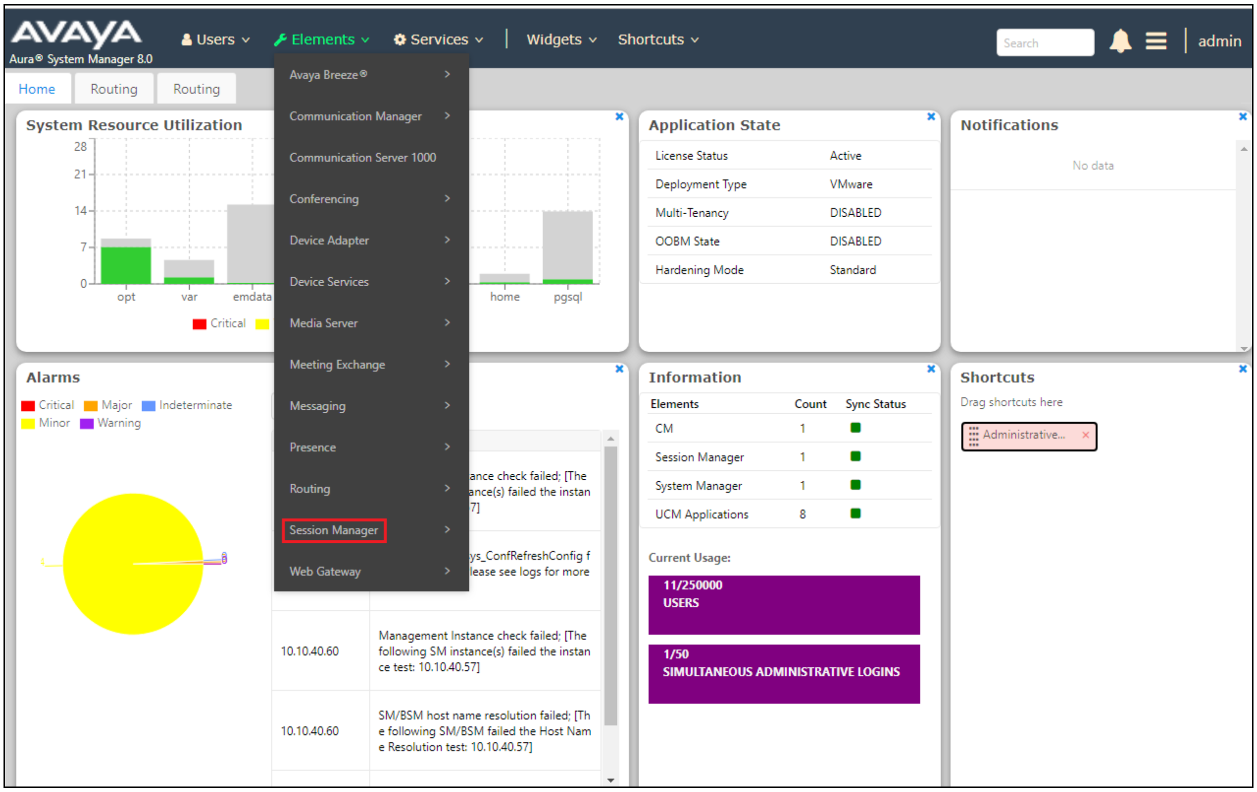


8. Verification Steps

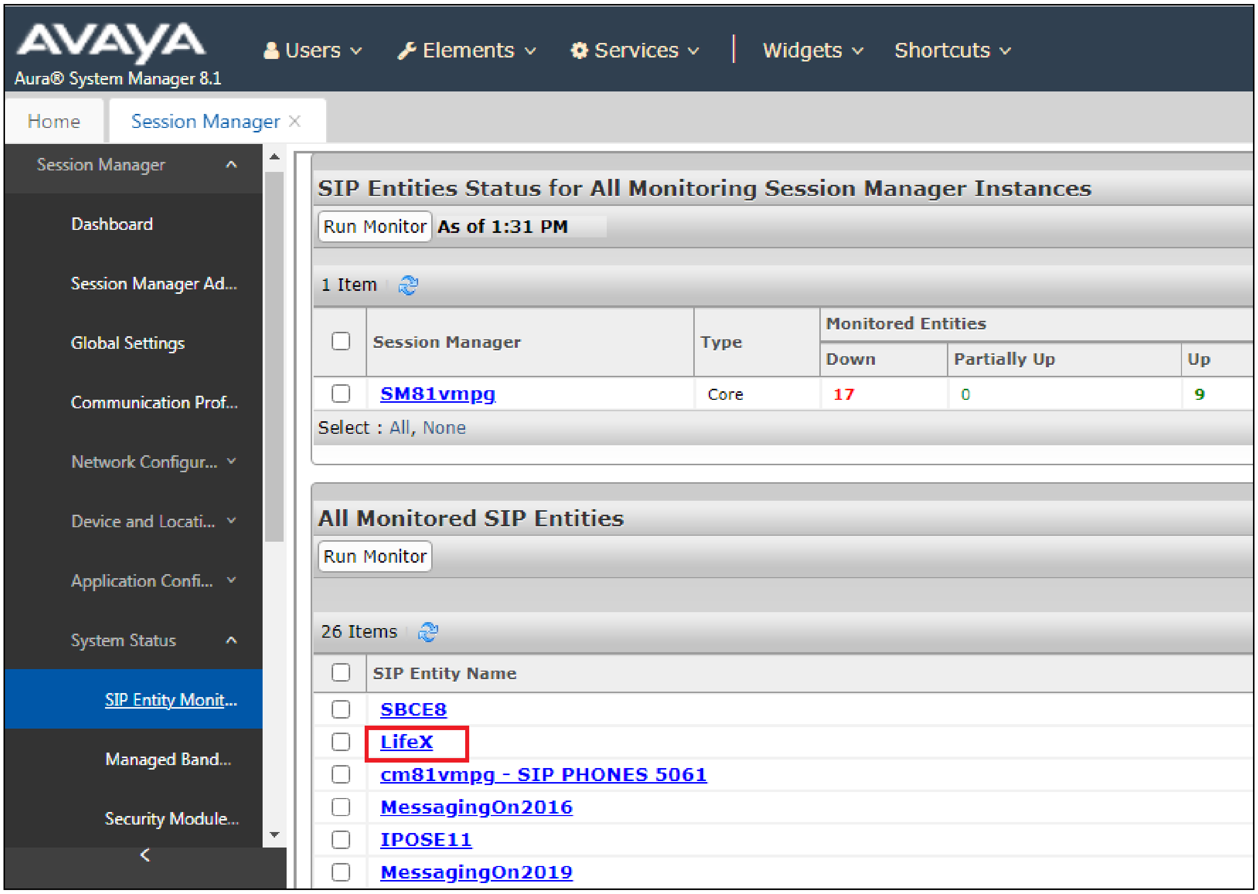
The following steps can be taken to ensure that connections between the Avaya platform and the Frequentis platform successfully in place.

8.1. Session Manager Registration

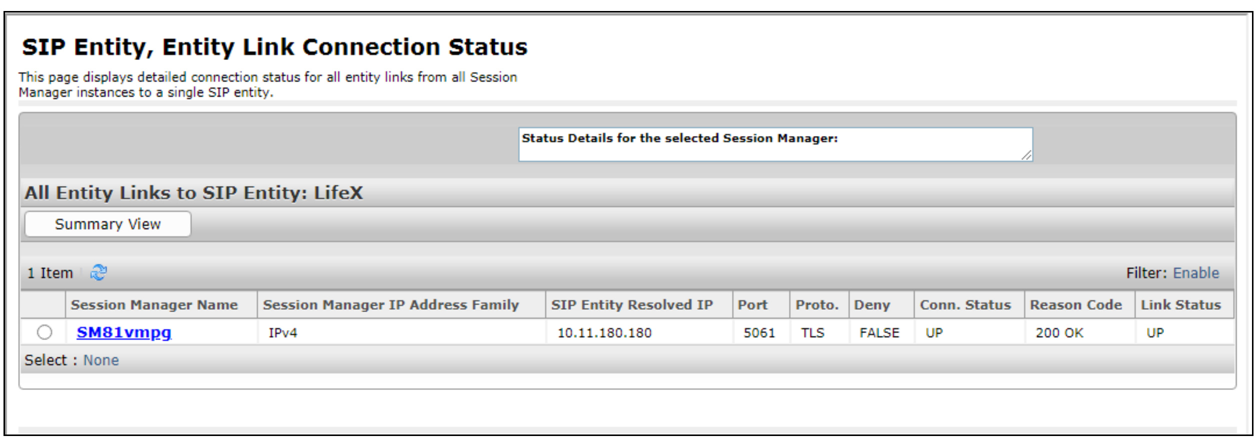
Log into System Manager as per **Section 6**. Navigate to **Elements** and click on **Session Manager**.



Select the **LifeX** SIP Entity.

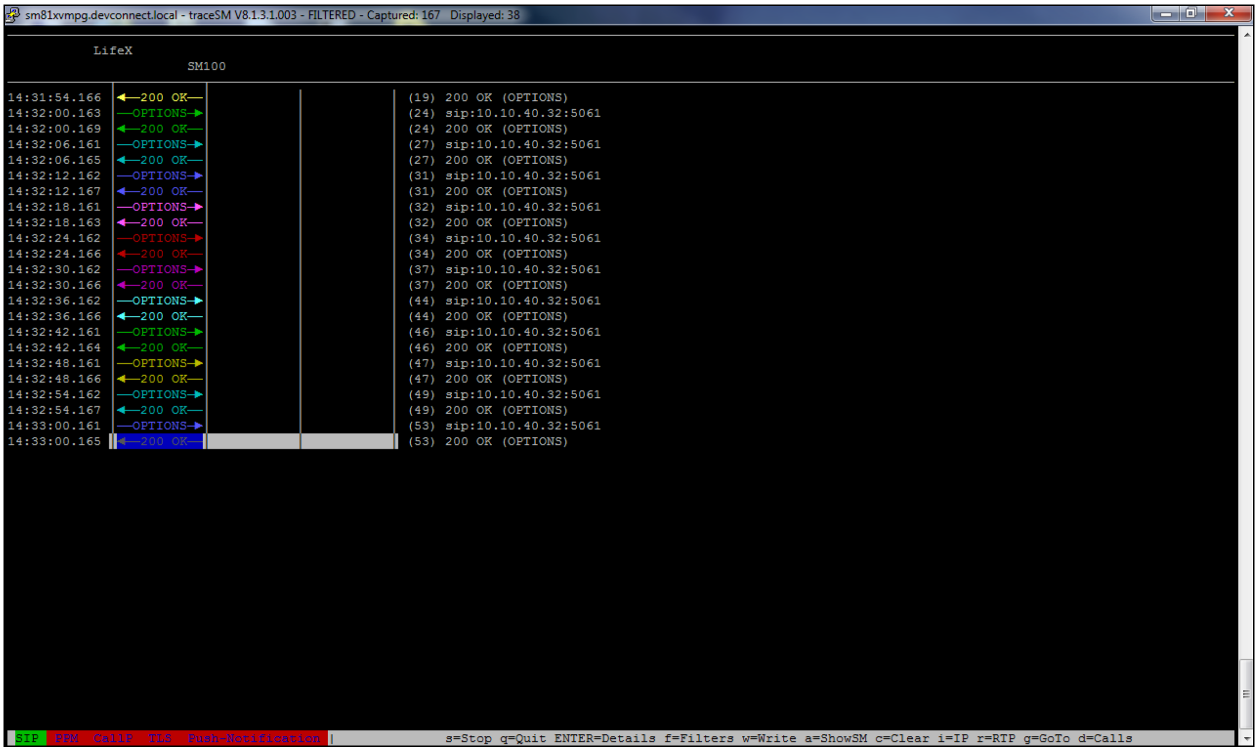


The SIP Entity should show as **UP** as it is shown below. The example below shows the **TLS** connection which was used during compliance testing.



8.2. Observe the connection using the Avaya Aura® Session Manager traceSM tool

By opening PuTTY and connecting to Session Manager, a **traceSM** tool can be run by typing in traceSM, 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.



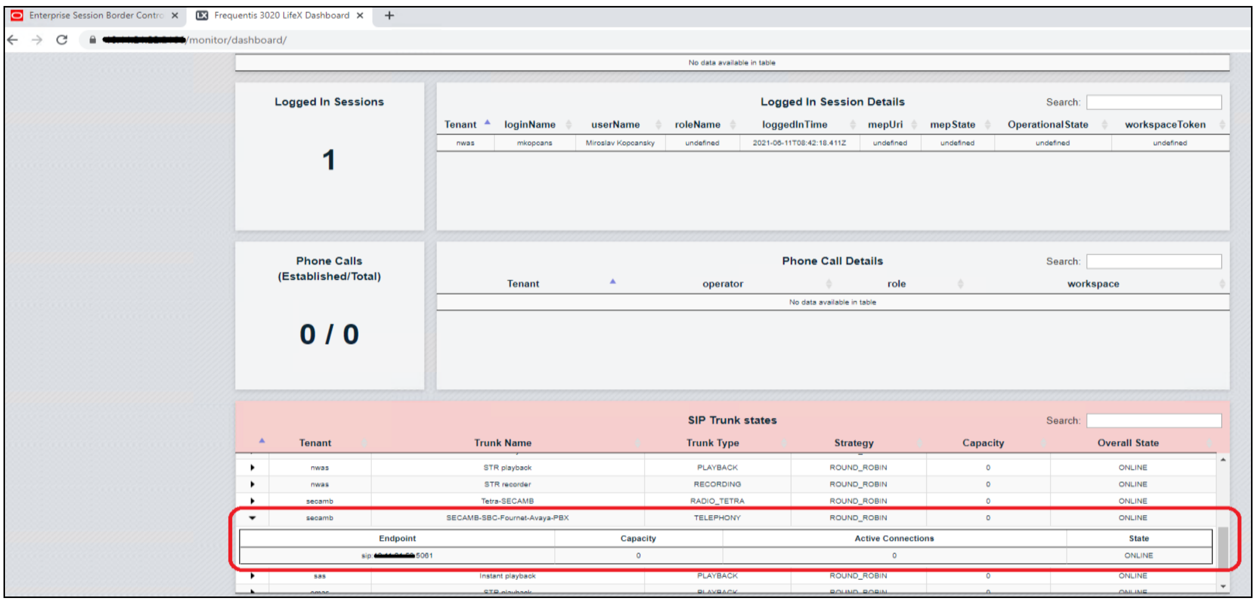
8.3. Verify LifeX

This section is showing the steps that can be taken to show how to verify the connection from the LifeX side.

8.3.1. Frequentis LifeX

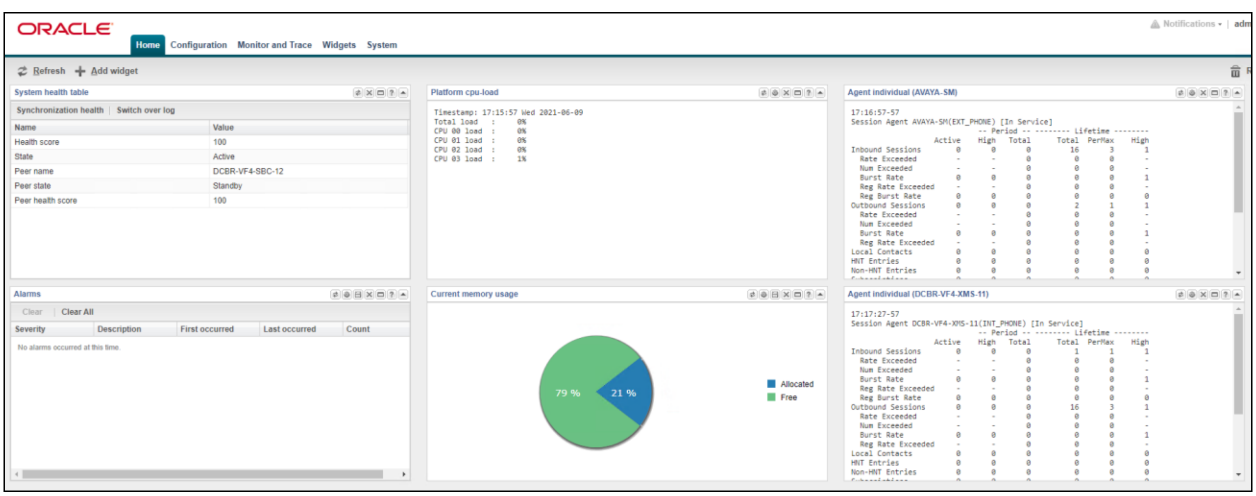
To verify a SIP trunk (**SBC**), access the LifeX dashboard webpage by using https://<IP_address>:<port>/**monitor/dashboard**/ where IP is the business main server of LifeX reference environment and port is the monitoring service running on it.

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

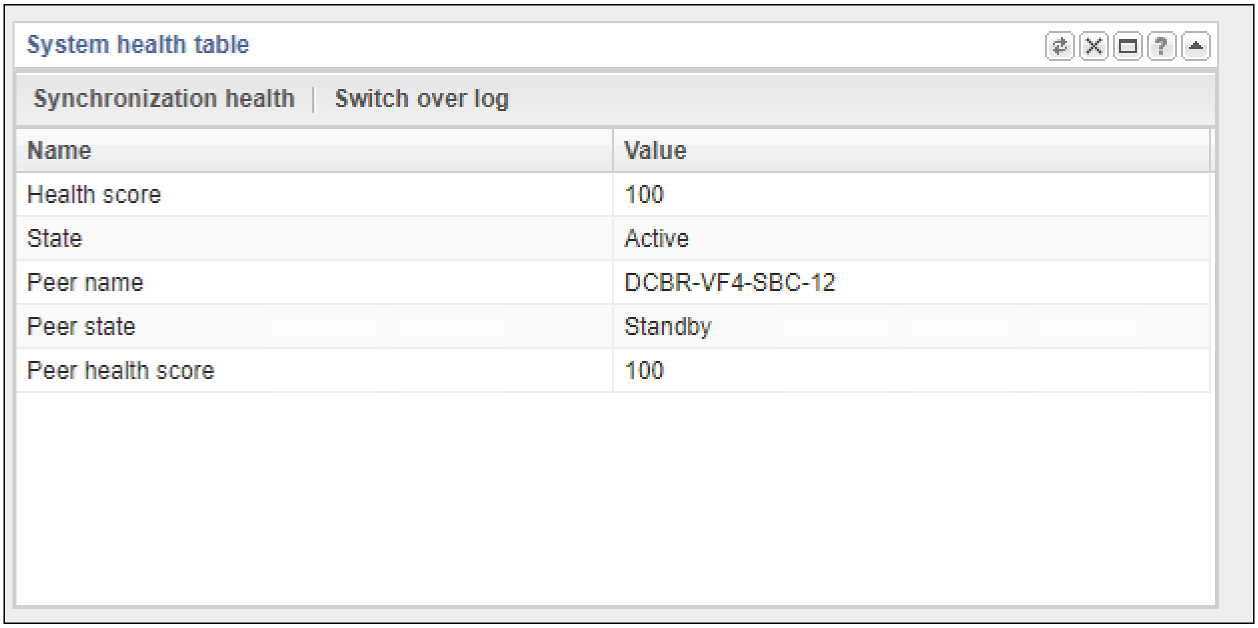


8.3.2. Frequentis Oracle SBC

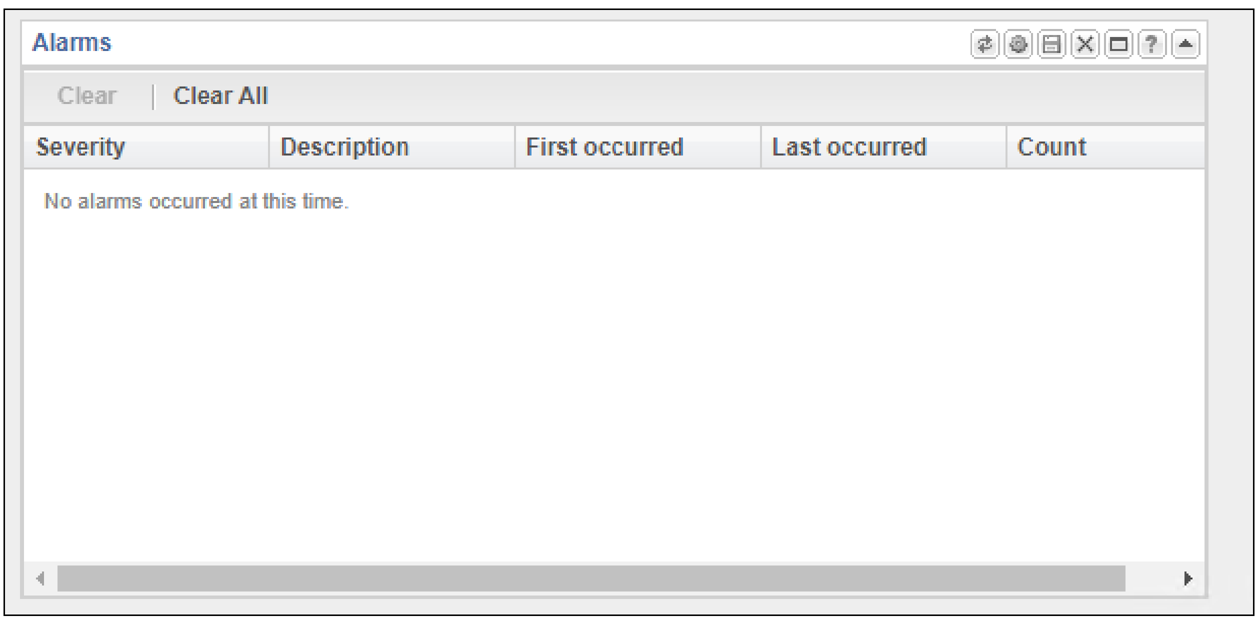
From the Oracle SBC, on the **Home** tab, widgets can be added dedicated for monitoring.



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

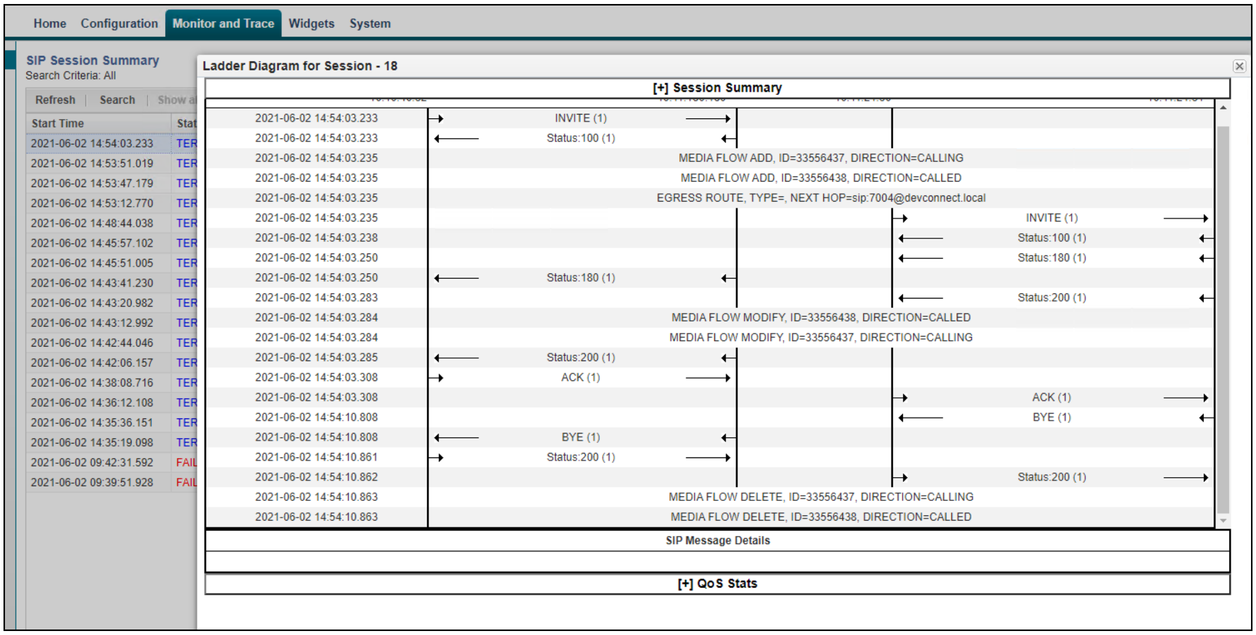
```
Timestamp: 17:15:57 Wed 2021-06-09
Total load   :      0%
CPU 00 load  :      0%
CPU 01 load  :      0%
CPU 02 load  :      0%
CPU 03 load  :      1%
```

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.



9. 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 using a direct connection to Avaya Aura® Session Manager. Please refer to **Section 2.2** for test results and observations.

10. 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 and Updating Avaya Aura® Media Server Appliance*, Release 8.0.x, Issue 11, October 2020.
[8] *Implementing and Administering Avaya Aura® Media Server*. Release 8.0.x, Issue 11, October 2020.
[9] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[10] *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.