Avaya Solution & Interoperability Test Lab

Application Notes for Semafone Voice+ Rushmore 5.0 with Avaya Session Border Controller for Enterprise 8.1 and Avaya Aura® Environment 8.1.2 - Issue 1.0

Abstract

These Application Notes contain instructions for Semafone Voice+ Rushmore 5.0 with Avaya Session Border Controller for Enterprise 8.1 and Avaya Aura® Environment 8.1.2 to successfully interoperate. Semafone Voice+ extracts DTMF tones entered by the caller from SIP signaling and replaces them with a generic tone for a call center agent to hear. The extracted DTMF tones can then be sent to a payment platform for processing.

Readers should pay particular attention to the scope of testing as outlined in **Section 2.1**, as well as 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

Semafone's Voice+ Rushmore is a solution that allows data to be captured securely over the telephone from an end customer for credit card payments or other services. Semafone Voice+ Rushmore can be used as an appliance with on premises or cloud hybrid solutions. The Semafone solution in conjunction with Avaya Session Border Controller for Enterprise (ASBCE) enables DTMF tones delivered over a SIP trunk provided by a 3rd party service provider to be extracted and replaced with a generic DTMF tone. The DTMF tones captured can then be sent to a payment platform for processing; the agent hears only the replaced generic tone.

Rushmore is deployed so that media can remain local to the Avaya SBCE, when the CCM is hosted in a Semafone, Partner or Customer Data Center, so the CCM and SIG5 become geographically separated. The Rushmore SED and SIG5 are deployed together on a Semafone managed server. Rushmore is then deployed locally to the ASBCE. Rushmore is connected back to a hosted CCM to access all of Semafone's core services.

The Semafone Voice+ Rushmore solution has four server components:

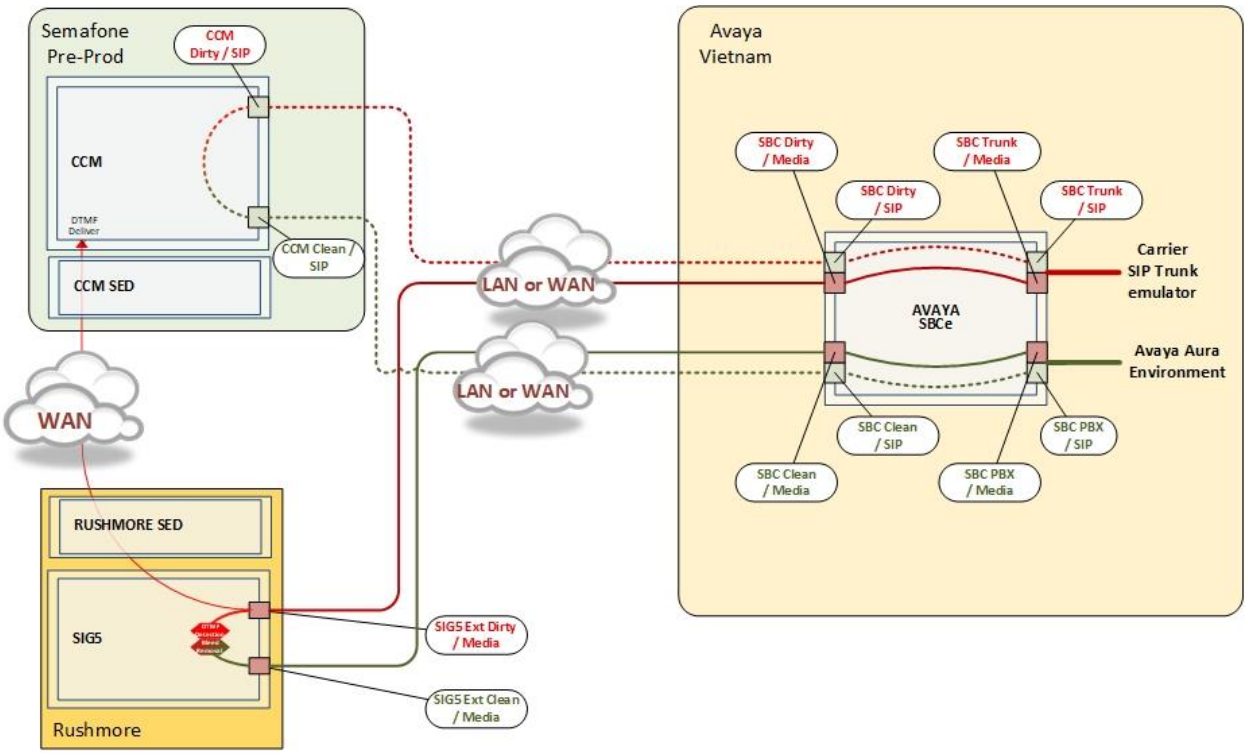
- CCM: At the core site this is a SIP Proxy that will be connecting to the ASBCE via SIP trunk. ASBCE will redirect incoming CC calls to the CCM.
- CCM SED: At the core site this provides logs and audit trail.
- Rushmore: Has 2 components, SIG5 and Security Edge Device (SED). SIG5 Media processing server anchors the calls and keeps the call nailed up throughout its duration. The SIG5 then proxies the call back to ASBCE to be routed into the enterprise CC environment. DTMF capture occurs on the SIG5 when triggered by the agent. SIG5 substitutes the tones so that the agent (and call recorder) only hear a series of 1's. Rushmore SED is a soft firewall internal to Semafone. With the Rushmore architecture the SED on both sides protect the CCM and SIG5.
- DPM: At the core site this processes the actual credit card transactions based on DTMF capture from the SIG5. Also provides CRM matching and agent information via a web interface (should be integrated with Workspaces once the SDK's become available but does not presently integrate to Avaya).

These Application Notes contain instructions for Semafone's Voice+ Rushmore with Avaya Session Border Controller for Enterprise (Avaya SBCE) and Avaya Aura® environment to successfully interoperate.

The Avaya SBCE interacts with Semafone Voice+ Rushmore via 2 SIP Trunks: Dirty SIP Trunk and Clean SIP Trunk with call flow for Inbound and Outbound calls below:

- Inbound: Service Provider → SBC External Interface → SBC Dirty Interface → Semafone Dirty → Semafone Clean → SBC Clean Interface → SBC Internal Interface → Avaya SM → Avaya Endpoints (Agents)

- Outbound: Avaya Endpoints (Agent) → Avaya SM → SBC Internal Interface → SBC Clean Interface → Semafone Clean → Semafone Dirty → SBC Dirty Interface → SBC External Interface → Service Provider



Contact centers that use Avaya Aura® environment to accept payments over the phone face operational and technical challenges to ensure compliance when handling sensitive cardholder data. Semafone's Voice+ allows contact centers using Avaya Aura® environment to take card payments securely, using DTMF (telephone keypad) capture technology while the contact center agent and customer remain in conversation.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls from customer and agent were made manually with DTMFs sent from both customer and agent. Necessary user actions were performed from the agent telephones to test different call scenarios. The serviceability test cases were performed manually by disconnecting/reconnecting the network to Semafone Voice+ Rushmore.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance

Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and Semafone Voice+ utilized encryption capabilities of SIP TLS.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g., jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g., session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

The interoperability Compliance test included feature and serviceability testing. Feature testing included the validation of the following:

- Inbound calls to Avaya Aura® environment (agents and IVR)
- Outbound calls to VoIP Service Provider
- Proper transmissions of RFC2833 DTMF from Agent, Service Provider to Avaya SBCE
- Proper transmissions of RFC2833 DTMF to/from Semafone Voice+ Rushmore
- Codec negotiations between Avaya SBCE and Semafone Voice+ Rushmore
- Routing of RTP from Avaya SBCE to Semafone Voice+ Rushmore
- Calls for scenarios involving internal, external, IVR, ACD, non-ACD, mute, hold, reconnect, conference, and transfer.

The serviceability testing focused on verifying the ability of Semafone Voice+ Rushmore to recover from adverse conditions, such as disconnecting/reconnecting the network to Semafone Voice+ Rushmore.

2.2. Test Results

All test cases passed successfully.

2.3. Support

Support is available via www.semafone.com

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya Products and Semafone Voice+ Rushmore. All SIP traffic to and from VoIP service provider to Avaya Aura® environment was routed via Semafone Voice+ Rushmore though Avaya SBCE.

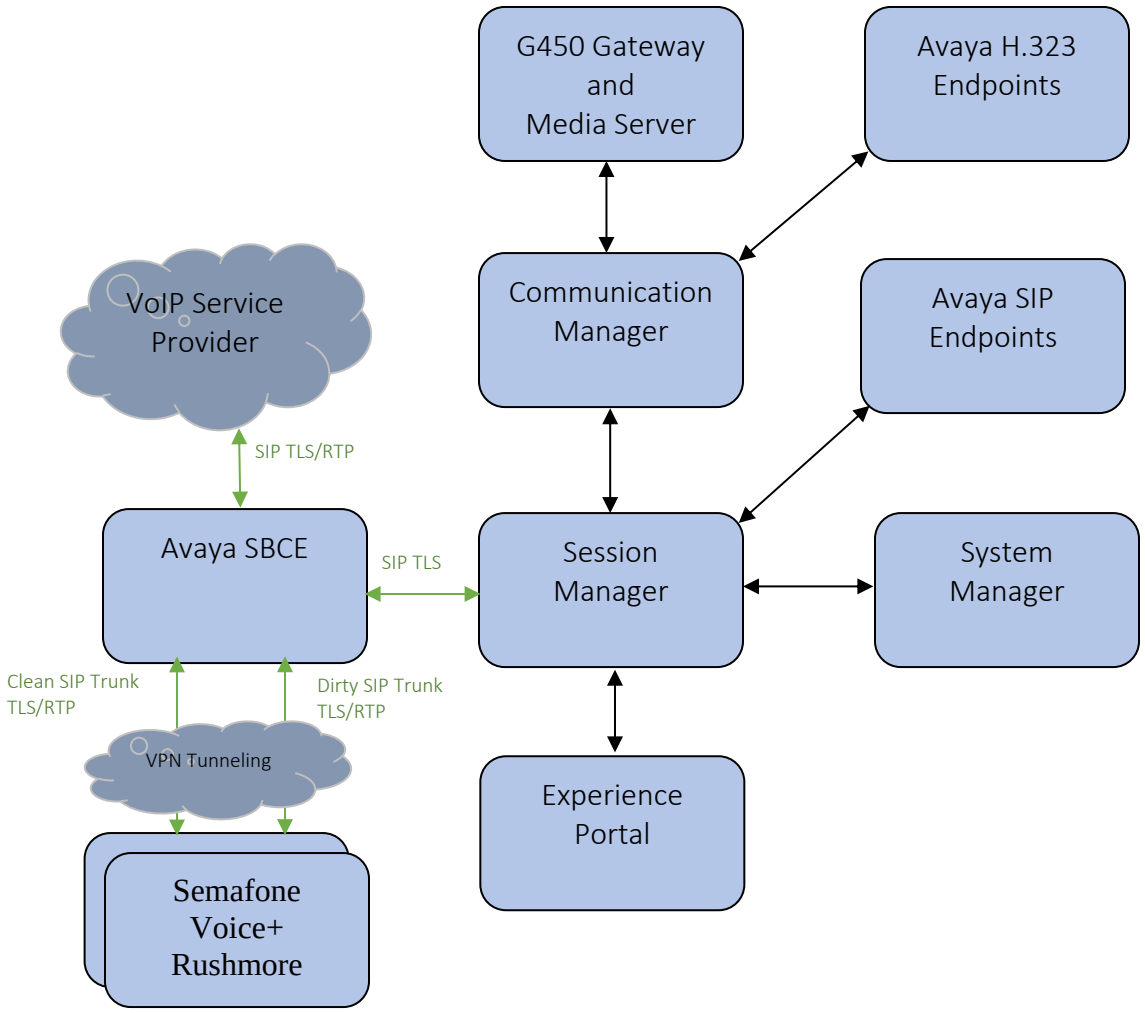


Figure 1: Test Configuration for Semafone Voice+ Rushmore and Avaya Aura® Environment.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager in Virtual Environment	8.1.2
Avaya Aura® Session Manager in Virtual Environment	8.1.2
Avaya Aura® Communication Manager in Virtual Environment	8.1.2
Avaya G450 Media Gateway • MGP	41.16.30
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.0.0-14-18490
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
Avaya IX Workplace	3.8.4.10.2
Avaya 9641 & 9621 IP Deskphone (SIP)	7.1.9
Semafone Voice+ Rushmore	5.0

5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure Semafone Voice+ successfully with Communication Manager.
A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G450 Media Gateway and the Media Server has been previously completed and is not discussed here. The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Some screen captures will show the use of the change command instead of the add command, since the configuration used for the testing was previously added.

5.1. Verify Avaya Aura® Communication Manager License

Enter the **display system-parameters customer-options** command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. If there is insufficient capacity of SIP Trunks or a required feature is not enabled, contact an Avaya representative to make the appropriate changes.

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

                                OPTIONAL FEATURES

IP PORT CAPACITIES                                          USED
                 Maximum Administered H.323 Trunks: 12000      0
       Maximum Concurrently Registered IP Stations:  2400      1
         Maximum Administered Remote Office Trunks: 12000      0
Max Concurrently Registered Remote Office Stations:  2400      0
          Maximum Concurrently Registered IP eCons:  128       0
     Max Concur Reg Unauthenticated H.323 Stations:   100      0
                    Maximum Video Capable Stations:  36000     0
                Maximum Video Capable IP Softphones:   2400     0
                    Maximum Administered SIP Trunks: 12000     10
  Max Administered Ad-hoc Video Conferencing Ports: 12000      0
   Max Number of DS1 Boards with Echo Cancellation: 688    0
```

5.2. System Features

Use the change system-parameters features command to set the Trunk-to-Trunk Transfer field to all to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave the field set to none.

```
change 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? all
              DID/Tie/ISDN/SIP Intercept Treatment: attendant
    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? nsmsip92
```

5.3. Configure IP Node Names

All calls from and to Communication Manager are signaled over a SIP trunk to Session Manager. The signaling interface on Session Manager is provided by the SM100 security module. Use the **change node-names ip** command to add the **Name** and **IP Address** for the SIP security module of Session Manager. **smsip92** and **10.30.5.92** was used in this example.

```
change node-names ip                                             Page   1 of   2

                                   IP NODE NAMES
    Name              IP Address
aes95               10.30.5.95
ams137              10.30.5.137
ams94               10.30.5.94
cmlsp132            10.30.5.132
default             0.0.0.0
procr               10.30.5.93
procr6              ::
smsip92             10.30.5.92
```

5.4. Configure IP Codec Set

Use the **change ip-codec-set n** command to specify **G.711MU, G711A** and **G.729** codecs under **Audio Codec** where **n** is the codec set used in the configuration. Configure the **Media Encryption** and **Encrypted SRTCP** as shown below.

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

                           IP MEDIA PARAMETERS
    Codec Set: 2

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

     Media Encryption                  Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: none
```

5.5. Configure IP network Region

Create a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP Network Region 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is ***devconnect.com*** as assigned to the shared test environment in the Avaya test lab. This domain name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to ***yes***, the default setting. This will enable **IP-IP Direct Audio** (shuffling), to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway or Media Server. Shuffling can be further restricted at the trunk level on the Signaling Group form if needed.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values may be used for all other fields.

```
change ip-network-region 2                                      Page   1 of 20
                              IP NETWORK REGION
  Region: 2
Location:         Authoritative Domain: devconnect.com
    Name:                      Stub Network Region: n
MEDIA PARAMETERS               Intra-region IP-IP Direct Audio: yes
      Codec Set: 2             Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 3329
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test. It indicates that codec set **2** will be used for calls between region **2** (the service provider region) and region 1 (the rest of the enterprise).

```
change ip-network-region 2                                      Page   4 of 20

 Source Region: 2     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening       Dyn A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions           CAC R  L    e
 1    2     y    NoLimit                                           n all   t
 2    2                                                             all   UDP Port
```

5.6. Add Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, ***tls*** was used.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field will initially be set to ***Others*** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer is a Session Manager.

Note: Once the **Peer-Server** field is updated to **SM**, the system changes the default values of the following fields, setting them to display–only:

- **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to ***y***.
- **Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to ***n***.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***smsip92***. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5071**.
- Set the **Far-end Network Region** to the IP network region defined for the Service Provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to ***n***, then the Avaya Media Gateway or Media Server will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Media Server, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields.

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

 Group Number: 2              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: smsip92
 Near-end Listen Port: 5071                Far-end Listen Port: 5071
                                        Far-end Network Region: 1
                                   Far-end Secondary Node Name:
Far-end Domain: devconnect.com
                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? y
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? y
```

5.7. Add SIP Trunk Group

Add the corresponding trunk group controlled by the above signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type:** **sip**
- **Group Name:** A descriptive name (e.g., **Service Provider)**
- **TAC:** An available trunk access code (e.g., **#02**)
- **Service Type:** ***public-ntwrk***
- **Signaling Group:** Number of the signaling group added in **Section 5.6**
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager (**must be within the limits of the total trunks available from licensed verified in **Section 5.1**)

```
add trunk-group 2                                                Page   1 of  5
                                 TRUNK GROUP

Group Number: 2                     Group Type: sip           CDR Reports: y
  Group Name: Service Provider            COR: 1        TN: 1        TAC: #02
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk                   Auth Code? n
                                              Member Assignment Method: auto
                                                        Signaling Group: 2
                                                      Number of Members: 50
```

On Page 3:

- Set the **Numbering Format** field to ***public***. This field specifies the format of the calling party number (CPN) sent to the far-end. When ***public*** format is used, Communication Manager automatically inserts a "+" sign, preceding the numbers in the "From", "Contact" and "P-Asserted Identity" (PAI) headers
- Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call has enabled CPN block.

```
change trunk-group 2                                             Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y

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

                                          Replace Restricted Numbers? y
                                          Replace Unavailable Numbers? y

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

 Show ANSWERED BY on Display? Y
```

On Page 4:

- Set the **Telephone Event Payload Type** to **101**, the value preferred by **Semafone Voice+.**

```
change trunk-group 2                                            Page   4 of   4
                             PROTOCOL VARIATIONS

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

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


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                           Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                               Request URI Contents: may-have-extra-digits
```

5.8. Configure Route Patterns

Configure a route pattern to correspond to the newly added SIP trunk group. Use **change route pattern n** command, where **n** is an available route pattern. When changing the route pattern, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Grp No:** The trunk group number from **Section 5.7**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 1      Pattern Name:Public
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1:  2   0                                                               n   user
 2:                                                                      n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format

 1: y y y y y n  n            rest                                unk-unk   none
 2: y y y y y n  n            rest                                          none
```

5.9. Configure Public Unknown Numbering

Use the **change public-unknown-numbering 0** command to assign number presented by Communication Manager for calls leaving for Session Manager. Add an entry for the Extensions configured in the dialplan. Enter the following values for the specified fields, and retain default values for the remaining fields.

- **Ext Len:** Number of digits of the Extension i.e., **5**
- **Ext. Code:** Leading digits of the Extension number, i.e., **7**
- **Trk Group:** Leave it blank (meaning any trunk)
- **CPN Prefix:** Enter a value a desired value or leave blank, i.e., **848333**
- **Total CPN Len** Total number of digits i.e., **11**

Note that the value entered in **CPN Prefix** will replace the agent's extensions value for outbound calls.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                              Total
Ext Ext              Trk       CPN             CPN
Len Code             Grp(s)    Prefix          Len
                                                   Total Administered: 1
 5  7                          848333          11    Maximum Entries: 240

                                                   Note: If an entry applies to
                                                   a SIP connection to Avaya
                                                   Aura(R) Session Manager,
                                                   the resulting number must
                                                   be a complete E.164 number.

                                                   Communication Manager
                                                   automatically inserts
                                                   a '+' digit in this case.
```

5.10. Configure ARS Analysis

This section shows a sample Auto Route Selection (ARS) entry used for routing calls with dialed digits beginning with **1416** and **1616**. Use the **change ars analysis 14** command to add an entry and specify routing of the calls to Session Manager. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Dialed String:** Dialed prefix digits to match on, in this case **1416, 1616**
- **Total Min:** Minimum number of digits, in this case **11**
- **Total Max:** Maximum number of digits, in this case **11**
- **Route Pattern:** The route pattern number from **Section 5.8** i.e., **2**
- **Call Type:** **intl**

Note that additional entries may be added for different number destinations.

```
change ars analysis 14                                          Page   1 of   2
                            ARS DIGIT ANALYSIS TABLE
                                  Location: all            Percent Full: 0

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    1416                   11   11     2       intl         n
    1616                   11   11     2       intl         n
```

5.11. Configure Feature Access Code

Use the **change feature access code** command to define a feature access code for **Auto Route Selection (ARS).** In the test, **9** was used.

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

5.12. Outbound Routing

Outbound Routing In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below with little elaboration. Use the change dialplan analysis command to define a dialed string beginning with 9 of length 1, as a feature access code (fac).

```
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
 10            3  udp
 5             4  udp
 6             5  udp
 7             5  ext
 8             5  ext
 9             1  fac
 *             3  fac
 #             3  dac
```

6. Configure Avaya Aura® Session Manager

All configuration for Session Manager is performed via System Manager web interface. Open a web browser session to System Manager URL. A SIP trunk and routing needs to be configured for Communication Manager and Avaya SBCE.

6.1. Configure SIP Entities

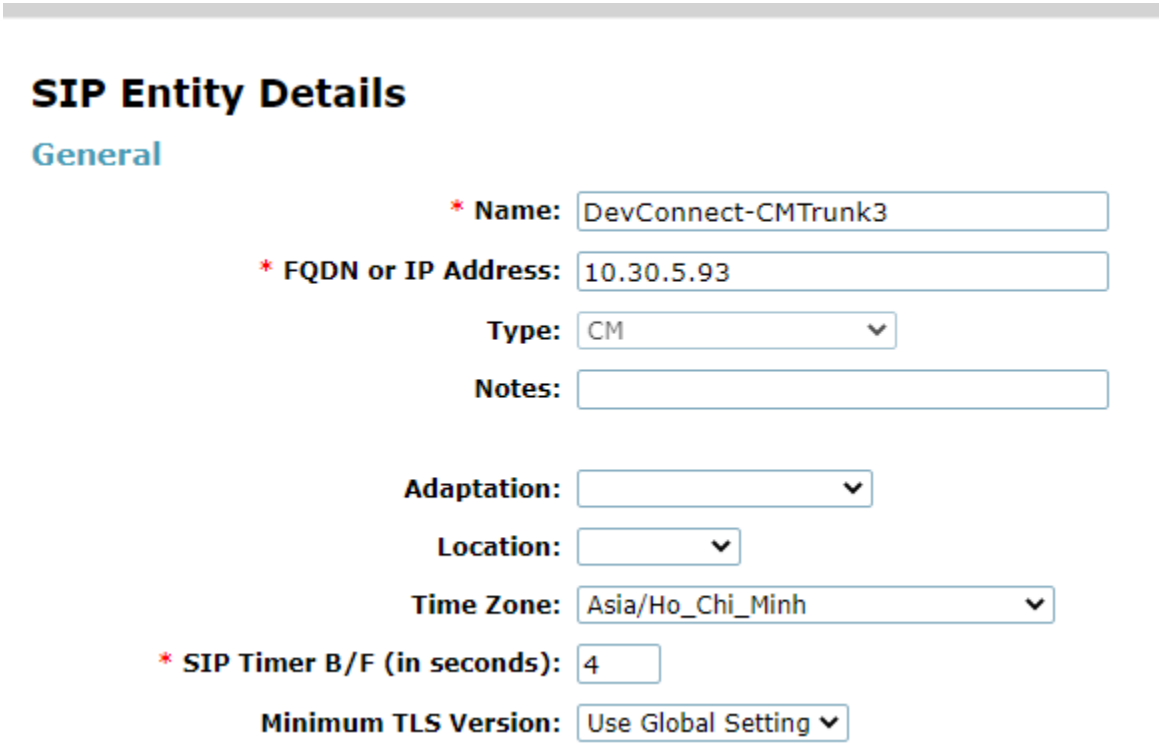
Add two new SIP entities, one for Communication Manager and another one for Avaya SBCE

6.1.1. SIP Entity for Communication Manager

Select **Routing → SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager.

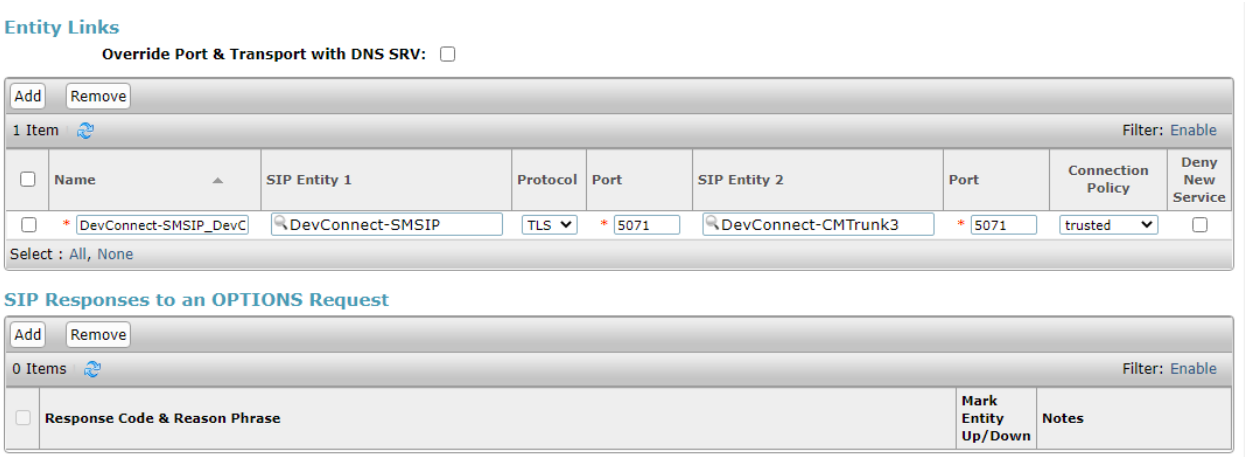
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The procr address of Communication Manager.
- **Type:** "CM"
- **Location:** Select a preconfigured Location.
- **Time Zone:** Select the applicable time zone.



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

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case "**DevConnect-SMSIP**".
- **Protocol:** "TLS"
- **Port:** "5071"
- **SIP Entity 2:** The Communication Manager entity name from this section, in this case "**DevConnect-CMTrunk3**"
- **Port:** "5071"
- **Connection Policy:** "trusted"

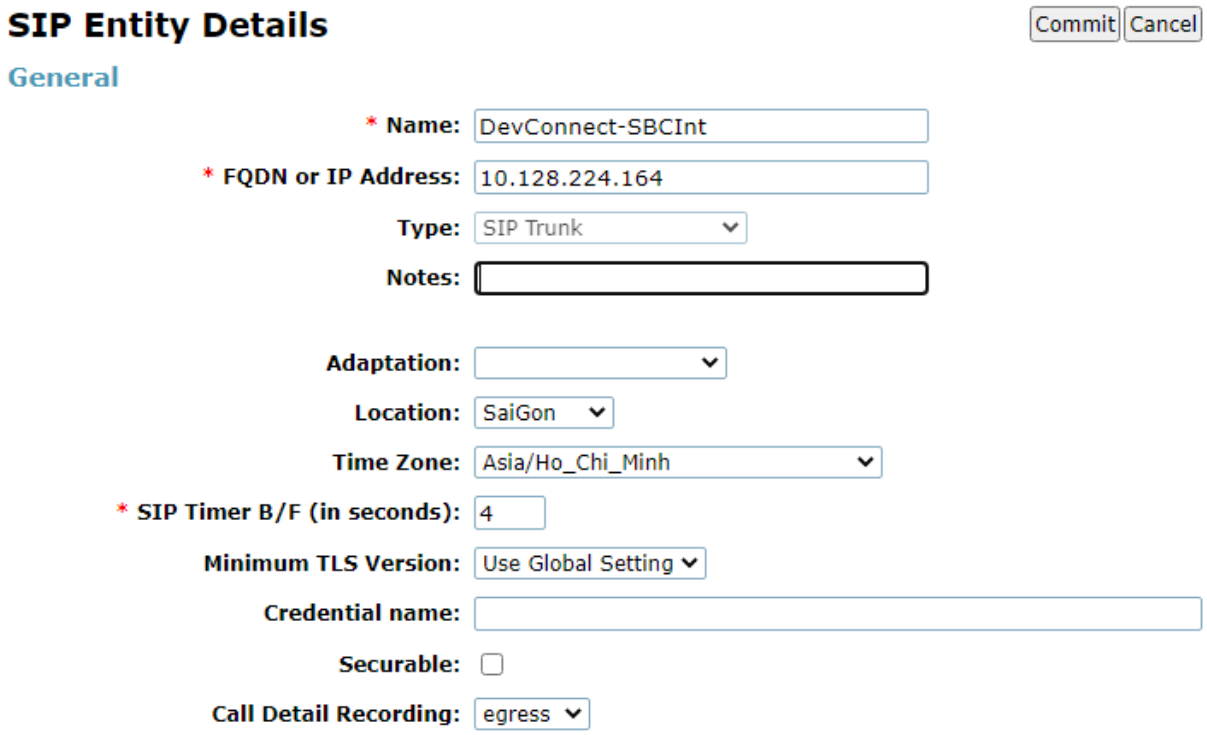


6.1.2. SIP Entity for Avaya SBCE

Select **Routing → SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Avaya SBCE.

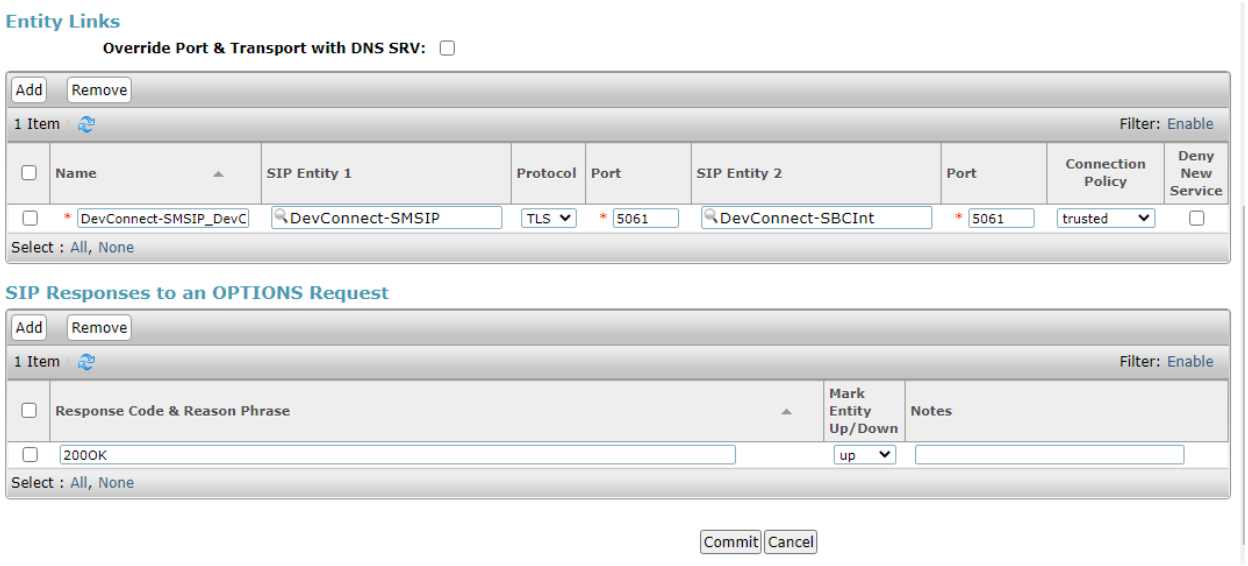
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The internal SIP IP address of Avaya SBCE.
- **Type:** "SIP Trunk"
- **Notes:** Any desired notes.
- **Location:** Select the applicable location.
- **Time Zone:** Select the applicable time zone.



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

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case "**DevConnect-SMSIP** ".
- **Protocol:** "TLS"
- **Port:** "5061"
- **SIP Entity 2:** The Avaya SBCE entity name from this section, in this case **"DevConnect-SBCInt"**
- **Port:** "5061"
- **Connection Policy:** "trusted"



6.2. Configure Routing Policies

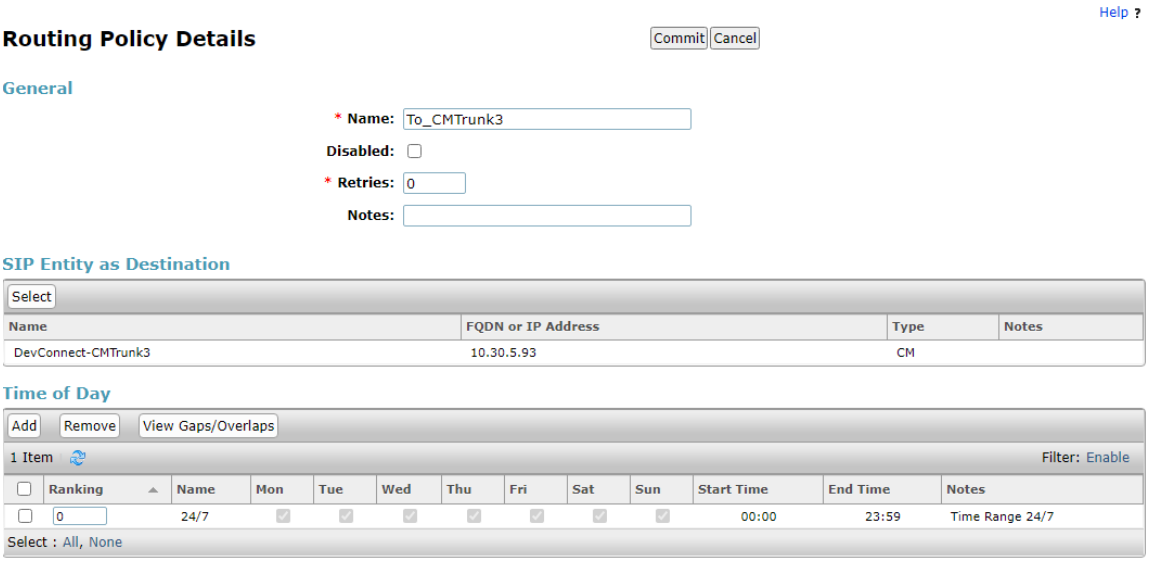
Add a new routing policy for routing calls to Communication Manager and Avaya SBCE.

6.2.1. Routing Policy for Communication Manager

Select **Routing → Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy to Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.1.1**.

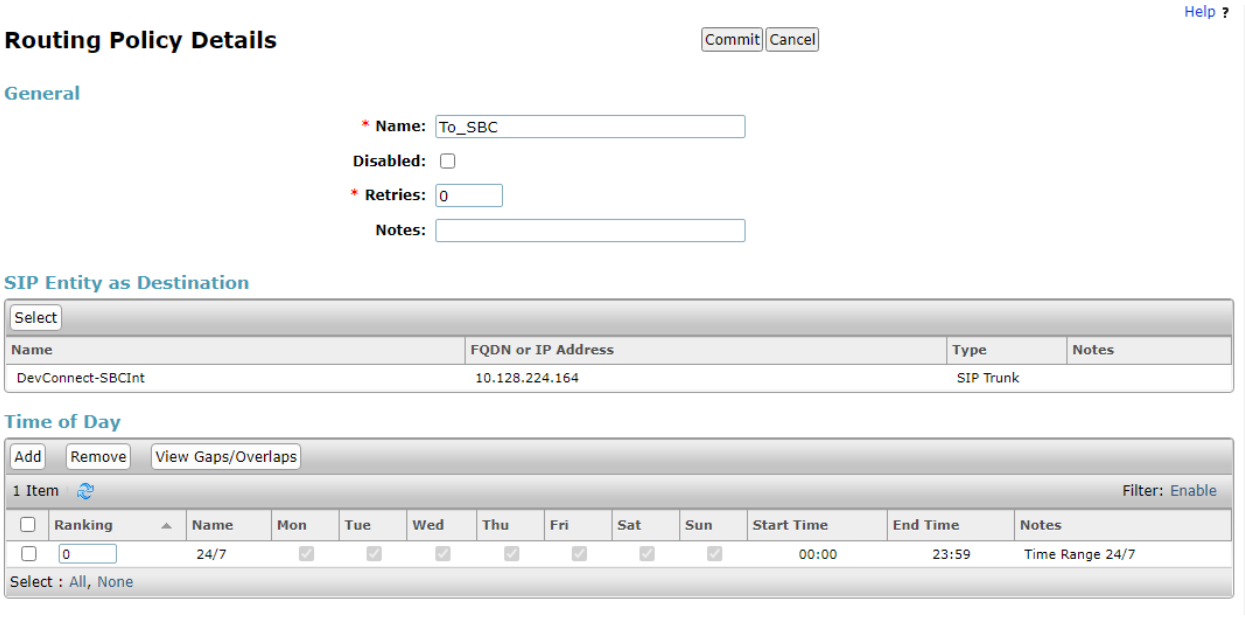


6.2.2. Routing Policy for Avaya SBCE

Select **Routing → Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy to Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Avaya SBCE entity name from **Section 6.1.2**.



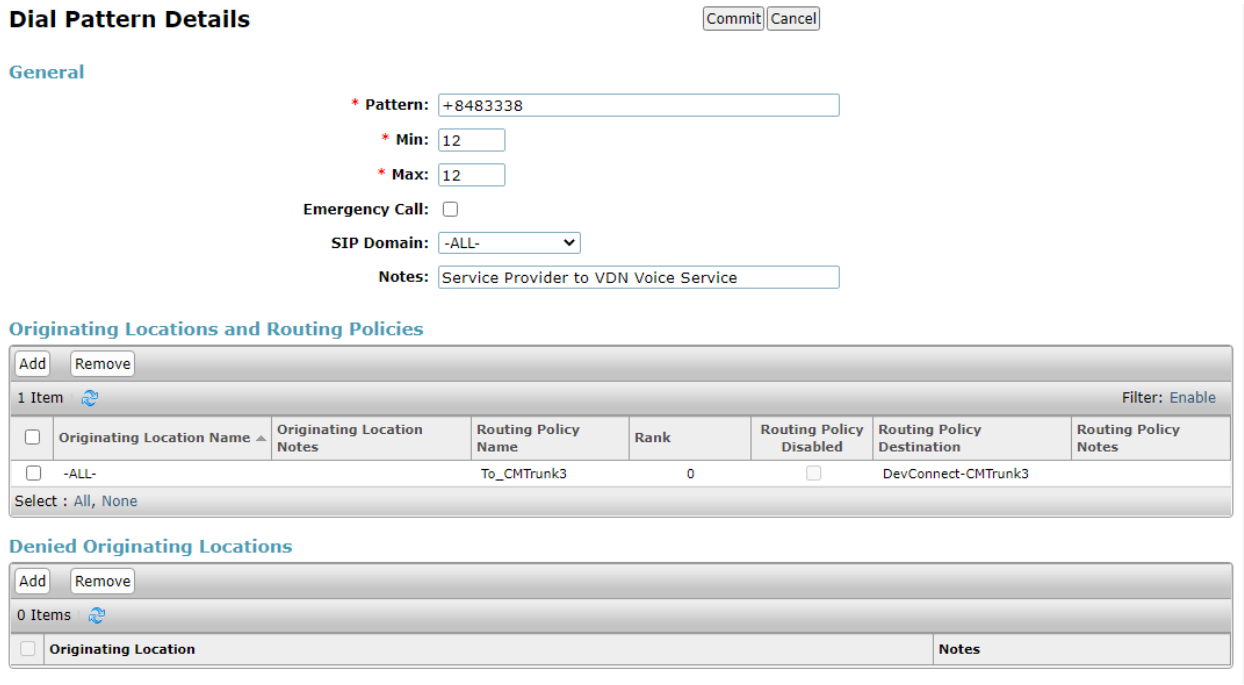
6.3. Configure Dial Patterns

Dial patterns needs to be configured for Session Manager to know where to route the calls.

6.3.1. Dial Pattern for Communication Manager

Select **Routing → Dial Patterns** from the left pane, and add a new Dial Pattern by select **Add** (not shown). The **Dial Pattern Details** screen is displayed.

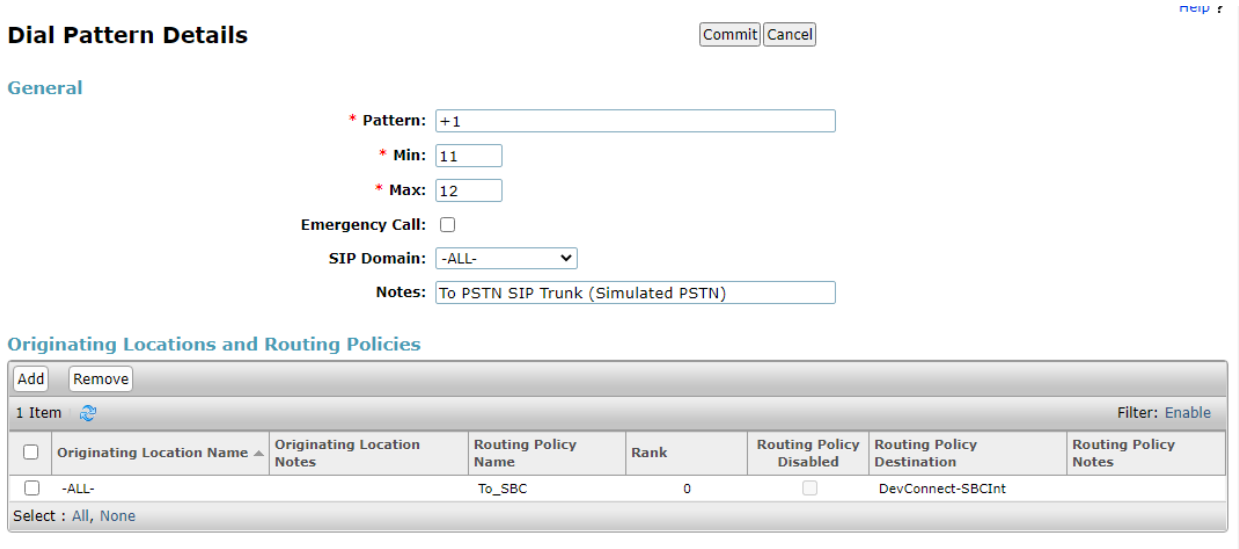
In the **Originating Locations and Routing Policies** sub-section, click **Add**. Select a preconfigured **Originating Location** and select the **Routing Polices** created in previous **Section 6.2.1** (not shown). The configuration below shows calls to **+8483338xxxxx** were routed to Communication Manager.



6.3.2. Dial Pattern for Avaya SBCE

Select **Routing → Dial Patterns** from the left pane, and add a new Dial Pattern by select **Add** (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add**. Select a preconfigured **Originating Location** and select the **Routing Polices** created in previous **Section 6.2.2** (not shown). The configuration below shows calls to **+1xxxxxxxxxx** were routed to Avaya SBCE.



7. Configure Avaya Session Border Controller for Enterprise

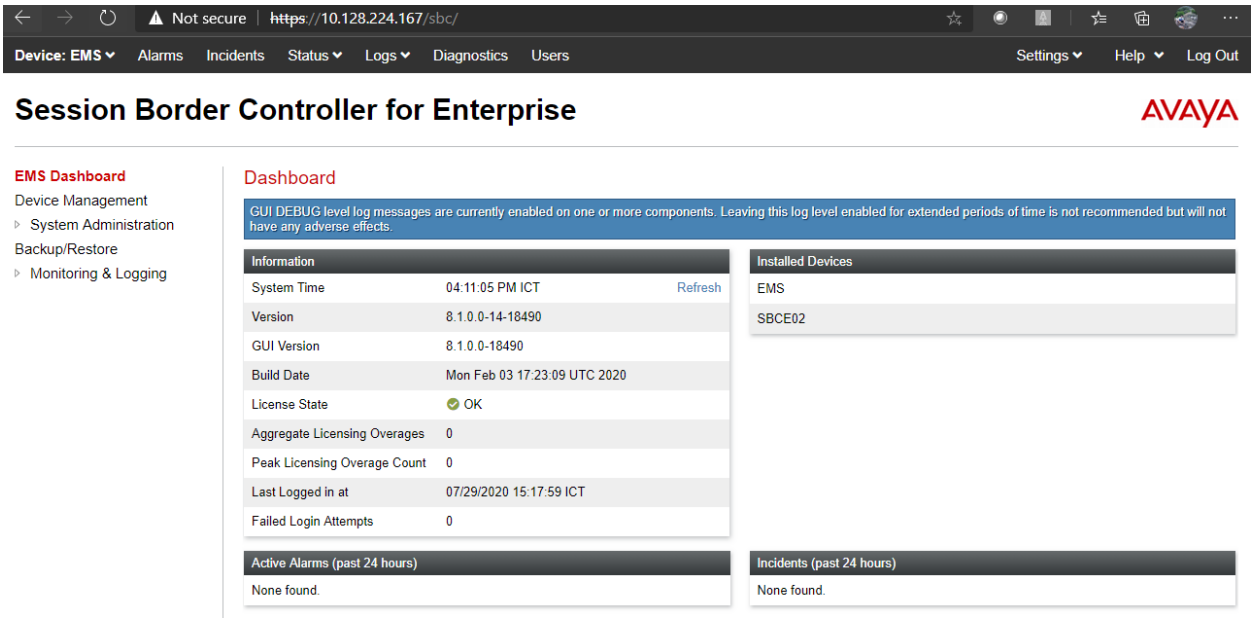
This section describes the configuration of the Avaya SBCE. The Avaya SBCE provides SIP connectivity to VoIP Service Provider, Semafone Voice+ and Session Manager.

Note: The Staging and Production Semafone Voice+ IP Addresses and ports for the relevant region will be shared with the Avaya customer during the integration phase. Capacity numbers used for the inbound and outbound routes will also be defined at the same time.

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A login screen is presented. Log in using the appropriate username and password.

7.1. Access Avaya Session Border Controller for Enterprise

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.

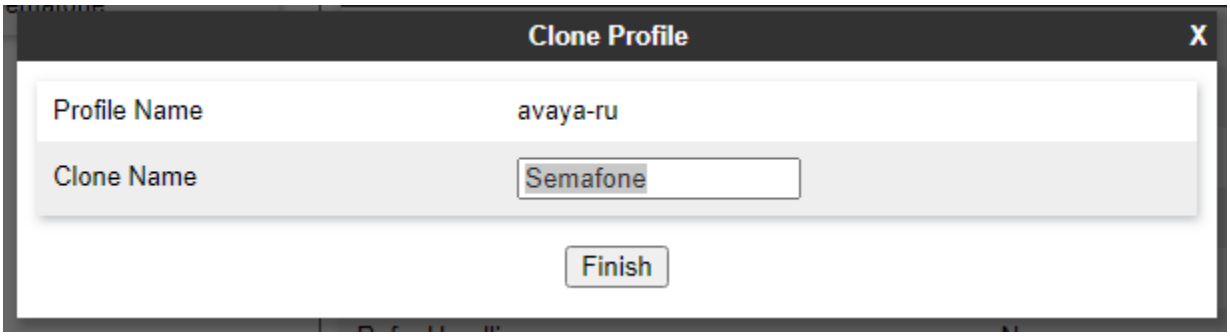


7.2. Define Server Interworking

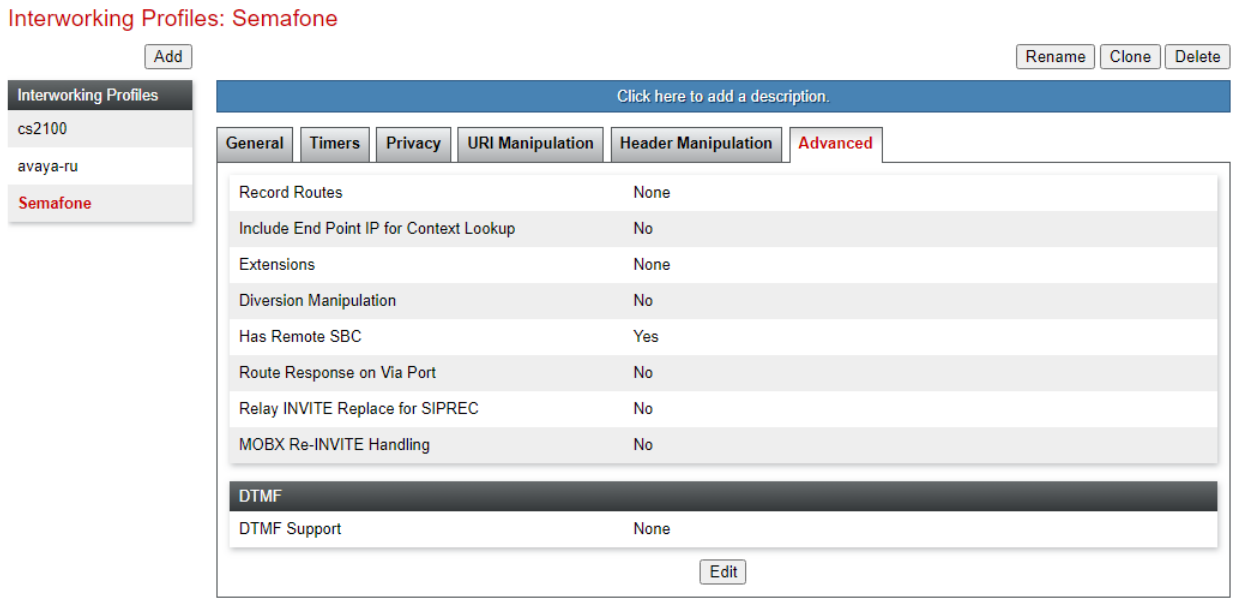
An interworking profile is needed for supported SIP functionality for a SIP server. During Compliance Testing, a pre-configured profile was used for Session Manager and VoIP Service Provider, but the screen captures for those are shown in this section. Add Interworking profile for VoIP Service Provider, Semafone Voice+ and Session Manager.

7.2.1. Server Interworking profile for Semafone

To add a Server Interworking profile, select **Configuration Profiles → Server Interworking** from the left-hand menu. Screen captures for the profile are shown below. Select the **avaya-ru** profile and select **Clone**. Type in a **Clone Name** for Semafone profile. Select **Finish** once done.



Select the **Advanced** tab and configure the fields as the screen capture below. Note that the **Record Routes** is set to **None.**

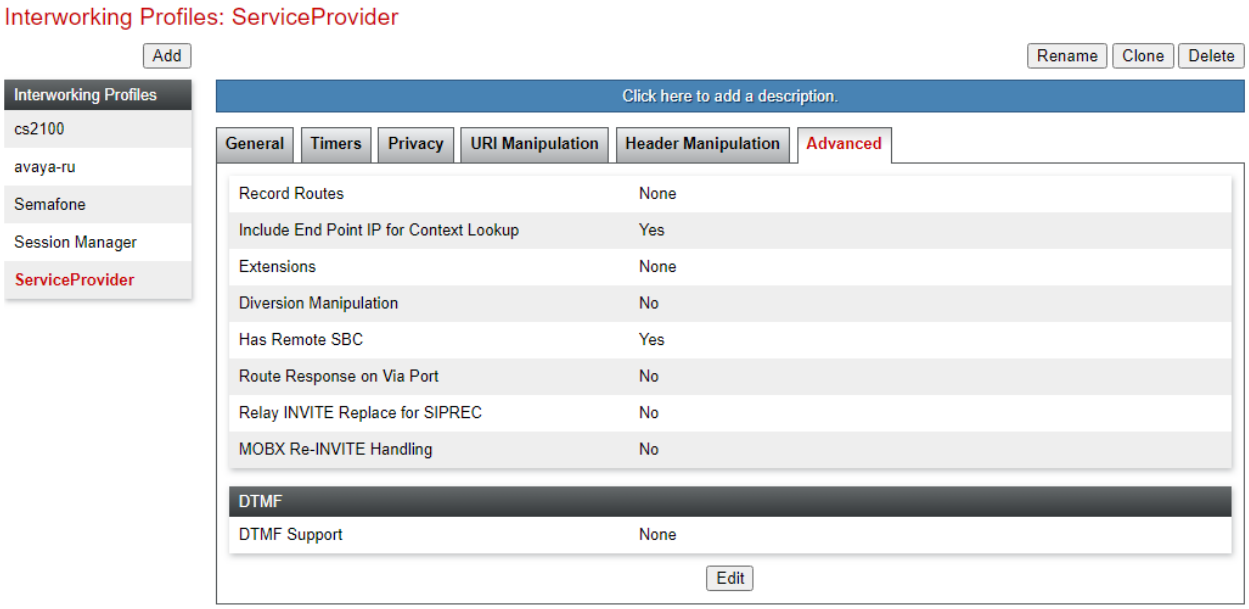


7.2.2. Server Interworking profile for Session Manager

Session Manager profile was cloned from the same **avaya-ru** profile. The **Advanced** tab screen capture is shown below:

7.2.3. Server Interworking profile for VoIP Service Provider

VoIP Service Provider profile was also cloned from the same **avaya-ru** profile. Select the **Advanced** tab and configure as shown in the screen capture below:



7.3. Define SIP Servers

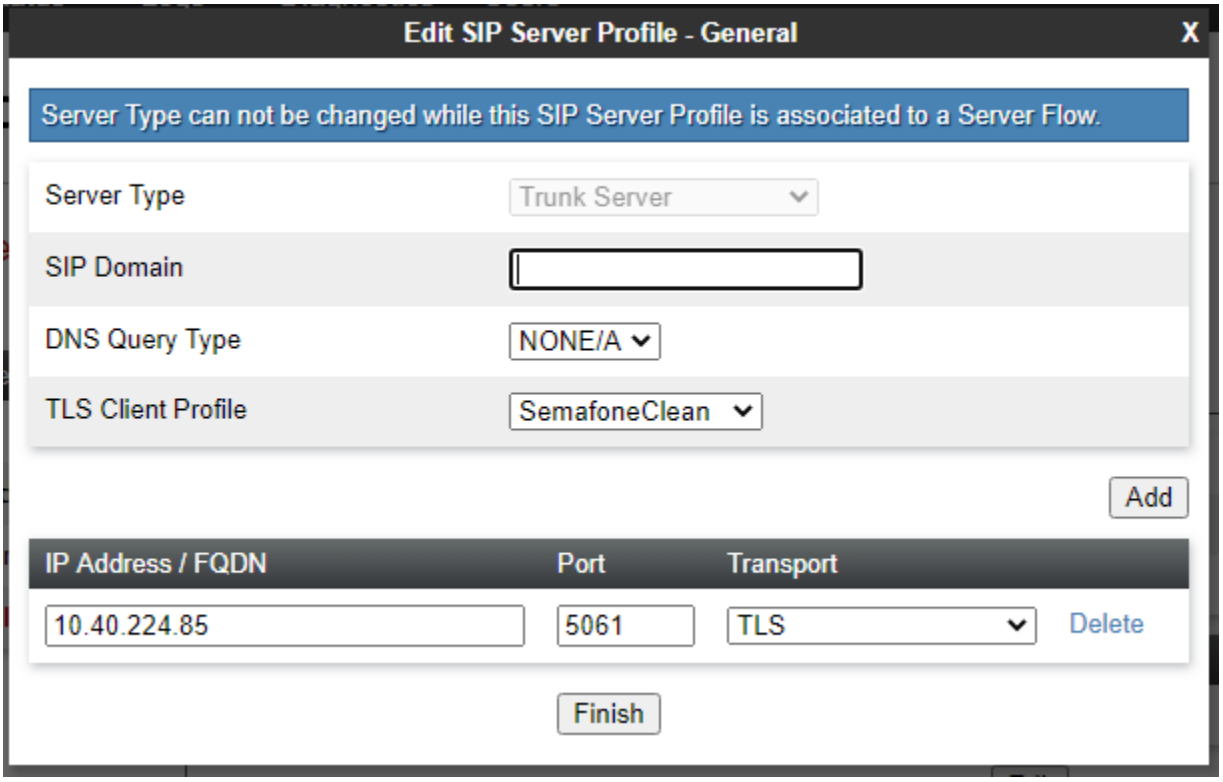
A SIP server definition is required for each server connected to the Avaya SBCE. Add SIP Servers for VoIP Service Provider, Semafone Voice+ and Session Manager.

7.3.1. SIP Server for Semafone Voice+ Clean

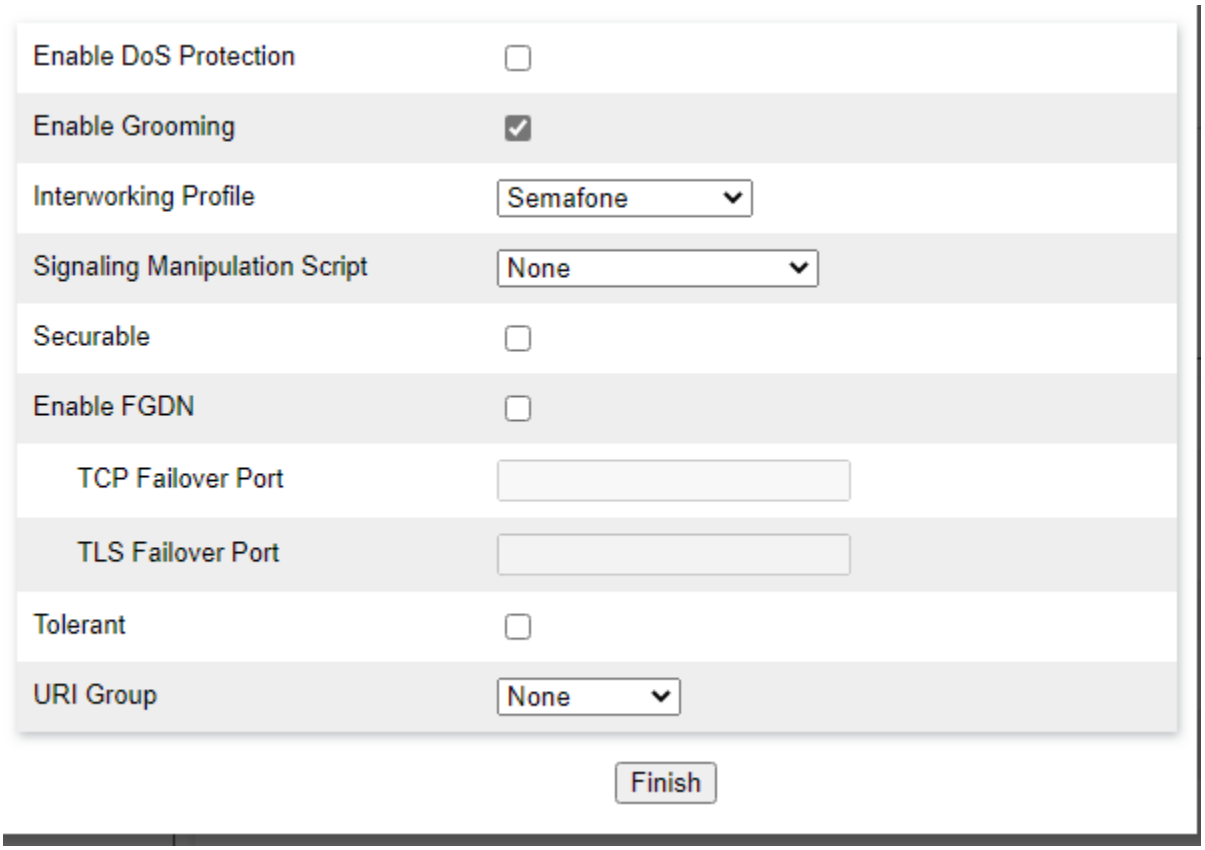
To define a server, navigate to **Services → SIP Servers** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the pop-up screen (not shown) and select **Next**. Note that for security purposes, Public IP Addresses have been changed to Private.

- **Server Type:** **Trunk Server**
- **TLS Client Profile:** Select a TLS profile for authentication
- **IP Address / FQDN** SIP IP Address of Semafone Voice+ Clean
- **Port:** SIP Port of Semafone Voice+ Clean
- **Transport:** **TLS**

Note that TLS profiles were preconfigured and are not shown in this document. TLS certificates were signed by Semafone.



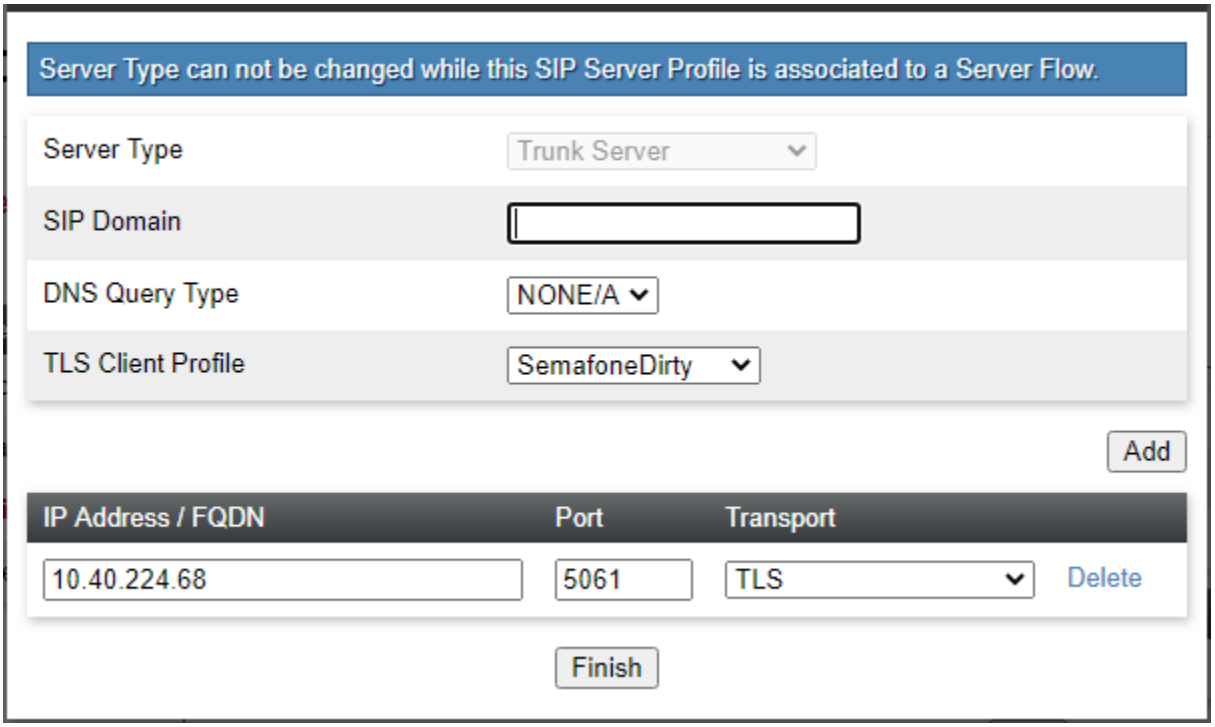
Select **Next** until **Add SIP Server Profile – Advanced** page. Select the **Interworking Profile** for Semafone from **Section 7.2.1** and select **Finish.**



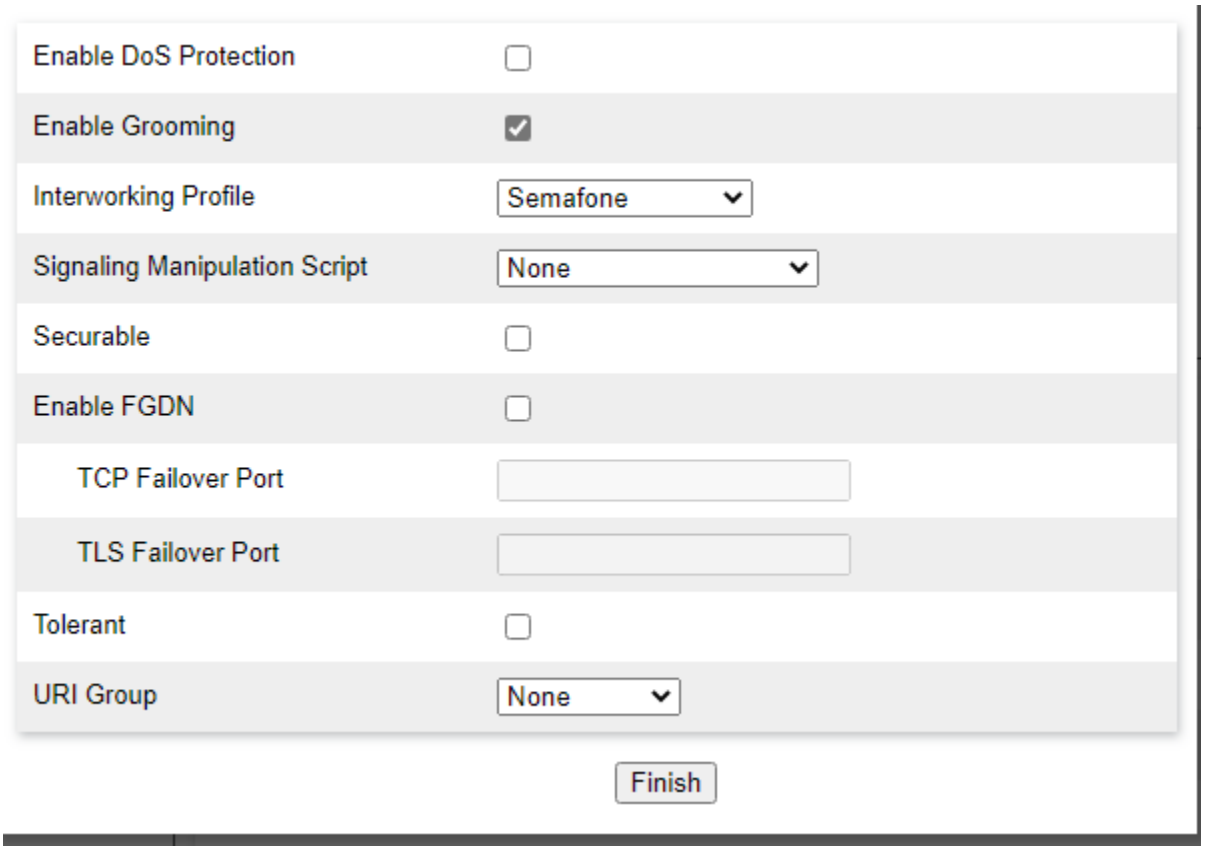
7.3.2. SIP Server for Semafone Voice+ Dirty

To define a server, navigate to **Services → SIP Servers** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the pop-up screen (not shown) and select **Next**. Note that for security purposes, Public IP Addresses have been changed to Private.

- **Server Type:** **Trunk Server**
- **TLS Client Profile:** Select a TLS profile for authentication
- **IP Address / FQDN** SIP IP Address of Semafone Voice+ Dirty
- **Port:** SIP Port of Semafone Voice+ Dirty
- **Transport:** **TLS**

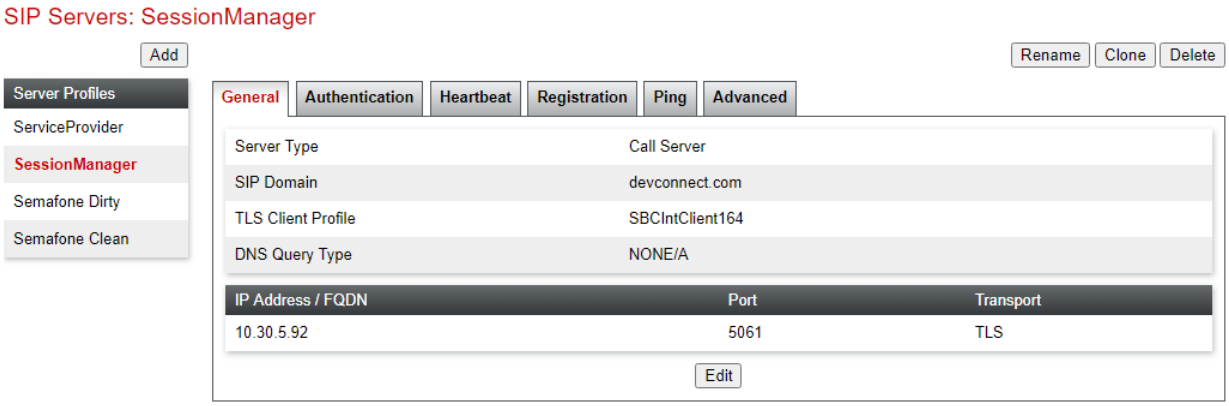


Select **Next** until **Add SIP Server Profile – Advanced** page. Select the **Interworking Profile** for Semafone from **Section 7.2.1** and select **Finish.**

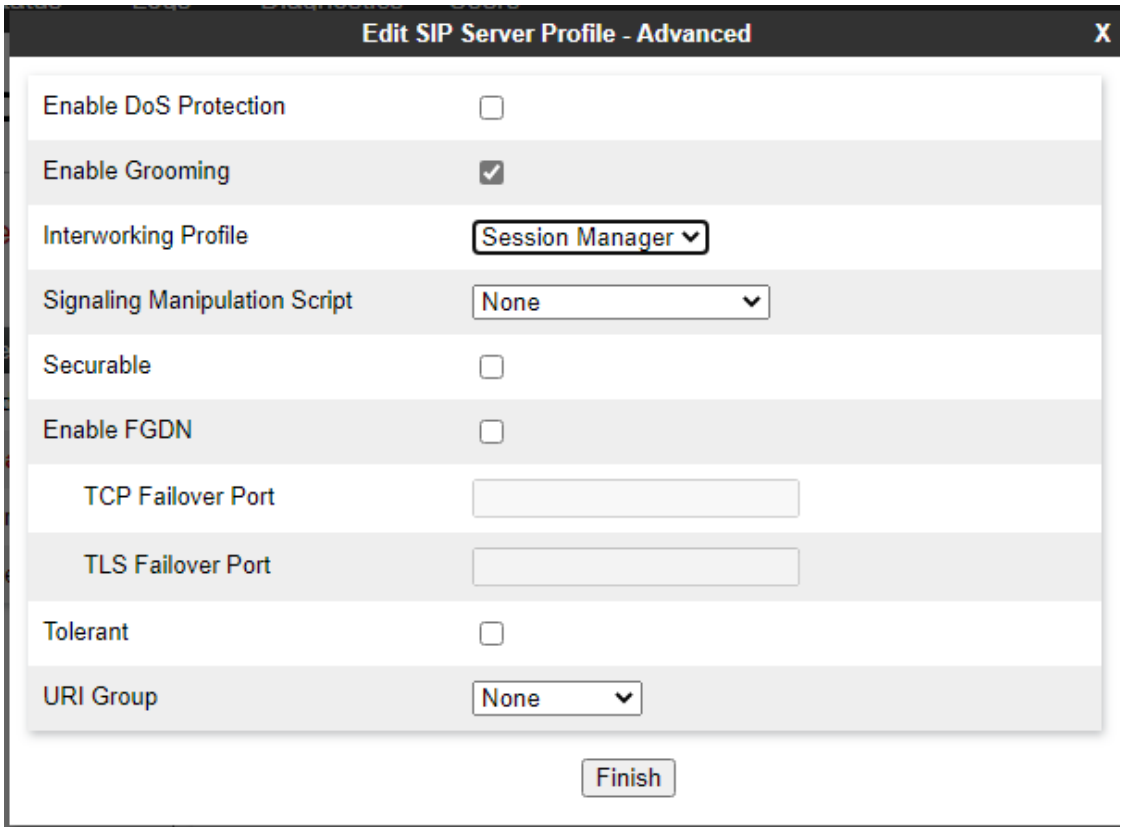


7.3.3. SIP Server for Session Manager

Session Manager SIP Server was preconfigured. The screen capture below shows the **General** tab:

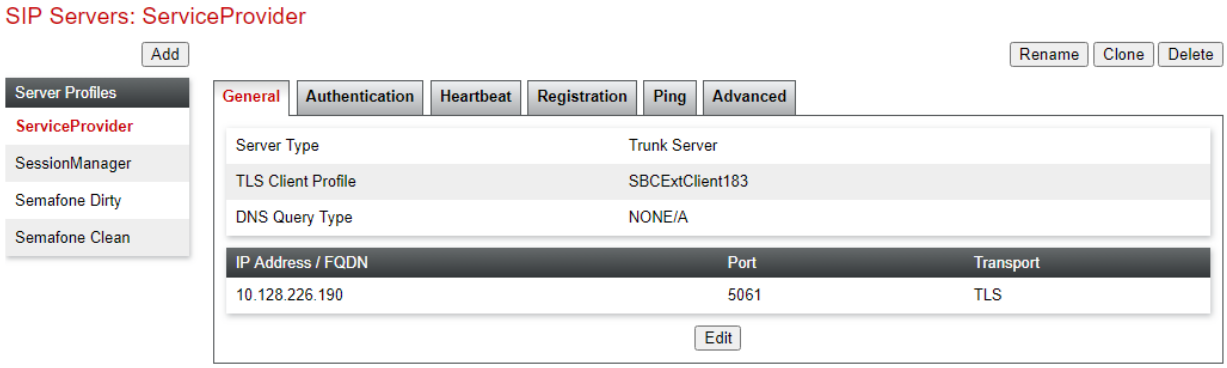


All the other tabs were of default value except for the **Advanced** tab. Note the Server Interworking profile from **Section 7.2.2.** was configured.

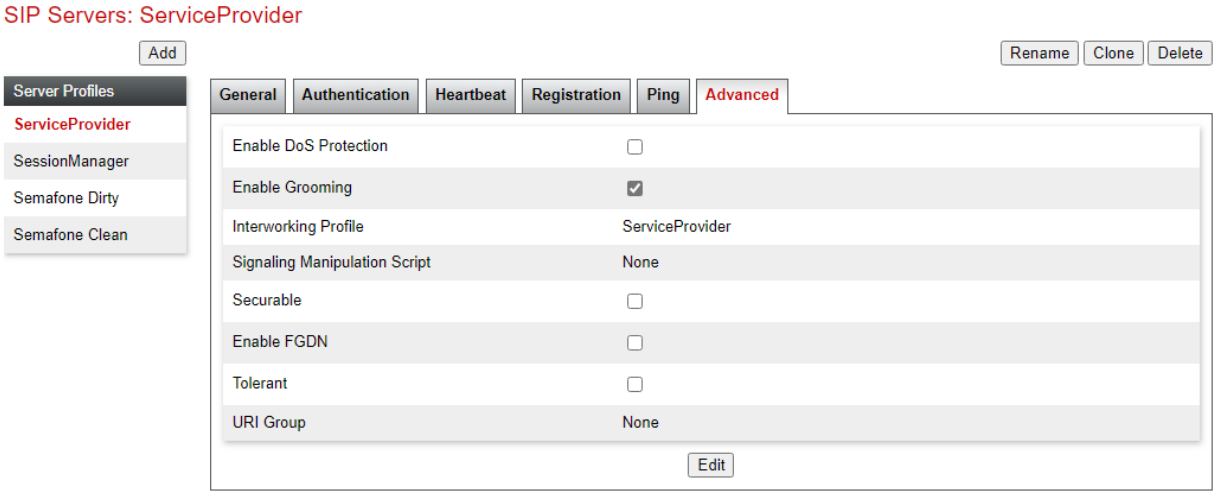


7.3.4. SIP Server for VoIP Service Provider

VoIP Service Provider SIP Server was preconfigured. The screen capture below shows the **General** tab:



All the other tabs were of default value except for the **Advanced** tab. Note the Server Interworking profile from **Section 7.2.3.** was configured.

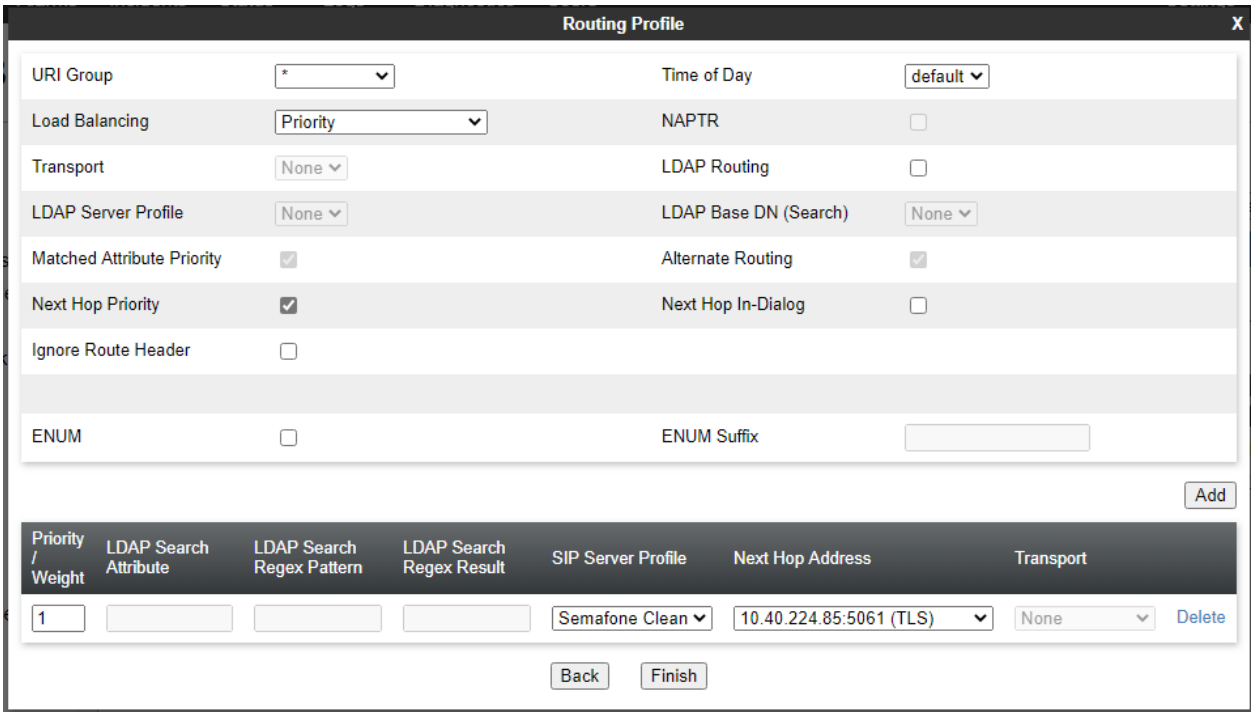


7.4. Define Routing

Routing information is required for routing calls to all configured SIP Servers. The IP addresses and ports defined here will be used as the destination addresses for signalling.

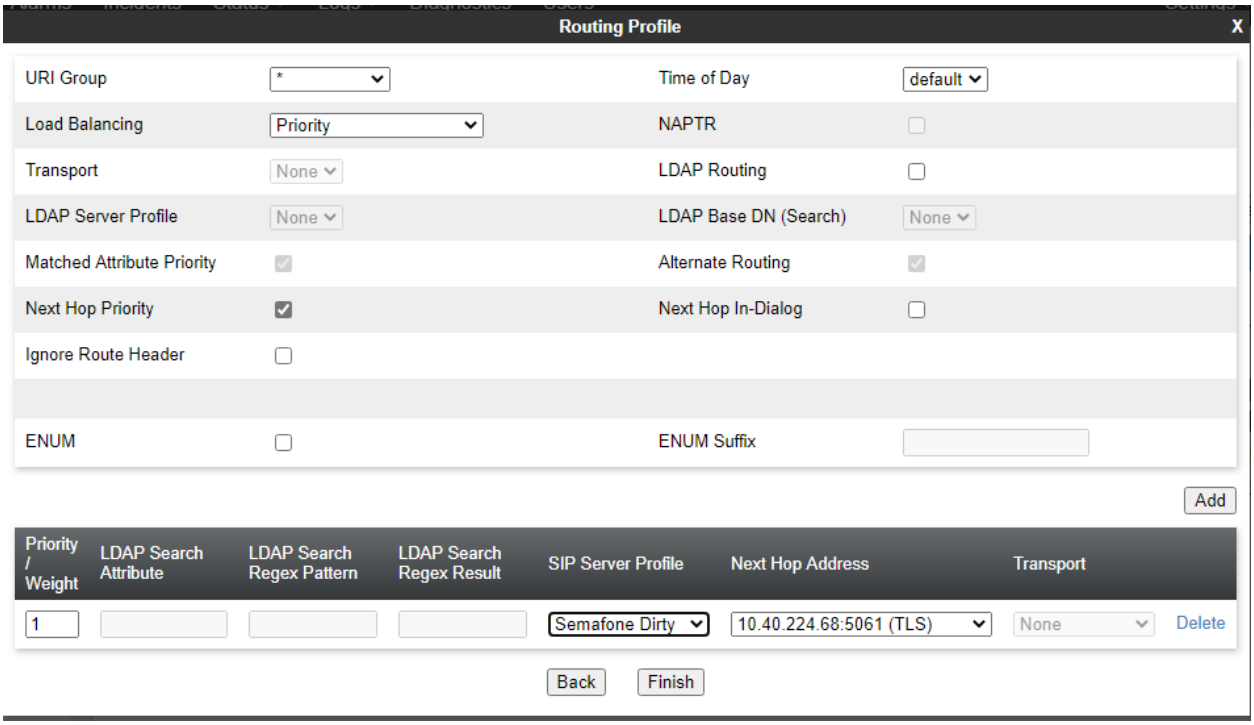
7.4.1. Routing Profile for Semafone Voice+ Clean

To define Routing profile for, navigate to **Configuration Profiles → Routing** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the dialogue box (not shown). Add entry for Semafone Voice+ Clean **SIP Server Profile**. Note the **Priority / Weight** value; lower the value, higher the priority. If calls to higher priority SIP Server fail, calls are routed to the next highest priority SIP Server. Select **Finish** once done.



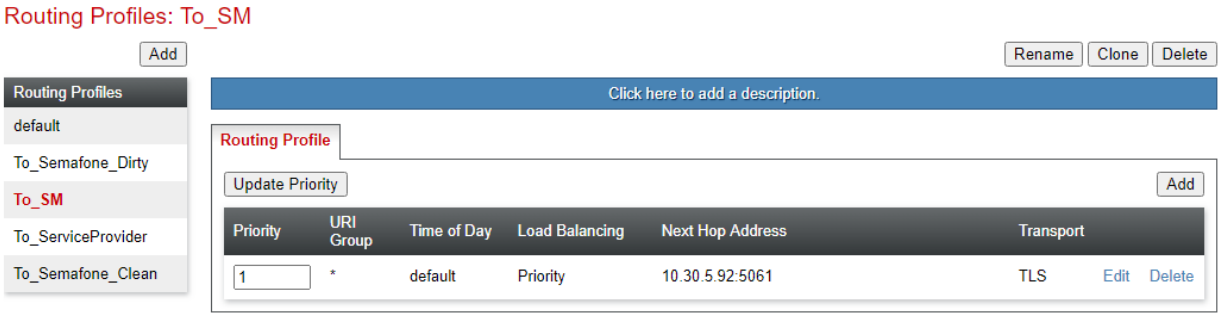
7.4.2. Routing Profile for Semafone Voice+ Dirty

Screen capture below shows the configured Routing Profile for Semafone Dirty



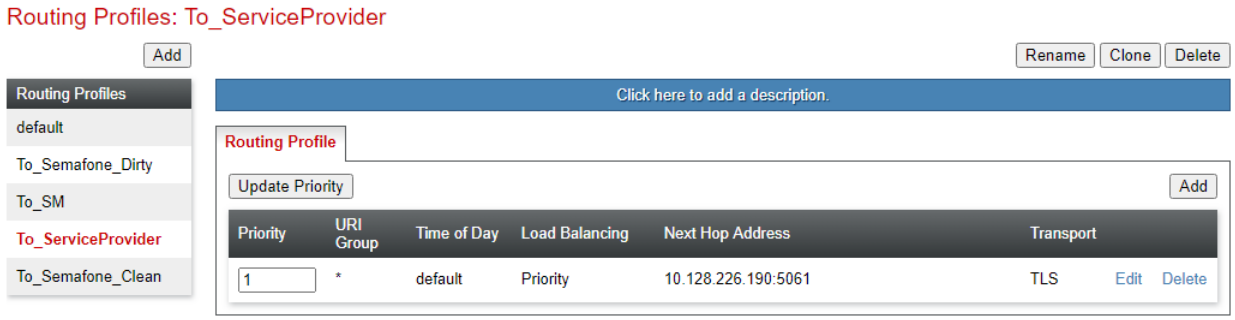
7.4.3. Routing Profile for Session Manager

Routing Profile for Session Manager was preconfigured. Screen capture below shows the configured Routing Profile for Session Manager.



7.4.4. Routing Profile for VoIP Service Provider

Routing Profile for VoIP Service Provider was preconfigured. Screen capture below shows the configured Routing Profile for VoIP Service Provider.



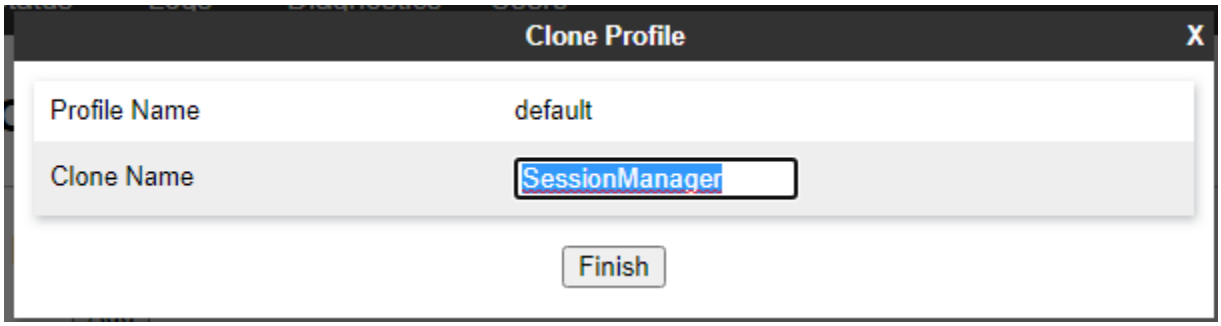
7.5. Topology Hiding

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.

7.5.1. Topology Hiding Profile – Enterprise

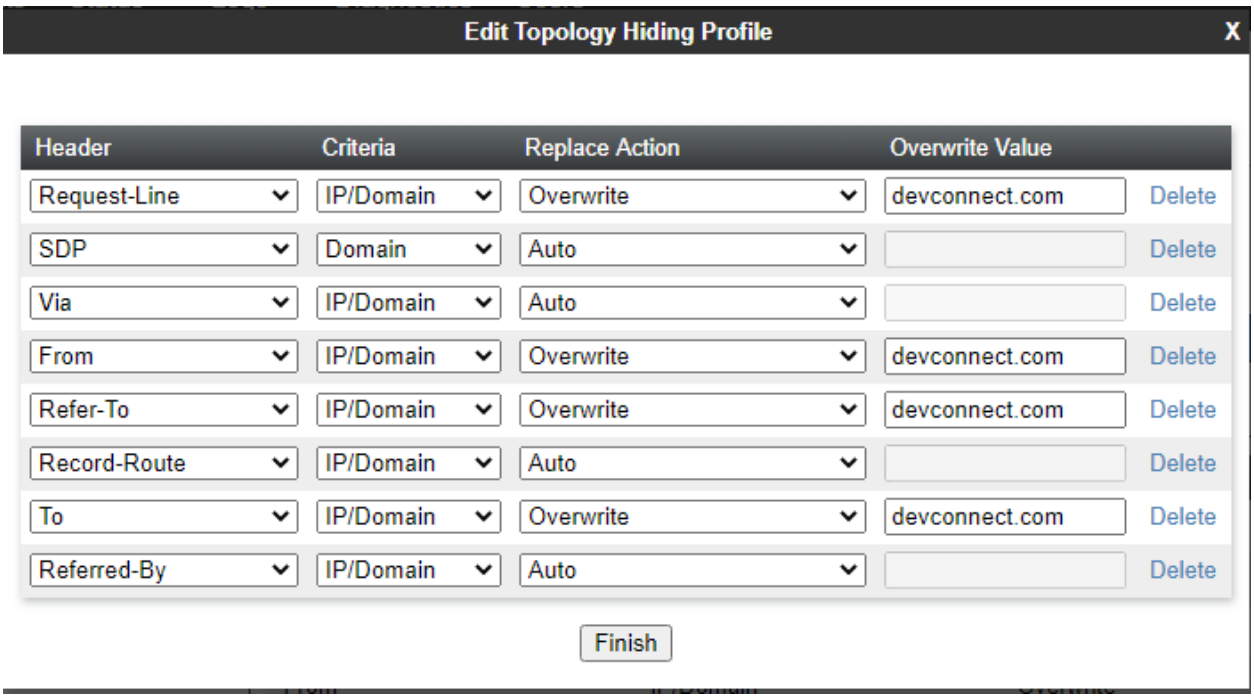
To add the Topology Hiding Profile in the enterprise direction, select Topology Hiding from the Global Profiles menu on the left-hand side, select default from the list of pre-defined profiles and click the Clone button (not shown).

- Enter a Clone Name such as the one shown below.
- Click **Finish**.



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

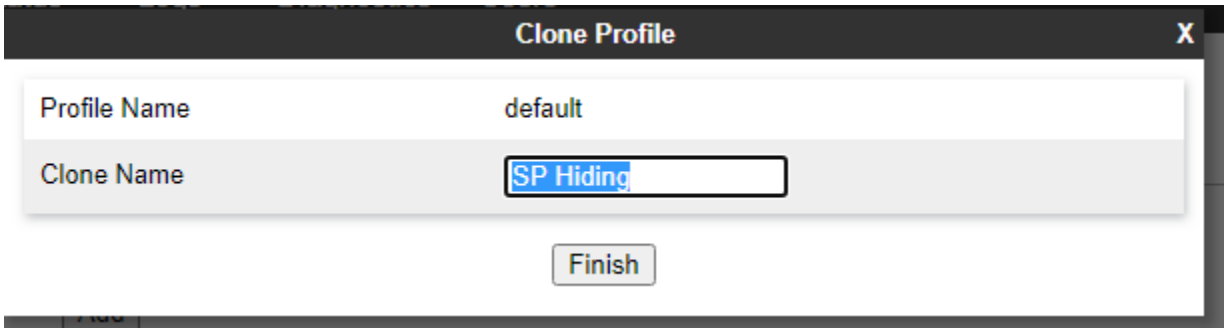
- For the, **From**, **To, Refer-To** and **Request-Line** headers, select **Overwrite** in the Replace Action column and enter the enterprise SIP domain **devconnect.com**, in the Overwrite Value column of these headers, as shown below. This is the domain known by Session Manager.
- Default values were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

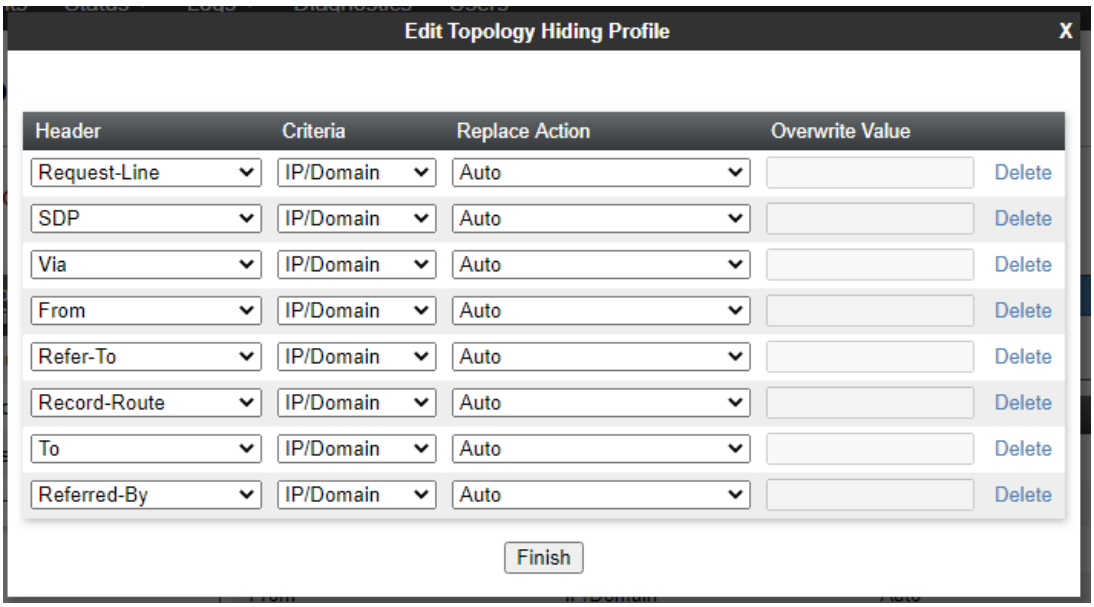


7.5.2. Topology Hiding Profile – Service Provider

To add the Topology Hiding Profile in the service provider direction, select Topology Hiding from the Global Profiles menu on the left-hand side, select default from the list of pre-defined profiles and click the Clone button (not shown).

- Enter a Clone Name such as the one shown below.
- Click **Finish**.

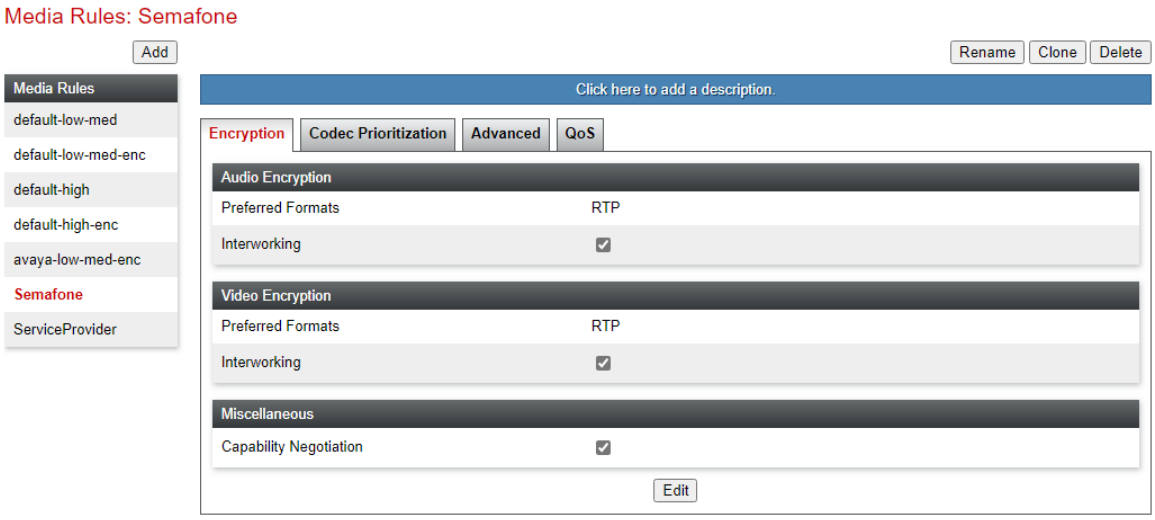




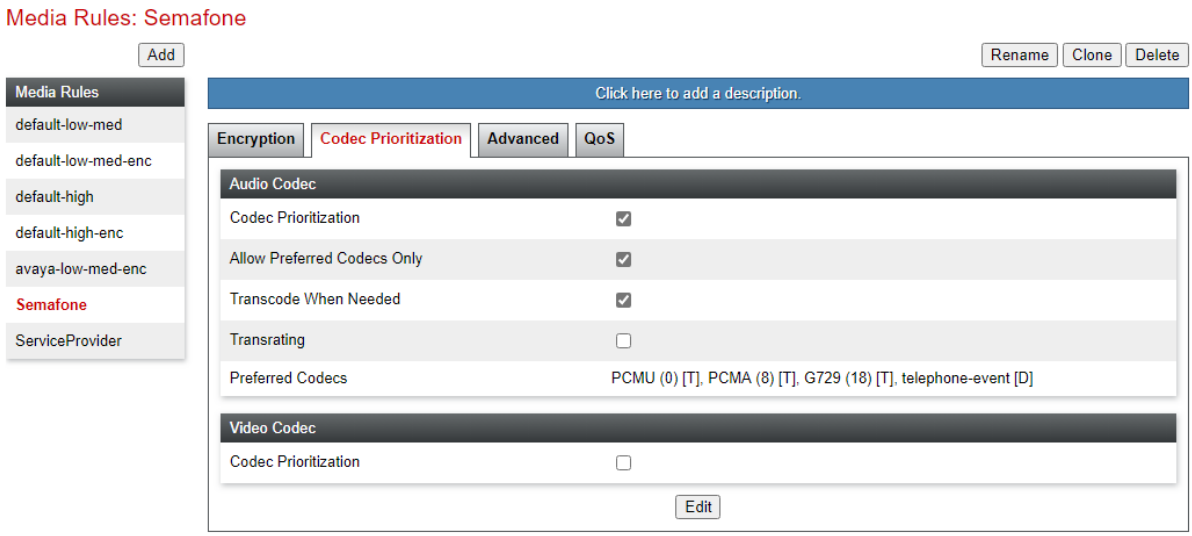
7.6. Define Media Rules

Media rules are used 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. Note that during Compliance Testing calls to all the SIP Servers used the same Media Rules.

To define a new Media Rule, navigate to **Domain Policies → Media Rules**. Clone **default-low-med** rule and provide a **Clone Name** for the new Media Rule (not shown). Once added, select the newly added **Media Rule** and Edit the **Encryption** tab, configure as shown in the screen capture below:



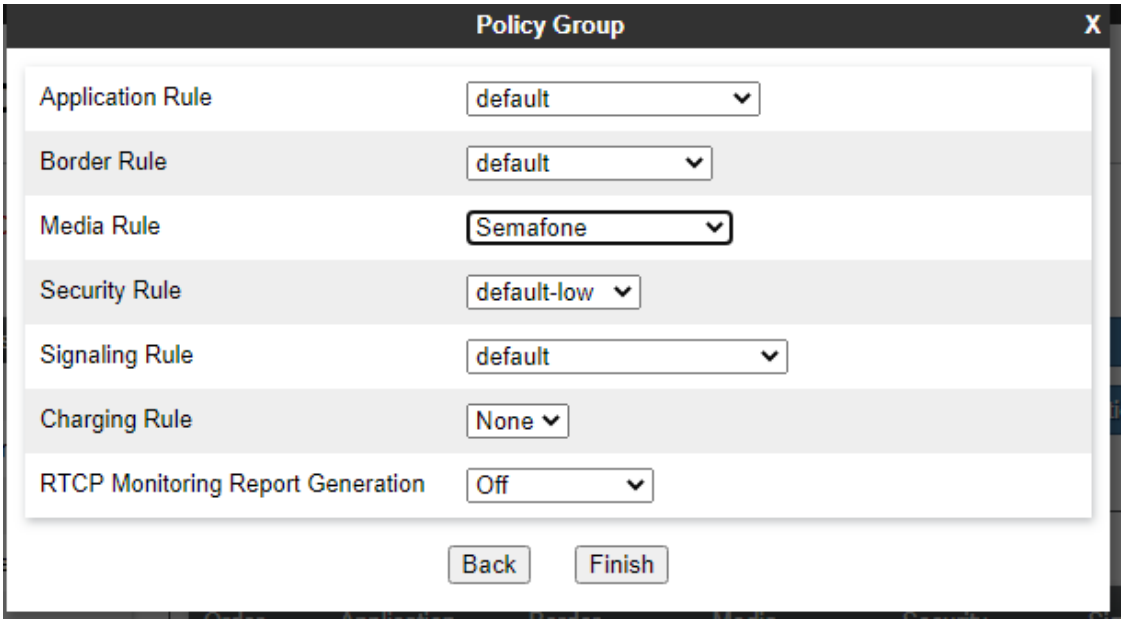
Select the **Codec Prioritization** tab and **Edit.** Configure as shown in the screen capture below:



7.7. Define Endpoint Policy Groups

Endpoint policy groups comprise a group of endpoint policy sets, all of which are specifically configured using a number of relevant parameters. Recently added Media Rule is associated with an Endpoint Policy Group.

To add an Endpoint Policy Group, navigate to **Domain Policies → Endpoint Policy Groups**. Clone **default-low** profile and provide a **Clone Name** for the new Endpoint Policy Group (not shown). Once added, **Edit** the newly cloned group and set the **Media Rule** to the Media Rule added in **Section 7.6.** Select **Finish** once done.



7.8. Signaling Interface

Signaling Interface needs to be defined for each SIP Server and SIP Remote Workers for SIP signaling. Navigate to **Networks & Flows → Signaling Interface** to define a new Signaling Interface. During the Compliance Testing the following interfaces were defined.

- **Ext-SignalingSP**: Signaling interface used by Service Provider to send and receive calls.
- **Int-Signaling1**: Signaling interface used by Session Manager to send and receive calls.
- **Ext-SignalingDirty**: Signaling interface used by Semafone Voice+ Dirty to send and receive calls.
- **Ext-SignalingClean**: Signaling interface used by Semafone Voice+ Clean to send and receive calls.

Note that, though TLS was used for Semafone Voice+ connectivity during the Compliance testing, TCP and UDP are also supported by Semafone Voice+.

Signaling Interface

Signaling Interface

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Int-Signaling1	10.128.224.164 IntA1 (A1, VLAN 0)	5060	5060	5061	SBCInt164	Edit Delete
Ext-SignalingSP	10.128.226.183 ExtB1 (B1, VLAN 0)	5060	5060	5061	SBCExt183	Edit Delete
Ext-SignalingDirty	10.128.226.179 ExtB1 (B1, VLAN 0)	5060	5060	5061	SemafoneDirty	Edit Delete
Ext-SignalingClean	10.128.226.181 ExtB1 (B1, VLAN 0)	5060	5060	5061	SemafoneClean	Edit Delete

7.9. Media Interface

Media Interface needs to be defined for each SIP Server and SIP Remote Workers to send and receive media (RTP or SRTP). Navigate to **Networks & Flows → Media Interface** to define a new Media Interface. During the Compliance Testing the following interfaces were defined.

- **Int-Media**: Interface used by Session Manager to send and receive media.
- **Ext-MediaSP**: Interface used by Service Provider to send and receive media.
- **Ext-MediaDirty**: Interface used by Semafone Voice+ Dirty to send and receive media.
- **Ext-MediaClean**: Interface used by Semafone Voice+ Clean to send and receive media.

Media Interface

Media Interface

Add

Name	Media IP Network	Port Range	
Ext-MediaSP	10.128.226.183 ExtB1 (B1, VLAN 0)	35000 - 40000	Edit Delete
Int-Media	10.128.224.164 IntA1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Ext-MediaDirty	10.128.226.179 ExtB1 (B1, VLAN 0)	20000 - 60000	Edit Delete
Ext-MediaClean	10.128.226.181 ExtB1 (B1, VLAN 0)	20000 - 60000	Edit Delete

7.10. Server 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 call flows for Inbound and Outbound calls are show as below through the Avaya SBCE and Semafone Voice+

- Inbound: Service Provider → SBC External Interface → SBC Dirty Interface → Semafone Dirty → Semafone Clean → SBC Clean Interface → SBC Internal Interface → Avaya SM → Avaya Endpoints (Agents)

- Outbound: Avaya Endpoints (Agent) → Avaya SM → SBC Internal Interface → SBC Clean Interface → Semafone Clean → Semafone Dirty → SBC Dirty Interface → SBC External Interface → Service Provider

Server Flows combine the previously defined profiles for Semafone Voice+/Session Manager and VoIP Service Provider. These End Point Server Flows allow calls to be routed to and from Semafone Voice+/Session Manager/VoIP Service Provider. Navigate to **Network & Flows → End Point Flows → Server Flows.** The screen capture below displays the configured Server Flows. The screen capture below displays the Server flows used during the Compliance test.

End Point Flows

Subscriber Flows | Server Flows

Add

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

Hover over a row to see its description.

SIP Server: Semafone Clean

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	SemafoneClear	*	Int-Signaling1	Ext-SignalingClean	Semafone	To_SM	View	Clone	Edit	Delete

SIP Server: Semafone Dirty

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	SemafoneDirty	*	Ext-SignalingSP	Ext-SignalingDirty	Semafone	To_ServiceProvider	View	Clone	Edit	Delete

SIP Server: ServiceProvider

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	ServiceProvider	*	Ext-SignalingDirty	Ext-SignalingSP	Semafone	To_Semafone_Dirty	View	Clone	Edit	Delete

SIP Server: SessionManager

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	SessionManager	*	Ext-SignalingClean	Int-Signaling1	Semafone	To_Semafone_Clean	View	Clone	Edit	Delete

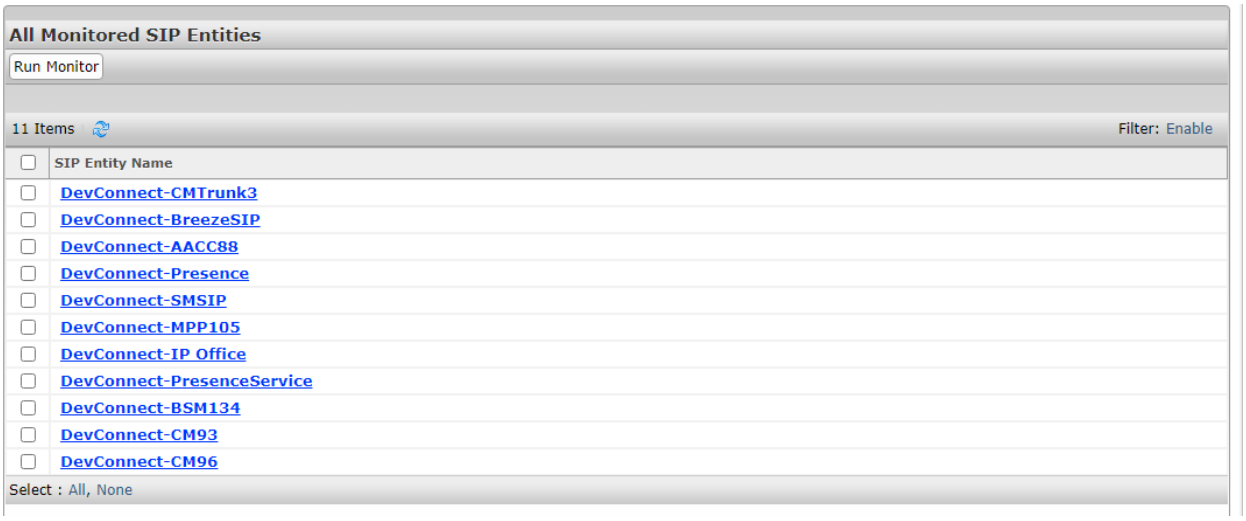
8. Configure Semafone Voice+

All configuration related to Semafone Voice+ is performed by Semafone engineers and, thus, is not documented.

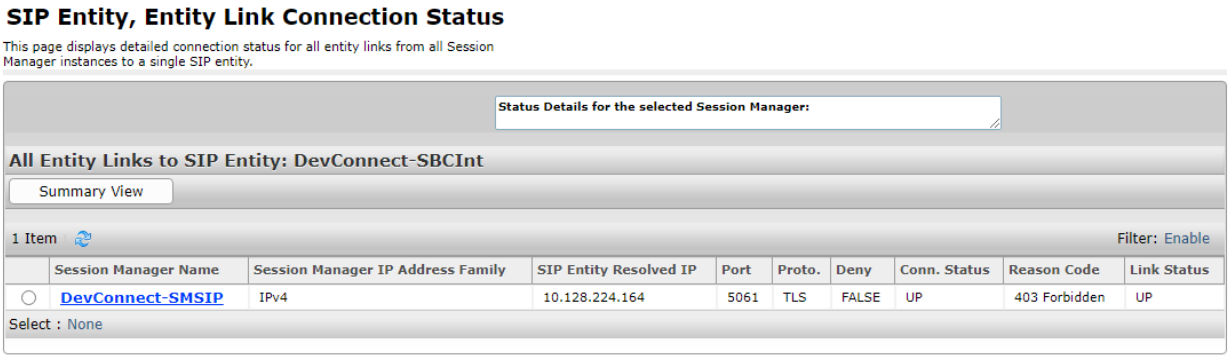
9. Verification Steps

9.1. Verify Entity Link to Avaya Session Border Controller for Enterprise and Entity Link to Avaya Aura Communication manager

To verify SIP connectivity to Avaya SBCE, via System Manager, navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring.** Under the **All Monitored SIP Entities,** select the Avaya SBCE Entity.



Verify **Conn. Status** is **UP.**



Select the Avaya Communication Manager Entity and verify **Conn. Status** is **UP.**

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: DevConnect-CMTrunk3

Summary View

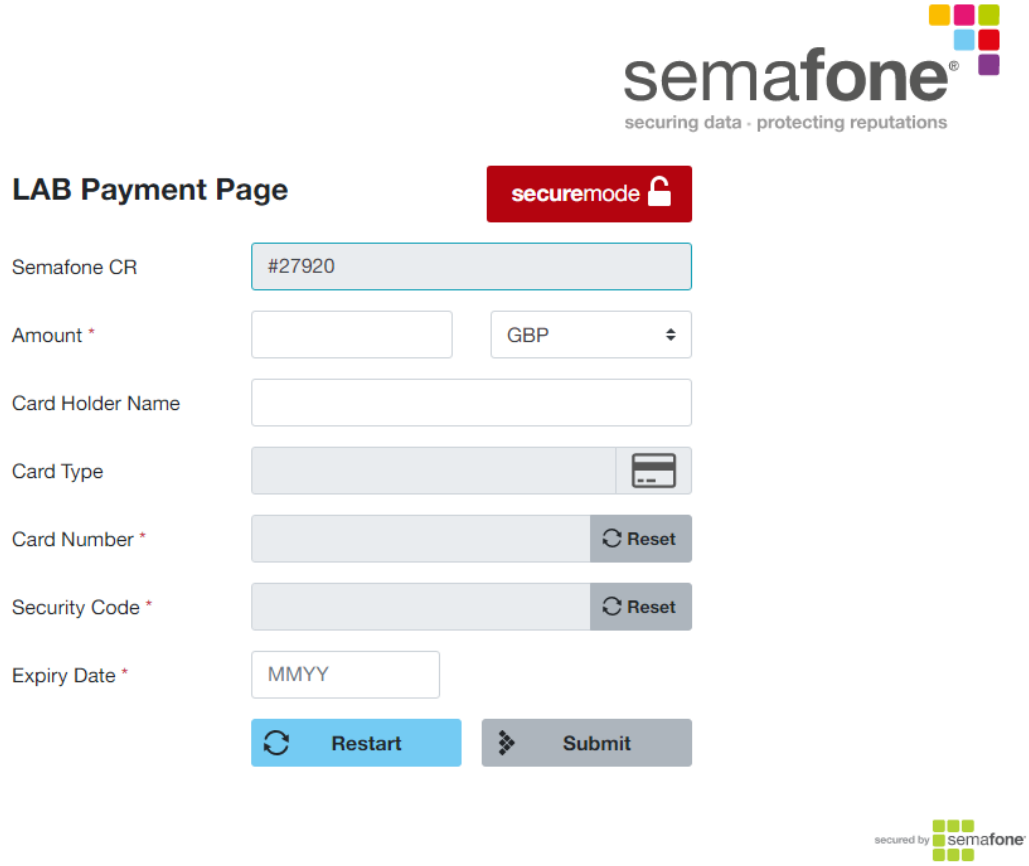
1 Item | Filter: Enable

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	DevConnect-SMSIP	IPv4	10.30.5.93	5071	TLS	FALSE	UP	200 OK	UP

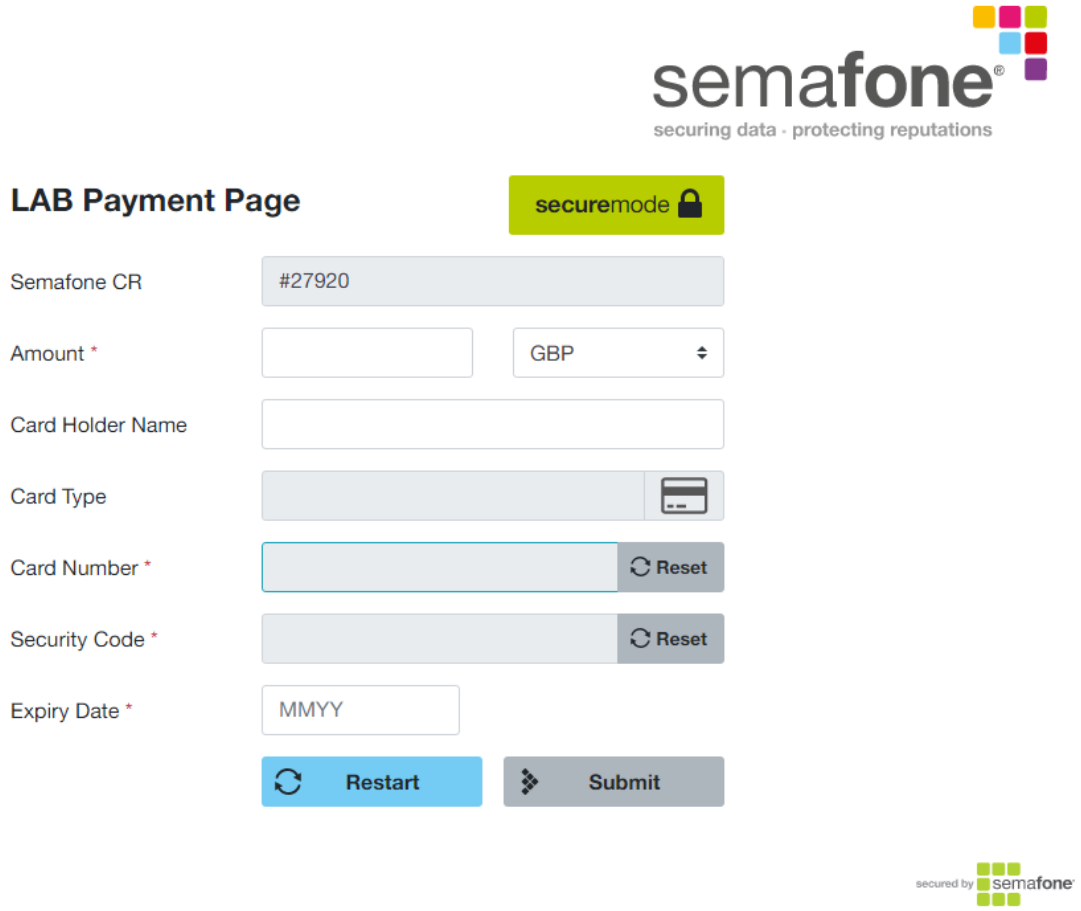
Select : None

9.2. Verify Call Routing, Semafone DTMF Manipulation and Semafone Payment Page Operation

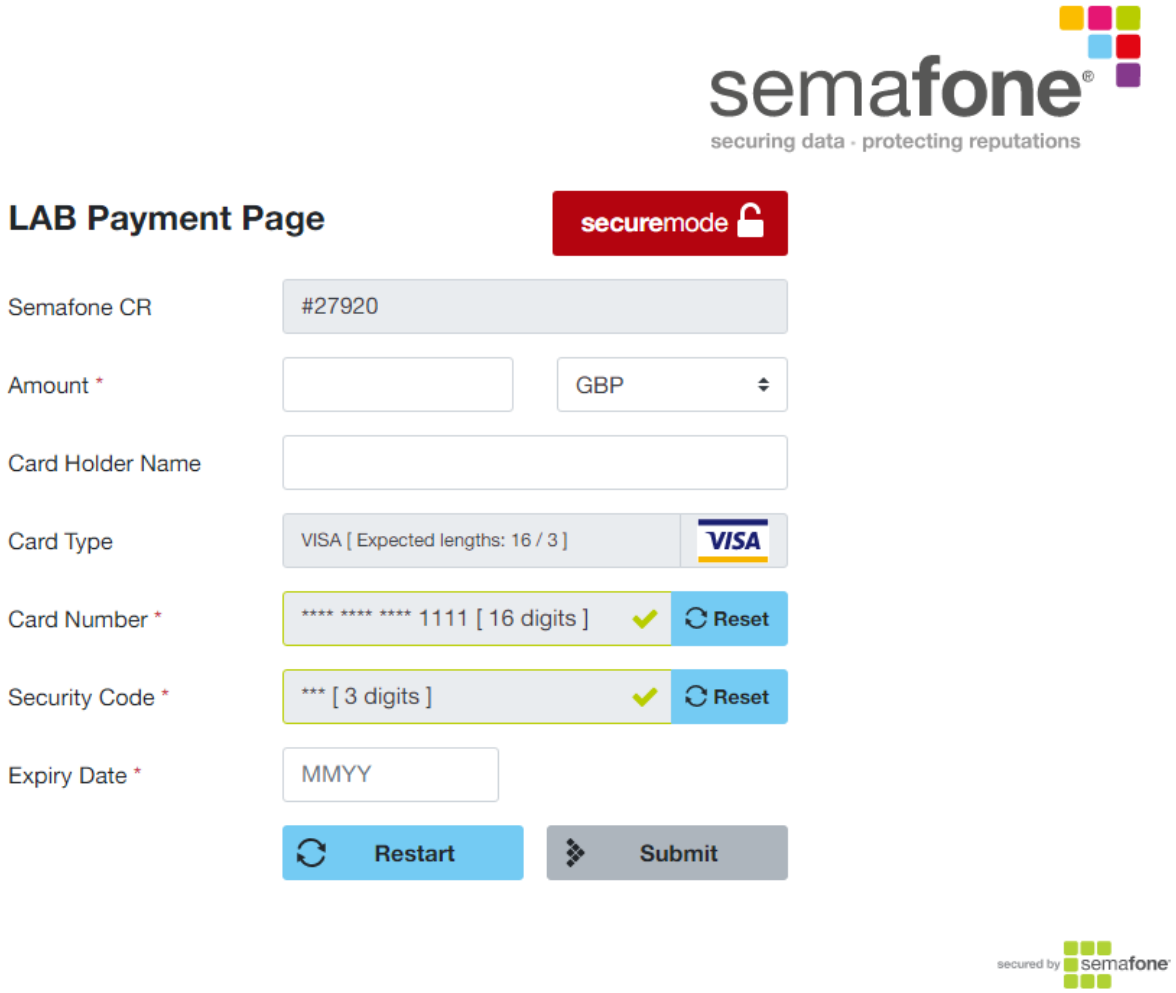
Place a call to/from the PSTN, ensure the call can be answered, controlled and terminated by a call center agent. When the agent receives a call, the agent navigates to the simulated payment page, retrieves the code displayed in the **Semafone CR** field, and enter the codes on the telephone keypad.



Verify the padlock icon changes indicating the secured state has been entered



Enter the appropriate card number using the keypad on the customer telephone and ensure the correct digits and number of digits are accurately captured on the payment page. Verify the agent hears only generic DTMF tones, and not that of the actual card number entered.



10. Conclusion

Semafone Voice+ Rushmore was able to successfully interoperate with Avaya Aura® environment and Avaya Session Border Controller for Enterprise.

11. Additional References

Documentation related to Avaya can be obtained from https://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020

[2] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 5, July 2020

[3] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020

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.