Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Windstream SIP Trunking Service with Avaya IP Office 10 and Avaya Session Border Controller for Enterprise Release 7.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Windstream Session Initiation Protocol (SIP) Trunking with Avaya IP Office Release 10 and Avaya Session Border Controller for Enterprise Release 7.1.

Windstream SIP Trunking provides PSTN access via a SIP trunk between the enterprise and the Windstream network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Windstream is a member of the Avaya DevConnect Service Provider program. 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 procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Windstream and the Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of an Avaya IP Office Server Edition release 10, Avaya Session Border Controller for Enterprise release 7.1 (Avaya SBCE), Avaya Voicemail Pro, Avaya Communicator for Windows, and Avaya H.323, SIP, digital, and analog endpoints.

The Windstream SIP Trunking service referenced within these Application Notes is designed for business customers. The service enables local long distance and international PSTN calling via standards-based SIP trunks as an alternative to legacy analog or digital trunks, without the need for additional TDM enterprise gateways and the associated maintenance costs.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office to connect to Windstream SIP Trunking service via the Avaya SBCE. This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**.

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 the Windstream SIP Trunking service did not include use of any specific encryption features as requested by Windstream.

2.1. Interoperability Compliance Testing

A simulated enterprise site with Avaya IP Office was connected to Windstream SIP Trunking service via the Avaya SBCE. To verify SIP trunking interoperability, the following features and functionality were exercised during the interoperability compliance test:

- Response to SIP OPTIONS queries.
- SIP trunk registration and authentication.
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound long holding time call stability.
- Various call types including: local, long distance, international, outbound toll-free, operator service and directory assistance.
- Codec G.711U and G.729.
- Caller number/ID presentation.
- Privacy requests (i.e. caller anonymity) and Caller ID restriction for inbound and outbound calls.
- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- Telephony features such as hold and resume, transfer, and conference.
- Fax G.711 mode.
- Off-net call forwarding.
- Twinning to mobile phones on inbound calls.
- Avaya Communicator for Windows.
- Avaya Communicator for Web client (WebRTC).
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

Note:
Remote Worker and Avaya Communicator for Web (WebRTC) were tested as part of this solution. The configuration necessary to support remote worker and Avaya Communicator for Web is beyond the scope of these Application Notes and are not included in these Application Notes. For these configuration details, see **Reference [8] and [9]**.

2.2. Test Results

Windstream SIP Trunking passed compliance testing.

Items supported or not tested included the following:

- Call redirection using REFER method is not supported by Windstream.
- Inbound Toll-Free, Local Directory Assistance, Emergency are supported but not tested.
- Fax T.38 is not supported.

Interoperability testing of Windstream SIP Trunking was completed with successful results for all test cases.

2.3. Support

For technical support on the Avaya products described in these Application Notes, visit http://support.avaya.com.

For technical support on Windstream SIP Trunking, contact Windstream at https://www.windstream.com.

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to the Windstream SIP Trunking service via the Avaya SBCE through the public IP network. For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

Located at the enterprise site is an Avaya IP Office Server Edition with an Avaya IP 500 V2 Expansion System which provides connections for 16 digital stations and the extension PHONE 8 card which provides connections for 8 analog stations to the PSTN as well as 64-channel VCM (Voice Compression Module) for supporting VoIP codecs. The LAN1 port of Avaya IP Office is connected to the enterprise LAN while the LAN2 port is connected to the public IP network via Avaya SBCE. Endpoints include an Avaya 9600 Series IP Telephone (with H.323 firmware), Avaya 11x0 Series IP Telephone (with SIP firmware), an Avaya 9508 Digital Telephone, an Avaya Symphony 2000 Analog Telephone and an Avaya Communicator for Windows. A separate Windows PC runs Avaya IP Office Manager to configure and administer the Avaya IP Office.

Mobility Twinning is configured for some of the Avaya IP Office users so that calls to these user phones will also ring and can be answered at the configured mobile phones.

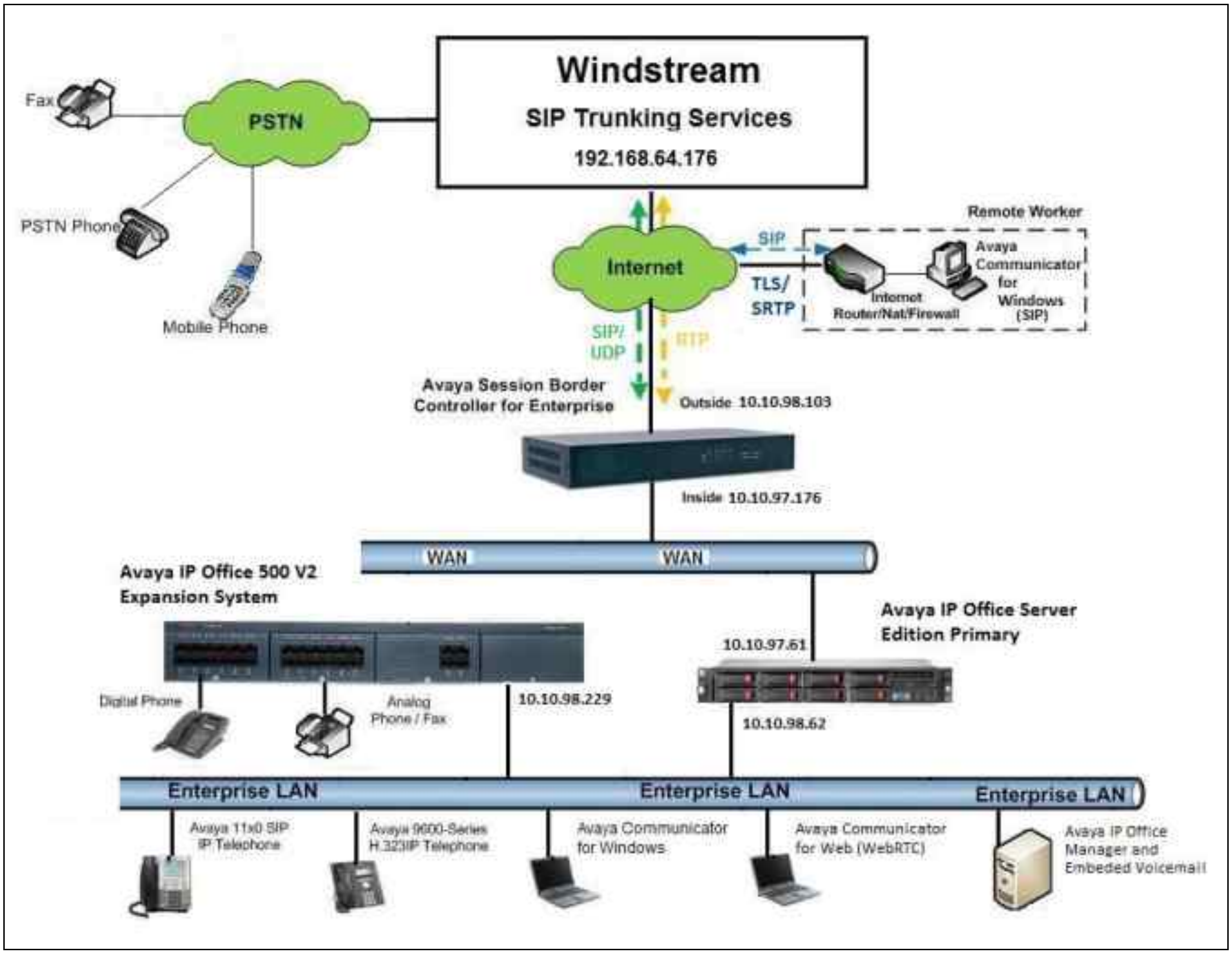


Figure 1: Test Configuration for Avaya IP Office with Windstream SIP Trunking Service

The transport protocol between the Avaya SBCE and Windstream, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network (LAN), is SIP over TLS.

For the purposes of the compliance test, Avaya IP Office users dialed a short code of 6 + N digits to send digits across the SIP trunk to Windstream. The short code of 6 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Windstream and no digit manipulation programming was required on Avaya SBCE. For calls within the North American Numbering Plan (NANP), the user would dial 11 (1 + 10) digits. Thus for these NANP calls, Avaya IP Office would send 11 digits in the Request URI and the To field of an outbound SIP INVITE message. Avaya IP Office was configured to send 10 digits in the From field. Windstream SIP Trunking would send 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment	**Release**
Avaya IP Office Server Edition	10.0.0.3.0.5
Avaya IP Office 500v2 (Expansion)	10.0.0.3.0.5
Avaya IP Office Manager	10.0.0.3.0.5
Avaya WebRTC Gateway	10.0.0.3.0 build 10
Avaya IP Office Embedded Voicemail	10.0.0.3.0.5
Avaya 11x0 IP Telephone (SIP)	SIP11x0e04.04.23.00
Avaya 9621G IP Telephone (H.323)	6.6.401
Avaya Communicator for Windows	2.0.3.237
Avaya Communicator for Web (WebRTC)	1.0.16.2220
Avaya Digital Telephone (9508)	0.45
Windstream SIP Trunking Service Components	
Component	Release
Broadsoft	R17SP4
Cisco UBE	15.4(3)M5

Note: The test results documented in these Application Notes apply to standalone IP Office V2 deployments as well as all configurations of IP Office Server Edition.

5. Configure Avaya IP Office

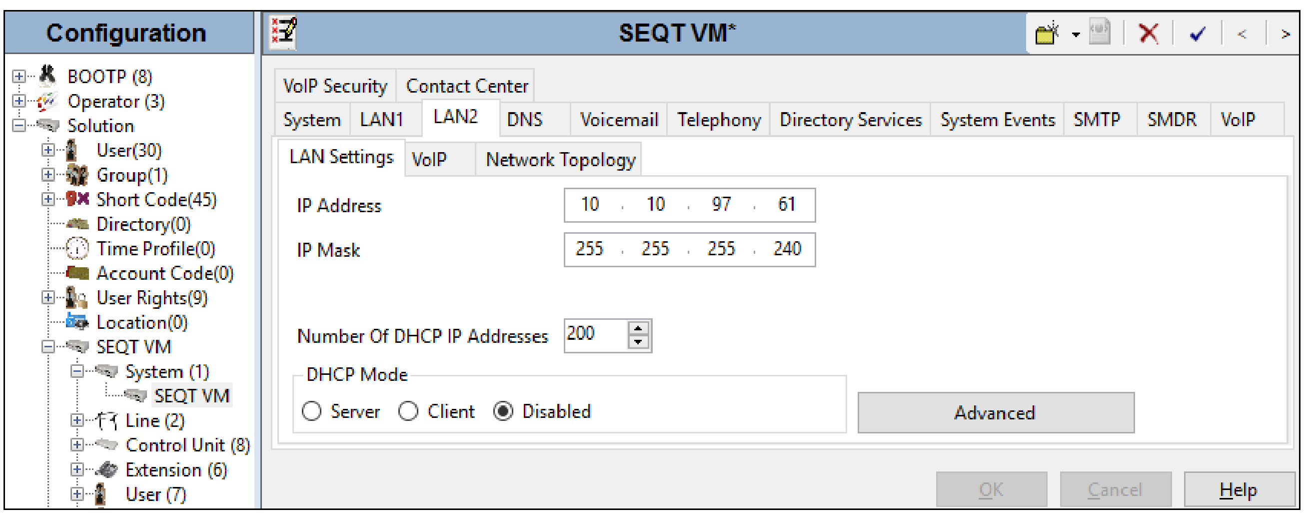
This section describes the Avaya IP Office configuration to support connectivity to Windstream SIP Trunking service through Avaya SBCE. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials. A management window will appear similar to the one shown in the next section. The appearance of the IP Office Manager can also be customized using the **View** menu. In some screens presented in this section, the **View** menu was configured to show the **Navigation** pane on the left side, the **Group** pane in the center, and the **Details** pane on the right side. Some of these panes will be referenced in Avaya IP Office configuration. Proper licensing as well as standard feature configurations that are not directly related to the interface with the service provider (such as LAN interface to the enterprise site) is assumed to be already in place.

5.1. LAN Settings

In the sample configuration, the **SEQT VM** was used as the system name and the WAN port was used to connect the Avaya IP Office to the public network. The LAN2 settings correspond to the WAN port on the Avaya IP Office.

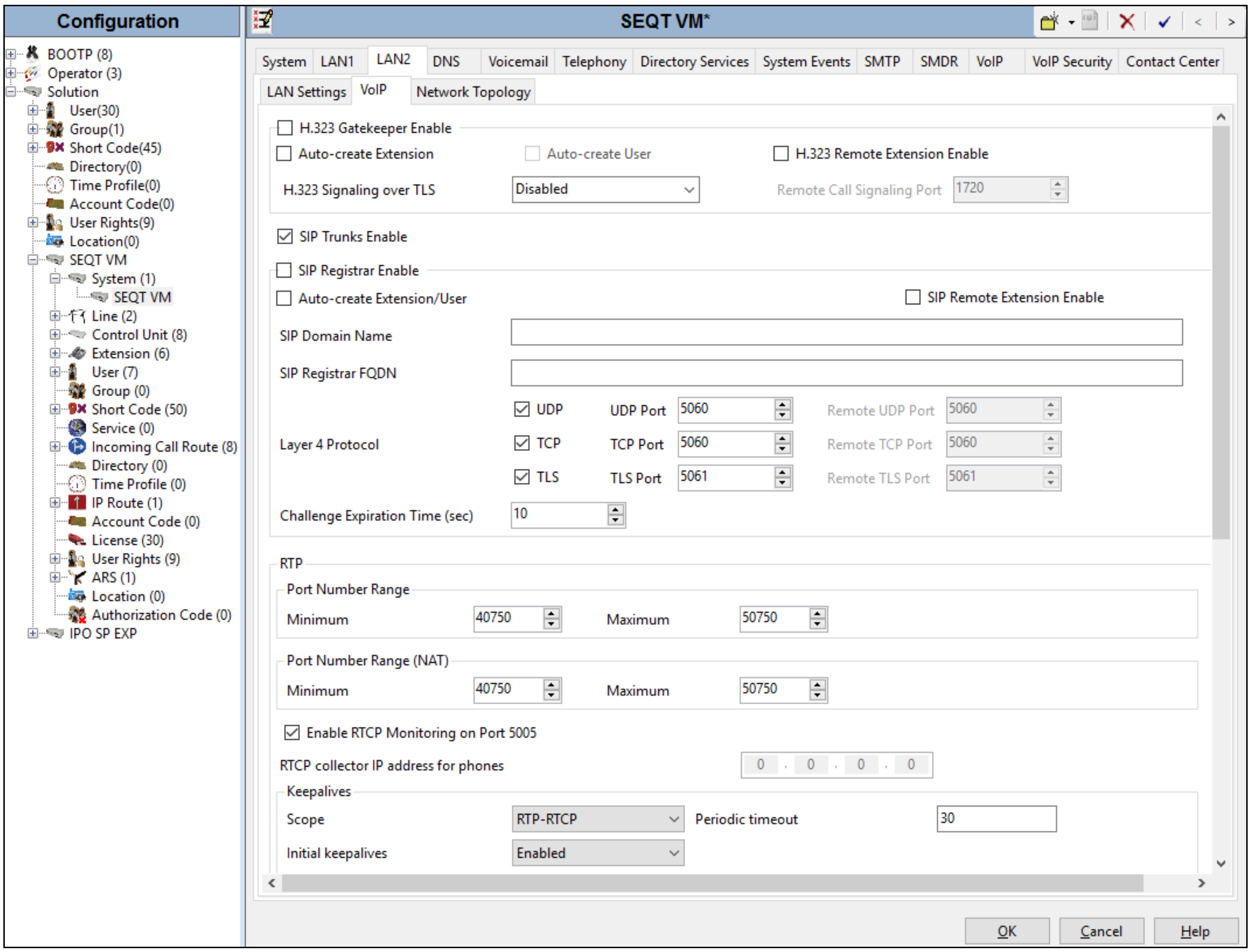
To access the LAN settings, first navigate to **System (1) → SEQT VM** in the **Navigation** pane and then navigate to the **LAN2 → LAN Settings** tab in the **Details** pane.

- Set the **IP Address** field to the IP address assigned to the IP Office WAN port.
- Set the **IP Mask** field to the mask used on the public network.
- All other parameters should be set according to customer requirements.
- Click **OK**.



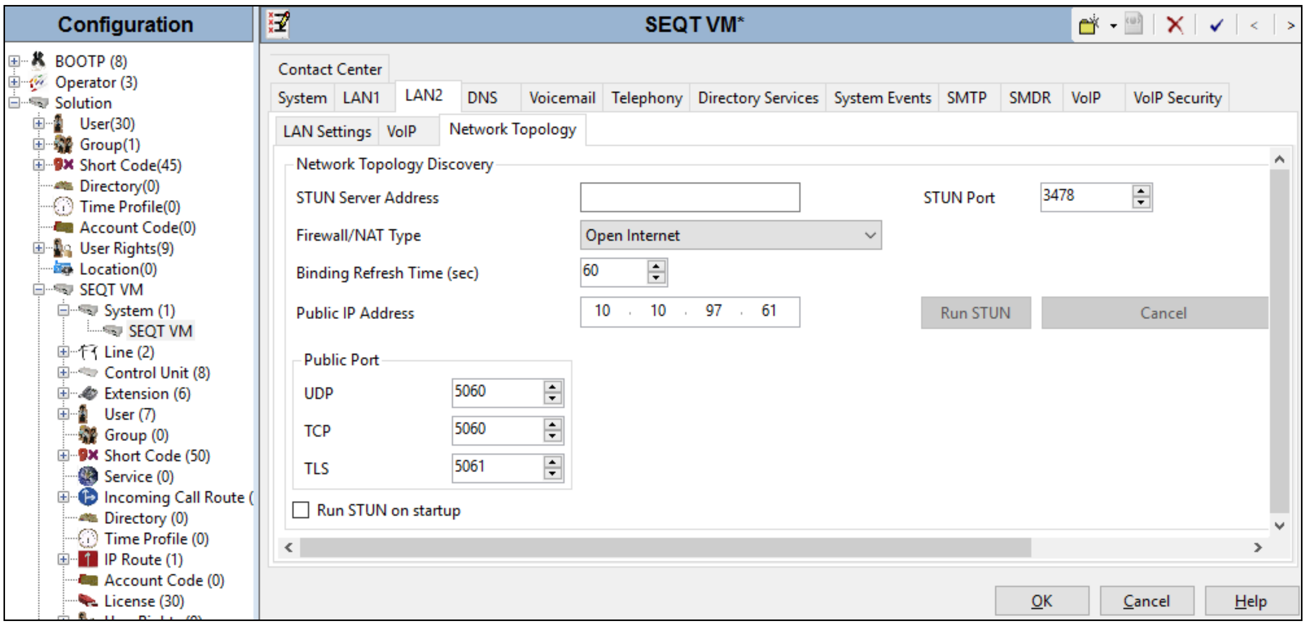
Select the **VoIP** tab as shown in the following screen.

- Ensure **H323 Gatekeeper Enable** box is unchecked.
- The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks to Windstream.
- The **Layer 4 Protocol,** check the **UDP**, **TCP** and **TLS** boxes. Then set **UDP** and **TCP Ports** to ***5060***, and **TLS port** to ***5061***.
- **Enable RTCP Monitoring on Port 5005** and **Keepalives** should be set as shown in capture below.
- All other parameters should be set according to customer requirements**.**
- Click **OK**.



On the **Network Topology** tab in the **Details** pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. No firewall or network address translation (NAT) device was used in the compliance test as shown in **Figure 1**, so the parameter was set to ***Open Internet***. With this configuration, **STUN** will not be used.
- Set **Binding Refresh Time (seconds)** to ***60***. This value is used as one input to determine the frequency at which IP Office will send SIP OPTIONS messages to the service provider.
- Set **Public IP Address** to the IP address of IP Office WAN port. **Public Port** is set to ***5060*** for **UDP** and **TCP**, and ***5061*** for **TLS**.
- All other parameters should be set according to customer requirements.
- Click **OK**.

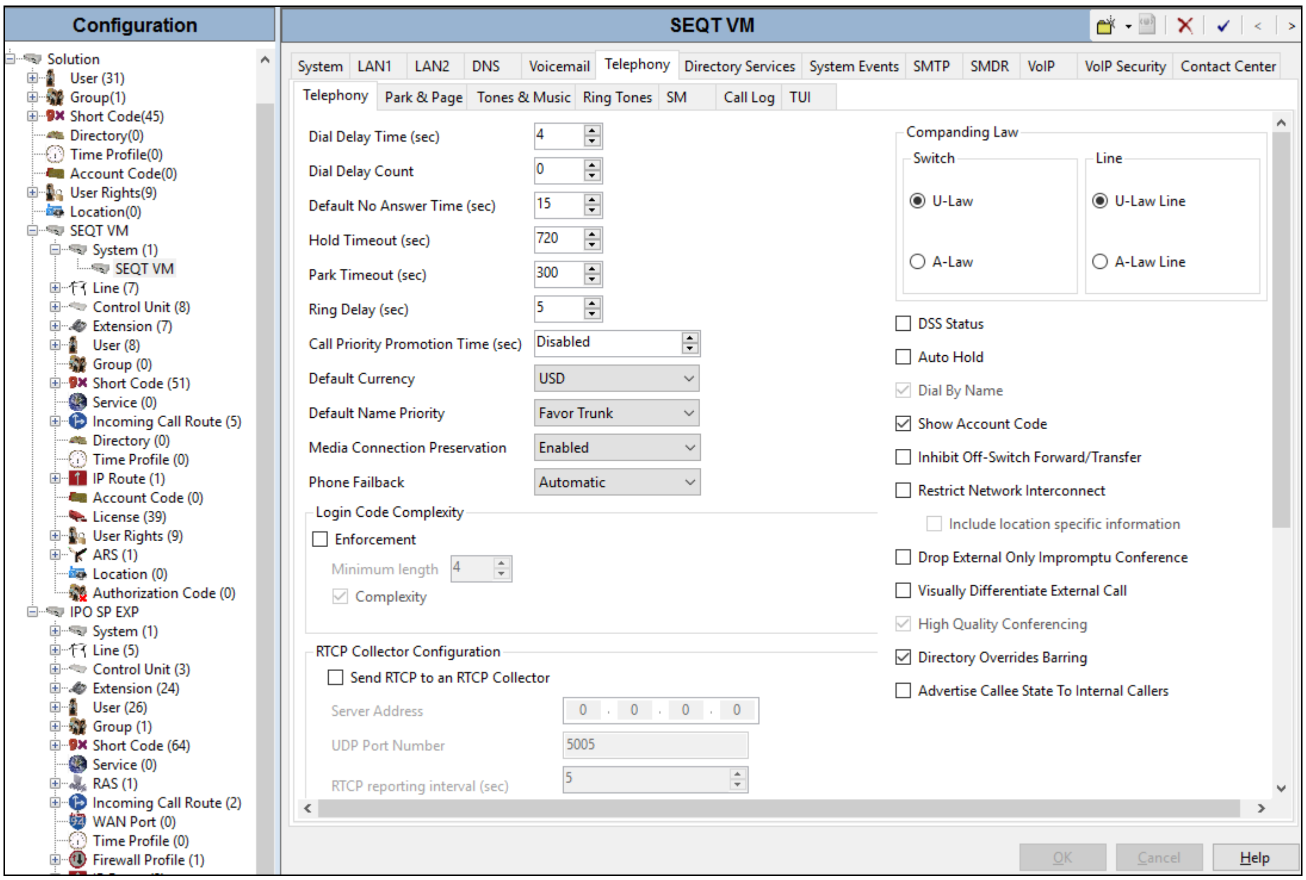


In the compliance test, the LAN1 interface was used to connect IP Office to the enterprise site IP network. The LAN1 interface configuration is not directly relevant to the interface with Windstream SIP Trunking service, and therefore is not described in these Application Notes.

5.2. System Telephony Settings

Navigate to the **Telephony → Telephony** Tab in the **Details** pane.

- Choose the **Companding Law** typical for the enterprise location. ***A-LAW*** is used as member is in Europe.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the service provider across the SIP trunk.
- Check the **Drop External Only Impromptu Conference** box to allow the host of the conference leaving the active call and forcing all the parties off the conference as member requested.
- Other parameters are left at default.
- Click **OK**.



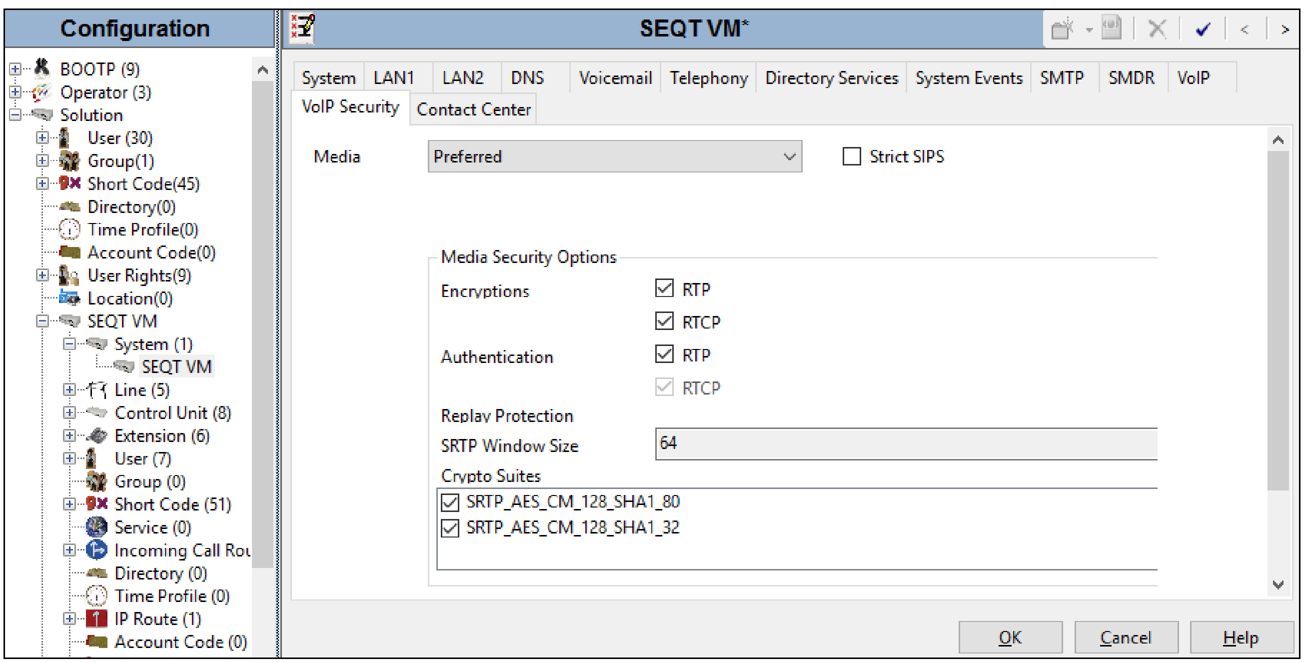
5.3. VoIP Security Settings

When enabling SRTP on the system, the recommended setting for **Media** is ***Preferred***. In this scenario, IP Office uses SRTP if supported by the other end, and otherwise uses RTP. If the ***Enforced*** setting is used, and SRTP is not supported by the other end, the call is not established.

Individual SIP lines and extensions have media security settings that can override system level settings. This can be used for special cases where the trunk or extension setting must be different from the system settings.

In the compliance testing, ***Preferred*** is set at system, trunk and extension level to allow the system to fall back to non-secure media in case there is issue with SRTP. This would help to avoid blackout situation within the enterprise network. In some specific deployments, if supported, ***Enforce***d is set at the trunk level to ensure the secured communication over the public internet using both signaling (TLS) and media (SRTP). Navigate to **System → VoIP Security** tab and configure as follows:

- Select ***Preferred*** for **Media Security.** The system attempts to use secure media first and if unsuccessful, falls back to non-secure media within the IP Office system.
- Check **RTCP** check-box.
- Other parameters are left as default.
- Click **OK**.



5.4. Administer a SIP Line

A SIP line is needed to establish the SIP connection between IP Office and Windstream SIP Trunking service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.4.1** to create the SIP Line from the template.

Some items relevant to a specific customer environment are not included in the template or may need to be updated after the SIP Line is created. Examples include the following:

- IP addresses.
- SIP Credentials (if applicable).
- SIP URI entries.
- Setting of the **Use Network Topology Info** field on the Transport tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.4.2**.

Also, the following SIP Line settings are not supported on Basic Edition:

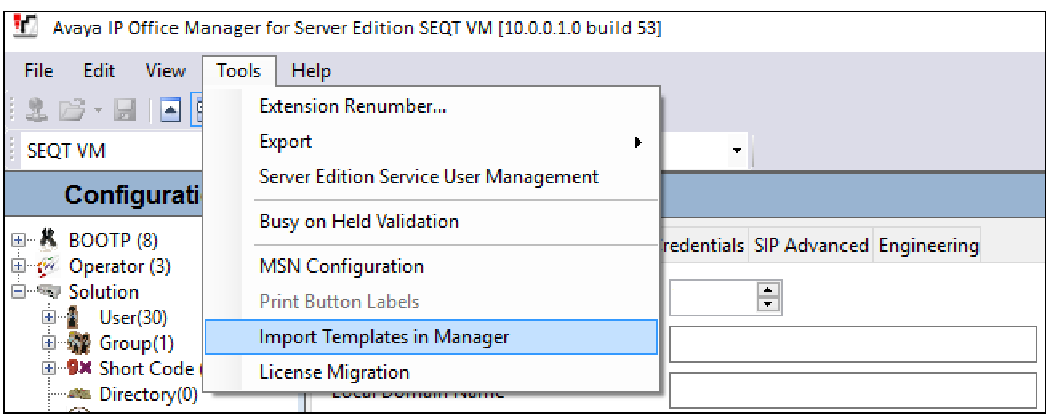
- SIP Line – Originator number for forwarded and twinning calls.
- Transport – Second Explicit DNS Server.
- SIP Credentials – Registration Required.

Alternatively, a SIP Line can be created manually. To do so right-click **Line** in the Navigation Pane and select **New → SIP Line**, then follow the steps outlined in **Sections 5.4.2**.

5.4.1. Create SIP Line from Template

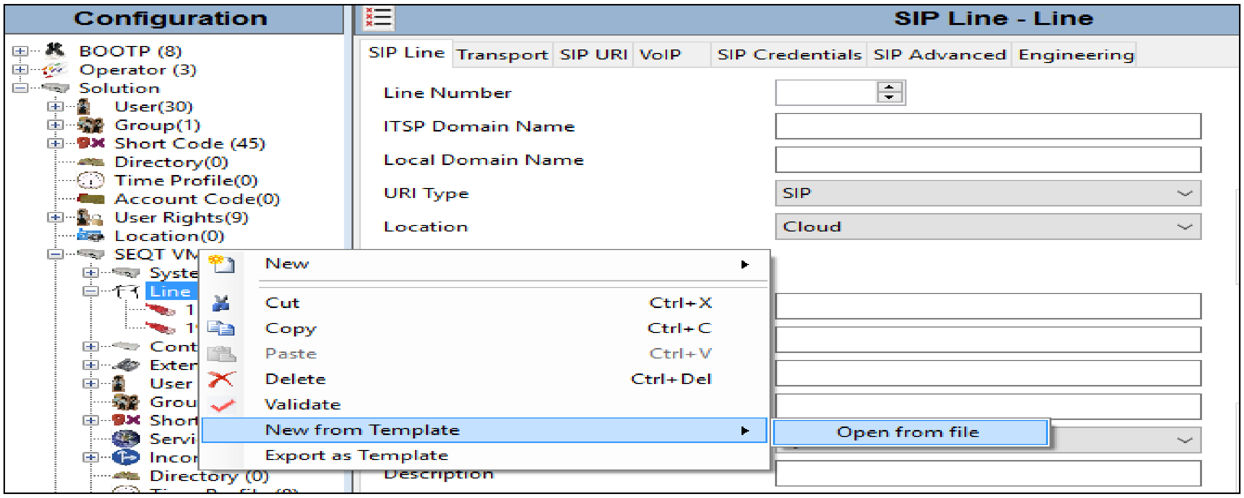
1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **WINDIPO10SBCE71.xml**.

2. Import the template into IP Office Manager.
From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.

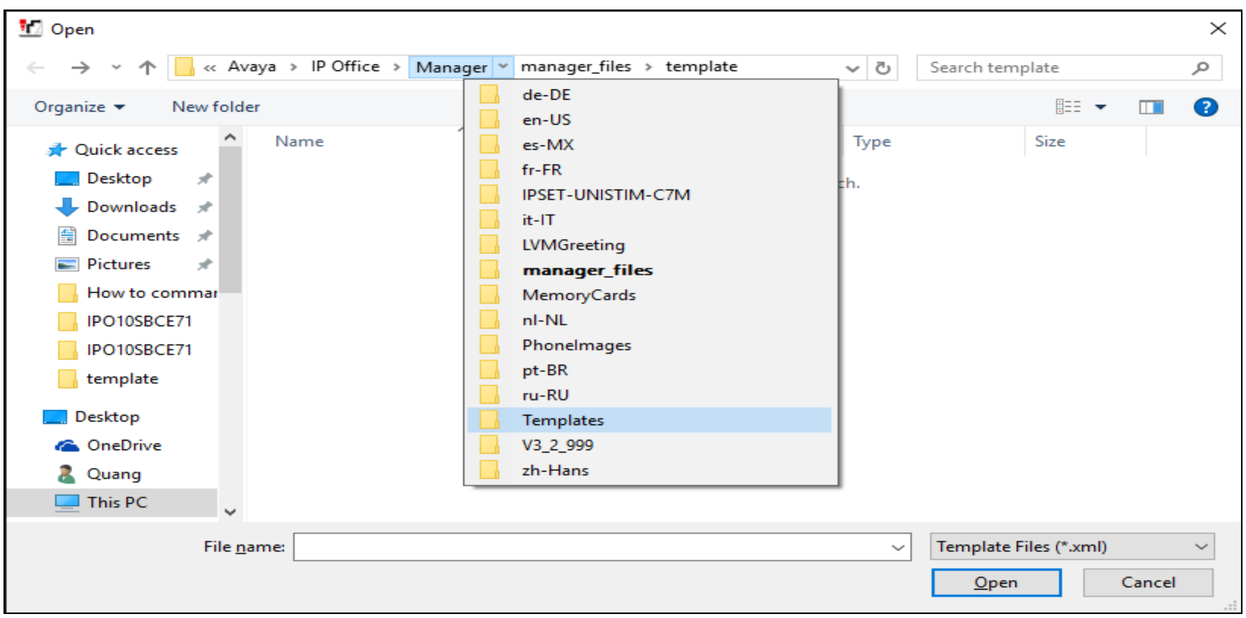


In the resulting pop-up window that appears (not shown), select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window will appear (not shown) stating success or failure. Next click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

3. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template → Open from file**.



4. On the "Open" pop-up window, navigate to **Manager → Templates** and make sure **Template File (.xml)** is the file type selected. Select the file "**WINDIPO10SBCE71.xml**". Click **Open** and **OK** (not shown).

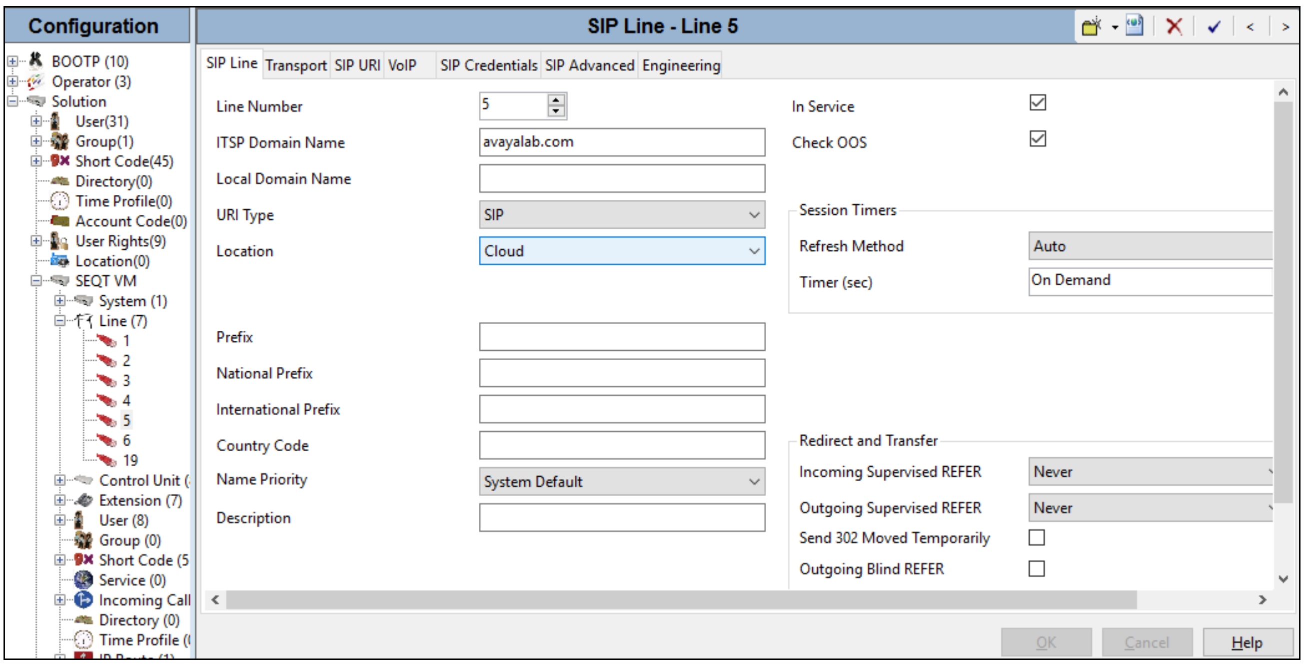


5. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Section 5.4.2.**

5.4.2. Create SIP Line Manually

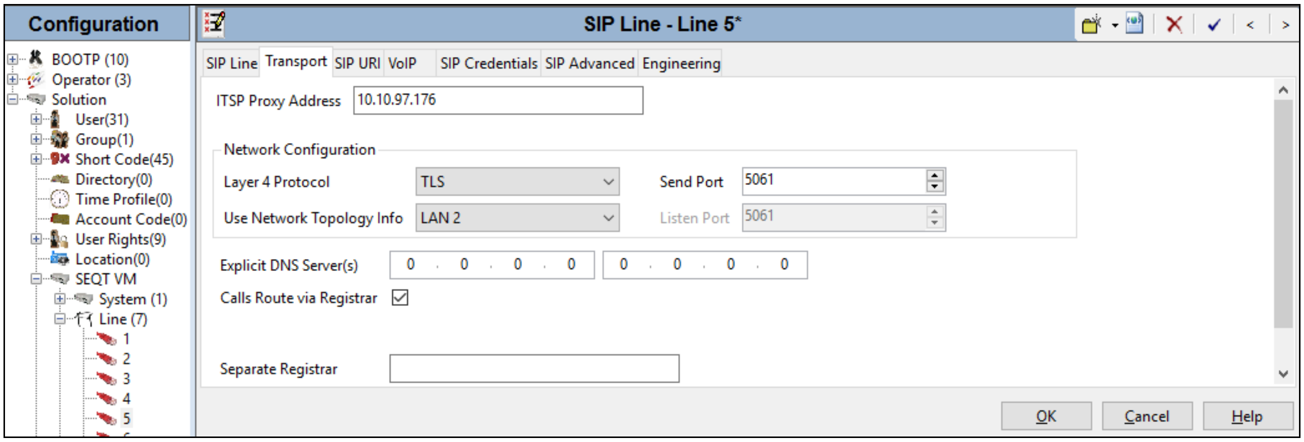
To create a SIP line, begin by navigating to **Line** in the left **Navigation** pane and then right click to select **New → SIP Line**. On the **SIP Line** tab in the **Details** pane, configure the parameters as shown below:

- Set **ITSP Domain Name** to the enterprise domain so that IP Office uses this domain as the host portion of SIP URI in SIP headers such as the From header.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- **Incoming Supervised REFER** is set to ***Never*** to allow IP Office to support call transfer using re-INVITE method only.
- **Outgoing Supervised REFER** is set to ***Never*** to allow IP Office to support call transfer using re-INVITE method only.
- Other parameters are set as default values.
- Click **OK**.



Select the **Transport** tab and enter the following information.

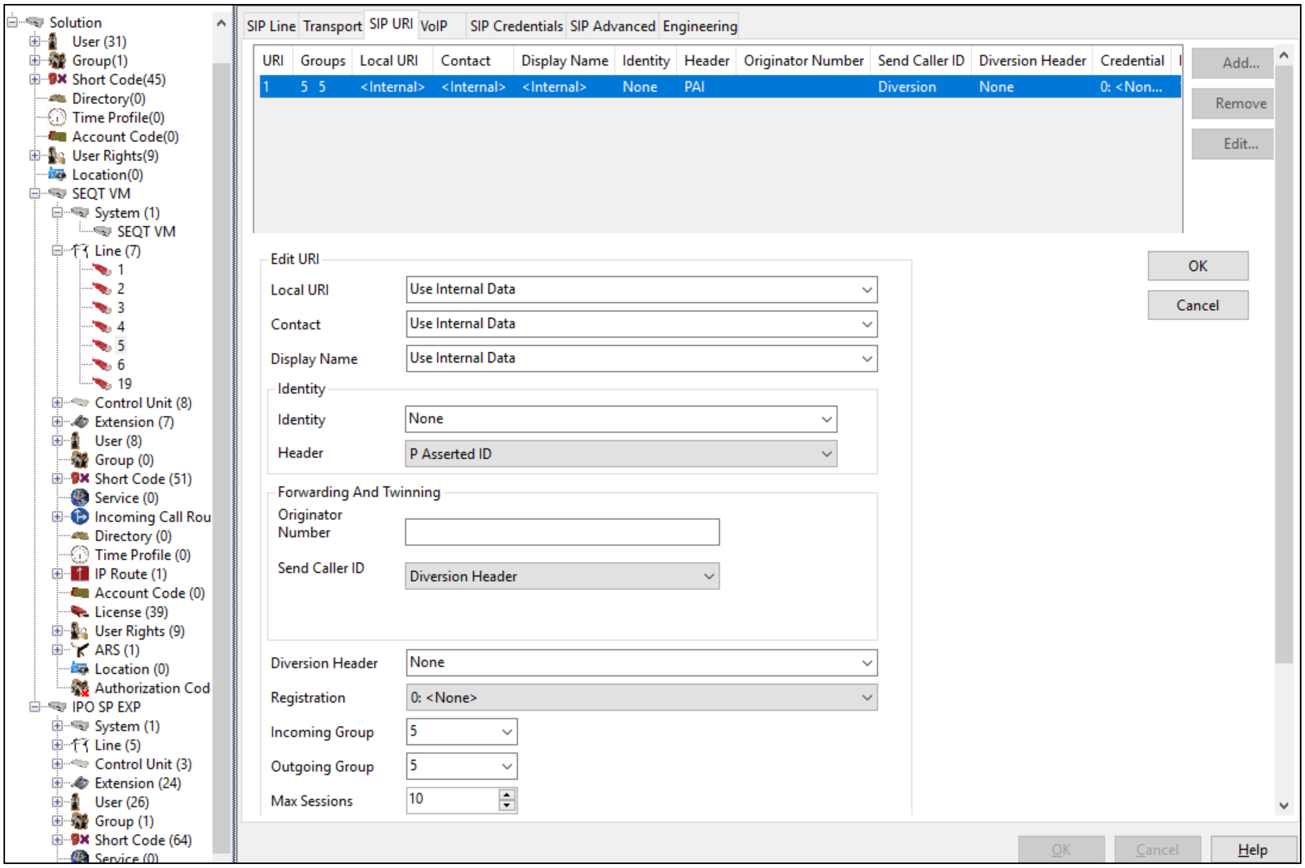
- The **ITSP Proxy Address** is set to the internal interface of Avaya SBCE.
- **Layer 4 Protocol** is set to ***TLS***.
- **Send Port** is set to the port number of IP Office, ***5061***.
- **Use Network Topology Info** parameter is set to ***LAN 2***. This associates the SIP Line with the parameters in the **System → LAN2 → Network Topology** tab.
- Other parameters retain default values in the screen below.
- Click **OK**.



A **SIP URI** entry **Channel 1** is created to match incoming numbers that IP Office will accept on this line. Select the **SIP URI** tab, click **Add** button and then **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit…** button. In the example screen below, a previously configured entry is edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an IP Office user. The entry was created with the parameters shown below:

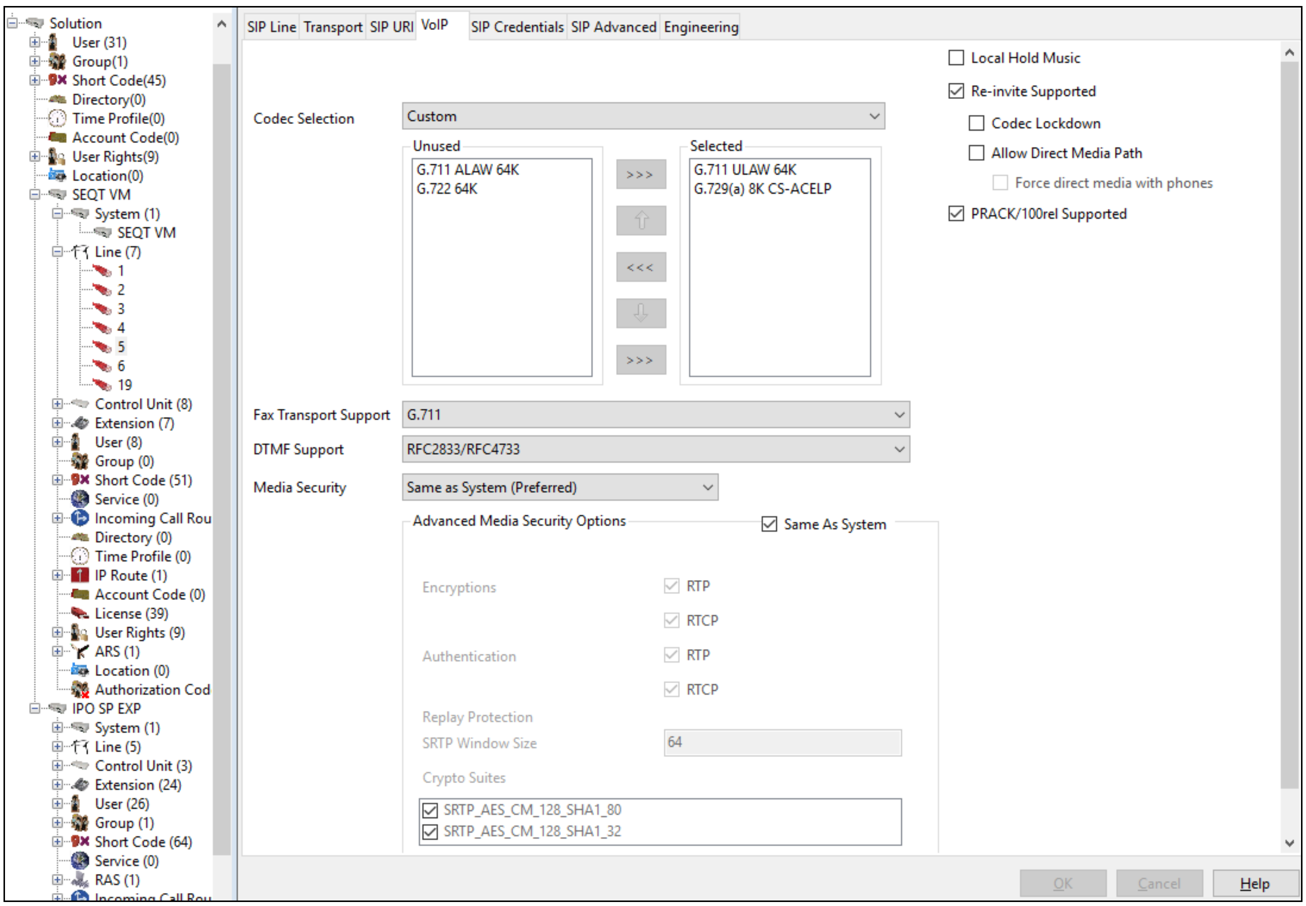
- Set **Local URI**, **Contact** and **Display Name** to ***Use Internal Data***. This setting allows calls on this line which SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.8**.
- Set **Identity** to ***None*** and **Header** to ***P Asserted ID*** for **Identity**.
- Set **Sent Caller ID** to ***Diversion Header*** for **Forward and Twinning**.
- Set **Diversion Header** to ***None***.
- Associate this line with an incoming line group in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. For the compliance test, a new incoming and outgoing group **5** was defined that only contains this line (line 5).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Other parameters retain default values and or set according customer requirements.
- Click **OK**.

SIP Entry **Channel 1** is shown below.



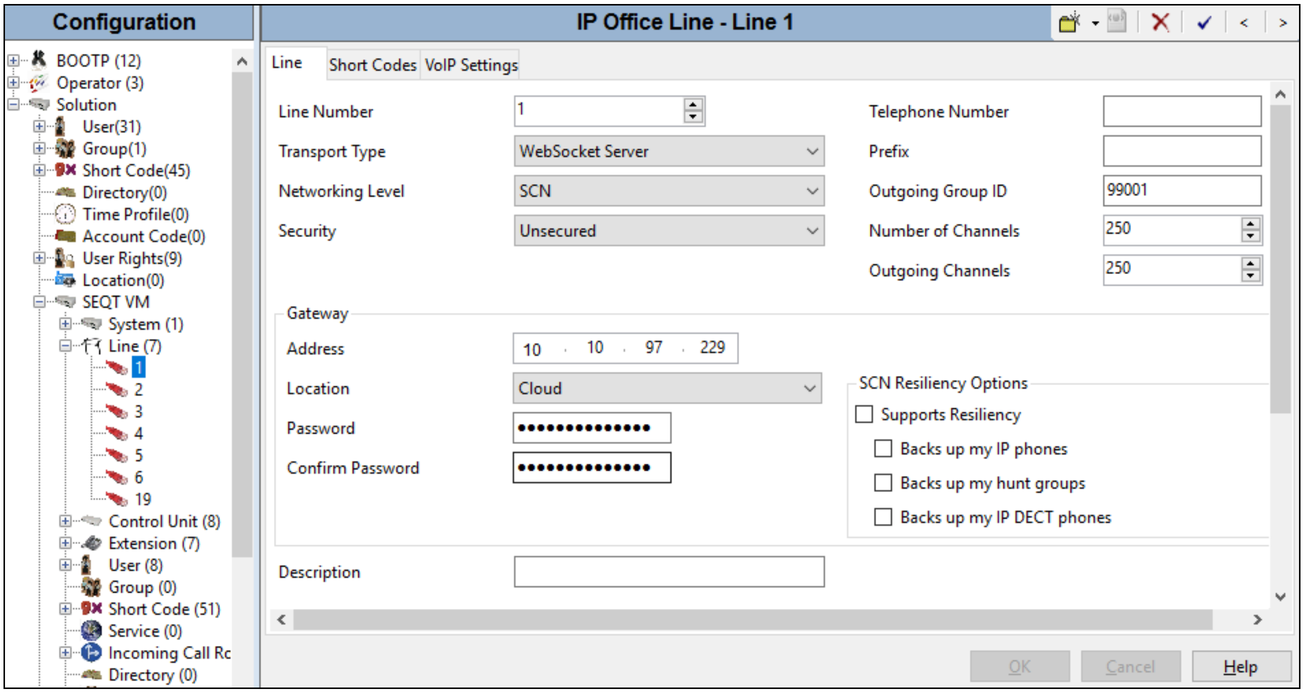
Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- The **Codec Selection** can be selected by choosing ***Custom*** from the pull-down menu, allowing an explicit ordered list of codecs to be specified.
- Selecting ***G.711 ULAW*** and ***G.729*** codec supported by the Windstream SIP Trunking service, in the Session Description Protocol (SDP) offer.
- Set **Fax Transport Support** to ***G.711*** from the pull-down.
- Set the **DTMF Support** field to ***RFC2833/RFC4733*** from the pull-down menu. This directs IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- **Media Security** is set to ***Same as System (Preferred)*** and check the **Same As System** checkbox.
- Default values may be used for all other parameters.
- Click **OK**.

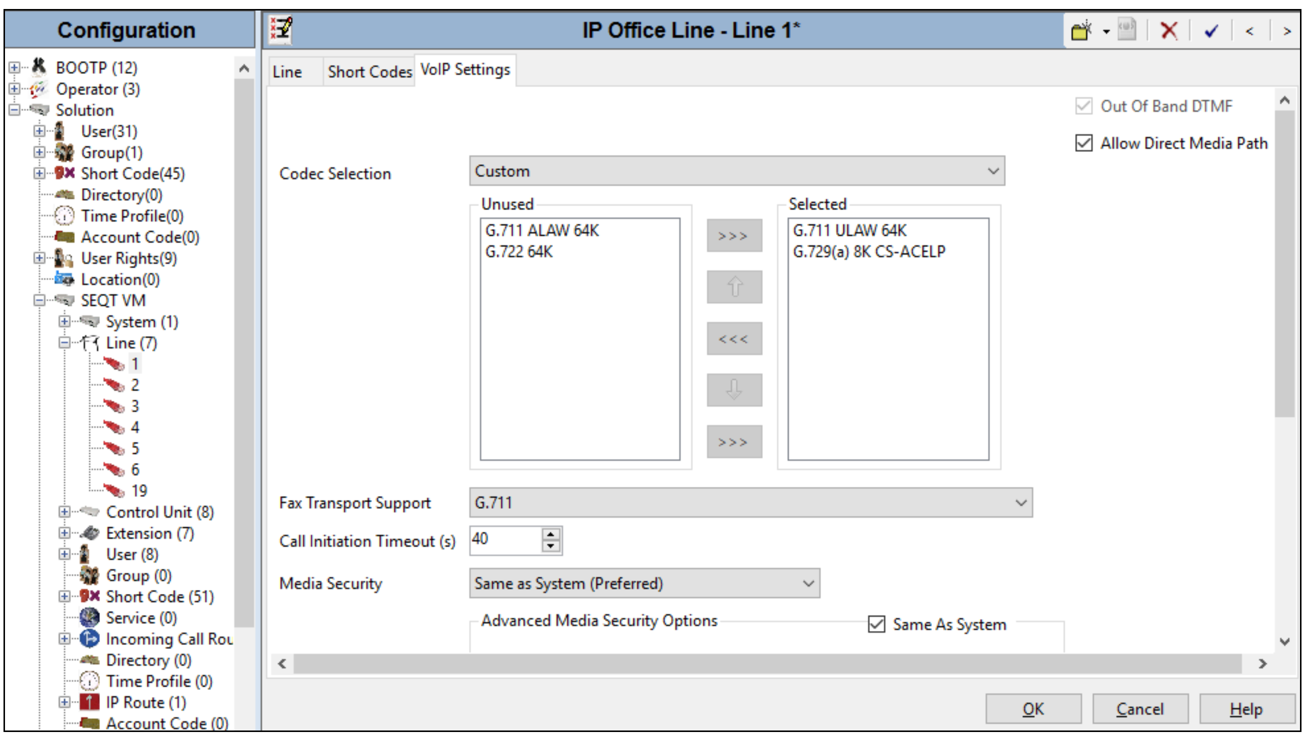


5.5. IP Office Line Server Eddition

The IP Office line on Server Edition is created below.

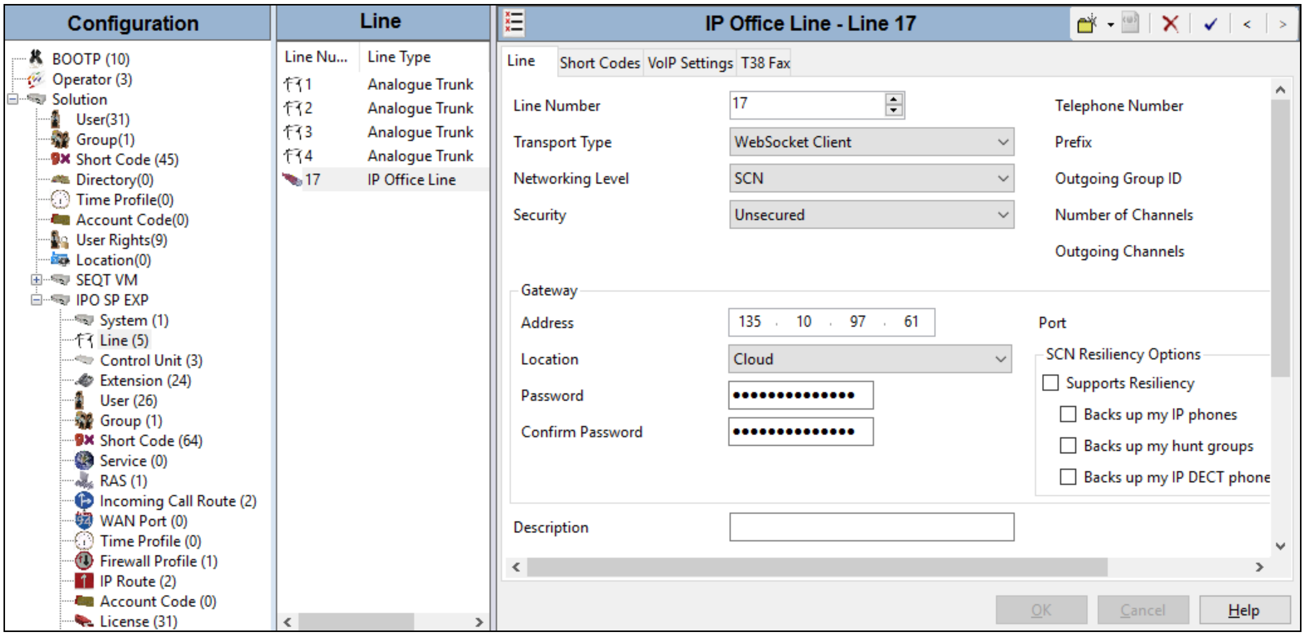


VoIP Settings tab is required to set for **Fax Transport Support** as ***G.711*** as the SIP trunk to service provider.



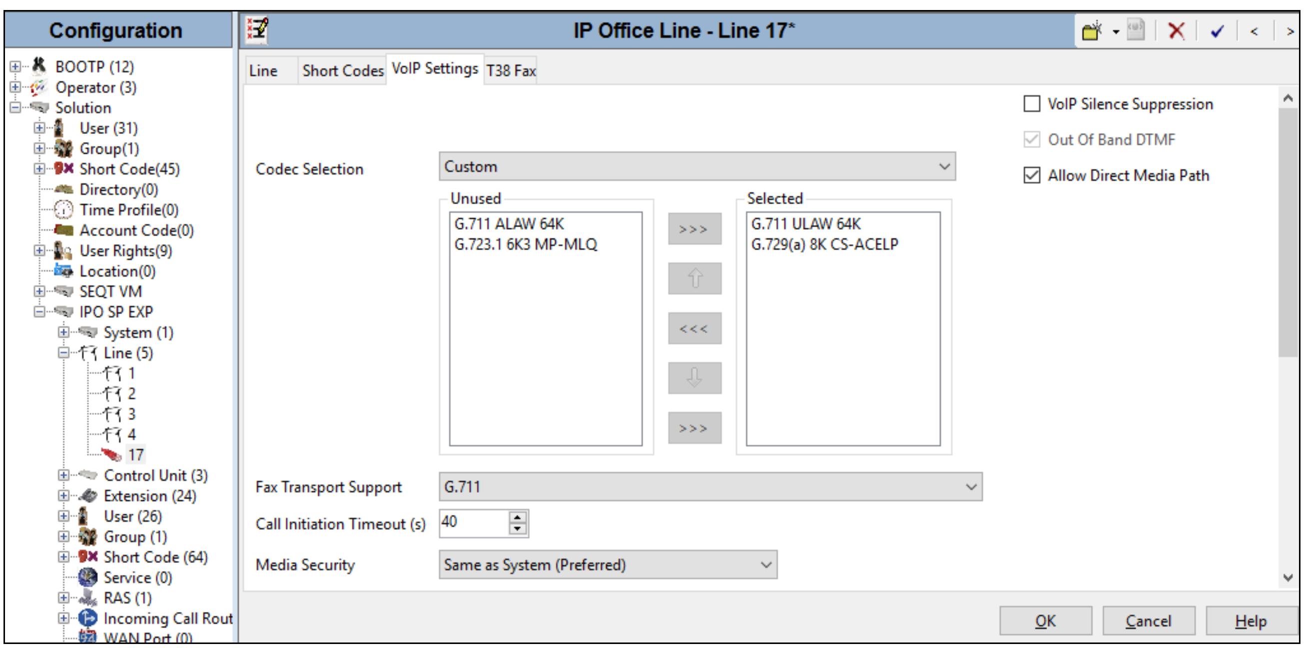
5.6. IP Office Line Secondary Server

The IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. Below is the IP Office Line to the Primary server.



In this testing configuration, a fax machine is connected to one of the analog ports on the Expansion System. To accommodate G.711 fax, select the **VoIP Settings** tab and configure the following:

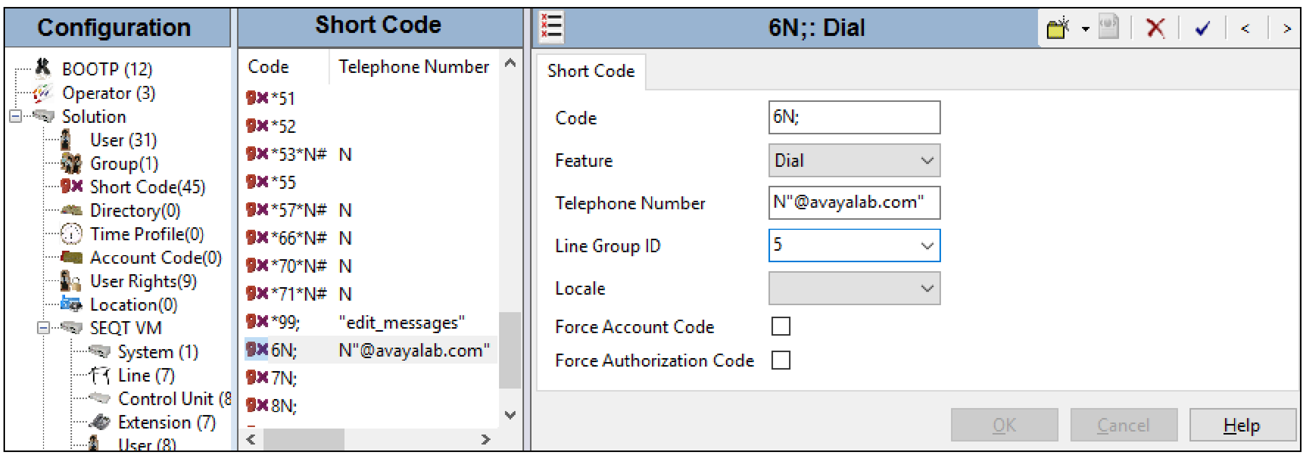
- Select ***G.711*** for **Fax Transport Support**.



5.7. Short Code

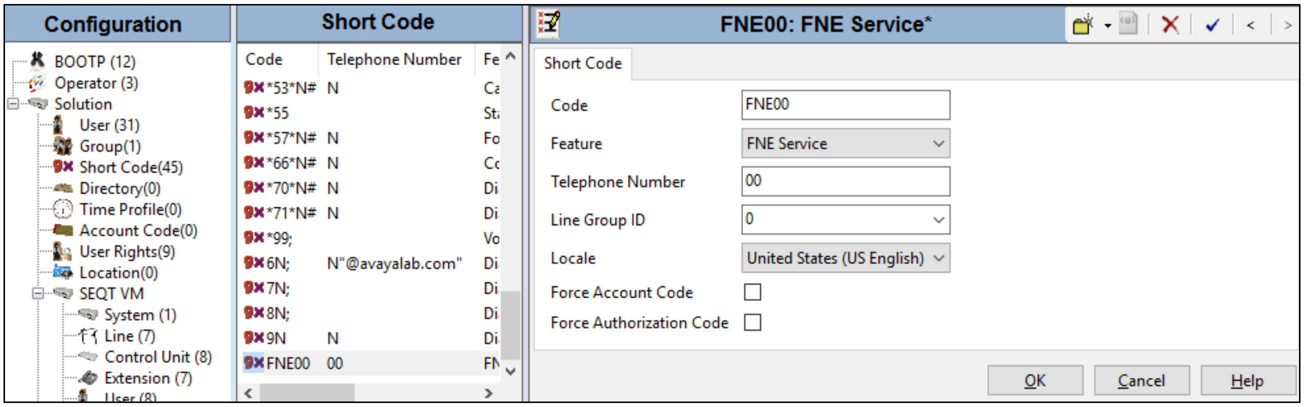
Define a short code to route outbound traffic to the SIP line. To create a short code, select **Short Code** in the left **Navigation** pane, then right-click in the **Group** pane and select **New**. On the **Short Code** tab in the **Details** pane, configure the parameters for the new short code to be created. The screen below shows the details of the previously administered "6N;" short code used in the test configuration.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, 6***N;*** this short code will be invoked when the user dials 6 followed by any number.
- Set **Feature** to ***Dial***. This is the action that the short code will perform.
- Set **Telephone Number** to the value shown in the capture bellow. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value ***N*** represents the number dialed by the user. The host part following the "@" is the domain of the service provider network.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4**. This short code will use this line group when placing the outbound call.
- Others parameters are at default values.
- Click **OK**.



For incoming calls from mobility extension to FNE (Feature Name/Number Extension) hosted by IP Office to provide dial tone functionality, Short Code **FNE00** was created. The FNE00 was configured with the following parameters.

- In the **Code** field, enter the FNE feature code as ***FNE00*** for dial tone.
- Set the **Feature** field to ***FNE Service***.
- Set the **Telephone Number** field to ***00***.
- Set the **Line Group ID** field to ***0***.
- Retain default values for other fields.
- Click **OK**.

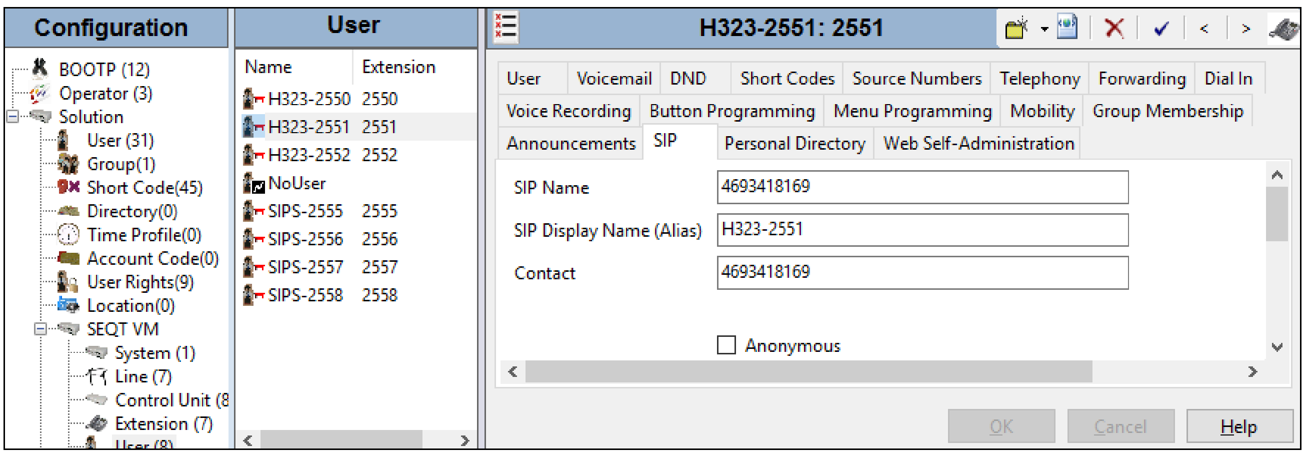


5.8. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.4**. To configure these settings, first select **User** in the left **Navigation** pane, then select the name of the user to be modified in the center **Group** pane. In the example below, the name of the user is "H323-2551". Select the **SIP** tab in the **Details** pane.

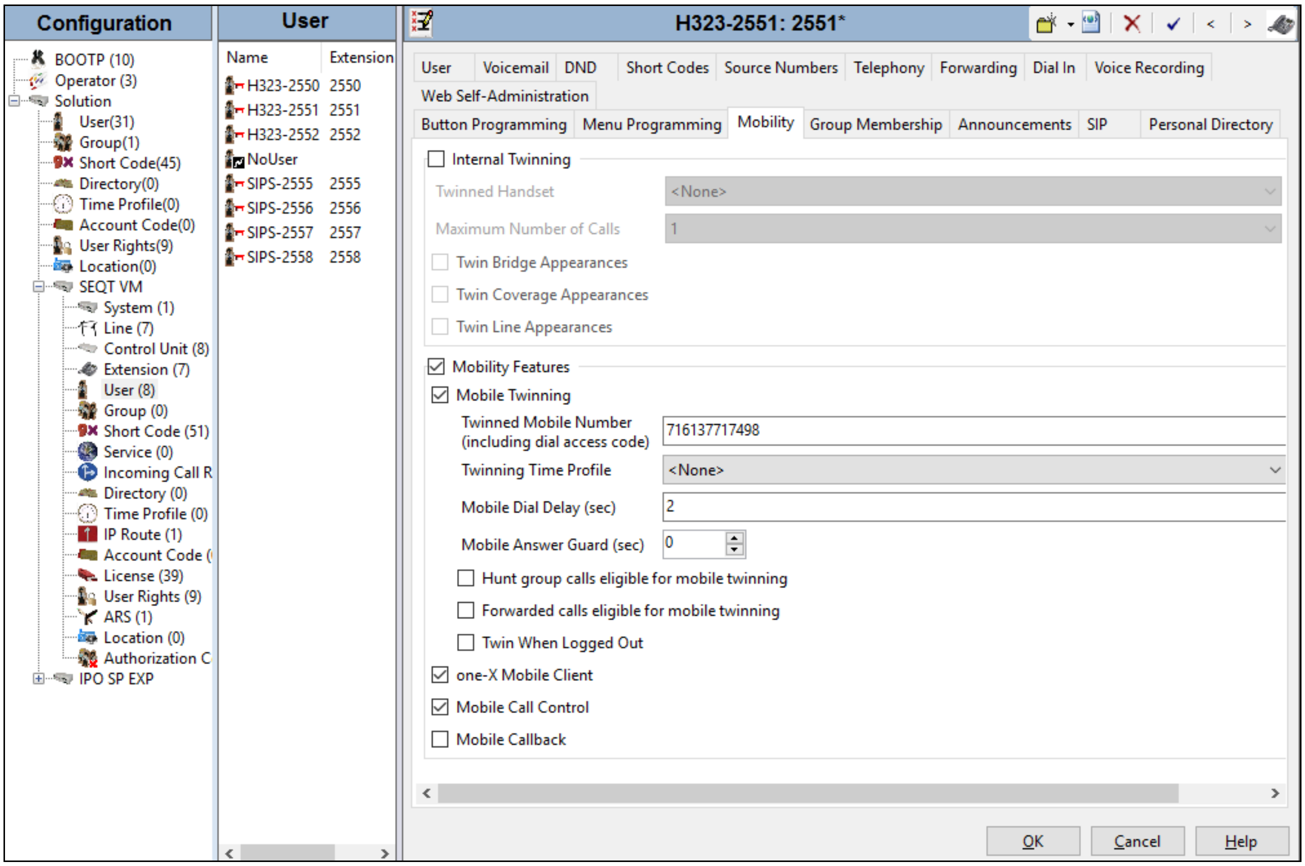
The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. They also allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.4**). The example below shows the settings for user H323-2551.

- The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise from service provider.
- The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.
- If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network.
- Click **OK**.



One of the H.323 IP Phones at the enterprise site uses the Mobile Twinning feature. The following screen shows the **Mobility** tab for User H323-2551.

- The **Mobility Features** and **Mobile Twinning** boxes are checked.
- The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone, in this case ***716137717498***.
- Check **Mobile Call Control** check-box.
- Other options can be set according to customer requirements.
- Click **OK**.

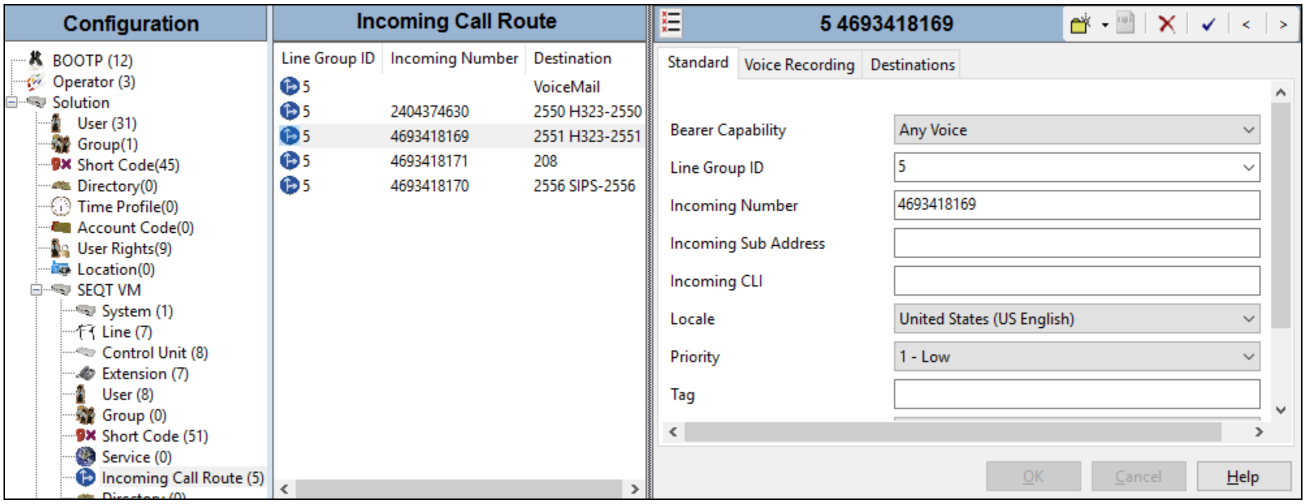


5.9. Incoming Call Route

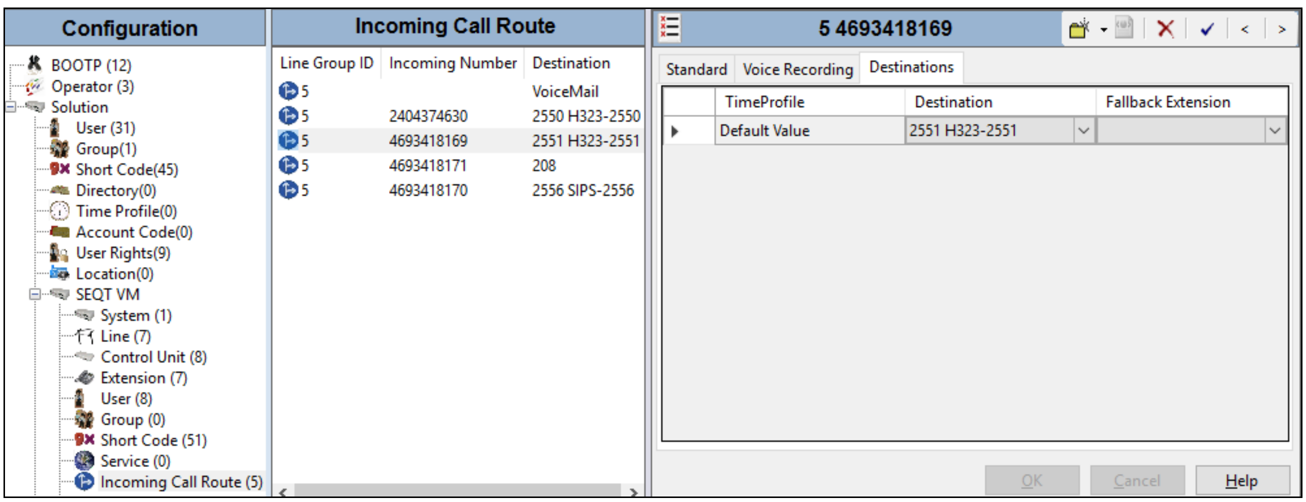
An incoming call route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by the service provider. To create an incoming call route, select **Incoming Call Route** in the left **Navigation** pane, then right-click in the center **Group** pane and select **New**. On the **Standard** tab of the **Details** pane, enter the parameters as shown below:

- Set the **Bearer Capacity** to ***Any Voice***.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.4**.
- Set the **Incoming Number** to the incoming number on which this route should match.
- Default values can be used for all other fields.
- Click **OK**.

An Incoming Call Route is shown below.



On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **4693418169** on line 5 are routed to extension ***2551***. Click **OK**.



5.10. Save Configuration

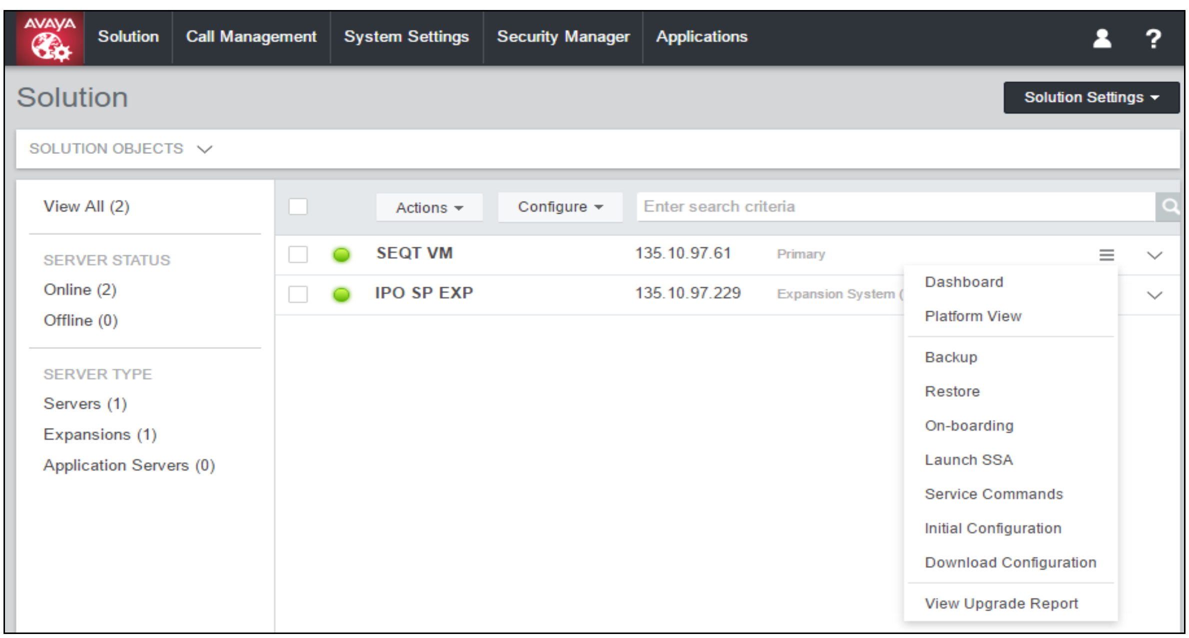
Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections.

5.11. Avaya IP Office TLS Certificate Management

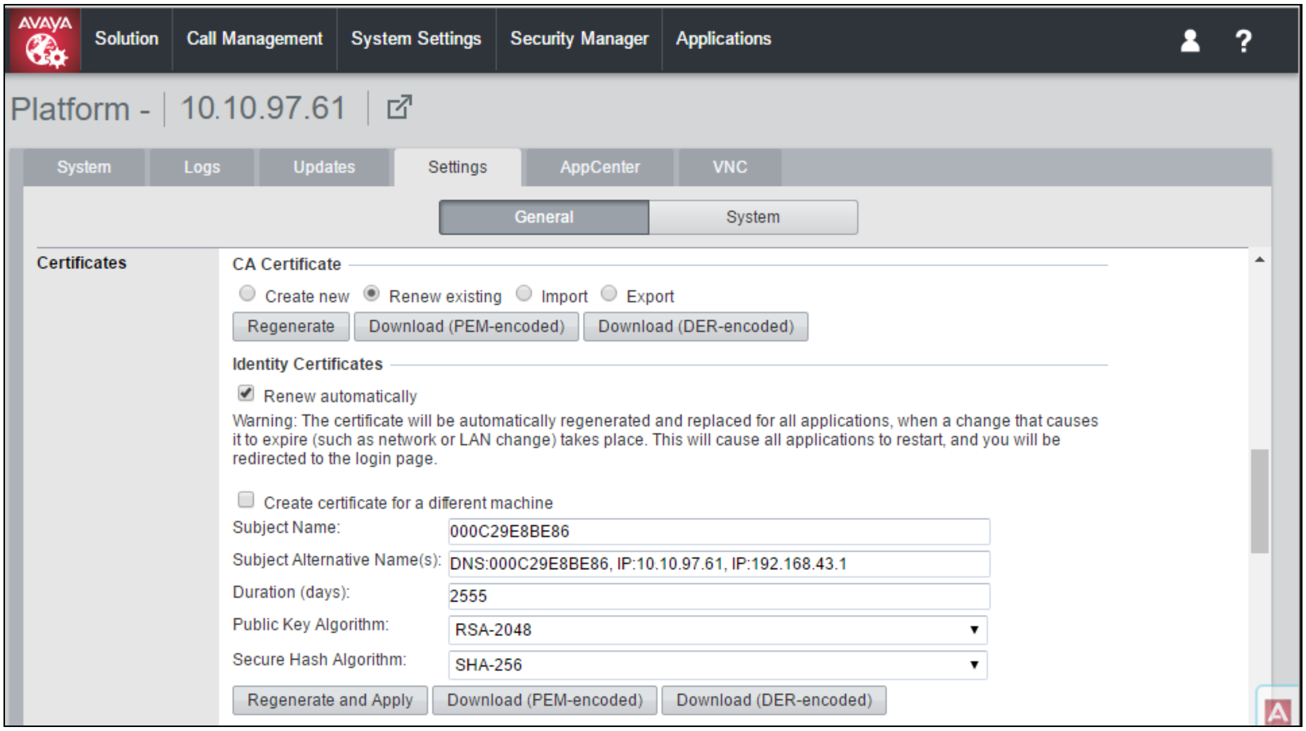
This section provides a procedure on how to download the IP Office certificate which is being installed on Avaya SBCE for the communication between Avaya system's components using TLS connectivity.

To download the IP Office certificate, launch a web browser and log in Avaya IP Office Web Management as shown below.

On the **Solution** page, click on drop-down menu on the right and select **Platform View** as shown.



On the **Platform** page, click on **Settings** and scroll down to **Certificates** section. At **CA Certificate** section, click on the **Download (PEM-encoded)** button to obtain the IP Office CA certificate.



6. Configure the Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the software has already been installed. For additional information on these configuration tasks, see **Section 10**.

The compliance testing comprised the configuration for two major components, Trunk Server for the service provider and Call Server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration is defined in the Avaya SBCE web user interface as described in the following sections.

Trunk Server configuration elements for the service provider - Windstream:

- Global Profiles:
    - URI Groups
    - Routing
    - Topology Hiding
    - Server Interworking
    - Signaling Manipulation
    - Server Configuration
- Domain Policies:
    - Application Rules
    - Media Rules
    - Signaling Rules
    - Endpoint Policy Group
    - Session Policy
- TLS Management
    - Certificates
    - Client Profiles
    - Server Profiles
- Device Specific Settings:
    - Network Management
    - Media Interface
    - Signaling Interface
    - End Point Flows → Server Flows
    - Session Flows

Call Server configuration elements for the enterprise - IP Office:

- Global Profiles:
    - URI Groups
    - Routing
    - Topology Hiding
    - Server Interworking
    - Server Configuration
- Domain Policies:
    - Application Rules
    - Media Rules

- Signaling Rules
- Endpoint Policy Group
- Session Policy
- TLS Management
  - Certificates
  - Client Profiles
  - Server Profiles
- Device Specific Settings:
  - Network Management
  - Media Interface
  - Signaling Interface
  - End Point Flows → Server Flows
  - Session Flows

The naming convention in this entire section is using as follow:

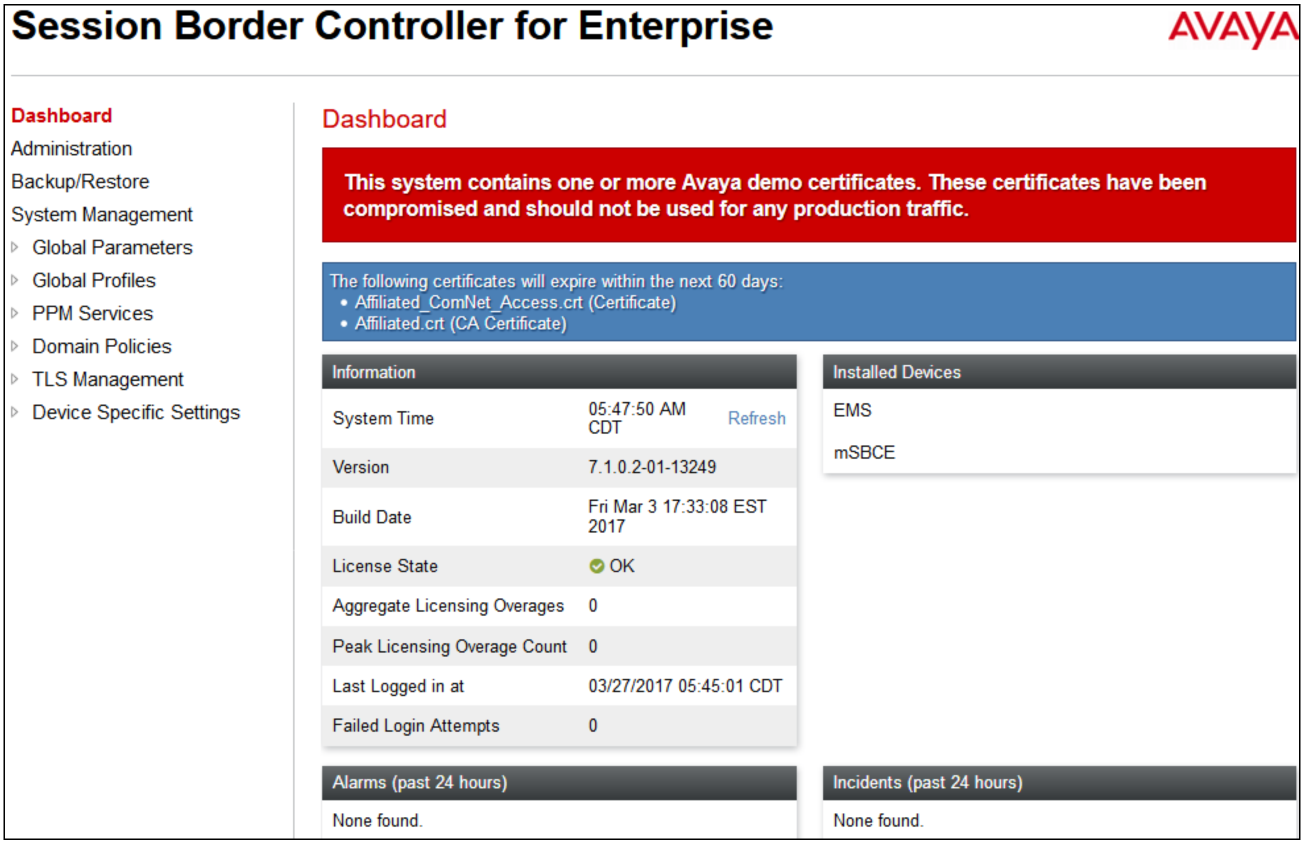
- **SP** is stand for Service Provider, which is Windstream in this case.
- **EN** is stand for Enterprise Network, which refers to Avaya IP Office.

6.1. Log into the Avaya Session Border Controller for Enterprise

Use a Web browser to access the Avaya SBCE Web interface, enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the management IP address.

Enter the appropriate credentials then click **Log In**.

The **Dashboard** main page will appear as shown below.



6.2. TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. The Avaya SBCE utilizes TLS primarily to facilitate secure communications with remote users.

Avaya SBCE is preinstalled with several certificates and profiles that can be used to quickly set up secure communication using TLS, which are listed in the Pre-installed Avaya Profiles and Certificates section. IP Office, Avaya SBCE and the 96x1 IP Deskphones are shipped with a default identity certificate to enable out-of-box support for TLS sessions. Do not use this default certificate in a production/customer environment since this certificate is common across all instances of IP Office, Avaya SBCE and the 96x1 IP Deskphones. Avaya SBCE supports the configuration of third-party certificates and TLS settings. For optimum security, Avaya recommends using third-party CA certificates for enhanced security.

Testing was done with default identity certificate. The procedure to obtain and install third party CA certificates is outside the scope of these application notes.

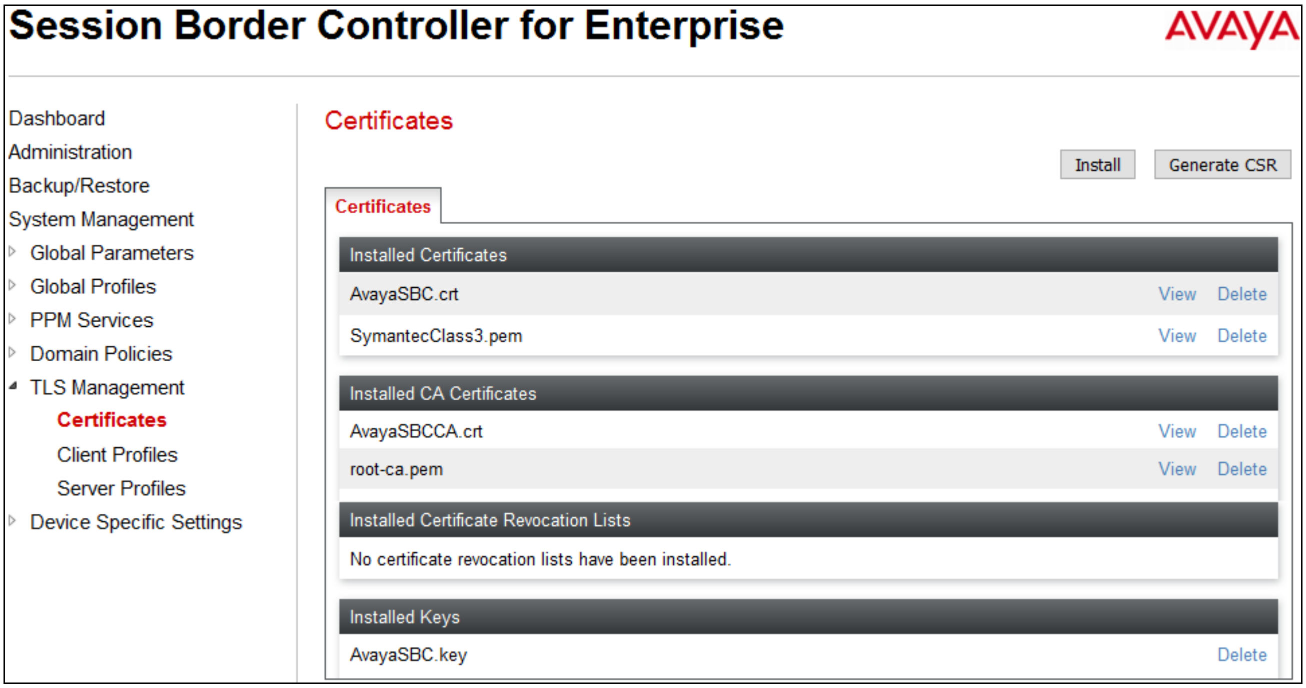
In this compliance testing, TLS transport is used for the communication between IP Office and Avaya SBCE. The following procedures show how to create the client and server profiles.

6.2.1. Certificates

You can use the certificate management functionality that is built into the Avaya SBCE to control all certificates used in TLS handshakes. You can access the Certificates screen from **TLS Management → Certificates**.

Ensure the preinstalled certificates are presented in the system as shown below.

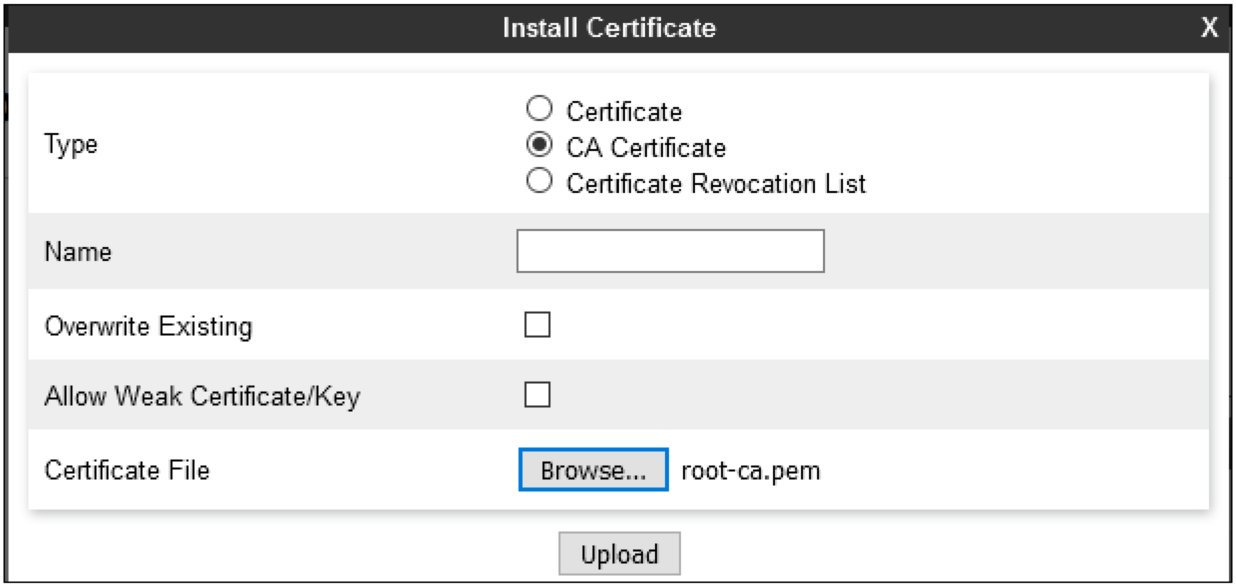
- **AvayaSBCCA.crt** is Avaya SBCE Certificate Authority root certificate.
- **root-ca.pem** is the IP Office root certificate obtained from **Section 5.11**.



If the IP Office Certificate Authority certificate (root-ca.pem) is not present, the following procedure will show how to install it here on Avaya SBCE.

IP Office CA certificate is obtained using procedure provided in **Section 5.11**. Then on Avaya SBCE, navigate to **TLS Management → Certificates**. Click on **Install** button.

- Select **CA Certificate**.
- Provide a descriptive **Name**. In the example below, the **Name** field was left empty and default name was used as root-ca.pem.
- **Browse** to the directory where the IP Office CA was previously saved and select it.
- Click **Upload**.



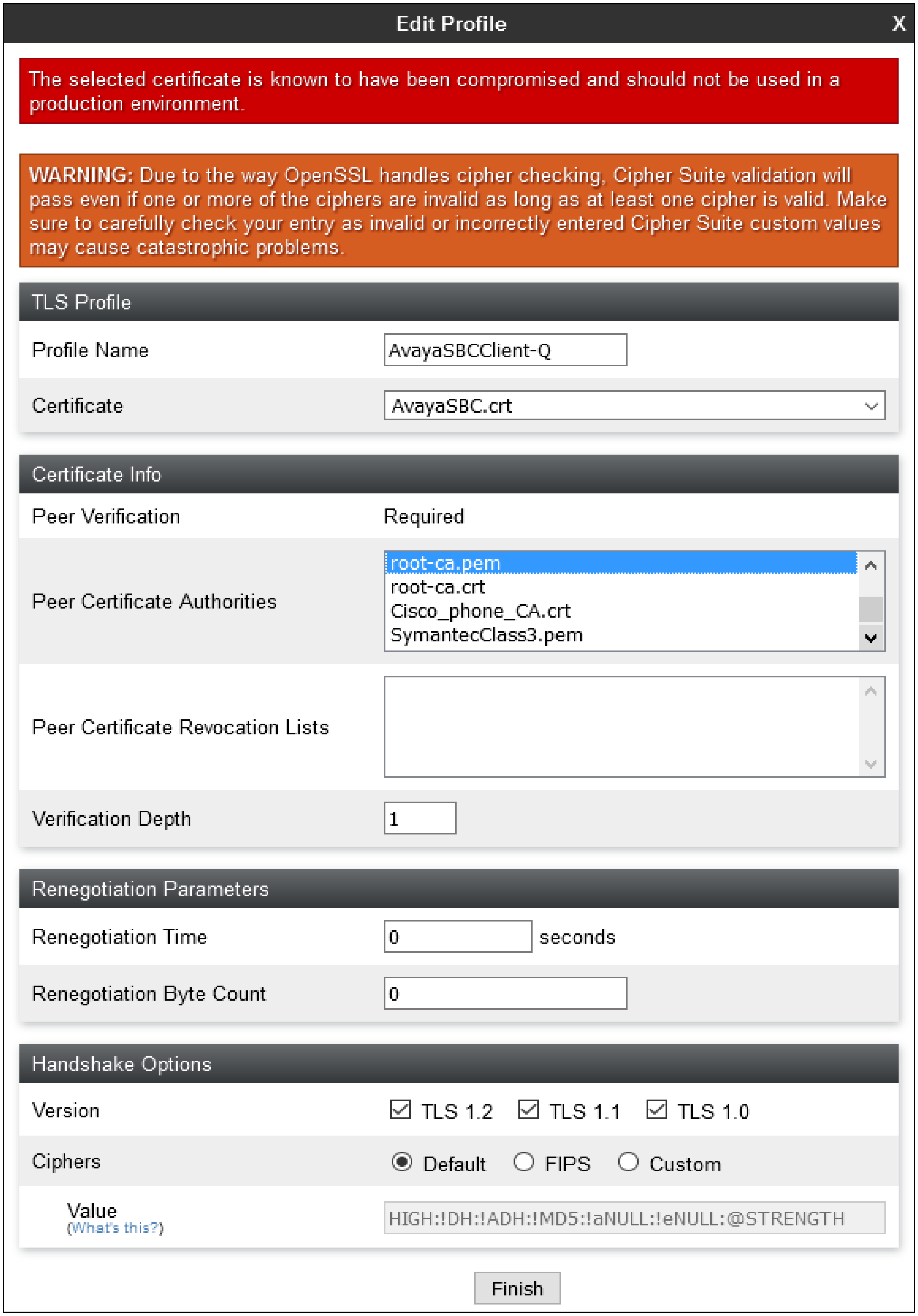
6.2.2. Client Profiles

This section describes the procedure to create client profile for Avaya SBCE to communicate with IP Office via TLS signalling. This will be used in **Section 6.3.3.2**.

To create Client profile, navigate to **TLS Management → Client Profiles**, click **Add**.

- Enter descriptive name in **Profile Name**.
- Select ***AvayaSBC.crt*** from pull down menu of **Certificate**.
- For **Peer Verification**, select IP Office CA certificate which was installed in the above section.
- Enter ***1*** as **Verification Depth**.
- Click **Finish**.

Capture below illustrates a client profile being created on Avaya SBCE.

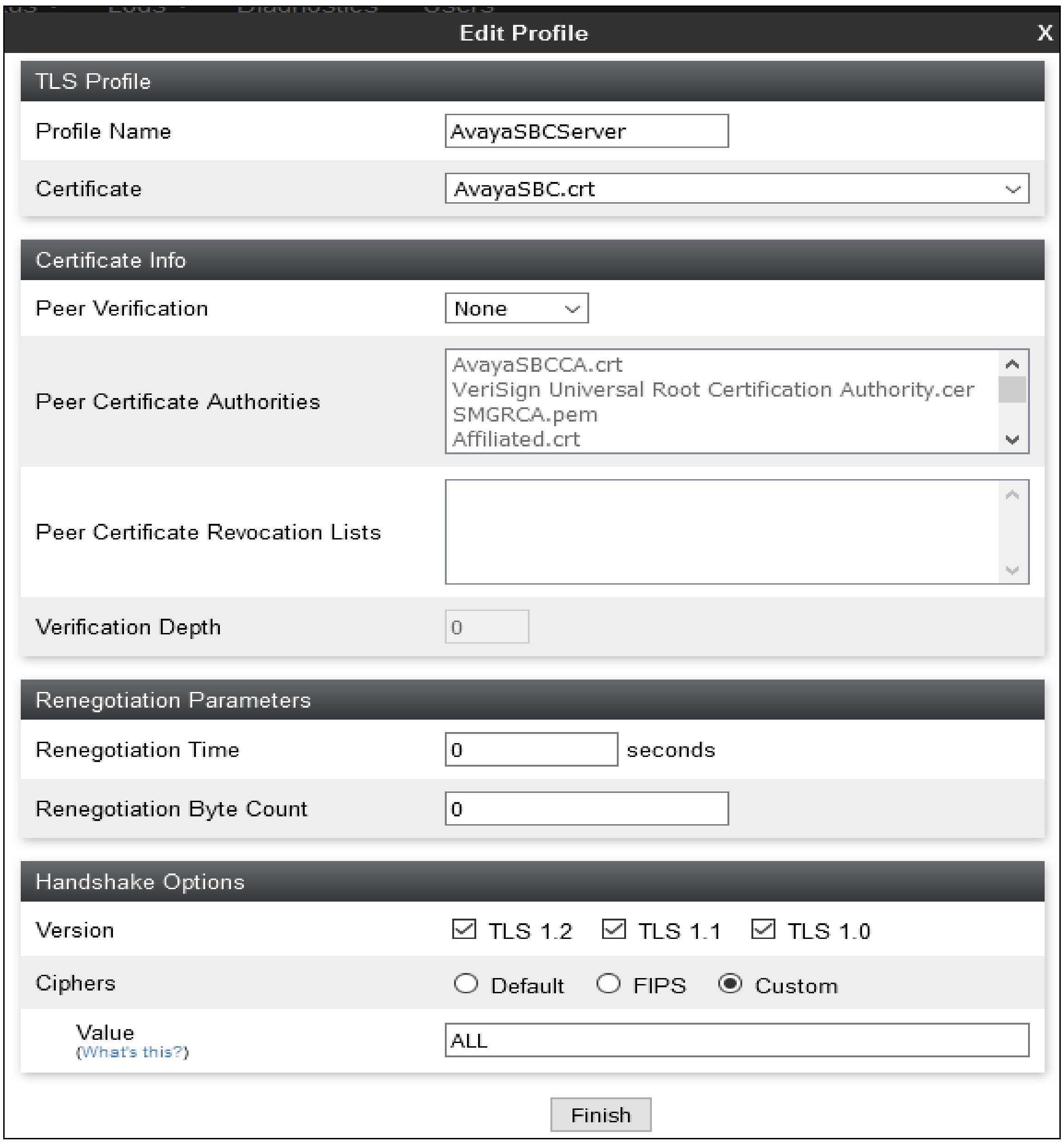


6.2.3. Server Profiles

This section describes the procedure to create server profile for Avaya SBCE to communicate with IP Office via TLS signalling. This will be used in **Section 6.5.3**.

To create Server profile, navigate to **TLS Management → Server Profiles**, click **Add**.

- Enter descriptive name in **Profile Name**.
- Select ***AvayaSBC.crt*** from pull down menu of **Certificate**.
- Select ***None*** from pull down menu of **Peer Verification**.
- Select ***Custom*** for Ciphers in **Cipher Suit Options** section. And **Value *ALL*** is specified in the capture shown below.
- Click **Finish**.



6.3. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

The naming convention in this entire section is using as follows:

- **SP** stands for Service Provider, which is Windstream in this case.
- **EN** stands for Enterprise Network, which is referred to Avaya IP Office.

6.3.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, “*****” is used for all incoming and outgoing traffic.

6.3.2. Server Interworking Profile

Interworking Profile features are configured differently for Call Server and Trunk Server.

To create a Server Interworking profile, select **Global Profiles → Server Interworking**. Click on the **Add** button.

In the compliance testing, two Server Interworking profiles were created for SP and EN respectively.

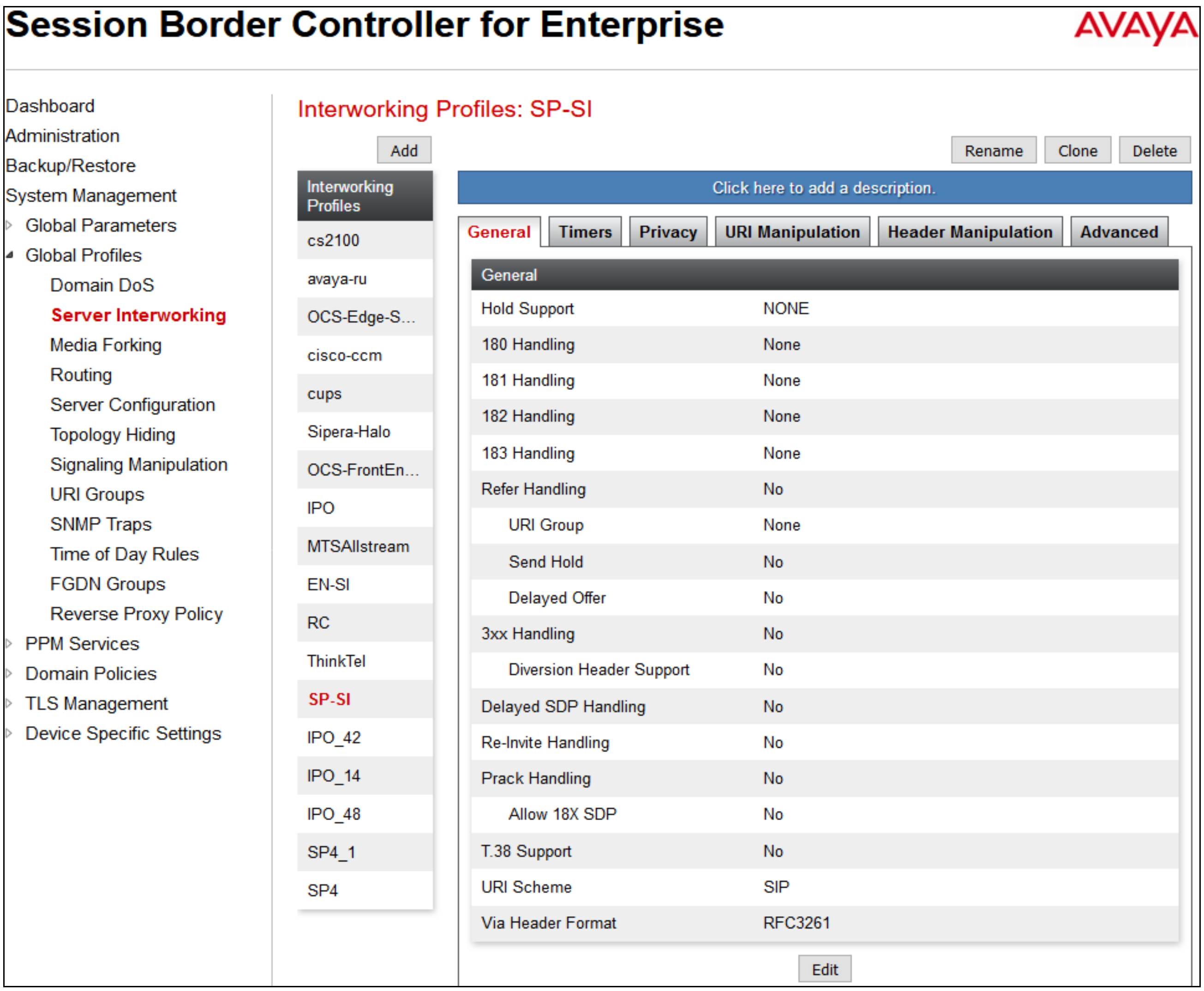
6.3.2.1 Server Interworking Profile for SP

Profile **SP-SI** was defined to match the specification of SP. The **General**, **URI Manipulation** and **Advanced** tabs are configured with the following parameters while the other tabs for **Timers**, **Privacy** and **Header Manipulations** are kept as default.

General tab:

- **Hold Support** = ***NONE***. The Avaya SBCE will not modify the hold/ resume signaling from EN to SP.
- **18X Handling** = ***None***. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from EN to SP.
- **Refer Handling** = ***No.*** The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from EN to SP.
- **T.38 Support** = ***No***. SP does not support T.38 fax in the compliance testing.
- Others are left as default values.

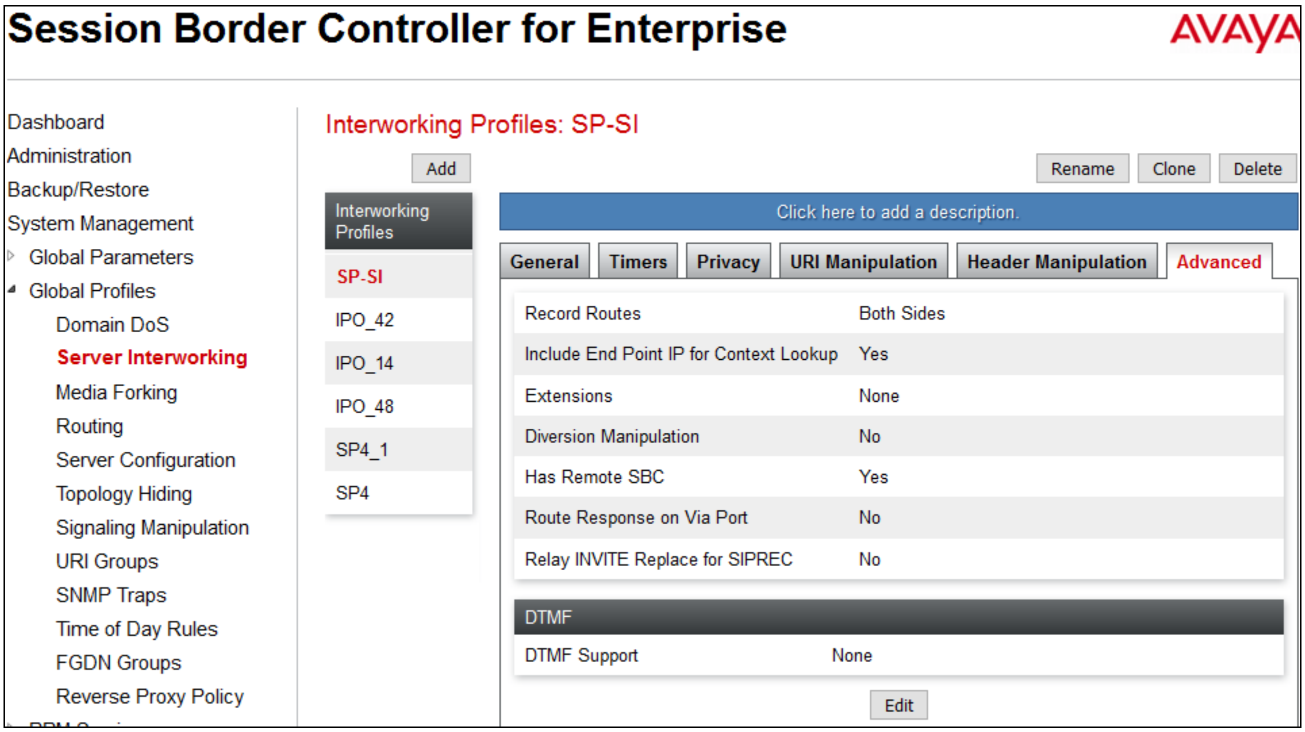
The screenshots below illustrate the Server Interworking profile **SP-SI, General**.



Advanced tab:

- **Record Routes** = ***Both Sides***. The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Include End Point IP for Context Lookup** = ***Yes***.
- **Extensions** = ***None***.
- **Has Remote SBC** = ***Yes***. This setting allows the Avaya SBCE to always use the SDP received from EN for the media.
- **DTMF Support** = ***None***. The Avaya SBCE will send original DTMF method from SP to EN.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **SP-SI**, **Advanced**.



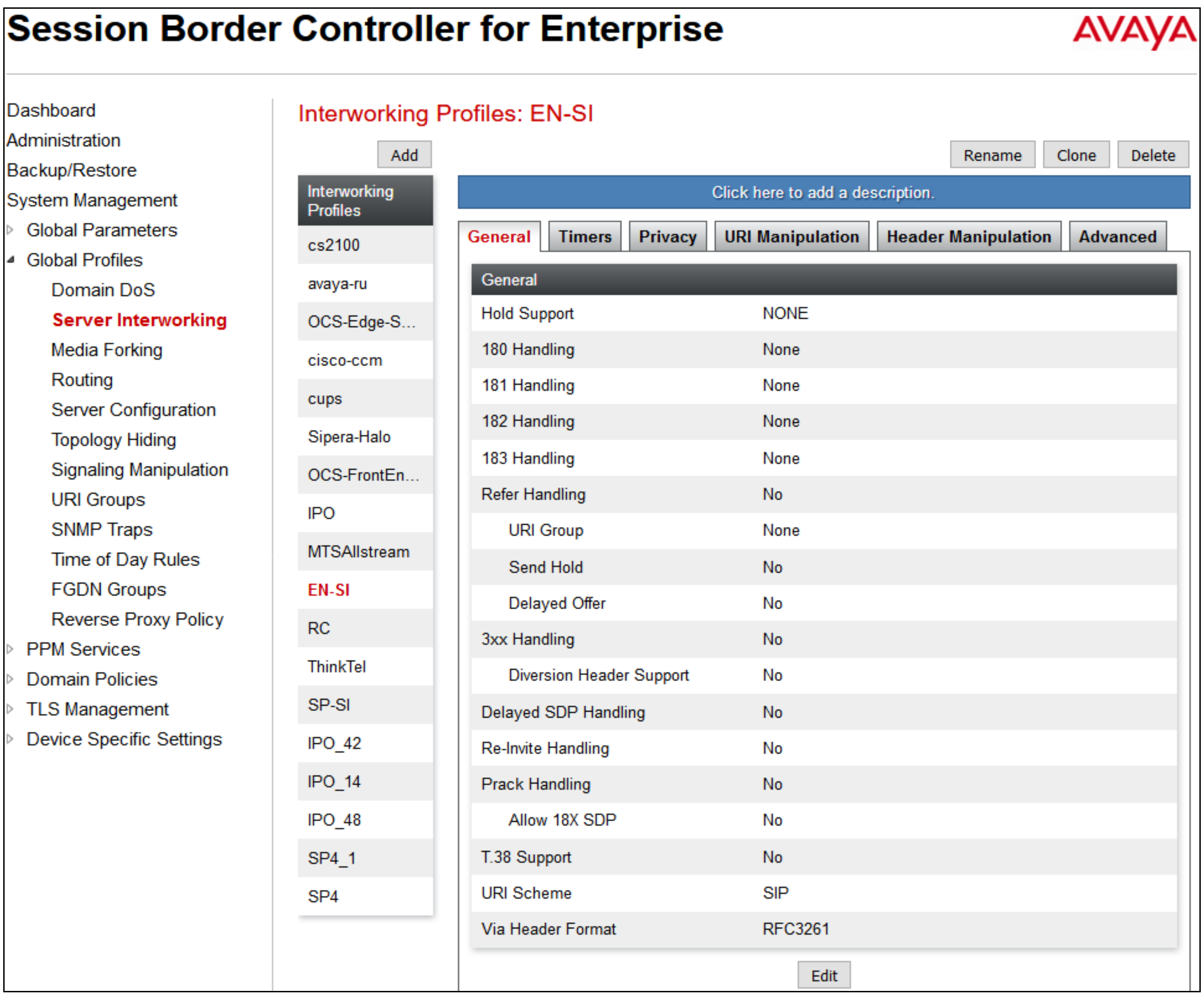
6.3.2.2 Server Interworking Profile for EN

Profile **EN-SI** was defined to match the specification of EN. The **General** and **Advanced** tabs are configured with the following parameters while the other settings for **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** are kept as default.

General tab:

- **Hold Support** = *NONE*.
- **18X Handling** = *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from SP to EN.
- **Refer Handling** = *No*. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from SP to EN.
- **T.38 Support** = *No*. To match with SP profile.
- Others are left as default values.

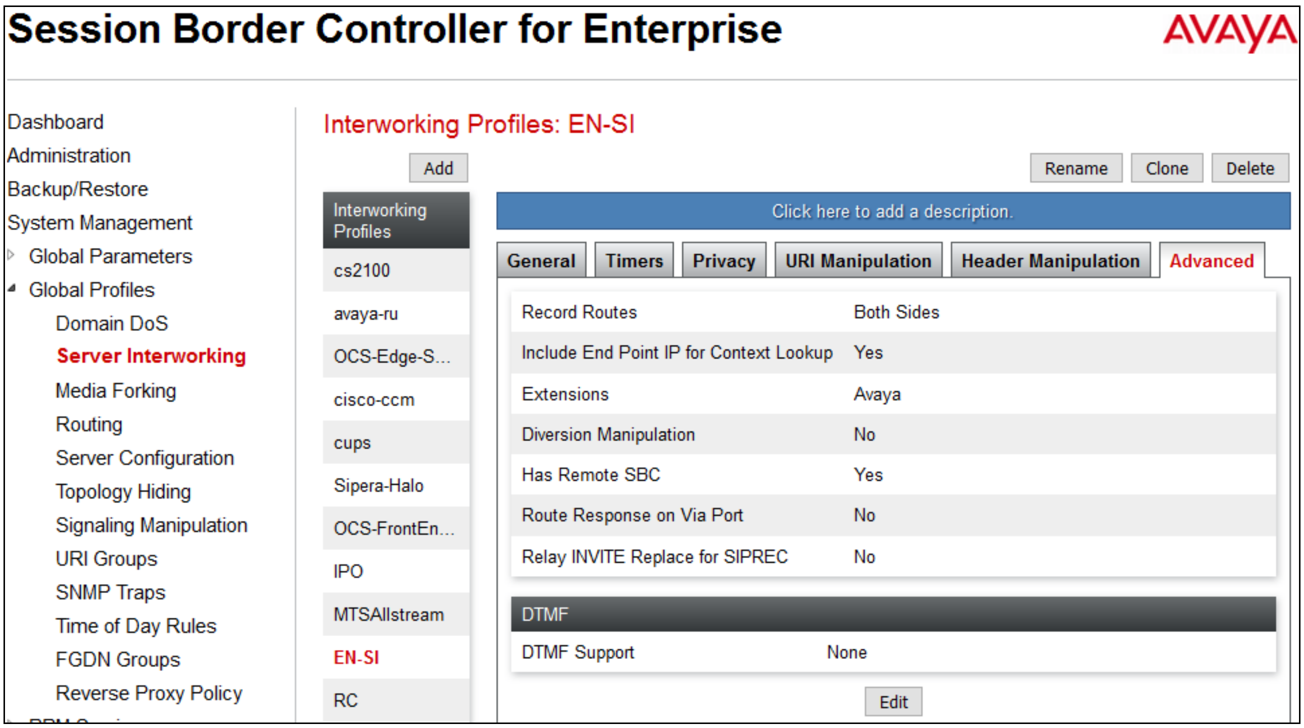
The screenshots below illustrate the Server Interworking profile **EN-SI**, **General**.



Advanced tab:

- **Record Routes** = ***Both Sides***. The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Include End Point IP for Context Lookup** = ***Yes***.
- **Extensions** = ***Avaya***.
- **Has Remote SBC** = ***Yes***. This setting allows the Avaya SBCE to always use the SDP received from EN for the media.
- **DTMF Support** = ***None***. The Avaya SBCE will send original DTMF method from SP to EN.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **EN-SI**, **Advanced**.



6.3.3. Server Configuration

Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

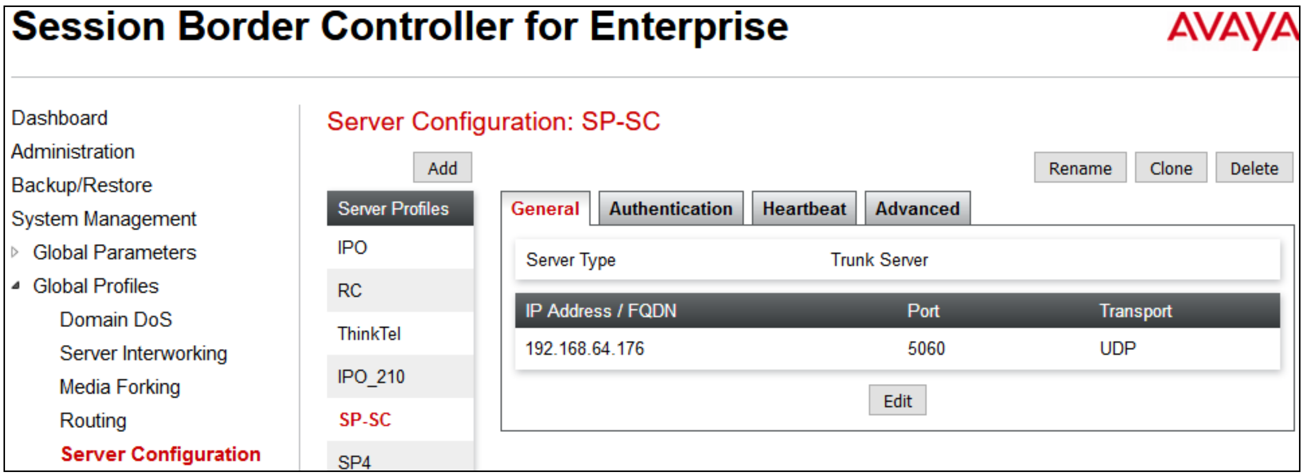
To create a Server Configuration entry, select **Global Profiles →Server Configuration**. Click **Add** button. In the compliance testing, two separate Server Configurations were created, server entry **SP-SC** for SP and server entry **EN-SC** for EN.

6.3.3.1 Server Configuration for SP

Server Configuration named **SP-SC** was created for the SP. It will be discussed in detail below. **General** and **Advanced** tabs are provisioned for SP on the SIP trunk for every outbound call from enterprise to PSTN. The **Authentication** and **Heartbeat** tabs are left at default, disabled.

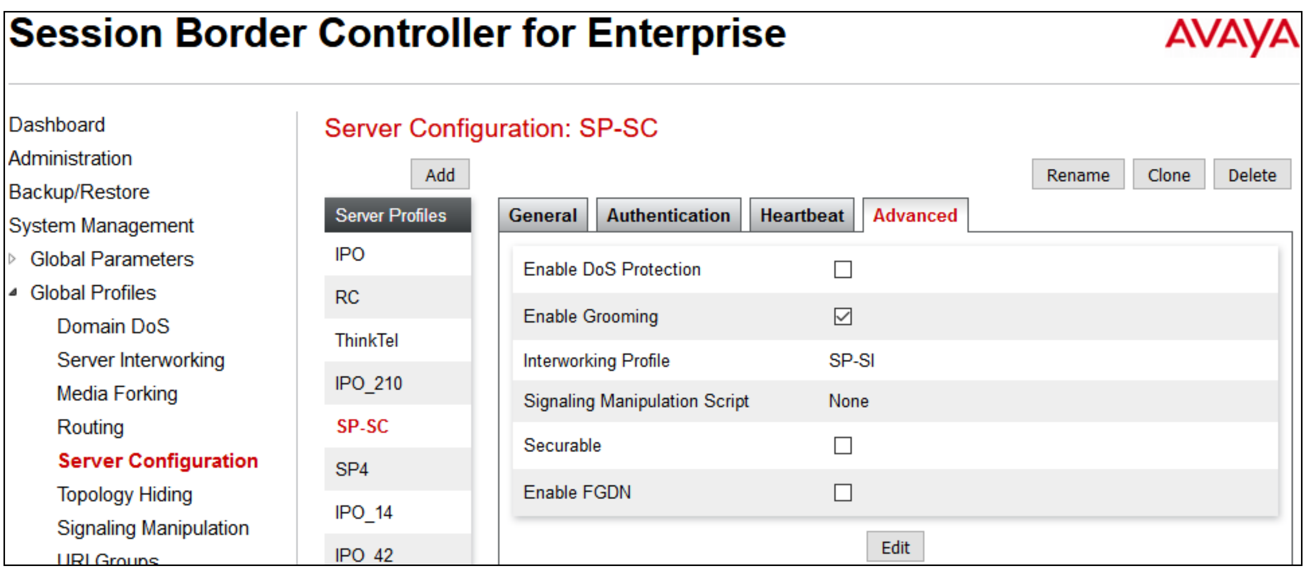
General tab: Click **Add** button and enter following information.

- Enter **Profile Name** ***SP-SC*** and click **Next** button (not shown).
- Set **Server Type** for SP as ***Trunk Server***.
- Enter provided **IP Address/FQDN** of SP. Transport ***UDP*** and listening on port ***5060***.
- Click **Next**, **Next** and **Finish** (not shown).



Advanced tab: Click **Edit** button and enter following information.

- **Interworking Profile** drop down list, select ***SP-SI*** as defined in **Section 6.3.2**.
- Check **Enable Grooming** check-box.
- The other settings are kept as default. Click **Finish** (not shown).

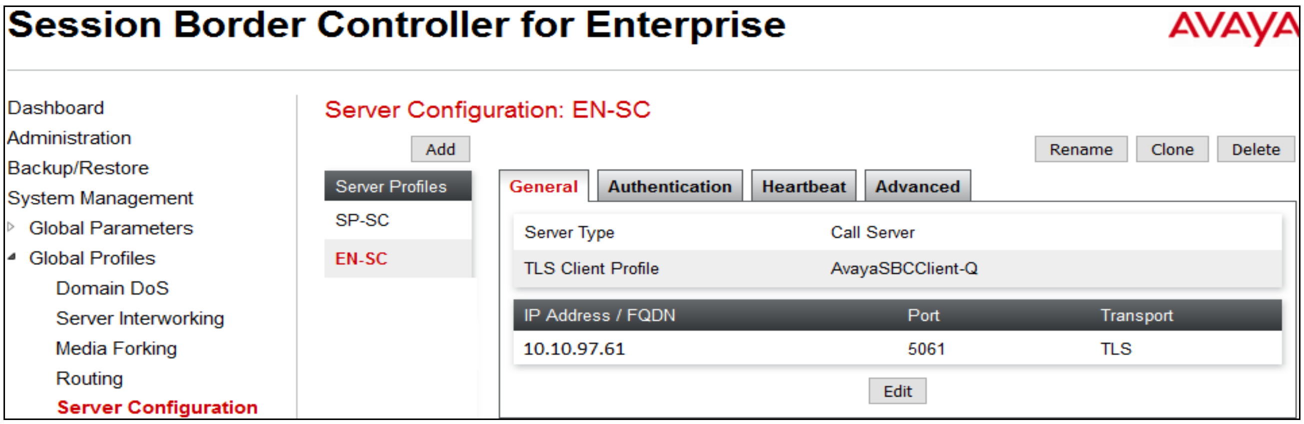


6.3.3.2 Server Configuration for EN

Server Configuration named **EN-SC** created for EN is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as ***disabled*** as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from SP to EN to query the status of the SIP trunk.

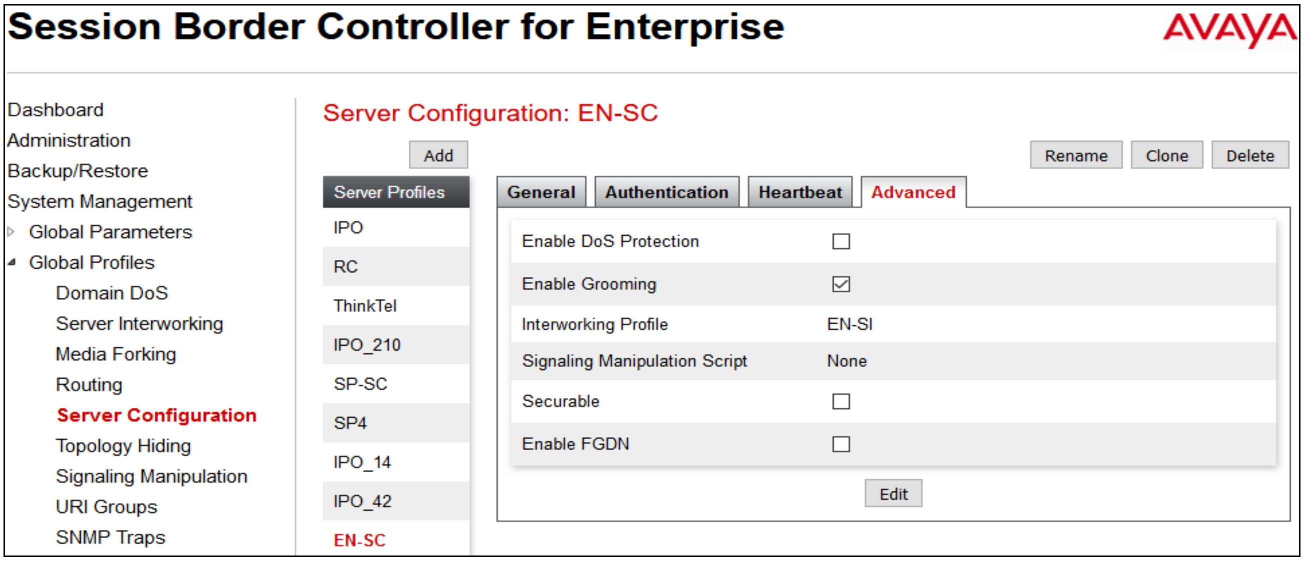
General tab: Click **Add** button then specifying the following.

- **Server Type** for EN as ***Call Server*** and click **Next** button (not shown).
- **IP Address/FQDN** is IP Office WAN port IP address.
- **Transport**, between the Avaya SBCE and IP Office was ***TLS***, and **Port** ***5061***.
- **TLS Client Profile** is the profile created in **Section 6.2.2**.
- Click **Next**, **Next** and **Finish** (not shown).



Advanced tab: Click **Edit** button then enter the following information.

- **Interworking Profile** drop down list select ***EN-SI*** as defined in **Section** Error! Reference source not found..
- Check **Enable Grooming** check-box.
- The other settings are kept as default.



6.3.4. Routing Profiles

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing profiles include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

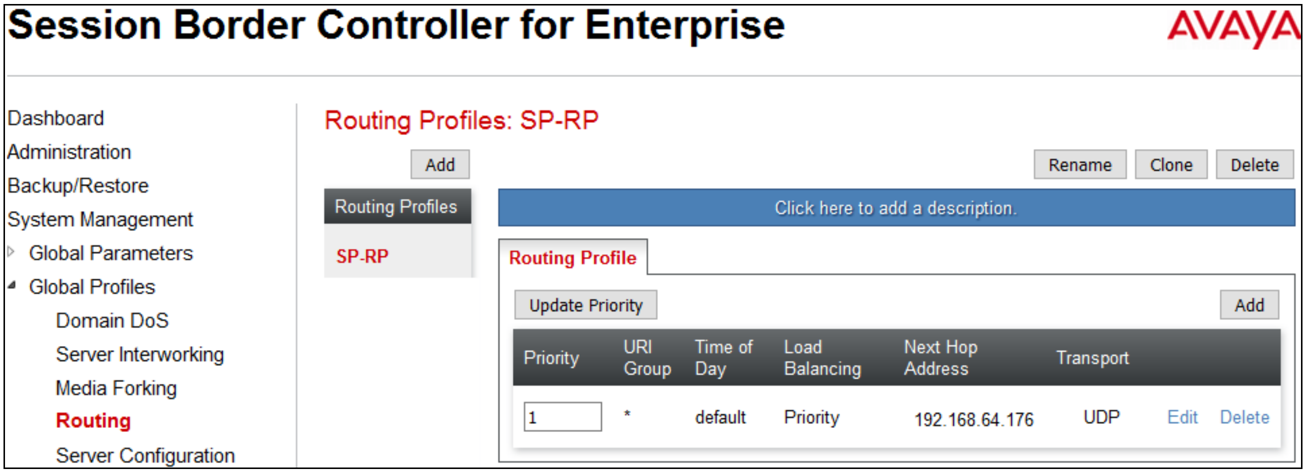
To create a Routing profile, select **Global Profiles → Routing** then click on the **Add** button.

In the compliance testing, routing profile **SP-RP** was created to be used in conjunction with the Server Flow (see **Section 6.5.4**) defined for EN. This entry is to route outgoing calls from the enterprise to SP.

In the opposite direction, Routing profile **EN-RP** was created to be used in conjunction with the Server Flow (see **Section 6.5.4**) defined for SP. This entry is to route incoming calls from SP to the EN.

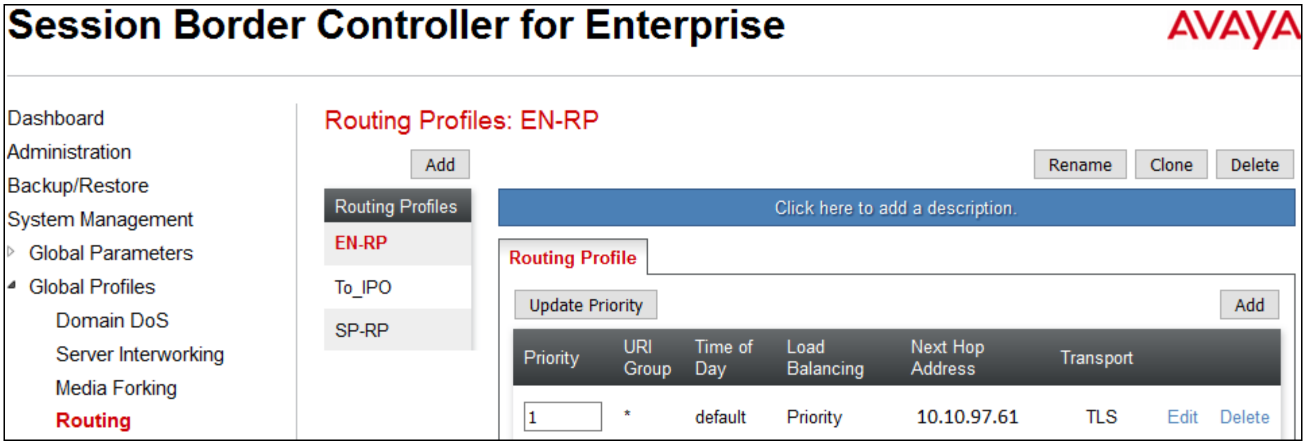
6.3.4.1 Routing Profile for SP

The screenshot below illustrates the routing profile from Avaya SBCE to the SP network, **Global Profiles → Routing**: **SP-RP**. As shown in **Figure 1**, the SP SIP trunk is connected with transportation protocol ***UDP***. If there is a match in the “To” or “Request URI” headers with the URI Group **“*”** defined in **Section** Error! Reference source not found., the call will be routed to the **Next Hop Address** which is the IP address of SP SIP trunk.


Session Border Controller for Enterprise
AVAYA
Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Server Configuration
Routing Profiles: SP-RP
Add
Rename
Clone
Delete
Routing Profiles
SP-RP
Click here to add a description.
Routing Profile
Update Priority
Add
Priority
URI Group
Time of Day
Load Balancing
Next Hop Address
Transport
1
*
default
Priority
192.168.64.176
UDP
Edit
Delete

6.3.4.2 Routing Profile for EN

The Routing Profile for SP to EN, **EN-RP** was defined to route call where the "To" header matches the URI Group **"*"** defined in **Section** Error! Reference source not found. to **Next Hop Address** which is the IP address of IP Office WAN port as a destination. As shown in **Figure 1**, the SIP trunk between EN and the Avaya SBCE is connected with transportation protocol ***TLS***.



6.3.5. Topology Hiding

Topology Hiding is a security feature of the Avaya SBCE which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

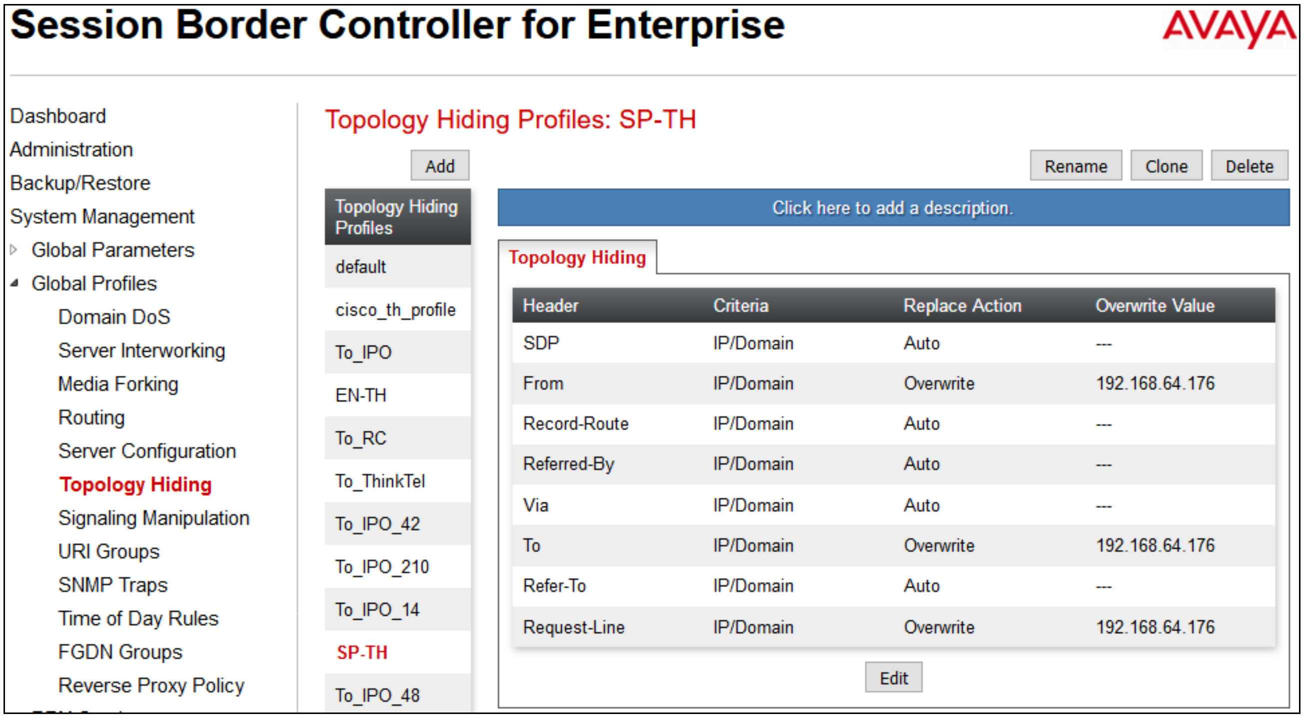
To create a Topology Hiding profile, select **Global Profiles → Topology Hiding** then click on the **Add Profile** (not shown).

In the compliance testing, two Topology Hiding profiles were created: **SP-TH** and **EN-TH**.

6.3.5.1 Topology Hiding Profile for SP

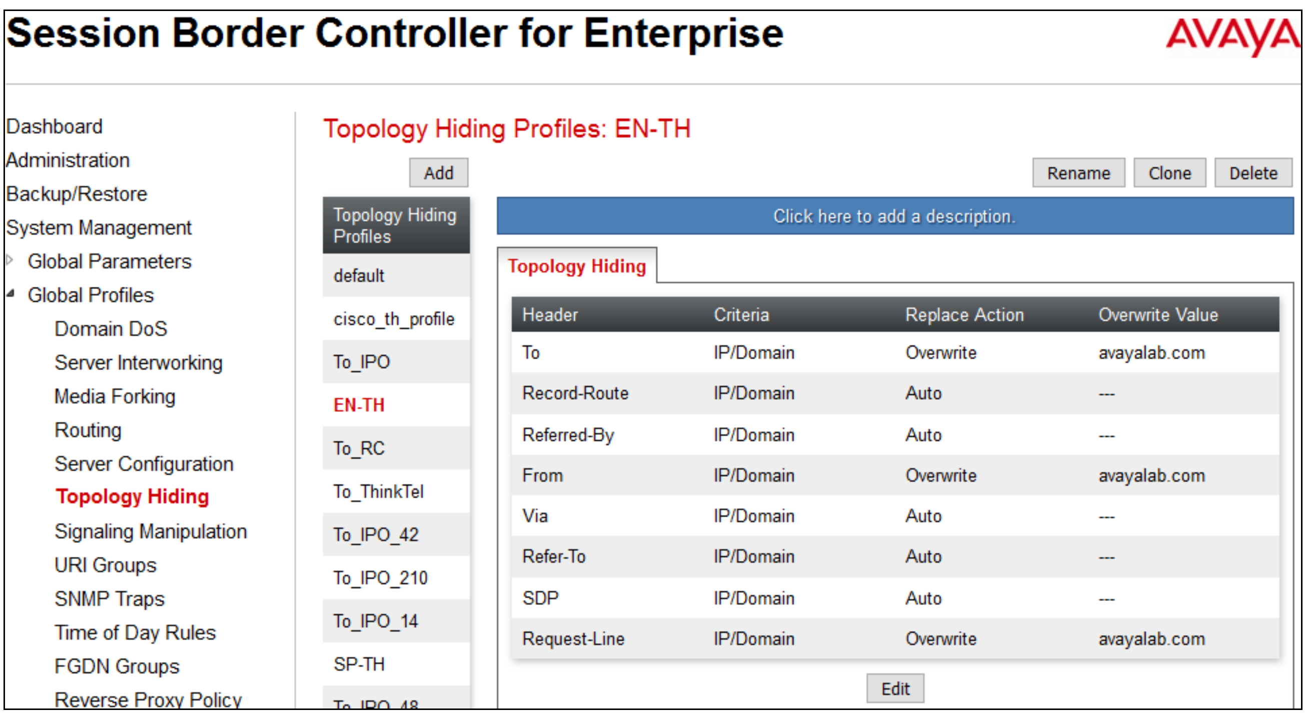
Topology Hiding profile **SP-TH** was defined for outgoing calls to SP as shown in the capture below.

The screenshots below illustrate the Topology Hiding profile **SP-TH**.



6.3.5.2 Topology Hiding Profile for EN

Topology Hiding profile **EN-TH** was defined for incoming calls to IP Office as shown in the capture below.



6.4. Domain Policies

The Domain Policies feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

6.4.1. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

To clone a signaling rule, navigate to **Domain Policies → Signaling Rules**, select the **default** rule then click on the **Clone Rule** button (not shown).

In the compliance testing, two **Signaling Rules** were created for the SP and EN.

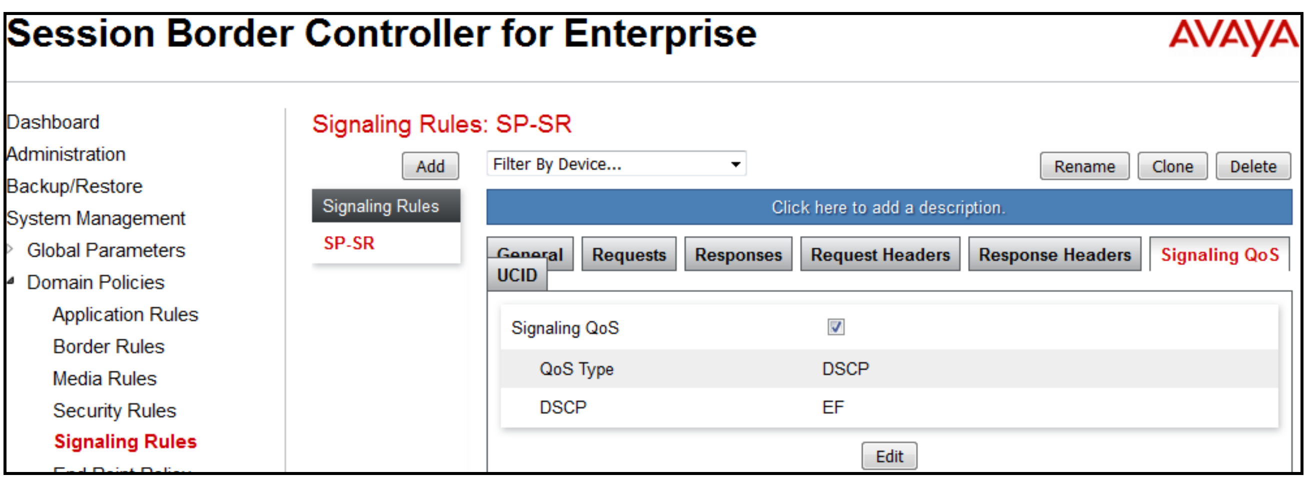
6.4.1.1 Signaling Rule for SP

Clone the Signaling Rule **default** with a descriptive name (e.g., **SP-SR**) and click on the **Finish** button (not shown). Verify that **General** settings of **SP-SR** with **Inbound** and **Outbound Request** are set to **Allow**, and **Enable Content-Type Checks** is enabled with **Action** and **Multipart-Action** are set to **Allow** (not shown).

On the **Signaling QoS** tab, enter the following information.

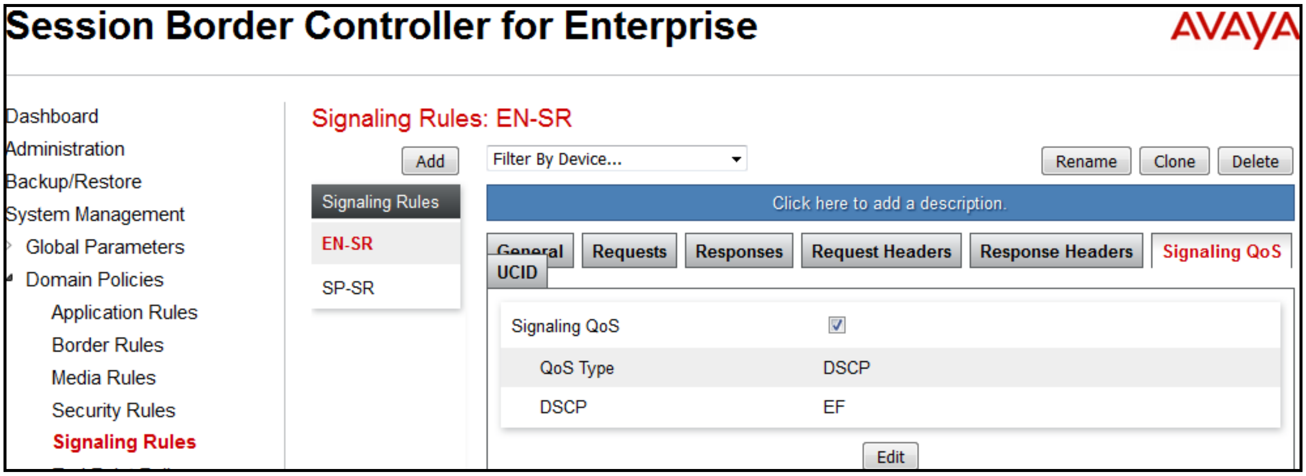
- Select the correct Quality of Service (QoS).
- The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for signaling.

The following screen shows the QoS value used for the compliance testing.



6.4.1.2 Signaling Rule for EN

Clone the Signaling Rule **default** with a descriptive name (e.g., **EN-SR** for EN) and click on the **Finish** button (not shown). Verify that **General** settings of **EN-SR** with **Inbound** and **Outbound Request** are set to **Allow**, and **Enable Content-Type Checks** is enabled with **Action** and **Multipart-Action** are set to **Allow** (not shown). Similarly the Signaling QoS rules are set as shown in capture below.

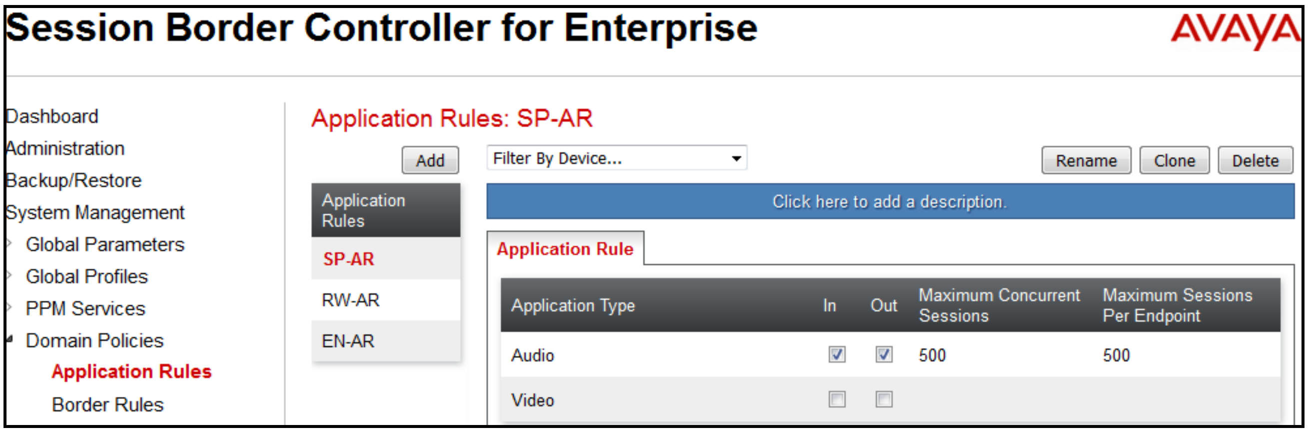


6.4.2. Application Rules

Application Rules define which type of SIP based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, user can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

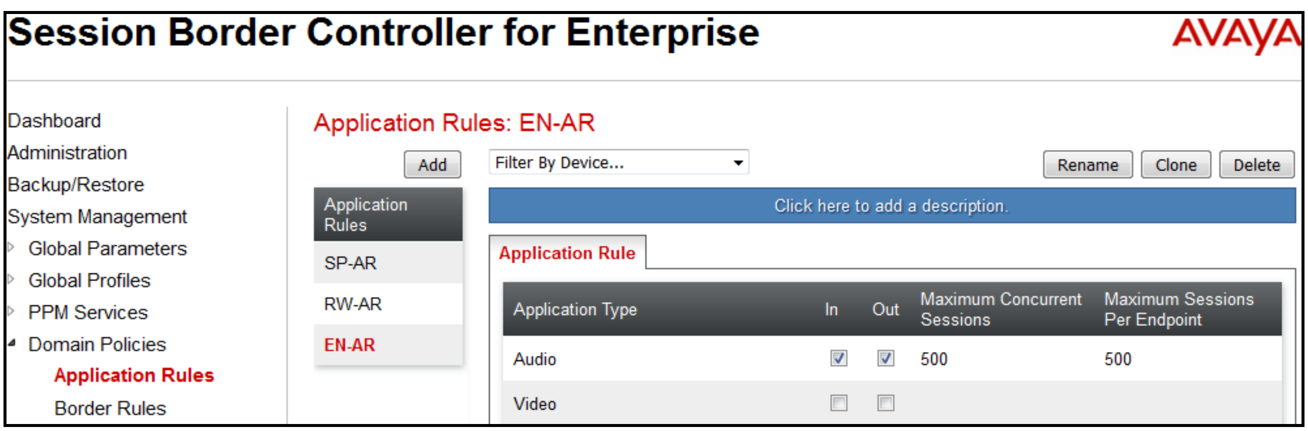
6.4.2.1 Application Rule for SP

Clone the Application Rule **default** with a descriptive name (e.g., **SP-AR** for service provider) and click the **Edit** button to change value of **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** to *500* respectively as shown and then click the **Finish** button (not shown). Others are left as default.



6.4.2.2 Application Rule for EN

Similarly, clone the Application Rule **default** with a descriptive name (e.g., **EN-AR** for IP Office) and click the **Edit** button to change value of **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** to *500* respectively as shown and then click the **Finish** button (not shown). Others are left as default.



6.4.3. Media Rules

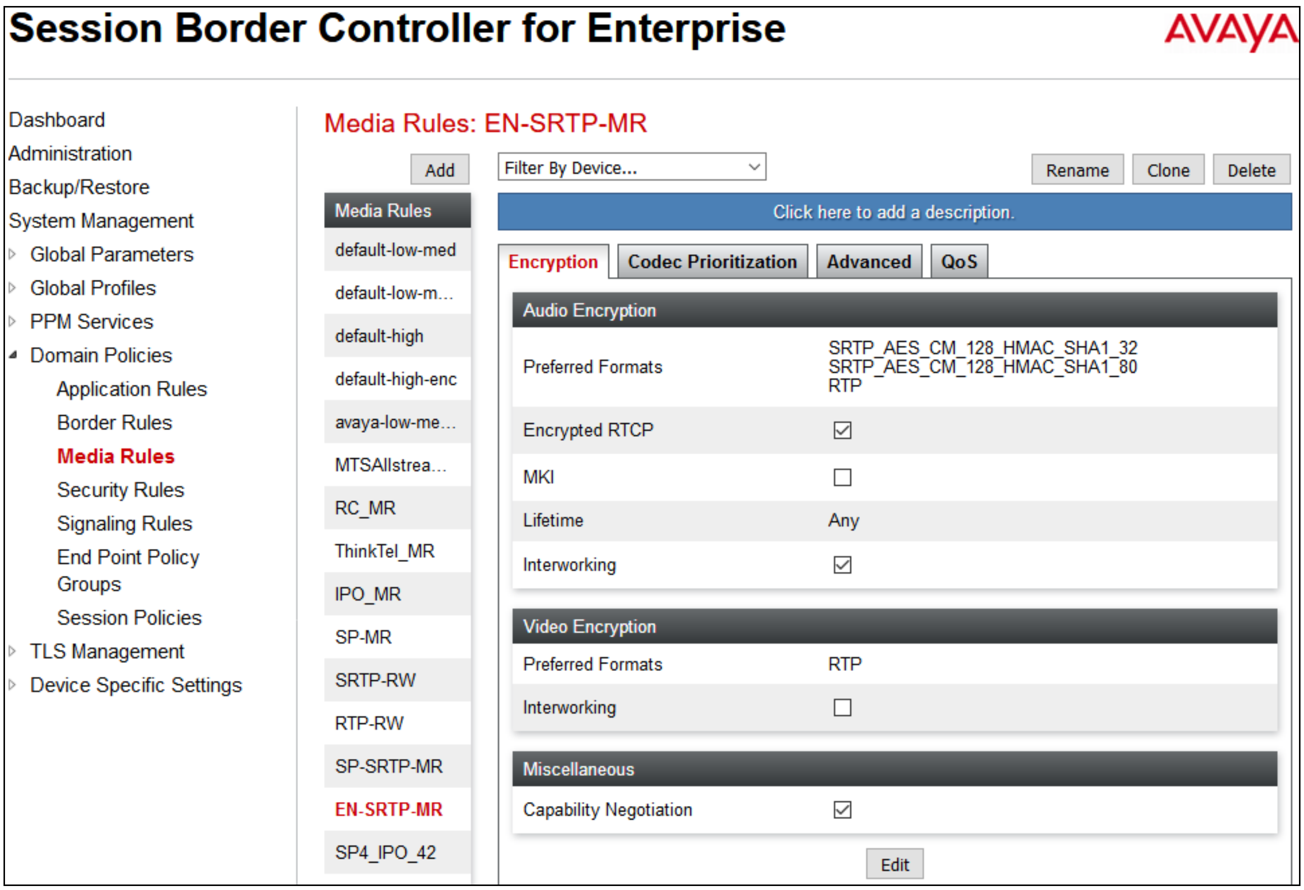
Media rules can be used to define RTP media packet parameters, such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies. You can also define how Avaya SBCE must handle media packets that adhere to the set parameters.

6.4.3.1 Media Rule for SP

In this compliance testing, Secure Real-Time Transport Protocol (SRTP, media encryption) is not supported by SP. Therefore, ***default-low-med*** rule is used for communication between Avaya SBCE and SP.

6.4.3.2 Media Rule for EN

Secure Real-Time Transport Protocol (SRTP, media encryption) is used between Avaya SBCE and IP Office. Therefore, it is necessary to create a media rule to apply to the internal interface of Avaya SBCE, EN. Created **EN-SRTP-MR** rule is shown below.



6.4.4. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to Server Flow defined in **Section 6.5.4**.

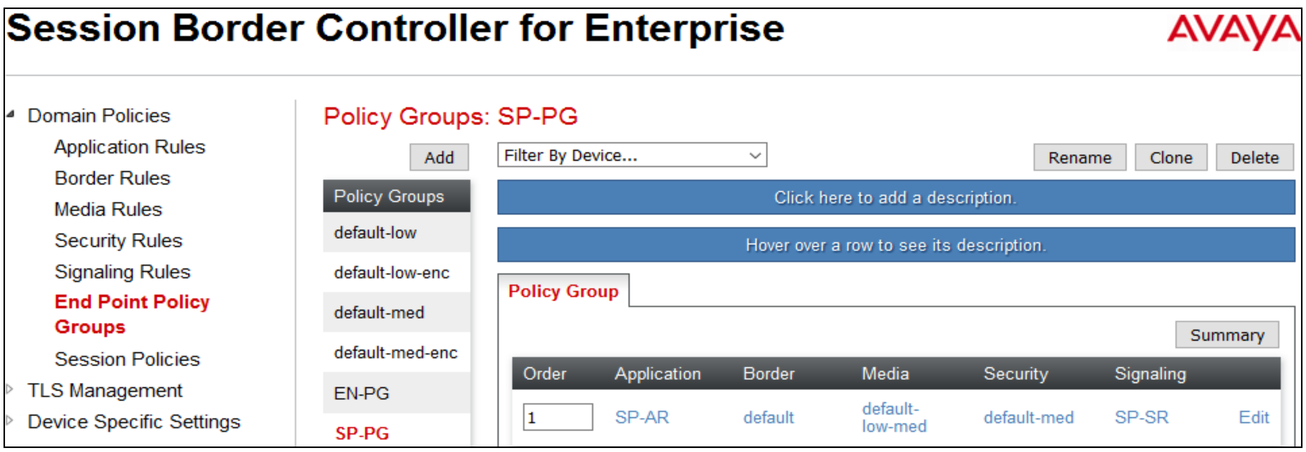
Endpoint Policy Groups were separately created for SP and EN.

To create a policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on the **Add** button.

6.4.4.1 Endpoint Policy Group for SP

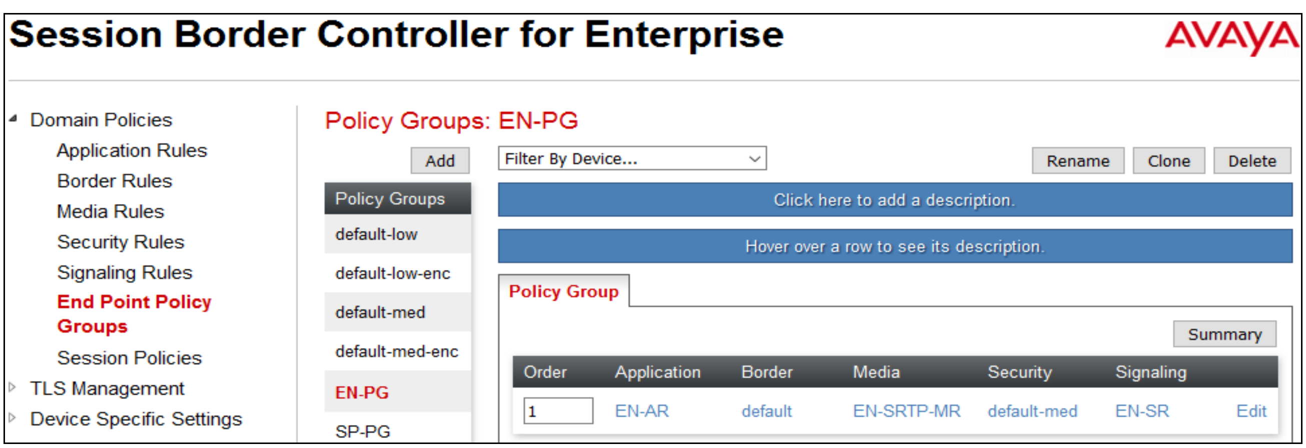
The following screen shows **SP-PG** created for SP.

- Set Application Rule to ***SP-AR*** which was created in **Section 6.4.2.1**.
- Set Media Rule to ***default-low-med***.
- Set Signaling Rule to ***SP-SR*** which was created in **Section 6.4.1.1**.
- Set Border Rule to ***default***.
- Set Security Rule to ***default-med***.



6.4.4.2 Endpoint Policy Group for EN

Similarly, the following screen shows policy group **EN-PG** created for EN.



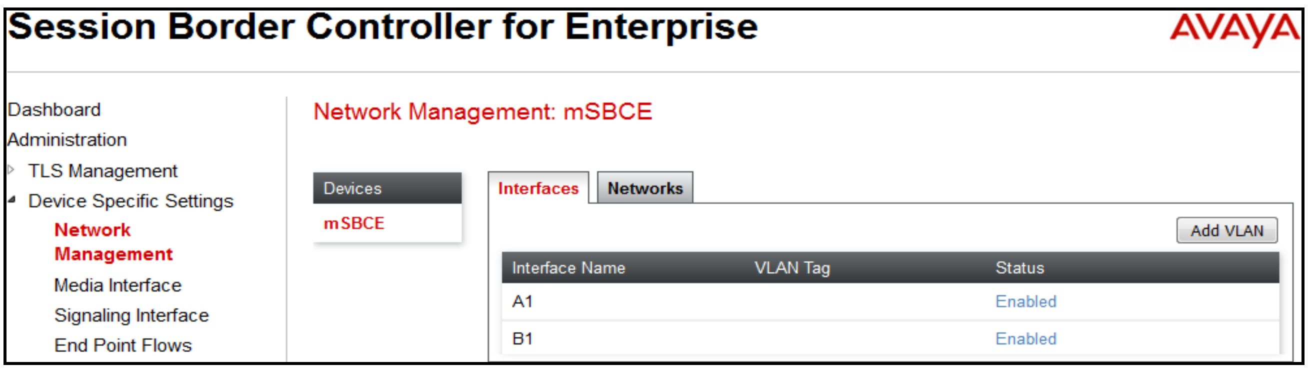
6.5. Device Specific Settings

The Device Specific Settings feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

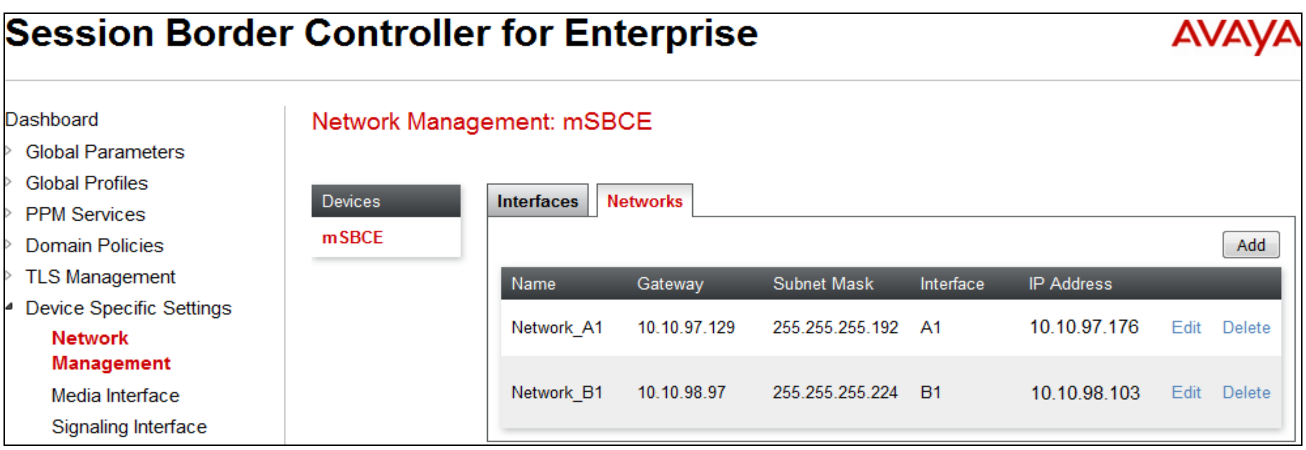
6.5.1. Network Management

The Network Management page is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP address, public IP address, subnet mask, gateway, etc., to interface the device to the networks. This information populates the various Network Management tabs which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Network Management**, under **Interfaces** tab, enable the interfaces connecting to the inside enterprise and outside service provider networks. To enable an interface, click on “Disable” Status. The following screen shows interface **A1** and **B1** were **Enabled**.



On the **Networks** tab, verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface was assigned to **A1** and the public interface was assigned to **B1** appropriate to the parameters shown in the **Figure 1**.



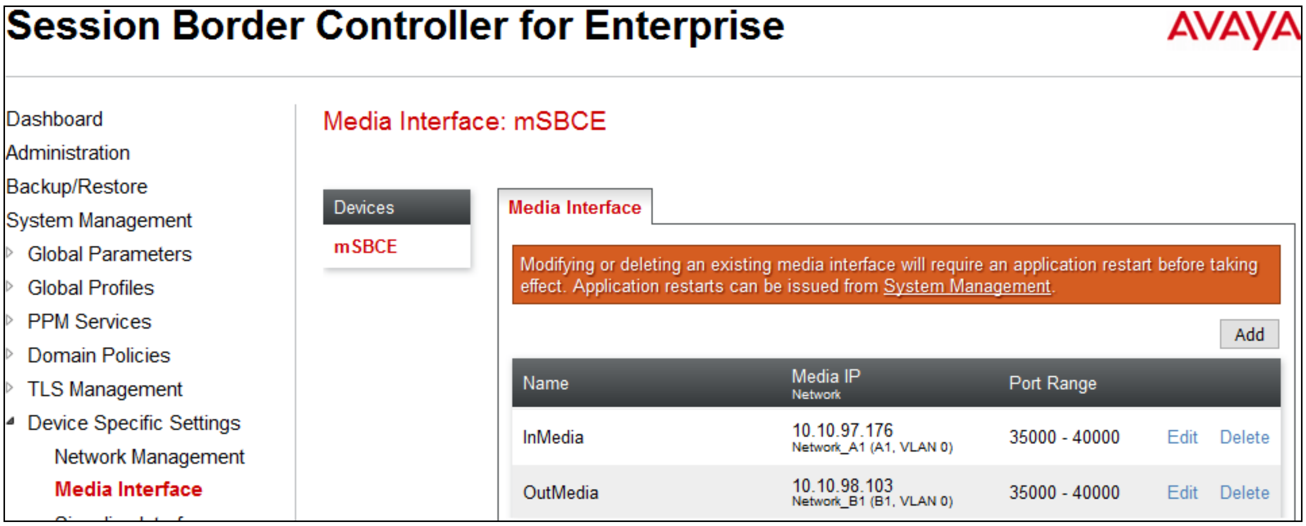
6.5.2. Media Interface

The Media Interface screen is where the media ports are defined. The Avaya SBCE will open connection for RTP traffic on the defined ports.

To create a new **Media Interface**, navigate to **Device Specific Settings → Media Interface** and click on the **Add Media Interface** button (not shown).

Two separate Media Interfaces are needed for both the inside and outside interfaces. The following screen shows the Media Interfaces **InMedia** and **OutMedia** were created for the compliance testing.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.

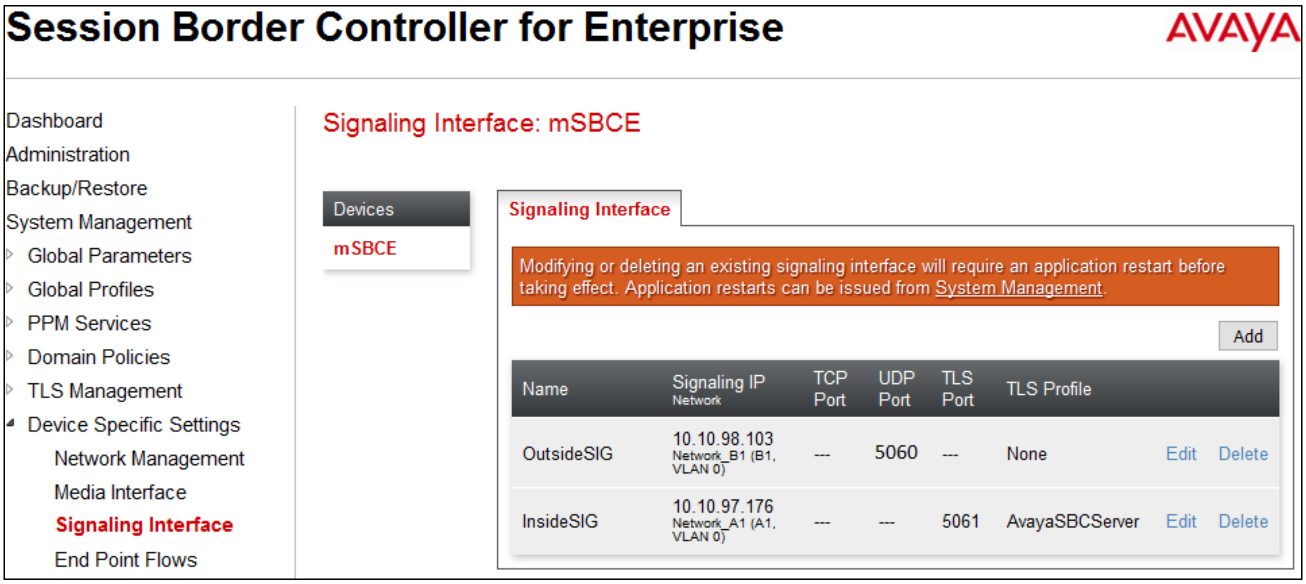


6.5.3. Signaling Interface

The Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP requests on the defined port.

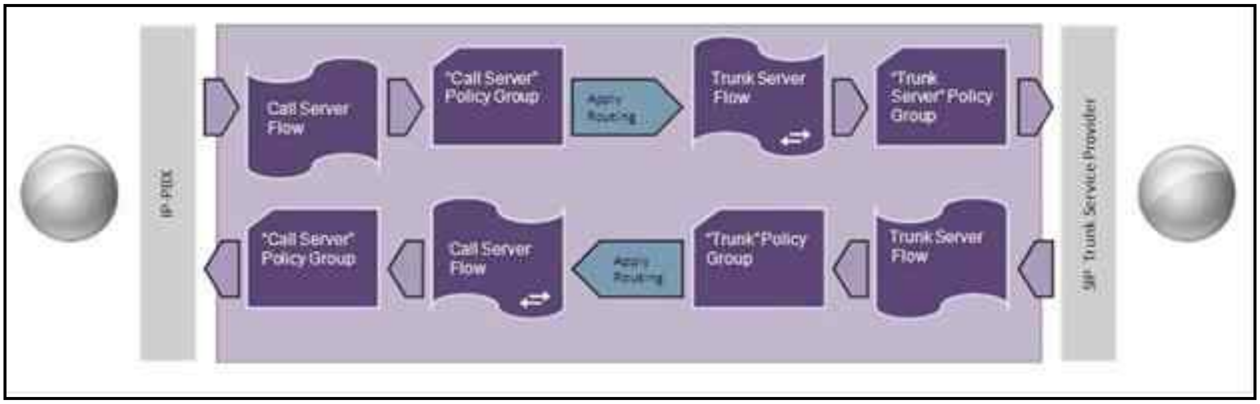
To create a new **Signaling Interface**, navigate to **Device Specific Settings → Signaling Interface** and click on the **Add** button.

Two separate Signaling Interfaces are needed for both inside and outside interfaces. The following screen shows the Signaling Interfaces **InsideSIG** and **OutsideSIG** were created in the compliance testing with **TLS/5061** and **UDP/5060** respectively configured for inside and outside interfaces.



6.5.4. End Point Flows - Server Flow

When a packet is received by the 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 which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

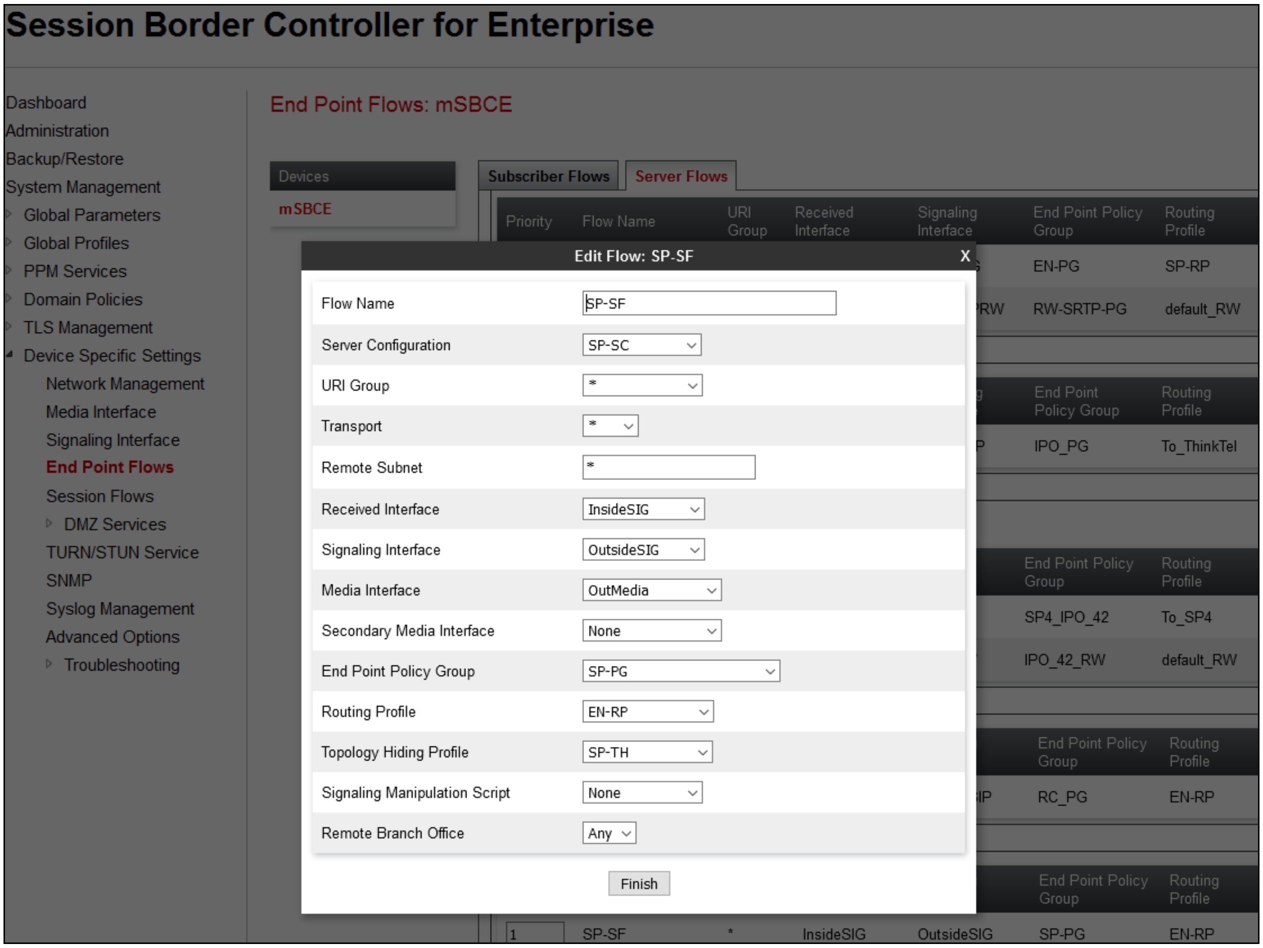


In the compliance testing, two separate Server Flows were created for SP and EN.

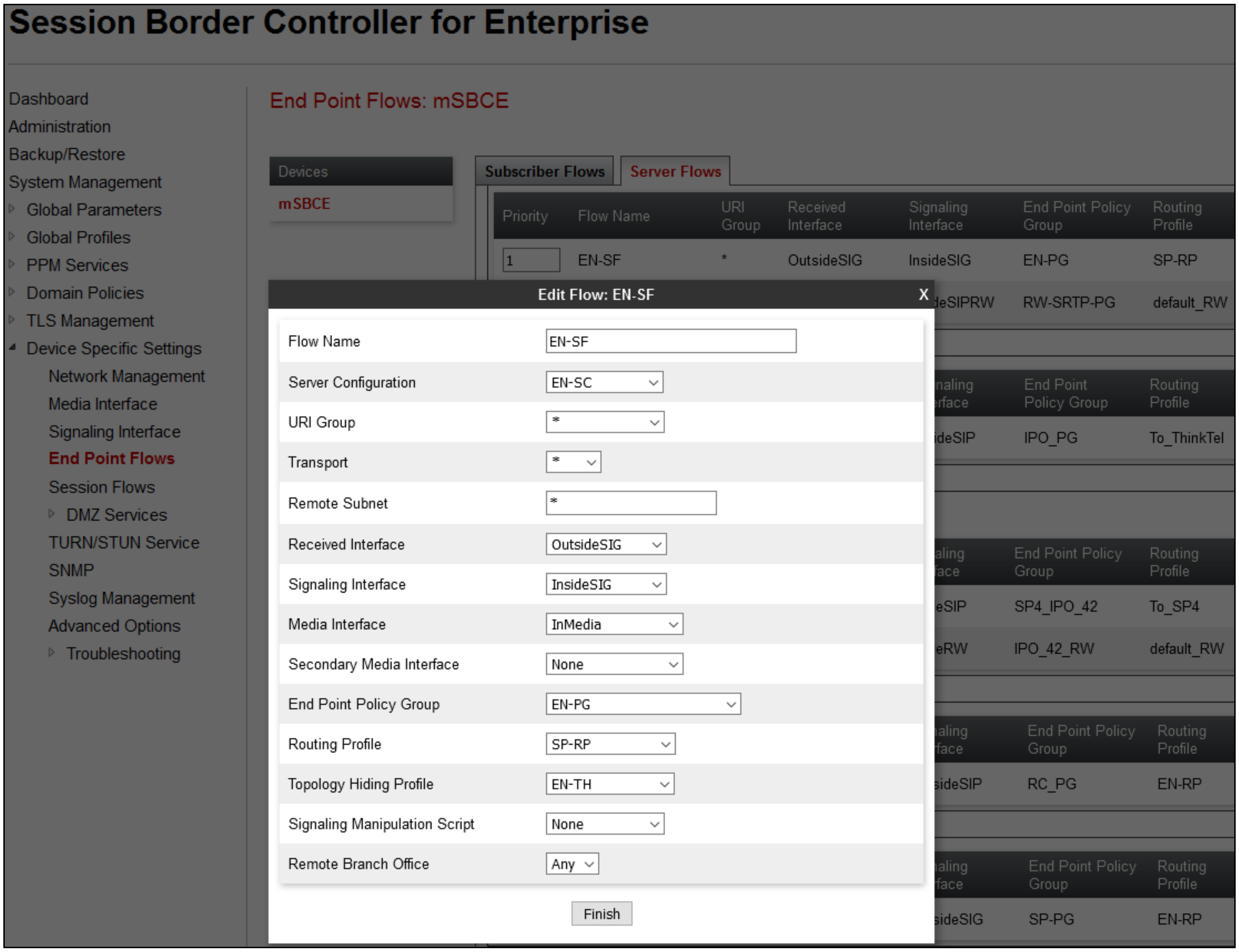
To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**, select the **Server Flows** tab and click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the other fields were kept as default.

- **Flow Name**: Enter a descriptive name.
- **Server Configuration**: Select Server Configuration created in **Section 6.3.3** which the Server Flow associates to.
- **URI Group**: Select "*****".
- **Received Interface**: Select the Signaling Interface created in **Section 6.5.3** which is the Server Configuration is designed to receive SIP signaling from.
- **Signaling Interface**: Select the Signaling Interface created in **Section 6.5.3** which is the Server Configuration is designed to send the SIP signaling to.
- **Media Interface**: Select the Media Interface created in **Section 6.5.2** which is the Server Configuration is designed to send the RTP to.
- **End Point Policy Group**: Select the End Point Policy Group created in **Section 6.4.4**.
- **Routing Profile**: Select the Routing Profile created in **Section 6.3.4.**
- **Topology Hiding Profile**: Select the Topology Hiding profile created in **Section 6.3.5** to apply toward the Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

The following screen shows the Server Flow **SP-SF** for SP.



Similarly, the following screen shows the Server Flow **EN-SF** for IP Office.



7. Windstream SIP Trunking Configuration

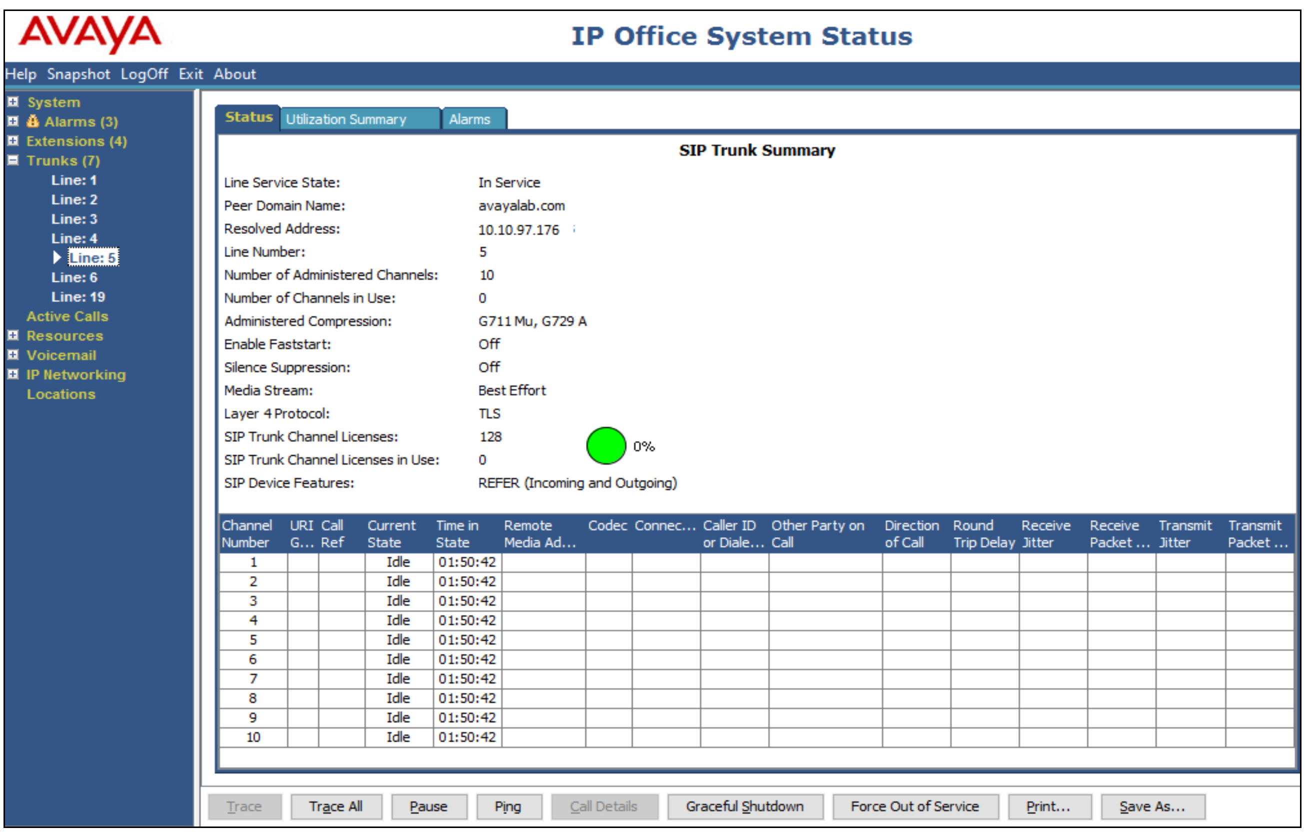
Windstream is responsible for the configuration of Windstream SIP Trunking service. The customer will need to provide the IP address used to reach the IP Office at the enterprise, this address will be the outside interface of the Avaya SBCE. Windstream will provide the customer the necessary information to configure the Avaya IP Office SIP connection to Windstream. The provided information from Windstream includes:

- IP address of the Windstream SIP proxy.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.
- SIP Credentials

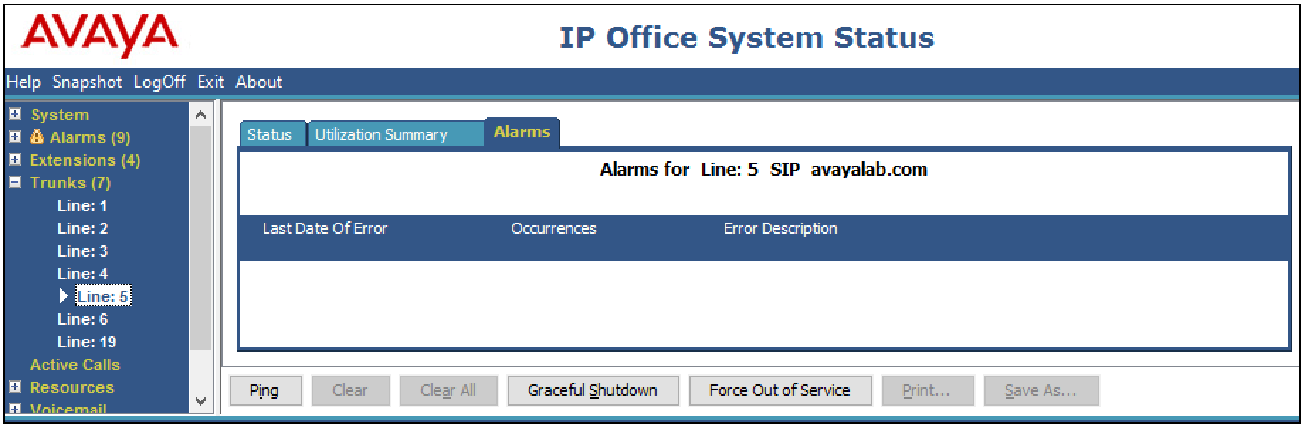
8. Verification Steps

The following steps may be used to verify the configuration:

- Use the Avaya IP Office System Status application to verify the state of the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select the SIP line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** is ***Idle*** for each channel (assuming no active calls at present time).



- Select the **Alarms** tab and verify that no alarms are active on the SIP line.



- Verify that a phone connected to PSTN can successfully place a call to the IP Office with two-way audio.
- Verify that a phone connected to IP Office can successfully place a call to the PSTN with two-way audio.
- Using a network sniffing tool (e.g., Wireshark) to monitor the SIP signaling between the enterprise and Windstream. The sniffer traces are captured at the public interface of the Avaya SBCE.

9. Conclusion

The Windstream SIP Trunking passed compliance testing with any observations/limitations detailed in **Section 2.2**. These Application Notes describe the procedures required to configure the SIP connection between Avaya IP Office, Avaya Session Border Controller for Enterprise and the Windstream SIP Trunking service as shown in **Figure 1**.

10. Additional References

[1] *Administering Avaya IP Office Platform with Manager*, Release 10.0, August 2016.
[2] *Avaya IP Office™ Platform Server Edition Reference Configuration, Release 10.0, Issue 04.AD, August 2016.*
[3] *Deploying IP Office™ Platform Server Edition Solution, Release 10.0, August 2016.*
[4] *IP Office™ Platform, Using a Voicemail Pro IP Office Mode Mailbox, Issue 10D, May 2016.*
[5] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 7.1, Issue 1, June 2016.
[6] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.1, Issue 1, June 2016.
[7] *Administering Avaya Session Border Controller for Enterprise*, Release 7.1, Issue 1, June 2016.
[8] *Application Notes for configuring Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.3 to support Remote Workers*, Issue 1.0.
[9] *Using Avaya Communicator for Web*, Release 1, Issue 1.0.6, May 2016.

Product documentation for Avaya products may be found at http://support.avaya.com. Additional IP Office documentation can be found at:
http://marketingtools.avaya.com/knowledgebase/

Product documentation for Windstream SIP Trunking is available from Windstream.

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.