Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 8.0 to support Telecom Liechtenstein SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 11.0 and Avaya Session Border Controller for Enterprise Release 8.0 to support Telecom Liechtenstein SIP Trunking Service. These Application Notes update previously published Application Notes with a newer software version of Avaya IP Office.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the public switched telephone network (PSTN) with various Avaya endpoints.

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.

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.

Table of Contents

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Telecom Liechtenstein and an Avaya SIP-enabled enterprise solution.

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of an Avaya IP Office Server Edition, two Avaya IP Office 500 V2 as expansion systems, running software release 11.0 (hereafter referred to as IP Office), Avaya Session Border Controller for Enterprise Release 8.0 (hereafter referred to as Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The Telecom Liechtenstein SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the IP Office solution are able to place and receive PSTN calls via a broadband wide area network (WAN) connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

The terms “service provider” or “Telecom Liechtenstein” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to Telecom Liechtenstein’s network via the public Internet, as depicted in **Figure 1**, and exercise the features and functionalities 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 this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). 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.

2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability the following features and functionalities were exercised during the interoperability compliance test:

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP and H.323 telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323 telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider network.
- Incoming and outgoing PSTN calls to/from Avaya Equinox for Windows soft-client.
- Dialing plans including local calls, international, outbound toll-free, etc.
- Caller ID presentation.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two-way speech-path. Testing was performed with codecs: G.711A and G.711MU, Telecom Liechtenstein's preferred codec order.
- Proper response to no matching codecs.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.
- T.38 and G.711 pass-through fax.

Items not supported or not tested included the following:

- Inbound toll-free call was not tested.
- 0, 0+10 digits, 411 Directory Assistance and 911 Emergency were not tested.

2.2. Test Results

Interoperability testing of Telecom Liechtenstein SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **OPTIONS –** Telecom Liechtenstein does not send OPTIONS messages to the Avaya enterprise network, but it does respond to OPTIONS messages it receives from the Avaya enterprise, this was sufficient to maintain the SIP trunk link up in service.
- **Telecom Liechtenstein supports SIP REFER and reINVITE methods for call transfers to the PSTN –** Telecom Liechtenstein supports SIP REFER and the reINVITE methods for call transfers to the PSTN, both methods were tested. With the SIP REFER method SIP trunk channel resources were NOT released when performing blind transfers to the PSTN, SIP trunk channels remained seized for the duration of the call, releasing only when PSTN parties hang-up. Traces showed Telecom Liechtenstein responding to the REFER sent by IP Office with 202 Accepted but the NOTIFY messages to update the call status or BYE to release the SIP trunk resources after the transfer was completed were never received from Telecom Liechtenstein. BYE messages were received only when the PSTN parties hang-up. This behavior was only seen with blind transfers to the PSTN, with consultative transfers SIP trunk resources were released as expected after the transfer was completed, SIP trunk resources were released after Telecom Liechtenstein responded to the REFER IP Office sent with 202 Accepted message. The behavior seen with blind transfers did not have any user impact, the transfers were successful with two-way audio, it's being mentioned here simply as an observation.
- **Support of Redirect/Transfers to the PSTN using reINVITE or SIP REFER methods –** As mentioned in the above observation, Telecom Liechtenstein supports SIP REFER and the reINVITE methods for call transfers to the PSTN, the Redirect and Transfer fields under the SIP Line controls which method is used, the options are **Always**, **Auto** or **Never**. For the compliance test the option **Auto** was used (refer to **Section 5.4.2**), with this option, the **Allow** header in SIP OPTIONS messages received from Telecom Liechtenstein is used to determine if the REFER method is supported. Currently, since Telecom Liechtenstein does not send SIP OPTIONS messages to the enterprise, the method for call transfers to the PSTN may default to reINVITE. If the REFER method for call transfers to the PSTN is preferred the option **Always** should be selected.
- **Outbound Calling Party Number block (calls with privacy enabled)** – The Calling Party Number is not blocked on calls from IP Office to the PSTN with privacy enabled at the IP Office station (Withhold Number enabled). This issue is caused by IP Office not including the privacy header (privacy = id) in the INVITE message sent to Telecom Liechtenstein. A Signaling Manipulation script (SigMa) was created in the Avaya SBCE to add "Privacy = id" to the INVITE messages on calls with privacy enabled in the IP Office stations (**Sections 7.3.3** and **12**). This issue is under investigation by Avaya.
- **No matching codecs on outbound calls –** Telecom Liechtenstein responds with 503 Service Unavailable instead of 488 Not Acceptable Here to calls with audio codecs not supported.

- **T.38 fax support –** Telecom Liechtenstein does not support multiple “m=” lines in reINVITE message IP Office sends to switch from voice to T.38 fax mode. Incoming T.38 fax calls (calls from the PSTN to IP Office) would always start with an INVITE containing only audio codecs in the SDP, when the fax tone is detected IP Office sends a reINVITE to switch from voice to T.38 mode, this reINVITE contains multiple “m=” lines in the SDP, one with “m=audio 0 RTP/AVP 8” (notice the port set to “0” meaning inactive) and one with “m=image xxxx udptl t.38” (with xxxx representing a valid port number). Telecom Liechtenstein responded with 488 Not Acceptable Here to the reINVITE message. Reversing the “m=” line order in the SDP, with T.38 listed first and audio with port 0 listed second did not make a difference, Telecom Liechtenstein still responded with 488 Not Acceptable Here. This behavior was not seen with outbound T.38 fax calls; outbound T.38 fax calls (calls from IP Office to the PSTN) were successful.
- **G.711 Pass-Through fax support –** Inbound G.711 pass-through fax (PSTN → IP Office) was unreliable during the compliance test. Outbound G.711 pass-through fax (IP Office → PSTN) was successful. The issue related to inbound G.711 pass-through fax being unreliable during the compliance test may be related to the unpredictability of G.711 pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay.
- **Caller ID display on Call Forward to the PSTN –** For Calls from the PSTN to IP Office that were forwarded back out to the PSTN, the caller ID number displayed at the PSTN was always of the first DID number assigned to the SIP Trunk, regardless of the PSTN number being used to originate the call.
- **Caller ID display on Mobile Twinning –** For Mobile Twinning calls the Caller ID display at the Mobile/Cellular station was always of the first DID number assigned to the SIP Trunk, regardless of the PSTN number being used to originate the call.
- **Incorrect Call Display on call transfers to the PSTN Phone** – Call display was not properly updated on PSTN phones involved in call transfers. After successful call transfers to the PSTN, the PSTN phone did not display the actual connected party, instead the DID number assigned to the IP Office station that initiated the transfer was displayed.
- **SIP endpoints may indicate the transfer failed even when it is successful** – Occasionally on a transfer operation, Avaya IP Office SIP endpoints (Avaya 1100 Series Deskphones and Avaya Equinox for Windows) may indicate on the local call display that the transfer failed even though it was successful. The frequency of this behavior can be reduced by enabling “Emulate Notify for REFER” on the IP Office SIP Line (**Section 5.4.6**). It was observed during the testing that this behavior still occurred after enabling this option on the SIP Line.

2.3. Support

For support on Telecom Liechtenstein systems visit the corporate Web page at: http://www.telecom.li/de

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates the test configuration used for the DevConnect compliance testing. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the Telecom Liechtenstein SIP Trunking Service through the public Internet.

The Avaya components used to create the simulated enterprise customer site includes:

- IP Office Server Edition running in VMware environment.
  - Avaya IP Office Voicemail Pro.
- Two Avaya IP Office 500 V2 as expansion systems.
- Avaya Session Border Controller for Enterprise.
- Avaya 96x1 Series IP Deskphones (H.323).
- Avaya J179 IP Deskphones (H.323).
- Avaya 1100 Series IP Deskphones (SIP).
- Avaya J129 IP Deskphones (SIP).
- Avaya 1400 Series Digital Deskphones.
- Analog Deskphones.
- Avaya Equinox™ for Windows softphone (SIP).
- Fax devices.

Avaya IP Office provides the voice communications services for the enterprise. In the reference configuration, Avaya IP Office runs on the Avaya IP Office Server Edition platform. Note that this solution is extensible to deployments using the standalone IP500 V2 standalone platform as well.

In the sample configuration, the Primary server runs the Avaya IP Office Server Edition Linux software. Avaya Voicemail Pro runs as a service on the Primary Server. The LAN1 port of the Primary Server is connected to the enterprise LAN. The LAN2 port was not used.

The Expansion Systems (IP500 V2) are used for the support of digital, analog and additional IP stations. The Avaya IP Office 500 V2 systems are equipped with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module). The LAN1 port of the Avaya IP Office IP500 V2 is connected to the enterprise LAN, while the LAN2 port was not used.

Located at the edge of the enterprise is the Avaya SBCE. The Avaya SBCE has two physical interfaces, interface **B1** is used to connect to the public network, interface **A1** is used to connect to the private network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. The Avaya SBCE provides network address translation at both the IP and SIP layers.

IP endpoints at the enterprise included 96x1 Series IP Deskphones (with H.323 firmware), Avaya 1100 (with SIP firmware), J100 Series IP Deskphones (with SIP and H.323 firmware), Avaya 1400 Series digital Deskphones, analog Deskphones and Avaya Equinox™ for Windows

Softphones (SIP). Some IP endpoints were registered to the Primary Server while others were registered to the IP500 V2 Expansion Systems. Avaya 1400 Series Digital Deskphones and analog telephones are connected to media modules on the Expansion Systems. The site also has a Windows PC running Avaya IP Office Manager to configure and administer the system. Mobile Twinning is configured for some of the IP Office users so that calls to these user's extensions will also ring and can be answered at the configured mobile phones.

The transport protocol between the Avaya SBCE and Telecom Liechtenstein, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network, is SIP over TLS.

For inbound calls, the calls flowed from Telecom Liechtenstein to the Avaya SBCE, then to IP Office.

Outbound calls to the PSTN were first processed by IP Office. Once IP Office selected the proper SIP trunk, the call was routed to the Avaya SBCE for egress to Telecom Liechtenstein's network.

During the compliance test, users dialed a short code of 9+00 and 11 digits including a 1 (US country code) since the testing was performed from North America (U.S) (e.g., 9 001 786 331 1234). For inbound calls from the PSTN to Avaya IP Office, the user dialed the international prefix 011 plus the 10 digits DID number provided by Telecom Liechtenstein (e.g., 011 423 237 1234).

In an actual customer configuration, the enterprise site may include additional network components between the service provider and the IP Office system, such as a session border controller or data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that all SIP and RTP traffic between the service provider and the IP Office system must be allowed to pass through these devices.

For confidentiality and privacy purposes, public IP addresses, domain names, and routable DID numbers used during the compliance testing have been masked.

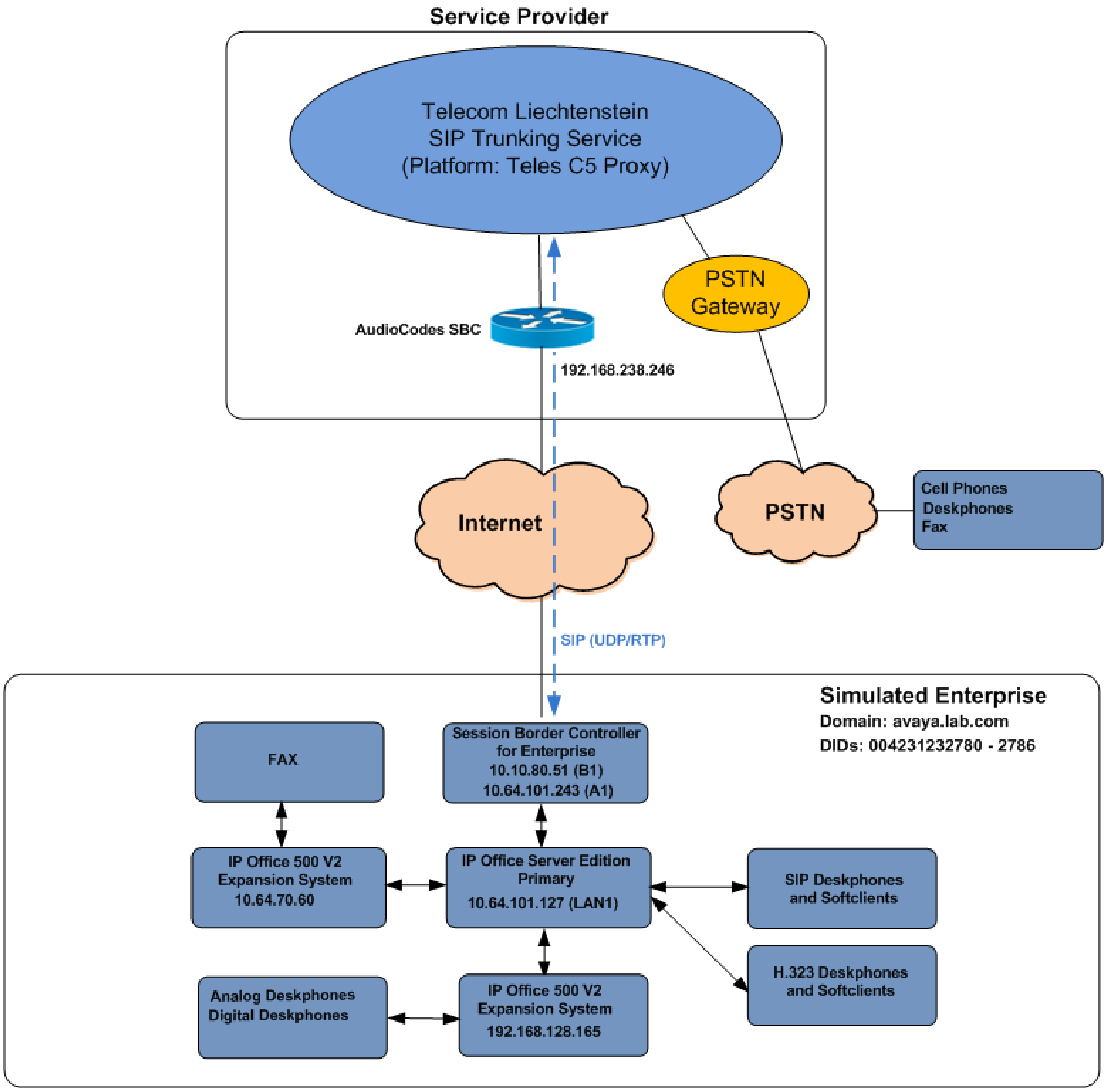


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

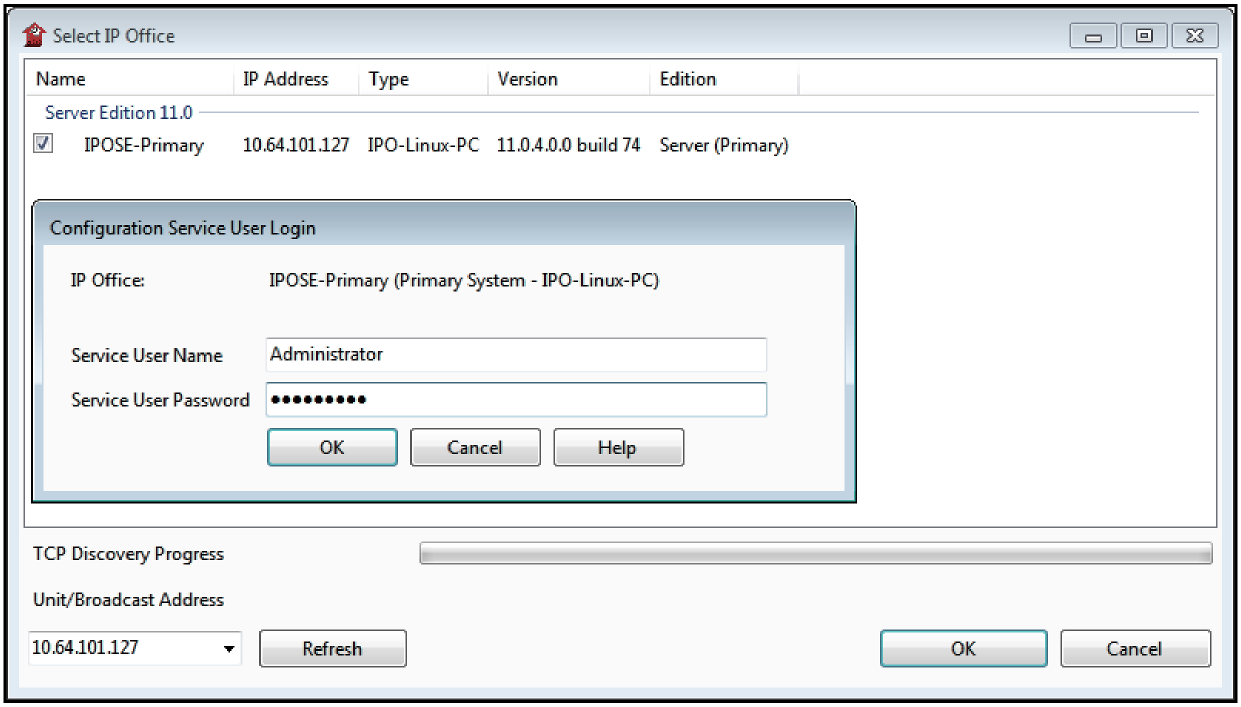
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server) • Avaya IP Office Voicemail Pro	11.0.4.0.0 Build 74 11.0.4.0.0 Build 5
Avaya IP Office IP500 V2 (Expansion Systems)	11.0.4.0.0 Build 74
Avaya IP Office Manager	11.0.4.0.0 Build 74
Avaya Session Border Controller for Enterprise	ASBCE 8.0 8.0.0.0-19-16991
Avaya 96x1 Series IP Deskphones (H.323)	6.8002
Avaya J179 IP Telephone (H.323)	6.8002
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.0.0.0.21
Avaya 1408 Digital Telephone	48.02
Avaya Equinox™ for Windows (SIP)	3.5.6.10.1
Analog Telephone	---
Telecom Liechtenstein	
AudioCodes SBC	7.20A
Teles C5 Proxy	6.0.2

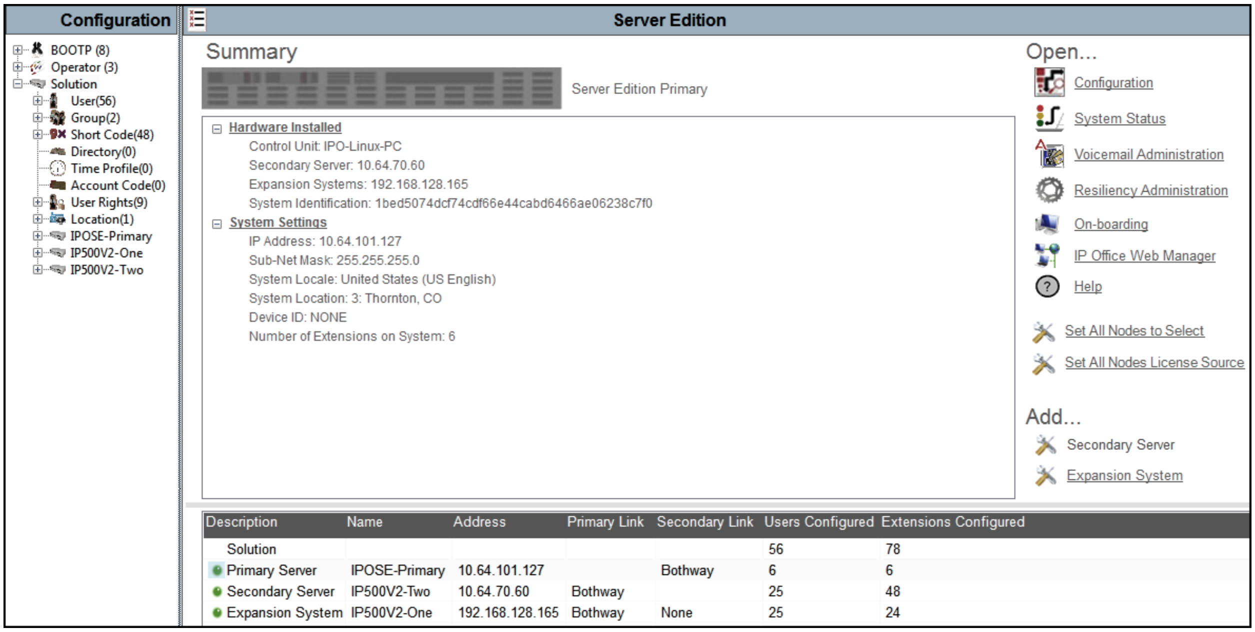
Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints.

5. Avaya IP Office Primary Server Configuration

Avaya IP Office is configured through the Avaya IP Office Manager application. From the PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the Manager application. Log in using the appropriate credentials.



On Server Edition systems, the Solution View screen will appear, similar to the one shown below. All the Avaya IP Office configurable components are shown in the left pane, known as the Navigation Pane. Clicking the “plus” sign next to the Primary server system name, e.g., **IPOSE-Primary**, on the navigation pane will expand the menu on this server.



In the screens presented in the following sections, the View menu was configured to show the Navigation pane on the left side and the Details pane on the right side. These panes will be referenced throughout the rest of this document.

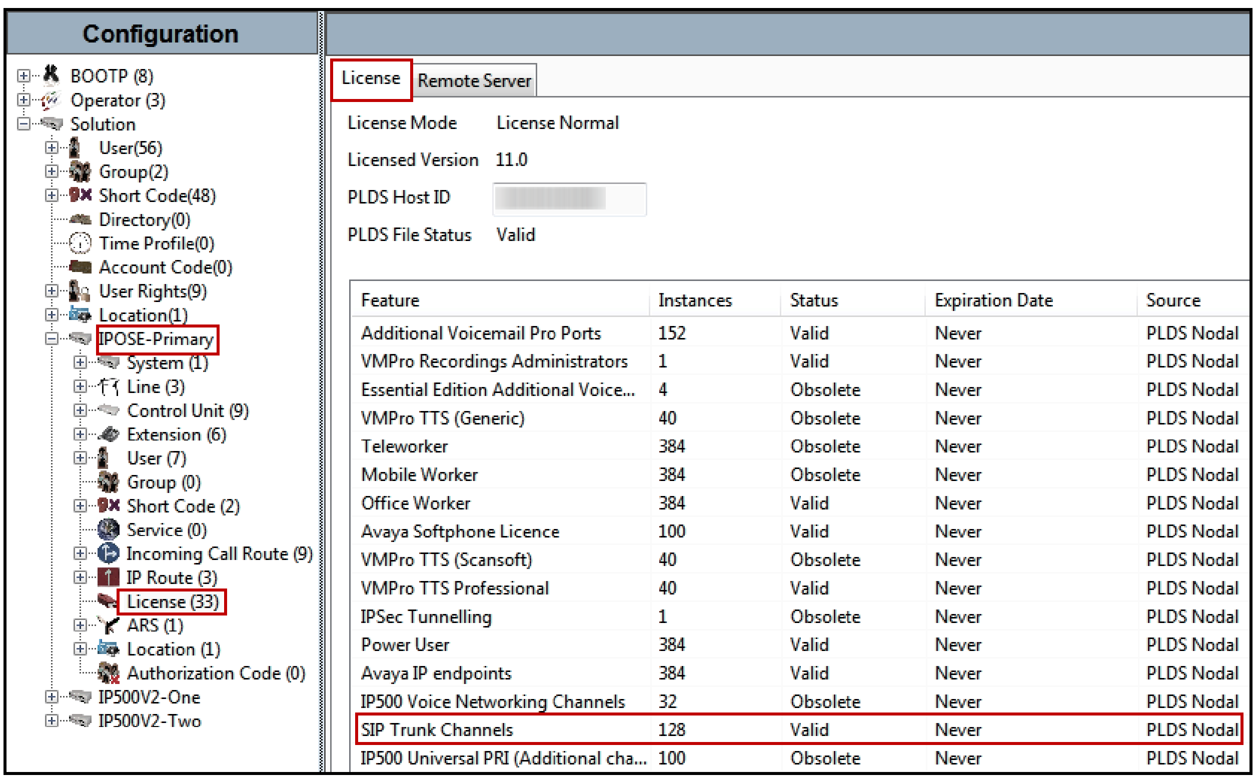
Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

5.1. Licensing

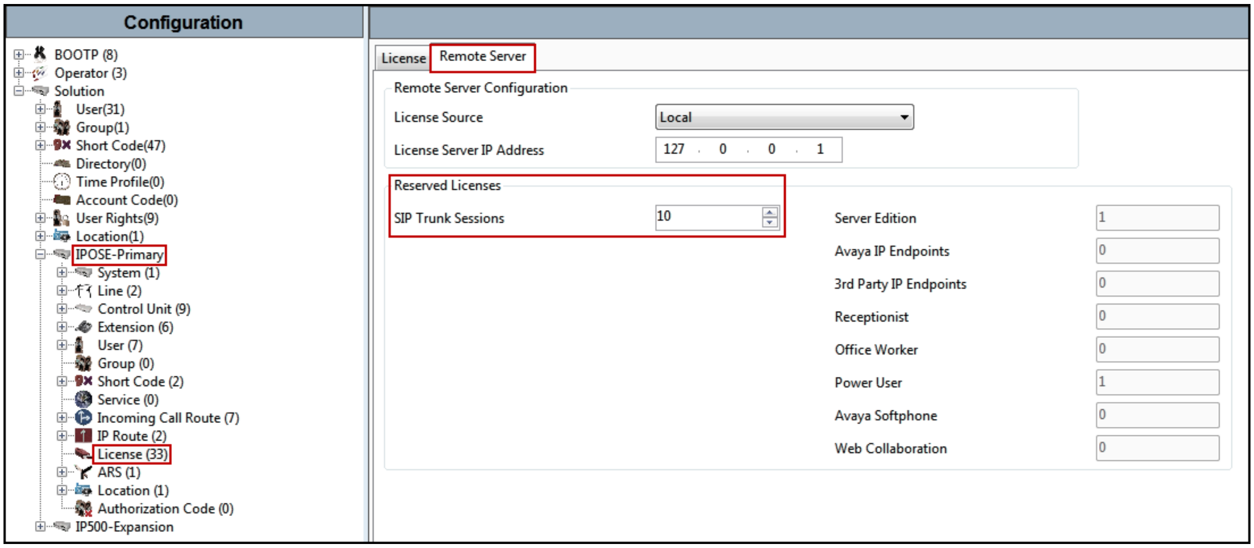
The configuration and features described in these Application Notes require the IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

In the reference configuration, **IPOSE-Primary** was used as the system name of the Primary Server, **IP500V2-One** and **IP500V2-Two** were used as the system name for the two Expansion Systems. All navigation described in the following sections (e.g., **License**) appears as submenus underneath the system name in the Navigation Pane.

Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of channels provisioned for the SIP trunk.



On Server Edition systems, the number of licenses to be assigned to the specific Server or Expansion System is reserved from the total pool of licenses present on the license server. On the screen below, 10 **SIP Trunk Sessions** licenses were reserved to be used by the Primary Server.



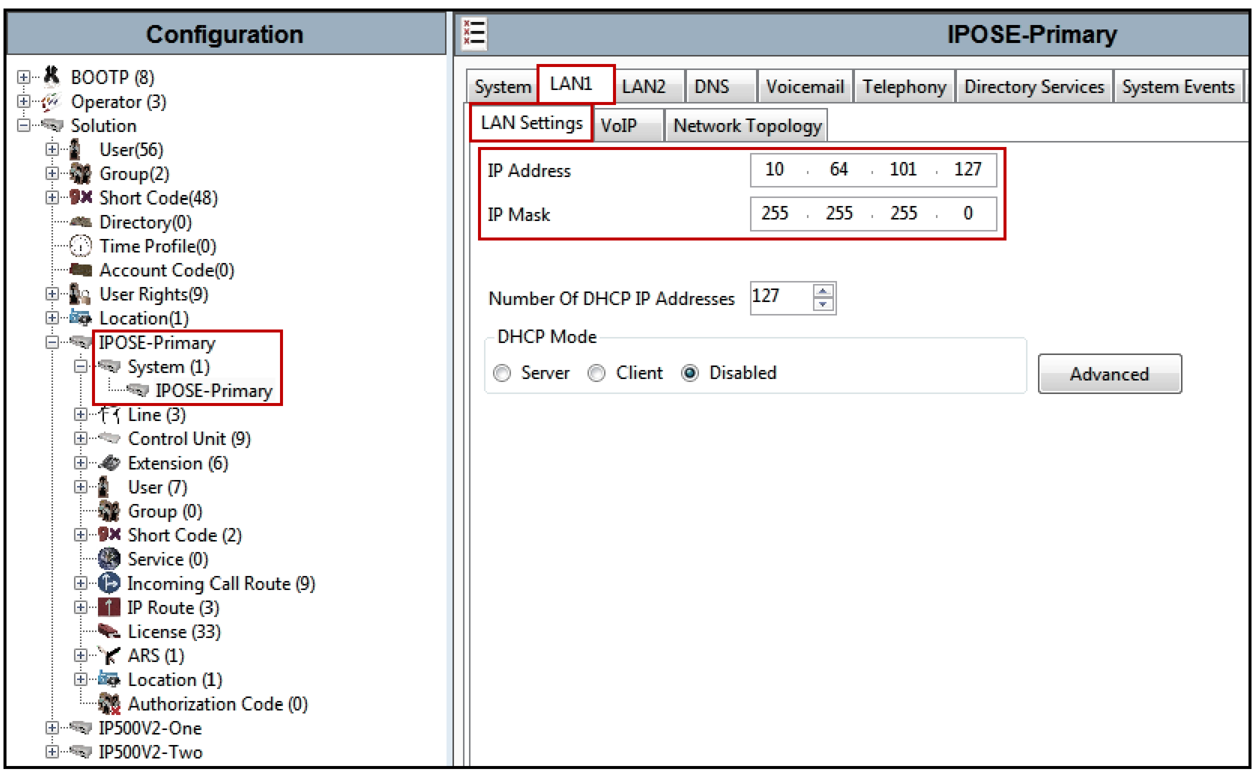
5.2. System Settings

Configure the necessary system settings. In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to connect IP Office to the enterprise private network (LAN), the **LAN2** was not used since in this configuration the connection to the public network is done via the **LAN1** port through the Avaya SBCE.

5.2.1. System - LAN1 Tab

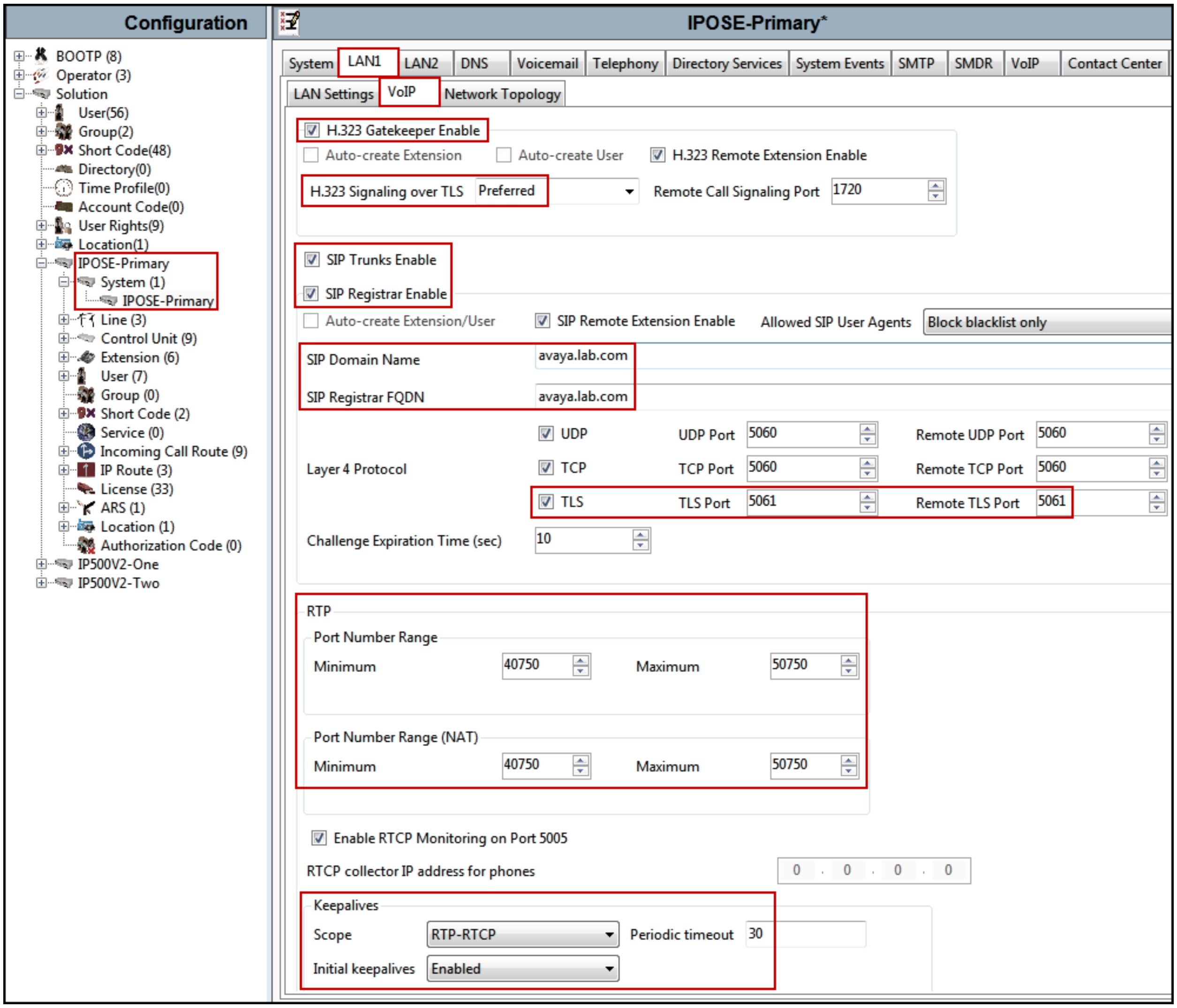
In the sample configuration, **IPOSE-Primary** was used as the system name and the **LAN1** port connects to the inside interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface (public, interface **B1**) of the Avaya SBCE connects to Telecom Liechtenstein's network via the public internet. The **LAN1** settings correspond to the **LAN** port in IP Office. To access the **LAN1** settings, navigate to **System (1) → IPOSE-Primary** in the Navigation Pane, then in the Details Pane navigate to the **LAN1→ LAN Settings** tab. The **LAN1** settings for the compliance testing were configured with following parameters:

- Set the **IP Address** field to the LAN IP address, e.g., **10.64.101.127**.
- Set the **IP Mask** field to the subnet mask of the enterprise private network, e.g., **255.255.255.0**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).



The **VoIP** tab as shown in the screenshot below was configured with following settings:

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Select **Preferred** under **H.323 Signaling over TLS**. When enabled, TLS is used to secure the registration and call signaling communication between IP Office and endpoints that support TLS. The H.323 phones that support TLS are 9608, 9611, 9621, and 9641 running firmware version 6.6 or higher.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Telecom Liechtenstein.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name of the enterprise under **SIP Domain Name**.
- Enter the SIP Registrar FQDN of the enterprise under **SIP Registrar FQDN**.
- Check TLS and verify the **TLS Port** numbers under **Layer 4 Protocol** is set to **5061**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP-RTCP**, **Periodic Timeout** to **30**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send RTP and RTCP keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP/RTCP traffic is present.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

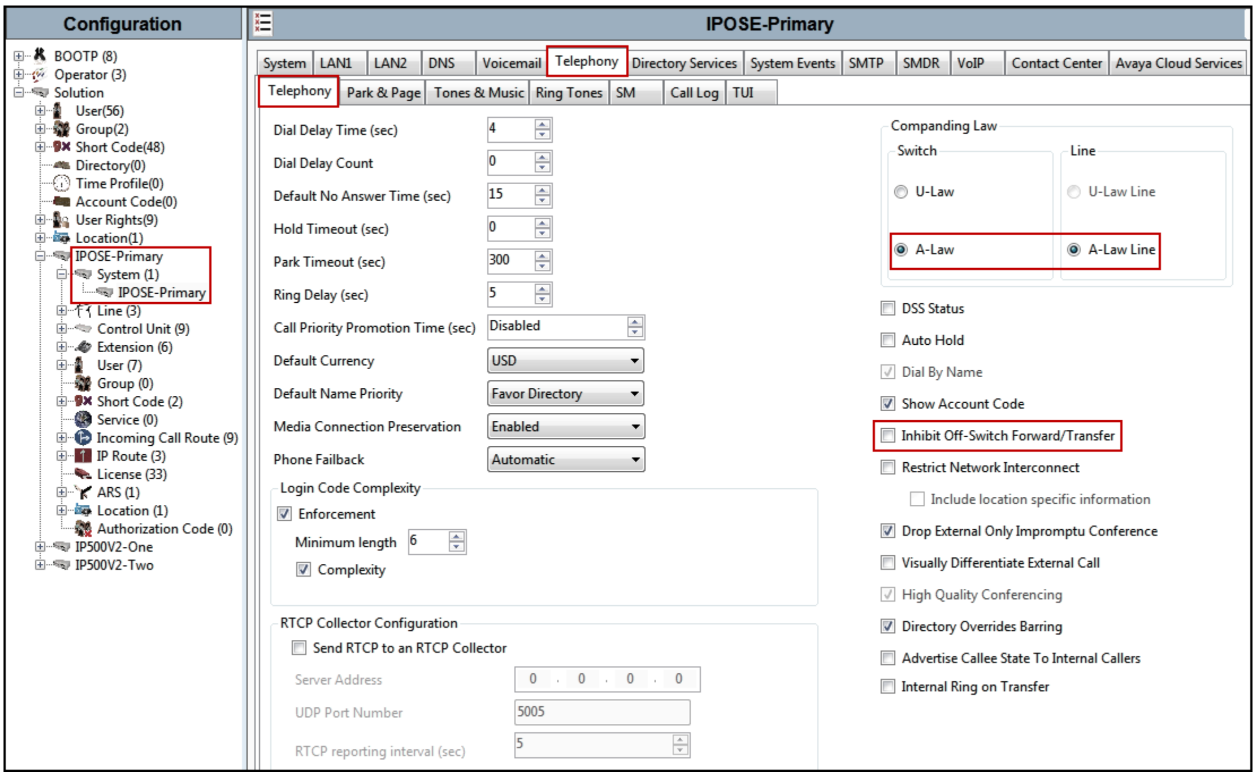


Note: In the compliance test, the **LAN1** interface was used to connect IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.2. System - Telephony Tab

To access the System Telephony settings, navigate to the **Telephony → Telephony** tab in the **Details** pane, configure the following parameters:

- Choose the **Companding Law** typical for the enterprise location; **A-Law** was used for the compliance test.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN. If for security reasons incoming calls should not be allowed to transfer back to the PSTN then leave this setting checked.
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).



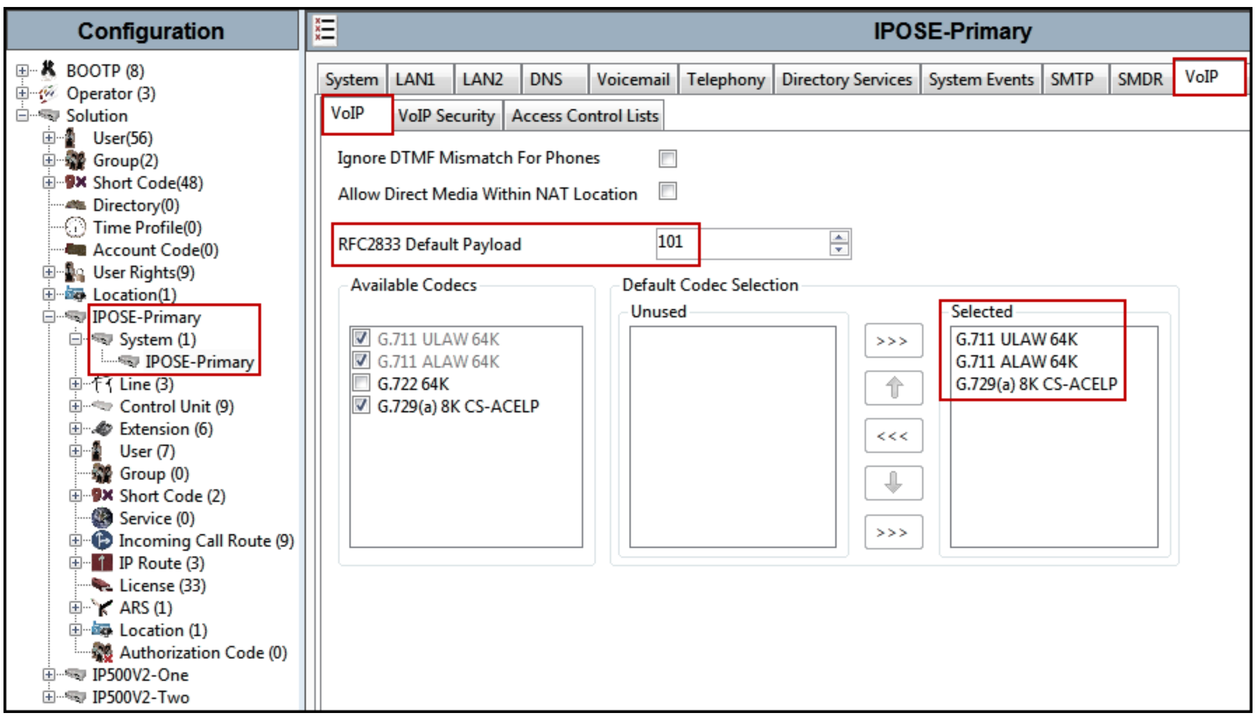
5.2.3. System - VoIP Tab

Navigate to the **VoIP** tab in the Details pane to view or change the system codecs and VoIP security settings.

5.2.3.1 VoIP - VoIP Tab

Select the **VoIP → VoIP** tab, configure the following parameters:

- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used.
- For codec selection, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order were used.
- Click **OK** to commit (not shown).



Note: The codec selections defined under this section (VoIP – VoIP Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.5** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.2.3.2 VoIP – VoIP Security Tab

Secure Real-Time Transport Protocol (SRTP) refers to the application of additional encryption and or authentication to VoIP calls (SIP and H.323). SRTP can be applied between telephones, between ends of an IP trunk or in various other combinations.

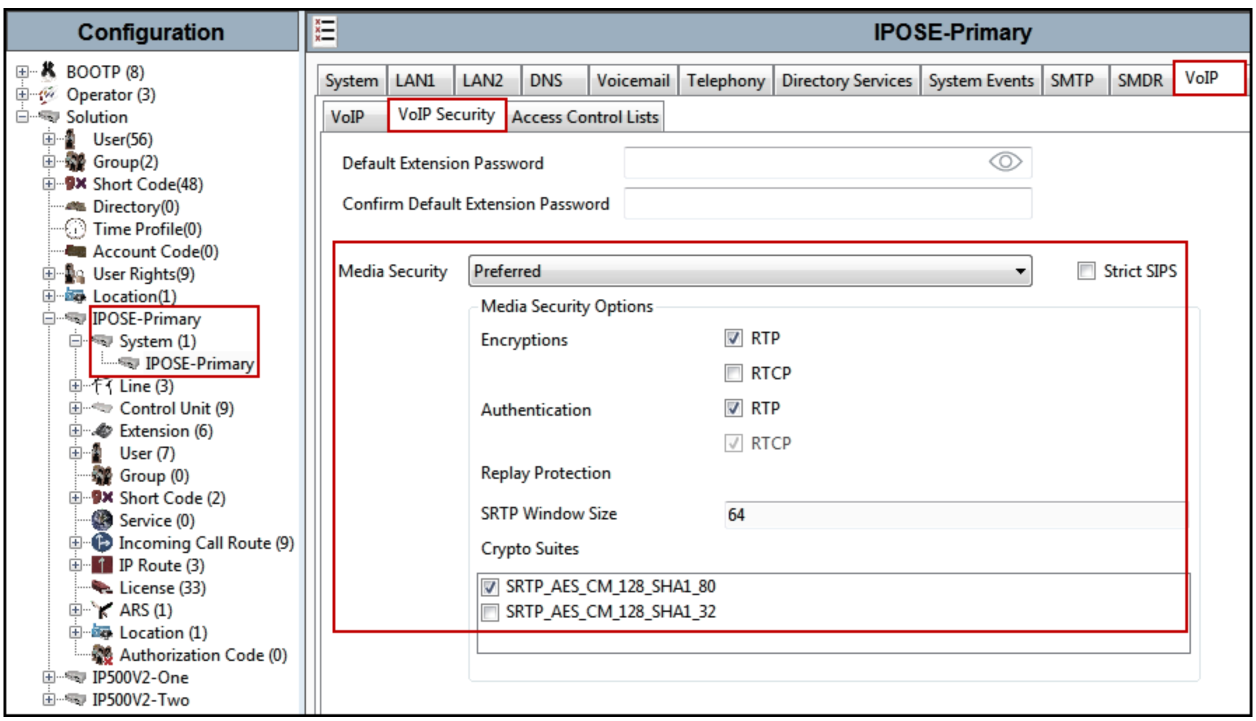
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

- Disabled (default).
- Preferred.
- Enforced.

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

To configure the use of SRTP, select the **VoIP → VoIP Security** tab on the Details pane.

- Set the **Media Security** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption.
- Verify **Strict SIPS** is not checked.
- Under **Media Security Options**, select **RTP** for the **Encryptions** and **Authentication** fields.
- Under **Crypto Suites**, select **SRTP_AES_CM_128_SHA1_80**.
- Click **OK** to commit (not shown).

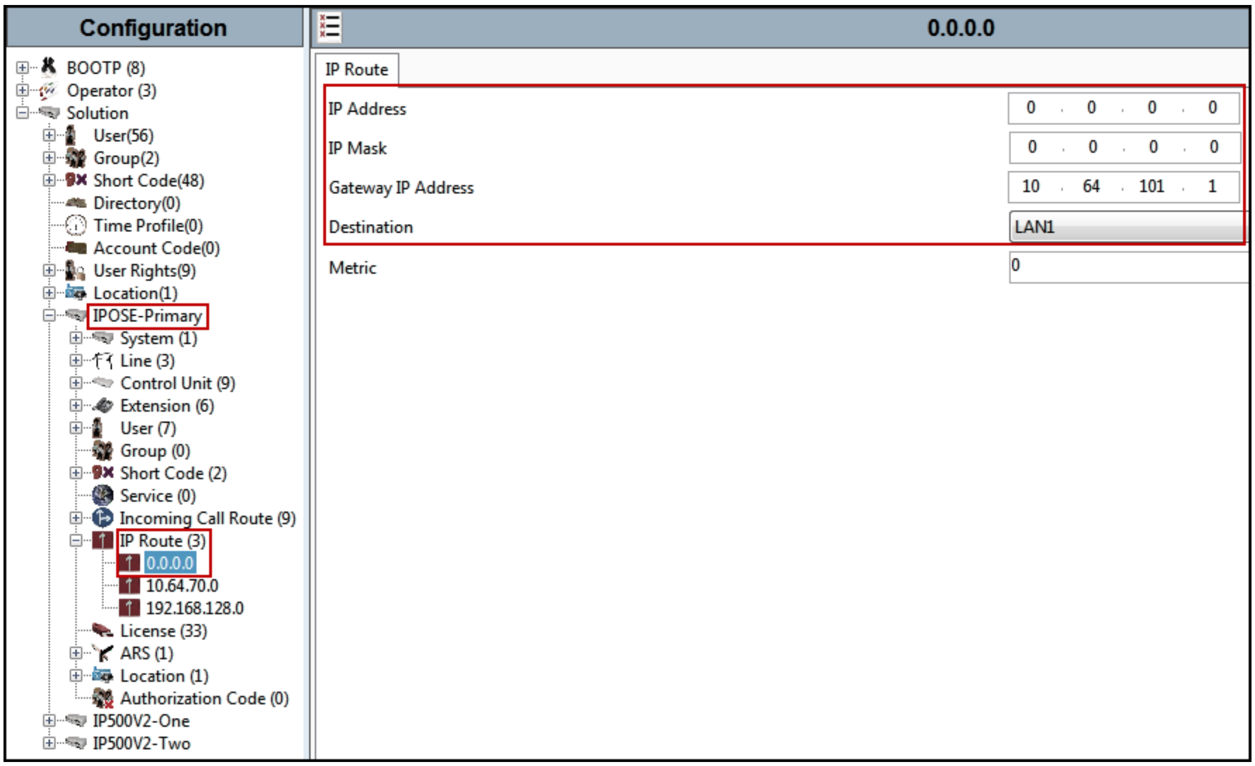


5.3. IP Route

Create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to route calls to Telecom Liechtenstein's network.

Navigate to **IP Route**, right-click on **IP Route** and select **New**. The values used during the compliance test are shown below:

- Set the **IP Address** and **IP Mask** to **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP address of the gateway/router used to route calls to the public network, e.g., **10.64.101.1**.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).



5.4. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Telecom Liechtenstein. 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 **Sections 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** to **5.4.6**.

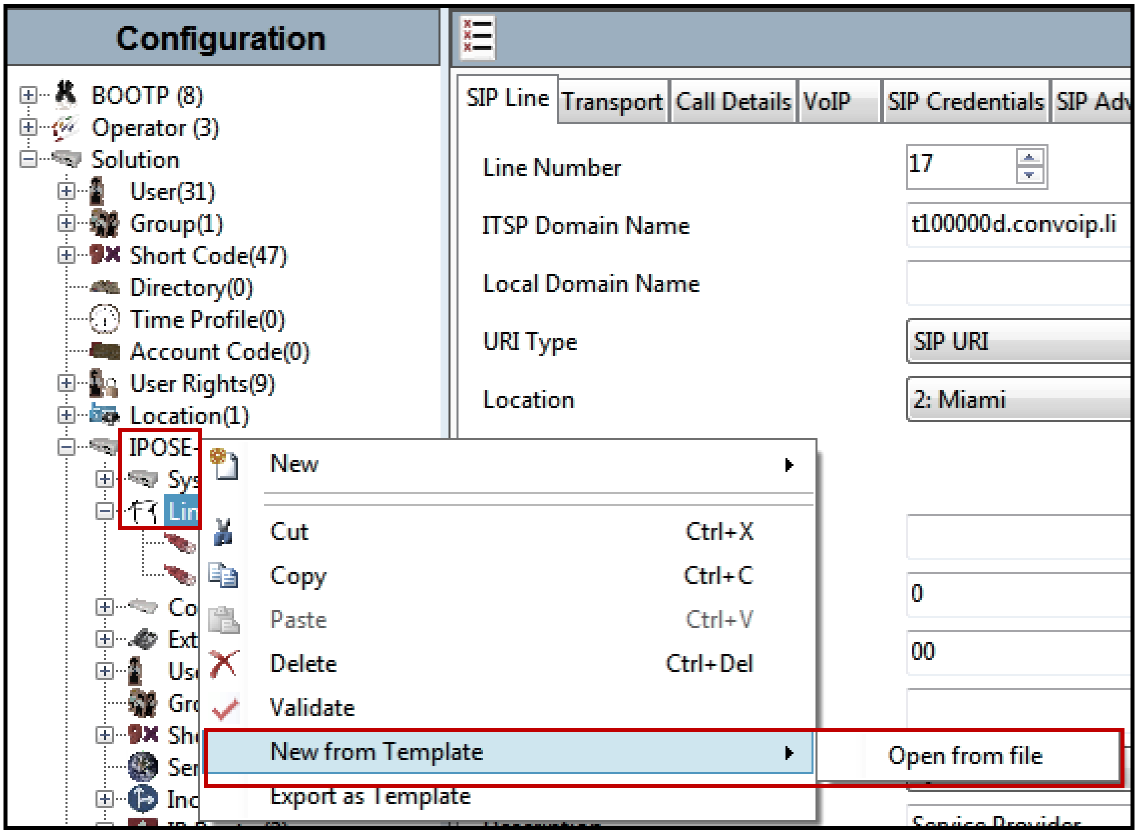
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.6**.

5.4.1. Creating a SIP Trunk from an XML Template

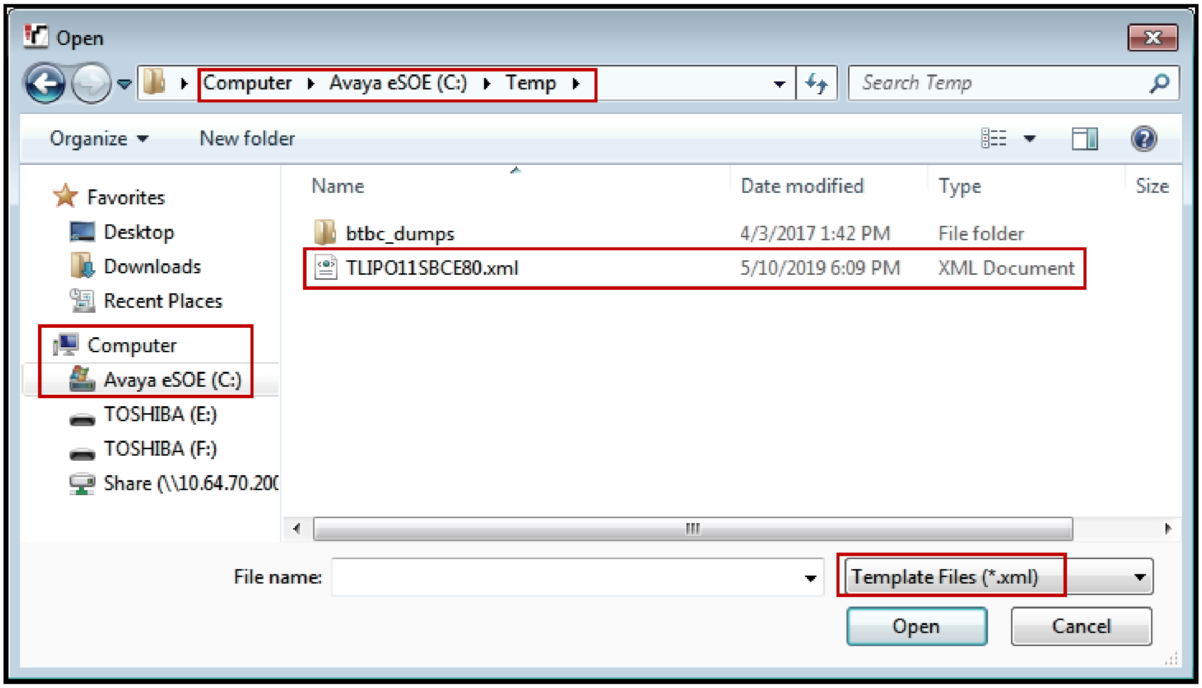
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

Copy a previously created template file to a location (e.g., *\Temp*) on the same computer where IP Office Manager is installed.

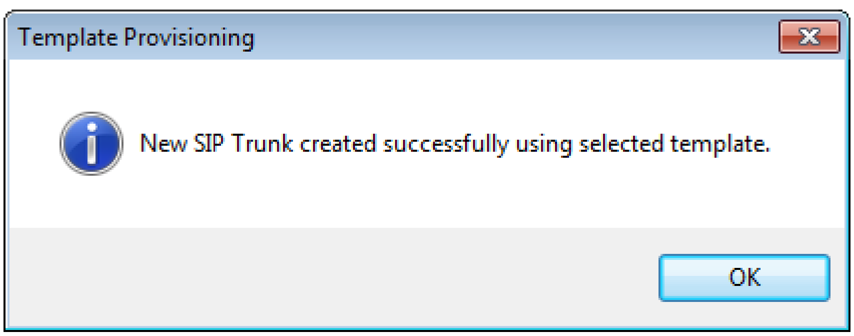
To create the SIP Trunk from the template, from the **Primary** server, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template→Open from file**.



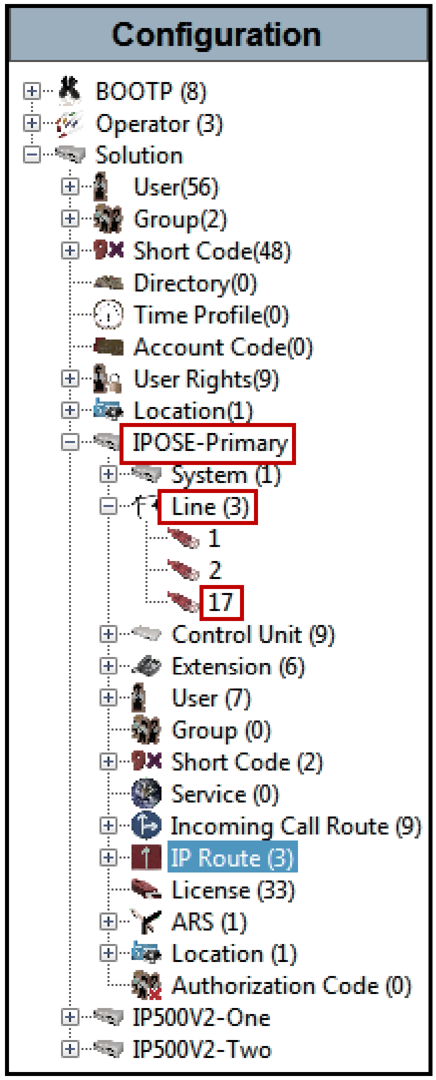
Navigate to the directory on the local machine where the template was copied and select the template.



After the import is complete, a final import status pop-up window will open stating success or failure. Click **OK**.



The newly created SIP Line will appear in the Navigation pane (e.g., SIP Line **17**).

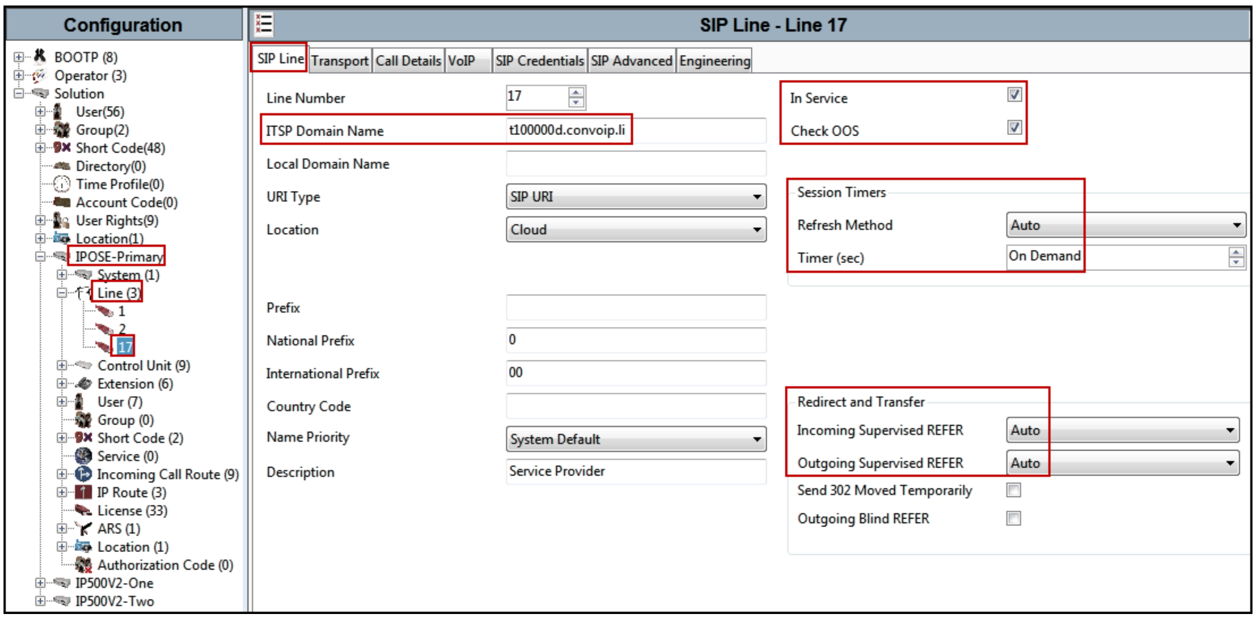


It is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2** to **5.4.6**.

5.4.2. SIP Line – SIP Line Tab

On the **SIP Line** tab in the **Details** pane, configure or verify the parameters as shown below:

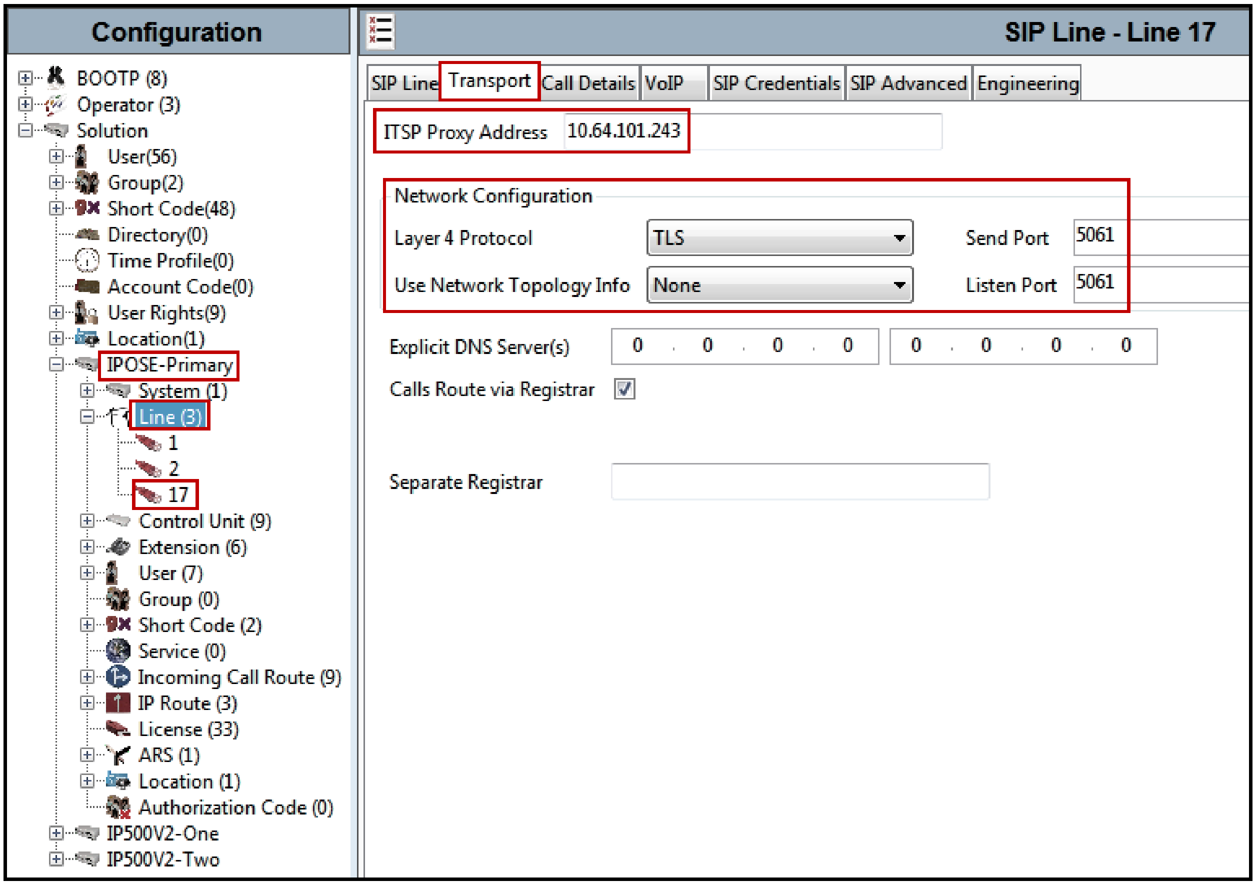
- Set **ITSP Domain Name** to the domain name provided by Telecom Liechtenstein.
- Verify that **In Service** box is checked, the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (sec)** is set to **On Demand**.
- For the compliance test REFER support was set to **Auto**, refer to **Section 2.2**.
- Click **OK** to commit (not shown).



5.4.3. SIP Line - Transport Tab

Select the **Transport** tab. Set or verify the parameters as shown below:

- Set the **ITSP Proxy Address** to the inside IP Address of the Avaya SBCE or **10.64.101.243** as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **TLS**.
- Set **Use Network Topology Info** to **None** (see note below).
- Set the **Send Port** to **5061**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

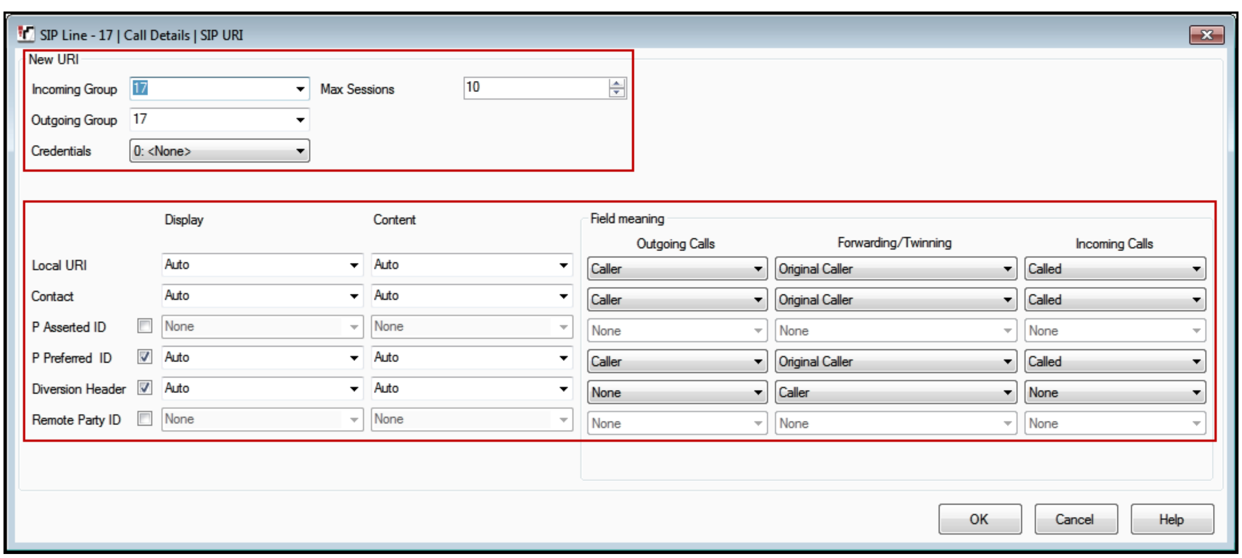


Note – For the compliance testing, the **Use Network Topology Info** field was set to **None**, since no NAT was used in the test configuration. In addition, it was not necessary to configure the **System → LAN1 → Network Topology** tab for the purposes of SIP trunking. If a NAT is used between Avaya IP Office and the other end of the trunk, then the **Use Network Topology Info** field should be set to the LAN interface (LAN1) used by the trunk and the **System → LAN1 → Network Topology** tab needs to be configured with the details of the NAT device.

5.4.4. SIP Line – Call Details Tab

Select the **Call Details** tab, and then click the **Add…** button (not shown) and the screen shown below will appear. 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 new entry was added. The entry was created with the parameters shown below:

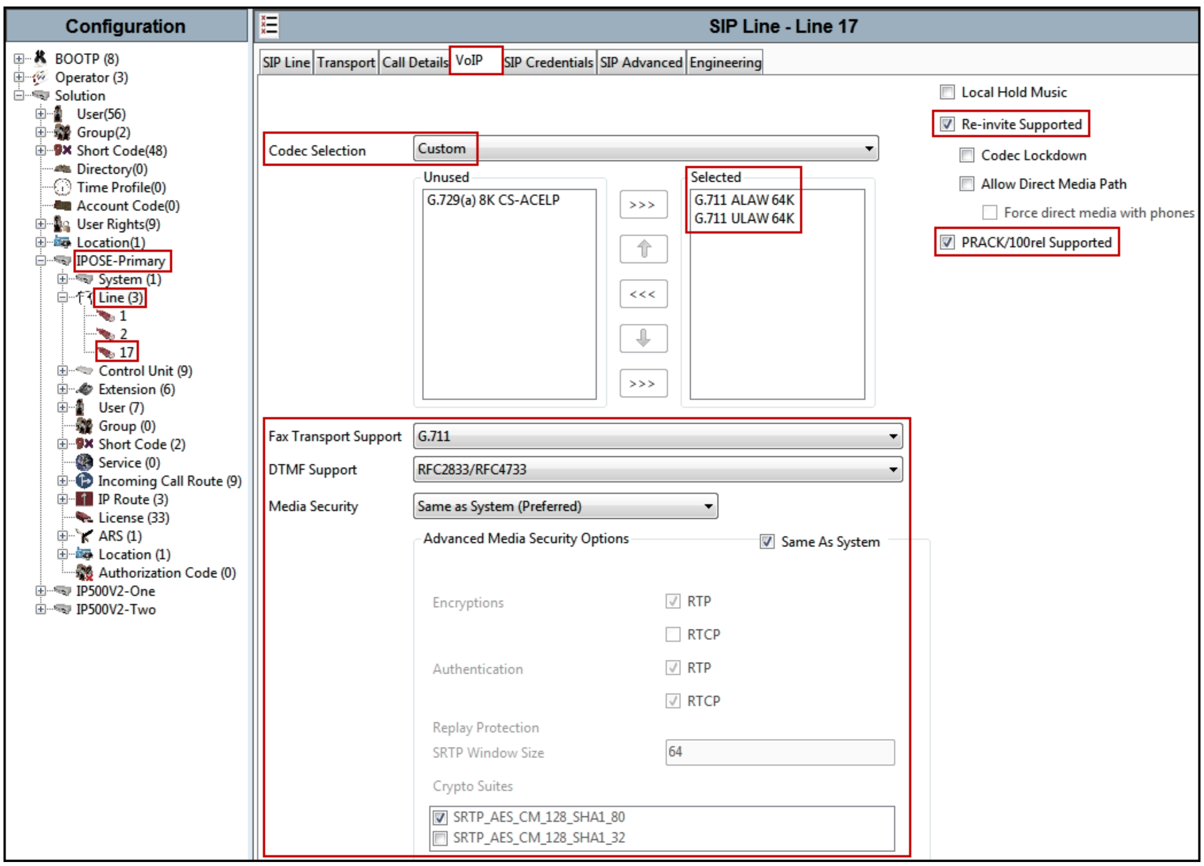
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Set the **Credentials** field to **0: <None**.
- Check the **P Preferred ID** and **Diversion Header**.
- For the **Local URI**, **Contact**, **P Preferred ID** and **Diversion Header** leave the selections under the **Display** and **Content** columns to the default **Auto**. With this setting, IP Office will use the information on the **Incoming Call Routes** (**Section 5.6**) to populate the From and Contact headers on outbound calls, and to determine which inbound calls will be allowed on the SIP line.
- On the **Field meaning** section, set the values under the **Outgoing Calls**, **Forwarding/ Twinning** and **Incoming Calls** columns as shown on the screenshot below.
- Click **OK**.
- Click **OK** to commit again (not shown).



5.4.5. SIP Line - VoIP Tab

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

- The **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line, as shown. Telecom Liechtenstein supports codecs **G.711ALAW** and **G.711ULAW** for audio.
- Select **G.711** for **Fax Transport Support** (Refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set the **Media Security** field to **Same as System (Preferred)**.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).

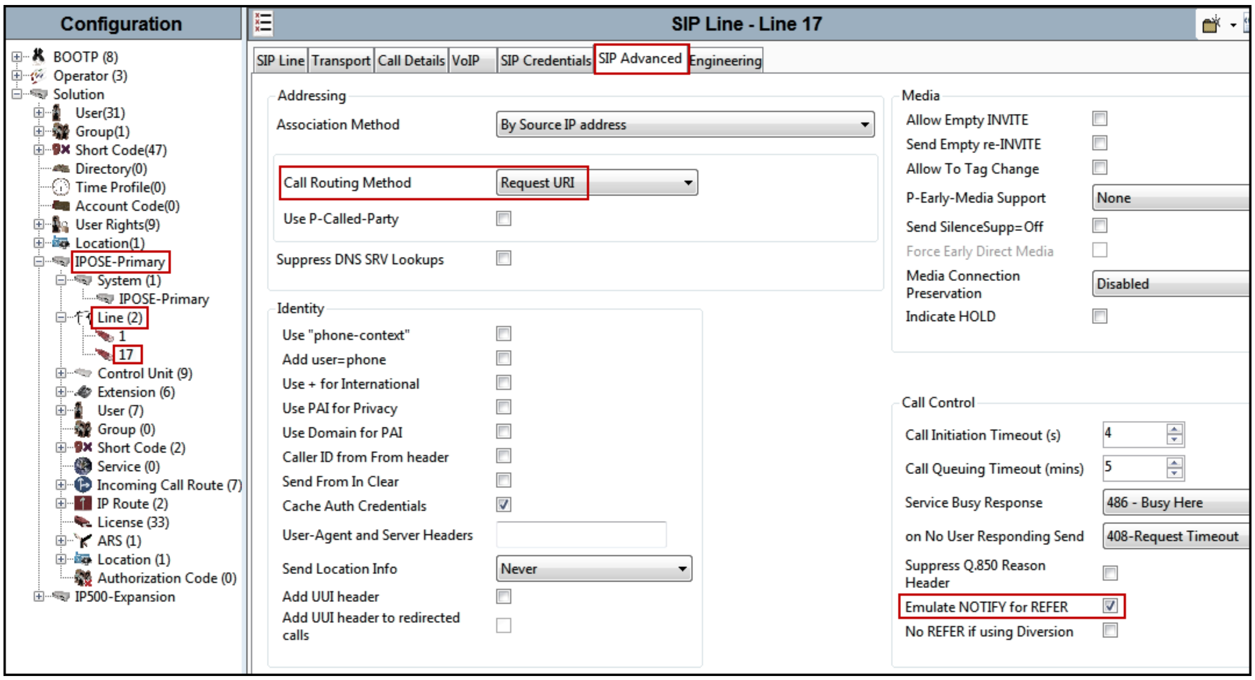


Note: The codec selections defined under this section are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.3** are the codecs selected for the IP phones/extension (H.323 and SIP).

5.4.6. SIP Line – SIP Advanced Tab

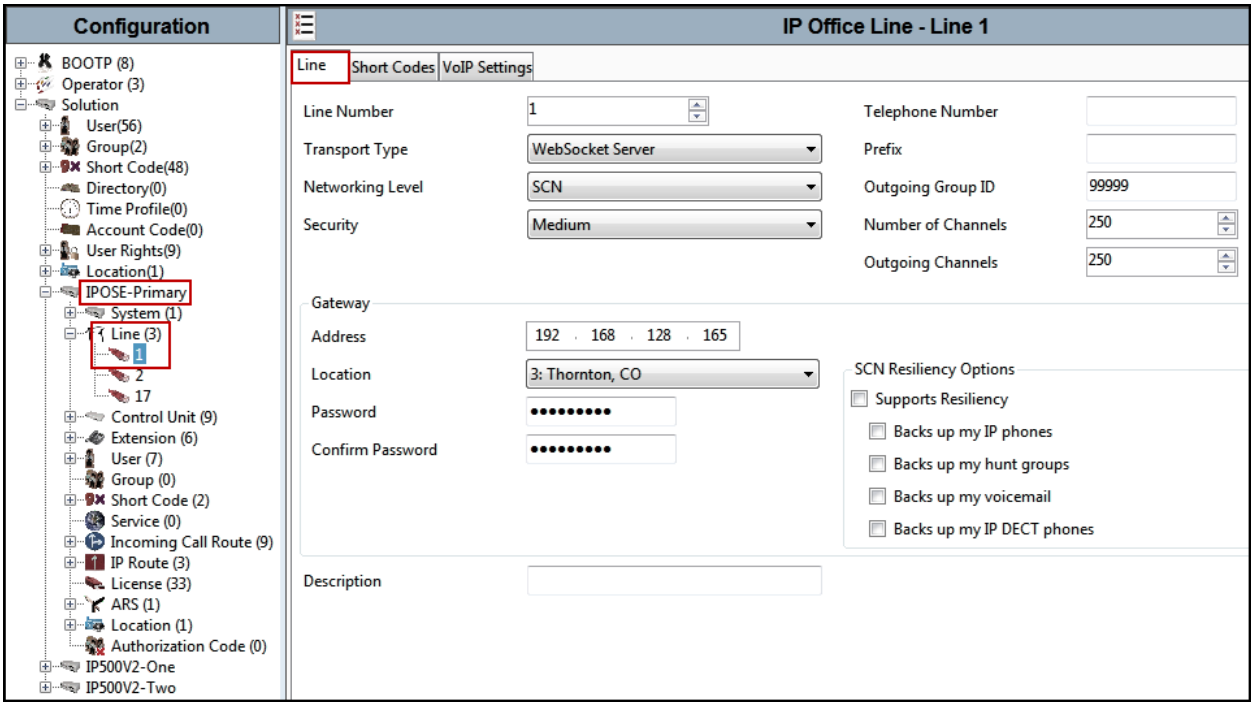
Select the **SIP Advanced** tab. Set or verify the parameters as shown below:

- Under **Call Routing Method** verify **Request URI** is selected (default value).
- Check the box for **Emulate NOTIFY for REFER** (refer to **Section 2.2**).
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



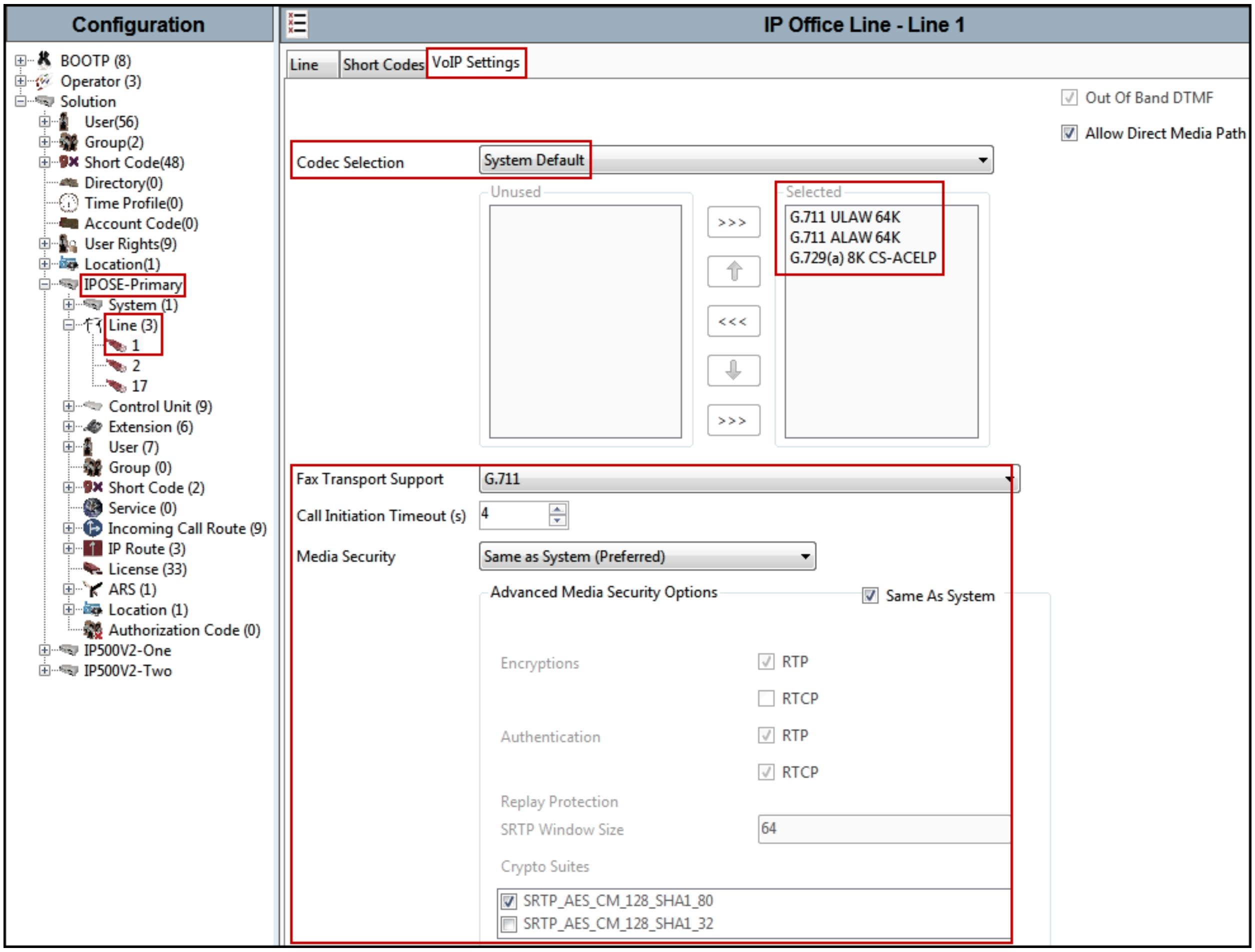
5.5. IP Office Line – Primary Server

In IP Office Server Edition systems, IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate line to be configured in the Group pane. The screen below shows the IP Office Line to the IP500V2-One Expansion System.



The screen below shows the IP Office Line, **VoIP Settings** tab:

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **G.711** for **Fax Transport Support**.
- Under **Media Security** verify **Same as System (Preferred)** is selected (default value).

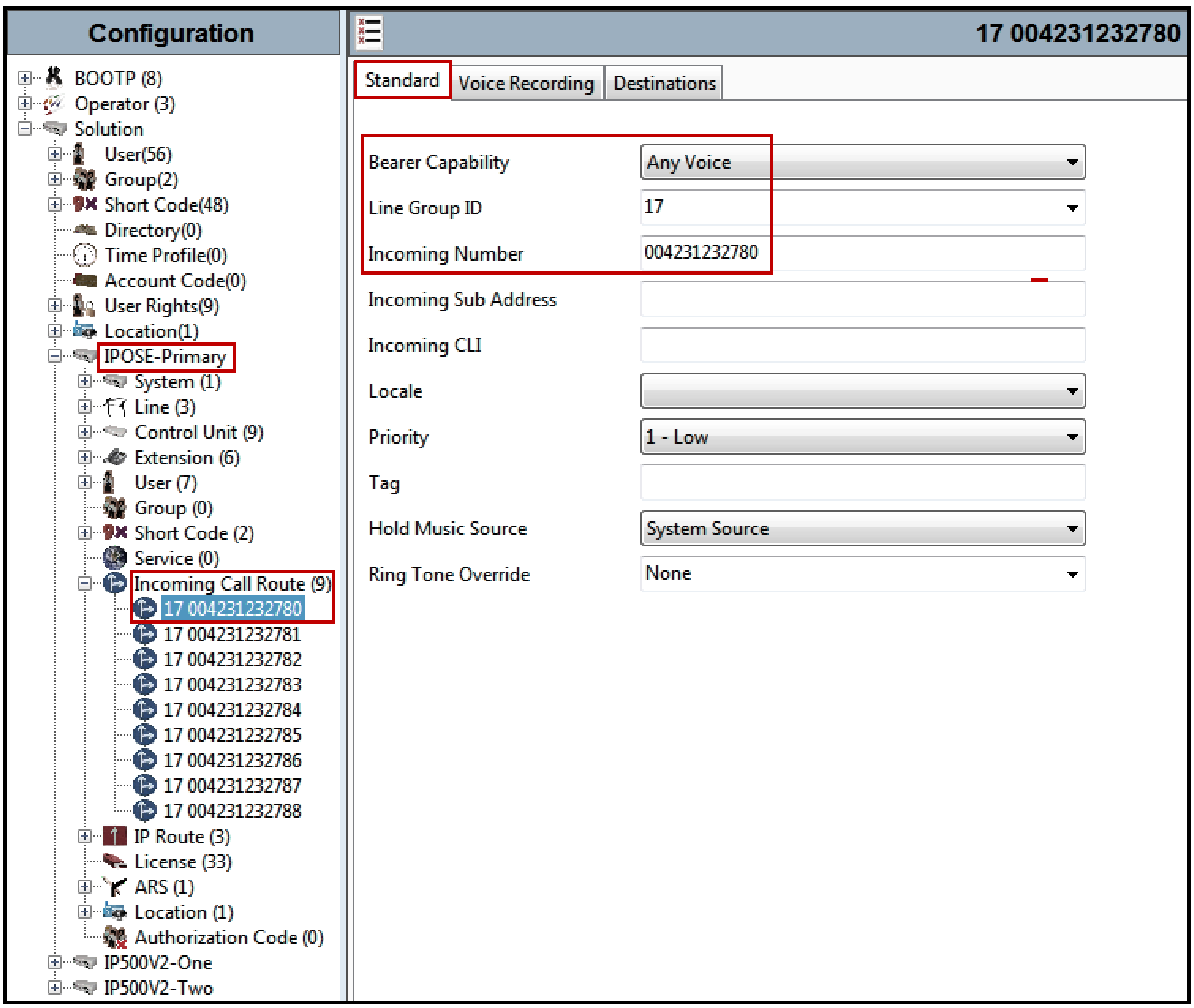


Repeat this process as needed to add additional Secondary server or Expansion Systems to the solution.

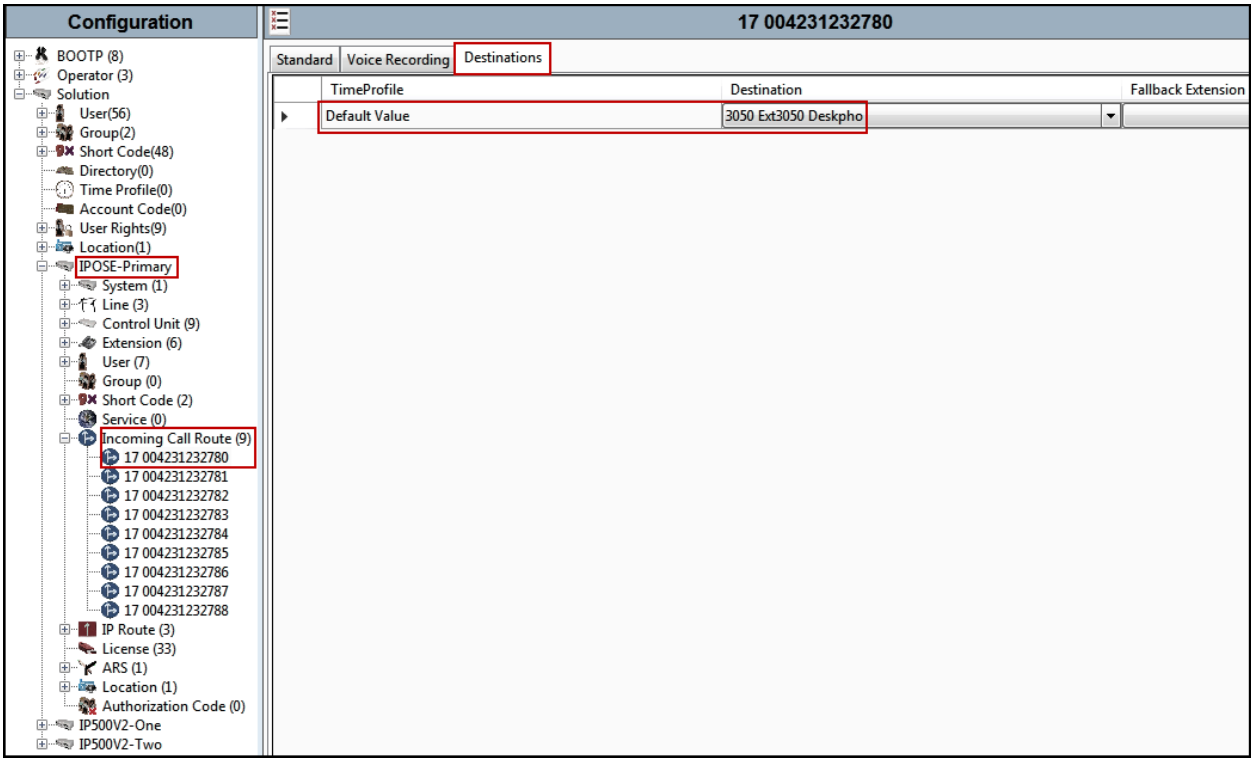
5.6. Incoming Call Route

Incoming call routes map inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system. To add an incoming call route, right click on **Incoming Call Route** in the **Navigation** pane and select **New** (not shown). On the Details Pane, under the **Standard** tab, set the parameters as show below:

- Set **Bearer Capacity** to **Any Voice**.
- The **Line Group ID** is set to **17**. This matches the **Incoming Group** field configured in the **Call Details** tab for the SIP Line on **Section 5.4.4**.
- On the **Incoming Number**, enter one of the DID numbers provided by Telecom Liechtenstein. When the destination is a user's extension, the **Incoming Number** can be used to construct the From and Contact headers to be used in place of the extension number in the outgoing SIP INVITE for that user.
- Default values may be used for all other parameters.



Select the **Destinations** tab. From the **Destination** drop-down menu, select the endpoint associated with this DID number. In the reference configuration, the DID number **004231232780** provided by Telecom Liechtenstein was associated with the Avaya IP Office extension **3050**.



Repeat this process as needed to assign incoming call routes to additional IP Office users, as well as for other Avaya IP Office destinations (Hunt Group, Voicemail, Short Codes, etc.).

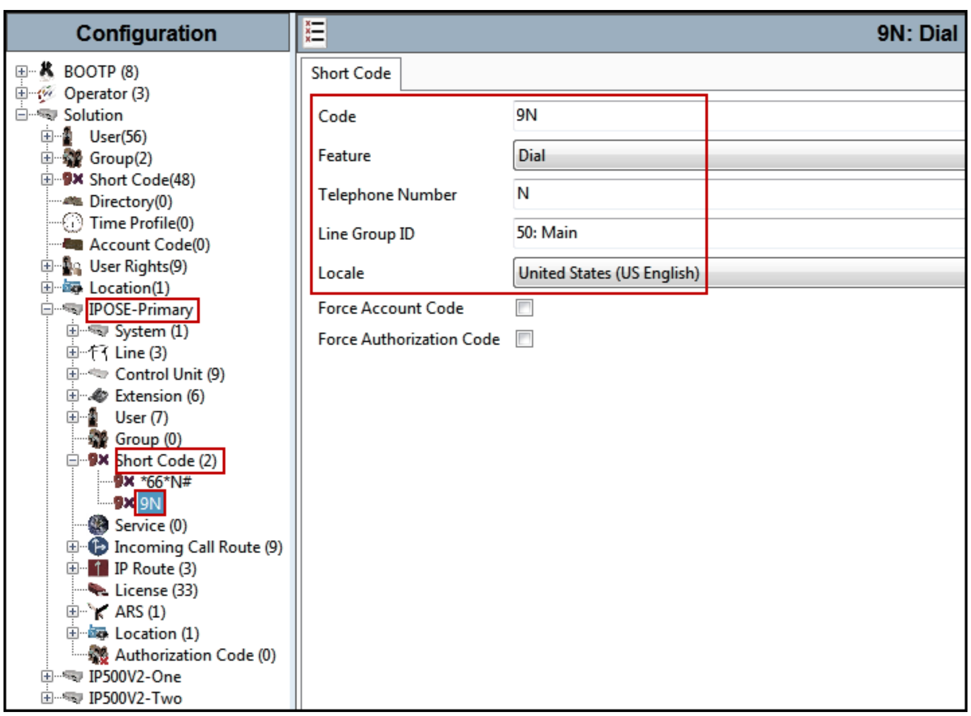
5.7. Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. While detailed coverage of ARS is beyond the scope of these Application Notes, and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance testing.

5.7.1. Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code**, the **Navigation** pane and select **New**. The screen below shows the short code **9N** created (note that the semi-colon is not used here). In this case, when the IP Office user dials 9 plus any number **N**, instead of being directed to a specific Line Group ID, the call is directed to **Line Group 50: Main**, which is configurable via ARS.

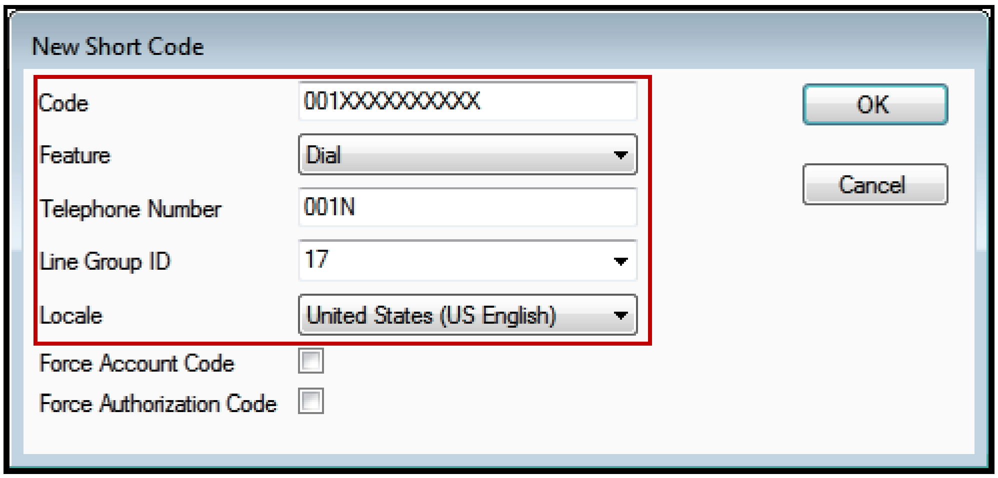
- In the **Code** field, enter the dial string which will trigger this short code. In this case, **9N** was used (note that the semi-colon is not used here).
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value is passed to ARS.
- Set the **Line Group ID** to **50: Main** to be directed to **Line Group 50: Main**, this is configurable via ARS.
- For **Locale**, **United States (US English)** was used.
- Click the **OK** to commit (not shown).



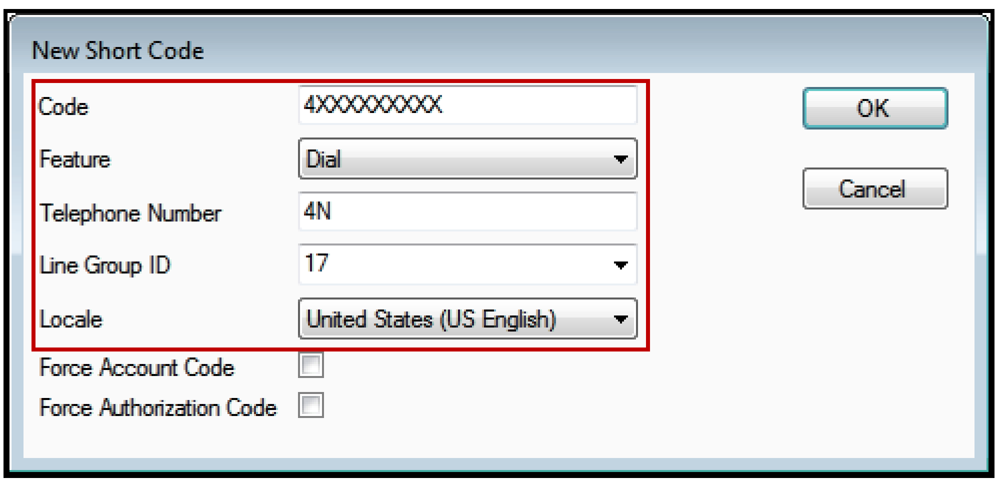
The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **X**'s used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string.

To create a short code to be used for ARS, select **ARS → 50: Main** on the Navigation Pane and click **Add** (not shown).

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **001** followed by **10 X**'s to represent the exact number of digits. This short code was used for international call to the U.S.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **001N**. The value **N** represents the additional number of digits dialed by the user after dialing **001** (The **9** will be stripped off).
- Set the **Line Group Id** to the Line Group number being used for the SIP Line, in this case Line **Group ID 17** was used.
- Set the **Locale** to the respective country (language).
- Click **OK** to commit.



The following example shows a short code created for local calls (e.g., 94231235512)



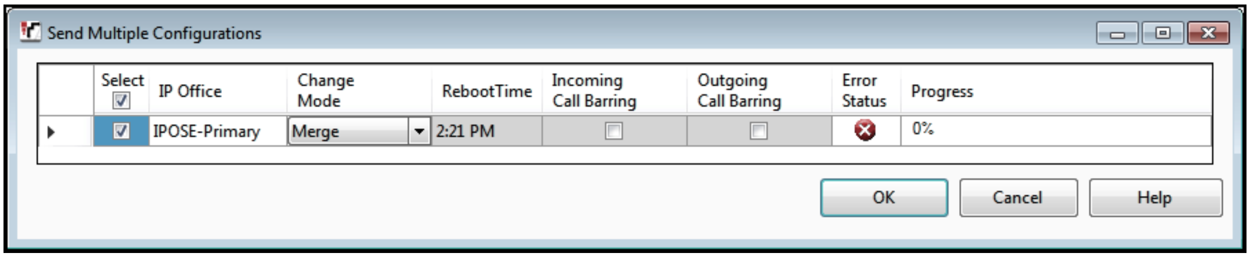
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

5.8. Save IP Office Primary Server Configuration

The provisioning changes made in Avaya IP Office Manager must be applied to the Avaya IP Office server in order for the changes to take effect. At the top of the Avaya IP Office Manager page, click **File → Save Configuration** (if that option is grayed out, no changes are pending).

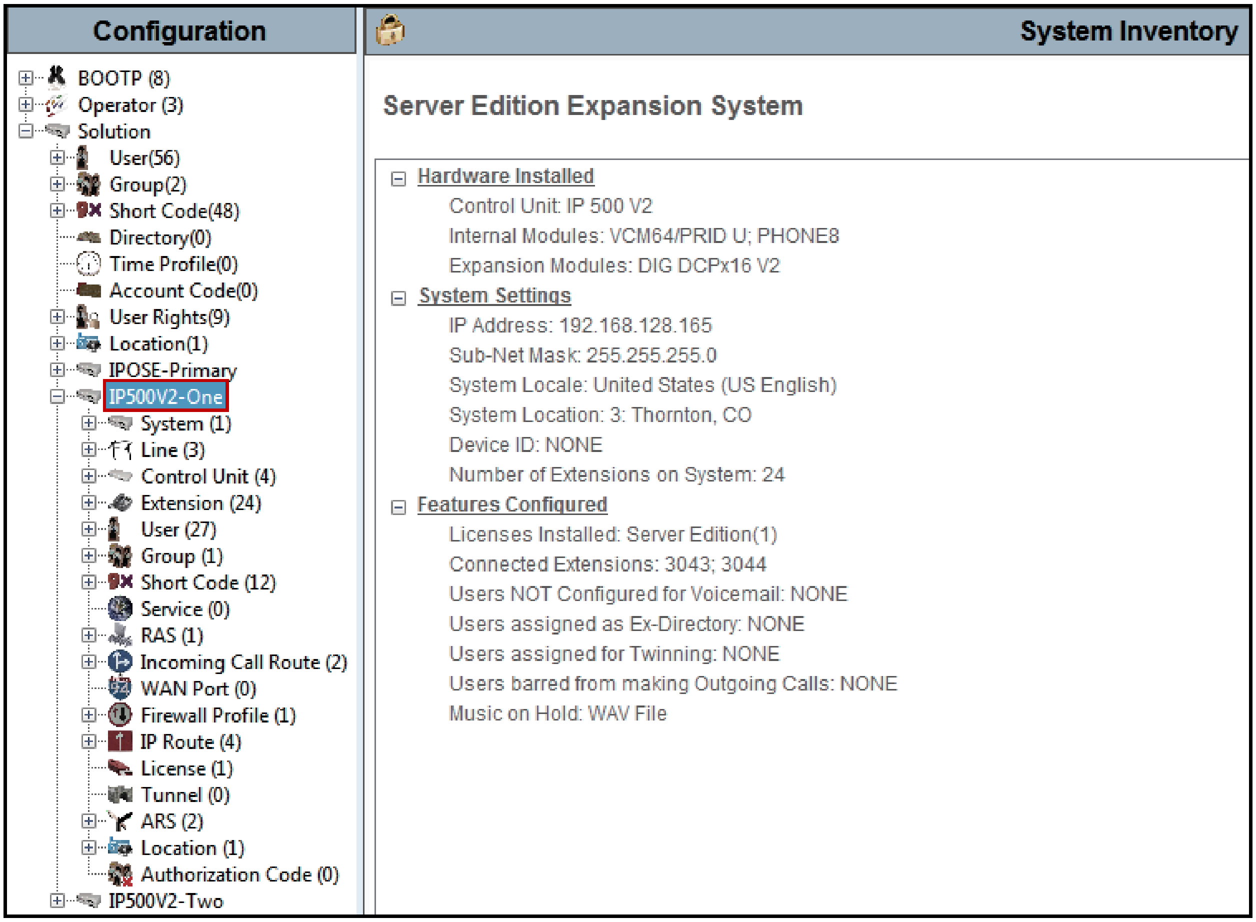
A screen similar to the one below will appear, with either **Merge** or **Immediate** automatically selected, based on the nature of the configuration changes. The **Merge** option will save the configuration change with no impact to the current system operation. The **Immediate** option will save the configuration and cause the Avaya IP Office server to reboot.

Click **OK** to execute the save.



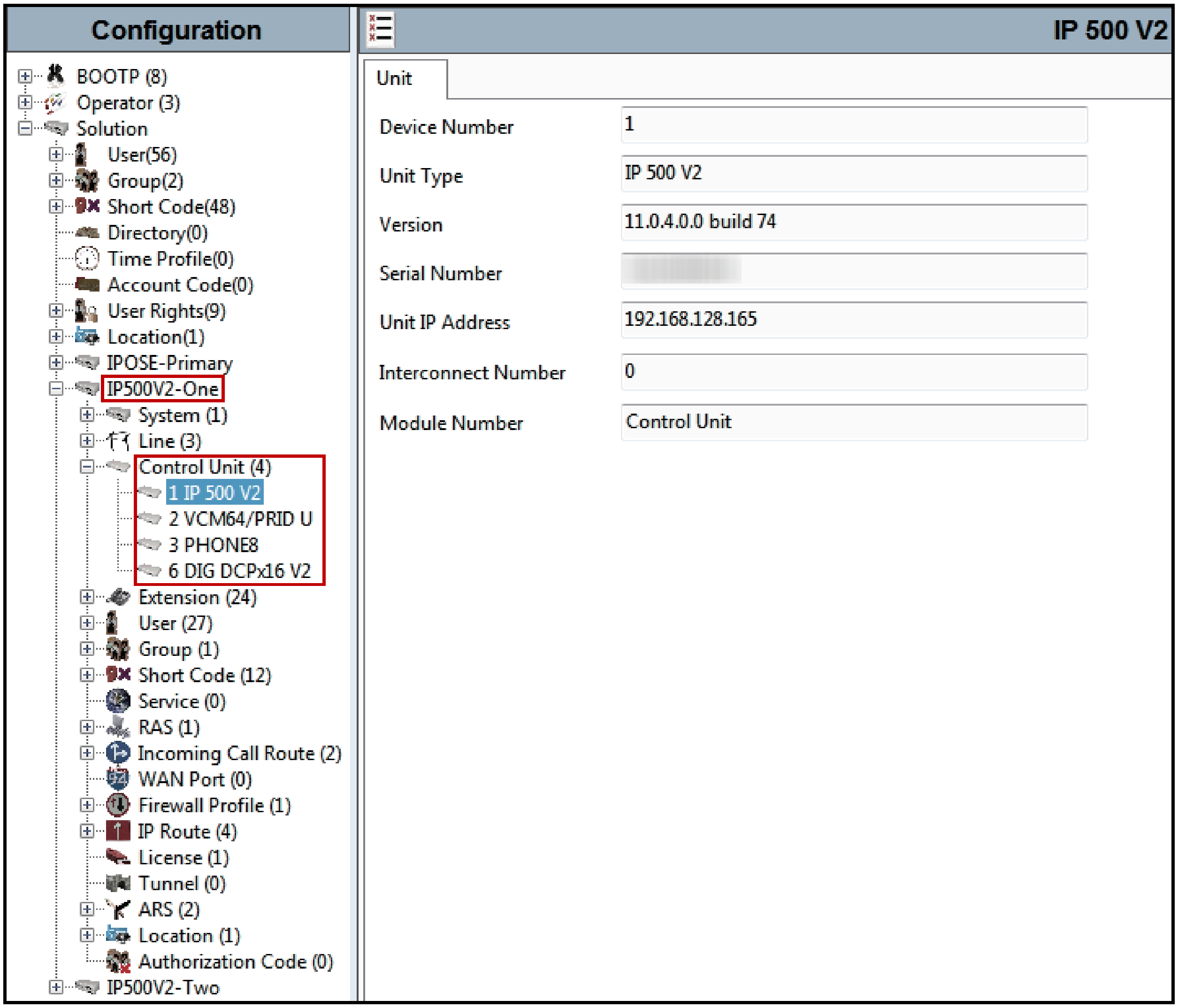
6. Avaya IP Office Expansion System Configuration

Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials. Clicking the "plus" sign next to **IP500V2-One** on the left navigation pane will expand the menu on this server.



6.1. Physical Hardware

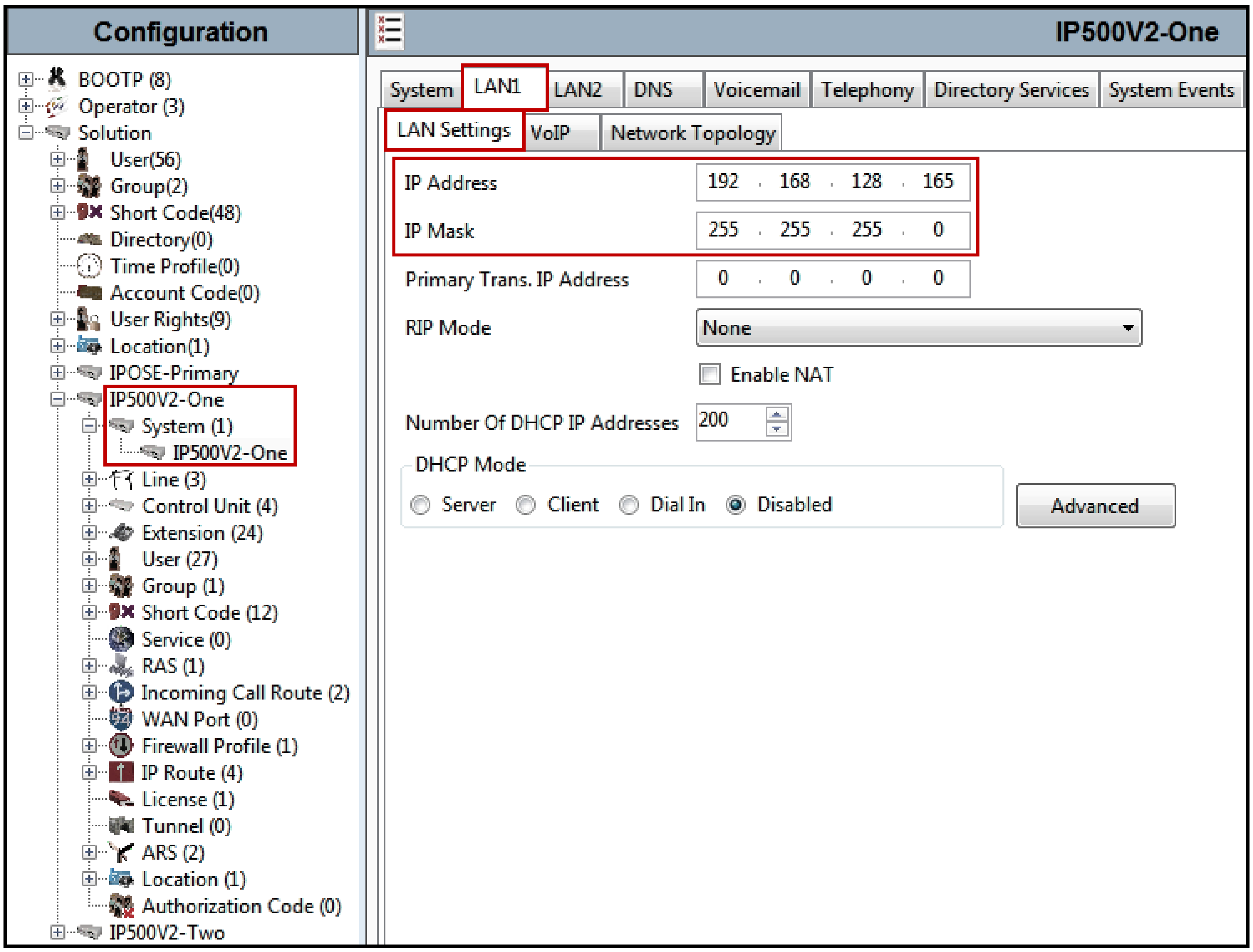
In the sample configuration, the IP500 V2 Expansion System contained a PHONE8 analog card, for the support of analog extensions, a DIG DCPx16 V2, for support of digital extensions. Also included is a VCM64 (Voice Compression Module). The VCM64 cards provide voice compression channels to the control unit. Voice compression channels are needed to support VoIP calls, including IP extensions and or IP trunks.



6.2. LAN Settings

In the sample configuration, LAN1 is used to connect the Expansion System to the enterprise network. To view or configure the LAN1 IP address, select **System** on the Navigation pane. Select the **LAN1 → LAN Settings** tab on the Details pane, and enter the following:

- **IP Address: 192.168.128.165** was used in the reference configuration.
- **IP Mask: 255.255.255.0** was used in the reference configuration
- Click the **OK** button (not shown).

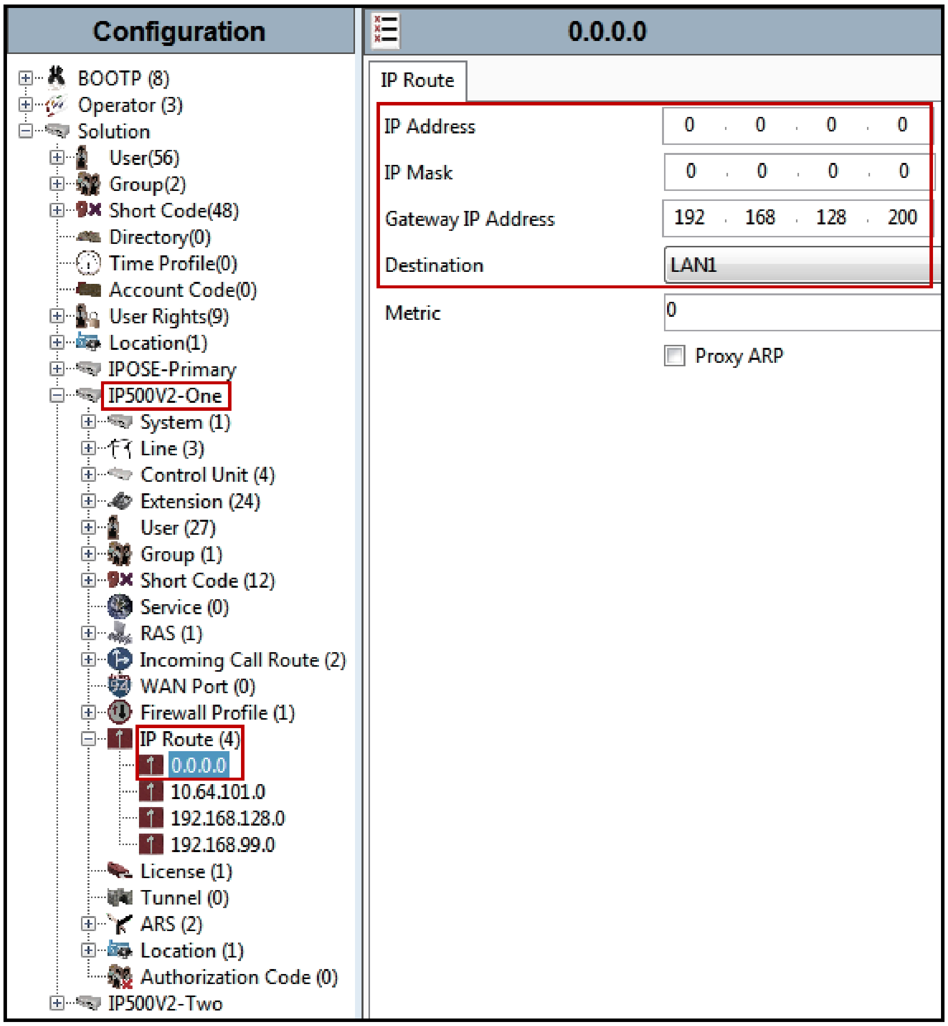


Default values were used on the **VoIP** and **Network Topology** tabs (not shown).

6.3. IP Route

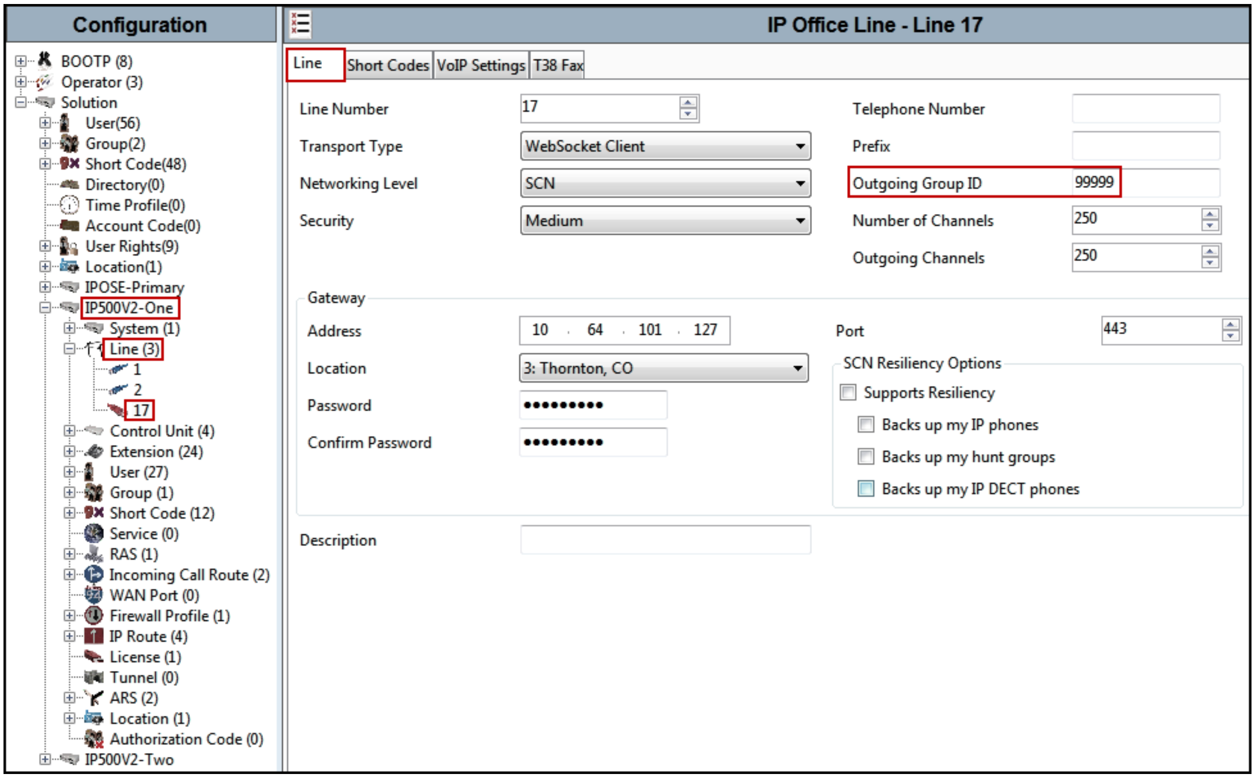
To create an IP route for the Expansion system, right-click on **IP Route** on the left Navigation pane. Select **New** (not shown).

- Enter **0.0.0.0** on the **IP Address** and **IP Mask** fields to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet. The default gateway in the reference configuration was **192.168.128.200**
- Set **Destination** to **LAN1** from the pull-down menu.



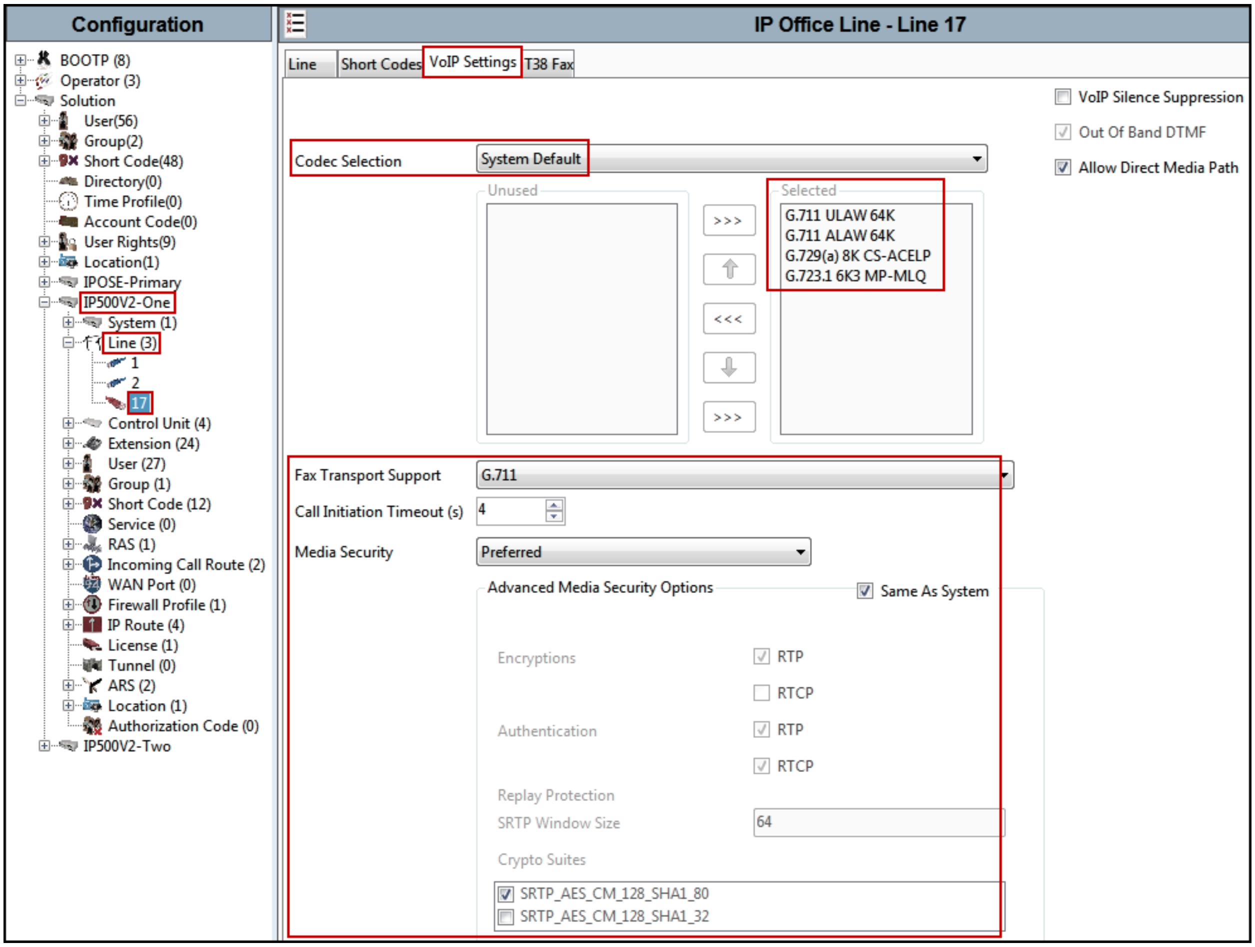
6.4. IP Office Line – IP500 V2 Expansion System

In IP Office Server Edition systems, IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate line to be configured in the Group pane. The screen below shows the IP Office Line to the Primary server.



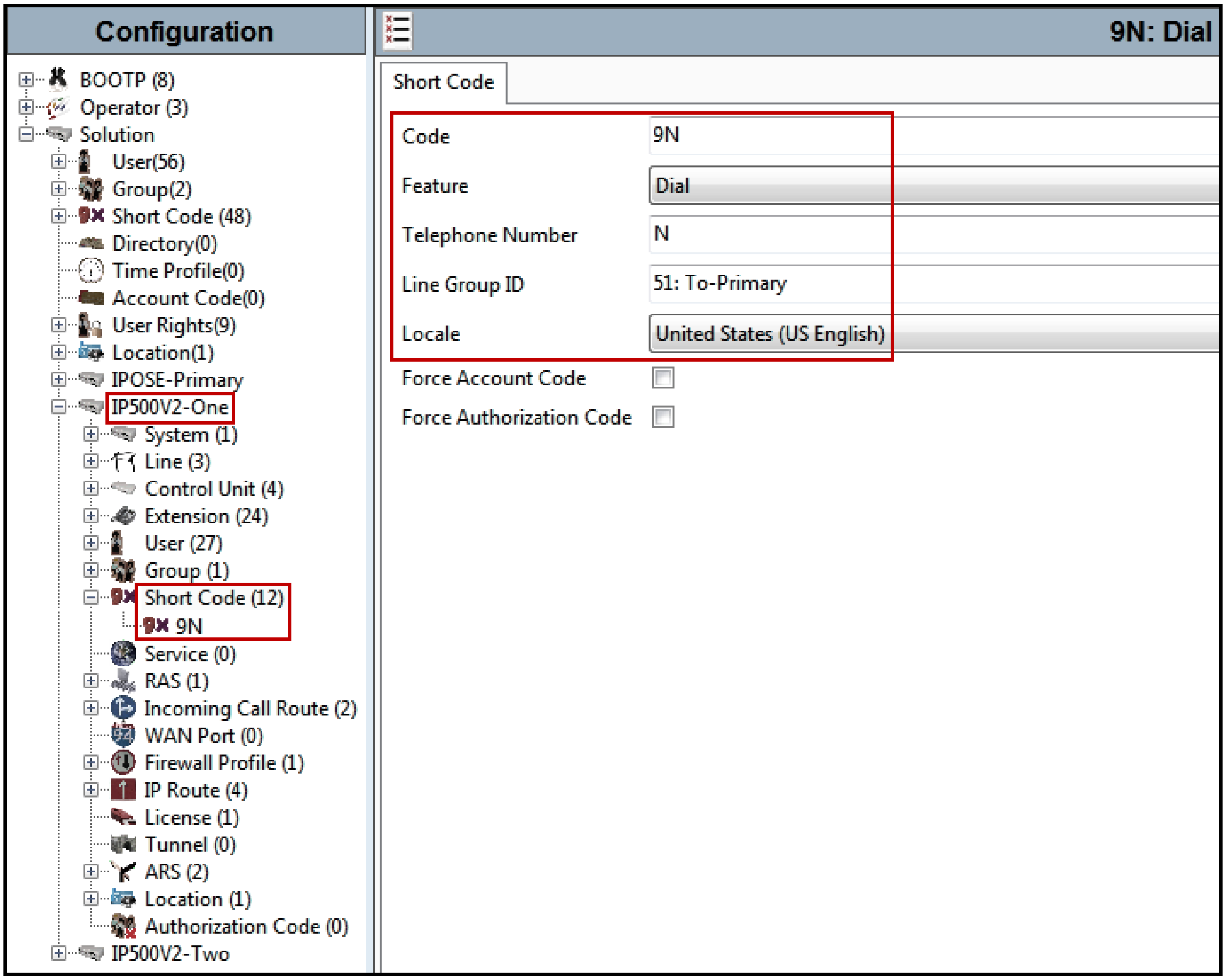
The screen below shows the IP Office Line, **VoIP Settings** tab:

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **G.711** for **Fax Transport Support**.
- Under **Media Security Preferred** was selected.



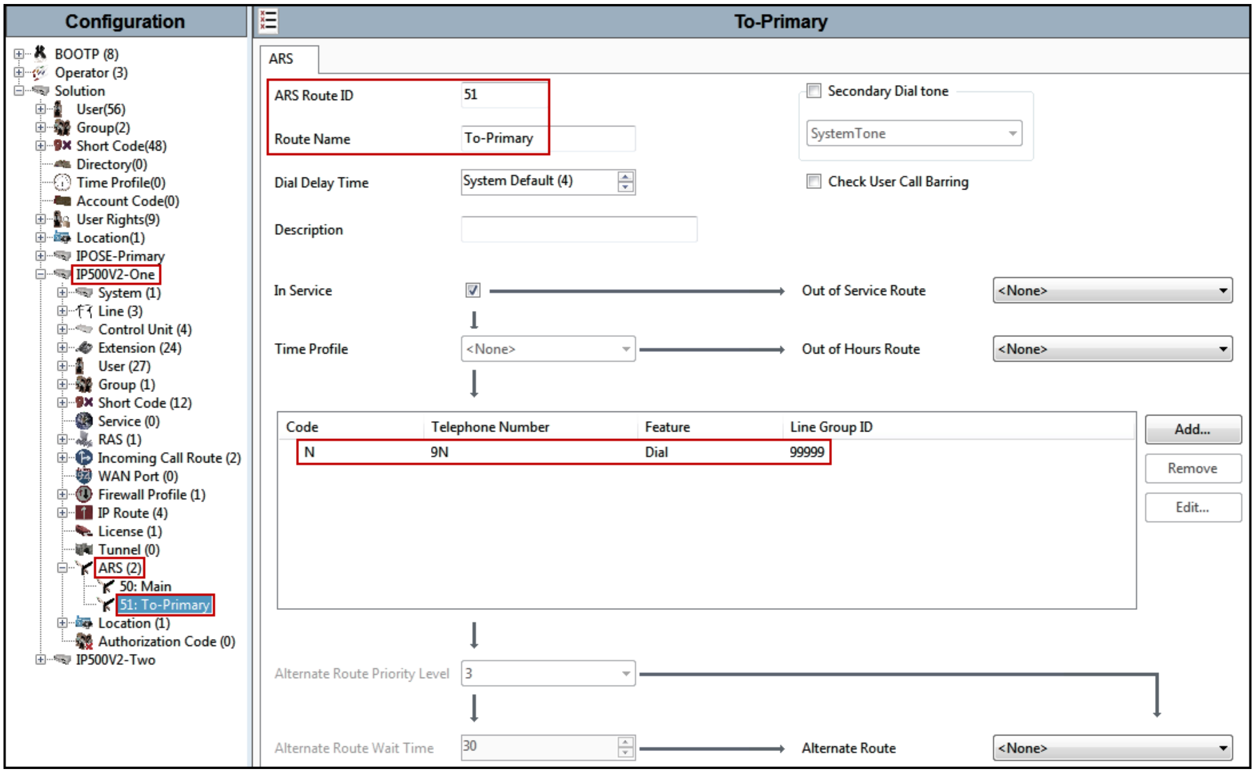
6.5. Short Codes

Similar to the configuration of the Primary server in **Section 5.7**, create a Short Code to access ARS. In the reference configuration, the **Line Group ID** is set to the ARS route illustrated in the next section.



6.6. Automatic Route Selection – ARS

The following screen shows an example ARS configuration for the route named "**To-Primary**" on the Expansion System. The **Telephone Number** is set to **9N**. The **Line Group ID** is set to "**99999**" matching the number of the **Outgoing Group ID** configured on the IP Office Line 17 to the Primary server (**Section 6.4**).

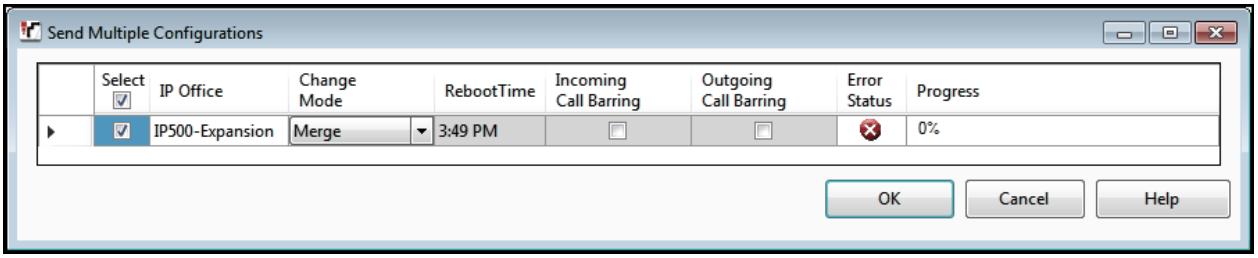


Repeat this process as needed to add additional Secondary server or Expansion Systems to the solution.

6.7. Save IP Office Expansion System 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

The following will appear, with either **Merge** or **Immediate** selected, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to proceed.



7. Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of the Avaya SBCE to connect to Telecom Liechtenstein SIP Trunking Service.

It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

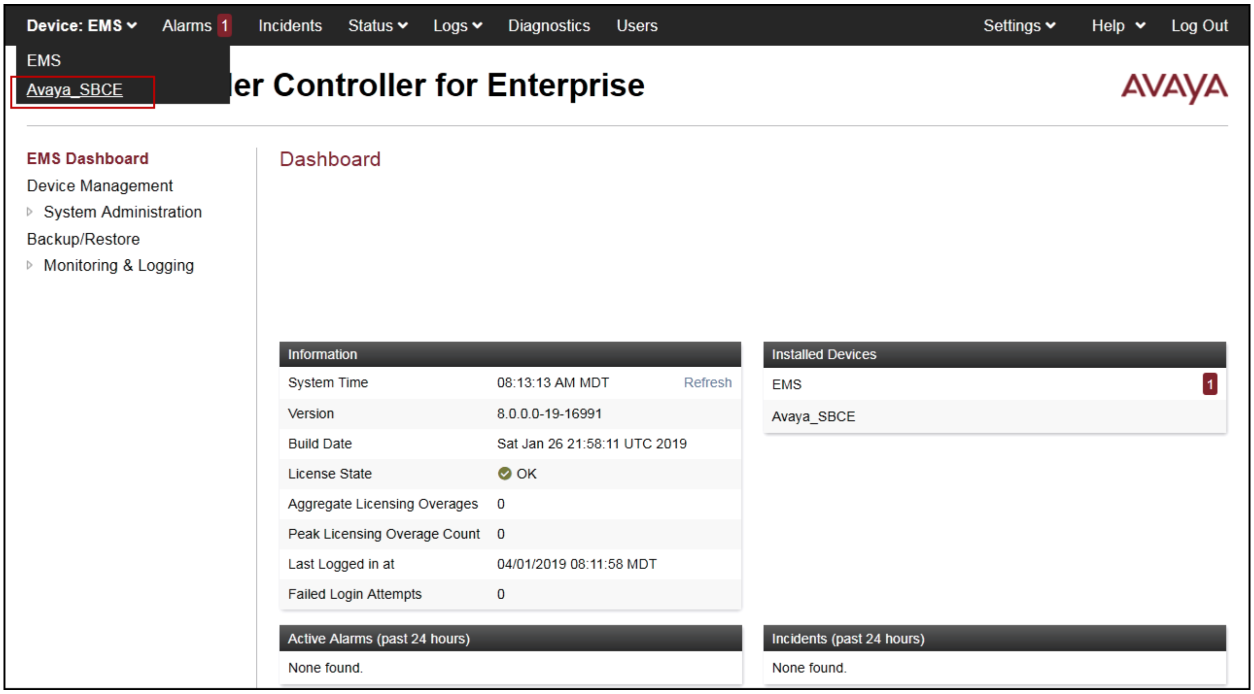
Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

7.1. Log in Avaya SBCE

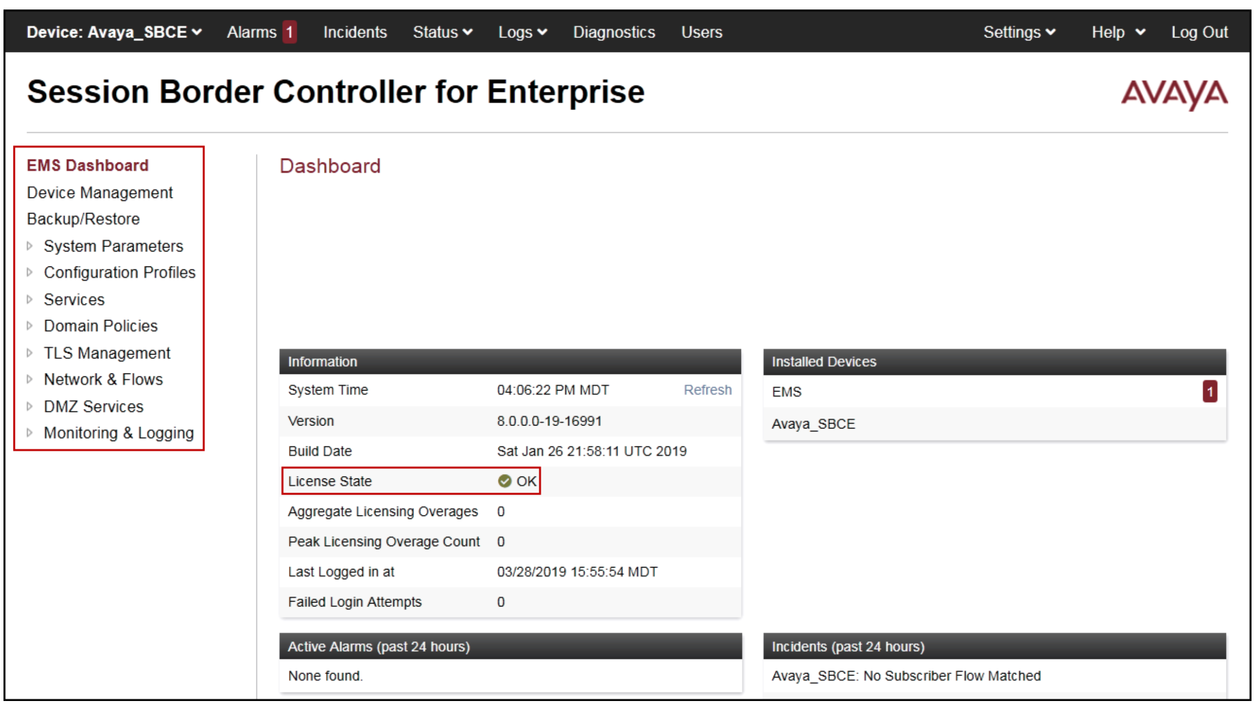
Use a Web browser to access the Avaya SBCE Web interface. Enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the Avaya SBCE management IP address.

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

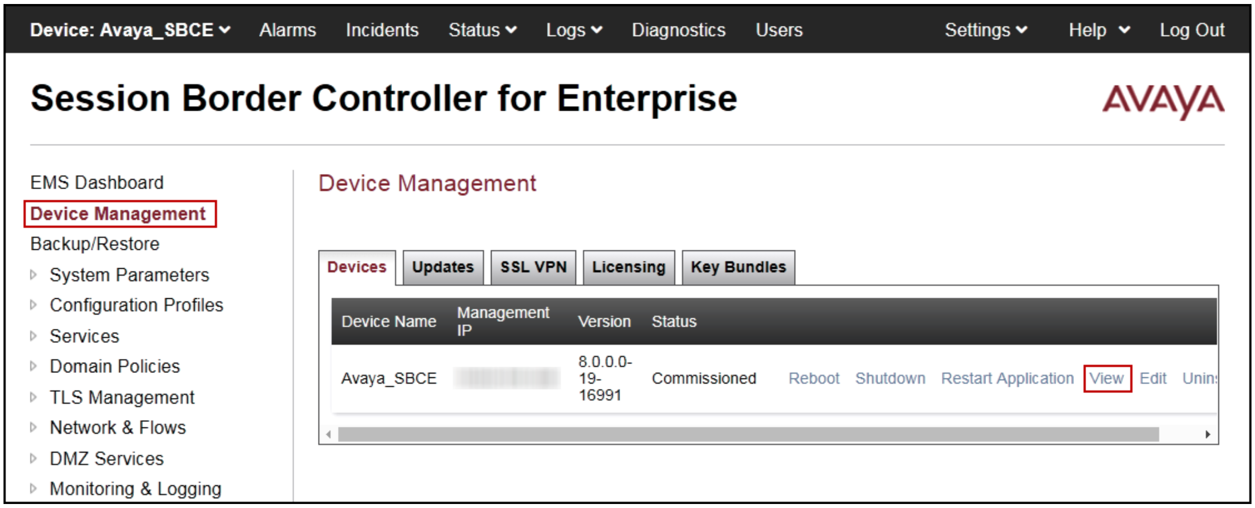
Once logged in, on the top left of the screen, under **Device:** select the device being managed, ***Avaya_SBCE*** in the sample configuration.



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

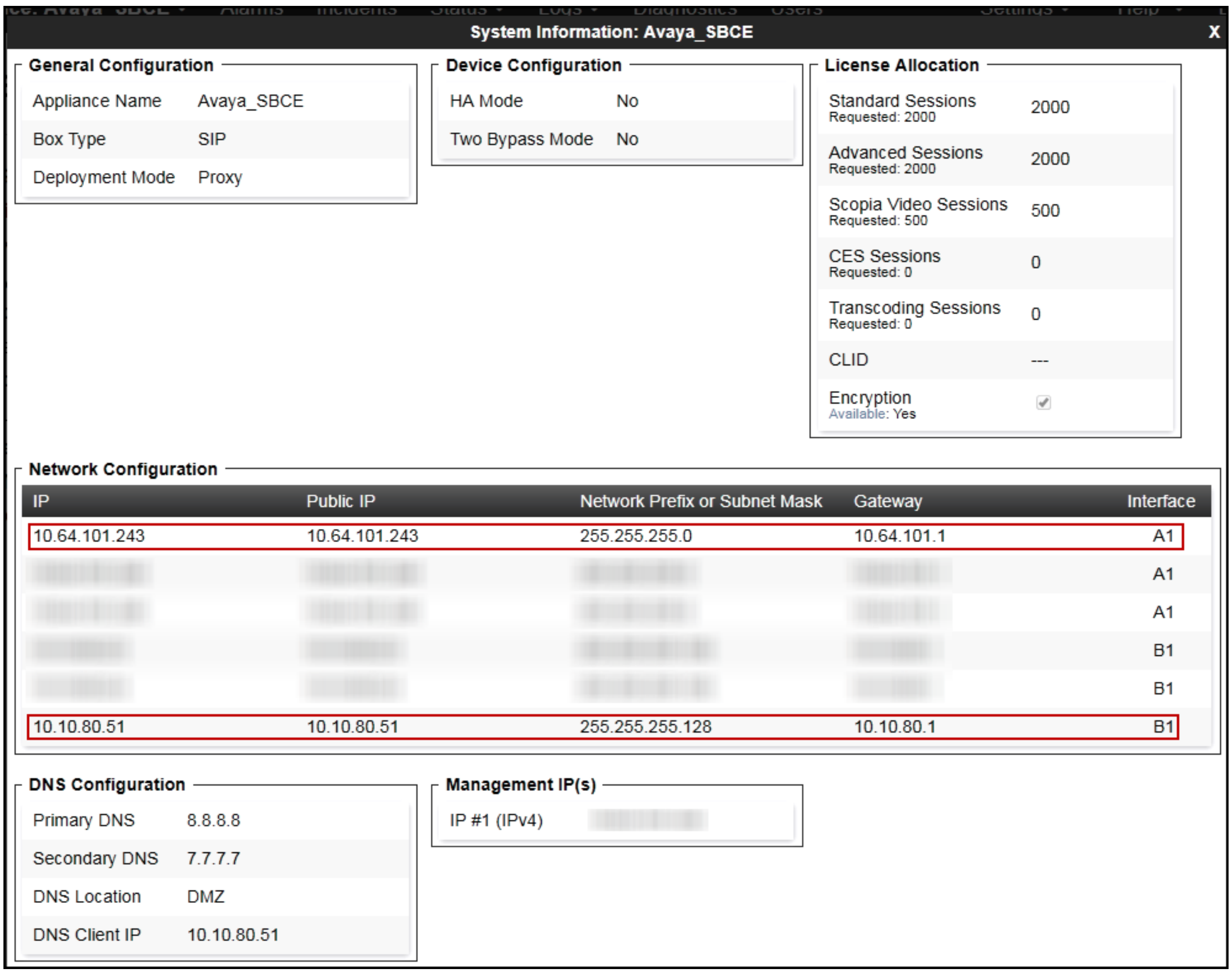


To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named ***Avaya_SBCE*** is shown. The management IP address that was configured during installation is blurred out for security reasons, the current software version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



The **System Information** window is displayed as shown below.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.



On the previous screen, **A1** corresponds to the inside interface (Private Network side) and **B1** corresponds to the outside interface (Public Network side) of the Avaya SBCE. (Refer to **Figure 1**).

The management IP was blurred out for security reasons. The IP addresses used for the remote worker configuration were also blurred out since the remote worker configuration is beyond the scope of these Application Notes and is not discussed in these Application Notes.

IMPORTANT! – During the Avaya SBCE installation, the Management interface (labeled "M1") of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to have this resolved.

7.2. 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. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

For the compliance testing, the transport protocol that was used between IP Office and the Avaya SBCE, across the enterprise private IP network (LAN), was SIP over TLS. SIP over UDP was used between the Avaya SBCE and Telecom Liechtenstein, across the public Internet.

It is assumed that generation and installation of certificates and the creation of TLS Profiles on the Avaya SBCE have been previously completed, as it's not discussed in this document. Refer to item [**7**] in **Section 11**.

7.3. Configuration Profiles

The Configuration Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

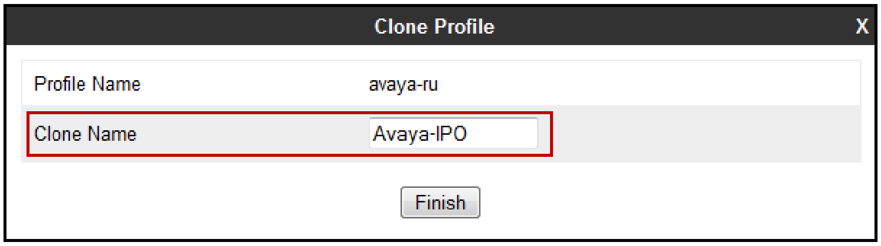
7.3.1. Server Interworking – Avaya-IPO

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or "cloned". Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or "cloned". If needed, the profile can then be modified to meet specific requirements for the enterprise SIP-enabled solution. For Telecom Liechtenstein, this profile was left with the **avaya-ru** default values.

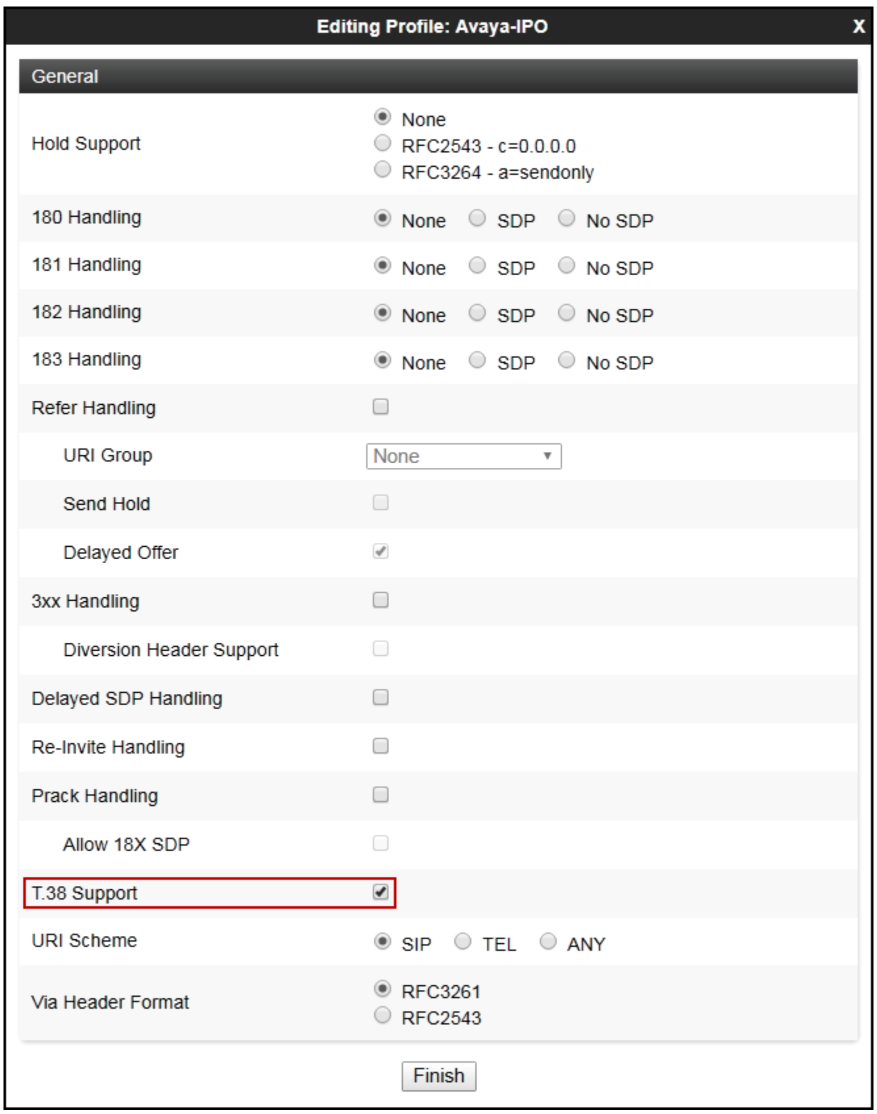
On the left navigation pane, select **Configuration Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone** on top right of the screen (not shown).

Enter the new profile name in the **Clone Name** field, the name of ***Avaya-IPO*** was chosen in this example. Click **Finish**.

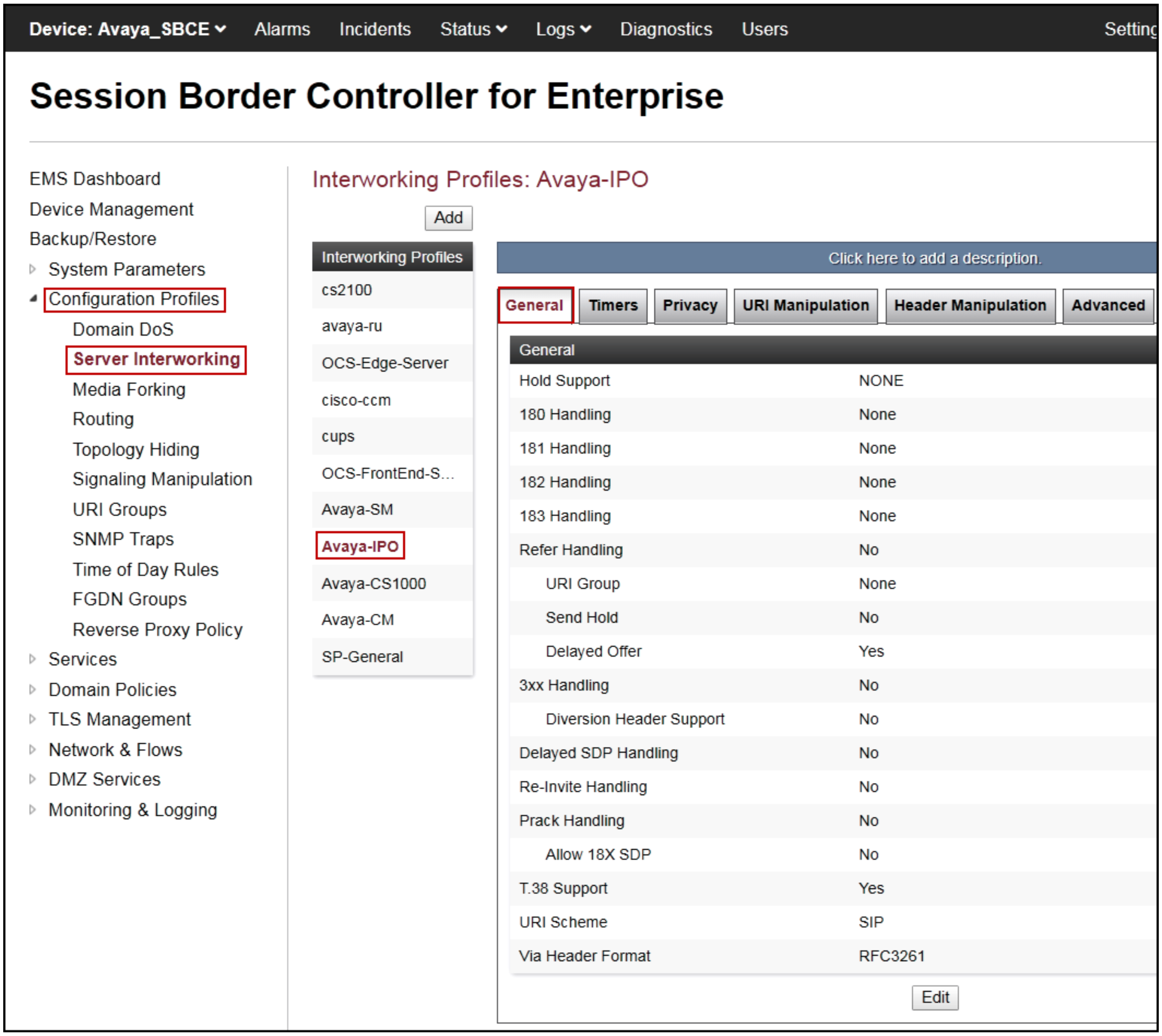


Click **Edit** on the newly cloned ***Avaya-IPO*** interworking profile:

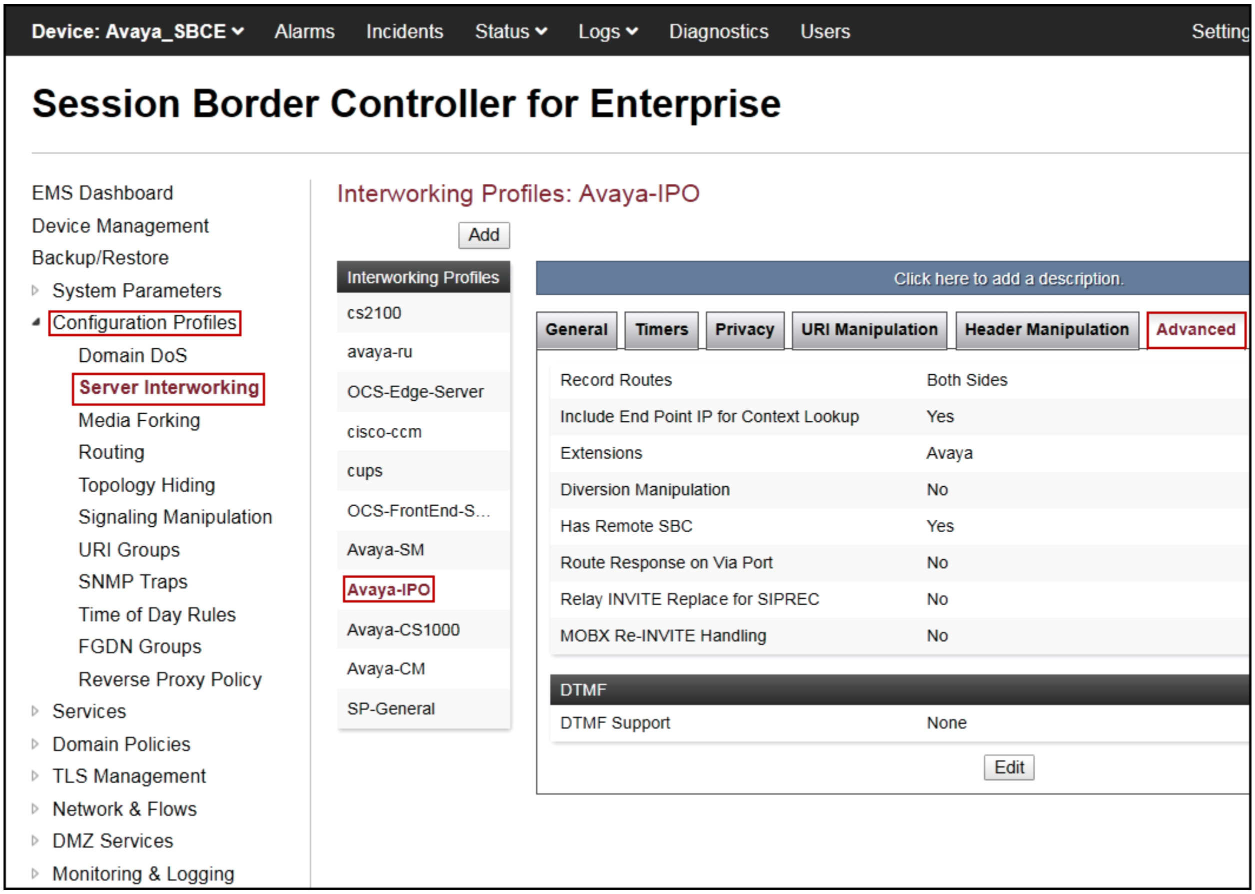
- On the **General** tab, check ***T.38 Support***.
- Leave remaining fields with default values.
- Click **Finish**.



The following screen capture shows the **General** tab of the newly created **Avaya-IPO** Server Interworking Profile.


Device: Avaya_SBCE
Alarms
Incidents
Status
Logs
Diagnostics
Users
Setting
Session Border Controller for Enterprise
EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups
Reverse Proxy Policy
Services
Domain Policies
TLS Management
Network & Flows
DMZ Services
Monitoring & Logging
Interworking Profiles: Avaya-IPO
Add
Interworking Profiles
cs2100
avaya-ru
OCS-Edge-Server
cisco-ccm
cups
OCS-FrontEnd-S...
Avaya-SM
Avaya-IPO
Avaya-CS1000
Avaya-CM
SP-General
Click here to add a description.
General
Timers
Privacy
URI Manipulation
Header Manipulation
Advanced
General
Hold Support NONE
180 Handling None
181 Handling None
182 Handling None
183 Handling None
Refer Handling No
URI Group None
Send Hold No
Delayed Offer Yes
3xx Handling No
Diversion Header Support No
Delayed SDP Handling No
Re-Invite Handling No
Prack Handling No
Allow 18X SDP No
T.38 Support Yes
URI Scheme SIP
Via Header Format RFC3261
Edit

The following screen capture shows the **Advanced** tab of the newly created **Avaya-IPO** Server Interworking Profile.



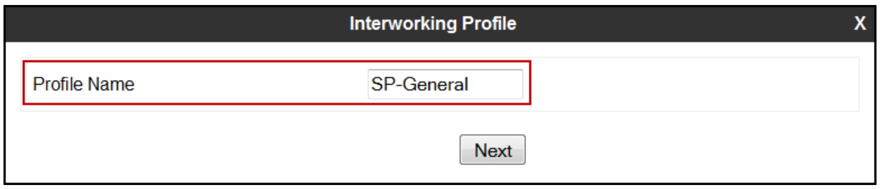
7.3.2. Server Interworking - SP-General

A second Server Interworking profile named **SP-General** was created for the Service Provider.

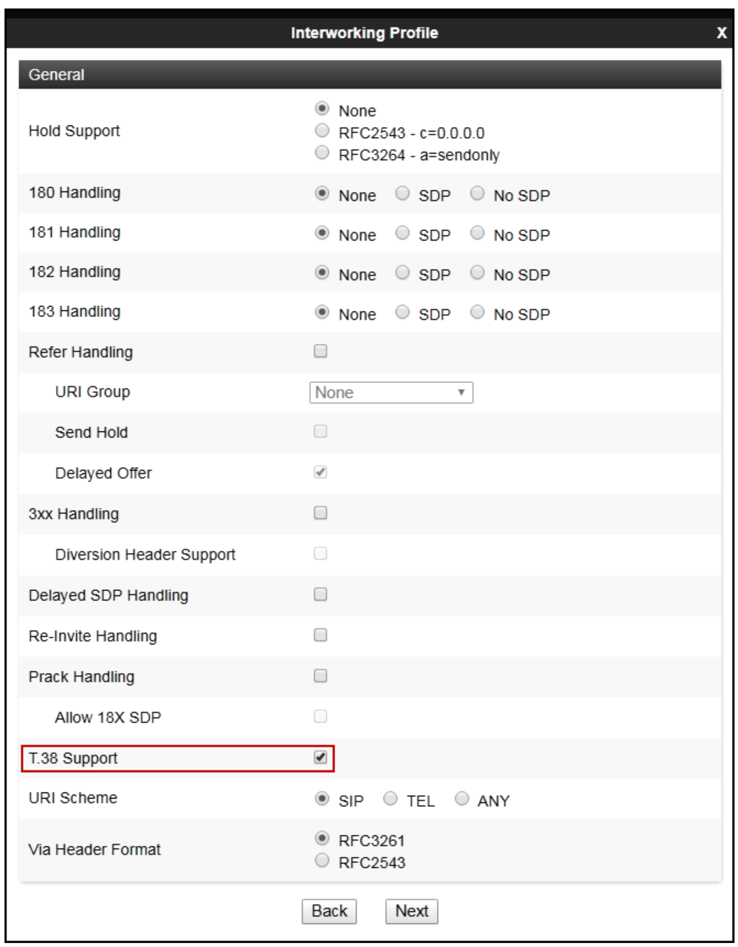
On the left navigation pane, select **Configuration Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **Add** (not shown) (note that **Add** is being used to create the SP-General profile instead of cloning the avaya-ru profile).

Enter the new profile name, the name of ***SP-General*** was chosen in this example.

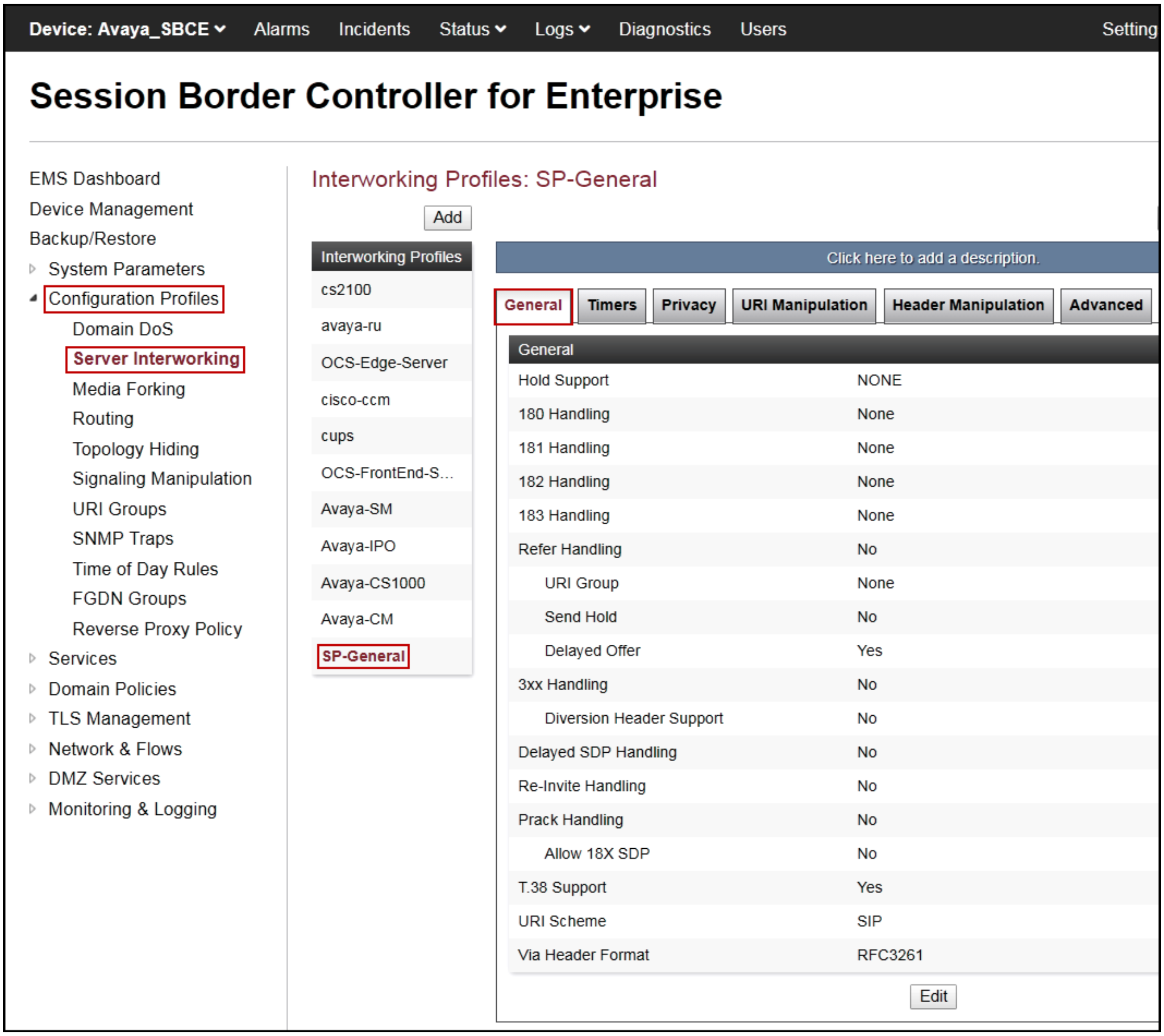
- Click **Next**.



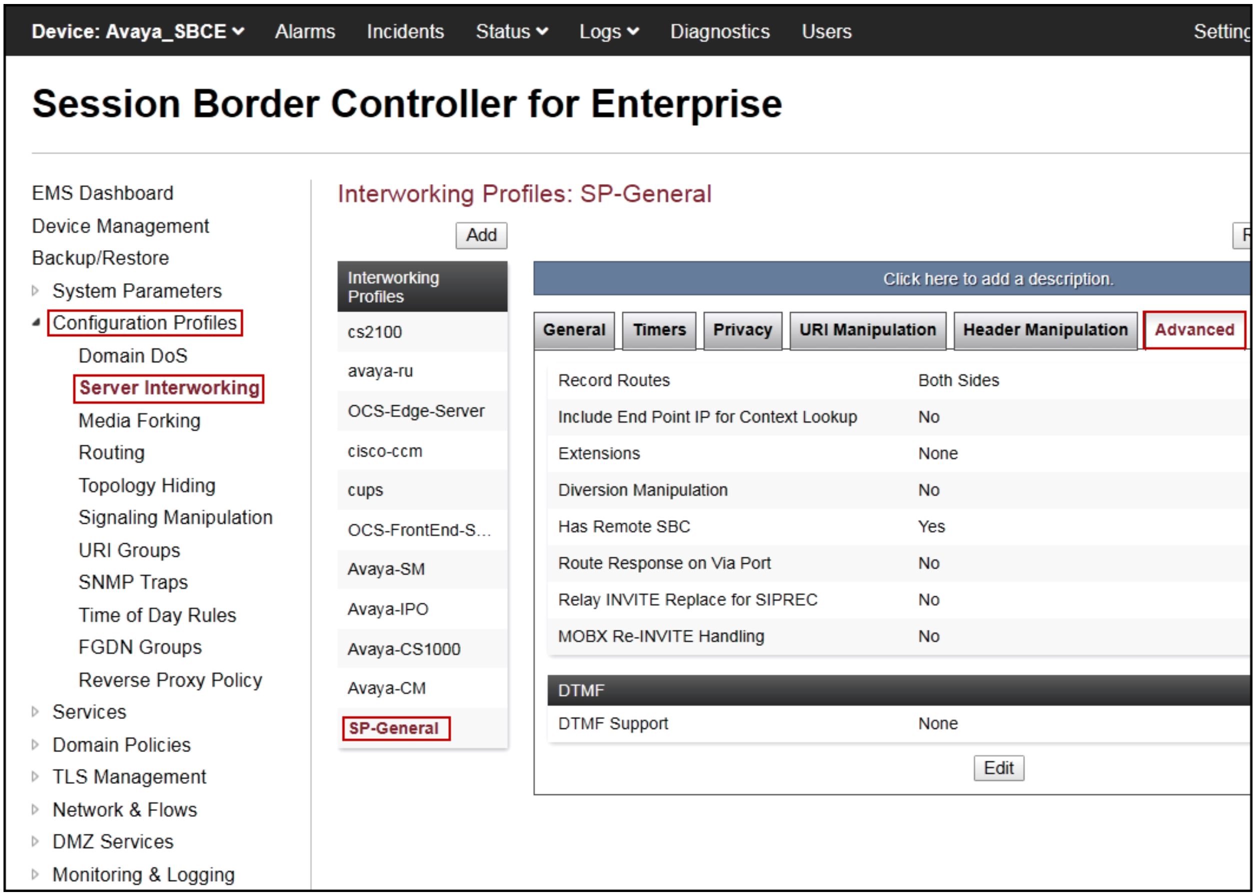
On the **General** tab, check ***T.38 Support***, click **Next** until the last tab is reached then click **Finish** on the last tab leaving remaining fields with default values (not shown).



The following screen capture shows the **General** tab of the newly created **SP-General** Server Interworking Profile.



The following screen capture shows the **Advanced** tab of the newly created **SP-General** Server Interworking Profile.



7.3.3. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform granular header manipulations on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult reference **[11]** in the **References** section for more information on this topic.

A Sigma scripts was created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

- Calls from IP Office to the PSTN with "privacy" enabled do not include the privacy header (privacy = id) in the INVITE message sent to Telecom Liechtenstein.

The scripts will later be applied to the SIP Server configuration profile corresponding to the service provider in **Section 7.3.4**.

To create the SigMa script to set the privacy header (privacy = id) in the INVITE message sent to Telecom Liechtenstein, on the left navigation pane, select **Configuration Profiles → Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name ***Add_Privacy_Header*** was chosen in this example.
- Copy the complete script from **Appendix A**.
- Click **Save**.

7.3.4. SIP Server Configuration

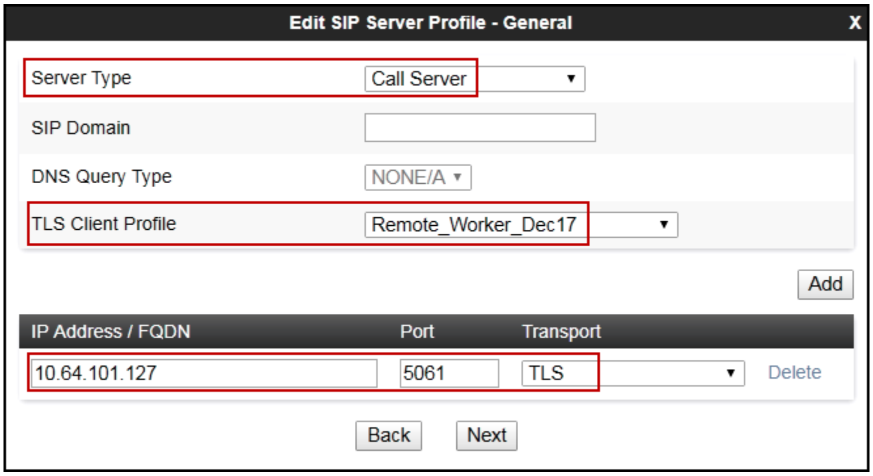
SIP Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (IP Office) and the Trunk Server or SIP Proxy at the service provider's network.

To add the SIP Server profile for the Call Server, from the **Services** menu on the left-hand navigation pane, select **SIP Servers** (not shown). Click **Add** (not shown) and enter the profile name: ***IP Office-Thornton***.

- Click **Next**.

On the Edit **SIP Server Profile – General** window:

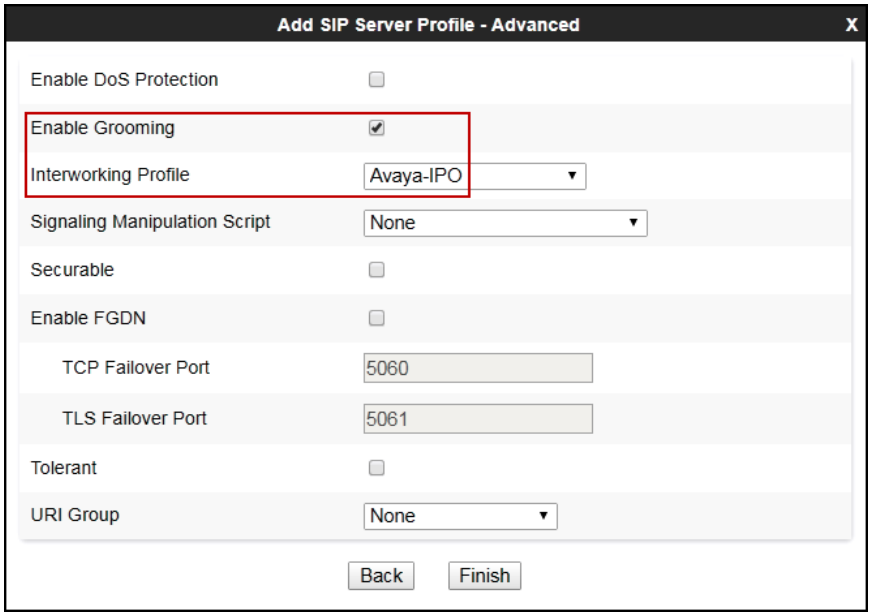
- **Server Type:** Select ***Call Server***.
- **IP Address / FQDN**: ***10.64.101.127*** (IP Address of IP Office).
- **Port:** ***5061*** (This port must match the port number defined in **Section 5.2.1**).
- **Transport**: Select ***TLS***.
- Select a **TLS Client Profile**.
- Click **Next**.



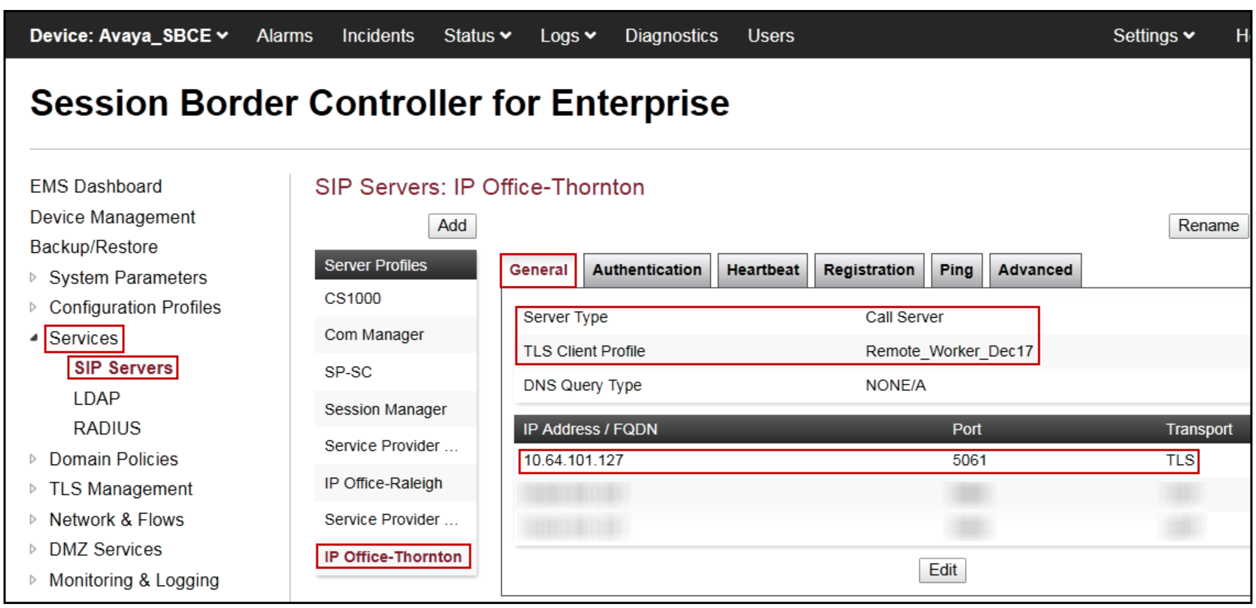
- Click **Next** on the **Add SIP Server Profile - Authentication** window (not shown).
- Click **Next** on the **Add Server Configuration Profile - Heartbeat** window (not shown).
- Click **Next** on the **Add SIP Server Profile - Registration** window (not shown).
- Click **Next** on the **Add SIP Server Profile - Ping** window (not shown).

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

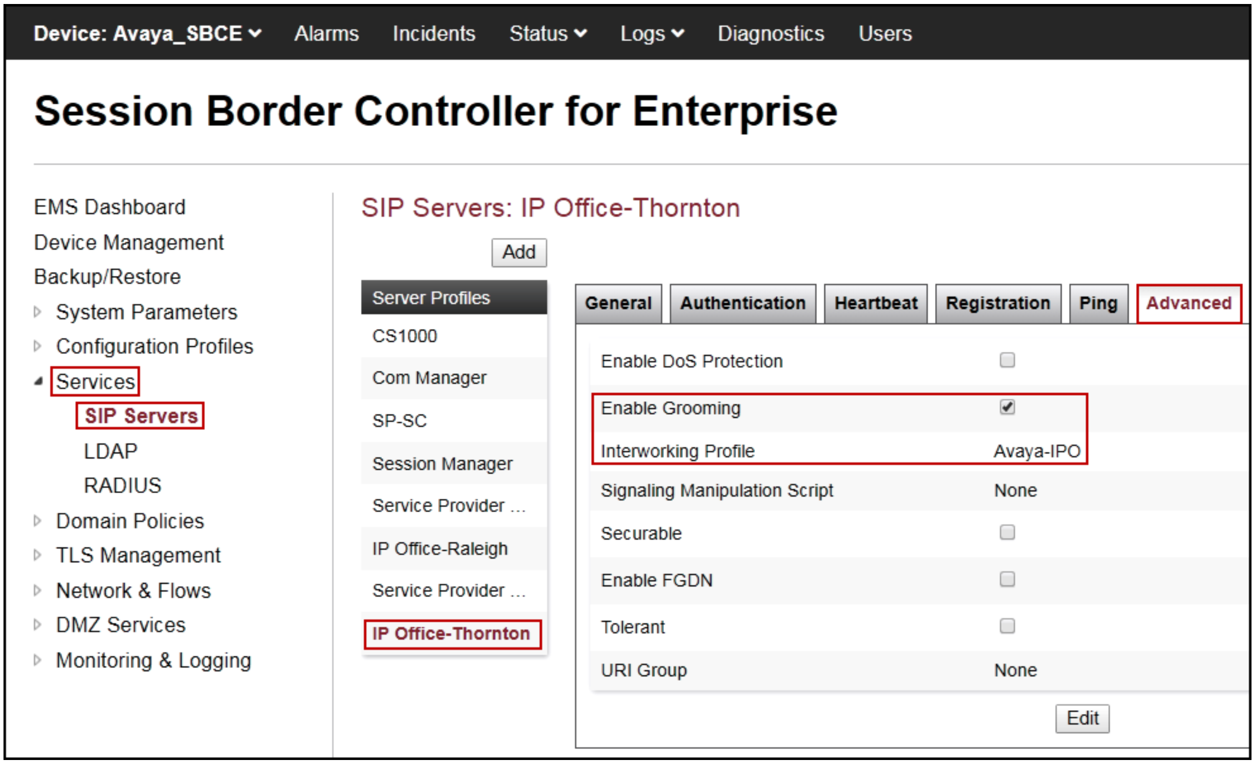
- Check ***Enable Grooming***.
- Select ***Avaya-IPO*** from the **Interworking Profile** drop down menu (**Section 7.3.1**).
- Leave the **Signaling Manipulation Script** at the default ***None***.
- Click **Finish**.



The following screen capture shows the **General** tab of the newly created **IP Office-Thornton** SIP Server Configuration Profile.

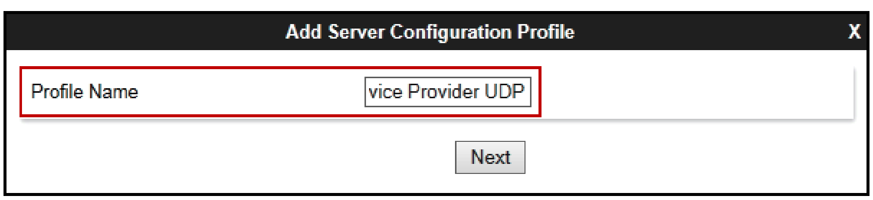


The following screen capture shows the **Advanced** tab of the newly created **IP Office-Thornton** SIP Server Configuration Profile.



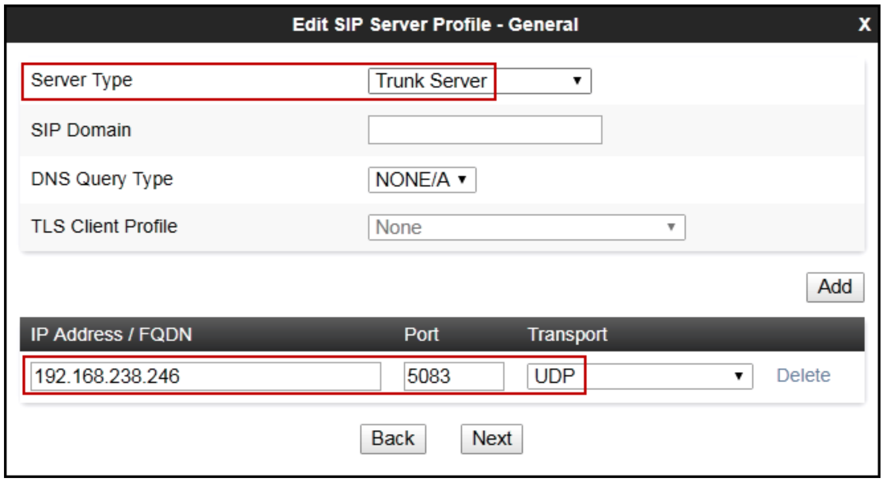
To add the SIP Server profile for the Trunk Server, from the **Services** menu on the left-hand navigation pane, select **SIP Servers** (not shown). Click **Add** (not shown) and enter the profile name: ***Service Provider UDP***.

- Click **Next**.



On the **Edit SIP Server Profile – General** window:

- **Server Type:** Select ***Trunk Server***.
- **IP Address / FQDN**: ***192.168.238.246*** (IP Address of the Service Provider SIP Proxy).
- **Port:** *5083*.
- **Transports**: Select ***UDP***.
- Click **Next**.



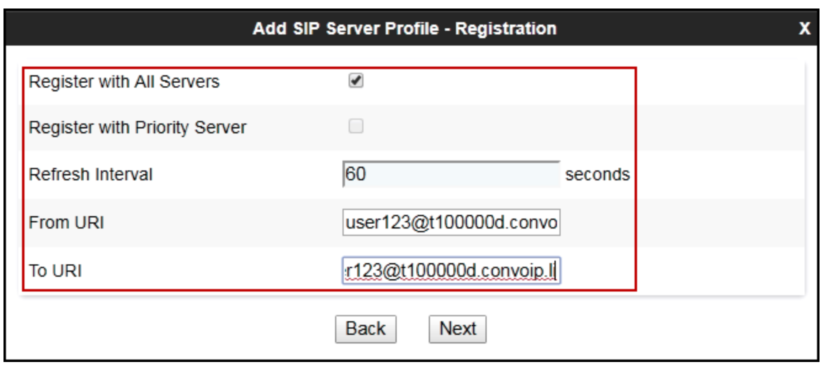
On the **Add SIP Server Profile – Authentication** window:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Leave **Realm** blank.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

Click **Next** on the **Add Server Configuration Profile - Heartbeat** window (not shown).

On the **Add SIP Server Profile – Registration** tab:

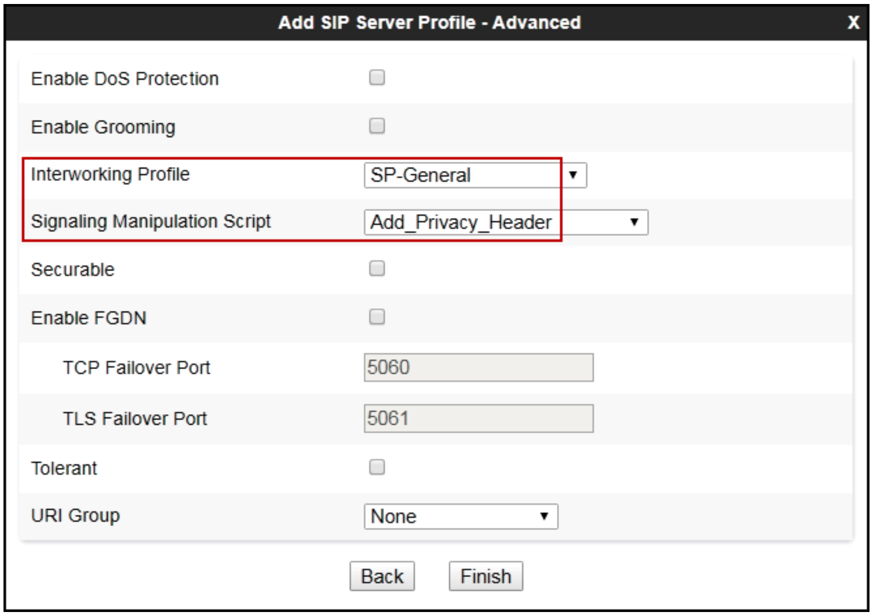
- Check the **Register with All Servers** box.
- On **Refresh Interval** enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with Telecom Liechtenstein, ***60*** seconds was the value used during the compliance test
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
  - **From URI**: Enter the **User Name**, same User Name provided above under the Authentication windows (***user123***) and the domain name (***t100000d.convoip.li***) provided by Telecom Liechtenstein, as shown on the screen below.
  - **To URI**: Enter the **User Name**, same User Name provided above under the Authentication windows (***user123***) and the domain name (***t100000d.convoip.li***) provided by Telecom Liechtenstein, as shown on the screen below.
- Click **Next**.



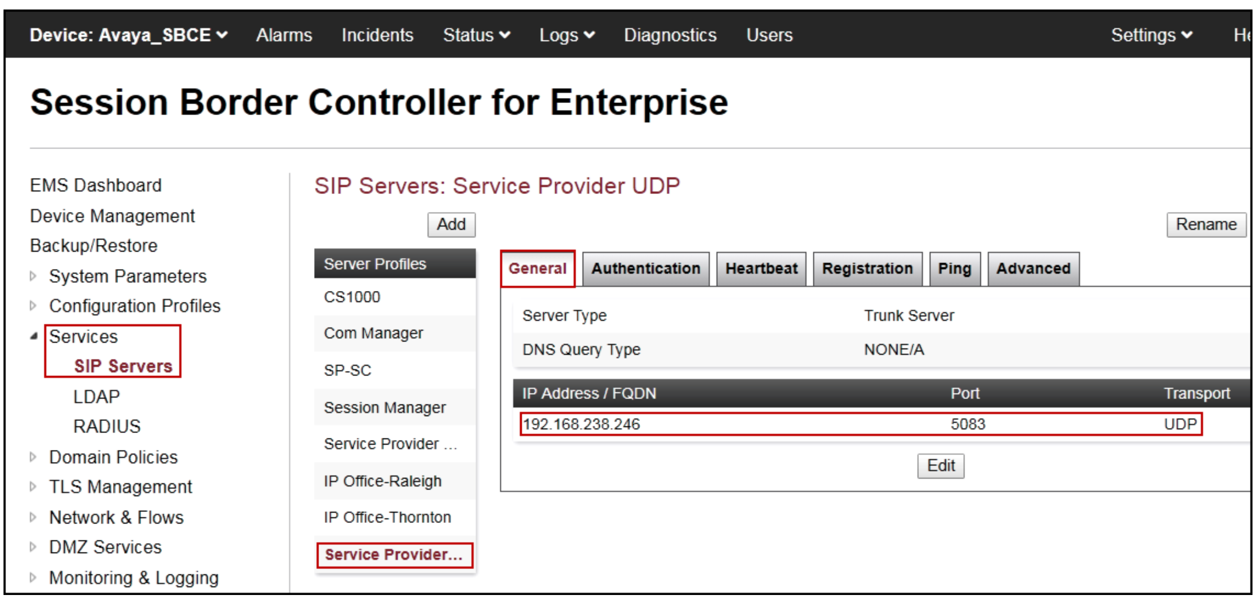
- Click **Next** on **Add SIP Server Profile – Ping** window (not shown).

In the **Add SIP Server Profile – Advanced** window:

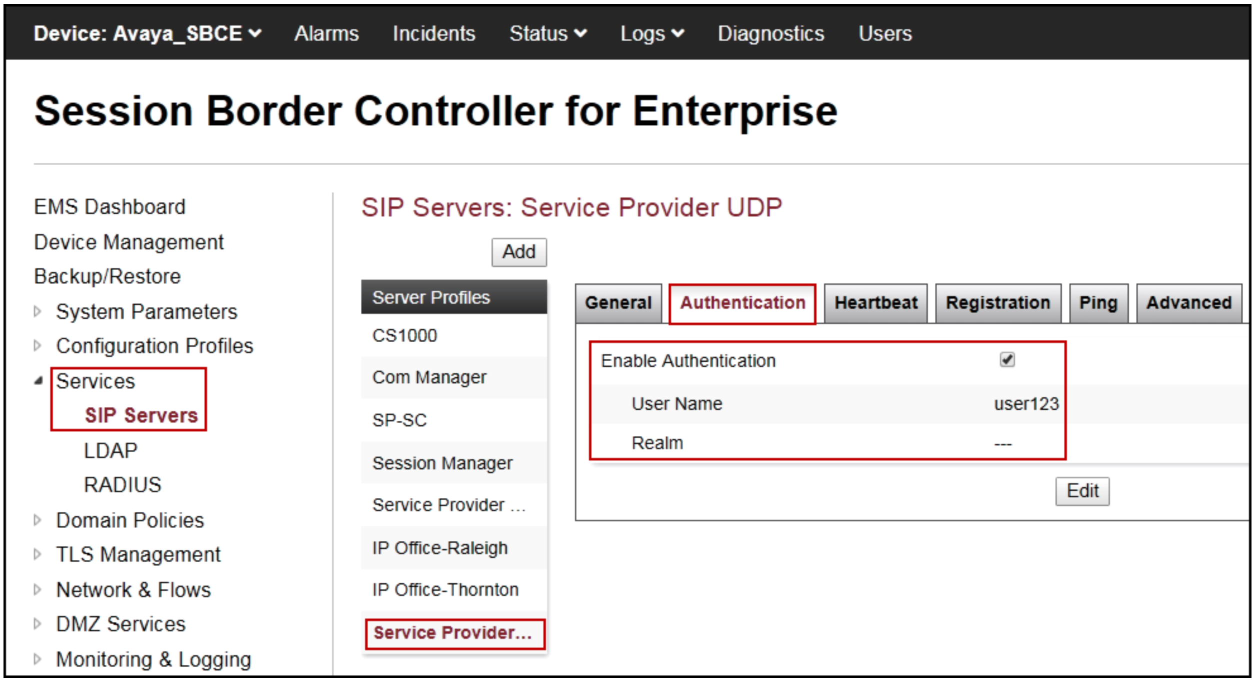
- Select ***SP-General*** from the **Interworking Profile** (**Section 7.3.2**).
- Select ***Add_Privacy_Header*** from the **Signaling Manipulation Script** (**Section 7.3.3**)
- Click **Finish**.



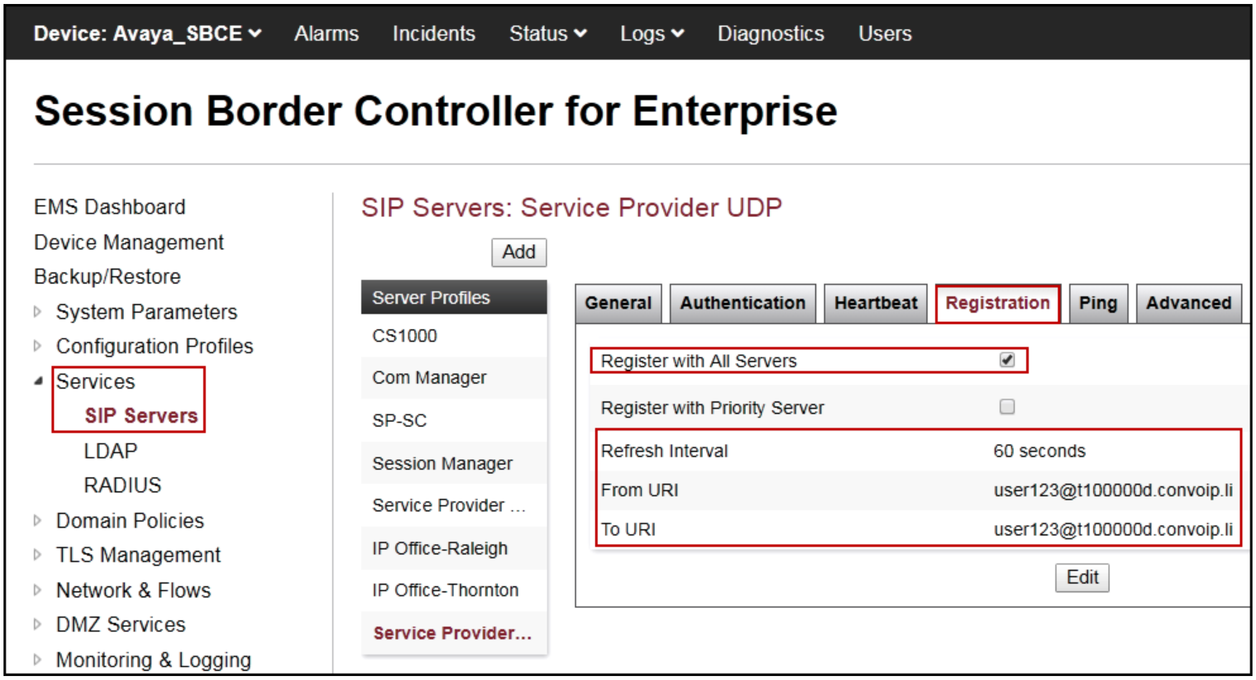
The following screen capture shows the **General** tab of the newly created **Service Provider UDP** SIP Server Configuration Profile.



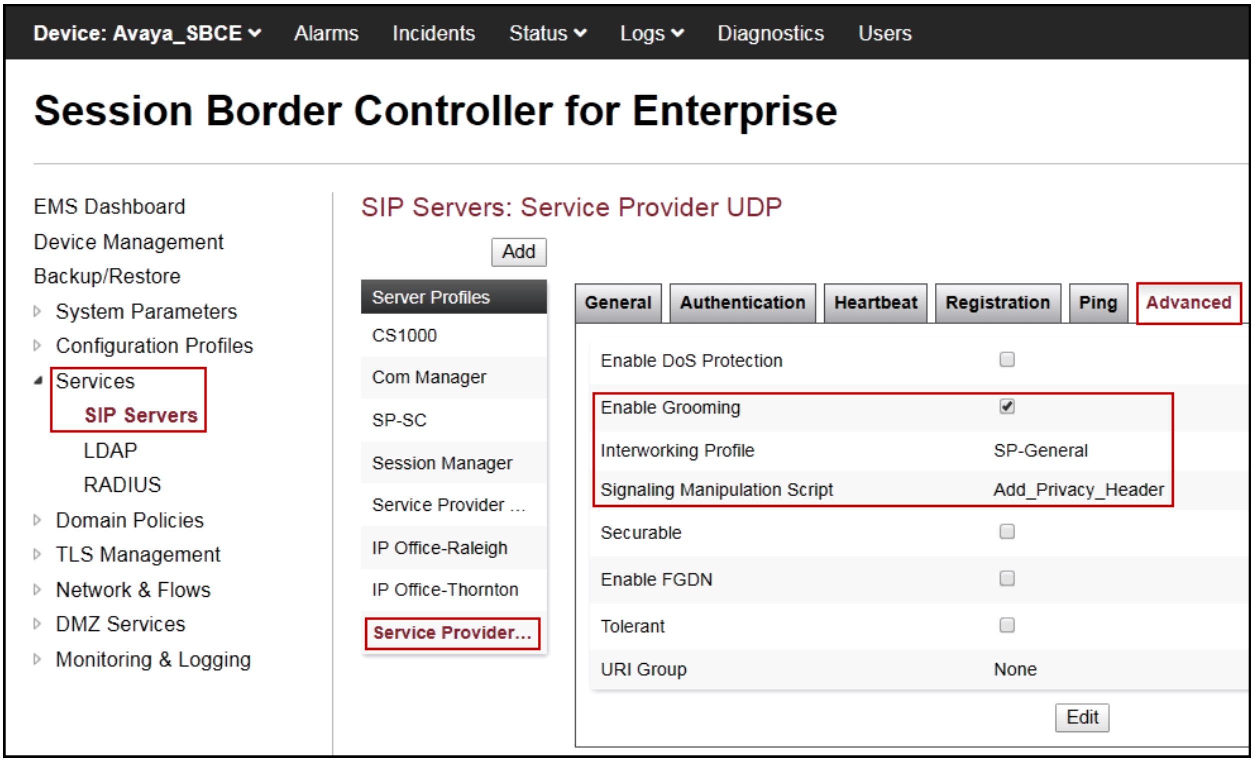
The following screen capture shows the **Authentication** tab of the newly created **Service Provider UDP** SIP Server Configuration Profile.



The following screen capture shows the **Registration** tab of the newly created **Service Provider UDP** SIP Server Configuration Profile.



The following screen capture shows the **Advanced** tab of the newly created **Service Provider UDP** SIP Server Configuration Profile.



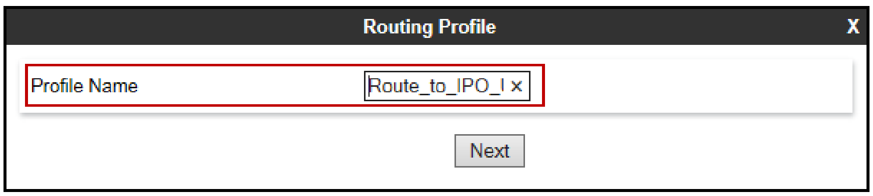
7.3.5. Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing profiles were created, one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

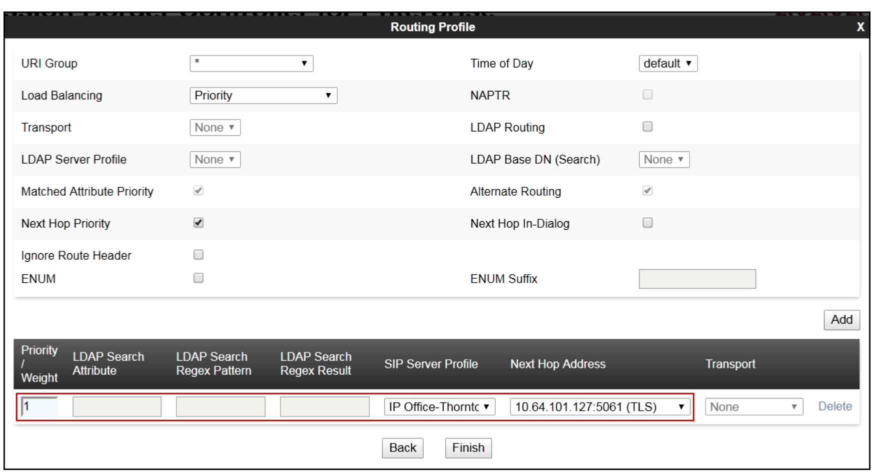
To create the inbound route, from the **Configuration Profiles** menu on the left-hand side (not shown):

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: ***Route_to_IPO_TLS***.
- Click **Next**.

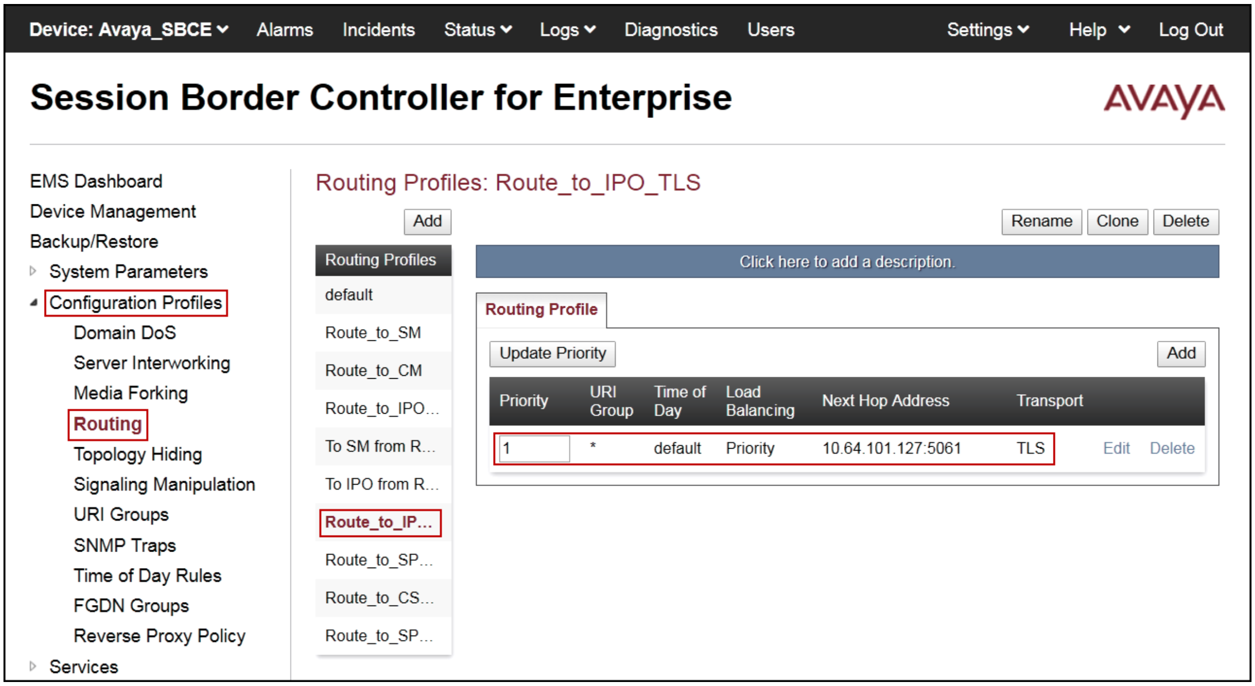


On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: ***1***
- **Server Configuration**: Select ***IP Office Thornton***.
- **Next Hop Address** is populated automatically with ***10.64.101.127:5061 (TLS)*** (IP Office IP address, Port and Transport).
- Click **Finish**.

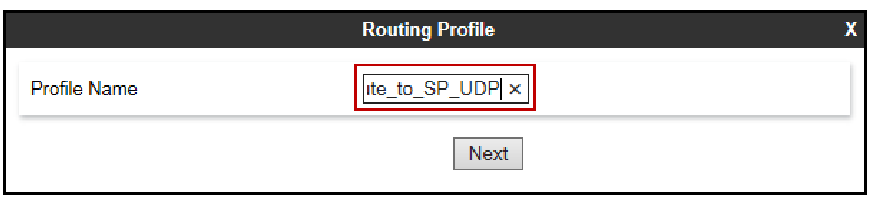


The following screen shows the newly created **Route_to_IPO_TLS** Routing Profile.



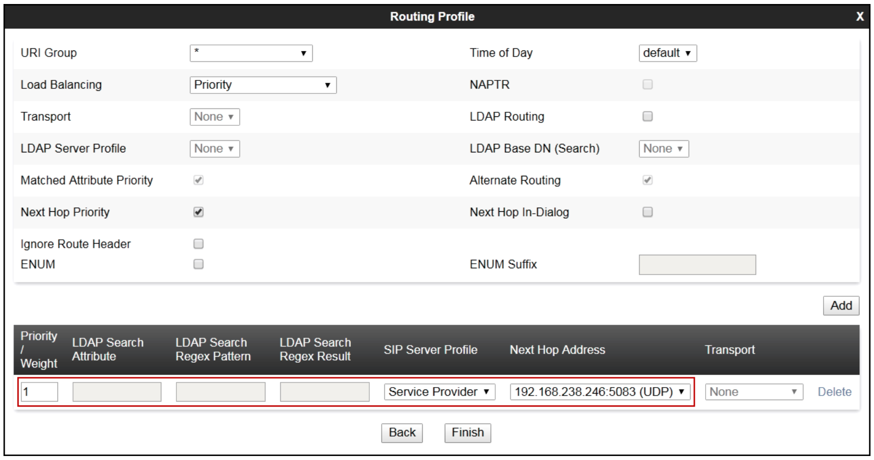
Similarly, for the outbound route:

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: ***Route_to_SP_UDP***.
- Click **Next**.

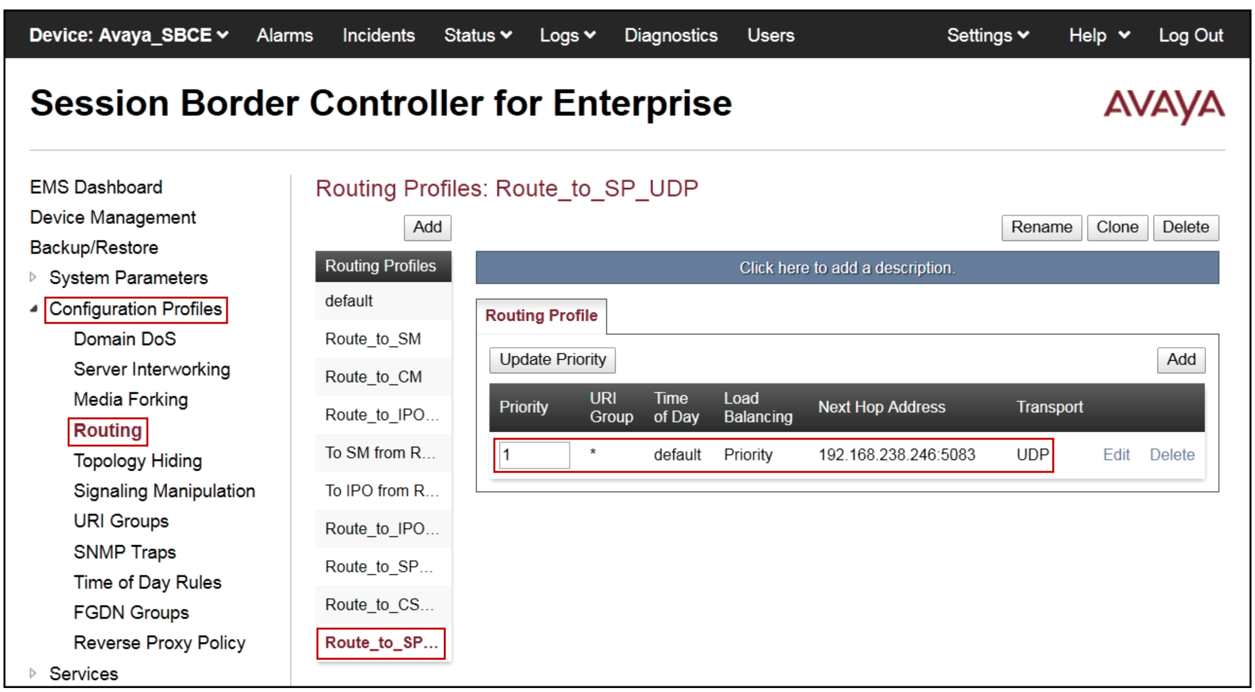


On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: ***1***
- **Server Configuration**: Select ***Service Provider UDP***.
- **Next Hop Address** is populated automatically with ***192.168.238.246:5083 (UDP)*** (Service Provider SIP Proxy IP address, Port and Transport).
- Click **Finish**.



The following screen capture shows the newly created **Route_to_SP_UDP** Routing Profile.



7.3.6. Topology Hiding

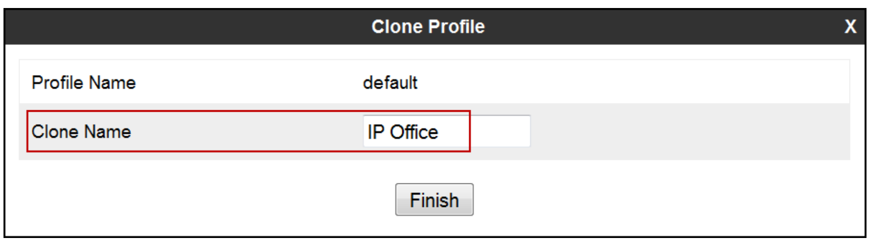
Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by IP Office and the SIP trunk service provider, allowing the call to be accepted in each case.

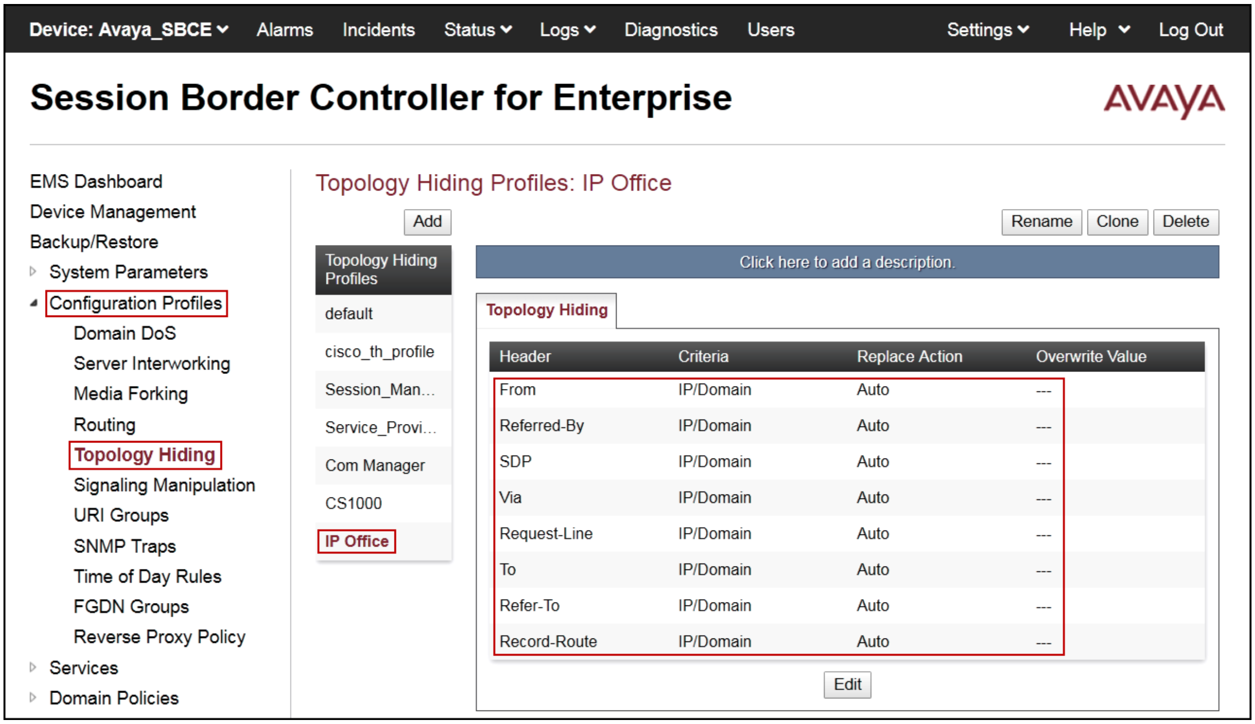
For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Profile Name**: ***IP Office***.
- Click **Finish**.

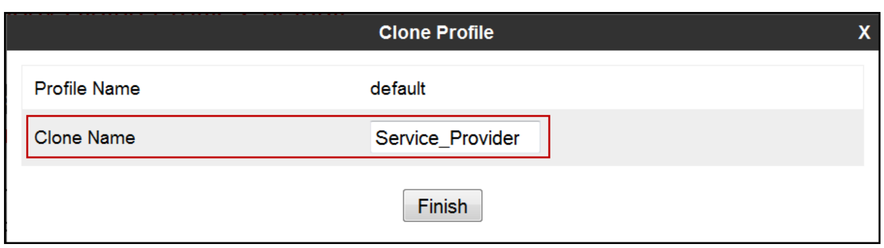


The following screen capture shows the newly added **IP Office** Topology Hiding Profile. Note that for IP Office no values were overwritten (left with default values).



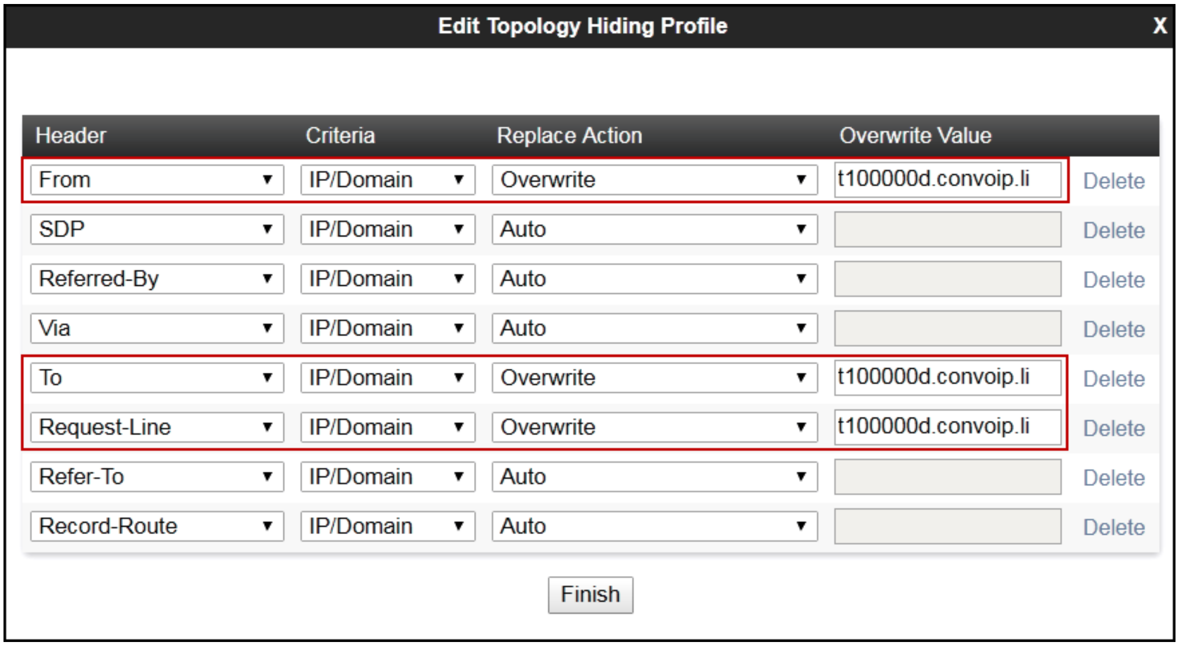
To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Profile Name**: ***Service_Provider***.
- Click **Finish**.

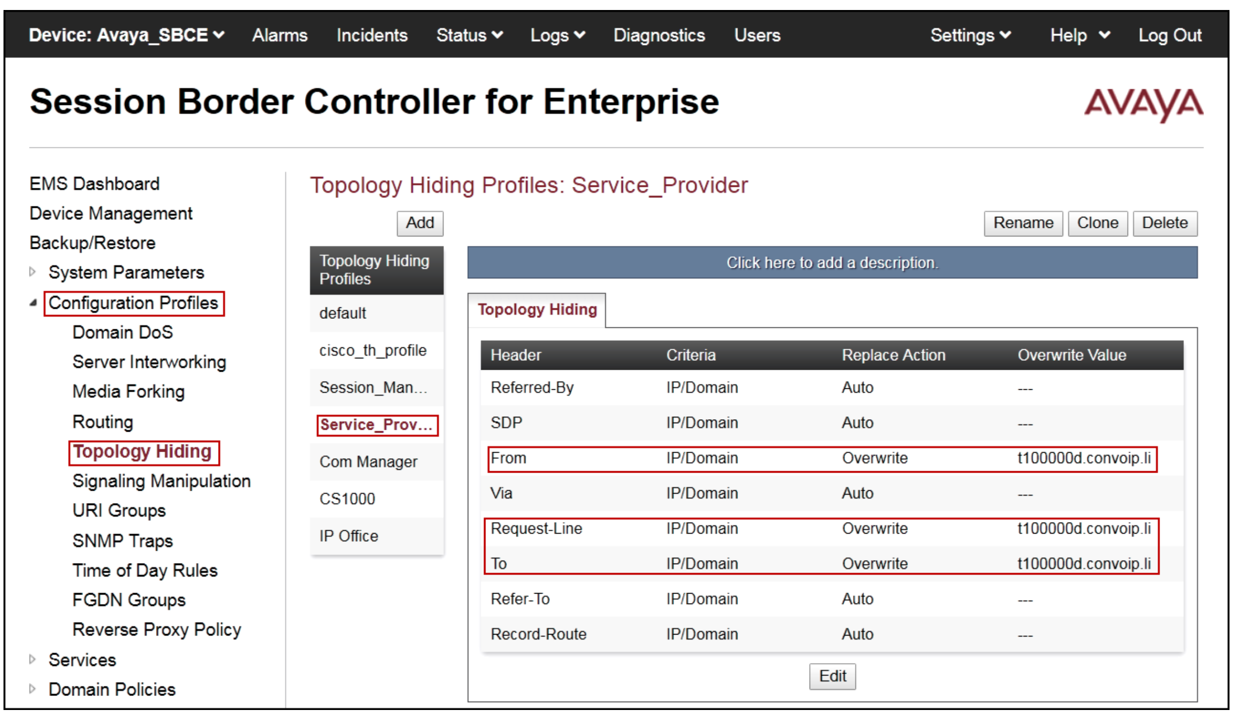


- Click **Edit** on the newly created **Service_Provider** Topology Hiding profile.
- On the **From** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the service provider (***t100000d.convoip.li***) under **Overwrite Value**.
- On the **To** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the service provider (***t100000d.convoip.li***) under **Overwrite Value**.
- On the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action;** enter the domain name for the service provider (***t100000.convoip.li***) under **Overwrite Value**.

- Click **Finish**.



The following screen capture shows the newly added **Service_Provider** Topology Hiding Profile.



7.4. Domain Policies

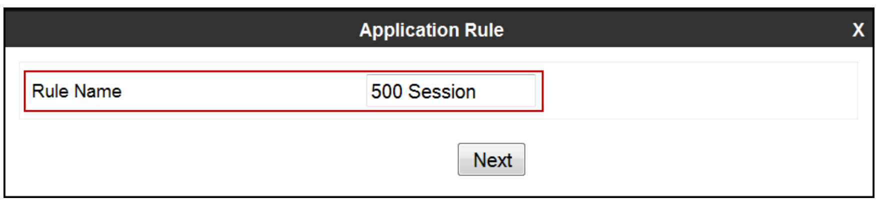
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.4.1. Application Rules

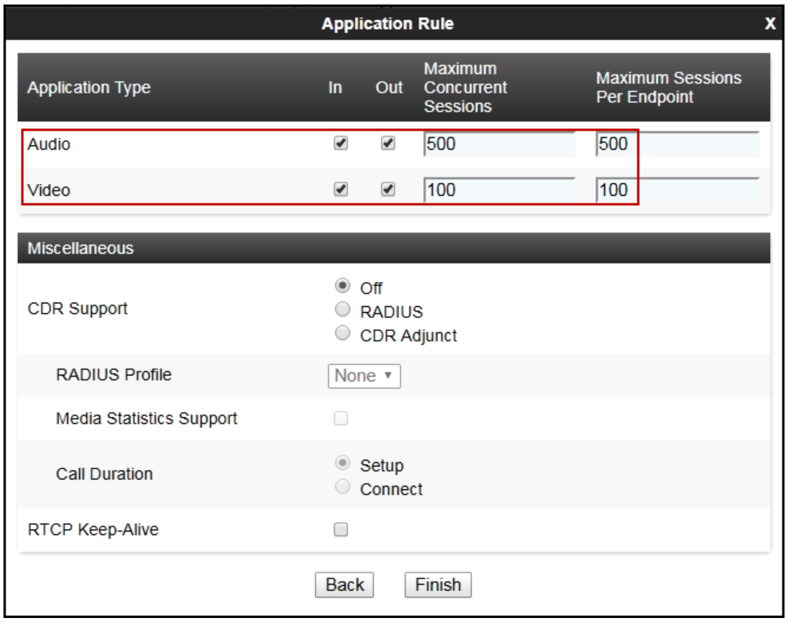
Application Rules defines which types of SIP-based Unified Communications (UC) applications the Avaya SBCE will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent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

From the menu on the left-hand side, select **Domain Policies → Application Rules** (not shown).

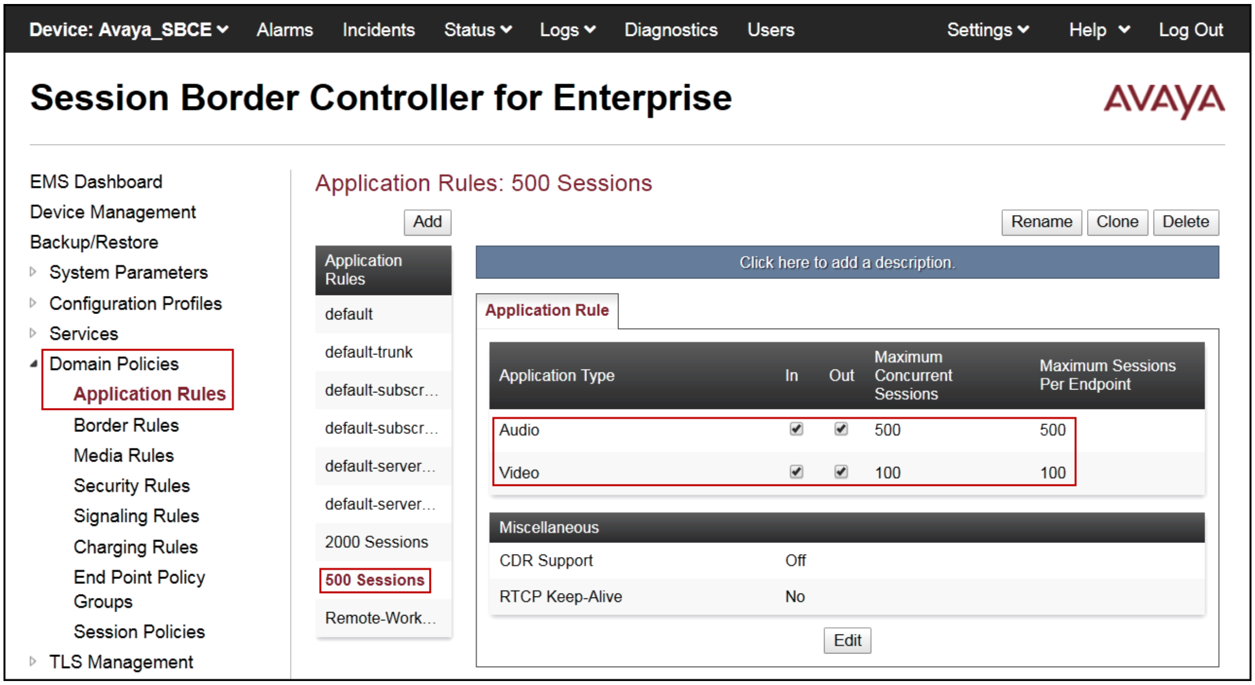
- Click on the **Add** button to add a new rule (not shown).
- **Rule Name:** enter the name of the profile, e.g., ***500 Session***.
- Click **Next**.



- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values; the value of ***500*** was used in the sample configuration.
- Under **Video** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values; the value of ***100*** was used in the sample configuration.
- Click **Finish**.



The following screen capture shows the newly created **500 Sessions** Application Rule.



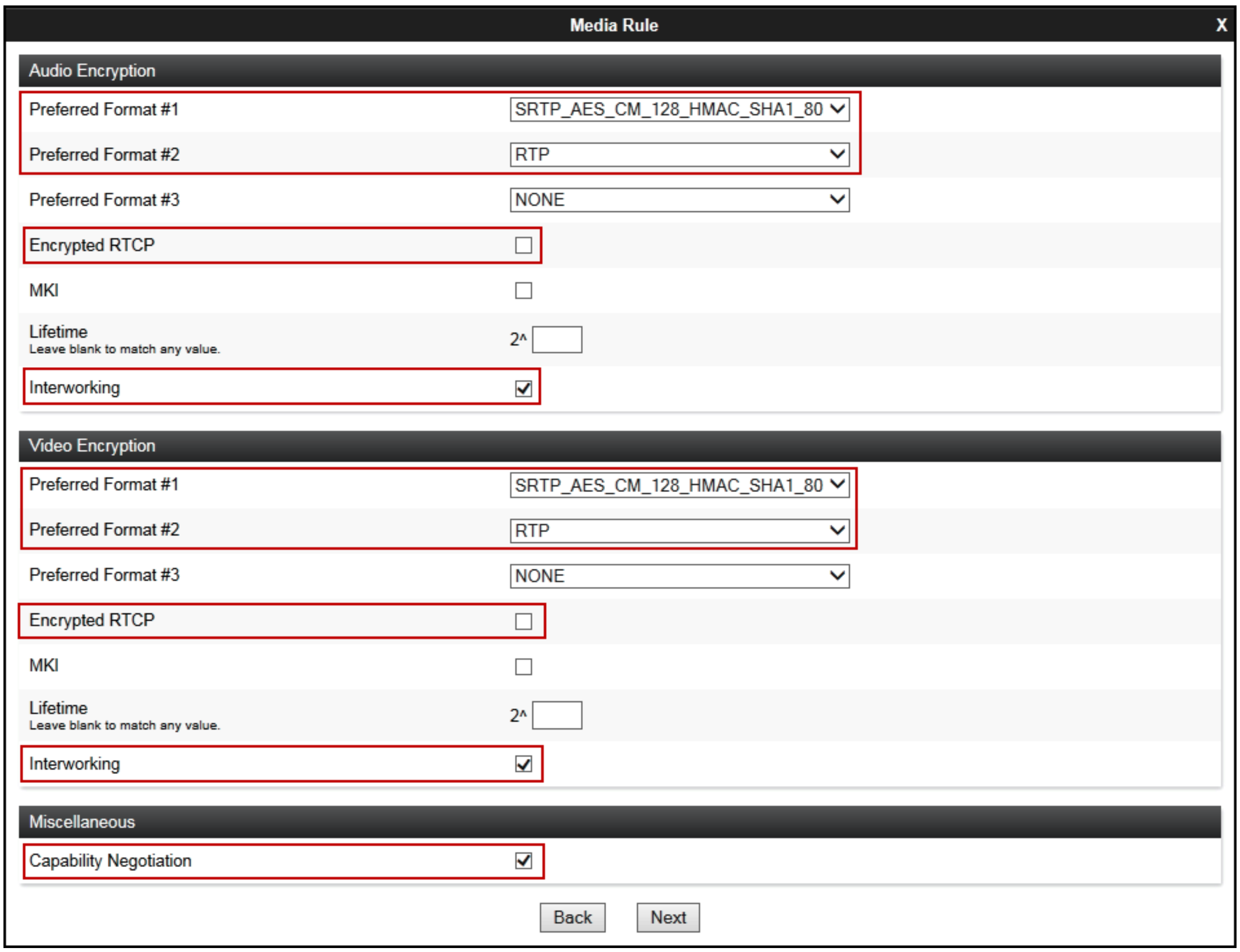
7.4.2. Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test one media rule was created toward IP Office, the existing ***default-low-med*** media rule was used toward the Service Provider.

To add a media rule in the IP Office direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

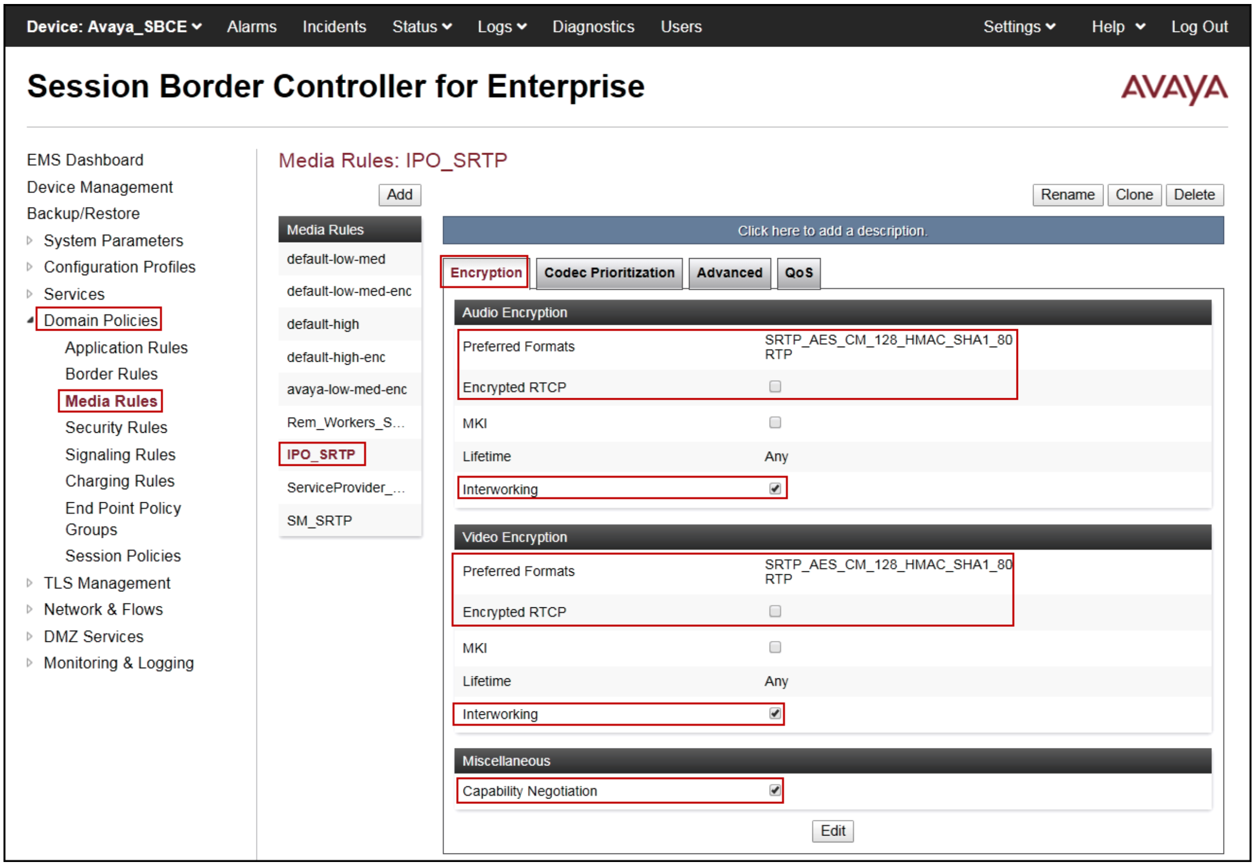
- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter ***IPO_SRTP***.
- Click Next.

- Under Audio Encryption, **Preferred Format #1**, select ***SRTP_AES_CM_128_HMAC_SHA1_80***.
- Under Audio Encryption, **Preferred Format #2**, select ***RTP***.
- Under Audio Encryption**,** uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous check **Capability Negotiation**.
- Click **Next**.



- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

The following screen capture shows the newly created **IPO_SRTP** Media Rule

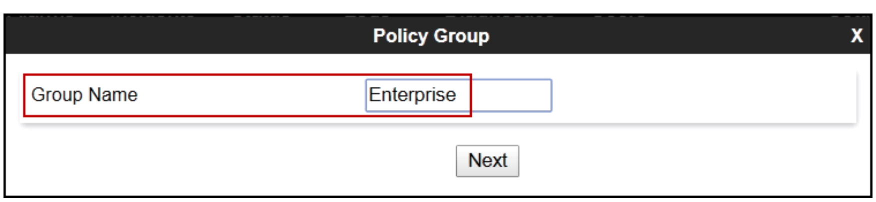


7.4.3. End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

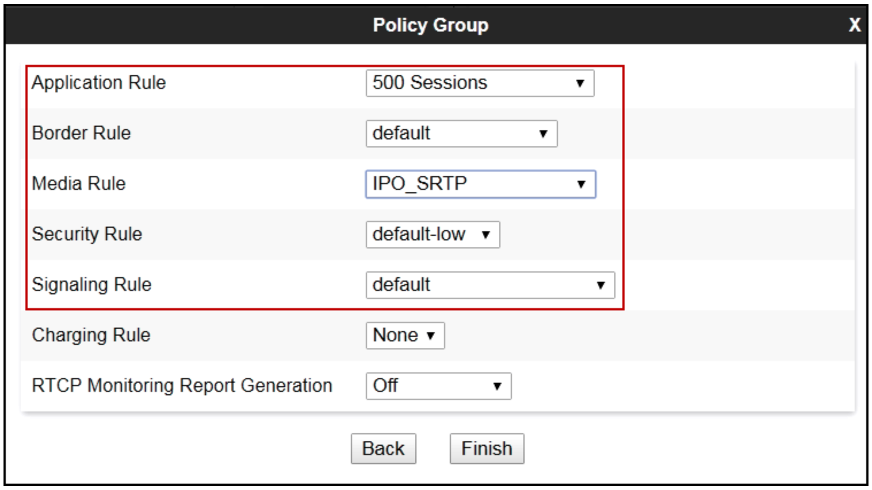
To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups** (not shown).

- Click on the **Add** button to add a new policy group (not shown).
- **Group Name:** ***Enterprise***.
- Click **Next**.

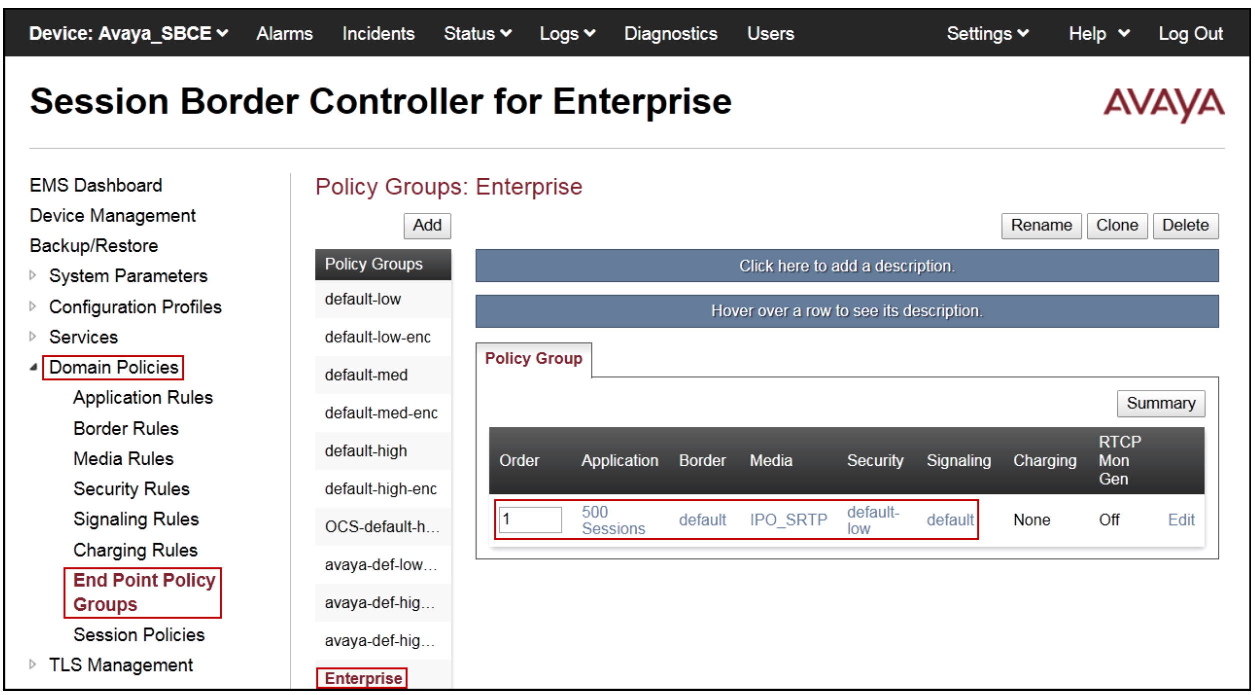


- **Application Rule:** ***500 Sessions***.
- **Border Rule:** ***default***.
- **Media Rule:** ***IPO_SRTP*** **(Section 7.4.2)**.

- **Security Rule: *default-low***.
- **Signaling Rule: *default***.
- Click **Finish**.

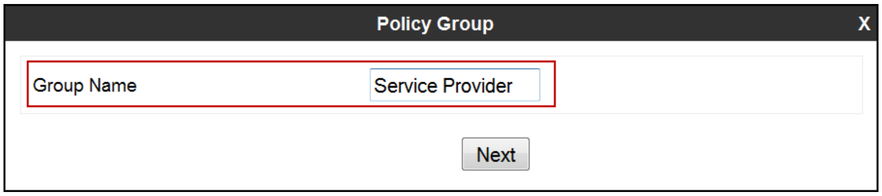


The following screen capture shows the newly created **Enterprise** End Point Policy Group.

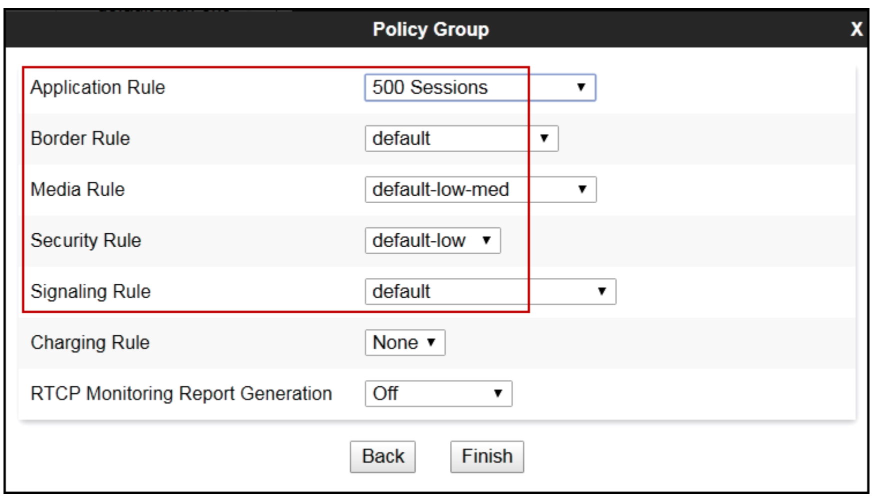


Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk.

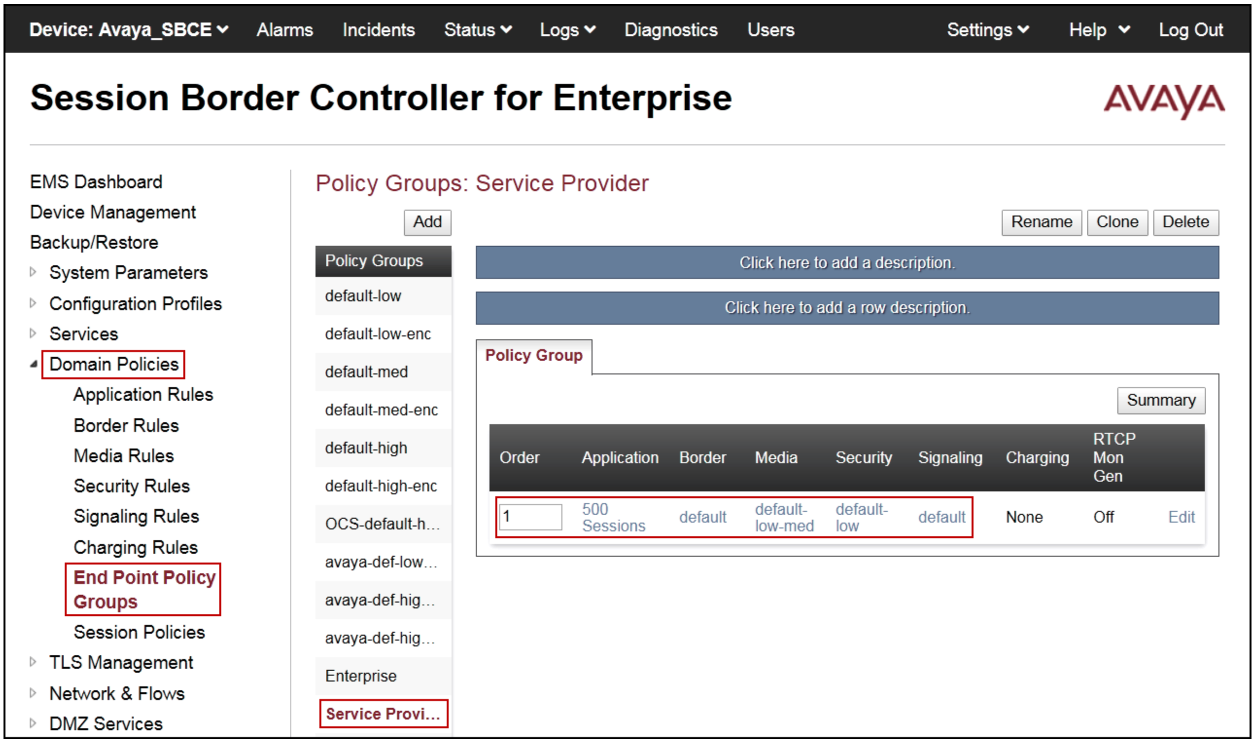
- Click on the **Add** button to add a new policy group (not shown).
- **Group Name:** ***Service Provider***.
- Click **Next**.



- **Application Rule:** ***500 Sessions***
- **Border Rule:** ***default.***
- **Media Rule:** ***default-low-med***.
- **Security Rule:** ***default-low***.
- **Signaling Rule:** ***default***.
- Click **Finish**.



The following screen capture shows the newly created **Service Provider** End Point Policy Group.



7.5. Network & Flows Settings

The **Network & Flows** settings allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

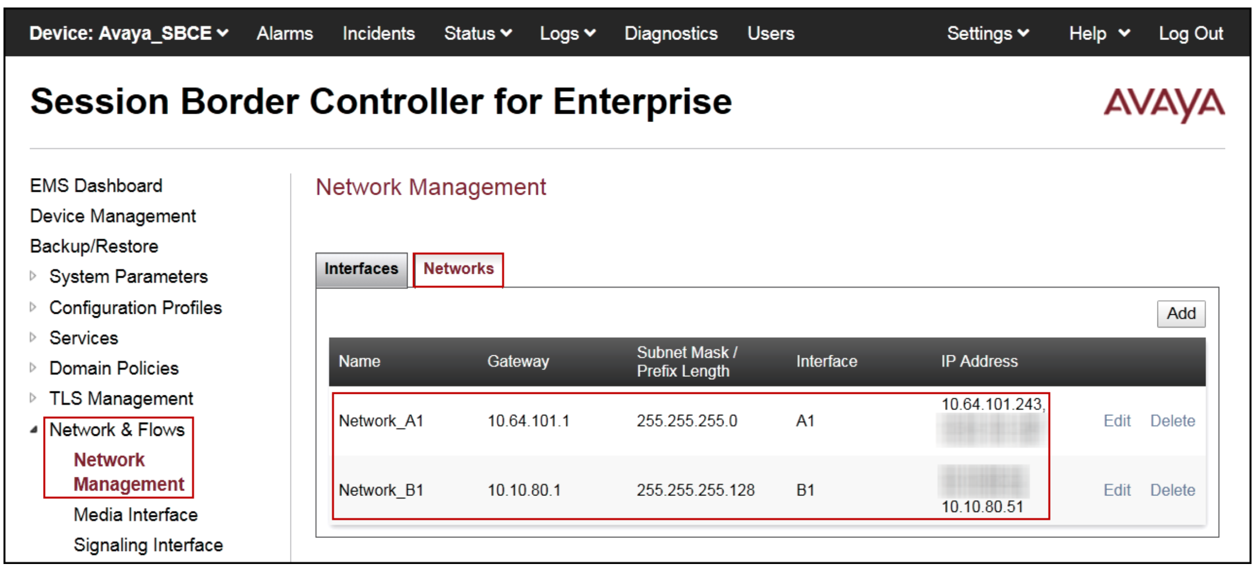
7.5.1. Network Management

The network information should have been previously completed. To verify the network configuration, from the **Network & Flows** on the left hand side, select **Network Management**. Select the **Networks** tab.

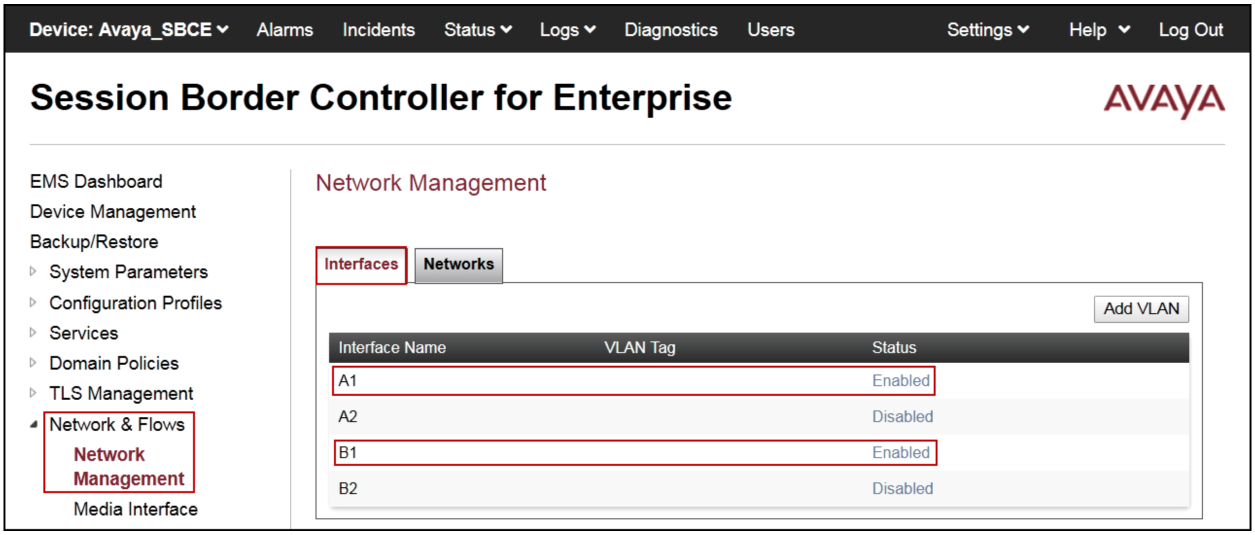
In the event that changes need to be made to the network configuration information, they can be entered here.

Use **Figure 1** as reference for IP address assignments.

Note: Only the highlighted entity items were created for the compliance test and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in these Application Notes.



On the Interfaces tab, click the **Status** control for interfaces **A1** and **B1** to change the status to ***Enabled***. It should be noted that the default state for all interfaces is ***Disabled***, so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.

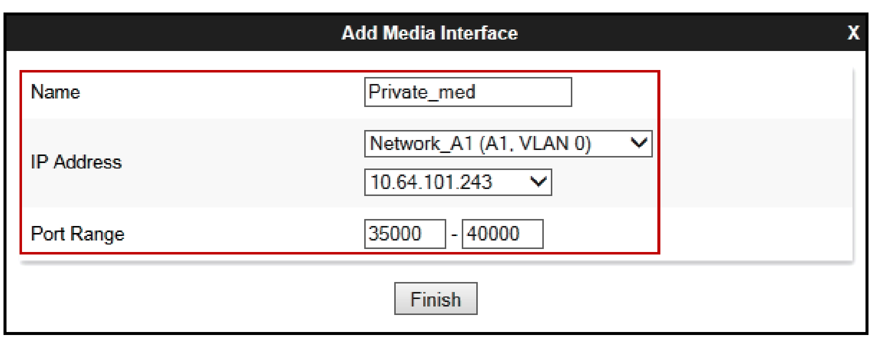


7.5.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

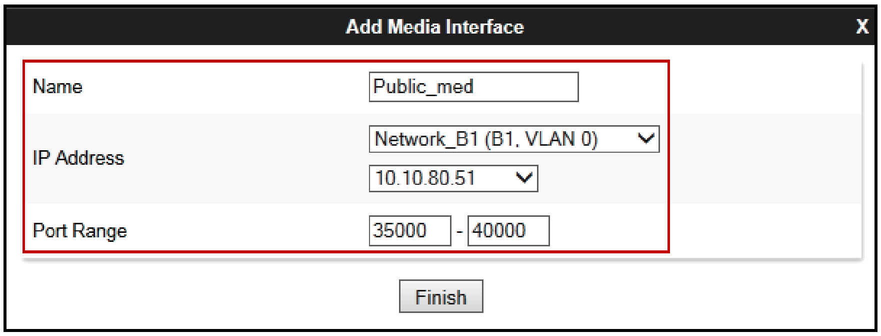
From the **Network & Flows** menu on the left-hand side, select **Media Interface** (not shown).

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** ***Private_med***.
- Under **IP Address** select: ***Network_A1 (A1, VLAN 0)***
- Select **IP Address:** ***10.64.101.243*** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **Port Range:** ***35000-40000***.
- Click **Finish**.

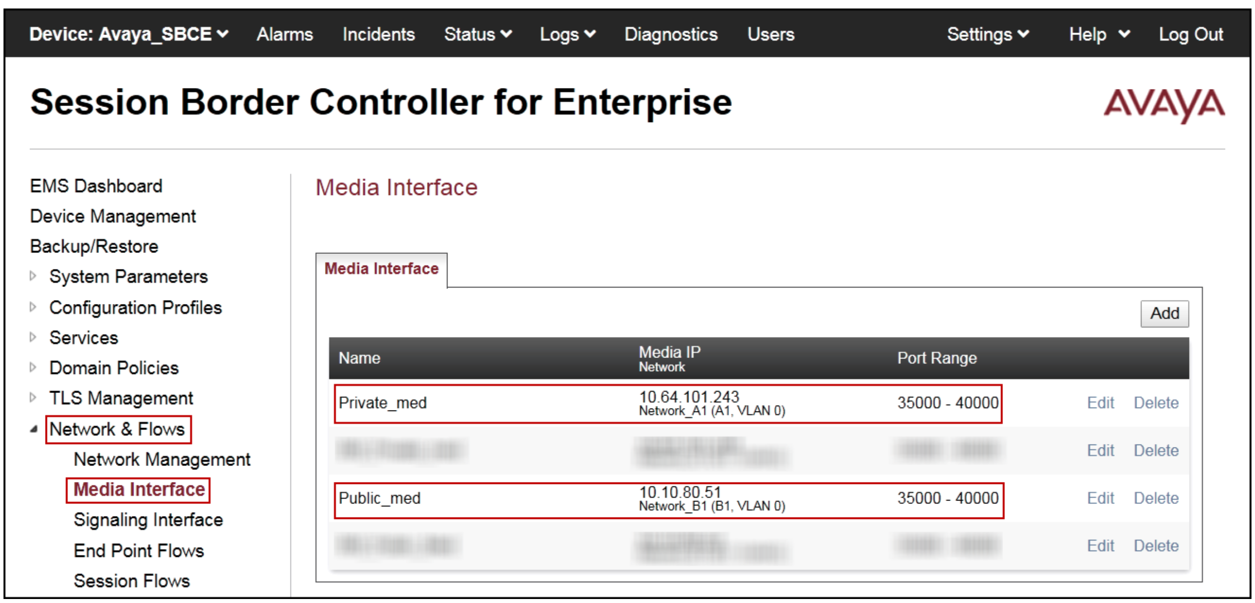


- Select **Add** in the **Media Interface** area (not shown).

- **Name:** ***Public_med***.
- Under **IP Address** select: ***Network_B1 (B1, VLAN 0)***
- Select **IP Address:** ***10.10.80.51*** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **Port Range:** ***35000-40000***.
- Click **Finish**.



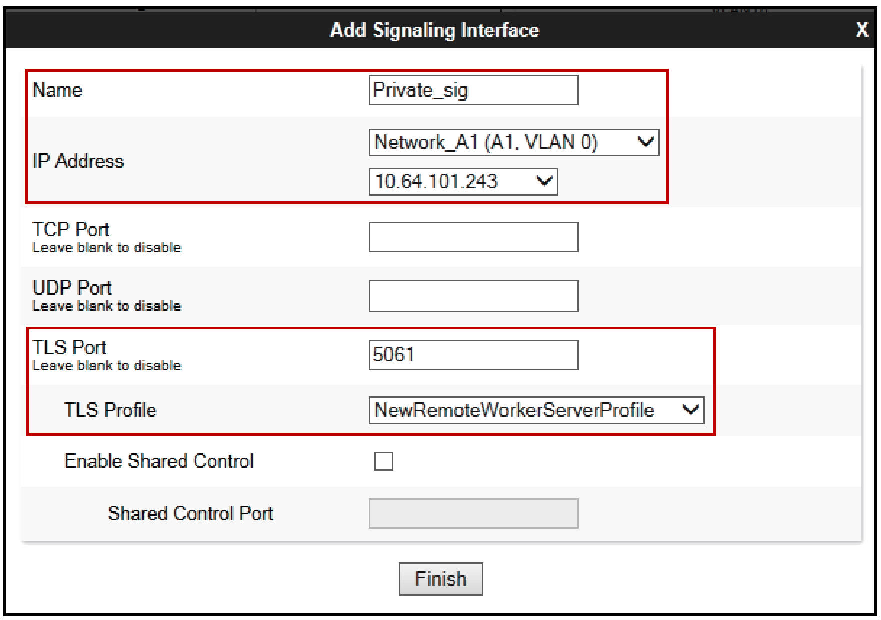
The following screen capture shows the newly created Media Interfaces.



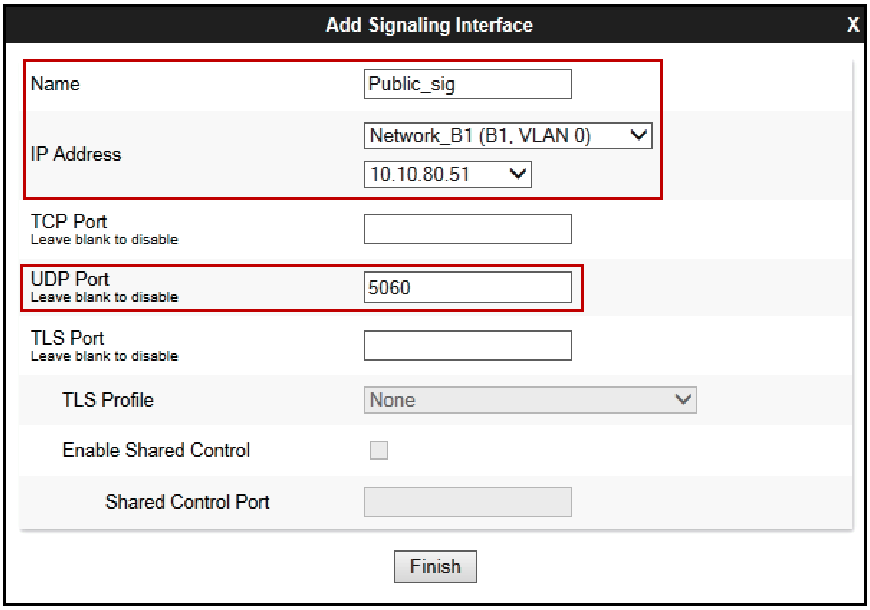
7.5.3. Signaling Interface

To create the Signaling Interface toward IP Office, from the **Network & Flows** menu on the left hand side, select **Signaling Interface** (not shown).

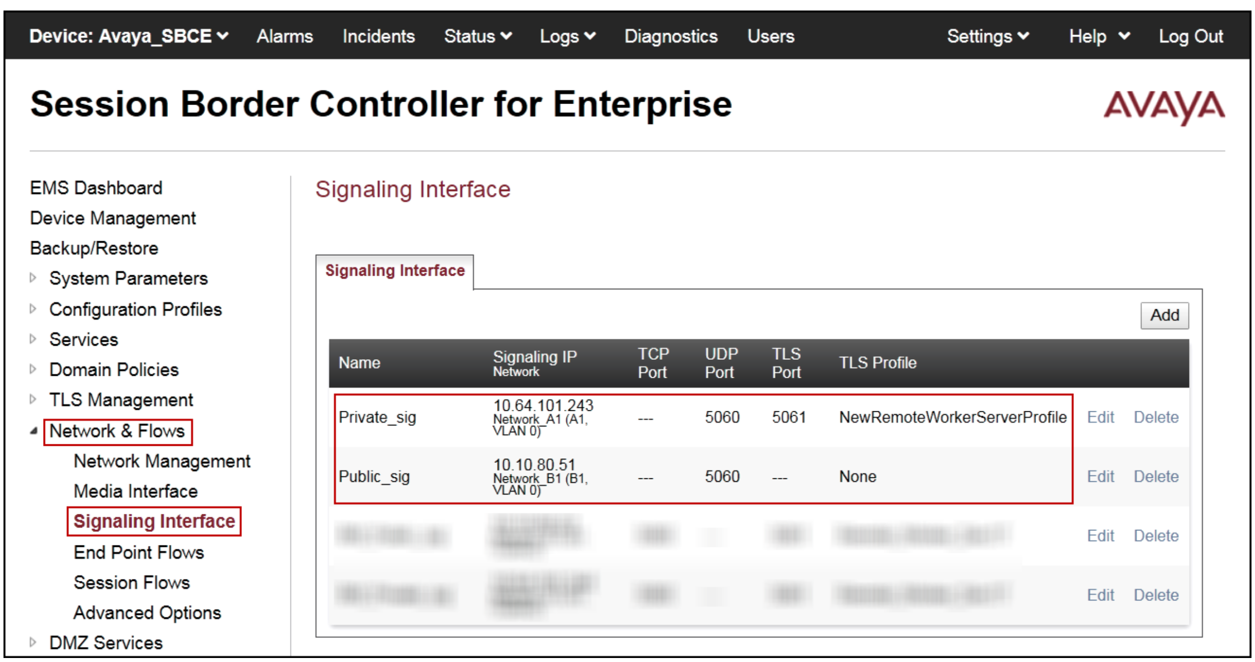
- Select **Add** in the **Signaling Interface** area (not shown).
- **Name: *Private_sig***.
- Under **IP Address** select: ***Network_A1 (A1, VLAN 0)***
- Select **IP Address: *10.64.101.243*** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **TLS Port: *5061***.
- Select a **TLS Profile**.
- Click **Finish**.



- Select **Add** in the **Signaling Interface** area (not shown).
- **Name:** ***Public_sig***.
- Under **IP Address** select: ***Network_B1 (B1, VLAN 0)***
- Select **IP Address:** ***10.10.80.51*** (outside or public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port:** ***5060***.
- Click **Finish**.

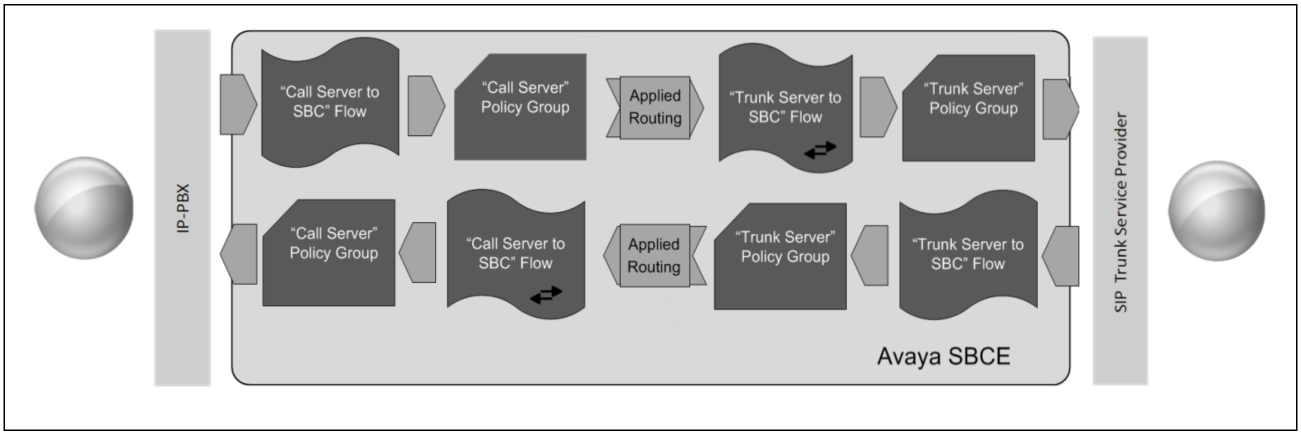


The following screen capture shows the newly created Signaling Interfaces.



7.5.4. End Point Flows

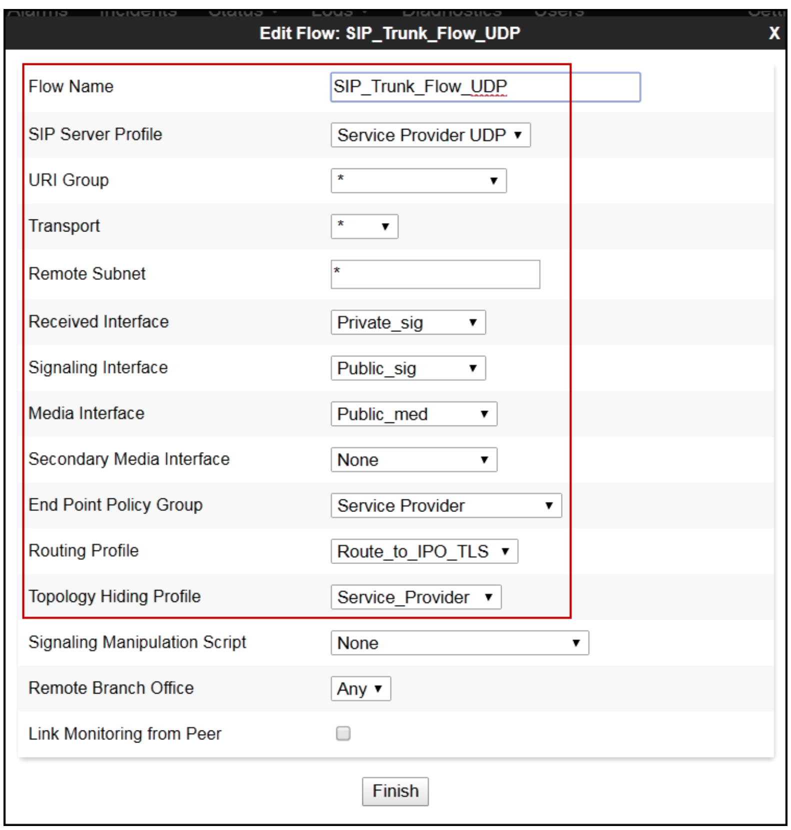
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing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



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

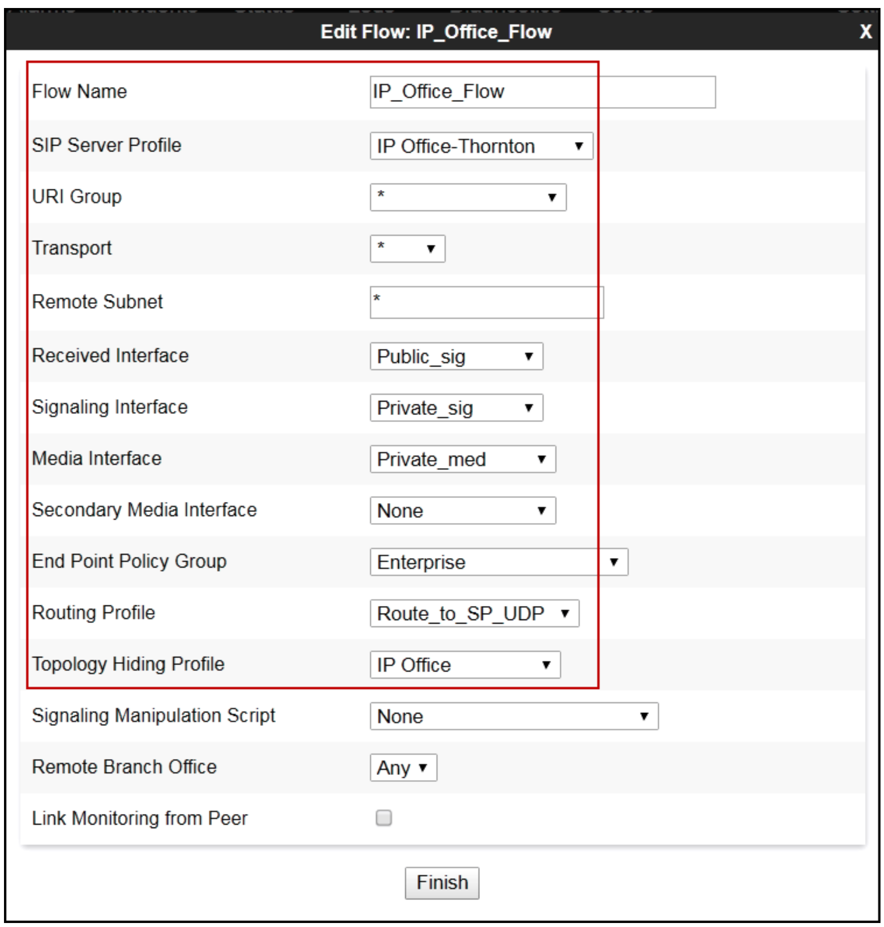
To create the call flow toward the Service Provider SIP trunk, from the **Network & Flows** menu, select **End Point Flows** (not shown**)**, then the **Server Flows** tab. Click **Add** (not shown).

- **Name:** ***SIP_Trunk_Flow_UDP***.
- **Server Configuration**: ***Service Provider UDP***.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: ***Private_sig***.
- **Signaling Interface:** ***Public_sig***.
- **Media Interface**: ***Public_med***.
- **Secondary Media Interface**: **None**.
- **End Point Policy Group:** ***Service Provider***.
- **Routing Profile:** ***Route_to_IPO_TLS*** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** ***Service_Provider***.
- Click **Finish**.

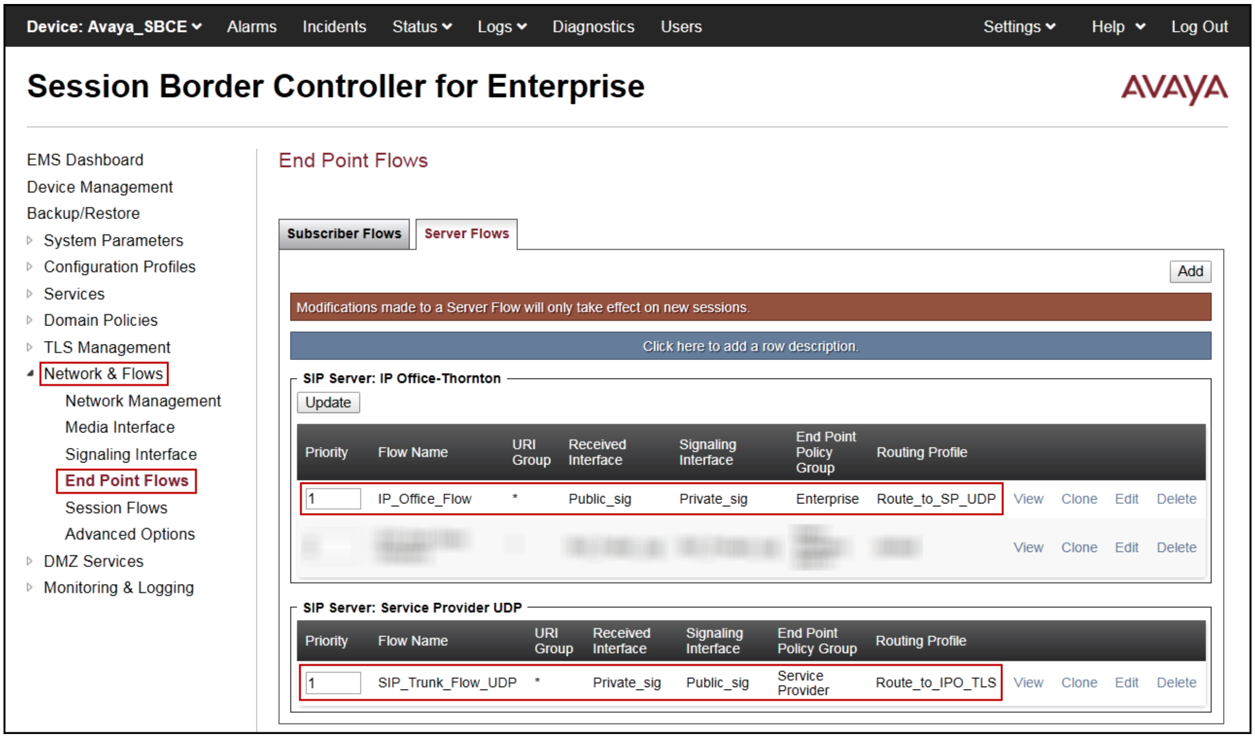


To create the call flow toward IP Office, click **Add** (not shown).

- **Name: *IP_Office_Flow***.
- **Server Configuration**: ***IP Office-Thornton***.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: ***Public_sig***.
- **Signaling Interface: Private_sig**.
- **Media Interface**: ***Private_med***.
- **Secondary Media Interface**: ***None***.
- **End Point Policy Group: *Enterprise***.
- **Routing Profile: *Route_to_SP_UDP*** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: *IP Office***.
- Click **Finish**.



The following screen capture shows the newly created **End Point Flows**.



8. Telecom Liechtenstein SIP Trunking Service Configuration

To use Telecom Liechtenstein's SIP Trunking Service, a customer must request the service from Telecom Liechtenstein using the established sales processes. The process can be started by contacting Telecom Liechtenstein via the corporate web site at: http://www.telecom.li/de and requesting information.

During the signup process, Telecom Liechtenstein and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Telecom Liechtenstein's network.

Telecom Liechtenstein is responsible for the configuration of Telecom Liechtenstein SIP Trunking Service. The customer will need to provide the public IP address used to reach the Avaya Session Border Controller for Enterprise at the enterprise, the public IP address assigned to interface B1.

Telecom Liechtenstein will provide the customer the necessary information to configure Avaya IP Office and the Avaya Session Border Controller for Enterprise following the steps discussed in the previous sections, including:

- SIP Trunk registration credentials (User Name, Password, etc.).
- Telecom Liechtenstein's Domain Name.
- DID numbers.
- UDP send Port number (e.g., port 5083 was used during the compliance test).
- Etc.

9. Verification Steps

This section provides verification steps that may be performed to verify that the solution is configured properly.

The following steps may be used to verify the configuration:

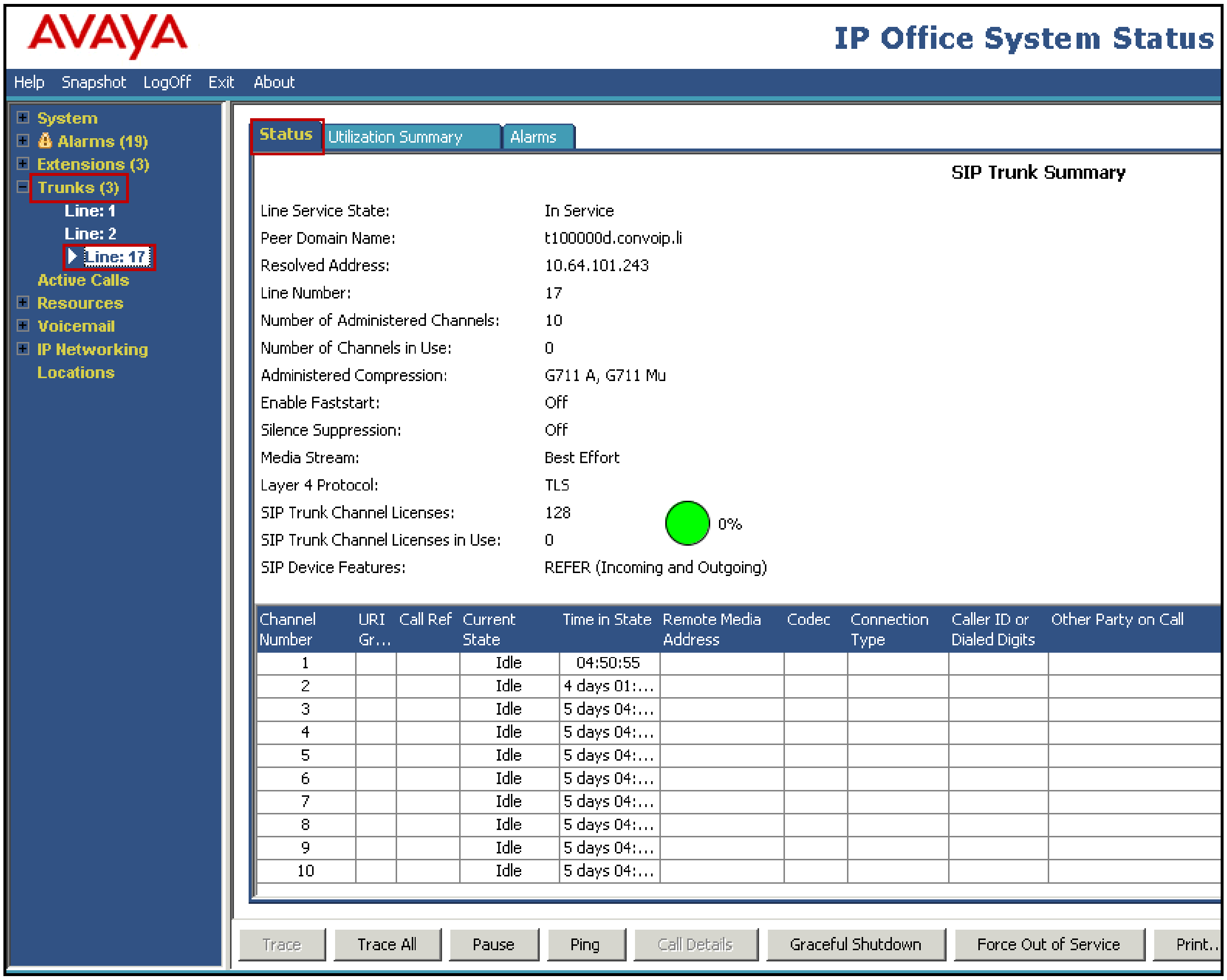
- Verify that endpoints at the enterprise site can place calls to the PSTN.
- Verify that endpoints at the enterprise site can receive calls from the PSTN.
- Verify that users at the PSTN can end active calls to endpoints at the enterprise by hanging up.
- Verify that endpoints at the enterprise can end active calls to PSTN users by hanging up.

9.1. IP Office System Status

The following steps can also be used to verify the configuration.

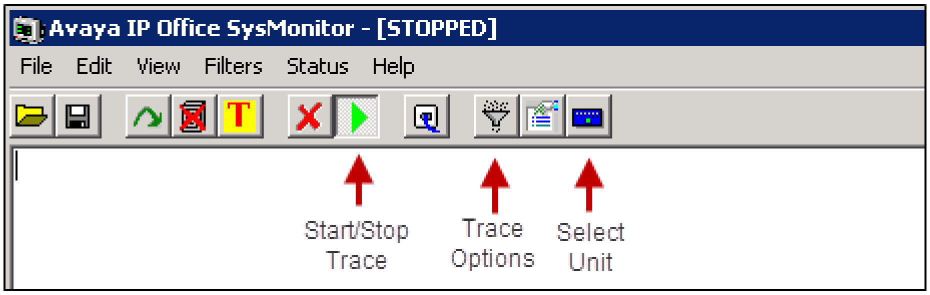
Use the IP Office **System Status** application to verify the state of SIP connections. Launch the application from **Start → Programs → IP Office → System Status** on the PC where IP Office Manager is installed, log in with the proper credentials.

Select the SIP line under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current Stat**e is **Idle** for each channel.

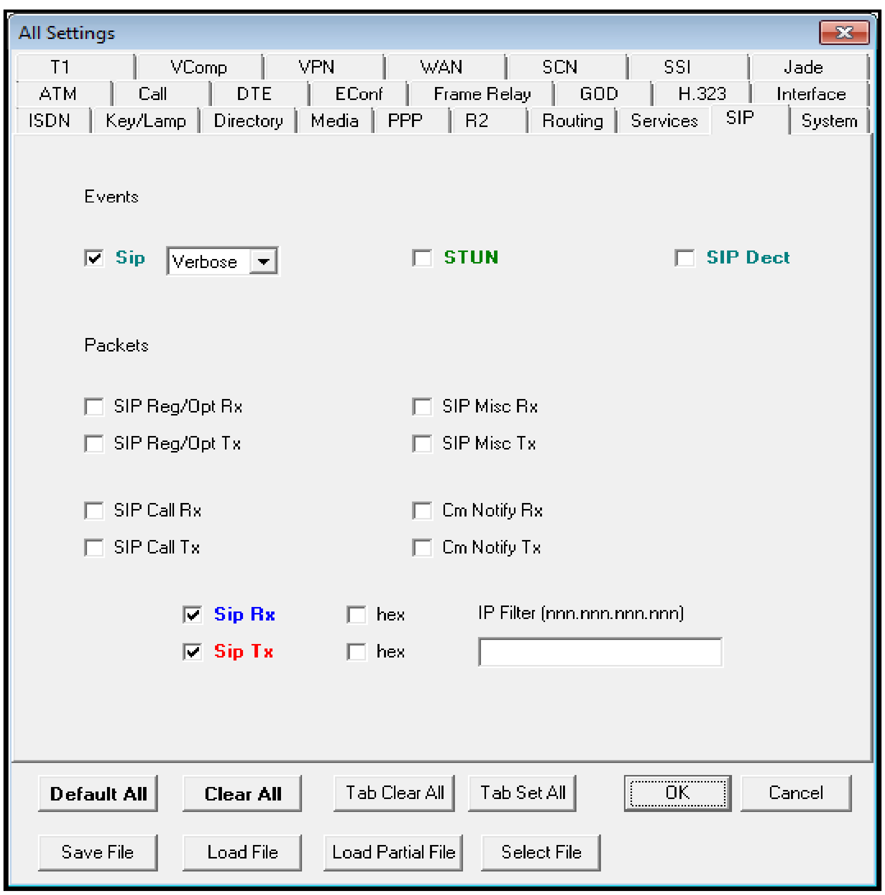


9.2. Monitor

The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the IP Office system under verification.



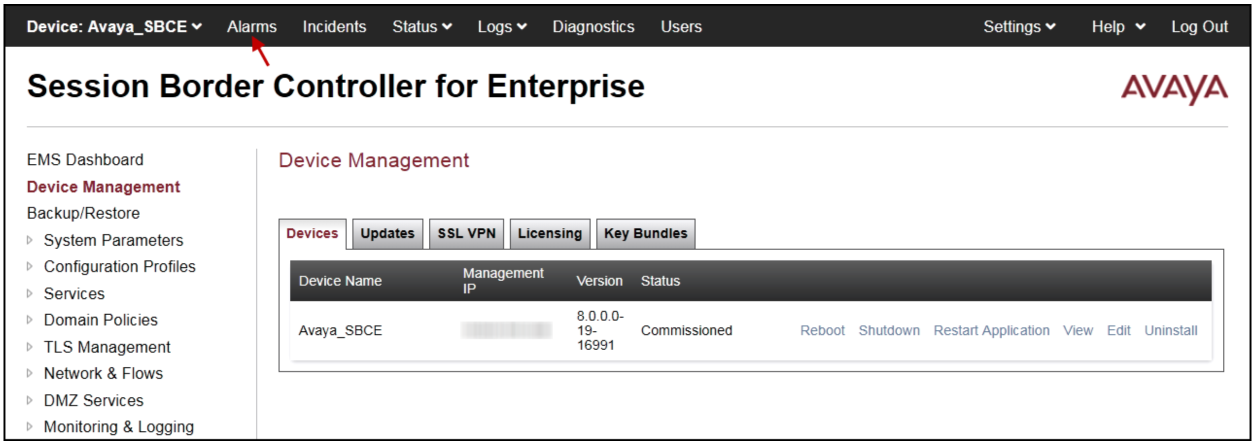
Clicking the **Trace Options** icon on the taskbar, selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting the desired color.



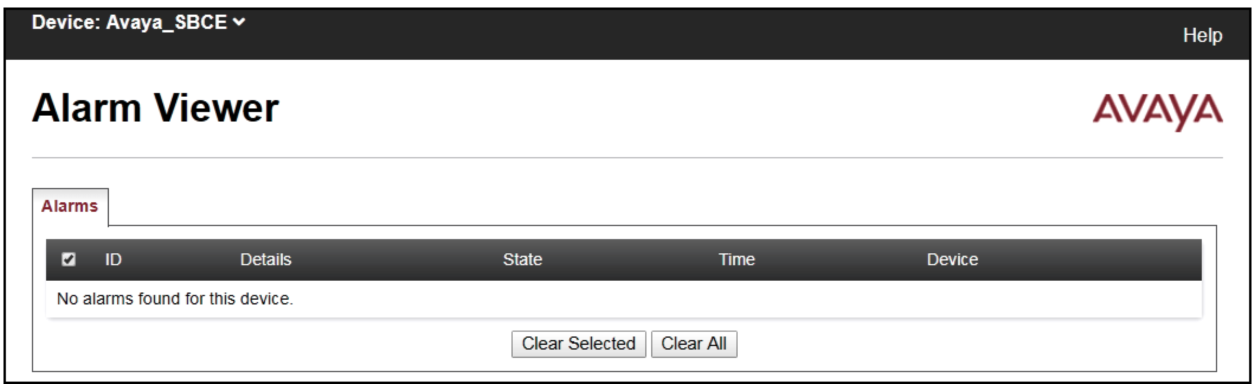
9.3. Avaya Session Border Controller for Enterprise

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

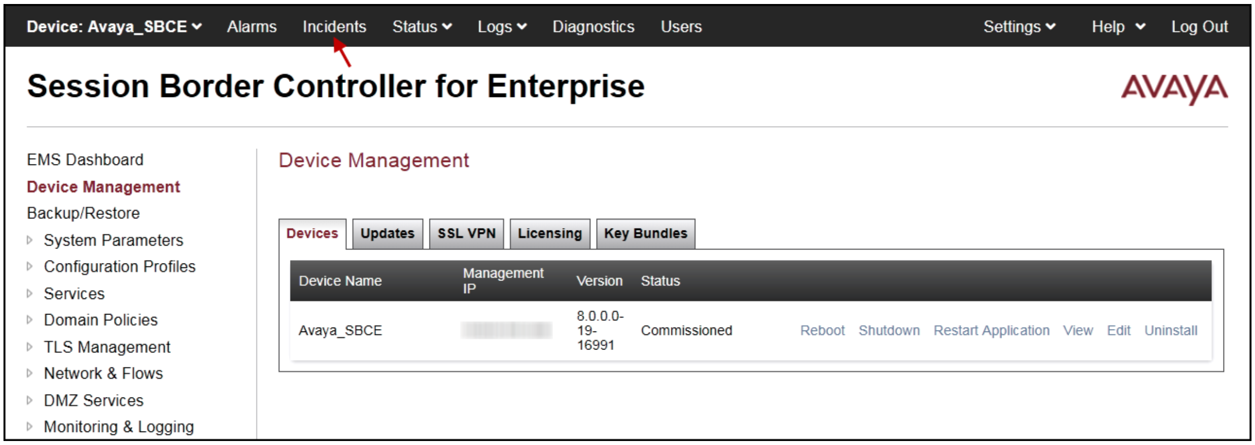
Alarms: Provides information about the health of the Avaya SBCE.



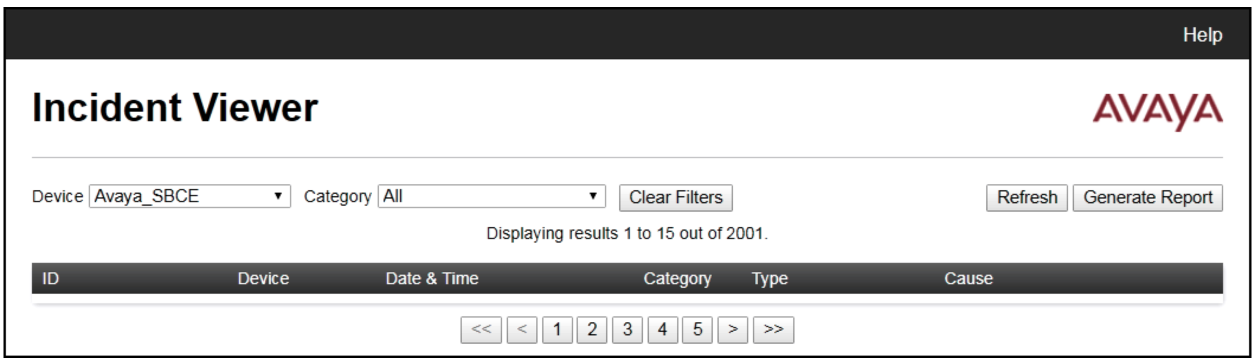
The following screen shows the **Alarm Viewer** page.



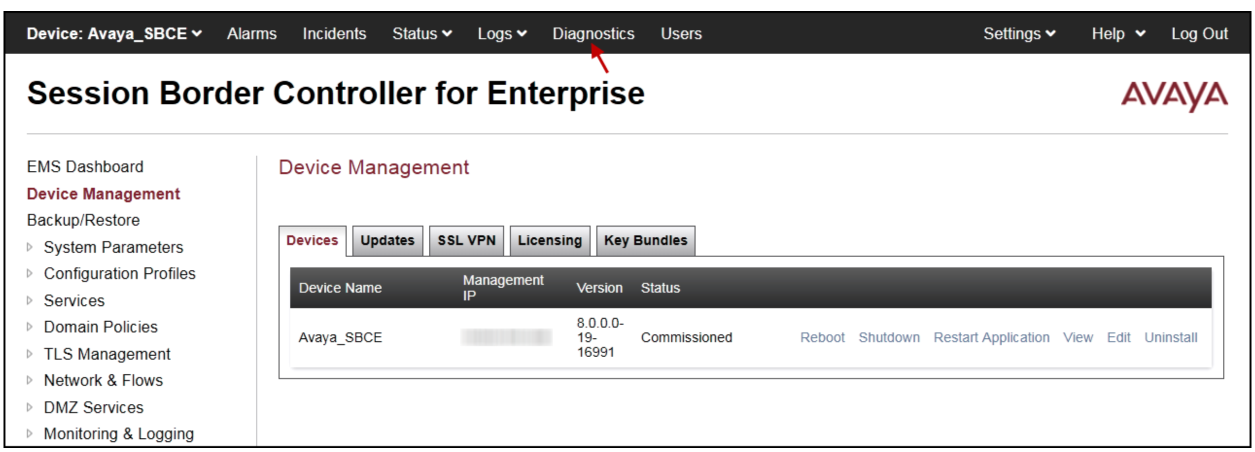
Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.



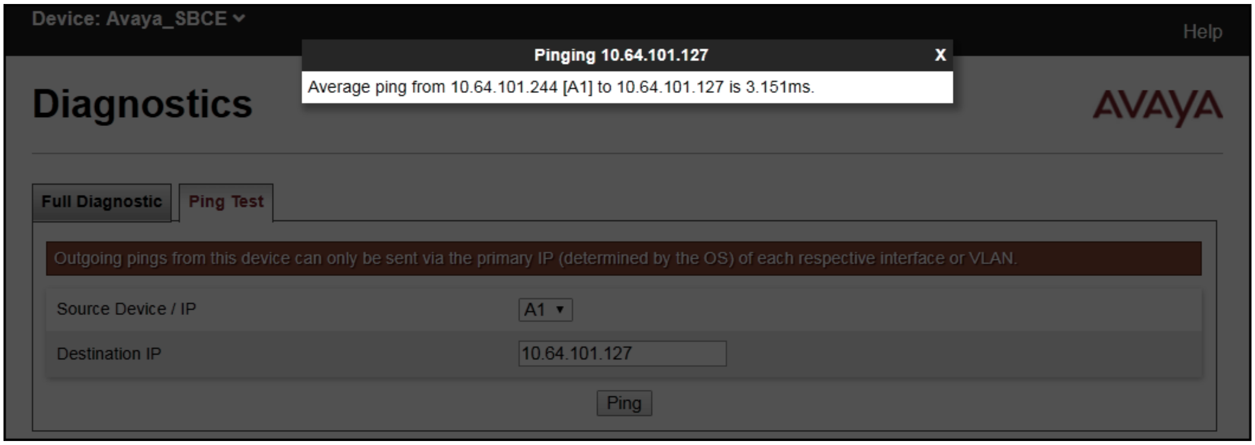
The following screen shows the Incident Viewer page.



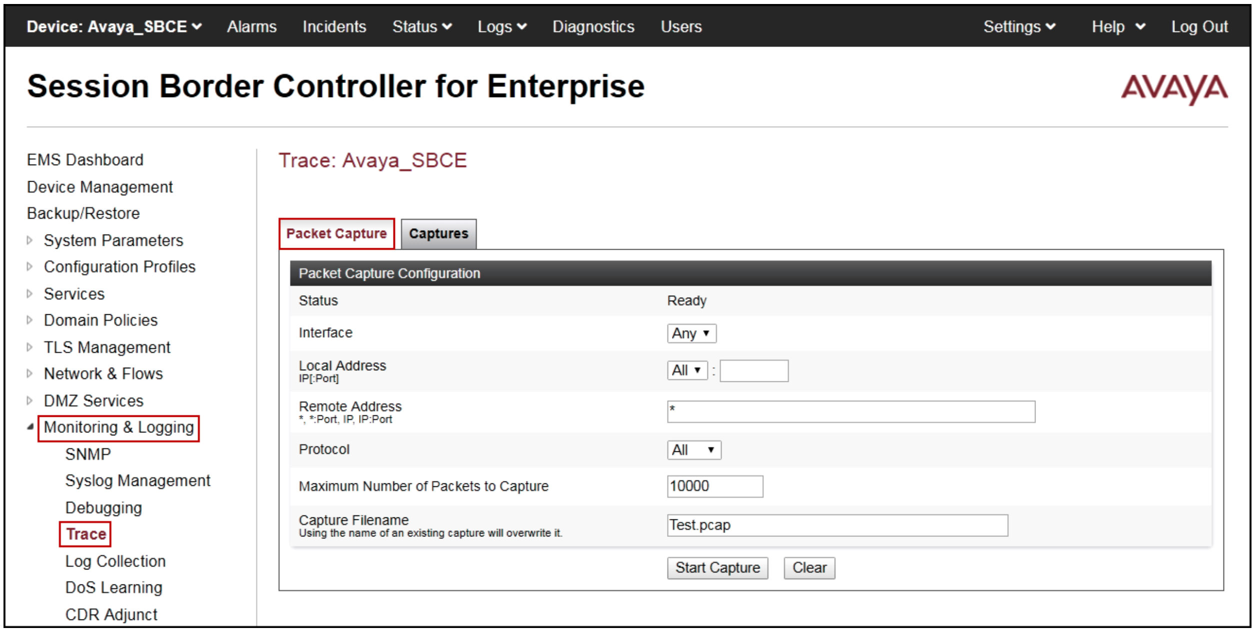
Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



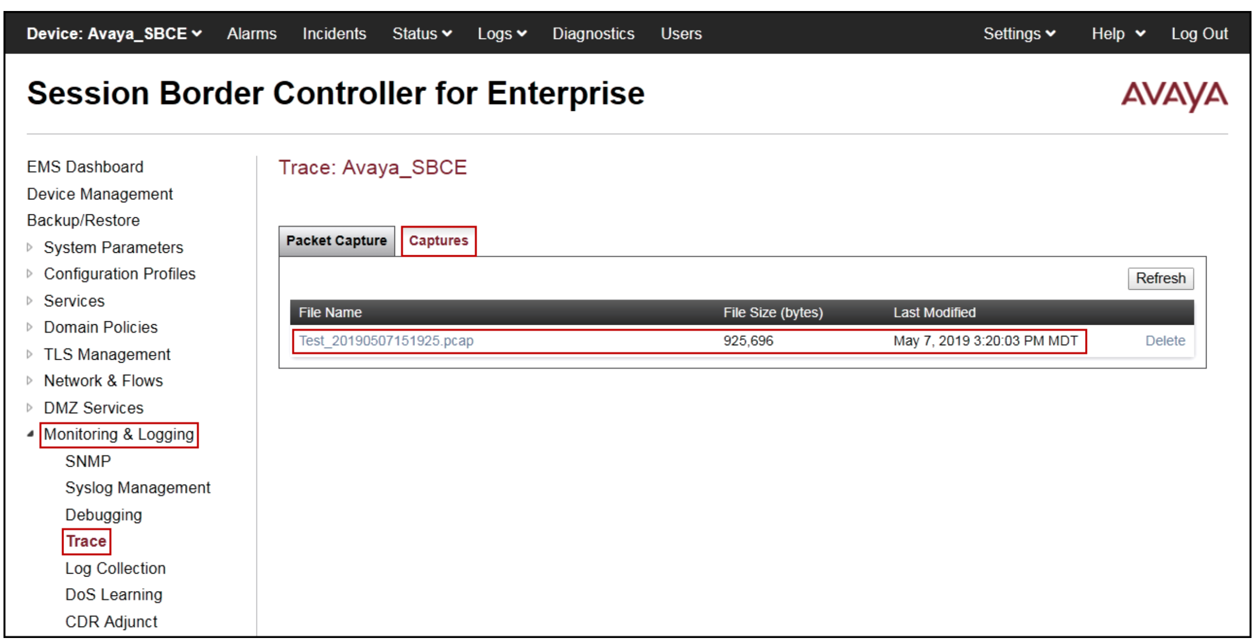
The following screen shows the Diagnostics page with the results of a ping test.



Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as pcap files. Navigate to **Monitor & Logging → → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.



Once the capture is stopped, click on the **Captures** tab and select the proper pcap file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.



10. Conclusion

These Application Notes describe the procedures required to configure Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 8.0 to connect to Telecom Liechtenstein SIP Trunking Services. Telecom Liechtenstein SIP Trunking Services is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

11. Additional References

This section references the documentation relevant to these Application Notes. Product documentation for Avaya IP Office, including the following, is available at: http://support.avaya.com/

[1] *Deploying IP Office Platform Server Edition Solution*, Release 11.0, May 2018

[2] *IP Office Platform 11.0, Deploying Avaya IP Office Servers as Virtual Machines*, January 2019

[3] *IP Office Platform 11.0, Deploying Avaya IP Office Essential Edition (IP500 V2)*, February 2019.

[4] *Administering Avaya IP Office Platform with Manager, Release 11.0 FP4*, February 2019.

[5] *Administering Avaya IP Office™ Platform with Web Manager, Release 11.0 FP4*, February 2019.

[6] *Deploying Avaya Session Border Controller* in a Virtualized Environment, Release 8.0, Issue 2, March 2019.

[7] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0, Issue 1, February 2019.

[8] *Planning for and Administering Avaya Equinox for Android, iOS, Mac and Windows, Release 3.4.8, November 2018*

[9] *Using Avaya Equinox for IP Office, Release 11.0 FP4*, February 2019

Additional Avaya IP Office documentation can be found at: http://marketingtools.avaya.com/knowledgebase/

12. Appendix A: SigMa Scripts

Following is the Signaling Manipulation scripts that was used in the configuration of the Avaya SBCE, **Section 7.3.3**. When adding these scripts as instructed in **Sections 7.3.4** enter a name for the script in the Title (e.g., ***Add_Privacy_Header***) and copy/paste the entire scripts shown below.

Title: Add_Privacy_Header

```
within session "INVITE"
{
 act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
  {
// fix anonymous
       if (%HEADERS["From"][1].URI.USER = "anonymous") then
       {
          if (exists(%HEADERS["Privacy"][1])) then
          {
             %do = "nothing";
             }
          else
          {
             %HEADERS["Privacy"][1] = "id";
             }
          }
       }
   }
```

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.