



## DevConnect Program

---

# Application Notes for Configuring Avaya IP Office Release 12.0 and Avaya Session Border Controller Release 10.2 to support Clearcom 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 12.0 and Avaya Session Border Controller Release 10.2 to support Clearcom SIP Trunking Service. These Application Notes update previously published Application Notes with newer versions of Avaya software.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consultative), 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.

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results .....	6
2.3.	Support .....	7
3.	Reference Configuration.....	7
4.	Equipment and Software Validated .....	10
5.	Avaya IP Office Primary Server Configuration.....	11
5.1.	Licensing .....	13
5.2.	System Settings .....	14
5.2.1.	System - LAN1 Tab.....	14
5.2.2.	System - Telephony Tab .....	18
5.2.3.	System - VoIP Tab.....	19
5.3.	IP Route.....	21
5.4.	SIP Line.....	22
5.4.1.	Creating a SIP Trunk from an XML Template.....	22
5.4.2.	SIP Line – SIP Line Tab .....	26
5.4.3.	SIP Line - Transport Tab .....	27
5.4.4.	SIP Line – Call Details Tab .....	28
5.4.5.	SIP Line - VoIP Tab .....	30
5.4.6.	SIP Line – SIP Advanced Tab .....	31
5.5.	IP Office Line – Primary Server .....	32
5.6.	Incoming Call Route .....	34
5.7.	Outbound Call Routing .....	36
5.7.1.	Short Codes and Automatic Route Selection.....	36
5.8.	Save IP Office Primary Server Configuration.....	38
6.	Avaya IP Office Expansion System Configuration .....	39
6.1.	Physical Hardware.....	40
6.2.	LAN Settings.....	41
6.3.	IP Route.....	42
6.4.	IP Office Line – IP500 V2 Expansion System.....	43
6.5.	Short Codes .....	45
6.6.	Automatic Route Selection – ARS.....	46
6.7.	Save IP Office Expansion System Configuration .....	47
7.	Configure Avaya Session Border Controller .....	48
7.1.	Log in Avaya SBC .....	48
7.2.	Device Management.....	50
7.3.	TLS Management.....	52
7.3.1.	Verify TLS Certificates – Avaya Session Border Controller .....	52
7.3.2.	Server Profiles.....	54
7.3.3.	Client Profiles .....	56
7.4.	Configuration Profiles .....	57

7.4.1.	Server Interworking – Avaya-IPO .....	57
7.4.2.	Server Interworking - SP-General .....	60
7.4.3.	SIP Server Configuration .....	64
7.4.4.	Routing Profiles .....	74
7.4.5.	Topology Hiding .....	78
7.5.	Domain Policies .....	82
7.5.1.	Application Rules.....	82
7.5.2.	Media Rules .....	84
7.5.3.	End Point Policy Groups.....	87
7.6.	Network & Flows Settings .....	91
7.6.1.	Network Management.....	91
7.6.2.	Media Interface .....	93
7.6.3.	Signaling Interface .....	95
7.6.4.	End Point Flows.....	98
8.	Clearcom SIP Trunking Service Configuration .....	102
9.	Verification Steps.....	103
9.1.	IP Office System Status.....	103
9.2.	Monitor.....	105
9.3.	Avaya Session Border Controller.....	106
10.	Conclusion .....	111
11.	Additional References.....	111

# 1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Clearcom 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 12.0 (hereafter referred to as IP Office), an Avaya Session Border Controller Release 10.2 (hereafter referred to as Avaya SBC) and various Avaya endpoints, listed in **Section 4**.

The Clearcom 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 “Clearcom” 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 Clearcom 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. 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, H.323, Digital and Analog telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider's network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323, Digital and Analog telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider's network.
- Incoming and outgoing PSTN calls to/from Avaya Workplace Client for Windows (SIP).
- Dialing plans including local calls, international calls, 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.729(a), G.711A and G.711MU, Clearcom 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.

**Note:** Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

Items not supported or not tested included the following:

- REFER message for call redirection was not tested for reasons noted under **Section 2.2**.
- T.38 and G.711 fax pass-through were not tested for reasons noted under **Section 2.2**.
- Inbound toll-free calls were not tested.
- 0, 0+10 digits, 911 Emergency and Local Directory Assistance calls were not tested.

## 2.2. Test Results

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

- **Call transfer to the PSTN using the SIP REFER method** – Calls from the PSTN to the enterprise that were transferred back to the PSTN network using the SIP REFER method did not work properly. REFER was left disabled in the Avaya IP Office for the tests (refer to **Sections 5.4.2**). With REFER disabled, blind, and attended call transfers to the PSTN were allowed to complete, with the caveat that the IP Office was not released from the call path, and two trunks circuits remained seized for the duration of the call.
- **Outbound Calling Party Number (CPN) Block** – Clearcom did not allow outbound calls with privacy enabled. When the IP Office user activated “Withhold Number” to enable user privacy on outbound calls, IP Office sent “anonymous” in the “From” header, while the caller information was still being sent in the “P-Asserted-Identity” header. Clearcom responded with a “403 PSTN calls are forbidden” message and the call was rejected.
- **Caller ID on inbound and outbound calls** – On calls originating from IP Office extensions to PSTN telephones, and from PSTN telephones to IP Office extensions, the caller ID number displayed at the terminating endpoint was always of the pilot number assigned by Clearcom to the SIP trunk, not of the specific number originating the call. This includes calls to “twinned” mobile phones, and calls that were forwarded or transferred back on the SIP trunk to the PSTN or IP Office. This may be a standard behavior in Mexico, it is listed here simply as an observation.
- **Fax support** – Fax calls using the T.38 protocol failed during the compliance test. G.711 pass-through fax was also tested, but it behaved unreliably. The issue related to G.711 pass-through fax failing 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. The issue related to T.38 fax calls failing is related to the PSTN carriers being used in Mexico, not all PSTN carriers in Mexico support T.38. This issue could be solved by Clearcom selecting and routing T.38 fax traffic via PSTN carriers that support T.38.
- **SIP OPTIONS Messages** – During the compliance test Clearcom did not send SIP OPTIONS messages to IP Office, IP Office did send SIP OPTION messages to Clearcom. This was sufficient to keep the SIP trunk up in service.

## 2.3. Support

For support on Clearcom systems visit the corporate Web page at: <http://www.clearcom.mx/>

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 Clearcom 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.
- 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 Workplace Client for Windows (SIP).

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

Located at the edge of the enterprise is the Avaya SBC. The Avaya SBC 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 SBC. The Avaya SBC provides network address translation at both the IP and SIP layers.

IP endpoints at the enterprise included Avaya 1100 Series IP Deskphones (with SIP firmware), Avaya J100 Series IP Deskphones (with SIP and H.323 firmware), Avaya Workplace Client for Windows (SIP), Avaya Digital and Analog Deskphones. IP endpoints were registered to the Primary Server; non IP endpoints (analog and digital) were registered to 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 SBC and Clearcom, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBC and IP Office, across the enterprise private IP network, is SIP over TLS.

For inbound calls, the calls flowed from Clearcom network to the Avaya SBC, then to IP Office.

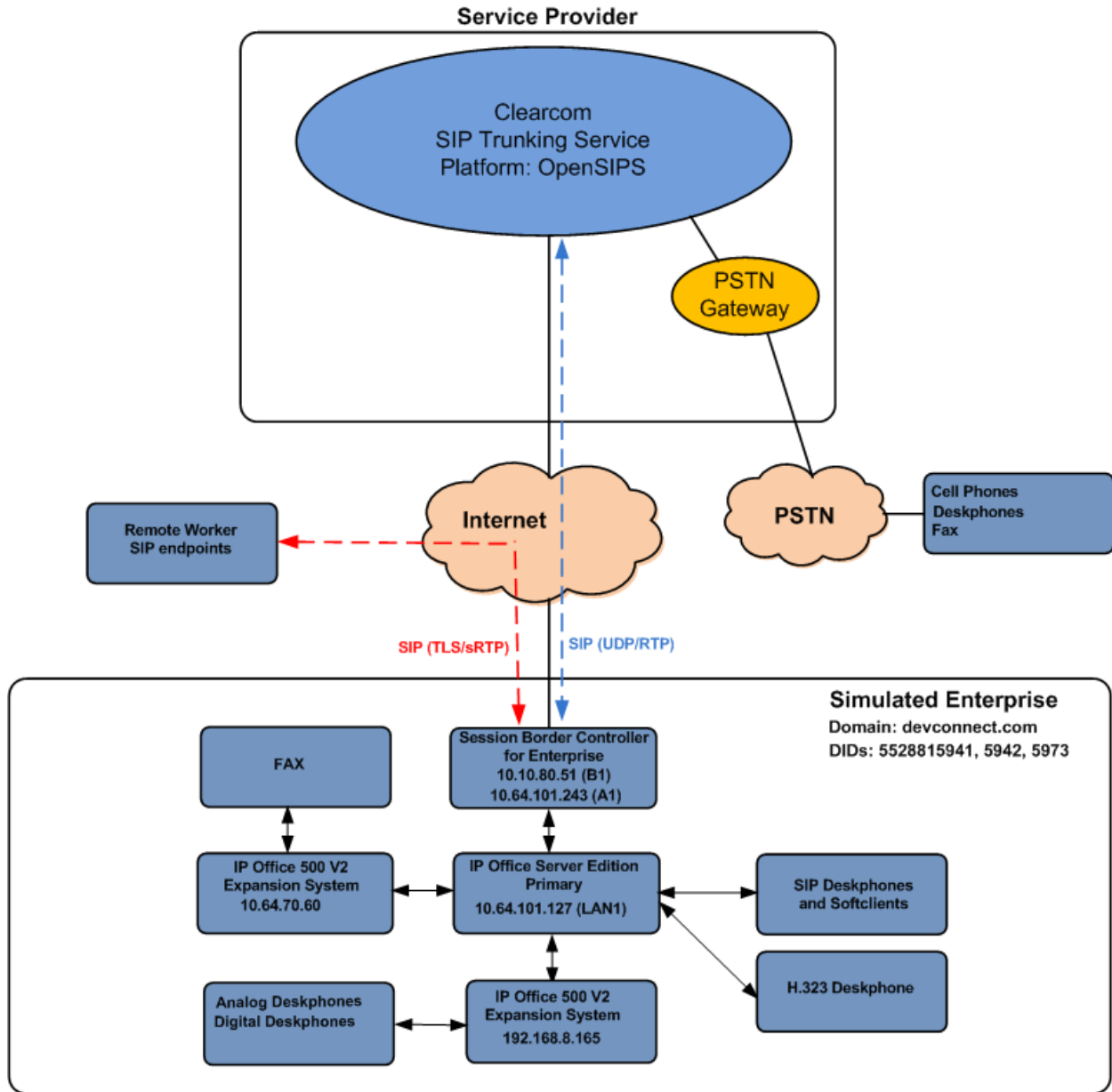
Outbound calls to the PSTN were first processed by IP Office. Once IP Office selected the proper SIP trunk, the call was routed to the Avaya SBC for egress to Clearcom network.

For the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Clearcom network. The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Clearcom network.

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

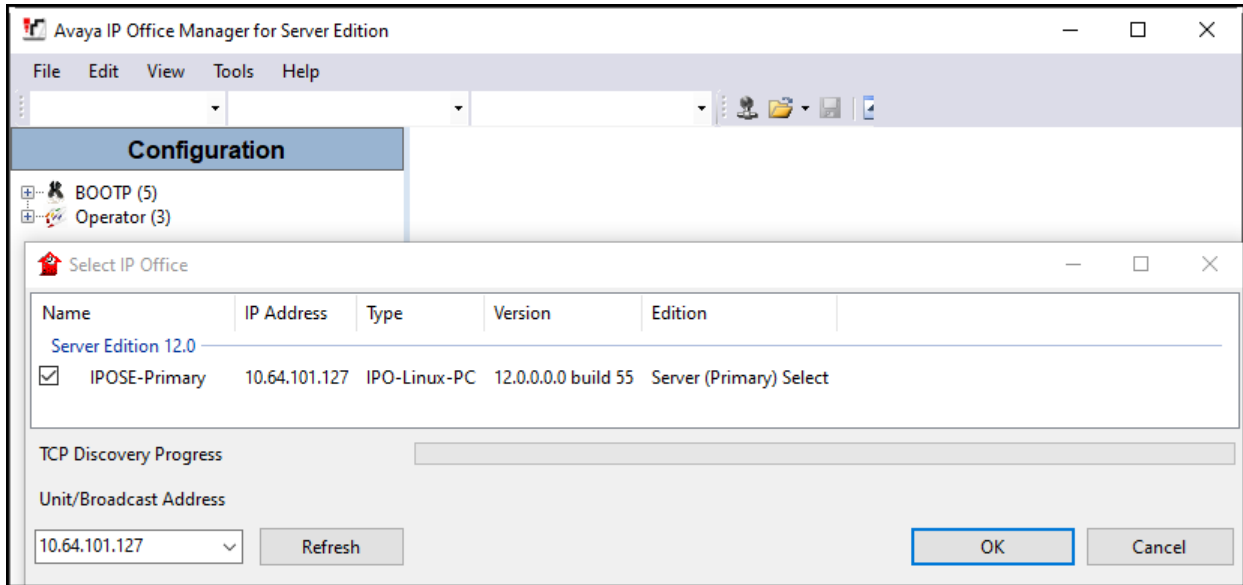
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya IP Office Server Edition (Primary Server)	12.0.0.0 Build 55
• Avaya IP Office Voicemail Pro	12.0.0.0 Build 14
Avaya IP Office IP500 V2 (Expansion Systems)	12.0.0.0 Build 55
Avaya IP Office Manager	12.0.0.0 Build 55
Avaya Session Border Controller	ASBC 10.2.0 0-86-2407
Avaya J179 IP Telephone (H.323)	6.8.5.5.1
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.0.10.3.2
Avaya 1408 Digital Telephone	48.02
Avaya Workplace Client for Windows (SIP).	3.36.0.137
Analog Telephone	---
<b>Clearcom</b>	
OpenSIPS Softswitch	2.6.6
OpenSIPS Session Border Controller	2.6.6

**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.

**Configuration** | **Server Edition**

**Summary**

Server Edition Primary

**Hardware Installed**

- Control Unit: IPO-Linux-PC
- Secondary Server: NONE
- Expansion Systems: 10.64.70.60; 192.168.8.165
- System Identification: bb2fda16200635373b6925fd6df8d37e291e5030

**System Settings**

- IP Address: 10.64.101.127
- Sub-Net Mask: 255.255.255.0
- System Locale: United States (US English)
- System Location: 3: Thornton, CO
- Device ID: NONE
- Number of Extensions on System: 6

Description	Name	Address	Primary Link	Secondary Link	Users Configured	Extensions Configured
Solution					32	54
Primary Server	IPOSE-Primary	10.64.101.127			6	6
Expansion System	IP500V2-One	192.168.8.165	Bothway		25	24
Expansion System	IP500V2-Two	10.64.70.60	Bothway		1	24

Ready

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.

The screenshot displays the Configuration Manager interface. On the left is the Navigation Pane with a tree view showing the hierarchy: Configuration > Solution > IPOSE-Primary > License (25). The main area shows the 'License Remote Server' configuration page. The 'License Mode' is set to 'License Normal' and the 'Licensed Version' is '12.0'. The 'PLDS Host ID' is empty, 'PLDS File Status' is 'Valid', and 'Select Licensing' is 'Valid'. Below this is a table of features and their licensing details.

Feature	Instances	Status	Expiration Date	Source
Customer Service Agent	20	Dormant	Never	PLDS Nodal
Customer Service Supervisor	20	Dormant	Never	PLDS Nodal
Avaya IP endpoints	1000	Valid	Never	PLDS Nodal
SIP Trunk Channels	256	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	1	Valid	Never	PLDS Nodal
Wave User	16	Obsolete	Never	PLDS Nodal
3rd Party IP Endpoints	1000	Valid	Never	PLDS Nodal
Server Edition	150	Valid	Never	PLDS Nodal
UMS Web Services	1000	Valid	Never	PLDS Nodal
Avaya Mac Softphone	1000	Valid	Never	PLDS Nodal

## 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), **LAN2** was not used.

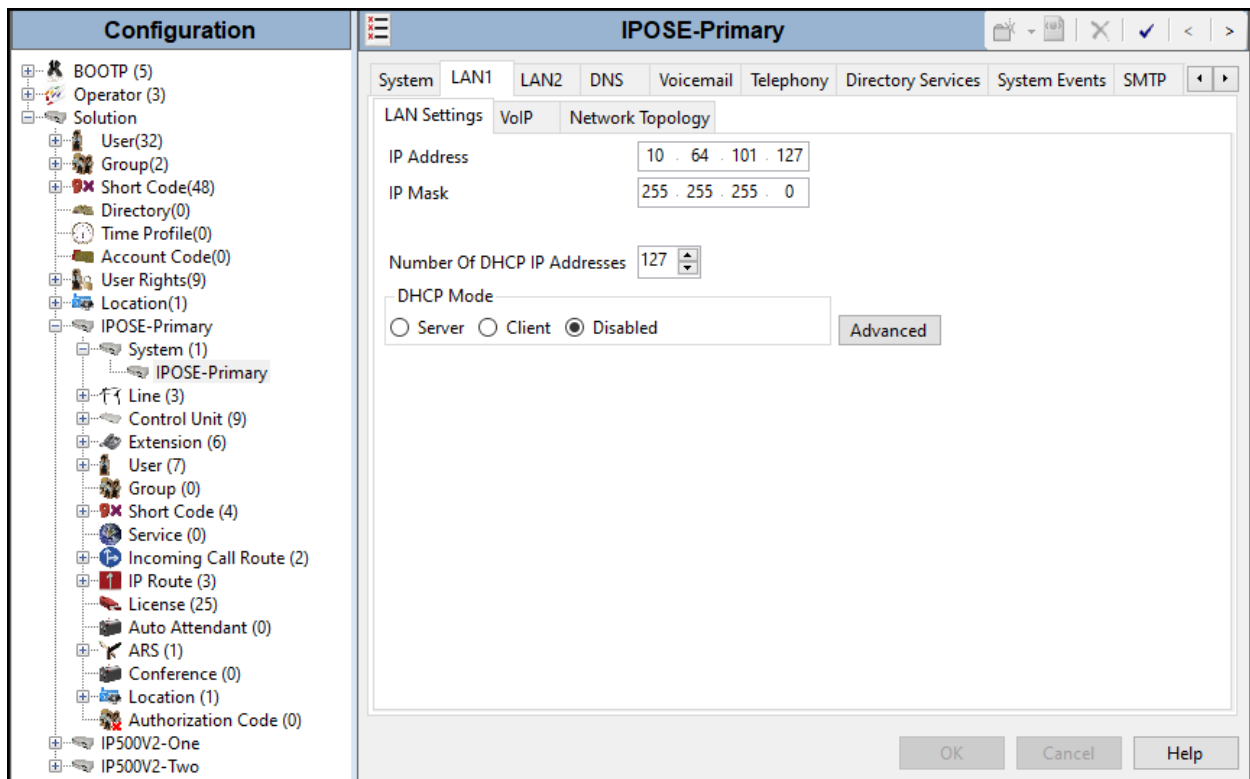
### 5.2.1. System - LAN1 Tab

In the sample configuration, **IPOSE-Primary** was used as the system name, the **LAN1** port connects to the inside interface (enterprise private network side) of the Avaya SBC across the enterprise LAN (private) network. The outside interface of the Avaya SBC connects to Clearcom network via the public internet. To access the **LAN1** settings, navigate to **System (1) → IPOSE-Primary** in the Navigation Pane.

#### 5.2.1.1 LAN1 LAN Settings tab

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

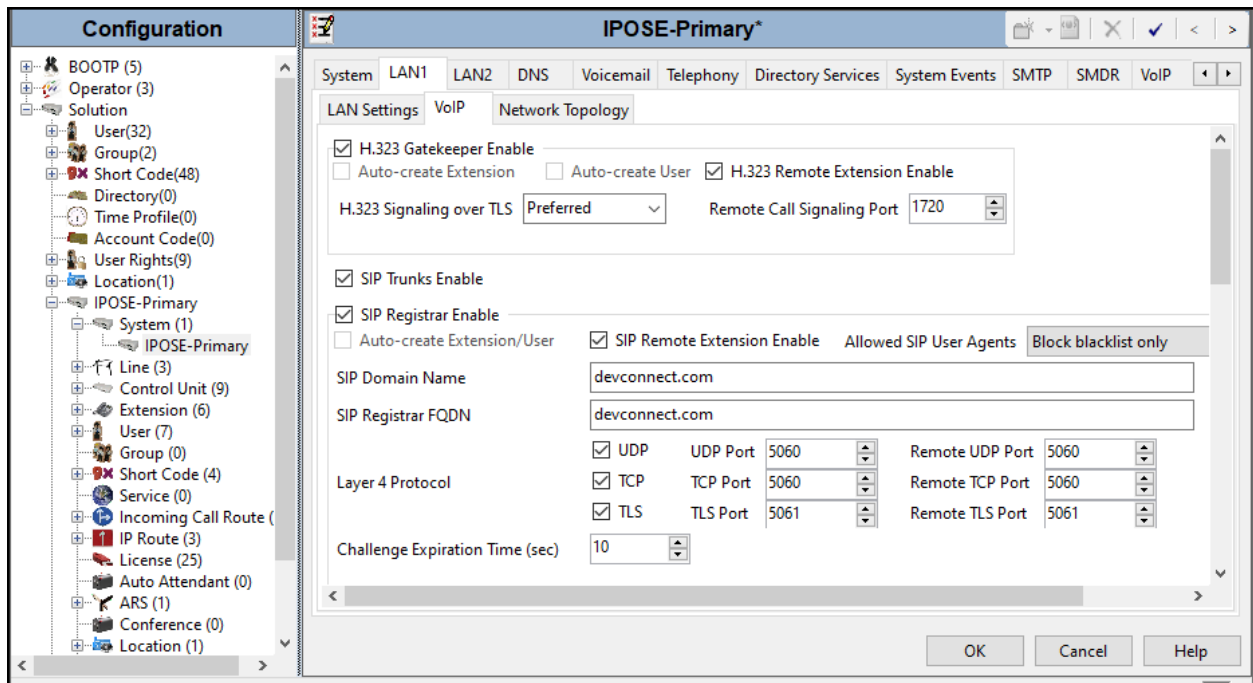
- Set the **IP Address** field to the LAN IP address, e.g., **10.64.101.127**.
- Set the **IP Mask** field to the subnet mask of the enterprise private network, e.g., **255.255.255.0**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit.



### 5.2.1.2 LAN1 VoIP Tab

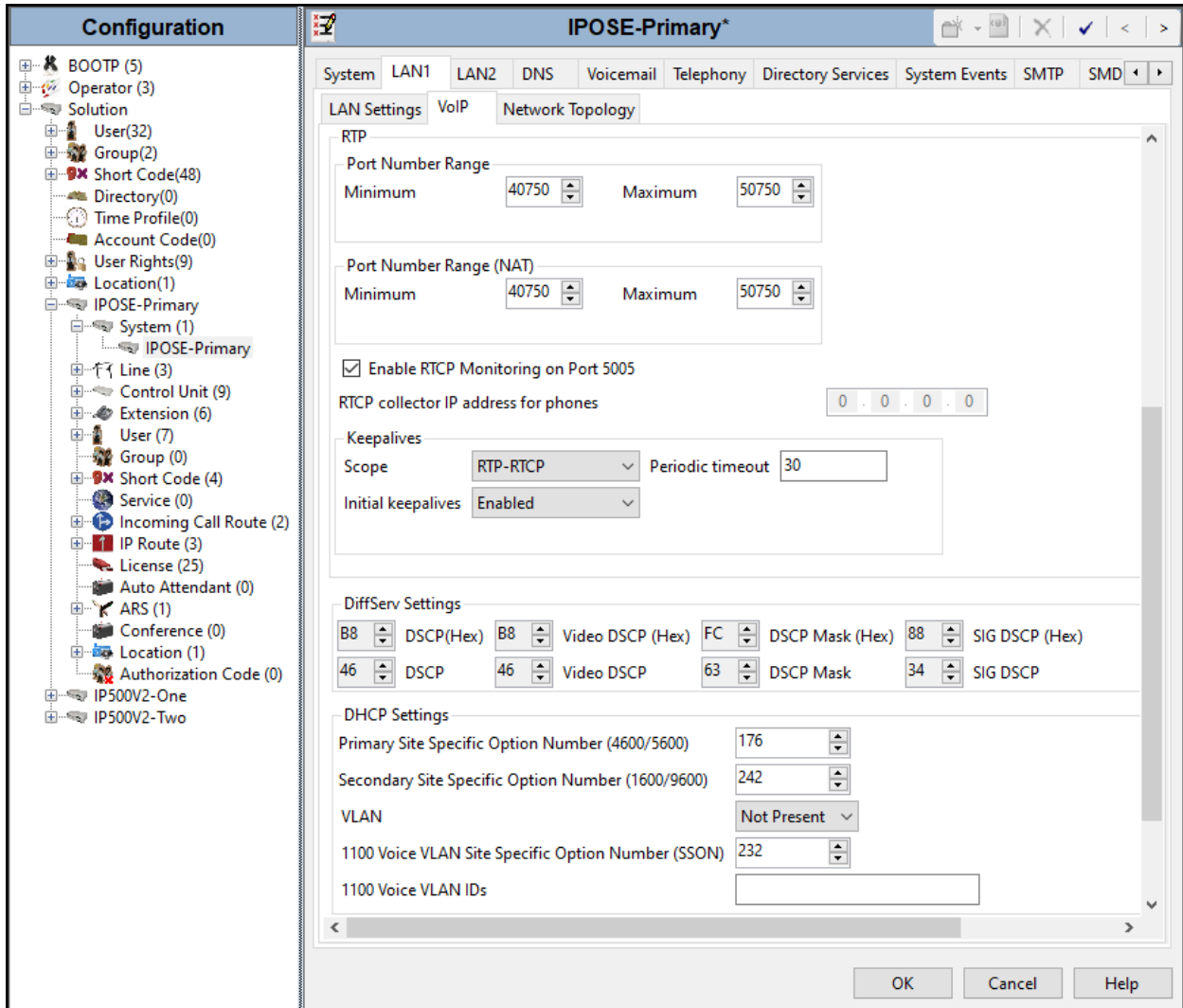
The VoIP tab as shown in the screenshot below was configured with following settings:

- 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, 9641 running firmware version 6.6 or higher and the Avaya J100 Series IP Deskphones.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Clearcom.
- 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** are set to **5061**.



Scroll down the page:

- 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.

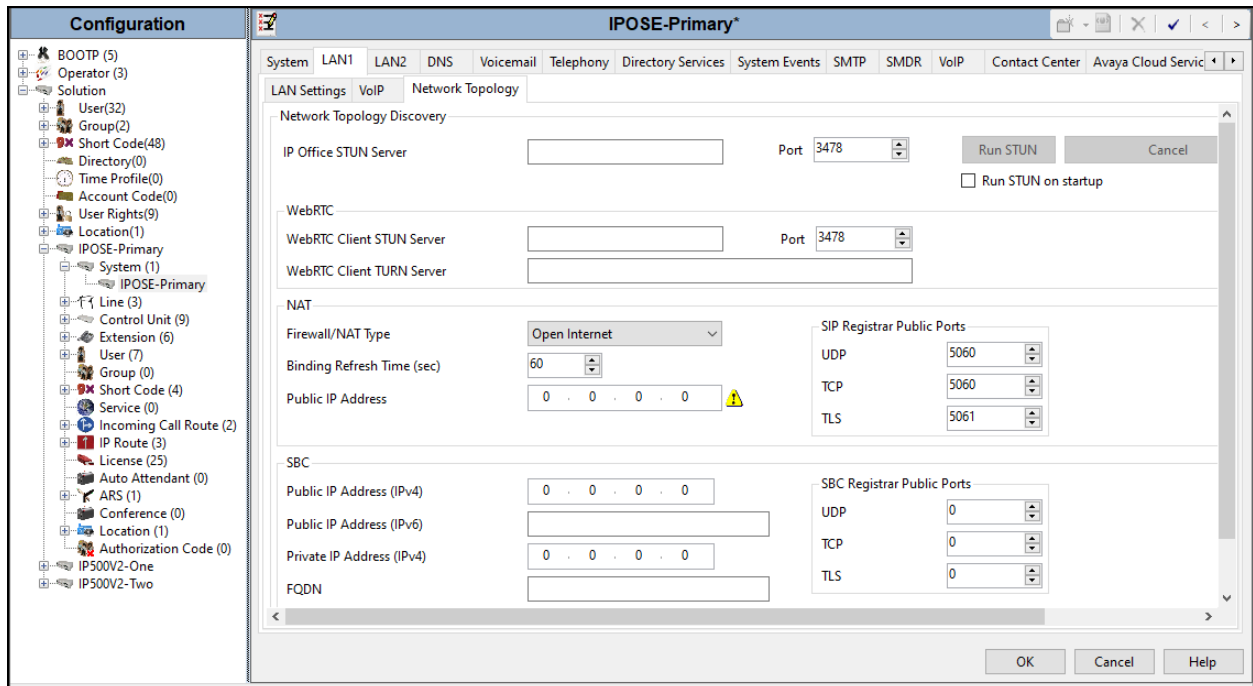




### 5.2.1.3 LAN1 Network Topology tab

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

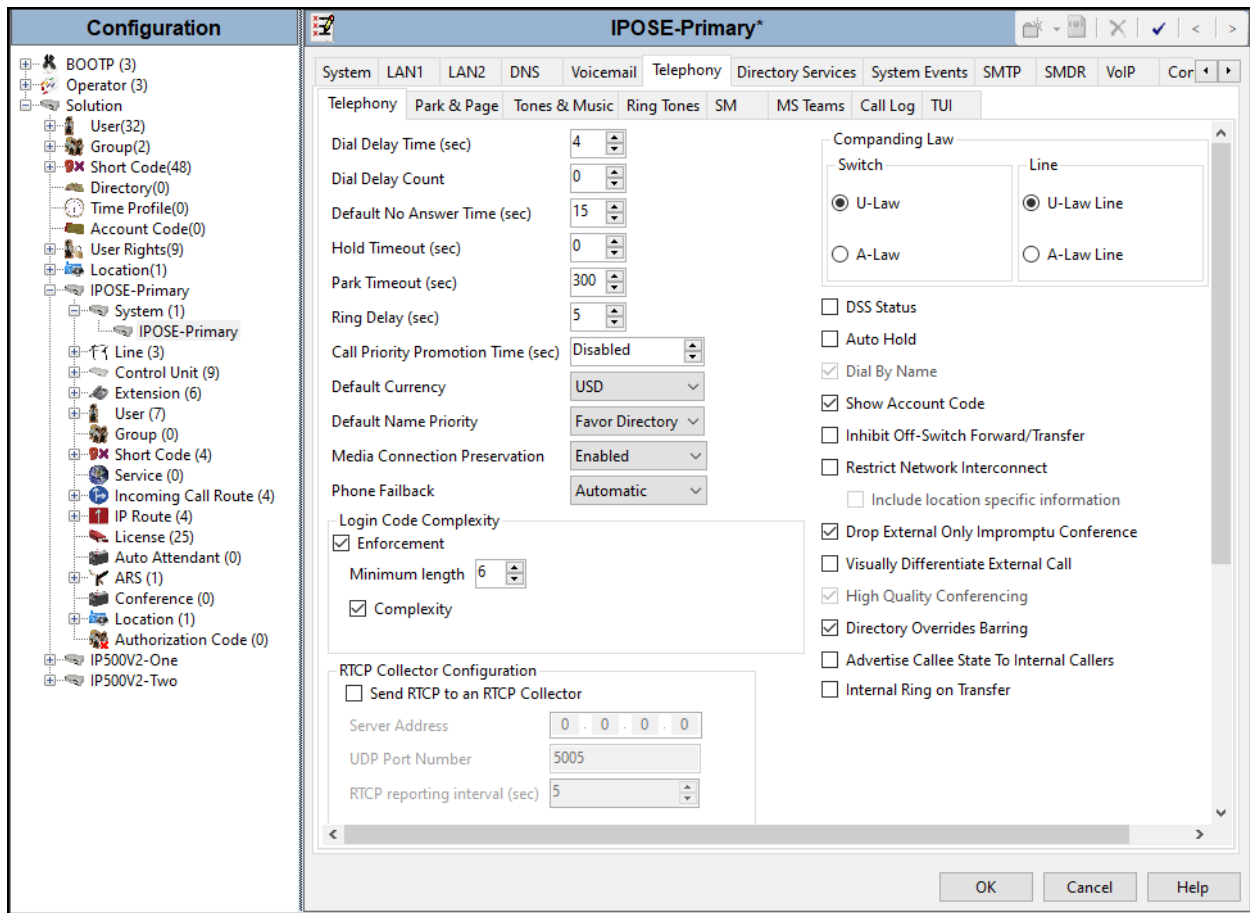
- The **Firewall/NAT Type** was set to **Open Internet** in the reference configuration.
- The **Binding Refresh Time (sec)** was set to **60** seconds. This is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages, to periodically check the status of the SIP lines configured on this interface.
- The **Public IP Address** and **Public Port** sections are not used.
- Click **OK** to commit.



## 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; **U-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.



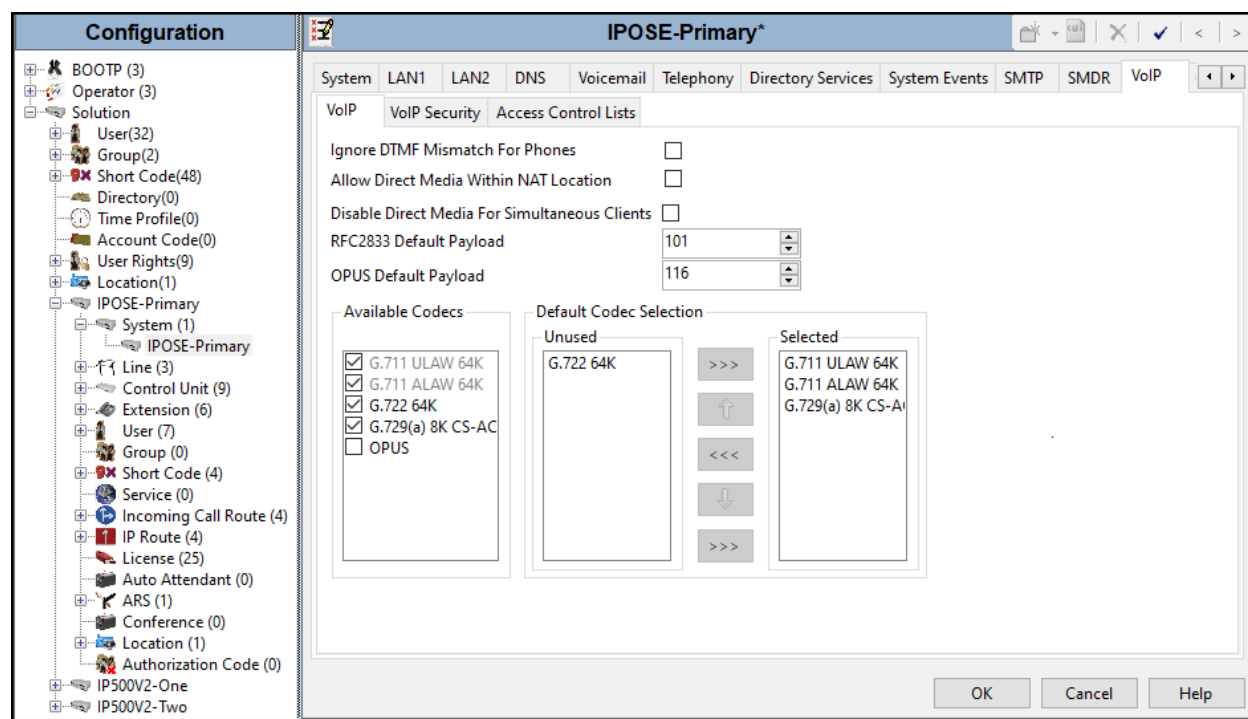
### 5.2.3. System - VoIP Tab

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.



**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.

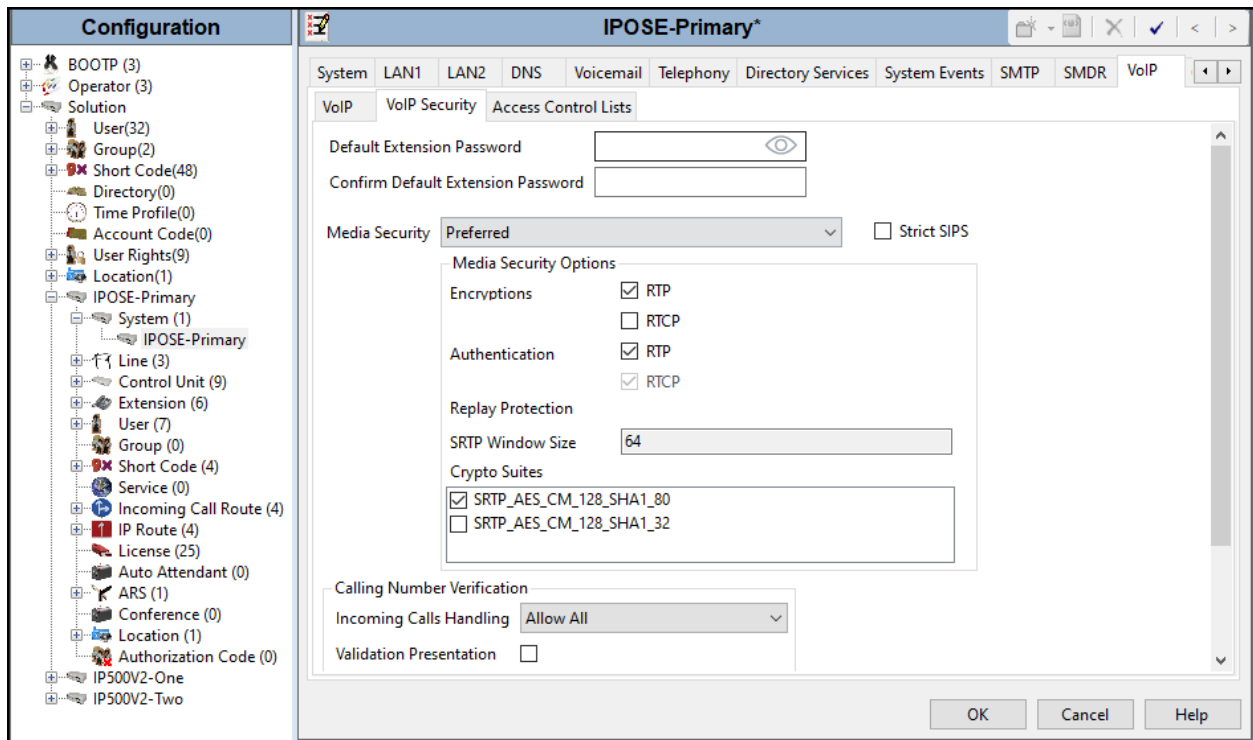
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

- 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.

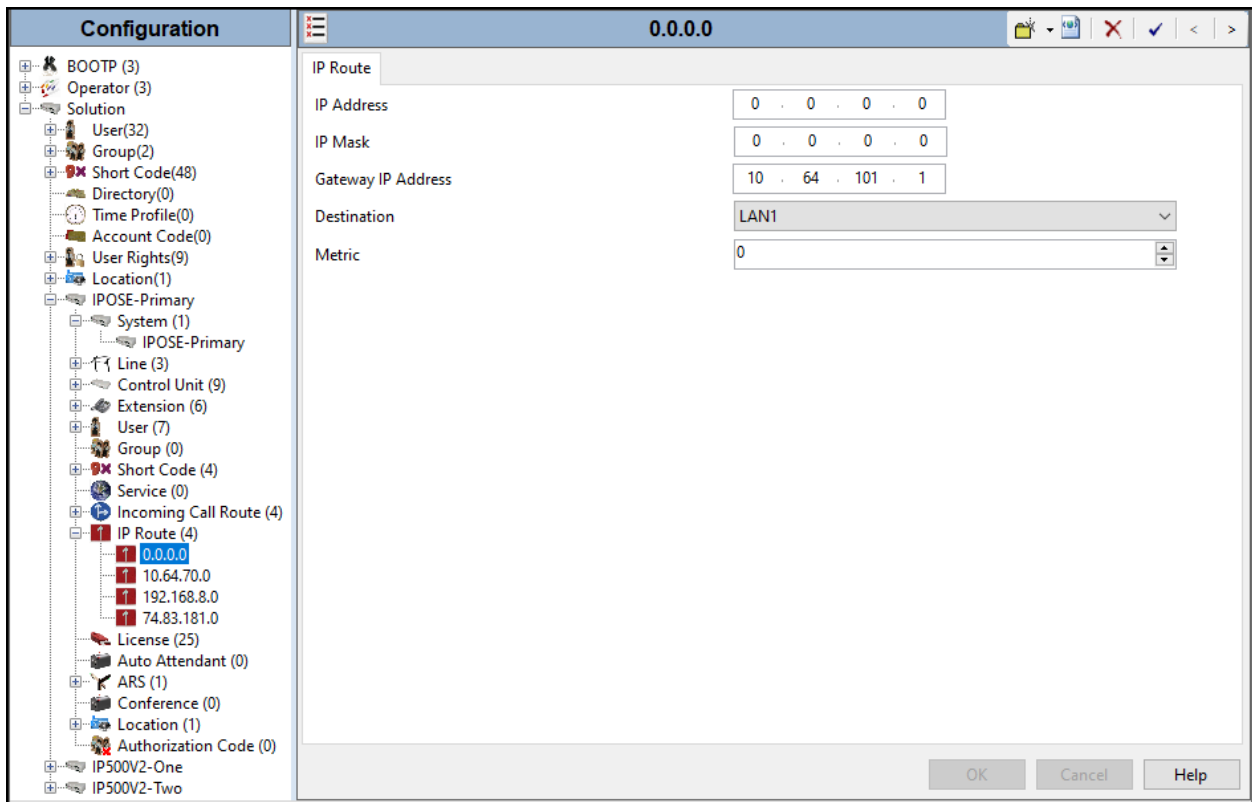


### 5.3. IP Route

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 Clearcom 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.



## 5.4. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Clearcom. 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

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**.

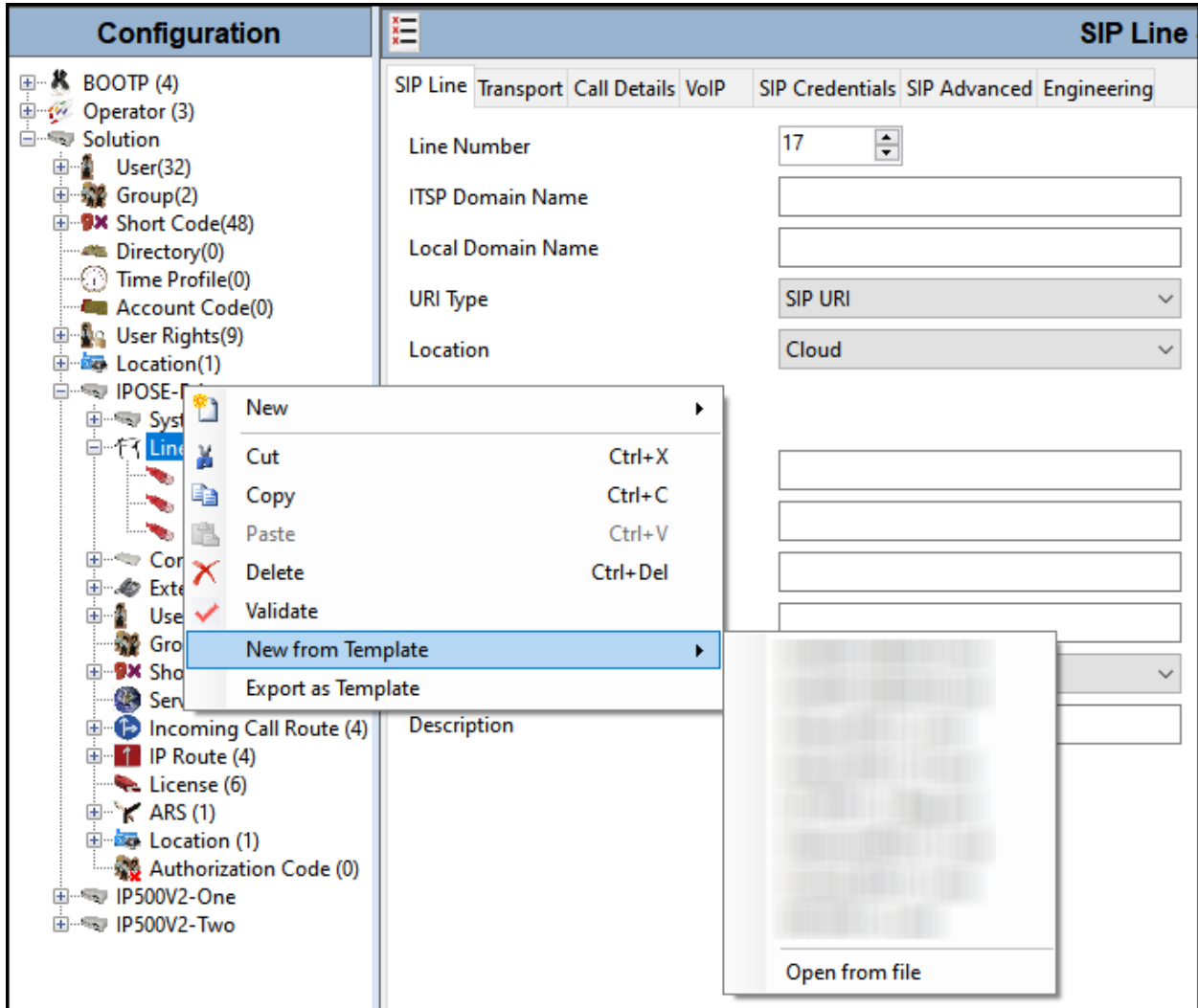
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New** → **SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.6**.

### 5.4.1. Creating a SIP Trunk from an XML Template

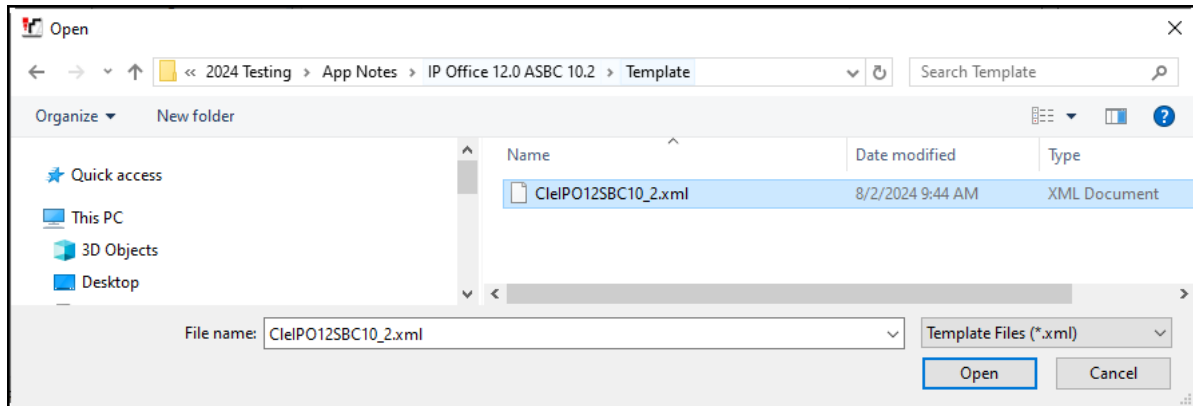
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and 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.

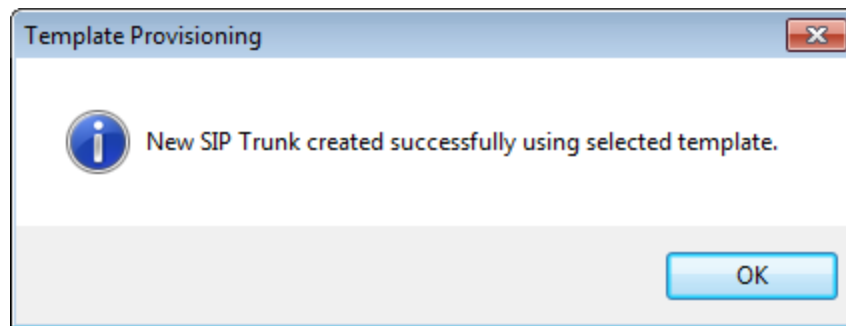
To create the SIP Trunk from the template, from the **Primary** server, right-click on **Line** in the Navigation Pane, then navigate to **New** → **New from Template** → **Open from file**.



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

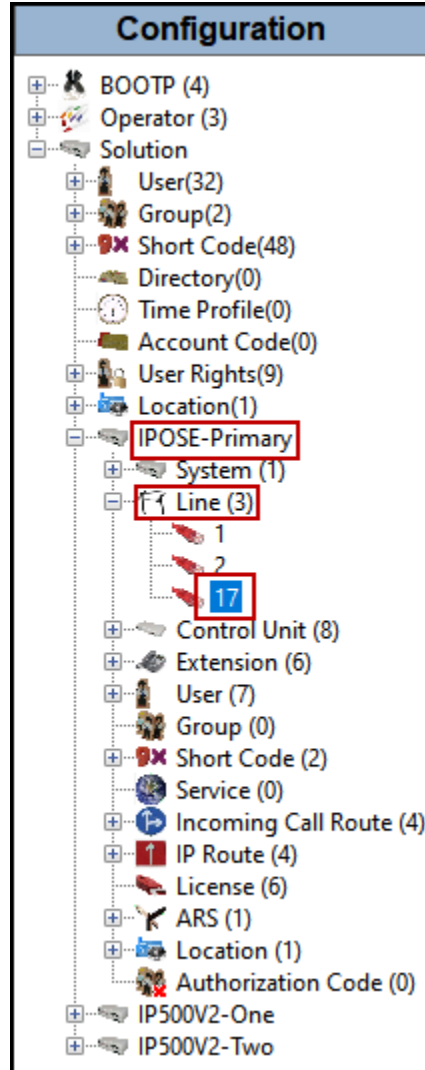


After the import is complete, a final import status pop-up window will open stating success or failure. Click **OK**.





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:

- Leave the **ITSP Domain Name** blank. Note that if this field is left blank, then IP Office inserts the ITSP Proxy Address from the Transport tab as the ITSP Domain in the SIP messaging.
- 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**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never** (refer to Section 2.2).
- Click **OK** to commit.

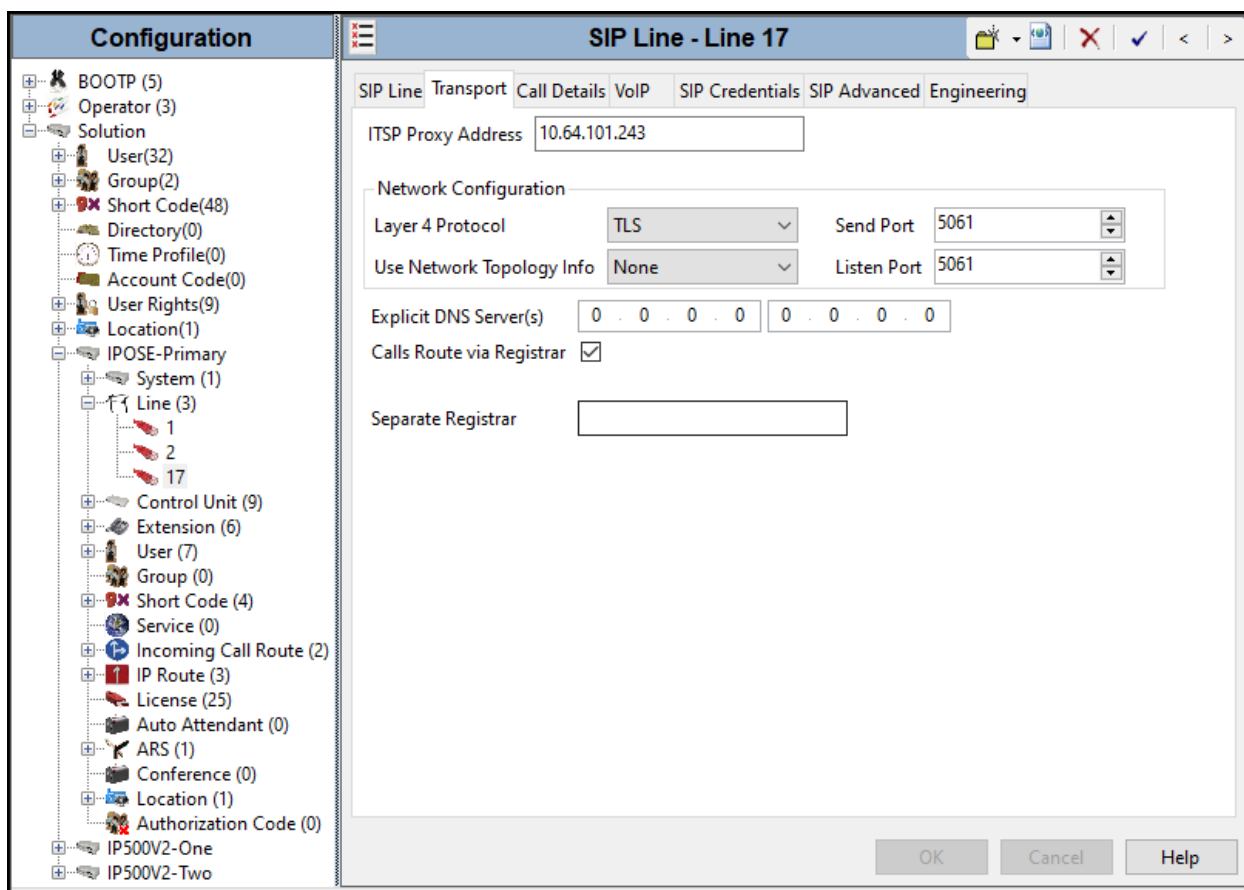
The screenshot displays the configuration window for 'SIP Line - Line 17'. The 'SIP Line' tab is selected, showing the following configuration details:

Field	Value	Field	Value
Line Number	17	In Service	<input checked="" type="checkbox"/>
ITSP Domain Name		Check OOS	<input checked="" type="checkbox"/>
Local Domain Name		Session Timers	
URI Type	SIP URI	Refresh Method	Auto
Location	Cloud	Timer (sec)	On Demand
Prefix		Redirect and Transfer	
National Prefix		Incoming Supervised REFER	Never
International Prefix		Outgoing Supervised REFER	Never
Country Code		Send 302 Moved Temporarily	<input type="checkbox"/>
Name Priority	System Default	Outgoing Blind REFER	<input type="checkbox"/>
Description	Service Provider		

### 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 SBC 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.



**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 two new entries were added, one for incoming calls and one for outgoing calls.

- Associate this entry 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 from this line. For the compliance test outgoing group **17** was used. Leave the **Incoming Group** field as 0.
- Under **Credentials**, select **0: <None>** from the pull-down menu.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Check the **P Asserted ID** and **Diversion Header**.
- Set the **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** fields to the values shown in the screenshot below. Note that the user name used under **SIP Credential** (Section 5.4.4) was used under the **Display** and **Content** columns for **Local URI**, this setting is needed since Clearcom required the user name to be sent in the “From” header.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.

The screenshot shows the configuration window for SIP Line - 17 | Call Details | SIP URI. The 'New URI' section includes:

- Incoming Group: 0
- Max Sessions: 10
- Outgoing Group: 17
- Credentials: 0: <None>

The main configuration area has the following fields:

	Display	Content
Local URI	user123	user123
Contact	Auto	Auto
P Asserted ID	<input checked="" type="checkbox"/> Auto	<input checked="" type="checkbox"/> Auto
P Preferred ID	<input type="checkbox"/> None	<input type="checkbox"/> None
Diversion Header	<input checked="" type="checkbox"/> Auto	<input checked="" type="checkbox"/> Auto
Remote Party ID	<input type="checkbox"/> None	<input type="checkbox"/> None

The 'Field meaning' table is as follows:

	Outgoing Calls	Forwarding/Twinning	Incoming Calls
Local URI	Explicit	Explicit	Explicit
Contact	Caller	Original Caller	Called
P Asserted ID	Caller	Original Caller	Called
P Preferred ID	None	None	None
Diversion Header	None	Caller	None
Remote Party ID	None	None	None

Buttons: OK, Cancel, Help

The entry for calls from the PSTN to IP Office (incoming calls) was created with the parameters shown below:

- Associate this entry to an incoming line group using the **Incoming Group** field. For the compliance test incoming group **17** was used. The **Outgoing Group** field was set to **100**, since it cannot be set to 0 in IP Office Server Edition systems, this is an arbitrary number.
- 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>** (SIP Trunk registration is being done at the Avaya SBC).
- For the **Local URI** and **Contact**, set the selections under the **Display** and **Content** columns to **Auto**.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.
- Click **OK** to commit again (not shown).

The screenshot shows the 'SIP Line - 17 | Call Details | SIP URI' configuration window. The 'New URI' section includes:
 

- Incoming Group: 17
- Outgoing Group: 100
- Credentials: 0: <None>
- Max Sessions: 10

 Below this, there are two columns: 'Display' and 'Content'. The 'Local URI' and 'Contact' fields are both set to 'Auto' in both columns. Other fields like 'P Asserted ID', 'P Preferred ID', 'Diversion Header', and 'Remote Party ID' are set to 'None' with checkboxes. To the right, a 'Field meaning' table is visible:
 

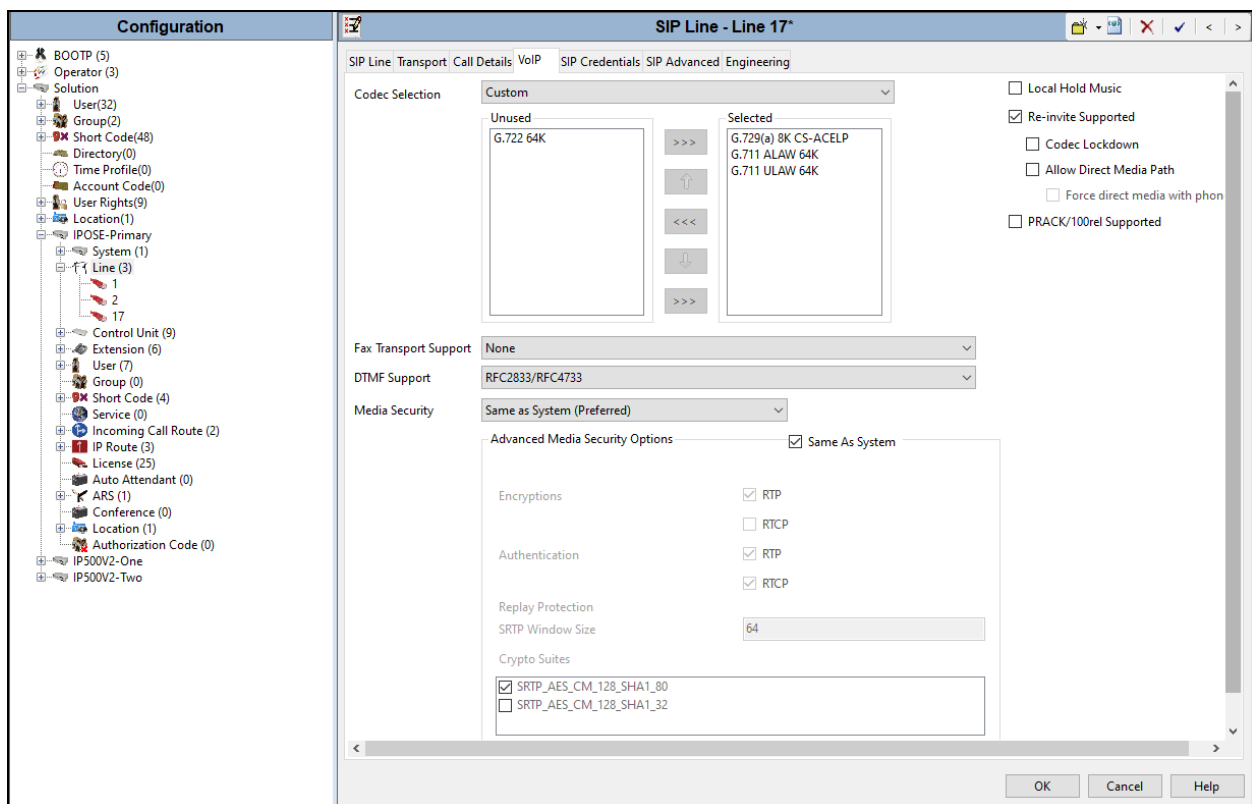
	Outgoing Calls	Forwarding/Twining	Incoming Calls
Local URI	Caller	Original Caller	Called
Contact	Caller	Original Caller	Called
P Asserted ID	None	None	None
P Preferred ID	None	None	None
Diversion Header	None	None	None
Remote Party ID	None	None	None

 At the bottom right, there are 'OK', 'Cancel', and 'Help' buttons.

### 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. Clearcom supports codecs **G.729(a)**, **G.711ALAW** and **G.711ULAW** for audio.
- Select **None** 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)**.
- On the **Advanced Media Security Options** check **Same As System (Preferred)**.
- Check the **Re-invite Supported** box.
- Verify **PRACK/100rel Supported** box is **unchecked**.
- Default values may be used for all other parameters.
- Click the **OK** to commit.



**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).

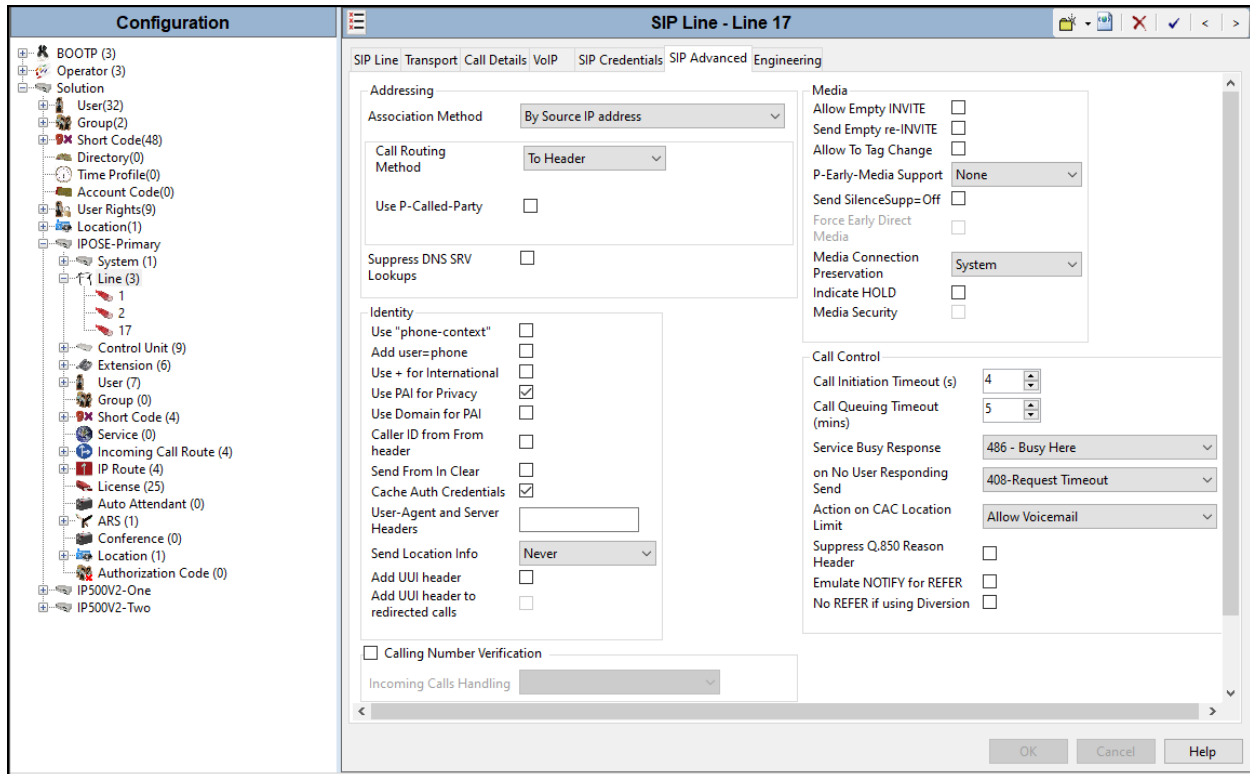
## 5.4.6. SIP Line – SIP Advanced Tab

In the **Addressing** area:

- Select **To Header** for **Call Routing Method**.

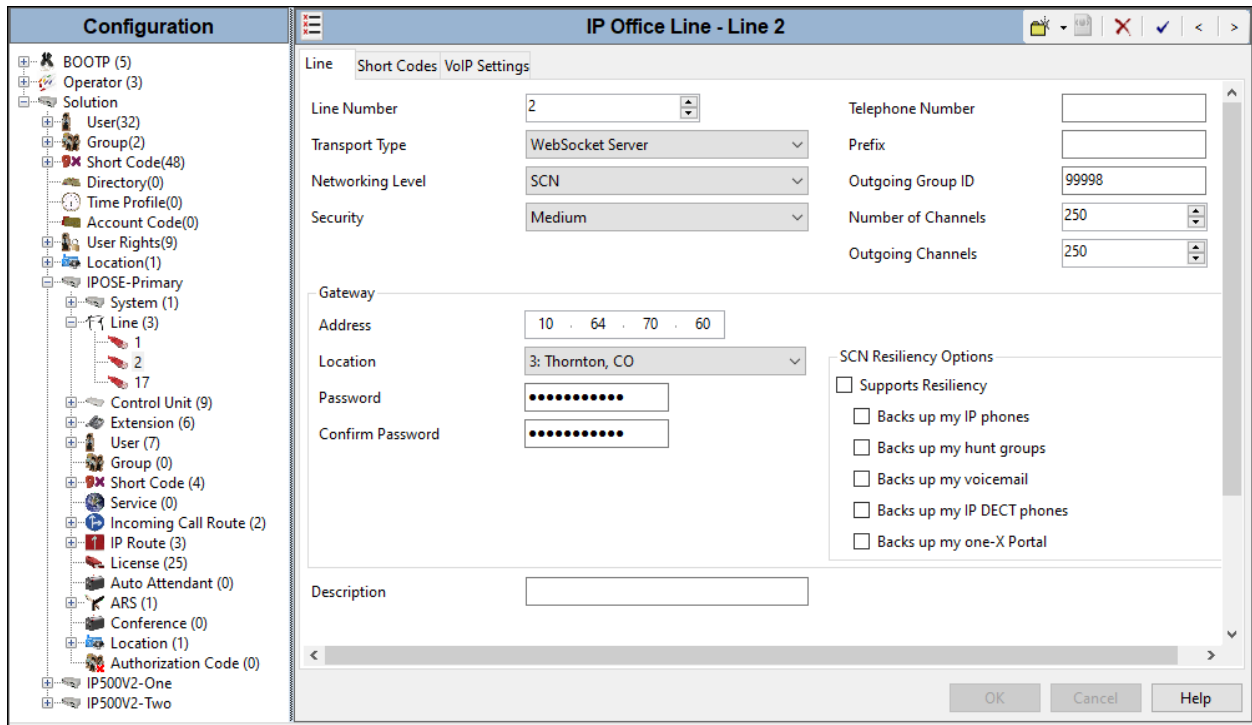
In the **Identity** area:

- Check the box for **Use PAI for Privacy**.
- Default values may be used for all other parameters.
- Click **OK** to commit.



## 5.5. IP Office Line – Primary Server

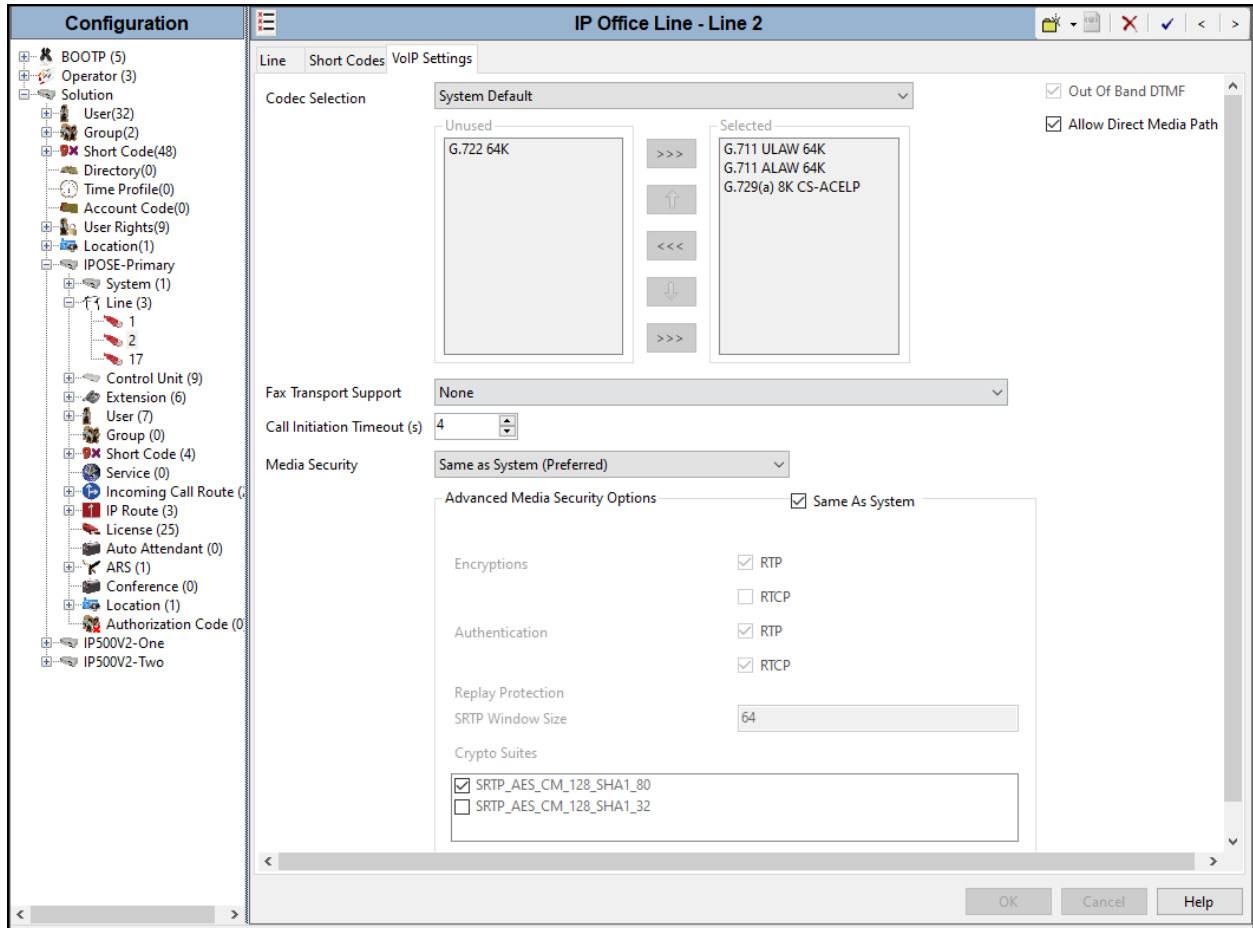
In IP Office Server Edition systems, IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate line to be configured in the Group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





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

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **None** for **Fax Transport Support** (refer to Section 2.2).
- Under **Media Security** verify **Same as System (Preferred)** is selected (default value).
- On the **Advanced Media Security Options** check **Same As System**.



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 Capability** 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 Clearcom.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'Configuration' tree, and on the right is the configuration details pane for the selected item '17 5528815941'.

**Configuration Tree (Left):**

- BOOTP (4)
- Operator (3)
- Solution
  - User(32)
  - Group(2)
  - Short Code(48)
  - Directory(0)
  - Time Profile(0)
  - Account Code(0)
  - User Rights(9)
  - Location(1)
  - IPOSE-Primary
    - System (1)
    - Line (3)
      - Control Unit (8)
      - Extension (6)
        - User (7)
          - Group (0)
          - Short Code (2)
          - Service (0)
            - Incoming Call Route (4)**
              - 17 5528815941** (selected)
              - 17 5528815942
              - 17 5528815973
              - 17 5528815974

- IP Route (4)
- License (6)
- ARS (1)
- Location (1)
- Authorization Code (0)
- IP500V2-One
- IP500V2-Two

**Configuration Details Pane (Right):**

17 5528815941

Standard | Voice Recording | Destinations

Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	5528815941
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

Select the **Destinations** tab. From the **Destination** drop-down menu, select the IP Office extension associated with this DID number. In the reference configuration, the DID number 5528815941 provided by Clearcom was associated with the Avaya IP Office extension **3041**.

The screenshot shows the Avaya configuration interface for DID 17 5528815941. The left sidebar displays a tree view of configuration objects, including Incoming Call Routes for the specified DID. The main panel shows the 'Destinations' tab with a table containing one row:

TimeProfile	Destination	Fallback Extension
Default Value	3041 Ext3041 H323	~

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**, **Mexico (Latin Spanish)** was used.
- Click the **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left is a navigation tree under 'Configuration' with various categories like BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line, Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, and IP500V2-One/Two. The 'Short Code' category is expanded, showing a list of short codes, with '9N' selected and highlighted in blue. On the right, the configuration details for '9N: Dial' are shown in a form. The fields are: Code (9N), Feature (Dial), Telephone Number (N), Line Group ID (50: Main), Locale (Mexico (Latin Spanish)), Force Account Code (checkbox), and Force Authorization Code (checkbox).

Configuration		9N: Dial	
Short Code			
Code	9N		
Feature	Dial		
Telephone Number	N		
Line Group ID	50: Main		
Locale	Mexico (Latin Spanish)		
Force Account Code	<input type="checkbox"/>		
Force Authorization Code	<input type="checkbox"/>		

The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **Xs** 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. This type of setting results in a much quicker response in the delivery of the call by IP Office.

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

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **001** followed by **10 Xs** to represent the exact number of digits.
- 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.
- For **Locale**, **Mexico (Latin Spanish)** was used
- Click **OK** to commit.

The following example shows the dial pattern for calls to the United States.

The screenshot shows a dialog box titled "Edit Short Code" with the following fields and values:

Code	001XXXXXXXXXX	OK
Feature	Dial	Cancel
Telephone Number	001N	
Line Group ID	17	
Locale	Mexico (Latin Spanish)	
Force Account Code	<input type="checkbox"/>	
Force Authorization Code	<input type="checkbox"/>	

The following example shows the dial pattern for local calls within Mexico.

The screenshot shows a dialog box titled "Edit Short Code" with the following fields and values:

Code	55XXXXXXXX	OK
Feature	Dial	Cancel
Telephone Number	55N	
Line Group ID	17	
Locale	Mexico (Latin Spanish)	
Force Account Code	<input type="checkbox"/>	
Force Authorization Code	<input type="checkbox"/>	

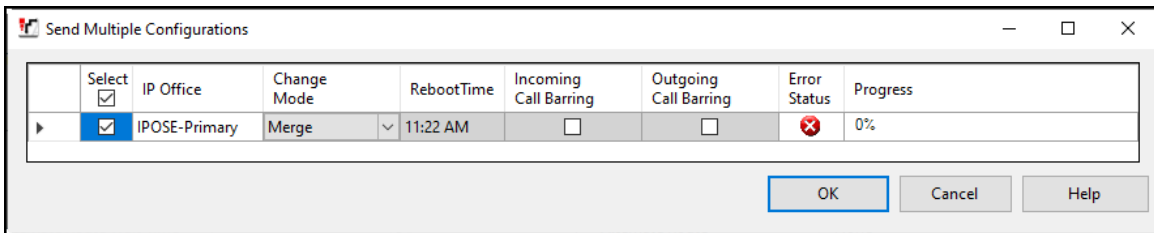
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

## 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 **Reboot** 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 **Reboot** 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-Two** on the left navigation pane will expand the menu on this server.

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'Configuration' tree, and on the right is the 'System Inventory' pane.

**Configuration Tree (Left):**

- BOOTP (5)
- Operator (3)
- Solution
  - User(32)
  - Group(2)
  - Short Code(48)
  - Directory(0)
  - Time Profile(0)
  - Account Code(0)
  - User Rights(9)
  - Location(1)
  - IPOSE-Primary
  - IP500V2-One
  - IP500V2-Two
    - System (1)
    - Line (19)
    - Control Unit (5)
    - Extension (24)
    - User (4)
    - Group (1)
    - Short Code (12)
    - Service (0)
    - RAS (1)
    - Incoming Call Route (4)
    - WAN Port (0)
    - Firewall Profile (1)
    - IP Route (2)
    - License (25)
    - Tunnel (0)
    - ARS (2)
    - Location (1)
    - Authorization Code (0)

**System Inventory (Right):**

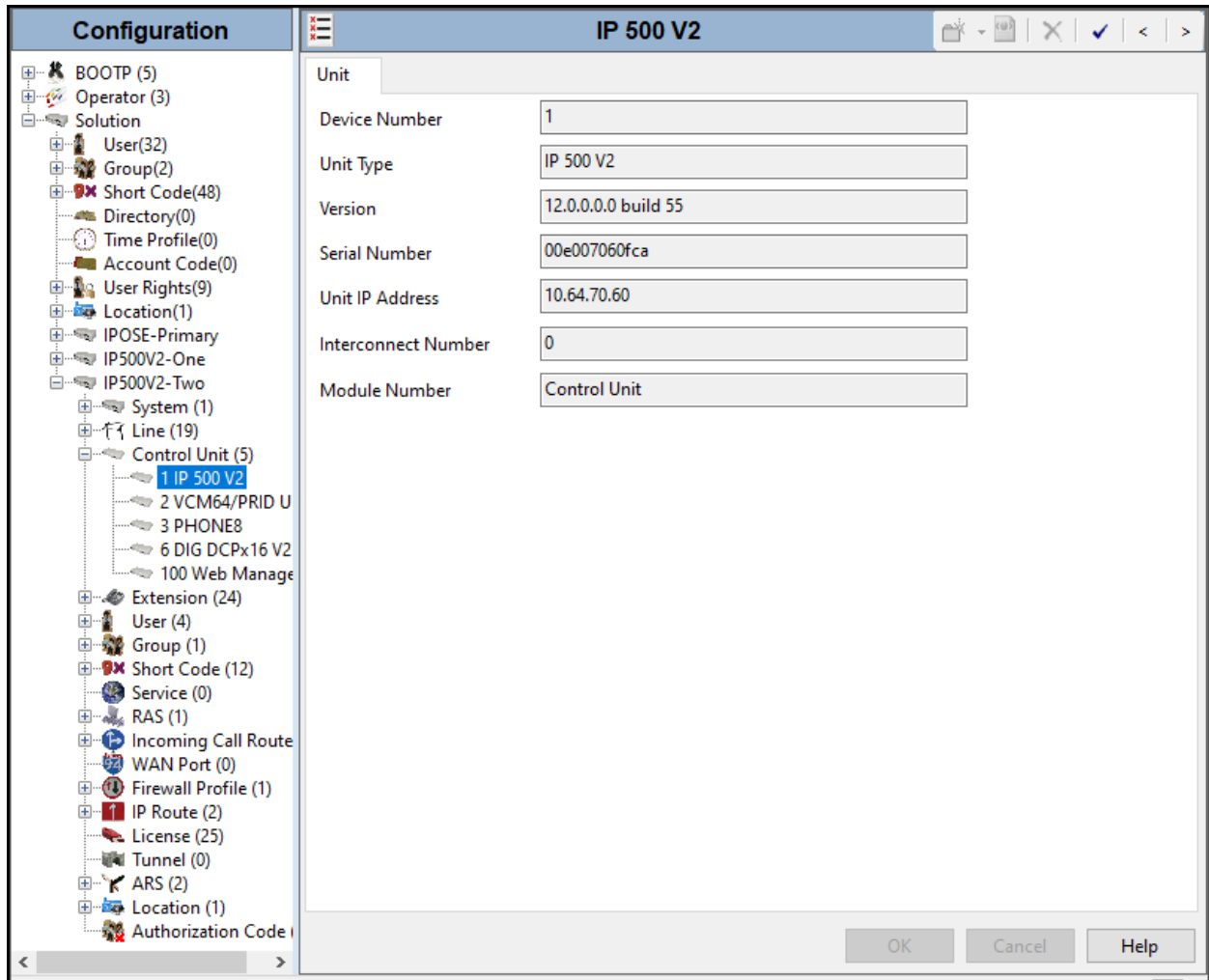
Server Edition Expansion System

- Hardware Installed**
  - Control Unit: IP 500 V2
  - Internal Modules: VCM64/PRID U; PHONE8; Web Manager
  - Expansion Modules: DIG DCPx16 V2
- System Settings**
  - IP Address: 10.64.70.60
  - Sub-Net Mask: 255.255.255.0
  - System Locale: United States (US English)
  - System Location: 3: Thornton, CO
  - Device ID: NONE
  - Number of Extensions on System: 24
- Features Configured**
  - Licenses Installed: Server Edition(1); IP Office Select(1); Receptionist(10); Additional Voice
  - Connected Extensions: NONE
  - Users NOT Configured for Voicemail: NONE
  - Users assigned as Ex-Directory: NONE
  - Users assigned for Twinning: NONE
  - Users barred from making Outgoing Calls: NONE
  - Music on Hold: WAV File

Ready

## 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.

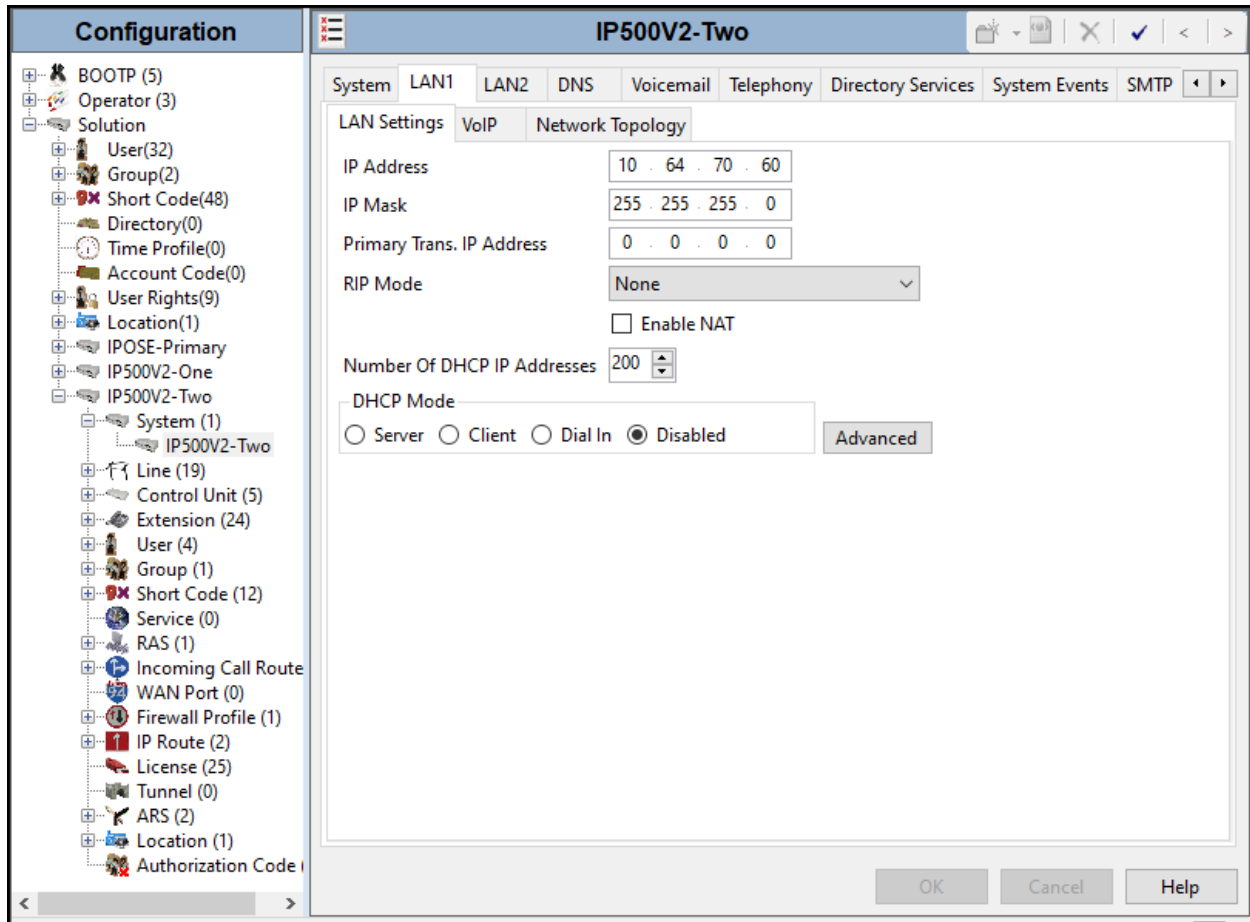




## 6.2. LAN Settings

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

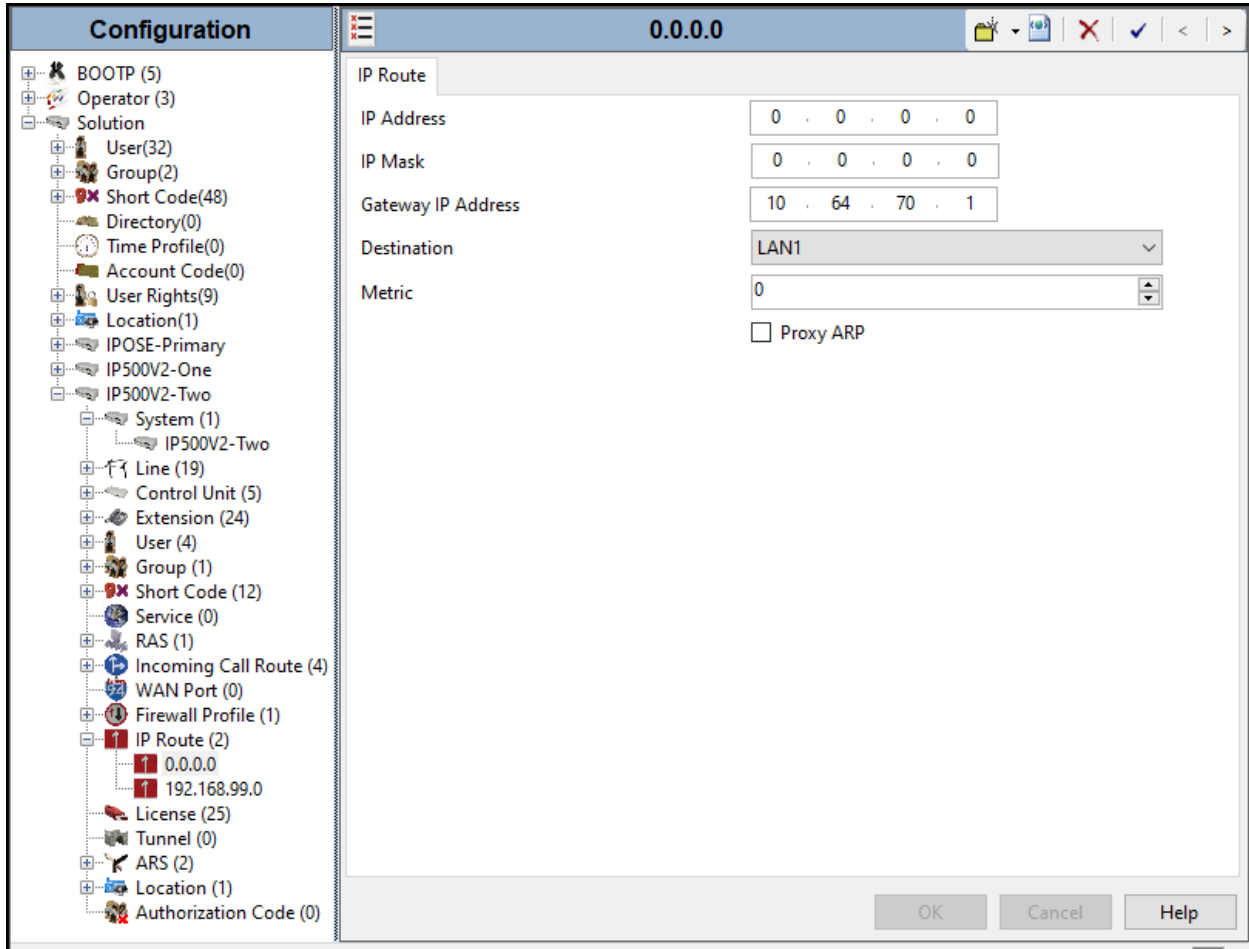


Default values were used on the **VoIP** and **Network Topology** tabs (not shown).

### 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 **10.64.70.1**
- 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.

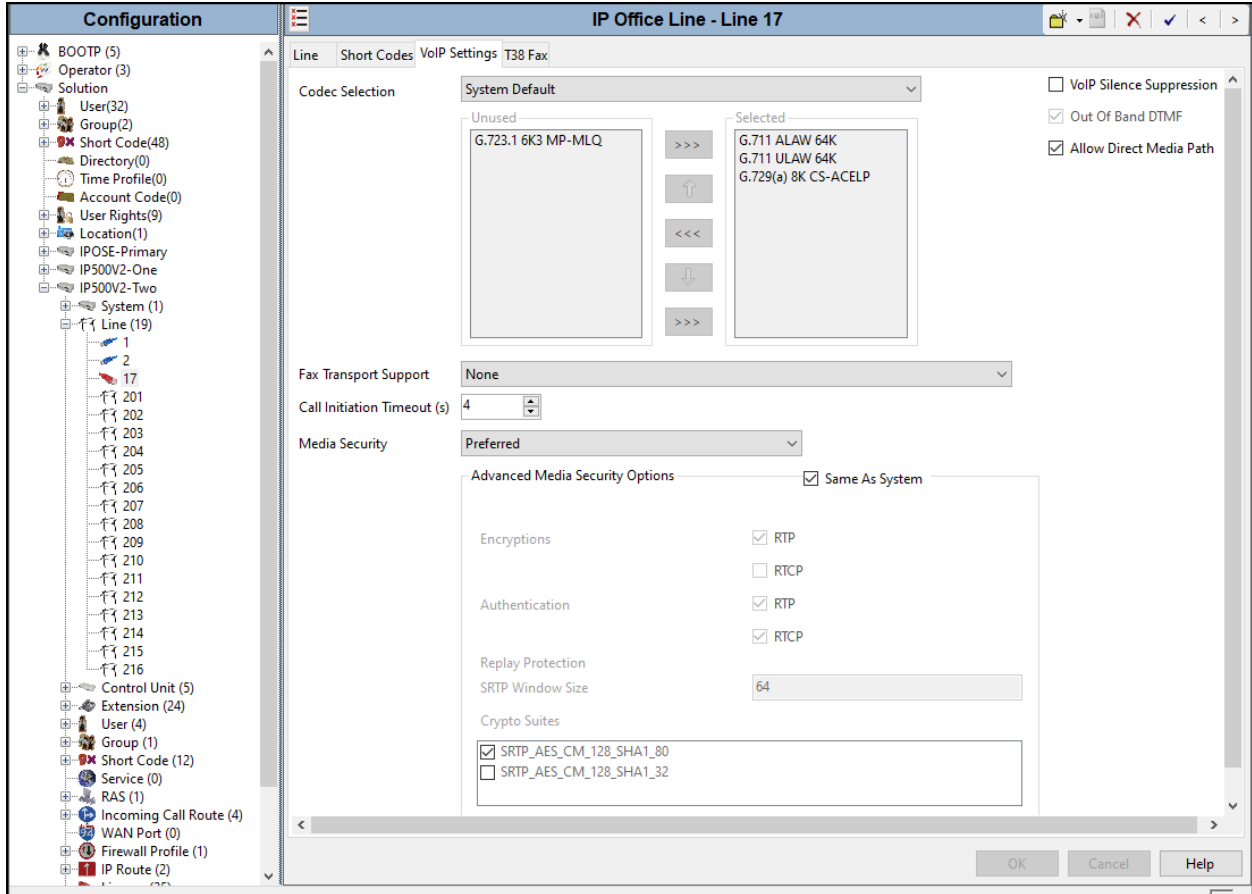
The screenshot displays the configuration interface for an IP Office Line. The window title is "IP Office Line - Line 17". On the left is a navigation tree showing a hierarchy from "Solution" down to "Line (19)", with "Line 17" selected. The main area is divided into several sections:

- Line Settings:** Line Number (17), Telephone Number (empty), Transport Type (WebSocket Client), Prefix (empty), Networking Level (SCN), Outgoing Group ID (99998), Security (Medium), Number of Channels (250), and Outgoing Channels (250).
- Gateway:** Address (10 . 64 . 101 . 127), Port (443), Location (3: Thornton, CO), Password (masked), and Confirm Password (masked).
- SCN Resiliency Options:** Includes checkboxes for "Supports Resiliency", "Backs up my IP phones", "Backs up my hunt groups", and "Backs up my IP DECT phones".
- Description:** A text field for entering a description.

At the bottom right, there are "OK", "Cancel", and "Help" buttons.

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

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **None** for **Fax Transport Support** (refer to Section 2.2).
- Under **Media Security Preferred** was selected.



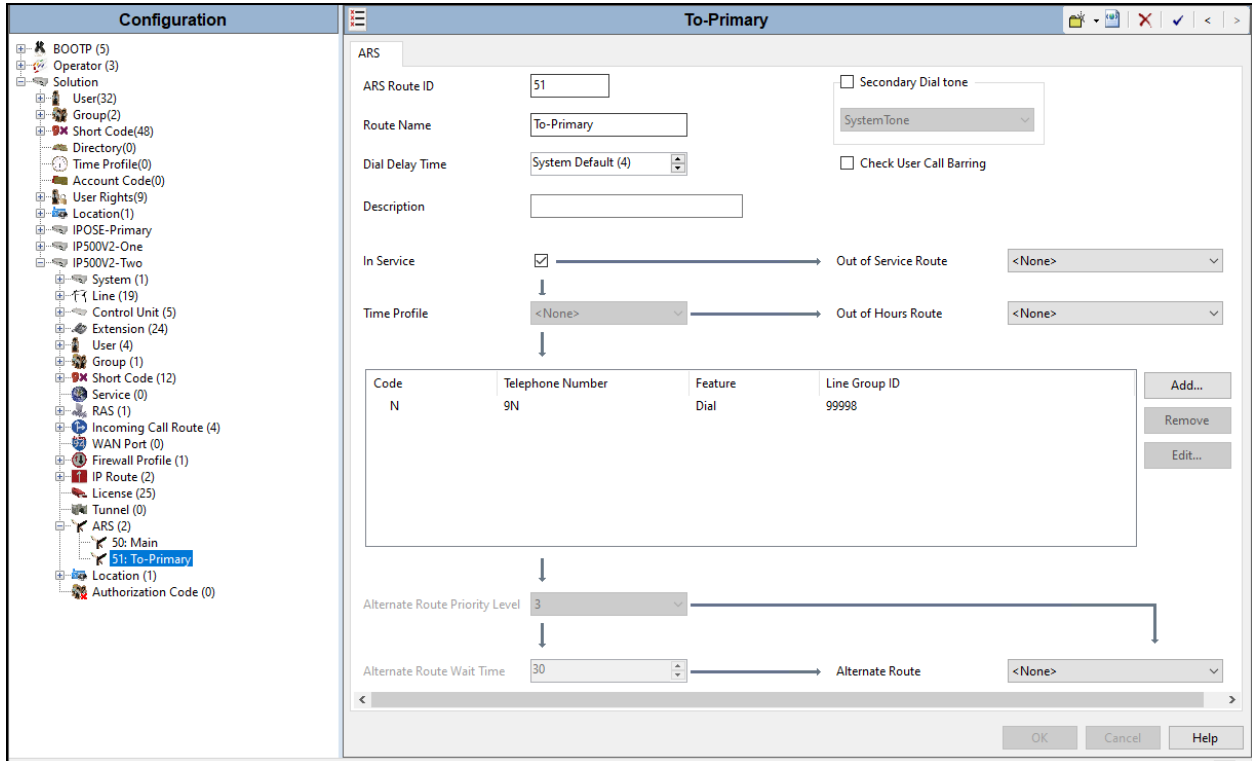
## 6.5. Short Codes

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.

The screenshot displays the Avaya Configuration Manager interface. On the left, a tree view shows the configuration hierarchy, with 'Short Code (12)' expanded to show a list of codes including \*29, \*39, \*40, \*41, \*42, \*43, \*44, \*66\*N#, \*9000\*, \*91N;, \*92N;, and 9N. The '9N' code is selected. The main pane on the right, titled '9N: Dial', shows the configuration for this short code. The 'Code' field is set to '9N', 'Feature' is 'Dial', 'Telephone Number' is 'N', and 'Line Group ID' is '51: To-Primary'. Other fields include 'Locale' set to 'Mexico (Latin Spanish)', and 'Force Account Code' and 'Force Authorization Code' are both unchecked. At the bottom right, there are 'OK', 'Cancel', and 'Help' buttons.

## 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 “**99998**” matching the number of the **Outgoing Group ID** configured on the IP Office Line 17 to the Primary server (**Section 6.4**).

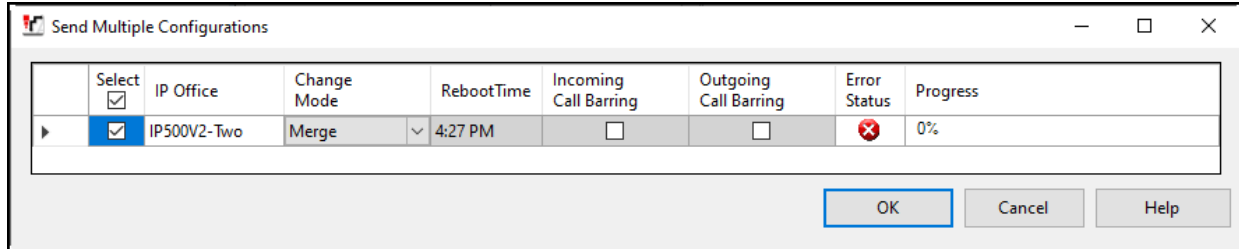


Repeat the process described in **Section 6** on any additional Secondary server or Expansion Systems in the solution, as required.

## 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 **Reboot** 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

This section describes the required configuration of the Avaya SBC to connect to Clearcom SIP Trunking Service.

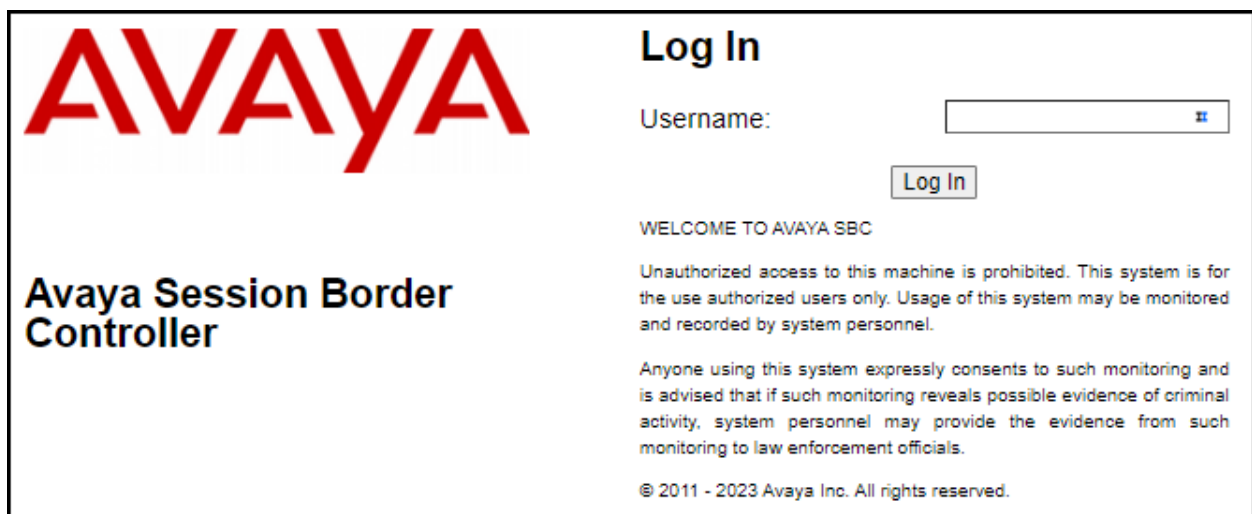
It is assumed that the Avaya SBC was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBC web interface.

**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 SBC

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

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



**AVAYA**

**Avaya Session Border Controller**

**Log In**

Username:

**Log In**

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2023 Avaya Inc. All rights reserved.



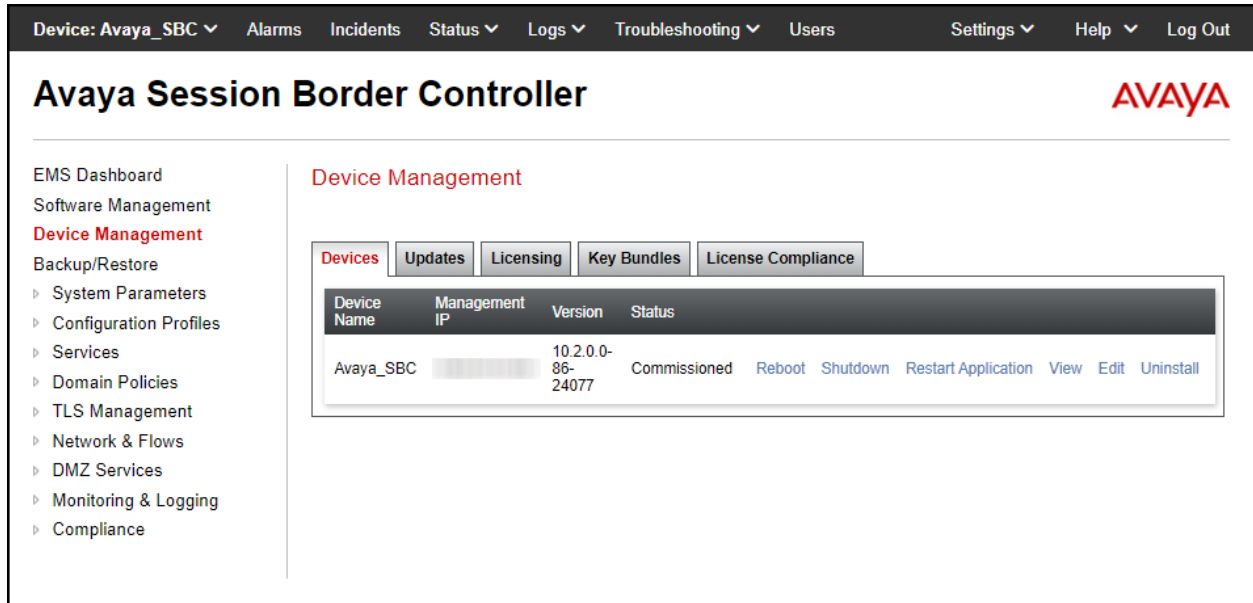
Once logged in, on the top left of the screen, under **Device:** select the device being managed, **Avaya\_SBC** in the sample configuration.

The screenshot shows the Avaya Session Border Controller (SBC) web interface. The top navigation bar includes 'Device: Avaya\_SBC' and various menu items. The main header displays 'Avaya Session Border Controller' and the AVAYA logo. The left sidebar lists 'EMS Dashboard' with sub-items: Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, Monitoring & Logging, and Compliance. The main content area is titled 'Dashboard' and contains two panels. The 'Information' panel shows system details: System Time (12:46:30 PM EDT), Version (10.2.0.0-86-24077), GUI Version (10.2.0.0-24065), Build Date (Thu Feb 22 20:27:46 IST 2024), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (August 1, 2024 at 9:11:02 AM EDT), and Failed Login Attempts (0). The 'Installed Devices' panel shows a list with 'Avaya\_SBC' selected under the 'EMS' category.

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

## 7.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named **Avaya\_SBC** 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 SBC, 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 screenshot displays the Avaya Session Border Controller (SBC) web interface. The top navigation bar includes "Device: Avaya\_SBC", "Alarms", "Incidents", "Status", "Logs", "Troubleshooting", "Users", "Settings", "Help", and "Log Out". The main header reads "Avaya Session Border Controller" with the AVAYA logo. The left navigation pane lists various management options, with "Device Management" highlighted. The main content area is titled "Device Management" and features several tabs: "Devices", "Updates", "Licensing", "Key Bundles", and "License Compliance". The "Devices" tab is selected, showing a table with the following data:

Device Name	Management IP	Version	Status						
Avaya_SBC	[Blurred]	10.2.0.0-86-24077	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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

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.

**System Information: Avaya\_SBC**

General Configuration		Management IP(s)		Dynamic License Allocation		
Appliance Name	Avaya_SBC	IP #1 (IPv4)	10.64.101.242		Min License Allocation	Max License Allocation
Box Type	SIP	DNS Configuration		Standard Sessions	100	200
Deployment Mode	Proxy	Primary DNS	8.8.8.8	Advanced Sessions	100	200
HA Mode	No	Secondary DNS	8.8.4.4	Scopia Video Sessions	0	0
		DNS Location	DMZ	CES Sessions	0	0
		DNS Client IP	10.10.80.51	Transcoding Sessions	75	100
				AMR	<input type="checkbox"/>	
				Premium Sessions	0	0
				CLID	---	
				Encryption	<input checked="" type="checkbox"/>	
				Available: Yes		

Network Configuration				
IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.101.243	10.64.101.243	255.255.255.0	10.64.101.1	A1
				A1
				A1
				B1
				B1
10.10.80.51	10.10.80.51	255.255.255.128	10.10.80.1	B1

The IP addresses in the **System Information** screen shown above are the ones used for the SIP trunk to Clearcom and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBC **A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

In the reference configuration, the private interface of the Avaya SBC (10.64.101.243) was used to connect to the enterprise network, while its public interface (10.10.80.51) was used to connect to the public network. See **Figure 1**.

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

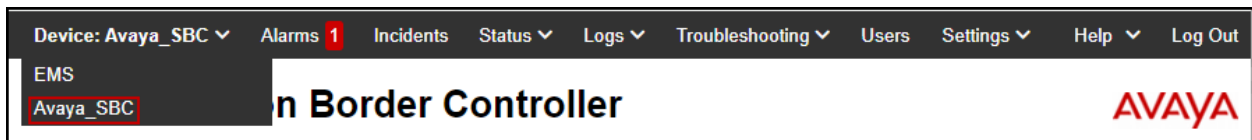
## 7.3. TLS Management

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

In the reference configuration, TLS transport is used for the communication between IP Office and Avaya SBC. The following procedures show how to create the client and server profiles to support the TLS connection.

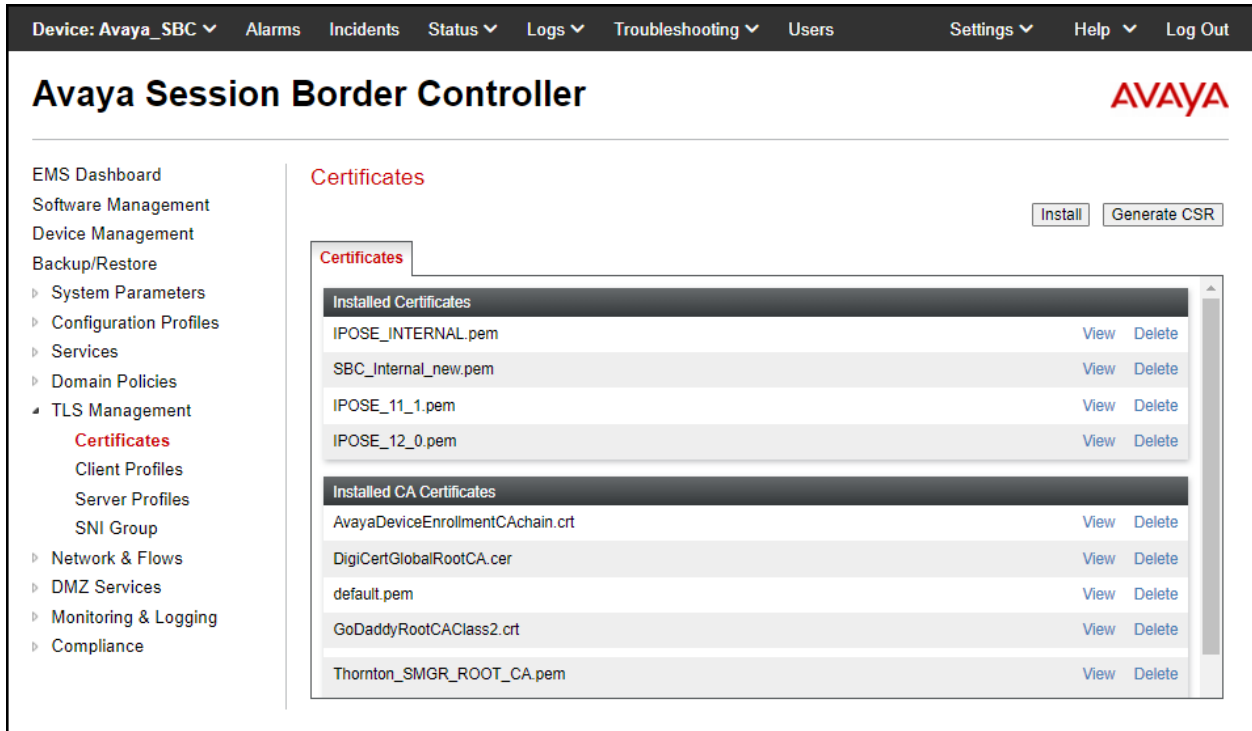
### 7.3.1. Verify TLS Certificates – Avaya Session Border Controller

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



**Step 1** - Select **TLS Management** → **Certificates** from the left-hand menu. Verify the following:

- System Manager Root CA certificate is present in the **Installed CA Certificates** area.
- System Manager CA signed identity certificate is present in the **Installed Certificates** area.
- Private key associated with the identity certificate is present in the **Installed Keys** area (not shown).



### 7.3.2. Server Profiles

**Step 1** - Select **TLS Management** → **Server Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name, e.g., **IPO\_12\_0\_Server\_Profile**.
- **Certificate:** select the identity certificate, e.g., **IPOSE\_12\_0.pem**, from pull down menu.
- **Peer Verification = None.**
- Click **Next**.

**Step 2** - Accept default values for the next screen (not shown) and click **Finish**.

**Edit Profile** X

**WARNING:** Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

**TLS Profile**

Profile Name: IPO\_12\_0\_Server\_Profile

Certificate: IPOSE\_12\_0.pem

SNI Options: None

SNI Group: None

**Certificate Verification**

Peer Verification: None

Peer Certificate Authorities: AvayaDeviceEnrollmentCAchain.crt, DigiCertGlobalRootCA.cer, default.pem, GoDaddyRootCAClass2.crt

Peer Certificate Revocation Lists:

Verification Depth: 0

Next

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

The screenshot displays the Avaya Session Border Controller (SBC) web interface. The top navigation bar includes 'Device: Avaya\_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo.

The left sidebar contains a navigation menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Certificates, Client Profiles, **Server Profiles** (highlighted), SNI Group, Network & Flows, DMZ Services, Monitoring & Logging, and Compliance.

The main content area is titled 'Server Profiles: IPO\_12\_0\_Server\_Profile'. It features an 'Add' button and a 'Delete' button. A blue bar contains the text 'Click here to add a description.' Below this is a 'Server Profile' form with the following sections:

- TLS Profile**
  - Profile Name: IPO\_12\_0\_Server\_Profile
  - Certificate: IPOSE\_12\_0.pem
  - SNI Options: None
- Certificate Verification**
  - Peer Verification: None
  - Extended Hostname Verification:
- Renegotiation Parameters**
  - Renegotiation Time: 0
  - Renegotiation Byte Count: 0
- Handshake Options**
  - Version:  TLS 1.3  TLS 1.2
  - Ciphers:  Default  FIPS  Custom
  - Value: DEFAULT:ISHA

An 'Edit' button is located at the bottom of the form.

### 7.3.3. Client Profiles

**Step 1** - Select **TLS Management** → **Client Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name, e.g., **IPO\_12\_0\_Client\_Profile**.
- **Certificate:** select the identity certificate, e.g., **IPOSE\_12\_0.pem**, from pull down menu.
- **Peer Verification = Required.**
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **Thornton\_SMGR\_ROOT\_CA.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

**Step 2** - Accept default values for the next screen (not shown) and click **Finish**.

**Edit Profile** X

**WARNING:** Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

**TLS Profile**

Profile Name: IPO\_12\_0\_Client\_Profile

Certificate: IPOSE\_12\_0.pem

SNI:  Enabled

**Certificate Verification**

Peer Verification: Required

Peer Certificate Authorities: GigiCertGlobalRootCA\_New.pem, Miguels\_CA\_Cert.pem, DigiCertGlobalRootG2.crt, Thornton\_SMGR\_ROOT\_CA.pem

Peer Certificate Revocation Lists: [Empty list]

Verification Depth: 1

Extended Hostname Verification:

Server Hostname: [Empty field]

Next



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

The screenshot displays the Avaya Session Border Controller (SBC) web interface. The top navigation bar includes 'Device: Avaya\_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo. The left navigation pane lists various management options, with 'Client Profiles' highlighted under 'TLS Management'. The main content area shows the configuration for the 'IPO\_12\_0\_Client\_Profile'. It includes a list of client profiles on the left, with 'IPO\_12\_0\_Cli...' selected. The configuration form is divided into several sections: 'Certificate' (IPOSE\_12\_0.pem, SNI Enabled), 'Certificate Verification' (Peer Verification Required, Peer Certificate Authorities Thornton\_SMGR\_ROOT\_CA.pem, Peer Certificate Revocation Lists ---, Verification Depth 1, Extended Hostname Verification disabled), 'Renegotiation Parameters' (Renegotiation Time 0, Renegotiation Byte Count 0), and 'Handshake Options' (Version TLS 1.3 and TLS 1.2 checked, Ciphers Default selected, Value DEFAULT:!SHA). Buttons for 'Add', 'Delete', and 'Edit' are visible.

## 7.4. Configuration Profiles

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

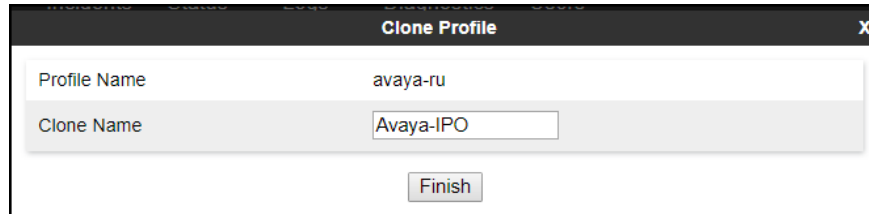
### 7.4.1. Server Interworking – Avaya-IPO

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 Clearcom, this profile was left with the **avaya-ru** default values.

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

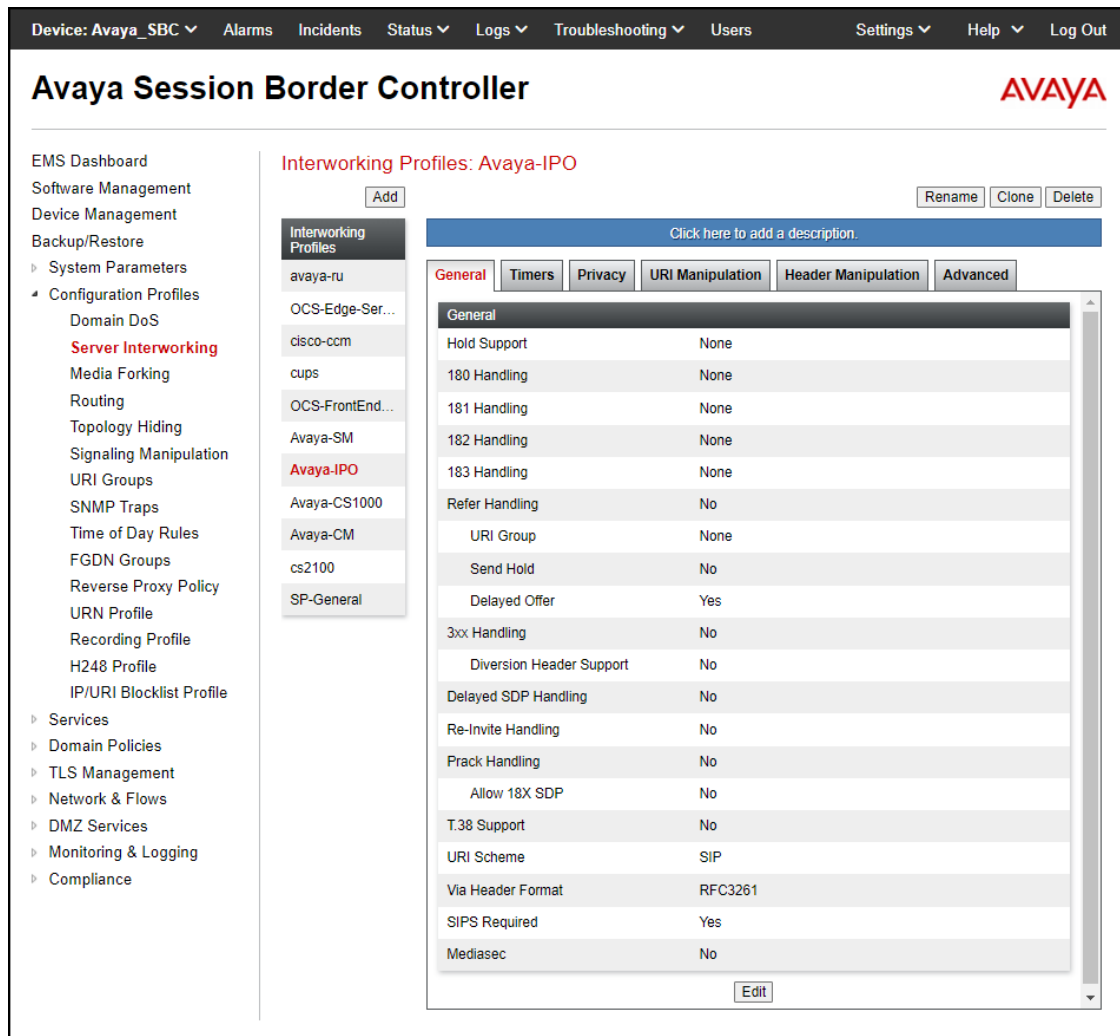
Enter the new profile name in the **Clone Name** field, the name of **Avaya-IPO** was chosen in this example. Click **Finish**.



The screenshot shows a 'Clone Profile' dialog box with the following fields and buttons:

- Profile Name: avaya-ru
- Clone Name: Avaya-IPO
- Finish button

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



The screenshot displays the Avaya Session Border Controller interface. The main content area shows the configuration for the 'Avaya-IPO' profile under the 'Interworking Profiles' section. The 'General' tab is selected, showing a table of configuration parameters.

Parameter	Value
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	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

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

The screenshot displays the Avaya Session Border Controller (SBC) configuration interface. At the top, a navigation bar includes 'Device: Avaya\_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo.

The left sidebar contains a navigation menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', and 'Domain Policies'. Under 'Configuration Profiles', 'Server' is expanded to show 'Interworking', which is further expanded to list profiles: 'avaya-ru', 'OCS-Edge-Ser...', 'cisco-ccm', 'cups', 'OCS-FrontEnd...', 'Avaya-SM', 'Avaya-IPO' (highlighted in red), 'Avaya-CS1000', 'Avaya-CM', 'cs2100', and 'SP-General'.

The main content area is titled 'Interworking Profiles: Avaya-IPO'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A blue bar prompts to 'Click here to add a description.' Below this are tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced' (selected). The 'Advanced' tab contains the following configuration table:

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes
<b>SIP Recording</b>	
Relay INVITE Replace	No
<b>Conference URI</b>	
Include Called Participant	No
<b>DTMF</b>	
DTMF Support	None

An 'Edit' button is located at the bottom right of the configuration area.

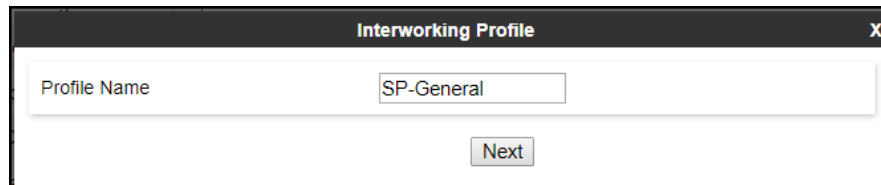
## 7.4.2. Server Interworking - SP-General

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**.



The screenshot shows a dialog box titled "Interworking Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "SP-General". Below the input field is a button labeled "Next".

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

The screenshot shows a dialog box titled "Editing Profile: SP-General" with a close button (X) in the top right corner. The "General" tab is active, displaying a list of settings:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly <input type="radio"/> Microsoft Teams
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None (dropdown menu)
Send Hold	<input type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
SIPS Required	<input type="checkbox"/>
Mediasec Handling	<input type="checkbox"/>

At the bottom of the dialog is a "Finish" button.

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

The screenshot displays the Avaya Session Border Controller management interface. At the top, there is a navigation bar with options like 'Device: Avaya\_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo.

On the left, a sidebar menu lists various configuration categories such as 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Server Interworking', 'Media Forking', 'Routing', 'Topology Hiding', 'Signalling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', 'URN Profile', 'Recording Profile', 'H248 Profile', 'IP/URI Blocklist Profile', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', 'Monitoring & Logging', and 'Compliance'.

The main content area is titled 'Interworking Profiles: SP-General'. It features an 'Add' button and three action buttons: 'Rename', 'Clone', and 'Delete'. Below this is a blue bar with the text 'Click here to add a description.' and a list of tabs: 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, showing a table of configuration parameters.

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	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	No
Mediasec	No

An 'Edit' button is located at the bottom right of the configuration table.

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

The screenshot displays the Avaya Session Border Controller (SBC) web interface. At the top, there is a navigation bar with the following items: Device: Avaya\_SBC, Alarms, Incidents, Status, Logs, Troubleshooting, Users, Settings, Help, and Log Out. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo.

On the left side, there is a navigation menu with the following categories: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles (with sub-items: Domain DoS, Server, Interworking, Media Forking, Routing, Topology Hiding, Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, FGDN Groups, Reverse Proxy Policy, URN Profile, Recording Profile, H248 Profile, IP/URI Blocklist Profile), Services, and Domain Policies. The 'Interworking' option is highlighted in red.

The main content area is titled 'Interworking Profiles: SP-General'. It includes an 'Add' button and three buttons: 'Rename', 'Clone', and 'Delete'. Below this is a blue bar with the text 'Click here to add a description.' and a list of tabs: 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced' (which is selected and highlighted in red).

The 'Advanced' tab contains the following configuration settings:

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes
<b>SIP Recording</b>	
Relay INVITE Replace	No
Conference URI	
Include Called Participant	No
<b>DTMF</b>	
DTMF Support	None

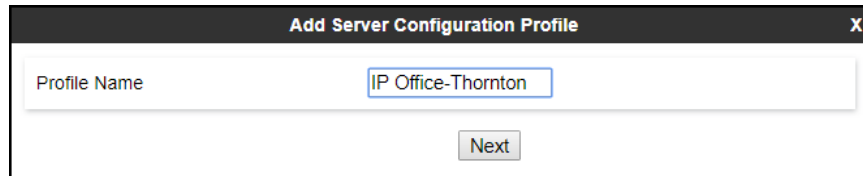
At the bottom of the configuration area, there is an 'Edit' button.

### 7.4.3. SIP Server Configuration

SIP Server Profiles should be created for the Avaya SBC'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**.

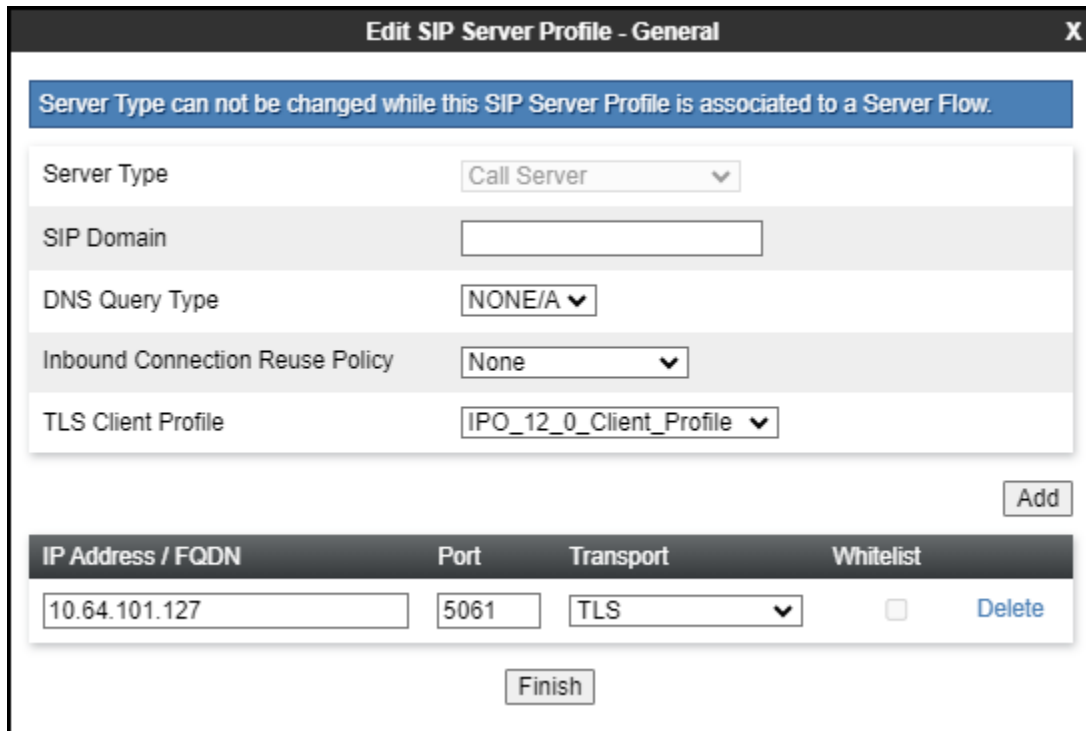
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. The "Profile Name" field contains the text "IP Office-Thornton". Below the field is a "Next" button.

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** (**Section 7.3.3**).
- Click **Next**.



The screenshot shows the "Edit SIP Server Profile - General" window. At the top, there is a blue warning banner: "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below this, several fields are visible: "Server Type" (Call Server), "SIP Domain" (empty), "DNS Query Type" (NONE/A), "Inbound Connection Reuse Policy" (None), and "TLS Client Profile" (IPO\_12\_0\_Client\_Profile). An "Add" button is at the bottom right of this section. Below is a table with columns: IP Address / FQDN, Port, Transport, and Whitelist. The table contains one row with values: 10.64.101.127, 5061, TLS, and a checkbox. A "Delete" button is next to the checkbox. At the bottom of the window is a "Finish" button.

IP Address / FQDN	Port	Transport	Whitelist
10.64.101.127	5061	TLS	<input type="checkbox"/>



- Click **Next** until the **Add SIP Server Profile - Advanced** tab is reached (not shown).
- On the **Add SIP Server Profile - Advanced** tab:
- Verify that **Enable Grooming** is checked.
- Select **Avaya-IPO** from the **Interworking Profile** drop down menu (**Section 7.4.1**).
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

Add SIP Server Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-IPO
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>
Back Finish	

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

The screenshot displays the Avaya Session Border Controller web interface. The top navigation bar includes 'Device: Avaya\_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo. On the left, a navigation menu lists various management options, with 'SIP Servers' highlighted under the 'Services' section. The main content area is titled 'SIP Servers: IP Office-Thornton' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' options. Below this, there are tabs for 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced', with 'General' selected. The configuration details for the 'General' tab are as follows:

Server Type	Call Server		
TLS Client Profile	IPO_12_0_Client_Profile		
DNS Query Type	NONE/A		
Inbound Connection Reuse Policy	None		
IP Address / FQDN	Port	Transport	Whitelist
10.64.101.127	5061	TLS	<input type="checkbox"/>

An 'Edit' button is located at the bottom right of the configuration area.

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

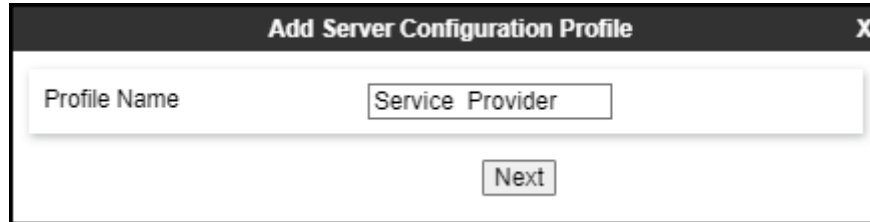
The screenshot displays the Avaya Session Border Controller web interface, showing the 'Advanced' tab for the 'IP Office-Thornton' SIP Server Configuration Profile. The navigation and header elements are consistent with the previous screenshot. The 'Advanced' tab is selected, and the configuration details are as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-IPO
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

An 'Edit' button is located at the bottom right of the configuration area.

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**.

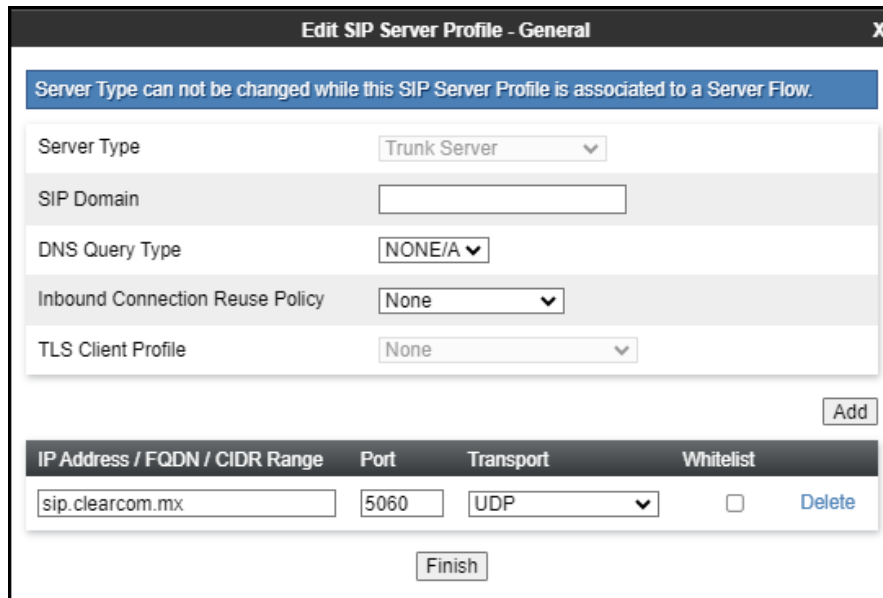
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. The main content area contains a text input field labeled "Profile Name" with the text "Service Provider" entered. Below the input field is a "Next" button.

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

- **Server Type:** Select **Trunk Server**.
- Click on **Add** and under **IP Address / FQDN** enter: **sip.clearcom.mx** (Clearcom SIP proxy server FQDN, this information is provided by Clearcom).
- **Port:** **5060**.
- **Transports:** Select **UDP**.
- Click **Next** (not shown).



The screenshot shows the "Edit SIP Server Profile - General" window. At the top, there is a blue warning banner: "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below this, there are several configuration fields:

- Server Type: Trunk Server (dropdown)
- SIP Domain: (empty text field)
- DNS Query Type: NONE/A (dropdown)
- Inbound Connection Reuse Policy: None (dropdown)
- TLS Client Profile: None (dropdown)

An "Add" button is located to the right of the TLS Client Profile field. Below these fields is a table with the following columns: IP Address / FQDN / CIDR Range, Port, Transport, and Whitelist.

IP Address / FQDN / CIDR Range	Port	Transport	Whitelist
sip.clearcom.mx	5060	UDP	<input type="checkbox"/>

A "Delete" button is next to the checkbox in the table row. At the bottom of the window is a "Finish" button.

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

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by Clearcom for SIP trunk registration.
- Enter the **Realm** credential provided by Clearcom for SIP trunk registration. Note that Clearcom Domain Name was used.
- Enter **Password** credential provided by Clearcom for SIP trunk registration.
- Click **Next**.

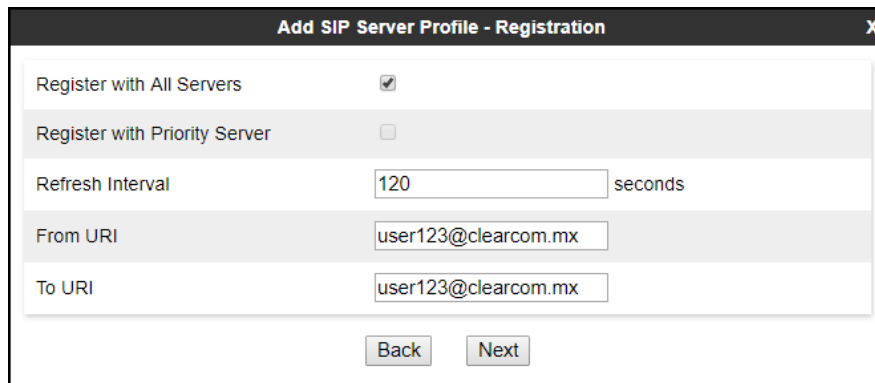
The screenshot shows a dialog box titled "Add SIP Server Profile - Authentication". It contains the following fields and controls:

- Enable Authentication:** A checkbox that is checked.
- User Name:** A text input field containing "user123".
- Realm:** A text input field containing "clearcom.mx". Below the field is the text "(Leave blank to detect from server challenge)".
- Password:** A text input field with masked characters "....".
- Confirm Password:** A text input field with masked characters "....".
- Navigation:** Two buttons at the bottom: "Back" and "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.
- **Frequency:** 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 Clearcom. **120** 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:** Use the **User Name** entered above in the **Authentication** screen (**user123**) and Clearcom domain name (**clearcom.mx**), as shown on the screen below.
  - **To URI:** Use the **User Name** entered above in the **Authentication** screen (**user123**) and Clearcom domain name (**clearcom.mx**), as shown on the screen below.
  - Click **Next**.



The screenshot shows a configuration window titled "Add SIP Server Profile - Registration". It contains the following fields and options:

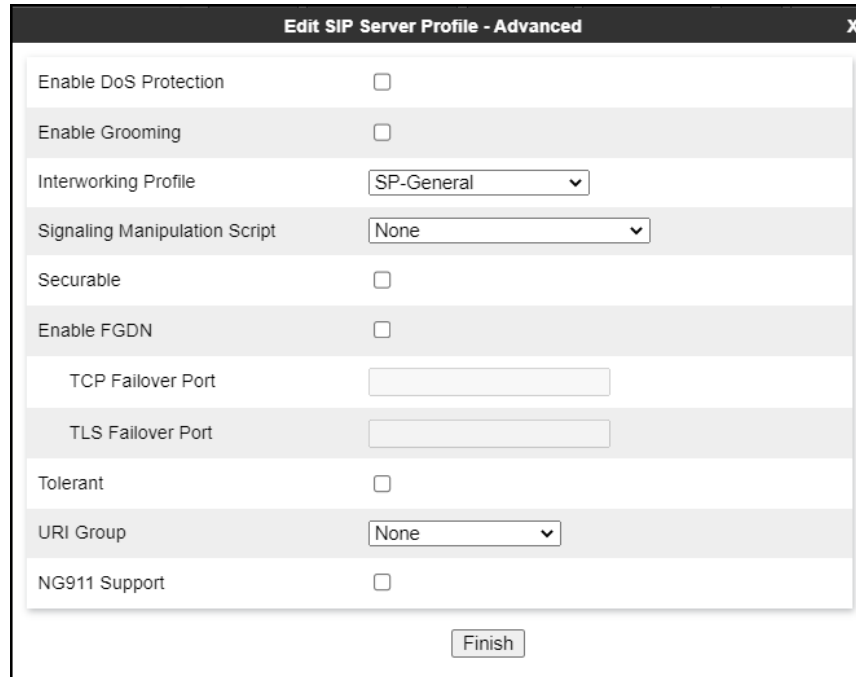
Register with All Servers	<input checked="" type="checkbox"/>
Register with Priority Server	<input type="checkbox"/>
Refresh Interval	<input type="text" value="120"/> seconds
From URI	<input type="text" value="user123@clearcom.mx"/>
To URI	<input type="text" value="user123@clearcom.mx"/>

At the bottom of the window, there are two buttons: "Back" and "Next".

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

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

- Uncheck **Enable Grooming**.
- Select **SP-General** from the **Interworking Profile** drop-down menu (**Section 7.4.2**).
- Click **Finish**.



The screenshot shows a configuration window titled "Edit SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several settings:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

At the bottom center of the window is a button labeled "Finish".

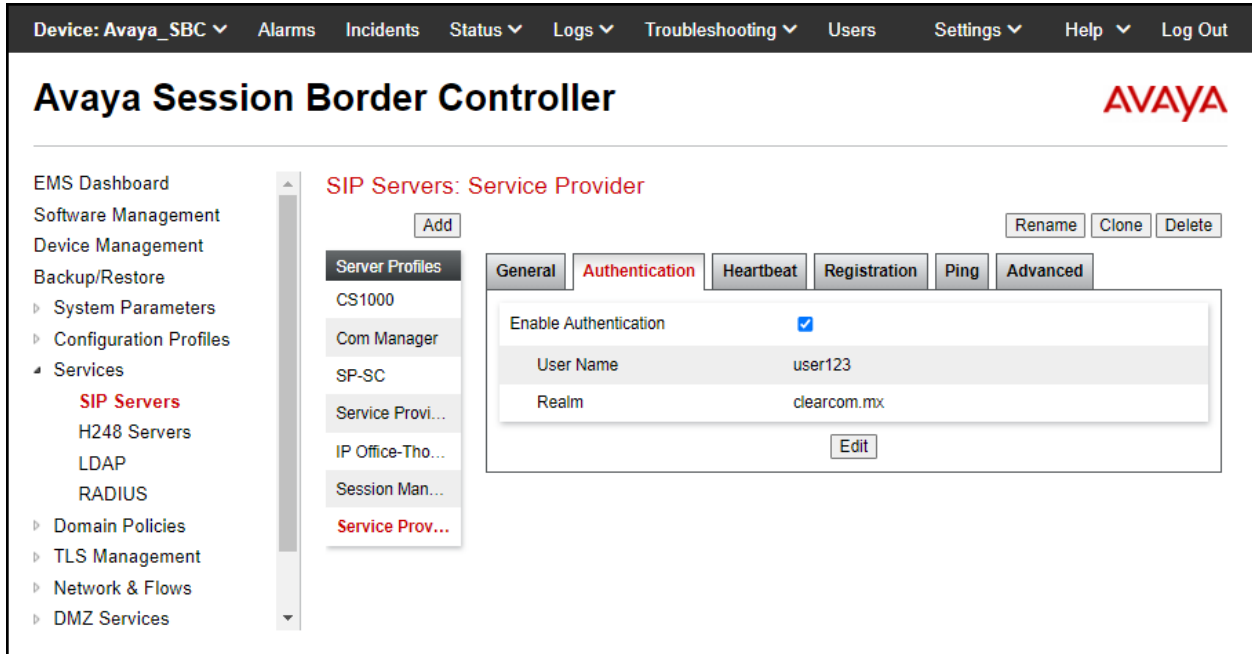
The following screen capture shows the **General** tab of the newly created **Service Provider** SIP Server Configuration Profile.

The screenshot displays the Avaya Session Border Controller web interface. At the top, a navigation bar includes 'Device: Avaya\_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo. A left sidebar lists navigation options: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services (with 'SIP Servers' expanded to show H248 Servers, LDAP, RADIUS, Domain Policies, and TLS Management), and a scrollable list of server profiles including CS1000, Com Manager, SP-SC, Service Provi..., IP Office-Tho..., Session Man..., and Service Prov... The main content area is titled 'SIP Servers: Service Provider' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this are tabs for 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced'. The 'General' tab is active, showing configuration details: Server Type (Trunk Server), DNS Query Type (NONE/A), and Inbound Connection Reuse Policy (None). A table lists IP addresses and ports:

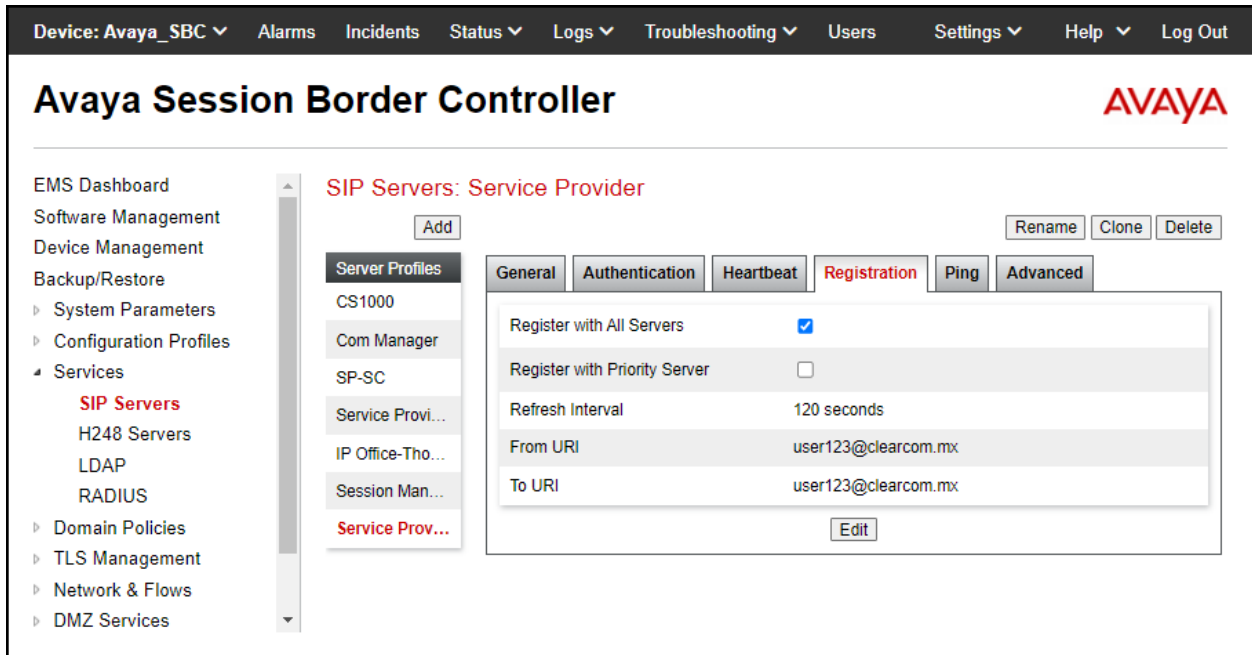
IP Address / FQDN /CIDR Range	Port	Transport	Whitelist
sip.clearcom.mx	5060	UDP	<input type="checkbox"/>

An 'Edit' button is located below the table.

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



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





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

The screenshot displays the Avaya Session Border Controller (SBC) configuration interface. At the top, a navigation bar includes 'Device: Avaya\_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo.

The left sidebar contains a navigation menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', 'Monitoring & Logging', and 'Compliance'. Under 'Services', 'SIP Servers' is expanded to show 'H248 Servers', 'LDAP', 'RADIUS', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', 'Monitoring & Logging', and 'Compliance'. The 'SIP Servers' section is further expanded to show 'H248 Servers', 'LDAP', 'RADIUS', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', 'Monitoring & Logging', and 'Compliance'. The 'SIP Servers' section is further expanded to show 'H248 Servers', 'LDAP', 'RADIUS', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', 'Monitoring & Logging', and 'Compliance'.

The main content area is titled 'SIP Servers: Service Provider'. It features an 'Add' button and three action buttons: 'Rename', 'Clone', and 'Delete'. Below this is a tabbed interface with tabs for 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced'. The 'Advanced' tab is selected, showing a list of configuration options:

Option	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

An 'Edit' button is located at the bottom right of the configuration table.

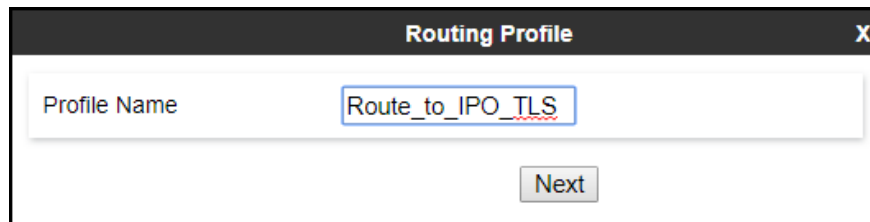
#### 7.4.4. Routing Profiles

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**.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Route\_to\_IPO\_TLS". Below the input field is a "Next" button.

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

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **SIP Server Profile:** 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**.

Profile : Route\_to\_IPO\_TLS - Edit Rule

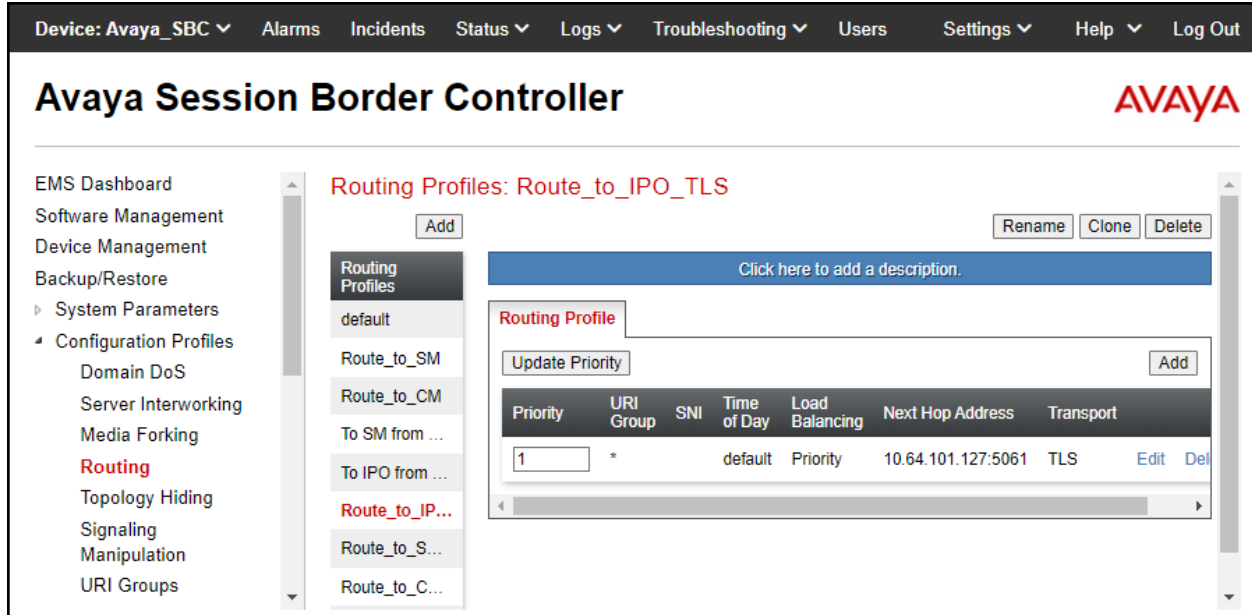
URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	
Server Name Indication (SNI)	<input type="checkbox"/>	Server Name	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				IP Office	10.64.101.127:5061	None	Delete

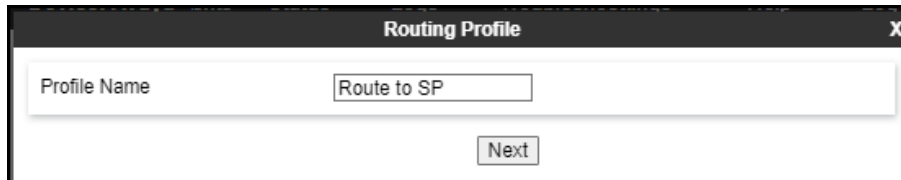
Finish

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**.
- Click **Next**.



On the Routing Profile screen complete the following:

- **Load Balancing:** Select **DNS/SRV**.
- Click on the **Add** button to add a **Next-Hop Address**.
- **SIP Server Profile:** Select **Service Provider**.
- The **Next Hop Address** is populated automatically with **sip.clearcom.mx:5060 (UDP)** (Clearcom SIP Proxy FQDN, port and transport).
- Click **Finish**.

The screenshot shows the 'Profile: Route to SP - Edit Rule' configuration window. The settings are as follows:

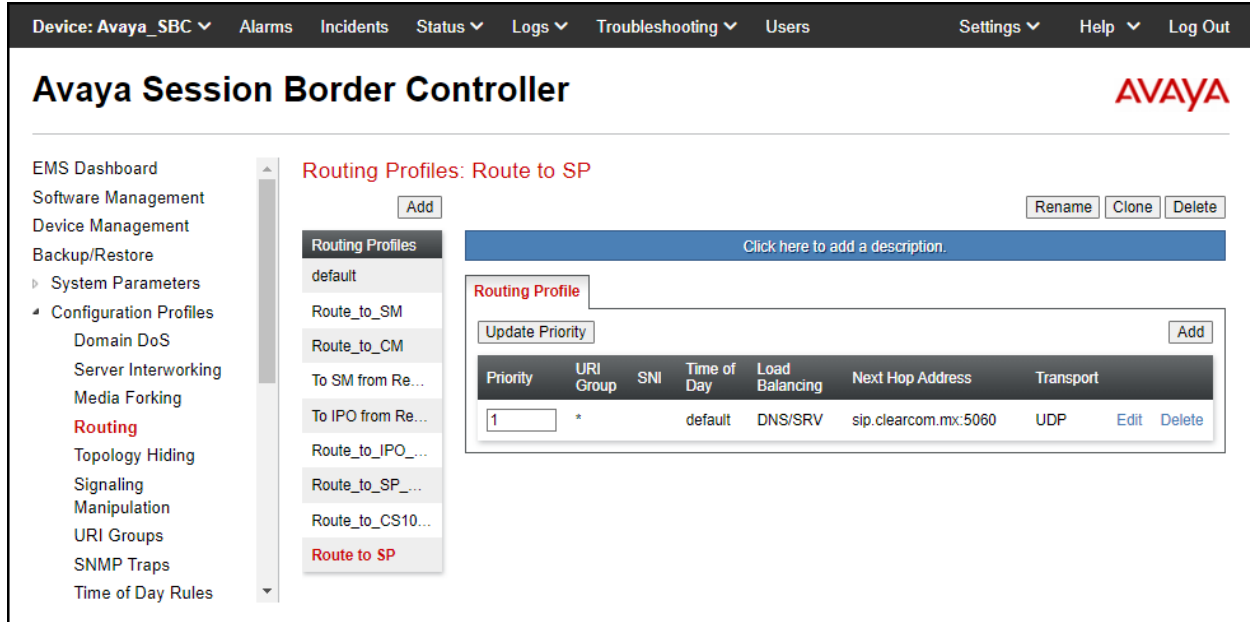
- URI Group: \*
- Time of Day: default
- Load Balancing: DNS/SRV
- NAPTR:
- Transport: None
- LDAP Routing:
- LDAP Server Profile: None
- LDAP Base DN (Search): None
- Matched Attribute Priority:
- Alternate Routing:
- Next Hop Priority:
- Next Hop In-Dialog:
- Ignore Route Header:
- ENUM:
- ENUM Suffix:
- Server Name Indication (SNI):
- Server Name:

At the bottom, there is an 'Add' button and a table with the following columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, and Transport. The table contains one entry:

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
				Service P	sip.clearcom.mx:5060	None

There is also a 'Delete' button next to the transport field and a 'Finish' button at the bottom center.

The following screen capture shows the newly created **Route to SP** Routing Profile.



### 7.4.5. 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**.

**Topology Hiding Profile**
X

Profile Name

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).

Device: Avaya\_SBC
Alarms Incidents Status Logs Troubleshooting Users
Settings Help Log Out

## Avaya Session Border Controller

AVAYA

- EMS Dashboard
- Software Management
- 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
  - URN Profile

### Topology Hiding Profiles: IP Office

Rename Clone Delete

[Click here to add a description.](#)

**Topology Hiding**

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---

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 (**clearcom.mx**) under **Overwrite Value**
- On the **To** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (**clearcom.mx**) 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 (**clearcom.mx**) under **Overwrite Value**.
- Click **Finish**.

Header	Criteria	Replace Action	Overwrite Value	
Record-Route	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	clearcom.mx	Delete
SDP	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	clearcom.mx	Delete
From	IP/Domain	Overwrite	clearcom.mx	Delete
Via	IP/Domain	Auto		Delete



The following screen capture shows the newly added **Service\_Provider** Topology Hiding Profile.

The screenshot displays the Avaya Session Border Controller configuration page. The top navigation bar includes 'Device: Avaya\_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo.

The left sidebar contains a navigation menu with categories like 'EMS Dashboard', 'Software Management', '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', and 'URN Profile'. The 'Topology Hiding' option is highlighted in red.

The main content area is titled 'Topology Hiding Profiles: Service\_Provider'. It features an 'Add' button and three buttons: 'Rename', 'Clone', and 'Delete'. Below this is a blue bar with the text 'Click here to add a description.' and a sub-header 'Topology Hiding'.

The central table lists the configuration for the 'Service\_Provider' profile:

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Overwrite	clearcom.mx
Request-Line	IP/Domain	Overwrite	clearcom.mx
From	IP/Domain	Overwrite	clearcom.mx
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---

An 'Edit' button is located at the bottom right of the table.

## 7.5. Domain Policies

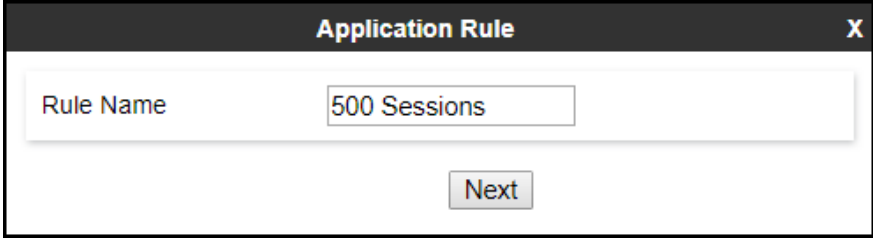
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

### 7.5.1. Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the Avaya SBC 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**.



The screenshot shows a dialog box titled "Application Rule" with a close button "X" in the top right corner. The dialog contains a text input field labeled "Rule Name" with the text "500 Sessions" entered. Below the input field is a "Next" button.

- 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**.

**Editing Rule: 500 Sessions** X

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	500	500
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100

**Miscellaneous**

CDR Support 
 Off  
 RADIUS  
 CDR Adjunct

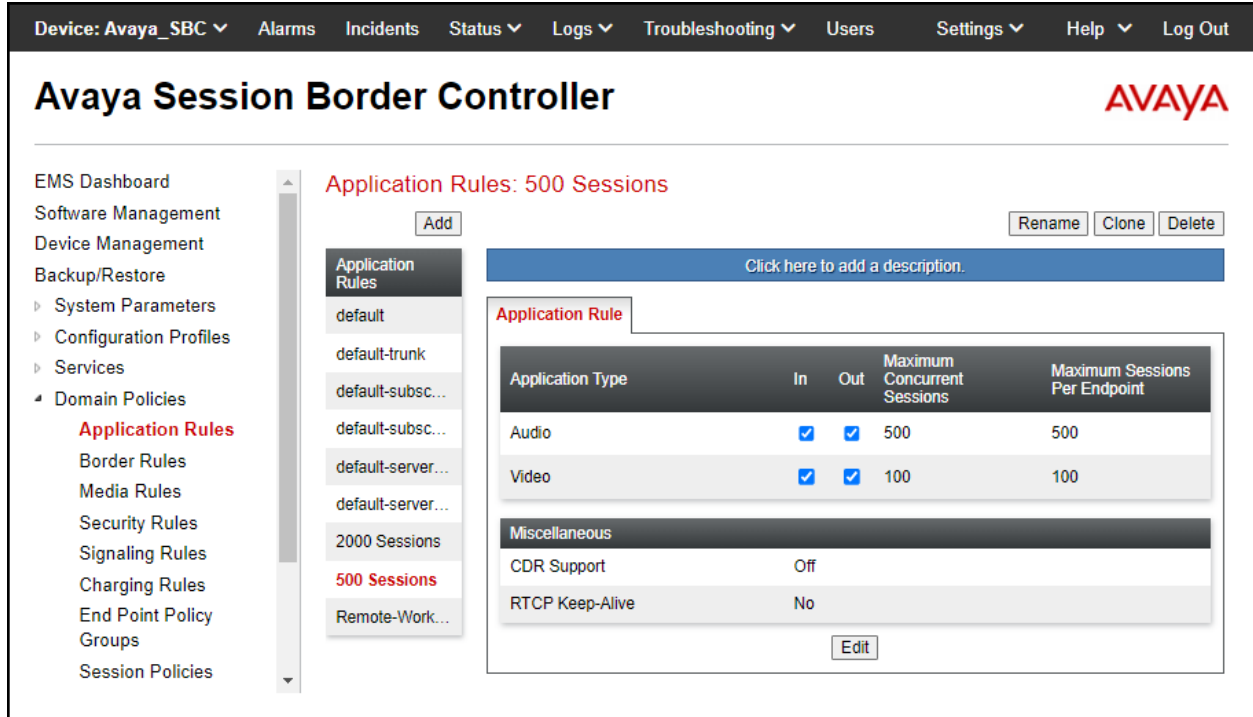
RADIUS Profile None ▾

Media Statistics Support

Call Duration 
 Setup  
 Connect

RTCP Keep-Alive

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



## 7.5.2. 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 SBC 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** (not shown).

The screenshot shows a configuration window titled "Media Encryption" with a close button (X) in the top right corner. The window is divided into three main sections: Audio Encryption, Video Encryption, and Miscellaneous.

**Audio Encryption Section:**

- Preferred Format #1: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80 (dropdown)
- Preferred Format #2: RTP (dropdown)
- Preferred Format #3: NONE (dropdown)
- Encrypted RTCP:
- MKI:
- Lifetime: 2^ [input field] (text: Leave blank to match any value.)
- Interworking:
- Symmetric Context Reset:
- Key Change in New Offer:

**Video Encryption Section:**

- Preferred Format #1: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80 (dropdown)
- Preferred Format #2: RTP (dropdown)
- Preferred Format #3: NONE (dropdown)
- Encrypted RTCP:
- MKI:
- Lifetime: 2^ [input field] (text: Leave blank to match any value.)
- Interworking:
- Symmetric Context Reset:
- Key Change in New Offer:

**Miscellaneous Section:**

- Capability Negotiation:

At the bottom of the window, there is a "Finish" button.

- 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.

The screenshot displays the Avaya Session Border Controller (SBC) web interface. At the top, there is a navigation bar with the following items: Device: Avaya\_SBC, Alarms, Incidents, Status, Logs, Troubleshooting, Users, Settings, Help, and Log Out. The main header shows "Avaya Session Border Controller" and the AVAYA logo.

On the left side, there is a navigation menu with the following categories and sub-items:

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
  - Application Rules
  - Border Rules
  - Media Rules**
  - Security Rules
  - Signaling Rules
  - Charging Rules
  - End Point Policy Groups
  - Session Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging
- Compliance

The main content area is titled "Media Rules: IPO\_SRTP". It includes an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." and a list of tabs: "Encryption", "Codec Prioritization", "Advanced", and "QoS".

The "Encryption" tab is active and contains the following configuration sections:

- Audio Encryption**
  - Preferred Formats: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80 RTP
  - Encrypted RTCP:
  - MKI:
  - Lifetime: Any
  - Interworking:
  - Symmetric Context Reset:
  - Key Change in New Offer:
- Video Encryption**
  - Preferred Formats: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80 RTP
  - Encrypted RTCP:
  - MKI:
  - Lifetime: Any
  - Interworking:
  - Symmetric Context Reset:
  - Key Change in New Offer:
- Miscellaneous**
  - Capability Negotiation:

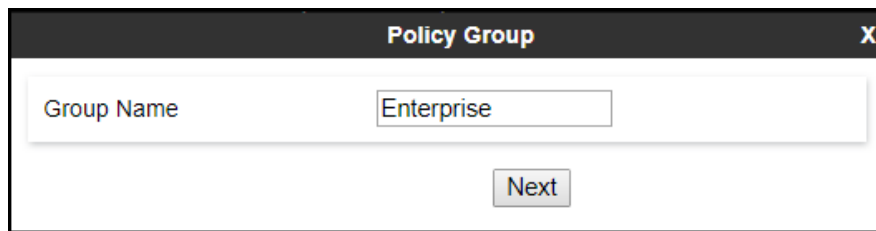
An "Edit" button is located at the bottom right of the configuration area.

### 7.5.3. 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 SBC.

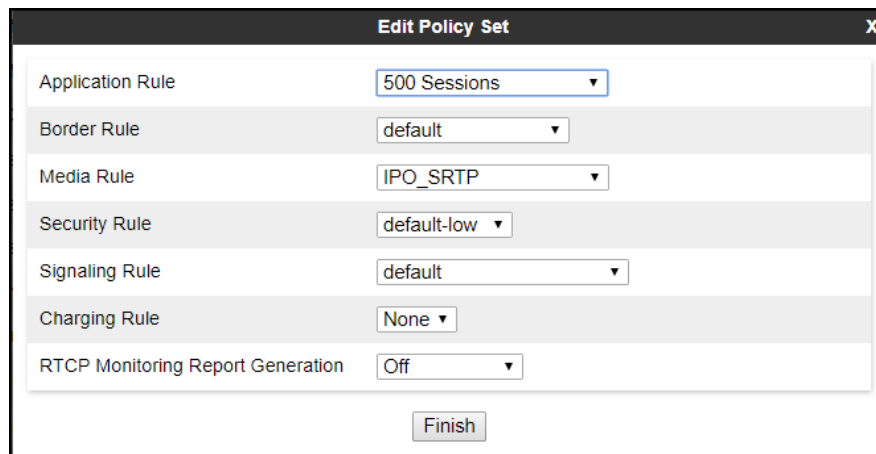
To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups** (not shown).

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



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" containing the text "Enterprise". Below the input field, there is a "Next" button.

- **Application Rule: 500 Sessions.**
- **Border Rule: default.**
- **Media Rule: IPO\_SRTP (Section 7.5.2).**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- Click **Finish**.



The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several rows of configuration options, each with a label and a dropdown menu:

Application Rule	500 Sessions
Border Rule	default
Media Rule	IPO_SRTP
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

At the bottom of the dialog, there is a "Finish" button.

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

The screenshot displays the Avaya Session Border Controller (SBC) web interface. At the top, a navigation bar includes 'Device: Avaya\_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo.

The left sidebar contains a navigation menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'Application Rules', 'Border Rules', 'Media Rules', 'Security Rules', 'Signaling Rules', 'Charging Rules', 'End Point Policy Groups', 'Session Policies', and 'TLS Management'. The 'End Point Policy Groups' option is highlighted in red.

The main content area is titled 'Policy Groups: Enterprise'. It features an 'Add' button and three action buttons: 'Rename', 'Clone', and 'Delete'. Below these are two blue boxes with the text 'Click here to add a description.' and 'Click here to add a row description.'.

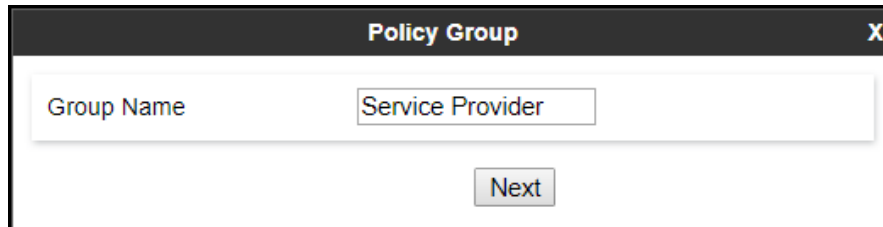
A 'Policy Group' configuration window is open, showing a table with the following data:

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	500 Sessions	default	IPO_SRTP	default-low	default	None	Off	Edit



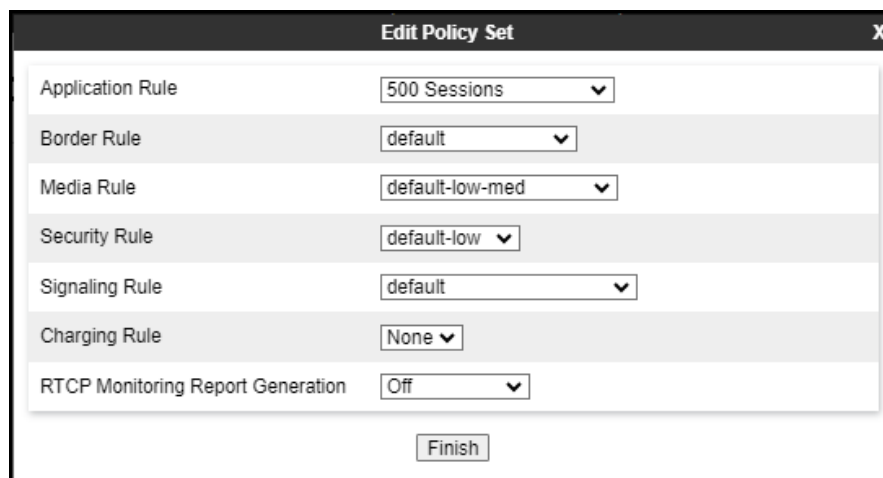
Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk.

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



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" containing the text "Service Provider". Below the input field is a button labeled "Next".

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



The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several rows, each with a label and a dropdown menu:

Application Rule	500 Sessions
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

At the bottom of the dialog is a button labeled "Finish".

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

The screenshot displays the Avaya Session Border Controller interface. At the top, there is a navigation bar with options like 'Device: Avaya\_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Avaya Session Border Controller' with the AVAYA logo on the right.

On the left, a navigation menu lists various management options, with 'End Point Policy Groups' highlighted in red. The main content area is titled 'Policy Groups: Service Provider' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this, there is a list of policy groups including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default...', 'avaya-def-low...', 'avaya-def-hig...', 'avaya-def-hig...', 'Enterprise', and 'Service Prov...'. The 'Service Prov...' group is selected.

The detailed view for the 'Service Provider' policy group shows a 'Summary' tab and a table with the following data:

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen
1	500 Sessions	default	default-low-med	default-low	default	None	Off

## 7.6. 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.

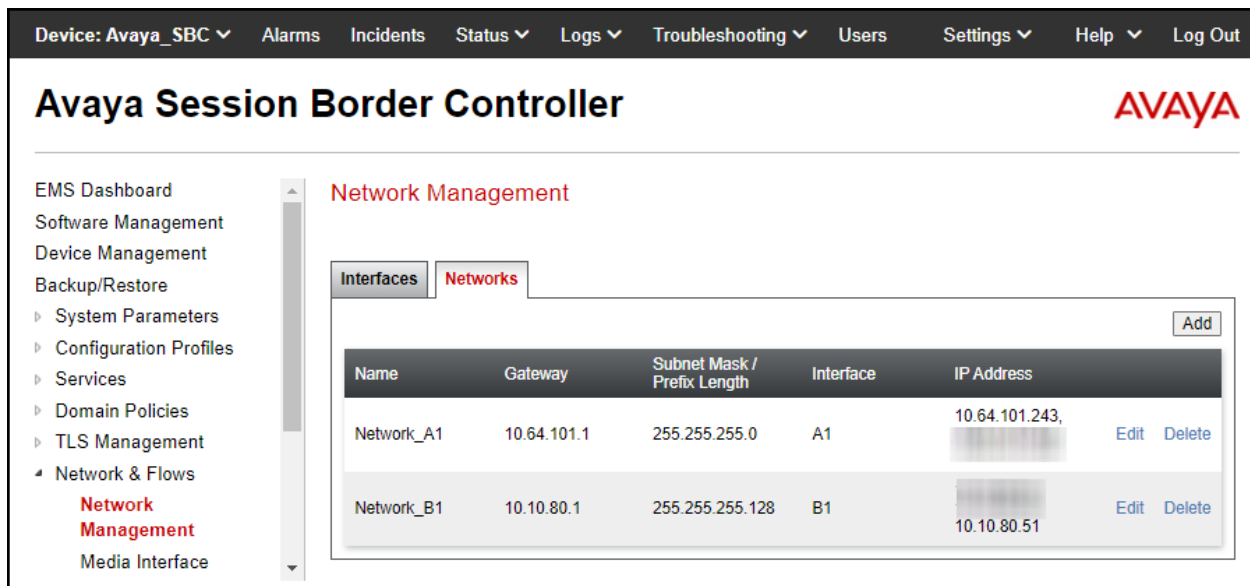
### 7.6.1. Network Management

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.

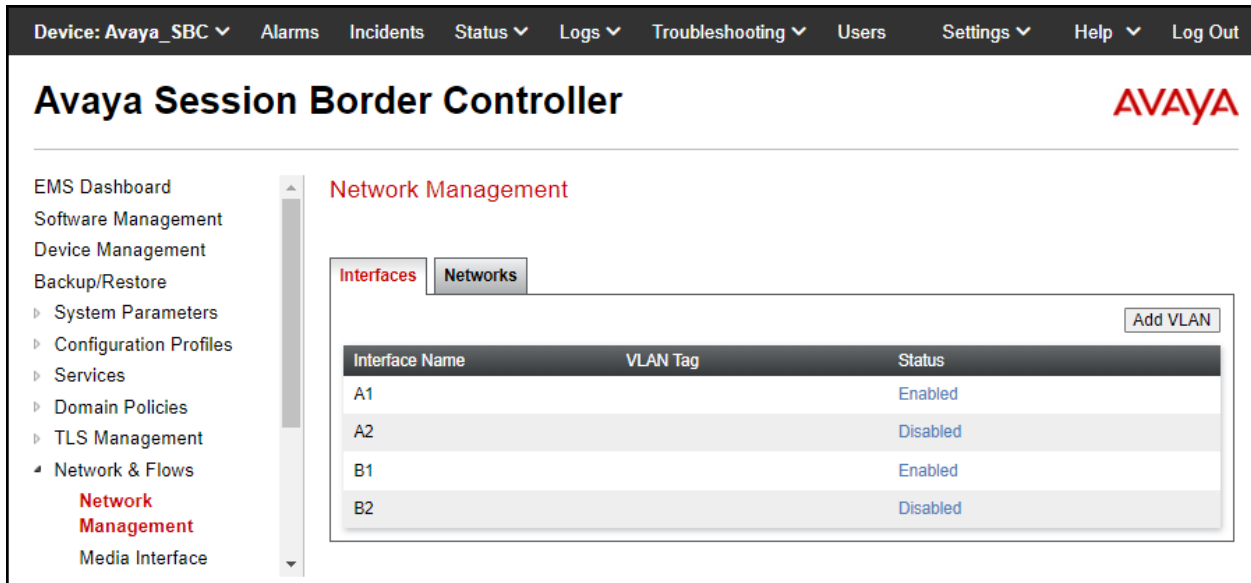
**Note:** Only the highlighted entity items were created for the compliance test and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in these Application Notes.



The screenshot displays the Avaya Session Border Controller interface. The top navigation bar includes 'Device: Avaya\_SBC' and various menu items like 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Avaya Session Border Controller' with the AVAYA logo. A left-hand navigation menu lists categories such as 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', and 'Network & Flows'. Under 'Network & Flows', 'Network Management' is selected and highlighted. The 'Network Management' section has two tabs: 'Interfaces' and 'Networks', with 'Networks' being the active tab. An 'Add' button is located in the top right of the network configuration area. Below the tabs is a table with the following data:

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Network_A1	10.64.101.1	255.255.255.0	A1	10.64.101.243	Edit	Delete
Network_B1	10.10.80.1	255.255.255.128	B1	10.10.80.51	Edit	Delete

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 SBC will not be able to communicate on any of its interfaces.



The screenshot displays the Avaya Session Border Controller (SBC) web interface. At the top, a navigation bar includes 'Device: Avaya\_SBC' and various menu items like 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo. On the left, a sidebar menu lists navigation options such as 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'Network Management', and 'Media Interface'. The 'Network Management' section is active, with the 'Interfaces' tab selected. A table below the tabs shows the status of four interfaces:

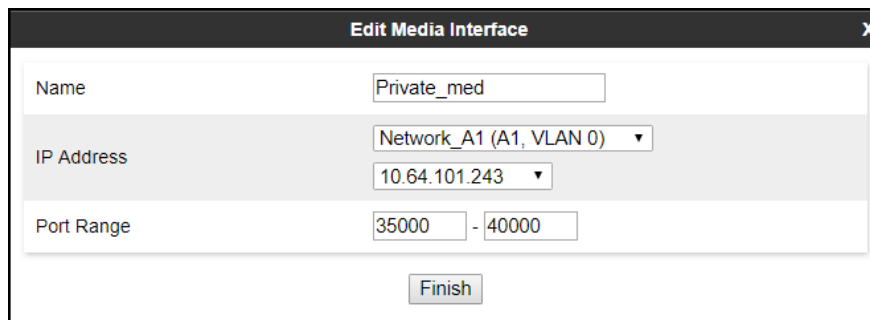
Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

## 7.6.2. Media Interface

Media Interfaces are created to specify the IP address and port range in which the Avaya SBC will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBC will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBC will accept media from the connected server. Create a SIP Media Interface for both the inside and outside IP interfaces. On the Private and Public interfaces of the Avaya SBC, 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 SBC, toward IP Office).
- **Port Range: 35000-40000.**
- Click **Finish**.

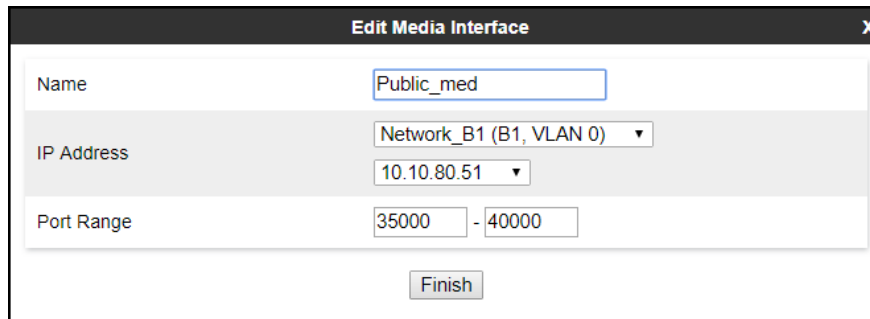


Name	Private_med
IP Address	Network_A1 (A1, VLAN 0) 10.64.101.243
Port Range	35000 - 40000

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 SBC, toward the Service Provider).
- **Port Range: 35000-40000.**
- Click **Finish**.



**Edit Media Interface**

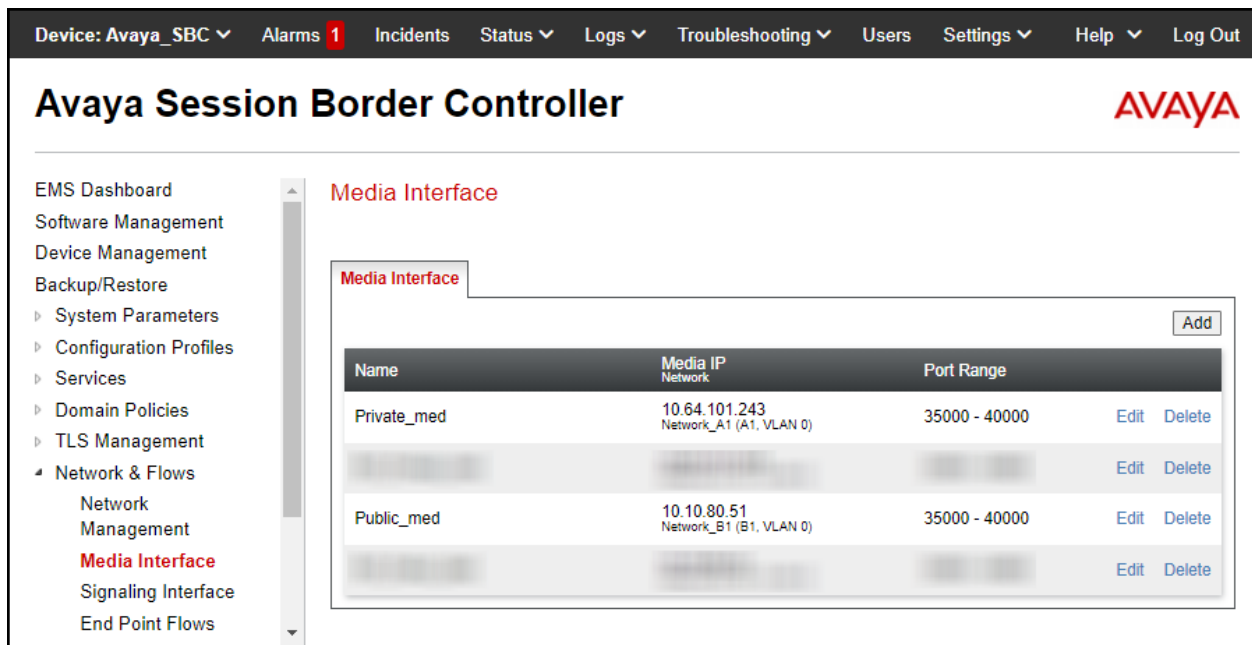
Name: Public\_med

IP Address: Network\_B1 (B1, VLAN 0) | 10.10.80.51

Port Range: 35000 - 40000

Finish

The following screen capture shows the newly created Media Interfaces.



Device: Avaya\_SBC | Alarms 1 | Incidents | Status | Logs | Troubleshooting | Users | Settings | Help | Log Out

## Avaya Session Border Controller

AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
System Parameters  
Configuration Profiles  
Services  
Domain Policies  
TLS Management  
Network & Flows  
Network Management  
**Media Interface**  
Signaling Interface  
End Point Flows

### Media Interface

Add

Name	Media IP Network	Port Range		
Private_med	10.64.101.243 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Public_med	10.10.80.51 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete

### 7.6.3. 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 SBC, toward IP Office).
- **TLS Port: 5061.**
- Select a **TLS Profile (Section 7.3.2).**
- Click **Finish.**

Name	Private_sig
IP Address	Network_A1 (A1, VLAN 0) 10.64.101.243
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	IPO_12_0_Server_Profile
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

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 SBC, toward the Service Provider).
- **UDP Port: 5060.**
- Click **Finish.**

Name	Public_sig
IP Address	Network_B1 (B1, VLAN 0) 10.10.80.51
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish



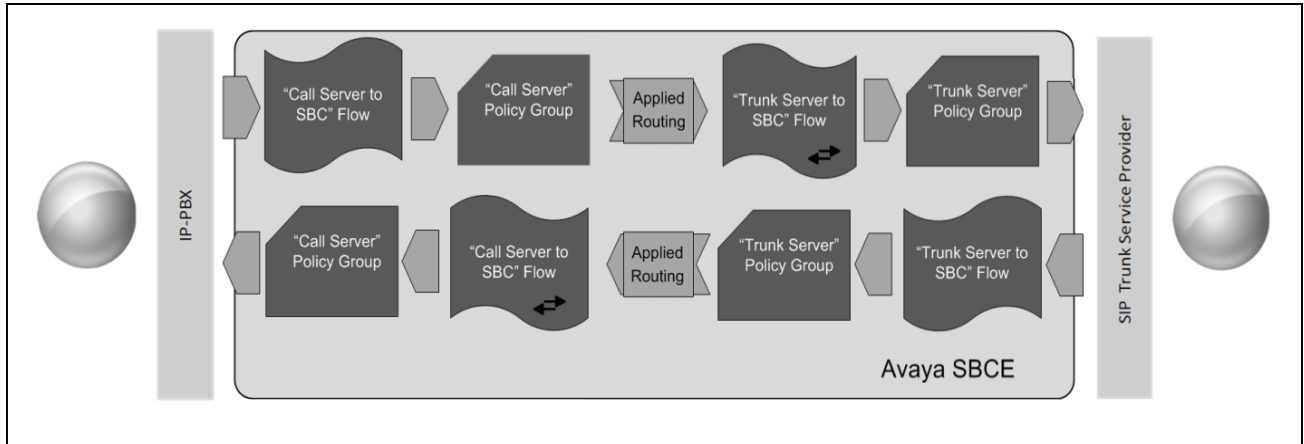
The following screen capture shows the newly created Signaling Interfaces.

The screenshot shows the Avaya Session Border Controller web interface. The top navigation bar includes 'Device: Avaya\_SBC', 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Avaya Session Border Controller' and the 'AVAYA' logo. A left-hand navigation menu lists various management options, with 'Signaling Interface' highlighted in red. The main content area is titled 'Signaling Interface' and features a table with the following data:

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	10.64.101.243 Network_A1 (A1, VLAN 0)	---	---	5061	IPO_12_0_Server_Profile	Edit Delete
Public_sig	10.10.80.51 Network_B1 (B1, VLAN 0)	---	5060	---	None	Edit Delete

### 7.6.4. End Point Flows

When a packet is received by Avaya SBC, 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 SBC 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: SP to IPO Flow**
- **Server Configuration: Service Provider (Section 7.4.3).**
- **URI Group: \***
- **Transport: \***
- **Remote Subnet: \***
- **Received Interface: Private\_sig (Section 7.6.3).**
- **Signaling Interface: Public\_sig (Section 7.6.3).**
- **Media Interface: Public\_med (Section 7.6.2).**
- **Secondary Media Interface: None.**
- **End Point Policy Group: Service Provider (Section 7.5.3).**
- **Routing Profile: Route\_to\_IPO\_TLS (Section 7.4.4).**
- **Topology Hiding Profile: Service\_Provider (Section 7.4.5).**
- Click **Finish**.

Field	Value
Flow Name	SP to IPO Flow
SIP Server Profile	Service Provider
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
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	

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

- **Name: IPO to SP Flow.**
- **Server Configuration: IP Office-Thornton (Section 7.4.3).**
- **URI Group: \***
- **Transport: \***
- **Remote Subnet: \***
- **Received Interface: Public\_sig (Section 7.6.3).**
- **Signaling Interface: Private\_sig (Section 7.6.3).**
- **Media Interface: Private\_med (Section 7.6.2).**
- **Secondary Media Interface: None.**
- **End Point Policy Group: Enterprise (Section 7.5.3).**
- **Routing Profile: Route\_to\_SP (Section 7.4.4).**
- **Topology Hiding Profile: IP Office (Section 7.4.5).**
- Click **Finish**.

The screenshot shows a configuration window titled "Edit Flow: IPO to SP Flow". The fields are as follows:

Flow Name	IPO to SP Flow
SIP Server Profile	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
Topology Hiding Profile	IP Office
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Finish

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

**Avaya Session Border Controller**

Device: Avaya\_SBC | Alarms | Incidents | Status | Logs | Troubleshooting | Users | Settings | Help | Log Out

EMS Dashboard  
 Software Management  
 Device Management  
 Backup/Restore  
 System Parameters  
 Configuration Profiles  
 Services  
 Domain Policies  
 TLS Management  
 Network & Flows  
 Network Management  
 Media Interface  
 Signaling Interface  
**End Point Flows**  
 Session Flows  
 Advanced Options  
 DMZ Services  
 Monitoring & Logging  
 Compliance

**End Point Flows**

Subscriber Flows | **Server Flows**

Filter Add

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

Click here to add a row description.

**SIP Server: IP Office-Thornton**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IPO to SP Flow	*	Public_sig	Private_sig	Enterprise	Route to SP	View Clone Edit Delete

**SIP Server: Service Provider**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SP to IPO Flow	*	Private_sig	Public_sig	Service Provider	Route_to_IPO_TLS	View Clone Edit Delete

## 8. Clearcom SIP Trunking Service Configuration

To use Clearcom SIP Trunking Service, a customer must request the service from Clearcom using the established sales processes. The process can be started by contacting Clearcom via the corporate web site at: <http://www.clearcom.mx/> and requesting information.

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

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

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

Clearcom will provide the following information:

- SIP Trunk registration credentials (User Name, Password, etc.).
- Clearcom's Domain Name and SIP Proxy FQDN.
- DNS IP addresses.
- DID numbers, etc.

## 9. Verification Steps

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

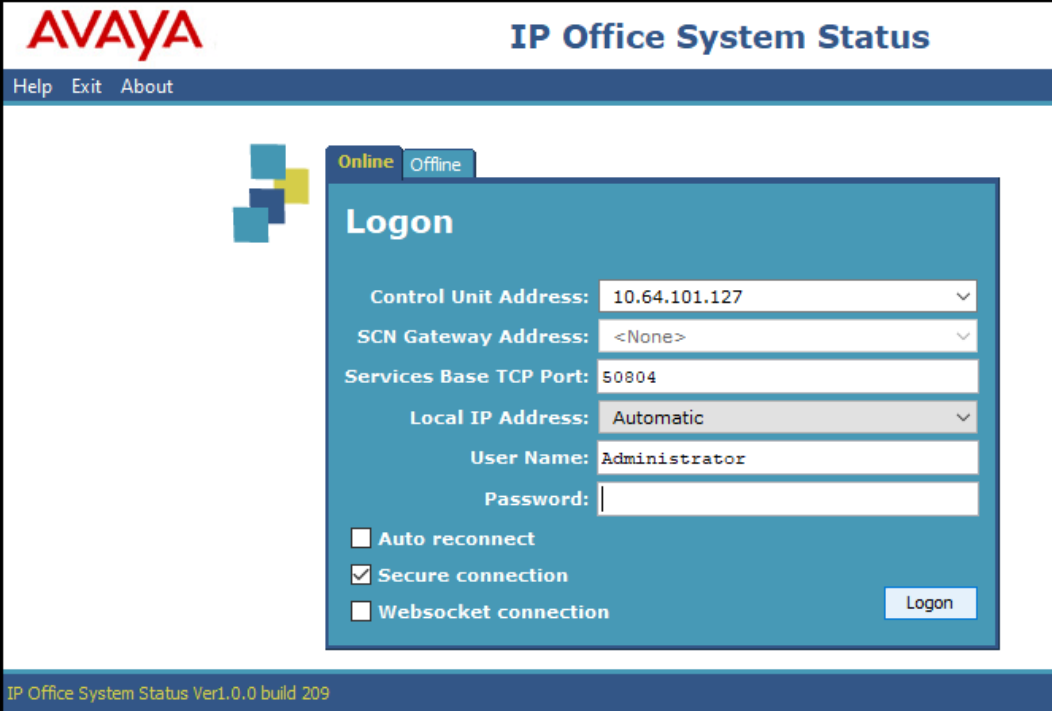
The following steps may be used to verify the configuration:

- 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.



The screenshot shows the AVAYA IP Office System Status application interface. At the top left is the AVAYA logo, and at the top right is the title "IP Office System Status". Below the title is a menu bar with "Help", "Exit", and "About". The main area features a "Logon" dialog box with a status indicator showing "Online" and "Offline" tabs. The dialog box contains the following fields and options:

- Control Unit Address: 10.64.101.127 (dropdown menu)
- SCN Gateway Address: <None> (dropdown menu)
- Services Base TCP Port: 50804
- Local IP Address: Automatic (dropdown menu)
- User Name: Administrator
- Password: (text input field)
- Auto reconnect:
- Secure connection:
- Websocket connection:
- Logon button

At the bottom of the application window, the text "IP Office System Status Ver1.0.0 build 209" is displayed.

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

The screenshot shows the Avaya IP Office System Status interface. The left pane contains a navigation tree with 'Trunks (3)' expanded to show 'Line: 17' selected. The main pane displays the 'Status' tab for the selected trunk, showing a 'SIP Trunk Summary' with various configuration details. Below the summary is a table with 10 columns: Chan..., U..., Call Ref, Current State, Time in State, Remote Media ..., Co..., Conn..., Caller ID or..., Other Party on Call, Direct..., Round Trip ..., Receive Jitter, Recei..., Trans..., and Trans... The table shows 10 channels, all with a 'Current State' of 'Idle' and a 'Time in State' of 9 or 15 days. At the bottom of the interface, there are buttons for 'Trace', 'Trace All', 'Pause', 'Ping', 'Call Details', 'Graceful Shutdown', 'Force Out of Service', 'Print...', and 'Save As...'. The status bar at the bottom right shows the time as 2:41:43 PM and the system as 'Online'.

**SIP Trunk Summary**

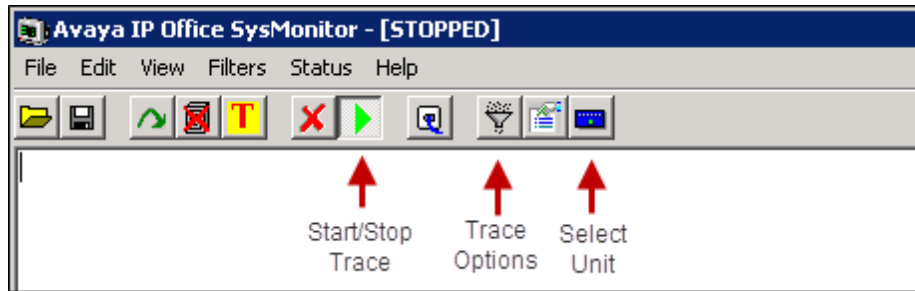
Line Service State: In Service  
Peer Domain Name: sip://10.64.101.243  
Resolved Address: 10.64.101.243  
Line Number: 17  
Number of Administered Channels: 20  
Number of Channels in Use: 0  
Administered Compression: G729 A, G711 A, G711 Mu  
Enable Faststart: Off  
Silence Suppression: Off  
Media Stream: Best Effort  
Layer 4 Protocol: TLS  
SIP Trunk Channel Licenses: 10  
SIP Trunk Channel Licenses in Use: 0 0%

Chan...	U...	Call Ref	Current State	Time in State	Remote Media ...	Co...	Conn...	Caller ID or...	Other Party on Call	Direct...	Round Trip ...	Receive Jitter	Recei...	Trans...	Trans...
1			Idle	9 day...											
2			Idle	9 day...											
3			Idle	13 da...											
4			Idle	15 da...											
5			Idle	15 da...											
6			Idle	15 da...											
7			Idle	15 da...											
8			Idle	15 da...											
9			Idle	15 da...											
10			Idle	15 da...											



## 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

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 SBC.

The screenshot shows the Avaya Session Border Controller web interface. At the top, there is a navigation bar with the following items: Device: Avaya\_SBC, Alarms, Incidents, Status, Logs, Troubleshooting, Users, Settings, Help, and Log Out. A red arrow points to the 'Alarms' link. Below the navigation bar, the main header reads 'Avaya Session Border Controller' with the AVAYA logo on the right. On the left side, there is a sidebar menu with the following items: EMS Dashboard, Software Management, Device Management (highlighted in red), Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, Monitoring & Logging, and Compliance. The main content area is titled 'Device Management' and contains several tabs: Devices, Updates, Licensing, Key Bundles, and License Compliance. The 'Devices' tab is active, displaying a table with the following data:

Device Name	Management IP	Version	Status						
Avaya_SBC	10.64.101.242	10.2.0.0-86-24077	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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

The screenshot shows the Avaya Session Border Controller web interface in the Alarm Viewer section. At the top, there is a navigation bar with the following items: Device: Avaya\_SBC and Help. The main header reads 'Alarm Viewer' with the AVAYA logo on the right. Below the header, there is a section titled 'Alarms' with a table containing the following data:

<input checked="" type="checkbox"/>	ID	Details	State	Time	Device
No alarms found for this device.					

Below the table, there are two buttons: 'Clear Selected' and 'Clear All'.

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

The screenshot shows the Avaya Session Border Controller interface. The top navigation bar includes 'Device: Avaya\_SBC', 'Alarms', 'Incidents' (highlighted with a red arrow), 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Avaya Session Border Controller' with the AVAYA logo. A left sidebar lists navigation options like 'EMS Dashboard', 'Software Management', 'Device Management' (selected), 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', 'Monitoring & Logging', and 'Compliance'. The 'Device Management' section contains tabs for 'Devices', 'Updates', 'Licensing', 'Key Bundles', and 'License Compliance'. Below these is a table with the following data:

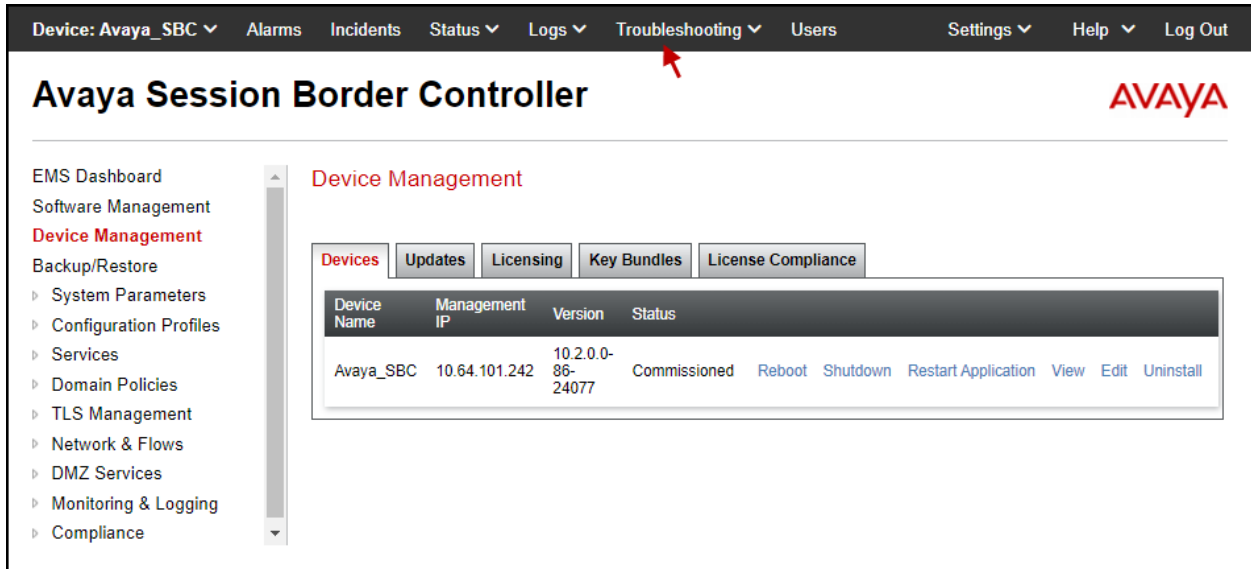
Device Name	Management IP	Version	Status						
Avaya_SBC	10.64.101.242	10.2.0.0-86-24077	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

The following screen shows the Incident Viewer page.

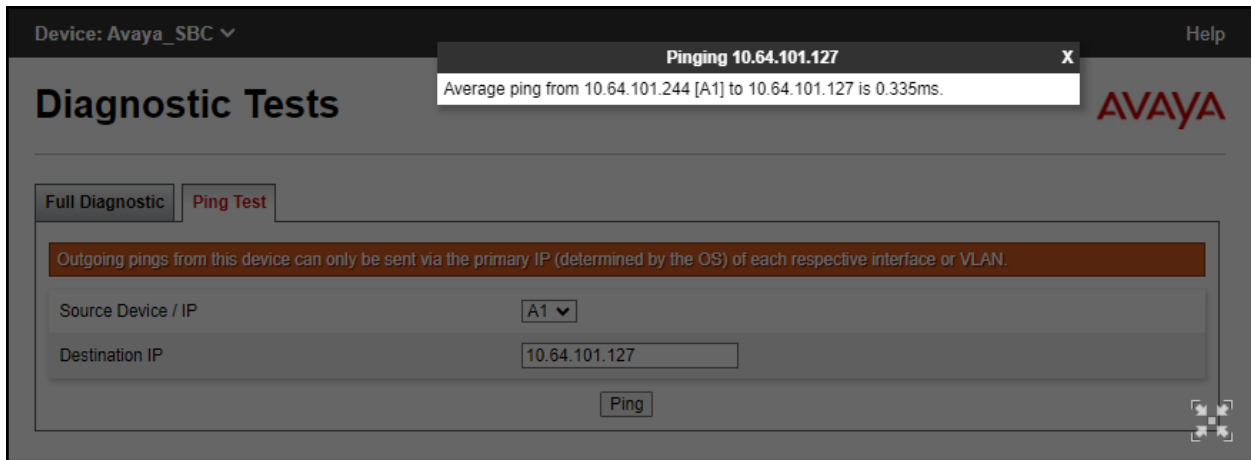
The screenshot shows the Avaya Incident Viewer interface. The top navigation bar includes 'Device: Avaya\_SBC' and 'Help'. The main header reads 'Incident Viewer' with the AVAYA logo. Below the header, there is a 'Category' dropdown set to 'All', a 'Clear Filters' button, and 'Refresh' and 'Generate Report' buttons. A 'Summary' tab is selected. The page displays a table of incidents with the following data:

ID	Date & Time	Category	Type	Cause
861479021261184	Aug 6, 2024 11:27:22 AM	Policy	Routing Failure	Timeout while contacting DNS serverssip.clearcom.mx
861478979865000	Aug 6, 2024 11:25:59 AM	Policy	Message Dropped	No Subscriber Flow Matched

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



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



Additionally, the Avaya SBC 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**.

The screenshot displays the Avaya Session Border Controller (SBC) web interface. At the top, a navigation bar includes 'Device: Avaya SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo. A left-hand navigation menu lists various management options, with 'Monitoring & Logging' expanded to show 'Trace' as the active section. The main content area is titled 'Trace: Avaya SBC' and features two tabs: 'Packet Capture' (selected) and 'Captures'. The 'Packet Capture Configuration' form includes the following fields: 'Status' (Ready), 'Interface' (Any), 'Local Address' (All), 'Remote Address' (\*), 'Protocol' (All), 'Maximum Number of Packets to Capture' (10000), and 'Capture Filename' (Test1.pcap). 'Start Capture' and 'Clear' buttons are located at the bottom of the configuration form.

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.

The screenshot shows the Avaya Session Border Controller web interface. The top navigation bar includes 'Device: Avaya SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Troubleshooting', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Avaya Session Border Controller' and the 'AVAYA' logo. The left sidebar contains a navigation menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The 'Monitoring & Logging' section is expanded, showing 'SNMP', 'Syslog Management', 'Debugging', 'Trace', 'Log Collection', and 'DoS Learning'. The 'Trace' option is highlighted in red. The main content area is titled 'Trace: Avaya SBC' and features two tabs: 'Packet Capture' and 'Captures'. The 'Captures' tab is active, showing a table of captured files. The table has columns for 'File Name', 'File Size (bytes)', and 'Last Modified', with a 'Delete' link for each entry. The table is sorted by 'Last Modified' in descending order.

File Name	File Size (bytes)	Last Modified	
Test1_20240723155527	221,184	July 23, 2024 at 3:55:41 PM MDT	Delete
Test1_20240501132013	376,832	May 1, 2024 at 1:20:40 PM MDT	Delete
OPTIONS1	2,975	August 4, 2023 at 7:56:59 AM MDT	Delete
test2	4,362	August 4, 2023 at 6:51:03 AM MDT	Delete
test1	6,188	August 4, 2023 at 6:48:20 AM MDT	Delete

Also, the **traceSBC** tool can be used to monitor the SIP signaling messages between the Service provider and the Avaya SBC.

## 10. Conclusion

These Application Notes describe the procedures required to configure Avaya IP Office Release 12.0 and Avaya Session Border Controller Release 10.2 to connect to Clearcom SIP Trunking Service. Clearcom SIP Trunking Service 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 Server Edition and Application Servers, Release 12.0, Issue 31, April 2024*
- [2] *IP Office Platform 12.0, Deploying Avaya IP Office Servers as Virtual Machines, June 2024*
- [3] *Avaya IP Office Platform Server Edition Reference Configuration Release 12.0, Issue 22, May 2024*
- [4] *IP Office Platform 12.0, Deploying an IP500 V2 IP Office Basic Edition System, Issue 41e, May 29, 2024*
- [5] *IP Office Platform 12.0, Deploying an IP500 V2 IP Office Essential Edition System, Issue 41e, May 29, 2024*
- [6] *Administering Avaya IP Office using Manager, Release 12.0, Issue 51.1.2, June 2024.*
- [7] *Administering Avaya IP Office with Web Manager, Release 12.0, Issue 46.1.1, May 2024.*
- [8] *Avaya IP Office Platform Feature Description, Release 12.0, Issue 21.1.1, May 2024.*
- [9] *Planning for and Administering Avaya Workplace Client for Android, iOS, Mac and Windows, September 2020*
- [10] *Deploying Avaya Session Border Controller on a Virtualized Environment Platform, Release 10.2, Issue 1, March 2024.*

---

**©2024 Avaya LLC All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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](mailto:devconnect@avaya.com).