



DevConnect Program

Application Notes for Configuring Avaya IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 10.1 to support Clearcom SIP Trunking Service using TLS - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 11.1 and Avaya Session Border Controller for Enterprise Release 10.1 to support Clearcom SIP Trunking Service using TLS. 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 Avaya 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.....	8
4.	Equipment and Software Validated	11
5.	Avaya IP Office Primary Server Configuration.....	12
5.1.	Licensing	14
5.2.	System Settings	15
5.2.1.	System - LAN1 Tab.....	15
5.2.2.	System - Telephony Tab	19
5.2.3.	System - VoIP Tab.....	20
5.3.	IP Route.....	22
5.4.	SIP Line.....	23
5.4.1.	Creating a SIP Trunk from an XML Template.....	23
5.4.2.	SIP Line – SIP Line Tab	27
5.4.3.	SIP Line - Transport Tab	28
5.4.4.	SIP Line – Call Details Tab	29
5.4.5.	SIP Line - VoIP Tab	31
5.4.6.	SIP Line – SIP Advanced Tab	32
5.5.	IP Office Line – Primary Server	33
5.6.	Incoming Call Route	35
5.7.	Outbound Call Routing	37
5.7.1.	Short Codes and Automatic Route Selection.....	37
5.8.	Save IP Office Primary Server Configuration.....	39
6.	Avaya IP Office Expansion System Configuration	40
6.1.	Physical Hardware.....	41
6.2.	LAN Settings.....	42
6.3.	IP Route.....	43
6.4.	IP Office Line – IP500 V2 Expansion System.....	44
6.5.	Short Codes	46
6.6.	Automatic Route Selection – ARS.....	47
6.7.	Save IP Office Expansion System Configuration	48
7.	Configure Avaya Session Border Controller for Enterprise	49
7.1.	Log in Avaya SBCE.....	49
7.2.	Device Management.....	51
7.3.	TLS Management.....	53
7.3.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise	53
7.3.2.	Server Profiles.....	56
7.3.3.	Client Profiles	60
7.4.	Configuration Profiles	64

7.4.1.	Server Interworking – Avaya-IPO	64
7.4.2.	Server Interworking - SP-General	67
7.4.3.	SIP Server Configuration	71
7.4.4.	Routing Profiles	82
7.4.5.	Topology Hiding	86
7.5.	Domain Policies	90
7.5.1.	Application Rules.....	90
7.5.2.	Media Rules	92
7.5.3.	End Point Policy Groups.....	97
7.6.	Network & Flows Settings	101
7.6.1.	Network Management.....	101
7.6.2.	Media Interface	103
7.6.3.	Signaling Interface	105
7.6.4.	End Point Flows.....	107
8.	Clearcom SIP Trunking Service Configuration	111
9.	Verification Steps.....	112
9.1.	IP Office System Status.....	112
9.2.	Monitor.....	114
9.3.	Avaya Session Border Controller for Enterprise.....	115
10.	Conclusion	120
11.	Additional References.....	120

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 using Transport Layer Security (TLS).

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of an Avaya IP Office Server Edition, two Avaya IP Office 500 V2 as expansion systems, running software release 11.1 (hereafter referred to as IP Office), an Avaya Session Border Controller for Enterprise Release 10.1 (hereafter referred to as Avaya SBCE) 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.

For the testing associated with these Application Notes, the interface between Avaya systems and Clearcom utilized enabled capabilities of TLS/RTP.

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.

- **Secure Real-time Transport Protocol (SRTP):** SRTP supports RTP media protection on a point to point basis providing confidentiality, message authentication, and replay protection. As SRTP is point to point, all individual links involved in the VoIP call, including key exchange/signaling, must be secure for the call to be secure from end to end. During the compliance test, it was observed that RTP, instead of SRTP, was always used outside of the enterprise (public network side). Calls would fail if the use of SRTP was used on the public network side. This behavior may be caused by the far-end not supporting SRTP. Thus, RTP was used on the public side during the compliance test, SRTP for media encryption was used inside of the enterprise (private network side).
- **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. Calls that were blind transferred dropped. On attended transfers, the REFER message was accepted by Clearcom with a 202 message, but the trunk resources were not released. Due to these reasons, 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 outbound calls** – On calls originating from IP Office extensions to PSTN telephones, the caller ID number displayed on the PSTN endpoint was always of the main (pilot) DID number assigned by Clearcom to the SIP trunk, not of the specific DID number assigned to the IP Office extension 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. This may be a requirement of the Clearcom service for all outbound calls, 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 OPTIONS 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 for Enterprise.
- Avaya 96x1 Series IP Deskphones (SIP).
- 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 SBCE. The Avaya SBCE has two physical interfaces, interface **B1** is used to connect to the public network, interface **A1** is used to connect to the private network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. The Avaya SBCE provides network address translation at both the IP and SIP layers.

IP endpoints at the enterprise included Avaya 96x1 Series IP Deskphones (with SIP firmware), 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 SBCE and Clearcom, across the public Internet, is SIP over TLS. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network, is SIP over TLS.

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

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

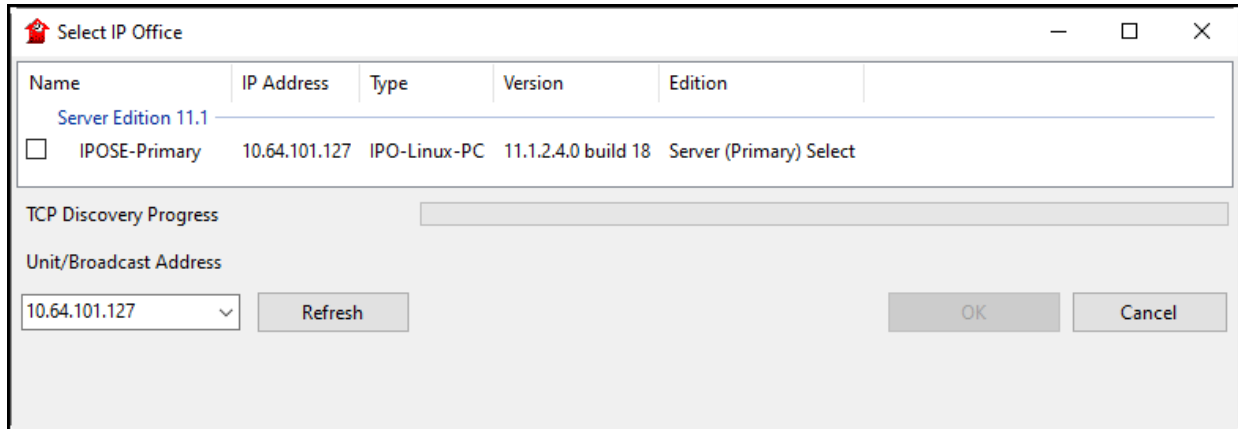
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server)	11.1.2.4.0 Build 18
• Avaya IP Office Voicemail Pro	11.1.2.4.0 Build 2
Avaya IP Office IP500 V2 (Expansion Systems)	11.1.2.4.0 Build 18
Avaya IP Office Manager	11.1.2.4.0 Build 18
Avaya Session Border Controller for Enterprise	ASBCE 10.1.0 0-32-21432
Avaya 96x1 Series IP Deskphones (SIP)	Version 7.1.15.2.1
Avaya J179 IP Telephone (H.323)	Version 6.8.5.3.2
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.1.1.0.7
Avaya 1408 Digital Telephone	48.02
Avaya Workplace Client for Windows (SIP).	3.32.0.75
Analog Telephone	---
Clearcom	
OpenSIPS Softswitch	2.6.2
OpenSIPS Session Border Controller	2.6.2

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

5. Avaya IP Office Primary Server Configuration

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



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

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: 8de6c6d337bc354d6ec88494533af87bb2d6e950

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

Open...

- Configuration
- System Status
- Voicemail Administration
- Resiliency Administration
- On-boarding
- IP Office Web Manager
- Help
- Set All Nodes License Source

Add...

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 shows the Configuration Manager interface. The left pane displays a tree view with 'License' selected under the 'IPOSE-Primary' system. The right pane shows the 'License Remote Server' configuration. The 'License Mode' is 'License Normal' and the 'Licensed Version' is '11.0'. Below this is a table of features with columns for Feature, Instances, Status, Expiration Date, and Source.

Feature	Instances	Status	Expiration Date	Source
Office Worker	1000	Valid	Never	PLDS Nodal
VMPPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	1	Obsolete	Never	PLDS Nodal
Power User	1000	Valid	Never	PLDS Nodal
Customer Service Agent	5	Dormant	Never	PLDS Nodal
Customer Service Supervisor	5	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
Avaya Softphone Licence	1000	Valid	Never	PLDS Nodal
SM Trunk Channels	128	Valid	Never	PLDS Nodal
Web Collaboration	64	Valid	Never	PLDS Nodal
Avaya Contact Center Select	1	Valid	Never	PLDS Nodal
Allow Virtualization	10	Valid	Never	PLDS Nodal
Devlink3 External Recorder	1	Valid	Never	PLDS Nodal
Basic User	1000	Obsolete	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.

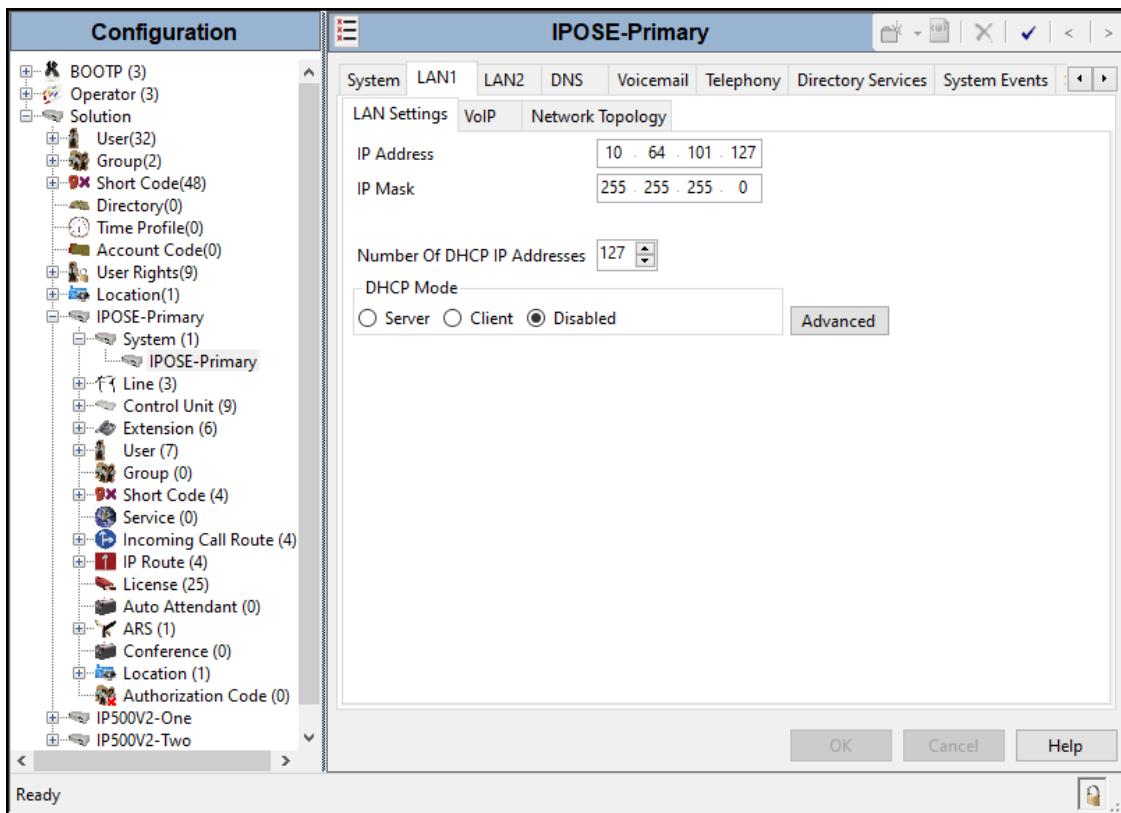
5.2.1. System - LAN1 Tab

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 SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE 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:

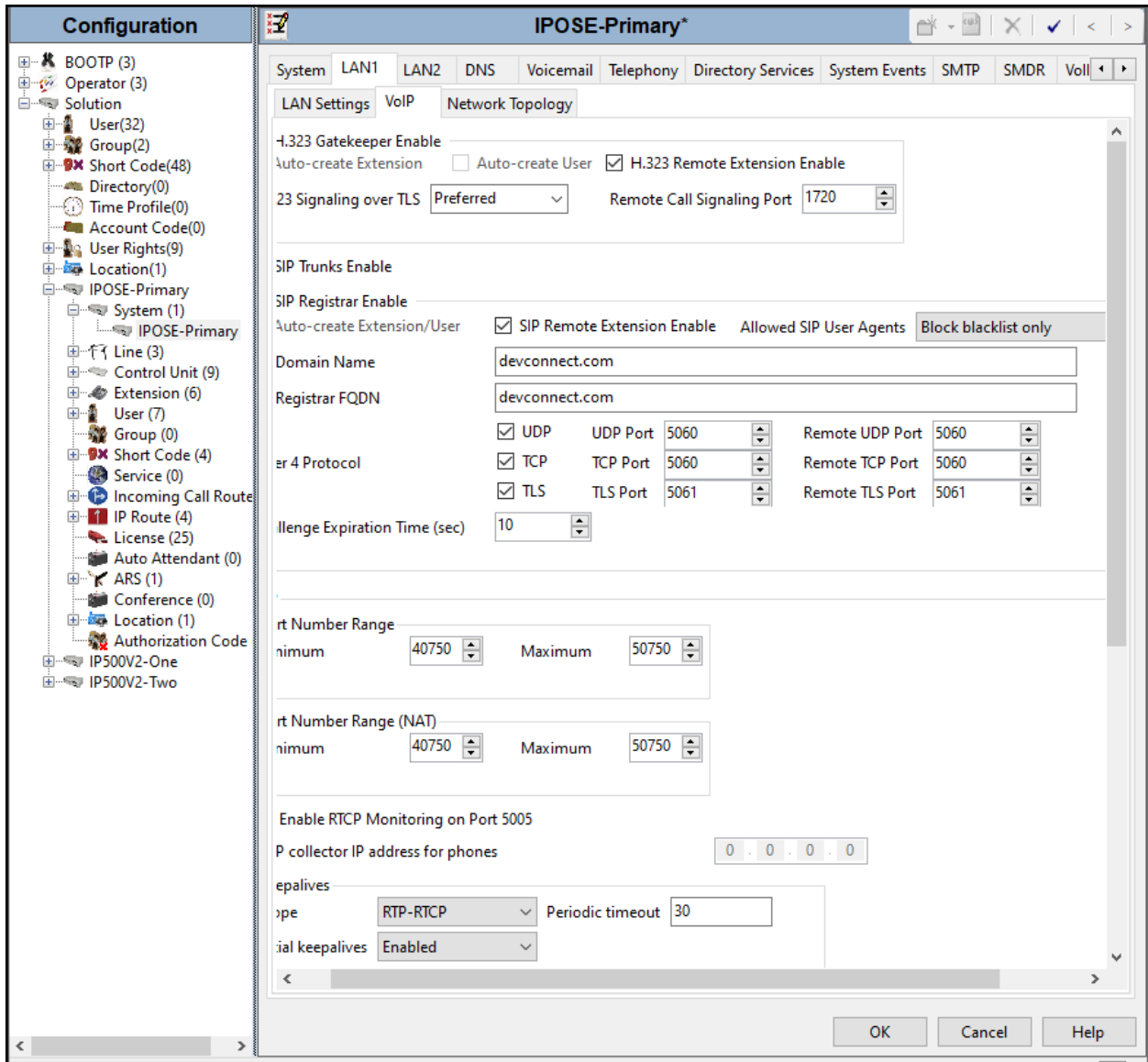
- Set the **IP Address** field to the LAN IP address, e.g., **10.64.101.127**.
- Set the **IP Mask** field to the subnet mask of the enterprise private network, e.g., **255.255.255.0**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit.



5.2.1.2 LAN1 VoIP Tab

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

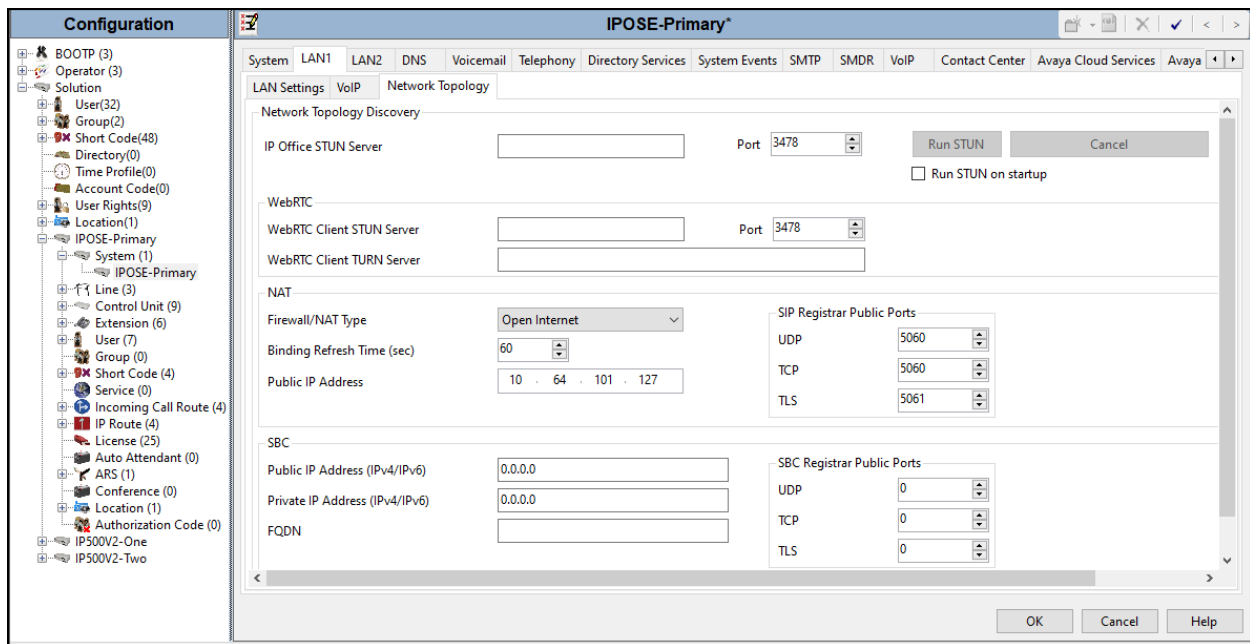
- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Select **Preferred** under **H.323 Signaling over TLS**. When enabled, TLS is used to secure the registration and call signaling communication between IP Office and endpoints that support 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**.
- 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:

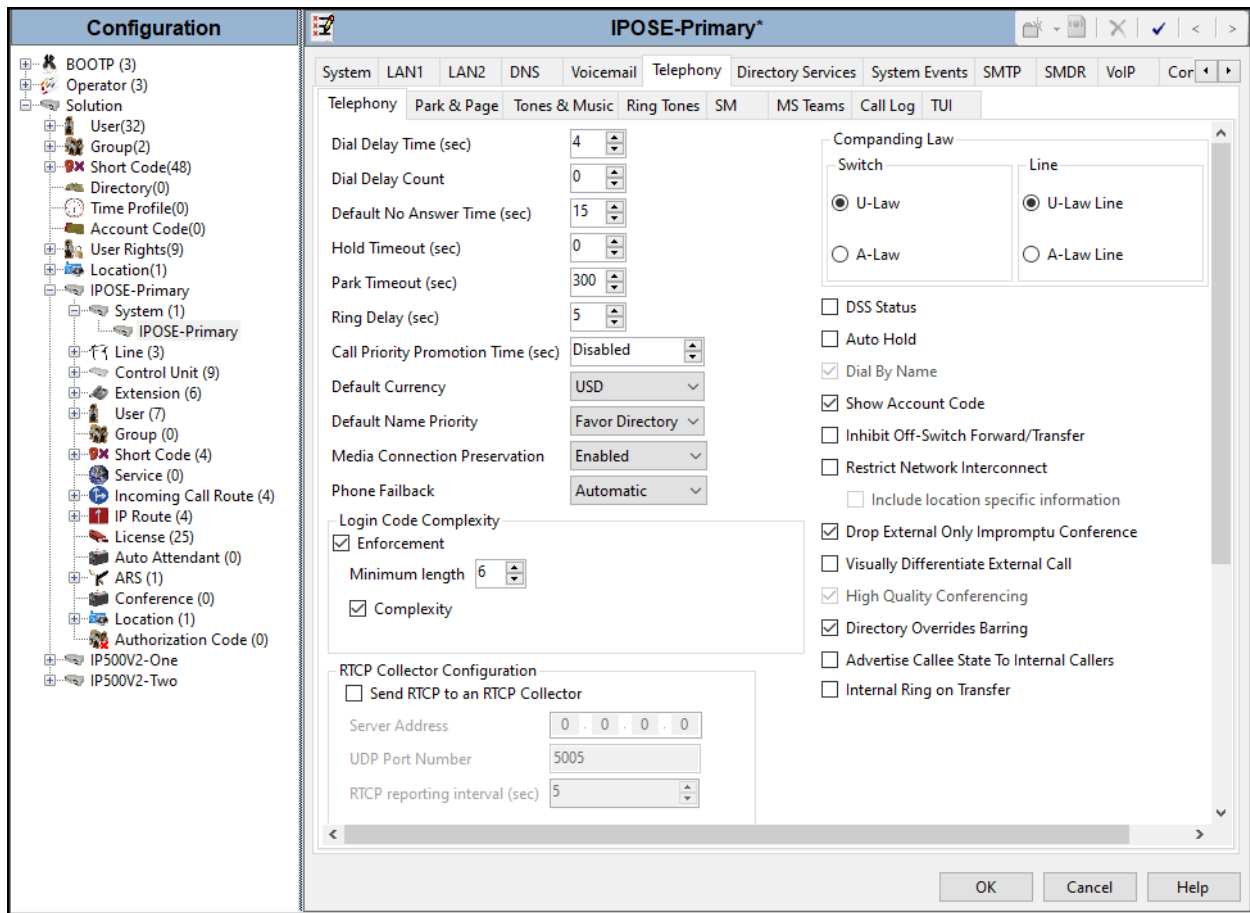
- The **Firewall/NAT Type** was set to **Open Internet** in the reference configuration.
- The **Binding Refresh Time (sec)** was set to **60** seconds. This is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages, to periodically check the status of the SIP lines configured 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.



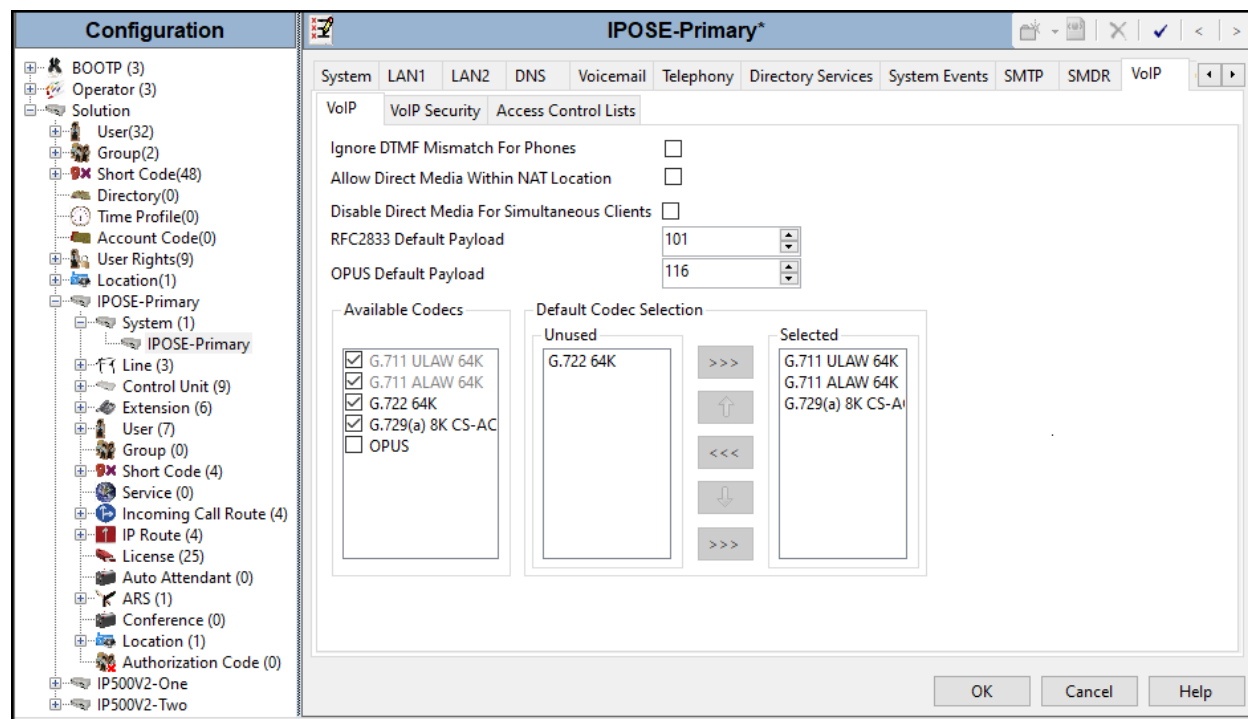
5.2.3. System - VoIP Tab

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.

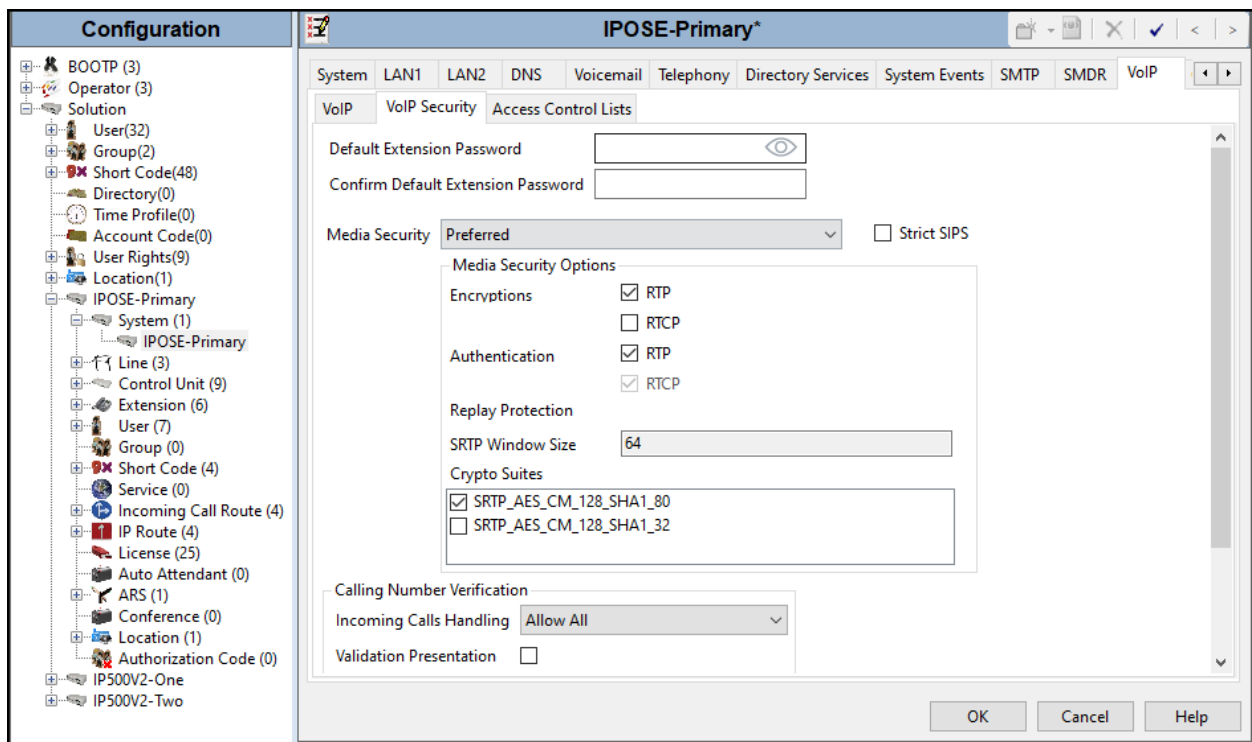
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

- 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.

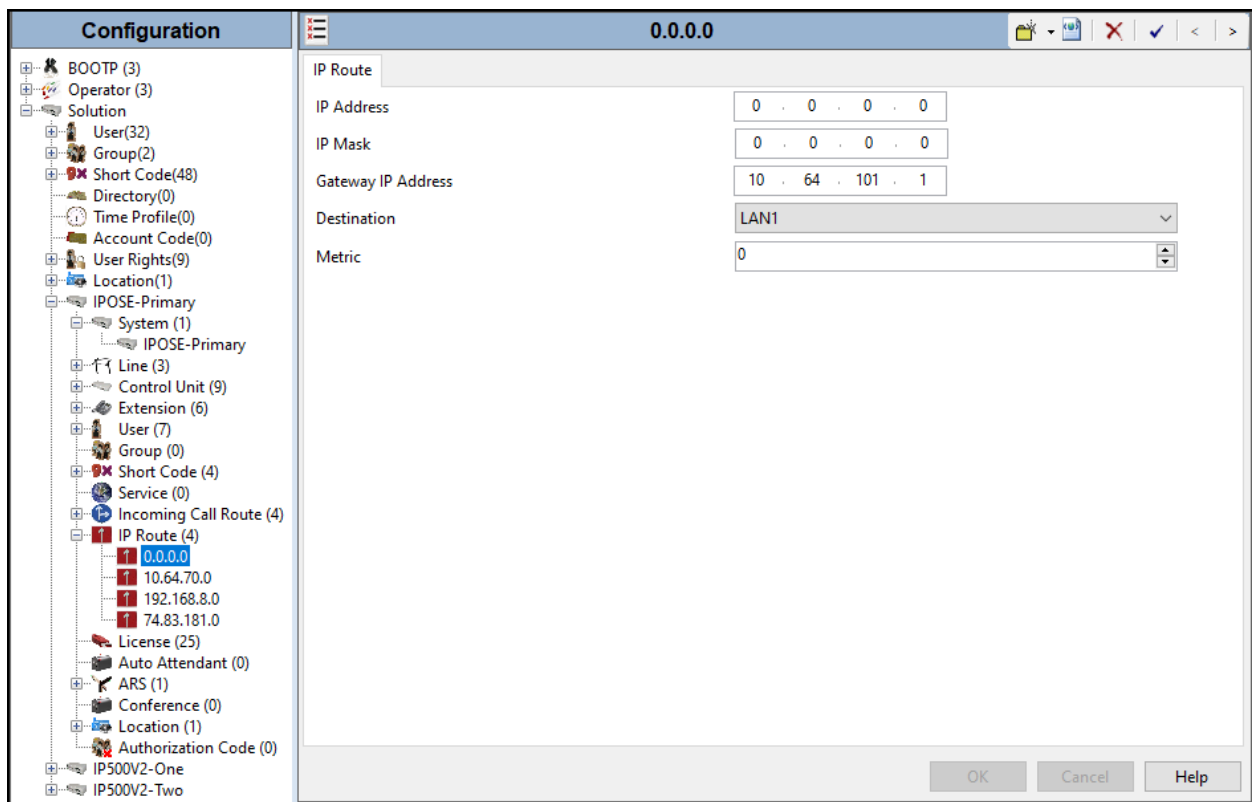


5.3. IP Route

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**.

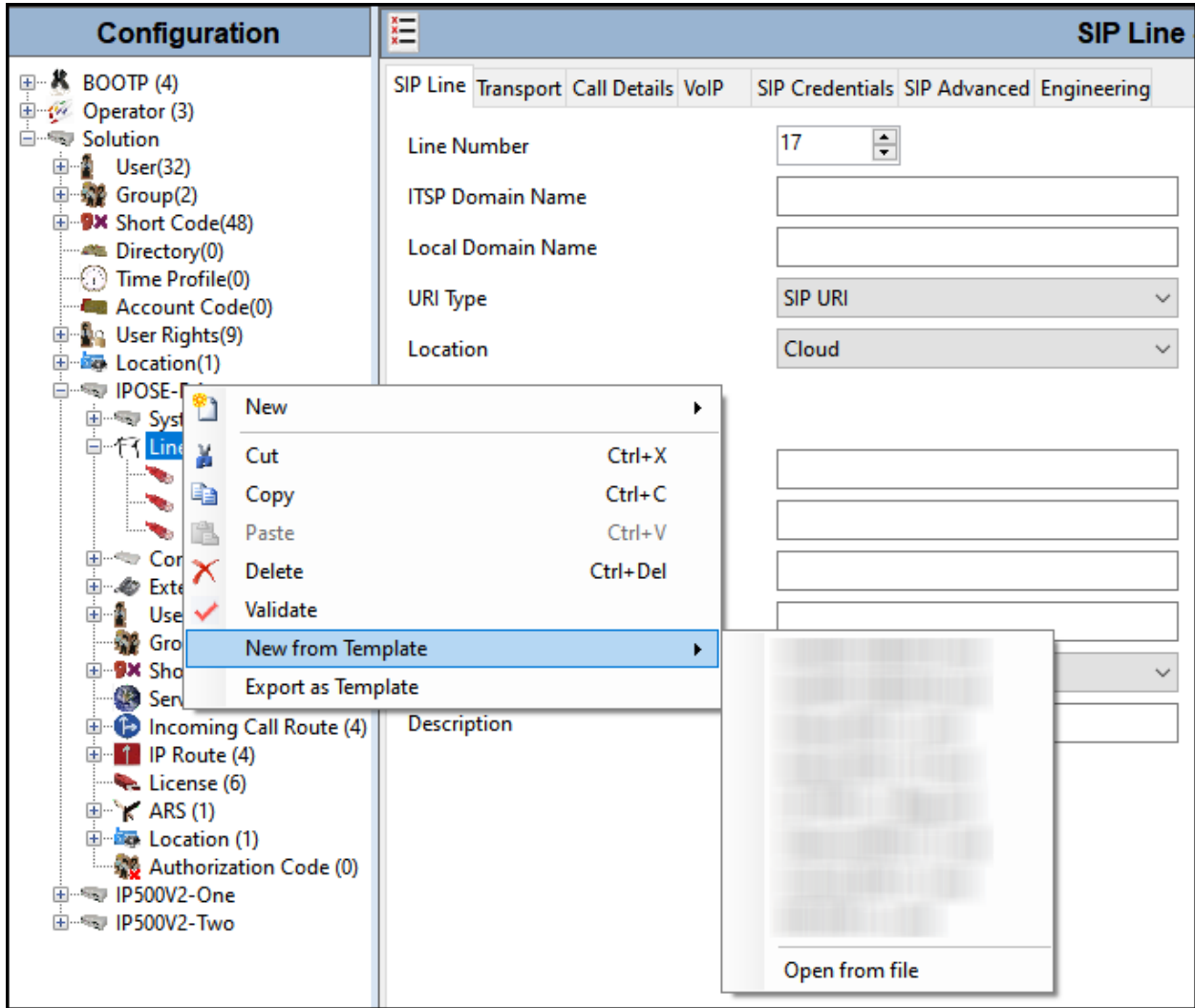
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New** → **SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.6**.

5.4.1. Creating a SIP Trunk from an XML Template

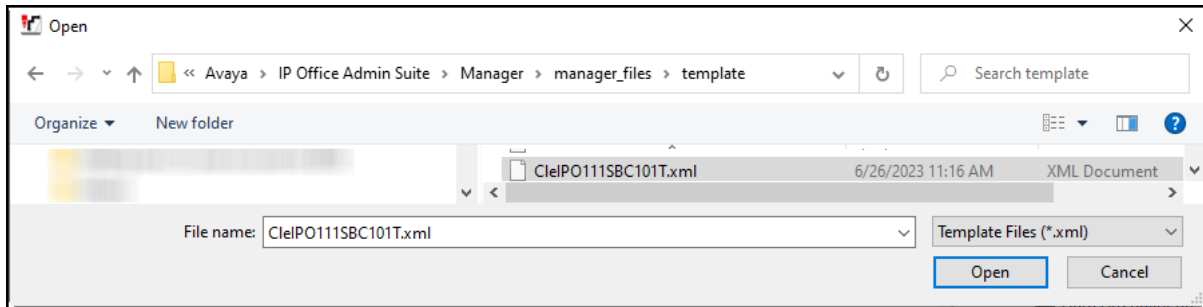
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and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

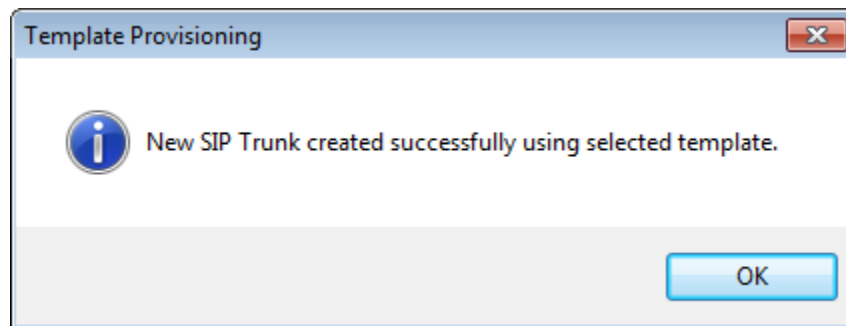
To create the SIP Trunk from the template, from the **Primary** server, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template→Open from file**.



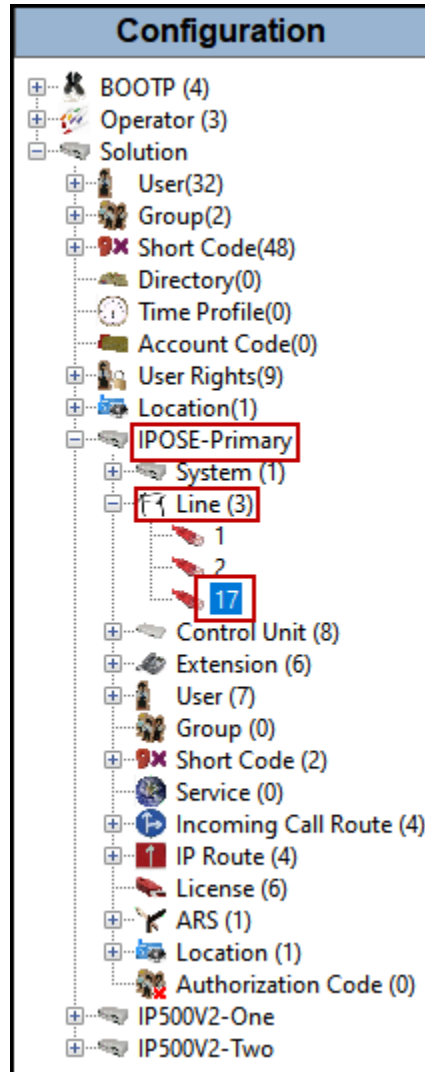
Navigate to the directory on the local machine where the template was copied and select the template.



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 Avaya IP Office configuration interface for a SIP Line. The left pane shows a tree view of the configuration hierarchy, including 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, Auto Attendant, ARS, Conference, Location, Authorization Code, and IP500V2-One/Two.

The main pane shows the **SIP Line - Line 17** configuration page. The **SIP Line** tab is selected. The configuration fields are as follows:

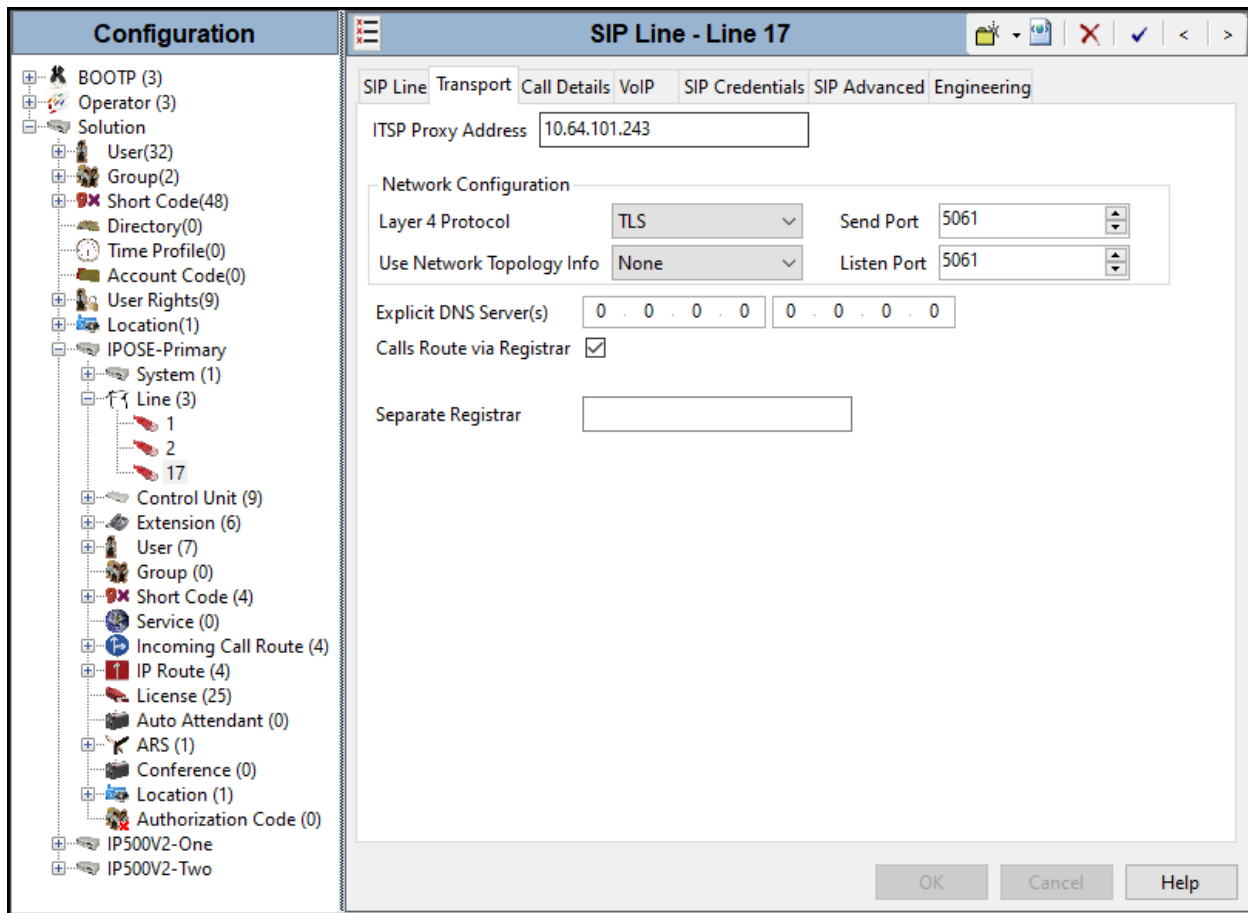
Field	Value	Field	Value
Line Number	17	In Service	<input checked="" type="checkbox"/>
ITSP Domain Name		Check OOS	<input checked="" type="checkbox"/>
Local Domain Name		Session Timers	
URI Type	SIP URI	Refresh Method	Auto
Location	Cloud	Timer (sec)	On Demand
Prefix		Redirect and Transfer	
National Prefix		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		

Buttons at the bottom: OK, Cancel, Help.

5.4.3. SIP Line - Transport Tab

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

- Set the **ITSP Proxy Address** to the inside IP Address of the Avaya SBCE or **10.64.101.243** as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **TLS**.
- Set **Use Network Topology Info** to **None** (see note below).
- Set the **Send Port** to **5061**.
- Default values may be used for all other parameters.
- Click **OK** to commit.



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 provided by Clearcom for SIP Trunk registration purpose was used under the **Display** and **Content** columns for **Local URI**, this setting is needed since Clearcom requires the user name to be sent in the “From” header.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.

	Display	Content	Field meaning		
			Outgoing Calls	Forwarding/Twining	Incoming Calls
Local URI	user123	user123	Explicit	Explicit	Explicit
Contact	Auto	Auto	Caller	Original Caller	Called
P Asserted ID	<input checked="" type="checkbox"/> Auto	Auto	Caller	Original Caller	Called
P Preferred ID	<input type="checkbox"/> None	None	None	None	None
Diversion Header	<input checked="" type="checkbox"/> Auto	Auto	None	Caller	None
Remote Party ID	<input type="checkbox"/> None	None	None	None	None

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 SBCE).
- 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.

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

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

 Below this, there are columns for 'Display' and 'Content' for various fields:

- Local URI: Display: Auto, Content: Auto
- Contact: Display: Auto, Content: Auto
- P Asserted ID: None, Content: None
- P Preferred ID: None, Content: None
- Diversion Header: None, Content: None
- Remote Party ID: None, Content: None

 A 'Field meaning' table is also present:

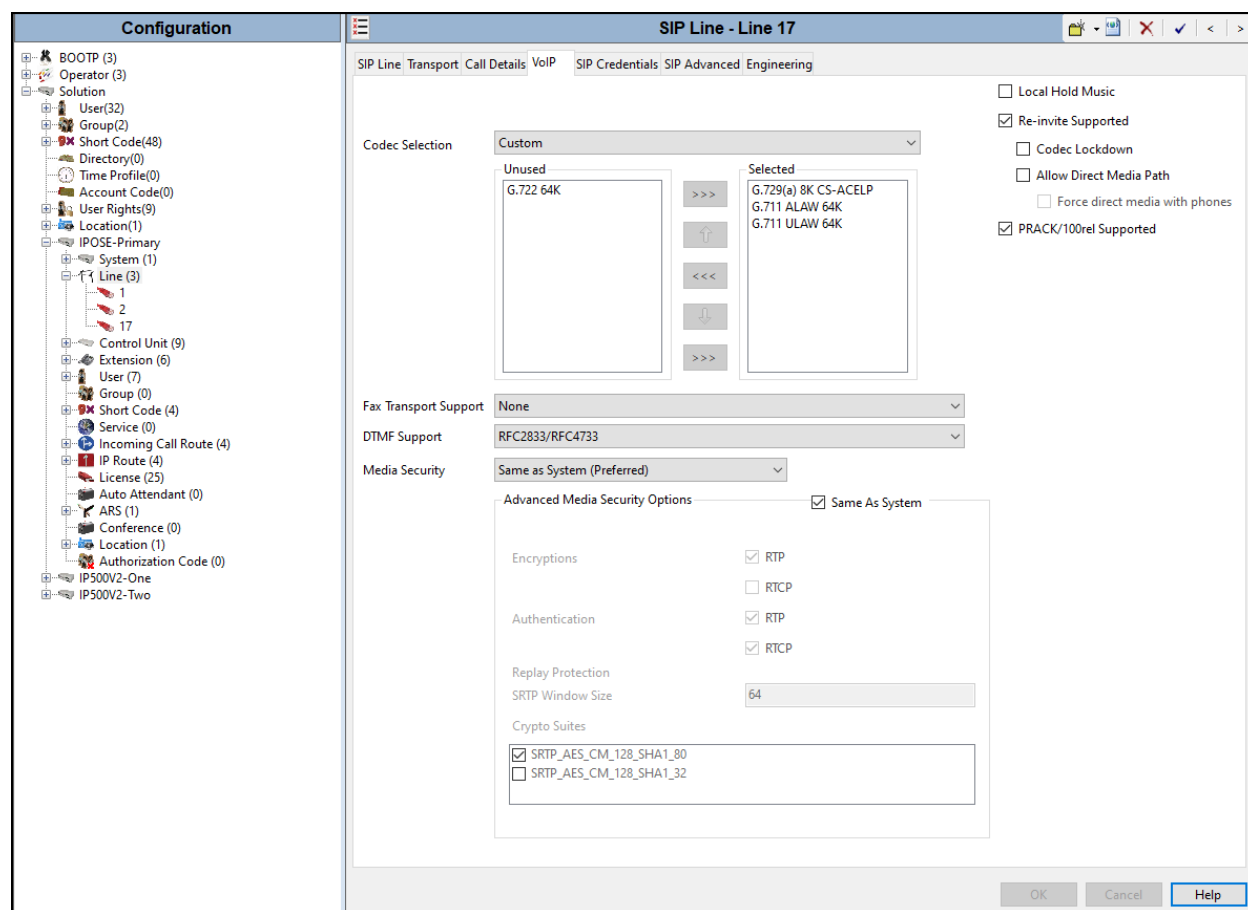
	Outgoing Calls	Forwarding/Twining	Incoming Calls
Local URI	Caller	Original Caller	Called
Contact	Caller	Original Caller	Called
P Asserted ID	None	None	None
P Preferred ID	None	None	None
Diversion Header	None	None	None
Remote Party ID	None	None	None

 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.
- Check the **PRACK/100rel Supported** box.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- Default values may be used for all other parameters.
- Click the **OK** to commit.



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).

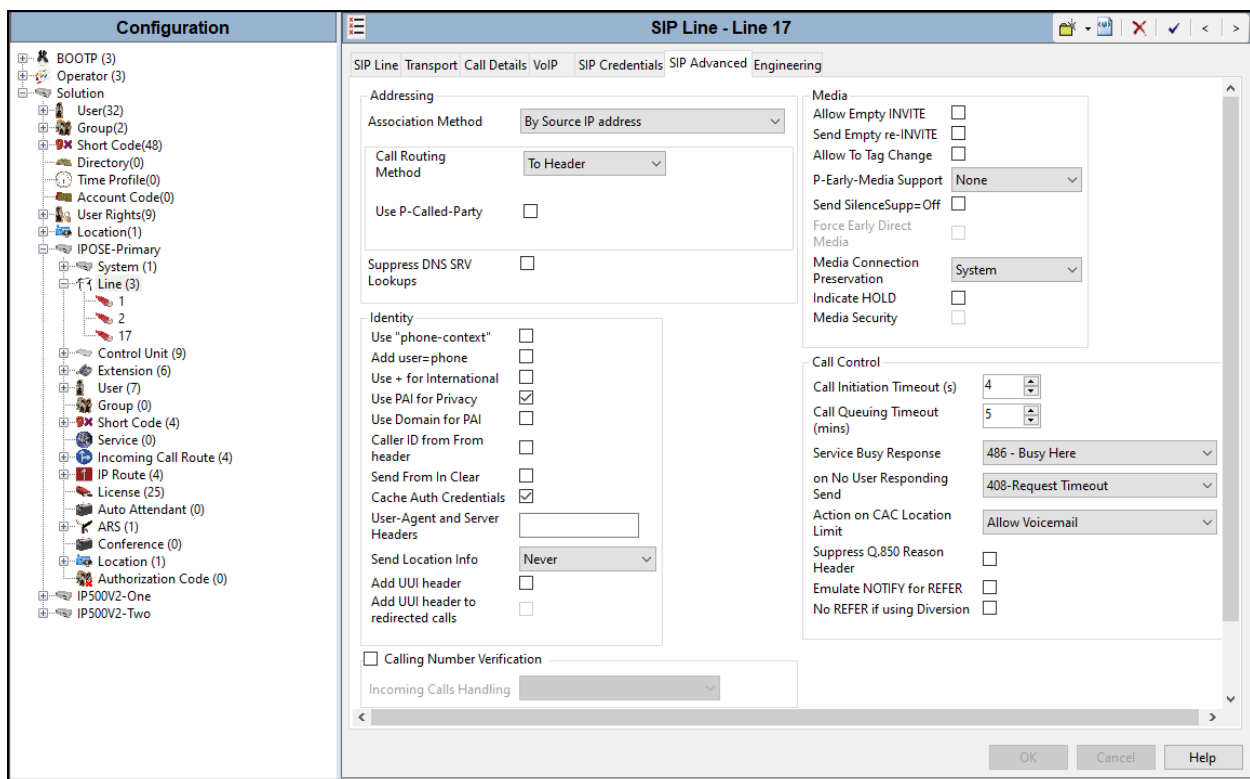
5.4.6. SIP Line – SIP Advanced Tab

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-One Expansion System.

The screenshot displays the configuration interface for an IP Office Line. On the left is a navigation tree under the 'Configuration' header, showing a hierarchy from 'Solution' down to 'IP500V2-One' and 'IP500V2-Two'. The main area is titled 'IP Office Line - Line 1' and contains several tabs: 'Line', 'Short Codes', and 'VoIP Settings'. The 'Line' tab is active, showing the following fields:

- Line Number: 1
- Transport Type: WebSocket Server
- Networking Level: SCN
- Security: Unsecured
- Telephone Number: (empty)
- Prefix: (empty)
- Outgoing Group ID: 99999
- Number of Channels: 250
- Outgoing Channels: 250

Below these fields is a 'Gateway' section with the following fields:

- Address: 192 . 168 . 8 . 165
- Location: 3: Thornton, CO
- Password: (masked with dots)
- Confirm Password: (masked with dots)

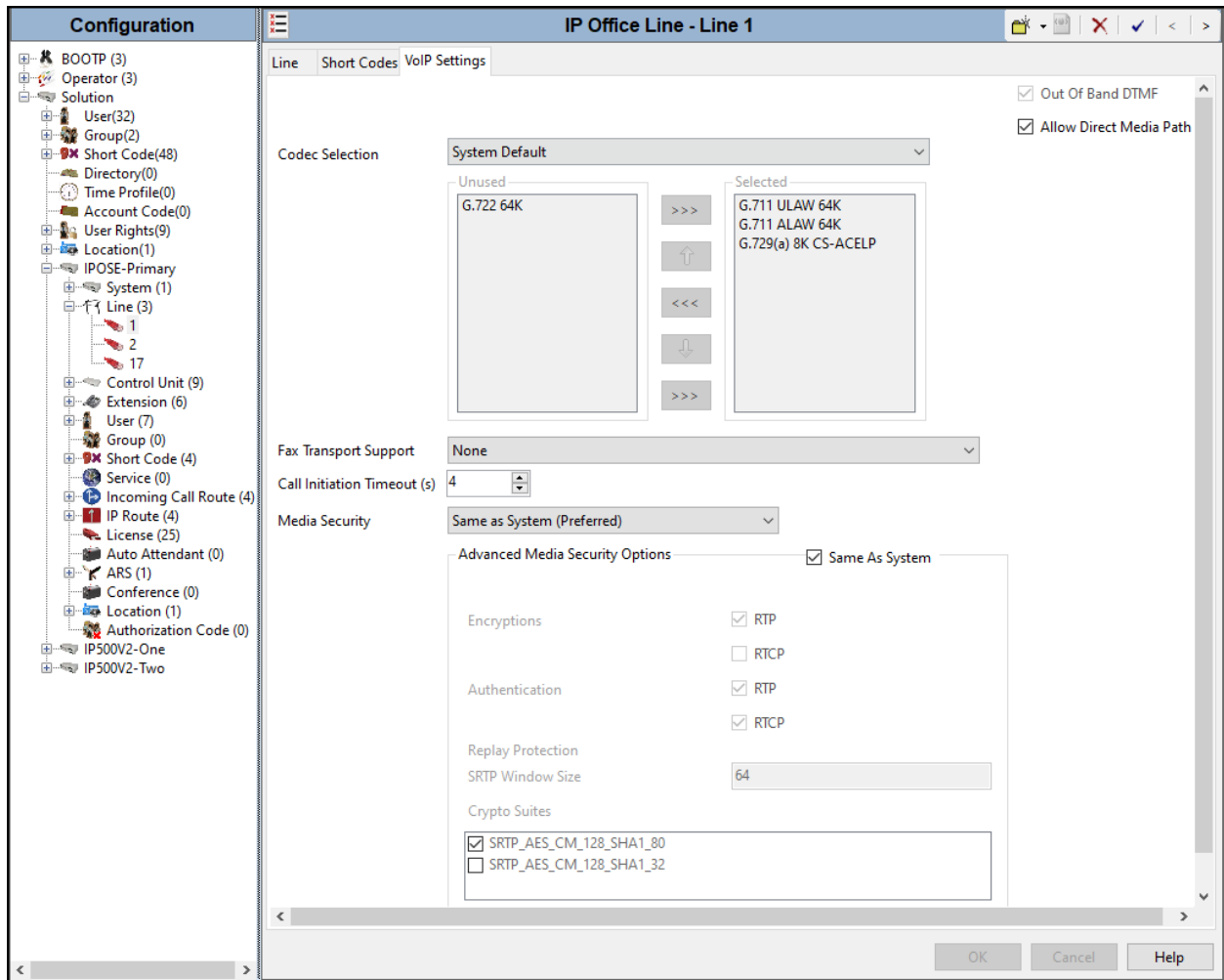
To the right of the Gateway fields is the 'SCN Resiliency Options' section, which includes a checkbox for 'Supports Resiliency' and three sub-options, all of which are currently unchecked:

- Supports Resiliency
 - Backs up my IP phones
 - Backs up my hunt groups
 - Backs up my voicemail
 - Backs up my IP DECT phones

At the bottom of the window is a 'Description' field (empty) and three buttons: 'OK', 'Cancel', and 'Help'.

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

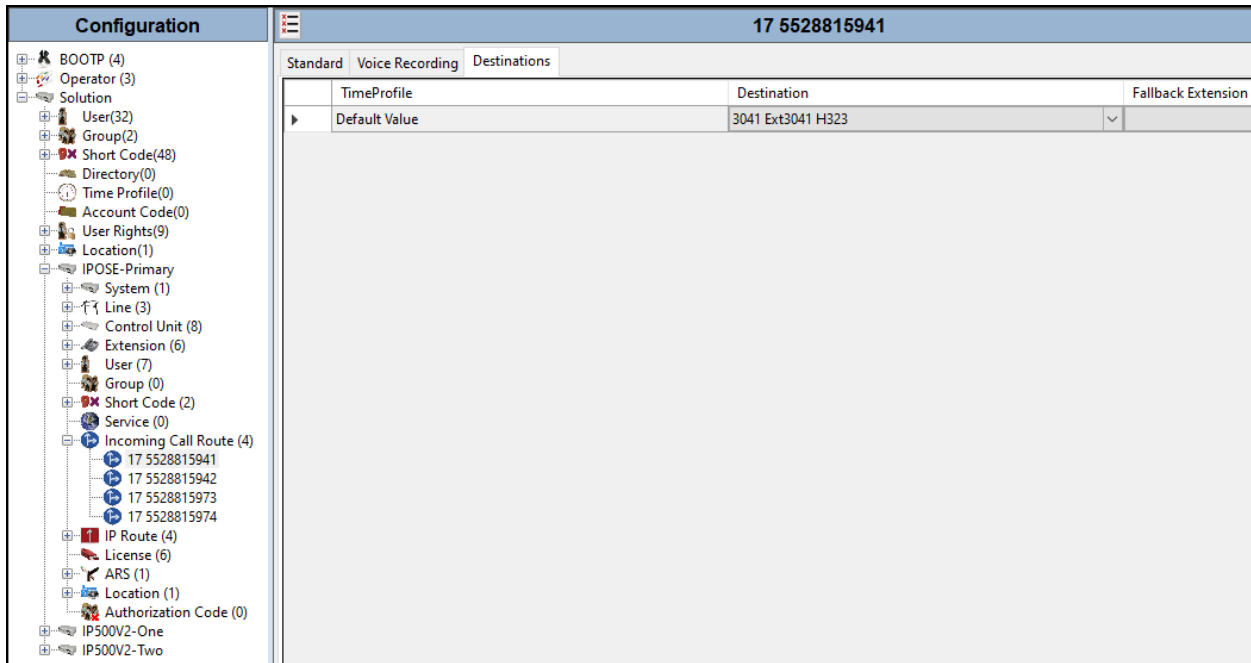
Incoming call routes map inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system. To add an incoming call route, right click on **Incoming Call Route** in the **Navigation** pane and select **New** (not shown). On the Details Pane, under 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 a navigation tree under the 'Configuration' header, showing a hierarchy of system components. The 'Incoming Call Route (4)' folder is expanded, and the entry '17 5528815941' is selected. On the right, the configuration details for this route are shown under the 'Standard' tab. The parameters are as follows:

Parameter	Value
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**.



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	81XXXXXXXX	OK
Feature	Dial	Cancel
Telephone Number	81N	
Line Group ID	17	
Locale	Mexico (Latin Spanish)	
Force Account Code	<input type="checkbox"/>	
Force Authorization Code	<input type="checkbox"/>	

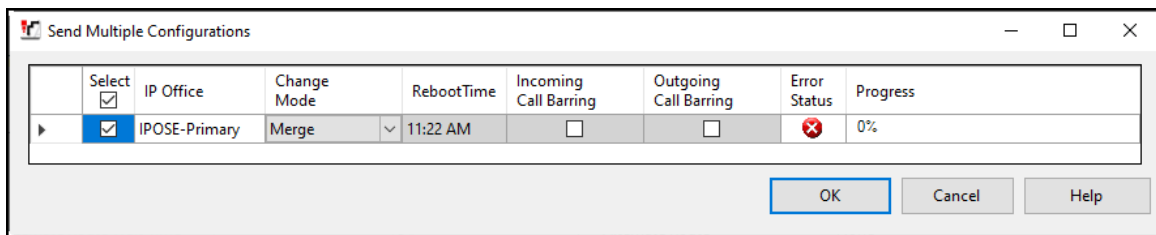
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

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-One** on the left navigation pane will expand the menu on this server.

Configuration	System Inventory
<ul style="list-style-type: none"> ⊕ BOOTP (4) ⊕ Operator (3) ⊖ Solution <ul style="list-style-type: none"> ⊕ User(32) ⊕ Group(2) ⊕ Short Code(48) ⊕ Directory(0) ⊕ Time Profile(0) ⊕ Account Code(0) ⊕ User Rights(9) ⊕ Location(1) ⊕ IPOSE-Primary ⊖ IP500V2-One <ul style="list-style-type: none"> ⊕ System (1) ⊕ Line (3) ⊕ Control Unit (4) ⊕ Extension (24) ⊕ User (27) ⊕ Group (1) ⊕ Short Code (12) ⊕ Service (0) ⊕ RAS (1) ⊕ Incoming Call Route (1) ⊕ WAN Port (0) ⊕ Firewall Profile (1) ⊕ IP Route (4) ⊕ License (2) ⊕ Tunnel (0) ⊕ ARS (2) ⊕ Location (1) ⊕ Authorization Code (0) ⊕ IP500V2-Two 	<div style="border: 1px solid #ccc; padding: 5px;"> <h3 style="margin: 0;">Server Edition Expansion System</h3> <ul style="list-style-type: none"> ⊖ <u>Hardware Installed</u> <ul style="list-style-type: none"> Control Unit: IP 500 V2 Internal Modules: VCM64/PRID U; PHONE8 Expansion Modules: DIG DCPx16 V2 ⊖ <u>System Settings</u> <ul style="list-style-type: none"> IP Address: 192.168.8.165 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 ⊖ <u>Features Configured</u> <ul style="list-style-type: none"> Licenses Installed: Server Edition(1); IP Office Select(1); Basic User(25) Connected Extensions: 3043; 3044 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 </div>

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.

The screenshot displays the Configuration Manager interface for an IP 500 V2 unit. The left pane shows a hierarchical tree of configuration objects, with the IP500V2-One system selected. The right pane shows the configuration details for the selected unit, including fields for Device Number, Unit Type, Version, Serial Number, Unit IP Address, Interconnect Number, and Module Number. The Module Number is set to Control Unit.

Field	Value
Device Number	1
Unit Type	IP 500 V2
Version	11.1.2.4.0 build 18
Serial Number	00e00706530f
Unit IP Address	192.168.8.165
Interconnect Number	0
Module Number	Control Unit

6.2. LAN Settings

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

- **IP Address: 192.168.8.165** was used in the reference configuration.
- **IP Mask: 255.255.255.0** was used in the reference configuration
- Click the **OK** button (not shown).

The screenshot displays the configuration interface for an IP500V2-One system. On the left is a navigation tree under 'Configuration' with 'IP500V2-One' selected. The main pane shows the 'LAN Settings' tab for 'LAN1'. The configuration fields are as follows:

Field	Value
IP Address	192 . 168 . 8 . 165
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	0 . 0 . 0 . 0
RIP Mode	None
Enable NAT	<input type="checkbox"/>
Number Of DHCP IP Addresses	200
DHCP Mode	<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dial In <input checked="" type="radio"/> Disabled

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

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

6.3. IP Route

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

- Enter **0.0.0.0** on the **IP Address** and **IP Mask** fields to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet. The default gateway in the reference configuration was **192.168.8.1**
- Set **Destination** to **LAN1** from the pull-down menu.

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view under 'Configuration' for 'IP500V2-One'. The 'IP Route' folder is expanded, showing four entries: '0.0.0.0' (highlighted in blue), '10.64.101.0', '192.168.8.0', and '192.168.99.0'. On the right, the configuration details for the selected '0.0.0.0' route are shown:

0.0.0.0	
IP Route	
IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	192 . 168 . 8 . 1
Destination	LAN1
Metric	0
	<input type="checkbox"/> Proxy ARP

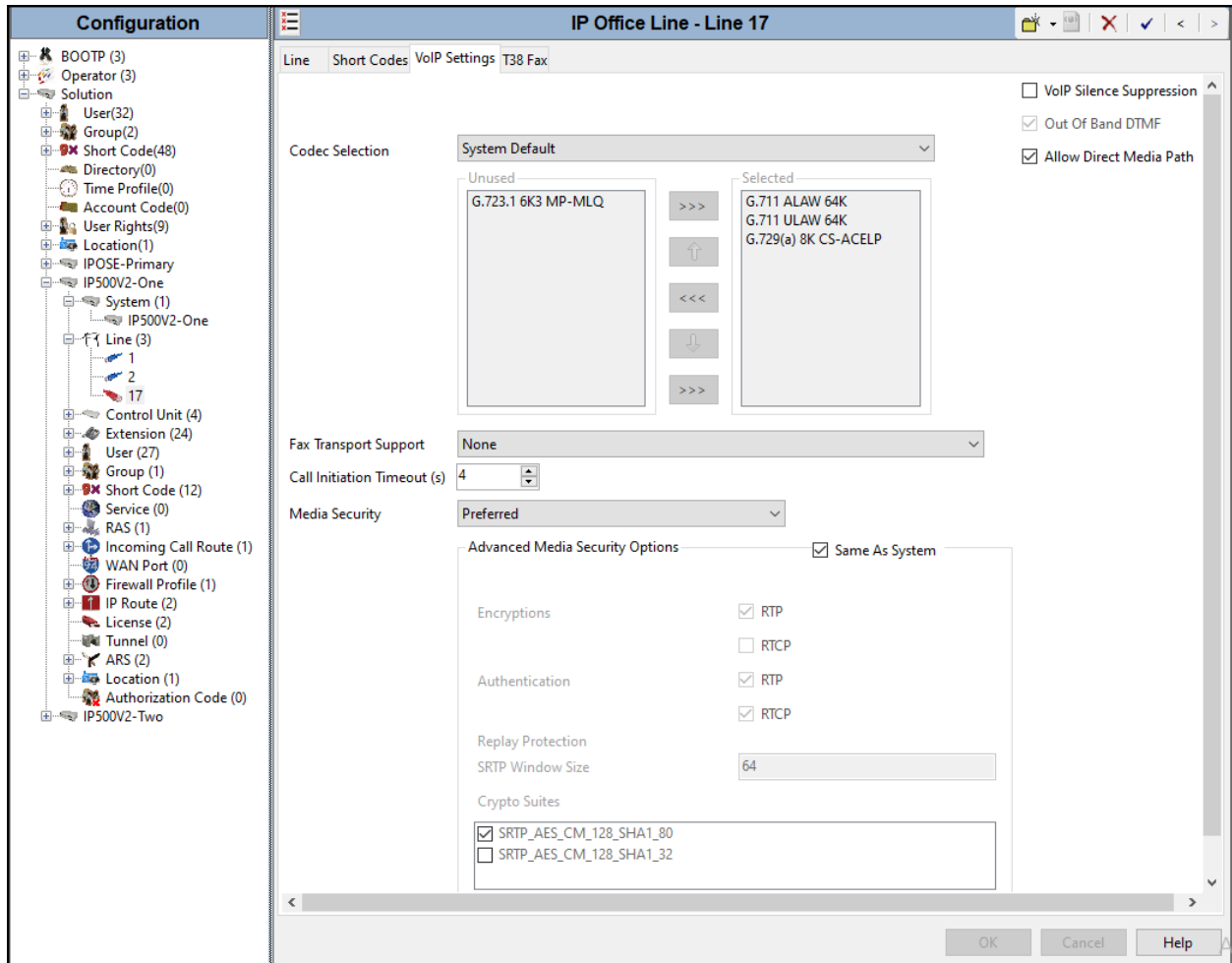
6.4. IP Office Line – IP500 V2 Expansion System

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.

Configuration	IP Office Line - Line 17*			
<ul style="list-style-type: none"> BOOTP (4) Operator (3) Solution <ul style="list-style-type: none"> User(32) Group(2) Short Code(48) Directory(0) Time Profile(0) Account Code(0) User Rights(9) Location(1) IPOSE-Primary IP500V2-One <ul style="list-style-type: none"> System (1) Line (3) <ul style="list-style-type: none"> 1 2 17 Control Unit (4) Extension (24) User (27) Group (1) Short Code (12) Service (0) RAS (1) Incoming Call Route (1) WAN Port (0) Firewall Profile (1) IP Route (4) License (2) Tunnel (0) ARS (2) Location (1) Authorization Code (0) IP500V2-Two 	Line Short Codes VoIP Settings T38 Fax			
	Line Number	<input type="text" value="17"/>	Telephone Number	<input type="text"/>
	Transport Type	WebSocket Client	Prefix	<input type="text"/>
	Networking Level	SCN	Outgoing Group ID	99999
	Security	Medium	Number of Channels	250
			Outgoing Channels	250
	Gateway		Port	443
	Address	10 . 64 . 101 . 127	SCN Resiliency Options <input type="checkbox"/> Supports Resiliency <input type="checkbox"/> Backs up my IP phones <input type="checkbox"/> Backs up my hunt groups <input type="checkbox"/> Backs up my IP DECT phones	
	Location	3: Thornton, CO		
	Password	••••••••		
Confirm Password	••••••••			
Description	<input type="text"/>			

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.

Configuration	9N: Dial														
<ul style="list-style-type: none"> ⊕ BOOTP (4) ⊕ Operator (3) ⊖ Solution <ul style="list-style-type: none"> ⊕ User(32) ⊕ Group(2) ⊕ 9X Short Code(48) ⊖ Directory(0) ⊖ Time Profile(0) ⊖ Account Code(0) ⊕ User Rights(9) ⊕ Location(1) ⊕ IPOSE-Primary ⊖ IP500V2-One <ul style="list-style-type: none"> ⊕ System (1) ⊕ Line (3) ⊕ Control Unit (4) ⊕ Extension (24) ⊕ User (27) ⊕ Group (1) ⊖ 9X Short Code (12) <ul style="list-style-type: none"> 9X *92N; 9X 9N ⊕ Service (0) ⊕ RAS (1) ⊕ Incoming Call Route (1) ⊕ WAN Port (0) ⊕ Firewall Profile (1) ⊕ IP Route (4) ⊕ License (2) ⊕ Tunnel (0) ⊕ ARS (2) ⊕ Location (1) ⊕ Authorization Code (0) ⊖ IP500V2-Two 	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 5px;">Short Code</div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Code</td> <td><input type="text" value="9N"/></td> </tr> <tr style="background-color: #f0f0f0;"> <td>Feature</td> <td><input type="text" value="Dial"/></td> </tr> <tr> <td>Telephone Number</td> <td><input type="text" value="N"/></td> </tr> <tr> <td>Line Group ID</td> <td><input type="text" value="51: To-Primary"/></td> </tr> <tr style="background-color: #f0f0f0;"> <td>Locale</td> <td><input type="text" value="Mexico (Latin Spanish)"/></td> </tr> <tr> <td>Force Account Code</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Force Authorization Code</td> <td><input type="checkbox"/></td> </tr> </table> </div>	Code	<input type="text" value="9N"/>	Feature	<input type="text" value="Dial"/>	Telephone Number	<input type="text" value="N"/>	Line Group ID	<input type="text" value="51: To-Primary"/>	Locale	<input type="text" value="Mexico (Latin Spanish)"/>	Force Account Code	<input type="checkbox"/>	Force Authorization Code	<input type="checkbox"/>
Code	<input type="text" value="9N"/>														
Feature	<input type="text" value="Dial"/>														
Telephone Number	<input type="text" value="N"/>														
Line Group ID	<input type="text" value="51: To-Primary"/>														
Locale	<input type="text" value="Mexico (Latin Spanish)"/>														
Force Account Code	<input type="checkbox"/>														
Force Authorization Code	<input type="checkbox"/>														

6.6. Automatic Route Selection – ARS

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

The screenshot displays the configuration for an ARS route named "To-Primary". The left sidebar shows a tree view of the configuration hierarchy, with "51: To-Primary" selected under the "ARS" category. The main configuration area includes the following fields and options:

- ARS Route ID:** 51
- Route Name:** To-Primary
- Dial Delay Time:** System Default (4)
- Description:** (empty field)
- In Service:** (checked)
- Out of Service Route:** <None>
- Time Profile:** <None>
- Out of Hours Route:** <None>
- Secondary Dial tone:** (unchecked), SystemTone (dropdown)
- Check User Call Barring:** (unchecked)

Below these fields is a table listing the route configuration:

Code	Telephone Number	Feature	Line Group ID
N	9N	Dial	99999

Additional configuration options include:

- Alternate Route Priority Level:** 3
- Alternate Route Wait Time:** 30
- Alternate Route:** <None>

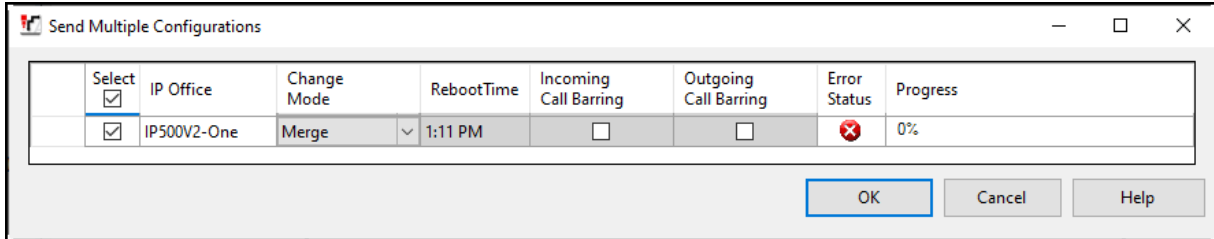
Buttons for "Add...", "Remove", and "Edit..." are visible next to the table.

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 for Enterprise

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

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

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

7.1. Log in Avaya SBCE

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

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



The screenshot shows the Avaya login interface. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right, under the heading "Log In", there are input fields for "Username:" (containing "test") and "Password:". Below these is a "Log In" button. At the bottom, there is a disclaimer: "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." and a copyright notice: "© 2011 - 2020 Avaya Inc. All rights reserved."

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

The screenshot displays the Avaya EMS Controller for Enterprise interface. At the top, the navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar, under 'EMS Dashboard', lists various management options. The main dashboard area is divided into two sections: 'Information' and 'Installed Devices'. The 'Information' section provides system status details, including system time, version, GUI version, build date, license state (OK), and licensing overages. The 'Installed Devices' section lists the current device as 'Avaya_SBCE'.

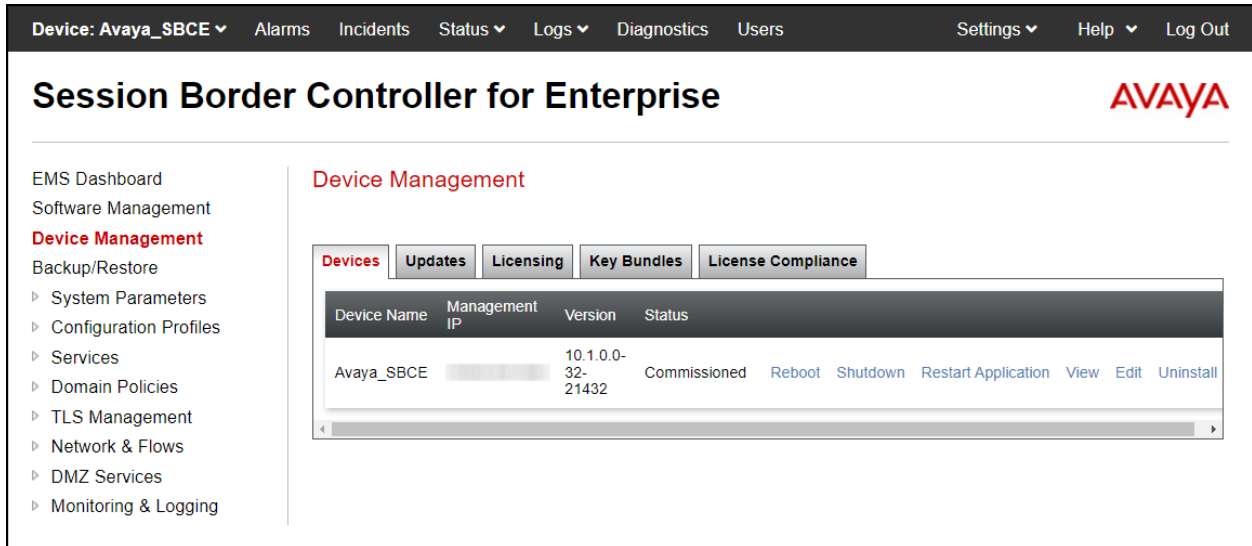
Information	
System Time	10:35:55 AM EDT Refresh
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-22609
Build Date	Thu Nov 10 12:33:00 UTC 2022
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	06/05/2023 10:31:52 EDT

Installed Devices	
EMS	
Avaya_SBCE	

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

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_SBCE** is shown. The management IP address that was configured during installation is blurred out for security reasons; the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



The screenshot displays the Avaya SBCE management interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo. The left navigation pane lists various management options, with 'Device Management' highlighted. The 'Device Management' section contains tabs for 'Devices', 'Updates', 'Licensing', 'Key Bundles', and 'License Compliance'. The 'Devices' tab is active, showing a table with the following data:

Device Name	Management IP	Version	Status						
Avaya_SBCE	[Blurred]	10.1.0.0-32-21432	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

To view the network configuration assigned to the Avaya SBCE, 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_SBCE

General Configuration

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	100	200
Advanced Sessions	100	200
Scopia Video Sessions	0	0
CES Sessions	0	0
Transcoding Sessions	100	200
AMR	<input type="checkbox"/>	
Premium Sessions	0	0
CLID	---	
Encryption Available: Yes	<input checked="" type="checkbox"/>	

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
[Masked]	[Masked]	[Masked]	[Masked]	A1
[Masked]	[Masked]	[Masked]	[Masked]	A1
[Masked]	[Masked]	[Masked]	[Masked]	B1
[Masked]	[Masked]	[Masked]	[Masked]	B1
10.10.80.51	10.10.80.51	255.255.255.128	10.10.80.1	B1

DNS Configuration

Primary DNS	75.75.75.75
Secondary DNS	75.75.76.76
DNS Location	DMZ
DNS Client IP	10.10.80.51

Management IP(s)

IP #1 (IPv4)	[Masked]
--------------	----------

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 SBCE **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 SBCE (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 to enable TLS encryption inside of the enterprise (private network side). Also, testing was done with identity certificates signed by a 3rd party trusted certificate authority (CA) for enhanced security to enable TLS encryption outside of the enterprise (public network side). The procedure to create/obtain the required TLS certificates is outside the scope of these Application Notes and it's not discussed in these Application Notes.

The following procedures show how to create the client and server profiles to support TLS encryption in the Avaya.

7.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

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



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

- Verify the System Manager Root CA certificate is present in the **Installed CA Certificates** area, this certificate is required to enable TLS encryption inside of the enterprise (private network side). This Root CA certificate needs to be manually downloaded from System Manager and installed in the Avaya SBCE; this Root CA certificate doesn't come pre-loaded in the Avaya SBCE. Certificates from a 3rd party trusted Certificate Authority (CA) could be used for TLS encryption inside of the enterprise (private network side) instead of using Avaya System Manager as the Certificate Authority.
- Verify the **Root CA** certificate for the trusted certificate authority being used by the Service Provider is present in the **Installed CA Certificates** area, required to enable TLS encryption outside of the enterprise (public network side). These Root CA certificates need to be manually loaded/installed in the Avaya SBCE; these Root CA certificates don't come pre-loaded in the Avaya SBCE. The Service Provider (Clearcom) could provide the Root CA certificate to the customer or the customer can download it directly from the 3rd party trusted Certificate Authority home page. The name of the 3rd party trusted Certificate Authority will be required when downloading from the 3rd party trusted Certificate Authority home page. The Service provider (Clearcom) can provide guidance to the customer on how to obtain these certificates.
- Verify the identity certificate signed by the System Manager CA is present in the **Installed Certificates** area.
- Verify the Private key associated with the identity certificate signed by the System Manager CA is present in the **Installed Keys** area (not shown).

Session Border Controller for Enterprise



- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- ▾ TLS Management
 - Certificates**
 - Client Profiles
 - Server Profiles
 - SNI Group
- Network & Flows
- DMZ Services
- Monitoring & Logging

Certificates

Certificates	
Installed Certificates	
sbceExternal.pem	View Delete
[REDACTED]	View Delete
[REDACTED]	View Delete
[REDACTED]	View Delete
IPOSE_INTERNAL.pem	View Delete
Installed CA Certificates	
[REDACTED]	View Delete
[REDACTED]	View Delete
[REDACTED]	View Delete
[REDACTED]	View Delete
default.pem	View Delete
[REDACTED]	View Delete
[REDACTED]	View Delete
[REDACTED].RootCA.crt	View Delete

7.3.2. Server Profiles

7.3.2.1 Inside Server Profile

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

- **Profile Name:** enter descriptive name, e.g., **IPO_Inside_Server**.
- **Certificate:** select the identity certificate, e.g., **IPOSE_INTERNAL.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:

Certificate:

SNI Options:

SNI Group:

Certificate Verification

Peer Verification:

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' 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 (expanded), Certificates, Client Profiles, **Server Profiles** (highlighted), SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging.

The main content area is titled 'Server Profiles: IPO_Inside_Server'. It features an 'Add' button and a 'Delete' button. Below this is a blue bar with the text 'Click here to add a description.' A 'Server Profile' tab is active, showing the configuration for the 'IPO_Inside_Server' profile.

The configuration is organized into several sections:

- TLS Profile**
 - Profile Name: IPO_Inside_Server
 - Certificate: IPOSE_INTERNAL.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 1.2 TLS 1.1 TLS 1.0
 - Ciphers: Default FIPS Custom
 - Value: HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

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

7.3.2.2 Outside Server Profile

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

- **Profile Name:** enter a descriptive name, **Clearcom_Outside_Server** was used.
- **Certificate:** select the identity certificate, e.g., **sbceExternal.pem**, from the pull-down menu.
- **Peer Verification:** Select **None** from the pull-down menu.
- 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: Clearcom_Outside_Server

Certificate: sbceExternal.pem

SNI Options: None

SNI Group: None

Certificate Verification

Peer Verification: None

Peer Certificate Authorities: AvayaDeviceEnrollmentCAchain.crt, avayaitrootca2.pem, entrust_g2_ca.cer, Avaya_EP_CA_cert.pem

Peer Certificate Revocation Lists:

Verification Depth: 0

Next

The following screen shows the completed **Clearcom_Outside_Server** profile form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' 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 (SIP Servers, LDAP, RADIUS), Domain Policies, TLS Management (Certificates, Client Profiles, **Server Profiles**, SNI Group), Network & Flows (Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, Advanced Options), DMZ Services, and Monitoring & Logging.

The main content area is titled 'Server Profiles: Clearcom_Outside_Server'. It features an 'Add' button and a 'Delete' button. Below this is a list of server profiles: 'Outside_Server', 'Inside_Server', 'Clearcom_Outside_Server' (highlighted in red), 'Remote_Worker_...', and 'IPO_Inside_Server'. A blue bar with the text 'Click here to add a description.' is visible.

The 'Server Profile' configuration form for 'Clearcom_Outside_Server' is shown with the following settings:

TLS Profile	
Profile Name	Clearcom_Outside_Server
Certificate	sbceExternal.pem
SNI Options	None
Certificate Verification	
Peer Verification	None
Extended Hostname Verification	<input type="checkbox"/>
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

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

7.3.3. Client Profiles

7.3.3.1 Inside Client Profile

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

- **Profile Name:** enter descriptive name, e.g., **IPO_Inside_Client**.
- **Certificate:** select the identity certificate, e.g., **IPOSE_INTERNAL.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., **default.pem**.
- **Verification Depth:** enter **2**.
- 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_Inside_Client

Certificate: IPOSE_INTERNAL.pem

SNI: Enabled

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities: avayaitrootca2.pem, entrust_g2_ca.cer, DigiCertGlobalRootCA.cer, default.pem

Peer Certificate Revocation Lists: [Empty list]

Verification Depth: 2

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 for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

On the left is a navigation menu with categories like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (Certificates, Client Profiles, Server Profiles, SNI Group), Network & Flows, DMZ Services, and Monitoring & Logging. The 'Client Profiles' section is highlighted.

The main content area is titled 'Client Profiles: IPO_Inside_Client' and features an 'Add' button. Below this is a list of client profiles: CenturyLink_Client, Outside_Client, Remote_Worker_Dec17, MIGUELSOUTSIDEPROFILE, sbcInternal, Clearcom_Outside_Client, and IPO_Inside_Client (selected). A 'Delete' button is visible in the top right of the main area.

The configuration form for the selected profile is shown, with a description field containing 'Click here to add a description.' The form is divided into several sections:

- TLS Profile:**
 - Profile Name: IPO_Inside_Client
 - Certificate: IPOSE_INTERNAL.pem
 - SNI: Enabled
- Certificate Verification:**
 - Peer Verification: Required
 - Peer Certificate Authorities: default.pem
 - Peer Certificate Revocation Lists: ---
 - Verification Depth: 2
 - Extended Hostname Verification:
- Renegotiation Parameters:**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options:**
 - Version: TLS 1.2 TLS 1.1 TLS
 - Ciphers: Default FIPS Custom
 - Value: HIGH-IDH:IADH:IMD5:1aNULL:1eNUL

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

7.3.3.2 Outside Client Profile

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

- **Profile Name:** enter a descriptive name, **Clearcom_Outside_Client** was used.
- **Certificate:** select **None** from the pull-down menu.
- **Peer Verification:** **Required** from the pull-down menu.
- **Peer Certificate Authorities:** select the Root CA certificates used to verify the identity certificate received from the Service Provider, e.g., **mycacertRootCA.crt** (Note: for security reasons fictitious certificate names were given).
- **Verification Depth:** enter **2**.
- 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: Clearcom_Outside_Client

Certificate: None

SNI: Enabled

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities: default.pem, GoDaddyRootCAClass2.crt, GoDaddyRootCAIntermediate.pem, RootCA.crt

Peer Certificate Revocation Lists: [Empty list]

Verification Depth: 2

Extended Hostname Verification:

Server Hostname: [Empty field]

Next

The following screen shows the completed **Clearcom_Outside_Client** profile form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' 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', 'Certificates', 'Client Profiles', 'Server Profiles', 'SNI Group', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The 'Client Profiles' section is expanded, showing a list of profiles: 'CenturyLink_Client', 'Outside_Client', 'Remote_Worker_Dec17', 'MiguelsOutsideProfile', 'sbcInternal', 'IPO_Inside_Client', and 'Clearcom_Outside_Client' (highlighted in red).

The main content area is titled 'Client Profiles: Clearcom_Outside_Client' and includes an 'Add' button and a 'Delete' button. Below this is a blue bar with the text 'Click here to add a description.' The profile configuration is divided into several sections:

- Client Profile**: A tabbed interface for the selected profile.
- TLS Profile**:

Profile Name	Clearcom_Outside_Client
Certificate	None
SNI	<input type="checkbox"/> Enabled
- Certificate Verification**:

Peer Verification	Required
Peer Certificate Authorities	RootCA.crt
Peer Certificate Revocation Lists	---
Verification Depth	2
Extended Hostname Verification	<input type="checkbox"/>
- Renegotiation Parameters**:

Renegotiation Time	0
Renegotiation Byte Count	0
- Handshake Options**:

Version	<input checked="" type="checkbox"/> TLS 1.2 <input checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:IDH:IADH:IMD5:faNULL:ieNULL:@STRENGTH

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

7.4. Configuration Profiles

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

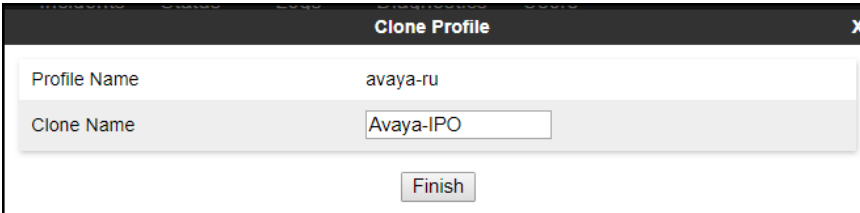
7.4.1. Server Interworking – Avaya-IPO

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**.



Clone Profile	
Profile Name	avaya-ru
Clone Name	Avaya-IPO
<input type="button" value="Finish"/>	

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

Device: Avaya_SBCE Alarms **2** Incidents Status Logs Diagnostics Users Settings

Session Border Controller for Enterprise

- 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
 - Recording Profile
- Services
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
 - Monitoring & Logging

Interworking Profiles: Avaya-IPO

[Add](#)

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

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-S...

Avaya-SM

Avaya-IPO

Avaya-CS1000

Avaya-CM

cs2100

SP-General

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

General

Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes

[Edit](#)

HG; Reviewed:
SPOC 8/11/2023

Avaya DevConnect Application Notes
©2023 Avaya Inc. All Rights Reserved.

65 of 121
CleIPO111SBC10T

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

The screenshot displays the Avaya SBCE management interface. At the top, the navigation bar shows 'Device: Avaya_SBCE', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The main title is 'Session Border Controller for Enterprise'. On the left is a navigation menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'Configuration Profiles', and 'Services'. The 'Server Interworking' profile is selected. The main content area is titled 'Interworking Profiles: Avaya-IPO' and features an 'Add' button. Below this is a list of profiles: avaya-ru, OCS-Edge-Server, cisco-ccm, cups, OCS-FrontEnd-S..., Avaya-SM, **Avaya-IPO**, Avaya-CS1000, Avaya-CM, cs2100, and SP-General. The 'Avaya-IPO' profile is selected, and its configuration is shown in a tabbed interface with tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'Advanced' tab is active, showing a table of settings:

Click here to add a description.					
General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
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
Relay INVITE Replace for SIPREC					No
MOBX Re-INVITE Handling					No
NATing for 301/302 Redirection					Yes
DTMF					
DTMF Support					None

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

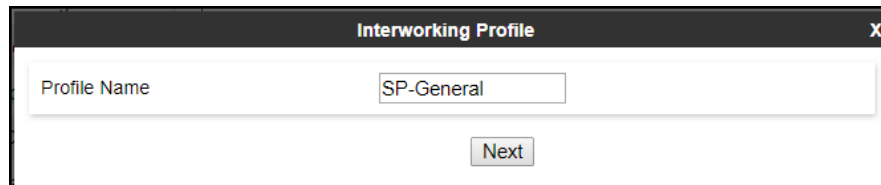
7.4.2. Server Interworking - SP-General

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 configuration window titled "Interworking Profile" with a close button (X) in the top right corner. The "General" tab is active, displaying various settings for SIP interworking. The settings are as follows:

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
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 checked="" type="checkbox"/>

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

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

Device: Avaya_SBCE ▾ Alarms 2 Incidents Status ▾ Logs ▾ Diagnostics Users Settings

Session Border Controller for Enterprise

- 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
 - Recording Profile
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

Interworking Profiles: SP-General

[Add](#)

Interworking Profiles

- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- OCS-FrontEnd-S...
- Avaya-SM
- Avaya-IPO
- Avaya-CS1000
- Avaya-CM
- cs2100
- SP-General**

Click here to add a description.

General
Timers
Privacy
URI Manipulation
Header Manipulation
Advanced

General

Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes

[Edit](#)

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

The screenshot displays the configuration interface for a Session Border Controller for Enterprise. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', and 'Settings'. The main heading is 'Session Border Controller for Enterprise'. On the left is a navigation menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'System Parameters', 'Configuration Profiles', 'Services', and 'Monitoring & Logging'. The 'Server Interworking' sub-category is expanded. The main content area is titled 'Interworking Profiles: SP-General' and features an 'Add' button. Below this is a list of profiles: 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-S...', 'Avaya-SM', 'Avaya-IPO', 'Avaya-CS1000', 'Avaya-CM', 'cs2100', and 'SP-General' (highlighted in red). To the right, the configuration for 'SP-General' is shown in the 'Advanced' tab. A blue bar at the top of the configuration area says 'Click here to add a description.' Below this are tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'Advanced' tab contains a table of 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
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes
DTMF	
DTMF Support	None

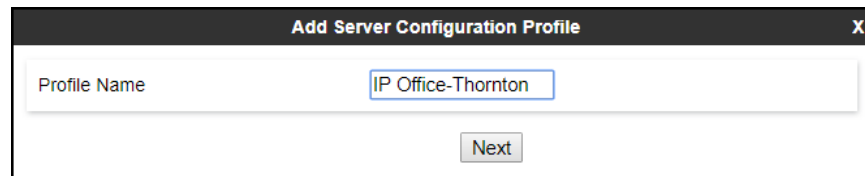
An 'Edit' button is located at the bottom right of the configuration area.

7.4.3. SIP Server Configuration

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

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

- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration 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 "IP Office-Thornton". Below the input 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 7.3.3.1**).
- Click **Next**.

IP Address / FQDN	Port	Transport	
10.64.101.127	5061	TLS	Delete

- 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 for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo on the right. A left-hand 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' buttons. Below this, there are tabs for 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced', with 'General' selected. The configuration details are as follows:

Server Type	Call Server	
TLS Client Profile	IPO_Inside_Client	
DNS Query Type	NONE/A	
IP Address / FQDN	Port	Transport
10.64.101.127	5061	TLS

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

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

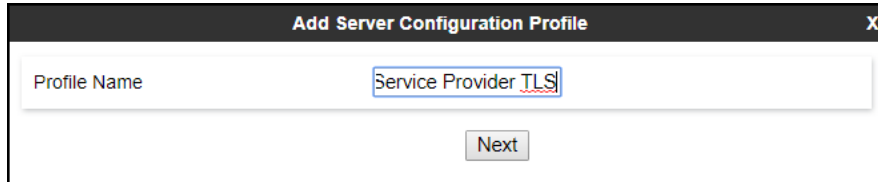
The screenshot displays the Avaya Session Border Controller for Enterprise web interface, showing the 'Advanced' tab of the 'SIP Servers: IP Office-Thornton' configuration profile. The top navigation bar and left-hand menu are identical to the previous screenshot. The 'Advanced' tab is selected, showing the following configuration options:

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 of the configuration table.

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 TLS**.

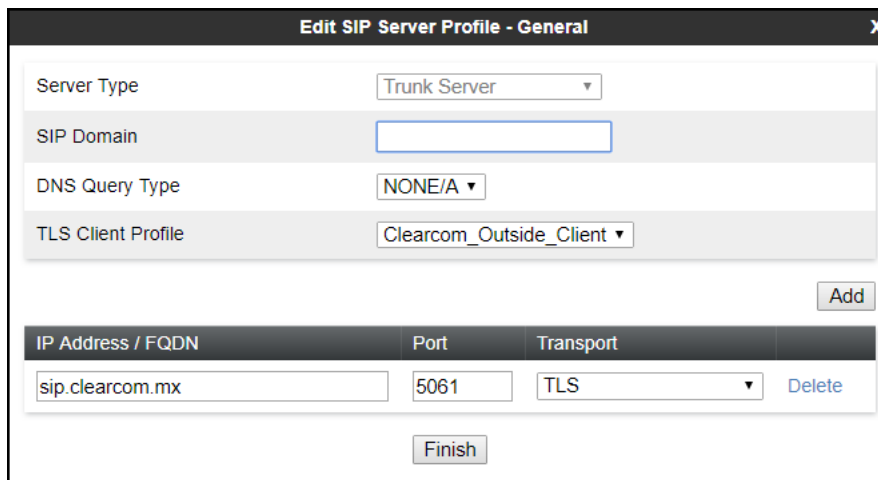
- Click **Next**.



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 is filled with "Service Provider TLS". Below the 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’s SIP proxy server FQDN, this information is provided by Clearcom).
- Enter **5061** under **Port** and select **TLS** for **Transport**.
- Select a **TLS Profile (Section 7.3.3.2)**.
- Click **Next**.



The screenshot shows the "Edit SIP Server Profile - General" window. It has a close button (X) in the top right corner. The "Server Type" dropdown is set to "Trunk Server". The "SIP Domain" field is empty. The "DNS Query Type" dropdown is set to "NONE/A". The "TLS Client Profile" dropdown is set to "Clearcom_Outside_Client". There is an "Add" button to the right of the "TLS Client Profile" field. Below this is a table with columns "IP Address / FQDN", "Port", "Transport", and "Delete". The table contains one row with the following values: "sip.clearcom.mx", "5061", "TLS", and a "Delete" link. At the bottom of the window is a "Finish" button.

IP Address / FQDN	Port	Transport	Delete
sip.clearcom.mx	5061	TLS	Delete

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**.

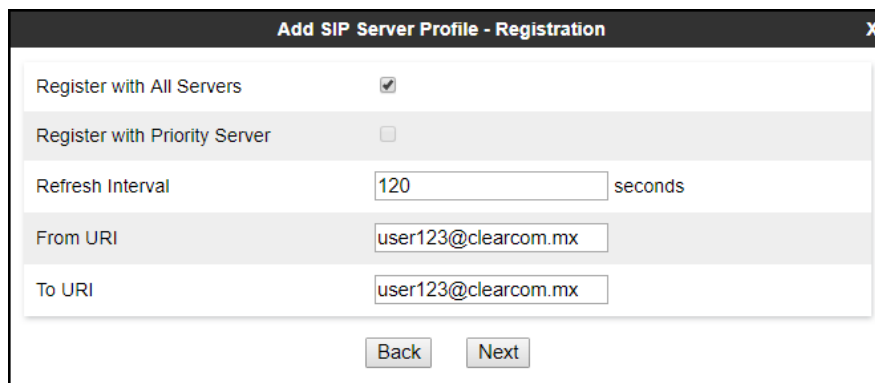
The screenshot shows a dialog box titled "Add SIP Server Profile - Authentication". It contains the following fields and controls:

- 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 password input field with four dots.
- Confirm Password:** A password input field with four dots.
- Navigation:** "Back" and "Next" buttons at the bottom.

- 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**.

Edit SIP Server Profile - Advanced	
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	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

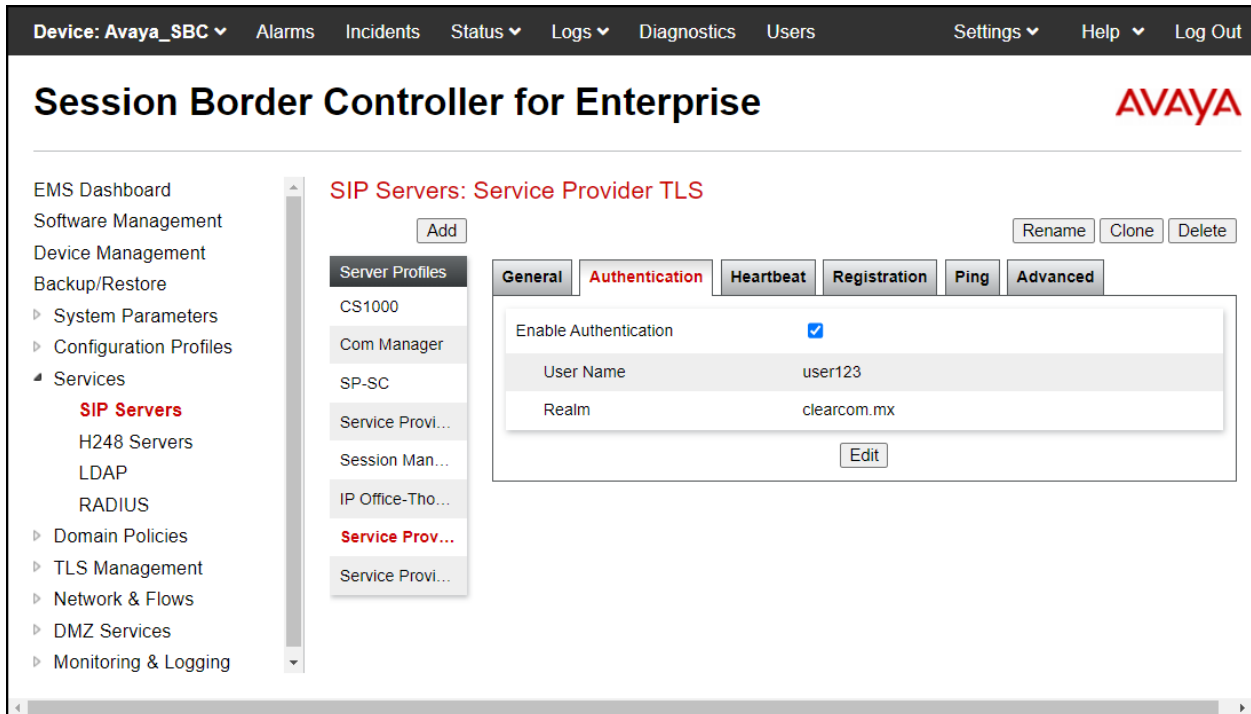
The following screen capture shows the **General** tab of the newly created **Service Provider TLS** SIP Server Configuration Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo on the right. A left-hand navigation menu lists various management options, with 'SIP Servers' highlighted under the 'Services' section. The main content area is titled 'SIP Servers: Service Provider TLS' 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 are as follows:

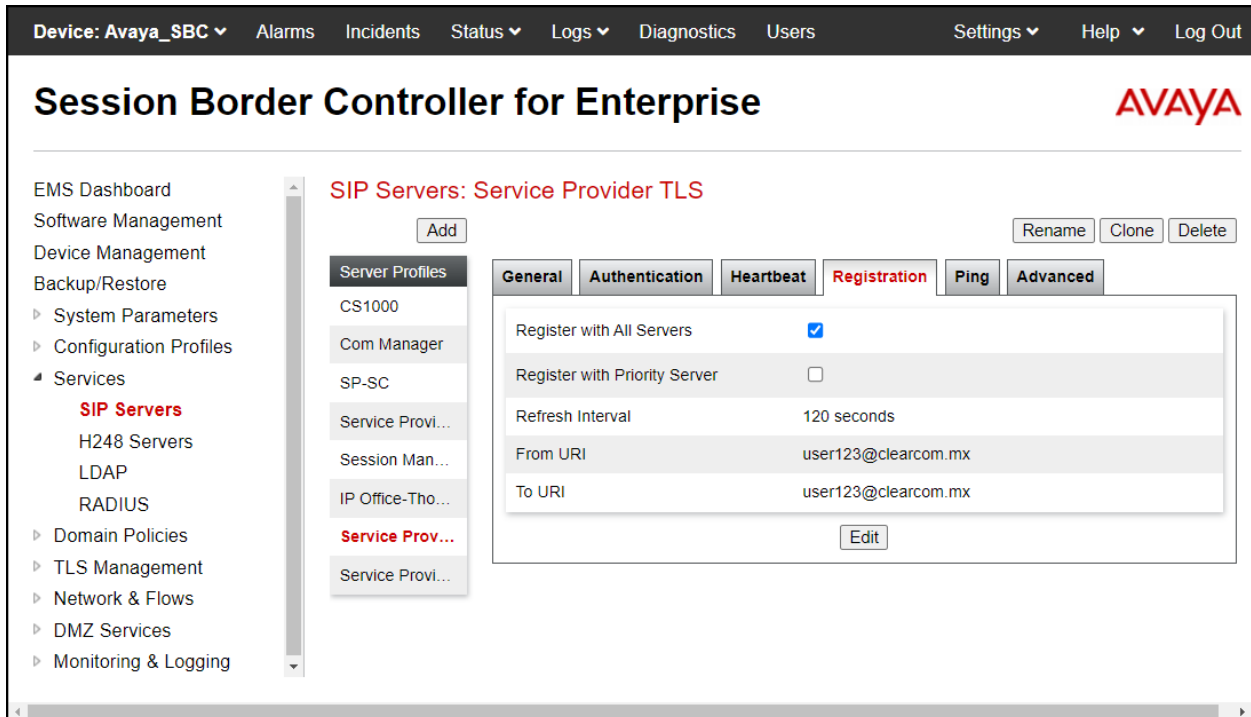
Server Type	Trunk Server	
TLS Client Profile	Clearcom_Outside_Client	
DNS Query Type	NONE/A	
IP Address / FQDN	Port	Transport
sip.clearcom.mx	5061	TLS

An 'Edit' button is located below the table.

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



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



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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. At the top, a navigation bar includes 'Device: Avaya_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' 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', 'H248 Servers', 'LDAP', 'RADIUS', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The 'Services' section is expanded to show 'SIP Servers'.

The main content area is titled 'SIP Servers: Service Provider TLS'. It features an 'Add' button and three action buttons: 'Rename', 'Clone', and 'Delete'. Below this is a list of server profiles: 'CS1000', 'Com Manager', 'SP-SC', 'Service Provi...', 'Session Man...', 'IP Office-Tho...', 'Service Prov...', and 'Service Provi...'. The 'Service Prov...' profile is selected.

The configuration for the selected profile is shown in a tabbed interface with tabs for 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced'. The 'Advanced' tab is active, displaying the following settings:

Setting	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 panel.

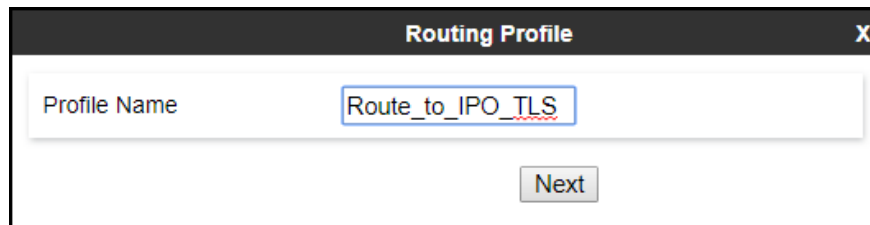
7.4.4. Routing Profiles

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**.

The screenshot shows the 'Routing Profile' configuration window. The top section contains various settings: URI Group (dropdown), Time of Day (default), Load Balancing (Priority), NAPTR (checkbox), Transport (None), LDAP Routing (checkbox), LDAP Server Profile (None), LDAP Base DN (Search) (None), Matched Attribute Priority (checked), Alternate Routing (checked), Next Hop Priority (checked), Next Hop In-Dialog (checkbox), Ignore Route Header (checkbox), ENUM (checkbox), and ENUM Suffix (text input). An 'Add' button is located at the bottom right of this section.

Below the settings is 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 row with the following values: Priority / Weight: 1, LDAP Search Attribute: (empty), LDAP Search Regex Pattern: (empty), LDAP Search Regex Result: (empty), SIP Server Profile: IP Office-Thornton, Next Hop Address: 10.64.101.127:5061 (TLS), and Transport: None. A 'Delete' button is located to the right of the table row.

At the bottom of the window are 'Back' and 'Finish' buttons.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the Avaya logo on the right. A left-hand navigation menu lists various configuration areas, with 'Routing' highlighted in red. The main content area is titled 'Routing Profiles: Route_to_IPO_TLS' and features an 'Add' button. Below this, a list of routing profiles is shown, with 'Route_to_IPO_TLS' selected. A detailed view of the selected profile is displayed, including an 'Update Priority' button and an 'Add' button. A table lists the profile's configuration:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.64.101.127:5061	TLS	Edit Delete

Similarly, for the outbound route:

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

The screenshot shows a 'Routing Profile' configuration window. The 'Profile Name' field contains the text 'Route_to_SP_TLS'. Below the field is a 'Next' button.

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 TLS**.
- The **Next Hop Address** is populated automatically with **sip.clearcom.mx:5061 (TLS)** (Clearcom SIP Proxy FQDN, port and transport).
- Click **Finish**.

Profile : Route_to_SP_TLS - Edit Rule

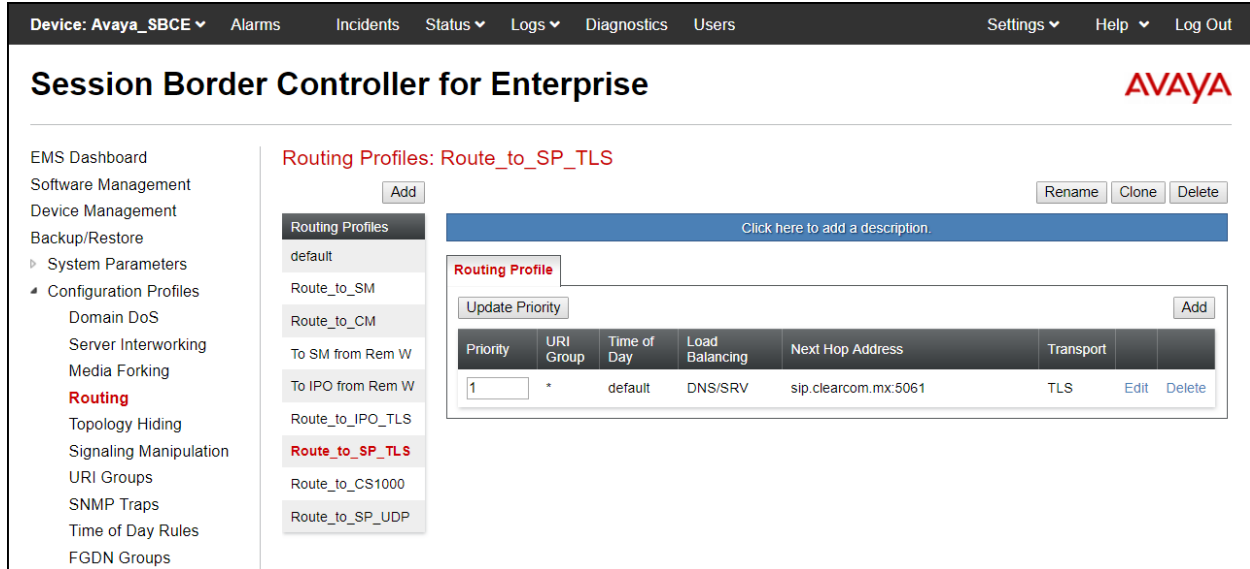
URI Group	*	Time of Day	default
Load Balancing	DNS/SRV	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority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

[Add](#)

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
0				Service Pr...	sip.clearcom.mx:50	None	Delete

[Finish](#)

The following screen capture shows the newly created **Route_to_SP_TLS** 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.

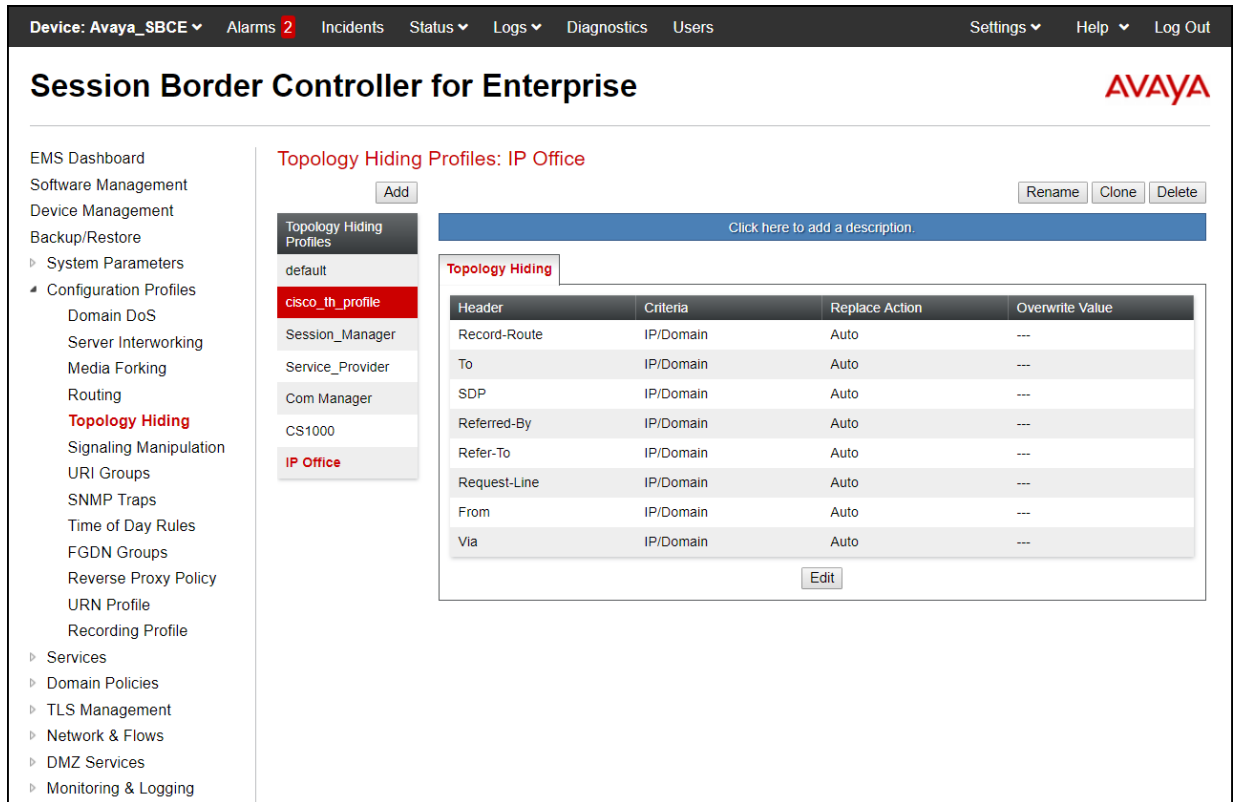
For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

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**.

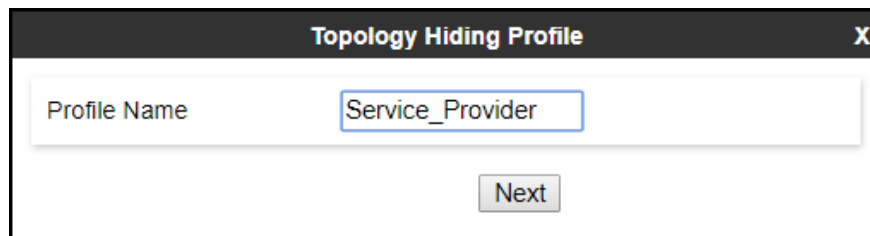


The following screen capture shows the newly added **IP Office** Topology Hiding Profile. Note that for IP Office no values were overwritten (left with default values).



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

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



- Click **Edit** on the newly created **Service_Provider** Topology Hiding profile.
- On the **From** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (**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**.

Edit Topology Hiding Profile X

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 for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' 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, Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, FGDN Groups, Reverse Proxy Policy, URN Profile, Recording Profile, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. 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 a list of profiles: 'default', 'cisco_th_profile', 'Session_Manager', 'Service_Provider' (highlighted in red), 'Com Manager', 'CS1000', and 'IP Office'. There are also 'Rename', 'Clone', and 'Delete' buttons.

Below the profile list, there is a section for the 'Service_Provider' profile. It includes a blue bar with the text 'Click here to add a description.' and a table titled 'Topology Hiding'.

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

An 'Edit' button is located below the table.

7.5. Domain Policies

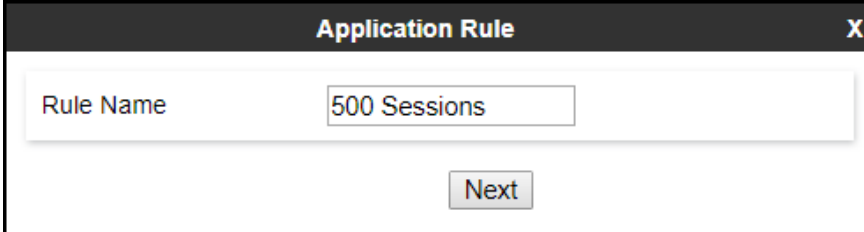
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.5.1. Application Rules

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

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

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



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

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

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

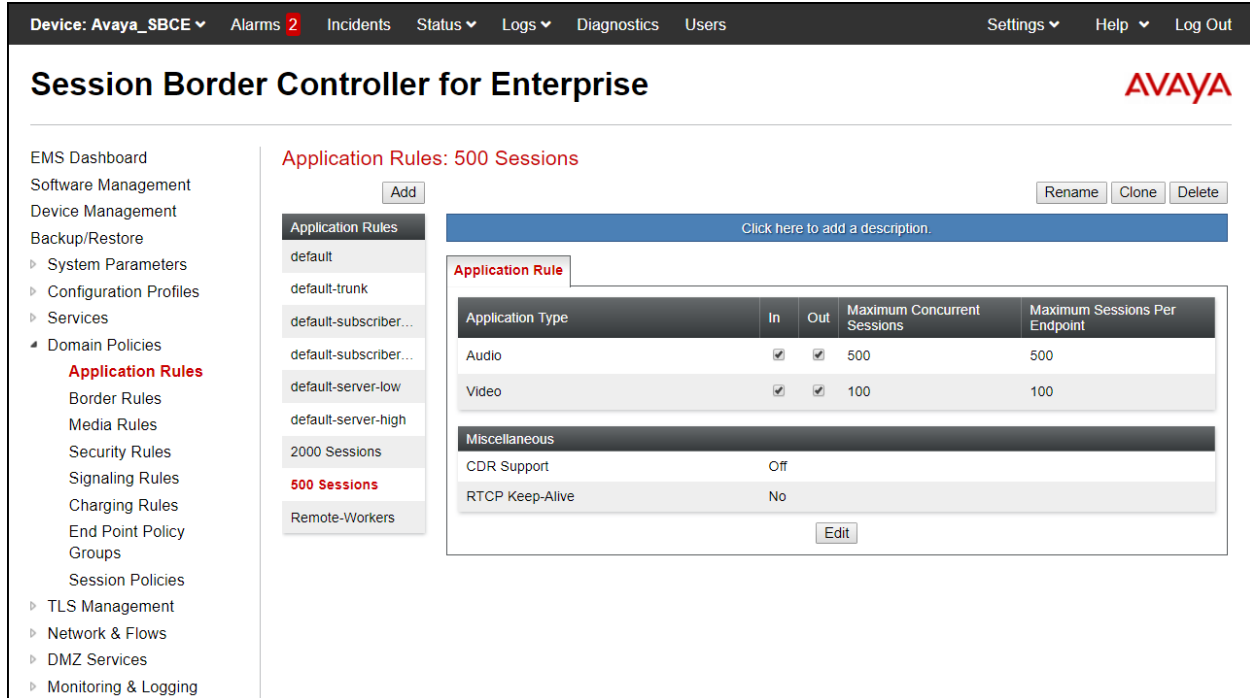
RADIUS Profile None ▾

Media Statistics Support

Call Duration Setup
 Connect

RTCP Keep-Alive

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

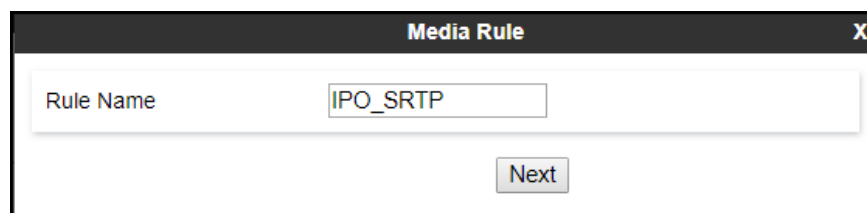


7.5.2. Media Rules

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 SBCE security product. For the compliance test one media rule was created toward IP Office, the existing **default-low-med** media rule was used toward the Service Provider.

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

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



- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous check **Capability Negotiation**.
- Click **Next** (not shown).

Audio Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▼
Preferred Format #2	RTP ▼
Preferred Format #3	NONE ▼
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▼
Preferred Format #2	RTP ▼
Preferred Format #3	NONE ▼
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input checked="" type="checkbox"/>

Finish

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

For the compliance test, the **default-low-med** Media Rule was used in the Service Provider direction.

Audio Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input type="checkbox"/>

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' 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', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The 'Media Rules' section is expanded, showing a list of rules including 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', 'Rem_Workers_S...', 'IPO_SRTP' (highlighted in red), 'ServiceProvider_...', and 'SM_SRTP'.

The main content area is titled 'Media Rules: IPO_SRTP' and features an 'Add' button. Below this is a description field with the placeholder text 'Click here to add a description.' and buttons for 'Rename', 'Clone', and 'Delete'. The configuration is organized into tabs: 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing the following settings:

Category	Setting	Value
Encryption	Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
	Encrypted RTCP	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	Any
	Interworking	<input checked="" type="checkbox"/>
	Symmetric Context Reset	<input checked="" type="checkbox"/>
	Key Change in New Offer	<input type="checkbox"/>
Video Encryption	Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
	Encrypted RTCP	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	Any
	Interworking	<input checked="" type="checkbox"/>
Miscellaneous	Symmetric Context Reset	<input checked="" type="checkbox"/>
	Key Change in New Offer	<input type="checkbox"/>
Miscellaneous	Capability Negotiation	<input checked="" type="checkbox"/>

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

The following screen capture shows the default-low-med Media Rule.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' 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', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The 'Media Rules' section is highlighted.

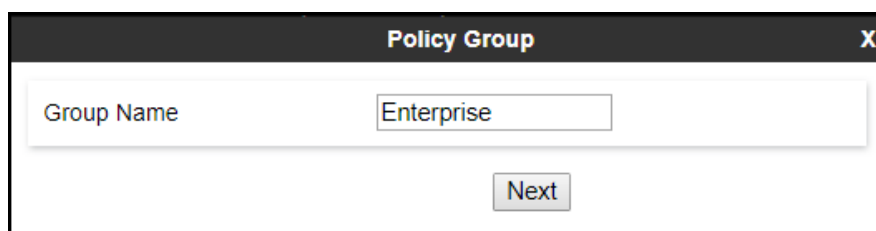
The main content area is titled 'Media Rules: default-low-med' and includes an 'Add' button and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing settings for 'Audio Encryption' and 'Video Encryption'. Both sections have 'Preferred Formats' set to 'RTP', 'Interworking' checked, 'Symmetric Context Reset' checked, and 'Key Change in New Offer' unchecked. A 'Miscellaneous' section at the bottom has 'Capability Negotiation' unchecked. 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 SBCE.

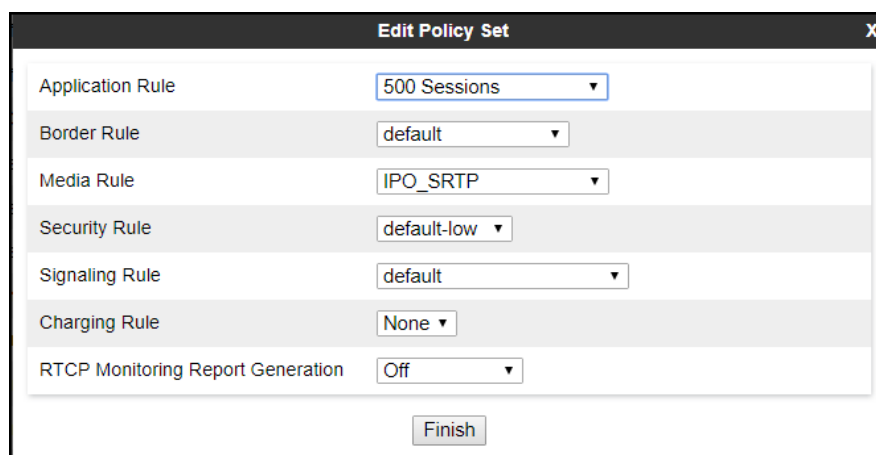
To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups** (not shown).

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



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 is a button labeled "Next".

- **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, 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 is a button labeled "Finish".

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo on the right.

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 (highlighted), Session Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging.

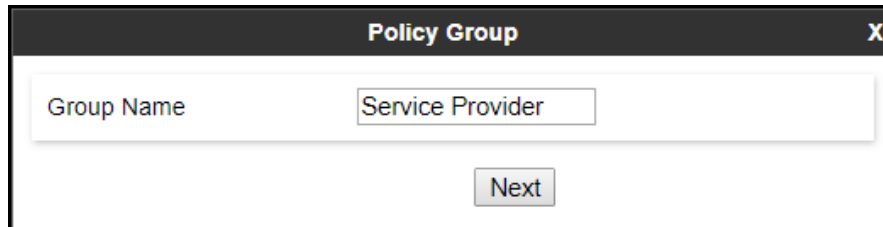
The main content area is titled 'Policy Groups: Enterprise' and features an 'Add' button. Below this, there are two blue bars with the text 'Click here to add a description.' and 'Click here to add a row description.' respectively. A 'Policy Group' configuration window is open, showing a table with the following data:

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

The 'Enterprise' policy group is highlighted in the left sidebar menu.

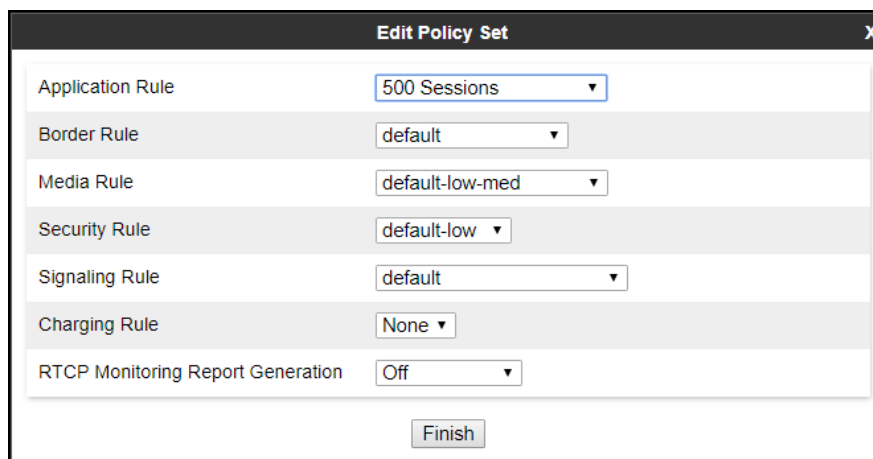
Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk.

- 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" which contains the text "Service Provider". Below the input field, there 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, there 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 for Enterprise web interface. The top navigation bar shows the device name 'Avaya_SBCE', a notification for 2 alarms, and various system status links. The main header identifies the application as 'Session Border Controller for Enterprise' with the Avaya logo.

The left-hand navigation menu lists various management sections, 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' options. Below this, there are two blue boxes with instructions to '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	default-low-med	default-low	default	None	Off	Edit

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 'Network Management' section of the Avaya Session Border Controller for Enterprise. The 'Networks' tab is selected, showing a table of network configurations. The table has 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 SBCE will not be able to communicate on any of its interfaces.

The screenshot shows the Avaya SBCE management console. At the top, there is a navigation bar with 'Device: Avaya_SBCE', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. Below this is the main header 'Session Border Controller for Enterprise' with the AVAYA logo on the right. A 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, and Network & Flows. Under 'Network & Flows', 'Network Management' is highlighted. The main content area is titled 'Network Management' and has two tabs: 'Interfaces' (selected) and 'Networks'. An 'Add VLAN' button is located in the top right of the interface table. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Disabled).

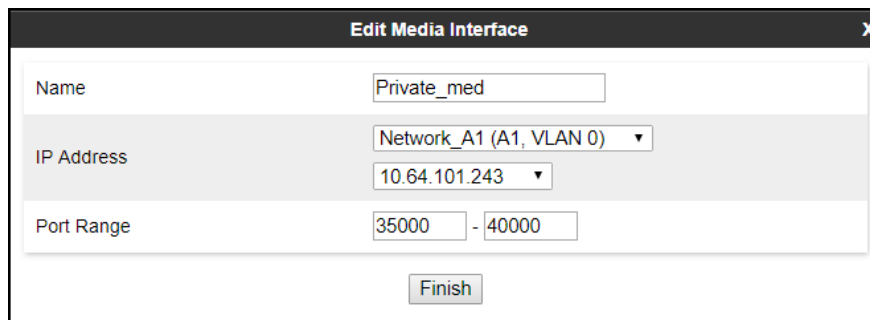
Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

7.6.2. Media Interface

Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBCE 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 SBCE, the port range 35000 to 40000 was used.

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

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

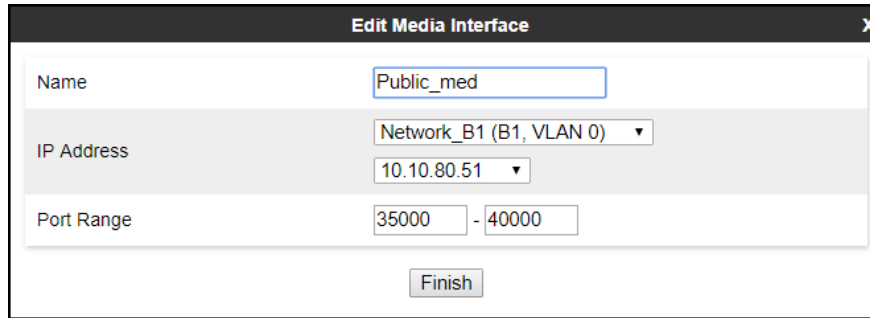


Name	Private_med
IP Address	Network_A1 (A1, VLAN 0) 10.64.101.243
Port Range	35000 - 40000

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



Edit Media Interface

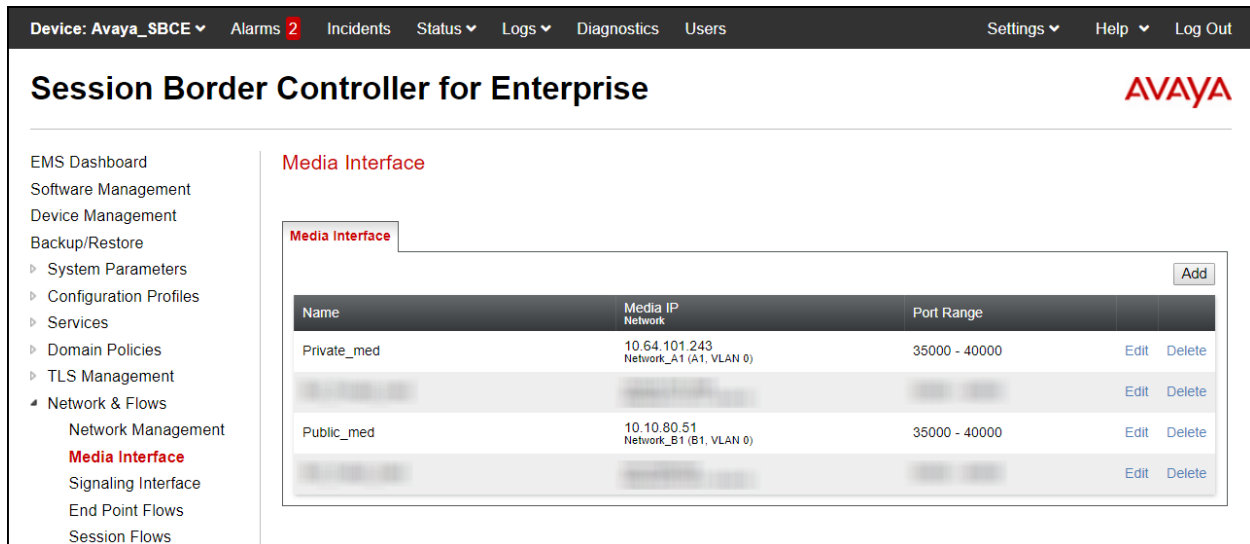
Name: Public_med

IP Address: Network_B1 (B1, VLAN 0)

Port Range: 35000 - 40000

Finish

The following screen capture shows the newly created Media Interfaces.



Device: Avaya_SBCE | Alarms 2 | Incidents | Status | Logs | Diagnostics | Users | Settings | Help | Log Out

Session Border Controller for Enterprise

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
Session Flows

Media Interface

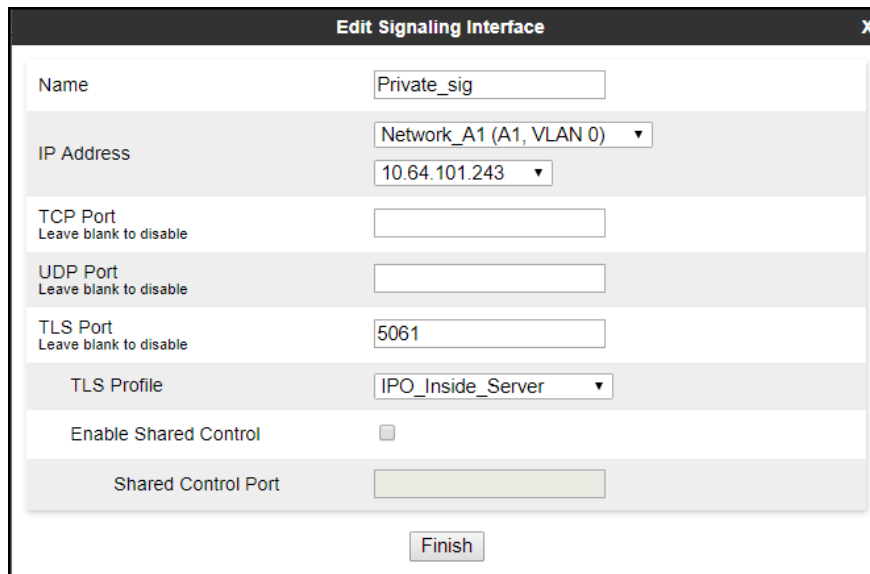
Add

Name	Media IP Network	Port Range	Edit	Delete
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 SBCE, toward IP Office).
- **TLS Port: 5061.**
- Select a **TLS Profile (Section 7.3.2.1).**
- Click **Finish.**



The screenshot shows a configuration window titled "Edit Signaling Interface" with a close button (X) in the top right corner. The window contains the following fields and options:

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_Inside_Server
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

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

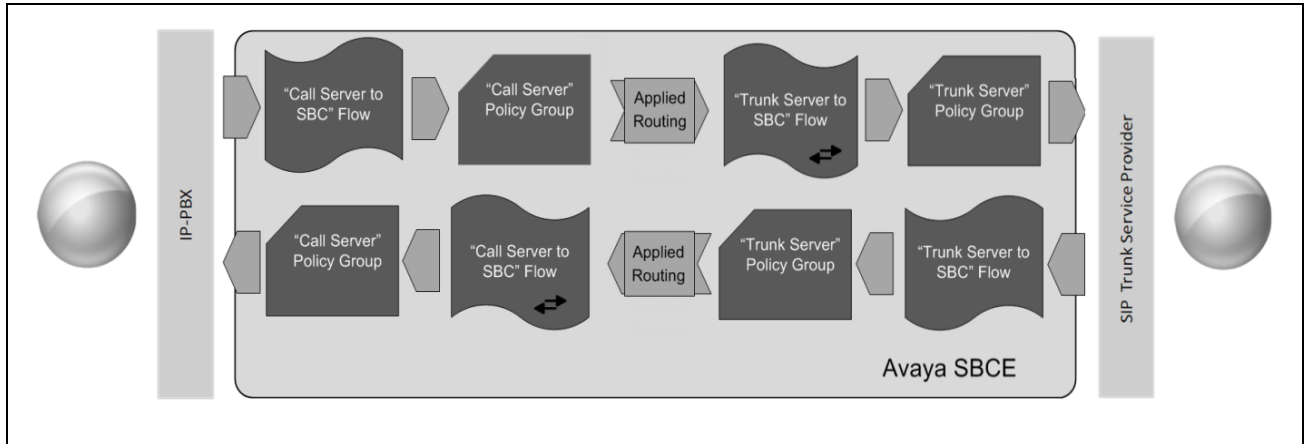
- Select **Add** in the **Signaling Interface** area (not shown).
- **Name: Public_sig**.
- Under **IP Address** select: **Network_B1 (B1, VLAN 0)**
- Select **IP Address: 10.10.80.51** (outside or public IP Address of the Avaya SBCE, toward the Service Provider).
- **TLS Port: 5061**.
- Select a **TLS Profile (Section 7.3.2.2)**.
- Click **Finish**.

The following screen capture shows the newly created Signaling Interfaces.

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_Inside_Server	Edit	Delete
						Edit	Delete
						Edit	Delete
Public_sig	10.10.80.51 Network_B1 (B1, VLAN 0)	---	---	5061	Clearcom_Outside_Server	Edit	Delete

7.6.4. End Point Flows

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



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

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

- **Name: SP to IPO Flow**
- **Server Configuration: Service Provider TLS (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.**

Edit Flow: SP to IPO Flow	
Flow Name	SP to IPO Flow
SIP Server Profile	Service Provider TLS
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	
<input type="button" value="Finish"/>	

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_TLS (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_TLS
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**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBC', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' 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, Network & Flows (expanded), Network Management, Media Interface, Signaling Interface, **End Point Flows** (highlighted), Session Flows, Advanced Options, DMZ Services, and Monitoring & Logging.

The main content area is titled 'End Point Flows' and features two tabs: 'Subscriber Flows' and 'Server Flows'. The 'Server Flows' tab is active, showing a table of configurations. An orange banner at the top of the table states: 'Modifications made to a Server Flow will only take effect on new sessions.' Below this is a blue banner with the text: 'Click here to add a row description.' An 'Add' button is located in the top right corner of the table area.

The table is divided into two sections based on the SIP Server:

- 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_TLS	View Clone Edit Delete
- SIP Server: Service Provider TLS**

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 for Enterprise 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 for Enterprise following the steps discussed in the previous sections, including:

Clearcom will provide the following information:

- SIP Trunk registration credentials (User Name, Password, etc.).
- Transport Layer Security (TLS) requirements (e.g., TLS certificate requirements).
- 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.

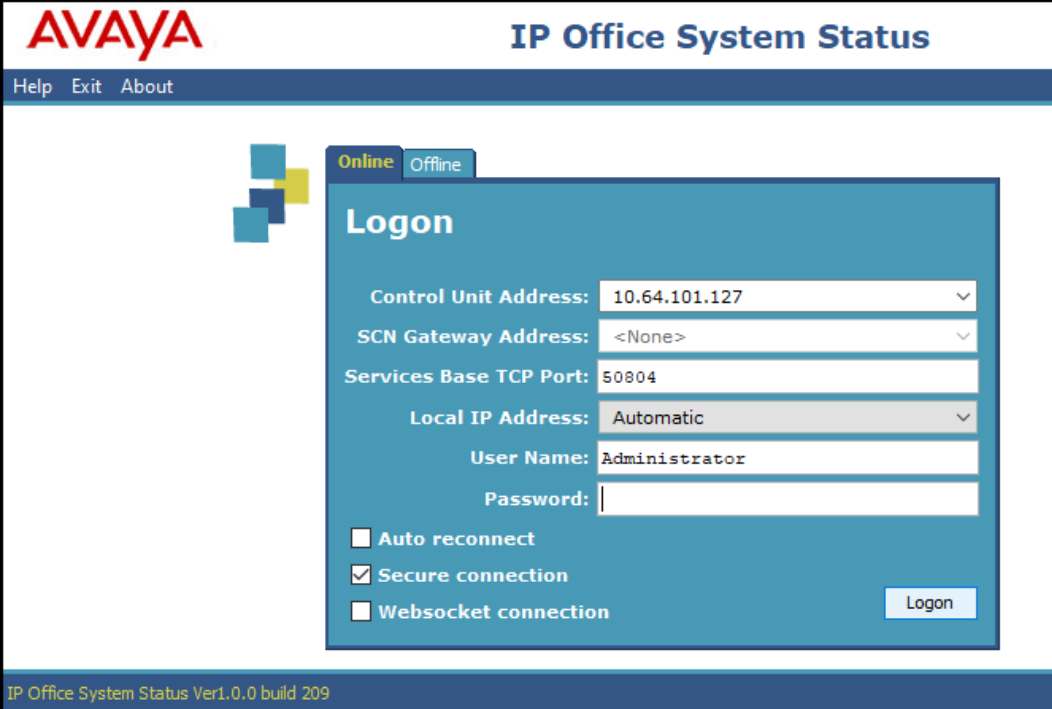
The following steps may be used to verify the configuration:

- 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 "Logon" button. The dialog box has a status indicator at the top with "Online" selected and "Offline" unselected. The fields are: Control Unit Address (10.64.101.127), SCN Gateway Address (<None>), Services Base TCP Port (50804), Local IP Address (Automatic), User Name (Administrator), and Password (empty). There are three checkboxes: "Auto reconnect" (unchecked), "Secure connection" (checked), and "Websocket connection" (unchecked). The footer of the application reads "IP Office System Status Ver1.0.0 build 209".

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.

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

- System
- Alarms (25)
- Extensions (3)
- Trunks (3)
 - Line: 1
 - Line: 2
 - Line: 17
- Active Calls
- Resources
- Voicemail
- IP Networking
- Locations

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%

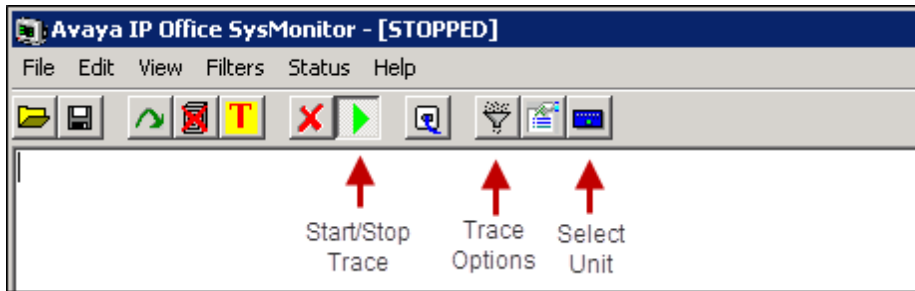
Chan...	U...	Call Ref	Current State	Time in State	Remote Media ...	Co...	Conn...	Caller ID or...	Other Party on Call	Direct...	Round Trip ...	Receive Jitter	Recei...	Trans...	Trans...
1			Idle	9 day...											
2			Idle	9 day...											
3			Idle	13 da...											
4			Idle	15 da...											
5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

Trace Trace All Pause Ping Call Details Graceful Shutdown Force Out of Service Print... Save As...

2:41:43 PM Online

9.2. Monitor

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



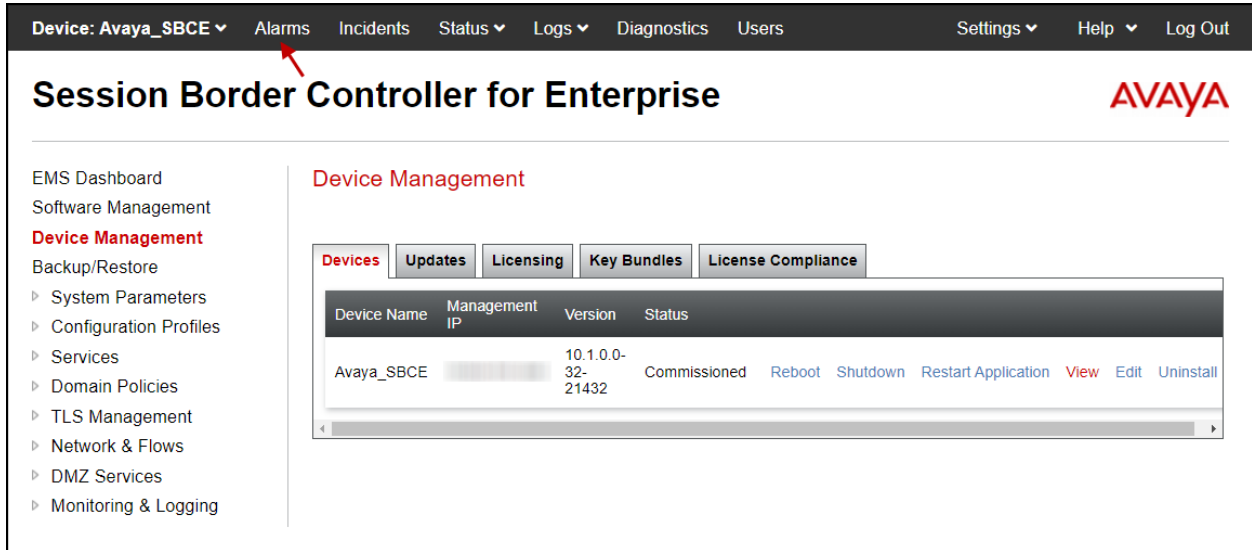
Clicking the **Trace Options** icon on the taskbar, selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of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



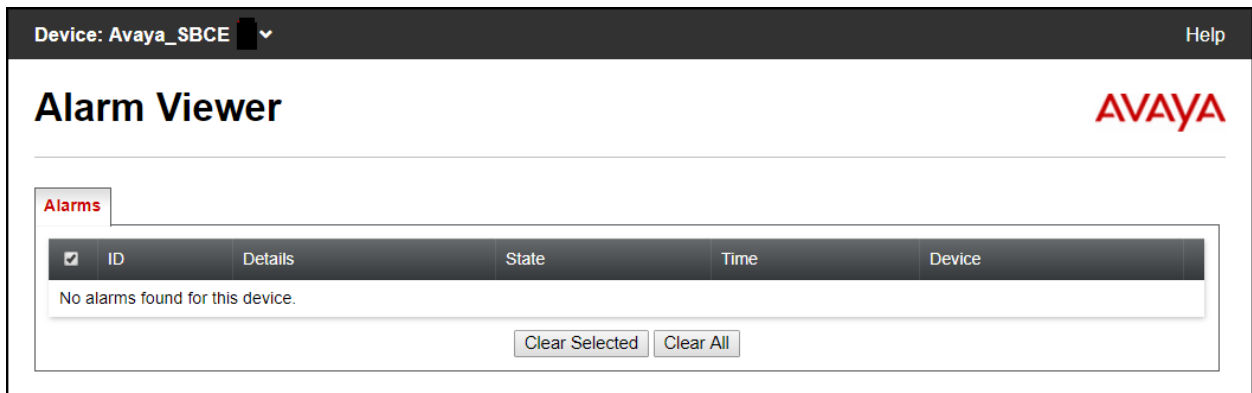
9.3. Avaya Session Border Controller for Enterprise

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

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



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



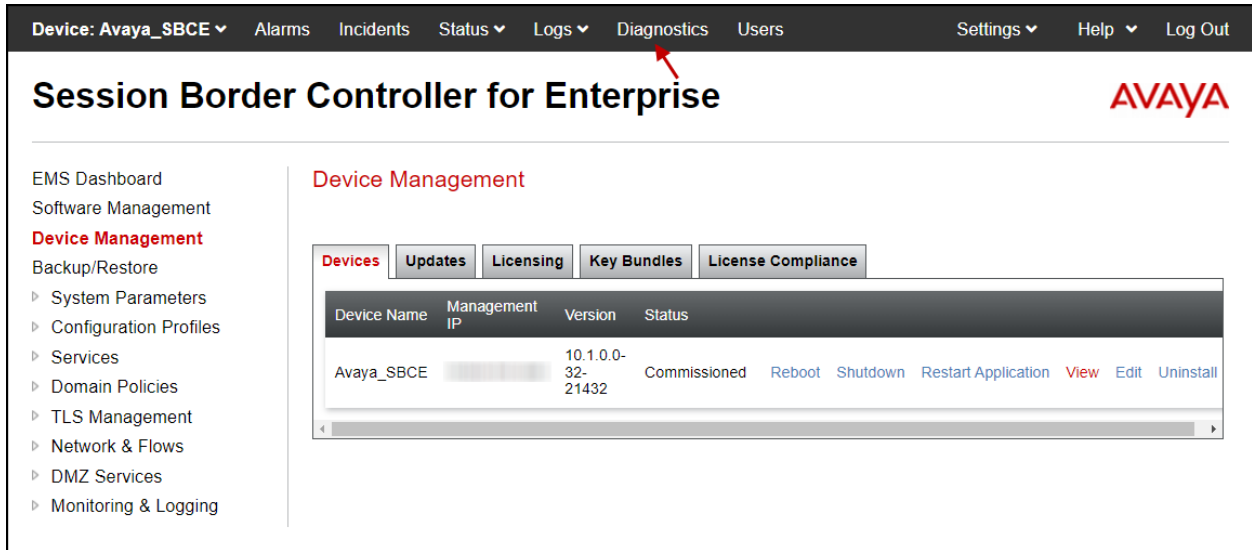
Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents' (highlighted with a red arrow), 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar lists navigation options: EMS Dashboard, Software Management, Device Management (highlighted), Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled 'Device Management' and contains tabs for 'Devices', 'Updates', 'Licensing', 'Key Bundles', and 'License Compliance'. The 'Devices' tab is active, showing a table with columns for Device Name, Management IP, Version, and Status. A single device, 'Avaya_SBCE', is listed with a Management IP, version '10.1.0.0-32-21432', and status 'Commissioned'. Action links for 'Reboot', 'Shutdown', 'Restart Application', 'View', 'Edit', and 'Uninstall' are provided for this device.

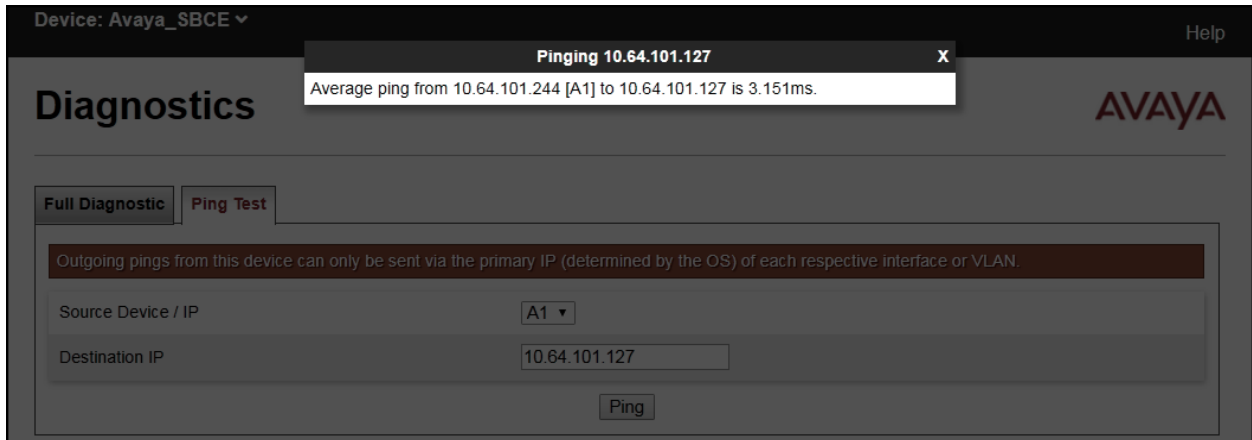
The following screen shows the Incident Viewer page.

The screenshot displays the Avaya Incident Viewer page. The top right corner has a 'Help' link. The main header shows 'Incident Viewer' and the 'AVAYA' logo. Below the header, there are filters for 'Device' (set to 'Avaya_SBCE') and 'Category' (set to 'All'), along with a 'Clear Filters' button. 'Refresh' and 'Generate Report' buttons are also present. A message indicates 'Displaying results 1 to 15 out of 2001.' Below this is a table with columns: ID, Device, Date & Time, Category, Type, and Cause. At the bottom of the table area, there are navigation buttons: '<<', '<', '1', '2', '3', '4', '5', '>', and '>>'.

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



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



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

The screenshot displays the Avaya SBCE web interface. At the top, a navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo on the right. A left-hand navigation menu lists various management options, with 'Monitoring & Logging' expanded to show 'Trace' in red. The main content area is titled 'Trace: Avaya_SBCE' and features two tabs: 'Packet Capture' (active) and 'Captures'. Below the tabs is a 'Packet Capture Configuration' form with the following fields: 'Status' (Ready), 'Interface' (Any), 'Local Address' (All), 'Remote Address' (*.*.Port. IP. IP:Port), 'Protocol' (All), 'Maximum Number of Packets to Capture' (10000), and 'Capture Filename' (Clearcom_Capture.pcap). 'Start Capture' and 'Clear' buttons are located at the bottom of the 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 for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various management options, with 'Trace' highlighted in red. The main content area is titled 'Trace: Avaya_SBCE' and contains two tabs: 'Packet Capture' and 'Captures'. The 'Captures' tab is active, showing a table with one entry. A 'Refresh' button is located in the top right of the table area.

File Name	File Size (bytes)	Last Modified	
Clearcom_Capture_20210415145422.pcap	286,720	April 15, 2021 at 2:54:41 PM EDT	Delete

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

10. Conclusion

These Application Notes describe the procedures required to configure Avaya IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 10.1 to connect to Clearcom SIP Trunking Service using Transport Layer Security (TLS). 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 Platform Server Edition, Release 11.1 FP2, Issue 26, January 2023.
- [2] IP Office Platform 11.1.2.4, Deploying Avaya IP Office Servers as Virtual Machines, Issue 13, January 2023.
- [3] Avaya IP Office Platform Server Edition Reference Configuration Release 11.1 FP2, Issue 18, January 2023.
- [4] IP Office Platform 11.1 FP2, Deploying an IP500 V2 IP Office Essential Edition System, Issue 39b, March 3, 2023.
- [5] Administering Avaya IP Office using Manager, Release 11.1.2.4, Issue 43, March 2023.
- [6] Avaya IP Office Platform Feature Description, Release 11.1 FP2, Issue 18, January 2023.
- [7] Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform, Release 10.1.x, Issue 1, December 2021.
- [8] Administering Avaya Session Border Controller for Enterprise, Release 10.1.x, Issue 2, January 2023.
- [9] Application Notes for Configuring Remote Workers with Avaya Session Border Controller for Enterprise 8.1 on the Avaya Aura® Platform – Issue 1.0

Additional Avaya IP Office documentation can be found at:

<http://marketingtools.avaya.com/knowledgebase/>

©2023 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. 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.