



Application Notes for Configuring Avaya IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 8.1 to support Avaya SIP Trunking Service using UDP Transport - 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 8.1 to support Avaya SIP Trunking Service using UDP transport on the public side.

The Avaya SIP Trunking service offer referenced within these Application Notes provides customers with PSTN access via a SIP trunk between the enterprise and the service provider network. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly as an alternative to legacy analog or digital trunks. The Avaya SIP Trunking service provides you with a cost effective and flexible way to connect your business to the outside world. It helps your business use the internet bandwidth you already pay for in a more flexible way.

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.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	6
2.3.	Support	6
3.	Reference Configuration.....	7
4.	Equipment and Software Validated	10
5.	Avaya IP Office Primary Server Configuration.....	11
5.1.	Licensing	13
5.2.	TLS Management.....	14
5.3.	System Settings	15
5.3.1.	System – LAN1 Tab	15
5.3.2.	System –Telephony Tab	19
5.3.3.	System – VoIP Tab.....	20
5.4.	IP Route.....	22
5.5.	SIP Line.....	23
5.5.1.	Creating a SIP Trunk from an XML Template.....	23
5.5.2.	SIP Line – SIP Line Tab	26
5.5.3.	SIP Line – Transport Tab.....	27
5.5.4.	SIP Line – Call Details Tab	28
5.5.5.	SIP Line – VoIP Tab.....	29
5.5.6.	SIP Line – SIP Advanced Tab	30
5.6.	Users.....	31
5.7.	IP Office Line – Primary Server	32
5.8.	Incoming Call Route	34
5.9.	Outbound Call Routing	36
5.9.1.	Short Codes and Automatic Route Selection.....	36
5.10.	Save IP Office Primary Server Configuration.....	39
6.	Avaya IP Office Expansion System Configuration	40
6.1.	Expansion System – Physical Hardware.....	41
6.2.	Expansion System – LAN Settings	42
6.3.	Expansion System – IP Route	43
6.4.	Expansion System – IP Office Line	44
6.5.	Expansion System – Short Codes.....	47
6.6.	Expansion System Automatic Route Selection – ARS	48
6.7.	Save Expansion System Configuration	49
7.	Configure Avaya Session Border Controller for Enterprise.....	50
7.1.	Log in Avaya SBCE.....	50
7.2.	Device Management.....	52
7.3.	TLS Management.....	54
7.3.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise	54
7.3.2.	Server Profiles.....	56
7.3.3.	Client Profiles	58
7.4.	Configuration Profiles	60

7.4.1.	Server Interworking – Avaya-IPO	60
7.4.2.	Server Interworking – SP-General	64
7.5.	SIP Server Configuration	67
7.5.1.	Routing Profiles	77
7.5.2.	Topology Hiding	81
7.6.	Domain Policies	85
7.6.1.	Application Rules.....	85
7.6.2.	Media Rules	87
7.6.3.	End Point Policy Groups.....	89
7.7.	Network & Flows Settings	93
7.7.1.	Network Management.....	93
7.7.2.	Media Interface	95
7.7.3.	Signaling Interface	97
7.7.4.	End Point Flows.....	99
8.	Avaya SIP Trunking Service Configuration	103
9.	Verification Steps.....	104
9.1.	IP Office System Status.....	104
9.2.	Monitor.....	106
9.3.	Avaya Session Border Controller for Enterprise.....	107
10.	Conclusion	114
11.	Additional References.....	114

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the Avaya SIP Trunking service offering and a simulated Avaya enterprise solution. User Datagram Protocol (UDP) transport was used to connect the simulated enterprise solution to the Avaya SIP Trunking service offering (public side network side).

In the configuration used during the testing, the simulated Avaya 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 8.1 (hereafter referred to as Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The terms “Avaya network” or “service provider” will be used interchangeably throughout these Application Notes to represent the far-end/service provider side of the Avaya SIP Trunking service offering handling calls to/from the PSTN across the SIP trunk. The terms “enterprise” or “Avaya enterprise” will be used interchangeably throughout these Application Notes to represent the Customer-Premises-Equipment site containing all the equipment for the Avaya enterprise solution.

2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya enterprise solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Avaya network via a broadband connection to the public Internet.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

For the testing associated with this Application Note, the interface between the simulated enterprise site (private network) and the Avaya network (public network) did not include the use of any specific encryption features, UDP/RTP was used.

Encryption (TLS/sRTP) was used internal to the enterprise between Avaya products wherever possible.

2.1. Interoperability Compliance Testing

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

- Public DNS “SRV” record queries to establish the SIP trunk connections across multiple servers.
- 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.
- Inbound and outbound PSTN calls to/from Remote Workers using the Avaya Workplace Client for Windows SIP softphone.
- 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.711MU, G.711A and G.729(a), Avaya preferred codec order.
- Proper response to no matching codecs.
- 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.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.
- T.38 fax.
- SIP REFER method for call re-direction from the enterprise to the PSTN.

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 that were not tested for not being available at the time of testing includes the following:

- 0, 0+10 digits and 411 calls were not tested.

2.2. Test Results

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

- **T.38 Fax** – IP Office negotiates the use of T.38 for fax by sending a re-INVITE message with two media lines in the SDP, with the first media line set for audio, with the port set to 0, and the second media line set for T.38, with a valid port number, thus de-activating audio transmission for the call. The Service Provider responded to this re-INVITE message sent by Avaya IP Office with "488 Not Acceptable Here". With IP Office configured to use T.38, the "488 Not Acceptable Here" response sent by the Service Provider did not have any impact on the fax transmission, both, inbound and outbound fax were successful transmitted via T.38. It's being mentioned here simply as an observation. The setting of T.38 Fall-Back in IP Office caused fax transmissions to fail intermittently, thus only the setting of T.38 is recommended for fax transmission.
- **SIP Trunk registrations** – After each successful SIP Trunk registration attempt the service provider would send a "484 Address Incomplete" message response to the enterprise. This behaviour did not have any service impact, registrations were successful, it's being mentioned here simply as an observation.
- **SIP OPTION Messages** – During the compliance test Avaya did not send SIP OPTION messages to IP Office, IP Office did send SIP OPTION messages to Avaya, this was sufficient to keep the SIP trunk up in-service.
- **SIP endpoints may indicate that a transfer failed even when it is successful** – Occasionally on a transfer operation, Avaya IP Office SIP endpoints (Avaya 1100 Series Deskphones) may indicate on the local call display that the transfer failed even though it was successful. The frequency of this behavior can be reduced by enabling "Emulate Notify for REFER" on the IP Office SIP Line (**Section 5.5.6**).

2.3. Support

For information on Avaya SIP Trunking service go to: <https://www.avaya.com/en/documents/fs-sip-uc8179en.pdf>

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

3. Reference Configuration

Figure 1 illustrates the sample Avaya enterprise solution connected to the Avaya SIP Trunking service through the public Internet.

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

- IP Office Server Edition running in VMware environment.
 - Avaya IP Office Voicemail Pro.
- Two Avaya IP Office 500 V2 as expansion systems.
- Avaya Session Border Controller for Enterprise.
- Avaya 96x1 Series IP Deskphones (H.323).
- Avaya J179 IP Deskphones (H.323).
- Avaya 1100 Series IP Deskphones (SIP).
- Avaya J129 IP Deskphones (SIP).
- Avaya 1400 Series Digital Deskphones.
- Analog Deskphones.
- Avaya 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 H.323 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 Avaya, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network, is SIP over TLS.

For inbound calls, the calls flowed from Avaya 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 Avaya network.

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

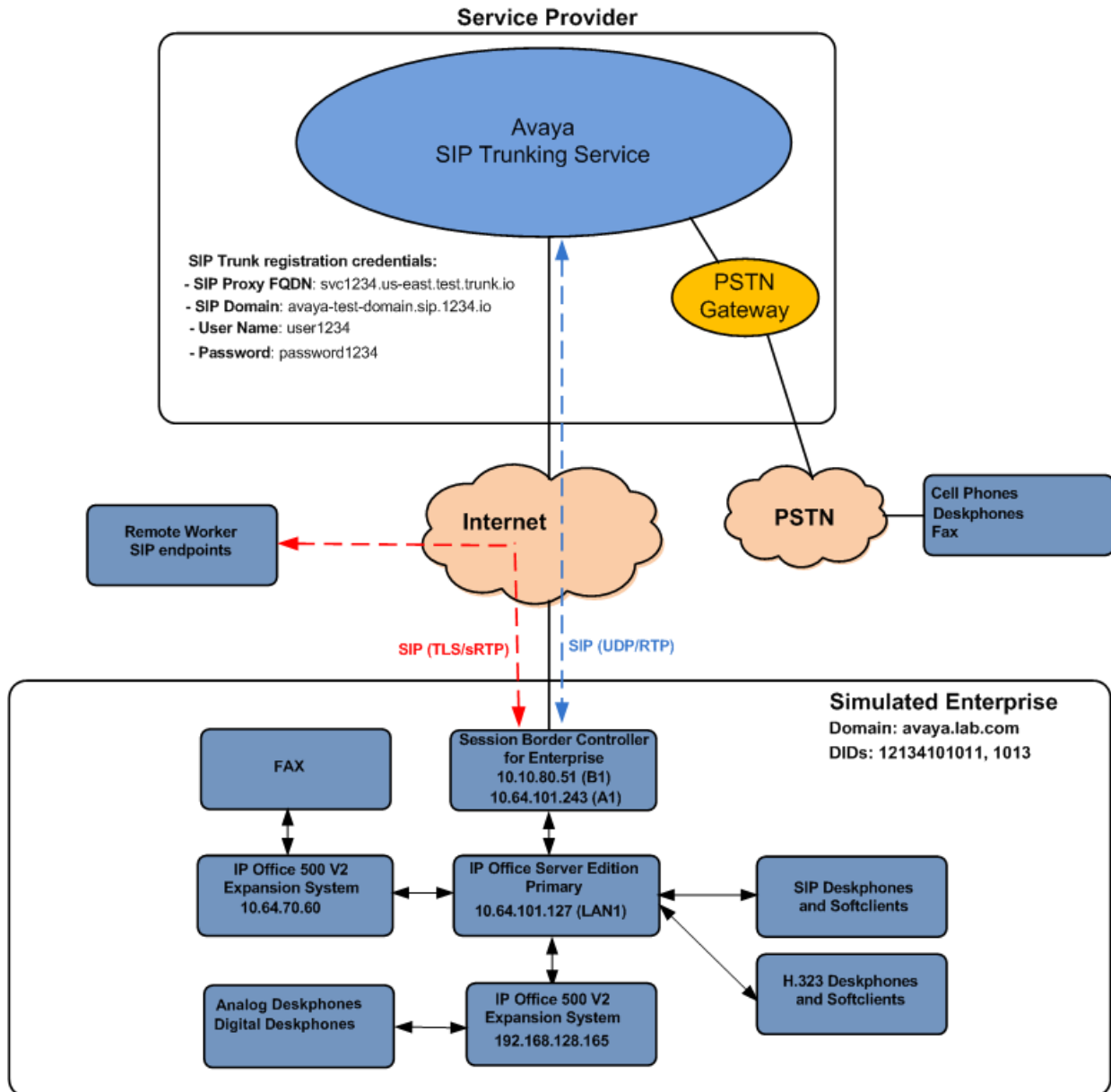


Figure 1: Avaya simulated enterprise site connected to the Avaya SIP Trunking service offering

4. Equipment and Software Validated

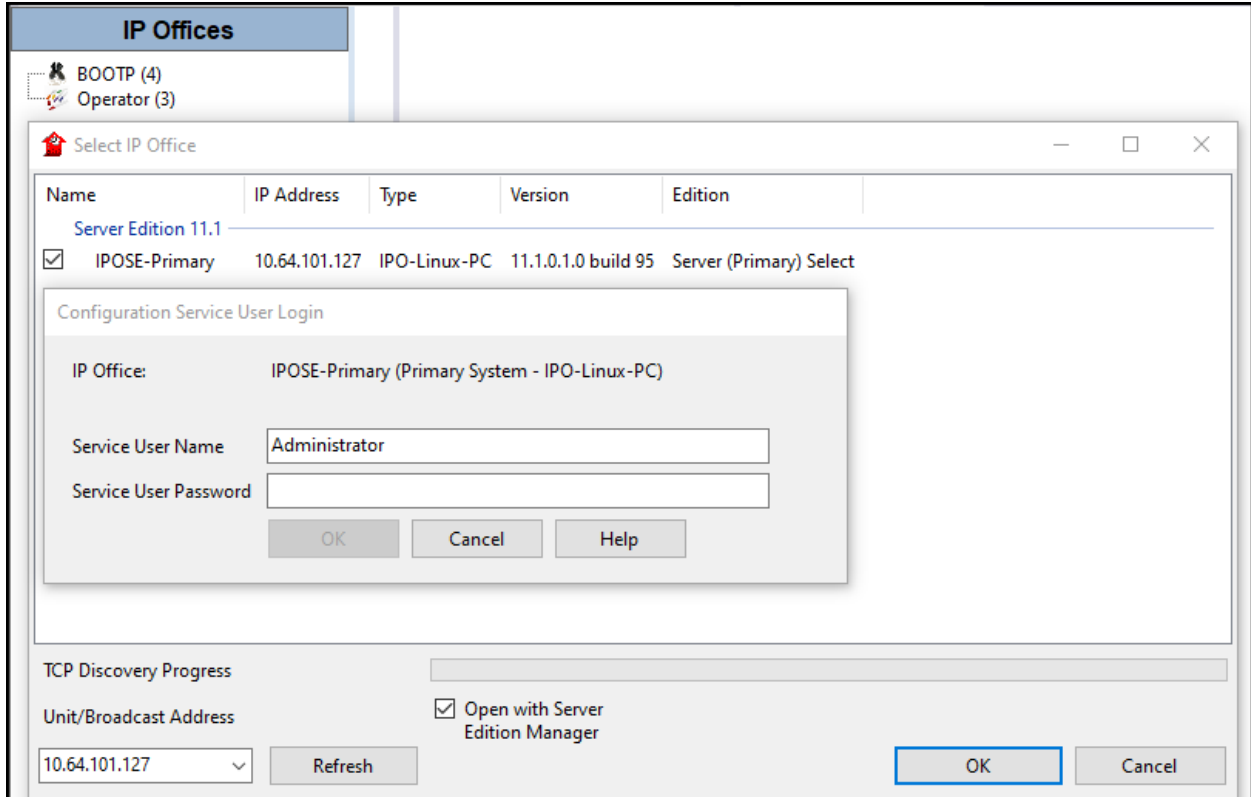
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server)	11.1.0.1 Build 95
• Avaya IP Office Voicemail Pro	11.1.0.1 Build 10
Avaya IP Office IP500 V2 (Expansion Systems)	11.1.0.1 Build 95
Avaya IP Office Manager	11.1.0.1 Build 95
Avaya Session Border Controller for Enterprise	ASBCE 8.1 8.1.1.0-26-19214
Avaya 96x1 Series IP Deskphones (H.323)	6.8304
Avaya J179 IP Telephone (H.323)	6.8304
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.0.6.0.8
Avaya 1408 Digital Telephone	48.02
Avaya Workplace Client for Windows (SIP)	3.11.0.44.25
Analog Telephone	---

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: 192.168.128.165; 10.64.70.60
- 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

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	192.168.128.165	Bothway		25	24
Expansion System	IP500V2-Two	10.64.70.60	Bothway		1	24

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

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

5.1. Licensing

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

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'Configuration' navigation pane, and on the right is the 'Details' pane for the 'License' configuration.

Configuration Pane (Left):

- BOOTP (4)
- Operator (3)
- Solution
 - User(32)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - System (1)
 - Line (3)
 - Control Unit (8)
 - Extension (6)
 - User (7)
 - Group (0)
 - Short Code (2)
 - Service (0)
 - Incoming Call Route (3)
 - IP Route (3)
 - License (6)**
 - ARS (1)
 - Location (1)
 - Authorization Code (0)
 - IP500V2-One
 - IP500V2-Two

Details Pane (Right):

License Remote Server

License Mode WebLM Normal

Licensed Version 11.0

Select Licensing Valid

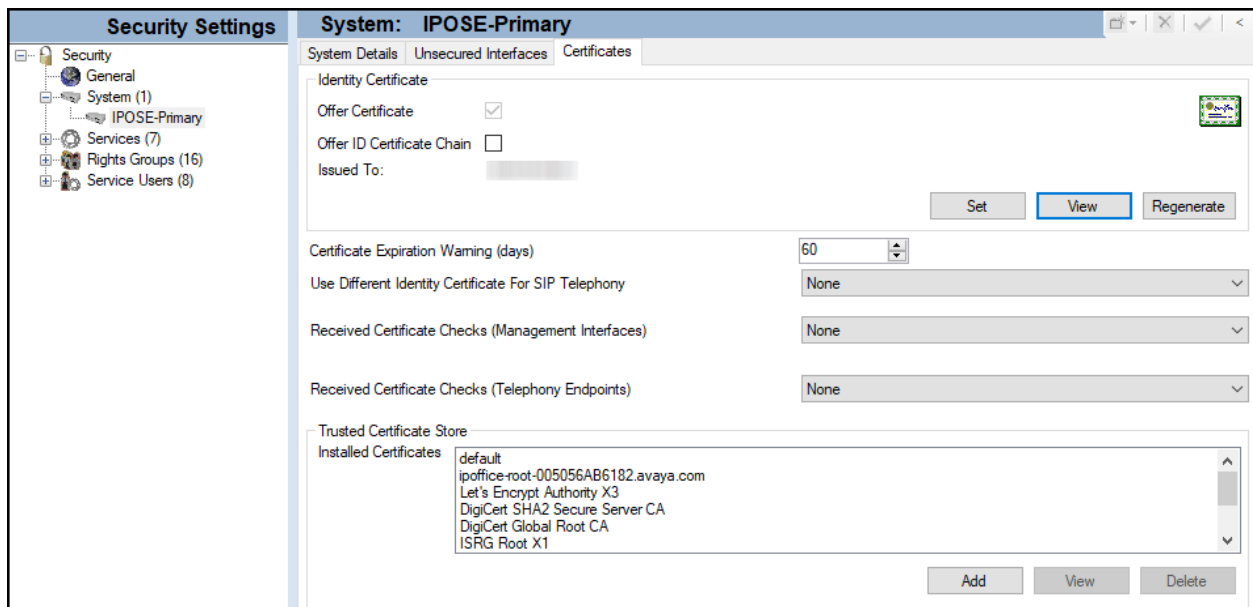
Feature	Instances	Status	Expiration Date	Source
Additional Voicemail Pro Ports	2	Valid	Never	WebLM
Power User	1	Valid	Never	WebLM
Avaya IP endpoints	6	Valid	Never	WebLM
SIP Trunk Channels	10	Valid	Never	WebLM
Server Edition	1	Valid	Never	WebLM
Basic User	5	Valid	Never	WebLM

5.2. TLS Management

For the compliance test, the signaling on the SIP trunk between IP Office and the Avaya SBCE was secured using TLS. Testing was done using identity certificates signed by a local certificate authority, Avaya Aura® System Manager. The generation and installation of these certificates are beyond the scope of these Application Notes. However, once the certificates are available, they can be viewed on IP Office in the following manner.

To view the certificates currently installed on IP Office, navigate to **File → Advanced → Security Settings**. Log in with the appropriate security credentials (not shown). In the Security Settings window, navigate to **Security → System** and select the **Certificates** tab.

To verify the identity certificate, locate the **Identity Certificate** section and click **View** to see the details of the certificate.



5.3. 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.

5.3.1. 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 Avaya network via the public internet. To access the **LAN1** settings, navigate to **System (1) → IPOSE-Primary** in the Navigation Pane, then in the Details Pane navigate to the **LAN1 → LAN Settings** tab. The **LAN1** settings for the compliance testing were configured with following parameters:

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

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'Configuration' tree, and on the right is the 'IPOSE-Primary' details pane. The 'LAN1' tab is selected, and the 'LAN Settings' sub-tab is active. The configuration fields are as follows:

Field	Value
IP Address	10 . 64 . 101 . 127
IP Mask	255 . 255 . 255 . 0
Number Of DHCP IP Addresses	127
DHCP Mode	<input type="radio"/> Server <input type="radio"/> Client <input checked="" type="radio"/> Disabled

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

5.3.1.1 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 Avaya.
- 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 (not shown).

System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	VoIP
LAN Settings		VoIP		Network Topology						
<input checked="" type="checkbox"/> H.323 Gatekeeper Enable <input type="checkbox"/> Auto-create Extension <input type="checkbox"/> Auto-create User <input checked="" type="checkbox"/> H.323 Remote Extension Enable H.323 Signaling over TLS Preferred Remote Call Signaling Port 1720										
<input checked="" type="checkbox"/> SIP Trunks Enable <input checked="" type="checkbox"/> SIP Registrar Enable <input type="checkbox"/> Auto-create Extension/User <input checked="" type="checkbox"/> SIP Remote Extension Enable Allowed SIP User Agents Block blacklist only										
SIP Domain Name		avaya.lab.com								
SIP Registrar FQDN		avaya.lab.com								
Layer 4 Protocol		<input checked="" type="checkbox"/> UDP	UDP Port	5060	Remote UDP Port	5060				
		<input checked="" type="checkbox"/> TCP	TCP Port	5060	Remote TCP Port	5060				
		<input checked="" type="checkbox"/> TLS	TLS Port	5061	Remote TLS Port	5061				
Challenge Expiration Time (sec)		10								
RTP										
Port Number Range		Minimum	40750	Maximum	50750					
Port Number Range (NAT)		Minimum	40750	Maximum	50750					
<input checked="" type="checkbox"/> Enable RTCP Monitoring on Port 5005 RTCP collector IP address for phones 0 . 0 . 0 . 0										
Keepalives										
Scope	RTP-RTCP		Periodic timeout	30						
Initial keepalives	Enabled									

5.3.1.2 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.

The screenshot shows the 'Network Topology' configuration window for LAN1. The window has a title bar with tabs for 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', 'System Events', 'SMTP', 'SMDR', 'VoIP', and 'Contact Center'. Below the title bar are sub-tabs for 'LAN Settings', 'VoIP', and 'Network Topology'. The 'Network Topology' sub-tab is active. The main area is titled 'Network Topology Discovery' and contains the following fields and controls:

- STUN Server Address:** An empty text input field.
- STUN Port:** A spinner box set to 3478.
- Firewall/NAT Type:** A dropdown menu set to 'Open Internet'.
- Binding Refresh Time (sec):** A spinner box set to 60.
- Public IP Address:** A text input field containing '0 . 0 . 0 . 0'.
- Public Port:** A section with three sub-fields: 'UDP' (spinner box set to 0), 'TCP' (spinner box set to 0), and 'TLS' (spinner box set to 0).
- Run STUN on startup:** An unchecked checkbox.
- Buttons:** 'Run STUN' and 'Cancel' buttons are located at the bottom right.

5.3.2. 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 (not shown).

The screenshot displays the 'Telephony' configuration tab within a system management interface. The top navigation bar includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and Contact Center. The 'Telephony' sub-tab is active, showing settings for Park & Page, Tones & Music, Ring Tones, SM, Call Log, and TUI.

Key configuration areas include:

- Dial Delay Time (sec):** 4
- Dial Delay Count:** 0
- Default No Answer Time (sec):** 15
- Hold Timeout (sec):** 0
- Park Timeout (sec):** 300
- Ring Delay (sec):** 5
- Call Priority Promotion Time (sec):** Disabled
- Default Currency:** USD
- Default Name Priority:** Favor Directory
- Media Connection Preservation:** Enabled
- Phone Failback:** Automatic
- Login Code Complexity:** Enforcement and Complexity are checked. Minimum length is 6.
- RTCP Collector Configuration:** Send RTCP to an RTCP Collector is unchecked. Server Address is 0.0.0.0, UDP Port Number is 5005, and RTCP reporting interval is 5 seconds.
- Companding Law:** U-Law and U-Law Line are selected.
- Other Settings:** DSS Status, Auto Hold, Dial By Name, Show Account Code, Inhibit Off-Switch Forward/Transfer, Restrict Network Interconnect, Drop External Only Impromptu Conference, Visually Differentiate External Call, High Quality Conferencing, Directory Overrides Barring, Advertise Callee State To Internal Callers, and Internal Ring on Transfer are also visible.

5.3.3. System – VoIP Tab

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

5.3.3.1 VoIP – VoIP Tab

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

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

The screenshot displays the VoIP configuration interface. At the top, there are tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. The VoIP tab is active, and sub-tabs for VoIP Security and Access Control Lists are visible. Below the tabs, there are two checkboxes: 'Ignore DTMF Mismatch For Phones' and 'Allow Direct Media Within NAT Location', both of which are unchecked. The 'RFC2833 Default Payload' field is set to '101'. The 'Default Codec Selection' section contains three columns: 'Available Codecs', 'Unused', and 'Selected'. The 'Available Codecs' list includes G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, and G.729(a) 8K CS-AC, with the first three checked. The 'Unused' column is empty. The 'Selected' column contains G.711 ULAW 64K, G.711 ALAW 64K, and G.729(a) 8K CS-A. Between the 'Unused' and 'Selected' columns are five buttons: '>>>', an up arrow, '<<<', a down arrow, and '>>>'.

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 5.5.5** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.3.3.2 VoIP – VoIP Security Tab

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

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

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

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

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

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

The screenshot shows the configuration interface for VoIP Security. At the top, there are tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. The VoIP tab is active, and the 'VoIP Security' sub-tab is selected. Below the tabs, there are fields for 'Default Extension Password' and 'Confirm Default Extension Password'. The 'Media Security' dropdown menu is set to 'Preferred'. To the right of this dropdown is a checkbox for 'Strict SIPS', which is unchecked. Below these are the 'Media Security Options' section, which includes 'Encryptions' (with 'RTP' checked and 'RTCP' unchecked), 'Authentication' (with 'RTP' and 'RTCP' both checked), and 'Replay Protection'. The 'SRTP Window Size' is set to 64. At the bottom, the 'Crypto Suites' section has 'SRTP_AES_CM_128_SHA1_80' checked and 'SRTP_AES_CM_128_SHA1_32' unchecked.

5.4. 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 Avaya network.

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view of the configuration hierarchy, with 'IP Route (3)' selected and expanded to show three entries: '0.0.0.0', '10.64.70.0', and '192.168.128.0'. The '0.0.0.0' entry is highlighted. The main pane on the right shows the configuration for the selected '0.0.0.0' IP Route. The configuration fields are as follows:

0.0.0.0	
IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	10 . 64 . 101 . 1
Destination	LAN1
Metric	0

5.5. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Avaya SIP Trunking Service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.5.1** 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 5.5.2** to **5.5.6**.

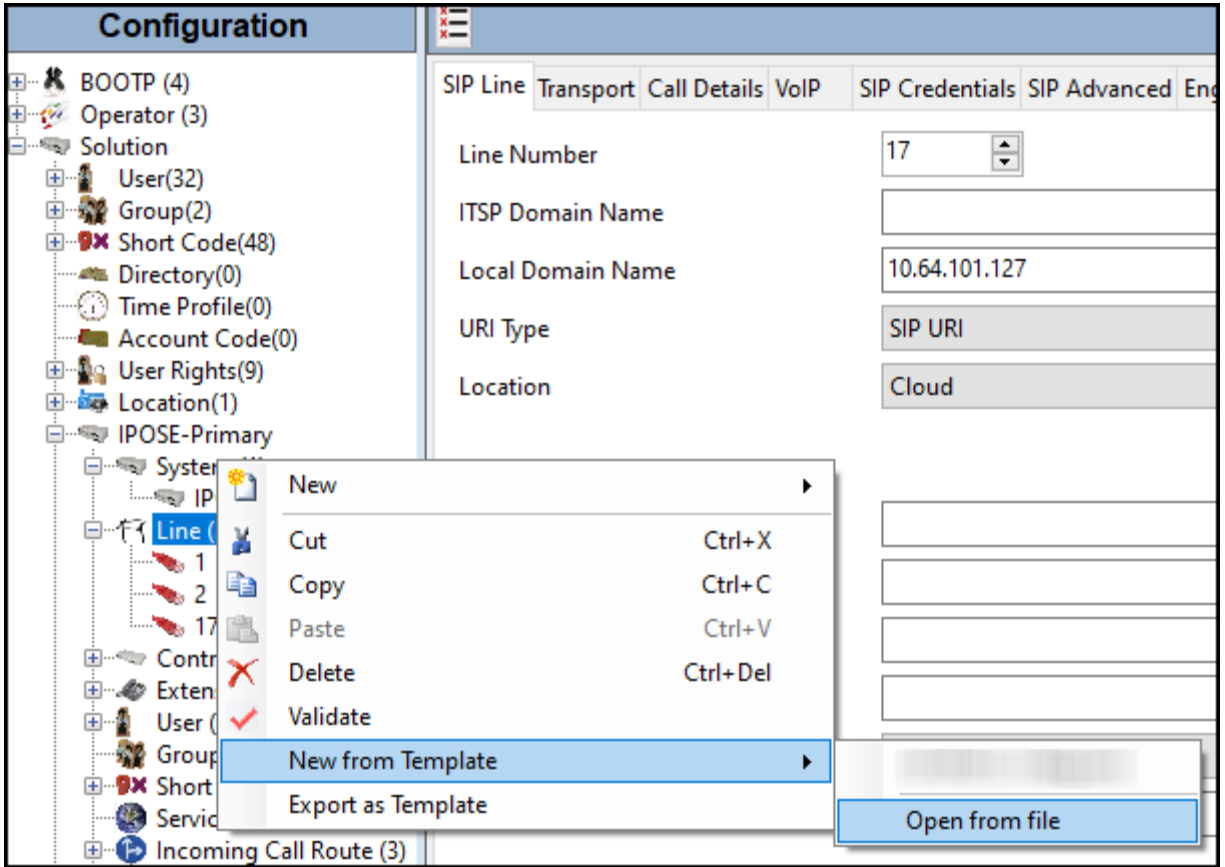
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.5.2** to **5.5.6**.

5.5.1. Creating a SIP Trunk from an XML Template

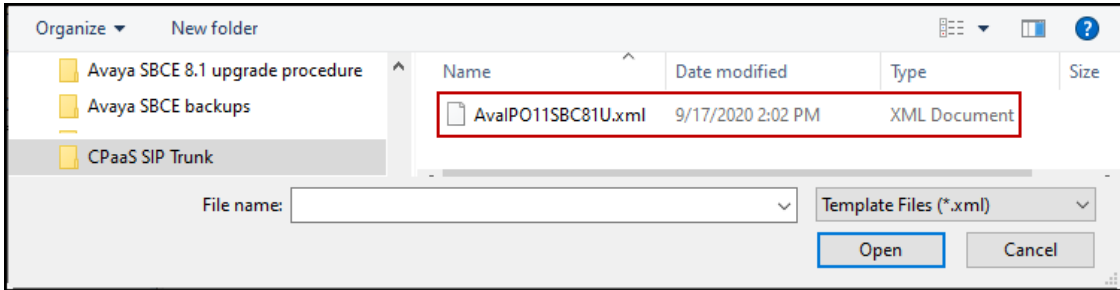
SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition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

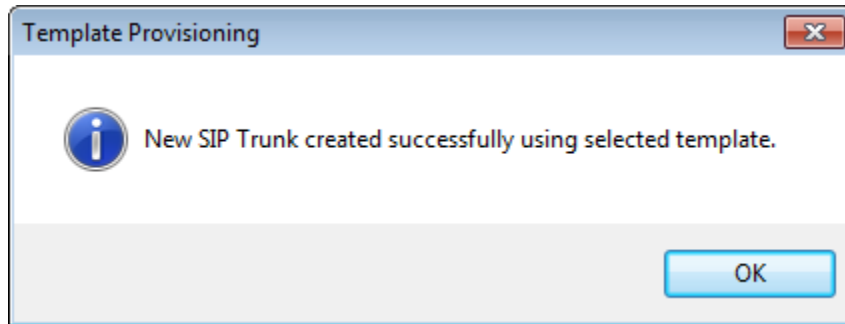
To create the SIP Trunk from the template, from the **Primary** server, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template→Open from file**.



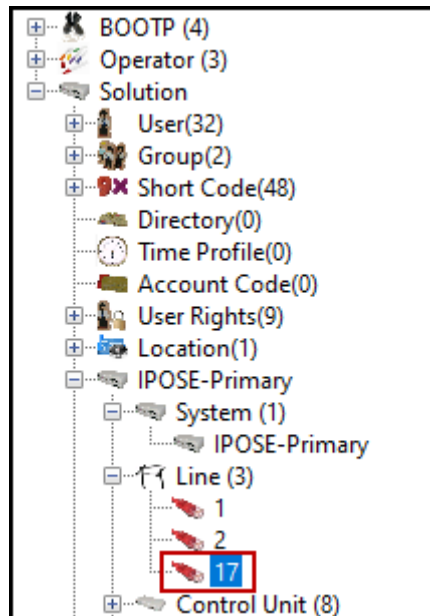
Navigate to the directory on the local machine where the template was copied and select the template.



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 5.5.2 to 5.5.6**.

5.5.2. SIP Line – SIP Line Tab

The **SIP Line** tab in the Details pane is shown below for Line Number **17**, 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.
- **Local Domain Name** is set to the IP address of the Avaya IP Office LAN1 interface (e.g., **10.64.101.127**).
- 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 **Always** (SIP REFER is supported by the Service Provider).
- Check **Outgoing Blind REFER** parameter to enable the use of REFER for blind transfers.
- Click **OK** to commit (not shown).

SIP Line - Line 17	
SIP Line Transport Call Details VoIP SIP Credentials SIP Advanced Engineering	
Line Number	17
ITSP Domain Name	
Local Domain Name	10.64.101.127
URI Type	SIP URI
Location	Cloud
Prefix	
National Prefix	
International Prefix	
Country Code	
Name Priority	System Default
Description	Service Provider
In Service	<input checked="" type="checkbox"/>
Check OOS	<input checked="" type="checkbox"/>
Session Timers	
Refresh Method	Auto
Timer (sec)	On Demand
Redirect and Transfer	
Incoming Supervised REFER	Always
Outgoing Supervised REFER	Always
Send 302 Moved Temporarily	<input type="checkbox"/>
Outgoing Blind REFER	<input checked="" type="checkbox"/>

5.5.3. SIP Line – Transport Tab

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

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

The screenshot shows the 'Transport' tab of the SIP Line configuration. The 'ITSP Proxy Address' field contains '10.64.101.243'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'TLS' and 'Send Port' is '5061'. 'Use Network Topology Info' is set to 'None' and 'Listen Port' is '5061'. 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0'. 'Calls Route via Registrar' is checked. 'Separate Registrar' is an empty field.

Note: For the compliance testing, the **Use Network Topology Info** field was set to **None**, since no NAT was used in the test configuration. 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.

5.5.4. 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 line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- 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.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.

The screenshot shows a configuration window titled "SIP Line - 17 | Call Details | SIP URI". The window contains the following fields and options:

- New URI** section:
 - Incoming Group: 17
 - Outgoing Group: 17
 - Credentials: 0: <None>
 - Max Sessions: 10
- Field meaning** table:

	Display	Content	Outgoing Calls	Forwarding/Twinning	Incoming Calls
Local URI	Auto	Auto	Caller	Original Caller	Called
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

Buttons at the bottom: OK, Cancel, Help.

5.5.5. 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. Avaya supports codecs **G.711ULAW**, **G.711ALAW** and **G.729(a)** for audio.
- Select **T38** for **Fax Transport Support** (Refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set the **Media Security** field to **Same as System (Preferred)**.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).

The screenshot displays the configuration interface for a SIP Line, specifically the VoIP tab. The interface includes several sections:

- Codec Selection:** A dropdown menu is set to "Custom". Below it, there are two lists: "Unused" (empty) and "Selected" (containing G.711 ULAW 64K, G.711 ALAW 64K, and G.729(a) 8K CS-ACELP). Navigation buttons (right arrow, up arrow, left arrow, down arrow, right arrow) are positioned between the lists.
- Fax Transport Support:** A dropdown menu is set to "T38".
- DTMF Support:** A dropdown menu is set to "RFC2833/RFC4733".
- Media Security:** A dropdown menu is set to "Same as System (Preferred)".
- Advanced Media Security Options:** A section with a "Same As System" checkbox checked. It includes:
 - Encryptions:** RTP (checked), RTCP (unchecked).
 - Authentication:** RTP (checked), RTCP (checked).
 - Replay Protection:** SRTP Window Size set to 64.
 - Crypto Suites:** SRTP_AES_CM_128_SHA1_80 (checked), SRTP_AES_CM_128_SHA1_32 (unchecked).
- Other Options:** Local Hold Music (unchecked), Re-invite Supported (checked), Codec Lockdown (unchecked), Allow Direct Media Path (unchecked), Force direct media with phones (unchecked), PRACK/100rel Supported (checked).

Note: The codec selections defined under this section are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.3.3** are the codecs selected for the IP phones/extension (H.323 and SIP).

5.5.6. 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**.

In the **Call Control** area:

- Check **Emulate NOTIFY for REFER** (Refer to **Section 2.2**).
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

SIP Line Transport Call Details VoIP SIP Credentials SIP Advanced Engineering

Addressing

Association Method: By Source IP address

Call Routing Method: To Header

Use P-Called-Party:

Suppress DNS SRV Lookups:

Identity

Use "phone-context":

Add user=phone:

Use + for International:

Use PAI for Privacy:

Use Domain for PAI:

Caller ID from From header:

Send From In Clear:

Cache Auth Credentials:

User-Agent and Server Headers:

Send Location Info: Never

Add UUI header:

Add UUI header to redirected calls:

Media

Allow Empty INVITE:

Send Empty re-INVITE:

Allow To Tag Change:

P-Early-Media Support: None

Send SilenceSupp=Off:

Force Early Direct Media:

Media Connection Preservation: Disabled

Indicate HOLD:

Call Control

Call Initiation Timeout (s): 4

Call Queuing Timeout (mins): 5

Service Busy Response: 486 - Busy Here

on No User Responding Send: 408-Request Timeout

Action on CAC Location Limit: Allow Voicemail

Suppress Q.850 Reason Header:

Emulate NOTIFY for REFER:

No REFER if using Diversion:

5.6. Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.5**. To configure these settings, first navigate to **User** → *Name* in the Navigation Pane where *Name* is the name of the user to be modified. In the example below, the name of the user is **Ext3041 H323**. Select the **SIP** tab in the Details Pane. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Avaya. Note the DID number is preceded by +1 since its required in order to conform with the E.164 numbering format. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network. This can also be accomplished by activating Withhold Number on H.323 Deskphones (not shown). Click the **OK** to commit (not shown).

The screenshot displays the Avaya configuration interface. On the left is a navigation tree under 'Configuration' with 'User (7)' selected and highlighted with a red box. The right pane shows the configuration for 'Ext3041 H323: 3041*'. The 'SIP' tab is active, showing the following fields:

Dial In	Voice Recording	Button Programming	Menu Programming	Mobility	Group Membership	Announcements	SIP
SIP Name							+12134101011
SIP Display Name (Alias)							Ext3041 H323
Contact							+12134101011
<input type="checkbox"/> Anonymous							

5.7. 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.

Configuration		IP Office Line - Line 1	
<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 <ul style="list-style-type: none"> System (1) <ul style="list-style-type: none"> IPOSE-Primary <ul style="list-style-type: none"> Line (3) <ul style="list-style-type: none"> 1 2 17 Control Unit (8) Extension (6) User (7) Group (0) Short Code (2) Service (0) Incoming Call Route (3) IP Route (3) License (6) ARS (1) Location (1) Authorization Code (0) IP500V2-One IP500V2-Two 		<div style="border: 1px solid gray; padding: 5px;"> <div style="display: flex; justify-content: space-between;"> Line Short Codes VoIP Settings </div> <hr/> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>Line Number: <input type="text" value="1"/></p> <p>Transport Type: <input type="text" value="WebSocket Server"/></p> <p>Networking Level: <input type="text" value="SCN"/></p> <p>Security: <input type="text" value="Medium"/></p> <hr/> <p>Gateway</p> <p>Address: <input type="text" value="192 . 168 . 128 . 165"/></p> <p>Location: <input type="text" value="3: Thornton, CO"/></p> <p>Password: <input type="password" value="....."/></p> <p>Confirm Password: <input type="password" value="....."/></p> </div> <div style="width: 45%;"> <p>Telephone Number: <input type="text"/></p> <p>Prefix: <input type="text"/></p> <p>Outgoing Group ID: <input type="text" value="99999"/></p> <p>Number of Channels: <input type="text" value="250"/></p> <p>Outgoing Channels: <input type="text" value="250"/></p> <hr/> <p>SCN Resiliency Options</p> <p><input type="checkbox"/> Supports Resiliency</p> <p><input type="checkbox"/> Backs up my IP phones</p> <p><input type="checkbox"/> Backs up my hunt groups</p> <p><input type="checkbox"/> Backs up my voicemail</p> <p><input type="checkbox"/> Backs up my IP DECT phones</p> </div> </div> <hr/> <p>Description: <input type="text"/></p> </div>	

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

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **T38** for **Fax Transport Support** (refer to Section 2.2).
- Under **Media Security** verify **Same as System (Preferred)** is selected (default value).

The screenshot displays the 'VoIP Settings' tab for an IP Office Line. The interface includes several configuration sections:

- Out Of Band DTMF**:
- Allow Direct Media Path**:
- Codec Selection**: A dropdown menu is set to 'System Default'. Below it are two columns: 'Unused' (empty) and 'Selected' (containing G.711 ULAW 64K, G.711 ALAW 64K, and G.729(a) 8K CS-ACELP). Navigation buttons (right, up, left, down, right) are positioned between the columns.
- Fax Transport Support**: A dropdown menu is set to 'T38'.
- Call Initiation Timeout (s)**: A numeric input field is set to '4'.
- Media Security**: A dropdown menu is set to 'Same as System (Preferred)'. Below it is an 'Advanced Media Security Options' section with a 'Same As System' checkbox checked. This section contains:
 - Encryptions**: RTP, RTCP
 - Authentication**: RTP, RTCP
 - Replay Protection**: **SRTP Window Size** is set to '64'.
 - Crypto Suites**: SRTP_AES_CM_128_SHA1_80, SRTP_AES_CM_128_SHA1_32

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

5.8. Incoming Call Route

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

- Set **Bearer Capacity** to **Any Voice**.
- The **Line Group ID** is set to **17**. This matches the **Incoming Group** field configured in the **Call Details** tab for the SIP Line on **Section 5.5.4**.
- On the **Incoming Number**, enter one of the DID numbers provided by Avaya. Note the DID number is preceded by **+1** since its required in order to conform with the E.164 numbering format.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the configuration window for an Incoming Call Route. The left pane shows a tree view with 'Incoming Call Route (3)' expanded to show three routes: '17 +12134101011', '17 +12134237452', and '17 +12134237986'. The right pane shows the configuration for the selected route, with the 'Standard' tab active. The configuration fields are as follows:

Parameter	Value
Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	+12134101011
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 +12134101011 provided by Avaya was associated with the Avaya IP Office extension **3041**.

Standard	Voice Recording	Destinations	
	TimeProfile	Destination	Fallback Extension
▶	Default Value	3041 Ext3041 H323	▼

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

5.9. 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.

5.9.1. Short Codes and Automatic Route Selection

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is a navigation tree under 'Configuration' with 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 including *66*N# and 9N. The '9N' short code is selected. On the right, the configuration details for '9N: Dial' are shown in a form:

9N: Dial	
Short Code	
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	50: Main
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

As described above, Short Code **9N** was defined for ARS access. Therefore, outbound calls via ARS are dialed as 9 plus the number. ARS will strip off the 9, and it will process the call based on the remaining digits. **ARS 50: Main** shown below was used during the compliance test.

Select **ARS → 50: Main** on the Navigation Pane and click **Add**.

The screenshot shows the configuration page for ARS 50: Main. The left navigation pane lists various system components, with 'ARS 50: Main' selected. The main configuration area includes the following fields and options:

- ARS Route ID: 50
- Route Name: Main
- Dial Delay Time: System Default (4)
- Description: (empty)
- In Service: (Out of Service Route: <None>)
- Time Profile: <None> (Out of Hours Route: <None>)
- Secondary Dial tone: (SystemTone)
- Check User Call Barring:

A table of codes is displayed below the configuration fields:

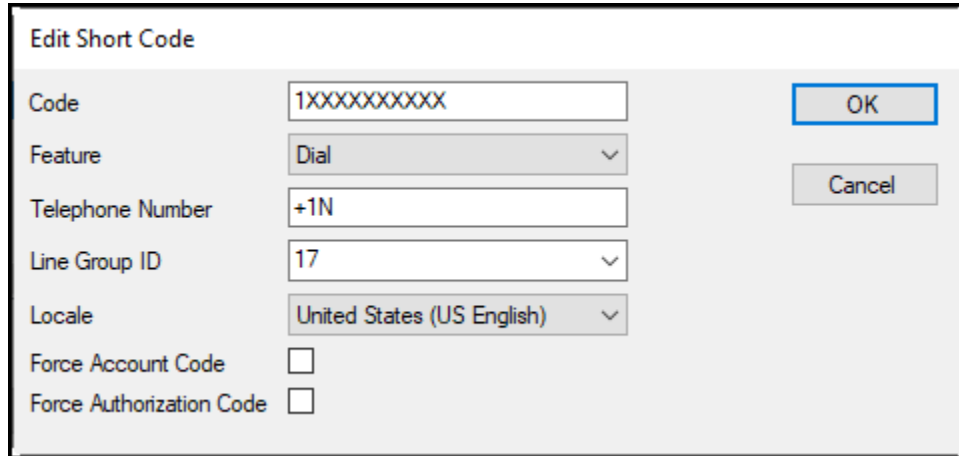
Code	Telephone Number	Feature	Line Group ID
01XXXXXXXXXX	01N	Dial	17
040	040	Dial	17
1XXXXXXXXXX	+1N	Dial	17
2XXXXXX	2N	Dial	17
411	411	Dial	17
0919XXXXXXXXXX	0919N	Dial	17
0N:	0N	Dial 3K1	17

Below the table, the 'Alternate Route Priority Level' is set to 3, and the 'Alternate Route Wait Time' is set to 30. The 'Alternate Route' dropdown is set to <None>.

Configure the following parameters:

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **1** 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 **+1N**. The value **N** represents the additional number of digits dialed by the user after dialing **1** (The **9** will be stripped off). With this setting, the 10 digit dialed number, preceded by prefix **+1** will be sent to the SIP trunk, required to conform with the E.164 numbering format.
- 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**, **United States (US English)** was used.
- Click **OK** to commit.

The following example shows the dial pattern for calls within the North American Numbering Plan.



Edit Short Code	
Code	1XXXXXXXXXX
Feature	Dial
Telephone Number	+1N
Line Group ID	17
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

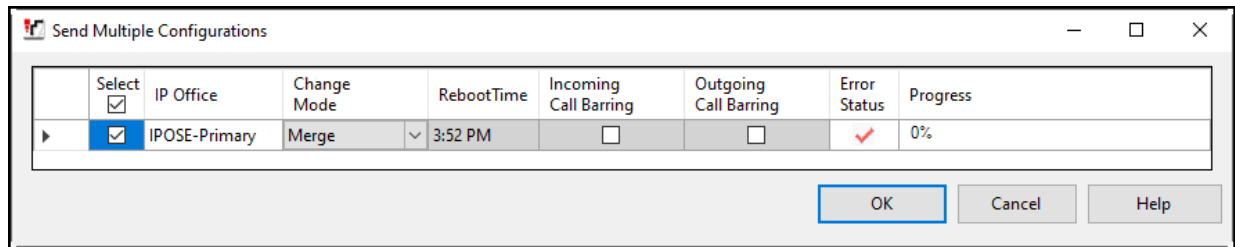
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

5.10. 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) <ul style="list-style-type: none"> ⊖ IP500V2-One ⊕ 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"> ⊖ Hardware Installed <ul style="list-style-type: none"> Control Unit: IP 500 V2 Internal Modules: VCM64/PRID U; PHONE8 Expansion Modules: DIG DCPx16 V2 ⊖ System Settings <ul style="list-style-type: none"> IP Address: 192.168.128.165 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 ⊖ Features Configured <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. Expansion System – 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 a configuration interface for an IP 500 V2 unit. The left pane shows a tree view of the configuration hierarchy, and the right pane shows the configuration details for the selected unit.

Configuration Hierarchy (Left Pane):

- Configuration
 - BOOTP (4)
 - Operator (3)
 - Solution
 - User(32)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - IP500V2-One
 - System (1)
 - Line (3)
 - Control Unit (4)
 - 1 IP 500 V2**
 - 2 VCM64/PRID U
 - 3 PHONE8
 - 6 DIG DCPx16 V2
 - 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)
 - 50: Main
 - 51: To-Primary
 - Location (1)
 - Authorization Code (0)
 - IP500V2-Two

Unit Configuration (Right Pane):

Unit	
Device Number	1
Unit Type	IP 500 V2
Version	11.1.0.1.0 build 95
Serial Number	
Unit IP Address	192.168.128.165
Interconnect Number	0
Module Number	Control Unit

6.2. Expansion System – LAN Settings

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

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

The screenshot displays the configuration interface for an IP500V2-One system. On the left is a navigation tree under 'Configuration', with 'IP500V2-One' expanded to show 'System (1)' and 'IP500V2-One'. The main pane shows the configuration for 'IP500V2-One' with tabs for 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', and 'System Events'. The 'LAN1' tab is active, showing 'LAN Settings' and 'Network Topology' sub-tabs. The 'LAN Settings' sub-tab is selected, displaying the following configuration:

IP Address	192 . 168 . 128 . 165
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	0 . 0 . 0 . 0
RIP Mode	None
<input type="checkbox"/> Enable NAT	
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	
<input type="button" value="Advanced"/>	

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

6.3. Expansion System – IP Route

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

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

The screenshot displays the configuration interface for an IP Office system. On the left is a tree view under 'Configuration' showing various system components. The 'IP Route' folder is expanded, and the route '0.0.0.0' is selected. On the right, the configuration details for this 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 . 128 . 200
Destination	LAN1
Metric	0
	<input type="checkbox"/> Proxy ARP

6.4. Expansion System – IP Office Line

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

The screenshot displays the configuration interface for an IP Office Line. On the left is a navigation tree under the 'Configuration' header, showing a hierarchy from Solution down to IP500V2-Two. The main area is titled 'IP Office Line - Line 17' and contains several tabs: 'Line', 'Short Codes', 'VoIP Settings', and 'T38 Fax'. The 'Line' tab is active, showing the following configuration fields:

- Line Number: 17
- Transport Type: WebSocket Client
- Networking Level: SCN
- Security: Medium
- Telephone Number: [Empty]
- Prefix: [Empty]
- Outgoing Group ID: 99999
- Number of Channels: 250
- Outgoing Channels: 250

Below these fields is the 'Gateway' section:

- Address: 10 . 64 . 101 . 127
- Port: 443
- Location: 3: Thornton, CO
- Password: [Masked]
- Confirm Password: [Masked]

At the bottom right, there are 'SCN Resiliency Options' with three checkboxes:

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

A 'Description' field is located at the bottom of the configuration area.

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

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **T38** for **Fax Transport Support** (refer to Section 2.2).
- Under **Media Security Preferred** was selected.

The screen below shows the IP Office Line, **T38 Fax** tab:

- Uncheck the **Use Default Values** at the bottom of the screen.
- Set the **T.38 Fax Version** to **0**.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).

Line	Short Codes	VoIP Settings	T38 Fax
T38 Fax Version			0
Transport			UDPTL
Redundancy			
Low Speed			0
High Speed			0
TCF Method			Trans TCF
Max Bit Rate (bps)			14400
EFlag Start Timer (ms)			2600
EFlag Stop Timer (ms)			2300
Tx Network Timeout (sec)			150
<input type="checkbox"/> Use Default Values			
<input checked="" type="checkbox"/> Scan Line Fix-up			
<input checked="" type="checkbox"/> TFO Enhancement			
<input type="checkbox"/> Disable T30 ECM			
<input type="checkbox"/> Disable EFlags For First DIS			
<input type="checkbox"/> Disable T30 MR Compression			
<input type="checkbox"/> NSF Override			
Country Code			0
Vendor Code			0

6.5. Expansion System – Short Codes

Similar to the configuration of the Primary server in **Section 5.9.1**, create a Short Code to access ARS. In the reference configuration, the **Line Group ID** is set to the ARS route illustrated in the next section.

The screenshot displays a configuration interface with a tree view on the left and a configuration form on the right. The tree view shows a hierarchy of configuration objects, including 'Solution', 'User(32)', 'Group(2)', 'Short Code(48)', 'Directory(0)', 'Time Profile(0)', 'Account Code(0)', 'User Rights(9)', 'Location(1)', 'IPOSE-Primary', 'IP500V2-One', '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)', and 'Authorization Code (0)'. The 'Short Code (12)' folder is expanded, showing a '9N' short code. The configuration form on the right is titled '9N: Dial' and contains the following fields:

Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	51: To-Primary
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

6.6. Expansion System 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 system configuration, with "ARS (2)" expanded to show "50: Main" and "51: To-Primary".

The main configuration area includes the following fields:

- ARS Route ID: 51
- Route Name: To-Primary
- Dial Delay Time: System Default (4)
- Description: (empty)
- In Service: (with arrows pointing to Out of Service Route: <None>)
- Time Profile: <None> (with arrows pointing to Out of Hours Route: <None>)
- Secondary Dial tone: (dropdown menu set to System Tone)
- Check User Call Barring:

A table lists the route entries:

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

Additional settings at the bottom include:

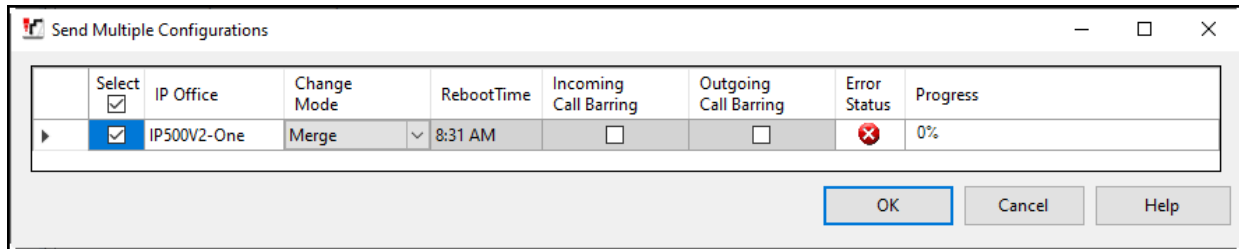
- Alternate Route Priority Level: 3 (with arrow pointing to Alternate Route: <None>)
- Alternate Route Wait Time: 30

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

6.7. Save 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 configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **References** section.

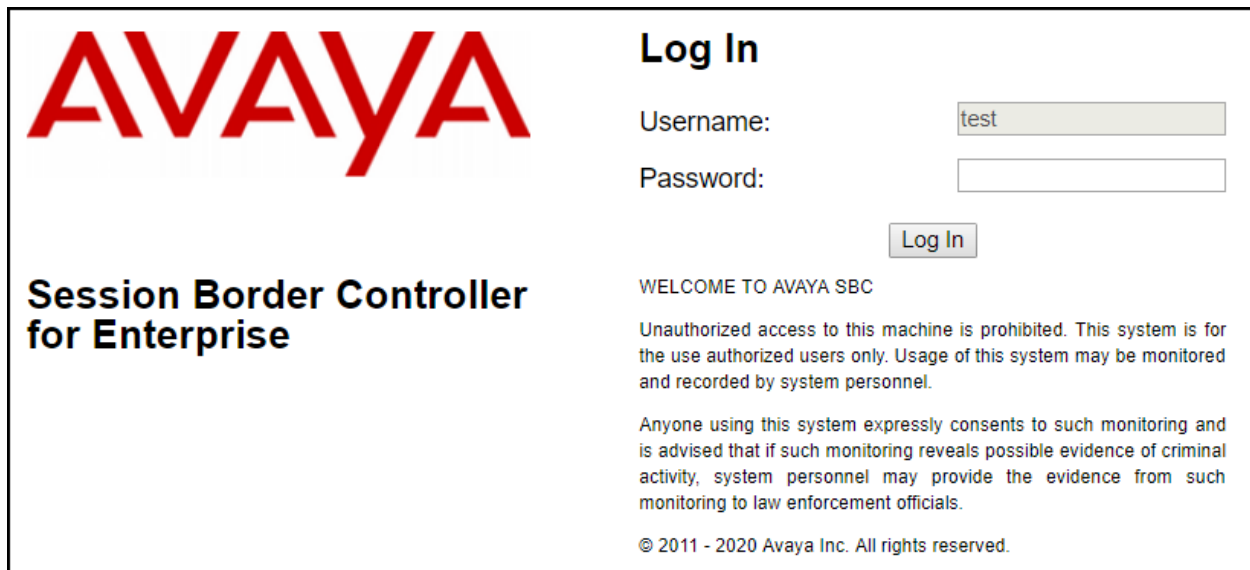
Some screens capture will show the use of the **Edit** command instead of the **add** command, since the configuration used for the testing was previously added.

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 Session Border Controller for Enterprise login interface. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, the "Log In" section contains a "Username:" field with the value "test" and a "Password:" field. Below the password field is a "Log In" button. Underneath the login fields, there is a "WELCOME TO AVAYA SBC" message, followed by a disclaimer: "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." Below the disclaimer is a statement: "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." At the bottom, the copyright notice reads: "© 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 shows the Avaya SBCE dashboard for device **EMS**. The top navigation bar includes **Device: EMS**, **Alarms**, **Incidents**, **Status**, **Logs**, **Diagnostics**, **Users**, **Settings**, **Help**, and **Log Out**. The left sidebar shows the **EMS Dashboard** with menu items: **Device Management**, **System Administration**, **Backup/Restore**, and **Monitoring & Logging**. The main content area is titled **Dashboard** and contains several sections:

- Information:** A table with the following data:

System Time	10:30:12 AM EDT	Refresh
Version	8.1.1.0-26-19214	
GUI Version	8.1.1.0-19189	
Build Date	Wed Jul 22 23:36:51 UTC 2020	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	09/10/2020 12:49:15 EDT	
Failed Login Attempts	0	
- Installed Devices:** A list showing **EMS** and **Avaya_SBCE**.
- Active Alarms (past 24 hours):** A section stating "None found."
- Incidents (past 24 hours):** A list of five incidents, all with the message "Avaya_SBCE: No Subscriber Flow Matched".

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.

The screenshot shows the Avaya SBCE dashboard for device **Avaya_SBCE**. The top navigation bar includes **Device: Avaya_SBCE**, **Alarms**, **Incidents**, **Status**, **Logs**, **Diagnostics**, **Users**, **Settings**, **Help**, and **Log Out**. The left sidebar shows the **EMS Dashboard** with menu items: **Device Management**, **Backup/Restore**, **System Parameters**, **Configuration Profiles**, **Services**, **Domain Policies**, **TLS Management**, **Network & Flows**, **DMZ Services**, and **Monitoring & Logging**. The main content area is titled **Dashboard** and contains several sections:

- Information:** A table with the following data:

System Time	10:32:23 AM EDT	Refresh
Version	8.1.1.0-26-19214	
GUI Version	8.1.1.0-19189	
Build Date	Wed Jul 22 23:36:51 UTC 2020	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	09/10/2020 12:49:15 EDT	
Failed Login Attempts	0	
- Installed Devices:** A list showing **EMS** and **Avaya_SBCE**.
- Active Alarms (past 24 hours):** A section stating "None found."
- Incidents (past 24 hours):** A list of one incident with the message "Avaya_SBCE: No Subscriber Flow Matched".

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 'Device Management' section of the Avaya Session Border Controller for Enterprise 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 sidebar lists various management options, with 'Device Management' highlighted. The main content area shows a 'Device Management' tab with sub-tabs for 'Devices', 'Updates', 'SSL VPN', 'Licensing', and 'Key Bundles'. A table lists the device 'Avaya_SBCE' with a blurred management IP, version '8.1.1.0-26-19214', and status 'Commissioned'. Action buttons for 'Reboot', 'Shutdown', 'Restart Application', 'View', 'Edit', and 'Uninstall' are visible for the device.

Device Name	Management IP	Version	Status	
Avaya_SBCE	[Blurred]	8.1.1.0-26-19214	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

To view the network configuration assigned to the Avaya SBCE, click **View** on the previous above. The **System Information** window is displayed, containing the current device configuration and network settings. Note that **DNS configuration** is required for this solution. The DNS information can be added by clicking on **Edit** shown on the previous screen.

System Information: Avaya_SBCE X

<p>General Configuration</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Appliance Name</td><td>Avaya_SBCE</td></tr> <tr><td>Box Type</td><td>SIP</td></tr> <tr><td>Deployment Mode</td><td>Proxy</td></tr> </table>	Appliance Name	Avaya_SBCE	Box Type	SIP	Deployment Mode	Proxy	<p>Device Configuration</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>HA Mode</td><td>No</td></tr> <tr><td>Two Bypass Mode</td><td>No</td></tr> </table>	HA Mode	No	Two Bypass Mode	No	<p>Dynamic License Allocation</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th></th> <th>Min License Allocation</th> <th>Max License Allocation</th> </tr> </thead> <tbody> <tr><td>Standard Sessions</td><td>100</td><td>200</td></tr> <tr><td>Advanced Sessions</td><td>100</td><td>200</td></tr> <tr><td>Scopia Video Sessions</td><td>0</td><td>0</td></tr> <tr><td>CES Sessions</td><td>0</td><td>0</td></tr> <tr><td>Transcoding Sessions</td><td>100</td><td>200</td></tr> <tr><td>Premium Sessions</td><td>0</td><td>0</td></tr> <tr><td>CLID</td><td>---</td><td></td></tr> <tr><td>Encryption Available: Yes</td><td><input checked="" type="checkbox"/></td><td></td></tr> </tbody> </table>		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	Premium Sessions	0	0	CLID	---		Encryption Available: Yes	<input checked="" type="checkbox"/>	
Appliance Name	Avaya_SBCE																																						
Box Type	SIP																																						
Deployment Mode	Proxy																																						
HA Mode	No																																						
Two Bypass Mode	No																																						
	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																																					
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
[Blurred]	[Blurred]	[Blurred]	[Blurred]	A1
[Blurred]	[Blurred]	[Blurred]	[Blurred]	A1
[Blurred]	[Blurred]	[Blurred]	[Blurred]	B1
[Blurred]	[Blurred]	[Blurred]	[Blurred]	B1
10.10.80.51	10.10.80.51	255.255.255.128	10.10.80.1	B1

<p>DNS Configuration</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Primary DNS</td><td>75.75.75.75</td></tr> <tr><td>Secondary DNS</td><td>75.75.76.76</td></tr> <tr><td>DNS Location</td><td>DMZ</td></tr> <tr><td>DNS Client IP</td><td>10.10.80.51</td></tr> </table>	Primary DNS	75.75.75.75	Secondary DNS	75.75.76.76	DNS Location	DMZ	DNS Client IP	10.10.80.51	<p>Management IP(s)</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>IP #1 (IPv4)</td><td>[Blurred]</td></tr> </table>	IP #1 (IPv4)	[Blurred]
Primary DNS	75.75.75.75										
Secondary DNS	75.75.76.76										
DNS Location	DMZ										
DNS Client IP	10.10.80.51										
IP #1 (IPv4)	[Blurred]										

The IP addresses in the **System Information** screen shown above are the ones used for the SIP trunk to the service provider and are the ones relevant to these Application Notes. The other IP addresses assigned to the Avaya SBCE **A1** and **B1** interfaces that are blurred out 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 **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

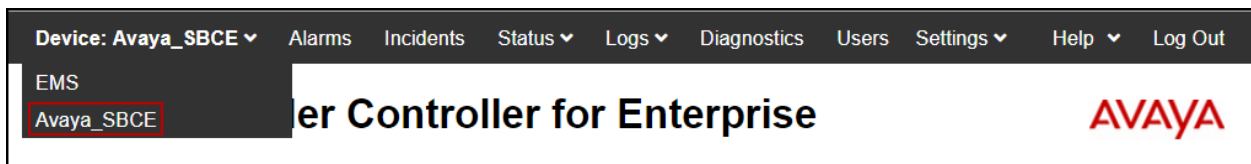
7.3. TLS Management

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

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

7.3.1. Verify TLS Certificates – Avaya Session Border Controller 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:

- System Manager CA certificate is present in the **Installed CA Certificates** area.
- System Manager CA signed identity certificate is present in the **Installed Certificates** area.
- Private key associated with the identity certificate is present in the **Installed Keys** area.

The screenshot displays the Avaya Session Border Controller for Enterprise 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 features the 'Session Border Controller for Enterprise' title and the 'AVAYA' logo. A left-hand navigation menu lists various management options, with 'TLS Management' and 'Certificates' highlighted. The main content area, titled 'Certificates', contains two buttons: 'Install' and 'Generate CSR'. Below these are four sections: 'Installed Certificates' (listing three certificates with 'View' and 'Delete' links), 'Installed CA Certificates' (listing one certificate named 'default.pem' with 'View' and 'Delete' links), 'Installed Certificate Revocation Lists' (displaying a message: 'No certificate revocation lists have been installed.'), and 'Installed Keys' (listing one key named 'IPO_INSIDE.key' with a 'Delete' link).

7.3.2. Server Profiles

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

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

TLS Profile	
Profile Name	IPO_Inside_Server
Certificate	IPO_INSIDE.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

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., **IPO_INSIDE.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 **1**.
- Click **Next**.

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

The screenshot shows a window titled "Edit Profile" with a close button (X) in the top right corner. At the top, there is a warning message in an orange box: "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." Below the warning, the form is organized into sections. The "TLS Profile" section includes: "Profile Name" (text input with "IPO_Inside_Client"), "Certificate" (dropdown menu with "IPO_INSIDE.pem"), and "SNI" (checkbox labeled "Enabled" which is unchecked). The "Certificate Verification" section includes: "Peer Verification" (checkbox labeled "Required" which is checked), "Peer Certificate Authorities" (dropdown menu with "Avaya_EP_CA_cert.pem", "DigiCertGlobalRootCA.cer", "GeoTrust_Global_CA_Trust.cer", and "default.pem"), "Peer Certificate Revocation Lists" (empty list box), "Verification Depth" (text input with "1"), "Extended Hostname Verification" (checkbox which is unchecked), and "Server Hostname" (empty text input). A "Next" button is located at the bottom center of the form.

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.

The left sidebar contains a navigation menu with categories like 'EMS Dashboard', '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: 'Remote_Worker_...', 'CenturyLink_Client', 'Outside_Client', 'Inside_Client', and 'IPO_Inside_Client' (which is highlighted in red).

The main content area is titled 'Client Profiles: IPO_Inside_Client' and features an 'Add' button and a 'Delete' button. Below this is a blue bar with the text 'Click here to add a description.' and a 'Client Profile' tab.

The configuration details for the 'IPO_Inside_Client' profile are as follows:

TLS Profile	
Profile Name	IPO_Inside_Client
Certificate	IPO_INSIDE.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	default.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
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:IDH:IADH:IMD5:1aNULL:1eNULL:@STRENGTH

An 'Edit' button is located at the bottom 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.

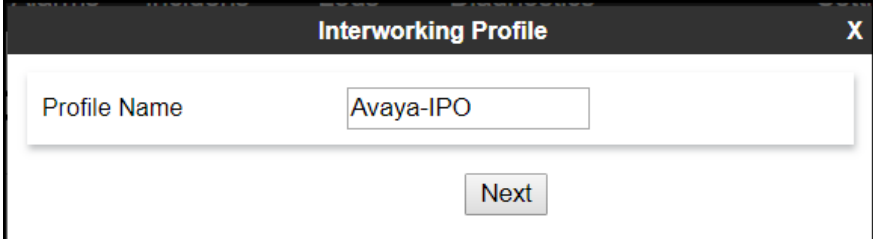
7.4.1. Server Interworking – Avaya-IPO

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

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

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



The screenshot shows a dialog box titled "Interworking Profile" with a close button (X) in the top right corner. The dialog contains a "Profile Name" label and a text input field containing the text "Avaya-IPO". Below the input field is a "Next" button.

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

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

The screenshot shows a dialog box titled "Editing Profile: Avaya-IPO" with a close button (X) in the top right corner. The dialog is divided into a "General" tab. The following table represents the configuration options visible in the dialog:

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

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

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

The screenshot displays the Avaya Session Border Controller 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', 'Device Management', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. Under 'Configuration Profiles', 'Server Interworking' is highlighted.

The main content area is titled 'Interworking Profiles: Avaya-IPO'. It features an 'Add' button and a list of profiles: 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-S...', 'Avaya-SM', 'Avaya-IPO' (highlighted), 'Avaya-CS1000', 'Avaya-CM', 'cs2100', and 'SP-General'. There are also 'Rename', 'Clone', and 'Delete' buttons.

The 'Avaya-IPO' profile configuration is shown in a modal window with the following tabs: 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, displaying a table of settings:

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

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. At the top, there is a navigation bar with the following items: 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.

On the left side, there is a navigation menu with the following items: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles (expanded), Domain DoS, **Server Interworking** (highlighted), 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, and Monitoring & Logging.

The main content area is titled "Interworking Profiles: Avaya-IPO". It features an "Add" button and three action buttons: "Rename", "Clone", and "Delete". Below this is a blue bar with the text "Click here to add a description." and a list of interworking profiles: avaya-ru, OCS-Edge-Se..., cisco-ccm, cups, OCS-FrontEn..., Avaya-SM, **Avaya-IPO** (highlighted), Avaya-CS1000, Avaya-CM, cs2100, and SP-General.

The configuration for the selected "Avaya-IPO" profile is shown in the "Advanced" tab. The configuration includes the following settings:

Setting	Value
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
DTMF	
DTMF Support	None

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

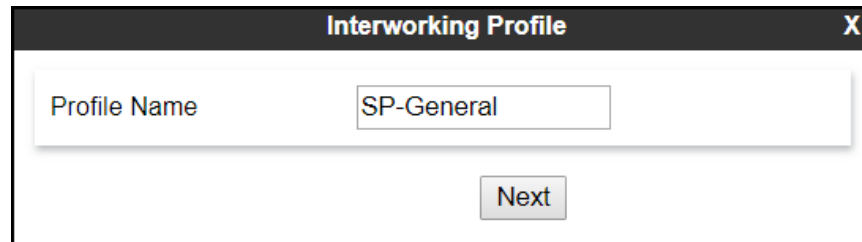
7.4.2. Server Interworking – SP-General

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. The dialog contains a text input field labeled "Profile Name" with the text "SP-General" entered. Below the input field is a "Next" button.

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

The screenshot shows a configuration window titled "Interworking Profile" with a close button (X) in the top right corner. The "General" tab is selected. The configuration options are as follows:

Field	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 checked="" 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

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.

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.

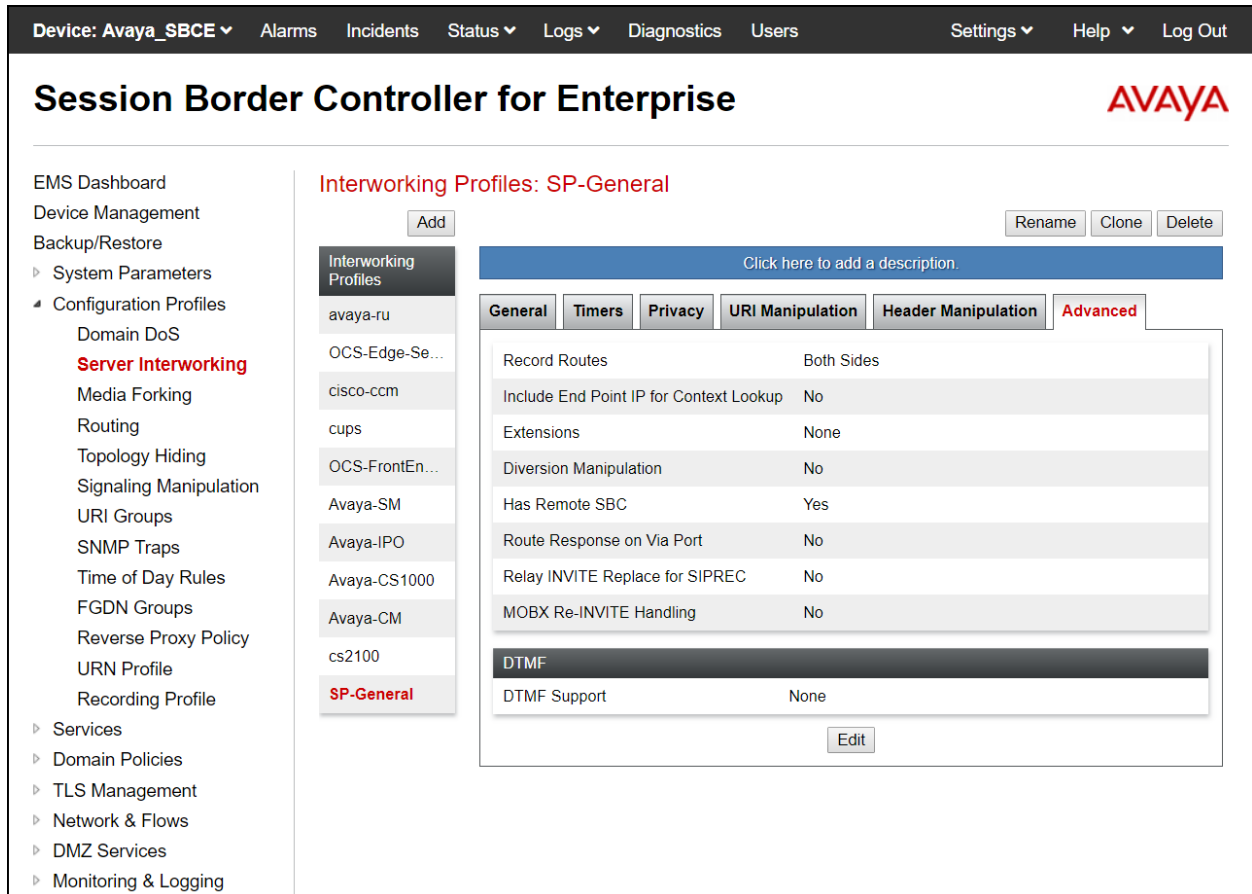
The left sidebar contains a navigation menu with categories like 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. Under 'Configuration Profiles', 'Server Interworking' is selected.

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

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

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

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

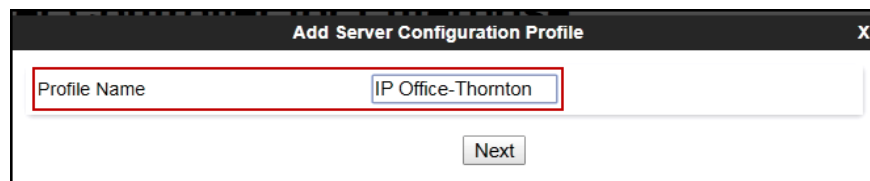


7.5. SIP Server Configuration

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

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

- Click **Next**.



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

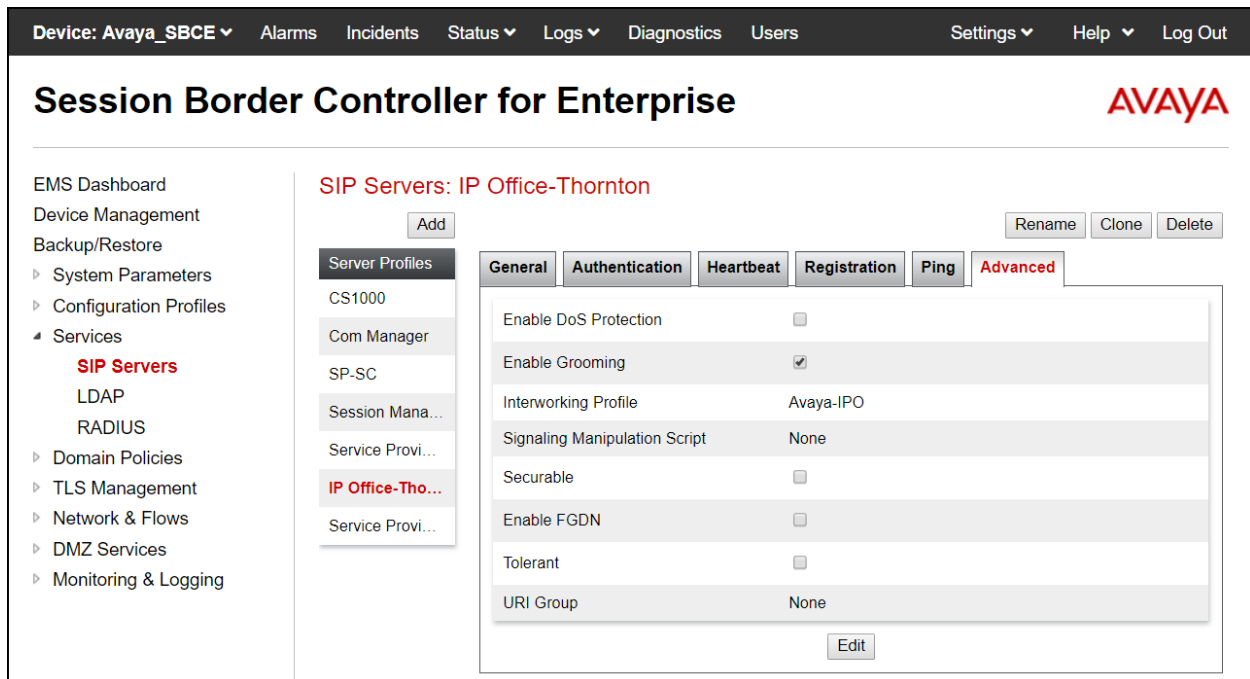
- **Server Type:** Select *Call Server*.
- **IP Address / FQDN:** *10.64.101.127* (IP Address of IP Office).
- **Port:** *5061* (This port must match the port number defined in **Section 5.3.1.1**).
- **Transport:** Select *TLS*.
- Select a **TLS Client Profile**.
- Click **Next**.

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**.

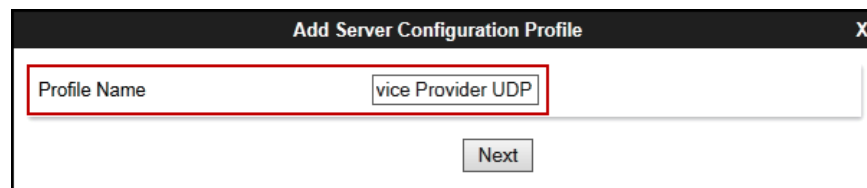
The following screen capture shows the **General** tab of the newly created **IP Office-Thornton** SIP Server Configuration Profile.

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



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

- Click **Next**.



- On the **Edit Server Configuration Profile - General** Tab select **Trunk Server** from the drop-down menu for the **Server Type**.
- Select **SRV** from the drop-down menu for **DNS Query Type**.
- On the **IP Addresses / FQDN** field, enter **svc1234.us-east.test.trunk.io** (service provider's SIP proxy server FQDN used for DNS SRV record queries). This information should be provided by the service provider.
- Select **UDP** for **Transport** (note that the port cannot be enter since SRV was selected for **DNS Query Type**, the port being used will be collected from the DNS response).
- Click **Next** (not shown).

Edit SIP Server Profile - General

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type: Trunk Server

SIP Domain:

DNS Query Type: SRV

TLS Client Profile: None

Add

FQDN	Port	Transport	
<input type="text" value="svc1234.us-east.test.trunk.io"/>	<input type="text"/>	UDP	Delete

Finish

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

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Leave the **Realm** blank.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next** (not shown).

Enable Authentication	<input checked="" type="checkbox"/>
User Name	<input type="text" value="user1234"/>
Realm <small>(Leave blank to detect from server challenge)</small>	<input type="text"/>
Password <small>(Leave blank to keep existing password)</small>	<input type="text"/>
Confirm Password	<input type="text"/>

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

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

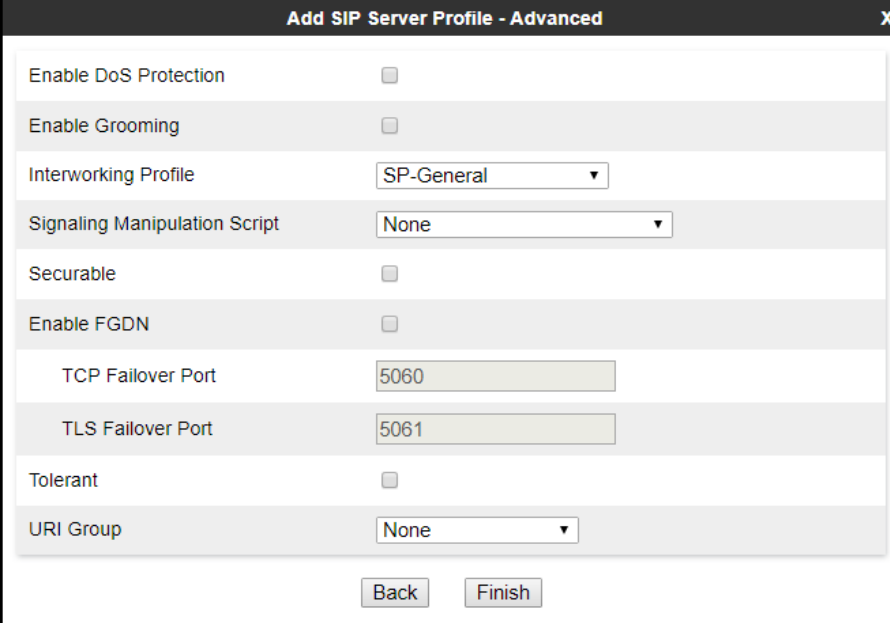
- Check the **Register with All Servers** box (**Register with Priority Server** could also be used).
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the service provider Proxy Servers to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. **30** 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 (**user1234**) and the service provider's SIP Domain (**avaya-test-domain.sip.1234.io**), as shown in the screen below. This information should be provided by the service provider.
 - **To URI**: Use the **User Name** entered above in the **Authentication** screen (**user1234**) and the service provider's SIP Domain (**avaya-test-domain.sip.1234.io**), as shown in the screen below. This information should be provided by the service provider.
 - Click **Next** (not shown).

Edit SIP Server Profile - Registration	
Register with All Servers	<input checked="" type="checkbox"/>
Register with Priority Server	<input type="checkbox"/>
Refresh Interval	<input type="text" value="30"/> seconds
From URI	<input type="text" value="user1234@avaya-test-don"/>
To URI	<input type="text" value="user1234@avaya-test-don"/>
<input type="button" value="Finish"/>	

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

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

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



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

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None ▼

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

The following screen capture shows the **General** tab of the newly created **Service Provider UDP** 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_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 system management options, with 'SIP Servers' highlighted under the 'Services' section. The main content area is titled 'SIP Servers: Service Provider UDP' 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	Trunk Server	
DNS Query Type	SRV	
IP Address / FQDN	Port	Transport
svc1234.us-east.test.trunk.io		UDP

An 'Edit' button is located below the configuration table.

The following screen capture shows the **Authentication** tab of the newly created **Service Provider UDP** 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 system management options, with 'Services' expanded to show 'SIP Servers' selected. The central content area is titled 'SIP Servers: Service Provider UDP' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' options. Below this, a tabbed interface shows 'Authentication' as the active tab, with other tabs for 'General', 'Heartbeat', 'Registration', 'Ping', and 'Advanced'. The 'Authentication' tab contains the following configuration:

Enable Authentication	<input checked="" type="checkbox"/>
User Name	user1234
Realm	---

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

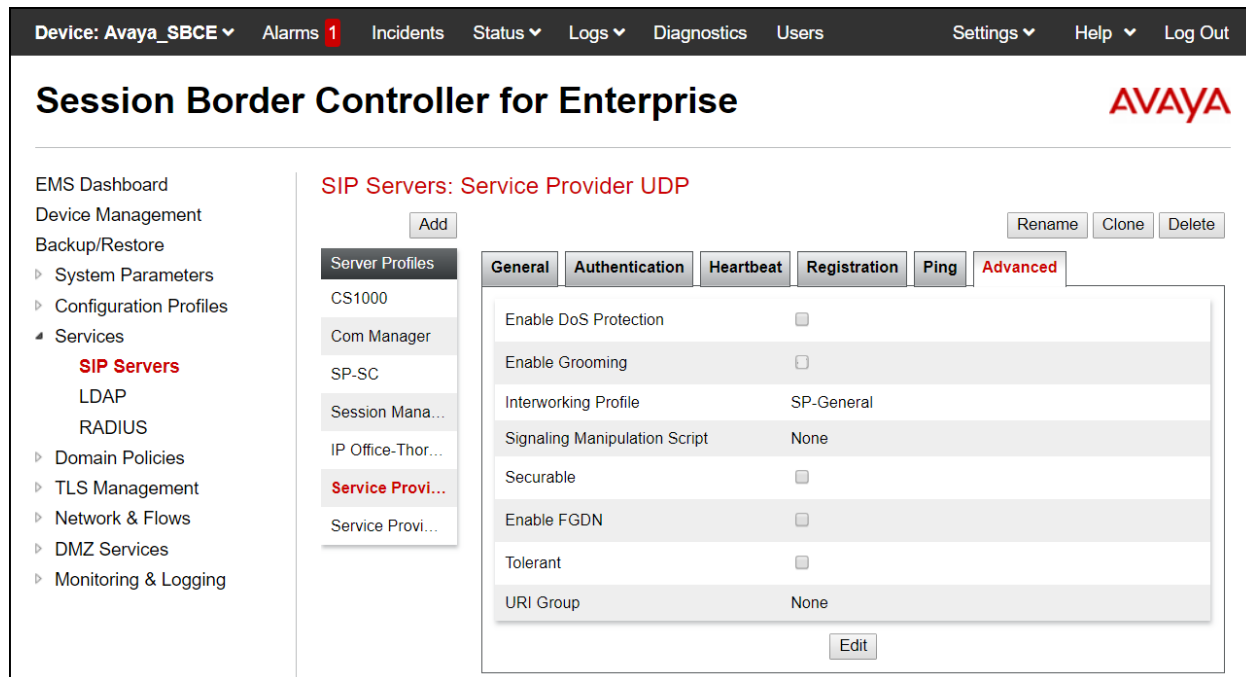
The following screen capture shows the **Registration** tab of the newly created **Service Provider UDP** Server Configuration Profile.

This screenshot shows the same Avaya Session Border Controller for Enterprise interface, but with the 'Registration' tab selected. The navigation and header elements are identical to the previous screenshot. The 'Registration' tab contains the following configuration:

Register with All Servers	<input checked="" type="checkbox"/>
Register with Priority Server	<input type="checkbox"/>
Refresh Interval	30 seconds
From URI	user1234@avaya-test-domain.sip.1234.io
To URI	user1234@avaya-test-domain.sip.1234.io

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

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



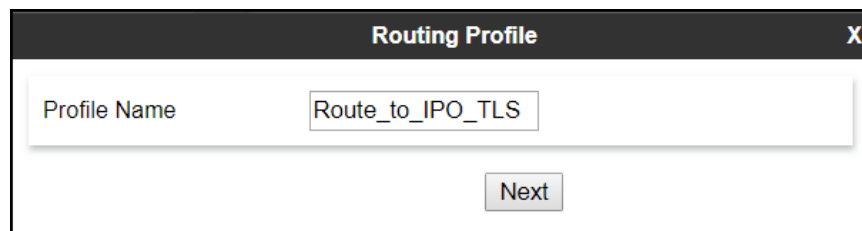
7.5.1. Routing Profiles

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

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

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

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



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

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

Profile : Route_to_IPO_TLS - Edit Rule X

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

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

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

The screenshot shows 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 displays 'Session Border Controller for Enterprise' and the Avaya logo. On the left is a navigation menu with categories like 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', and 'Routing'. The 'Routing Profiles' section is active, showing a list of profiles including 'default', 'Route_to_SM', 'Route_to_CM', 'To SM from R...', 'To IPO from R...', 'Route_to_IP...', 'Route_to_SP...', 'Route_to_CS...', and 'Route_to_SP...'. The 'Route_to_IP...' profile is selected, and its configuration is shown in a modal window. The modal has a title 'Routing Profile' and an 'Add' button. Below the title is a table with columns: Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, Transport, and Edit/Delete. The table contains one row with the following values: Priority: 1, URI Group: *, Time of Day: default, Load Balancing: Priority, Next Hop Address: 10.64.101.127:5061, Transport: TLS, and Edit/Delete buttons.

Similarly, for the outbound route:

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

The screenshot shows a 'Routing Profile' configuration dialog box. The title bar reads 'Routing Profile' with a close button 'X'. The main area contains a 'Profile Name' label and a text input field containing the text 'Route_to_SP_UDP'. Below the input field is a 'Next' button.

On the Routing Profile screen complete the following:

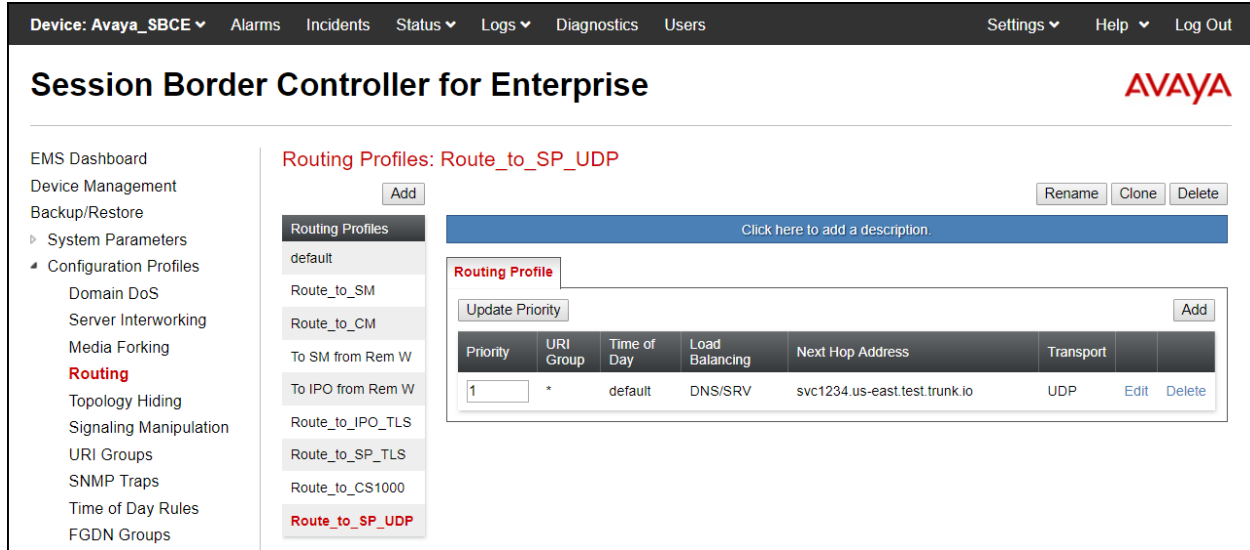
- **Load Balancing:** Select **DNS/SRV**.
- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight:** **1**
- **SIP Server Profile:** Select **Service Provider UDP**.
- The **Next Hop Address** is populated automatically with **svc1234.us-east.test.trunk.io (UDP)** (Avaya's SIP Proxy FQDN and transport).
- Click **Finish**.

Profile : Route_to_SP_UDP - Edit Rule X

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	<input style="width: 100px;" type="text"/>

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Service Pr ▾	svc1234.us-east.te: ▾	None ▾	Delete

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



7.5.2. Topology Hiding

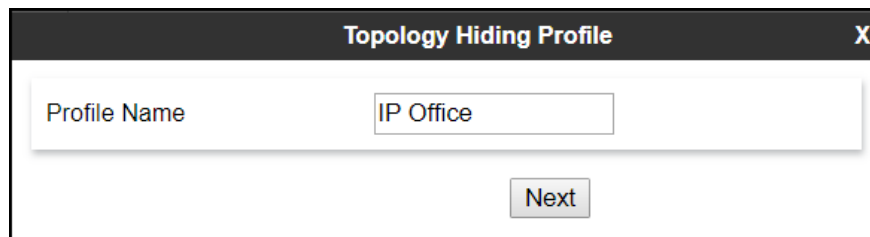
Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

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.

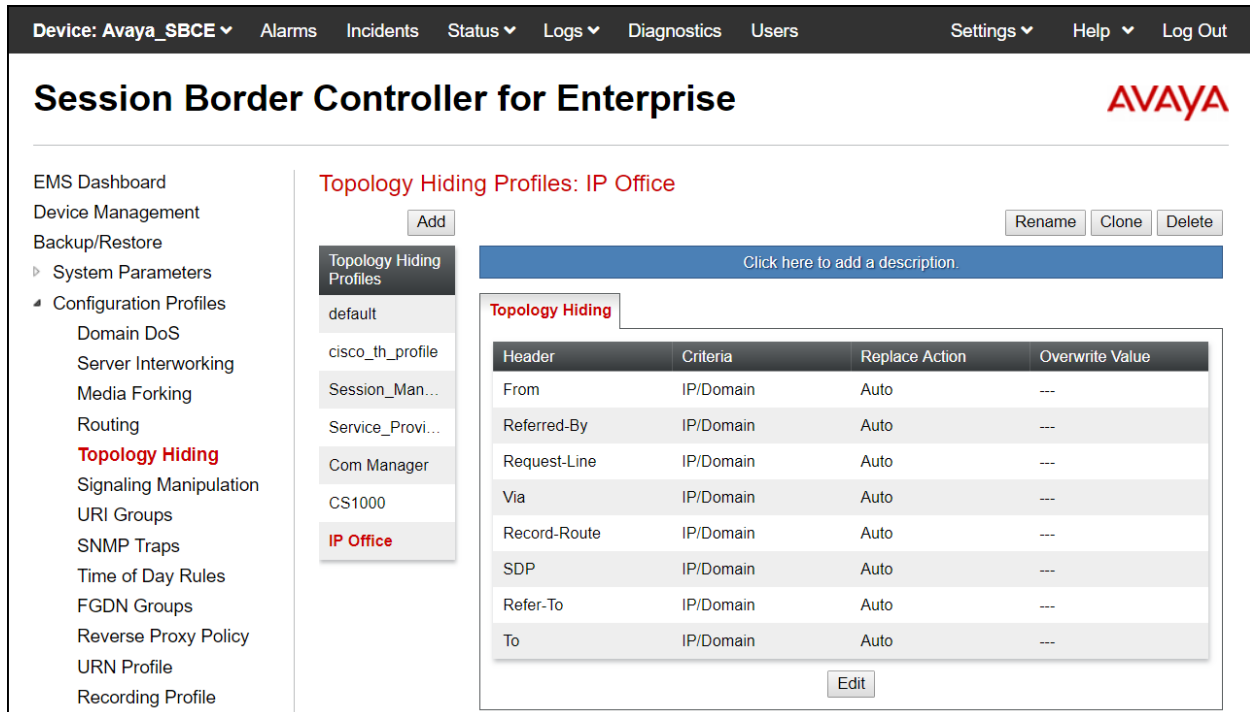
For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

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**.

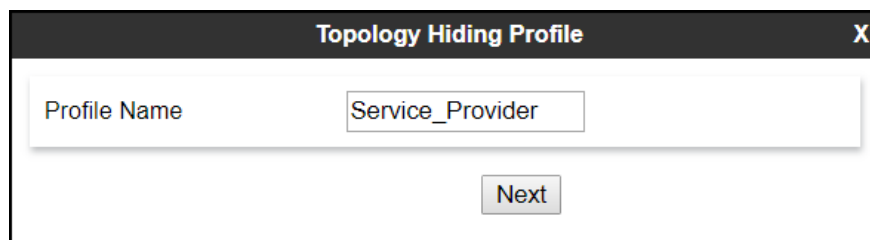


The following screen capture shows the newly added **IP Office** Topology Hiding Profile. Note that for IP Office no values were overwritten (left with default values).



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 (**avaya-test-domain.sip.1234.io**) under **Overwrite Value**
- On the **To** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (**avaya-test-domain.sip.1234.io**) 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 (**avaya-test-domain.sip.1234.io**) under **Overwrite Value**.
- Click **Finish**.

Edit Topology Hiding Profile
X

Header	Criteria	Replace Action	Overwrite Value	
From ▼	IP/Domain ▼	Overwrite ▼	avaya-test-domain.sip	Delete
Referred-By ▼	IP/Domain ▼	Auto ▼		Delete
Via ▼	IP/Domain ▼	Auto ▼		Delete
Request-Line ▼	IP/Domain ▼	Overwrite ▼	avaya-test-domain.sip	Delete
Record-Route ▼	IP/Domain ▼	Auto ▼		Delete
SDP ▼	IP/Domain ▼	Auto ▼		Delete
Refer-To ▼	IP/Domain ▼	Auto ▼		Delete
To ▼	IP/Domain ▼	Overwrite ▼	avaya-test-domain.sip	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', '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', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Routing', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', 'URN Profile', 'Recording Profile', 'Services', and 'Domain Policies'. 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 existing profiles: 'default', 'cisco_th_profile', 'Session_Man...', 'Service_Prov...', 'Com Manager', 'CS1000', and 'IP Office'. The 'Service_Prov...' profile is selected and highlighted in red.

Below the profile list, there is a blue bar with the text 'Click here to add a description.' and buttons for 'Rename', 'Clone', and 'Delete'. The main configuration area is titled 'Topology Hiding' and contains a table with the following data:

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	avaya-test-domain.sip.1234.io
Referred-By	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	avaya-test-domain.sip.1234.io
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Overwrite	avaya-test-domain.sip.1234.io

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

7.6. Domain Policies

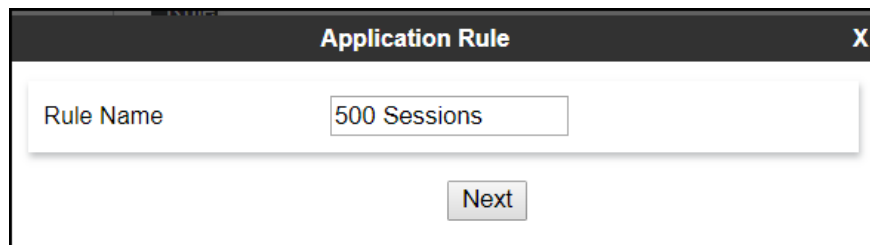
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.6.1. 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 label "Rule Name" followed by a text input field containing the text "500 Sessions". Below the input field, there 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"/>	<input type="text" value="500"/>	<input type="text" value="500"/>
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="100"/>	<input type="text" value="100"/>

Miscellaneous

CDR Support Off
 RADIUS
 CDR Adjunct

RADIUS Profile

Media Statistics Support

Call Duration Setup
 Connect

RTCP Keep-Alive

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

The screenshot shows 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 displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. On the left, a navigation menu lists various management options, with 'Application Rules' highlighted under 'Domain Policies'. The main content area is titled 'Application Rules: 500 Sessions' and features an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. A blue bar prompts the user to 'Click here to add a description.' Below this, a table lists application rules:

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

Below the table, a 'Miscellaneous' section contains 'CDR Support' (Off) and 'RTCP Keep-Alive' (No). An 'Edit' button is located at the bottom right of the configuration area.

7.6.2. 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_S RTP*.
- Click Next.

The screenshot shows a 'Media Rule' configuration dialog box. It has a title bar with 'Media Rule' and a close button 'X'. The main area contains a 'Rule Name' label and a text input field containing 'IPO_S RTP'. Below the input field is a 'Next' button.

- 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**.

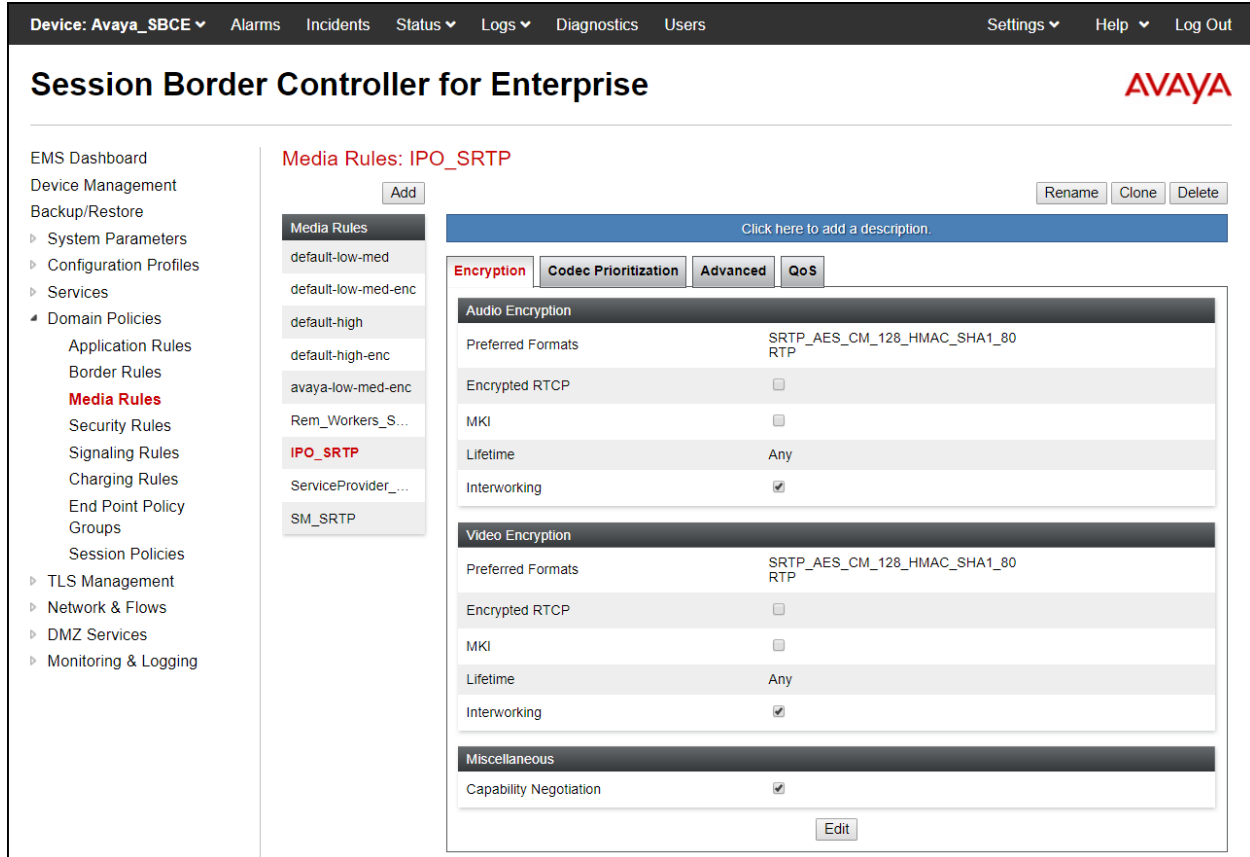
The screenshot shows a 'Media Rule' configuration window with three main sections: Audio Encryption, Video Encryption, and Miscellaneous. Each section contains several configuration options with default values.

Section	Option	Value
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 <small>Leave blank to match any value.</small>	2^ []
	Interworking	<input checked="" 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 <small>Leave blank to match any value.</small>	2^ []
	Interworking	<input checked="" type="checkbox"/>
Miscellaneous	Capability Negotiation	<input checked="" type="checkbox"/>

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

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

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

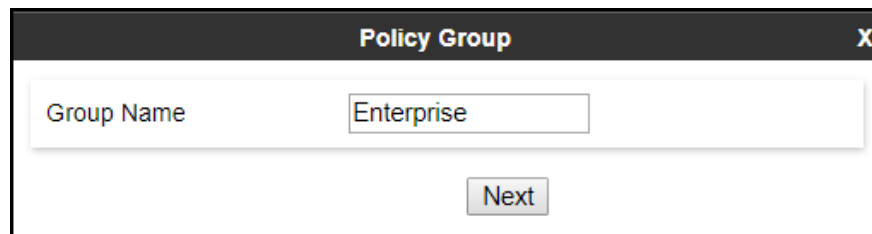


7.6.3. End Point Policy Groups

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

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

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



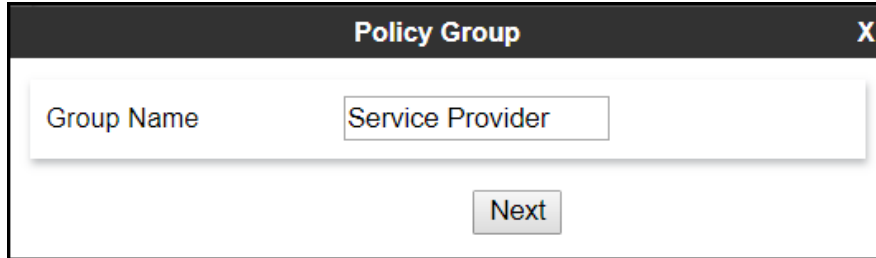
- **Application Rule:** *500 Sessions*.
- **Border Rule:** *default*.
- **Media Rule:** *IPO_SRTP* (Section 7.6.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default*.
- Click **Finish**.

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

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

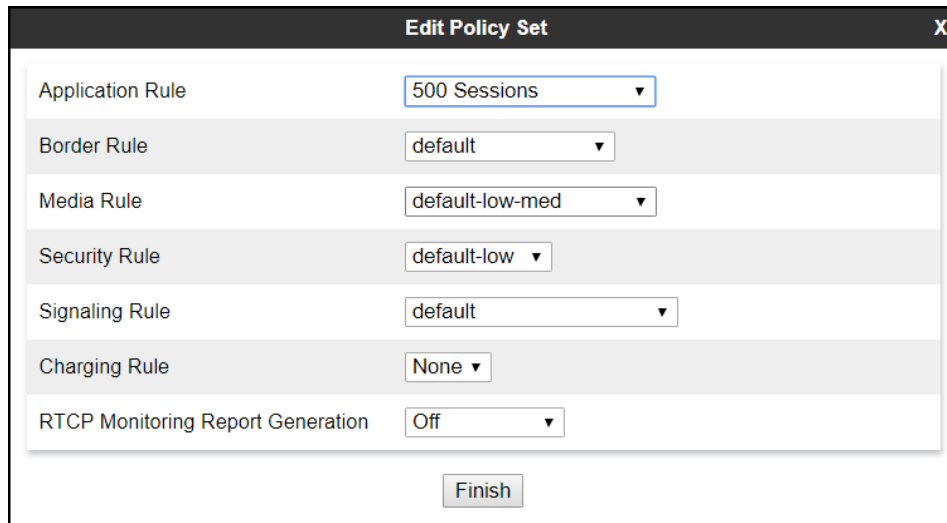
Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk.

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



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

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



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

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

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

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

The screenshot displays the Avaya Session Border Controller 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', '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 main content area is titled 'Policy Groups: Service Provider'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below these are two blue boxes with the text 'Click here to add a description.' and 'Click here to add a row description.' respectively.

A 'Policy Group' summary table is displayed, showing the configuration for the 'Service Provider' group. The table has columns for Order, Application, Border, Media, Security, Signaling, Charging, and RTCP Mon Gen. The first row shows an order of 1, 500 Sessions, default border, default-low-med media, default-low security, default signaling, None charging, and Off RTCP Mon Gen. An 'Edit' button is visible next to the row.

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

7.7. 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.

7.7.1. 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 interface includes a top navigation bar with options: Device: Avaya_SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is titled 'Session Border Controller for Enterprise' and features the AVAYA logo. A left-hand navigation menu lists various management options, with 'Network Management' highlighted under the 'Network & Flows' section. The 'Network Management' section contains two tabs: 'Interfaces' and 'Networks'. The 'Networks' tab is active, showing a table of network configurations. The table has columns for Name, Gateway, Subnet Mask / Prefix Length, Interface, and IP Address. Two networks are listed: Network_A1 and Network_B1. The IP address for Network_A1 is 10.64.101.243, and for Network_B1 it is 10.10.80.51. Each row includes 'Edit' and 'Delete' buttons. An 'Add' button is located in the top right corner of the table area.

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 web interface. At the top, there is a navigation bar with the following items: 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. On the left, there is a sidebar menu with the following items: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, Network Management (highlighted in red), Media Interface, and Signaling Interface. The main content area is titled "Network Management" and has two tabs: "Interfaces" (selected) and "Networks". Below the tabs is a table with the following data:

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

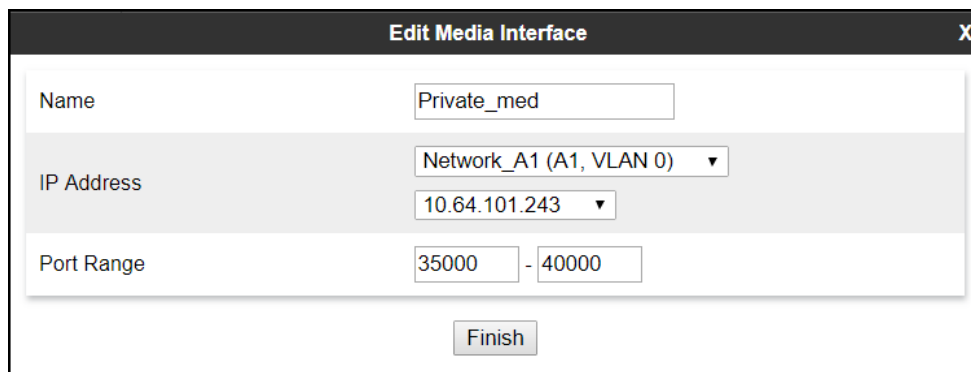
An "Add VLAN" button is located in the top right corner of the table area.

7.7.2. 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**.



Edit Media Interface		X
Name	<input type="text" value="Private_med"/>	
IP Address	<input type="text" value="Network_A1 (A1, VLAN 0)"/>	
	<input type="text" value="10.64.101.243"/>	
Port Range	<input type="text" value="35000"/>	<input type="text" value="40000"/>
<input type="button" value="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 X

Name: Public_med

IP Address: Network_B1 (B1, VLAN 0) | 10.10.80.51

Port Range: 35000 - 40000

Finish

The following screen capture shows the newly created Media Interfaces.

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

Session Border Controller for Enterprise

AVAYA

Media Interface

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

Add

7.7.3. Signaling Interface

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

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

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

Finish

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

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

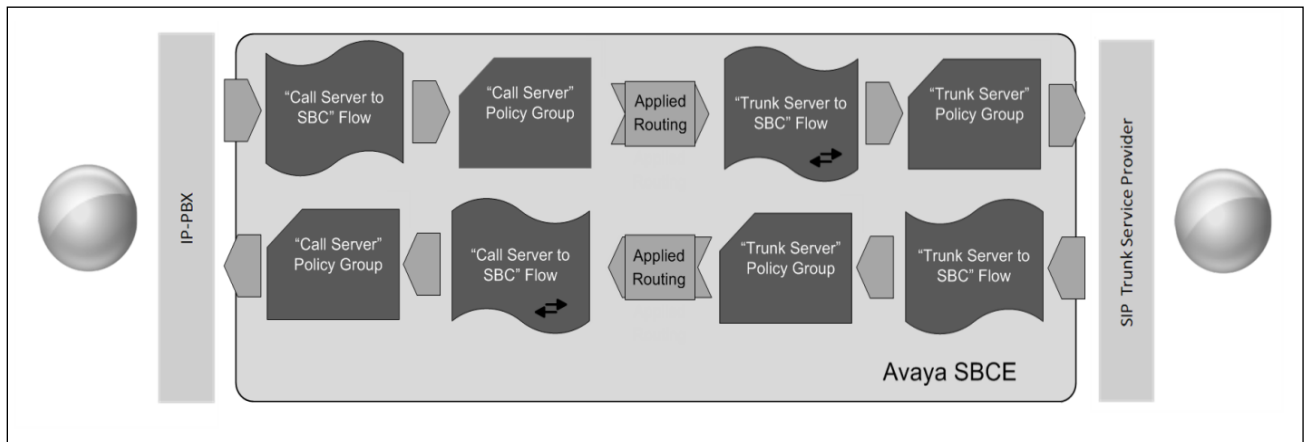
Finish

The following screen capture shows the newly created Signaling Interfaces.

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

7.7.4. End Point Flows

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



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

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

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

Field	Value
Flow Name	SIP_Trunk_Flow_UDP
SIP Server Profile	Service Provider UDP
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
Secondary Media Interface	None
End Point Policy Group	Service Provider
Routing Profile	Route_to_IPO_TLS
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

Finish

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

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

Field	Value
Flow Name	IP_Office_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_UDP
Topology Hiding Profile	IP Office
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

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_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', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'Network Management', 'Media Interface', 'Signaling Interface', 'End Point Flows', 'Session Flows', 'Advanced Options', 'DMZ Services', and 'Monitoring & Logging'. The 'End Point Flows' option is highlighted in red.

The main content area is titled 'End Point Flows' and has two tabs: 'Subscriber Flows' and 'Server Flows'. The 'Server Flows' tab is active. An 'Add' button is located in the top right corner of the main content area.

A warning message states: 'Modifications made to a Server Flow will only take effect on new sessions.' Below this is a blue button that says 'Click here to add a row description.'

There are two sections for SIP Servers:

- SIP Server: IP Office-Thornton**: Contains an 'Update' button and a table with the following data:

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	IP_Office_Flow	*	Public_sig	Private_sig	Enterprise	Route_to_SP_UDP	View	Clone	Edit	Delete
- SIP Server: Service Provider UDP**: Contains a table with the following data:

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

8. Avaya SIP Trunking Service Configuration

To use Avaya SIP Trunking Service, a customer must request the service from Avaya using the established sales processes. The process can be started by contacting Avaya via the corporate web site at: <https://www.avaya.com/en/documents/fs-sip-uc8179en.pdf> and requesting information.

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

Avaya will provide the following information:

- SIP Proxy FQDN to be used for public DNS SRV record queries.
- SIP domain name to be used.
- SIP Trunk registration credentials (User Name, Password, etc.).
- DID numbers.
- Public DNS IP addresses.
- 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. The window title is "IP Office System Status". The AVAYA logo is in the top left. A menu bar contains "Help", "Exit", and "About". The main area has a "Logon" dialog box with the following fields and options:

- Control Unit Address: 10.64.101.127
- Proxy Server Address: <None>
- Services Base TCP Port: 50804
- Local IP Address: Automatic
- User Name: Administrator
- Password: [empty]
- Auto reconnect
- Secure connection
- Websocket connection
- Logon button

The status bar at the bottom reads "IP Office System Status Version 11.1.0.1.0 build 95".

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

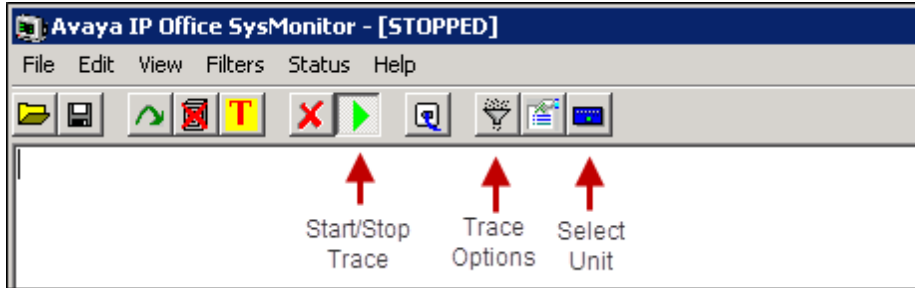
The screenshot displays the Avaya IP Office System Status interface. The left sidebar shows a navigation menu with 'Trunks (3)' expanded to show 'Line: 1', 'Line: 2', and 'Line: 17' (selected). The main content area is titled 'IP Office System Status' and has tabs for 'Status', 'Utilization Summary', and 'Alarms'. The 'Status' tab is active, showing a 'SIP Trunk Summary' with the following details:

- 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: 10
- Number of Channels in Use: 0
- Administered Compression: G711 Mu, G711 A, G729 A
- 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%)
- SIP Device Features: UPDATE (Incoming and Outgoing)

Below the summary is a table with columns: Cha... U.. Call Curr... Time in Remote C... Con... Caller Other Dire... Round Rec... Rec... Tran... Tran... The table lists 10 channels, all with a 'Curr...' state of 'Idle' and 'Time in Remote' of '10 d...'. At the bottom of the interface, there are buttons for 'Trace', 'Trace All', 'Pause', 'Ping', 'Call Details', 'Graceful Shutdown', 'Force Out of Service', 'Print...', and 'Save As...'. The status bar at the bottom right shows '11:51:08 AM' and '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.

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

Session Border Controller for Enterprise

EMS Dashboard

- Device Management
- Backup/Restore
 - System Parameters
 - Configuration Profiles
 - Services
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
 - Monitoring & Logging

Dashboard

Information	
System Time	01:32:22 PM EDT Refresh
Version	8.1.1.0-26-19214
GUI Version	8.1.1.0-19189
Build Date	Wed Jul 22 23:36:51 UTC 2020
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	09/18/2020 13:22:54 EDT
Failed Login Attempts	0

Installed Devices

- EMS
- Avaya_SBCE

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya_SBCE: No Subscriber Flow Matched

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

Device: Avaya_SBCE ▾ Help

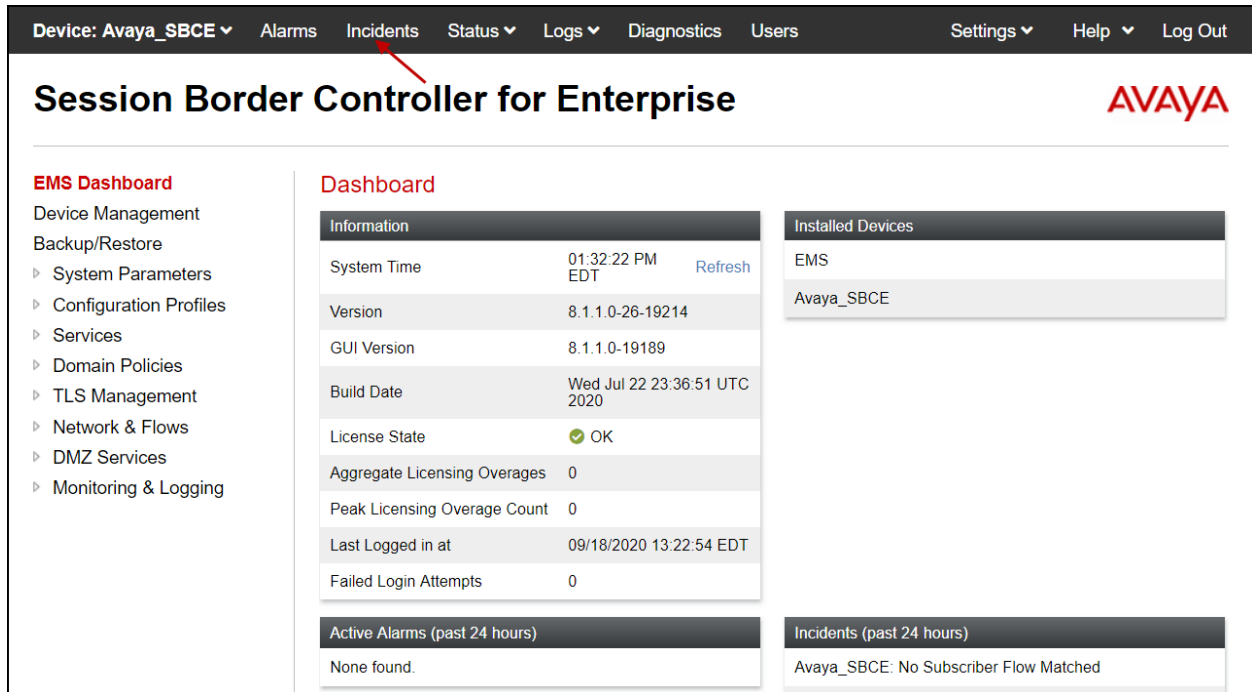
Alarm Viewer

Alarms

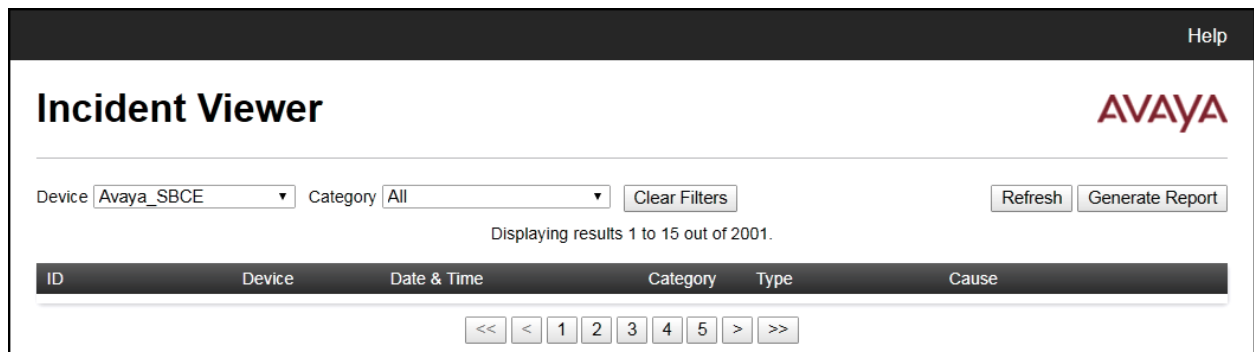
<input checked="" type="checkbox"/>	ID	Details	State	Time	Device
No alarms found for this device.					

[Clear Selected](#) [Clear All](#)

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



The following screen shows the Incident Viewer page.



Status : Provides the status for each server resolved during DNS SRV queries handling calls to/from the PSTN. Note that Server FQDN and Server IP/Port were blurred out for security reasons.

Session Border Controller for Enterprise

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

EMS Dashboard

- Device Management
- Backup/Restore
 - System Parameters
 - Configuration Profiles
 - Services
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
 - Monitoring & Logging

Dashboard

Information

System Time	01:32:22 PM EDT	Refresh
Version	8.1.1.0-26-19214	
GUI Version	8.1.1.0-19189	
Build Date	Wed Jul 22 23:36:51 UTC 2020	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	09/18/2020 13:22:54 EDT	
Failed Login Attempts	0	

Installed Devices

- EMS
- Avaya_SBCE

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya_SBCE: No Subscriber Flow Matched

Status

Device: Avaya_SBCE | Help

Server Status

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Service Provider UDP	[Blurred]	[Blurred]	5090	UDP	UNKNOWN	REGISTERED	09/21/2020 12:02:48 EDT
Service Provider UDP	[Blurred]	[Blurred]	5090	UDP	UNKNOWN	REGISTERED	09/21/2020 12:02:50 EDT

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

The screenshot shows the Avaya SBCE dashboard. At the top, there is a navigation bar with tabs for "Device: Avaya_SBCE", "Alarms", "Incidents", "Status", "Logs", "Diagnostics" (highlighted with a red arrow), "Users", "Settings", "Help", and "Log Out". Below the navigation bar is the main header "Session Border Controller for Enterprise" and the Avaya logo.

The dashboard is divided into several sections:

- EMS Dashboard:** A sidebar menu with options like "Device Management", "Backup/Restore", "System Parameters", "Configuration Profiles", "Services", "Domain Policies", "TLS Management", "Network & Flows", "DMZ Services", and "Monitoring & Logging".
- Dashboard:** A central area with several panels:
 - Information:** A table showing system details:

System Time	01:32:22 PM EDT	Refresh
Version	8.1.1.0-26-19214	
GUI Version	8.1.1.0-19189	
Build Date	Wed Jul 22 23:36:51 UTC 2020	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	09/18/2020 13:22:54 EDT	
Failed Login Attempts	0	
 - Installed Devices:** A list showing "EMS" and "Avaya_SBCE".
 - Active Alarms (past 24 hours):** A panel stating "None found.".
 - Incidents (past 24 hours):** A panel stating "Avaya_SBCE: No Subscriber Flow Matched".

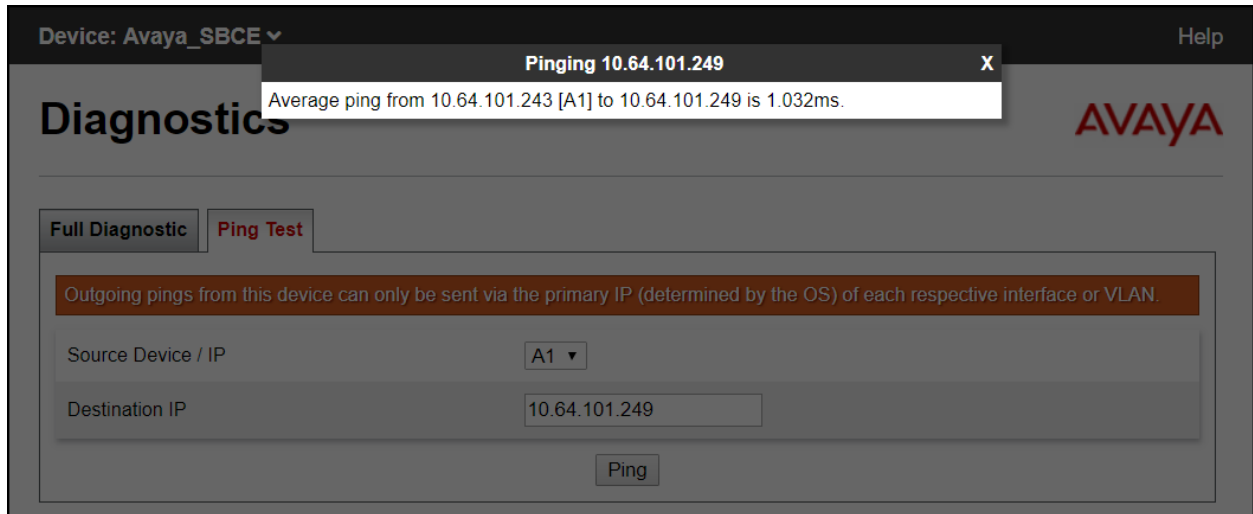
The screenshot shows the "Diagnostics" page in the Avaya SBCE interface. At the top, there is a navigation bar with "Device: Avaya_SBCE" and "Help". The main header is "Diagnostics" and the Avaya logo is on the right.

Below the header, there are two tabs: "Full Diagnostic" (selected) and "Ping Test". A warning message states: "Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN." A "Start Diagnostic" button is located to the right of this message.

The main content is a table with the following columns: "Task Description" and "Status".

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: SBC (A1) to Gateway (10.64.101.1)	Average ping from 10.64.101.243 [A1] to 10.64.101.1 is 0.296ms.
✓ Ping: SBC (A1) to Primary DNS (75.75.75.75)	Average ping from 10.64.101.243 [A1] to 75.75.75.75 is 1.762ms.
✓ Ping: SBC (A1) to Secondary DNS (75.75.76.76)	Average ping from 10.64.101.243 [A1] to 75.75.76.76 is 3.282ms.
✓ Ping: SBC (B1) to Gateway (10.64.101.1)	Average ping from 10.64.101.243 [B1] to 10.64.101.1 is 0.276ms.
✓ Ping: SBC (B1) to Primary DNS (75.75.75.75)	Average ping from 10.64.101.243 [B1] to 75.75.75.75 is 1.718ms.
✓ Ping: SBC (B1) to Secondary DNS (75.75.76.76)	Average ping from 10.64.101.243 [B1] to 75.75.76.76 is 3.162ms.

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



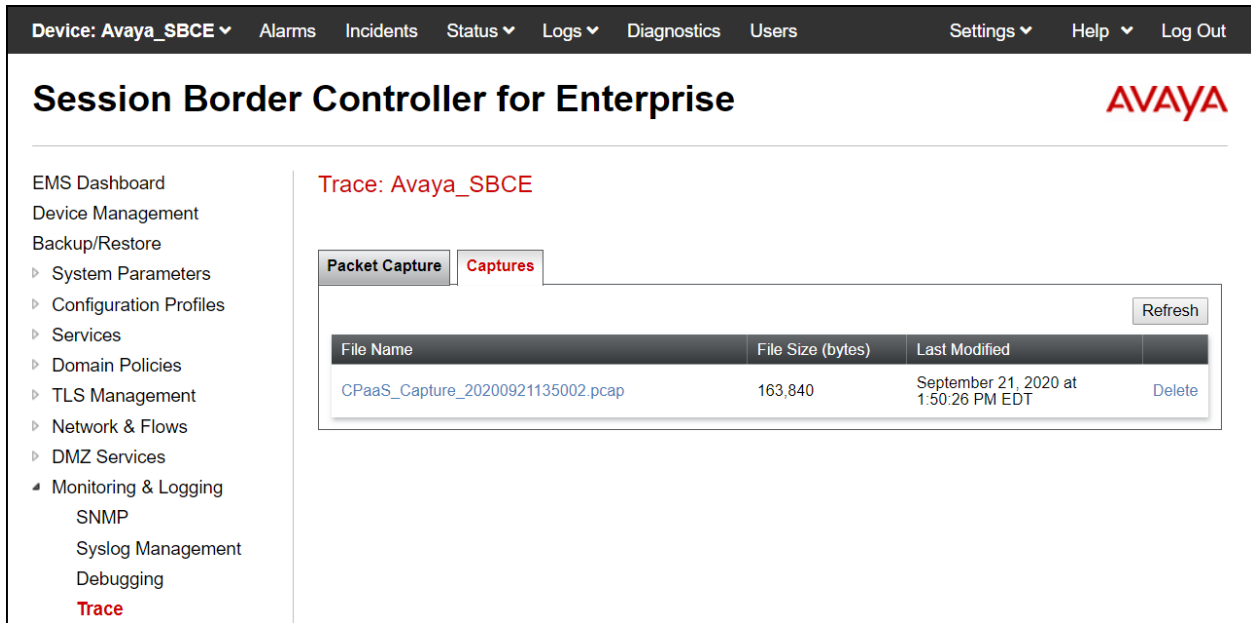
Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as pcap files. Navigate to **Monitor & Logging** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start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

The screenshot shows the Avaya SBCE web interface. At the top, there is a navigation bar with the following items: 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 contains a "Packet Capture" configuration form. The form has two tabs: "Packet Capture" (active) and "Captures". The configuration fields are as follows:

Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address IP[Port]	All : []
Remote Address *, *.Port, IP, IP:Port	[*]
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	CPaaS_Capture.pcap

At the bottom of the form are two buttons: "Start Capture" and "Clear".

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', '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 sidebar lists various management options, with 'Trace' highlighted in red. The main content area is titled 'Trace: Avaya_SBCE' and features two tabs: 'Packet Capture' and 'Captures'. The 'Captures' tab is active, showing a table with the following data:

File Name	File Size (bytes)	Last Modified	
CPaaS_Capture_20200921135002.pcap	163,840	September 21, 2020 at 1:50:26 PM EDT	Delete

A 'Refresh' button is located in the top right corner of the table area.

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 8.1 to interoperate with the Avaya SIP Trunking service, as shown in **Figure 1**.

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, Issue 14, April 2020*
- [2] *IP Office Platform 11.1, Deploying Avaya IP Office Servers as Virtual Machines, August 2020*
- [3] *Avaya IP Office Platform Server Edition Reference Configuration Release 11.1, Issue 2, May 2020*
- [4] *IP Office Platform 11.1, Deploying an IP500 V2 IP Office Basic Edition System, Issue 36g, September 10, 2020*
- [5] *IP Office Platform 11.1, Deploying an IP500 V2 IP Office Essential Edition System, Issue 36g, September 10, 2020*
- [6] *Administering Avaya IP Office Platform with Manager, Release 11.1 SP1, July 2020.*
- [7] *Administering Avaya IP Office Platform with Web Manager, Release 11.1 SP1, Issue 22, July 2020.*
- [8] *Avaya IP Office Platform Feature Description, Release 11.1, Issue 2, May 2020.*
- [9] *Deploying Avaya Session Border Controller on a Virtualized Environment Platform, Release 8.1, Issue 3, August 2020.*
- [10] *Administering Avaya Session Border Controller for Enterprise, Release 8.1.x, Issue 3, August 2020.*
- [11] *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac and Windows, August 2020*
- [12] *Using Avaya Avaya IX™ Workplace Client for Android, iOS, Mac and Windows, August 2020*

Additional Avaya IP Office documentation can be found at:
<https://ipofficekb.avaya.com/>

©2020 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 Solution & Interoperability Test Lab at interopnotesdl@avaya.com