



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 8.0.1 to support Clearcom SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 11.0 and Avaya Session Border Controller for Enterprise Release 8.0.1 to support Clearcom SIP Trunking Service. These Application Notes update previously published Application Notes with newer versions of Avaya software.

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

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	6
2.3.	Support	8
3.	Reference Configuration.....	8
4.	Equipment and Software Validated	11
5.	Avaya IP Office Primary Server Configuration.....	12
5.1.	Licensing	14
5.2.	System Settings	16
5.2.1.	System - LAN1 Tab.....	16
5.2.2.	System - Telephony Tab	19
5.2.3.	System - VoIP Tab.....	20
5.3.	IP Route.....	22
5.4.	SIP Line.....	23
5.4.1.	Creating a SIP Trunk from an XML Template.....	23
5.4.2.	SIP Line – SIP Line Tab	27
5.4.3.	SIP Line - Transport Tab	28
5.4.4.	SIP Line – Call Details Tab	29
5.4.5.	SIP Line - VoIP Tab	31
5.4.6.	SIP Line – SIP Advanced Tab	32
5.5.	Users.....	33
5.6.	IP Office Line – Primary Server	34
5.7.	Incoming Call Route	36
5.8.	Outbound Call Routing	38
5.8.1.	Short Codes and Automatic Route Selection.....	38
5.9.	Save IP Office Primary Server Configuration.....	40
6.	Avaya IP Office Expansion System Configuration	41
6.1.	Physical Hardware.....	42
6.2.	LAN Settings.....	43
6.3.	IP Route.....	44
6.4.	IP Office Line – IP500 V2 Expansion System.....	45
6.5.	Short Codes	47
6.6.	Automatic Route Selection – ARS.....	48
6.7.	Save IP Office 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
7.4.	Configuration Profiles	54
7.4.1.	Server Interworking – Avaya-IPO.....	54
7.4.2.	Server Interworking - SP-General	57

7.4.3.	Signaling Manipulation.....	60
7.4.4.	SIP Server Configuration.....	62
7.4.5.	Routing Profiles	70
7.4.6.	Topology Hiding.....	74
7.5.	Domain Policies	77
7.5.1.	Application Rules.....	77
7.5.2.	Media Rules	79
7.5.3.	End Point Policy Groups.....	81
7.6.	Network & Flows Settings	85
7.6.1.	Network Management.....	85
7.6.2.	Media Interface	86
7.6.3.	Signaling Interface	88
7.6.4.	End Point Flows.....	90
8.	Clearcom SIP Trunking Service Configuration.....	94
9.	Verification Steps.....	95
9.1.	IP Office System Status.....	95
9.2.	Monitor.....	97
9.3.	Avaya Session Border Controller for Enterprise.....	98
10.	Conclusion	103
11.	Additional References.....	103

1. Introduction

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

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of an Avaya IP Office Server Edition, two Avaya IP Office 500 V2 as expansion systems, running software release 11.0 (hereafter referred to as IP Office), an Avaya Session Border Controller for Enterprise Release 8.0.1 (hereafter referred to as Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

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

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to Clearcom network via the public Internet, as depicted in **Figure 1**, and exercise the features and functionalities listed in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

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

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

2.1. Interoperability Compliance Testing

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

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, Digital and Analog telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider's network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323, Digital and Analog telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider's network.
- Incoming and outgoing PSTN calls to/from Avaya Equinox for Windows soft-client.
- Dialing plans including local calls, international calls, outbound toll-free, etc.
- Caller ID presentation.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two-way speech-path. Testing was performed with codecs: G.729(a), G.711A and G.711MU, Clearcom preferred codec order.
- Proper response to no matching codecs.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.

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

Items not supported or not tested included the following:

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

2.2. Test Results

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

- **Call transfer to the PSTN using the SIP REFER method** – Calls from the PSTN to the enterprise that were transferred back to the PSTN network using the SIP REFER method did not work properly. Calls that were blind transferred dropped. On attended transfers, the REFER message was accepted by Clearcom with a 202 message, but the trunk resources were not released. Due to these reasons, REFER was left disabled in the Avaya IP Office for the tests (refer to **Sections 5.4.2**). With REFER disabled, blind and attended call transfers to the PSTN were allowed to complete, with the caveat that the IP Office was not released from the call path, and two trunks circuits remained seized for the duration of the call.
- **Outbound Calling Party Number (CPN) Block** – Clearcom did not allow outbound calls with privacy enabled. When the IP Office user activated “Withhold Number” to enable user privacy on outbound calls, IP Office sent “anonymous” in the “From” header, while the caller information was still being sent in the “P-Asserted-Identity” header. Clearcom responded with a “403 PSTN calls are forbidden” message and the call was rejected.
- **Outbound Calling Party Number block (calls with privacy enabled)** – IP Office is not including the privacy header (privacy = id) in the INVITE message sent to Clearcom on calls with privacy enabled in the IP Office stations. A Signaling Manipulation script (SigMa) was created in the Avaya SBCE to add “Privacy = id” to the INVITE messages on calls with privacy enabled in the IP Office stations (**Sections 7.4.3**). This issue is under investigation by Avaya.
- **Outbound call from an enterprise extension to a busy PSTN number** – Clearcom did not send a “486 Busy Here” message on an outbound call to a PSTN number that was busy, as it was expected on this condition. There was no direct impact to the user, who heard busy tone.
- **Caller ID on outbound calls** – On calls originating from IP Office extensions to PSTN telephones, the caller ID number displayed on the PSTN endpoint was always of the main (pilot) DID number assigned by Clearcom to the SIP trunk, not of the specific DID number assigned to the IP Office extension originating the call. This includes calls to “twinned” mobile phones, and calls that were forwarded or transferred back on the SIP trunk to the PSTN. This may be a requirement of the Clearcom service for all outbound calls, it is listed here simply as an observation.
- **Fax support** – Fax calls using the T.38 protocol failed during the compliance test. G.711 pass-through fax was also tested, but it behaved unreliably. The issue related to G.711 pass-through fax failing during the compliance test may be related to the unpredictability of G.711 pass-through techniques, which only works well on networks with very few

hops and with limited end-to-end delay. The issue related to T.38 fax calls failing is related to the PSTN carriers being used in Mexico, not all PSTN carriers in Mexico support T.38. This issue could be solved by Clearcom selecting and routing T.38 fax traffic via PSTN carriers that support T.38.

- **SIP OPTION Messages** – During the compliance test Clearcom did not send SIP OPTION messages to IP Office, IP Office did send SIP OPTION messages to Clearcom, this was sufficient to keep the SIP trunk up in-service.

2.3. Support

For support on Clearcom systems visit the corporate Web page at:

<http://www.Clearcom.com.mx/>

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

3. Reference Configuration

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

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

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

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 Equinox™ for Windows Softphones, Avaya Digital and Analog Deskphones. IP endpoints were registered to the Primary Server; non IP endpoints (analog and digital) were registered to the Expansion Systems. The site also has a Windows PC running Avaya IP Office Manager to configure and administer the system. Mobile Twinning is configured for some of the IP Office users so that calls to these user's extensions will also ring and can be answered at the configured mobile phones.

The transport protocol between the Avaya SBCE and Clearcom, across the public Internet, is SIP over 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 Clearcom network to the Avaya SBCE, then to IP Office.

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

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

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

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

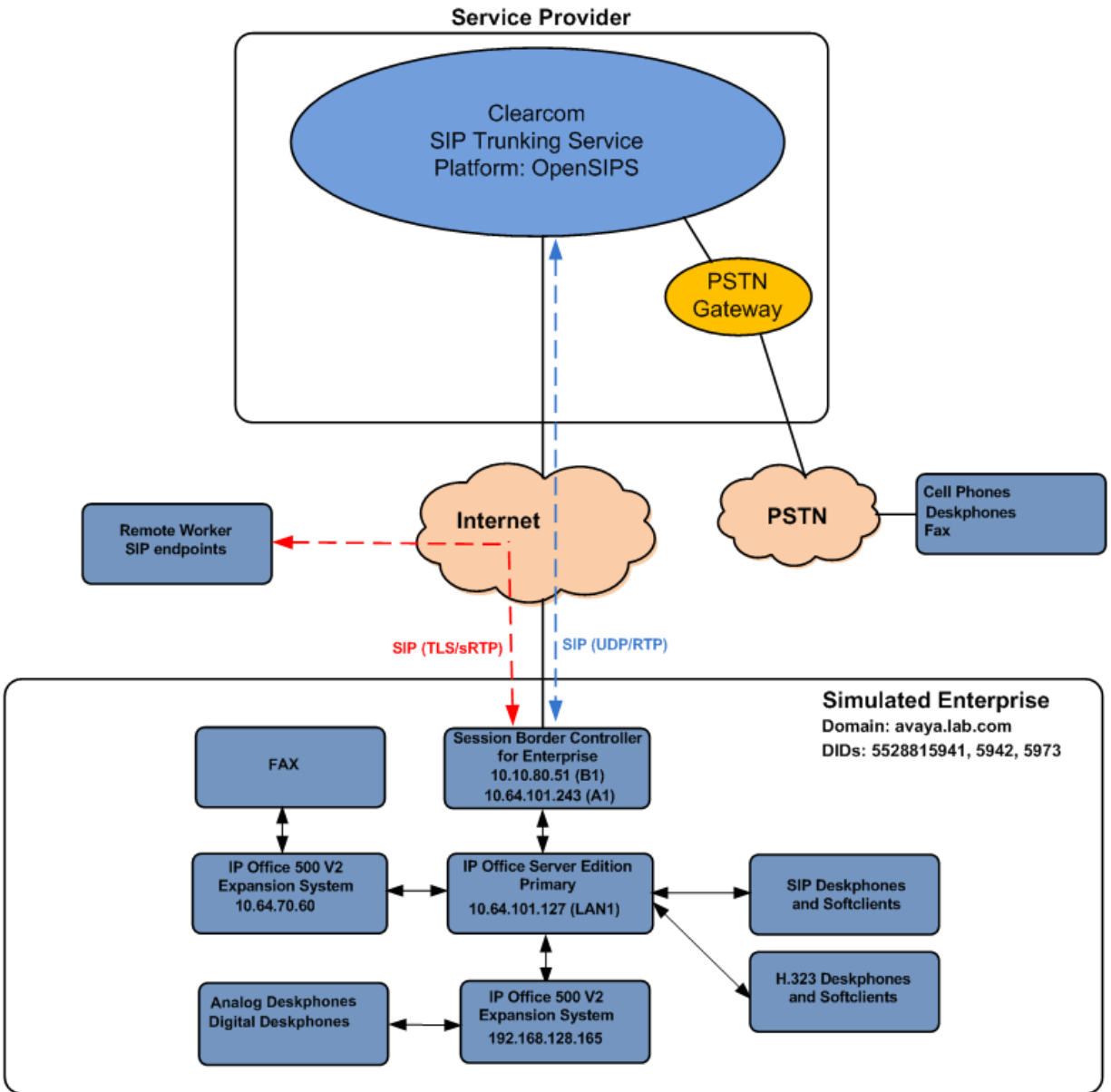


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server)	11.0.4.1.0 Build 11
• Avaya IP Office Voicemail Pro	11.0.4.1.0 Build 2
Avaya IP Office IP500 V2 (Expansion Systems)	11.0.4.1.0 Build 11
Avaya IP Office Manager	11.0.4.1.0 Build 11
Avaya Session Border Controller for Enterprise	ASBCE 8.0 8.0.1.0-10-17555
Avaya 96x1 Series IP Deskphones (H.323)	6.8002
Avaya J179 IP Telephone (H.323)	6.8002
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.0.3.0.10
Avaya 1408 Digital Telephone	48.02
Avaya Equinox™ for Windows (SIP)	3.6.4.31.2
Analog Telephone	---
Clearcom	
OpenSIPS Softswitch	1.9
OpenSIPS Session Border Controller	1.9

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.

Select IP Office

Name	IP Address	Type	Version	Edition
Server Edition 11.0				
<input checked="" type="checkbox"/> IPOSE-Primary	10.64.101.127	IPO-Linux-PC	11.0.4.1.0 build 11	Server (Primary)

Configuration Service User Login

IP Office: IPOSE-Primary (Primary System - IPO-Linux-PC)

Service User Name:

Service User Password:

TCP Discovery Progress:

Unit/Broadcast Address:

☒ Open with Server Edition Manager

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

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - IP500V2-One
 - IP500V2-Two

Server Edition

Summary

Server Edition Primary

Hardware Installed

- Control Unit: IPO-Linux-PC
- Secondary Server: 10.64.70.60
- Expansion Systems: 192.168.128.165
- System Identification: 1bed5074dcf74cdf66e44cabd6466ae06238c710

System Settings

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

Open...

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

Add...

- Secondary Server
- Expansion System

Description	Name	Address	Primary Link	Secondary Link	Users Configured	Extensions Configured
Solution					56	78
Primary Server	IPOSE-Primary	10.64.101.127			6	6
Expansion System	IP500V2-One	192.168.128.165	Bothway		25	24
Secondary Server	IP500V2-Two	10.64.70.60	Bothway		25	48

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

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

5.1. Licensing

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

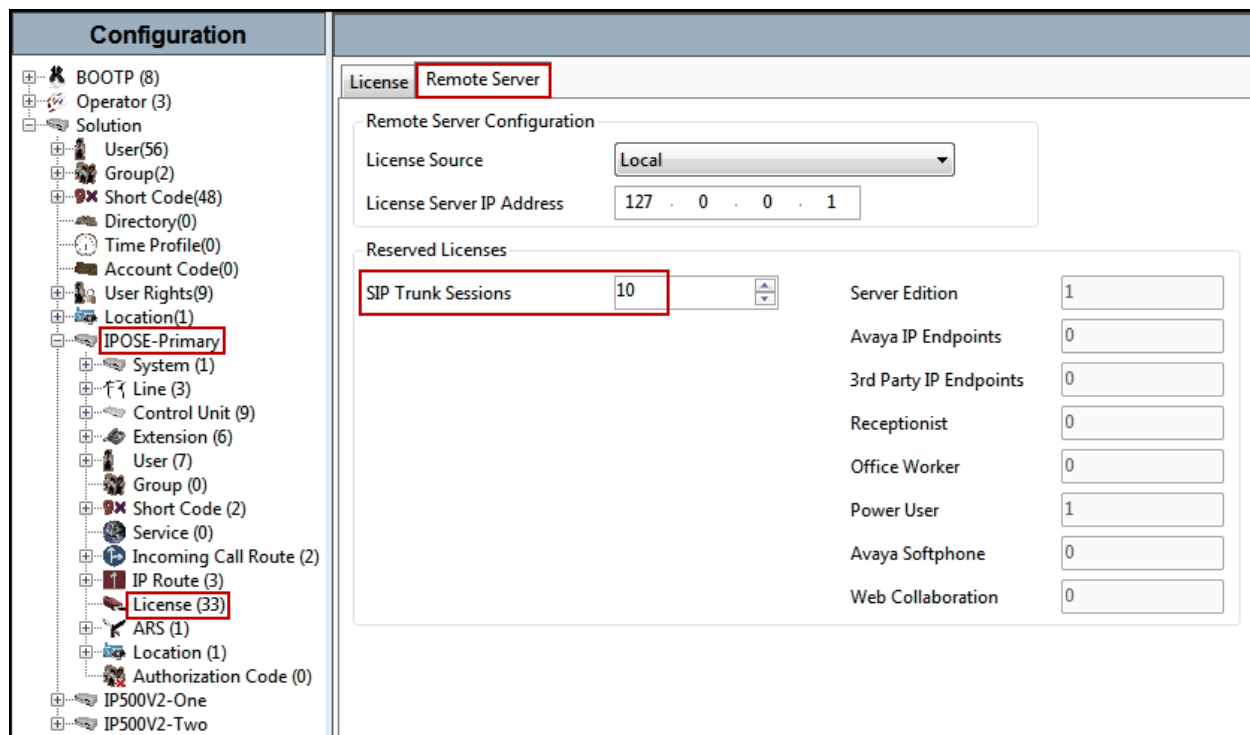
In the reference configuration, **IPOSE-Primary** was used as the system name of the Primary Server, **IP500V2-One** and **IP500V2-Two** were used as the system name for the two Expansion Systems. All navigation described in the following sections (e.g., **License**) appears as submenus underneath the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

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

The screenshot shows the Avaya IP Office Configuration window. On the left is the 'Configuration' tree with 'IPOSE-Primary' selected. On the right is the 'License' details pane. The 'License Mode' is 'License Normal' and the 'Licensed Version' is '11.0'. Below this is a table of features and their licensing details.

Feature	Instances	Status	Expiration Date	Source
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	1	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	4	Obsolete	Never	PLDS Nodal
VMPro TTS (Generic)	40	Obsolete	Never	PLDS Nodal
Teleworker	384	Obsolete	Never	PLDS Nodal
Mobile Worker	384	Obsolete	Never	PLDS Nodal
Office Worker	384	Valid	Never	PLDS Nodal
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	40	Obsolete	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	1	Obsolete	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal
SIP Trunk Channels	128	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal

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



Configuration

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - 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 (9)
 - Extension (6)
 - User (7)
 - Group (0)
 - Short Code (2)
 - Service (0)
 - Incoming Call Route (2)
 - IP Route (3)
 - License (33)**
 - ARS (1)
 - Location (1)
 - Authorization Code (0)
- IP500V2-One
- IP500V2-Two

License Remote Server

Remote Server Configuration

License Source: Local

License Server IP Address: 127 . 0 . 0 . 1

Reserved Licenses

SIP Trunk Sessions	10	Server Edition	1
		Avaya IP Endpoints	0
		3rd Party IP Endpoints	0
		Receptionist	0
		Office Worker	0
		Power User	1
		Avaya Softphone	0
		Web Collaboration	0

5.2. System Settings

Configure the necessary system settings. In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to connect IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.1. System - LAN1 Tab

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

Configuration Pane: A tree view showing the system hierarchy. The 'IPOSE-Primary' system is selected, and its sub-items are expanded. The 'System (1)' item is highlighted with a red box, and the 'IPOSE-Primary' sub-item under it is also highlighted with a red box.

IPOSE-Primary Details Pane: The 'LAN1' tab is selected, and the 'LAN Settings' sub-tab is active. The 'IP Address' field is set to '10 . 64 . 101 . 127' and the 'IP Mask' field is set to '255 . 255 . 255 . 0'. These two fields are enclosed in a red box. Below these fields, the 'Number Of DHCP IP Addresses' is set to '127'. The 'DHCP Mode' is set to 'Disabled' (indicated by a selected radio button). An 'Advanced' button is visible at the bottom right of the settings area.

5.2.1.1 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 Clearcom.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name of the enterprise under **SIP Domain Name**.
- Enter the SIP Registrar FQDN of the enterprise under **SIP Registrar FQDN**.
- Check TLS and verify the **TLS Port** numbers under **Layer 4 Protocol** are set to **5061**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP-RTCP**, **Periodic Timeout** to **30**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send RTP and RTCP keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP/RTCP traffic is present.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

Configuration

IPOSE-Primary*

System **LAN1** LAN2 DNS Voicemail Telephony Directory Services System Events SMTP SMDR VoIP Contact Center

LAN Settings **VoIP** Network Topology

☒ H.323 Gatekeeper Enable

☐ Auto-create Extension ☐ Auto-create User ☒ H.323 Remote Extension Enable

H.323 Signaling over TLS Preferred Remote Call Signaling Port 1720

☒ SIP Trunks Enable

☒ SIP Registrar Enable

☐ Auto-create Extension/User ☒ 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 ☒ UDP UDP Port 5060 Remote UDP Port 5060

☒ TCP TCP Port 5060 Remote TCP Port 5060

☒ 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

☒ 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

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

5.2.2. System - Telephony Tab

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

- Choose the **Companding Law** typical for the enterprise location; **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 IPOSE-Primary configuration window. On the left is a tree view of the configuration hierarchy, with 'IPOSE-Primary' and its sub-items highlighted. The main area shows the 'Telephony' tab, which contains various settings. A red box highlights the 'Companding Law' section, showing 'Switch' set to 'U-Law' and 'Line' set to 'U-Law Line'. Another red box highlights the 'Inhibit Off-Switch Forward/Transfer' checkbox, which is currently checked. Other visible settings include 'Dial Delay Time (sec)' set to 4, 'Default No Answer Time (sec)' set to 15, 'Park Timeout (sec)' set to 300, and 'Ring Delay (sec)' set to 5. The 'RTCP Collector Configuration' section at the bottom shows 'Send RTCP to an RTCP Collector' checked, with a server address of 0.0.0.0 and a UDP port of 5005.

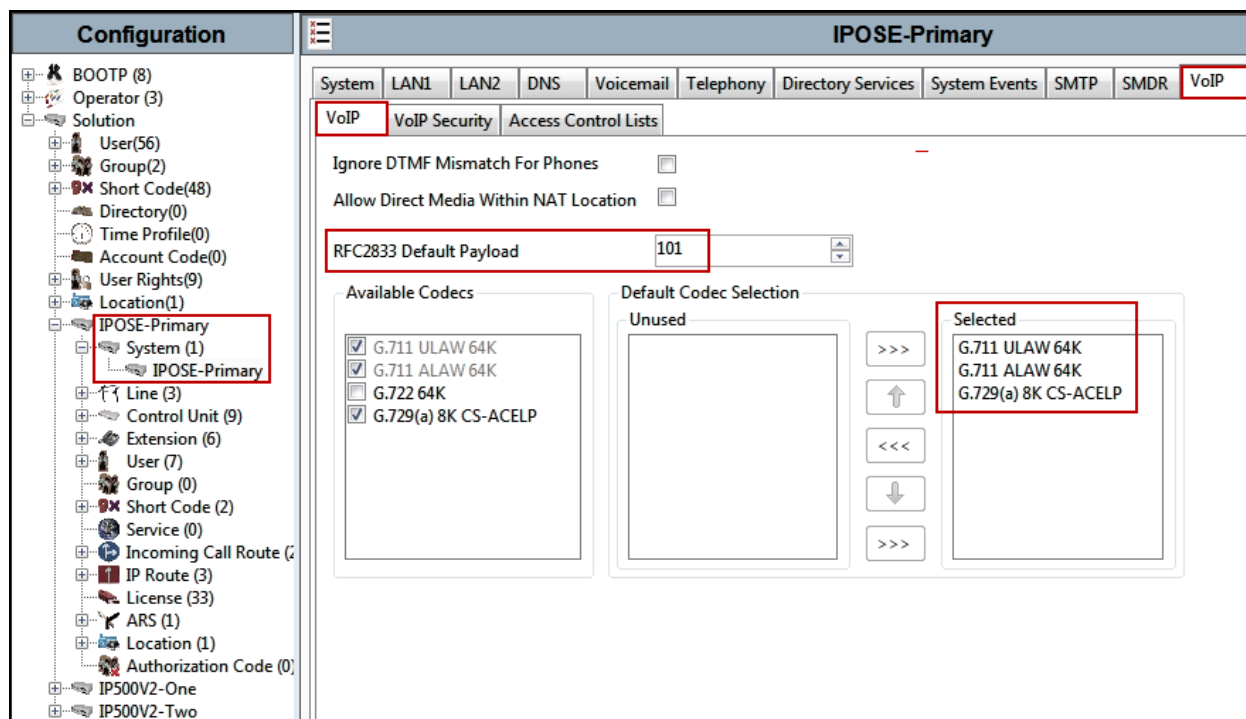
5.2.3. System - VoIP Tab

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

5.2.3.1 VoIP - VoIP Tab

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

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



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

5.2.3.2 VoIP – VoIP Security Tab

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

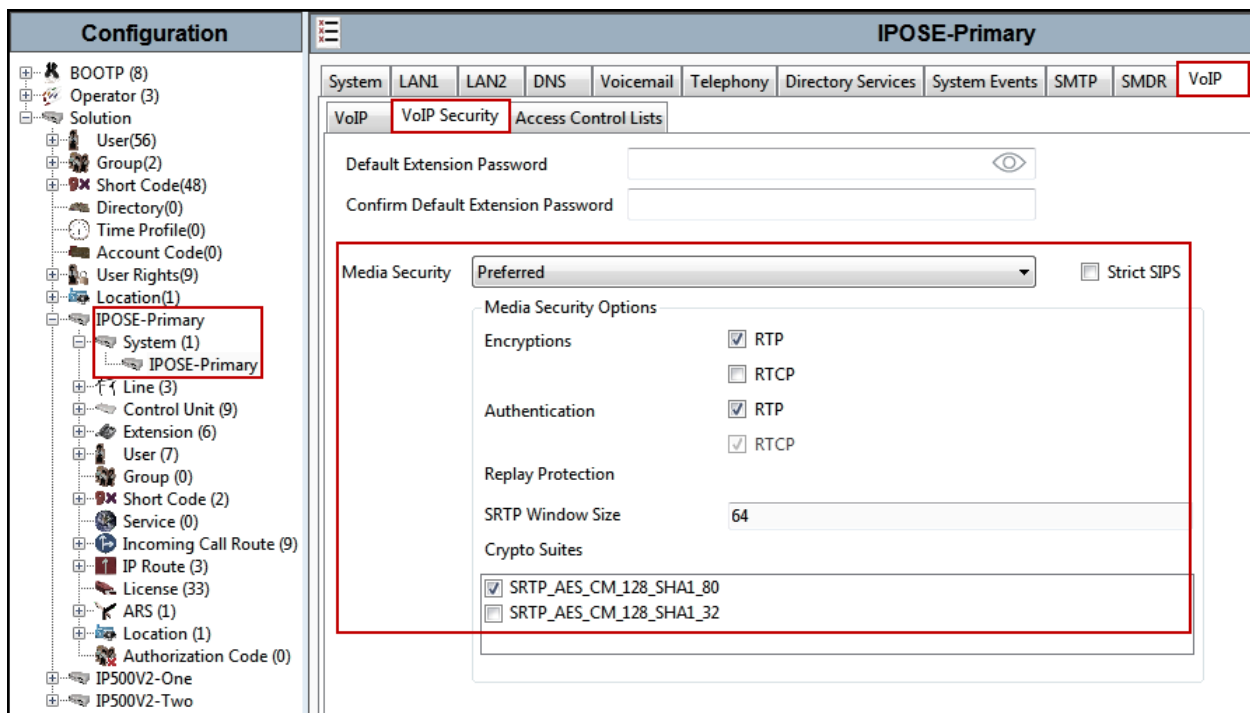
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

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

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

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

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



5.3. IP Route

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

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

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

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

5.4. SIP Line

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

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

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries

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

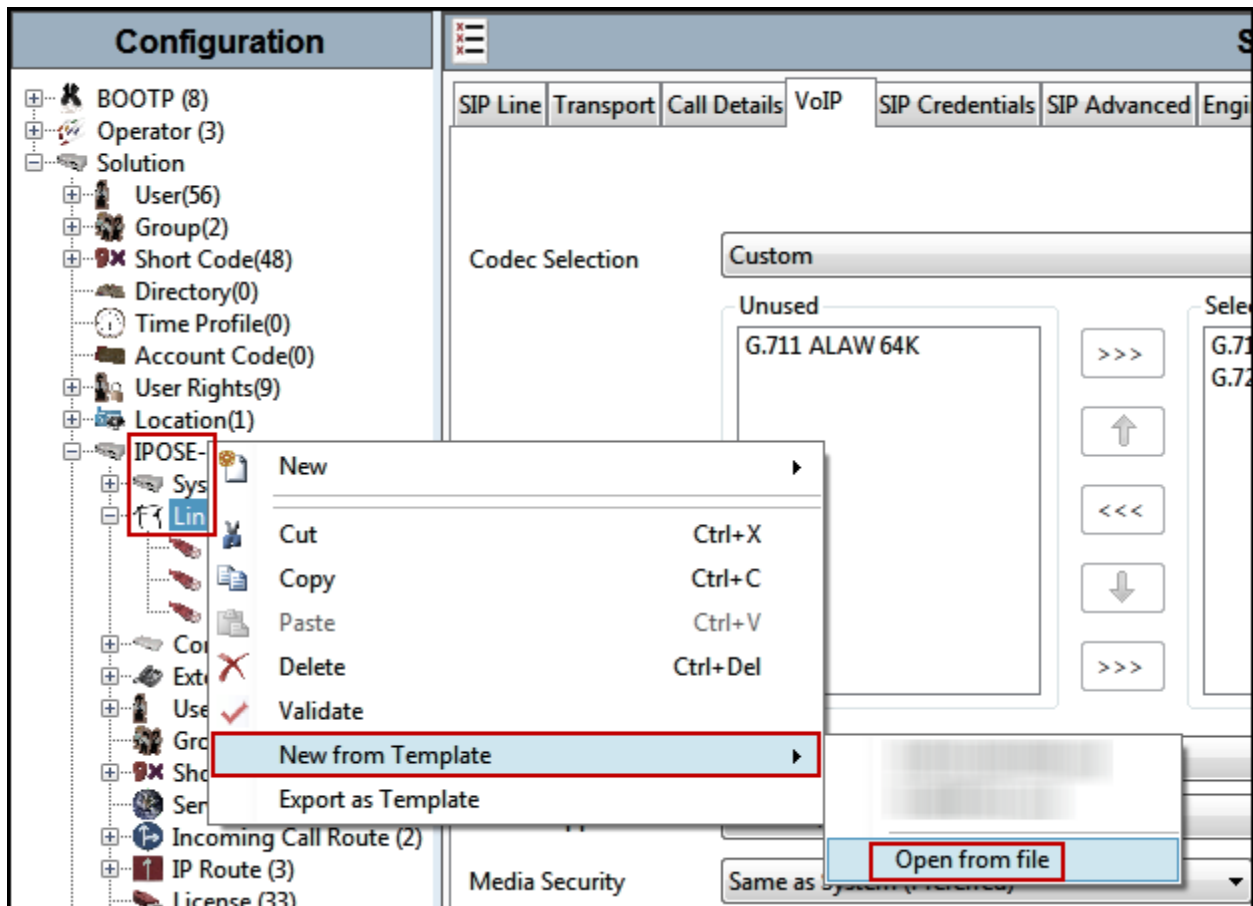
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.6**.

5.4.1. Creating a SIP Trunk from an XML Template

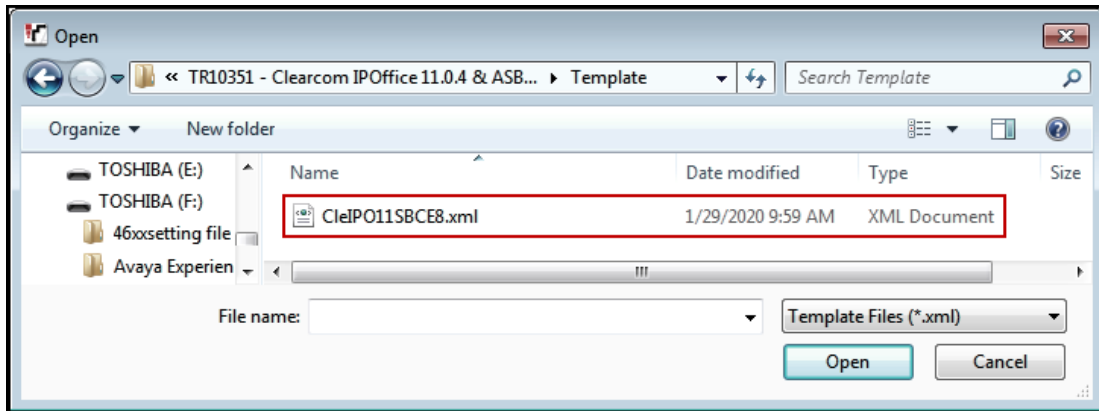
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and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

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

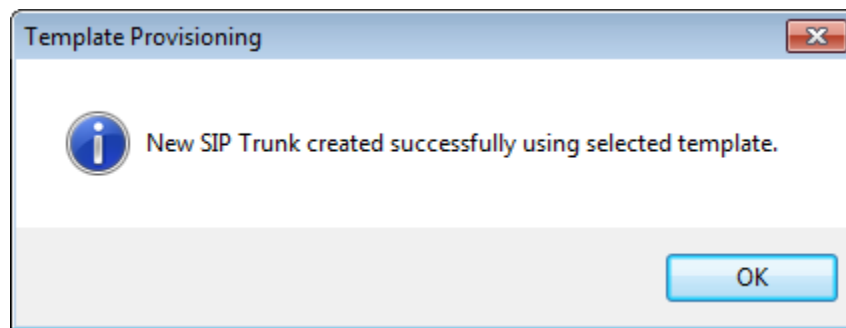
To create the SIP Trunk from the template, from the **Primary** server, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template→Open from file**.



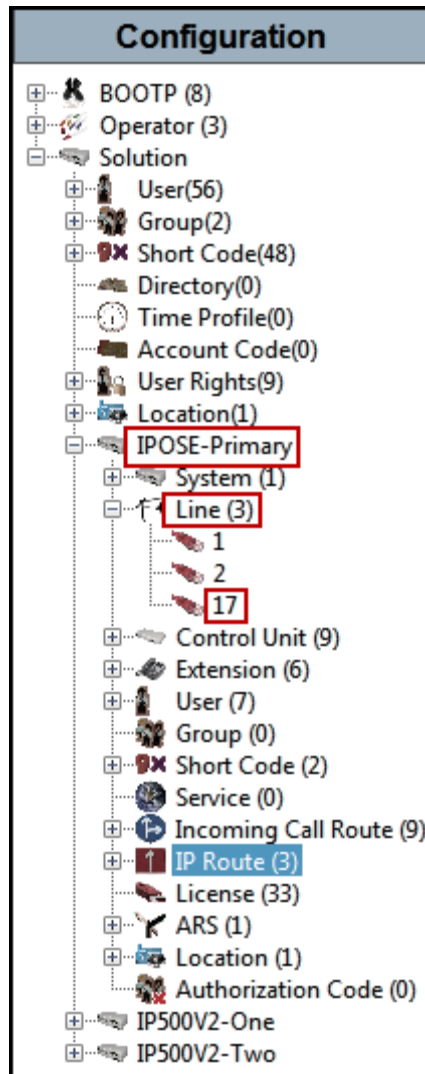
Navigate to the directory on the local machine where the template was copied and select the template.



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



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



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

5.4.2. SIP Line – SIP Line Tab

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

- Leave the **ITSP Domain Name** blank. Note that if this field is left blank, then IP Office inserts the ITSP Proxy Address from the Transport tab as the ITSP Domain in the SIP messaging.
- Verify that **In Service** box is checked, the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (sec)** is set to **On Demand**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never** (refer to Section 2.2).
- Click **OK** to commit (not shown).

Configuration

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - System (1)
 - Line (3)
 - 1
 - 2
 - 17
 - Control Unit (9)
 - Extension (6)
 - User (7)
 - Group (0)
 - Short Code (2)
 - Service (0)
 - Incoming Call Route (5)
 - IP Route (3)
 - License (33)
 - ARS (1)
 - Location (1)
 - Authorization Code (0)
 - IP500V2-One
 - IP500V2-Two

SIP Line - Line 17

SIP Line | Transport | Call Details | VoIP | SIP Credentials | SIP Advanced | Engineering

Line Number: 17

ITSP Domain Name:

Local Domain Name:

URI Type: SIP URI

Location: Cloud

Prefix:

National Prefix: 0

International Prefix: 00

Country Code:

Name Priority: System Default

Description: Service Provider

In Service: ☒

Check OOS: ☒

Session Timers

Refresh Method: Auto

Timer (sec): On Demand

Redirect and Transfer

Incoming Supervised REFER: Never

Outgoing Supervised REFER: Never

Send 302 Moved Temporarily: ☐

Outgoing Blind REFER: ☐

5.4.3. SIP Line - Transport Tab

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

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

The screenshot shows the Avaya SIP Line configuration interface. On the left is a tree view of the configuration hierarchy. The 'Line (3)' item is selected, and its sub-items are expanded, showing 'Line 17' selected. The main panel on the right is titled 'SIP Line - Line 17' and has several tabs: 'SIP Line', 'Transport', 'Call Details', 'VoIP', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'Transport' tab is active. It contains the following fields:

- ITSP Proxy Address**: 10.64.101.243
- Network Configuration** section:
 - Layer 4 Protocol**: TLS
 - Send Port**: 5061
 - Use Network Topology Info**: None
 - Listen Port**: 5061
- Explicit DNS Server(s)**: 0 . 0 . 0 . 0
- Calls Route via Registrar**: ☒
- Separate Registrar**: (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. In addition, it was not necessary to configure the **System → LAN1 → Network Topology** tab for the purposes of SIP trunking. If a NAT is used between Avaya IP Office and the other end of the trunk, then the **Use Network Topology Info** field should be set to the LAN interface (LAN1) used by the trunk and the **System → LAN1 → Network Topology** tab needs to be configured with the details of the NAT device.

5.4.4. SIP Line – Call Details Tab

Select the **Call Details** tab, and then click the **Add...** button (not shown) and the screen shown below will appear. To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button. In the example screen below two new entries were added, one for incoming calls and one for outgoing calls.

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

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

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

- Associate this entry to an incoming line group using the **Incoming Group** field. For the compliance test incoming group **17** was used. The **Outgoing Group** field was set to **100**, since it cannot be set to 0 in IP Office Server Edition systems, this is an arbitrary number.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Set the **Credentials** field to **0: <None>** (SIP Trunk registration is being done at the Avaya SBCE).
- For the **Local URI** and **Contact**, set the selections under the **Display** and **Content** columns to **Auto**.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.
- Click **OK** to commit again (not shown).

Display		Content	Field meaning		
			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 type="checkbox"/> None	None	None	None	None
P Preferred ID	<input type="checkbox"/> None	None	None	None	None
Diversion Header	<input type="checkbox"/> None	None	None	None	None
Remote Party ID	<input type="checkbox"/> None	None	None	None	None

5.4.5. SIP Line - VoIP Tab

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

- The **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line, as shown. Clearcom supports codecs **G.729(a)**, **G.711ALAW** and **G.711ULAW** for audio.
- Select **None** for **Fax Transport Support** (Refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set the **Media Security** field to **Same as System (Preferred)**.
- 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 Avaya IP Office configuration interface for the SIP Line - Line 17*. The left-hand navigation tree shows the hierarchy of configuration objects, with 'Line (3)' selected under 'IPOSE-Primary'. The main configuration area is divided into tabs: SIP Line, Transport, Call Details, VoIP, SIP Credentials, SIP Advanced, and Engineering. The VoIP tab is active, showing the following settings:

- Codec Selection:** Set to 'Custom'. A list of selected codecs is shown: G.729(a) 8K CS-ACELP, G.711 ALAW 64K, and G.711 ULAW 64K.
- Fax Transport Support:** Set to 'None'.
- DTMF Support:** Set to 'RFC2833/RFC4733'.
- Media Security:** Set to 'Same as System (Preferred)'.
- Advanced Media Security Options:** Includes checkboxes for Encryptions (RTP, RTCP), Authentication (RTP, RTCP), and Replay Protection (SRTP Window Size: 64). The 'Same As System' checkbox is checked.
- Other Options:** Includes checkboxes for Local Hold Music, Re-invite Supported (checked), Codec Lockdown, Allow Direct Media Path, and Force direct media with phones.

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

5.4.6. SIP Line – SIP Advanced Tab

In the **Addressing** area:

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

In the **Identity** area:

- Check the box for **Use PAI for Privacy**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot shows the 'SIP Line - Line 17*' configuration window with the 'SIP Advanced' tab selected. The left sidebar shows a tree view of the configuration hierarchy, with 'Line (3)' and '17' highlighted. The main area is divided into three sections: Addressing, Identity, and Media/Call Control.

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 UII header: ☐
- Add UII header to redirected calls: ☐

Media

- Allow Empty INVITE: ☐
- Send Empty re-INVITE: ☐
- Allow To Tag Change: ☐
- P-Early-Media Support: None
- Send SilenceSup=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: ☐

5.5. Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.4**. To configure these settings, first 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 Clearcom. 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).

Configuration

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - 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 (9)
 - Extension (6)
 - User (7)
 - NoUser
 - 3050 3050
 - 3040 Ext3040 H323
 - 3041 Ext3041 H323
 - 3042 Ext3042 H323
 - 3047 Ext3047 SIPSc
 - 3051 Ext3051 Desk
 - Group (0)
 - Short Code (2)
 - Service (0)
 - Incoming Call Route (
 - IP Route (3)
 - License (33)
 - ARS (1)
 - Location (1)
 - Authorization Code (0)
 - IP500V2-One
 - IP500V2-Two

Ext3041 H323: 3041

Voice Recording

Button Programming

Menu Programming

Mobility

Group Membership

Announcements

SIP

SIP Name

5528815941

SIP Display Name (Alias)

Ext3041 H323

Contact

5528815941

☐ Anonymous

5.6. IP Office Line – Primary Server

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

The screenshot displays the 'IP Office Line - Line 1' configuration window. On the left is a 'Configuration' tree with a red box around 'IPOSE-Primary' and another around 'Line (3)'. The main area has three tabs: 'Line' (selected), 'Short Codes', and 'VoIP Settings'. The 'Line' tab contains the following fields:

Field	Value
Line Number	1
Transport Type	WebSocket Server
Networking Level	SCN
Security	Medium
Telephone Number	
Prefix	
Outgoing Group ID	99999
Number of Channels	250
Outgoing Channels	250
Gateway Address	192 . 168 . 128 . 165
Location	3: Thornton, CO
Password	••••••••
Confirm Password	••••••••
Description	

Below the Gateway section, there is a 'SCN Resiliency Options' section with the following options:

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

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

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

Configuration

IP Office Line - Line 1

Line Short Codes **VoIP Settings**

Out Of Band DTMF ☒ Allow Direct Media Path ☒

Codec Selection **System Default**

Unused

Selected

G.711 ULAW 64K
G.711 ALAW 64K
G.729(a) 8K CS-ACELP

Fax Transport Support **None**

Call Initiation Timeout (s) 4

Media Security **Same as System (Preferred)**

Advanced Media Security Options ☒ Same As System

Encryptions ☒ RTP ☐ RTCP

Authentication ☒ RTP ☒ RTCP

Replay Protection

SRTP Window Size 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.

5.7. Incoming Call Route

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

- Set **Bearer Capacity** to **Any Voice**.
- The **Line Group ID** is set to **17**. This matches the **Incoming Group** field configured in the **Call Details** tab for the SIP Line on **Section 5.4.4**.
- On the **Incoming Number**, enter one of the DID numbers provided by Clearcom.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot shows the IP Office Configuration window. On the left is the 'Configuration' tree with a red box around 'IPOSE-Primary' and another red box around 'Incoming Call Route (2)' which has the number '17 5528815941' listed below it. On the right is the 'Details' pane for the selected route, titled '17 5528815941'. It has three tabs: 'Standard' (selected and highlighted with a red box), 'Voice Recording', and 'Destinations'. The 'Standard' tab contains the following fields:

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view of the configuration hierarchy. The 'Incoming Call Route' for '17 5528815941' is selected and highlighted with a red box. The main panel on the right shows the 'Destinations' tab for this specific DID. A table lists the destinations, with the first row highlighted by a red box:

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.).

5.8. 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.

5.8.1. Short Codes and Automatic Route Selection

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

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

The screenshot displays the Avaya IP Office Configuration interface. On the left is the 'Configuration' tree, and on the right is the '9N: Dial' configuration pane.

Configuration Tree (Left):

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - 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 (9)
 - Extension (6)
 - User (7)
 - Group (0)
 - Short Code (2) [highlighted]
 - 9N [highlighted]
 - Service (0)
 - Incoming Call Route (3)
 - IP Route (3)
 - License (33)
 - ARS (1)
 - Location (1)
 - Authorization Code (0)
- IP500V2-One
- IP500V2-Two

9N: Dial Configuration (Right):

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

The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **Xs** used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office.

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

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

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

The screenshot shows the 'Edit Short Code' dialog box. A red rectangle highlights the following fields: Code (001XXXXXXXXXX), Feature (Dial), Telephone Number (001N), Line Group ID (17), and Locale (Mexico (Latin Spanish)). The 'Force Account Code' and 'Force Authorization Code' checkboxes are unchecked. 'OK' and 'Cancel' buttons are on the right.

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

The screenshot shows the 'Edit Short Code' dialog box. A red rectangle highlights the following fields: Code (81XXXXXXXX), Feature (Dial), Telephone Number (81N), Line Group ID (17), and Locale (Mexico (Latin Spanish)). The 'Force Account Code' and 'Force Authorization Code' checkboxes are unchecked. 'OK' and 'Cancel' buttons are on the right.

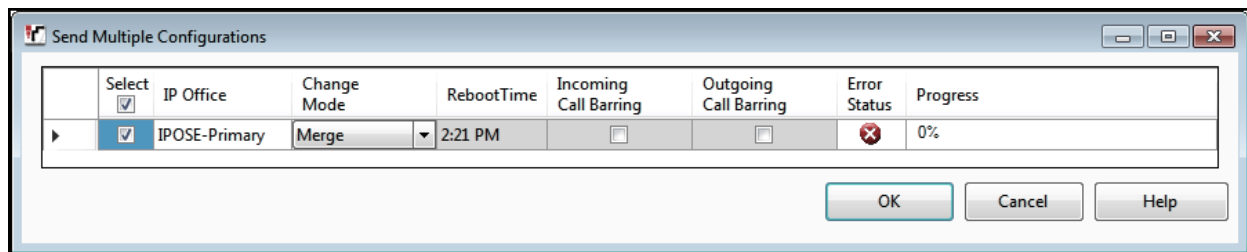
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

5.9. 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 (8)Operator (3)Solution<ul style="list-style-type: none">User(56)Group(2)Short Code(48)Directory(0)Time Profile(0)Account Code(0)User Rights(9)Location(1)IPOSE-PrimaryIP500V2-OneSystem (1)Line (3)Control Unit (4)Extension (24)User (27)Group (1)Short Code (12)Service (0)RAS (1)Incoming Call Route (2)WAN Port (0)Firewall Profile (1)IP Route (4)License (1)Tunnel (0)ARS (2)Location (1)Authorization Code (0)IP500V2-Two	<h3>Server Edition Expansion System</h3> <ul style="list-style-type: none">Hardware Installed<ul style="list-style-type: none">Control Unit: IP 500 V2Internal Modules: VCM64/PRID U; PHONE8Expansion Modules: DIG DCPx16 V2System Settings<ul style="list-style-type: none">IP Address: 192.168.128.165Sub-Net Mask: 255.255.255.0System Locale: United States (US English)System Location: 3: Thornton, CODevice ID: NONENumber of Extensions on System: 24Features Configured<ul style="list-style-type: none">Licenses Installed: Server Edition(1)Connected Extensions: 3043; 3044Users NOT Configured for Voicemail: NONEUsers assigned as Ex-Directory: NONEUsers assigned for Twinning: NONEUsers barred from making Outgoing Calls: NONEMusic on Hold: WAV File

6.1. Physical Hardware

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

The screenshot displays the Avaya IP500 V2 Configuration interface. The left pane shows a hierarchical tree of configuration objects. The right pane shows the configuration details for a selected unit.

Configuration Tree (Left Pane):

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - 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 (2)
 - WAN Port (0)
 - Firewall Profile (1)
 - IP Route (4)
 - License (1)
 - Tunnel (0)
 - ARS (2)
 - Location (1)
 - Authorization Code (0)
- IP500V2-Two

Unit Configuration (Right Pane):

Unit	
Device Number	1
Unit Type	IP 500 V2
Version	11.0.4.1.0 build 11
Serial Number	
Unit IP Address	192.168.128.165
Interconnect Number	0
Module Number	Control Unit

6.2. LAN Settings

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

- **IP Address:** 192.168.128.165 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 'Configuration' tree with a red box around 'IP500V2-One' and its sub-item 'System (1)'. The main panel on the right has tabs for 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', and 'System Events'. The 'LAN1' tab is active, and within it, the 'LAN Settings' sub-tab is selected. A red box highlights the 'IP Address' field (192 . 168 . 128 . 165) and the 'IP Mask' field (255 . 255 . 255 . 0). Other visible settings include 'Primary Trans. IP Address' (0 . 0 . 0 . 0), 'RIP Mode' (None), 'Enable NAT' (unchecked), 'Number Of DHCP IP Addresses' (200), and 'DHCP Mode' (Disabled, with radio buttons for Server, Client, Dial In, and Disabled). An 'Advanced' button is located at the bottom right of the settings area.

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

6.3. IP Route

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

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

Configuration	
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. IP Office Line – IP500 V2 Expansion System

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

The screenshot displays the 'IP Office Line - Line 17' configuration window. On the left is a 'Configuration' navigation pane with a tree structure. The 'Line' tab is selected, and 'Line (3)' is highlighted. The main configuration area is divided into several sections:

- Line Tab:** Contains fields for Line Number (17), Transport Type (WebSocket Client), Networking Level (SCN), Security (Medium), Telephone Number, Prefix, Outgoing Group ID (99999), Number of Channels (250), and Outgoing Channels (250).
- Gateway Section:** Includes Address (10 . 64 . 101 . 127), Location (3: Thornton, CO), Password, and Confirm Password.
- SCN Resiliency Options:** A section with checkboxes for 'Supports Resiliency', 'Backs up my IP phones', 'Backs up my hunt groups', and 'Backs up my IP DECT phones'.
- Description:** A text field at the bottom.

Red boxes highlight the 'Line' tab, 'Line (3)' in the navigation pane, and the 'Outgoing Group ID' field.

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

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

Configuration

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - 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)
 - 1
 - 2
 - 17
 - Control Unit (4)
 - Extension (24)
 - User (27)
 - Group (1)
 - Short Code (12)
 - Service (0)
 - RAS (1)
 - Incoming Call Route (2)
 - WAN Port (0)
 - Firewall Profile (1)
 - IP Route (4)
 - License (1)
 - Tunnel (0)
 - ARS (2)
 - Location (1)
 - Authorization Code (0)
 - IP500V2-Two

IP Office Line - Line 17

Line Short Codes **VoIP Settings** T38 Fax

Codec Selection System Default

Unused

Selected

- G.711 ULAW 64K
- G.711 ALAW 64K
- G.729(a) 8K CS-ACELP
- G.723.1 6K3 MP-MLQ

Fax Transport Support None

Call Initiation Timeout (s) 4

Media Security Preferred

Advanced Media Security Options ☒ Same As System

Encryptions ☒ RTP ☐ RTCP

Authentication ☒ RTP ☒ RTCP

Replay Protection

SRTP Window Size 64

Crypto Suites

☐ VoIP Silence Suppression

☒ Out Of Band DTMF

☒ Allow Direct Media Path

6.5. Short Codes

Similar to the configuration of the Primary server in **Section 5.8**, create a Short Code to access ARS. In the reference configuration, the **Line Group ID** is set to the ARS route illustrated in the next section.

The screenshot displays the Avaya configuration interface. On the left, a tree view shows the configuration hierarchy. The 'Short Code (12)' is selected under the 'IP500V2-One' node. On the right, the 'Short Code' configuration page is shown for '9N: Dial*'. The configuration details are as follows:

Short Code	
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	51: To-Primary
Locale	Mexico (Latin Spanish)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

6.6. Automatic Route Selection – ARS

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

The screenshot displays the ARS configuration for the 'To-Primary' route. The left sidebar shows the configuration tree with 'ARS (2)' expanded, and '51: To-Primary' selected. The main configuration area includes the following fields:

- ARS Route ID:** 51
- Route Name:** To-Primary
- Dial Delay Time:** System Default (4)
- Description:**
- In Service:** ☒ (Out of Service Route: <None>)
- Time Profile:** <None> (Out of Hours Route: <None>)
- Table:**

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

Buttons: Add..., Remove, Edit...

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

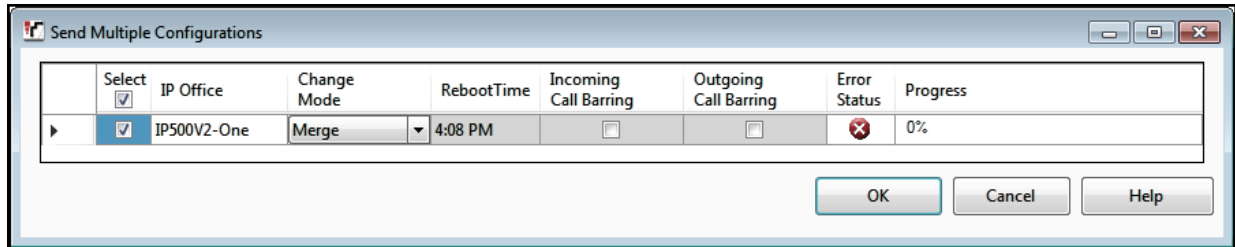
Alternate Route: <None>

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

6.7. Save IP Office Expansion System Configuration

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

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



7. Configure Avaya Session Border Controller for Enterprise

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

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

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

7.1. Log in Avaya SBCE

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

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



The screenshot shows the Avaya Session Border Controller for Enterprise login page. On the left, the Avaya logo is displayed in a large, stylized red font. Below it, the text "Session Border Controller for Enterprise" is written in a bold, black font. On the right, the "Log In" section contains a "Username:" label followed by a text input field with the placeholder text "username". Below this is a "Password:" label followed by an empty password input field. A "Log In" button is positioned to the right of the password field. Below 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." and a consent 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 "© 2011 - 2019 Avaya Inc. All rights reserved." is displayed.

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

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

EMS
Avaya_SBCE

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

- Device Management
 - System Administration
 - Backup/Restore
 - Monitoring & Logging

Information		
System Time	09:31:52 AM EST	Refresh
Version	8.0.1.0-10-17555	
Build Date	Tue Jul 30 22:53:51 UTC 2019	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	01/30/2020 09:27:06 EST	
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 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.

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

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

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

Information		
System Time	09:34:10 AM EST	Refresh
Version	8.0.1.0-10-17555	
Build Date	Tue Jul 30 22:53:51 UTC 2019	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	01/30/2020 09:27:06 EST	
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

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.

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

Session Border Controller for Enterprise

AVAYA

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

Device Management

Devices Updates SSL VPN Licensing Key Bundles

Device Name	Management IP	Version	Status	
Avaya_SBCE		8.0.1.0-10-17555	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

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

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

System Information: Avaya_SBCE

General Configuration

Appliance Name Avaya_SBCE
Box Type SIP
Deployment Mode Proxy

Device Configuration

HA Mode No
Two Bypass Mode No

License Allocation

Standard Sessions Requested: 2000 2000
Advanced Sessions Requested: 2000 2000
Scopia Video Sessions Requested: 500 500
CES Sessions Requested: 0 0
Transcoding Sessions Requested: 0 0
CLID ---
Encryption Available: Yes ☒

Network Configuration

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

DNS Configuration

Primary DNS 8.8.8.8
Secondary DNS 7.7.7.7
DNS Location DMZ
DNS Client IP 10.10.80.51

Management IP(s)

IP #1 (IPv4)

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

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

On the **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

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

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

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

7.4. Configuration Profiles

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

7.4.1. Server Interworking – Avaya-IPO

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

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

On the left navigation pane, select **Configuration Profiles → Server Interworking** (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**.



Clone Profile	
Profile Name	avaya-ru
Clone Name	Avaya-IPO
<button>Finish</button>	

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries.

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 configuration 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 (highlighted), 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, 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 a list of interworking profiles: cs2100, avaya-ru, OCS-Edge-Server, cisco-ccm, cups, OCS-FrontEnd-S..., Avaya-SM, Avaya-IPO (highlighted), Avaya-CS1000, Avaya-CM, and SP-General. Above the profile list are buttons for 'Rename', 'Clone', and 'Delete'.

The 'Avaya-IPO' profile is selected, and its configuration is shown in the 'General' tab. The 'General' tab contains 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	No
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 **Avaya-IPO** Server Interworking Profile.

Device: Avaya_SBCE ▾
Alarms
Incidents
Status ▾
Logs ▾
Diagnostics
Users
Setting

Session Border Controller for Enterprise

EMS Dashboard

Device Management

Backup/Restore

▸ System Parameters

▸ **Configuration Profiles**

Domain DoS

Server Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Interworking Profiles: Avaya-IPO

Add

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-S...

Avaya-SM

Avaya-IPO

Avaya-CS1000

Avaya-CM

SP-General

Click here to add a description.

General
Timers
Privacy
URI Manipulation
Header Manipulation
Advanced

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
--------------	------

Edit

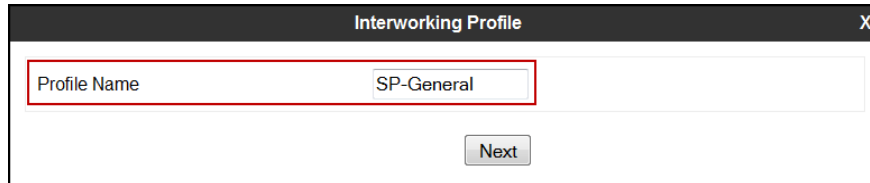
7.4.2. Server Interworking - SP-General

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

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

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

- Click **Next**.



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

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

Interworking Profile

X

General

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

Back

Next

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

Device: Avaya_SBCE ▾
Alarms
Incidents
Status ▾
Logs ▾
Diagnostics
Users
Setting

Session Border Controller for Enterprise

EMS Dashboard

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Interworking Profiles

Add

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

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation Advanced

General

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

Edit

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

Device: Avaya_SBCE | Alarms | Incidents | Status | Logs | Diagnostics | Users | Settings

Session Border Controller for Enterprise

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups
Reverse Proxy Policy
Services
Domain Policies
TLS Management
Network & Flows
DMZ Services
Monitoring & Logging

Interworking Profiles: SP-General

Interworking Profiles

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

Advanced

Click here to add a description.	
Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
DTMF	
DTMF Support	None

[Edit](#)

7.4.3. Signaling Manipulation

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

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult reference [7] in the **References** section for more information on this topic.

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

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

The scripts will later be applied to the SIP Server configuration profile corresponding to the service provider in **Section 7.4.4**.

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

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

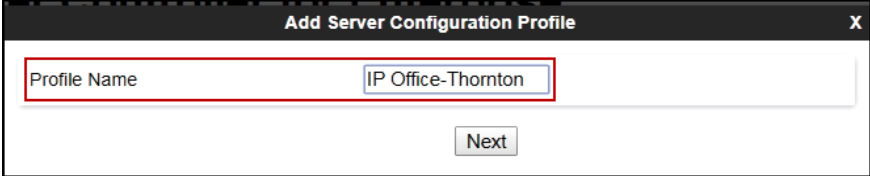
```
within session "INVITE"
{
  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    // fix anonymous
    if (%HEADERS["From"][1].URI.USER = "anonymous") then
    {
      if (exists(%HEADERS["Privacy"][1])) then
      {
        %do = "nothing";
      }
      else
    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

7.4.4. SIP Server Configuration

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

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

- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "IP Office-Thornton". The input field is highlighted with a red rectangular border. Below the input field, there is a button labeled "Next".

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

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

IP Address / FQDN	Port	Transport
10.64.101.127	5061	TLS

- 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**.

Interworking Profile
Avaya-IPO

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

The screenshot displays the 'Session Border Controller for Enterprise' management interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', and 'H'. The left sidebar shows a tree view with 'Services' expanded, and 'SIP Servers' selected. The main content area is titled 'SIP Servers: IP Office-Thornton' and features an 'Add' button and a 'Rename' button. Below this is a tabbed interface with 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced'. The 'General' tab is active, showing the following configuration:

- Server Type: Call Server
- TLS Client Profile: Remote_Worker_Dec17
- DNS Query Type: NONE/A

IP Address / FQDN	Port	Transport
10.64.101.127	5061	TLS

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

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

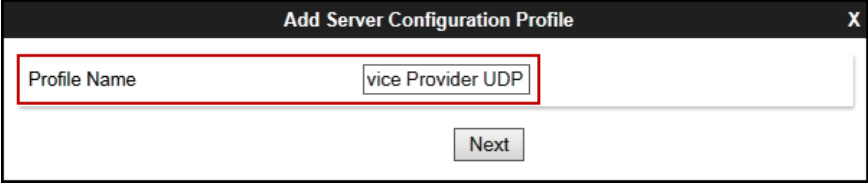
The screenshot displays the 'Session Border Controller for Enterprise' management interface, showing the 'Advanced' tab for the 'IP Office-Thornton' SIP Server Configuration Profile. The top navigation bar and left sidebar are identical to the previous screenshot. The 'Advanced' tab is active, showing the following configuration:

- Enable DoS Protection: ☐
- Enable Grooming: ☒
- Interworking Profile: Avaya-IPO
- Signaling Manipulation Script: None
- Securable: ☐
- Enable FGDN: ☐
- Tolerant: ☐
- URI Group: None

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

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

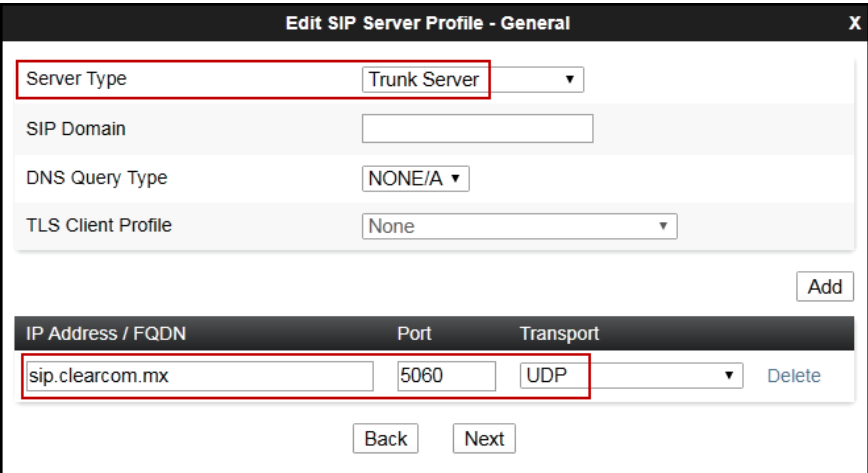
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "vice Provider UDP". This field is highlighted with a red rectangular box. Below the input field is a button labeled "Next".

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

- **Server Type:** Select **Trunk Server**.
- Click on **Add** and under **IP Address / FQDN** enter: **sip.clearcom.mx** (Clearcom's SIP proxy server FQDN, this information is provided by Clearcom).
- **Port:** **5060**.
- **Transports:** Select **UDP**.
- Click **Next**.



The screenshot shows a window titled "Edit SIP Server Profile - General". It has a close button (X) in the top right corner. The window contains several fields: "Server Type" (dropdown menu set to "Trunk Server"), "SIP Domain" (text input field), "DNS Query Type" (dropdown menu set to "NONE/A"), and "TLS Client Profile" (dropdown menu set to "None"). Below these fields is an "Add" button. At the bottom, there is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The table contains one row with the values "sip.clearcom.mx", "5060", and "UDP". This row is highlighted with a red rectangular box. To the right of the table is a "Delete" button. At the very bottom of the window are "Back" and "Next" buttons.

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


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



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

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

- Check the **Register with All Servers** box.
- **Frequency:** Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with Clearcom. **120** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
 - **From URI:** Use the **User Name** entered above in the **Authentication** screen (**user123**) and Clearcom's domain name (**clearcom.mx**), as shown on the screen below.
 - **To URI:** Use the **User Name** entered above in the **Authentication** screen (**user123**) and Clearcom's domain name (**clearcom.mx**), as shown on the screen below.
 - Click **Next**.



The screenshot shows a window titled "Add SIP Server Profile - Registration". Inside, there is a red rectangular box highlighting a section of the form. This section includes the following elements:

- A checkbox labeled "Register with All Servers" which is checked.
- A checkbox labeled "Register with Priority Server" which is unchecked.
- A text input field labeled "Refresh Interval" containing the value "120", followed by the text "seconds".
- A text input field labeled "From URI" containing the value "user123@clearcom.mx".
- A text input field labeled "To URI" containing the value "user123@clearcom.mx".

Below the red box, there are two buttons: "Back" and "Next".

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

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

- Uncheck **Enable Grooming**.
- Select **SP-General** from the **Interworking Profile** drop-down menu (Section 7.4.2).
- Select the **Add_Privacy_Header** from the **Signaling Manipulation Script** drop down menu (Sections 7.4.3).
- Click **Finish**.

Add SIP Server Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General ▼

Signaling Manipulation Script Add_Privacy_Header ▼

Securable ☐

Enable FGDN ☐

TCP Failover Port 5060

TLS Failover Port 5061

Tolerant ☐

URI Group None ▼

Back Finish

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

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
 SIP Servers
 LDAP
 RADIUS
Domain Policies
TLS Management
Network & Flows
DMZ Services
Monitoring & Logging

SIP Servers: Service Provider UDP

Add Rename Clone Delete

Server Profiles
CS1000
Com Manager
SP-SC
Service Provider ...
IP Office-Raleigh
IP Office-Thornton
Session Manager
Service Provider...

General | Authentication | Heartbeat | Registration | Ping | Advanced

Server Type Trunk Server

DNS Query Type NONE/A

IP Address / FQDN	Port	Transport
sip.clearcom.mx	5060	UDP

Edit

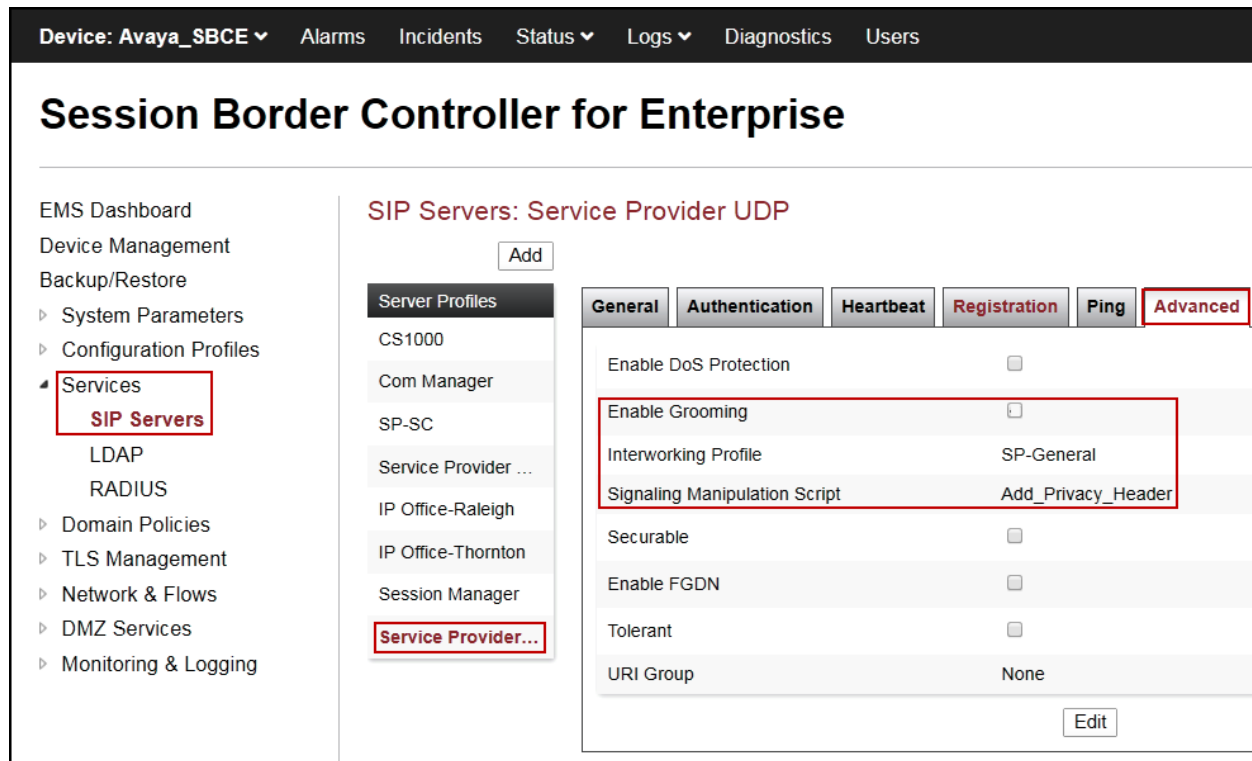
The following screen capture shows the **Authentication** tab of the newly created **Service Provider UDP** Server Configuration Profile.

The screenshot displays the 'Session Border Controller for Enterprise' management interface. At the top, a navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar contains a menu with 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services' (highlighted), 'LDAP', 'RADIUS', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. Under 'Services', 'SIP Servers' is selected. The main content area is titled 'SIP Servers: Service Provider UDP' and features an 'Add' button. Below this is a list of 'Server Profiles' including 'CS1000', 'Com Manager', 'SP-SC', 'Service Provider ...', 'IP Office-Raleigh', 'IP Office-Thornton', 'Session Manager', and 'Service Provider...' (highlighted). The 'Authentication' tab is active, showing a form with the following fields: 'Enable Authentication' (checked), 'User Name' (user123), and 'Realm' (clearcom.mx). An 'Edit' button is located at the bottom right of the form.

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

This screenshot shows the same 'Session Border Controller for Enterprise' interface, but with the 'Registration' tab selected. The navigation and sidebar elements are identical to the previous screenshot. The 'Registration' tab displays a form with the following fields: 'Register with All Servers' (checked), 'Register with Priority Server' (unchecked), 'Refresh Interval' (120 seconds), 'From URI' (user123@clearcom.mx), and 'To URI' (user123@clearcom.mx). An 'Edit' button is positioned at the bottom right of the form.

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



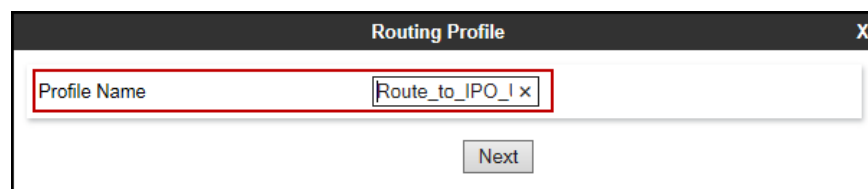
7.4.5. Routing Profiles

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

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

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

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



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

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

Routing Profile

URI Group: * Time of Day: default

Load Balancing: Priority NAPTR: ☐

Transport: None LDAP Routing: ☐

LDAP Server Profile: None LDAP Base DN (Search): None

Matched Attribute Priority: ☒ Alternate Routing: ☒

Next Hop Priority: ☒ Next Hop In-Dialog: ☐

Ignore Route Header: ☐ ENUM Suffix:

ENUM: ☐

Add

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

Back **Finish**

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

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

On the left sidebar, the "Configuration Profiles" section is expanded, and "Routing" is selected. The main content area shows the "Routing Profiles: Route_to_IPO_TLS" configuration page. It includes an "Add" button and a "Click here to add a description." link. Below this, a table lists the routing profiles:

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

The "Route_to_IP..." profile is highlighted in the list on the left, and the "Route_to_IP..." profile is selected in the table.

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 "Profile Name" field is highlighted with a red box and contains the text "ite_to_SP_UDP". A "Next" button is visible below the field.

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 **sip.clearcom.mx:5060 (UDP)** (Clearcom's SIP Proxy FQDN, port and transport).
- Click **Finish**.

The screenshot shows the 'Routing Profile' configuration window. The 'Load Balancing' dropdown is highlighted with a red box and set to 'DNS/SRV'. The 'Next Hop Address' is 'sip.clearcom.mx:5060 (UDP)'. The 'Priority' is '1'. The 'Finish' button is visible at the bottom.

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

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The 'Routing Profiles: Route_to_SP_UDP' section is highlighted. The 'Route_to_SP_UDP' profile is selected. The 'Next Hop Address' is 'sip.clearcom.mx:5060 (UDP)'. The 'Priority' is '1'.

7.4.6. Topology Hiding

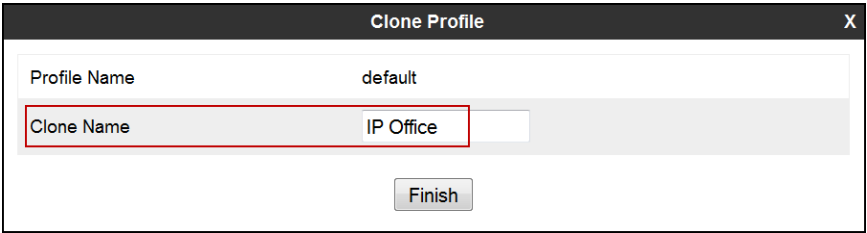
Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

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

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

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

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



The screenshot shows a 'Clone Profile' dialog box. It has a title bar with 'Clone Profile' and a close button 'X'. Inside, there are two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'IP Office'. The 'Clone Name' field is highlighted with a red border. At the bottom right, there is a 'Finish' button.

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).

Session Border Controller for Enterprise AVAYA

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

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups
Reverse Proxy Policy
Services
Domain Policies

Topology Hiding Profiles: IP Office

Add Rename Clone Delete

Click here to add a description.

Topology Hiding

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

Edit

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**.

Clone Profile X

Profile Name default

Clone Name Service_Provider

Finish

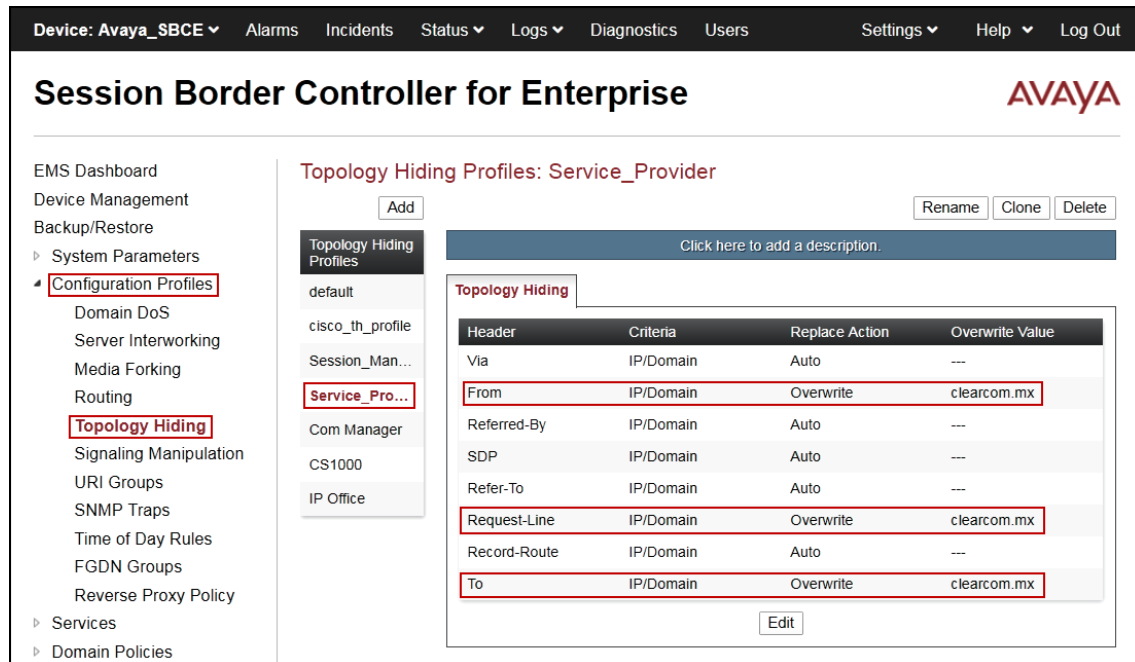
- Click **Edit** on the newly created **Service_Provider** Topology Hiding profile.
- On the **From** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (**clearcom.mx**) under **Overwrite Value**
- On the **To** choose **Overwrite**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

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

Edit Topology Hiding Profile X

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

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



7.5. Domain Policies

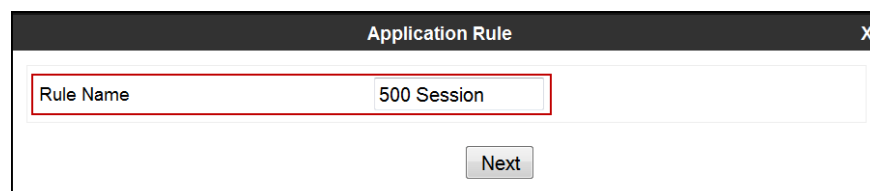
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.5.1. Application Rules

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

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

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



- 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**.

Application Rule

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

Miscellaneous

CDR Support

☒ Off
 ☐ RADIUS
 ☐ CDR Adjunct

RADIUS Profile

None

Media Statistics Support

☐

Call Duration

☒ Setup
 ☐ Connect

RTCP Keep-Alive

☐

Back

Finish

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

The screenshot displays the Avaya SBCE 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 left, the 'Domain Policies' menu is expanded, and 'Application Rules' is highlighted. The main content area is titled 'Application Rules: 500 Sessions'. It features an 'Add' button and a list of existing rules: 'default', 'default-trunk', 'default-subscr...', 'default-server...', '2000 Sessions', '500 Sessions' (highlighted), and 'Remote-Work...'. There are also 'Rename', 'Clone', and 'Delete' buttons.

The '500 Sessions' rule configuration is shown in a table with the following data:

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, the 'Miscellaneous' section shows 'CDR Support' set to 'Off' and 'RTCP Keep-Alive' set to 'No'. An 'Edit' button is located at the bottom right of the configuration area.

7.5.2. Media Rules

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

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

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

The screenshot shows a 'Media Rule' configuration dialog box. The 'Rule Name' field is highlighted with a red box and contains the text 'IPO_S RTP'. Below the 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 the 'Media Rule' configuration window. It is divided into three main sections: Audio Encryption, Video Encryption, and Miscellaneous. In the Audio Encryption section, 'Preferred Format #1' is set to 'SRTP_AES_CM_128_HMAC_SHA1_80', 'Preferred Format #2' is set to 'RTP', 'Encrypted RTCP' is unchecked, and 'Interworking' is checked. The Video Encryption section has identical settings. In the Miscellaneous section, 'Capability Negotiation' is checked. At the bottom, there are 'Back' and 'Next' buttons.

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^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

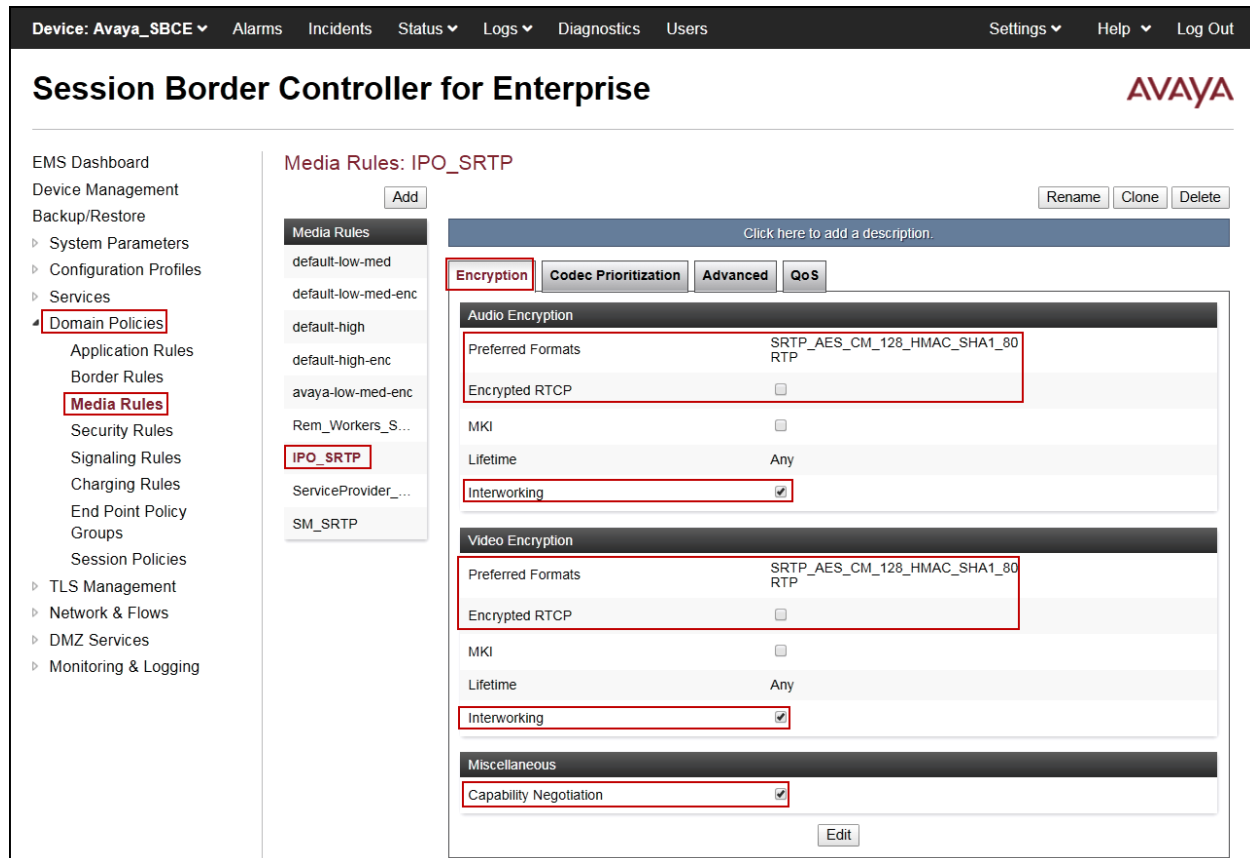
Video Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

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

Back 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.



7.5.3. End Point Policy Groups

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

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

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

- **Application Rule:** *500 Sessions*.
- **Border Rule:** *default*.
- **Media Rule:** *IPO_SRTP* (Section 7.5.2).

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

Policy Group [X]

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

Back Finish

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

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

Session Border Controller for Enterprise

AVAYA

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

Policy Groups: Enterprise

Add [Rename] [Clone] [Delete]

Click here to add a description.

Hover over a row to see its description.

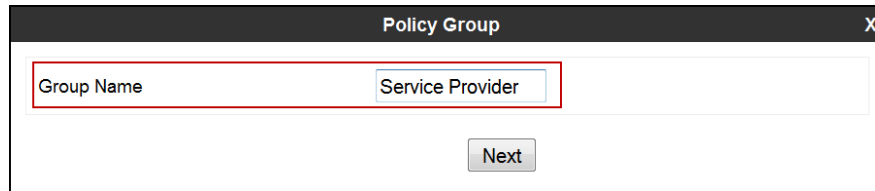
Policy Group [Summary]

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

Enterprise

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**.

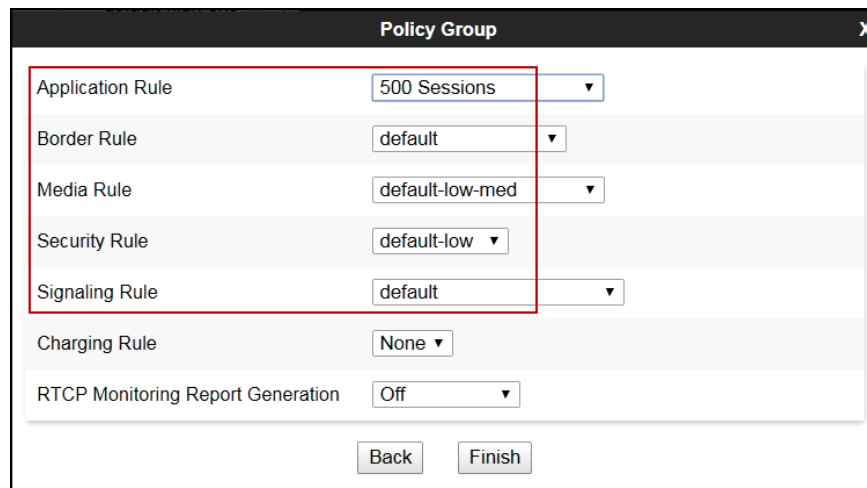


Policy Group

Group Name Service Provider

Next

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



Policy Group

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

Back Finish

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

Device: Avaya_SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services▸ **Domain Policies**Application RulesBorder RulesMedia RulesSecurity RulesSignaling RulesCharging Rules**End Point Policy Groups**Session Policies▸ TLS Management▸ Network & Flows▸ DMZ Services

Policy Groups: Service Provider

Add

Policy Groups

default-lowdefault-low-encdefault-meddefault-med-encdefault-highdefault-high-encOCS-default-h...avaya-def-low...avaya-def-hig...avaya-def-hig...Enterprise**Service Provi...**

RenameCloneDelete

Click here to add a description.

Click here to add a row description.

Policy Group

Summary

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

HG; Reviewed:
SPOC 3/2/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

84 of 104
CleIPO11SBCE8

7.6. Network & Flows Settings

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

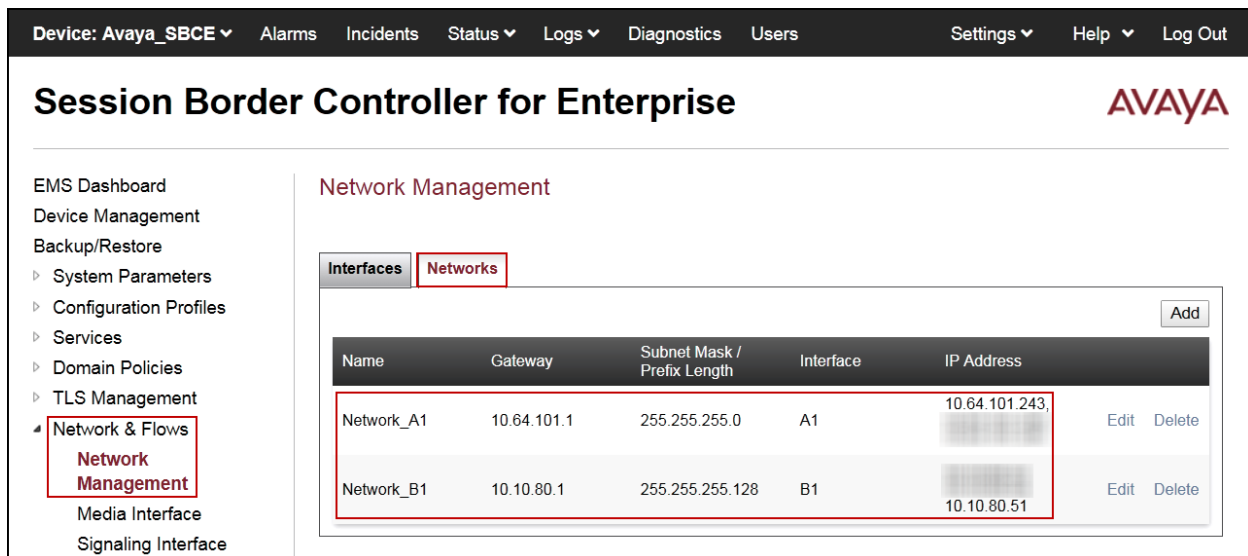
7.6.1. Network Management

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

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

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

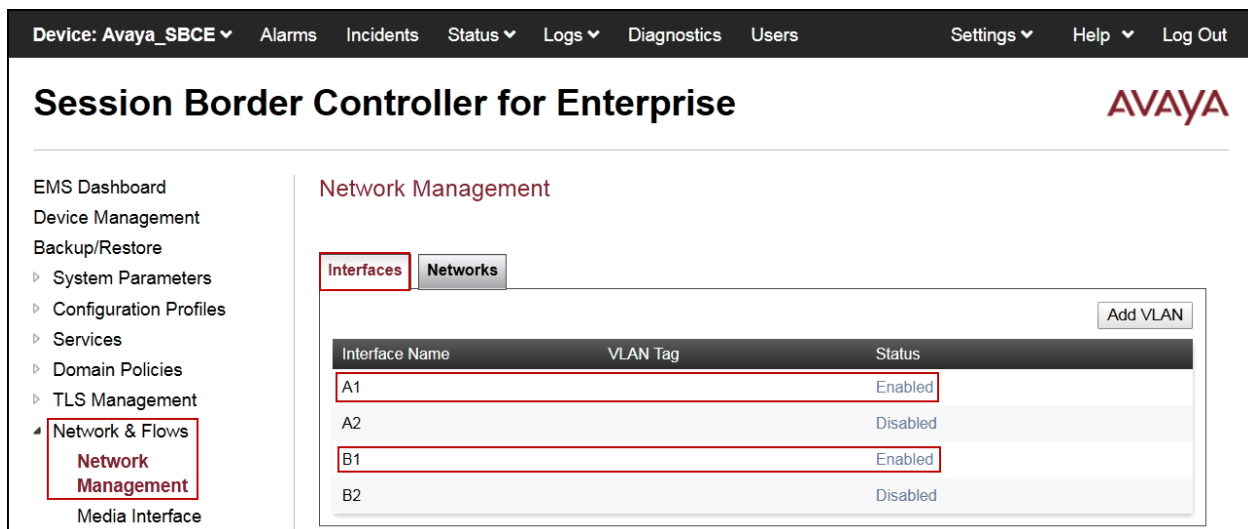
Note: Only the highlighted entity items were created for the compliance test and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in these Application Notes.



The screenshot displays the Avaya Session Border Controller 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 lists various management options, with 'Network & Flows' selected and 'Network Management' highlighted. The main content area is titled 'Network Management' and features two tabs: 'Interfaces' and 'Networks'. The 'Networks' tab is active, showing a table with the following data:

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

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



7.6.2. Media Interface

Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBCE will accept media from the connected server. Create a SIP Media Interface for both the inside and outside IP interfaces. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

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

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

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**.

Add 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

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

Media Interface

Media Interface Add

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

7.6.3. Signaling Interface

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

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

Add Signaling Interface X

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

Finish

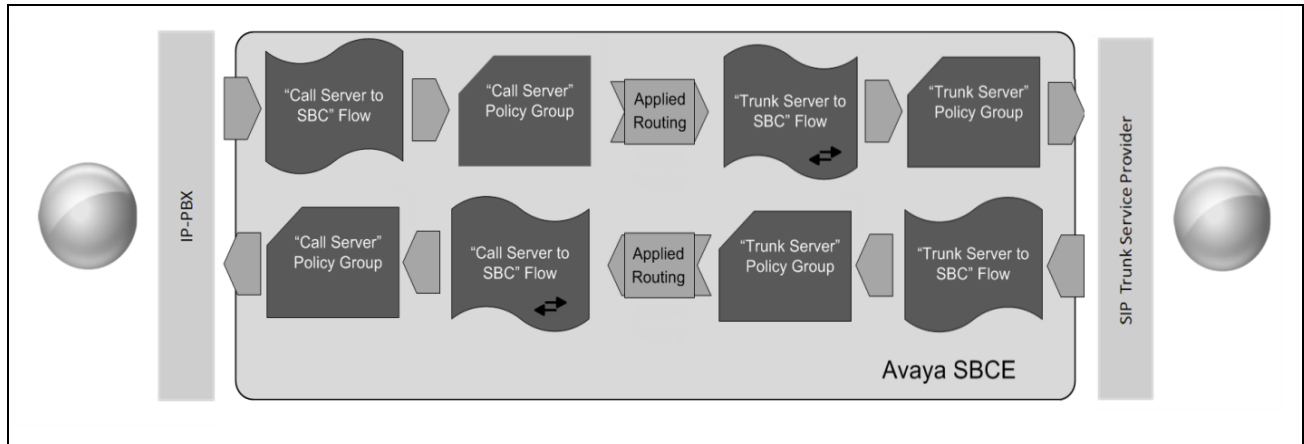
- Select **Add** in the **Signaling Interface** area (not shown).
- **Name:** *Public_sig*.
- Under **IP Address** select: *Network_B1 (B1, VLAN 0)*
- Select **IP Address:** *10.10.80.51* (outside or public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port:** *5060*.
- Click **Finish**.

The following screen capture shows the newly created Signaling Interfaces.

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

7.6.4. End Point Flows

When a packet is received by Avaya 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**.

Edit Flow: SIP_Trunk_Flow_UDP	
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**.

Edit Flow: IP_Office_Flow	
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**.

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

Session Border Controller for Enterprise

AVAYA

- 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
- Monitoring & Logging

End Point Flows

Subscriber Flows **Server Flows** Add

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

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

SIP Server: IP Office-Thornton Update

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
							View Clone Edit Delete

SIP Server: Service Provider UDP

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. Clearcom SIP Trunking Service Configuration

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

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

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

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

Clearcom will provide the following information:

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

9. Verification Steps

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

The following steps may be used to verify the configuration:

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

9.1. IP Office System Status

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

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



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

Avaya IP Office System Status - IPOSE-Primary (10.64.101.127) - IP Office Linux PC 11.0.4.1.0 build 11

IP Office System Status

Help Snapshot LogOff Exit About

- System
- Alarms (31)
- Extensions (4)
- Trunks (3)
 - Line: 1
 - Line: 2
 - Line: 17
- Active Calls
- Resources
- Voicemail
- IP Networking
- Locations

Status Utilization Summary Alarms

SIP Trunk Summary

Line Service State: In Service
 Peer Domain Name: sip://10.64.101.243
 Resolved Address: 10.64.101.243
 Line Number: 17
 Number of Administered Channels: 20
 Number of Channels in Use: 0
 Administered Compression: G729 A, G711 A, G711 Mu
 Enable Faststart: Off
 Silence Suppression: Off
 Media Stream: Best Effort
 Layer 4 Protocol: TLS
 SIP Trunk Channel Licenses: 128
 SIP Trunk Channel Licenses in Use: 0
 SIP Device Features: UPDATE (Incoming and Outgoing)

Cha...	U..	Call Ref	Curr...	Time in Remote S...	Medi...	C...	Con...	Caller ID o...	Other Party o...	Dire...	Round Trip...	Rec...	Rec...	Tran...	Tra...
1			Idle	2 da...											
2			Idle	2 da...											
3			Idle	2 da...											
4			Idle	2 da...											
5			Idle	2 da...											
6			Idle	2 da...											
7			Idle	2 da...											
8			Idle	2 da...											
9			Idle	2 da...											
10			Idle	2 da...											
11			Idle	2 da...											
12			Idle	2 da...											
13			Idle	2 da...											
14			Idle	2 da...											

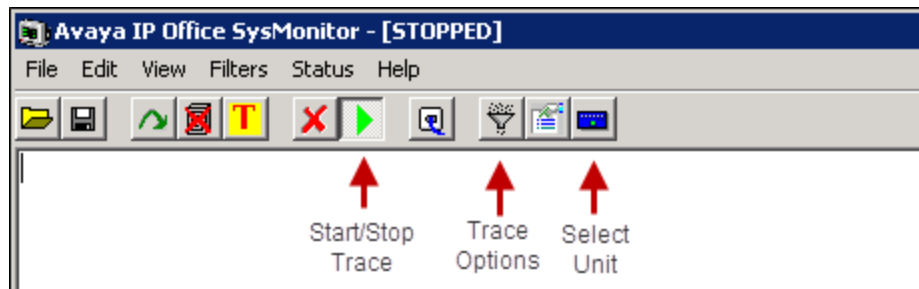
Trace Trace All Pause Ping Call Details Graceful Shutdown

Force Out of Service Print... Save As...

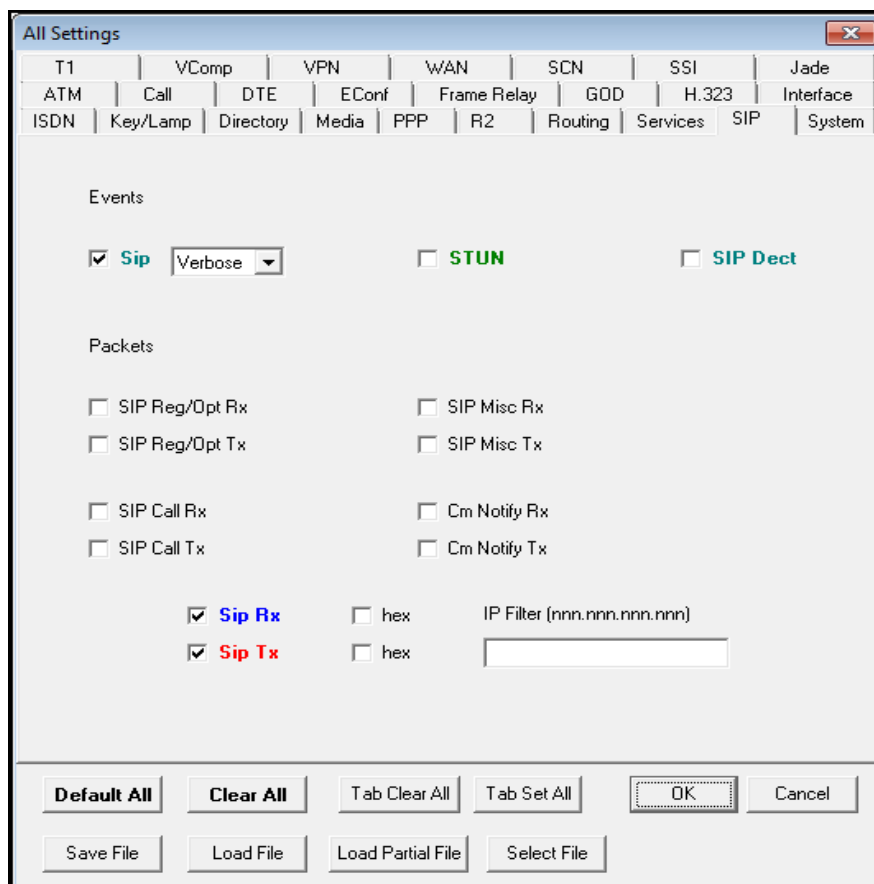
1:59:06 PM Online

9.2. Monitor

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



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



9.3. Avaya Session Border Controller for Enterprise

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

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

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	10:29:22 AM EDT	Refresh
Version	8.0.1.0-10-17555	
Build Date	Tue Jul 30 22:53:51 UTC 2019	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	09/26/2019 17:32:37 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**

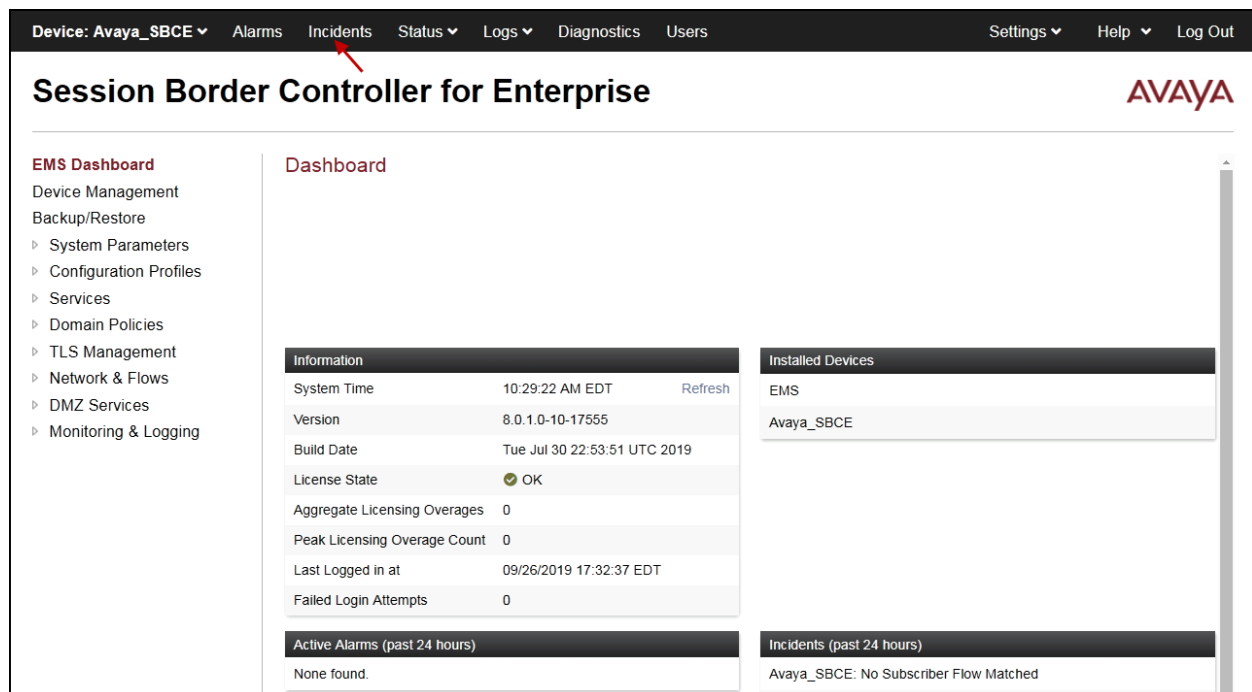
Alarm Viewer

Alarms

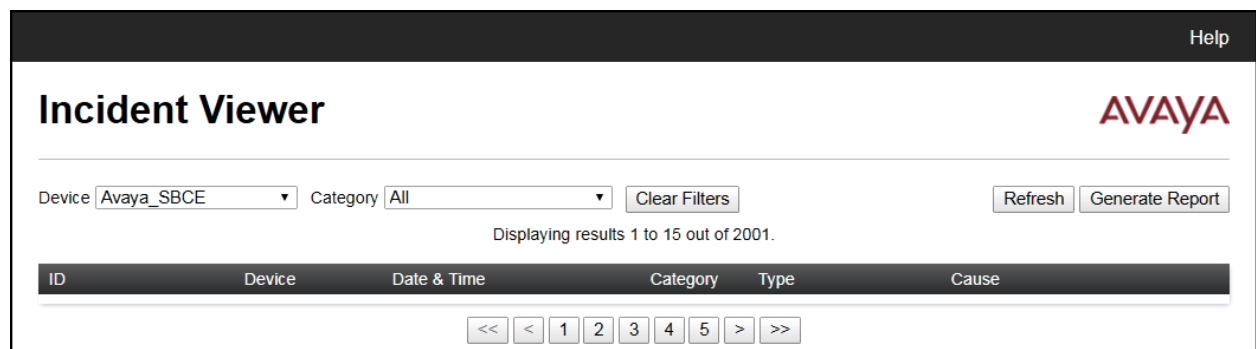
<input checked="" type="checkbox"/>	ID	Details	State	Time	Device
No alarms found for this device.					

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

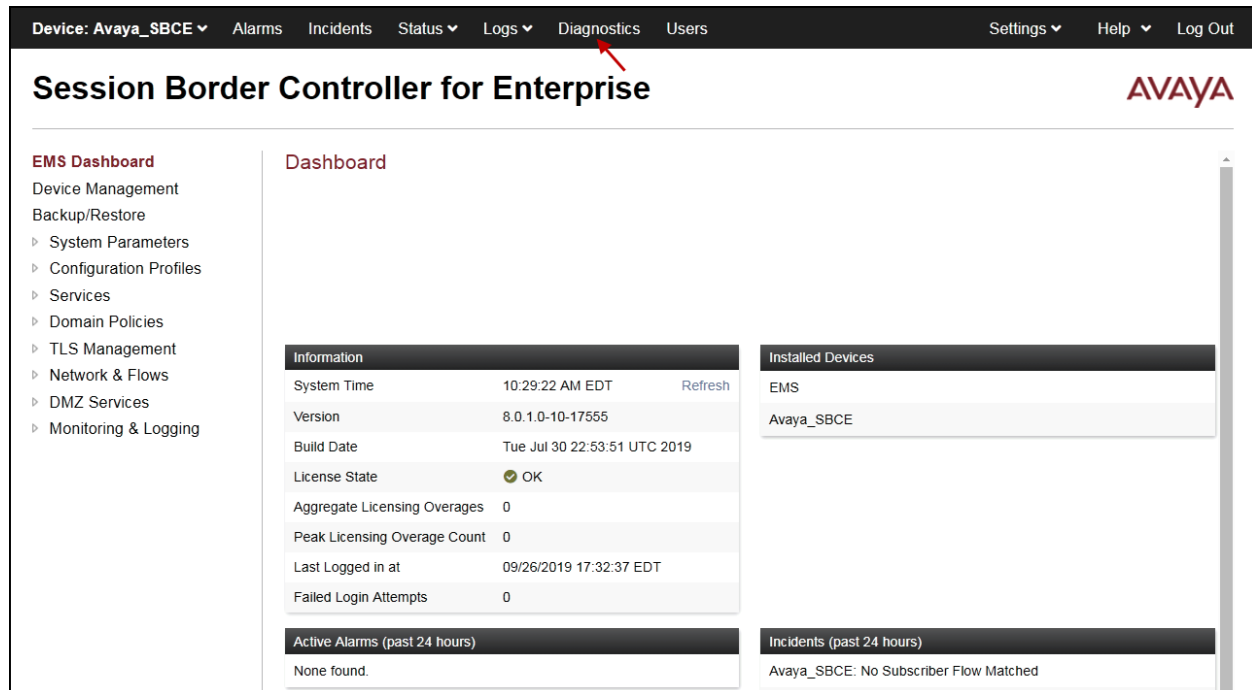
Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.



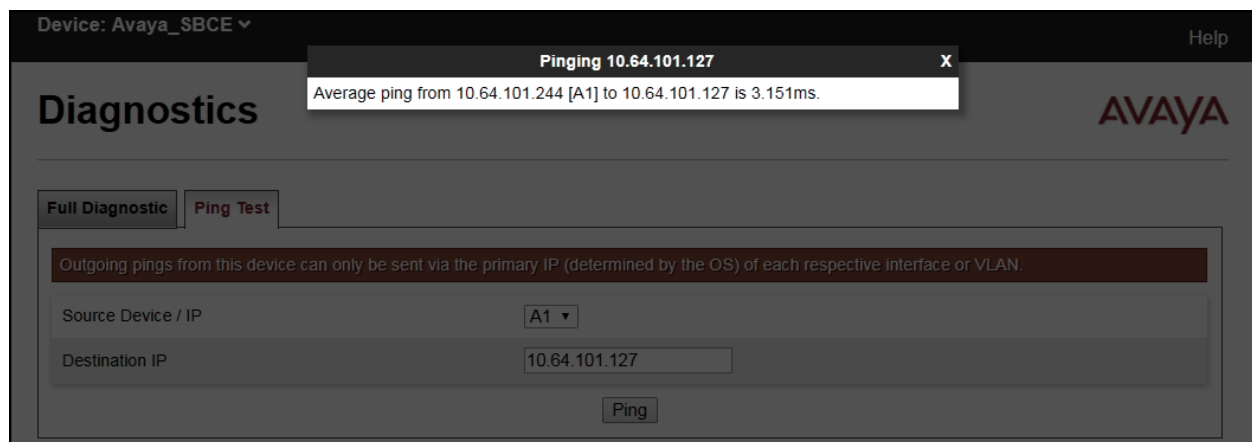
The following screen shows the Incident Viewer page.



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



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



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

The screenshot displays the Avaya SBCE web interface. 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 'Monitoring & Logging' and its sub-item 'Trace' highlighted. The main content area, titled 'Trace: Avaya_SBCE', features two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' form is shown with the following fields: 'Status' (Ready), 'Interface' (Any), 'Local Address' (All), 'Remote Address' (*), 'Protocol' (All), 'Maximum Number of Packets to Capture' (10000), and 'Capture Filename' (Test.pcap). A red box highlights the configuration fields. 'Start Capture' and 'Clear' buttons are at the bottom right.

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>	Test.pcap

Start Capture 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.

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

Session Border Controller for Enterprise

AVAYA

- EMS Dashboard
- Device Management
- Backup/Restore
 - System Parameters
 - Configuration Profiles
 - Services
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
 - Monitoring & Logging**
 - SNMP
 - Syslog Management
 - Debugging
 - Trace**
 - Log Collection
 - DoS Learning
 - CDR Adjunct

Trace: Avaya_SBCE

Packet Capture **Captures**

Refresh

File Name	File Size (bytes)	Last Modified	
Test_20191212131401.pcap	651,264	December 12, 2019 1:14:30 PM EST	Delete

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

10. Conclusion

These Application Notes describe the procedures required to configure Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 8.0.1 to connect to Clearcom SIP Trunking Service. Clearcom SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

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

11. Additional References

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

<http://support.avaya.com/>

- [1] *Deploying IP Office Platform Server Edition Solution*, Release 11.0, May 2018
- [2] *IP Office Platform 11.0, Deploying Avaya IP Office Servers as Virtual Machines*, January 2019
- [3] *IP Office Platform 11.0, Deploying Avaya IP Office Essential Edition (IP500 V2)*, February 2019.
- [4] *Administering Avaya IP Office Platform with Manager, Release 11.0 FP4*, February 2019.
- [5] *Administering Avaya IP Office™ Platform with Web Manager, Release 11.0 FP4*, February 2019.
- [6] *Deploying Avaya Session Border Controller in a Virtualized Environment*, Release 8.0, Issue 2, March 2019.
- [7] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0, Issue 1, February 2019.
- [8] *Planning for and Administering Avaya Equinox for Android, iOS, Mac and Windows, Release 3.4.8*, November 2018
- [9] *Using Avaya Equinox for IP Office, Release 11.0 FP4*, February 2019

Additional Avaya IP Office documentation can be found at:

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

©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 DevConnect Program at devconnect@avaya.com.