



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 10 and Avaya Session Border Controller for Enterprise Release 7.1 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 10 and Avaya Session Border Controller for Enterprise Release 7.1 to support Clearcom SIP Trunking Service.

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

Clearcom SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Clearcom's network as an alternative to legacy analog or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

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.

Clearcom is a member of the Avaya DevConnect Service Provider Program. 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.....	7
3. Reference Configuration	7
4. Equipment and Software Validated	10
5. Configure IP Office	11
5.1 Licensing.....	11
5.2 System.....	12
5.2.1 System - LAN1 Tab	12
5.2.2 System - Telephony Tab	15
5.2.3 System - VoIP Tab	16
5.2.4 System – VoIP Security Tab.....	17
5.3 IP Route	18
5.4 SIP Line	19
5.4.1 Importing a SIP Line Template.....	19
5.4.2 Creating a SIP Trunk from an XML Template	21
5.4.3 SIP Line - SIP Line Tab	23
5.4.4 SIP Line - Transport Tab	24
5.4.5 SIP Line - SIP URI Tab	25
5.4.6 SIP Line - VoIP Tab	27
5.4.7 SIP Line – SIP Advanced Tab	28
5.5 Extension.....	29
5.6 Users	31
5.7 Incoming Call Route	35
5.8 Outbound Call Routing.....	37
5.8.1 Short Codes and Automatic Route Selection.....	37
5.9 Save Configuration	40
6. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE).....	41
6.1 Log in Avaya SBCE.....	41
6.2 TLS Management.....	44
6.3 Global Profiles	44
6.3.1 Server Interworking – Avaya-IPO	44
6.3.2 Server Interworking - SP-General.....	47
6.3.3 Server Configuration.....	50
6.3.4 Routing Profiles	58
6.3.5 Topology Hiding.....	61
6.4 Domain Policies	65
6.4.1 Application Rules.....	65
6.4.2 Media Rules	67
6.4.3 End Point Policy Groups.....	70
6.5 Device Specific Settings	74
6.5.1 Network Management.....	74

6.5.2 Media Interface	75
6.5.3 Signaling Interface	77
6.5.4 End Point Flows	79
7. Clearcom SIP Trunking Service Configuration.....	83
8. Verification and Troubleshooting	84
8.1 Verification Steps.....	84
8.2 Protocol Traces	84
8.3 IP Office System Status	85
8.4 IP Office Monitor.....	88
8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE)	89
9. Conclusion	94
10. References.....	95

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 Avaya IP Office 500 V2 Release 10 (hereafter referred to as IP Office), Avaya Session Border Controller for Enterprise Release 7.1 (hereafter referred to as Avaya SBCE), Avaya Communicator for Windows and Avaya Deskphones, including SIP, H.323.

The Clearcom SIP Trunking service referenced within these Application Notes is designed for business customers. Customers using this service with the Avaya IP Office solution are able to place and receive PSTN calls via a broadband 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 interchangeable throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Solution & Interoperability Test Lab by connecting IP Office and the Avaya SBCE to the Clearcom SIP Trunking service via the public Internet, as depicted in **Figure 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.

2.1 Interoperability Compliance Testing

To verify the Clearcom SIP Trunking service offering with Avaya IP Office and the Avaya SBCE, the following features and functionalities were exercised during the compliance testing:

- SIP Trunk Registration (Dynamic Authentication).
- Incoming PSTN calls to various Avaya endpoints, including SIP and H.323 telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323 telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider network.
- Incoming and outgoing PSTN calls to/from Avaya Communicator for Windows.
- Dialing plans including local calls (within Mexico), international, outbound toll-free, etc.
- Caller ID presentation.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two way speech-path. Testing was performed with codecs: G.729A, G.711U and G.711A, Clearcom's preferred codec order.
- Proper response to no matching codecs.
- Fax.
- 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:

- Operator (0) and operator assisted calls (0+10).
- REFER message for call redirection was not tested for reasons noted under **Section 2.2**.
- T.38 and G.711 pass-through fax was not tested for reasons noted under **Section 2.2**.

2.2 Test Results

Interoperability testing with Clearcom SIP Trunking service was successfully completed with the exception of observations/limitations described below:

- **Caller ID on outbound calls:** On calls originating from IP Office extensions to PSTN telephones, the caller ID number shown on the PSTN endpoint was always of the main DID number assigned by Clearcom to the SIP trunk, not the specific DID assigned to that extension. This includes calls to “twinned” mobile phones, and calls that were forwarded or transferred back out on the SIP trunk to the PSTN, where the number displayed on the PSTN endpoint was the main DID number assigned to the trunk, not the originator’s caller’s ID. This may be a requirement of the Clearcom service for all outbound calls, it is listed here simply as an observation.
- **Caller ID on inbound calls:** On inbound calls made from the test lab in the U.S., the caller ID shown on the enterprise extensions occasionally showed “Unavailable”, while in other cases showed numbers corresponding to local PSTN numbers in Mexico, not the number of the original caller. Calls made from a test number in Mexico showed the correct caller ID.
- **Outbound Calling Party Number (CPN) Block:** Clearcom did not allow outbound calls with privacy enabled. When an IP Office user activated “Withhold Number” to enable user privacy on an outbound call, IP Office sent “anonymous” in the “From” header and the “Privacy:id” header, while the caller information was still being sent in the “P-Asserted-Identity” header. Clearcom responded with a 403 error message and the call was rejected.
- **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.
- **Call transfer to the PSTN using REFER:** PSTN calls that were transferred back to the network using REFER messages 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 trunks were not released. Due to these reasons, REFER was left disabled in the Avaya IP Office for the tests. 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 remained busy for the complete duration of the call.
- **Fax support:** Fax calls using the T.38 protocol failed during the test. G.711 fax was also tested, but it behaved unreliably. Fax should not be used in this solution.
- **Incoming Call, SIP Trunk Signaling Failure:** When the SIP trunk was forced to an “Out of Service” condition, and an incoming call was attempted to one of the DID numbers, it took from 15 to 30 seconds, depending on the source of the call, for the caller to receive an error recording from the network. This amount of time seems excessive in these conditions.
- **PRACK support:** PRACK/100rel support was disabled in IP Office, if left enabled; Clearcom would return a “500 Internal Server Error” message followed by a “400 Bad Request” message in response to the PRACK sent by IP Office. The testing was done with PRACK/100rel disabled in IP Office (**Section 5.4.6**).

2.3 Support

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

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

3. Reference Configuration

Figure 1 illustrates the test configuration used. 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:

- Avaya IP Office 500v2.
- Avaya IP Office Voicemail Pro.
- Avaya Session Border Controller for Enterprise.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 1100 Series SIP IP Deskphones.
- Avaya 1408 Digital Telephones.
- Avaya 9508 Digital Telephones.
- Avaya Communicator for Windows.

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.

Also located at the enterprise site is Avaya IP Office 500 V2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codec's. The IP Office **LAN1** interface connects to the inside (**A1**) interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE (**B1**) connects to Clearcom's network via the public Internet.

For inbound calls, the calls flowed from the PSTN to Clearcom's 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, across the public Internet, to Clearcom's network.

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 (LAN), is SIP over TLS.

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

In an actual customer configuration, the enterprise site may also include additional network components between Clearcom and the enterprise. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that SIP and RTP traffic between the service provider and the enterprise must be allowed to pass through these devices.

For confidentiality and privacy purposes, actual public IP addresses and DID numbers used during the compliance test have been replaced with fictitious IP addresses and DID numbers throughout these Application Notes.

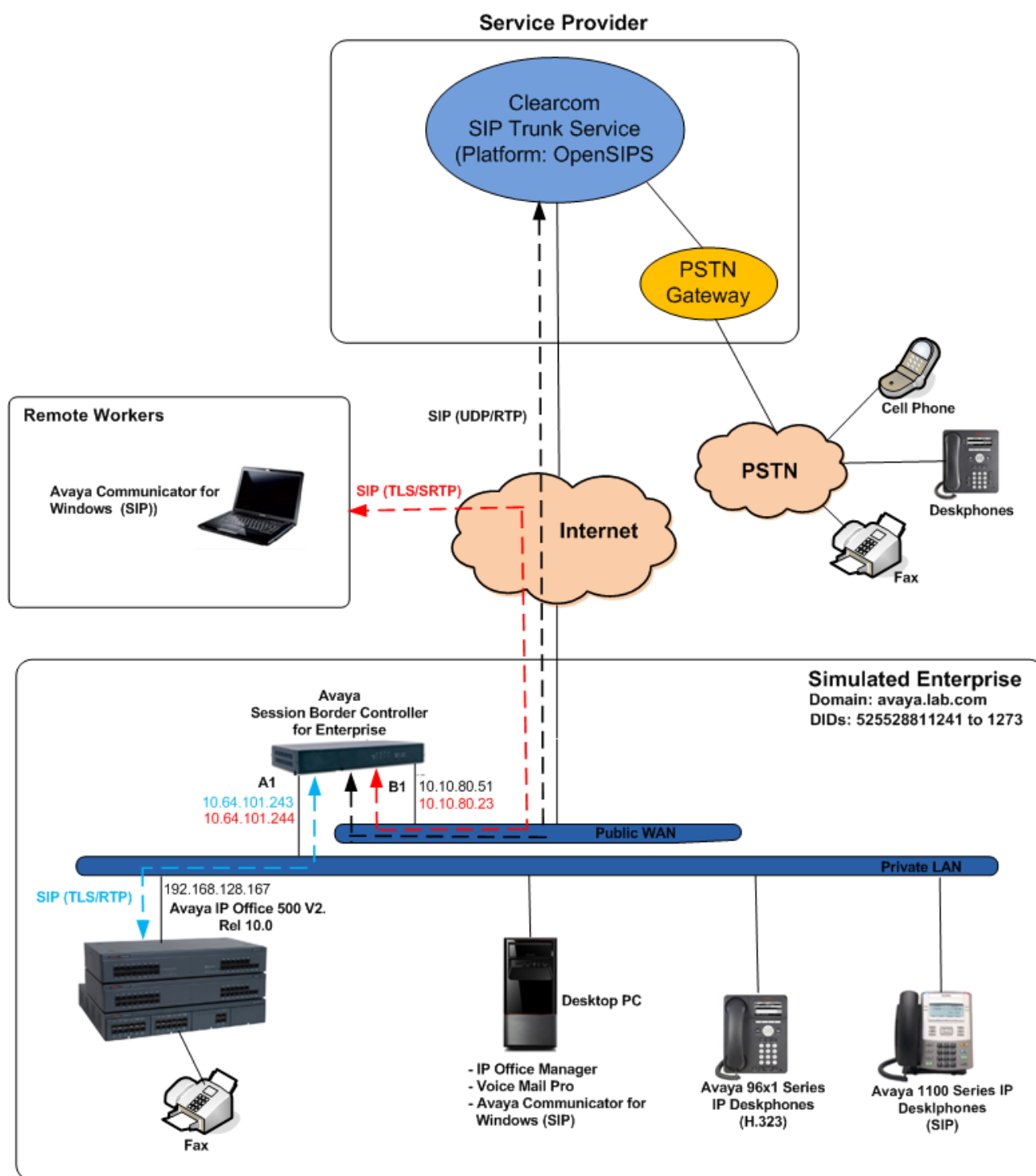


Figure 1: Avaya Interoperability Test Lab Configuration.

4. Equipment and Software Validated

The following equipment and software/firmware were used for the compliance testing.

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	10.0.0.2.0 Build 10
Avaya IP Office DIG DCPx16 V2	10.0.0.2.0 Build 10
Avaya IP Office Manager	10.0.0.2.0 Build 10
Avaya Voicemail Pro Client	10.0.0.2.0 Build 29
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.1.0.1-07-12368
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6302
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya Communicator for Windows	2.1.3.237
Avaya Digital Deskphones 1408	R46
Avaya Digital Deskphones 9508	R59
Lucent Analog Phone	--
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 500v2 and also when deployed with all configurations of IP Office Server Edition.

5. Configure IP Office

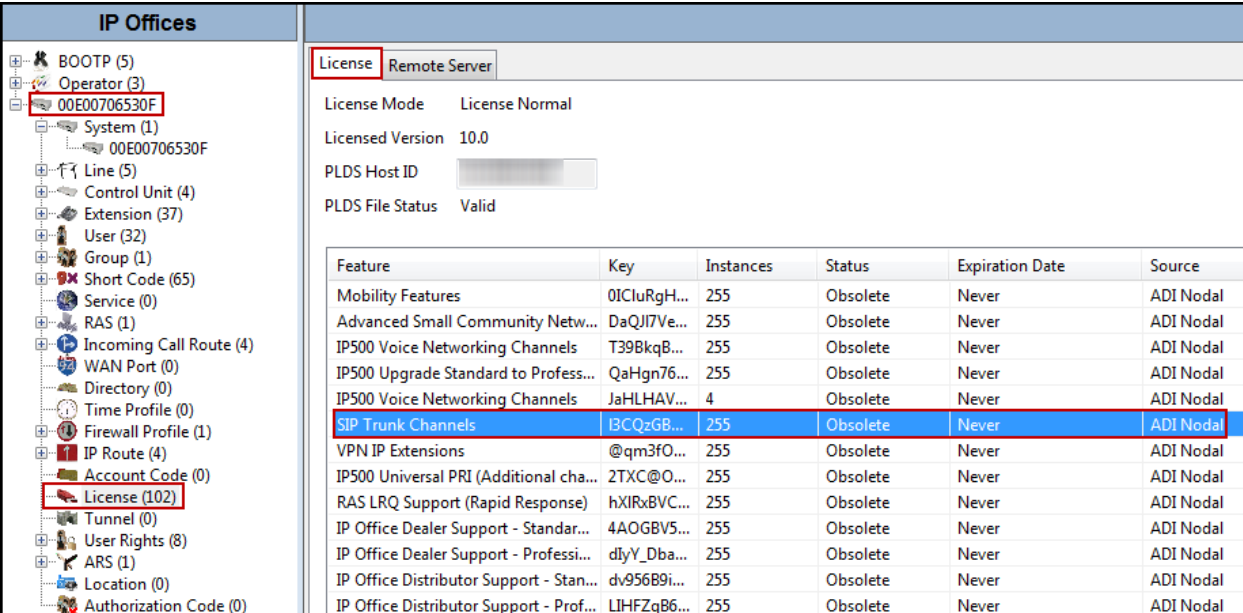
This section describes the IP Office configuration required to interwork with Clearcom SIP Trunking service. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP Office Manager. Navigate to **File → Open Configuration**, select the proper IP Office from the pop-up window, and log in with the appropriate credentials. A management window will appear as shown in the next sections. The appearance of IP Office Manager can be customized using the **View** menu (not shown). In the screenshots presented in this section, 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 these Application Notes.

These Application Notes assume the basic installation and configuration of IP Office have already been completed and are not discussed here. For further information on IP Office, please consult References in **Section 10**.

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.

To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License**, then from the license tab, locate **SIP Trunk Channels**. Confirm that there is a valid license with sufficient “Instances” (trunk channels) in the Details pane. Note that the full License Keys in the screen below is not shown for security purposes.



The screenshot displays the IP Office Manager interface. On the left, the 'IP Offices' tree view shows a hierarchy of components, with 'License (102)' selected and highlighted with a red box. The main area on the right is divided into two tabs: 'License' (active) and 'Remote Server'. The 'License' tab shows the following details:

- License Mode: License Normal
- Licensed Version: 10.0
- PLDS Host ID: [Redacted]
- PLDS File Status: Valid

Below these details is a table listing various features and their license status:

Feature	Key	Instances	Status	Expiration Date	Source
Mobility Features	0ICluRgH...	255	Obsolete	Never	ADI Nodal
Advanced Small Community Netw...	DaQJITVe...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	T39BkqB...	255	Obsolete	Never	ADI Nodal
IP500 Upgrade Standard to Profess...	QaHgn76...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	JaHLHAV...	4	Obsolete	Never	ADI Nodal
SIP Trunk Channels	IBCQzGB...	255	Obsolete	Never	ADI Nodal
VPN IP Extensions	@qm3fO...	255	Obsolete	Never	ADI Nodal
IP500 Universal PRI (Additional cha...	2TXC@O...	255	Obsolete	Never	ADI Nodal
RAS LRQ Support (Rapid Response)	hXIRxBVC...	255	Obsolete	Never	ADI Nodal
IP Office Dealer Support - Standar...	4A0GBV5...	255	Obsolete	Never	ADI Nodal
IP Office Dealer Support - Professi...	dlyY_Dba...	255	Obsolete	Never	ADI Nodal
IP Office Distributor Support - Stan...	dv956B9i...	255	Obsolete	Never	ADI Nodal
IP Office Distributor Support - Prof...	LIHFZqB6...	255	Obsolete	Never	ADI Nodal

5.2 System

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 Avaya IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.1 System - LAN1 Tab

In the sample configuration, the MAC address **00E00706530F** was used as the system name. The **LAN** port connects to the Avaya SBCE across the enterprise LAN (private) network. The **LAN1** settings correspond to the **LAN** port in IP Office. To access the **LAN1** settings, navigate to **System (1) → 00E00706530F** 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., **192.168.128.167**.
- Set the **IP Mask** field to the subnet mask of the 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 'IP Offices' navigation pane, showing a tree structure with 'System (1)' selected, which contains the system '00E00706530F'. On the right is the configuration details pane for this system. The 'LAN1' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The 'IP Address' is set to '192 . 168 . 128 . 167' and the 'IP Mask' is set to '255 . 255 . 255 . 0'. Other settings include 'Primary Trans. IP Address' as '0 . 0 . 0 . 0', 'RIP Mode' as 'None', 'Enable NAT' as an unchecked checkbox, 'Number Of DHCP IP Addresses' as '200', and 'DHCP Mode' with 'Disabled' selected. An 'Advanced' button is visible at the bottom right of the settings pane.

00E00706530F	
System	LAN1
LAN2	DNS
Voicemail	Telephony
Directory Services	System Events
LAN Settings	
IP Address	192 . 168 . 128 . 167
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	0 . 0 . 0 . 0
RIP Mode	None
<input type="checkbox"/> Enable NAT	
Number Of DHCP IP Addresses	200
DHCP Mode	
<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dial In <input checked="" type="radio"/> Disabled	
Advanced	

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.
- Under **H.323 Signaling over TLS** select **Preferred**.
- 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 **Domain Name**.
- Verify the **UDP Port**, **TCP Port** numbers under **Layer 4 Protocol** are set to **5060** and **TLS** port is set to **5061**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP-RTCP**, **Periodic Timeout** to **30**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP traffic is present.
- 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 for the system 00E00706530F. The left sidebar shows a tree view of configuration objects, with 'System (1)' selected. The main panel shows the 'VoIP' tab configuration. Key settings are highlighted with red boxes:

- H.323 Gatekeeper Enable** is checked.
- H.323 Signaling over TLS** is set to **Preferred**.
- SIP Trunks Enable** is checked.
- SIP Registrar Enable** is checked.
- SIP Domain Name** is set to **avaya.lab.com**.
- Layer 4 Protocol** settings:

Protocol	Port	Remote Port
UDP	5060	5060
TCP	5060	5060
TLS	5061	5061
- RTP Port Number Range** settings:

Range	Minimum	Maximum
Port Number Range	49152	53246
Port Number Range (NAT)	49152	53246
- Keepalives** settings:

Field	Value
Scope	RTP-RTCP
Periodic timeout	30
Initial keepalives	Enabled

In the **Network Topology** tab, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu to the option that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even though the default STUN settings are populated, they will not be used.
- Set the **Binding Refresh Time (seconds)** to a desired value. The value of **300** (or every 5 minutes) was used during the compliance testing. This value is used to determine the **frequency** that IP Office will send OPTIONS heartbeats to the service provider.
- Set the **Public IP Address** to the IP address assigned under the LAN Settings tab, e.g., **192.168.128.167**.
- Set the **Public Port** to **5061** for **TLS**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot displays the IP Office configuration window for system 00E00706530F. The left sidebar shows a tree view of configuration elements, with 'System (1)' and its sub-item '00E00706530F' highlighted. The main window has tabs for 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', 'System Events', 'SMTP', 'SMDR', 'VCM', and 'VoIP'. The 'LAN1' tab is active, and within it, the 'Network Topology' sub-tab is selected. The 'Network Topology Discovery' section contains the following fields: 'STUN Server Address' (69.90.168.13), 'STUN Port' (3478), 'Firewall/NAT Type' (Open Internet), 'Binding Refresh Time (sec)' (300), 'Public IP Address' (192 . 168 . 128 . 167), 'Public Port' (UDP: 0, TCP: 0, TLS: 5061), and a 'Run STUN on startup' checkbox. The 'Run STUN' and 'Cancel' buttons are located at the bottom right of the configuration area.

Note: 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 on IP Office have been previously completed, as it's not discussed in this document.

5.2.2 System - Telephony Tab

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.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

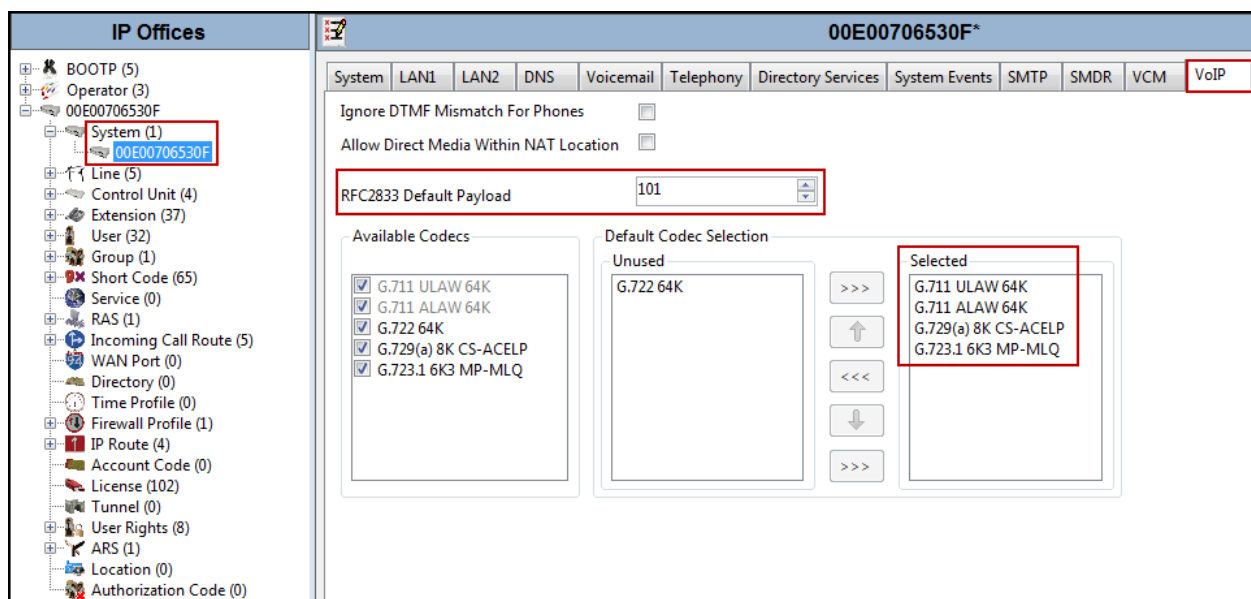
The screenshot displays the Avaya System Manager interface for configuring the Telephony tab of system 00E00706530F. The left-hand pane shows the 'IP Offices' tree with 'System (1)' selected, and '00E00706530F' highlighted. The main configuration area is divided into several sections:

- Analogue Extensions:** Includes dropdowns for Default Outside Call Sequence (Normal), Default Inside Call Sequence (Ring Type 1), and Default Ring Back Sequence (Ring Type 2). A checkbox for Restrict Analogue Extension Ringer Voltage is present.
- Companding Law:** A section with two columns, 'Switch' and 'Line'. Both have radio buttons for 'U-Law' (selected) and 'A-Law'. The 'U-Law Line' option is also selected.
- Call Parameters:** Includes numeric input fields for Dial Delay Time (3), Dial Delay Count (0), Default No Answer Time (20), Hold Timeout (0), Park Timeout (300), Ring Delay (5), and Call Priority Promotion Time (Disabled).
- Media and Security:** Includes dropdowns for Default Currency (USD), Default Name Priority (Favor Trunk), Media Connection Preservation (Disabled), and Phone Failback (Manual).
- Login Code Complexity:** Includes checkboxes for 'Enforcement' and 'Complexity'. The 'Enforcement' checkbox is checked, and the 'Minimum length' is set to 4.
- Advanced Features:** A list of checkboxes including DSS Status, Auto Hold, Dial By Name, Show Account Code, Inhibit Off-Switch Forward/Transfer (unchecked), Restrict Network Interconnect, Drop External Only Impromptu Conference, Visually Differentiate External Call, Unsupervised Analog Trunk Disconnect Handling, High Quality Conferencing, Digital/Analogue Auto Create User, Directory Overrides Barring, and Advertise Callee State To Internal Callers.

5.2.3 System - VoIP Tab

For **Codecs** settings, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **VoIP** tab and 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 was used.
- Click **OK** to commit (not shown).



Note: The codec selections defined under this section (System – VoIP Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.6** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.2.4 System – 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.

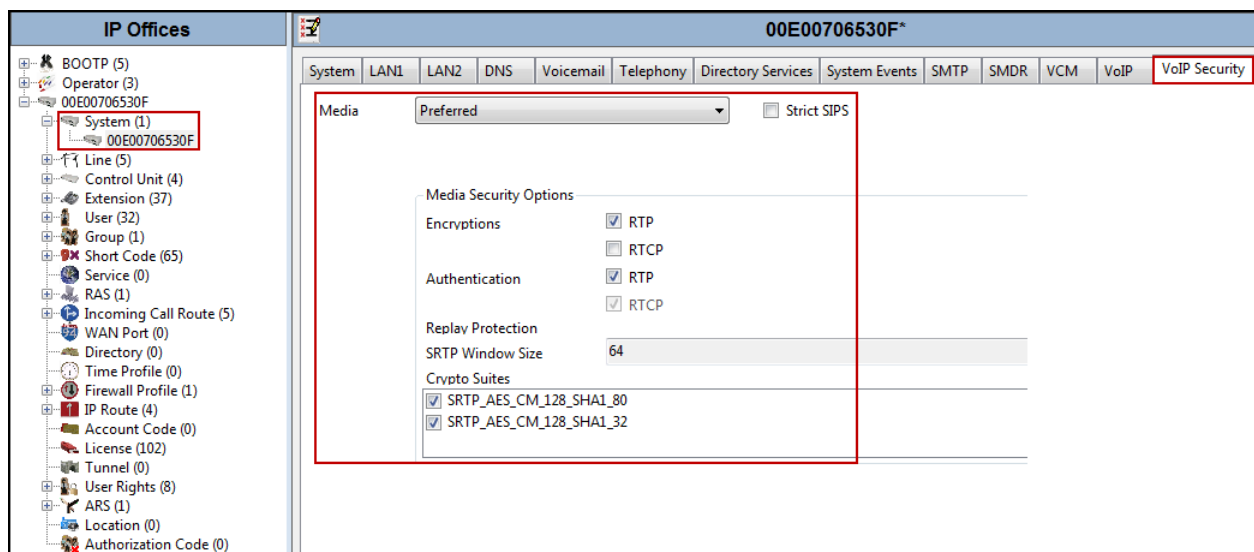
Configuring the use of SRTP at the system level is done on the **System VoIP Security** tab using the Media Security setting. The options are:

- 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, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **VoIP Security** tab and configure the following parameters:

- Under **Media Security** select **Preferred** from the pull down menu.
- Verify that Strict **SIPS** is not checked.
- Under **Media Security Options** ensure that **RTP** is checked under **Encryptions** and **Authentication**.
- Under **Crypto Suites** ensure that **SRTP_AES_CM_128_SHA1_80** and **SRTP_AES_CM_128_SHA1_32** are checked.
- Click **OK** to commit (not shown).



5.3 IP Route

In the reference configuration, the IP Office LAN1 interface and the private interface of the Avaya SBCE resided on different IP subnet, so an IP route was necessary. In an actual customer configuration, these two interfaces may be in different IP subnets, and in that case an IP route would have to be created to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to reach the IP subnet where the Avaya SBCE resides.

To 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 reach the IP subnet where the Avaya SBCE resides (if located in different subnets), on the left **Navigation** pane, right-click on **IP Route** and select **New**.

- 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., **192.168.128.200**.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).

The screenshot displays the IP Office configuration interface. On the left is the **Navigation** pane with a tree structure. The **IP Route (4)** folder is expanded, showing a list of routes. The first route is highlighted with a red box, showing an IP Address of **0.0.0.0** and a Gateway IP Address of **192.168.99.0**. On the right is the configuration window for the selected route, titled **IP Route** with a subtitle **0.0.0.0**. The window contains the following fields:

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	

5.4 SIP Line

A SIP Line is needed to establish the SIP connection between IP Office and the Charter SIP Trunking Service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by Avaya IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.4.1** and **5.4.2** 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 trunk Registration Credentials.
- SIP URI entries.
- Setting of the Use Network Topology Info field on the Transport tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.4.3** to **5.4.7**.

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 5.4.3** to **5.4.7**.

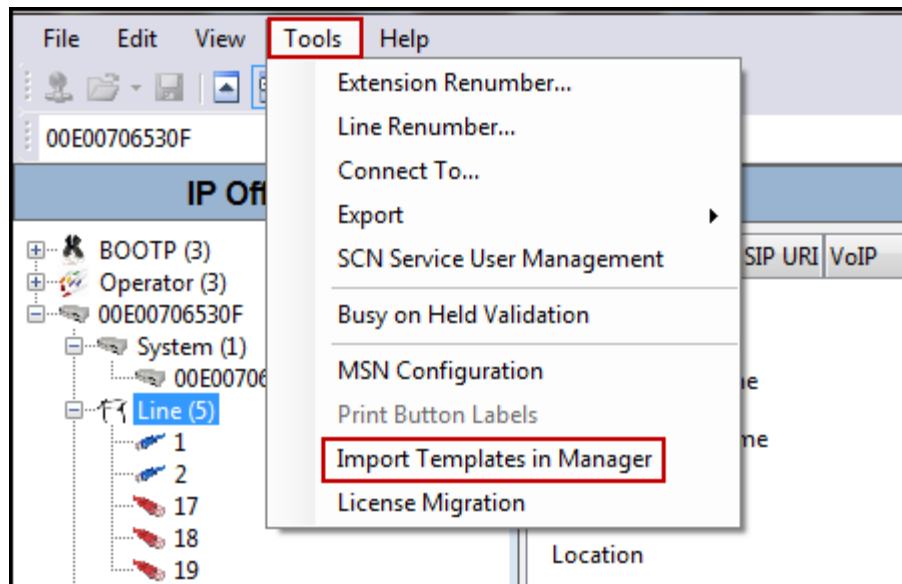
5.4.1 Importing a SIP Line Template

Note – 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 (500v2) 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.

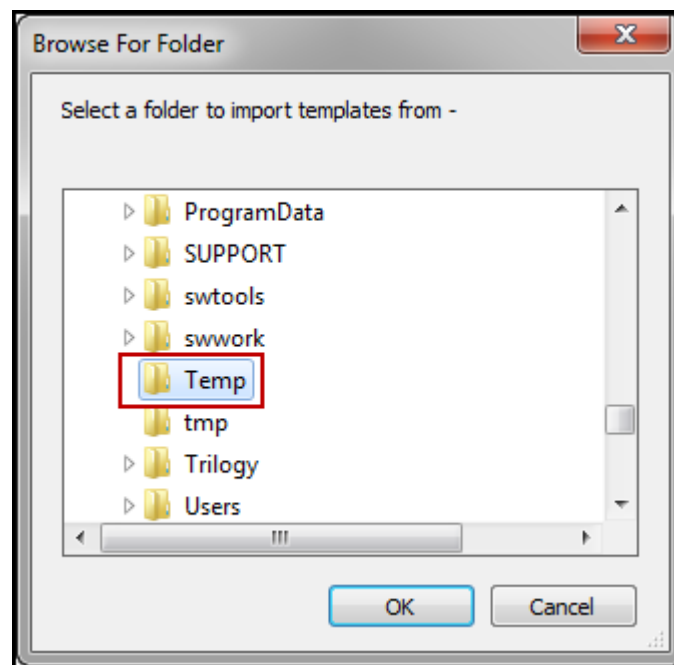
1. Copy a previously created template file to a location (e.g., C:\Temp) on the same computer where IP Office Manager is installed. By default, the template file name will have the format **<user supplied text>.xml**, where the **<user supplied text>** portion is entered during template file creation.

Note – If necessary, the **<user supplied text>** portion of the template file name may be modified, however the **<user supplied text>.xml** format of the file name must be maintained. For example, an original template file **Test.xml** could be changed to **Test1.xml**. The template file name is selected in **Section 5.4.2, step 1**, to create a new SIP Line.

2. Import the template into IP Office Manager. From IP Office Manager, select **Tools** → **Import Templates in Manager**.

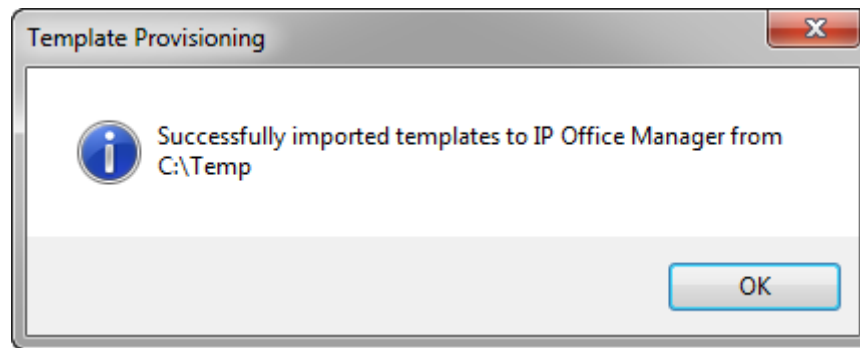


A folder browser will open. Select the directory used in **step 1** to store the template(s) (e.g., *C:\Temp*).



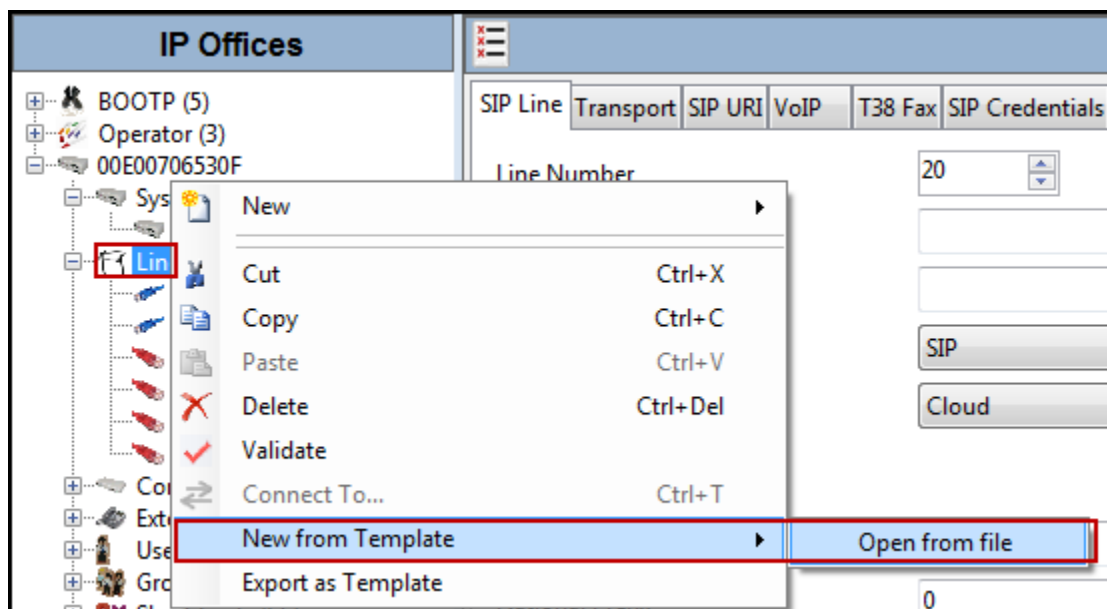
In the reference configuration, template files **ClearIPO10SBC71.xml** was imported. The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.

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

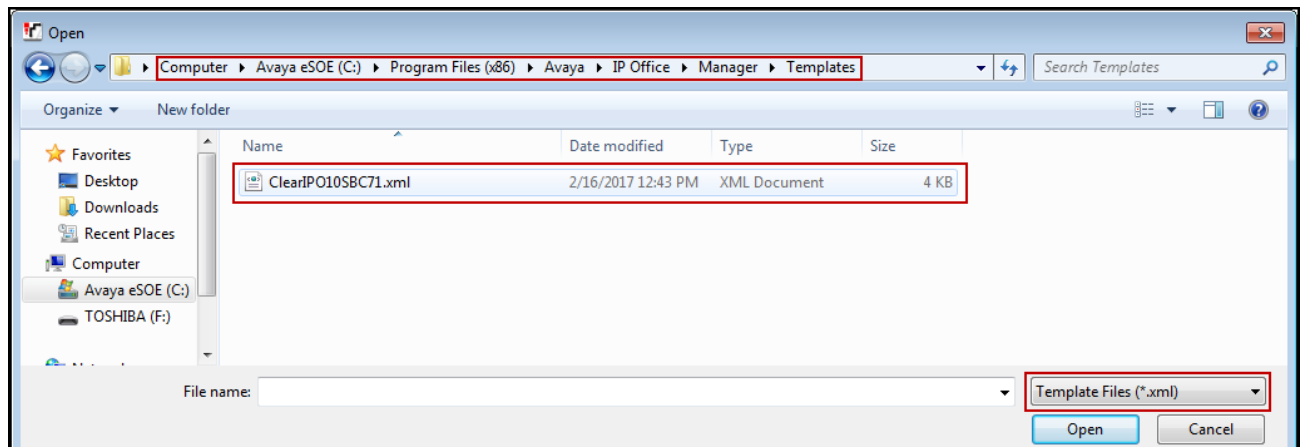


5.4.2 Creating a SIP Trunk from an XML Template

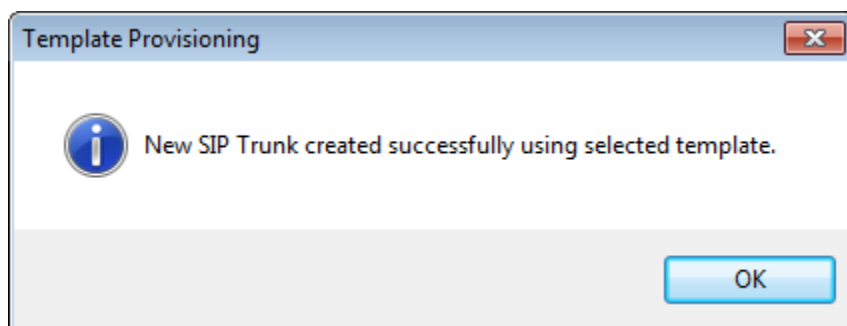
1. To create the SIP Trunk from a template, right-click on **Line** in the **Navigation** pane, and select **New from Template**→**Open from file**.



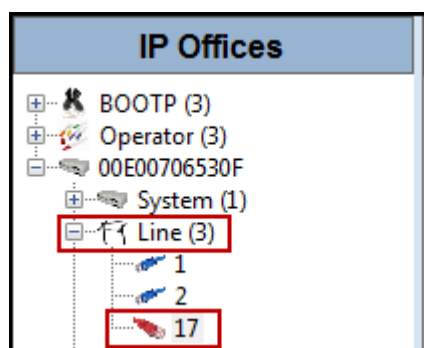
Navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates** (or *C:\Program Files (x86)\Avaya\IP Office\Manager\Templates*), on the bottom right hand side chose **Template Files (*.xml)** format and select the template, in this case **ClearIPO10SBC71.xml** was selected.



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 5.4.3 to 5.4.7**.

5.4.3 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 **URI Type** is set to **SIPS**.
- Verify that **In Service** box is checked, which is 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. The time between SIP OPTIONS sent by IP Office will use the Binding Refresh Time for LAN1, as shown in **Section 5.2.1**.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (seconds)** is set to **On Demand**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never** (Refer to **Section 2.2**).
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot displays the 'SIP Line - Line 17' configuration window. The left sidebar shows a tree view of system components, with 'Line (5)' selected. The main configuration area is divided into tabs: 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'SIP Line' tab is active, showing the following fields and values:

- Line Number:** 17
- ITSP Domain Name:** (blank)
- Local Domain Name:** (blank)
- URI Type:** SIPS
- Location:** Cloud
- Prefix:** (blank)
- National Prefix:** (blank)
- International Prefix:** (blank)
- Country Code:** (blank)
- Name Priority:** System Default
- Description:** (blank)
- 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:** ☐

5.4.4 SIP Line - Transport Tab

Select the **Transport** tab; configure the parameters as shown below:

- Set the **ITSP Proxy Address** to the IP address of the inside interface (or private side) assigned to the Avaya SBCE, as shown on **Figure 1**.
- Set the **Layer 4 Protocol** to **TLS**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2.1**.
- Set the **Send Port** to **5061**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya SIP Line configuration interface. On the left, a tree view shows the hierarchy of system components, with 'Line (5)' selected. The right pane shows the configuration for 'SIP Line - Line 17'. The 'Transport' tab is active, and the following parameters are configured:

- ITSP Proxy Address:** 10.64.101.243
- Network Configuration:**
 - Layer 4 Protocol:** TLS
 - Send Port:** 5061
 - Use Network Topology Info:** LAN1
 - Listen Port:** 5061
- Explicit DNS Server(s):** 0 . 0 . 0 . 0
- Calls Route via Registrar:** ☒
- Separate Registrar:** (empty field)

5.4.5 SIP Line - SIP URI Tab

Two SIP URI entries must be created to match each outgoing number that Avaya IP Office will send on this line and incoming numbers that Avaya IP Office will accept on this line.

To set the SIP URI for outgoing numbers, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. The entry was created with the parameters shown below:

- Set **Local URI** to the user name associated with the SIP trunk credentials provided by Clearcom. Clearcom required the user name to be sent in the “From” header.
- Set **Contact** and **Display Name** to **Use Internal Data**
- Set **Identity** under **Identity** to **None**.
- Set **Header** under **Identity** to **P Asserted ID**.
- Set **Originator Number** under **Forwarding and Twinning** to the user name associated with the SIP trunk credentials provided by Clearcom.
- Set **Send Caller ID** under **Forwarding and Twinning** to **Diversion Header**.
- Set **Diversion Header** to **Auto**.
- Under **Registration**, select **0: <None>** from the pull-down menu.
- Set **Incoming Group** to **0**.
- Set **Outgoing Group** to **17** (SIP Line number being used).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit.
- Click **OK** to commit again (not shown).

URI	Groups	Local URI	Contact	Display Name	Identity	Header	Originator Number	Send Caller ID	Diversion Header	Credential	Max
1	0 17	User123	<Internal>	<Internal>	None	PAI	User123	Diversion	Auto	0: <Non...	10
2	17 0	<Internal>	<Internal>	<Internal>	None	PAI		None	None	0: <Non...	10

Edit URI	
Local URI	User123
Contact	Use Internal Data
Display Name	Use Internal Data
Identity	
Identity	None
Header	P Preferred ID
Forwarding And Twinning	
Originator Number	User123
Send Caller ID	Diversion Header
Diversion Header	Auto
Registration	0: <None>
Incoming Group	0
Outgoing Group	17
Max Sessions	10

To set the SIP URI for inbound calls, select the **SIP URI** tab and click the **Add** button. The **New Channel** area will appear at the bottom of the pane. Set the parameters as shown below:

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**. This setting allows calls on this line that have a SIP URI that matches the number set in the **SIP** tab of any user as shown later in **Section 5.6**.
- Set **Identity** under **Identity** to **None**.
- Set **Header** under **Identity** to **P Asserted ID**.
- Set **Send Caller ID** under **Forwarding and Twinning** to **None**.
- Set **Diversion Header** to **None**.
- Under **Registration**, select **0: <None>** from the pull-down menu.
- Set **Incoming Group** to **17** (SIP Line number being used).
- Set **Outgoing Group** to **0**.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit.
- Click **OK** to commit again (not shown).

The screenshot displays the 'SIP Line - Line 17*' configuration window. The 'SIP URI' tab is selected, showing a table with two entries. The second entry is highlighted in blue. Below the table, the 'Edit URI' form is visible, with a red box highlighting the fields: Local URI, Contact, Display Name, Identity, Header, Forwarding And Twinning (Send Caller ID), Diversion Header, Registration, Incoming Group, Outgoing Group, and Max Sessions.

URI	Groups	Local URI	Contact	Display Name	Identity	Header	Originator Number	Send Caller ID	Diversion Header	Credential	Max Calls	
1	0	17	User123	<Internal>	<Internal>	None	PPI	User123	Diversion	Auto	0: <Non...	10
2	17	0	<Internal>	<Internal>	<Internal>	None	PAI	None	None	0: <Non...	10	

Edit URI

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

Identity: None

Header: P Preferred ID

Forwarding And Twinning

Originator Number:

Send Caller ID: None

Diversion Header: None

Registration: 0: <None>

Incoming Group: 17

Outgoing Group: 0

Max Sessions: 10

5.4.6 SIP Line - VoIP Tab

Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set 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 codec G.729(a), G.711 ULAW and G.711 ALAW for audio, with G.729(a) being the preferred codec.
- Select **None** for **Fax Transport Support** (Refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set the **Media Security** field to **Disabled**. **Note:** If set to “Same as System (Preferred)” calls that are forwarded to the PSTN will fail due to a re-INVITE sent by IP Office.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.
- Uncheck **PRACK/100rel Supported** box. **Note:** If enabled, Clearcom will return a “500 Internal Server Error” message followed by a “400 Bad Request” message.
- Default values may be used for all other parameters (Refer to **Section 2.2**).
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface for the SIP Line - Line 17. The left sidebar shows the system hierarchy with 'Line 17' selected. The main window has the 'VoIP' tab active. The 'Codec Selection' is set to 'Custom', showing a list of selected codecs: G.729(a) 8K CS-ACELP, G.711 ULAW 64K, and G.711 ALAW 64K. The 'Fax Transport Support' is set to 'None', 'DTMF Support' is set to 'RFC2833', and 'Media Security' is set to 'Disabled'. On the right, the 'Re-invite Supported' checkbox is checked, and the 'PRACK/100rel Supported' checkbox is unchecked.

Note: The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.4** (System – VoIP tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

5.4.7 SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab. For outbound calls with privacy enabled, Avaya IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with “anonymous”. IP Office can be configured to use the P-Preferred-Identity (PPI) or P-Asserted-Identity (PAI) header to pass the actual calling party information for authentication and billing purposes. By default, IP Office will use the PPI header for privacy. To configure IP Office to use the PAI header for privacy calls:

- Select **To Header** for **Call Routing Method**.
- 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 displays the Avaya IP Office configuration interface for a SIP Line. The left sidebar shows a tree view of the system configuration, with 'Line (5)' selected. The main panel is titled 'SIP Line - Line 17' and contains several tabs: 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced' (selected), and 'Engineering'. The 'SIP Advanced' tab is divided into four sections:

- Addressing:** 'Association Method' is set to 'By Source IP address'. 'Call Routing Method' is set to 'To Header' (highlighted with a red box). 'Suppress DNS SRV Lookups' is unchecked.
- Identity:** 'Use "phone-context"' is unchecked. 'Add user=phone' is unchecked. 'Use + for International' is unchecked. 'Use PAI for Privacy' is checked (highlighted with a red box). 'Use Domain for PAI' is unchecked. 'Swap From and PAI/Diversion' is unchecked. 'Caller ID from From header' is unchecked. 'Send From In Clear' is unchecked. 'Cache Auth Credentials' is checked. 'User-Agent and Server Headers' is empty. 'Send Location Info' is set to 'Never'.
- Media:** 'Allow Empty INVITE' is unchecked. 'Send Empty re-INVITE' is unchecked. 'Allow To Tag Change' is unchecked. 'P-Early-Media Support' is set to 'None'. 'Send SilenceSupp=Off' is unchecked. 'Force Early Direct Media' is unchecked. 'Media Connection Preservation' is set to 'Disabled'. 'Indicate HOLD' is unchecked.
- Call Control:** 'Call Initiation Timeout (s)' is set to 4. 'Call Queuing Timeout (mins)' is set to 5. 'Service Busy Response' is set to '486 - Busy Here'. 'on No User Responding Send' is set to '408-Request Timeout'. 'Action on CAC Location Limit' is set to 'Allow Voicemail'. 'Suppress Q.850 Reason Header' is unchecked. 'Emulate NOTIFY for REFER' is unchecked. 'No REFER if using Diversion' is unchecked.

5.5 Extension

In this section, an example of an Avaya IP Office extension will be illustrated. In the interests of brevity, not all users and extensions will be presented, since the configuration can be easily extrapolated to other users and extensions. To add an extension, right click on **Extension** then select **New → Select H323 or SIP**.

Select the **Extn** tab. Following is an example of extension 3040; this extension corresponds to an H.323 extension.

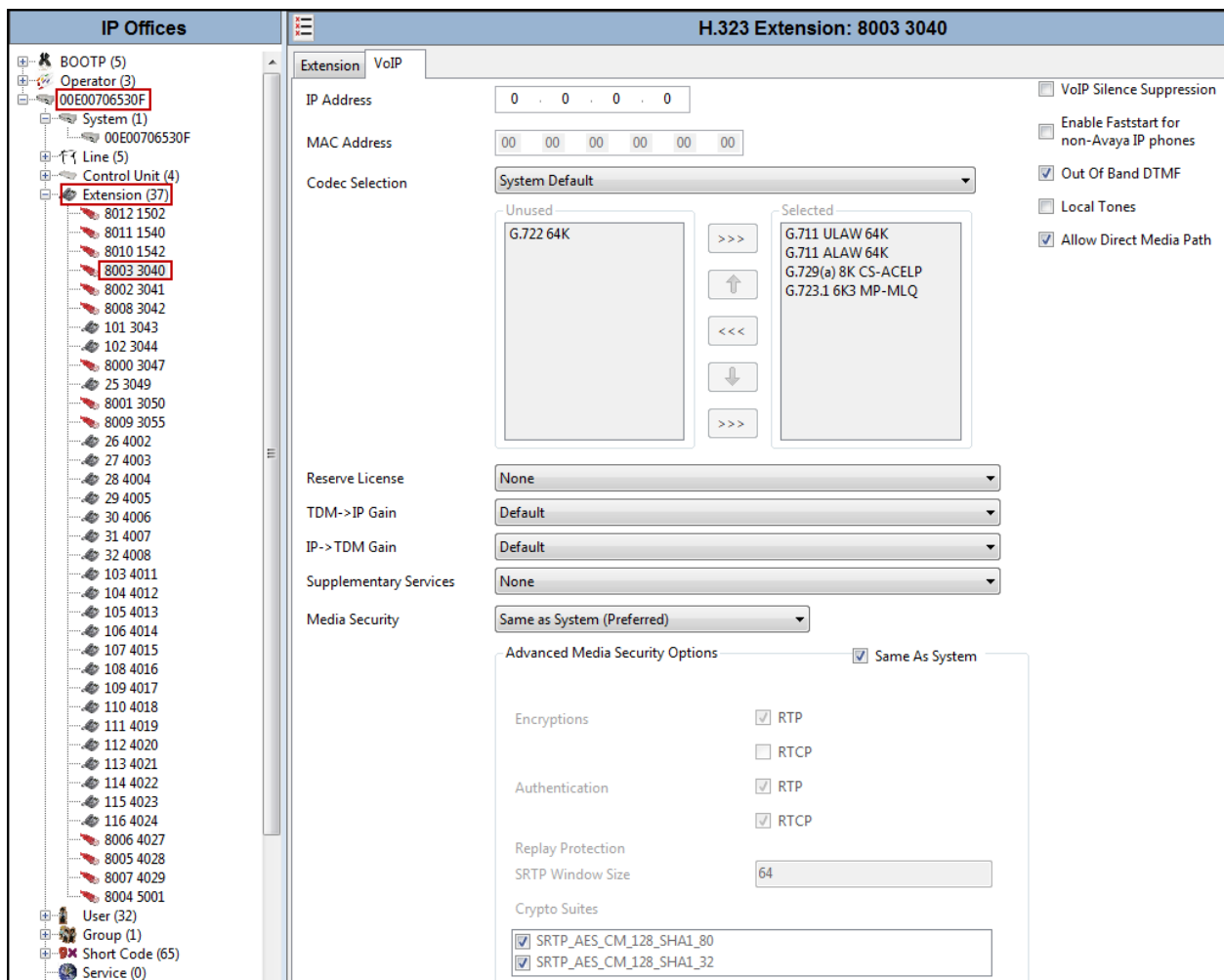
The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' tree shows a hierarchy: BOOTP (5), Operator (3), System (1) with ID 00E00706530F, Line (5), and Control Unit (4). Under the Control Unit, the 'Extension (37)' list is visible, with extension 8003 3040 highlighted. The right pane shows the configuration for 'H.323 Extension: 8003 3040'. The 'Extension' tab is selected, and the configuration fields are as follows:

Field	Value
Extension ID	8003
Base Extension	3040
Phone Password	
Confirm Phone Password	
Caller Display Type	On
Reset Volume After Calls	<input type="checkbox"/>
Device Type	Avaya 9641
Location	Automatic
Fallback As Remote Worker	Auto
Module	0
Port	0
Disable Speakerphone	<input type="checkbox"/>

Select the **VOIP** tab. Use default values on VoIP tab. Following is an example for extension 3040; this extension corresponds to an H.323 extension.

By default, all IP phones (SIP and H.323) will use the system default codec selection configured under the System Codecs tab (**Section 5.2.3**), unless configured otherwise for a specific extension by selecting **Custom** under **Codec Selection** on the screenshot shown below. The example below shows the codecs used for IP phones (SIP and H.323).

By default, all IP phones (SIP and H.323) will use the system default Media Security selection configured under the System **VoIP Security** tab (**Section 5.2.4**), unless configured otherwise for a specific extension by selecting **Media Security** under **VoIP** tab on the screenshot shown below. The **Media Security** field was set to **Same as System (Preferred)**. The example below shows the Media Security used for IP phones (SIP and H.323).




5.6 Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.4**. To configure these settings, first navigate to **User** in the left Navigation Pane, and then select the name of the user to be modified. In the example below, the name of the user is **Ext3040 H323**.

The screenshot displays the Avaya User Configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'User (32)' selected. Within the 'User' list, '3040 Ext3040 H323' is highlighted. The main panel shows the configuration for this user, with the 'User' tab selected. The configuration includes fields for Name, Password, Confirm Password, Unique Identity, Conference PIN, Confirm Audio Conference PIN, Account Status (set to 'Enabled'), Full Name, Extension (3040), Email Address, Locale, Priority (5), System Phone Rights (None), Profile (Basic User), and Device Type (Avaya 9641). The 'Basic User' profile is expanded, showing various options like Receptionist, Enable Softphone, and Enable Remote Worker, most of which are unchecked.

Ext3040 H323: 3040	
User	VoiceMail DND Short Codes Source Numbers Telephony Forwarding Dial In Voice Recording Button
Name	Ext3040 H323
Password	••••
Confirm Password	••••
Unique Identity	
Conference PIN	
Confirm Audio Conference PIN	
Account Status	Enabled
Full Name	Ext3040 H323
Extension	3040
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Basic User
<input type="checkbox"/> Receptionist	
<input type="checkbox"/> Enable Softphone	
<input type="checkbox"/> Enable one-X Portal Services	
<input type="checkbox"/> Enable one-X TeleCommuter	
<input checked="" type="checkbox"/> Enable Remote Worker	
<input checked="" type="checkbox"/> Enable Communicator	
<input type="checkbox"/> Enable Mobile VoIP Client	
<input type="checkbox"/> Send Mobility Email	
<input type="checkbox"/> Web Collaboration	
<input type="checkbox"/> Exclude From Directory	
Device Type	Avaya 9641

In the example below, the name of the user is **Ext3047 SIP**. This is a Softphone user, set the **Profile** to **Power User** and check **Enable Softphone**.

IP Offices		Ext3047 SIP: 3047									
		User	Voicemail	DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Name		Ext3047 SIP									
Password		••••••									
Confirm Password		••••••									
Conference PIN											
Confirm Conference PIN											
Account Status		Enabled									
Full Name		Softclient 3047									
Extension		3047									
Email Address											
Locale											
Priority		5									
System Phone Rights		None									
Profile		Power User									
		<input type="checkbox"/> Receptionist <input checked="" type="checkbox"/> Enable Softphone <input checked="" type="checkbox"/> Enable one-X Portal Services <input checked="" type="checkbox"/> Enable one-X TeleCommuter <input type="checkbox"/> Enable Remote Worker <input checked="" type="checkbox"/> Enable Communicator <input checked="" type="checkbox"/> Enable Mobile VoIP Client <input type="checkbox"/> Send Mobility Email <input type="checkbox"/> Ex Directory <input type="checkbox"/> Web Collaboration									
Device Type		 Unknown SIP device									

Select the **Voicemail** tab. The following screen shows the **Voicemail** tab for the user with extension 3040. The **Voicemail On** box is checked. Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters. In the verification of these Application Notes, incoming calls from Clearcom to this user were redirected to Voicemail Pro after no answer. Voicemail messages were recorded and retrieved successfully. Voice mail navigation and retrieval were performed locally and from PSTN telephones to test DTMF using RFC 2833.

Select the **Mobility** tab. In the sample configuration user 3041 was one of the users configured to test the Mobile Twinning feature. The following screen shows the **Mobility** tab for user 3041. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned telephone, including the dial access code “9”, in this case **928815943**. Other options can be set according to customer requirements.

To program a key on the telephone to turn Mobile Twinning on and off, select the **Button Programming** tab on the user, then select the button to program to turn Mobile Twinning on and off, click on **Edit → Action → Emulation**, select **Twinning** (not shown). In the sample below, button 4 was programmed to turn Mobile Twinning on and off for user 3041.

Button ...	Label	Action	Action Data
1		Appearance	a=
2		Appearance	b=
3		Appearance	c=
4		Twinning	
5			
6			
7			
8			
9			
10			
11			

Select the **SIP** tab. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the “From” and “Contact” headers for outgoing SIP trunk calls. In addition, these settings are used to match against the SIP URI of incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.4**). The example below shows the settings for user “Ext3040 H323”. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Clearcom. In the example, DID number **5528811241** was used. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.

If all calls involving this user should be considered private, then the **Anonymous** box may be checked to withhold the Caller ID information from the network.

Dial In	Voice Recording	Button Programming	Menu Programming	Mobility	Group Membership	Announcements	SIP
<div>SIP Name: 5528811241</div> <div>SIP Display Name (Alias): Ext3040 H323</div> <div>Contact: 5528811241</div> <div><input type="checkbox"/> Anonymous</div>							

5.7 Incoming Call Route

An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system.

From the left Navigation Pane, right-click on **Incoming Call Route** and select **New**.

On the Details Pane (not shown), under the **Standard** tab, set the parameters as show below:

- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group ID** to the incoming line group of the SIP line defined in **Section 5.4**.
- Set **Incoming Number** to the incoming number in which the route should match.
- Default values may be used for all other parameters.

The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'Incoming Call Route (5)' selected and highlighted with a red box. Below it, the specific route '17 5528811241' is also highlighted with a red box. The main configuration area on the right shows the 'Standard' tab selected, with a red box around the 'Bearer Capacity', 'Line Group ID', and 'Incoming Number' fields. The 'Incoming Number' field is set to '5528811241'. Other fields like 'Incoming Sub Address', 'Incoming CLI', 'Locale', 'Priority', 'Tag', 'Hold Music Source', and 'Ring Tone Override' are visible but not highlighted.

17 5528811241		
Standard	Voice Recording	Destinations
Bearer Capacity	Any Voice	
Line Group ID	17	
Incoming Number	5528811241	
Incoming Sub Address		
Incoming CLI		
Locale		
Priority	1 - Low	
Tag		
Hold Music Source	System Source	
Ring Tone Override	None	

- Under the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field.
- Click **OK** to commit (not shown).

The screenshot shows the Avaya IP Office configuration interface. On the left is a tree view of the system hierarchy. The 'Incoming Call Route (5)' is selected, and its sub-items are expanded, showing a list of extensions: 0, 18, 19, 17 5528811241 (highlighted with a red box), and 17. The main panel on the right displays the configuration for extension 17 5528811241. It has tabs for 'Standard', 'Voice Recording', and 'Destinations'. The 'Destinations' tab is active, showing a table with columns: 'TimeProfile', 'Destination', and 'Fallback Extension'. The table contains one row with 'Default Value' in the 'TimeProfile' column, '3040 Ext3040 H323' in the 'Destination' column, and a dropdown arrow in the 'Fallback Extension' column.

TimeProfile	Destination	Fallback Extension
Default Value	3040 Ext3040 H323	

Repeat the above procedure for each DID number assigned by Clearcom to the Enterprise.

5.8 Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used.

5.8.1 Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code** on 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 Avaya 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. Configure the following parameters:

- 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.
- Click the **OK** to commit (not shown).

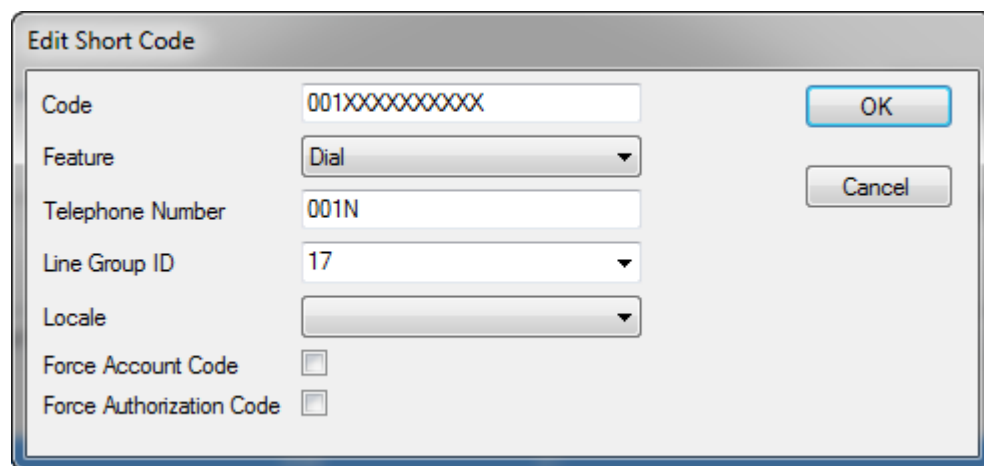
The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' navigation pane lists various system objects, with '9N' highlighted in blue. The main configuration area on the right is titled '9N: Dial' and contains the following fields:

Short Code	
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	50: Main
Locale	
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**. 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. Note that **001** is used for international calls from Mexico to North America (U.S.).
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **001N**. The value **N** represents the additional number of digits dialed by the user after dialing **001** (The **9** will be stripped off).
- Set the **Line Group Id** to the Line Group number being used for the SIP Line, in this case **Line Group ID 17** was used.
- Click OK to commit.



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

The first example highlighted below shows that for calls from Mexico to the North American Numbering Plan, the user dialed **9**, followed by **001** and **10** digits (represented by **10 Xs**). The second example highlighted shows an eight digit number starting with a **28**, which is for local calls in Mexico. The user dialed **9**, followed by the local number (e.g., 28811234). In each case the **9** is stripped off, the remaining digits, including the **001** and **28** shown in the examples below, are included in the SIP INVITE message IP Office sends to Clearcom.

IP Offices

- BOOTP (3)
- Operator (3)
- 00E00706530F
- System (1)
- Line (3)
- Control Unit (4)
- Extension (37)
- User (32)
- Group (1)
- Short Code (65)
- Service (0)
- RAS (1)
- Incoming Call Route (2)
- WAN Port (0)
- Directory (0)
- Time Profile (0)
- Firewall Profile (1)
- IP Route (6)
- Account Code (0)
- License (74)
- Tunnel (0)
- User Rights (8)
- ARS (1)**
 - 50: Main**
- RAS Location Request (0)
- Location (0)

Main

ARS

ARS Route Id: 50

Route Name: Main

Dial Delay Time: System Default (3)

☒ Secondary Dial tone

☒ Check User Call Barring

In Service: ☒ Out of Service Route: <None>

Time Profile: <None> Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
001XXXXXXXXX	001N	Dial	17
8XXXXXXXXX	8N	Dial	17
1XXXXXXXXX	1N	Dial	17
6XXXXXXXXX	6N	Dial	17
3XXXXXXXXX	3N	Dial	17
28XXXXXXXX	28N	Dial	17
55XXXXXXXX	55N	Dial	17

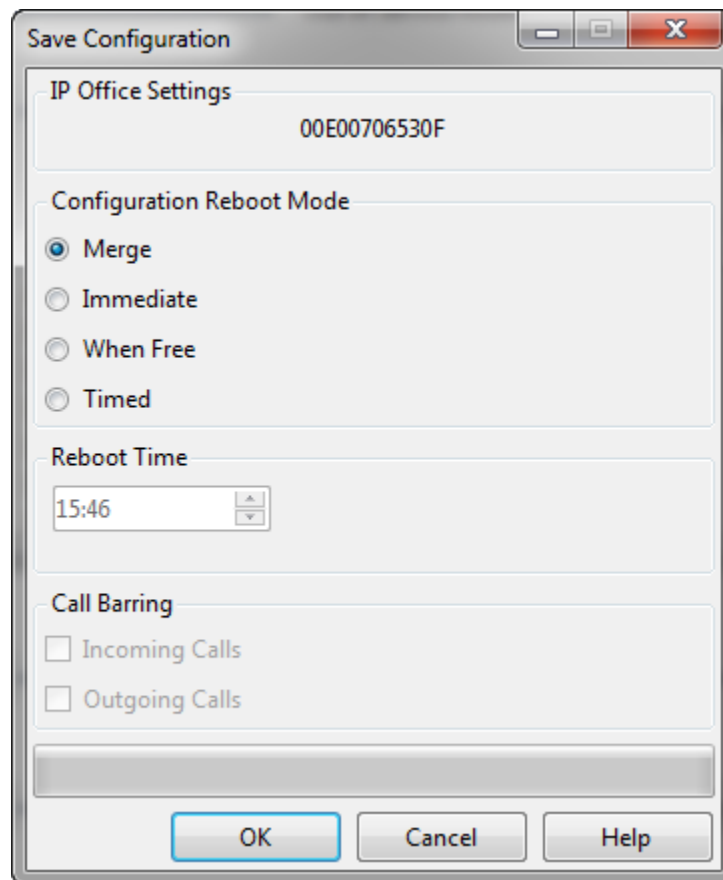
Alternate Route Priority Level: 3

5.9 Save Configuration

When desired, send the configuration changes made in Avaya IP Office Manager to the Avaya IP Office server in order for the changes to take effect.

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

Once the configuration is validated, a screen similar to the following will appear, with either the **Merge** or the **Immediate** radio button chosen based on the nature of the configuration changes made since the last save. Note that clicking OK may cause a service disruption due to system reboot. Click **OK** if desired.



The image shows a 'Save Configuration' dialog box with a title bar containing standard window controls. The dialog is divided into several sections. The first section, 'IP Office Settings', contains a text field with the value '00E00706530F'. The second section, 'Configuration Reboot Mode', contains four radio buttons: 'Merge' (selected), 'Immediate', 'When Free', and 'Timed'. The third section, 'Reboot Time', contains a time selection control showing '15:46'. The fourth section, 'Call Barring', contains two checkboxes: 'Incoming Calls' and 'Outgoing Calls', both of which are unchecked. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

6. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE)

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.

6.1 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**.



AVAYA

Log In

Username:

Password:

**Session Border Controller
for Enterprise**

WELCOME TO AVAYA SBC

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

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

© 2011 - 2016 Avaya Inc. All rights reserved.

The **Dashboard** main page will appear as shown below.

Alarms 2IncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

DashboardAdministrationBackup/RestoreSystem Management▸ Global Parameters▸ Global Profiles▸ PPM Services▸ Domain Policies▸ TLS Management▸ Device Specific Settings

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

Information

System Time	12:10:01 PM EST	Refresh
Version	7.1.0.1-07-12368	
Build Date	Fri Nov 11 09:21:54 EST 2016	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	01/06/2017 12:06:58 EST	
Failed Login Attempts	0	

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Add

Notes
No notes found.

Installed Devices

EMS

Avaya_SBCE2

To view the system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Avaya SBCE** was already added. To view the configuration of this device, click on **View** as shown in the screenshot below.

Alarms 1IncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

DashboardAdministrationBackup/RestoreSystem Management▸ Global Parameters▸ Global Profiles▸ PPM Services▸ Domain Policies▸ TLS Management▸ Device Specific Settings

System Management

DevicesUpdatesSSL VPNLicensingKey Bundles

Device Name	Management IP	Version	Status	
Avaya_SBCE		7.1.0.1-07-12368	Commissioned	RebootShutdownRestart ApplicationViewEditUninstall

HG; Reviewed:
SPOC 4/15/2017

Solution & Interoperability Test Lab Application Notes
©2017 Avaya Inc. All Rights Reserved.

42 of 96
ClearIPO10SBC71

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed as shown below.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**.

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

Encryption

☒

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

75.75.75.75

Secondary DNS

75.75.75.76

DNS Location

DMZ

DNS Client IP

10.10.80.51

Management IP(s)

IP #1 (IPv4)

On the previous screen, note that **A1** corresponds to the inside interface (Private Network side) and **B1** corresponds to the outside interface (Public Network side) of the Avaya SBCE. (Use **Figure 1** as reference for IP addresses assignments). The configuration required for Remote Worker is beyond the scope of these Application Notes and is not discussed in these Application Notes, thus IP addresses used for Remote Worker assigned to interfaces **A1** and **B1** were blurred out. The management IP address was also blurred out for security reasons.

Note: Valid public DNS IP addresses are required with this solution.

IMPORTANT! – During the Avaya SBCE installation, the Management interface (labeled “M1”) of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).

6.2 TLS Management

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

For the compliance testing, the transport protocol that was used between IP Office and the Avaya SBCE, across the enterprise private IP network (LAN), was SIP over TLS. SIP over UDP was used between the Avaya SBCE and 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 [11] in **Section 10**.

6.3 Global Profiles

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

6.3.1 Server Interworking – Avaya-IPO

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

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

On the left navigation pane, select **Global 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

Finish

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

Alarms 2
Incidents
Status
Logs
Diagnostics
Users

Session Border Controller for Enterprise

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

Interworking Profiles: Avaya-IPO

Add

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

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	No
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

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

The screenshot displays the 'Session Border Controller for Enterprise' management interface. The top navigation bar includes 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar contains a tree view with categories like 'Dashboard', 'Administration', 'System Management', 'Global Parameters', 'Global Profiles', and 'PPM Services'. Under 'Global Profiles', 'Server Interworking' is selected. The main content area is titled 'Interworking Profiles: Avaya-IPO' and features an 'Add' button. A list of profiles is shown, with 'Avaya-IPO' highlighted. The 'Advanced' tab is active, displaying a table of settings for the selected profile.

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				
DTMF					
DTMF Support	None				

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

6.3.2 Server Interworking - SP-General

A second Server Interworking profile named **SP-General** was created for the service provider.

On the left navigation pane, select **Global 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 window titled "Interworking Profile" with a close button (X) in the top right corner. Inside the window, 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.

- Click **Next**.
- Click **Next** until the Advanced window is reached, then click **Finish** on the Advanced window.

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

The screenshot displays the 'Session Border Controller for Enterprise' management interface. The top navigation bar includes 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar contains a tree view with categories like 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'Domain DoS', 'Media Forking', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Global Profiles' section is expanded, showing 'Server Interworking' as the selected profile. The main content area is titled 'Interworking Profiles: SP-General' and features an 'Add' button. Below this is a list of interworking profiles: 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General' (highlighted), 'Avaya-IPO', 'Avaya-CS1000', and 'Avaya-CM'. The 'General' tab is selected, showing a table of settings for the 'SP-General' profile. The table has columns for the setting name and its value.

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	No
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

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

The screenshot displays the 'Session Border Controller for Enterprise' management interface. The top navigation bar includes 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar contains a tree view with categories like 'Dashboard', 'Administration', 'System Management', 'Global Parameters', 'Global Profiles', 'Domain DoS', 'Media Forking', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Global Profiles' section is expanded, showing 'Server Interworking' as the selected profile. The main content area is titled 'Interworking Profiles: SP-General' and features an 'Add' button. Below this is a list of interworking profiles: 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General' (highlighted), 'Avaya-IPO', 'Avaya-CS1000', and 'Avaya-CM'. To the right of the list is a configuration panel for the 'SP-General' profile. It has tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced' (selected). The 'Advanced' tab shows settings for '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), and 'DTMF Support' (None). An 'Edit' button is located at the bottom right of the configuration panel.

Alarms 2 Incidents Status Logs Diagnostics Users

Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ Domain DoS
‣ **Server Interworking**
‣ Media Forking
‣ Routing
‣ Server Configuration
‣ Topology Hiding
‣ Signaling Manipulation
‣ URI Groups
‣ SNMP Traps
‣ Time of Day Rules
‣ FGDN Groups
‣ Reverse Proxy Policy
‣ PPM Services
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings

Interworking Profiles: SP-General

Add

Interworking Profiles

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

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	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No

DTMF

DTMF Support	None
--------------	------

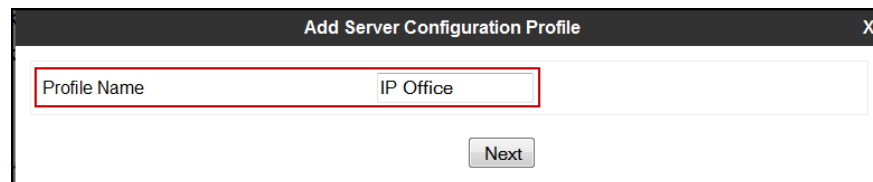
Edit

6.3.3 Server Configuration

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 profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** (not shown). Click **Add Profile** (not shown) and enter the profile name: **IP Office**.

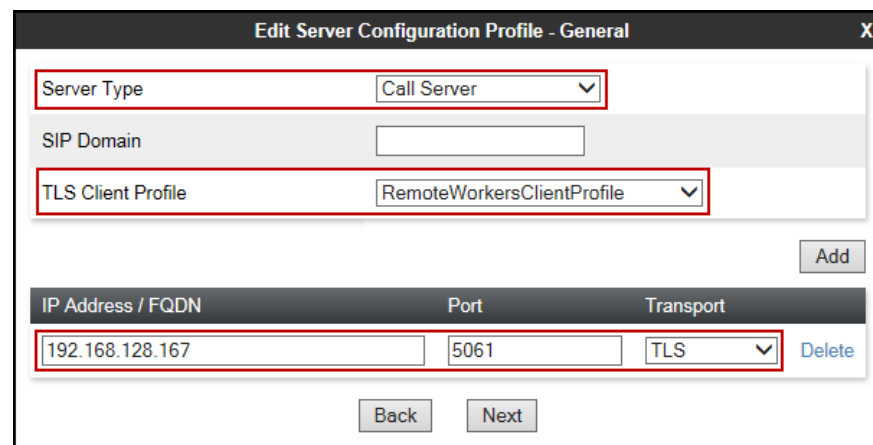
- Click **Next**.



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 "IP Office". Below this field is a "Next" button.

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

- **Server Type:** Select **Call Server**.
- **TLS Client Profile:** Select the appropriate **TLS Client Profile**.
- **IP Address / FQDN:** **192.168.128.167** (IP Address of IP Office).
- **Port:** **5061** (This port must match the port number defined in **Section 5.4.4**).
- **Transports:** Select **TLS**.
- Click **Next**



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General". It has a close button (X) in the top right corner. The dialog contains several fields: "Server Type" is a dropdown menu set to "Call Server"; "SIP Domain" is an empty text field; "TLS Client Profile" is a dropdown menu set to "RemoteWorkersClientProfile"; "IP Address / FQDN" is a text field containing "192.168.128.167"; "Port" is a text field containing "5061"; and "Transport" is a dropdown menu set to "TLS". There is an "Add" button to the right of the "TLS Client Profile" field. At the bottom, there are "Back" and "Next" buttons. A "Delete" button is also visible next to the "Transport" dropdown.

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

On the **Add Server Configuration Profile - Advanced** window:

- Select **Avaya-IPO** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile **Avaya-IPO**

Signaling Manipulation Script **None**

Securable ☐

Enable FGDN ☐

TCP Failover Port 5060

TLS Failover Port 5061

Back Finish

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

Session Border Controller for Enterprise

Alarms 1 Incidents Status Logs Diagnostics Users Settings Help Log Out

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

Server Configuration: IP Office

Add Rename Clone Delete

Server Profiles Com Manager CS1000 Session Mana... IP Office Service Provid... Service Provid...

General Authentication Heartbeat Advanced

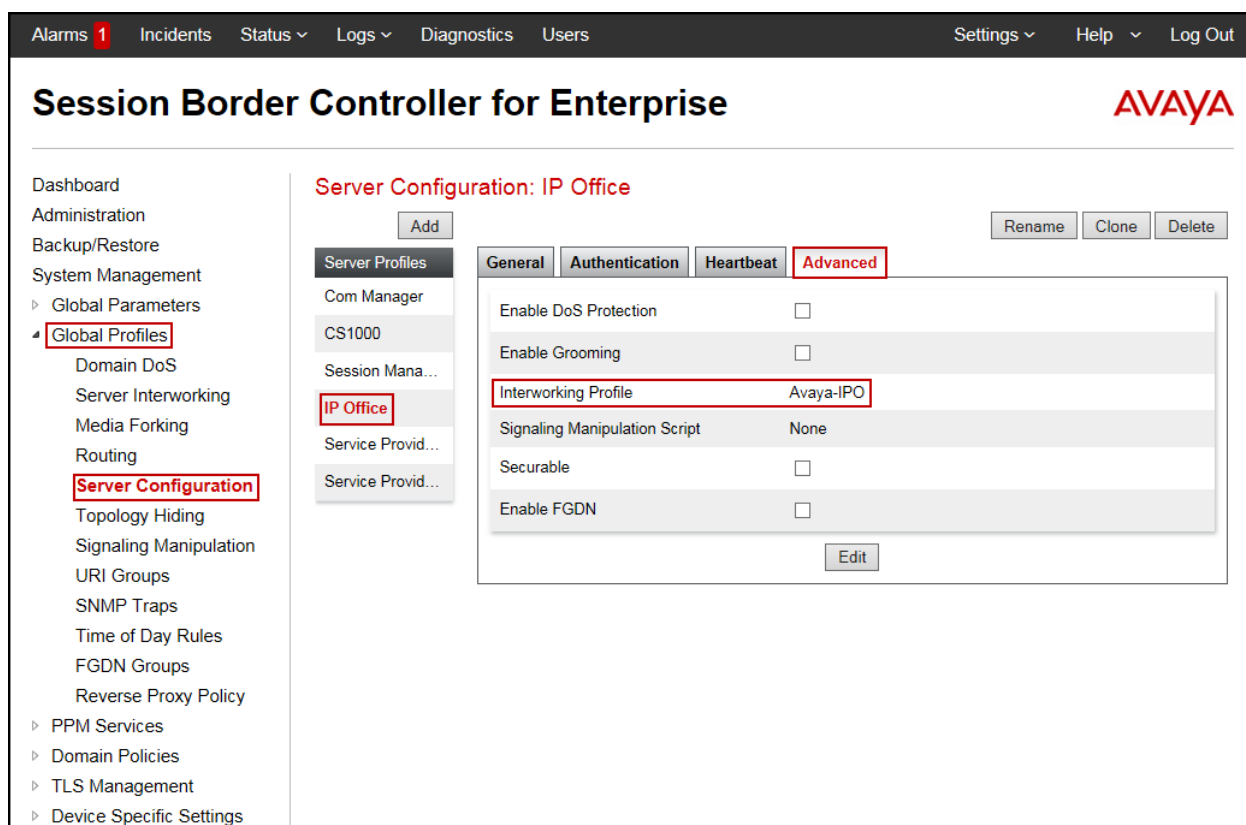
Server Type Call Server

TLS Client Profile RemoteWorkersClientProfile

IP Address / FQDN	Port	Transport
192.168.128.167	5061	TLS
192.168.128.167	5060	TCP
192.168.128.167	5060	UDP

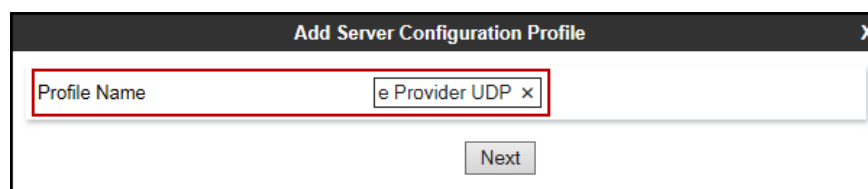
Edit

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



To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** (not shown) section and enter the profile name: **Service Provider UDP**.

- Click **Next**.



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

- **Server Type:** Select **Trunk Server**.
- **IP Address / FQDN:** **sip.clearcom.mx** (Clearcom's SIP proxy server FQDN).
- **Port:** **5060**.
- **Transports:** Select **UDP**.
- Click **Next**.

Edit Server Configuration Profile - General

Server Type: Trunk Server

SIP Domain:

TLS Client Profile: None

Add

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

Delete

Back Next

On the **Authentication** tab:

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

Add Server Configuration Profile - Authentication

Enable Authentication: ☒

User Name: User123

Realm: Clearcom.mx
(Leave blank to detect from server challenge)

Password:

Confirm Password:

Back Next

On the **Heartbeat** tab:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **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 the service provider. **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 the Service Provider'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 the Service Provider Proxy Provider's domain name (**clearcom.mx**), as shown on the screen below.
 - Click **Next**.

The screenshot shows a window titled "Add Server Configuration Profile - Heartbeat". Inside, there are several configuration fields. A red rectangular box highlights the following fields: "Enable Heartbeat" (with a checked checkbox), "Method" (a dropdown menu showing "REGISTER"), "Frequency" (a text box with "120" and "seconds" next to it), "From URI" (a text box with "User123@clearcom.mx"), and "To URI" (a text box with "er123@clearcom.mx" and a small 'x' icon). Below these fields are two buttons: "Back" and "Next".

On the **Add Server Configuration Profile - Advanced** window:

- Select **SP-General** from the **Interworking Profile**.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile **SP-General**

Signaling Manipulation Script **None**

Securable ☐

Enable FGDN ☐

TCP Failover Port 5060

TLS Failover Port 5061

Back Finish

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

Session Border Controller for Enterprise AVAYA

Alarms 1 Incidents Status Logs Diagnostics Users Settings Help Log Out

Dashboard
Administration
Backup/Restore
System Management
▸ Global Parameters
▸ **Global Profiles**
 Domain DoS
 Server Interworking
 Media Forking
 Routing
 Server Configuration
 Topology Hiding
 Signaling Manipulation
 URI Groups
 SNMP Traps
 Time of Day Rules
 FGDN Groups
 Reverse Proxy Policy
▸ PPM Services
▸ Domain Policies
▸ TLS Management
▸ Device Specific Settings

Server Configuration: Service Provider UDP

Add Rename Clone Delete

Server Profiles
Com Manager
CS1000
Session Mana...
IP Office
Service Provid...
Service Provi...

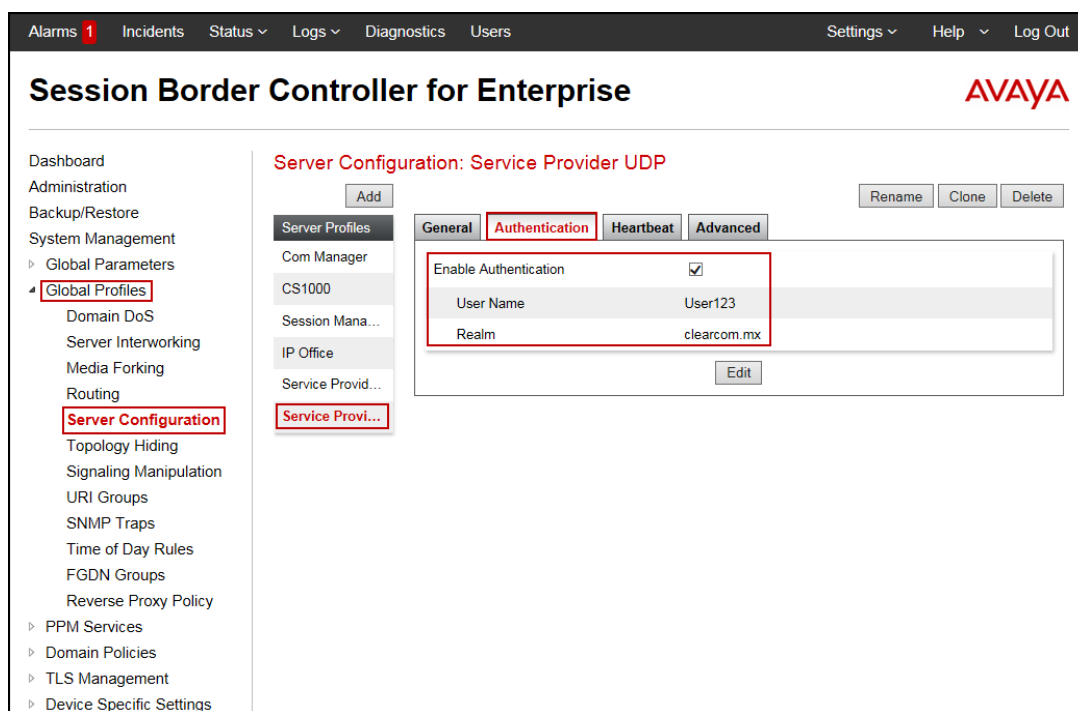
General Authentication Heartbeat Advanced

Server Type Trunk Server

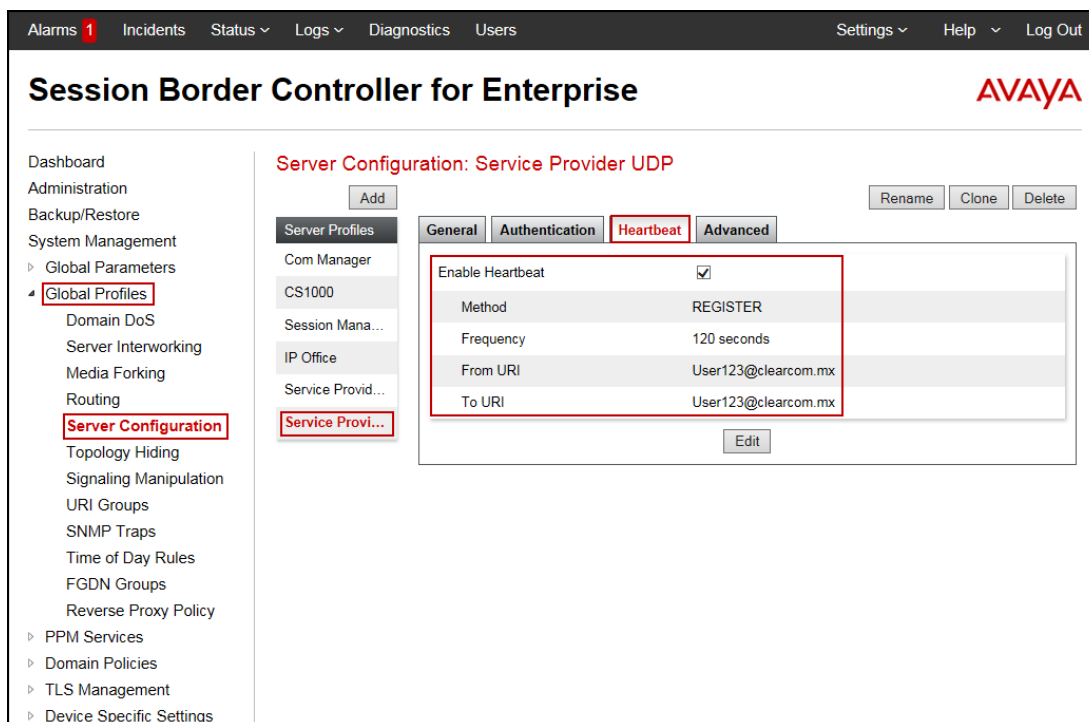
IP Address / FQDN	Port	Transport
sip.clearcom.mx	5060	UDP

Edit

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



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



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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms (1), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various configuration categories, with 'Server Configuration' highlighted. The main content area is titled 'Server Configuration: Service Provider UDP' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced', with 'Advanced' being the active tab. The 'Advanced' tab contains a table with the following settings:

Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>

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

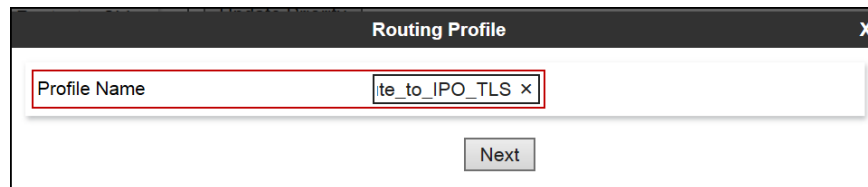
6.3.4 Routing Profiles

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

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

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

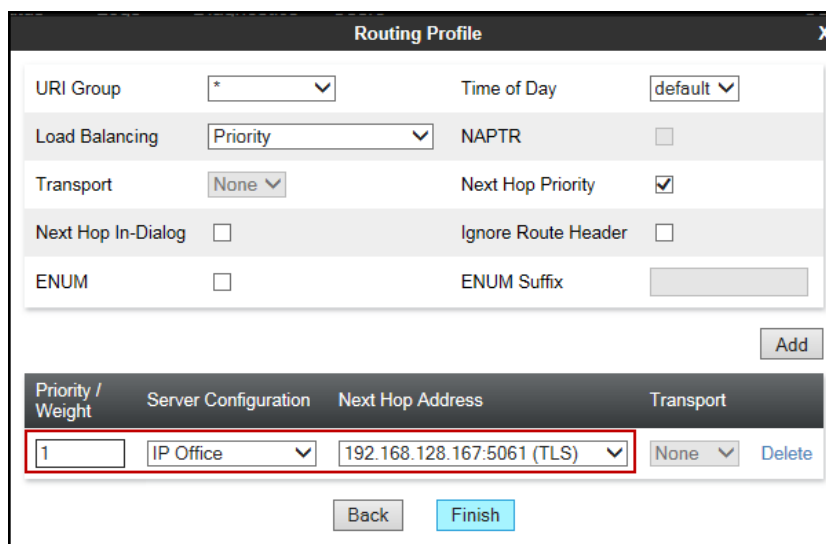
- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route_to_IPO_TLS**.
- Click **Next**.



The screenshot shows a 'Routing Profile' window. The 'Profile Name' field contains 'te_to_IPO_TLS' with a small 'x' icon to its right. Below the field is a 'Next' button.

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

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **IP Office**.
- The **Next Hop Address** is populated automatically with **192.168.128.167:5061 (TLS)** (IP Office IP address, Port and Transport).
- Click **Finish**.



The screenshot shows the 'Routing Profile' window with various configuration options. The 'Add' button is visible. Below the configuration options is a table with one entry. The table has four columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', and 'Transport'. The entry has a value of '1' in the first column, 'IP Office' in the second, '192.168.128.167:5061 (TLS)' in the third, and 'None' in the fourth. There is a 'Delete' button next to the entry. At the bottom are 'Back' and 'Finish' buttons.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	IP Office	192.168.128.167:5061 (TLS)	None

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 Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various configuration categories, with 'Routing' highlighted under 'Global Profiles'. The main content area is titled 'Routing Profiles: Route_to_IPO_TLS'. It features a list of routing profiles on the left, including 'default', 'Route_to_SM', 'Route_to_CM', 'Route_to_IPO...', 'To SM from R...', 'To IPO from R...', 'Route_to_IPO...', 'Route_to_SP...', 'Route_to_CS1...', and 'Route_to_SP...'. The 'Route_to_IPO...' profile is selected. On the right, the configuration details for the selected profile are shown. A table lists the routing profile's parameters: Priority (1), URI Group (*), Time of Day (default), Load Balancing (Priority), Next Hop Address (192.168.128.167), and Transport (TLS). The table also includes 'Edit' and 'Delete' buttons for each row. Above the table, there are buttons for 'Add', 'Update Priority', 'Rename', 'Clone', and 'Delete'.

Similarly, for the outbound route:

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

The screenshot shows a 'Routing Profile' configuration dialog box. It has a title bar with 'Routing Profile' and a close button (X). The main area contains a 'Profile Name' label and a text input field. The input field contains the text 'ite_to_SP_UDP x'. Below the input field is a 'Next' button.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Load Balancing:** Select **DNS/SRV**.
- **Priority / Weight:** **1**
- **Server Configuration:** 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**.

Routing Profile

URI Group: * Time of Day: default

Load Balancing: DNS/SRV NAPTR: ☐

Transport: None Next Hop Priority: ☐

Next Hop In-Dialog: ☐ Ignore Route Header: ☐

ENUM: ☐ ENUM Suffix:

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Service Provider	sip.clearcom.mx:5060 (UDP)	None

Back Finish

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

Alarms 1 Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise AVAYA

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

Routing Profiles: Route_to_SP_UDP

Add Rename Clone Delete

Click here to add a description.

Routing Profile

Update Priority Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	DNS/SRV	sip.clearcom.mx	UDP

Edit Delete

6.3.5 Topology Hiding

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

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

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

Alarms 1 Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Dashboard
Administration
Backup/Restore
System Management
▸ Global Parameters
▾ **Global Profiles**
 Domain DoS
 Server Interworking
 Media Forking
 Routing
 Server Configuration
 Topology Hiding
 Signaling Manipulation
 URI Groups
 SNMP Traps
 Time of Day Rules
 FGDN Groups
 Reverse Proxy Policy
▸ PPM Services

Topology Hiding Profiles: IP Office

Add Rename Clone Delete

Topology Hiding Profiles
default
cisco_th_profile
Session_Manager
Service_Provider
Com Manager
CS1000
IP Office

Click here to add a description.

Topology Hiding

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

Edit

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

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Clone 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	
Referred-By	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	clearcom.mx	Delete
To	IP/Domain	Overwrite	clearcom.mx	Delete
Via	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	clearcom.mx	Delete
Record-Route	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms 1', '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: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (highlighted), Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, FGDN Groups, Reverse Proxy Policy, and PPM Services.

The main content area is titled 'Topology Hiding Profiles: Service_Provider'. It features an 'Add' button and a list of profiles: default, cisco_th_profile, Session_Manager, Service_Provider (highlighted), Com Manager, CS1000, and IP Office. The 'Service_Provider' profile is selected, showing a table of topology hiding rules.

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

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

6.4 Domain Policies

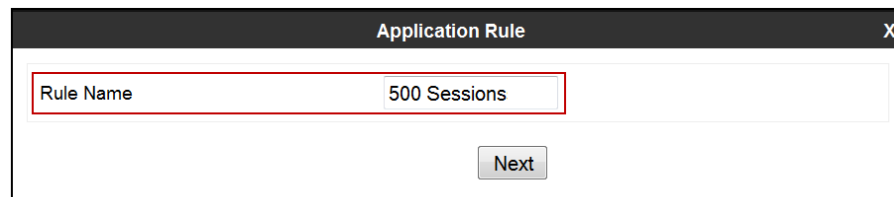
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

6.4.1 Application Rules

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

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

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



The screenshot shows a web-based configuration window titled "Application Rule". It features a text input field with the label "Rule Name" and the value "500 Sessions". A "Next" button is positioned below the input field.

- 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 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: ☒ None ☐ CDR w/o RTP

RTCP Keep-Alive: ☐

Back Finish

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

Alarms 1 Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ PPM Services
‣ **Domain Policies**
‣ **Application Rules**
‣ Border Rules
‣ Media Rules
‣ Security Rules
‣ Signaling Rules
‣ End Point Policy Groups
‣ Session Policies
‣ TLS Management
‣ Device Specific Settings

Application Rules: 500 Sessions

Add Filter By Device... Rename Clone Delete

Click here to add a description.

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: None

RTCP Keep-Alive: No

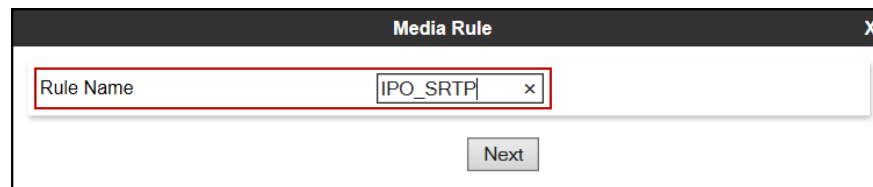
Edit

6.4.2 Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, two media rules (shown below) were used; one toward IP Office and one toward the Service Provider.

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

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



The screenshot shows a dialog box titled "Media Rule" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Rule Name" which contains the text "IPO_SRTP". To the right of the input field is a small "x" icon. Below the input field is a "Next" button.

- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **SRTP_AES_CM_128_HMAC_SHA1_32**.
- Under Audio Encryption, **Preferred Format #3**, 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 SRTP_AES_CM_128_HMAC_SHA1_32, Preferred Format #3 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. Red boxes highlight these specific settings. At the bottom, there are 'Back' and 'Next' buttons.

Audio Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	SRTP_AES_CM_128_HMAC_SHA1_32
Preferred Format #3	RTP
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	SRTP_AES_CM_128_HMAC_SHA1_32
Preferred Format #3	RTP
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	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.

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

The left sidebar contains a tree view of system management options, with 'Media Rules' highlighted under 'Domain Policies'. The main content area is titled 'Media Rules: IPO_SRTP' and features a list of media rules on the left, including 'default-low-med', 'default-low-m...', 'default-high', 'default-high-enc', 'avaya-low-me...', 'Rem_Workers...', 'IPO_SRTP', 'ServiceProvid...', and 'SM_SRTP'. The 'IPO_SRTP' rule is selected.

The configuration for the 'IPO_SRTP' rule is shown in the 'Encryption' tab. The 'Audio Encryption' section includes the following settings:

- Preferred Formats: SRTP_AES_CM_128_HMAC_SHA1_80, SRTP_AES_CM_128_HMAC_SHA1_32, RTP
- Encrypted RTCP: ☐
- MKI: ☐
- Lifetime: Any
- Interworking: ☒

The 'Video Encryption' section includes the following settings:

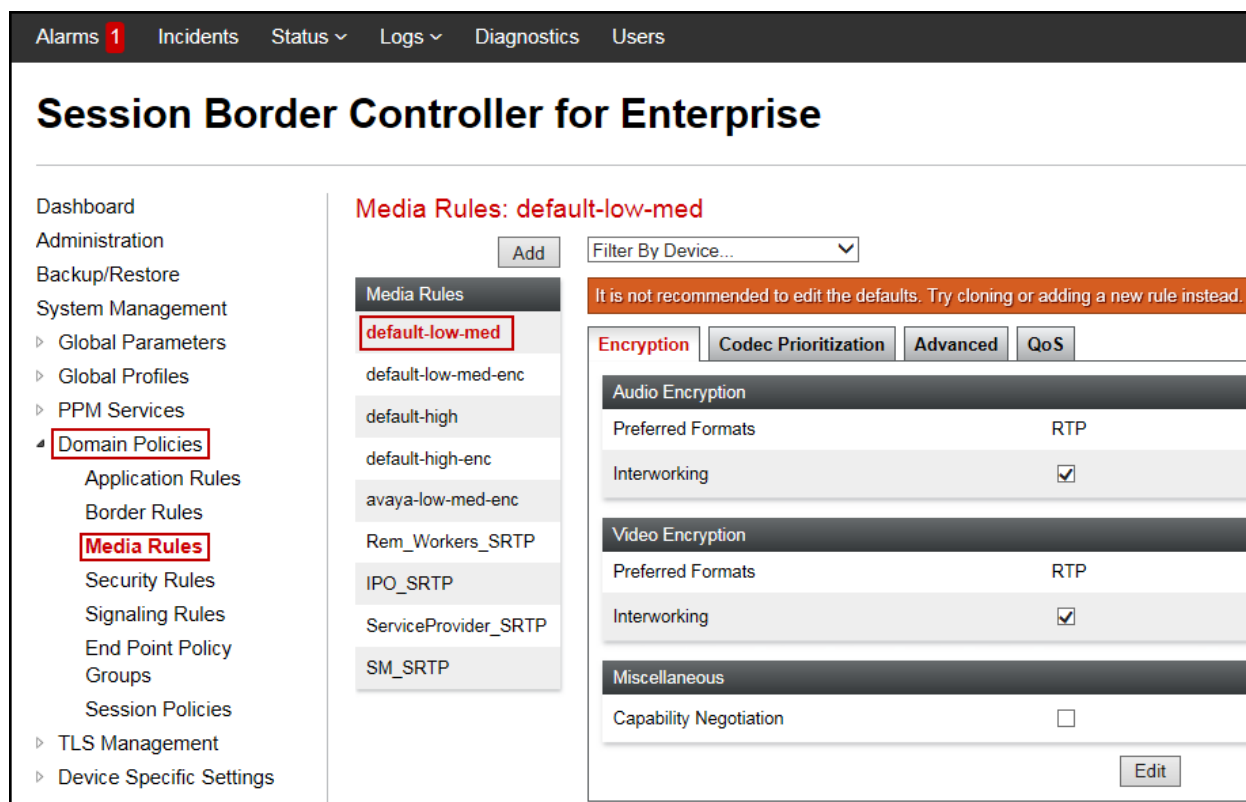
- Preferred Formats: SRTP_AES_CM_128_HMAC_SHA1_80, SRTP_AES_CM_128_HMAC_SHA1_32, RTP
- Encrypted RTCP: ☐
- MKI: ☐
- Lifetime: Any
- Interworking: ☒

The 'Miscellaneous' section includes the following settings:

- Capability Negotiation: ☒

In the Service Provider direction, the existing **default-low-med** Media Rule was used.

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



6.4.3 End Point Policy Groups

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

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

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



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

Policy Group

Application Rule: 500 Sessions

Border Rule: default

Media Rule: IPO_SRTP

Security Rule: default-low

Signaling Rule: default

Back Finish

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

Session Border Controller for Enterprise

Alarms 1 Incidents Status Logs Diagnostics Users Settings Help Log Out

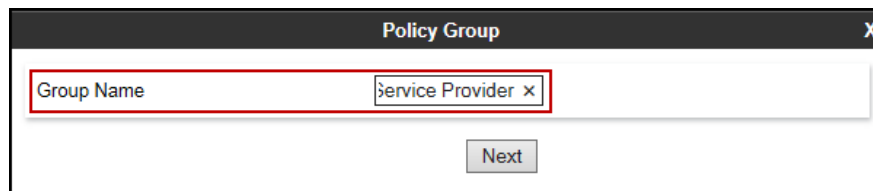
Policy Groups: IPO SRTP

Policy Groups

Order	Application	Border	Media	Security	Signaling
1	500 Sessions	default	IPO_SRTP	default-low	default

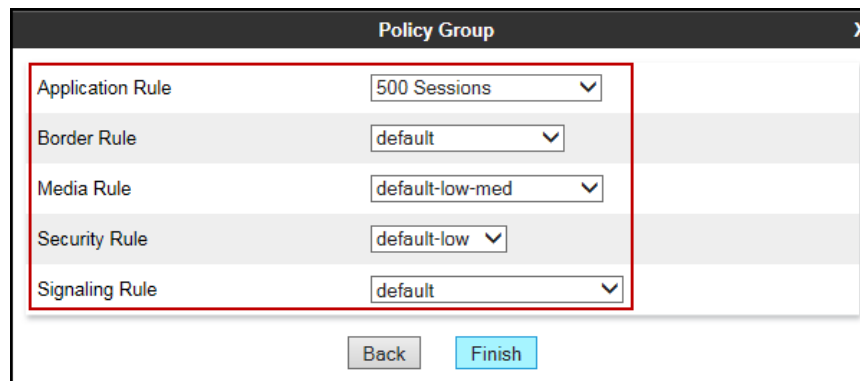
Similarly, to create an End Point Policy Group toward the Service Provider.

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



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" which contains the text "Service Provider x". A red rectangular box highlights this input field. Below the input field, there is a "Next" button.

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



The screenshot shows the same "Policy Group" dialog box. This time, several dropdown menus are visible and highlighted with a red rectangular box. The dropdowns are labeled "Application Rule", "Border Rule", "Media Rule", "Security Rule", and "Signaling Rule". The selected values are "500 Sessions", "default", "default-low-med", "default-low", and "default" respectively. At the bottom of the dialog, there are two buttons: "Back" and "Finish". The "Finish" button is highlighted in blue.

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

Alarms 1IncidentsStatus ▾Logs ▾DiagnosticsUsers

Settings ▾Help ▾Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▸ Global Profiles

▸ PPM Services

▸ Domain Policies

▸ Application Rules

▸ Border Rules

▸ Media Rules

▸ Security Rules

▸ Signaling Rules

▸ End Point Policy Groups

▸ Session Policies

▸ TLS Management

▸ Device Specific Settings

Policy Groups: Service Provider

Add

Filter By Device...

Rename

Clone

Delete

Policy Groups

default-low

default-low-enc

default-med

default-med-enc

default-high

default-high-enc

OCS-default-high

avaya-def-low-enc

avaya-def-high-subs...

avaya-def-high-server

Enterprise

Service Provider

Rem Workers Inside

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	
1	500 Sessions	default	default-low-med	default-low	default	Edit

HG; Reviewed:
SPOC 4/15/2017

Solution & Interoperability Test Lab Application Notes
©2017 Avaya Inc. All Rights Reserved.

73 of 96
ClearIPO10SBC71

6.5 Device Specific Settings

The **Device Specific 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.

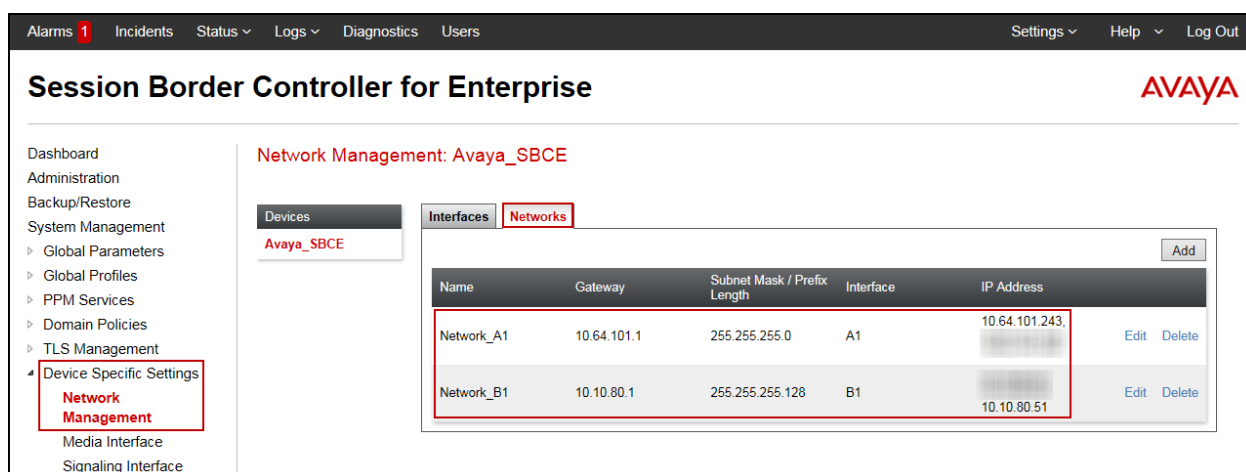
6.5.1 Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** under **Device Specific Settings** on the left hand side, select **Network Management**. Select the **Network Configuration** 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.

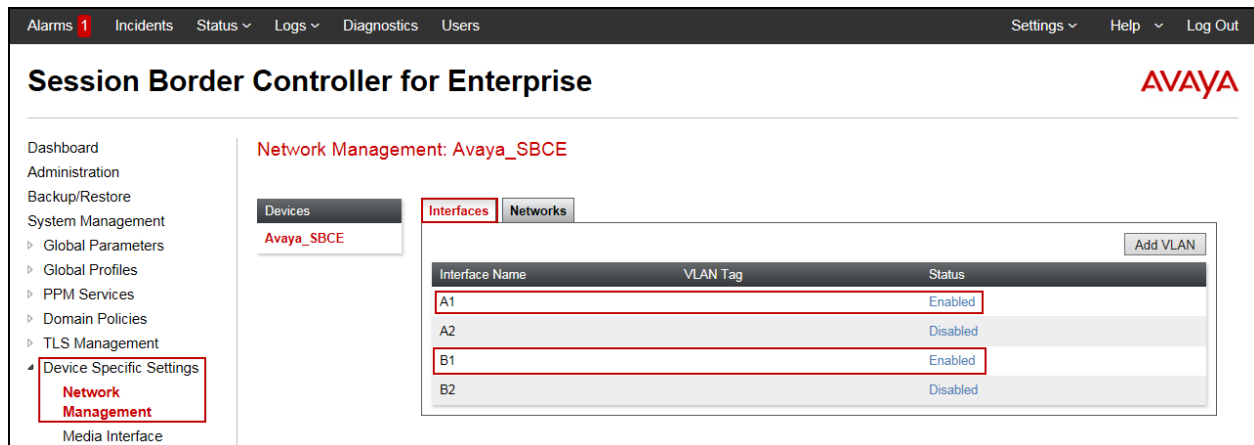
Note: Only the highlighted items were created for the compliance test, and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in these Application Notes.



The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) Network Management interface. The sidebar on the left contains navigation options, with 'Device Specific Settings' expanded and 'Network Management' selected. The main content area shows the 'Networks' tab, which contains a table of network configurations. The table has columns for Name, Gateway, Subnet Mask / Prefix Length, Interface, and IP Address. Two networks are listed: Network_A1 and Network_B1. The IP addresses are highlighted with a red box.

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 Interface Configuration tab, click the **Status** 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.



6.5.2 Media Interface

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

From the **Device Specific Settings** 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 or A1 IP Address of the Avaya SBCE, toward IP Office)
- **Port Range:** **35000-40000**.
- Click **Finish**.

Add Media Interface

Name: Private_med

IP Address: Network_A1 (A1, VLAN 0)

Port Range: 35000 - 40000

Finish

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** **Public_med**.
- Under **IP Address** select: **Network_B1 (B1, VLAN 0)**.
Select **IP Address:** **10.10.80.51** (Outside public IP Address of the Avaya SBCE, toward Clearcom).
- **Port Range:** **35000-40000**.
- Click **Finish**.

The following screen capture shows the newly created Media Interfaces.

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

6.5.3 Signaling Interface

To create the Signaling Interface toward IP Office, from the **Device Specific** 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 or A1 IP Address of the Avaya SBCE, toward IP Office).
- **TLS Port:** **5061**.
- Under **TLS Profile** select the appropriate TLS Profile.
- Click **Finish**.

Add Signaling Interface X

Name: Private_sig

IP Address: Network_A1 (A1, VLAN 0) 10.64.101.243

TCP Port: Leave blank to disable

UDP Port: Leave blank to disable

TLS Port: 5061 Leave blank to disable

TLS Profile: RemoteWorkerServerProfile

Enable Shared Control: ☐

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/public IP Address of the Avaya SBCE, toward Clearcom).
- **UDP Port:** **5060**.
- Click **Finish**.

Add Signaling Interface

Name: Public_sig

IP Address: Network_B1 (B1, VLAN 0) 10.10.80.51

TCP Port: Leave blank to disable

UDP Port: 5060

TLS Port: Leave blank to disable

TLS Profile: None

Enable Shared Control: ☐

Shared Control Port:

Finish

The following screen capture shows the newly created Signaling Interfaces.

Session Border Controller for Enterprise AVAYA

Alarms 1 Incidents Status Logs Diagnostics Users Settings Help Log Out

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
DMZ Services

Signaling Interface: Avaya_SBCE

Devices: Avaya_SBCE

Signaling Interface

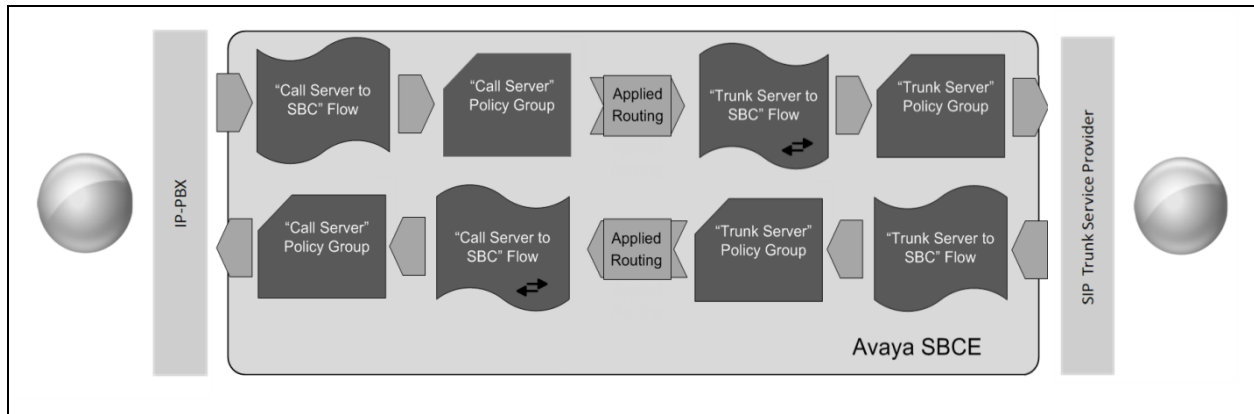
Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add

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)	---	---	5061	RemoteWorkerServerProfile	Edit	Delete
Public_sig	10.10.80.51 Network_B1 (B1, VLAN 0)	---	5060	---	None	Edit	Delete

6.5.4 End Point Flows

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



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

To create the call flow toward Clearcom, from the **Device Specific Settings** 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.
- **Signaling Manipulation Script:** None.
- **Remote Branch Office:** Any.
- Click **Finish**.

Edit Flow: SIP_Trunk_Flow_UDP	
Flow 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
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

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

- **Name:** IP_Office_Flow.
- **Server Configuration:** IP Office.
- **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:** IPO SRTP.
- **Routing Profile:** Route_to_SP_UDP (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** IP Office.
- **Signaling Manipulation Script:** None.
- **Remote Branch Office:** Any.
- Click **Finish**.

Flow Name: IP_Office_Flow

Server Configuration: IP Office

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: IPO SRTP

Routing Profile: Route_to_SP_UDP

Topology Hiding Profile: IP Office

Signaling Manipulation Script: None

Remote Branch Office: Any

Finish

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for 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 "Device Specific Settings" menu is expanded, and "End Point Flows" is highlighted. The main content area is titled "End Point Flows: Avaya_SBCE". It features a tabbed interface with "Subscriber Flows" and "Server Flows" tabs. The "Server Flows" tab is active, showing a table of configured flows.

The table lists three server configurations:

- Server Configuration: IP Office**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IP_Office_Flow	*	Public_sig	Private_sig	IPO SRTP	Route_to_SP_UDP	View Clone Edit Delete
- Server Configuration: 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
- Server Configuration: Session Manager**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
							View Clone Edit Delete

7. Clearcom SIP Trunking Service Configuration

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

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

Clearcom is responsible for the configuration of Clearcom SIP Services. The customer will need to provide a public IP address to be used to reach the Avaya SBCE at the enterprise. In the case of the compliance test, this is the outside or public IP address of the Avaya SBCE (B1 interface). The customer will also need the IP addresses for the primary and the secondary public DNS servers, these addresses can be obtained from the local ISP in Mexico.

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

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

8. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting tips that can be used to troubleshoot the solution.

8.1 Verification Steps

The following steps may be used to verify the configuration:

- Verify that endpoints at the enterprise site can place calls to PSTN and that calls remain active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from PSTN and that calls can remain active for more than 35 seconds.
- Verify that the user on the PSTN side can end an active call by hanging up.
- Verify that an Avaya endpoint at the enterprise site can end an active call by hanging up.

8.2 Protocol Traces

The following SIP message headers are inspected using a sniffer trace analysis tool:

- Request-URI: Verify the request number and SIP domain.
- From: Verify the display name and display number.
- To: Verify the display name and display number.
- P-Asserted-Identity: Verify the display name and display number.
- Privacy: Verify privacy masking with “user, id”.
- Diversion: Verify the display name and display number.

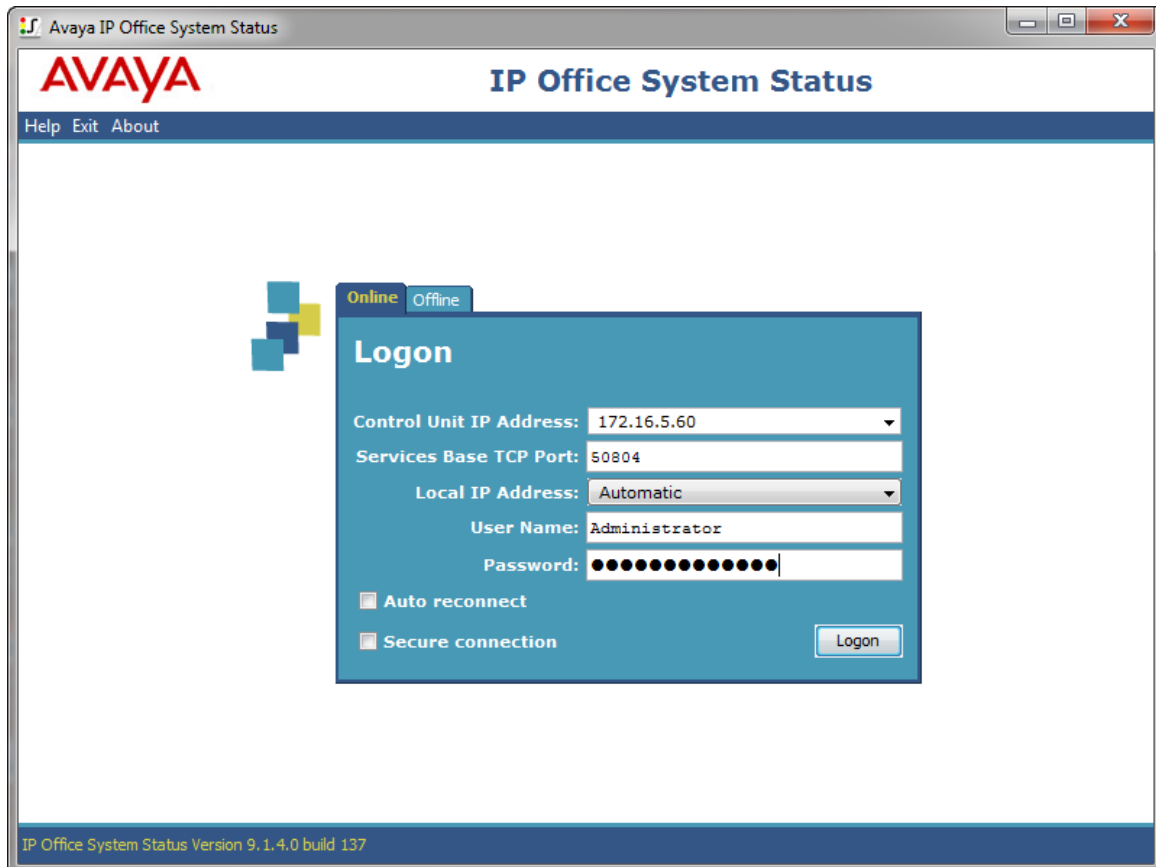
The following attributes in SIP message body are inspected using a sniffer trace analysis tool:

- Connection Information (c line): Verify IP addresses of near end and far end endpoints.
- Time Description (t line): Verify session timeout value of near end and far end endpoints.
- Media Description (m line): Verify audio port, codec, DTMF event description.
- Media Attribute (a line): Verify specific audio port, codec, ptime, send/ receive ability, DTMF events.

8.3 IP Office System Status

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

Use the Avaya 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.



1. Select the SIP Line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** is **Idle** for each channel (assuming no active calls at present time).

Avaya IP Office System Status - 00E00706530F (192.168.128.167) - IP500 V2 10.0.0.2.0 build 10

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

- System
- Alarms (21)
- Extensions (26)
- Trunks (5)
 - Line: 1
 - Line: 2
 - Line: 17
 - Line: 18
 - Line: 19
- Active Calls
- Resources
- Voicemail
- IP Networking
- Locations

Status

Utilization Summary Alarms

SIP Trunk Summary

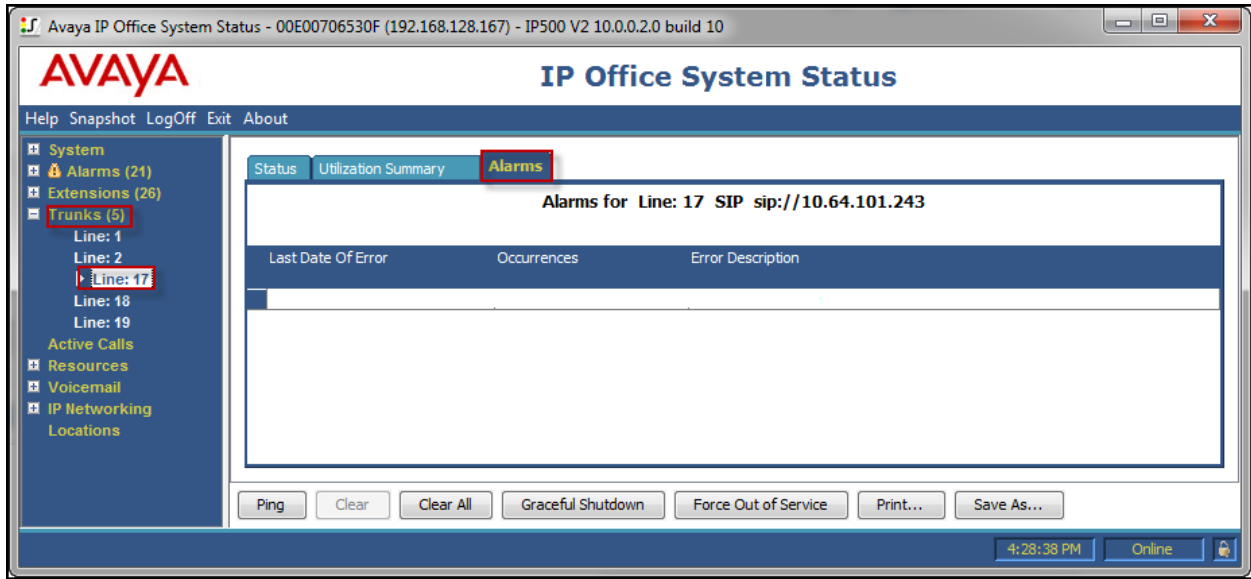
Line Service State: In Service
Peer Domain Name: sip://10.64.101.243
Resolved Address: 10.64.101.243
Line Number: 17
Number of Administered Channels: 20
Number of Channels in Use: 0
Administered Compression: G729 A, G711 Mu, G711 A
Enable Faststart: Off
Silence Suppression: Off
Media Stream: RTP
Layer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

Channel Number	U...	Call Ref	Current State	Time in State	Remote Media ...	Co...	Conn...	Caller ID or ...	Other Party on Call	Directi...	Round Trip ...	Receive Jitter	Receive Pack...	Trans...	Trans...
1			Idle	1 day ...											
2			Idle	1 day ...											
3			Idle	1 day ...											
4			Idle	1 day ...											
5			Idle	1 day ...											
6			Idle	1 day ...											
7			Idle	1 day ...											
8			Idle	1 day ...											
9			Idle	1 day ...											
10			Idle	1 day ...											
11			Idle	1 day ...											

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

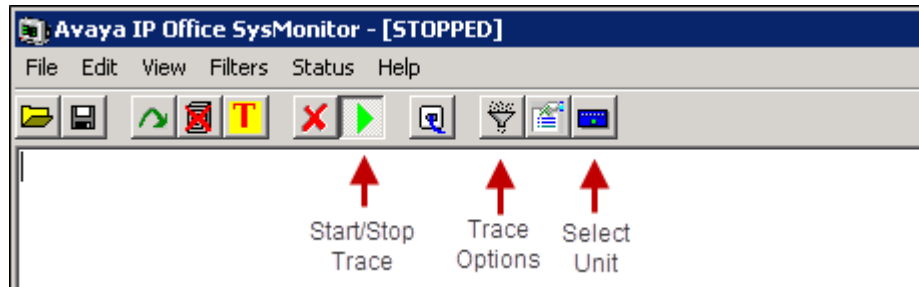
4:25:07 PM Online

2. Select the **Alarms** tab and verify that no alarms are active on the SIP Line.

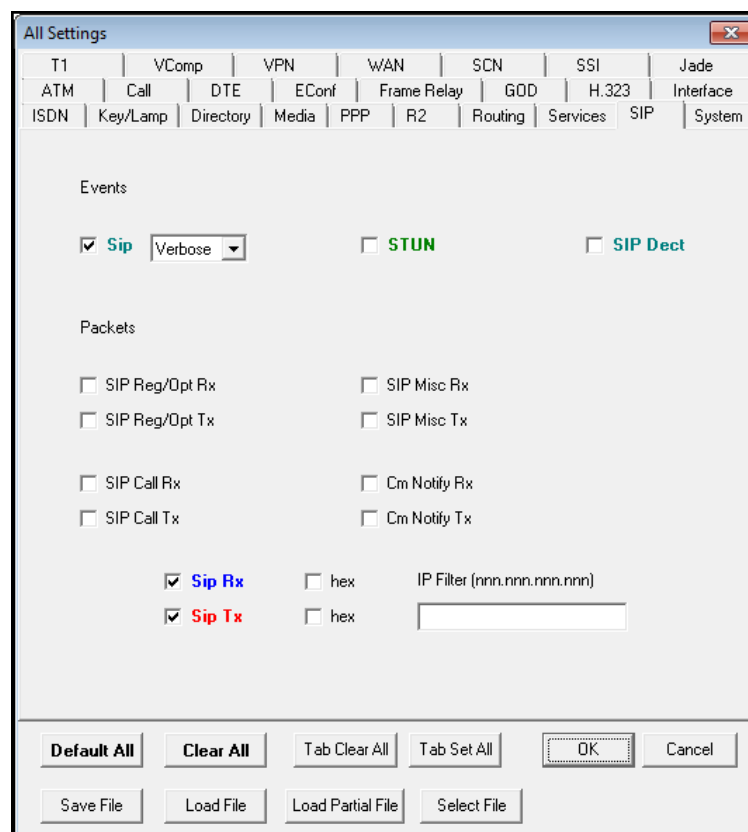


8.4 IP Office Monitor

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 Avaya 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 and 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 to the desired color.



8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE)

There are several links and menus located on the taskbar at the top of the screen of the web interface that can be used for diagnostic and troubleshooting.

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

Session Border Controller for Enterprise

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

Information	
System Time	10:15:19 AM EST Refresh
Version	7.1.0.1-07-12368
Build Date	Fri Nov 11 09:21:54 EST 2016
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	01/06/2017 15:28:20 EST
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched

[Add](#)

Notes

No notes found.

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

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.

Session Border Controller for Enterprise

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

Information

System Time	10:15:19 AM EST	Refresh
Version	7.1.0.1-07-12368	
Build Date	Fri Nov 11 09:21:54 EST 2016	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	01/06/2017 15:28:20 EST	
Failed Login Attempts	0	

Installed Devices

EMS
Avaya_SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched

Notes

No notes found.

The following screen shows the Incident Viewer page.

Incident Viewer

Device: Avaya SBCE Category: Policy Clear Filters Refresh Generate Report

Displaying results 1 to 5 out of 5.

Type	ID	Date	Time	Category	Device	Cause
Message Dropped	722182809923738	10/8/15	11:40 PM	Policy	Avaya SBCE	No Subscriber Flow Matched
Server Heartbeat	721576665666258	9/24/15	10:55 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down
Server Heartbeat	720627871533350	9/2/15	11:49 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down
Server Heartbeat	720627092366599	9/2/15	11:23 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down
Server Heartbeat	720581909185100	9/1/15	10:16 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down

<< < 1 > >>

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 **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo. The left sidebar contains a menu with categories like Dashboard, Administration, System Management, and Troubleshooting. The "Troubleshooting" category is expanded, showing "Debugging" and "Trace". The "Trace" option is selected, leading to the "Trace: Avaya_SBCE" page. This page has two tabs: "Devices" and "Packet Capture". The "Packet Capture" tab is active, displaying the "Packet Capture Configuration" window. This window is outlined with a red border and contains the following fields: Status (Ready), Interface (A1), Local Address (All), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (Wireshark_Capture_1.pcap). At the bottom of the configuration window are "Start Capture" and "Clear" buttons.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various management options, with 'Device Specific Settings' and 'Troubleshooting' expanded. The 'Trace' option under Troubleshooting is highlighted. The main content area is titled 'Trace: Avaya_SBCE' and features a 'Devices' dropdown menu set to 'Avaya_SBCE'. Two tabs, 'Packet Capture' and 'Captures', are visible, with 'Captures' being the active tab. Below the tabs is a table listing captured files. The table has columns for File Name, File Size (bytes), Last Modified, and a Delete link. Two files are listed: 'Wireshark_Capture_1_20161024173718.pcap' (135,168 bytes, Oct 24, 2016 5:37:35 PM EDT) and 'Wireshark_Capture_1_20161024173655.pcap' (8,192 bytes, Oct 24, 2016 5:37:06 PM EDT). The first file is highlighted with a red border.

File Name	File Size (bytes)	Last Modified	
Wireshark_Capture_1_20161024173718.pcap	135,168	October 24, 2016 5:37:35 PM EDT	Delete
Wireshark_Capture_1_20161024173655.pcap	8,192	October 24, 2016 5:37:06 PM EDT	Delete

9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 10 and the Avaya Session Border Controller for Enterprise Release 7.1 to support Clearcom SIP Trunking Service, as shown in **Figure 1**.

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

10. 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] *Avaya IP Office Platform Solution Description, Release 10.0.0.1*, September 2016.
- [2] *Avaya IP Office Platform Feature Description, Release 10.0*, August 2016.
- [3] *Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 30zc, March 21, 2016.
- [4] *IP Office Platform 10.0 Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 31m, 01 December 2016.
- [5] *Administering Avaya IP Office Platform with Manager, Release 10.0*, September 2016.
- [6] *IP Office Platform 10.0 Using Avaya IP Office Platform System Status*, Document 15-601758, Issue 11e, 07 July, 2016.
- [7] *IP Office Platform 10.0 Using IP Office System Monitor*, Document 15-601019, Issue 08b, 25 November, 2016.
- [8] *Using Avaya Communicator for Windows on IP Office, Release 10*, August 2016.
- [9] *Administering Avaya Communicator on IP Office, Release 10.0, Issue 01.01*, August 2016..
- [10] *Deploying Avaya Session Border Controller for Enterprise, Release 7.1, Issue 1*, June 2016.
- [11] *Administering Avaya Session Border Controller for Enterprise, Release 7.1, Issue 1*, June 2016.
- [12] *Troubleshooting and Maintaining Avaya session Border Controller for Enterprise, Release 7.1, Issue 1*, June 2016.
- [13] *Avaya IP Office Platform Security Guidelines, Release 10*. Issue 01.05, October 2015.
- [14] *IP Office Technical Bulletin number 175* (<http://www.ipofficeinfo.com/TechBulletins/tb175.pdf>)

Additional Avaya IP Office documentation can be found at:

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

©2017 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.