



Application Notes for Configuring Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 6.3 to support Alestra SIP Trunking Service on Broadsoft Platform- 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 9.1 and Avaya Session Border Controller for Enterprise Release 6.3, to interoperate with Alestra SIP Trunking Service on the Broadsoft platform.

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.

Alestra SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Alestra'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.

Alestra 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	4
2.2 Test Results	6
2.3 Support.....	6
3. Reference Configuration	7
4. Equipment and Software Validated	9
5. Configure IP Office	10
5.1 Licensing.....	11
5.2 System.....	11
5.2.1 System - LAN1 Tab	11
5.2.2 System - Telephony Tab	15
5.2.3 System - Twinning Tab.....	16
5.2.4 System - Codecs 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	23
5.4.3 SIP Line - SIP Line Tab.....	25
5.4.4 SIP Line - Transport Tab	26
5.4.5 SIP Line - SIP URI Tab	27
5.4.6 SIP Line - VoIP Tab	28
5.4.7 SIP Line – SIP Advanced Tab	29
5.5 Users	30
5.6 Incoming Call Route	31
5.6.1 Incoming Call Route – Standard Tab.....	31
5.6.2 Incoming Call Route – Destinations Tab.....	32
5.7 Outbound Call Routing	33
5.7.1 Short Codes and Automatic Route Selection.....	33
5.8 Save Configuration	36
6. Configure Avaya Session Border Controller for Enterprise	37
6.1 Log in Avaya SBCE.....	37
6.2 Global Profiles	40
6.2.1 Server Interworking – Avaya-IPO	40
6.2.2 Server Interworking - SP-General	43
6.2.3 Signaling Manipulation.....	45
6.2.4 Server Configuration.....	46
6.2.5 Routing Profiles	55
6.2.6 Topology Hiding.....	58
6.3 Domain Policies	61
6.3.1 Application Rules.....	61
6.3.2 End Point Policy Groups.....	63
6.4 Device Specific Settings	66
6.4.1 Network Management.....	66
6.4.2 Media Interface	68
6.4.3 Signaling Interface	70

6.4.4 End Point Flows	72
7. Alestra SIP Trunking Configuration	76
8. Verification and Troubleshooting	77
8.1 Verification Steps.....	77
8.2 IP Office System Status	78
8.3 IP Office Monitor.....	80
8.4 Avaya Session Border Controller for Enterprise	81
9. Conclusion	86
10. References	87
11. Appendix A: SigMa Script	88

1. Introduction

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

In the sample configuration, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office 500v2 Release 9.1 (hereafter referred to as IP Office), Avaya Session Border Controller for Enterprise Release 6.3 (hereafter referred to as Avaya SBCE), Avaya Communicator for Windows, Avaya IP Office Video Softphone and Avaya Deskphones, including SIP, H.323, digital, and analog.

Alestra SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the IP Office solution are able to place and receive PSTN calls via a broadband 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” and “Alestra” 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 Alestra’s SIP Trunking service across the public internet. The configuration in **Figure 1** was used to exercise the features and functionality tests listed in **Section 2.1**.

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

2.1 Interoperability Compliance Testing

To verify SIP Trunk interoperability, the following features and functionalities were exercised during the compliance testing:

- SIP OPTIONS queries and responses.
- Incoming calls from the PSTN were routed to the DID numbers assigned by Alestra. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x0 Series IP Deskphones (H.323), Avaya 96x1 Series IP Deskphones (H.323), Avaya 1100 Series IP Deskphones (SIP), Avaya Communicator for Windows, Avaya IP Office Video Softphone, Avaya 1400 Series Digital Deskphones, Avaya 9500 Series Digital Deskphones, and analog Deskphones.
- Outgoing calls to the PSTN were routed via Alestra’s network to various PSTN destinations.
- 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 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.711A and G.711MU, Alestra's preferred codec order).
- No matching codecs.
- Proper early media transmissions.
- Voicemail and DTMF tone support (leaving and retrieving voice mail messages from PSTN phones).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.
- T.38 and G.711 pass-through fax.

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 discussed in these Application Notes, see **References [11]**.

Items not supported or not tested included the following:

- Inbound toll-free calls, 911 calls (emergency), "0" calls (Operator), 0+10 digits calls (Operator Assisted), were not tested.

2.2 Test Results

Interoperability testing with Alestra was successfully completed with the following observations/limitations.

- **Caller ID on incoming calls from the U.S.:** Calls originating from PSTN telephones in the U.S. to DID numbers in Mexico assigned to the IP Office SIP trunk displayed a caller ID “anonymous” on the enterprise extensions. The “From” header on the INVITE of these incoming calls was “[anonymous@anonymous.invalid](#)”. This seems to be a PSTN restriction for all international inbound calls from the U.S. to Mexico, not limited just to Alestra. This behavior is not necessarily indicative of a limitation of the combined Alestra/Avaya solution, and it is listed here simply as an observation.
- **No matching codec on outbound call:** On outbound calls containing only one codec in its SDP offer that was not supported by Alestra, Alestra would reply with “480 Temporarily Unavailable”, instead of the expected “488 Not Acceptable Here”. There is no impact to the user, the user will hear error tones.
- **Caller ID on call forward to the PSTN:** For Calls from the PSTN to IP Office, that were forwarded back out to the PSTN, the caller ID number displayed at the PSTN was always of the DID number assigned to the SIP Trunk, regardless of the PSTN number being used to originate the call.
- **Caller ID display on Mobile Twinning:** For Mobile Twinning calls the Caller ID display at the mobile/cellular station was always of the DID number assigned to the SIP Trunk, regardless of the PSTN number being used to originate the call.
- **Outbound Calling Party Number (CPN) Block:** When an enterprise user activated “Withhold Number” on an outbound call, IP Office sent “anonymous” in the From header, included the “Privacy:id” header, and the complete DID number in the P-Asserted-Identity (PAI) header of the outbound INVITE, as expected. In this scenario, Alestra returned a “404 Not Found” resulting in call failure.
- **Voice quality when using codec G.729A:** During the compliance test poor voice quality was observed on calls when codec G729A was used. The voice quality was normal (good quality) when using codecs G.711A and G.711U. This condition may be limited to the testing environment and not be present in a real customer scenario. It is listed here as an observation. This observation was reported to Alestra.
- **Fax support:** Inbound and outbound fax calls using the T.38 protocol or G.711 fax pass-through mode failed during the test. The use of T.38 fax or G.711 fax pass-through is not recommended with this solution.
- **Response to OPTIONS:** During the compliance test, Alestra responded to OPTIONS messages sent from the IP Office with a “405 Method Not Allowed” message. Since the OPTIONS messages were used to check the status of the network connectivity to the service provider, any response received from Alestra was sufficient to achieve that purpose.

2.3 Support

For support on Alestra systems visit the corporate Web page at: <http://www.alestra.com.mx/>

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

3. Reference Configuration

Figure 1 below illustrates the test configuration used. It shows a simulated enterprise site connected to Alestra's network through the public internet.

For confidentiality and privacy purposes, actual public IP addresses and PSTN routable phone numbers (DIDs) used during the compliance testing have been replaced with fictitious IP addresses and PSTN non-routable phone numbers throughout the Application Notes.

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

- Avaya IP Office 500v2.
- Avaya Session Border Controller for Enterprise.
- Avaya Voicemail Pro for IP Office.
- Avaya 96x0 Series H.323 IP Deskphones.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 11x0 Series SIP IP Deskphones.
- Avaya Communicator for Windows.
- Avaya IP Office Video Softphone.
- Avaya 1408 Digital Deskphones.
- Avaya 9508 Digital Deskphones.

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 500v2 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 Alestra's network via the public Internet.

The transport protocol between the Avaya SBCE and Alestra, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network, is also SIP over UDP.

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

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

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Alestra's network (refer to **Section 5.7**). The short code 9 was stripped off by IP Office but the remaining N digits were sent unaltered to the network.

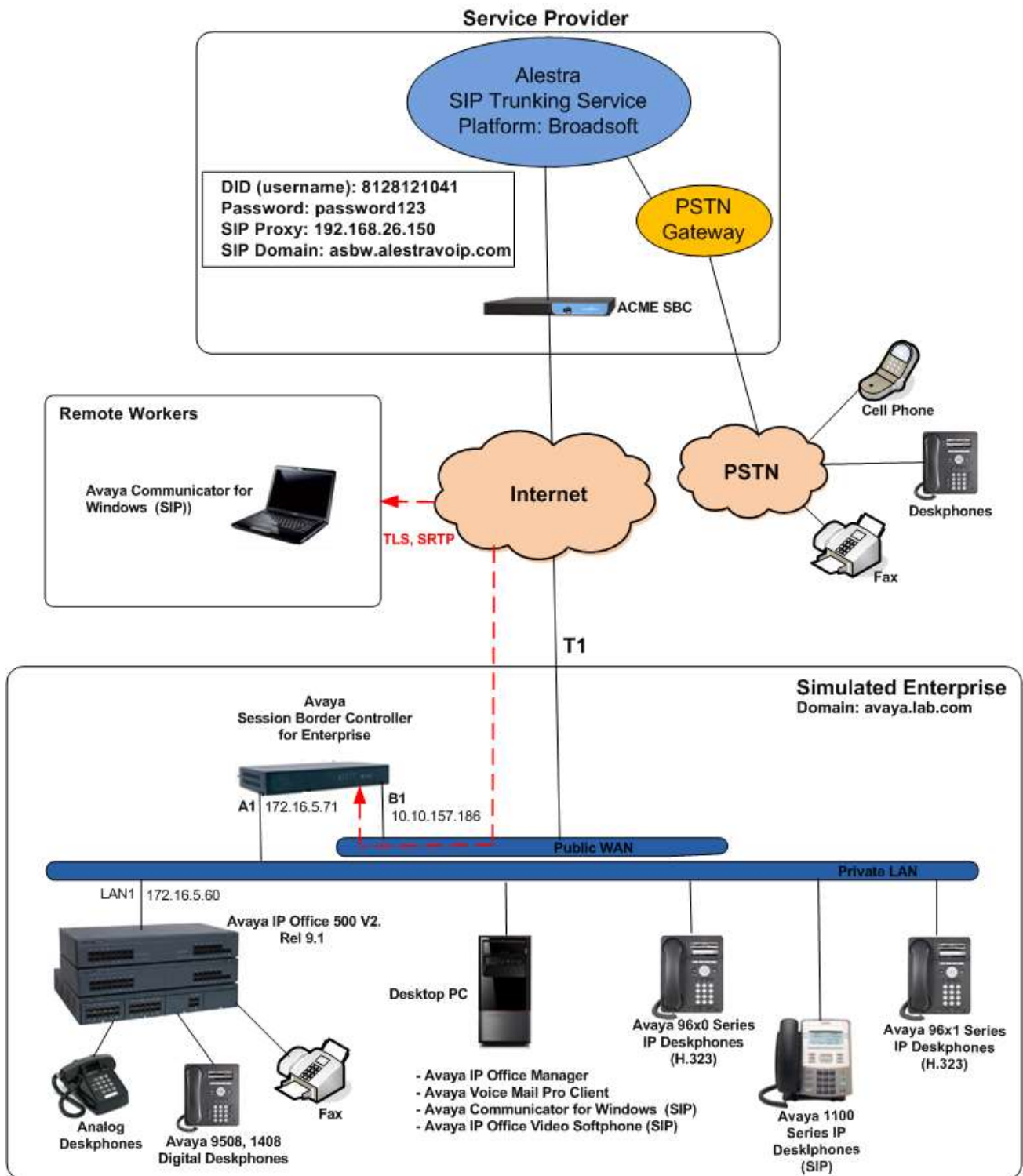


Figure 1: Avaya Interoperability Test Lab Configuration.

4. Equipment and Software Validated

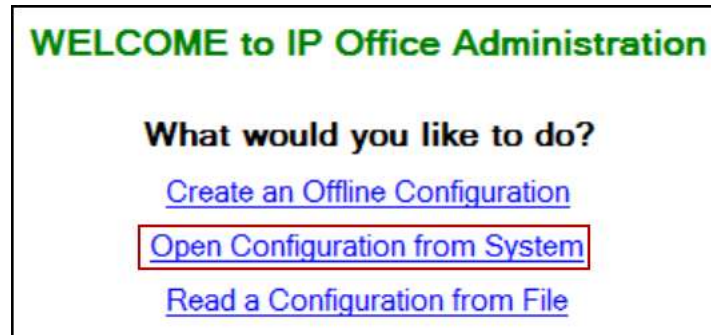
The following equipment and software/firmware were used for the sample configuration.

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	9.1.1.0 Build 10
Avaya IP Office DIG DCPx16 V2	9.1.1.0 Build 10
Avaya IP Office Manager	9.1.1.0 Build 10
Avaya Voicemail Pro Client	9.1.1.0 Build 3
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.3.1-22-4653
Avaya 96x0 IP Deskphones (H.323)	Avaya one-X® Deskphone Edition S3.230A
Avaya 96x1 Series IP Deskphones (H.323)	Avaya one-X® Deskphone H.323 Version 6.4014
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.18.00
Avaya IP Office Video Softphone	3.2.3.49 68975
Avaya Communicator for Windows	2.0.3.30
Avaya Digital Deskphones 1408	40.0
Avaya Digital Phone 9508	0.55
Lucent Analog Phone	--
Alestra	
Broadsoft Softswitch	Release 17 SP 4
Acme Packet SBC	V6.2
Lucent 5ESS	V16.1

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 without T.38 Fax Service.

5. Configure IP Office

This section describes the IP Office configuration required to interwork with Alestra. 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. A screen that includes the following may be displayed.



Select **Open Configuration from System**. If the above screen does not appear, the configuration may be alternatively opened by navigating to **File → Open Configuration** at the top of the Avaya IP Office Manager window. Select the proper IP Office from the pop-up window, and log in with the appropriate credentials.

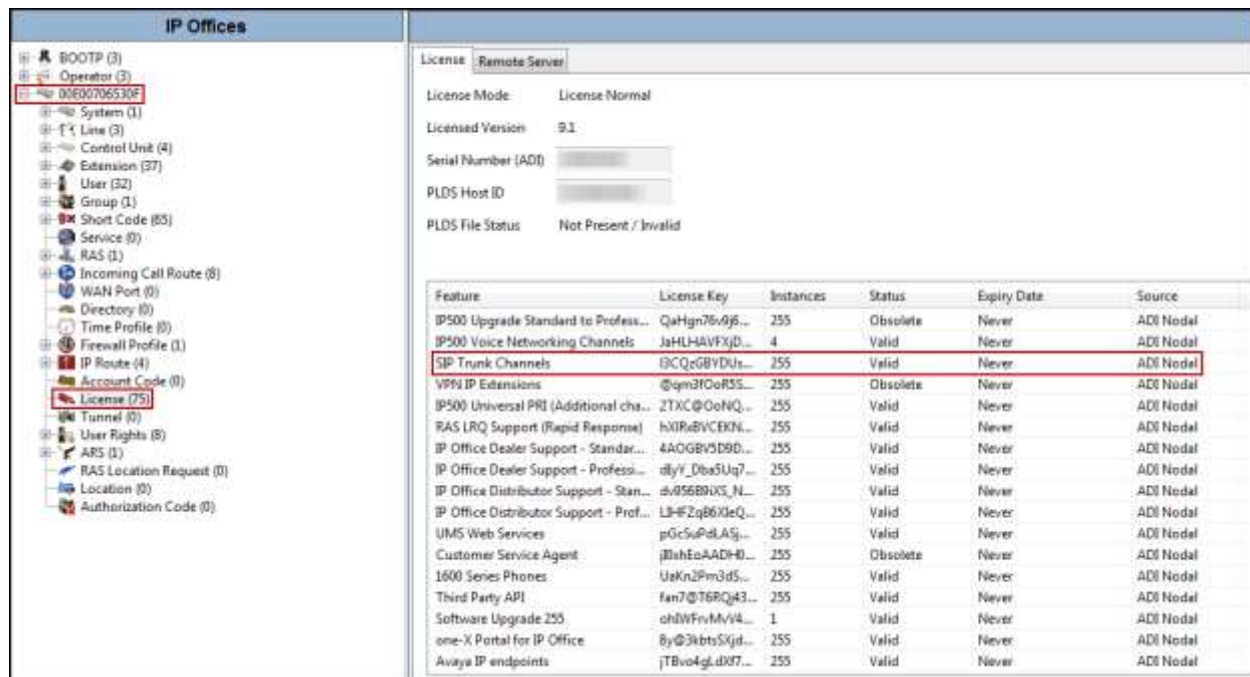
The appearance of the Avaya IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation pane on the left side, omit the Group pane in the center, and show the Details pane on the right side. Since the Group pane has been omitted, its content is shown as submenus in the Navigation pane. These panes (Navigation and Details) will be referenced throughout the IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the service provider is assumed to already be in place.

In the sample configuration, the MAC address **00E00706530F** was used as the system name. All navigation described in the following sections (e.g., **License → SIP Trunk Channels**) appears as submenus underneath the system name **00E00706530F** in the Navigation Pane.

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** in the Navigation pane and examine **SIP Trunk Channels** in the Detail pane. 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 are not shown for security purposes.



Feature	License Key	Instances	Status	Expiry Date	Source
IP500 Upgrade Standard to Profess...	QaHgn76v9j6...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	JaHLH4VFXjD...	4	Valid	Never	ADI Nodal
SIP Trunk Channels	l3CQzGBYDU...	255	Valid	Never	ADI Nodal
V999 IP Extensions	@qgn3FOuR55...	255	Obsolete	Never	ADI Nodal
IP500 Universal PRI (Additional cha...	2TXC@OoNQ...	255	Valid	Never	ADI Nodal
RAS LRQ Support (Rapid Response)	hXIRuBVCEK3...	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Standar...	4A0GBVSD9D...	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Professi...	dlyf_Dba5Uq7...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Stan...	dv956B9UXJ...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Prof...	L3-FZqB6XdeQ...	255	Valid	Never	ADI Nodal
UMS Web Services	pGc5uPdLAsj...	255	Valid	Never	ADI Nodal
Customer Service Agent	jBlahEaAADH...	255	Obsolete	Never	ADI Nodal
1600 Series Phones	UaKn2Pm3dS...	255	Valid	Never	ADI Nodal
Third Party API	fan7@T6RQ43...	255	Valid	Never	ADI Nodal
Software Upgrade 255	chWfFvMv4...	1	Valid	Never	ADI Nodal
one-X Portal for IP Office	8y@3kbtSxjd...	255	Valid	Never	ADI Nodal
Avaya IP endpoints	jTBv4gldXf7...	255	Valid	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 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 and the **LAN** port connects to the inside interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE connects to Alestra's network via the public internet. 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., **172.16.5.60**.
- Set the **IP Mask** field to the subnet mask of the enterprise private network, e.g., **255.255.255.0**.

- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' tree shows a hierarchy where 'System (1)' is expanded, and '00E00706530F' is selected. The main panel on the right is titled '00E00706530F' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', and 'System Events'. The 'LAN1' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The configuration fields are as follows:

IP Address	172 . 16 . 5 . 60
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	0 . 0 . 0 . 0
RIP Mode	None
Enable NAT	<input type="checkbox"/>
Number Of DHCP IP Addresses	200
DHCP Mode	<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dialin <input checked="" type="radio"/> Disabled

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

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

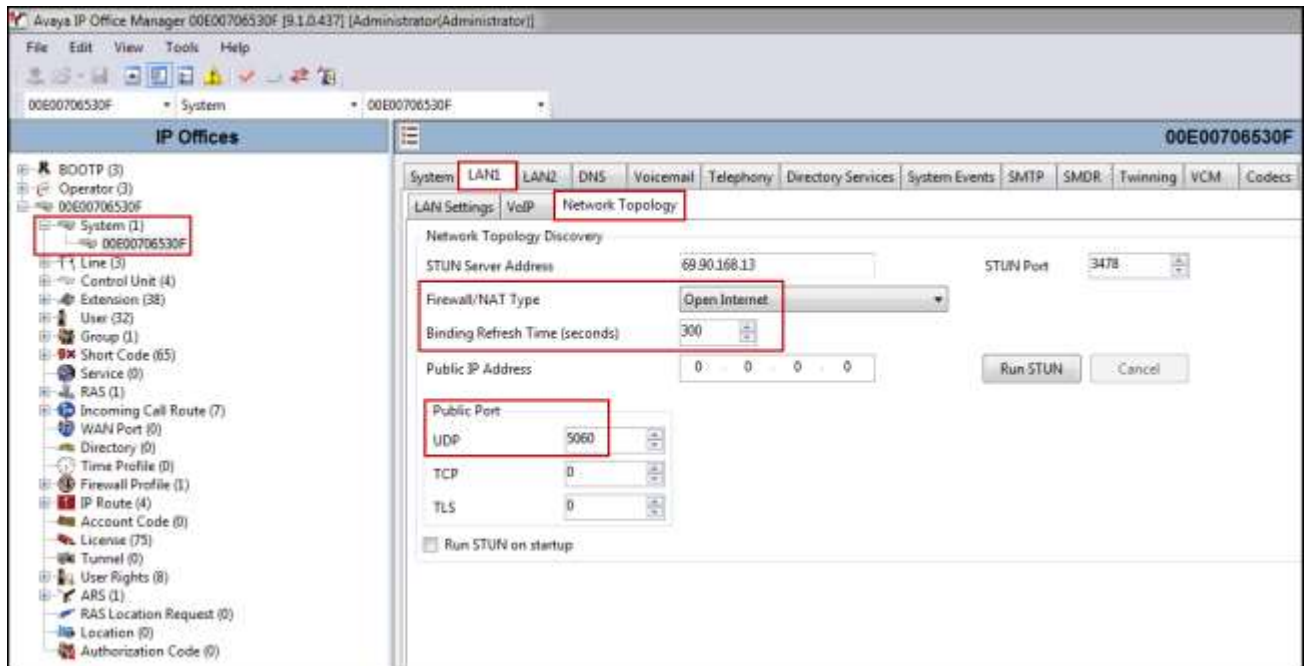
- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Alestra.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name of the enterprise under **Domain Name**.
- Verify the **UDP Port** and **TCP Port** numbers under **Layer 4 Protocol** are set to **5060**.
- 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**, **Periodic Timeout** to **30**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send RTP 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, specifically the **VoIP** tab. The interface is divided into a left sidebar with a tree view of configuration objects and a main right pane for configuration details. The top of the right pane shows tabs for **System**, **LAN1**, **LAN2**, **DNS**, **Voicemail**, **Telephony**, **Directory Services**, **System Events**, **SMTP**, **SMDR**, **Twinning**, **VCM**, and **Codecs**. The **VoIP** tab is selected, and the **LAN Settings** sub-tab is active. The configuration details are as follows:

- H323 Gatekeeper Enable**: Checked.
- SIP Trunks Enable**: Checked.
- SIP Registrar Enable**: Checked.
- Domain Name**: **avaya.lab.com**.
- Layer 4 Protocol**:
 - UDP**: **UDP Port** is **5060**.
 - TCP**: **TCP Port** is **5060**.
 - TLS**: **TLS Port** is **5061**.
- RTP**:
 - Port Number Range**: **Minimum** is **49152**, **Maximum** is **53248**.
 - Port Number Range (NAT)**: **Minimum** is **49152**, **Maximum** is **53248**.
- Keepalives**:
 - Enable RTCP Monitoring on Port 5005**: Checked.
 - RTCP collector IP address for phones**: **0.0.0.0**.
 - Scope**: **RTP**.
 - Periodic timeout**: **30**.
 - Initial keepalives**: **Enabled**.
- DiffServ Settings**:
 - DSCP (Hex)**: **B8**.
 - Video DSCP (Hex)**: **B8**.
 - DSCP Mask (Hex)**: **FC**.
 - SG DSCP (Hex)**: **88**.
 - DSCP**: **46**.
 - Video DSCP**: **46**.
 - DSCP Mask**: **63**.
 - SG DSCP**: **34**.

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

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, the default STUN settings 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 heartbeat to the service provider.
- Verify the **Public IP Address** is set to **0.0.0.0**.
- Set the **Public Port** to **5060** for **UDP**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

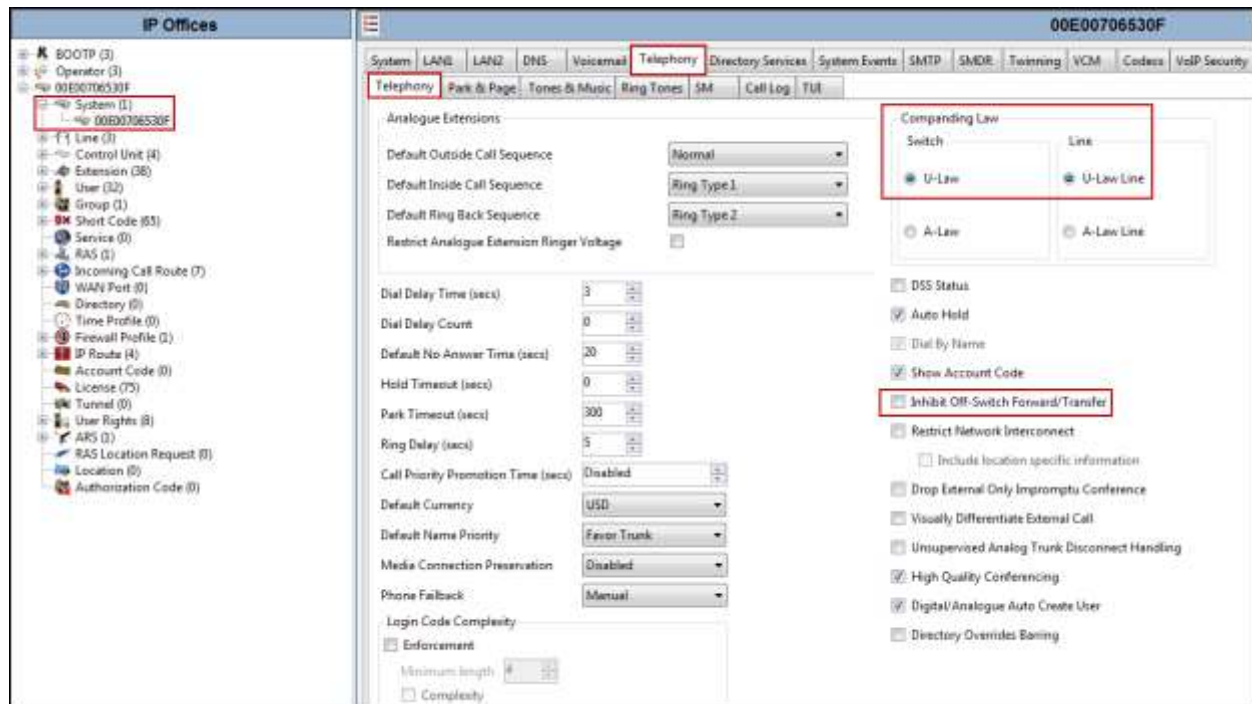


Note: In the compliance test, the **LAN1** interface was used to connect IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.2 System - Telephony Tab

Navigate to the **Telephony** → **Telephony** Tab in the Details Pane, configure the following parameters:

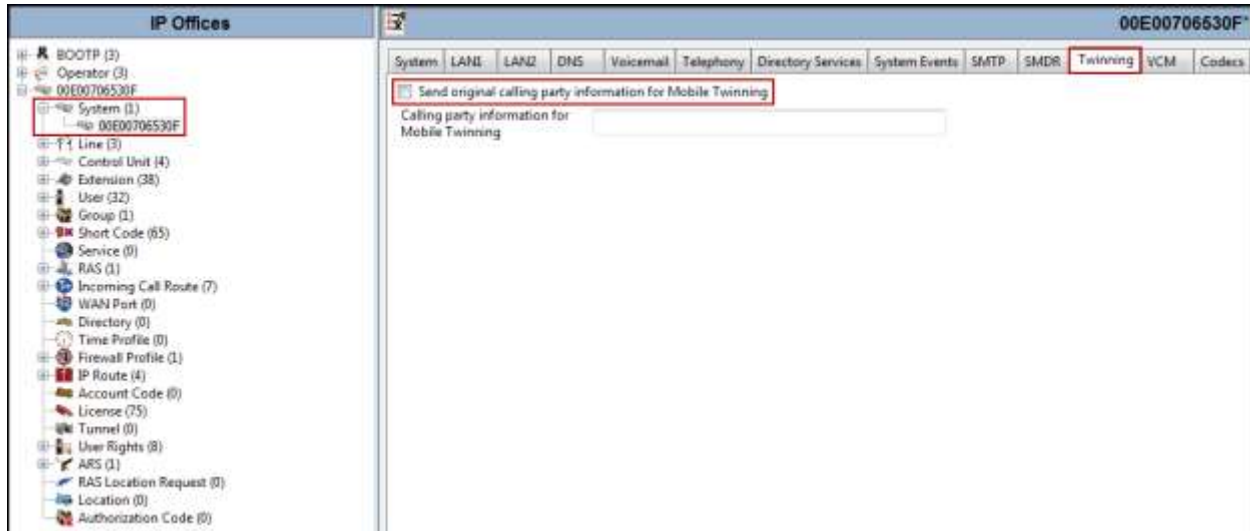
- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).



5.2.3 System - Twinning Tab

Navigate to the **Twinning** tab on the Details Pane, configure the following parameters:

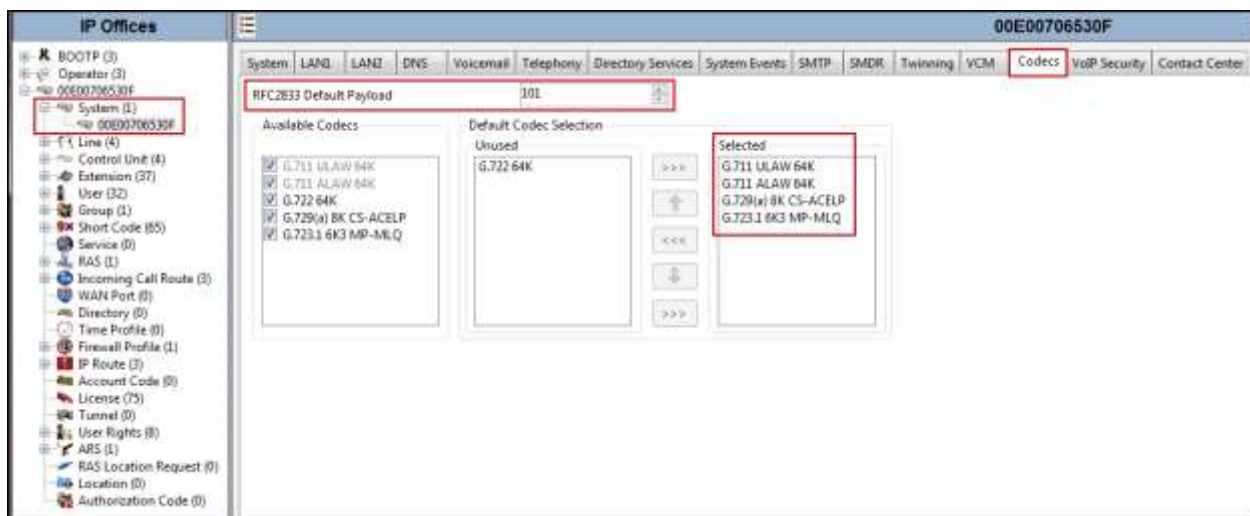
- Uncheck the **Send original calling party information for Mobile Twinning** box. This will allow the Caller ID for Twinning to be controlled by the setting on the SIP Line (**Section 5.4**). This setting also impacts the Caller ID for call forwarding.
- Click **OK** to commit (not shown).



5.2.4 System - Codecs Tab

For **Codec's** settings, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **Codecs** tab and configure the following parameters:

- Select or enter **101** for **RFC2833 Default Payload**. This setting was recommended by Alestra for use with out-band DTMF tone transmissions.
- 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 phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific extension. The example below shows the codecs used for IP phones (SIP and H.323). The system's default codecs and order was used.



Note: The codec selections defined under this section (System – Codecs 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).

5.3 IP Route

In the reference configuration, the IP Office LAN1 interface and the private interface of the Avaya SBCE resided on the same IP subnet, so an IP route was not 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 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 IP subnets), on the left navigation pane, right-click on **IP Route** and select **New**.

- Set the **IP Address** and **IP Mask** of the IP subnet of the private side of the Avaya SBCE, or enter **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office IP subnet.
- 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, the 'IP Offices' tree shows a hierarchy of components. The 'IP Route (4)' entry is highlighted with a red box, and its configuration is shown in the right pane. The right pane has a title bar with '0.0.0.0' and a tab labeled 'IP Route'. The configuration fields are as follows:

Field	Value
IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	172 . 16 . 5 . 254
Destination	LAN1
Metric	0
Proxy ARP	<input type="checkbox"/>

5.4 SIP Line

A SIP Line is needed to establish the SIP connection between IP Office and Alestra 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**

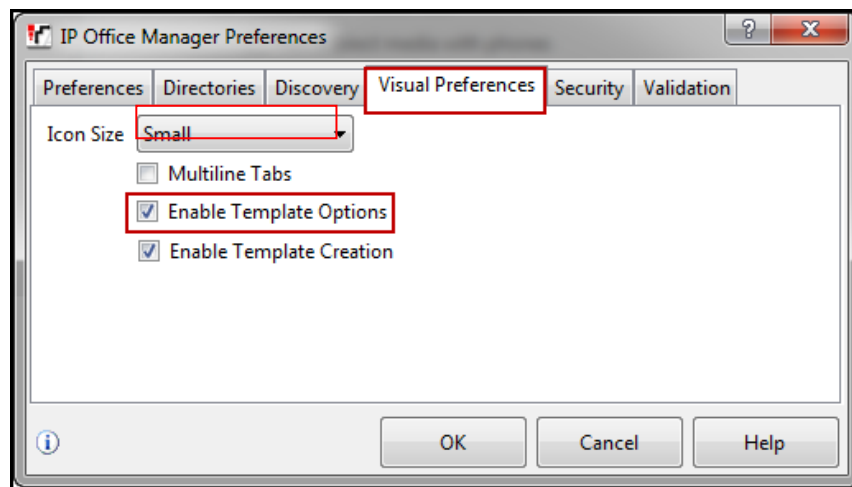
5.4.1 Importing a SIP Line Template

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.

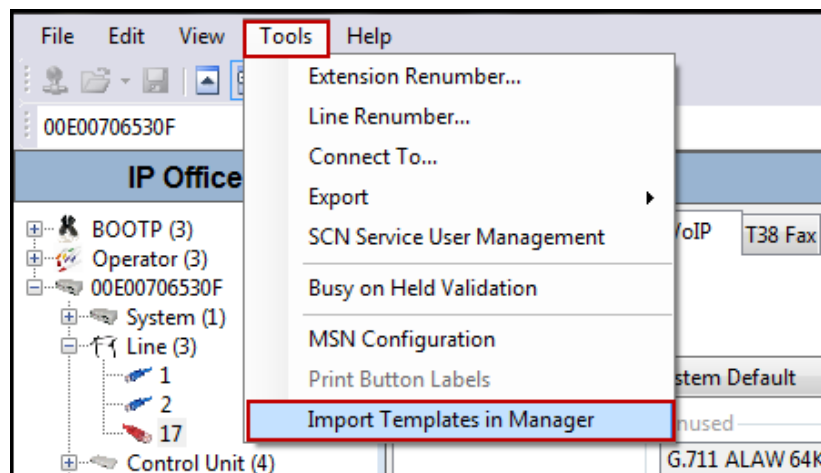
1. Copy a previously created template file to a location (e.g., C:\Temp) on the same computer where IP Office Manager is installed. By default, the template file name will have the format **AF_<user supplied text>_SIPTrunk.xml**, where the **<user supplied text>** portion is entered during template file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

Note – If necessary, the **<user supplied text>** portion of the template file name may be modified, however the **AF_<user supplied text>_SIPTrunk.xml** format of the file name must be maintained. For example, an original template file **AF_TEST _SIPTrunk.xml** could be changed to **AF_Test1_SIPTrunk.xml**. The template file name is selected in **Section 5.4.2, step 2**, to create a new SIP Line.

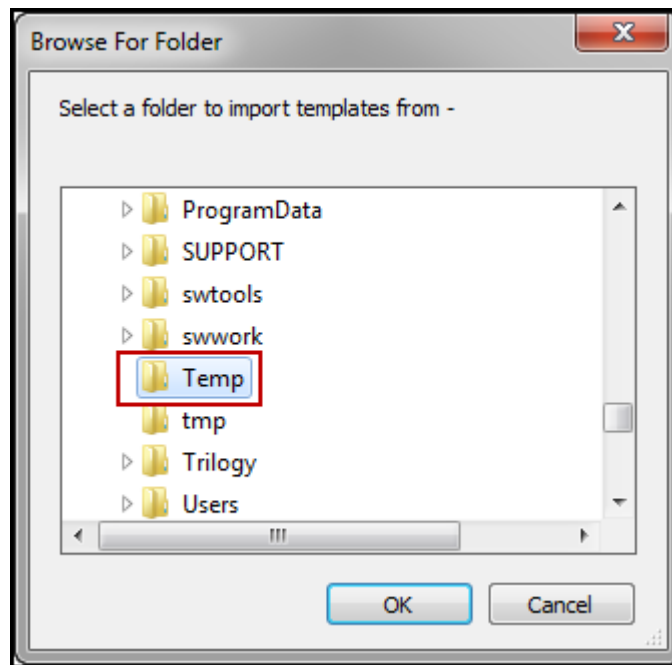
2. Verify that Template Options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the **Visual Preferences** tab. Check the box next to **Enable Template Options**. Click **OK**.



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



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

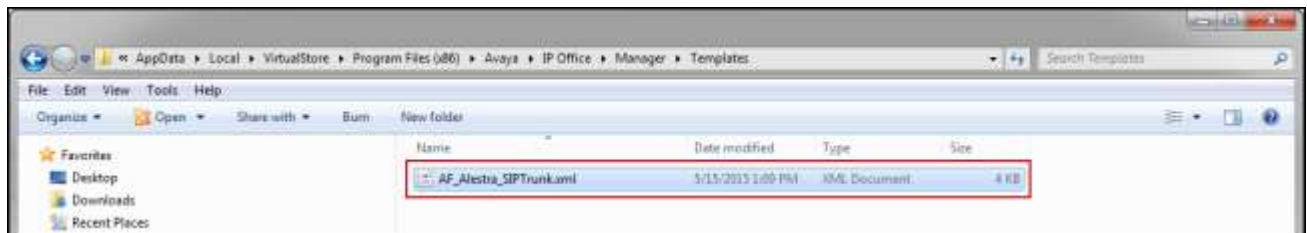
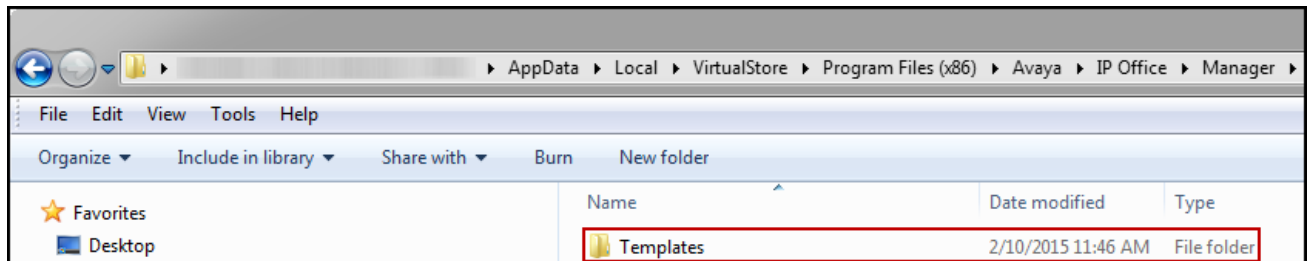
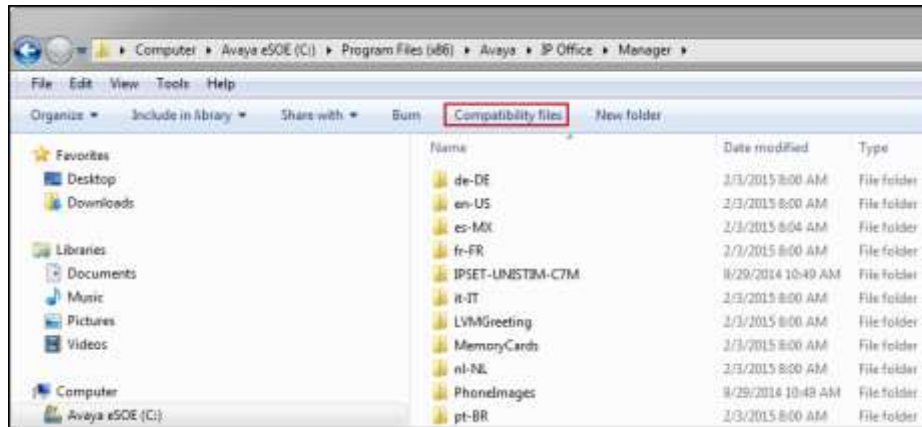


In the reference configuration, template files **AF_Alestra_SIPTrunk.xml** was imported. The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.

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

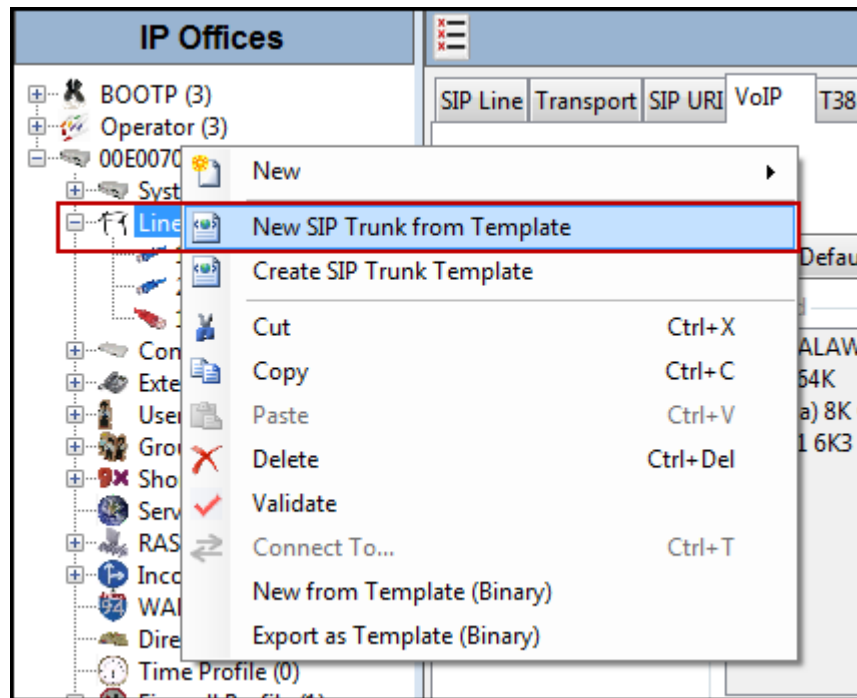


Note –Windows 7 (and later) locks the Avaya IP Office 9.1 \Templates directory, and it cannot be viewed. To enable browsing of the \Templates directory, open Windows Explorer, navigate to **C:\Program Files\Avaya\IP Office\Manager** (or C:\Program Files (x86)\Avaya\IP Office\Manager), and then click on the **Compatibility files** option shown below. The \Templates directory and its contents can then be viewed.



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 SIP Trunk from Template**.

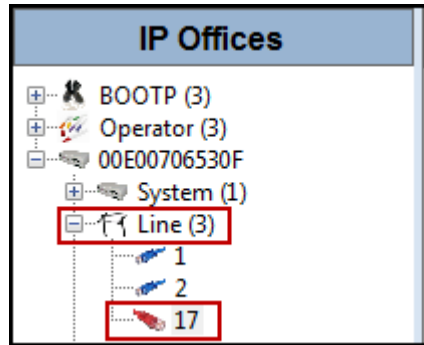


2. In the subsequent **Template Type Selection** pop-up window, from the **Service Provider** pull-down menu, select the XML template name from **Section 5.4.1**. Click **Create new SIP Trunk**.

Note – The drop down menu will display the *<user supplied text>* part of the template file name (see **Section 5.4.1**). If you check the **Display All** box, then the full template file name is displayed.



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 **SIP**.
- 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**.
- Set the **Originator number for forwarded and twinning calls** to **8128121041**. This is the authentication name or User Name credentials used for SIP Trunk registration purposes in the Avaya SBCE (Refer to **Section 6.2.4**). This setting was required for forwarded and twinned calls to be accepted by Alestra. SIP Trunk registration is done by the Avaya SBCE; credentials information should be provided by Alestra.
- Set **Send Caller ID** to **Diversion Header**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Always**.
- All other parameters should be set to default or according to customer requirements. Click **OK** to commit (not shown).

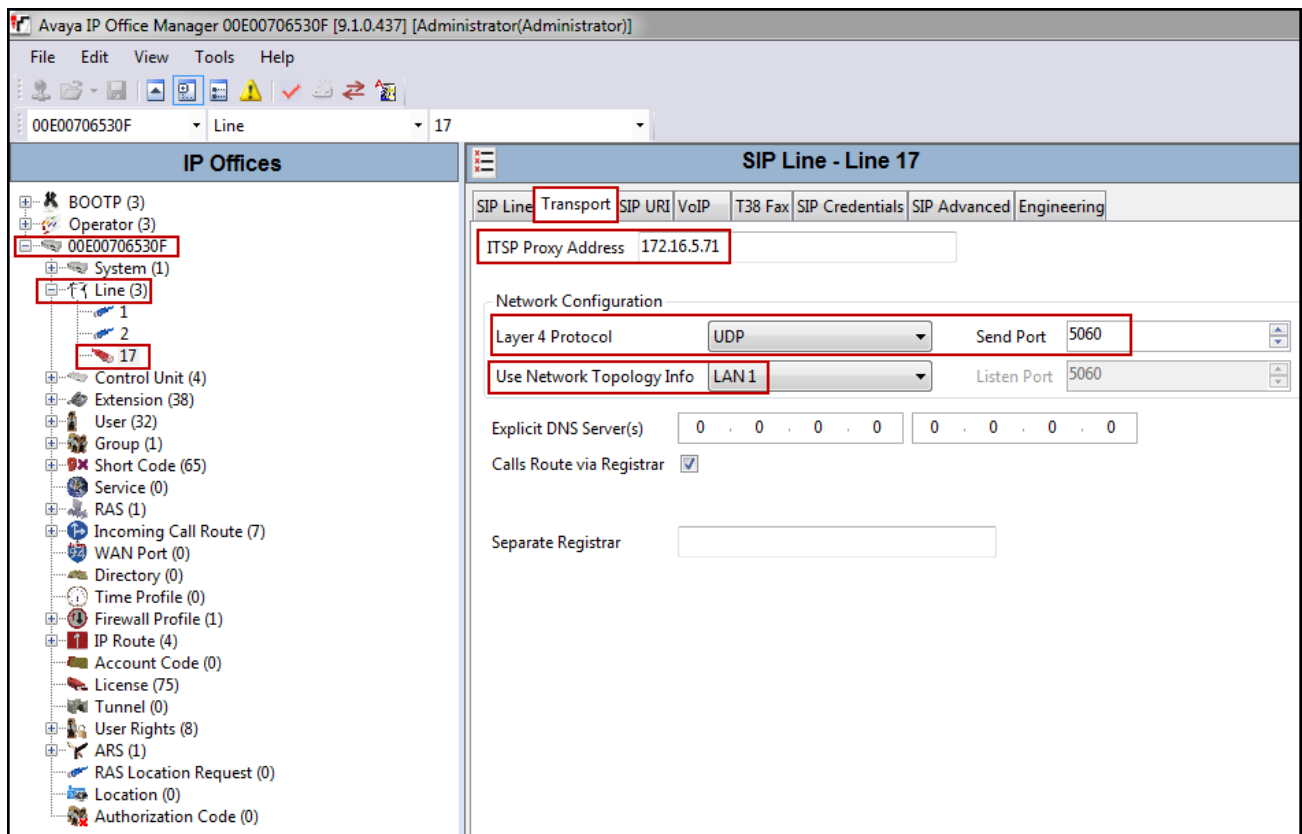
The screenshot displays the 'SIP Line - Line 17' configuration window. The left pane shows a tree view of system components, with 'Line 17' selected. The main pane has tabs for 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'SIP Line' tab is active, showing the following configuration fields:

- Line Number:** 17
- ITSP Domain Name:** (blank)
- URI Type:** SIP
- 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 (seconds):** On Demand
- Forwarding and Twinning:**
 - Originator number:** 8128121041
 - Send Caller ID:** Diversion Header
- Redirect and Transfer:**
 - Incoming Supervised REFER:** Always
 - Outgoing Supervised REFER:** Always
 - Send 302 Moved Temporarily:** ☐
 - Outgoing Blind REFER:** ☐

5.4.4 SIP Line - Transport Tab

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

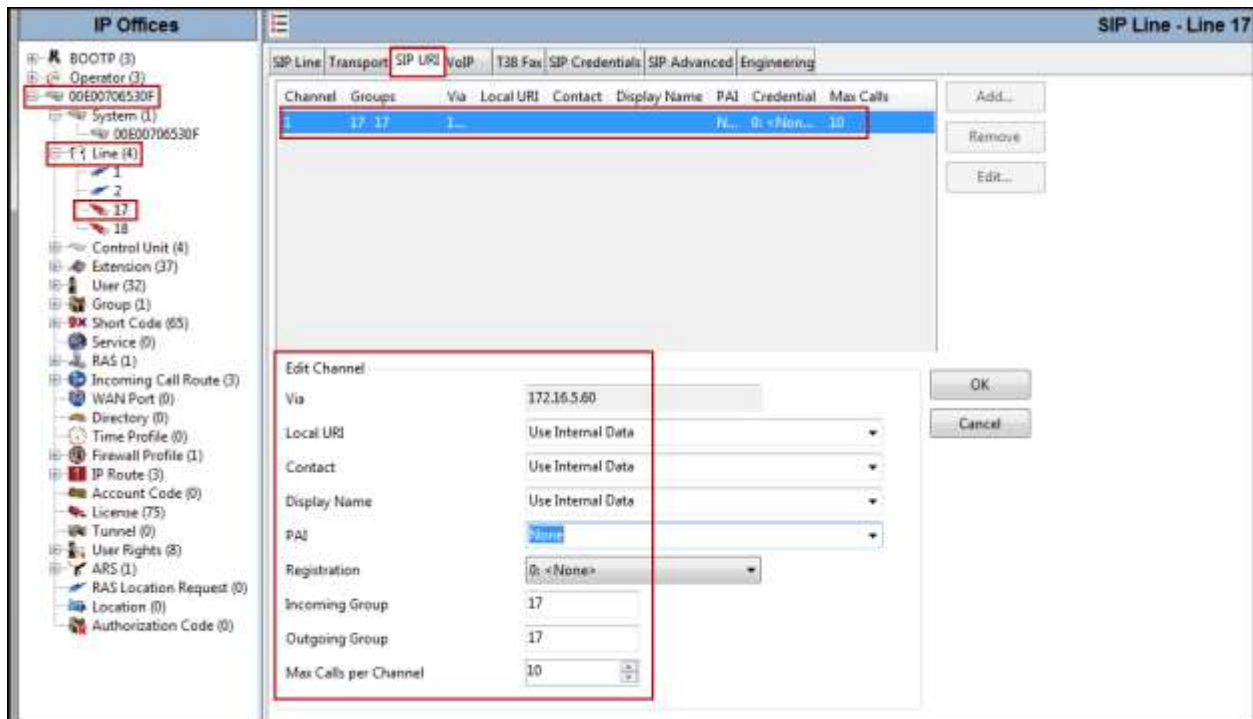
- Set the **ITSP Proxy Address** to the inside IP Address of the Avaya SBCE or **172.16.5.71** as shown in **Figure 1**.
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2.1**
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



5.4.5 SIP Line - SIP URI Tab

A SIP URI entry needs to be created to match each incoming number that IP Office will accept on this line. Select the **SIP URI** tab, and 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. In the example screen below, a previously configured entry was edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an IP Office user. The entry was created with the parameters shown below:

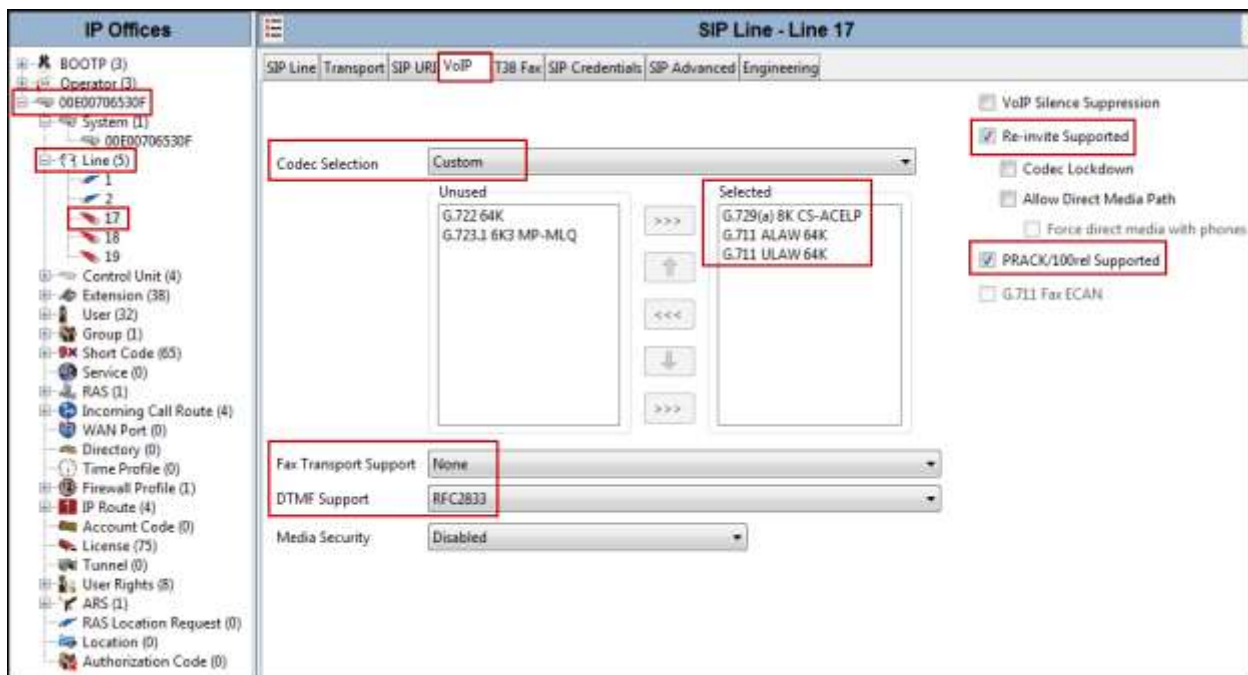
- Set **Local URI**, **Contact**, **Display Name** to **Use Internal Data**.
- Set **PAI** to **None**.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Set **Max Calls per Channel** 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)



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:

- In the sample configuration, 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, codec's **G.729(a)**, **G.711ALAW** and **G.711ULAW** were selected for audio.
- Set **Fax Transport Support** to **None** (Refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833**. This directs IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- 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.
- Check the **PRACK/100rel Supported** box, to advertise the support for reliable provisional responses and Early Media to Alestra.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

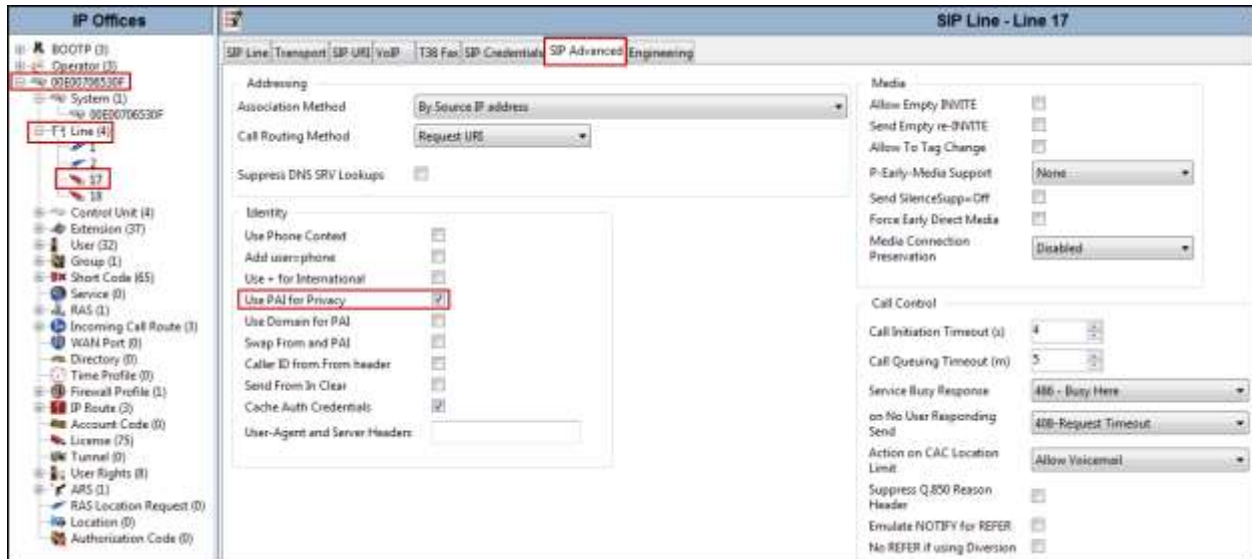


Note: The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.4** (System –Codec tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

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:

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



5.5 Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.4**. To configure these settings, first navigate to **User** → *Name* in the Navigation Pane where *Name* is the name of the user to be modified. In the example below, the name of the user is **Ext3041 H323**. Select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP Line (**Section 5.4.5**). The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Alestra. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network. This can also be accomplished by activating Withhold Number on H.323 Deskphones (not shown). Click the **OK** to commit (not shown).

The screenshot displays the Avaya User Configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'User (32)' selected, and '3041 Ext3041 H323' highlighted. The main pane is titled 'Ext3041 H323: 3041' and contains several tabs: 'Voice Recording', 'Button Programming', 'Menu Programming', 'Mobility', 'Group Membership', 'Announcements', and 'SIP'. The 'SIP' tab is active, showing three input fields: 'SIP Name' with the value '8128121041', 'SIP Display Name (Alias)' with the value 'Ext3041 H323', and 'Contact' with the value '8128121041'. Below these fields is an 'Anonymous' checkbox, which is currently unchecked.

Ext3041 H323: 3041	
Voice Recording Button Programming Menu Programming Mobility Group Membership Announcements SIP	
SIP Name	8128121041
SIP Display Name (Alias)	Ext3041 H323
Contact	8128121041
<input type="checkbox"/> Anonymous	

5.6 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. In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in IP Office. The routing decision for the call is based on the parameters previously configured for **Call Routing Method** (Section 5.4.7) and **SIP URI** (Section 5.4.5) and the users **SIP Name** and **Contact**, already populated with the assigned Alestra DID numbers (Section 5.5).

5.6.1 Incoming Call Route – Standard Tab

To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**.

On the **Standard** tab of the Details Pane, enter the parameters as shown below.

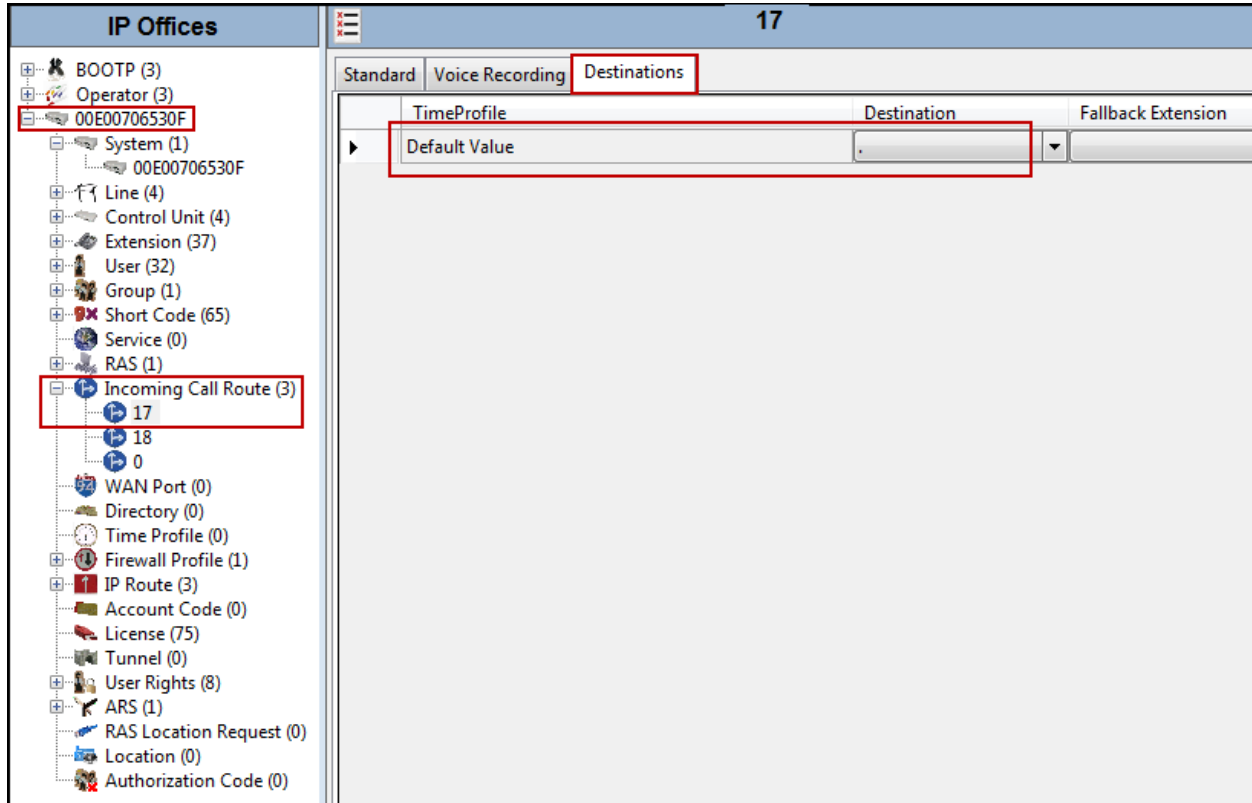
- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in Section 5.4.
- Default values can be used for all other fields.

The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'Incoming Call Route (3)' selected and highlighted with a red box. The main pane shows the configuration for 'Incoming Call Route 17'. The 'Standard' tab is active, and the 'Line Group ID' is set to '17'. The 'Bearer Capacity' is set to 'Any Voice'. Other fields like 'Incoming Number', 'Incoming Sub Address', 'Incoming CLI', 'Locale', 'Priority', 'Tag', 'Hold Music Source', and 'Ring Tone Override' are also visible.

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

5.6.2 Incoming Call Route – Destinations Tab

- Under the **Destinations** tab, enter “.” for the **Default Value**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of that **User**, which matches the number present on the user part of the incoming Request URI.
- Click **OK** to commit (not shown).



5.7 Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. While detailed coverage of ARS is beyond the scope of these Application Notes, and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance testing.

5.7.1 Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code** 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 IP Office user dials 9 plus any number N, instead of being directed to a specific Line Group ID, the call is directed to **Line Group 50: Main**, which is configurable via ARS.

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

IP Offices	9N: Dial*																
<ul style="list-style-type: none">*33*N#*34N;*35*N#*36*37*N#*38*N#*39*40*41*42*43*44*45*N#*468N9NFNE00	<table><tr><td>Short Code</td><td></td></tr><tr><td>Code</td><td>9N</td></tr><tr><td>Feature</td><td>Dial</td></tr><tr><td>Telephone Number</td><td>N</td></tr><tr><td>Line Group ID</td><td>50: Main</td></tr><tr><td>Locale</td><td></td></tr><tr><td>Force Account Code</td><td><input type="checkbox"/></td></tr><tr><td>Force Authorization Code</td><td><input type="checkbox"/></td></tr></table>	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"/>
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 a sample ARS configuration for the route **50: Main**. Note the sequence of **X**'s used in the **Code** field of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office.

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

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **8** followed by **9 X**'s to represent the exact number of digits.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **8N**. The value **N** represents the additional number of digits dialed by the user after dialing **8** (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.
- Set **Locale** to **United States (US English)**.
- 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 entry highlighted below shows another example ARS dial string used during the compliance test., The user dialed **9**, followed by **001** and **10** digits (represented by **10 X**'s). The **9** is stripped off, the remaining digits, including the **001**, are included in the SIP INVITE message IP Office sends to Alestra. This dial string was used to make international calls to PSTN numbers in the U.S.

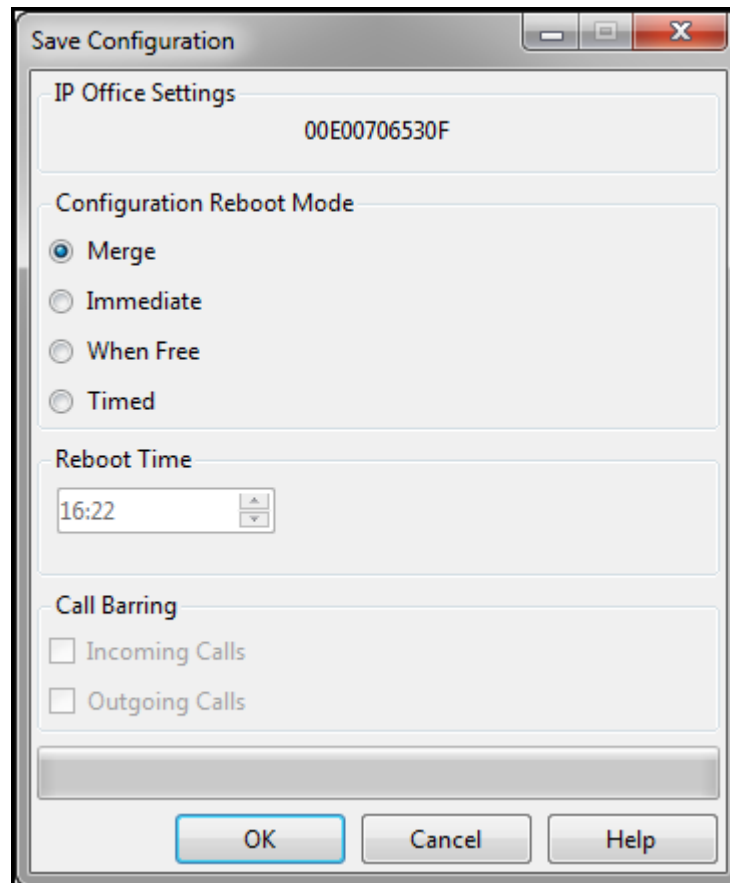
The second highlighte entry below of **8** plus **9** digits (represented by **9 X**'s) was used to make call within Mexico.

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
001XXXXXXXX	001N	Dial	17
8XXXXXXXX	8N	Dial	17
1XXXXXXXX	1N	Dial	17
6XXXXXX	6N	Dial	17
3XXXXXXXX	3N	Dial	17

5.8 Save Configuration

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

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



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 field showing '16:22'. 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

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

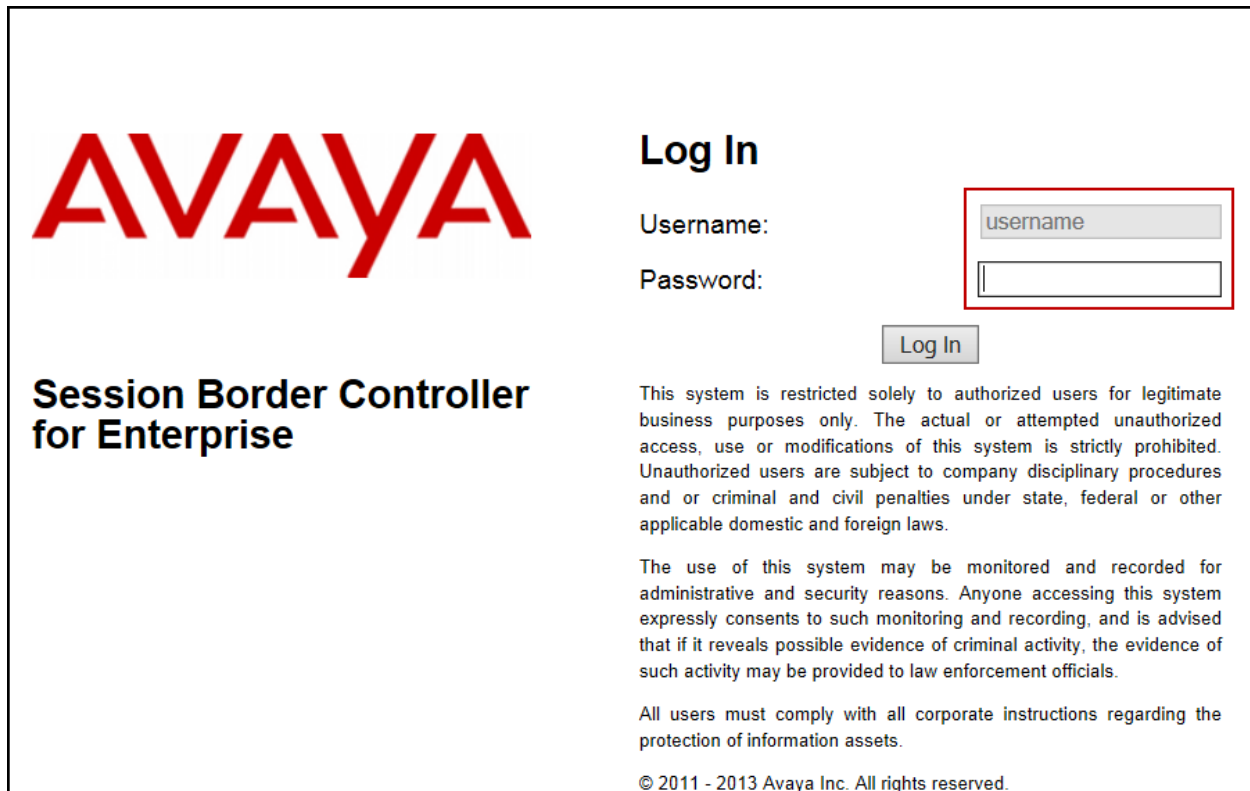
It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

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

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

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

Session Border Controller for Enterprise

Dashboard

Information

System Time	08:58:52 PM GMT-06:00	Refresh
Version	6.3.1-22-4653	
Build Date	Fri Nov 21 17:35:09 EST 2014	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	

Installed Devices

Device Name	Management IP
EMS	
Avaya SBCE	

Incidents (past 24 hours)

Incident ID	Message	Time
1	Avaya SBCE: No Server Flow Matched for Incoming Message	
2	Avaya SBCE: No Server Flow Matched for Incoming Message	
3	Avaya SBCE: No Server Flow Matched for Incoming Message	
4	Avaya SBCE: No Server Flow Matched for Incoming Message	
5	Avaya SBCE: No Server Flow Matched for Incoming Message	

Notes

No notes found

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.

Session Border Controller for Enterprise

System Management

Devices | Updates | SSL VPN | Licensing

Device Name	Management IP	Version	Status	Actions
Avaya SBCE		6.3.1-22-4653	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed 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**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

System Information: Avaya SBCE

General Configuration

Appliance Name

Avaya SBCE

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

License Allocation

Standard Sessions

2000

Requested: 2000

Advanced Sessions

2000

Requested: 2000

Scopia Video Sessions

500

Requested: 500

Encryption

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
172.16.5.71	172.16.5.71	255.255.255.0	172.16.5.254	A1
10.10.157.186	10.10.157.186	255.255.255.192	10.10.157.129	B1

DNS Configuration

Primary DNS

172.16.5.102

Secondary DNS

DNS Location

DMZ

DNS Client IP

172.16.5.71

Management IP(s)

IP

On the previous screen, **A1** correspond to the inside interface (Private Network side) and **B1** correspond to the outside interface (Public Network side) of the Avaya SBCE. (Refer to **Figure 1**).

The management IP was blurred out for security reasons. The IP addresses used for the remote worker configuration were also blurred out since the remote worker configuration is beyond the scope of these Application Notes and is not discussed in these Application Notes.

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). If this is not the case, contact your Avaya representative to have this resolved.

6.2 Global Profiles

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

6.2.1 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 Alestra, 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
<button>Finish</button>	

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

Alarms Incidents Status Logs Diagnostics Users

Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups
PPM Services
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
DMZ Services
TURN/STUN Service
SNMP
Syslog Management
Advanced Options
Troubleshooting

Interworking Profiles: Avaya-IPO
Add

Interworking Profile
ca210E
avaya-ns
OCS-Edge-Server
cisco-com
cups
Sipera-Itale
OCS-FrontEnd-Server
Avaya-SM
SP-General
Avaya-CS1000
Avaya-IPO
Avaya-CM

Click here to add a description
General Timers URI Manipulation Reader Manipulation Advanced

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URF Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	sip
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	
DTMF	
DTMF Support	None

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' web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, System Management, Global Parameters, Global Profiles, and Device Specific Settings. The 'Global Profiles' section is expanded, showing 'Server Interworking' as the selected option. The main content area is titled 'Interworking Profiles: Avaya-IPO' and features a list of profiles on the left, including 'cs2100', 'avaya-ts', 'OCS-Edge-Server', 'cisco-com', 'cops', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General', 'Avaya-CS1000', 'Avaya-IPO' (highlighted), and 'Avaya-UM'. The 'Avaya-IPO' profile is selected, and its configuration is shown on the right. The configuration is divided into tabs: General, Timers, URI Manipulation, Header Manipulation, and Advanced (selected). The Advanced tab contains a table of settings for various protocols and services.

Setting	Value
Record Routes	Both
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	Yes
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No
Lync Extensions	No

6.2.2 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).

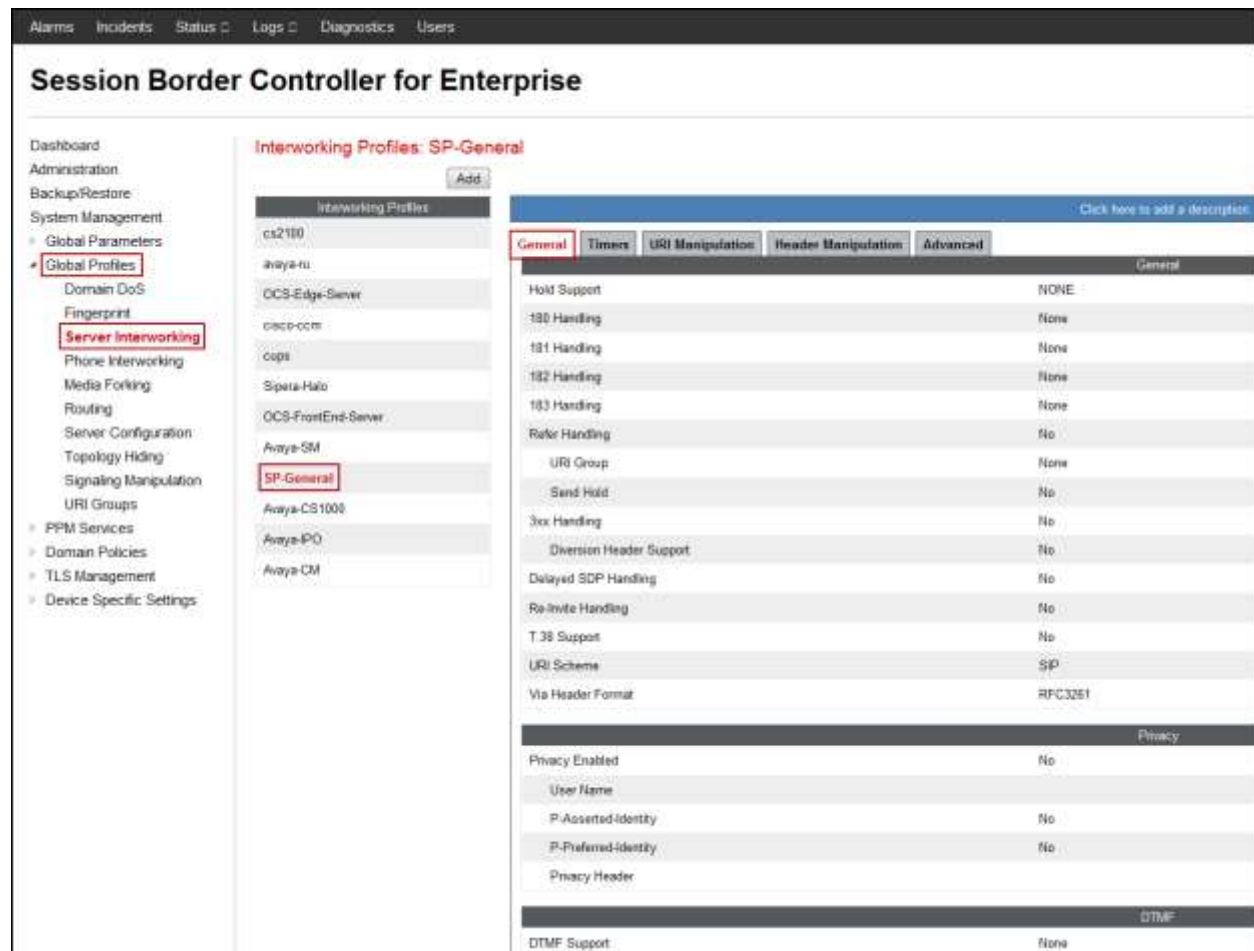
Enter the new profile name, the name of **SP-General** was chosen in this example.

- Click **Next**.



- Accept all other default values by clicking **Next** and then **Finish** (not shown).

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



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
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

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' web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar contains a menu with 'Global Profiles' and 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: SP-General' and features a list of profiles on the left, with 'SP-General' selected. The right pane shows the 'Advanced' tab of the configuration, with a table of settings.

General	Timers	URI Manipulation	Header Manipulation	Advanced
Record Routes				Both
Topology Hiding: Change Call-ID				Yes
Call-Info NAT				No
Change Max Forwards				Yes
Include End Point IP for Context Lookup				No
OCS Extensions				No
AVAYA Extensions				No
NORTEL Extensions				No
Diversion Manipulation				No
Metaswitch Extensions				No
Reset on Talk Spurt				No
Reset SRTP Context on Session Refresh				No
Has Remote SBC				Yes
Route Response on Via Port				No
Cisco Extensions				No
Lync Extensions				No

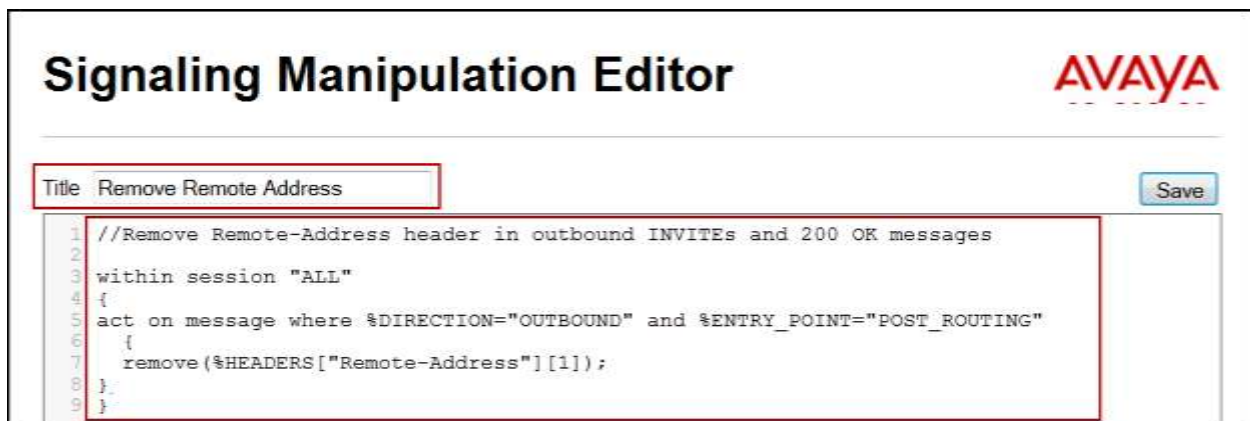
6.2.3 Signaling Manipulation

The Avaya SBCE is capable of doing header manipulation by means of Signaling Manipulation (or SigMa) Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For the test configuration, the Editor was used to create the script needed to handle the header manipulation described below.

The Signaling Manipulation Script shown below is needed to remove unwanted headers to prevent them from being sent to the Service provider.

From the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click on **Add Script** to open the SigMa Editor screen (not shown).

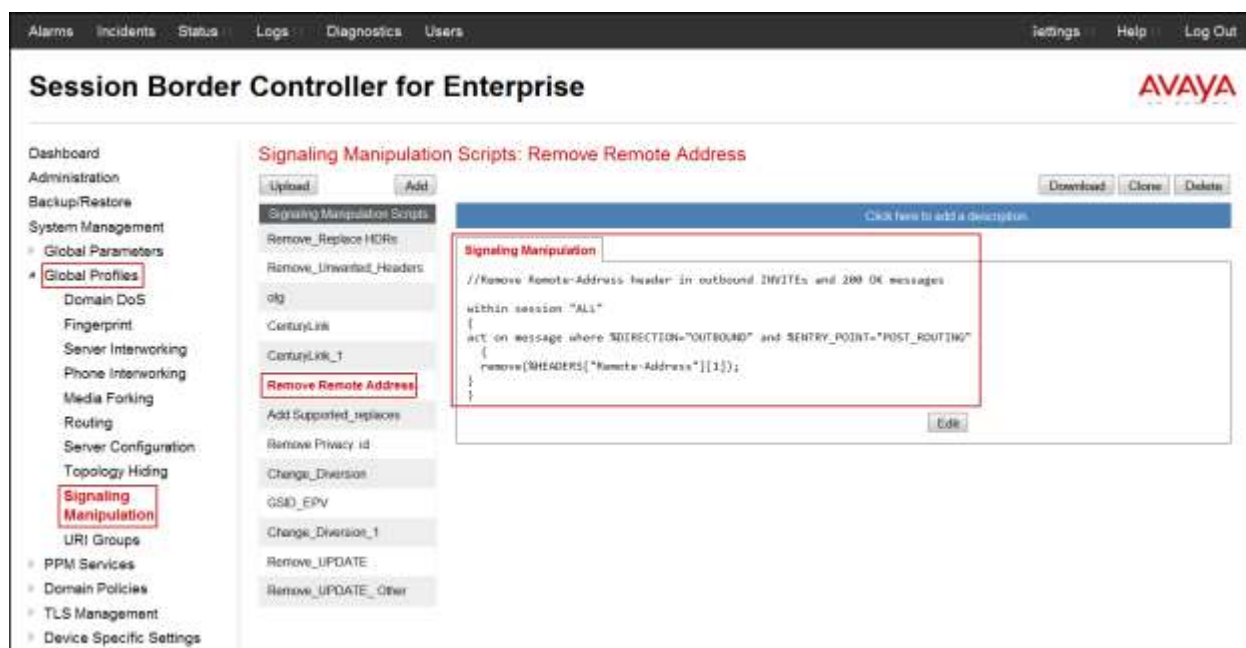
- For **Title** enter a name, the name of *Remove Remote Address* was chosen in this example.
- Enter the script as shown on the screen below (**Note**: The script can be copied from **Appendix A**).
- Click **Save**.



The screenshot displays the 'Signaling Manipulation Editor' window with the Avaya logo in the top right corner. A text box labeled 'Title' contains the text 'Remove Remote Address'. To the right of this box is a 'Save' button. Below the title box is a large text area containing a script. The script is as follows:

```
1 //Remove Remote-Address header in outbound INVITEs and 200 OK messages
2
3 within session "ALL"
4 {
5   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
6   {
7     remove(%HEADERS["Remote-Address"][1]);
8   }
9 }
```

The following screen capture shows the newly added **Remove Remote Address** Signaling Manipulation Script.



6.2.4 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**.



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

- **Server Type:** Select *Call Server*.
- **IP Address / FQDN:** *172.16.5.60* (IP Address of IP Office).
- **Port:** *5060* (This port must match the port number defined in **Section 5.2.1**).
- **Transports:** Select *UDP*.
- Click **Next**.

IP Address / FQDN	Port	Transport
172.16.5.60	5060	UDP

Note: UDP transport protocol was used on the connection between the Avaya SBCE and IP Office. However, TCP can be used instead if necessary.

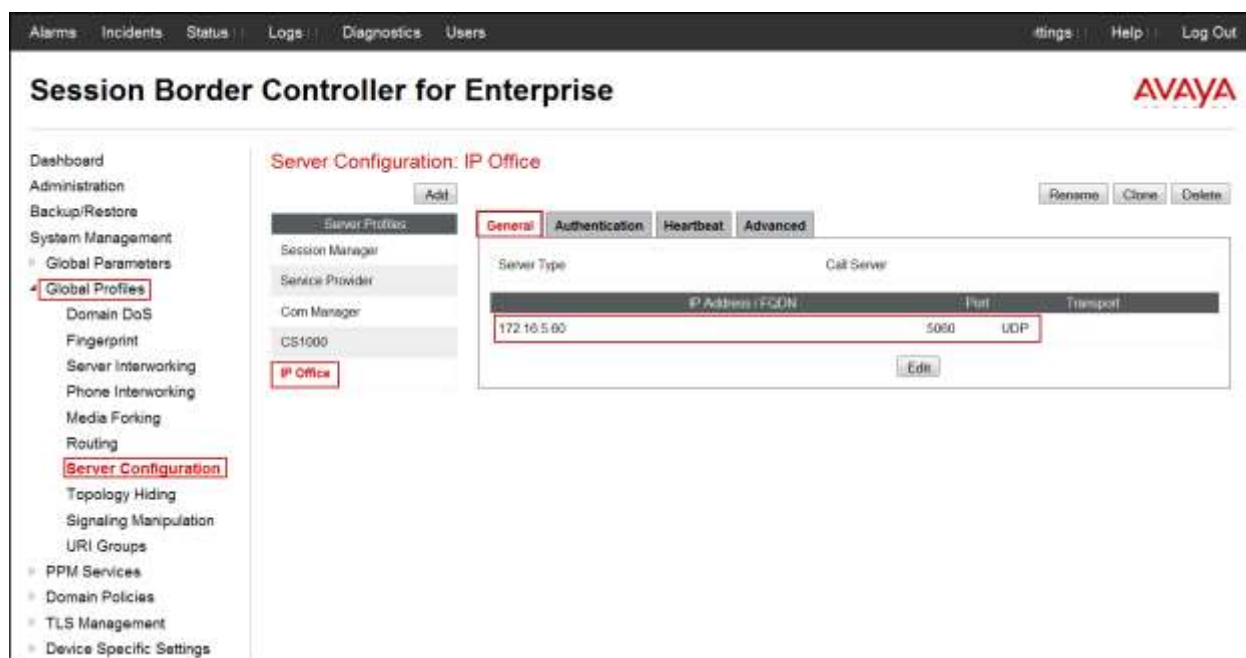
- Click **Next** on the **Authentication** window (not shown).
- Click **Next** on the **Heartbeat** window (not shown).

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

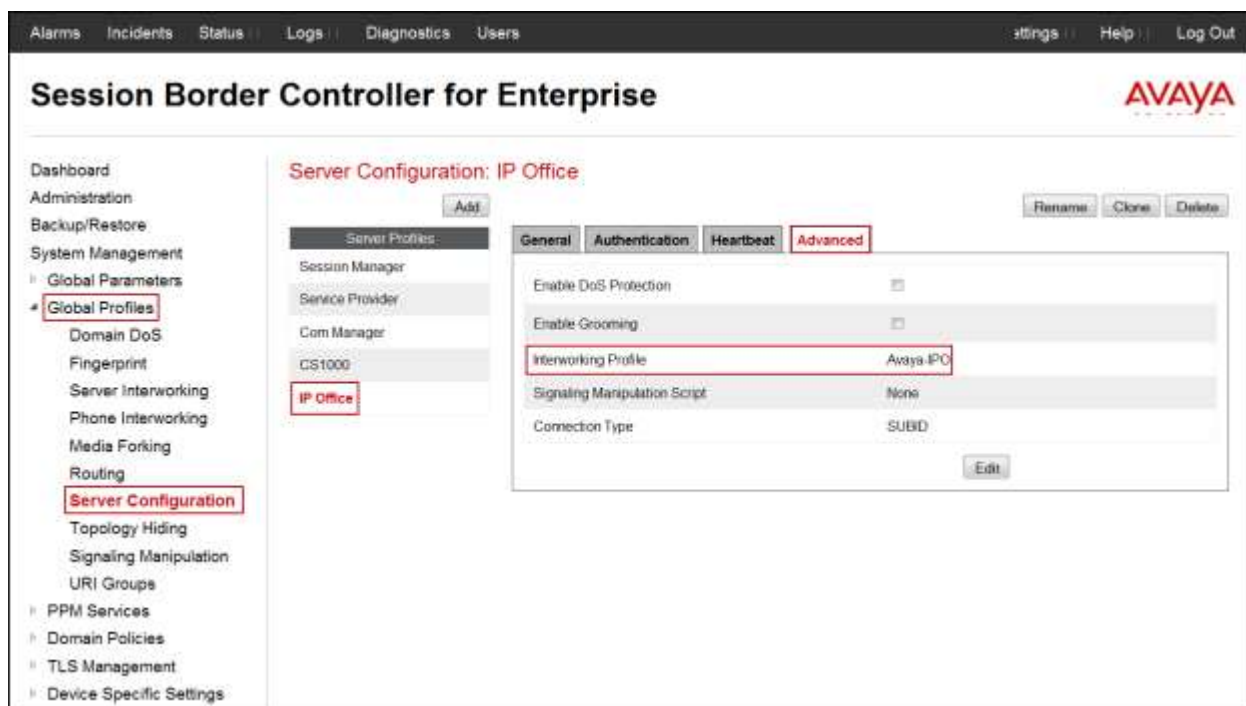
- Select *Avaya-IPO* from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default *None*.
- Click **Finish**.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya-IPO
Signaling Manipulation Script	None
Connection Type	SUBID

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

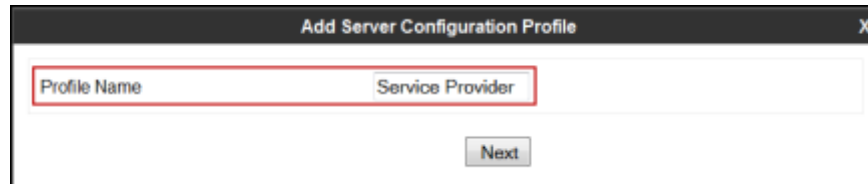


The following screen capture shows the **Advanced** tab of the newly created **IP Office** Server Configuration Profile.



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*.

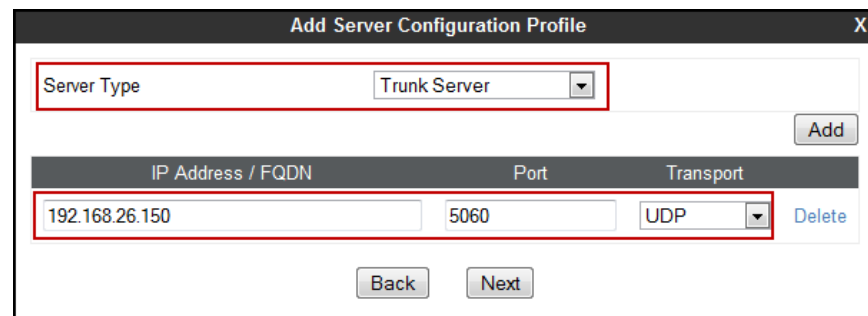
- Click **Next**.



The screenshot shows a window titled "Add Server Configuration Profile". Inside, there is a text input field labeled "Profile Name" which contains the text "Service Provider". This field is highlighted with a red rectangular box. Below the input field, there is a "Next" button.

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

- **Server Type:** Select *Trunk Server*.
- **IP Address / FQDN:** *192.168.26.150* (IP Address of the Service Provider SIP Proxy).
- **Port:** *5060*.
- **Transports:** Select *UDP*.
- Click **Next**.



The screenshot shows the "Add Server Configuration Profile" window. At the top, the "Server Type" dropdown menu is set to "Trunk Server" and is highlighted with a red box. Below this, there is an "Add" button. Underneath, there is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The table contains one row with the values "192.168.26.150", "5060", and "UDP". This row is highlighted with a red box. To the right of the table is a "Delete" button. At the bottom of the window, there are "Back" and "Next" buttons.

IP Address / FQDN	Port	Transport
192.168.26.150	5060	UDP

On the **Authentication** tab:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Leave **Realm** blank.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

The screenshot shows a window titled "Add Server Configuration Profile - Authentication". Inside the window, there is a form with a red border. The form contains the following elements:

- Enable Authentication:** A checkbox that is checked.
- User Name:** A text field containing the value "8128121041".
- Realm:** A text field with the placeholder text "(Leave blank to detect from server challenge)".
- Password:** A text field with masked characters (dots).
- Confirm Password:** A text field with masked characters (dots).

Below the form, there are two buttons: "Back" and "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, **60** 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 under the **Authentication** screen (**8128121041**) and the service provider's domain name (**asbw.alestravoip.com**), as shown on the screen below.
 - **To URI**: Use the **User Name** entered above under the **Authentication** screen (**8128121041**) and the service provider proxy provider's domain name (**asbw.alestravoip.com**), as shown on the screen below.

Note: The **User Name** and **domain name** should be provided by the service provider.
- Click **Next**.

Add Server Configuration Profile - Heartbeat X

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	REGISTER ▾
Frequency	60 seconds
From URI	8128121041@asbw.ales
To URI	@asbw.alestravoip.com

Back Next

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

- Select **SP-General** from the **Interworking Profile**.
- Select **Remove Remote Address** from the **Signaling Manipulation Script**, script created in **Section 6.2.3**.
- Click **Finish**.

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile: SP-General

Signaling Manipulation Script: Remove Remote Address

Connection Type: SUBID

Back Finish

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

Alarms 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 Fingerprint Server Interworking Phone Interworking Media Forking Routing Server Configuration Topology Hiding Signaling Manipulation URI Groups PPM Services Domain Policies TLS Management Device Specific Settings

Server Configuration: Service Provider

Add Rename Clone Delete

Server Profiles: Session Manager Service Provider Com Manager CS1002 IP Office

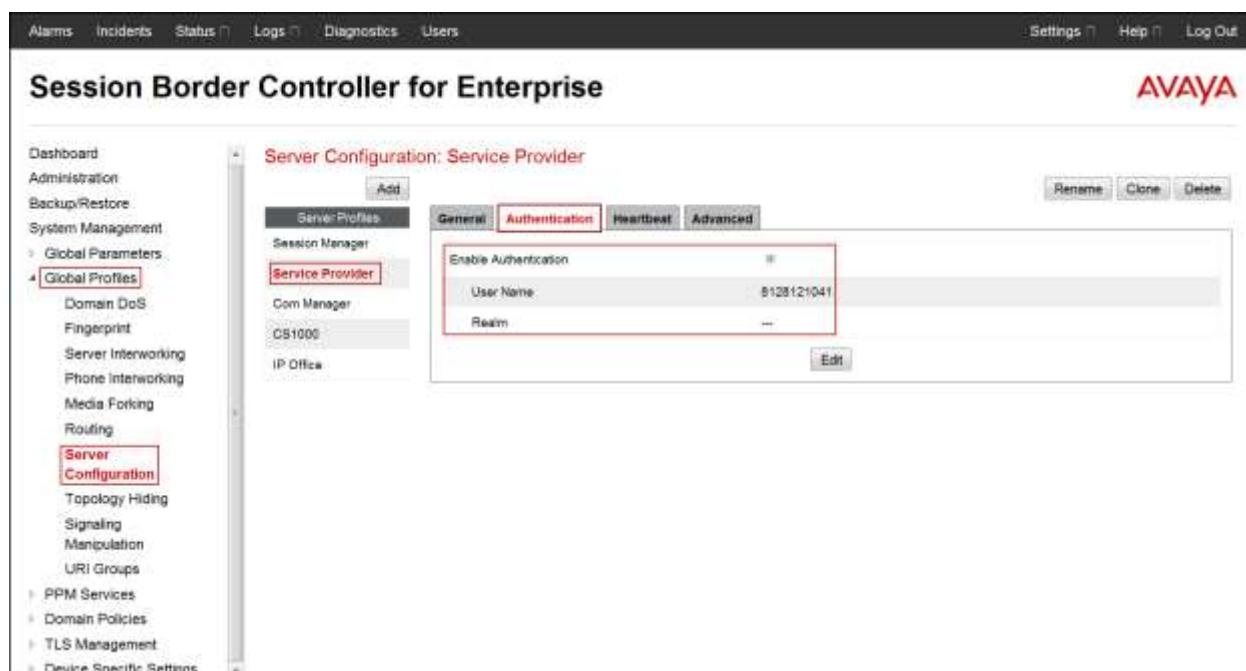
General Authentication Heartbeat Advanced

Server Type: Trunk Server

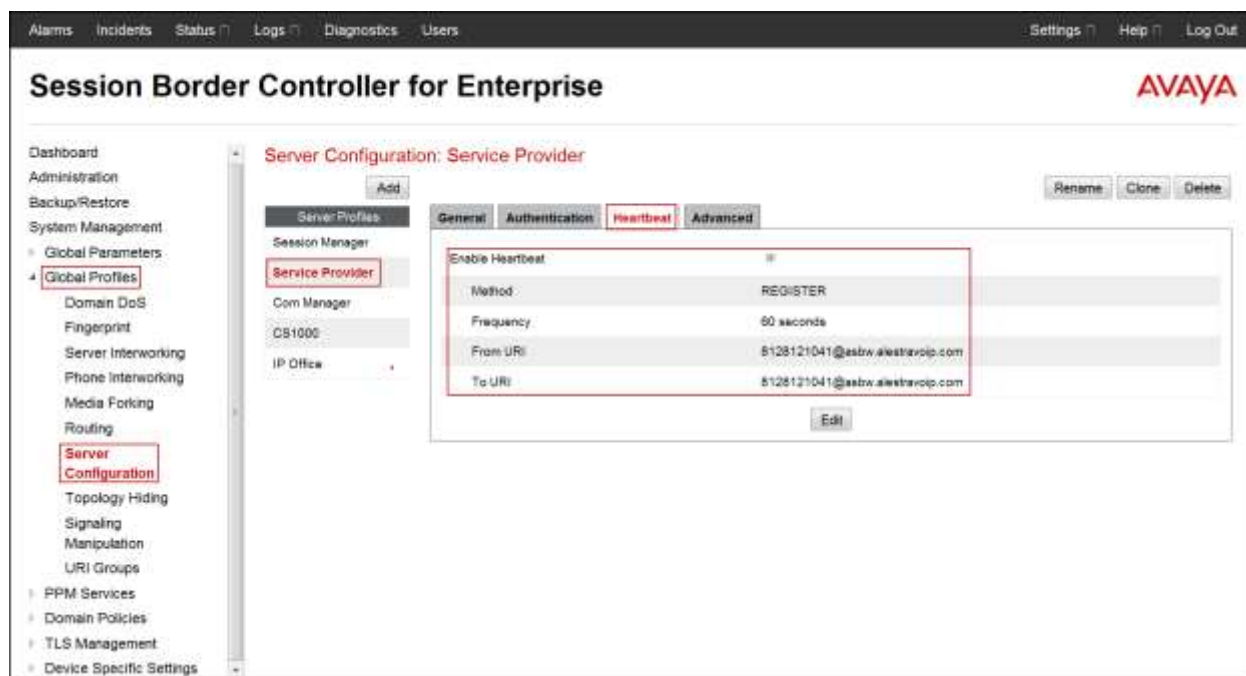
IP Address / FQDN	Port	Transport
192.168.28.150	5060	UDP

Edit

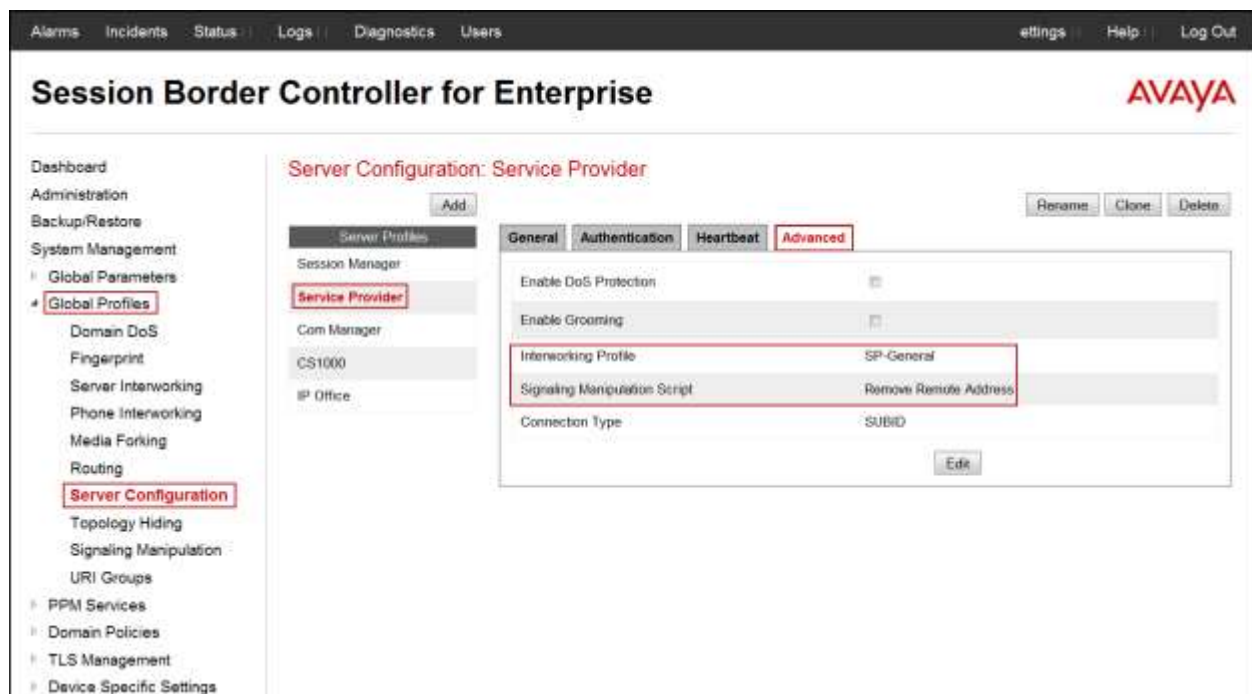
The following screen capture shows the **Authentication** tab of the newly created **Service Provider** Server Configuration Profile.



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



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



6.2.5 Routing Profiles

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

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

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

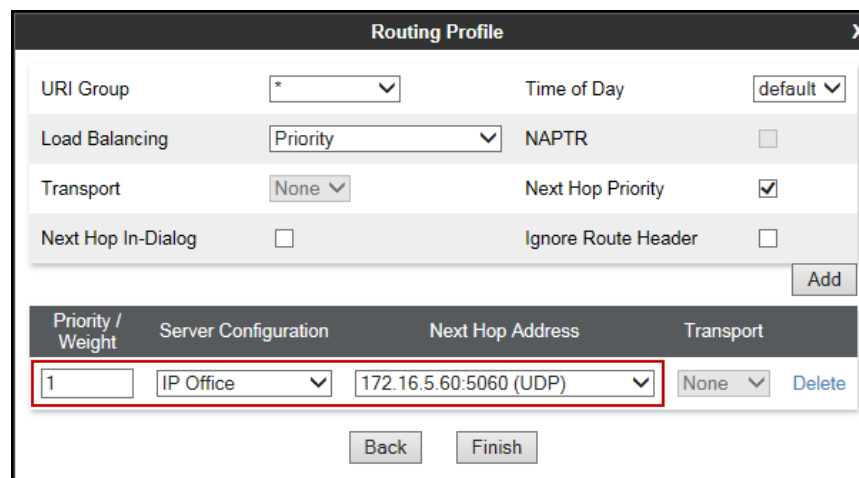
- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route_to_IPO**.
- Click **Next**.



The screenshot shows a 'Routing Profile' dialog box. The 'Profile Name' field is highlighted with a red rectangle and contains the text 'Route_to_IPO'. 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**.
- **Next Hop Address:** Select **172.16.5.60:5060 (UDP)** (IP Office IP address, Port and Transport).
- Click **Finish**.



The screenshot shows the 'Routing Profile' dialog box with various configuration options. The 'Add' button is highlighted with a red rectangle. Below the configuration options is a table with columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport. The first row in the table is highlighted with a red rectangle and contains the values: 1, IP Office, 172.16.5.60:5060 (UDP), and None. Below the table are 'Back' and 'Finish' buttons.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	IP Office	172.16.5.60:5060 (UDP)	None

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



Similarly, for the outbound route:

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



On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select *Service Provider*.
- **Next Hop Address:** Select *192.168.26.150:5060 (UDP)* (Service Provider SIP Proxy IP address, Port and Transport).
- Click **Finish**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Service Provider	192.168.26.150:5060 (UDP)	None

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

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	192.168.26.150	UDP

6.2.6 Topology Hiding

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

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

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

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



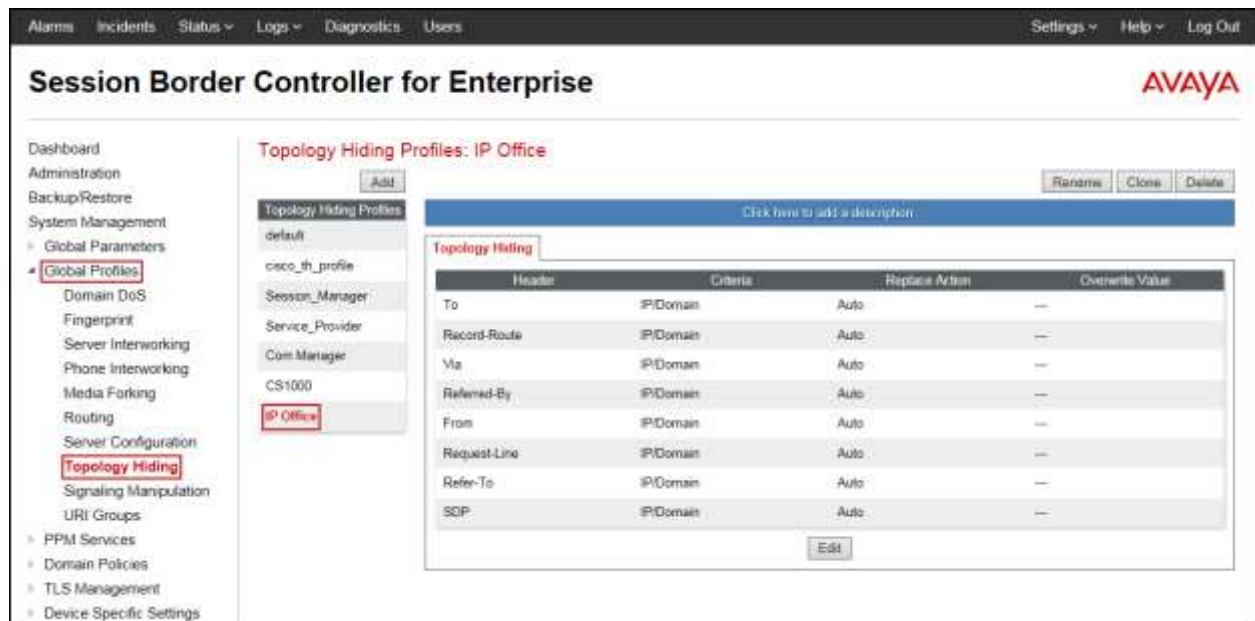
Clone Profile

Profile Name: default

Clone Name: IP Office

Finish

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



Alarms 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 Fingerprint Server Interworking Phone Interworking Media Forking Routing Server Configuration Topology Hiding Signaling Manipulation URI Groups PPM Services Domain Policies TLS Management Device Specific Settings

Topology Hiding Profiles: IP Office

default clone_th_profile Session_Manager Service_Provider Com_Manage CS1000 IP Office

Click here to add a description

Header	Criteria	Replace Action	Override Value
To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Refered-By	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Refer-To	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 **Profile Name: Service_Provider**.
- Click **Finish**.

Clone Profile

Profile Name: default

Clone Name: Service_Provider

Finish

- Click **Edit** on the newly created **Service_Provider** Topology Hiding profile.
- On the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the service provider (*asbw.alestravoip.com*) under **Overwrite Value**.
- On the **From** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (*asbw.alestravoip.com*) under **Overwrite Value**.
- On the **To** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (*asbw.alestravoip.com*) under **Overwrite Value**.
- Click **Finish**.

Edit Topology Hiding Profile

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

Finish

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 left sidebar shows the navigation menu with 'Topology Hiding' selected under 'Server Configuration'. The main content area is titled 'Topology Hiding Profiles: Service_Provider'. It features a list of profiles on the left, including 'default', 'cisco_th_profile', 'Session_Manager', 'Service_Provider' (highlighted), 'Com Manager', 'CS1000', 'IP Office', and 'test'. The 'Service_Provider' profile is selected, showing a table of topology hiding rules. The table has columns for Header, Criteria, Replace Action, and Overwrite Value. The rules are as follows:

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Refered-By	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	asbw.aliestravip.com
From	IP/Domain	Overwrite	asbw.aliestravip.com
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	asbw.aliestravip.com
Refer-To	IP/Domain	Auto	---

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible. A link 'Click here to add a description.' is also present.

6.3 Domain Policies

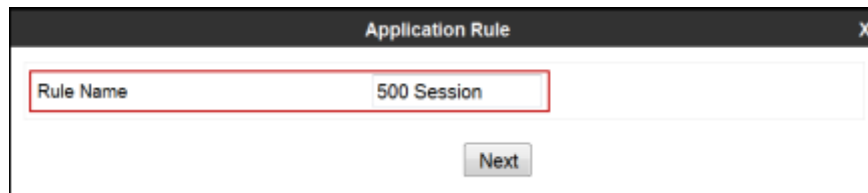
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

6.3.1 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**.

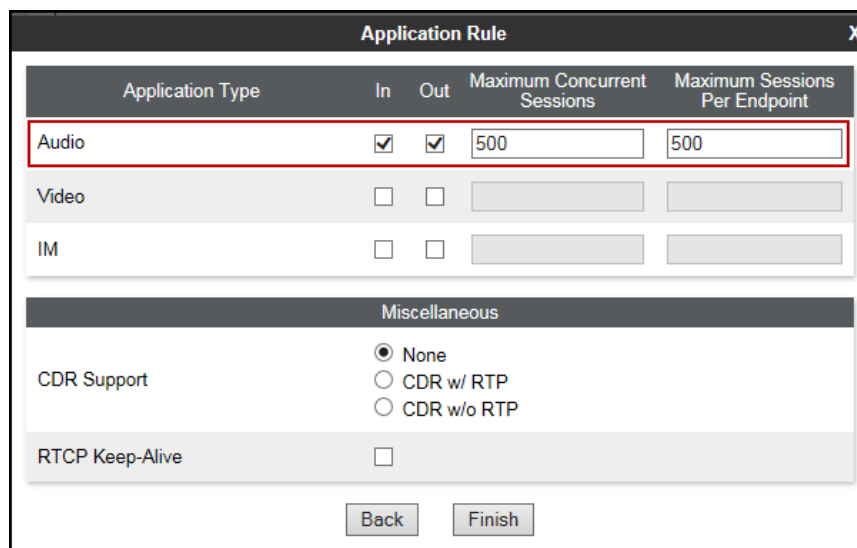


Application Rule

Rule Name 500 Session

Next

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



Application Rule

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

Miscellaneous

CDR Support ☒ None ☐ CDR w/ RTP ☐ CDR w/o RTP

RTCP Keep-Alive ☐

Back Finish

The following screen capture shows the newly created **500 Sessions** Application 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. A left-hand navigation menu lists various configuration areas, with 'Domain Policies' and 'Application Rules' highlighted. The main content area is titled 'Application Rules: 500 Sessions' and features a list of rules on the left, including 'default', 'default-trunk', 'default-subscriber-low', 'default-subscriber-high', 'default-server-low', 'default-server-high', '2000 Sessions', '500 Sessions' (highlighted), 'Remote-Workers', and 'test'. The '500 Sessions' rule is selected, showing its configuration details. The 'Application Rule' section includes a table for 'Application Type' with columns for 'In', 'Out', 'Maximum Concurrent Sessions', and 'Maximum Sessions Per Endpoint'. The 'Audio' rule is configured with 'In' and 'Out' checked, and both session limits set to 500. The 'Video' and 'IM' rules are listed but not configured. Below the table, the 'Miscellaneous' section shows 'CDR Support' set to 'None' and 'RTCP Keep-Alive' set to 'No'. An 'Edit' button is located at the bottom right of the configuration area.

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

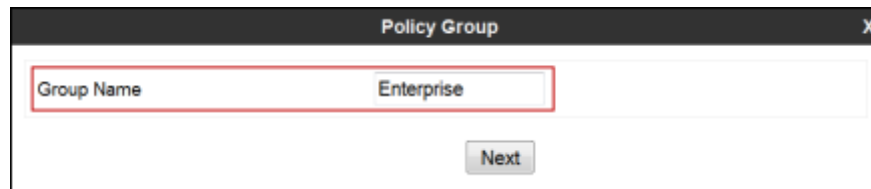
Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

6.3.2 End Point Policy Groups

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

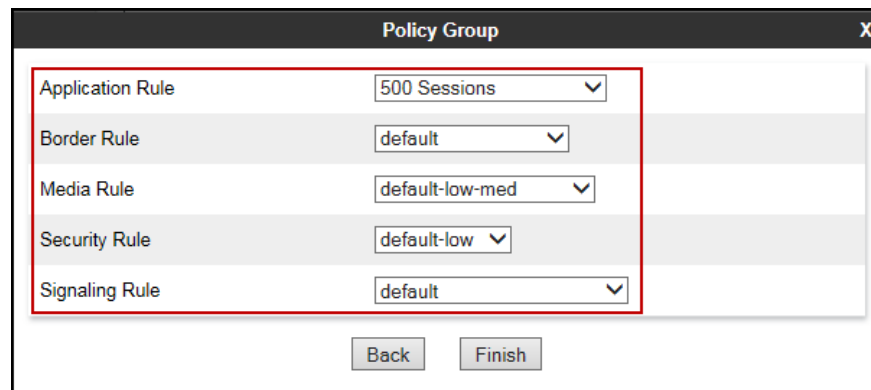
To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups** (not shown).

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



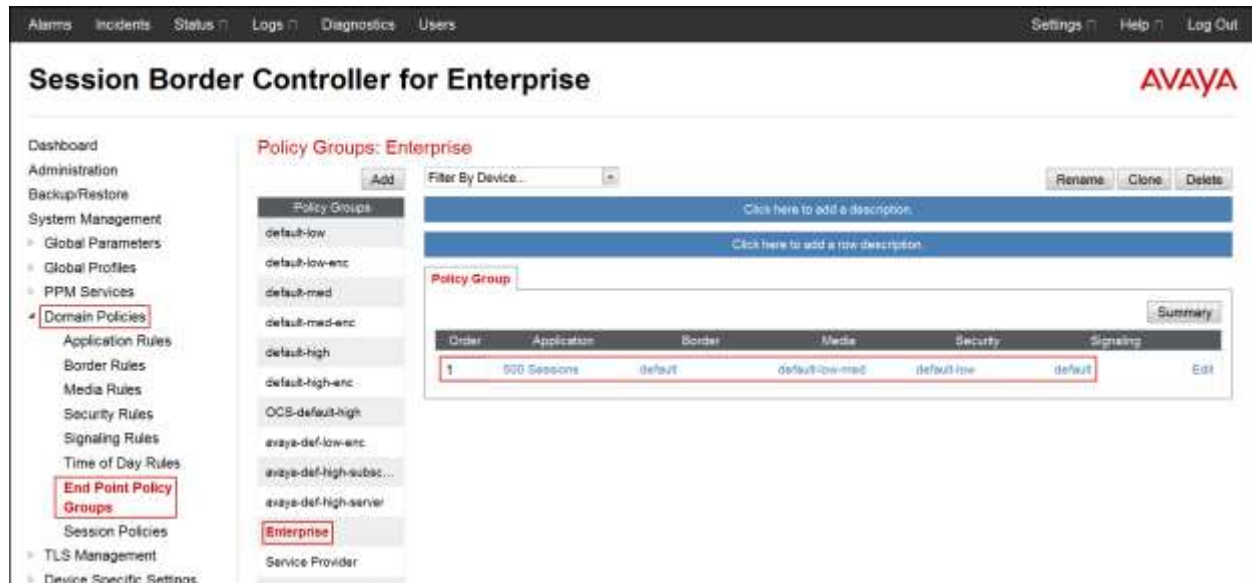
The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" containing the text "Enterprise". Below the input field is a "Next" button.

- **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, but now with five dropdown menus for configuring rules. The rules are: Application Rule (500 Sessions), Border Rule (default), Media Rule (default-low-med), Security Rule (default-low), and Signaling Rule (default). At the bottom of the dialog, there are "Back" and "Finish" buttons. A red rectangle highlights the rule configuration area.

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



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

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

The screenshot shows a 'Policy Group' dialog box. The 'Group Name' field is highlighted with a red border and contains the text 'Service Provider'. A 'Next' button is located below the field.

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

Rule Type	Value
Application Rule	500 Sessions
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default

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

Policy Groups: Service Provider

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

6.4 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.

6.4.1 Network Management

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

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

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

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



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

The screenshot 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 reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. Under "Device Specific Settings", "Network Management" is highlighted. The main content area is titled "Network Management: Avaya SBCE" and features three tabs: "Devices", "Interfaces", and "Networks". The "Interfaces" tab is selected, showing a table with the following data:

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

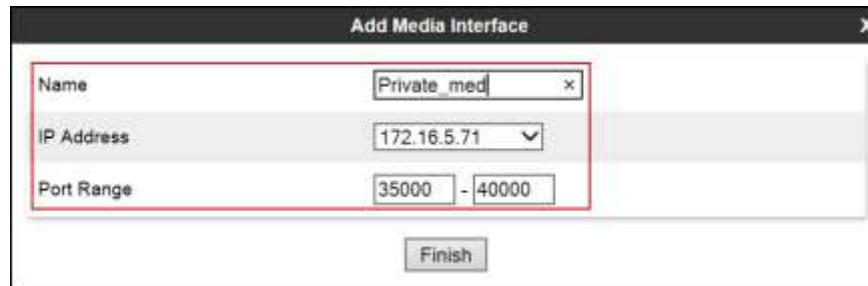
An "Add VLAN" button is located in the top right corner of the interface table.

6.4.2 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.

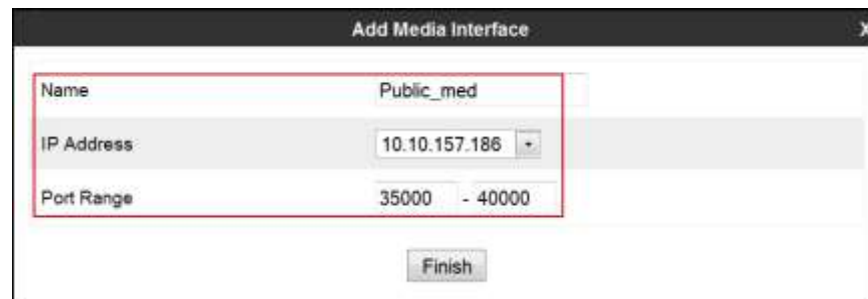
From the **Device Specific Settings** menu on the left-hand side, select **Media Interface** (not shown).

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** *Private_med*.
- Select **IP Address:** *172.16.5.71* (Inside IP Address of the Avaya SBCE, toward IP Office).
- **Port Range:** *35000-40000*.
- Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "Private_med", "IP Address" with the value "172.16.5.71", and "Port Range" with the value "35000 - 40000". A red rectangular box highlights the "Name", "IP Address", and "Port Range" fields. Below the input fields is a "Finish" button.

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** *Public_med*.
- Select **IP Address:** *10.10.157.186* (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **Port Range:** *35000-40000*.
- Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "Public_med", "IP Address" with the value "10.10.157.186", and "Port Range" with the value "35000 - 40000". A red rectangular box highlights the "Name", "IP Address", and "Port Range" fields. Below the input fields is a "Finish" button.

The following screen capture shows the newly created Media Interfaces.

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, a sidebar menu lists various configuration areas, with "Device Specific Settings" and "Media Interface" highlighted. The main content area is titled "Media Interface: Avaya SBCE" and features a "Media Interface" tab. A warning message states: "Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below this, a table lists the configured media interfaces:

Name	Media IP	Port Range	Edit	Delete
Private_med	172.16.5.71	35000 - 40000	Edit	Delete
Public_med	10.10.157.156	35000 - 40000	Edit	Delete
10.10.157.156	10.10.157.156	35000 - 40000	Edit	Delete
10.10.157.156	10.10.157.156	35000 - 40000	Edit	Delete

6.4.3 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*.
- Select **IP Address:** *172.16.5.71* (Inside IP Address of the Avaya SBCE, toward IP Office).
- **UDP Port:** *5060*.
- Click **Finish**.

Add Signaling Interface X

Name	Private_sig
IP Address	172.16.5.71 ▼
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None ▼
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name:** *Public_sig*.
- Select **IP Address:** *10.10.157.186* (outside or public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port:** *5060*.
- Click **Finish**.

Add Signaling Interface

Name: Public_sig

IP Address: 10.10.157.186

TCP Port:
Leave blank to disable

UDP Port: 5060
Leave blank to disable

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

Signaling Interface: Avaya SBCE

Devices: Avaya SBCE

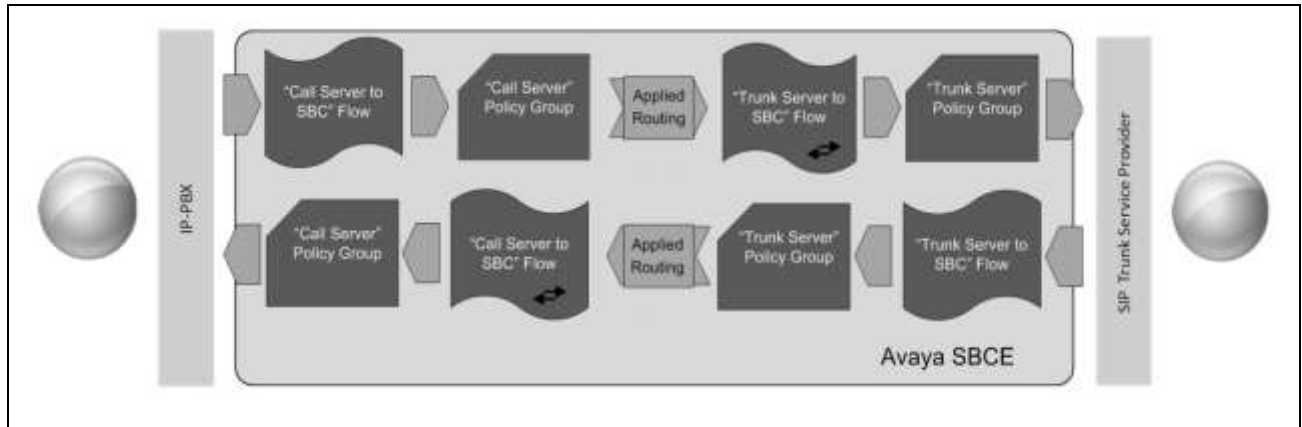
Signaling Interface

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

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	172.16.6.71		5060	---	None	Edit Delete
Public_sig	10.10.157.186	---	5060	---	None	Edit Delete
10.10.157.186	10.10.157.186	---	5060	---	None	Edit Delete
10.10.157.186	10.10.157.186	---	5060	---	None	Edit Delete

6.4.4 End Point Flows

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



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

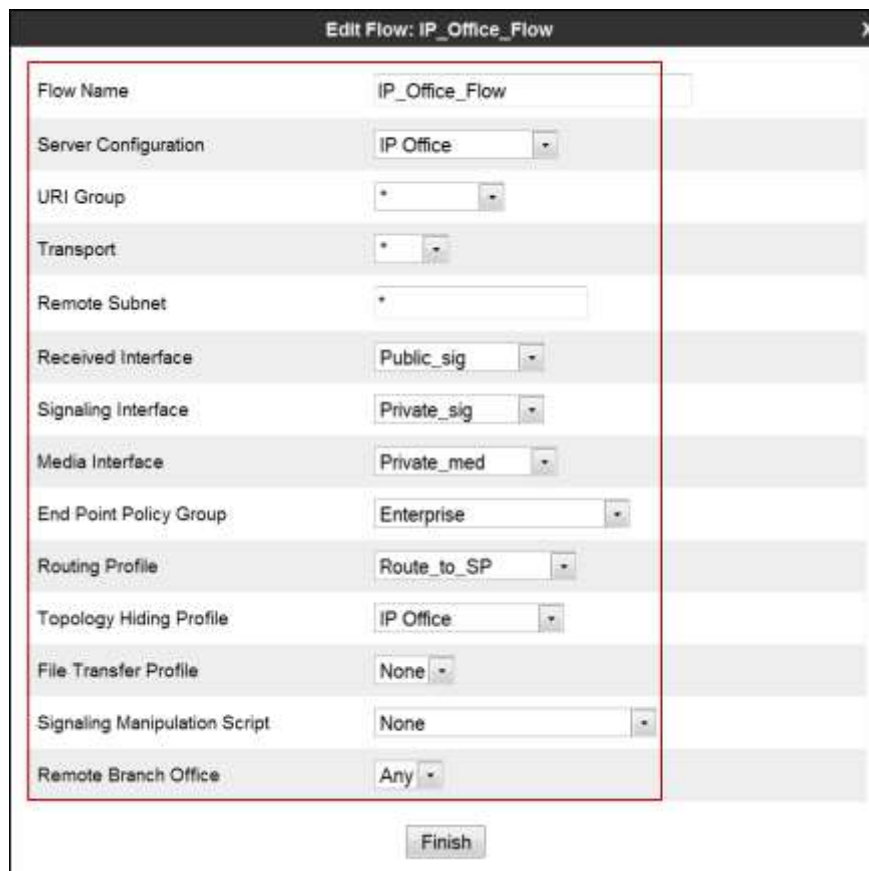
To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows** (not shown), then the **Server Flows** tab. Click **Add** (not shown).

- **Name:** *SIP_Trunk_Flow*.
- **Server Configuration:** *Service Provider*.
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** *Private_sig*.
- **Signaling Interface:** *Public_sig*.
- **Media Interface:** *Public_med*.
- **End Point Policy Group:** *Service Provider*.
- **Routing Profile:** *Route_to_IPO* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *Service_Provider*.
- **File Transfer Profile:** *None*.
- **Signaling Manipulation Script:** *None*.
- **Remote Branch Office:** *Any*.
- Click **Finish**.

Edit Flow: SIP_Trunk_Flow	
Flow Name	SIP_Trunk_Flow
Server Configuration	Service Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
End Point Policy Group	Service Provider
Routing Profile	Route_to_IPO
Topology Hiding Profile	Service_Provider
File Transfer Profile	None
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*.
- **End Point Policy Group:** *Enterprise*.
- **Routing Profile:** *Route_to_SP* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *IP Office*.
- **File Transfer Profile:** *None*.
- **Signaling Manipulation Script:** *None*.
- **Remote Branch Office:** *Any*.
- Click **Finish**.



Edit Flow: IP_Office_Flow	
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
End Point Policy Group	Enterprise
Routing Profile	Route_to_SP
Topology Hiding Profile	IP Office
File Transfer Profile	None
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 "Session Border Controller for Enterprise" and the Avaya logo. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (highlighted), Network Management, Media Interface, Signaling Interface, End Point Flows (highlighted), Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options, and Troubleshooting. The main content area is titled "End Point Flows: Avaya SBCE" and features tabs for "Subscriber Flows" and "Server Flows". Under the "Server Flows" tab, there are two sections: "Server Configuration: IP Office" and "Server Configuration: Service Provider". Each section contains a table of flows. In the "IP Office" section, a flow named "IP_Office_Flow" is highlighted with a red box. In the "Service Provider" section, a flow named "SIP_Trunk_Flow" is highlighted with a red box. Both flows have a priority of 1, a URI Group of "*", and are associated with "Public_sig" and "Private_sig" interfaces. The "IP_Office_Flow" is associated with the "Enterprise" End Point Policy Group and the "Route_to_SP" Routing Profile. The "SIP_Trunk_Flow" is associated with the "Service Provider" End Point Policy Group and the "Route_to_IPD" Routing Profile. Each flow entry includes "View", "Clone", "Edit", and "Delete" action links.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IP_Office_Flow	*	Public_sig	Private_sig	Enterprise	Route_to_SP	View Clone Edit Delete

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

7. Alestra SIP Trunking Configuration

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

During the signup process, Alestra and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Alestra's network. Alestra will provide IP addresses, Direct Inward Dialed (DID) numbers to be assigned to the enterprise. The customer will need to provide the IP address used to reach the Avaya Session Border Controller for Enterprise at the customer's enterprise site. This information is used to complete the Avaya IP Office and Avaya Session Border Controller for Enterprise configuration discussed in the previous sections.

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

8.2 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 Avaya IP Office System Status is installed, log in with the proper credentials.



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).

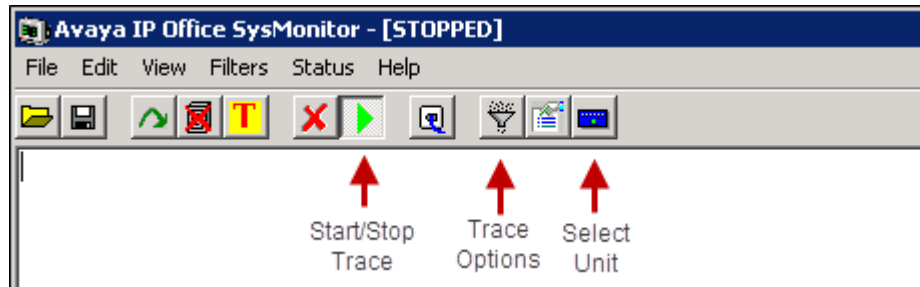
The screenshot shows the Avaya IP Office System Status window. The left pane has a tree view with 'System', 'Alarms (16)', 'Extensions (24)', and 'Trunks (8)'. Under 'Trunks (8)', 'Line:17' is selected. The right pane has tabs for 'Status', 'Unlabeled Summary', and 'Alarms'. The 'Status' tab is active, showing the 'SIP Trunk Summary' for Line 17. The summary includes fields for Line Service State (In Service), Peer Domain Name (sip://172.16.5.71), Resolved Address (172.16.5.71), Line Number (17), Number of Administered Channels (10), Number of Channels in Use (0), Administered Compression (G729 A, G711 A, G711 Mu), Enable Faststart (OFF), Silence Suppression (OFF), Media Stream (RTP), Layer 4 Protocol (UDP), SIP Trunk Channel Licenses (Unlimited), SIP Trunk Channel Licenses in Use (0), and SIP Device Features (REFER (Incoming and Outgoing), UPDATE (Incoming and Outgoing)). A green circle indicates 0% usage. Below the summary is a table with 10 columns: Channel Number, URI Group, Call Ref, Current State, Time in State, Remote Media Address, Codec, Connection Type, Caller ID or Dated Digits, and Other Party on Call. The table shows 10 channels, all with a 'Current State' of 'Idle' and 'Time in State' of '2 days 18:35:29'. At the bottom are buttons for Trace, Trace All, Pause, Ping, Call Details, Graceful Shutdown, Force Out of Service, Print..., and Save As...

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

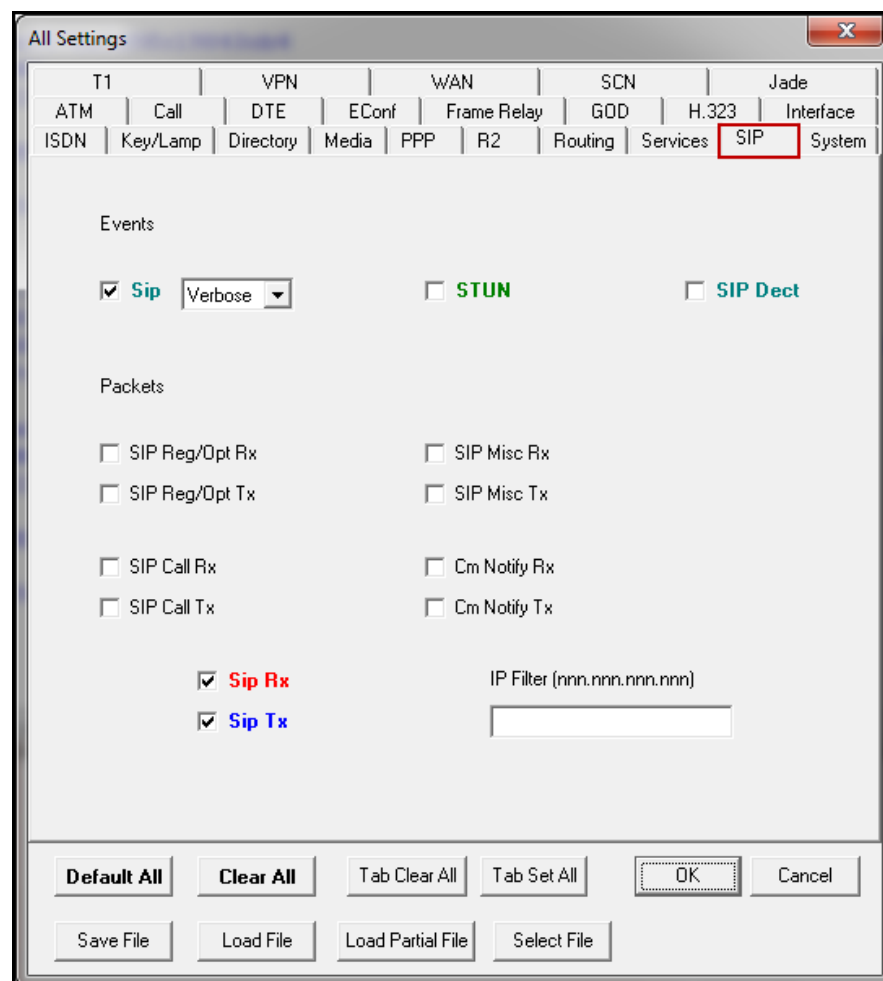
The screenshot shows the Avaya IP Office System Status window with the 'Alarms' tab selected. The left pane is the same as the previous screenshot. The right pane shows 'Alarms for Line: 17 SIP sip://172.16.5.71'. Below this is a table with 3 columns: Last Date Of Error, Occurrences, and Error Description. The table contains one row with the date '5/15/2015 2:28:04 PM', 1 occurrence, and the error description 'Trunk out of Service'. At the bottom are buttons for Ping, Clear, Clear All, Graceful Shutdown, Force Out of Service, Print..., and Save As...

8.3 IP Office Monitor

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



Clicking the **Trace Options** icon on the taskbar 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 the desired color.



8.4 Avaya Session Border Controller for Enterprise

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

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

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) Dashboard. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is divided into several sections:

- Information:** A table showing system details.

Information	
System Time	11:51:08 PM GMT-06:00 Refresh
Version	6.3.1-22-4653
Build Date	Fri Nov 21 17:35:09 EST 2014
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
- Installed Devices:** A list of devices.

Installed Devices
EMS
Avaya SBCE
- Alarms (past 24 hours):** A section indicating "None found."
- Incidents (past 24 hours):** A list of incidents.

Incidents (past 24 hours)
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
- Notes:** A section indicating "No notes found."

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

The screenshot shows the Avaya Alarm Viewer page. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is divided into several sections:

- Devices:** A list of devices.

Devices
EMS
Avaya SBCE
- Alarms:** A section showing a table of alarms for the selected device.

ID	ID	Details	State	Time	Device
No alarms found for this device.					
- Buttons:** Two buttons, "Clear Selected" and "Clear All", are located at the bottom of the Alarms section.

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

Session Border Controller for Enterprise AVAYA

Dashboard

Information

System Time	11:51:08 PM GMT-06:00	Refresh
Version	6.3.1-22-4653	
Build Date	Fri Nov 21 17:35:08 EST 2014	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	

Installed Devices

EMS
Avaya SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message

[Add](#)

Notes

No notes found.

The following screen shows the Incident Viewer page.

Incident Viewer AVAYA

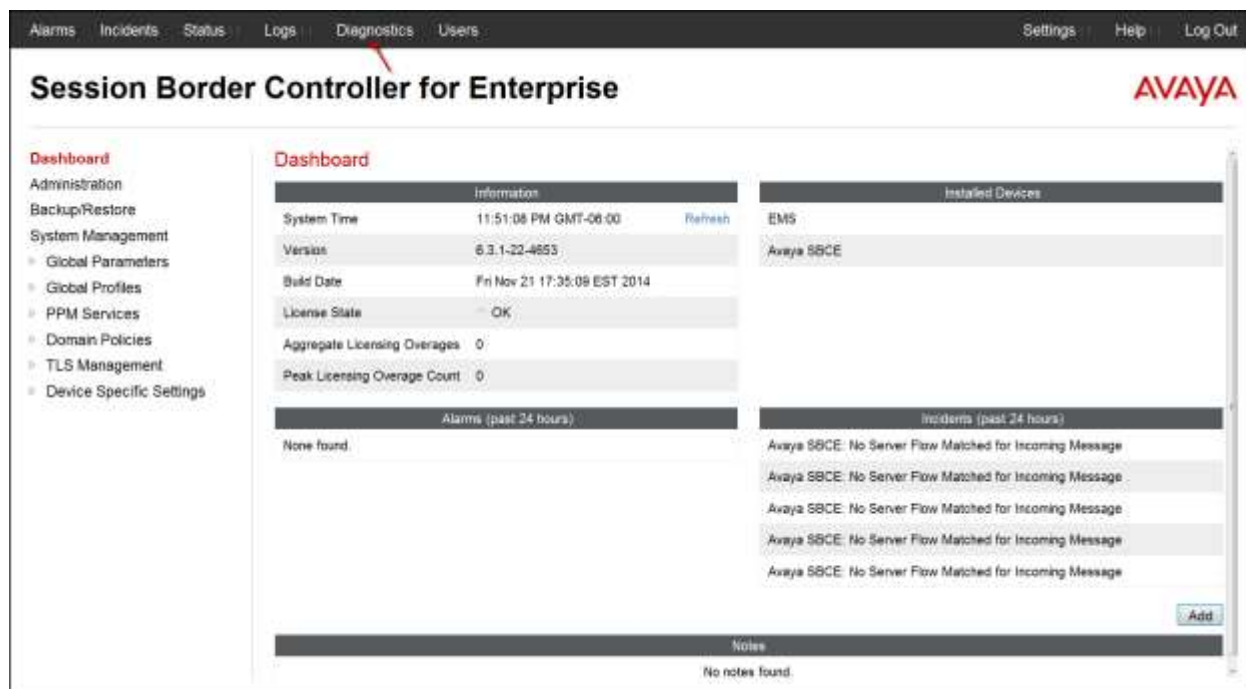
Device: Avaya SBCE Category: Protocol Discrepancy [Clear Filters](#) [Refresh](#) [Generate Report](#)

Displaying results 0 to 0 out of 0.

Type	ID	Date	Time	Category	Device	Cause
No incidents found.						

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. Note that IP addresses have been blurred out for security reasons.



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 SBCE web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand sidebar contains a tree menu with categories like Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (highlighted), Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options, Troubleshooting (highlighted), Debugging, Trace (highlighted), DoS, and Learning. The main content area is titled "Trace: Avaya SBCE" and features three tabs: Devices, Packet Capture (selected), and Captures. Under the "Packet Capture" tab, there is a "Packet Capture Configuration" form. The form includes the following fields: Status (Ready), Interface (Any), Local Address (IPv4) (All), Remote Address (IPv4 Port, IPv6 Port) (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (Test_1.pcap, with a note: "Using the name of an existing capture will overwrite it."). At the bottom of the form 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 (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 "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration options, with "Device Specific Settings" and "Troubleshooting" highlighted. The "Trace" option under "Troubleshooting" is also visible. The main content area is titled "Trace: Avaya SBCE" and features two tabs: "Packet Capture" and "Captures". The "Captures" tab is active, showing a table of captured files. The table has columns for "File Name", "File Size (bytes)", and "Last Modified". A single entry is listed: "Test_1_20150309040311.pcap" with a size of 1,088,560 bytes and a last modified date of March 9, 2015 3:04:02 AM GMT-06:00. A "Delete" link is present next to the entry. A "Refresh" button is located in the top right corner of the table area.

File Name	File Size (bytes)	Last Modified
Test_1_20150309040311.pcap	1,088,560	March 9, 2015 3:04:02 AM GMT-06:00

9. Conclusion

These Application Notes describe the configuration steps necessary for configuring Session Initiation Protocol (SIP) Trunk Service for an enterprise solution consisting of Avaya IP Office Release 9.1 and the Avaya Session Border Controller for Enterprise Rel. 6.3 to interoperate with Alestra SIP Trunking Service, as shown in **Figure 1**.

Alestra SIP Trunking Service passed compliance testing 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 and the Avaya Session Border Controller for Enterprise, including the following, is available at: <http://support.avaya.com/>

- [1] *Avaya IP Office Platform Solution Description, Release 9.1*, Issue 1, December 2014.
- [2] *Avaya IP Office Platform Feature Description, Release 9.1*, Issue 1, December 2014.
- [3] *IP Office Platform 9.1 Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 30g, January 2015.
- [4] *Administering Avaya IP Office Platform with Manager*, Release 9.1, Issue 10.04, February 2015.
- [5] *IP Office Platform 9.1 Using Avaya IP Office Platform System Status*, Document 15-601758, Issue 10b, October 30, 2014.
- [6] *IP Office Platform 9.1 Using IP Office System Monitor*, Document 15-601019, Issue 06b, November 13, 2014.
- [7] *Using Avaya Communicator for Windows on IP Office*, Release 9.1, December 2014.
- [8] *Administering Avaya Communicator on IP Office*, Release 9.1, December 2014.
- [9] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.
- [10] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 6.3, Issue 3, October 2014.
- [11] *Configuring the Avaya Session Border Controller for IP Office Remote Workers*.
<https://downloads.avaya.com/css/P8/documents/100177106>

Additional Avaya IP Office documentation can be found at:
<http://marketingtools.avaya.com/knowledgebase/>

Product documentation for Alestra SIP Trunking Service is available from Alestra.

11. Appendix A: SigMa Script

The following Signaling Manipulation script was used in the configuration of the Avaya SBCE,
Section 6.2.3:

Title: Remove Remote Address

```
//Remove Remote-Address header in outbound INVITEs and 200 OK messages
```

```
within session "ALL"
```

```
{  
act on message where %DIRECTION="OUTBOUND" and  
%ENTRY_POINT="POST_ROUTING"  
{  
  remove(%HEADERS["Remote-Address"][1]);  
}  
}
```

©2015 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.