



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Frontier SIP Trunking with Avaya IP Office 9.0.3 and Avaya Session Border Controller 6.2.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Frontier (Metaswitch platform) and Avaya IP Office release 9.0.3 and Avaya Session Border Controller for Enterprise release 6.2.1.

Frontier SIP Trunking provides PSTN access via a SIP trunk between the enterprise and the Frontier network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Frontier 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.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking with service provider Frontier, Avaya IP Office system and Avaya Session Border Controller for Enterprise (Avaya SBCE). In the sample configuration, the Avaya IP Office (IPO) solution consists of an Avaya IP Office 500v2 Release 9.0, Avaya Voicemail Pro, Avaya IP Office Softphone, and Avaya H.323, digital, and analog endpoints.

The Frontier SIP Trunking service referenced within these Application Notes is designed for business customers. The service enables local and long distance PSTN calling via standards-based SIP trunks as an alternative to legacy analog or digital trunks, without the need for additional TDM enterprise gateways and the associated maintenance costs.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office to connect to Frontier SIP Trunking service via Avaya SBCE. This configuration (shown 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

A simulated enterprise site with Avaya IP Office was connected to Frontier's SIP Trunking service via Avaya Session Border Controller. To verify SIP trunking interoperability, the following features and functionality were exercised during the interoperability compliance test:

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types. Phone types included H.323, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from the Avaya IP Office Softphone.
- Inbound and outbound long holding time call stability.
- Various call types including: local, long distance, international, outbound toll-free, operator service and directory assistance.
- Codec G.711MU and G.729A.
- Caller number/ID presentation.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.

- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- Telephony features such as hold and resume, transfer, and conference.
- Use of SIP REFER for call transfer to PSTN
- FAX G.711 Pass Through and T.38.
- Off-net call forwarding.
- Twinning to mobile phones on inbound calls
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public internet as enterprise phones.

2.2. Test Results

Frontier SIP Trunking passed compliance testing.

Items not supported or not tested included the following:

- Inbound toll-free and outbound emergency calls (911) are supported but were not tested as part of the compliance test.
- T.38 Fax is not fully supported.

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

- **Incorrect Call Display on PSTN Phone** – Call display was not properly updated on PSTN phone involved in a call transfer. After the call transfer was completed, the PSTN phone did not display the actual connected party but instead showed the party that initiated the transfer. However, the call transfer is completed with 2 way voice path.
- **Consultative Transfer using REFER on SIP Desk-phone** – Scenario of Inbound and Outbound calls to transfer the calls from one PSTN to another PSTN phone. After pressing “Transfer” button to complete the call transfer on the SIP Desk-phone, 11XX series, the phone displayed “Transfer failed”. The 11XX desk-phone is still active and in off-hook state. Hanging up the phone will put the phone back on-hook state. There is no impact on user experience; both PSTN phones have 2 ways speech path, PSTN originator and PSTN transferee. Work around is from **Line** → Line Number (in this case is **19**), select **SIP Line** tab. Leave **REFER Support** checked, but for **Incoming** and **Outgoing**, select **NEVER** from pull down menu.
- **Call Display on PSTN Phone on PSTN Hold and Resume** – Call display was not properly updated on PSTN phone involved in PSTN Hold and Resume operation. After the inbound call from PSTN to Avaya IP Office, the call was put on hold by PSTN phone, when the call was resumed, the PSTN phone displayed trunk number instead of the calling party ID.
- **T.38 Faxing** – Frontier supports outbound T.38 faxing only for local calls. Outbound long-distance T.38 faxing failed: Frontier responded to T.38 re-INVITE from Avaya IP Office with "488 Not Acceptable Here". Inbound T.38 faxing worked properly. Plain G.711u faxing worked fine for outbound faxing. During compliance testing, a workaround configuration (T.38 with Fallback) was administered on Avaya IP Office (see **Section 5.4.2**) so that inbound faxing used T.38; outbound faxing used T.38 for local faxing call and G.711u for long-distance faxing call.

2.3. Support

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

For technical support on Frontier SIP Trunking service, contact Frontier at <https://frontier.com/enterprise>

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to Frontier SIP Trunking service via Avaya SBCE through the public IP network. For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers.

Located at the enterprise site is an Avaya IP Office 500v2 with the MOD DGTL STA16 expansion which provides connections for 16 digital stations to the PSTN. The extension PHONE 8 card which provides connections for 8 analog stations to the PSTN as well as 64-channel VCM (Voice Compression Module) for supporting VoIP codecs. The LAN port of Avaya IP Office is connected to the enterprise LAN while the WAN port is connected to the public IP network.

The enterprise endpoints include both Remote Worker and local extensions. The local endpoints are an Avaya 9600 Series IP Telephone (with H.323 firmware), an Avaya 9508 Digital Telephone, an Avaya Symphony 2000 Analog Telephone, Avaya IP Office Softphone and 11XX series SIP phone. A separate Windows XP PC runs Avaya IP Office Manager to configure and administer the Avaya IP Office. The Remote Worker is Avaya Flare Experience for Windows.

Mobility Twinning is configured for some of the Avaya IP Office users so that calls to these user phones will also ring and can be answered at the configured mobile phones.

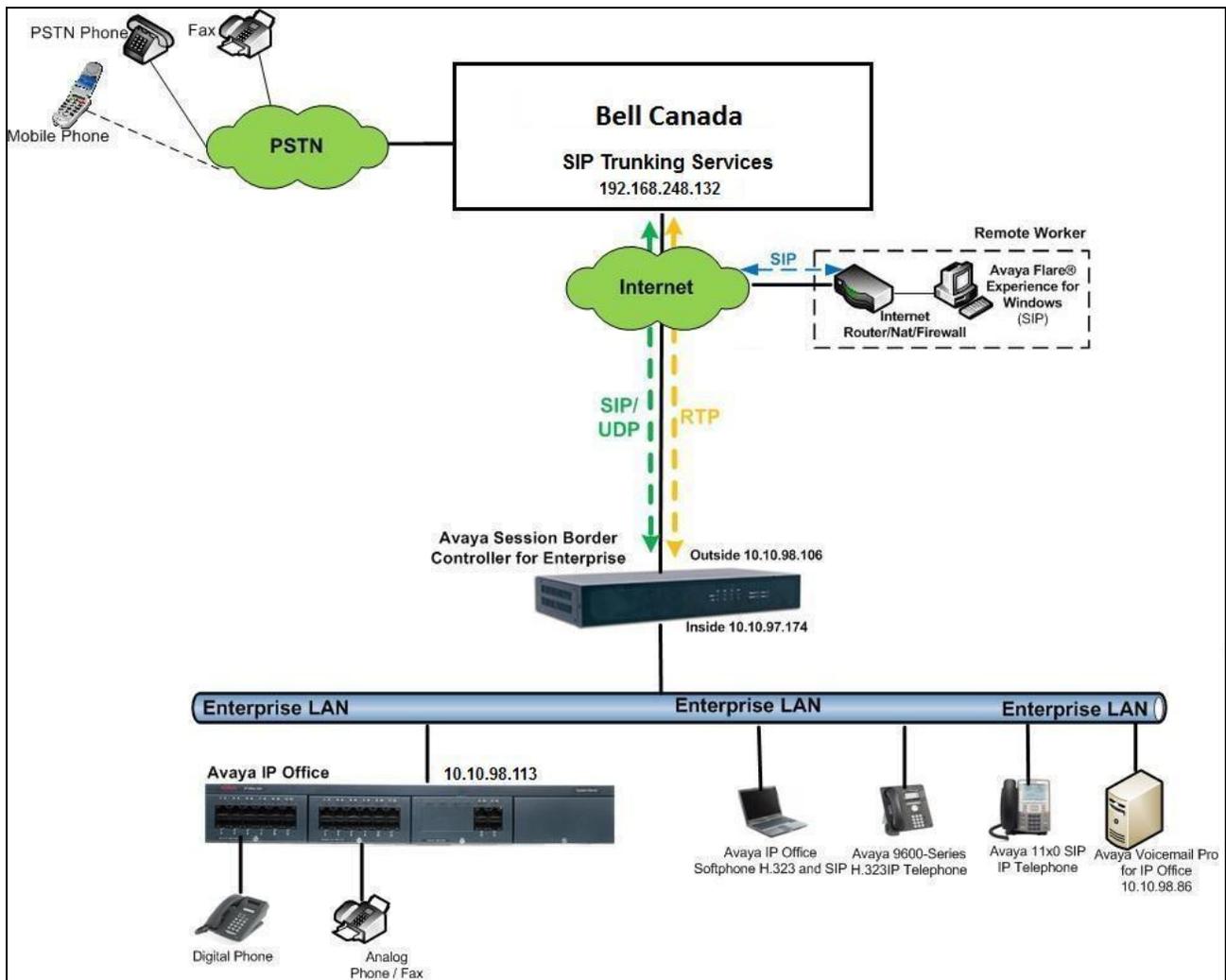


Figure 1: Test Configuration for Avaya IP Office with Frontier SIP Trunking Service

For the purposes of the compliance test, Avaya IP Office users dialed a short code of 9 + N digits to send digits across the SIP trunk via Avaya SBCE to Frontier. The short code of 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Frontier. For calls within the North American Numbering Plan (NANP), the user would dial 11 (1 + 10) digits. Thus for these NANP calls, Avaya IP Office would send 11 digits in the Request URI and the To field of an outbound SIP INVITE message. It was configured to send 10 digits in the From field. For inbound calls, Frontier SIP Trunking sent 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

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

4. Equipment and Software Validated

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

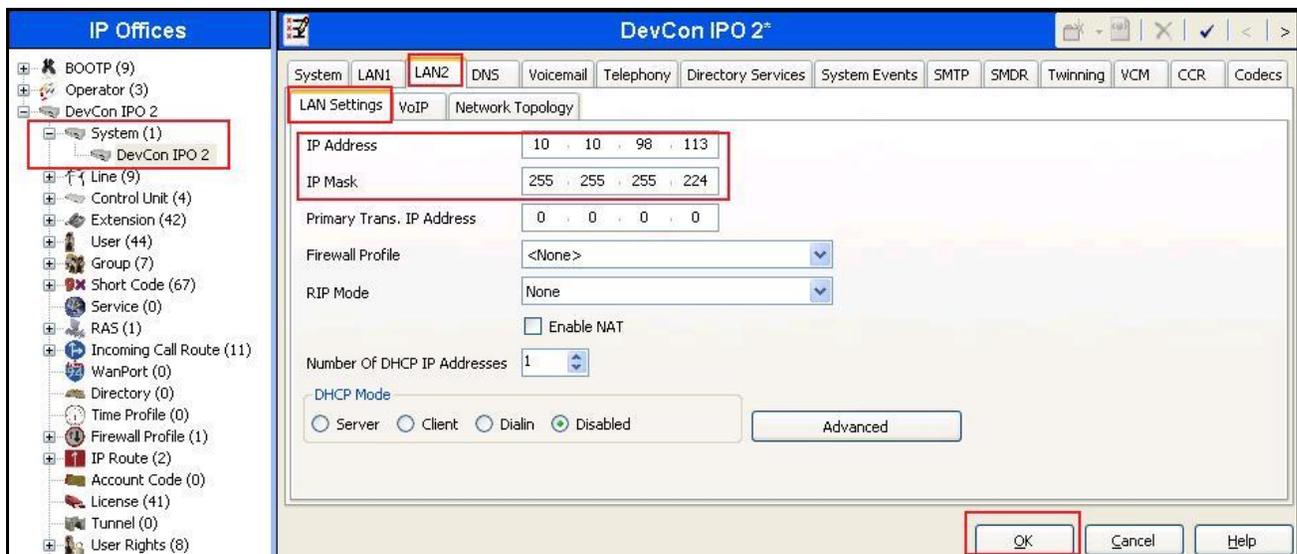
Avaya Telephony Components	
Equipment	Release
Avaya IP Office 500v2	9.0.300.941
Avaya IP Office Manager	9.0.300.941
Avaya Voicemail Pro for IP Office	9.0.300.941
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.2 (6.2.1.Q07)
Avaya 11x0 IP Telephone (SIP)	SIP11x0e04.03.12.00
Avaya 9630G IP Telephone (H.323)	Avaya one-X® Deskphone Edition S3.2
Avaya IP Office Softphone	3.2.3.20 64770
Avaya Digital Telephone (9508)	N/A
Avaya Symphony 2000 Analog Telephone	N/A
Frontier SIP Trunking Service Components	
Component	Release
Acme Packet Net-Net 4000 SBC	6.2
Metaswitch	8.1

5. Configure IP Office

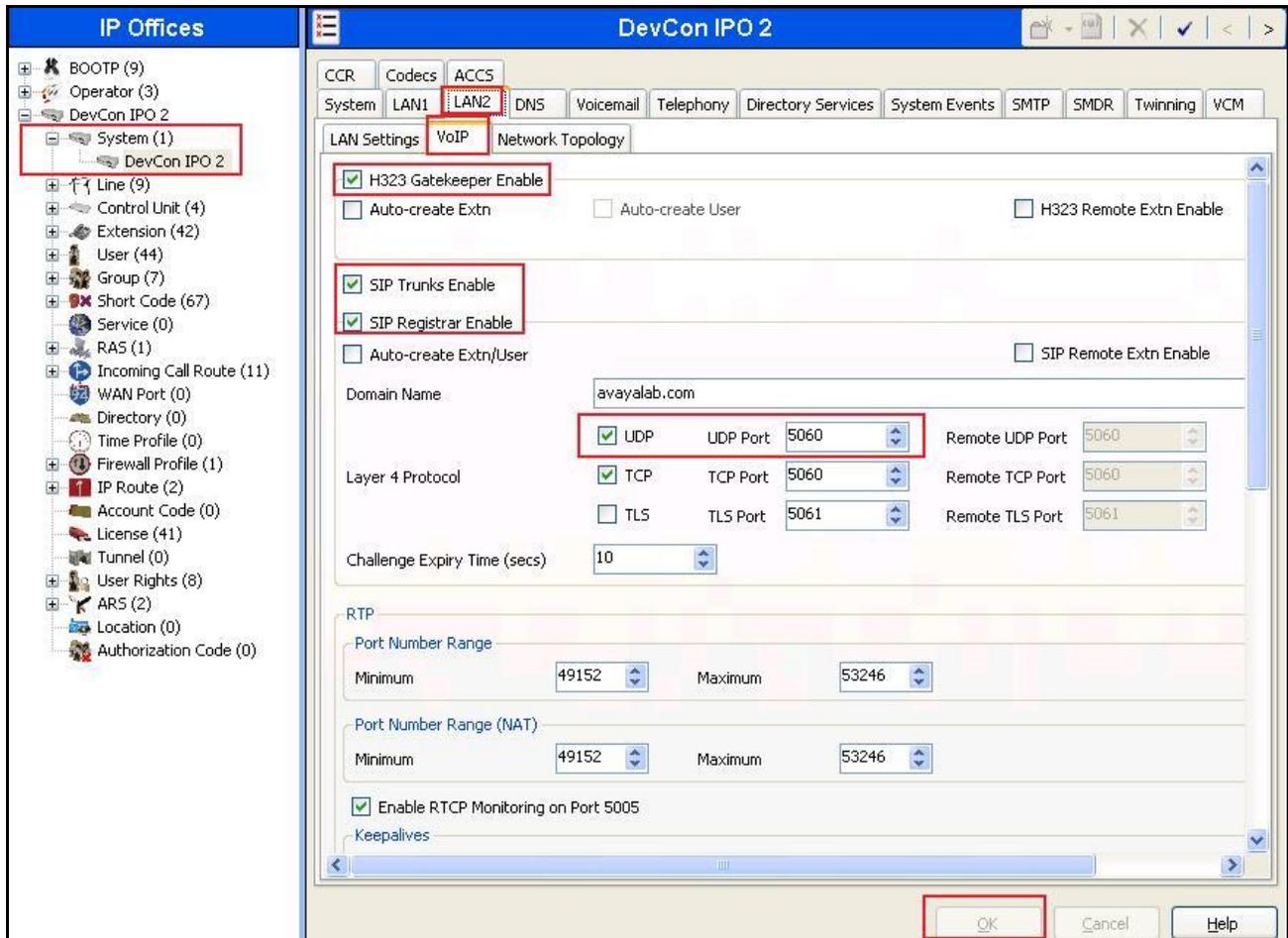
This section describes the Avaya IP Office configuration to support connectivity to Frontier SIP Trunking service through Avaya SBCE. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials. A management window will appear similar to the one shown in the next section. The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this section, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center, and the Details pane on the right side. These panes will be referenced throughout the Avaya IP Office configuration. Proper licensing as well as standard feature configurations that are not directly related to the interface with the service provider (such as LAN interface to the enterprise site and IP Office Softphone support) is assumed to be already in place.

5.1. LAN Settings

In the sample configuration, the **DevCon IPO2** was used as the system name and the WAN port was used to connect the Avaya IP Office to the public network. The LAN2 settings correspond to the WAN port on the Avaya IP Office. To access the LAN settings, first navigate to **System (1) → DevCon IPO2** in the Navigation and Group Panes and then navigate to the **LAN2 → LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office WAN port. Set the **IP Mask** field to the mask used on the public network. All other parameters should be set according to customer requirements. Then click **OK** to submit.



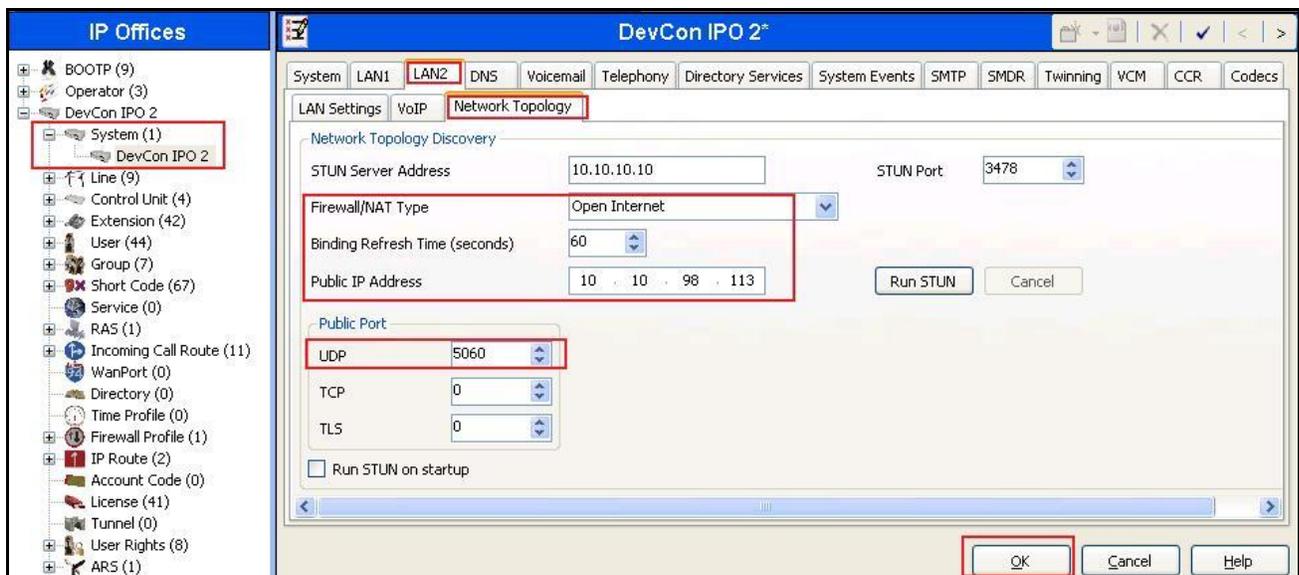
Select the **VoIP** tab as shown in the following screen. The **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such the 9600-Series IP Telephones used in the sample configuration. The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks to Frontier. The **SIP Registrar Enable** box is checked to allow Avaya IP Office Softphone usage. The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Based on this setting, Avaya IP Office would request RTP media be sent to a UDP port in the configurable range for calls using **LAN2**. The specific values used for the compliance test are shown in the example below. All other parameters should be set according to customer requirements. Then click **OK** to submit.



On the **Network Topology** tab in the Details Pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. No firewall or network address translation (NAT) device was used in the compliance test as shown in **Figure 1**, so the parameter was set to **Open Internet**. With this configuration, STUN will not be used.
- Set **Binding Refresh Time (seconds)** to **60**. This value is used as one input to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider. See **Section 5.9** for complete details.
- Set **Public IP Address** to the IP address of the Avaya IP Office WAN port. **Public Port** is set to **5060**.
- All other parameters should be set according to customer requirements.

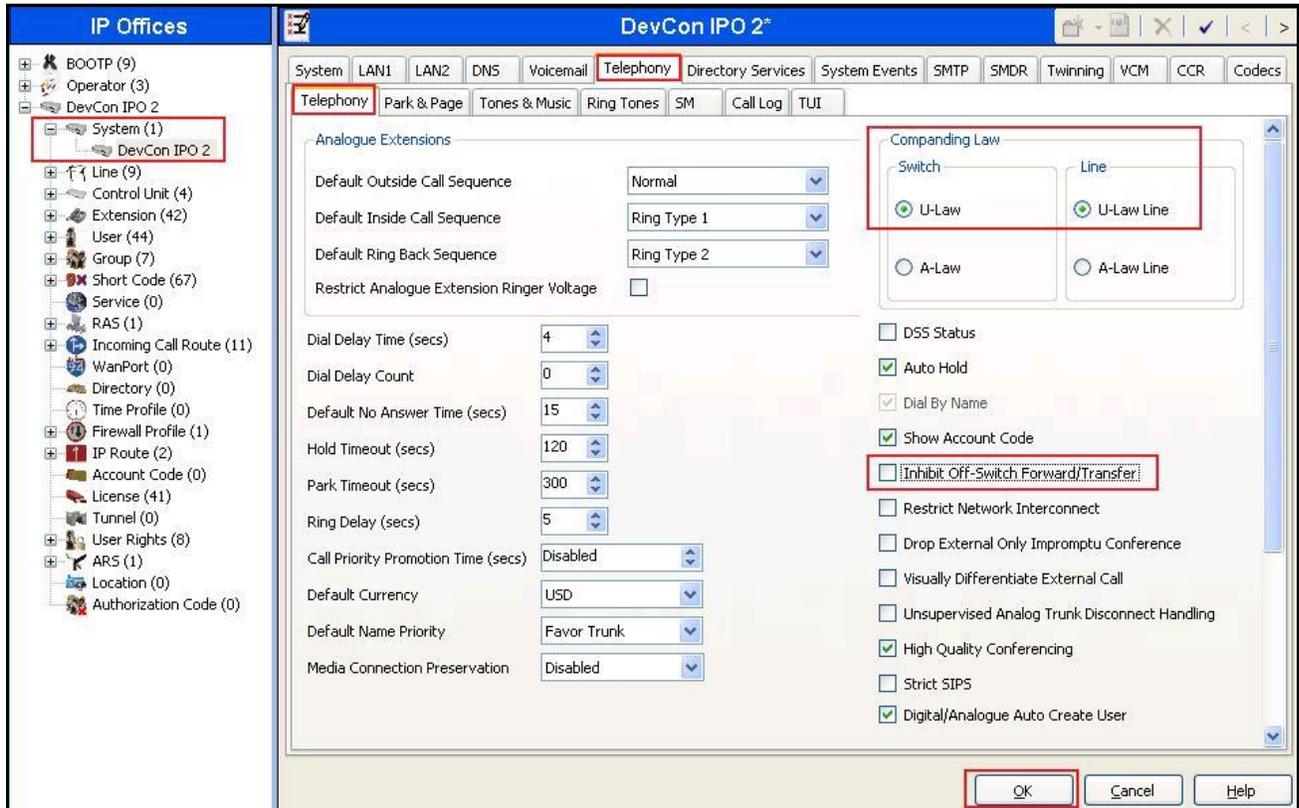
Click **OK** to submit.



In the compliance test, the **LAN1** interface was used to connect the Avaya IP Office to the enterprise site IP network. The **LAN1** interface configuration is not directly relevant to the interface with Frontier SIP Trunking service, and therefore is not described in these Application Notes.

5.2. System Telephony Settings

Navigate to the **Telephony** → **Telephony** Tab in the Details Pane. Choose the **Companding Law** typical for the enterprise location. For North America, **U-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the service provider across the SIP trunk. Then click **OK**.



5.3. Twinning Calling Party Settings

When using twinning, the calling party number displayed on the twinned phone is controlled by two parameters. These parameters only affect twinning and do not impact the messaging or operation of other redirected calls such as forwarded calls. The first parameter is the **Send original calling party information for Mobile Twinning** box on the **System→Twinning** tab. The second parameter is the **Send Caller ID** parameter on the **SIP Line** form (shown in **Section 5.4**).

For the compliance testing, the **Send original calling party information for Mobile Twinning** as shown below was unchecked. This setting allows the **Send Caller ID** parameter that is set to **Diversion Header** in **Section 5.4.2** to be used. IP Office will send the following in the “From” header:

- On calls from an internal extension to a twinned phone, IP Office sends Calling Party Number of the originating extension.
- On calls from the PSTN to a twinned phone, IP Office sends Calling Party Number of the originating PSTN party.
- Click **OK** (not shown).



5.4. Administer SIP Line

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

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

- IP addresses.
- SIP Credentials (if applicable).
- SIP URI entries.
- 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 **Sections 5.4.2**.

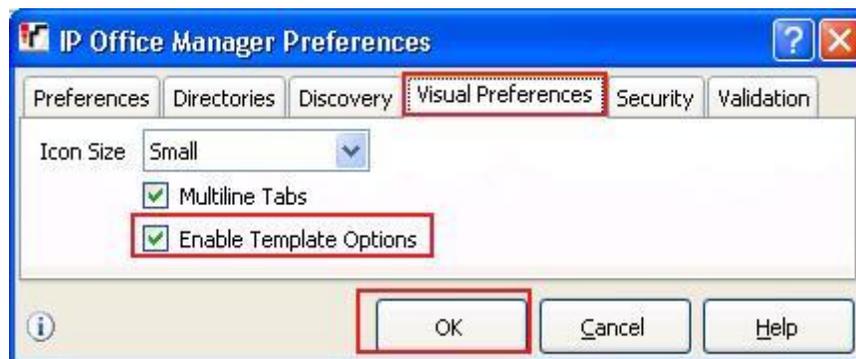
Also, the following SIP Line settings are not supported on Basic Edition:

- SIP Line – Originator number for forwarded and twinning calls.
- Transport – Second Explicit DNS Server.
- SIP Credentials – Registration Required.

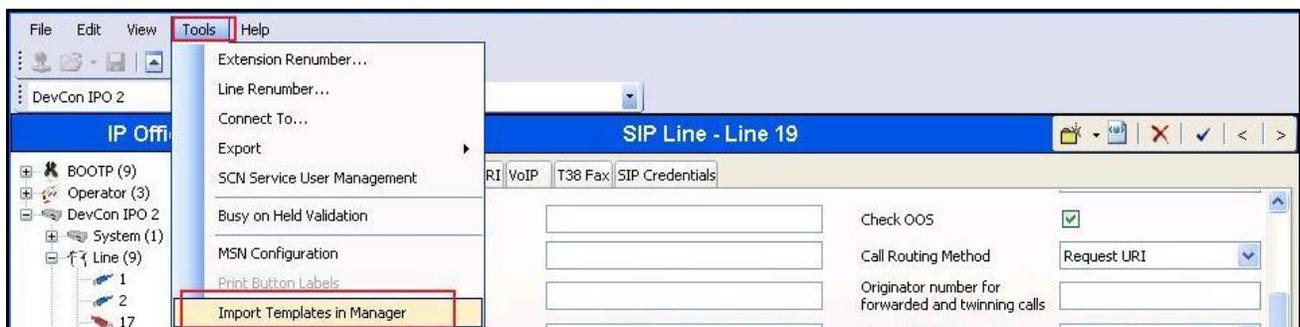
Alternatively, a SIP Line can be created manually. To do so right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2**.

5.4.1. Create SIP Line From Template

1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **FTSIPTIPO9SBC62.xml**. The file name is important in locating the proper template file in **Step 5**.
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. Verify that the box is checked next to **Enable Template Options**. Click **OK**.

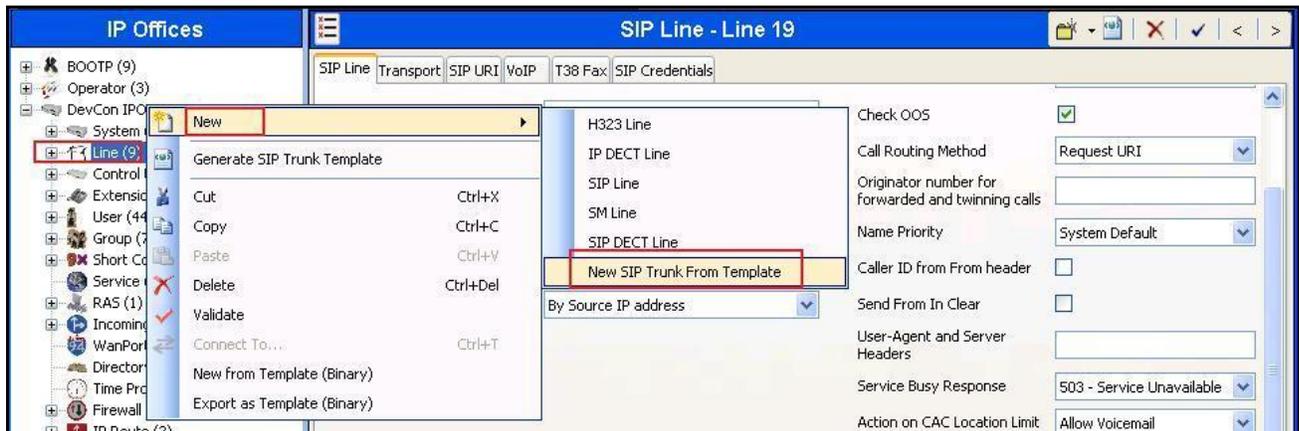


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.



In the pop-up window (not shown) that appears, select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Then click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

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



- In the subsequent Template Type Selection pop-up window, select **United States** from the **Country** pull-down menu and select **Frontier** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**FTSIPTIPO9SBC62.xml**) created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.



- Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2**.

5.4.2. Create SIP Line Manually

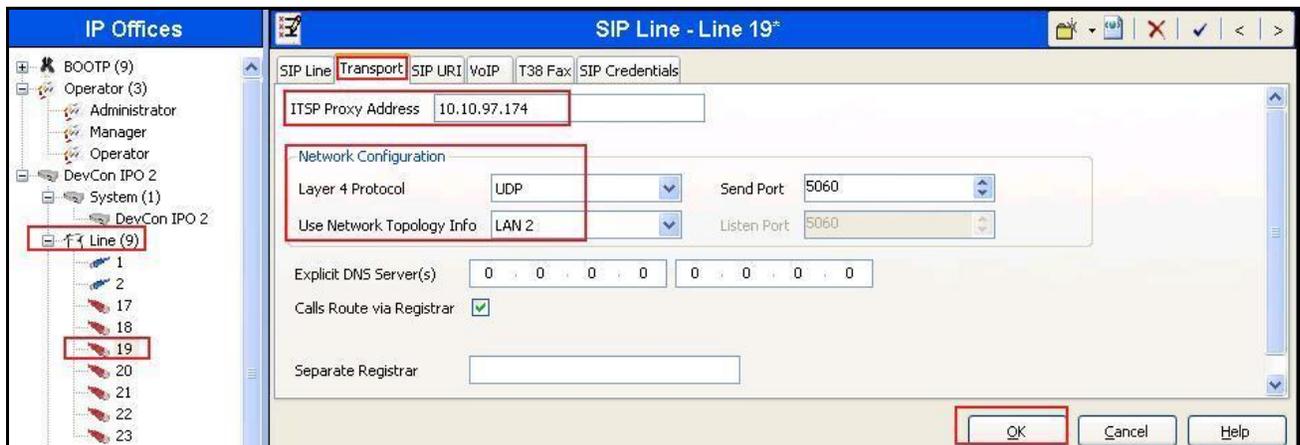
To create a SIP line, begin by navigating to **Line** in the left Navigation Pane, then right-click in the Group Pane and select **New** → **SIP Line**. On the **SIP Line** tab in the Details Pane, configure the parameters as shown below:

- Set **ITSP Domain Name** to the enterprise domain so that IP Office uses this domain as the host portion of SIP URI in SIP headers such as the From header. In this configuration, **ITSP Domain Name** is the internal interface IP address of AVAYA SBCE as shown in **Figure 1**.
- Set **Send Caller ID** to **Diversion Header**.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Default values may be used for all other parameters.

The area of the screen entitled **REFER Support** is used to enable/disable SIP REFER for call transfers. The default values of “Auto” for **Incoming** and **Outgoing** effectively disable use of SIP REFER. To enable SIP REFER, select “**Always**” from the drop-down menu for **Incoming** and **Outgoing**. In the compliance test, both configurations were successfully tested to transfer a call between a PSTN phone and an enterprise phone to a second PSTN phone. Then click **OK**.

The screenshot displays the Avaya IP Office configuration interface for a SIP Line. The left pane shows a tree view of IP Offices with 'Line (9)' selected. The main pane shows the 'SIP Line - Line 19*' configuration. Key fields are highlighted with red boxes: Line Number (19), ITSP Domain Name (10.10.97.174), In Service (checked), Check OOS (checked), Send Caller ID (Diversion Header), and the REFER Support section (checked, Incoming: Auto, Outgoing: Auto). The bottom right shows OK, Cancel, and Help buttons.

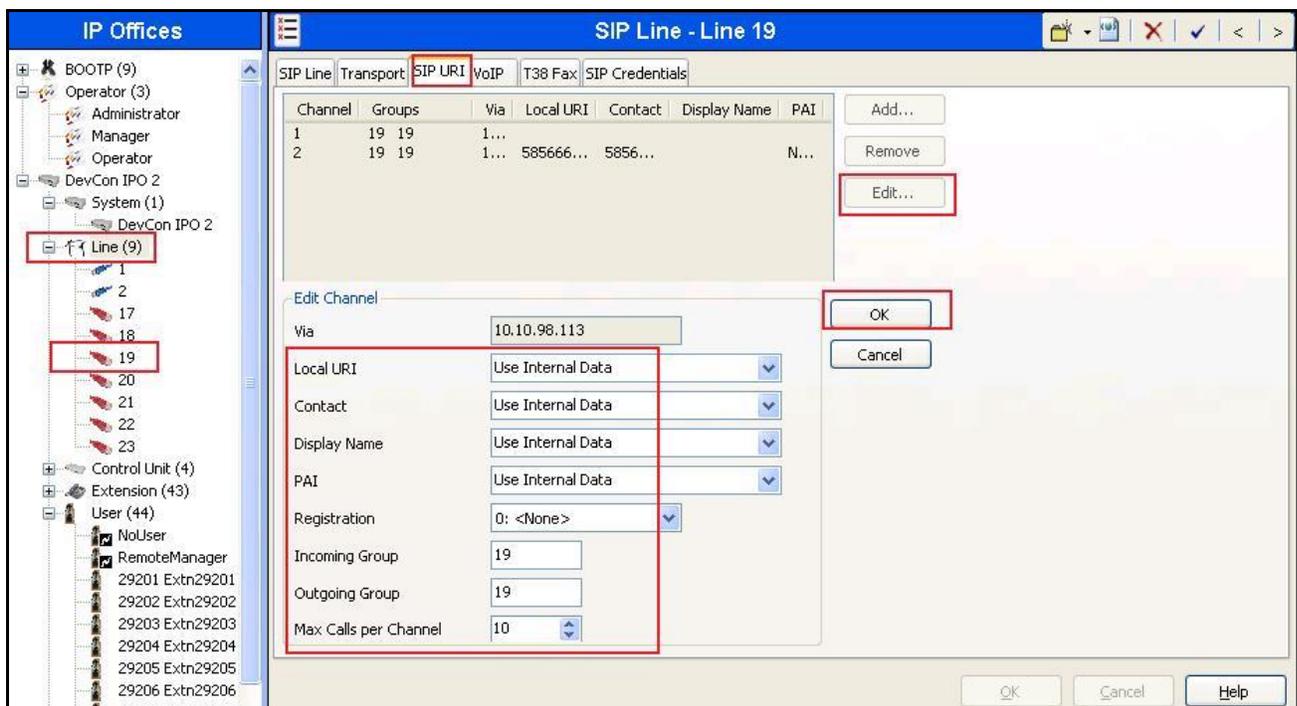
Select the **Transport** tab. The **ITSP Proxy Address** is set to internal interface IP address of AVAYA SBCE as shown in **Figure 1**. In the **Network Configuration** area, **UDP** is selected as the **Layer 4 Protocol**, and the **Send Port** is set to the port number provided by Frontier. The **Use Network Topology Info** parameter is set to **LAN 2**. This associates the SIP Line with the parameters in the **System** → **LAN2** → **Network Topology** tab. Other parameters retain default values in the screen below. Then click **OK**.



A SIP URI entry must be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab, click the **Add** button and then **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 is edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact** and **Display Name** to *Internal Data*. This setting allows calls on this line which SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.6**.
- Set **PAI** to *Internal Data*. With this setting IP Office will populate the SIP P-Asserted-Identity header on outgoing calls with the data set in the **SIP** tab of the call initiating **User** as shown in **Section 5.6**.
- For **Registration**, select the account credentials previously configured on the line's **SIP Credentials** tab.
- Associate this line with an incoming line group 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. For the compliance test, a new incoming and outgoing group **19** was defined that only contains this line (line 19).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK**.

SIP URI entry for Channel 1



SIP URI entry **Channel 2** was similarly created for incoming calls appropriately to pre-define DID numbers as shown in capture below to access to Feature Name Extension 00 (FNE00). The Short Codes for FNE00 was defined in **Section 5.5** to provide Dial Tone and Mobile Callback for mobility extension.

Channel 2 as shown in the screenshot below was configured with following parameters.

- Set the **Local URI** and **Contact** fields to pre-define DID number as mentioned in capture for **Channel 2**.
- Associate **Incoming Group** and **Outgoing Group** to SIP Line **19**.
- Set the **Max Calls per Channel** field to **10**.
- Other parameters retain default values.

Click **OK** to commit.

SIP URI entry for **Channel 2**

The screenshot shows the 'SIP Line - Line 19' configuration window. On the left is a tree view of 'IP Offices' with 'Line (9)' expanded and '19' selected. The main window has tabs for 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', and 'SIP Credentials'. A table lists two channels:

Channel	Groups	Via	Local URI	Contact	Display Name	PAI
1	19 19	1...				
2	19 19	1...	585666...	5856...		N...

The 'Edit Channel' dialog box is open, showing the following fields:

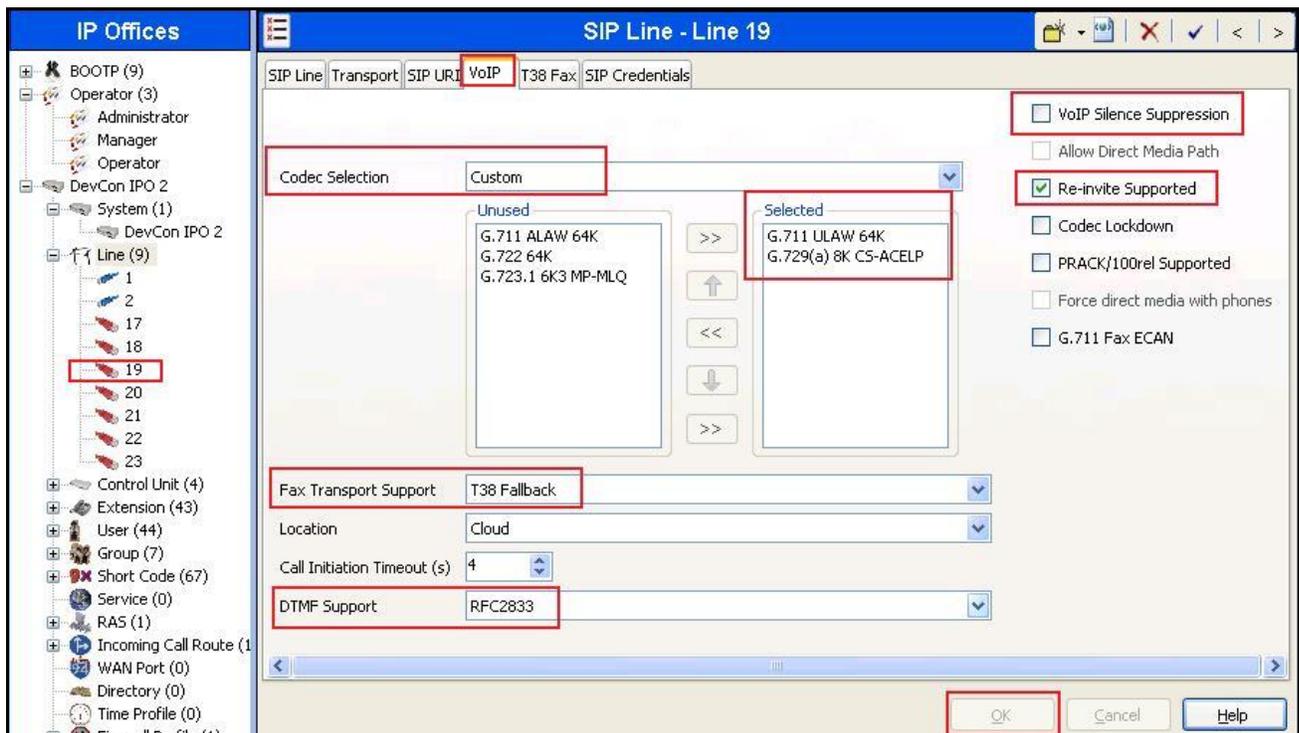
- Via: 135.10.98.113
- Local URI: 5856664803
- Contact: 5856664803
- Display Name: Use Internal Data
- PAI: None
- Registration: 0: <None>
- Incoming Group: 19
- Outgoing Group: 19
- Max Calls per Channel: 10

Buttons for 'Add...', 'Remove', 'Edit...', 'OK', and 'Cancel' are visible. The 'Edit...' and 'OK' buttons are highlighted with red boxes.

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

- The **Codec Selection** can be selected by choosing **Custom** from the pull-down menu, allowing an explicit ordered list of codecs to be specified. Select **G.711 ULAW 64K** as first choice and **G.729(a) 8K CS-ACELP** as second choice of codecs, cause Avaya IP Office to include these codes, supported by the Frontier SIP Trunking service, in the Session Description Protocol (SDP) offer, in that order.
- Set **Fax Transport Support** to **T.38 Fallback** from the pull-down menu.
- Set the **DTMF Support** field to **RFC2833** from the pull-down menu. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Uncheck the **VoIP Silence Suppression** box. By unchecking the **VoIP Silence Suppression** box, calls can be established with the G.729 codec but without silence suppression.
- Check the **Re-invite Supported** box.
- Check the **Re-invite Supported** box.
- Default values may be used for all other parameters.

Click **OK** to commit.



5.5. Short Code

Define a short code to route outbound traffic to the SIP line. To create a short code, select **Short Code** in the left Navigation Pane, then right-click in the Group Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters for the new short code to be created. The screen below shows the details of the previously administered “9N;” short code used in the test configuration.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **9N;**; this short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N"@10.10.97.174"**. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value **N** represents the number dialed by the user. The host part following the “@” is the domain of the service provider network.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4**. This short code will use this line group when placing the outbound call.
- Set **Locale** to **United States (US English)**.

Click **OK** to commit.

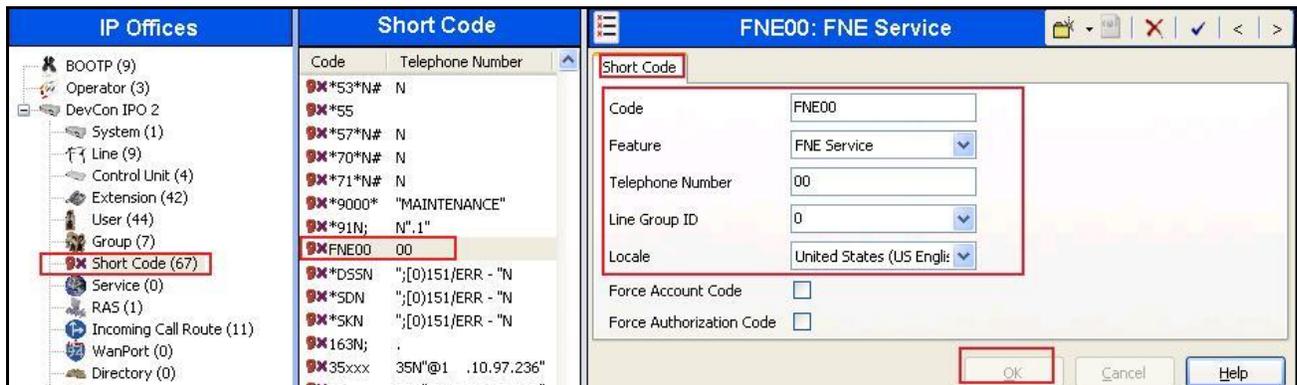
The screenshot displays the Avaya configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'Short Code (67)' selected. The main area is divided into two panes: 'Short Code' and '9N;: Dial'. The 'Short Code' pane shows a list of short codes, with '9N;: N"@192.168.248.132"' highlighted. The '9N;: Dial' pane shows the configuration details for the selected short code:

Field	Value
Code	9N;
Feature	Dial
Telephone Number	N"@10.10.97.174"
Line Group ID	19
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

At the bottom of the '9N;: Dial' pane, there are three buttons: 'OK', 'Cancel', and 'Help'. The 'OK' button is highlighted with a red box.

For incoming calls from mobility extension to FNE features hosted by IP Office to provide **Dial Tone** functionality, Short Code **FNE00** was created. The **FNE00** was configured with the following parameters.

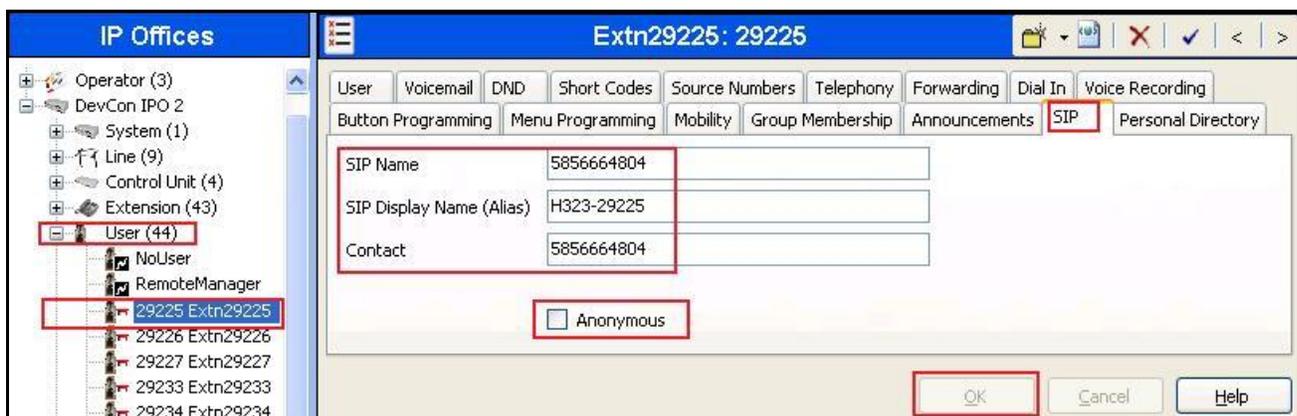
- In the **Code** field, enter the FNE feature code as **FNE00** for **Dial Tone**.
- Set the **Feature** field to **FNE Service**.
- Set the **Telephone Number** field to **00** for **FNE00**.
- Set the **Line Group ID** field to **0**.
- Retain default values for other fields.



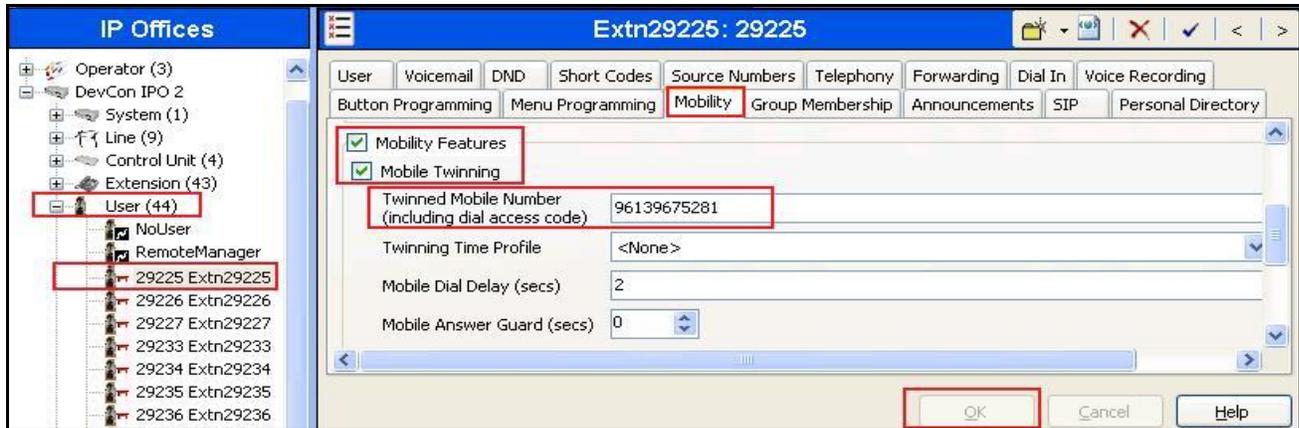
5.6. User

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 select **User** in the left Navigation Pane, then select the name of the user to be modified in the center Group Pane. In the example below, the name of the user is “H323-29225”. Select the **SIP** tab in the Details Pane.

The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. They also 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**). The example below shows the settings for user H323-29225. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise from Frontier. 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. Click **OK** to commit.



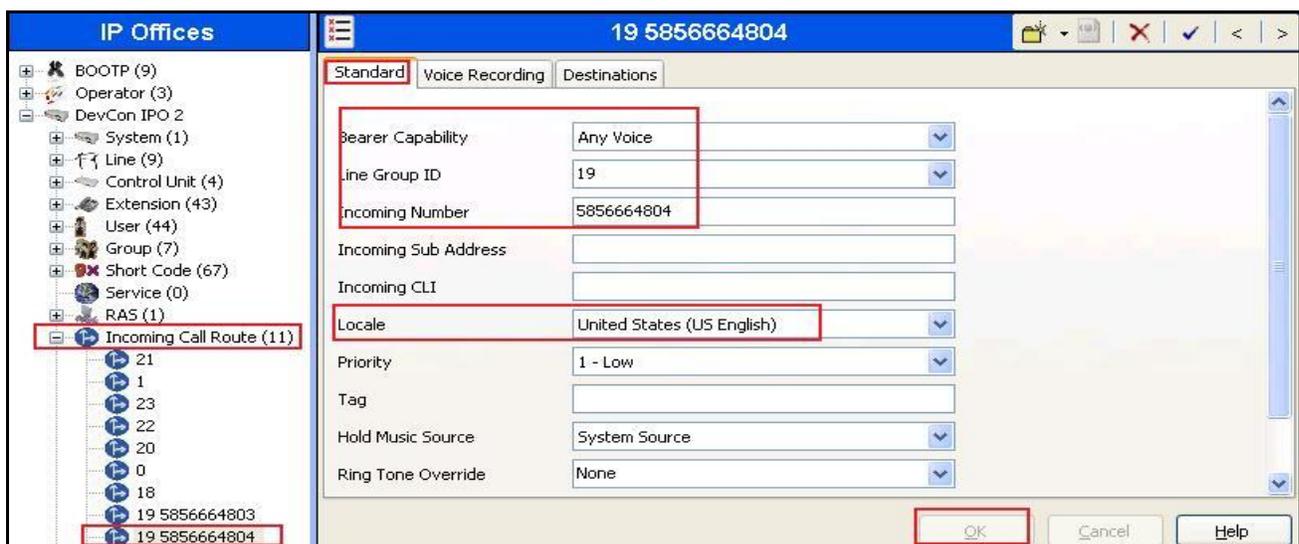
One of the H.323 IP Phones at the enterprise site uses the Mobile Twinning feature. The following screen shows the **Mobility** tab for User H323-29225. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone, in this case 96139675281. Other options can be set according to customer requirements.



5.7. Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by the service provider. To create an incoming call route, select **Incoming Call Route** in the left Navigation Pane, then right-click in the center Group 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**.
- Set the **Incoming Number** to the incoming number on which this route should match.
- Set **Locale** to **United States (US English)**
- Default values can be used for all other fields.



On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to 585-666-4804 on line 19 are routed to extension **29225**. Click **OK** to commit.

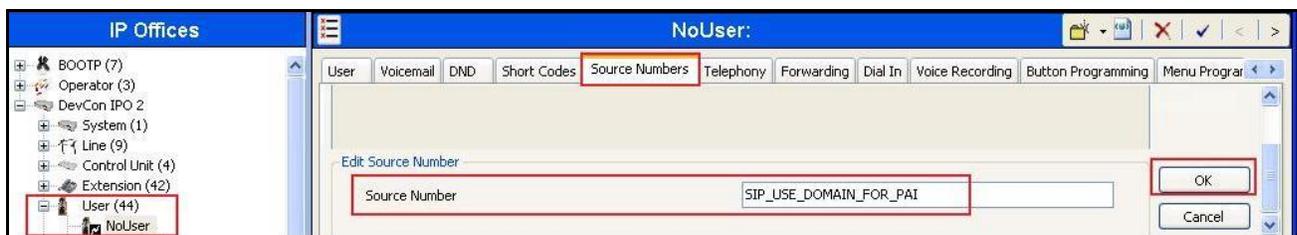


5.8. Privacy/Anonymous Calls

For outbound calls with privacy (anonymous) enabled, Avaya IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with “restricted” and “anonymous” respectively. Avaya 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. For the compliance test, PAI was used for the purposes of privacy.

To configure Avaya IP Office to use PAI for privacy calls, navigate to **User** → **noUser** in the Navigation / Group Panes. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button (not shown).

At the bottom of the Details Pane, the **Source Number** field will appear. Enter **SIP_USE_DOMAIN_FOR_PA**. Click **OK**.



The **SIP_USE_DOMAIN_FOR_PA** parameter will appear in the list of Source Numbers as shown below.



5.9. SIP Options

Avaya IP Office sends SIP OPTIONS messages periodically to determine if the SIP connection is active. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time** (in seconds) set on the **Network Topology** tab in **Section 5.1** and the **SIP_OPTIONS_PERIOD** parameter (in minutes) that can be set on the **Source Number** tab of the **noUser** user. The OPTIONS period is determined in the following manner:

- If no **SIP_OPTIONS_PERIOD** parameter is defined and the **Binding Refresh Time** is **0**, then the default value of 300 seconds is used.
- To establish a period less than 300 seconds, do not define a **SIP_OPTIONS_PERIOD** parameter and set the **Binding Refresh Time** to a value less than 300 seconds. The OPTIONS message period will be equal to the **Binding Refresh Time**.
- To establish a period greater than 300 seconds, a **SIP_OPTIONS_PERIOD** parameter must be defined. The **Binding Refresh Time** must be set to a value greater than 300 seconds. The OPTIONS message period will be the smaller of the **Binding Refresh Time** and the **SIP_OPTIONS_PERIOD**.

To configure the **SIP_OPTIONS_PERIOD** parameter, navigate to **User → noUser** in the Navigation / Group Panes (not shown). Select the **Source Numbers** tab in the Details Pane. Click the **Add** button (not shown). At the bottom of the Details Pane, the **Source Number** field will appear. Enter **SIP_OPTIONS_PERIOD=X**, where **X** is the desired value in minutes. Click the **OK** button (not shown).

In this testing, **SIP_OPTIONS_PERIOD** parameter was not defined in order for IPO to send SIP options messages periodically every **60** seconds, which is the **Binding Refresh Time** value set in **Section 5.1**.

5.10. 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.

6. Configure the Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the software has already been installed. For additional information on these configuration tasks, see Error! Reference source not found. **Error! Reference source not found.**, **Error! Reference source not found.** and Error! Reference source not found..

The compliance testing comprised the configuration for two major components, Trunk Server for the service provider and Call Server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration was defined in the Avaya SBCE web user interface as described in the following sections.

Trunk Server configuration elements for the service provider - Frontier:

- Global Profiles:
 - URI Groups
 - Routing
 - Topology Hiding
 - Server Interworking
 - Signaling Manipulation
 - Server Configuration
- Domain Policies:
 - Application Rules
 - Media Rules
 - Signaling Rules
 - Endpoint Policy Group
 - Session Policy
- Device Specific Settings:
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows → Server Flows
 - Session Flows

Call Server configuration elements for the enterprise - IP Office:

- Global Profiles:
 - URI Groups
 - Routing
 - Topology Hiding
 - Server Interworking
 - Server Configuration
- Domain Policies:
 - Application Rules
 - Media Rules
 - Signaling Rules
 - Endpoint Policy Group

- Session Policy
- Device Specific Settings:
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows → Server Flows
 - Session Flows

6.1. Log into the Avaya Session Border Controller for Enterprise

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 management IP address.

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

AVAYA

Session Border Controller for Enterprise

Log In

Username:

Password:

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.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise **AVAYA**

Dashboard

Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings

Dashboard

Information		
System Time	01:11:16 PM GMT	Refresh
Version	6.2.1.Q07	
Build Date	Mon Dec 9 17:33:02 CST 2013	

Installed Devices
EMS
mSBCE

Alarms (past 24 hours)

None found.

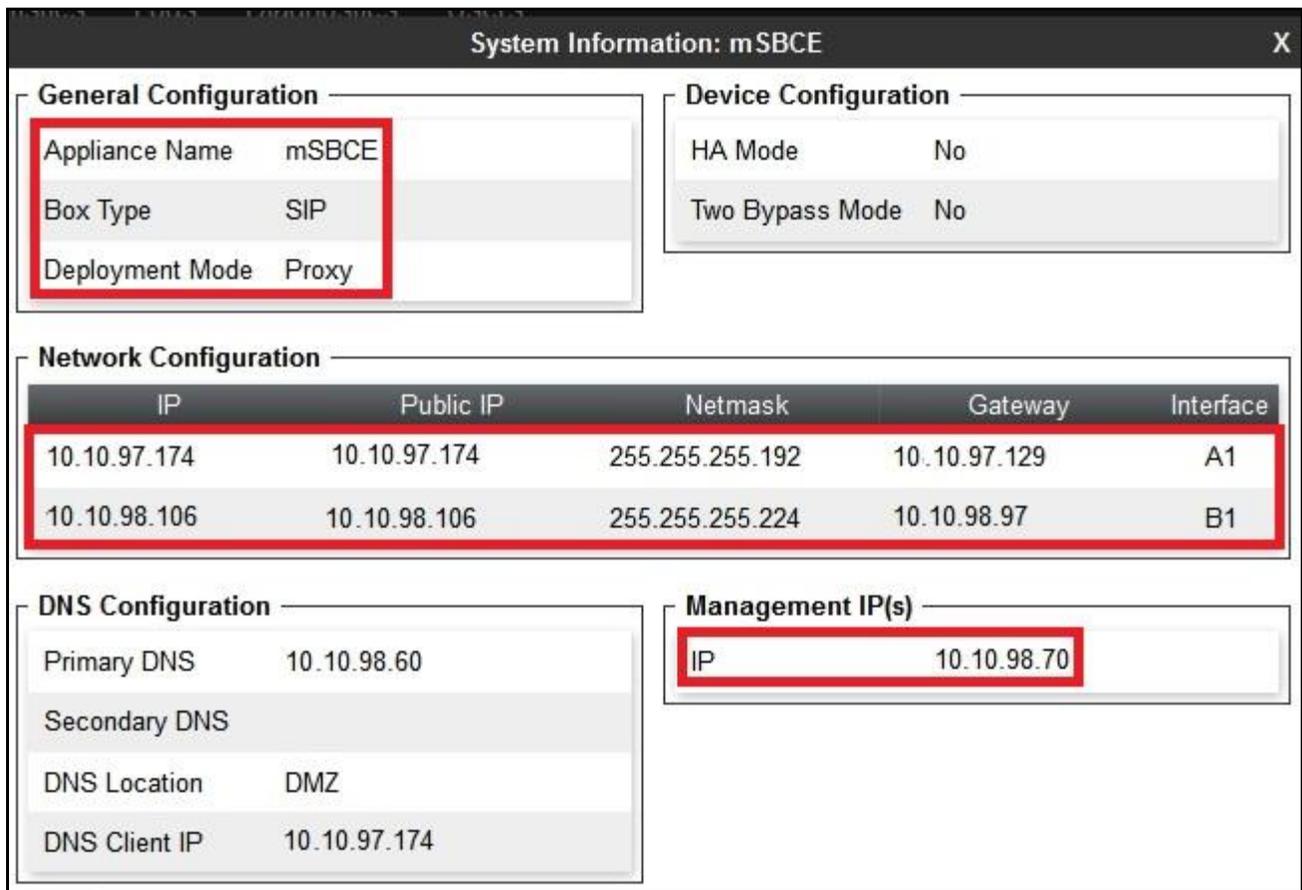
Incidents (past 24 hours)

mSBCE: Server Config Found. But no server flow matched, Sending 500 Server Internal Error

To view system information that has been 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 **mSBCE** was already added. To view the configuration of this device, click the **View** as shown in the screenshot below.



The **System Information** screen shows **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponded 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.



6.2. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

6.2.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, we use “*” for all incoming and outgoing traffic.

6.2.2. Routing Profiles

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing profiles include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

To create a Routing profile, select **Global Profiles → Routing** then click on the **Add Profile** button (not shown).

In the compliance testing, Routing profile **To-SP** was created to be used in conjunction with Server Flow (see **Section 6.4.4**) defined for IP Office. This entry is to route outgoing calls from the enterprise to Frontier.

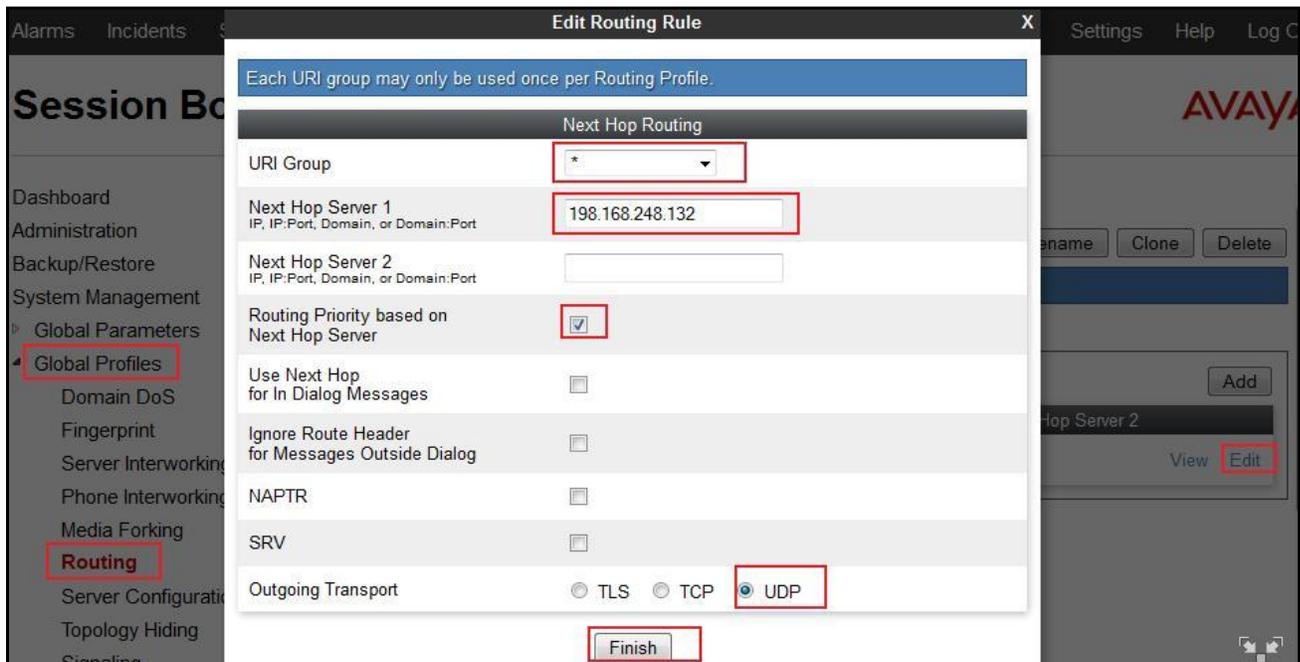
On the opposite direction, Routing profile **To-IPO-113** was created to be used in conjunction with Server Flow (see **Section 6.4.4**) defined for Frontier This entry is to route incoming calls from Frontier to the enterprise.

Note: The **Routing Priority based on Next Hop Server** was checked to use the default settings for both profiles as shown bellow.

Routing Profile for Frontier

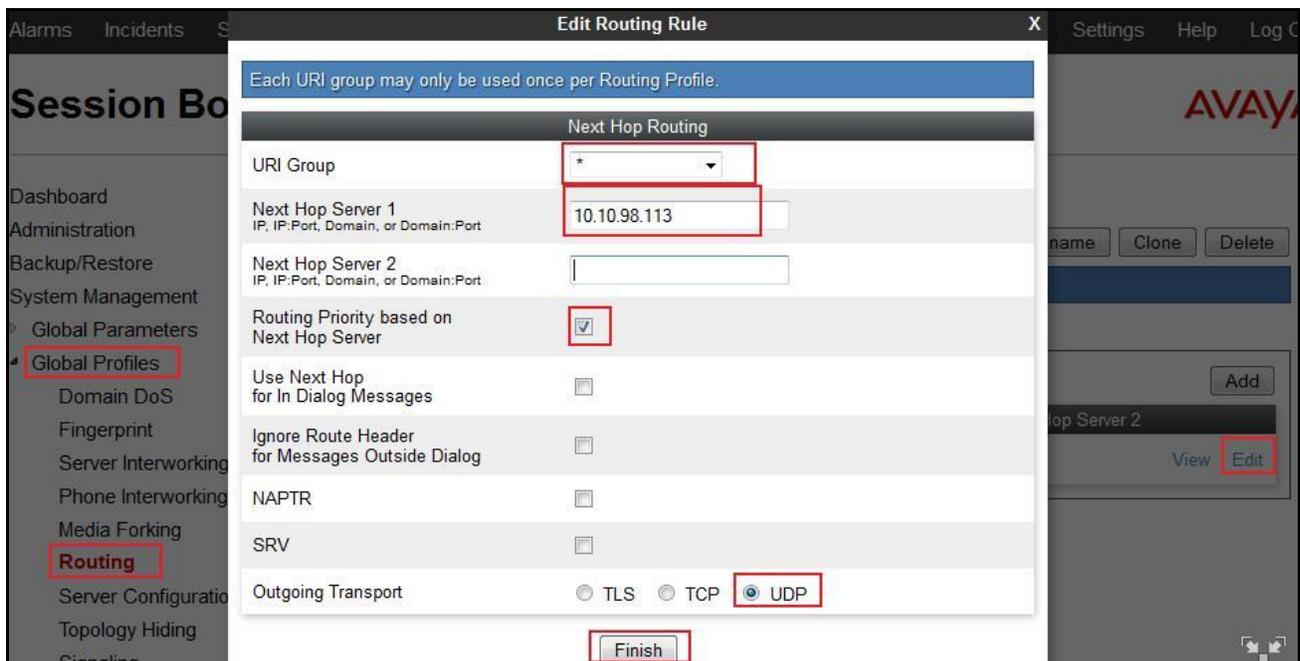
To display **Edit Routing Rule** dialog of Routing profile **To-SP**, select **Global Profiles → Routing: To-SP**. As shown in the screenshot below, outgoing calls will be routed to the **Next Hop Server 1** as defined as the IP address of Frontier Trunk Server.

As shown in **Figure 1**, Frontier SIP Trunking was connected with transportation protocol **UDP**. The other options were kept as default.



Routing Profile for Avaya IP Office

Similarly, Routing profile **To-IPO-113** was created to route incoming calls to the **Next Hop Server 1** as defined as the IP address of IP Office. As shown in **Figure 1**, IP Office was connected with transportation protocol **UDP**. To display **Edit Routing Rule** dialog of Routing profile **To-IPO-113**, select **Global Profiles** → **Routing: To-IPO-113** then click **Edit** (not shown).



6.2.3. Topology Hiding

Topology Hiding is a security feature of the Avaya SBCE which allows changing certain key SIP message parameters to ‘hide’ or ‘mask’ how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select **Global Profiles → Topology Hiding** then click on the **Add Profile** (not shown).

In the compliance testing, two Topology Hiding profiles were created: **To-SP** and **To-IPO-113**.

Topology Hiding Profile for Frontier

Topology Hiding profile **To-SP** was defined for outgoing calls to Frontier to:

- Mask URI-Host of the “Request-URI” and “To” headers with service provider SIP domain/IP address to meet the requirements of Frontier as shown in **Figure 1**.
- Mask URI-Host of the “From” header to IP address of AVAYA SBCE external interface as shown in **Figure 1**.

This implementation is to secure the enterprise network topology and also to meet the SIP requirements from the service provider.

The screenshots below illustrate the Topology Hiding profile **To-SP**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo. The left navigation menu includes "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles" (highlighted), "Domain DoS", "Fingerprint", "Server Interworking", "Phone Interworking", "Media Forking", "Routing", "Server Configuration", "Topology Hiding" (highlighted), "Signaling Manipulation", "URI Groups", and "SIP Cluster".

The main content area is titled "Topology Hiding Profiles: To-SP". It features an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a "Click here to add a description." link. A "Topology Hiding" tab is active, showing a table with the following data:

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	198.168.248.132
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	10.10.98.106
SDP	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	198.168.248.132
Referred-By	IP/Domain	Auto	---

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

Topology Hiding Profile for IP Office

Topology Hiding profile **To-IPO-113** was defined for incoming calls to IP Office to:

- Mask URI-Host of the “Request-URI” and “To” headers with the enterprise SIP domain/IP address as IP Office IP address as shown in **Figure 1**.
- Mask URI-Host of the “From” header to IP address of AVAYA SBCE internal interface as shown in **Figure 1**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand navigation menu includes "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles" (highlighted), "Domain DoS", "Fingerprint", "Server Interworking", "Phone Interworking", "Media Forking", "Routing", "Server Configuration", "Topology Hiding" (highlighted), "Signaling Manipulation", "URI Groups", and "SIP Cluster".

The main content area is titled "Topology Hiding Profiles: To-IPO-113". It features an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a description field with the text "Click here to add a description." and a "Topology Hiding" tab.

The "Topology Hiding" tab contains a table with the following data:

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	10.10.98.113
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	10.10.97.174
SDP	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	10.10.98.113
Referred-By	IP/Domain	Auto	---

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

6.2.4. Server Interworking

Server Interworking profile features are configured differently for Call Server and Trunk Server. To create a Server Interworking profile, select **Global Profiles** → **Server Interworking** then click on the **Add Profile** button (not shown). In the compliance testing, two Server Interworking profiles **SP-SI** and **IPO-113** were created for Frontier (Trunk Server) and IP Office (Call Server) respectively.

Server Interworking Profile for Frontier

Server Interworking profile **SP-SI** was defined to match the specification of Frontier. The **General** and **Advanced** tabs were configured with the following parameters while the other tabs **Timers**, **URI Manipulation** and **Header Manipulation** were kept as default. Settings are being set as shown in capture bellow. Others are left as default.

Editing Profile: SP-SI

General

Hold Support None RFC2543 - c=0.0.0.0 RFC3264 - a=sendonly

180 Handling None SDP No SDP

181 Handling None SDP No SDP

182 Handling None SDP No SDP

183 Handling None SDP No SDP

Refer Handling

URI Group

3xx Handling

Diversion Header Support

Delayed SDP Handling

Re-Invite Handling

T.38 Support

URI Scheme SIP TEL ANY

Via Header Format RFC3261 RFC2543

Next

Advanced settings are being set as shown in capture bellow and others are left as default.

Editing Profile: SP-SI

Record Routes None Single Side Both Sides

Topology Hiding: Change Call-ID

Call-Info NAT

Change Max Forwards

Include End Point IP for Context Lookup

OCS Extensions

AVAYA Extensions

NORTEL Extensions

Diversion Manipulation

Diversion Header URI

Metaswitch Extensions

Reset on Talk Spurt

Reset SRTP Context on Session Refresh

Has Remote SBC

Route Response on Via Port

Cisco Extensions

Finish

Server Interworking Profile for Avaya IP Office

Server Interworking profile **IPO-113** shown in the screenshots below, was similarly defined to match the specification of IP Office with the exception of the support for **Avaya Extensions** was enabled.

Editing Profile: IPO-113

General

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

Next

Advanced settings are being set as shown in capture bellow and others are left as default.

Editing Profile: IPO-113

Record Routes	<input type="radio"/> None	<input type="radio"/> Single Side	<input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>		
Call-Info NAT	<input type="checkbox"/>		
Change Max Forwards	<input checked="" type="checkbox"/>		
Include End Point IP for Context Lookup	<input type="checkbox"/>		
OCS Extensions	<input type="checkbox"/>		
AVAYA Extensions	<input checked="" type="checkbox"/>		
NORTEL Extensions	<input type="checkbox"/>		
Diversion Manipulation	<input type="checkbox"/>		
Diversion Header URI			
Metaswitch Extensions	<input type="checkbox"/>		
Reset on Talk Spurt	<input type="checkbox"/>		
Reset SRTP Context on Session Refresh	<input type="checkbox"/>		
Has Remote SBC	<input checked="" type="checkbox"/>		
Route Response on Via Port	<input type="checkbox"/>		
Cisco Extensions	<input type="checkbox"/>		

Finish

6.2.5. Server Configuration

Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

To create a Server Configuration entry, select **Global Profiles** → **Server Configuration** then click on the **Add Profile** button (not shown).

In the compliance testing, two separate Server Configurations were created, server entry **SP-SC** for Frontier and server entry **IPO-113** for IP Office.

Server Configuration for Frontier

The Server Configuration **SP-SC** was added for Frontier, it is discussed in detail as below. The **General** and **Advanced** tabs were provisioned. The **General** setting for Server Configuration **SP-SC** is being set as shown in following capture.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. A left-hand navigation menu includes "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles", "Domain DoS", "Fingerprint", "Server Interworking", "Phone Interworking", "Media Forking", "Routing", and "Server Configuration". The "Server Configuration" menu item is highlighted. The main content area is titled "Server Configuration: SP-SC" and features an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a tabbed interface with tabs for "General", "Authentication", "Heartbeat", "Advanced", "DoS Whitelist", and "DoS Protection". The "General" tab is active, showing a table of configuration parameters:

Server Type	Trunk Server
IP Addresses / FQDNs	192.168.248.132
Supported Transports	UDP
UDP Port	5060

An "Edit" button is located below the table.

The Advanced setting is being set as shown in capture. Where the **SP-SI** Interworking Profile is selected as defined in **Section 6.2.4**.

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

Server Configuration: SP-SC

Add Rename Clone Delete

Server Profiles

- IPO
- MTSAlltream
- IPO-113
- RC
- ThinkTel
- SP-SC**
- IPO_14

General Authentication Heartbeat **Advanced** DoS Whitelist DoS Protection

Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-SI
Signaling Manipulation Script	None
UDP Connection Type	SUBID

Edit

Server Configuration for Avaya IP Office

The Server Configuration **IPO-113** was similarly created for IP Office. It is discussed in detail as below. Only the **General** and **Advanced** tabs required provisioning. The **General** setting for Server Configuration **IPO-113** is being set as shown in following capture.

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

Server Configuration: IPO-113

Add Rename Clone Delete

Server Profiles

- IPO
- MTSAlltream
- IPO-113**
- RC
- ThinkTel
- SP-SC
- IPO_14

General Authentication Heartbeat Advanced

Server Type	Call Server
IP Addresses / FQDNs	10.10.98.113
Supported Transports	UDP
UDP Port	5060

Edit

The Advanced setting is being set as shown in capture. Where the **IPO-113** Interworking Profile is selected as defined in **Section 6.2.4**.

The screenshot shows the Avaya Session Border Controller for Enterprise configuration interface. The main title is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. On the left is a navigation menu with items like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, and Server Configuration (highlighted). The main content area is titled "Server Configuration: IPO-113" and includes an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a "Server Profiles" list with "IPO-113" selected. The configuration tabs are "General", "Authentication", "Heartbeat", and "Advanced" (highlighted). The "Advanced" tab contains the following settings: "Enable DoS Protection" (checkbox), "Enable Grooming" (checkbox), "Interworking Profile" (set to "IPO-113"), "Signaling Manipulation Script" (set to "None"), and "UDP Connection Type" (set to "SUBID"). An "Edit" button is located at the bottom right of the configuration area.

6.3. Domain Policies

Domain Policies feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

6.3.1. End Point Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to Server Flow defined in **Section 6.4.4**.

Endpoint Policy Groups were separately created for Frontier and IP Office.

To create a policy group, navigate to **Domain Policies** → **Endpoint Policy Groups** and click on the **Add Group** button (not shown).

End Point Policy Group for Frontier

The following screen shows **SP-PG** created for Frontier.

- Set Application Rule to **default-trunk**.
- Set Media Rule to **default-low-med**.
- Set Signaling Rule to **default**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-high**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows a navigation menu with 'Domain Policies' and 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: SP-PG' and includes an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are two blue bars with the text 'Click here to add a description.' and 'Click here to add a row description.' A 'Policy Group' section contains a 'Summary' button and an 'Add' button. A table lists the policy group configuration:

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	default-trunk	default	default-low-med	default-high	default	default	Edit Clone

End Point Policy Group for Avaya IP Office

Similarly, **IPO-113-PG** was created for Avaya IP Office with same values as End Point Policy Group for Frontier (not shown).

6.4. Device Specific Settings

Device Specific Settings feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

6.4.1. Network Management

Network Management page is where the network interface settings are configured and enabled. During the installation process of the AVAYA SBCE, certain network-specific information is defined such as device IP address, public IP address, subnet mask, gateway, etc. to interface the device to the networks. This information populates the various Network Management tabs which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Network Management**, under **Network Configuration** tab and verify the IP addresses assigned to the interfaces, and that the interfaces were enabled. The following screen shows the private interface was assigned to **A1** and the public interface was assigned to **B1** appropriate to the parameters shown in the **Figure 1**.

Session Border Controller for Enterprise AVAYA

Network Management: mSBCE

Network Configuration Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask	A2 Netmask	B1 Netmask
255.255.255.192		255.255.255.224

Add Save Clear

IP Address	Public IP	Gateway	Interface	
10.10.97.174		10.10.97.129	A1	Delete
10.10.98.106		10.10.98.97	B1	Delete

On the **Interface Configuration** tab, enable the interfaces connecting to the inside enterprise and outside service provider networks. To enable an interface click its **Toggle State** button. The following screen shows interface **A1** and **B1** were **Enabled**.

Session Border Controller for Enterprise AVAYA

Network Management: mSBCE

Network Configuration Interface Configuration

Name	Administrative Status	
A1	Enabled	Toggle
B1	Enabled	Toggle

6.4.2. Media Interface

Media Interface screen is where the media ports are defined. The Avaya SBCE will open connection for RTP traffic on the defined ports.

To create a new **Media Interface**, navigate to **Device Specific Settings** → **Media Interface** and click on the **Add Media Interface** button (not shown).

Two separate Media Interfaces are needed for both the inside and outside interfaces. The following screen shows the Media Interfaces **InsideMedia** and **OutsideMedia** were created for the compliance testing.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.

Name	Media IP	Port Range	Edit	Delete
InsideMedia	10.10.97.174	35000 - 40000	Edit	Delete
OutsideMedia	10.10.98.106	35000 - 40000	Edit	Delete

6.4.3. Signaling Interface

Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP request on the defined port.

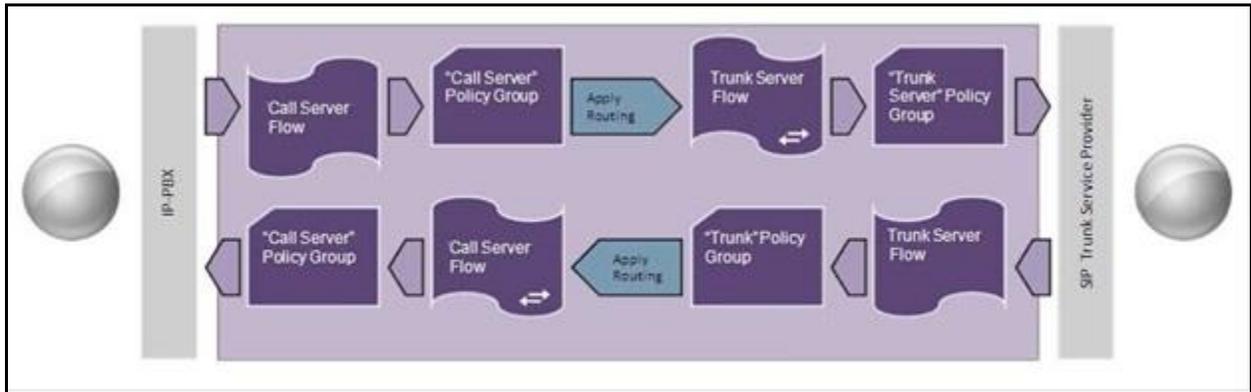
To create a new **Signaling Interface**, navigate to **Device Specific Settings** → **Signaling Interface** and click on the **Add Signaling Interface** button (not shown).

Two separate Signaling Interfaces are needed for both inside and outside interfaces. The following screen shows the Signaling Interfaces **InsideSIP** and **OutsideSIP** were created in the compliance testing with **UDP/5060** configured for inside and outside interfaces.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
InsideSIP	10.10.97.174	---	5060	---	None	Edit	Delete
OutsideSIP	10.10.98.106	---	5060	---	None	Edit	Delete

6.4.4. End Point Flows - Server Flow

When a packet is received by the 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 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.



In the compliance testing, two separate Server Flows were created for Frontier and IP Office.

Server Flow for Frontier

To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**, select the **Server Flows** tab and click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the other fields were kept as default.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 6.2.5** which the Server Flow associates to.
- **URI Group:** Select the "*" as in **Section 6.2.1**.
- **Received Interface:** Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration is designed to receive SIP signaling from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration is designed to send the SIP signaling to.
- **Media Interface:** Select the Media Interface created in **Section Error! Reference source not found.** which is the Server Configuration is designed to send the RTP to.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section Error! Reference source not found.**
- **Routing Profile:** Select the Routing Profile created in **Section Error! Reference source not found.** which is used to which is the Server Configuration is designed to route the calls to.
- **Topology Hiding Profile:** Select the Topology Hiding profile created in **Section Error! Reference source not found.** to apply toward the Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

The following screen shows the Server Flow **SP** for Frontier.

Flow Name	SP
Server Configuration	SP-SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	InsideSIP
Signaling Interface	OutsideSIP
Media Interface	OutsideMedia
End Point Policy Group	SP-PG
Routing Profile	To-IPO-113
Topology Hiding Profile	To-SP
File Transfer Profile	None

Finish

Similarly, the following screen shows the Server Flow **IPO-113** for IP Office

Flow Name	IPO-113
Server Configuration	IPO-113
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP
Signaling Interface	InsideSIP
Media Interface	InsideMedia
End Point Policy Group	IPO-113-PG
Routing Profile	To-SP
Topology Hiding Profile	To-IPO-113
File Transfer Profile	None

Finish

7. Frontier SIP Trunking Configuration

Frontier is responsible for the configuration of Frontier SIP Trunking service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise. Frontier will provide the customer the necessary information to configure the Avaya IP Office SIP connection to Frontier. The provided information from Frontier includes:

- IP address of the Frontier SIP proxy.
- Supported codecs
- DID numbers
- IP addresses and port numbers used for signaling or media through any security devices.

8. Verification Steps

The following steps may be used to verify the solution is configured properly.

8.1. Avaya IP Office System Status

Use the Avaya IP Office System Status application to verify the SIP Line channels state and to check alarms:

- Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. 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 application. The left pane shows a tree view with 'Line: 19' selected. The main pane displays the 'SIP Trunk Summary' for Line 19. The summary includes the following information:

- Peer Domain Name: 192.168.248.132
- Resolved Address: 192.168.248.132
- Line Number: 19
- Number of Administered Channels: 20
- Number of Channels in Use: 0
- Administered Compression: G711 Mu, G729 A
- Silence Suppression: Off
- Layer 4 Protocol: UDP
- SIP Trunk Channel Licenses: Unlimited
- SIP Trunk Channel Licenses in Use: 0
- SIP Device Features: REFER (Incoming and Outgoing), UPDATE (Incoming and Outgoing)

A green circle indicates 0% utilization. Below the summary is a table with the following columns: Channel Number, U..., Call Ref, Current State, Time in State, Remote Media A..., Co..., Conne..., Caller ID or Dial..., Other Party on Call, Direction of Call, Round Trip D..., Receive Jitter, Receive Packe..., Transmit Jitter, and Transmit Packe... The table shows four channels, all in an 'Idle' state with a time in state of 01:02:57.

Buttons at the bottom include Trace, Trace All, Pause, Ping, Call Details, Print..., and Save As... The status bar shows 4:18:22 PM and Online.

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

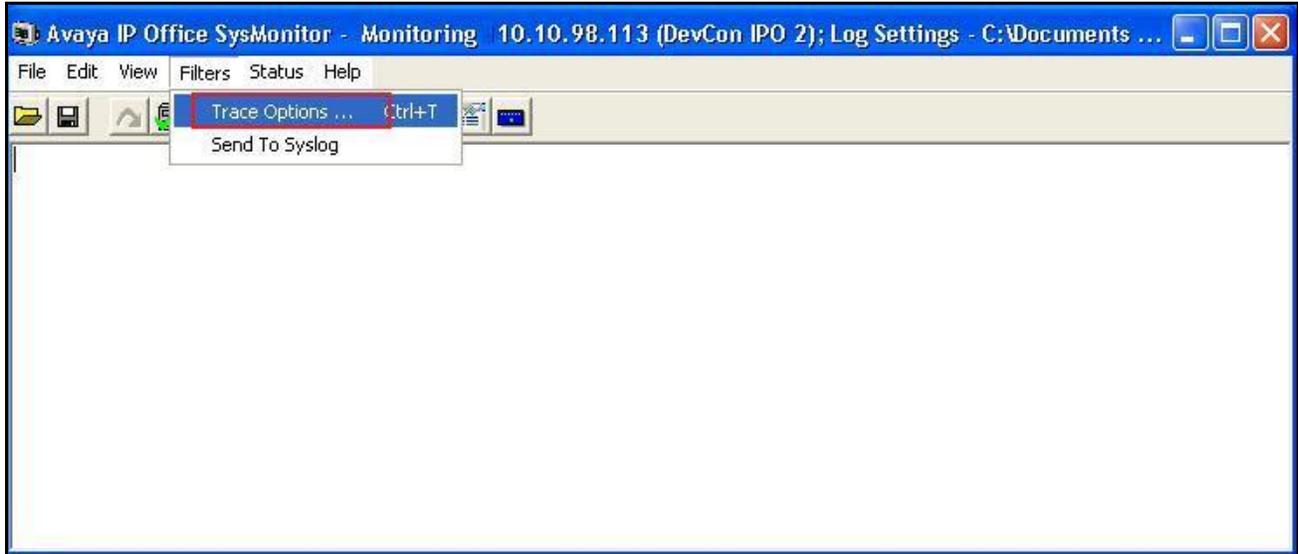
The screenshot shows the Avaya IP Office System Status application with the 'Alarms' tab selected. The main pane displays 'Alarms for Line: 19 SIP 192.168.248.132'. The table below is empty, indicating no active alarms.

Last Date Of Error	Occurrences	Error Description
--------------------	-------------	-------------------

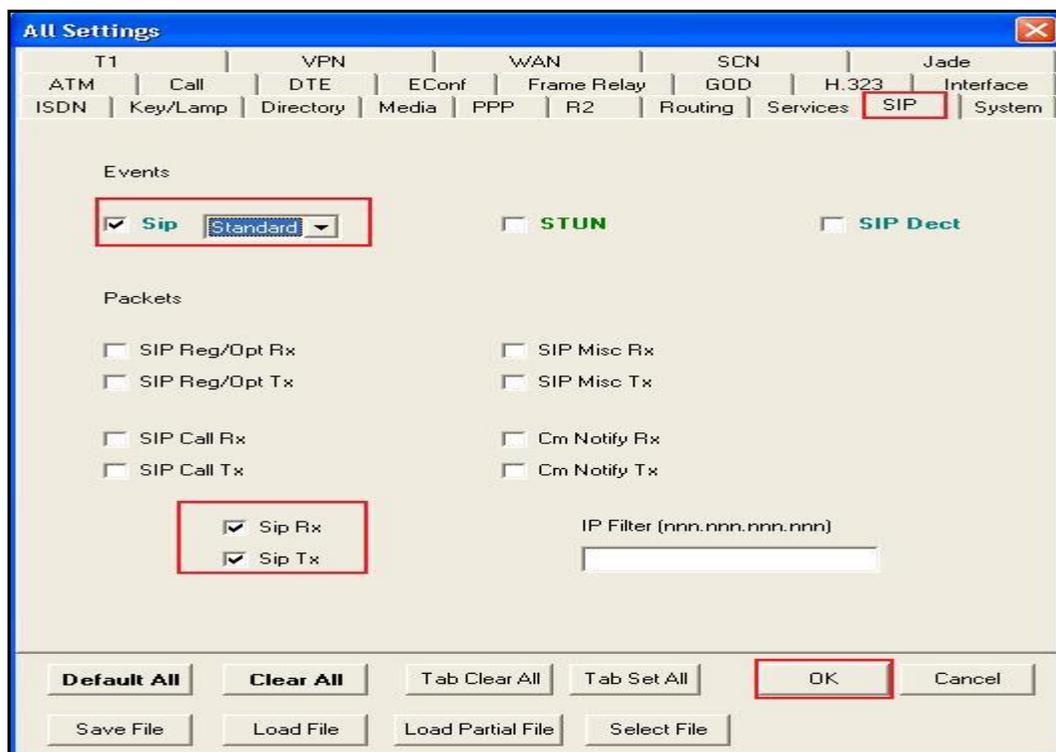
Buttons at the bottom include Ping, Clear, Clear All, Print..., and Save As... The status bar shows 9:54:40 AM and Online.

8.2. Avaya IP Office Monitor

The Monitor application can be used to monitor and troubleshoot Avaya IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor** on the Avaya IP Office Manager PC. The application allows the monitored information to be customized. To customize, select **Filters → Trace Options ...** as shown below:



The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, **Standard** SIP Events and the **SIP Rx** and **SIP Tx** boxes are checked.



8.3. Avaya SBCE Protocol Trace

The Avaya SBCE can take internal traces on specified interfaces. Both SIP signaling crossing interfaces A1 and B1 can be captured for troubleshooting. In the Avaya SBCE web interface, navigate to **Device Specific Settings** → **Troubleshooting** → **Trace** to invoke this facility, select or supply the relevant information (e.g., A1 or B1 or any interfaces, IP/port, protocol, number of packets to capture, capture file name, etc.), then start the trace. The captured trace can then be downloaded for examination using a protocol sniffer application such as Wireshark.

9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk to connect Avaya IP Office release 9.0.3 and Avaya Session Border Controller for Enterprise release 6.2.1 to the Frontier SIP Trunking Service as shown in **Figure 1**. The Frontier SIP Trunking passed compliance testing.

10. Additional References

- [1] IP Office 9.0 Installation, Document number 15-601042 Issue 28, 11 October 2013
- [2] IP Office 9.0 Manager 9.0, Document number 15-601011 Issue 9.01, 09 September 2013
- [3] IP Office 9.0 Administering Voicemail Pro, Document number 15-601063 Issue 9.0 Release 1.0, September 2013
- [4] IP Office Embedded Voicemail User Guide (IP Office Mode), Document number 15-604067 Issue 9.0, 10 September 2013
- [5] [10] *Avaya Session Border Controller for Enterprise Overview and Specification*, Issue 2, December 2013
- [6] [11] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, January 2014
- [7] [12] *Configuring the Avaya Session Border Controller for IP Office Remote Workers*, September 2013

Product documentation for Avaya products may be found at <http://support.avaya.com>. Additional IP Office documentation can be found at: <http://marketingtools.avaya.com/knowledgebase/>

Product documentation for Frontier SIP Trunking is available from Frontier. <https://frontier.com/enterprise>

11. Appendix – Remote Worker Configuration via Avaya SBC

This section describes the process for connecting select remote Avaya SIP endpoints on the public Internet to Avaya IP Office on the private enterprise network via the AVAYA SBCE. The provisioning builds on the reference configuration described in previous sections of this document.

Note – This Remote Worker configuration is based on provisioning the Avaya SBCE. It is not to be confused with “native” Avaya IP Office Remote Worker configurations.

Supported Remote Worker endpoints for Avaya IP Office are:

- Flare® Experience for iPad
- Flare® Experience for Windows
- one-X® Mobile Preferred VoIP client for iOS
- one-X® Mobile Preferred VoIP client for Android

For Avaya IP Office R9.0, the following table summarizes encryption support for these remote worker endpoints (see **Section 11.1.8**):

Client type	Uses to the external interface of the SBCE		
	TLS	SRTP Audio	SRTP Video
Flare Experience for iPad	Y*	Y*	N
Flare Experience for Windows	Y*	Y*	N
one-X Mobile Preferred VoIP client for iOS	Y	N	N
one-X Mobile Preferred VoIP client for Android	N	N	N

* If the client is used inside and outside of the IP Office core, the signalling type must be changed. IP Office 9.0 does not support TLS or SRTP connections to these clients on the inside of the SBCE.

In the configuration for the compliance test, Avaya Flare® Experience for Windows was used as the Remote Worker SIP endpoint.

The reference configuration for the compliance test, including the Remote Worker endpoint, is shown in **Figure 1** in **Section 3**. Internet access by the Remote Worker endpoint is through a Router/NAT/Firewall/Default Gateway located between the Remote Worker private LAN and the public Internet.

Note that the configuration/provisioning of Router/NAT/Firewall/Default Gateway is beyond the scope of this document.

11.1. Provisioning Avaya SBCE for Remote Worker

Provisioning of the Avaya SBCE to support Avaya IP Office SIP connection to the service provider is described in **Section 6**. The following sections build on that provisioning.

11.1.1. Network Management

This section shows the **Network Management** configuration of the Avaya SBCE to support Remote Worker. For this purpose, the Avaya SBCE is configured with a second outside IP address assigned to physical interface **B1**, and a second inside address assigned to physical interface **A1**.

The screenshot shows the 'Network Management: mSBCE' configuration page. The 'Network Configuration' tab is active. A warning message states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, a blue bar indicates: 'Changes will not take effect until the interface is updated.'

Configuration fields include:

- A1 Netmask: 255.255.255.192
- A2 Netmask: (empty)
- B1 Netmask: 255.255.255.224

Buttons: Add, Save, Clear.

IP Address	Public IP	Gateway	Interface	
10.10.97.174		10.10.97.129	A1	Delete
10.10.98.106		10.10.98.97	B1	Delete
10.10.97.173		10.10.97.129	A1	Delete
10.10.98.102		10.10.98.97	B1	Delete

11.1.2. Signalling Interfaces

As shown in capture below, two new Signalling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic. Interface **InsideSIPRW** supports TCP, while interface **OutsideSIPRW** supports TLS.

The screenshot shows the 'Signaling Interface: mSBCE' configuration page. The 'Signaling Interface' tab is active. An 'Add' button is visible in the top right corner.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIP	10.10.97.174	---	5060	---	None	Edit Delete
OutsideSIP	10.10.98.106	5060	5060	---	None	Edit Delete
InsideSIPRW	10.10.97.173	5060	---	---	None	Edit Delete
OutsideSIPRW	10.10.98.102	---	---	5061	AvayaSBCServer	Edit Delete

11.1.3. Media Interfaces

Two new Media interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

The screenshot shows the 'Media Interface: mSBCE' configuration page. On the left is a navigation menu with 'Media Interface' highlighted. The main content area has a warning box: '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 is a table of media interfaces:

Name	Media IP	Port Range	Edit	Delete
InsideMedia	10.10.97.174	35000 - 40000		
OutsideMedia	10.10.98.106	35000 - 40000		
InsideMediaRW	10.10.97.173	35000 - 55000		
OutsideMediaRW	10.10.98.102	35000 - 55000		

11.1.4. Server Profile for Avaya IP Office

TCP transport protocol (which is required for the Remote Worker connection between the Avaya SBCE and Avaya IP Office) needs to be added to the existing **IPO-113** Server Profile (see **Section 6.2.5**).

The screenshot shows the 'Server Configuration: IPO-113' page. The left navigation menu has 'Server Configuration' highlighted. The main content area shows the 'General' tab with the following configuration:

Server Type	Call Server
IP Addresses / FQDNs	10.10.98.113
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

11.1.5. Routing Profiles

Use steps in **Section 6.2.2** to create two new Routing Profiles that are required to support Remote Worker namely; **default_RW** and **To-IPO-113-RW**

Remote Worker Routing Profile **default_RW**

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	<input type="checkbox"/>
Use Next Hop for In Dialog Messages	<input type="checkbox"/>
Ignore Route Header for Messages Outside Dialog	<input checked="" type="checkbox"/>
NAPTR	<input checked="" type="checkbox"/>
SRV	<input checked="" type="checkbox"/>
Outgoing Transport	<input type="radio"/> TLS <input type="radio"/> TCP <input type="radio"/> UDP

Finish

Remote Worker Routing Profile **To-IPO-113-RW**

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	10.10.98.113
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	<input checked="" type="checkbox"/>
Use Next Hop for In Dialog Messages	<input type="checkbox"/>
Ignore Route Header for Messages Outside Dialog	<input type="checkbox"/>
NAPTR	<input type="checkbox"/>
SRV	<input type="checkbox"/>
Outgoing Transport	<input type="radio"/> TLS <input checked="" type="radio"/> TCP <input type="radio"/> UDP

Finish

11.1.6. User Agent

User Agents are created for each type of Remote Worker endpoint used. In the configuration for the compliance test, the Avaya Flare® Experience for Windows SIP softphone was used, and its configuration is shown below.

Navigate to **Global Parameters** on the left-hand menu, select **User Agents** and then click **Add** button to create a new User Agent. Enter the following:

- **User Agent = Flare**
- **Regular expression = Avaya Flare.***

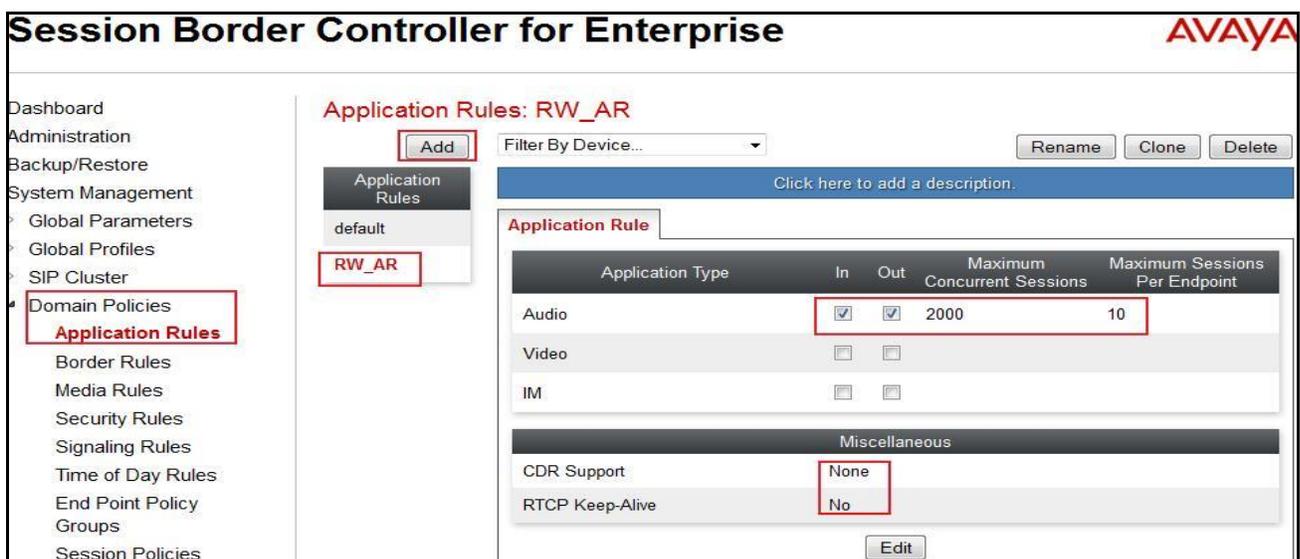
In this expression, “Avaya Flare.*” will match any software version listed after the user agent name.



11.1.7. Application Rules

Application Rule **RW_AR** is created for Remote Worker. From **Domain Policies** on the left-hand menu, select **Application Rules** and then select **Add** button to create a new Application Rule. Enter a name and click on **Next** (not shown). In the **Audio** field:

- Check **In** and **Out**.
- Enter an appropriate value in the **Maximum Concurrent Sessions** field, (e.g., **2000**).
- Enter **10** in the **Maximum Session per Endpoint** field.
- Leave the **CDR** field at **None** and the **RTCP Keep-Alive** field unchecked (**No**).



11.1.8. Media Rules

Two Media Rules are defined. Rule **SRTP_RW** is defined to enable the use of SRTP between the Avaya Flare® Experience for Windows Remote Worker (which also uses TLS for transport; see **Section 11.3.1**) and the Avaya SBCE. Rule **RTP_RW** is created for the Remote Worker connection from the Avaya SBCE to Avaya IP Office.

From **Domain Policies** on the left-hand menu, select **Media Rules**. To create the **SRTP_RW** rule, select the **default-low-med** and click on the **Clone** button. Enter a name (e.g., **SRTP_RW**) and click **Finish** (not shown). Edit the created Media Rule to populate the fields in the **Media Encryption** tab as shown below.

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

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

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

Create the Media Rule **RTP_RW** from cloning the **default-low-med** again. The screen below shows the rule's Media encryption tab.

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

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

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

11.1.9. End Point Policy Groups

Two new End Point Policy Groups are defined for Remote Worker. Group **RW_SRTP_PG** is defined for the SRTP connection and **RW_RTP_PG** is defined for the RTP connection.

From **Domain Policies** on the left-hand menu, select **End Point Policy**. Select **Add** button to create a new End Point Policy Group. Enter a name, and click on **Next** (not shown). The **Policy Group** window will open. Enter the values as shown in capture bellow.

End Point Policy Group **RW_SRTP_PG**

Rule Type	Value
Application Rule	RW_AR
Border Rule	default
Media Rule	SRTP_RW
Security Rule	default-low
Signaling Rule	default
Time of Day Rule	default

Finish

End Point Policy Group **RW_RTP_PG**

Rule Type	Value
Application Rule	RW_AR
Border Rule	default
Media Rule	RTP_RW
Security Rule	default-low
Signaling Rule	default
Time of Day Rule	default

Finish

11.1.10. End Point Flows

A Subscriber Flow and a Server Flow are created for Remote Worker.

11.1.10.1 Subscriber Flow

A **Subscriber Flow** is defined as follow.

From **Device Specific Settings** on the left-hand menu, select **End Point Flows**. Click on **Add** and the **Criteria** window will open (not shown).

- Enter a name (e.g., **Flare_RW**)
- **URI Group** = * (default)
- **User Agent** = **Flare**
- **Source Subnet** = * (default)
- **Via Host** = * (default)
- **Contact Host** = * (default)
- **Signaling Interface** = **OutsideSIPRW** (Section 11.1.2)

Click on **Next** (not shown) and the **Profile** window will open (not shown).

- **Source** = **Subscriber**
- **Methods Allowed Before REGISTER**: Leave as default
- **Media Interface** = **OutsideMediaRW** (Section 11.1.3)
- **End Point Policy Group** = **RW_SRTP_PG** (Section 11.1.9).
- **SIP Cluster Flow**: unchecked
- **Routing Profile** = **To-IPO-113-RW** (Section 11.1.5)
- **Topology Hiding Profile** = **None**
- **Phone Interworking Profile** = **Avaya-Ru**
- **TLS Client Profile** = **AvayaSBCCClient**
- **Radius Profile** = **None**
- **File Transfer Profile** = **None**
- **Signaling Manipulation Script** = **None**

The **Subscriber Flows** tab shown below displays the finished Subscribe Flow **Flare_RW**.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
• **Device Specific Settings**
 Network Management
 Media Interface
 Signaling Interface
 Signaling Forking
• **End Point Flows**

End Point Flows: mSBCE

Devices
mSBCE

Subscriber Flows | Server Flows

Click here to add a row description.

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group	
1	Flare_RW	*	*	Flare	RW_SRTP_PG	View Clone Edit Delete

[Add](#)

Clicking on the highlighted **View** link brings up the following **View Flow** window.

Criteria		Optional Settings	
Flow Name	Flare_RW	Topology Hiding Profile	None
URI Group	*	Phone Interworking Profile	Avaya-Ru
User Agent	Flare	TLS Client Profile	AvayaSBCCClient
Source Subnet	*	RADIUS Profile	None
Via Host	*	File Transfer Profile	None
Contact Host	*	Signaling Manipulation Script	None
Signaling Interface	OutsideSIPRW		

Profile	
Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	Flare
Media Interface	OutsideMediaRW
End Point Policy Group	RW_S RTP_PG
Routing Profile	To-IPO-113-RW

11.1.10.2 Server Flow

The following section shows the new **Server Flow** settings for Remote Worker.

From **Device Specific Settings** on the left-hand menu, select **End Point Flows**, then the **Server Flows** tab. Select **Add** (not shown), and enter the following:

- **Name = IPO-113-RW**
- **Server Configuration = IPO-113 (Section 6.2.5)**
- **URI Group = *** (default)
- **Transport = *** (default)
- **Remote Subnet = *** (default)
- **Received Interface = OutsideSIPRW (Section 11.1.2)**
- **Signaling Interface = InsideSIPRW (Section 11.1.2)**
- **Media Interface = InsideMediaRW (Section 11.1.3)**
- **End Point Policy Group = RW RTP_PG (Section 11.1.9)**
- **Routing Profile = default_RW (Section 11.1.5)**
- **Topology Hiding Profile = default**
- **File Transfer Profile = None (default)**

Criteria		Profile	
Flow Name	IPO-113-RW	Signaling Interface	InsideSIPRW
Server Configuration	IPO-113	Media Interface	InsideMediaRW
URI Group	*	End Point Policy Group	RW RTP_PG
Transport	*	Routing Profile	default_RW
Remote Subnet	*	Topology Hiding Profile	default
Received Interface	OutsideSIPRW	File Transfer Profile	None

If this Remote Worker server flow is listed ahead of the flow for SIP Trunking (**IPO-113** as created in **Section 6.4.4**), enter **2** in the **Priority** box at the start of the Remote Worker flow entry and click the **Update** button under the server name. The completed flow should show up in the **Server Flows** tab as below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The title bar includes "Session Border Controller for Enterprise" and the Avaya logo. The left sidebar contains a navigation menu with "Device Specific Settings" and "End Point Flows" highlighted. The main content area is titled "End Point Flows: mSBCE" and has tabs for "Devices", "Subscriber Flows", and "Server Flows". The "Server Flows" tab is active, showing a table of server configurations for "IPO-113". The table has columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. Two rows are visible: one for "IPO-113" with priority 1, and one for "IPO-113-RW" with priority 2. The "IPO-113-RW" row is highlighted with a red border. An "Update" button is located above the table.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IPO-113	*	OutsideSIP	InsideSIP	IPO-113-PG	To-SP	View
2	IPO-113-RW	*	OutsideSIPRW	InsideSIPRW	RW RTP_PG	default_RW	View

11.2. Remote Worker Endpoint Configuration on Avaya IP Office

The Remote Worker Avaya Flare® Experience for Windows endpoint is added to the Avaya IP Office **User** and **Extension** configuration.

11.2.1. Extension and User Configuration

No special configurations are required to create the Remote Worker extension and user in Avaya IP Office. Follow the same standard procedures for creating a local extension and user for Avaya Flare® Experience for Windows.

The Remote Worker user provisioned is shown below. Note that since the Remote Worker endpoint used in the reference configuration is Avaya Flare® Experience for Windows, the **Enable Softphone** and **Enable Flare** options are selected.

Note – Do not check the **Enable Remote Worker** option. This is only enabled for Avaya IP Office “native” Remote Worker configurations, not for Remote Worker configurations utilizing the Avaya SBCE.

The screenshot displays the Avaya IP Office configuration interface for extension 29236. The left sidebar shows a list of users and extensions, with '29236 Extn29236' selected. The main window shows the configuration for this extension, with the 'User' tab active. The configuration fields are as follows:

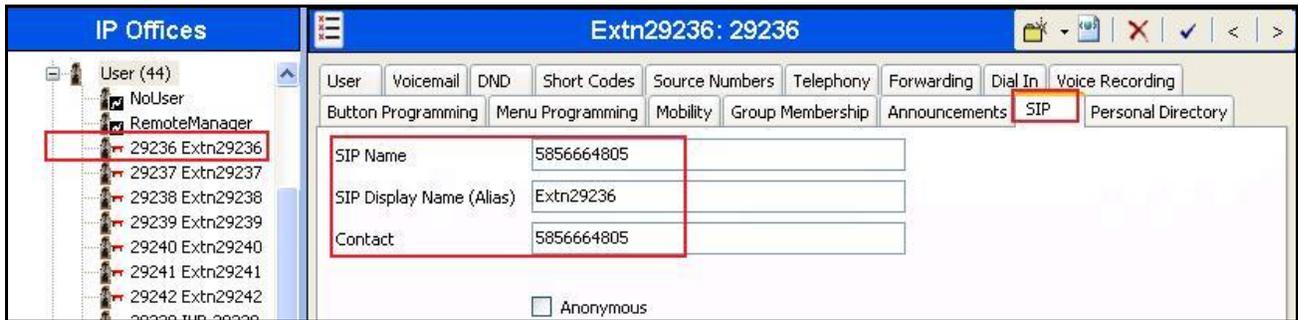
Field	Value
Name	Extn29236
Password	••••
Confirm Password	••••
Account Status	Enabled
Full Name	SIP User PM
Extension	29236
Email Address	
Locale	United States (US English)
Priority	5
System Phone Rights	None
ACCS Agent Type	None
Profile	Power User

Below the fields, there are several checkboxes:

- Receptionist
- Enable Softphone
- Enable one-X Portal Services
- Enable one-X TeleCommuter
- Enable Remote Worker
- Enable Flare
- Enable Mobile VoIP Client
- Send Mobility Email

The 'OK' button is highlighted with a red box.

The **SIP** tab for the Remote User is configured the same way as with local IP Office user (see **Section 5.6**).



11.2.2. Incoming Call Route

Follow the same procedures described in **Section 5.7** for defining an Incoming Call Route to the Remote Worker.



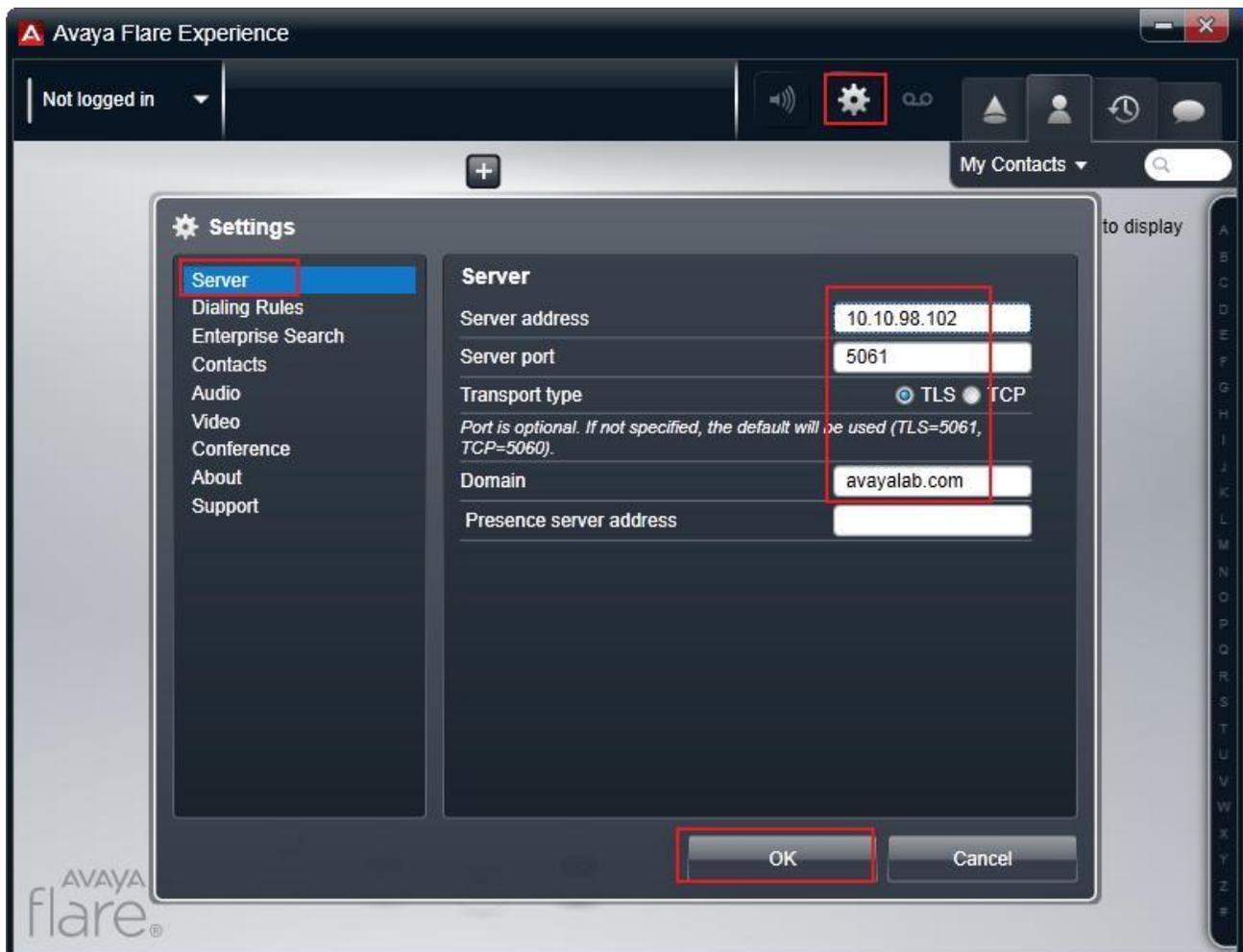
11.3. Remote Worker Avaya Flare® Experience for Windows Configuration

The following screens illustrate Avaya Flare® Experience for Windows administration settings for Remote Worker as used in the reference configuration.

11.3.1. Settings – Server Screen

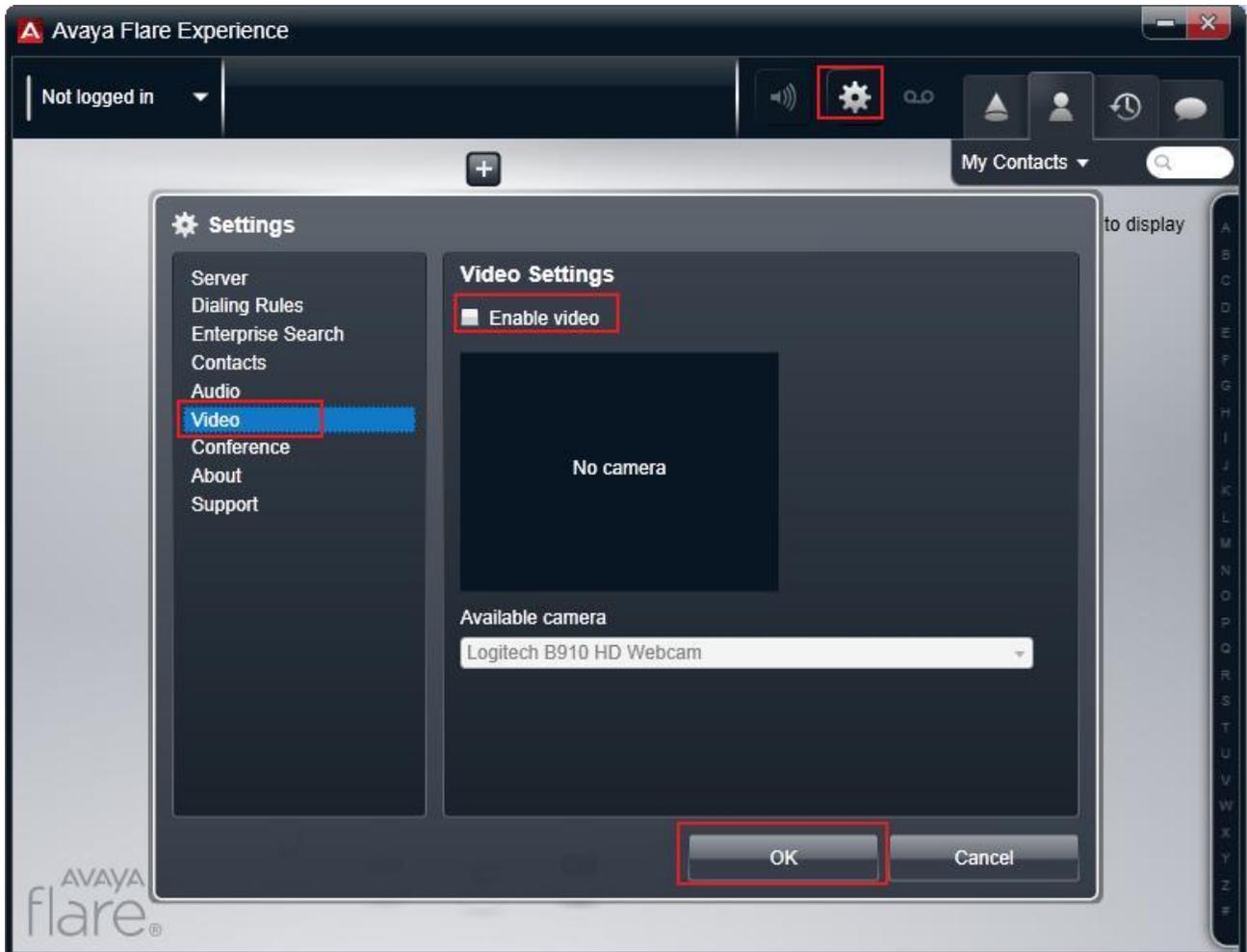
After opening the Avaya Flare® Experience for Windows application, select the Settings icon, select **Server** from the Settings menu, and enter the following:

- **Server address** = **10.10.98.102** (the IP address of Remote Worker outside interface **B1** on Avaya SBCE (see **Section 11.1.1**).
- **Server port** = **5061** (note that the **Transport type** will automatically change to **TLS**).
- **Domain** = IP Office SIP Registrar domain name (**avayalab.com** was used for the compliance test. See the VoIP tab screenshot in **Section 5.1**).



11.3.2. Setting – Video Screen

Select **Video** from the Settings menu, *unselect* the **Enable Video** option. In Release 1.1 of Avaya Flare® Experience for Windows, only audio calls are supported with SRTP media encryption (see **Section 11.1.8**).



©2014 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.