Avaya Solution & Interoperability Test Lab

Application Notes for Configuring IDT Net2Phone® SIP Trunking Service with Avaya IP Office R9.1 and Avaya Session Border Controller for Enterprise 6.3 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 6.3 to inter-operate with the IDT Corporation Net2Phone® SIP Trunking Service. IDT is a member of the Avaya DevConnect Service Provider program.

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

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

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.

©2015 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction 4
2. General Test Approach and Test Results 4
   2.1. Interoperability Compliance Testing 4
   2.2. Test Results 5
   2.3. Support 6
3. Reference Configuration 7
4. Equipment and Software Validated 9
5. Configure Avaya IP Office 10
   5.1. Licensing and Physical Hardware 11
   5.2. System 13
      5.2.1. System – LAN1 Tab 13
      5.2.2. System - Voicemail Tab 17
      5.2.3. System - Telephony Tab 18
      5.2.4. System - Twinning Tab 19
      5.2.5. System – Codecs Tab 19
   5.3. IP Route 20
   5.4. Administer SIP Line 21
      5.4.1. Create SIP Line From Template 22
      5.4.2. SIP Line – SIP Line Tab 26
      5.4.3. SIP Line – Transport Tab 27
      5.4.4. SIP Line – SIP URI Tab 28
      5.4.5. SIP Line – VoIP Tab 30
      5.4.6. SIP Line – T38 Fax 31
      5.4.7. SIP Line – SIP Credentials Tab 31
      5.4.8. SIP Line – SIP Advanced Tab 32
   5.5. Short Code 33
   5.6. User 35
   5.7. Incoming Call Route 36
   5.8. ARS and Alternate Routing 38
   5.9. Mobility 39
   5.10. SIP Options 40
   5.11. Save Configuration 41
6. Configure Avaya Session Border Controller for Enterprise 42
   6.1. Access Management Interface 42
   6.2. Verify Network Configuration and Enable Interfaces 44
   6.3. Signaling Interface 46
   6.4. Media Interface 47
   6.5. Server Interworking 48
      6.5.1. Server Interworking – Avaya IP Office 49
      6.5.2. Server Interworking – IDT 51
   6.6. Server Configuration 53
      6.6.1. Server Configuration – Avaya IP Office 54

©2015 Avaya Inc. All Rights Reserved.

6.6.2. Server Configuration – IDT 55
6.7. Application Rules 58
6.8. Media Rules 59
6.9. Signaling Rules 61
6.10. End Point Policy Groups 62
6.10.1. End Point Policy Group – Avaya IP Office 63
6.10.2. End Point Policy Group – IDT 64
6.11. Routing 65
6.11.1. Routing – Avaya IP Office 66
6.11.2. Routing – IDT 67
6.12. Topology Hiding 69
6.13. End Point Flows 71
6.13.1. End Point Flow – Avaya IP Office 72
6.13.2. End Point Flow – IDT 74
7. IDT SIP Trunking Service Configuration 75
8. Verification Steps 76
8.1. Avaya IP Office System Status 76
8.2. Avaya IP Office Monitor 78
8.3. Avaya SBCE Protocol Trace 79
9. Conclusion 79
10. Additional References 80

©2015 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedures for configuring an enterprise solution using Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.3 to interoperate with the IDT Corporation Net2Phone® SIP Trunking Service.

The IDT Net2Phone® SIP Trunking Service referenced within these Application Notes is positioned for customers who have an IP-PBX or IP-based network equipment with SIP functionality, but need a network service to access the PSTN from the enterprise using IP transport to complete their solution.

The IDT Net2Phone® SIP Trunking Service will enable delivery of origination and termination of local, long-distance, toll-free, international, and other types of calls across a single broadband IP connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE).

For brevity, the remainder of this document refers to the IDT Net2Phone® SIP Trunking Service as IDT SIP Trunking Service or simply IDT.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the IDT SIP Trunking Service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site comprised of an Avaya IP Office 500 V2 running Release 9.1 software, Avaya Voicemail Pro messaging application, Avaya H.323 and SIP deskphones, and the SIP-based Avaya Communicator softphone. The enterprise solution connects to the IDT network via the Avaya SBCE.

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

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- SIP trunk registration with the IDT SIP Trunking Service.
- SIP OPTIONS queries to and responses from the service provider.
- Incoming calls from the PSTN to H.323 and SIP telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing calls to the PSTN from H.323 and SIP telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Digest Authentication on outbound calls to the PSTN.

©2015 Avaya Inc. All Rights Reserved.

- Various call types including: local, long distance, toll-free and international calls.
- G.711MU and G.729A codecs.
- Caller ID presentation and Caller ID restriction.
- DTMF transmission using RFC 2833.
- Voicemail access and navigation for inbound and outbound calls.
- Telephony supplementary features such as hold and resume, transfer, and conference.
- Off-net call forwarding and call transfer/conference.
- Twinning on inbound calls to PSTN mobile phones.
- Use of the SIP INVITE method for call redirection (call transfer) to the PSTN.
- Inbound and outbound long-duration calls stability.
- Inbound and outbound long hold time call stability.
- Response to incomplete call attempts and trunk busy or error conditions.
- T.38 and G.711 pass-through fax.
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise extensions.

2.2. Test Results

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

- **SIP Trunk Registration –** For the compliance test, SIP trunk registration was configured on Avaya SBCE instead of on IP Office. This choice was necessitated by the following problem: certain configuration changes (e.g., codec changes on SIP Line, or changing Max Calls per Channel in SIP URI on SIP Line) will cause IP Office to take the SIP trunk out of service, then bring it back in service again by issuing 2 REGISTER messages in quick succession within one second. The first REGISTER is for de-registering the trunk, the 2nd REGISTER is for re-registering the trunk. However, if the service provider would respond to the 2nd re-registration REGISTER first, and to the 1st de-registration REGISTER second, the SIP trunk would be effectively disabled from this point on until the next REGISTER from IP Office after the registration expiry has been reached. This would create a large window of down circuit if the registration expiry is set to a relatively large value (default is 60 minutes). This problem was reported to the Avaya IP Office development. Before a fix becomes available, it is recommended that SIP trunk registration be configured on Avaya SBCE (see **Section 6.6.2**) instead of on IP Office (see **Section 5.4.7**).
- **OPTIONS –** The IDT SIP Trunking Service was configured not to send OPTIONS to the enterprise site during compliance testing. IDT responded to OPTIONS from the enterprise site properly with “200 OK”.
- **Codec Negotiation –** When outbound call was configured to use G.729a as the preferred codec of multiple codecs offer, IDT responded with G.711u in the SDP of the call connect "200 OK" message, and G.711u was used in the RTP media of the connected call. G.729a should have been used in this call scenario. IDT indicated that this might be an issue with the specific backbone PSTN carrier being used by IDT. Note that a single G.729a codec offer worked as expected.
- **Inbound Busy –** For an inbound call to a busy IP Office user, IP Office properly returned "486 Busy Here" to IDT, but the PSTN caller did not receive busy tones as expected.

©2015 Avaya Inc. All Rights Reserved.

Instead, an announcement was heard about leaving a message, followed by a prompting beep tone. This was because IDT configured network-based messaging on the test circuit as with some of its SIP Trunking customers. Note that routing calls to network-based messaging also applied to other call exception conditions, like no answer to inbound calls and/or inbound calls to an invalid enterprise extension, etc..

- **Caller ID Block –** When a PSTN caller blocked Caller ID by dialing "*67" before the destination DID, the Caller ID was not blocked by IDT; the caller name/number was still displayed at the called IPO endpoint. Caller ID blocking on outbound calls worked properly. This problem is under investigation by IDT SIP Trunking support and development.
- **Inbound Fax –** Inbound fax, either T.38 or G.711 pass-through, failed. The failures were caused by incorrect From and To header settings in the T.38 re-INVITE from IDT or in the IDT "200 OK" response to the re-INVITE message from IP Office. Consequently, the Avaya SBCE either sent a 481 error status message to IDT or did not ACK the "200 OK" messages from IDT. This problem is under investigation by IDT SIP Trunking support and development. Until a resolution becomes available, IDT customers should refrain from using inbound fax via the IDT SIP Trunking Service. Outbound fax, either T.38 or G.711 pass-through, was tested/verified successfully.
- **Direct Media –** The Direct Media capability on IP Office allows RTP media directly between the inside interface of the Avaya SBCE and the IP endpoints rather than having all the media flow through the IP Office, using up VoIP and relay resources. This capability is not supported by Avaya IP Office on the SIP trunk connection which allows T.38 fax in addition to voice calls. Consequently, Direct Media was disabled for the test circuit configured for the compliance test.

Items not supported or not tested include the following:

- **Operator Calls** – IDT does not support Operator (0), Operator-Assisted (0 + 10-digits), and Directory Assistance (411) calls.
- **REFER** – IDT does not support use of the SIP REFER method for transferring calls off-net to the PSTN. In the compliance test, off-net call transfer was tested using the SIP INVITE method.
- **UPDATE –** IDT does not support the SIP UPDATE message (the Allowed header in SIP messages from IDT does not contain UPDATE). Consequently, Avaya IP Office used re-INVITE messages to refresh active call sessions during the compliance test.
- **Session Timer –** Session timer based on RFC 4028 is not implemented by IDT. During compliance testing, the enterprise sent session refresh re-INVITE messages towards IDT with the configured session timer on Avaya IP Office.
- **Call Types Not Tested –** Emergency 911 and inbound toll-free calls were not tested.

2.3. Support

Contact information for technical support on the IDT Net2Phone SIP Trunking Service:

- Web: http://www.net2phonesiptrunking.com
- Email: via the Contac link on above web site

©2015 Avaya Inc. All Rights Reserved.

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

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The sample configuration shows an enterprise site connected to the IDT SIP Trunking Service.

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.

The enterprise endpoints include both local extensions and Remote Worker phones that are connected directly to the public Internet. The same Avaya SBCE was configured to connect to both the service provider network and Remote Worker using separate sets of public/private interfaces (**Figure 1** only shows the public/private interfaces used for connecting to the service provider network).

Within the enterprise site is an Avaya IP Office 500 V2 running the Release 9.1 software. Endpoints include various Avaya IP Deskphones (with H.323 and SIP firmware) and the SIP-based Avaya Communicator softphone. The site also has a Windows PC running Avaya Preferred Edition (a.k.a. Voicemail Pro) for providing voice messaging service to the Avaya IP Office users, and Avaya IP Office Manager for administering the Avaya IP Office.

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.

©2015 Avaya Inc. All Rights Reserved.

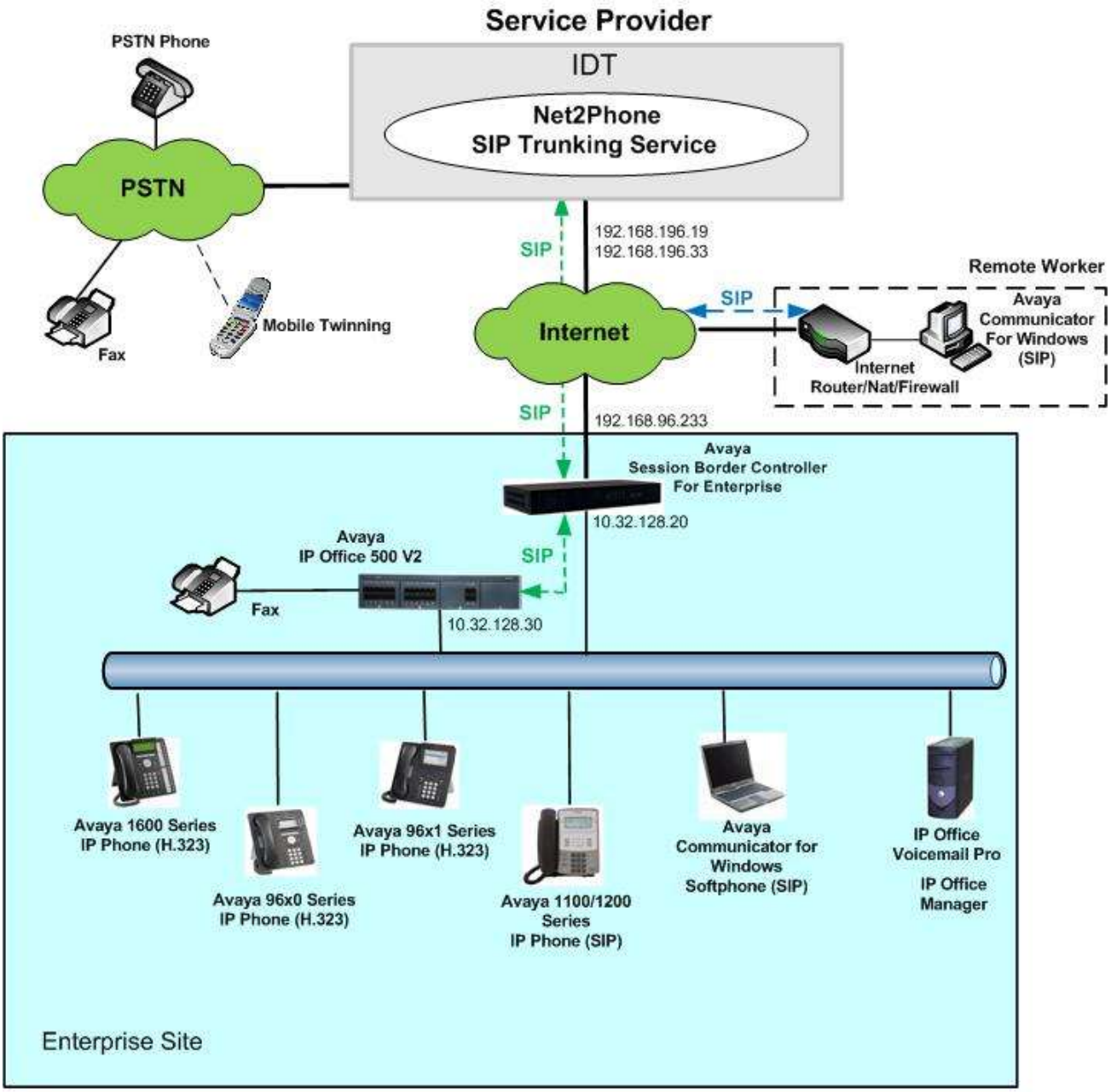


Figure 1: Test Configuration

For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses in these Application Notes.

During compliance testing, users dialed a prefix digit 8 or 9 plus N digits to send an outbound call to the number N across the SIP trunk to IDT. The short code of 8 or 9 was stripped off by Avaya IP Office but the remaining N digits were sent to the service provider network. For calls within the North American Numbering Plan (NANP), the user dialed 11 (1 + 10) digits for long distance and local calls. Thus, for these NANP calls, Avaya IP Office sent 11 digits in the Request URI and the

©2015 Avaya Inc. All Rights Reserved.

To header of an outbound SIP INVITE message. IDT also sent 11 digits in the Request URI and the To header of inbound SIP INVITE messages.

IDP provided 2 access interface IP addresses for the test circuit. The enterprise was configured to receive inbound calls from any of these 2 IP addresses. Outbound calls were configured to be routed to the 2 IDT IP addresses alternately on a round-robin basis.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the enterprise network such as a 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 Avaya IP Office must be allowed to pass through these devices.

The administration of the Avaya Voicemail Pro messaging service and endpoints on Avaya IP Office are standard. Since these configuration tasks are not directly related to the inter-operation with the IDT SIP Trunking Service, they are not included in these Application Notes. Remote Worker configuration is also not covered by these Application Notes. For configuration details on Avaya IP Office and Avaya SBCE to support Remote Worker, see **[9]** in **Section 10**.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment / Software	**Release / Version**
Avaya IP Office 500 V2	9.1.2.0 build 91
Avaya IP Office COMBO6210/ATM4 Module	9.1.2.0 build 91
Avaya IP Office Manager	9.1.2.0 build 91
Avaya Preferred Edition (a.k.a Voicemail Pro)	9.1.200.61
Avaya Session Border Controller for Enterprise running on a Portwell CAD-0208 server	6.3.2-08-5478
Avaya 1616 IP Telephones (H.323)	Avaya one-X® Deskphone 1.3 SP5
Avaya 9611G IP Telephones (H.323)	Avaya one-X® Deskphone 6.6.0.29_V474
Avaya 9630G IP Telephones (H.323)	Avaya one-X® Deskphone 3.2.3
Avaya 1120E IP Telephone (SIP)	4.04.18.00
Avaya Communicator for Windows	2.0.3.30
IDT Components	
Equipment / Software	**Release / Version**
Net2Phone IPPBX	IDT SBC2 1.0
Net2Phone SIPTSS Signaling Gateway	IDT SBC2 1.0

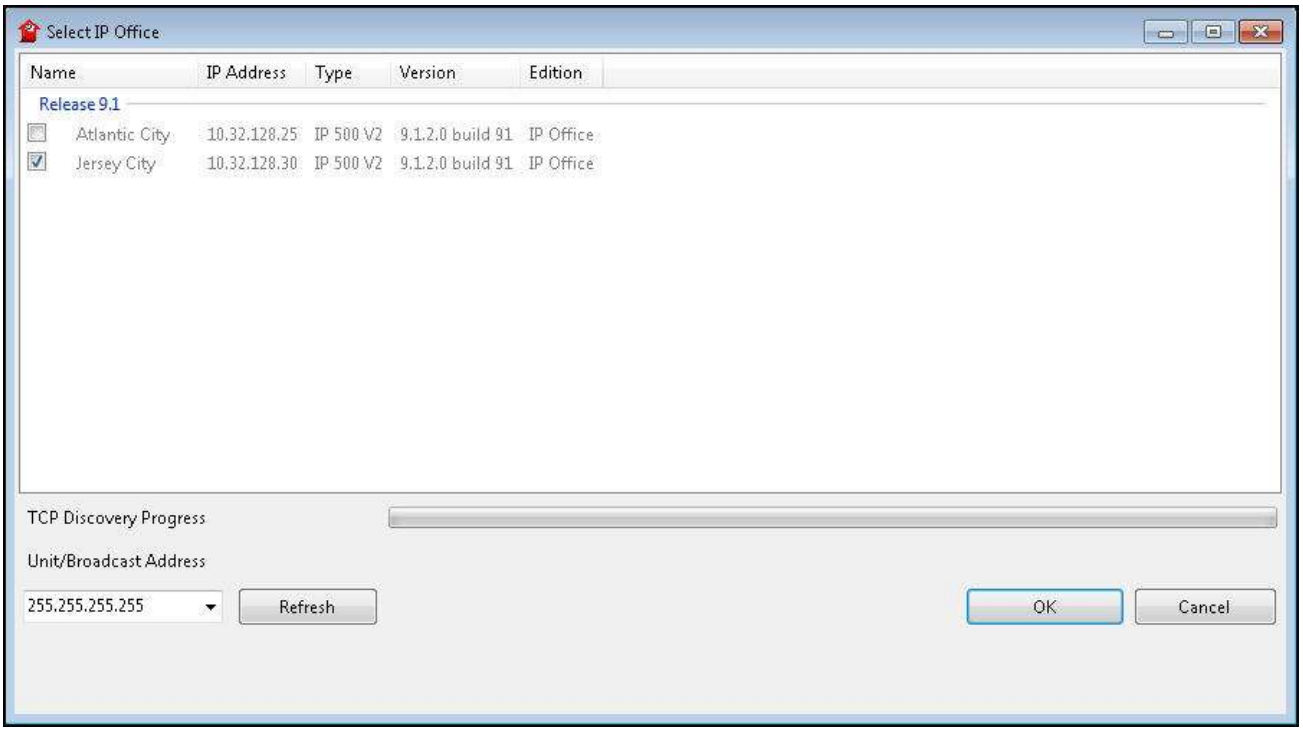
Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2, and also when deployed with all configurations of IP Office Server Edition without T.38

©2015 Avaya Inc. All Rights Reserved.

Fax service (T.38 Fax is not supported on IP Office Server Edition). Note that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog/digital endpoints or trunks.

5. Configure Avaya IP Office

Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the PC running Avaya IP Office Manager, select **Start → All Programs → IP Office → Manager** to launch the application. A **Select IP Office** pop-up window is displayed as shown below. Select the proper Avaya IP Office system from the pop-up window and click **OK** to log in with the appropriate credentials (not shown). The configuration may alternatively be opened by navigating to **File → Open Configuration** at the top of the Avaya IP Office Manager window.



The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation Pane on the left side, omit the Group Pane in the center, and show the Details Pane on the right side. Since the Group Pane has been omitted, its content is shown as submenus in the Navigation Pane. These panes (Navigation and Details) will be referenced throughout the Avaya IP Office configuration.

All licensing and feature configuration that is not directly related to the interface with the service provider (such as administering IP endpoints) is assumed to already be in place.

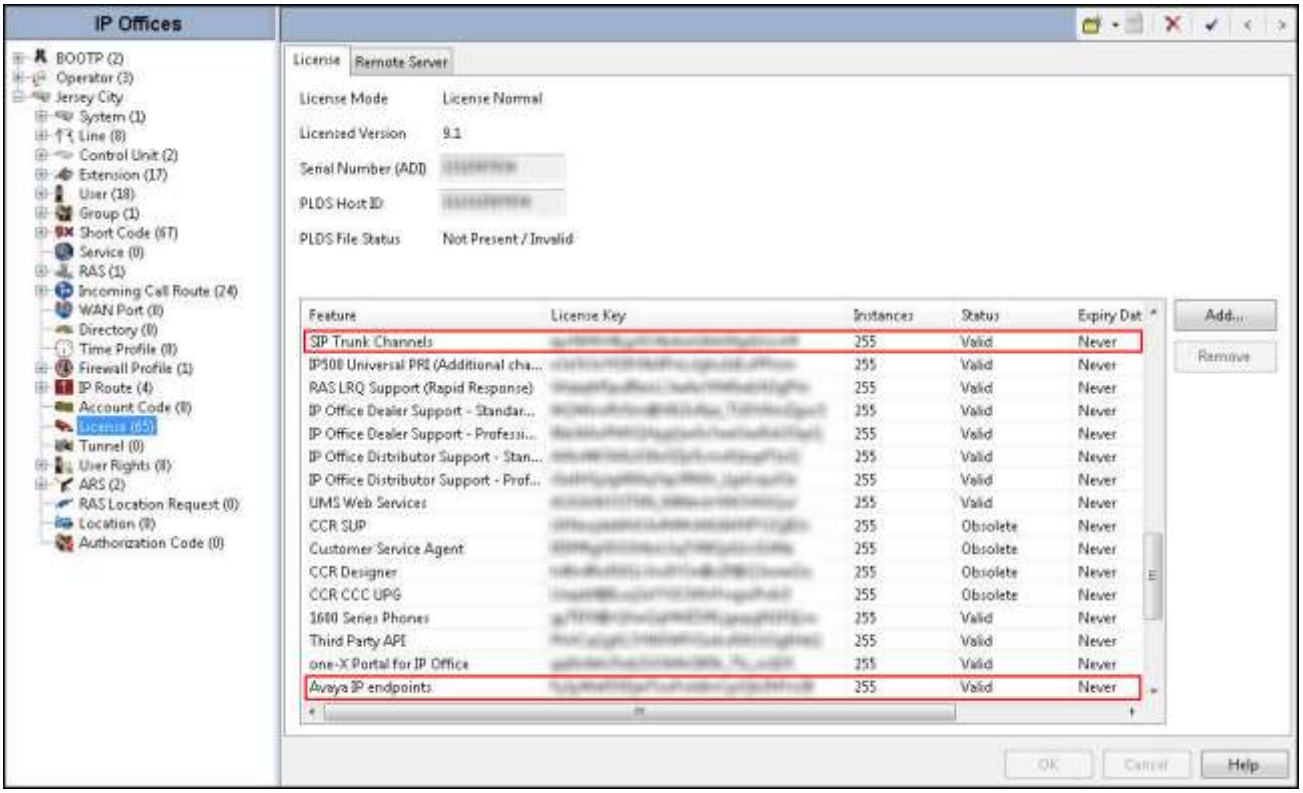
In the sample configuration, **Jersey City** was used as the system name. All navigation described in the following sections (e.g., **Control Unit → IP 500 V2)** appears as submenus underneath the system name **Jersey City** in the Navigation Pane. The configuration screens highlight values/settings configured for the compliance test. Defaults were used for other values and may be customized based upon requirements in the field.

©2015 Avaya Inc. All Rights Reserved.

5.1. Licensing and Physical Hardware

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

To verify that there is a **SIP Trunk Channels** License with sufficient capacity, click **License** in the Navigation Pane. Confirm a valid license with sufficient **Instances** (trunk channels) in the Details Pane. The screen below also shows the valid license for **Avaya IP endpoints**.

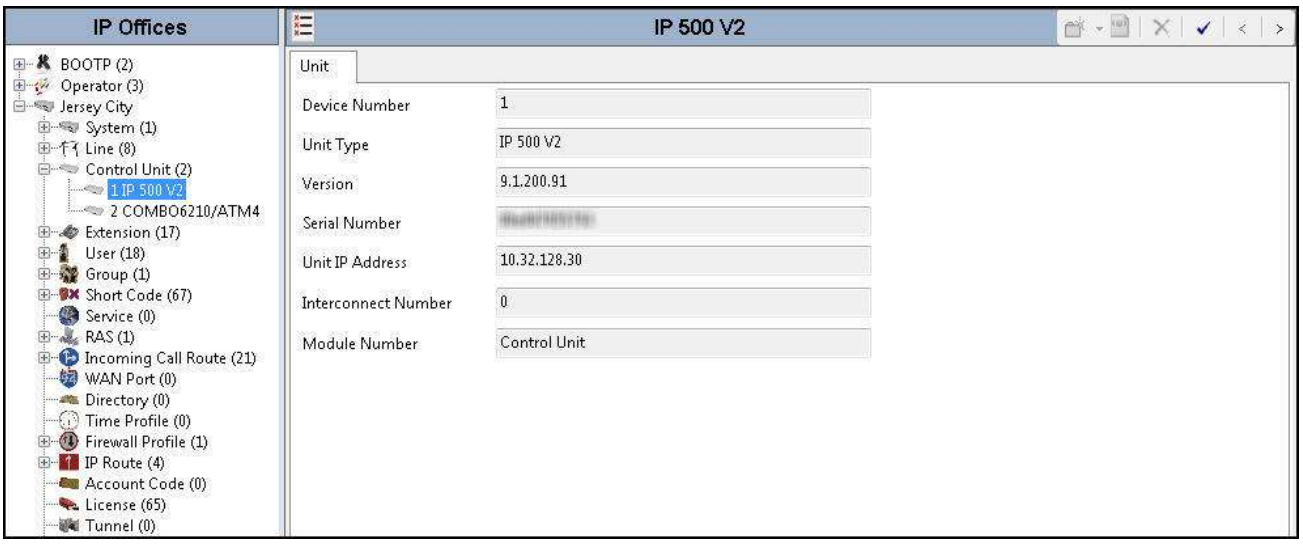


©2015 Avaya Inc. All Rights Reserved.

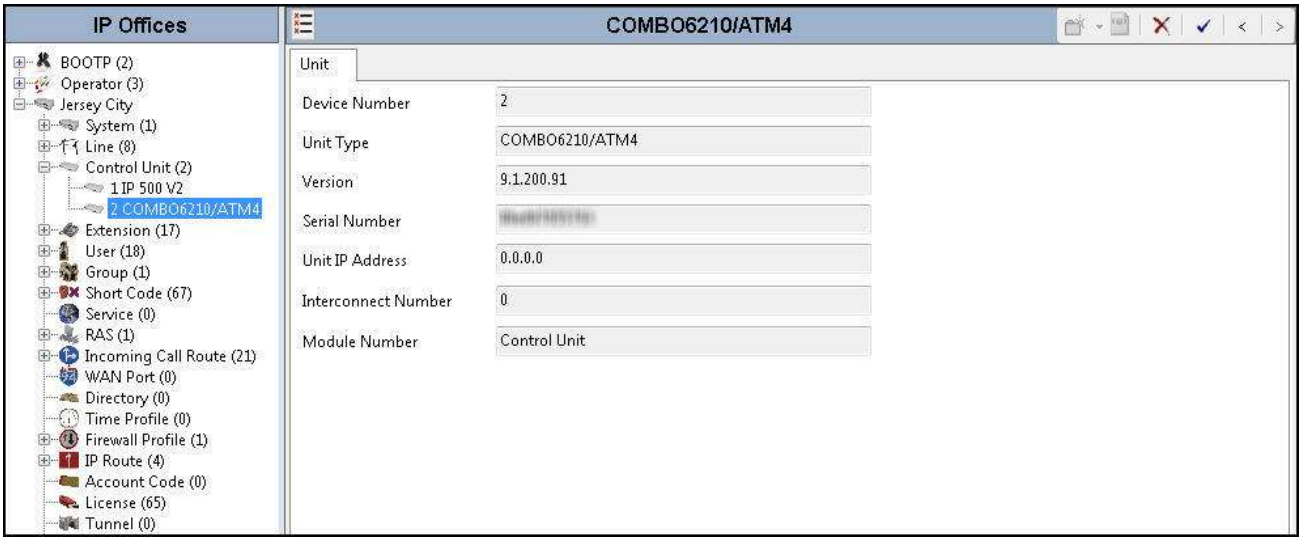
To view the physical hardware comprising the Avaya IP Office system, expand the components under **Control Unit** in the Navigation Pane. In the sample configuration, the second component listed is a Combination Card. This module has 6 digital station ports, two analog extension ports, 4 analog trunk ports and 10 VCM channels. The VCM is a Voice Compression Module supporting VoIP codecs. An Avaya IP Office hardware configuration with a VCM component is necessary to support SIP Trunking.

To view the details of the component, select the component in the Navigation Pane.

The screen below shows the details of the IP 500 V2.



The screen below shows the details of the Combination Card.



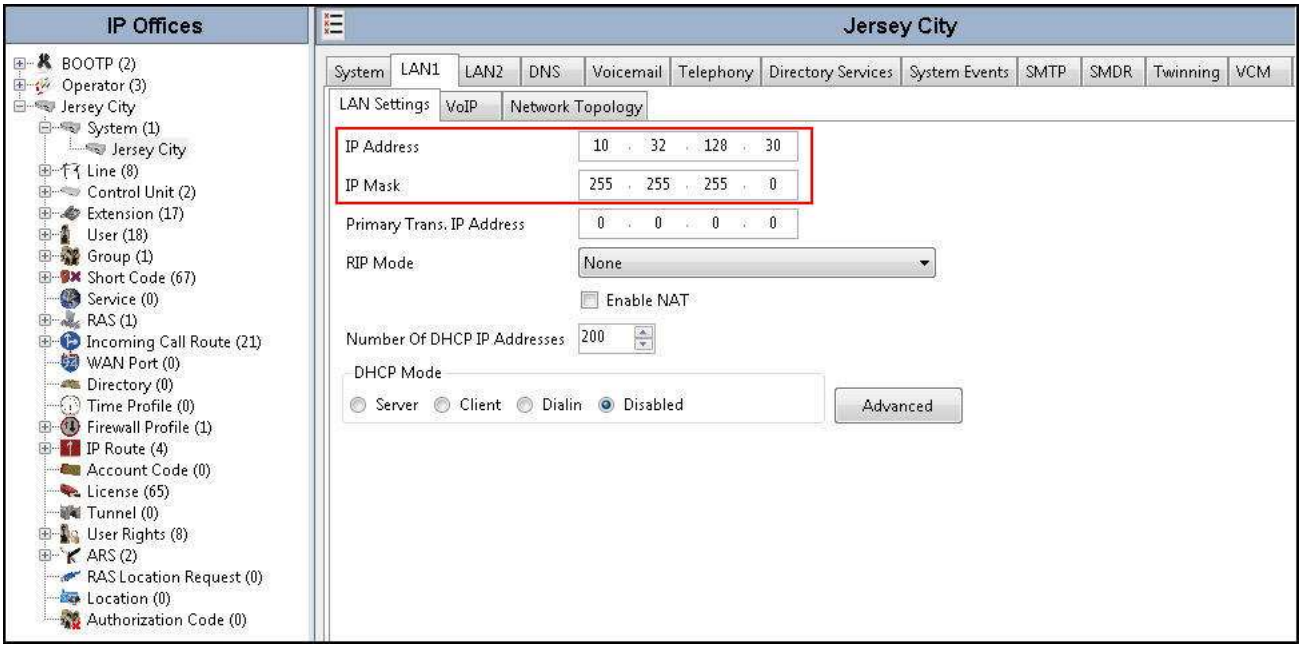
©2015 Avaya Inc. All Rights Reserved.

5.2. System

This section configures the necessary system settings.

5.2.1. System – LAN1 Tab

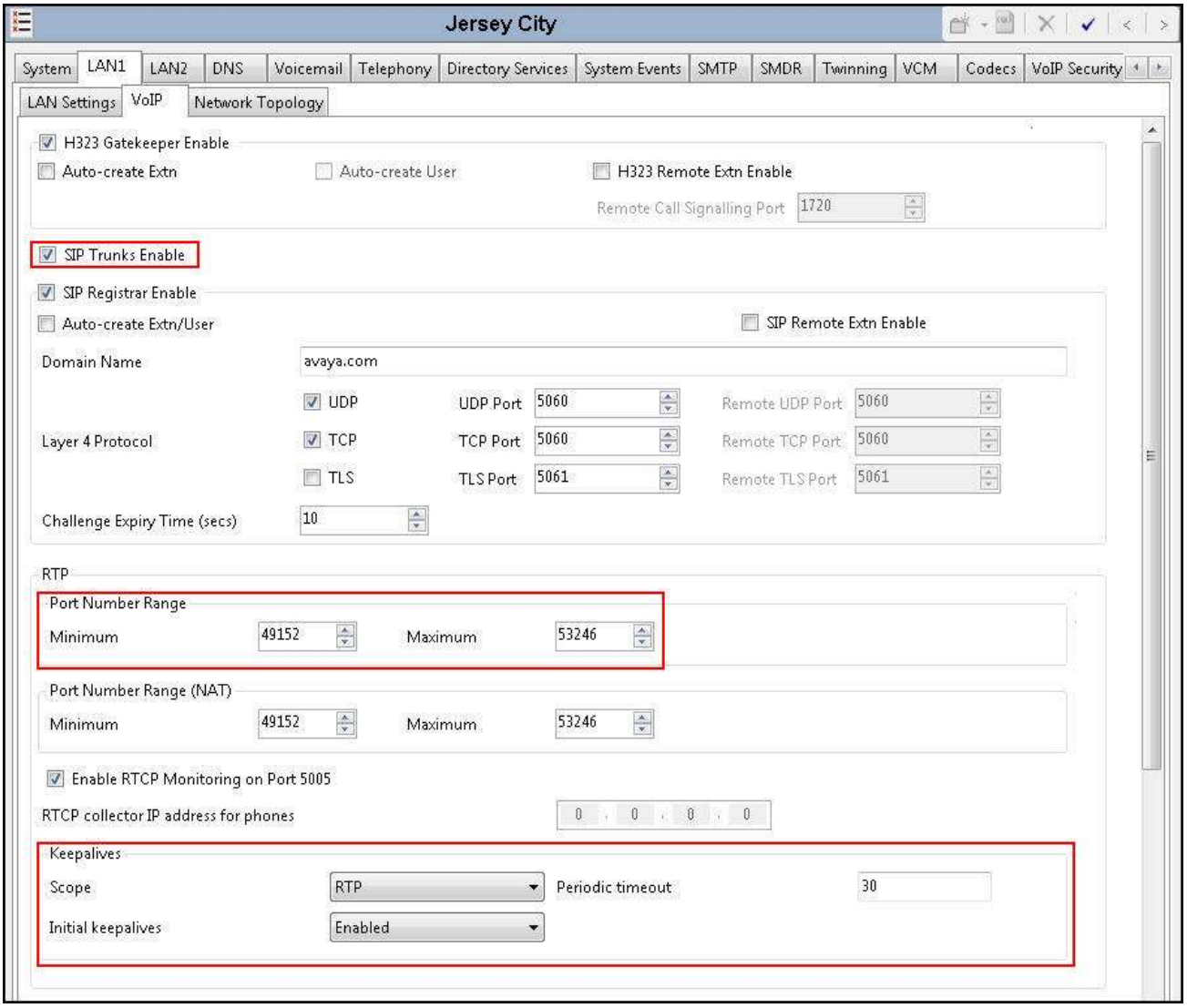
In the sample configuration, the Avaya IP Office LAN port was used to connect to the enterprise network. The LAN1 settings correspond to the LAN port on the Avaya IP Office 500 V2. To access the LAN1 settings, first navigate to **System → <*Name*>**, where <*Name*> is the system name assigned to the IP Office. In the case of the compliance test, the system name is **Jersey City**. Next, navigate to the **LAN1 → LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office LAN port. Set the **IP Mask** field to the mask used on the enterprise network.



©2015 Avaya Inc. All Rights Reserved.

On the **VoIP** tab of LAN1 in the Details Pane, configure the following parameters:

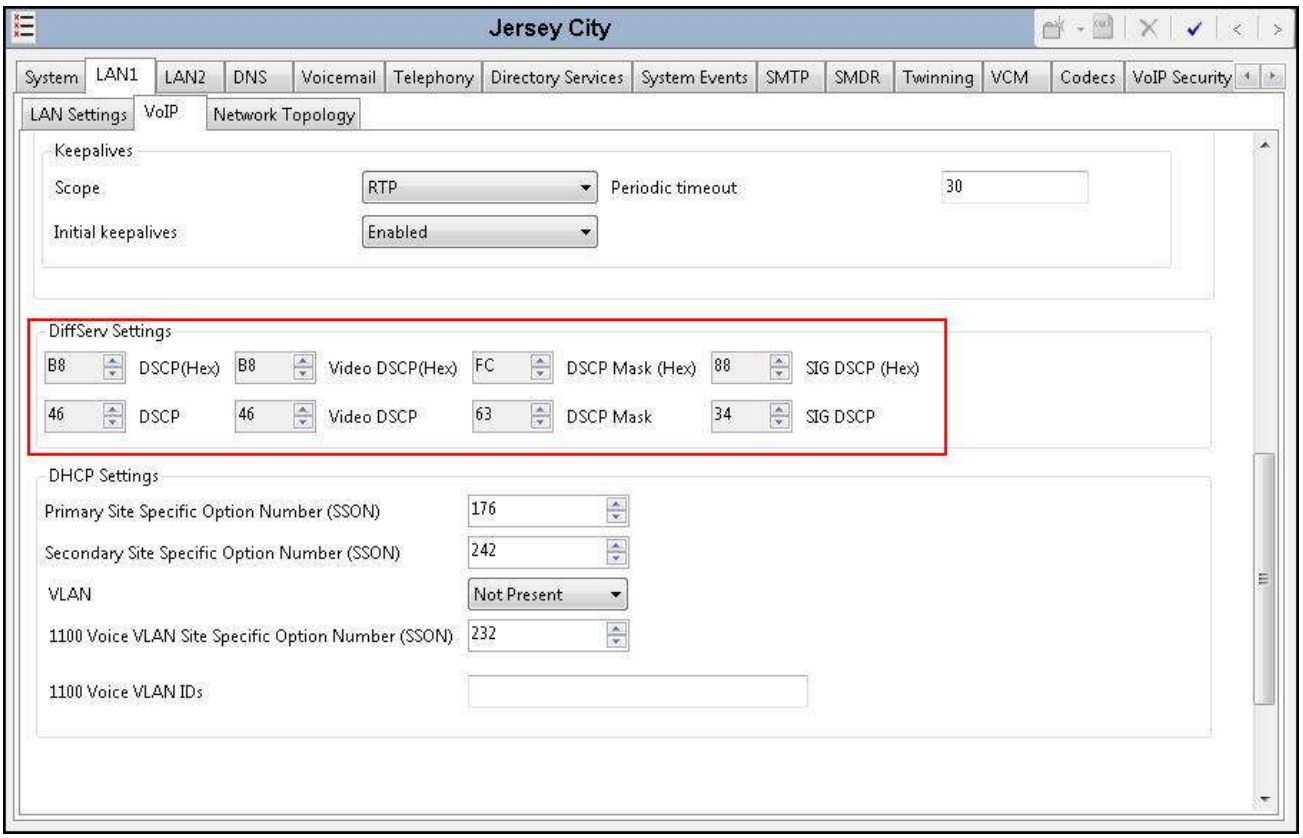
- Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks.
- In the **RTP** section, the **RTP Port Number Range** can be customized to a specific range of receiving ports for the RTP media, as agreed with the service provider. Based on this setting, Avaya IP Office would request RTP media be sent to a port in the configurable range for calls using LAN1.
- In the **Keepalives** section, select ***RTP*** for **Scope**; select ***Enabled*** for **Initial keepalives**; enter ***30*** for **Periodic timeout**. These settings direct IP Office to send a RTP keepalive packet starting at the time of initial connection and every 30 seconds thereafter if no other RTP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting for media from the other, as well as helping to keep firewall (if used) ports open for the duration of the call.



©2015 Avaya Inc. All Rights Reserved.

Though not highlighted in the above screen, note the settings for **SIP Registrar Enable**, **Domain Name**, and **Layer 4 Protocol**. These settings are necessary for the IP Office to serve as the SIP Registrar Server for the IP Office SIP endpoints.

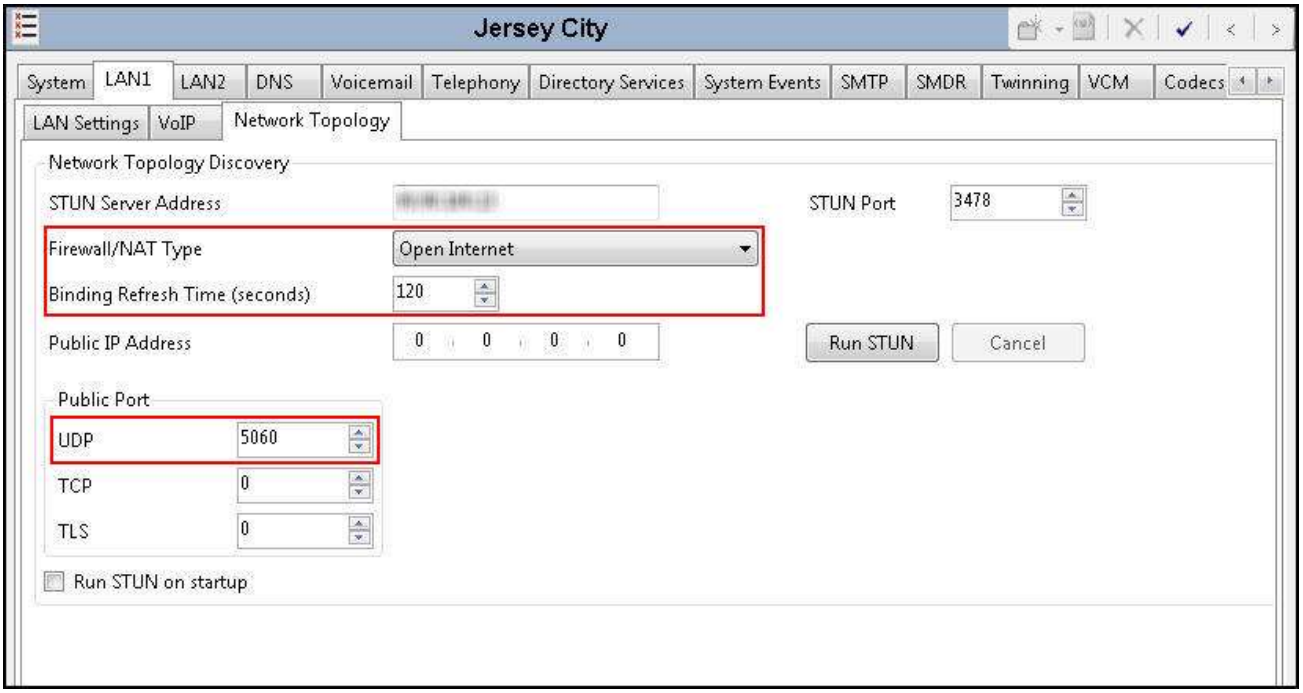
Scroll down to the **DiffServ Settings** section. Avaya IP Office can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for both signaling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling. The specific values used for the compliance test are shown in the screen below and are also the default values. For a customer installation, if the default values are not sufficient, appropriate values should be provided by the customer.



©2015 Avaya Inc. All Rights Reserved.

On the **Network Topology** tab of LAN1 in the Details Pane, configure the following parameters:

- Select **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 the ***Open Internet*** setting, **STUN Server Address** is not used.
- Set **Binding Refresh Time (seconds)** to a desired value. 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 5.10** for complete details.
- Set **Public Port** to ***5060*** for **UDP**.

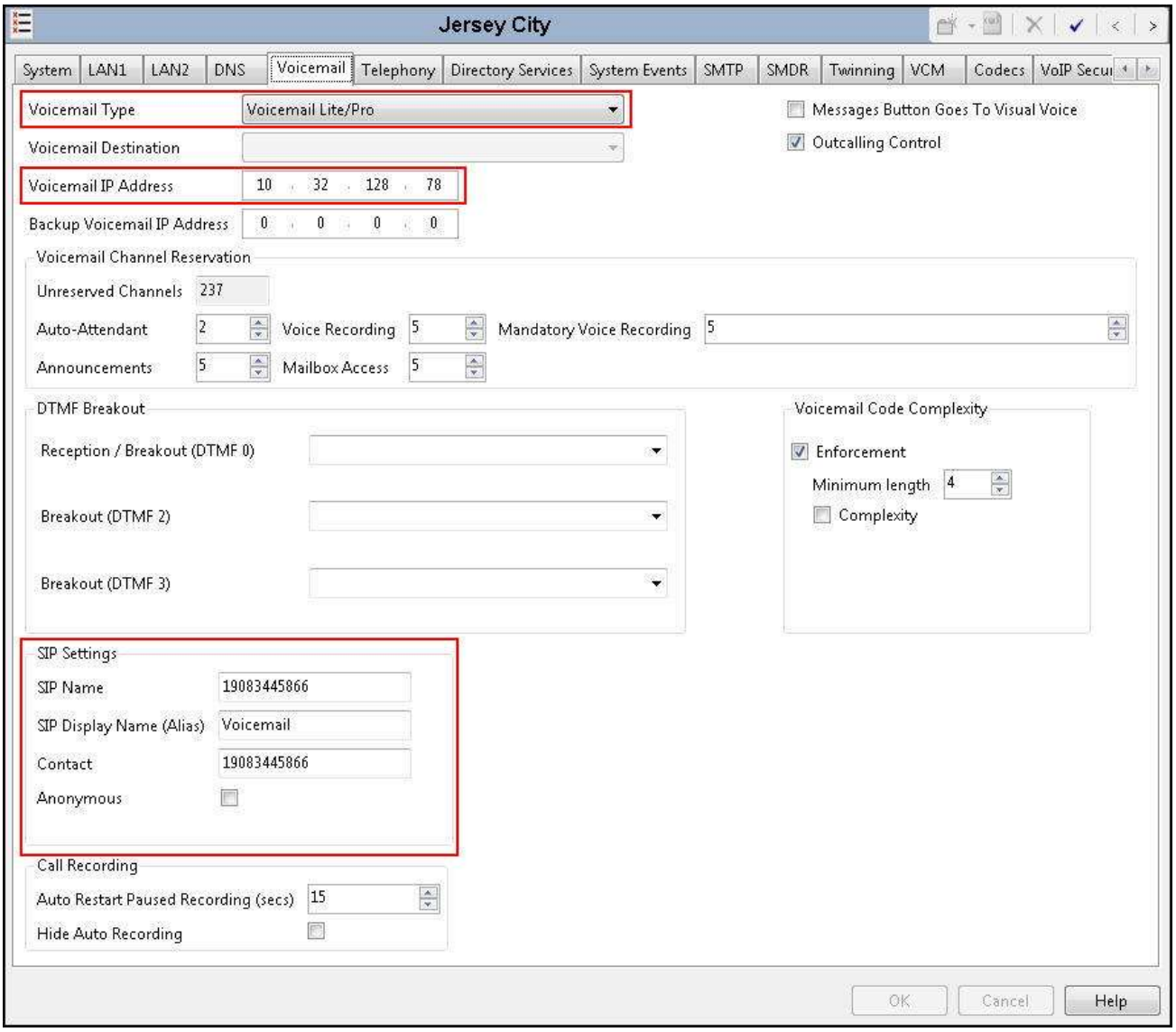


©2015 Avaya Inc. All Rights Reserved.

5.2.2. System - Voicemail Tab

In the **Voicemail** tab of the Details Pane, configure the **SIP Settings** section. The **SIP Name** and **Contact** are set to one of the DID numbers provided by IDT. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. Uncheck the **Anonymous** box to allow the Voicemail Caller ID information to be sent to the network.

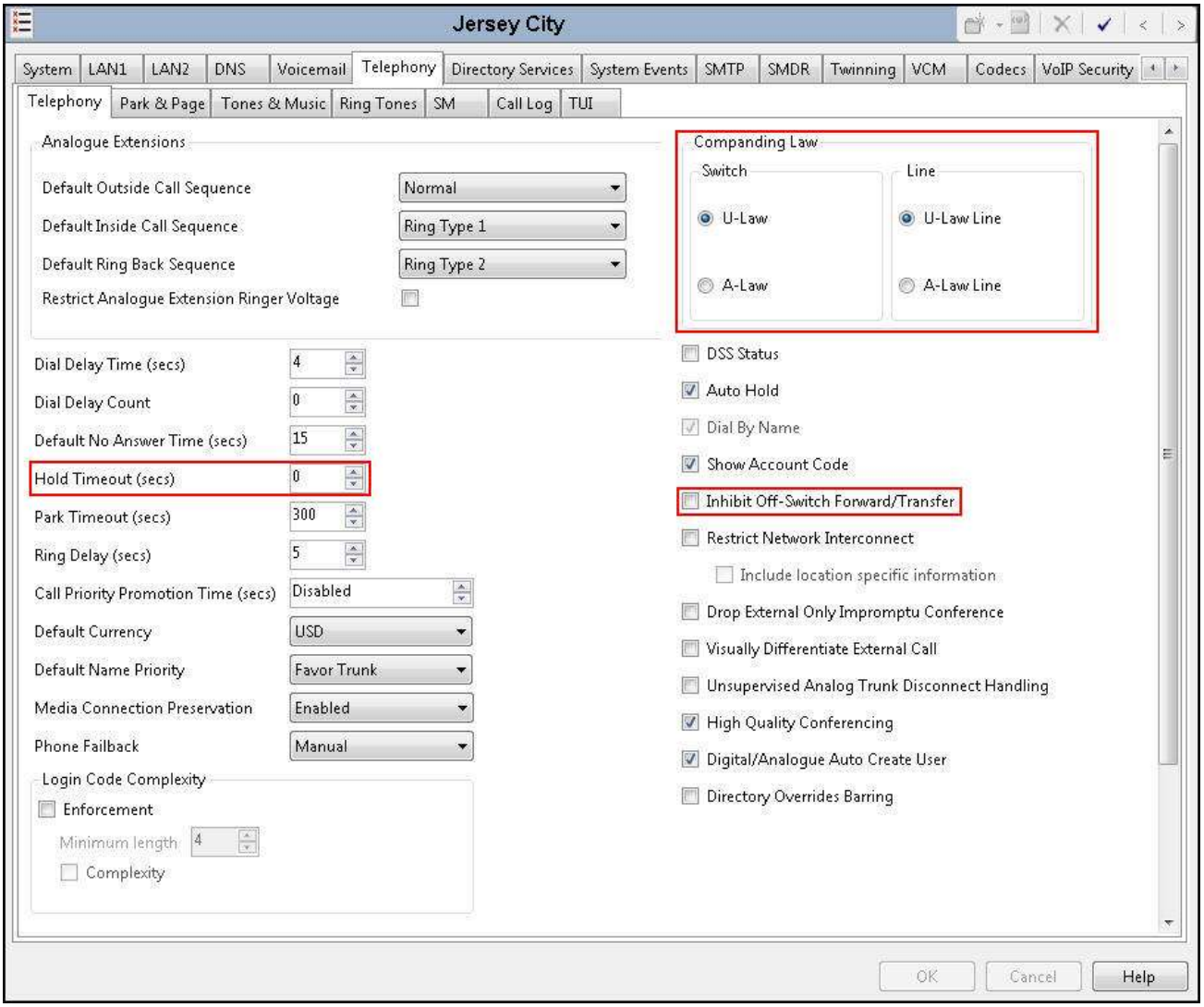
Note the selection for **Voicemail Type** and the IP address setting for **Voicemail IP Address**. These are for configuring Voicemail Pro as the voice messaging service for Avaya IP Office users (part of the standard IP Office setup beyond the scope of these Application Notes).



©2015 Avaya Inc. All Rights Reserved.

5.2.3. System - Telephony Tab

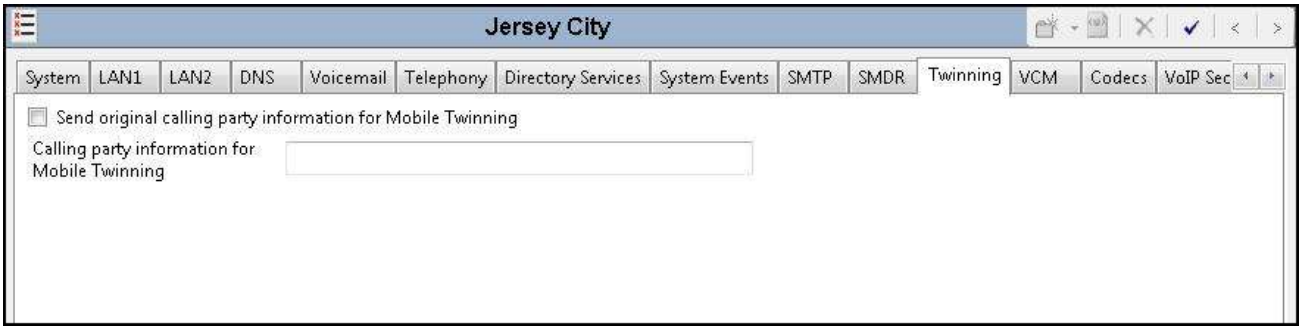
Navigate to the **Telephony → Telephony** tab in the Details Pane. Enter or select ***0*** for **Hold Timeout (secs)** so that calls on hold will not time out. Choose the **Companding Law** typical for the enterprise site. For the compliance test, ***U-LAW*** was used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the service provider per customer business policies. Note that this configuration might pose a security issue (Toll Fraud). Customers should exercise caution with this configuration.



©2015 Avaya Inc. All Rights Reserved.

5.2.4. System - Twinning Tab

To view or change the System Twinning settings, navigate to the **Twinning** tab in the Details Pane as shown in the following screen. The **Send original calling party information for Mobile Twinning** box is not checked in the sample configuration, and the **Calling party information for Mobile Twinning** is left blank.



5.2.5. System – Codecs Tab

In the **Codecs** tab of the Details Pane, select or enter ***101*** for **RFC2833 Default Payload**. This setting was preferred by IDT for use with out-band DTMF tone transmissions.

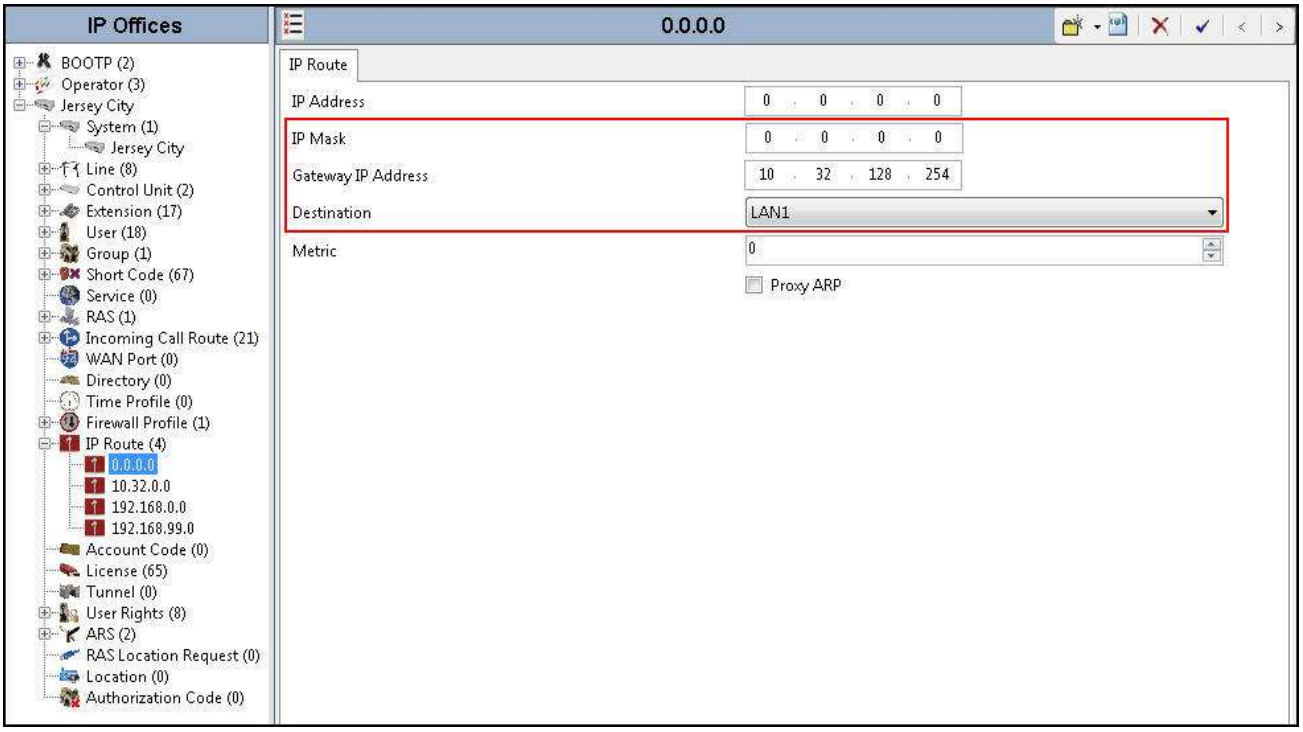
On the left, observe the list of **Available Codecs**. In the screen below, which is not intended to be prescriptive, the box next to each codec is checked, making all the codecs available in other screens where codec configuration may be performed. The **Default Codec Selection** area enables the codec preference order on a system-wide basis. By default, all IP (SIP and H.323) lines and extensions will assume the system default codec selection, unless configured otherwise for the specific line or extension.

©2015 Avaya Inc. All Rights Reserved.

5.3. IP Route

Navigate to **IP Route → 0.0.0.0** in the left Navigation Pane if a default route already exists. Otherwise, create the default route by right-clicking on **IP Route** and select **New** (not shown)**.** Create and verify a default route with the following parameters:

- Set **IP Address** and **IP Mask** to ***0.0.0.0***.
- Set **Gateway IP Address** to the IP address of the enterprise LAN gateway for the subnet where the Avaya IP Office is connected.
- Set **Destination** to ***LAN1*** from the drop-down list.



©2015 Avaya Inc. All Rights Reserved.

5.4. Administer SIP Line

A SIP Line is needed to establish the SIP trunk connection between Avaya IP Office and the IDT network. 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.

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

Some items relevant to a specific customer environment are not included in the template associated with these Application Notes, 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 SIP Line **Transport** tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated after the SIP Line is created via the template. The resulting SIP Line configuration can be verified against the manual configuration shown in **Sections 5.4.2** through **5.4.8**.

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

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

©2015 Avaya Inc. All Rights Reserved.

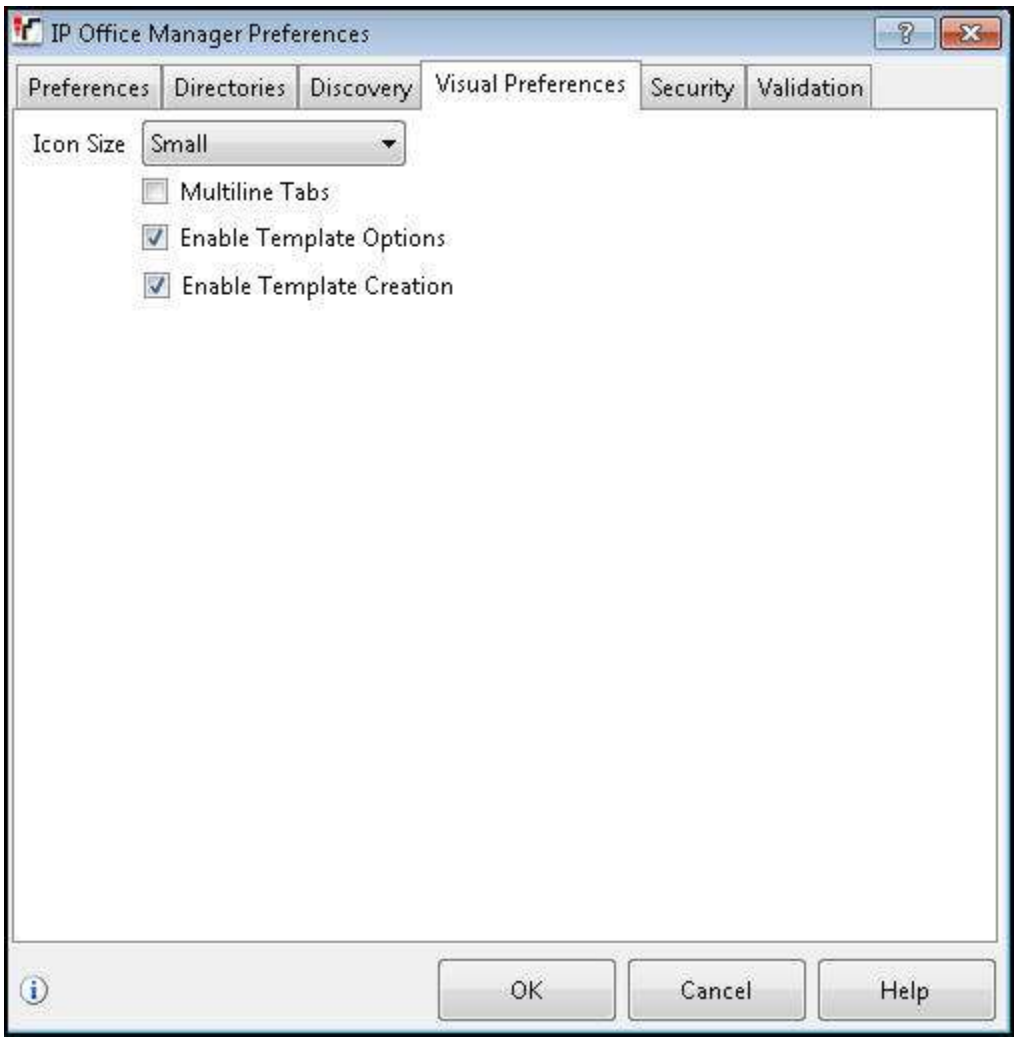
5.4.1. Create SIP Line From Template

1. Copy the template file associated with these Application Notes to a location (e.g., C:\Temp) on the computer where IP Office Manager is installed. Verify that the template file name is

   AF_IDT_SIPTrunk.xml

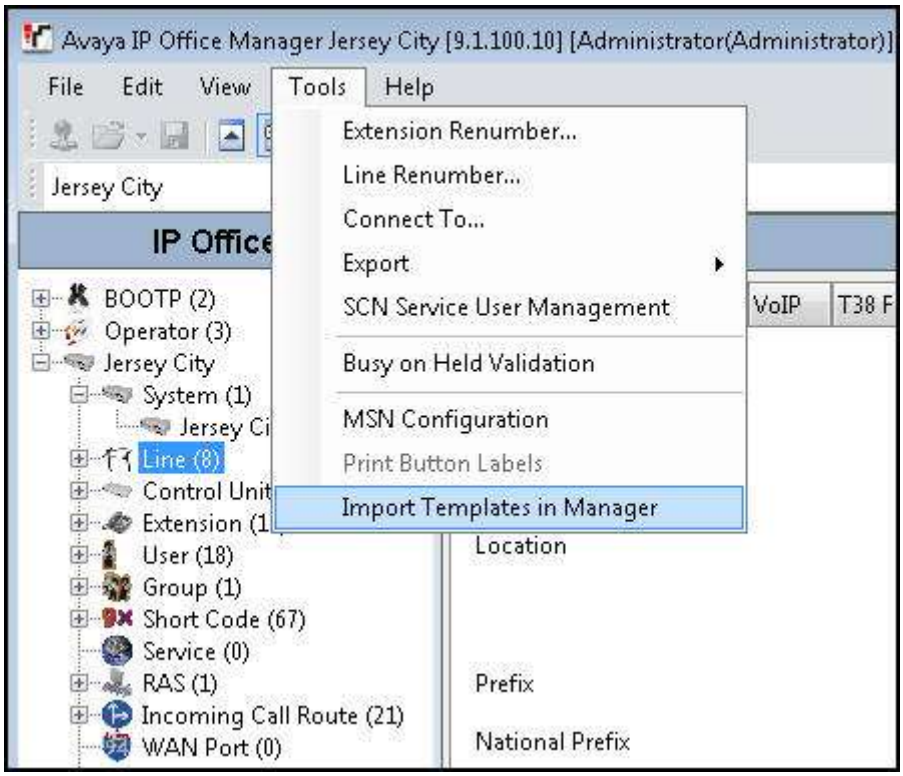
   The file name is important in locating the proper template file in **Step 4**.

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 option box is checked next to **Enable Template Options**. Click **OK**.



©2015 Avaya Inc. All Rights Reserved.

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 4**. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.

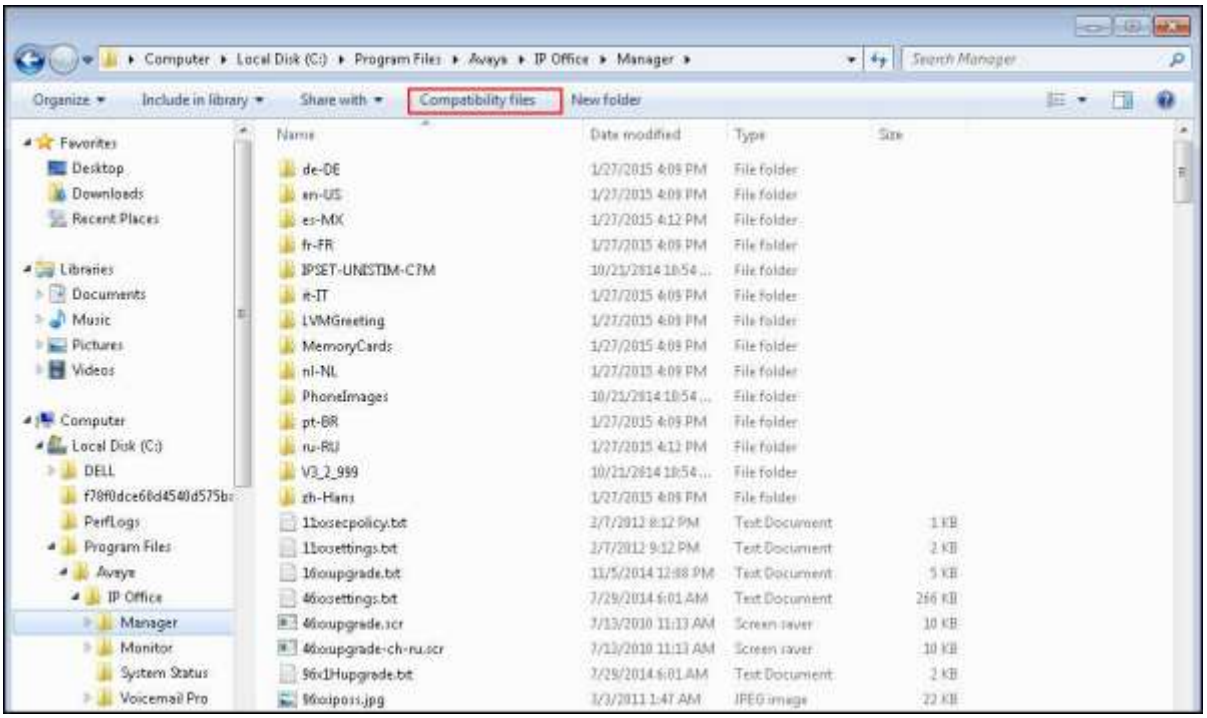


In the pop-up window that appears (not shown), select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue.

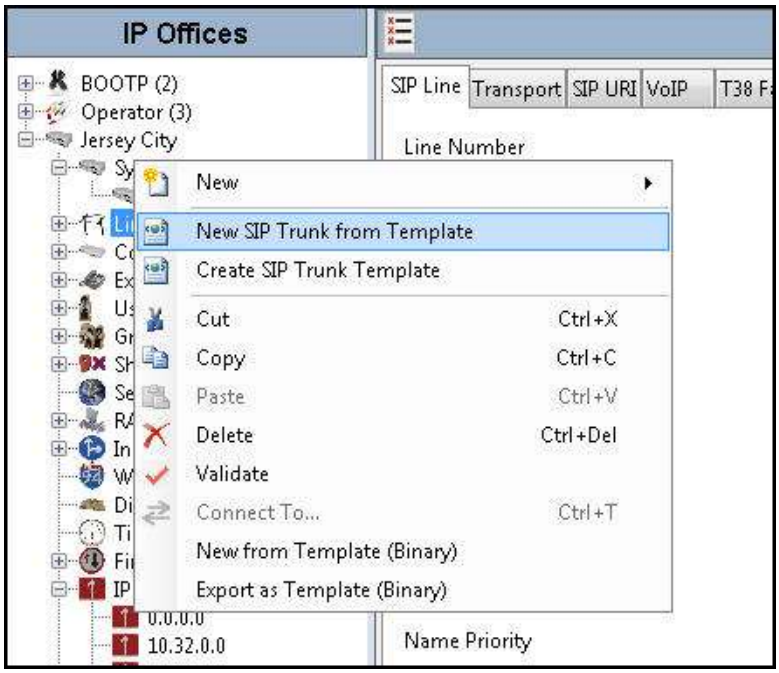
If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

©2015 Avaya Inc. All Rights Reserved.

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



4. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then select **New SIP Trunk from Template**.



©2015 Avaya Inc. All Rights Reserved.

In the subsequent **Template Type Selection** pop-up window, select ***IDT*** from the **Service Provider** drop-down list as shown below. This selection corresponds to parts of the template file name as specified in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.

Note that the newly created SIP Line may not immediately appear in the Navigation pane until the configuration was saved, closed and reopened in IP Office Manager.

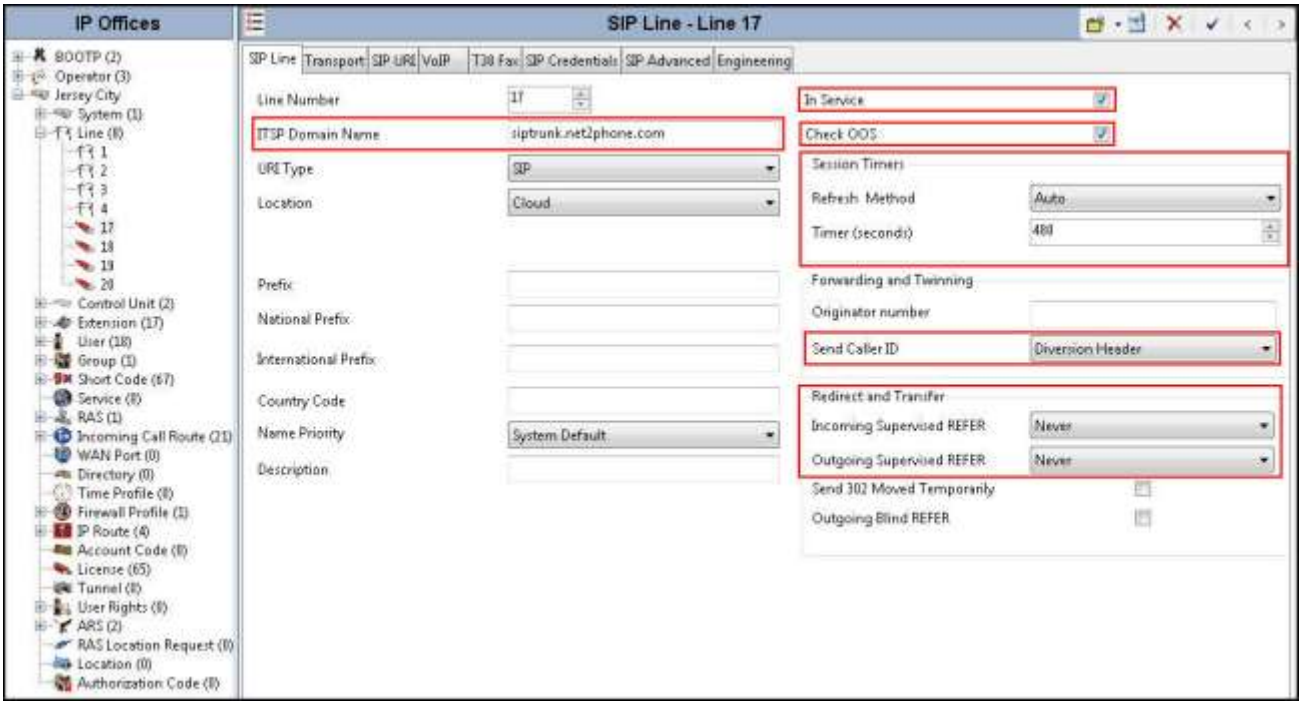
5. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2** through **5.4.8**.

©2015 Avaya Inc. All Rights Reserved.

5.4.2. SIP Line – SIP Line Tab

In the **SIP Line** tab of the Details Pane, configure the parameters as shown below:

- Set **ITSP Domain Name** to the domain name for the IDT SIP Trunking Service (provided by IDT).
- Check the **In Service** box.
- Check **OOS** box. Avaya IP Office will check the SIP OPTIONS response from the far end to determine whether to take the SIP Line out of service.
- In the **Session Timers** section, set **Method for Session Refresh** to ***Auto***. With this setting Avaya IP Office will send UPDATE messages for session refresh if the other party supports UPDATE. If UPDATE is not supported, re-INVITE messages are sent. Set **Timer (seconds)** to a desired value. Avaya IP Office will send out session refresh UPDATE or re-INVITE at the specified intervals (half of the specified value).
- Set **Send Caller ID** under **Forwarding and Twinning** to ***Diversion Header***. With this setting and the related configuration in **Section 5.2.4**, Avaya IP Office will include the Diversion Header for calls that are redirected via Mobile Twinning out the SIP Line to the PSTN. It will also include the Diversion Header for calls that are forwarded out the SIP Line.
- Under **Redirect and Transfer**, select ***Never*** for **Incoming Supervised REFER** and **Outgoing Supervised REFER**. IDT does not support use of the REFER method for off-net call transfer.

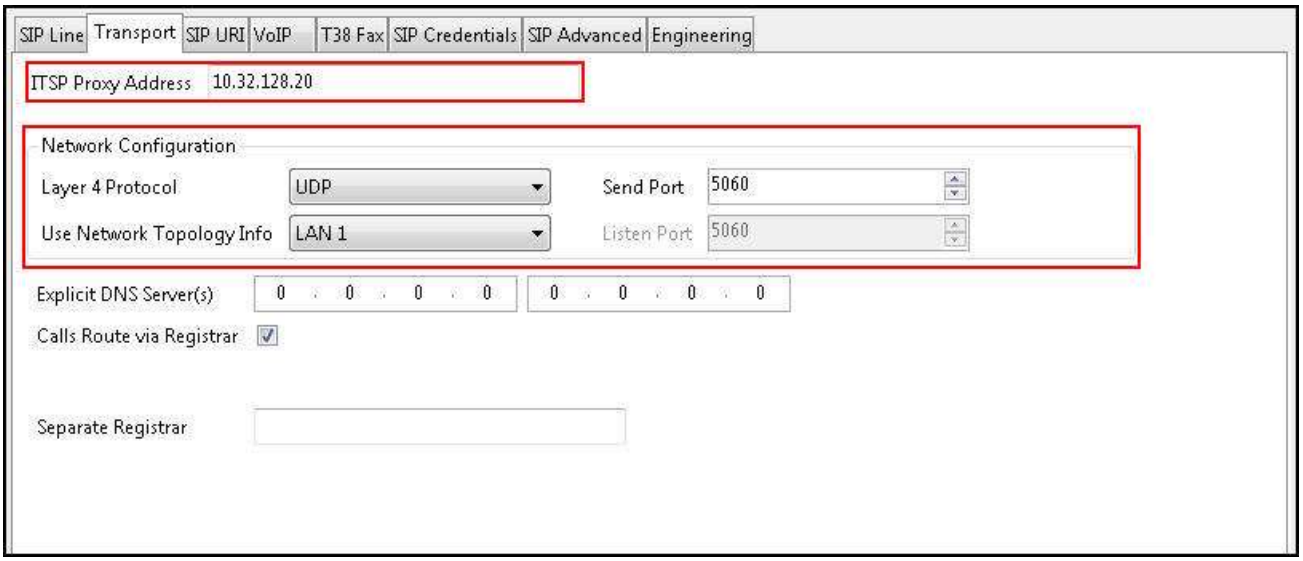


©2015 Avaya Inc. All Rights Reserved.

5.4.3. SIP Line – Transport Tab

Navigate to the **Transport** tab and set the following:

- Set the **ITSP Proxy Address** to the IP address of the internal signaling interface of the Avaya SBCE.
- Set the **Layer 4 Protocol** to ***UDP***.
- Set **Use Network Topology Info** to the network port used by the SIP line to access the far-end as configured in **Section 5.2.1**.
- Set the **Send Port** to ***5060***.



©2015 Avaya Inc. All Rights Reserved.

5.4.4. SIP Line – SIP URI Tab

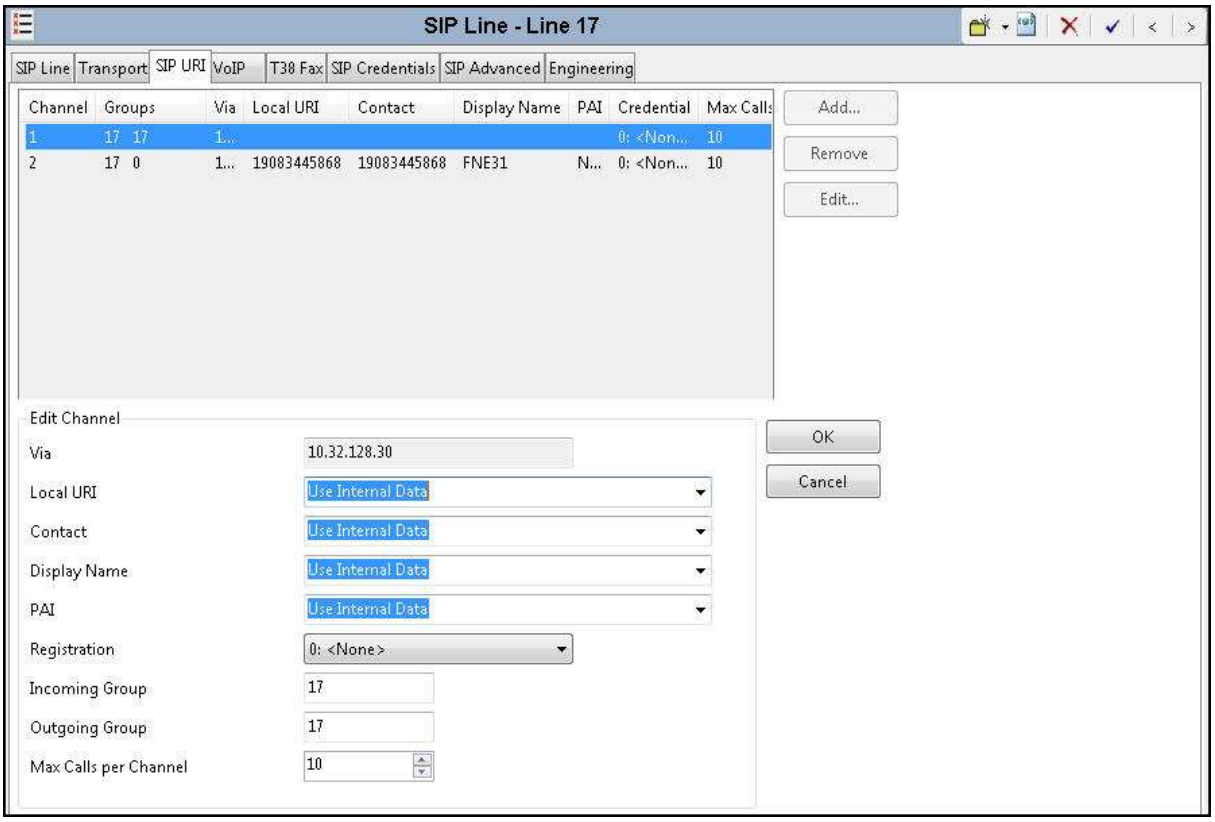
Select the **SIP URI** tab to create or edit a SIP URI entry. A SIP URI entry matches each incoming number that Avaya IP Office will accept on this line. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane.

For the compliance test, two SIP URI entries were created to match DID number assigned to

- Each Avaya IP Office user (H.323 and SIP endpoints), the fax machine (analog endpoint), as well as the Voicemail messaging application (Voicemail Pro)
- The Mobile Call Control application (see **Section 5.9**)

The screen below shows the edit window for the pre-configured SIP URI entry for matching inbound calls to Avaya IP Office users, fax endpoint, and the Voicemail messaging application.

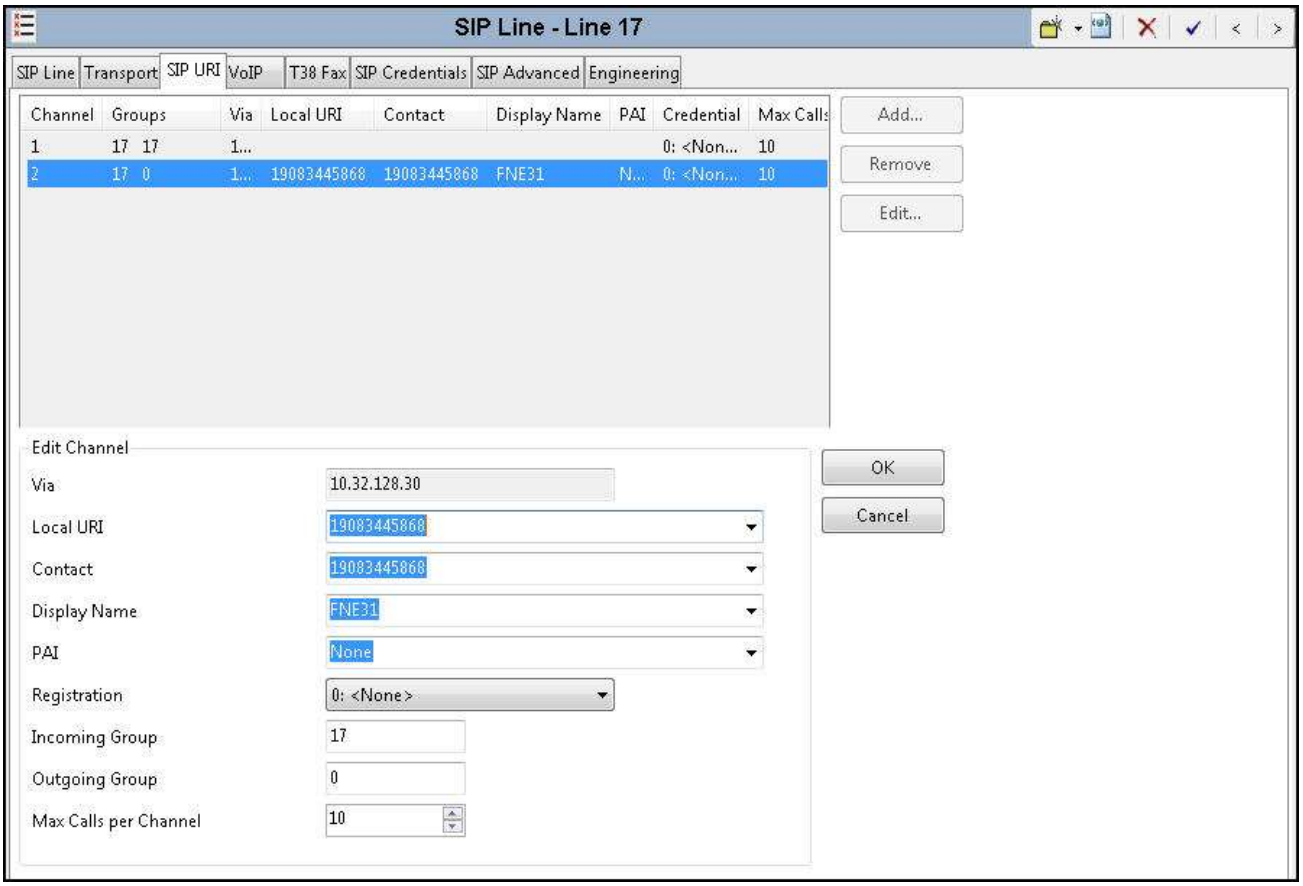
- Set **Local URI** to ***Use Internal Data***. This setting allows calls on this line whose SIP URI matches the **SIP Name** set on the **SIP** tab of any **User** as shown in **Section 5.6**, or the **SIP Name** as set in the **SIP Settings** area of the System **Voicemail** tab as shown in **Section 5.2.2**.
- Set **Contact**, **Display Name** and **PAI** to ***Use Internal Data***.
- Select ***0: <None>*** for **Registration**.
- Associate this line with an incoming line group by entering line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. For the compliance test, the incoming and outgoing group ***17*** was specified.
- Set **Max Calls per Channel** to the number of simultaneous SIP calls allowed.



©2015 Avaya Inc. All Rights Reserved.

The screen below shows the edit window for the pre-configured SIP URI entry for matching inbound calls to the Mobile Call Control application (see **Section 5.9**). This entry was necessary since the DID number assigned to the Mobile Call Control application was not configured elsewhere for matching the incoming call Request URI. Without this SIP URI entry, the Avaya IP Office would have responded to an incoming call to the DID meant for the Mobile Call Control application with a "404 Not Found" status message and the call would have failed.

The number ***19083445868*** entered for the **Local URI** field will be configured in the Incoming Call Route in **Section** Error! Reference source not found. to deliver the call to the Mobile Call Control application. Note the settings for **Contact**, **Display Name** and **PAI**, different than the settings for these same fields in the above SIP URI entry for the Avaya IP Office users. Also note the setting for **Outgoing Group**: a setting of ***0*** means no outgoing group is configured with this SIP URI entry since it is used only for mapping incoming calls to the Mobile Control Application.

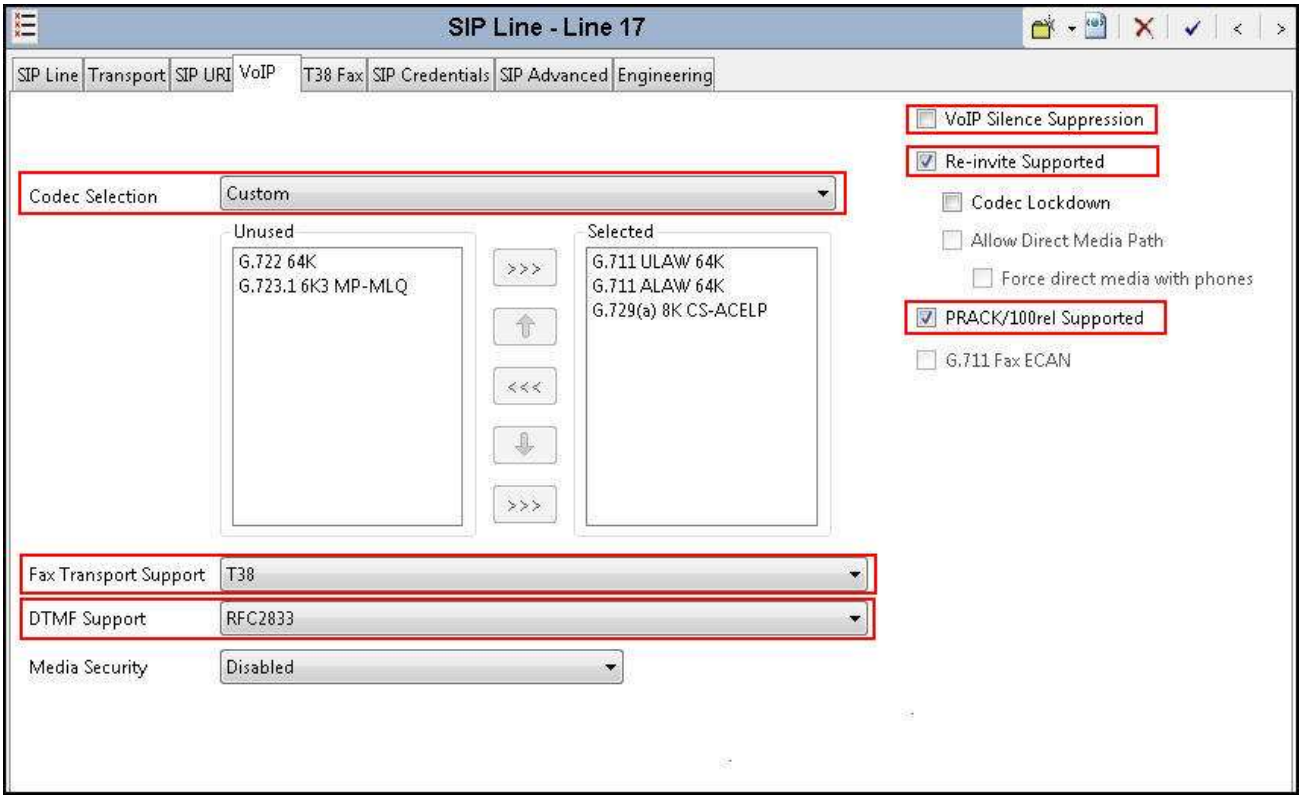


©2015 Avaya Inc. All Rights Reserved.

5.4.5. SIP Line – VoIP Tab

Select the **VoIP** tab. Set the parameters as shown below.

- Select ***Custom*** for **Codec Selection**.
- Choose ***G.711 ULAW 64K***, ***G.711ALAW 64K*** and ***G.729(a) 8K CS-ACELP*** from the **Unused** box and move the selections to the **Selected** box. Use the up and down arrows in the middle to order these 3 codes as shown. These 3 codecs are supported by IDT and the order of them matches that on inbound calls from IDT.
- Select ***T38*** for **Fax Transport Support** to direct Avaya IP Office to use T.38 for fax. See the item **T.38 Fax** in **Section 2.2** for limitations of T.38 fax on the IDT SIP Trunking Service.
- Select ***RFC2833*** for **DTMF Support**. This directs Avaya IP Office to send DTMF tones as out-band RTP events as per RFC2833.
- Uncheck the **VoIP Silence Suppression** option box.
- Check the **Re-invite Supported** option box. When enabled, re-INVITE can be used during a call session to change the characteristics of the session including codec re-negotiation.
- Check the **PRACK/100rel Supported** option box. This setting enables support by Avaya IP Office for the PRACK (Provisional Reliable Acknowledgement) message on SIP trunks.

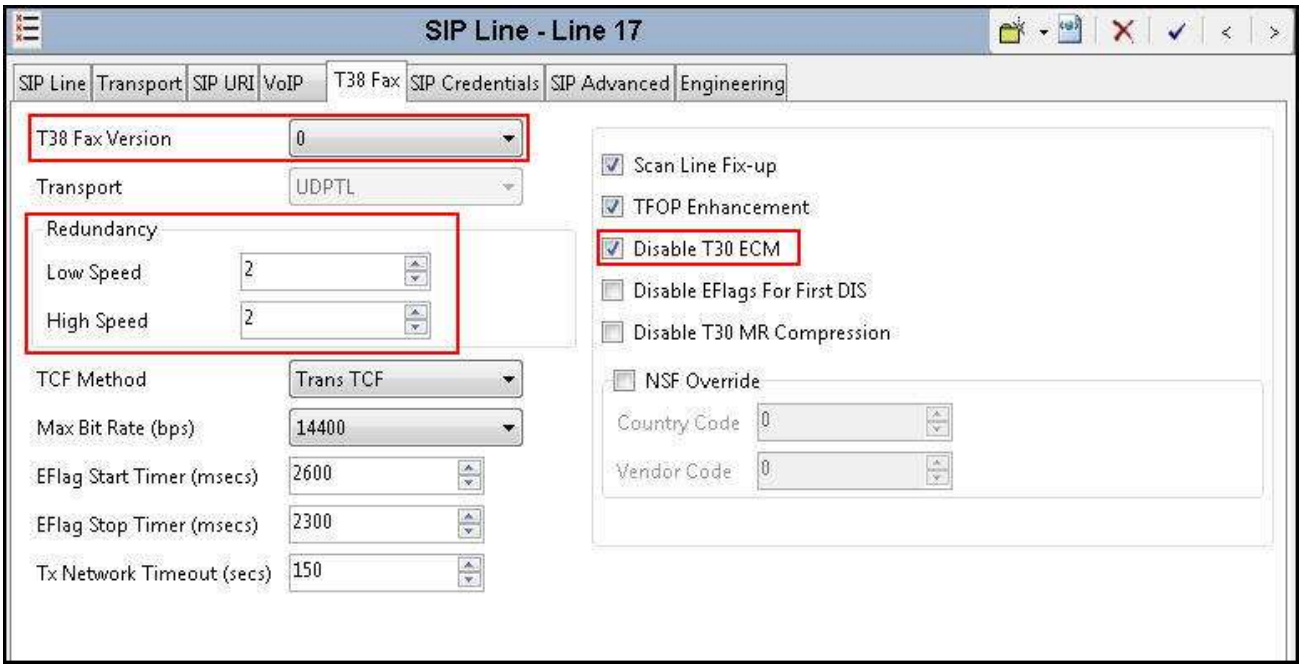


©2015 Avaya Inc. All Rights Reserved.

5.4.6. SIP Line – T38 Fax

The settings on this tab configures T.38 fax parameters and are only accessible if **Re-invite Supported** was checked and either ***T38*** or ***T38 Fallback*** was selected for **Fax Transport Support** in the **VoIP** tab in **Section 5.4.5**.

The screen below shows the settings used for the compliance test. The **T38 Fax Version** is set to ***0***. In the **Redundancy** area, **Low Speed** and **High Speed** are set to ***2***. The **Disable T30 ECM** is checked to disables the T.30 Error Correction Mode used for fax transmission. All other values are left at default.



5.4.7. SIP Line – SIP Credentials Tab

SIP Credentials are used to register the SIP Trunk with a service provider that requires SIP Registration. SIP Credentials are also used to provide the required information for Digest Authentication of outbound calls. SIP Credentials are unique per customer and therefore customers must contact the service provider to obtain the proper registration and/or Digest Authentication credentials for their deployment.

For the compliance test, the IDT SIP Trunking Service requires trunk registration as well as Digest Authentication for outbound calls.

Due to a problem on IP Office for SIP trunk registration (see the item **SIP Trunk Registration** in the limitation/exception list in **Section 2.2** for details), the SIP credentials were configured on the Avaya SBCE rather than on IP Office itself for the compliance test, therefore this tab needs not to be visited.

©2015 Avaya Inc. All Rights Reserved.

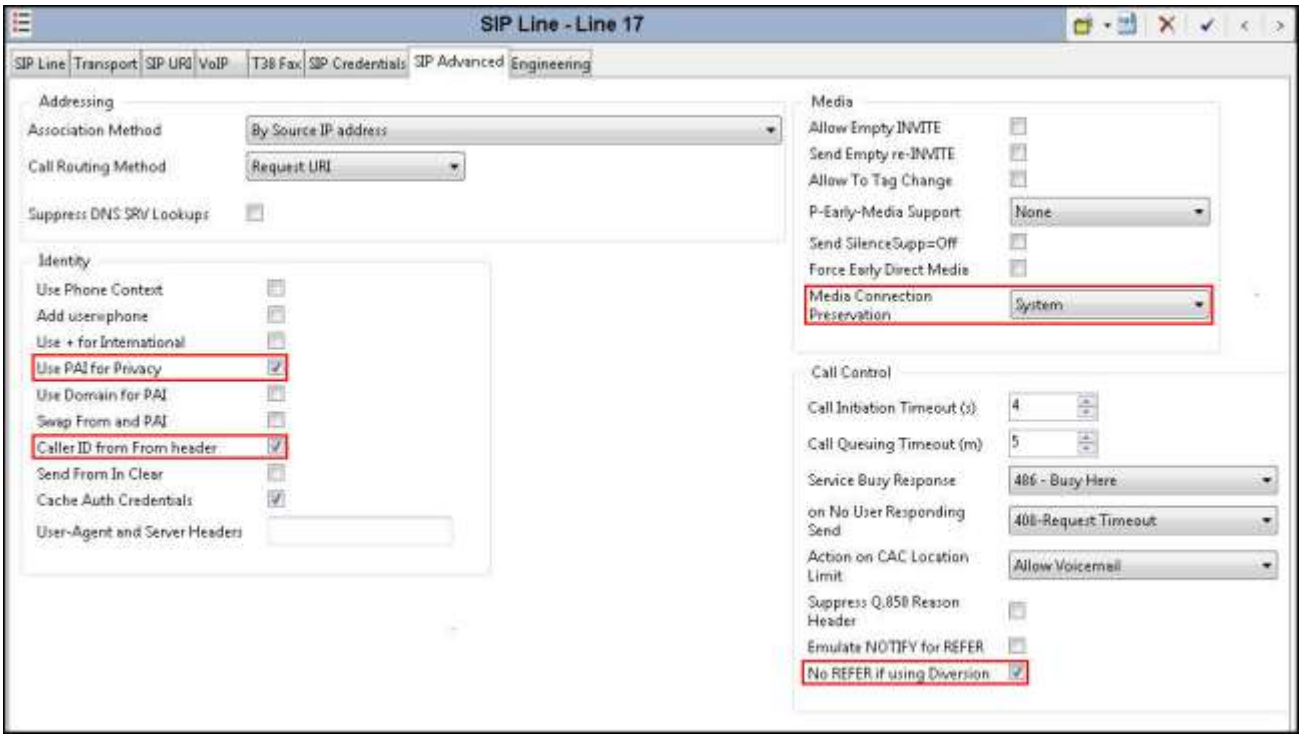
5.4.8. SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab to configure advanced SIP Line parameters.

In the **Identity** area, the **Use PAI for Privacy** box is checked for Avaya IP Office to use the P-Asserted-Identity (PAI) SIP header for privacy-requested outbound calls. With this configuration, Avaya IP Office will populate the From and Contact headers of the anonymous outbound call INVITE with "anonymous" as the URI user part, but include the normal calling user information in the PAI header. The **Caller ID from From header** box is checked for Avaya IP Office to use the Caller ID information in the From SIP header rather than the PAI or Contact SIP header for inbound calls.

In the **Media** area, select ***System*** for **Media Connection Preservation** to allow established calls to continue despite brief network failures.

In the **Call Controll** area, **No REFER if using Diversion** is checked to prevent Avaya IP Office from using the SIP REFER method on call scenarios that use the Diversion SIP header (e.g., off-net call forward or outbound call to mobile twinning number).

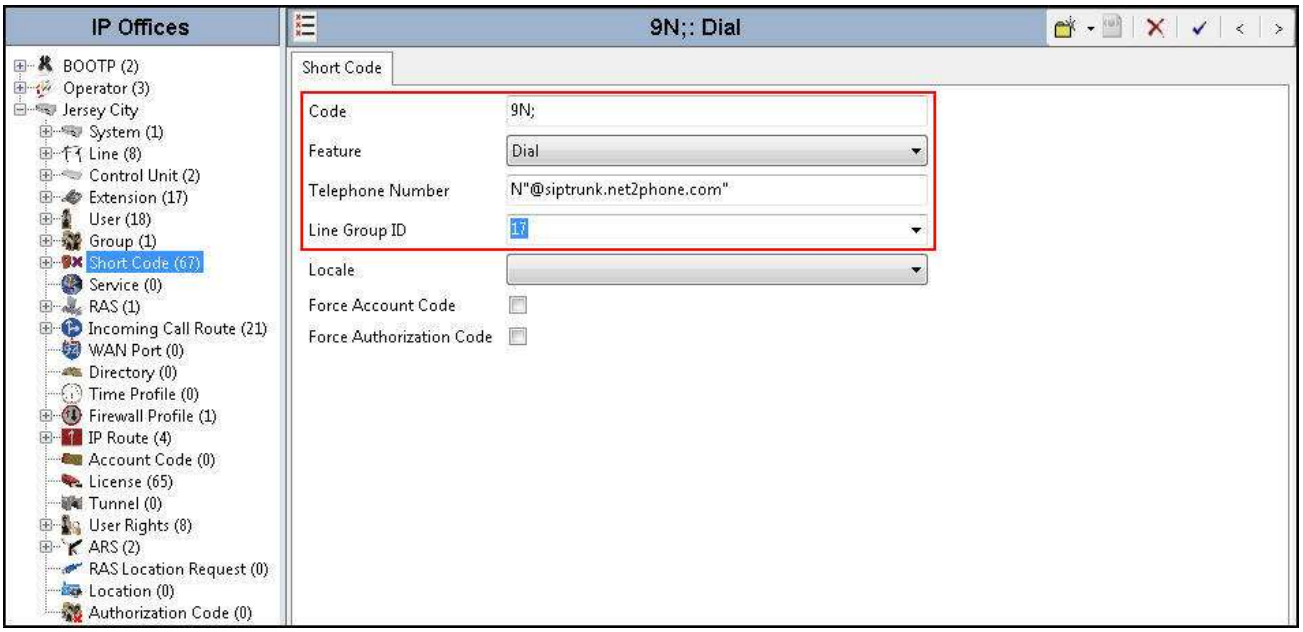


©2015 Avaya Inc. All Rights Reserved.

5.5. Short Code

Define a short code to route outbound calls to the SIP Line. To create a short code, right-click on **Short Code** in the Navigation Pane and select **New** (not shown). On the **Short Code** tab in the Details Pane, configure the parameters as shown below:

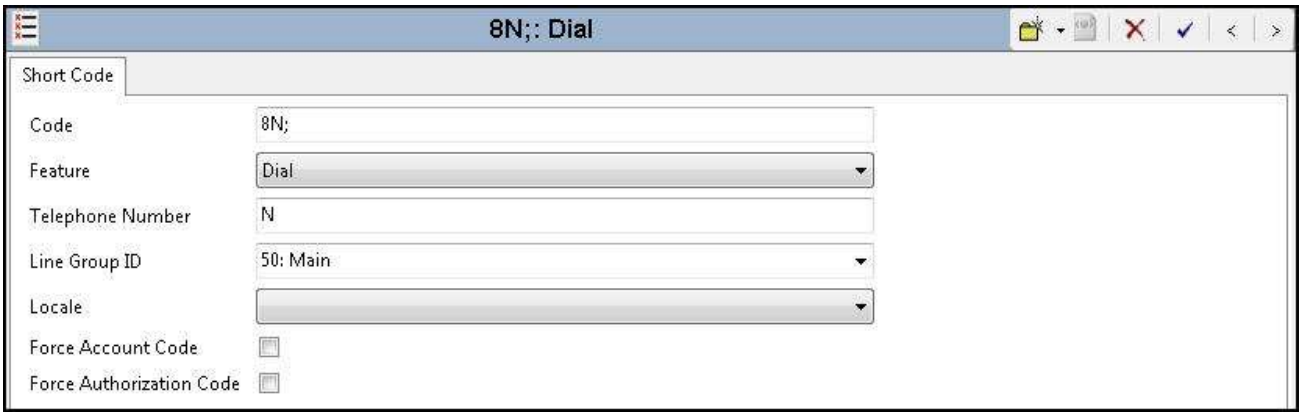
- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. The ***9N;*** short code, used for the compliance test, will be invoked when the user dials 9 followed by any number.
- Set **Feature** to ***Dial***. This is the action that the short code will perform.
- Set **Telephone Number** to ***N"@siptrunk.net2phone.com"***. This field is used to construct the Request URI and the To header in the outgoing SIP INVITE message. The value ***N*** represents the number dialed by the user. The text string following the **@** sign is the domain of the IDT SIP Trunking Service (provided by IDT).
- Set the **Line Group Id** to the **Outgoing Group** number defined on the **SIP URI** tab of the SIP Line in **Section 5.4.4**. This short code will use this line group when placing outbound calls.



The simple **9N;** short code illustrated above does not provide a means of alternate routing if the configured SIP Line is out of service or temporarily not responding. When alternate routing options and/or more customized analysis of the dialed digits following the short code are desired, the Automatic Route Selection (ARS) feature may be used.

©2015 Avaya Inc. All Rights Reserved.

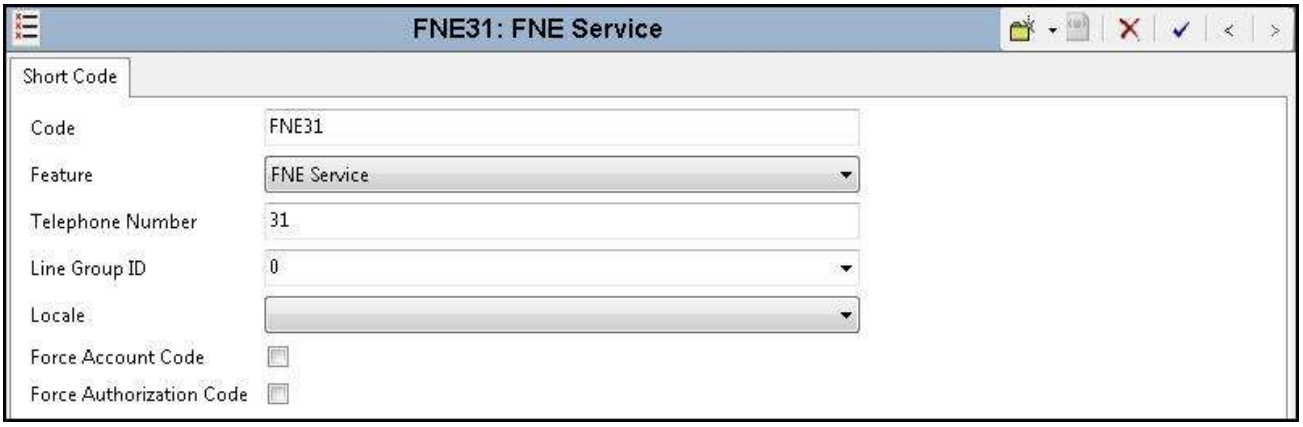
In the screen below, the short code ***8N;*** is illustrated for access to ARS. When the Avaya IP Office user dials 8 plus any number ***N***, rather than being directed to a specific **Line Group ID**, the call is directed to ***50: Main***, configurable via ARS. See **Section 5.8** for an ARS route configuration example.



Optionally, add or edit a short code used to access the SIP Line anonymously. In the screen shown below, the short code ****67N;*** is illustrated. This short code is similar to the **9N;** short code except that the **Telephone Number** field begins with the letter ***W***, which means "withhold the outgoing calling line identification". In the case of the compliance test, when a user dialed *67 plus the destination number, Avaya IP Office would include the user's telephone number (DID number assigned to the user) in the **P-Asserted-Identity** (PAI) header, populate the URI user part with "anonymous" in the From and Contact headers, and include the **Privacy: id** header in the outbound INVITE message. Consequently IDT would prevent presentation of the caller id to the called PSTN destination.

©2015 Avaya Inc. All Rights Reserved.

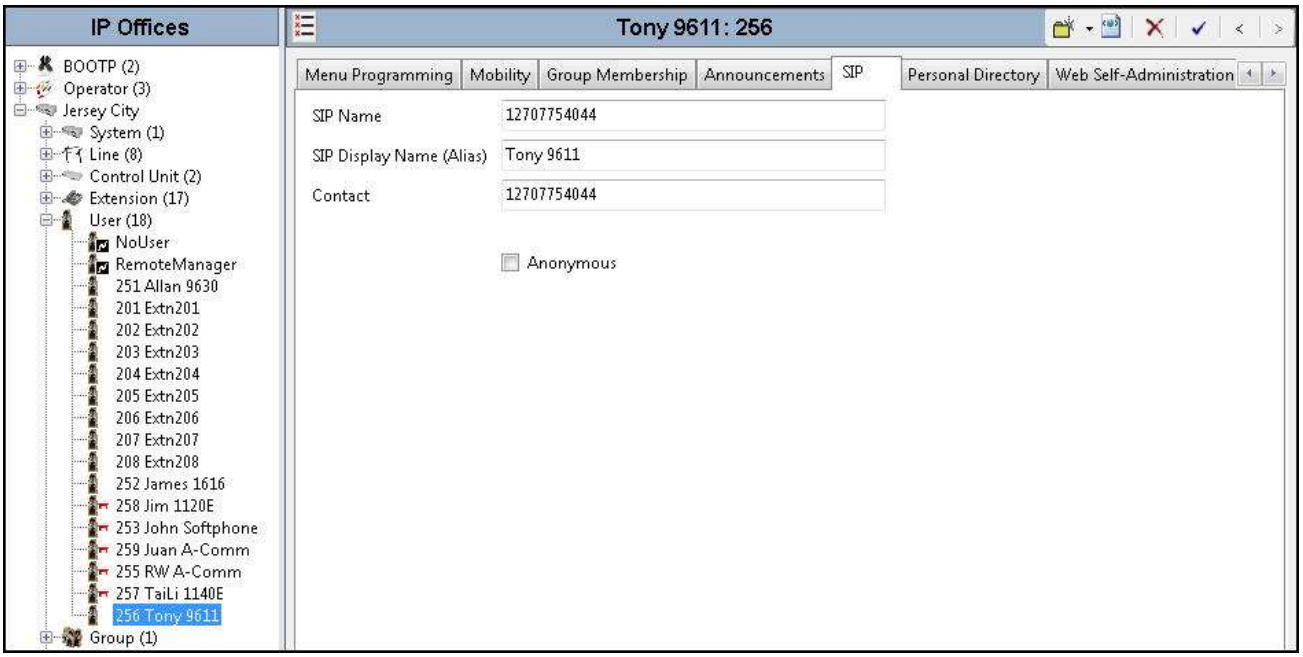
For completeness, the short code ***FNE31*** for the Mobile Call Control application is shown below. See **Section 5.7** for routing incoming call to this application to receive internal IP Office dial tones. See **Section 5.9** for configuration to enable this mobility feature.



5.6. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line. To configure these settings, first navigate to **User→Name** in the Navigation Pane, where **Name** is the name of the user to be modified. In the example shown below, the name of the user is "Tony 9611" at extension 256. Select the **SIP** tab in the Details Pane. The **SIP Name** and **Contact** are set to one of the DID numbers provided by IDT. The **SIP Display Name (Alias)** can optionally be configured with a descriptive text string.

If outbound calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user information from the network (or alternatively use the ***67N;** short code as defined in **Section 5.5**).

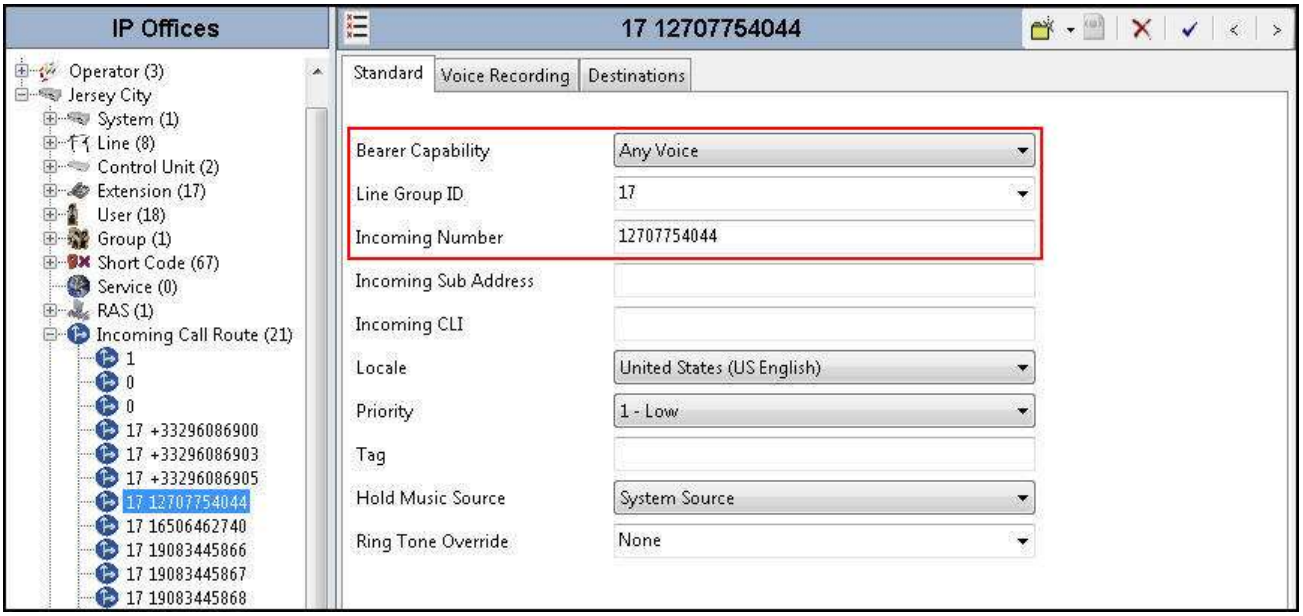


©2015 Avaya Inc. All Rights Reserved.

5.7. Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal destination. This procedure should be repeated for each DID number provided by the service provider. To create an incoming call route, right-click **Incoming Call Route** in the Navigation Pane and select **New** (not shown). On the **Standard** tab in the Details Pane, enter the parameters settings as shown below:

- Set the **Bearer Capability** to ***Any Voice***.
- Set the **Line Group Id** to the **Incoming Group** of the SIP Line defined in **Section 5.4.4**.
- Set the **Incoming Number** to the incoming DID number on which this route should match.



On the **Destinations** tab, select the destination from the pull-down list of the **Destination** field. In this example, incoming calls to 12707754044 on Incoming Group 17 are to be routed to the user "Tony 9611" at extension 256.

©2015 Avaya Inc. All Rights Reserved.

The screen below shows calls routed to the IP Office fax endpoint which is an analog extension (Extn 208).

The screen below shows calls routed to IP Office Voicemail Pro for message retrieval. Note that the DID 19083445866 was assigned to Voicemail in **Section 5.2.2**.

The following **Destinations** tab for an incoming call route contains the **Destination** "FNE31" entered manually. The name "FNE31" is the short code for accessing the Mobile Call Control application. An incoming call to 19083445868 from an IP Office user's twinned mobile phone will be delivered directly to an internal dial tone from the Avaya IP Office, allowing the caller to dial call destinations, both internal and external. See **Section 5.9** on configuration to enable the Mobile Call Control application.

©2015 Avaya Inc. All Rights Reserved.

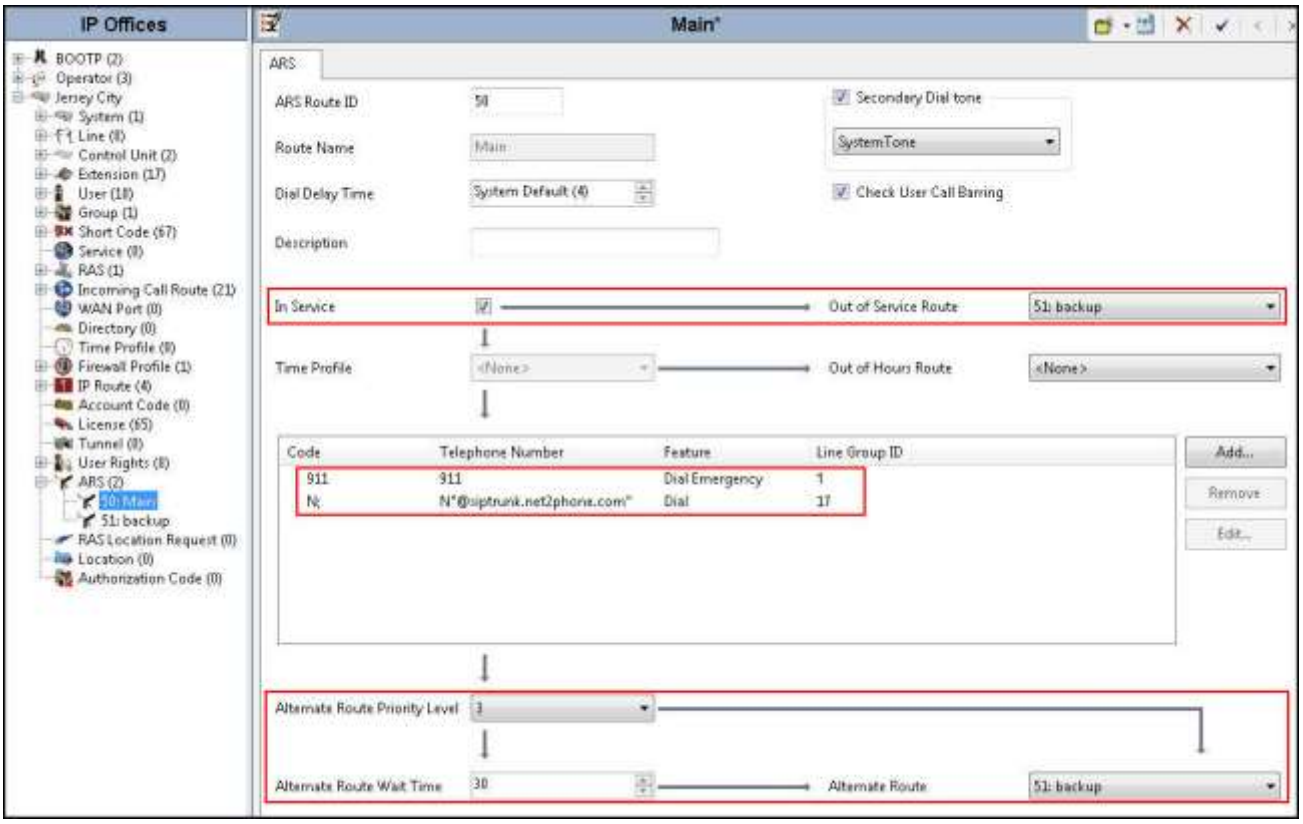
5.8. ARS and Alternate Routing

While detailed coverage of Automatic Route Selection (ARS) is beyond the scope of these Application Notes, this section includes basic ARS screen illustration and considerations.

Optionally, ARS can be used to supplement or replace the simple **9N;** short code approach documented in **Section 5.5**. With ARS, secondary dial tone can be provided after the access code, time-based routing criteria can be introduced, and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. ARS also facilitates more specific dialed telephone number matching, enabling immediate routing and alternate treatment for different types of numbers following the access code. For example, if all local and long distance calls should use the SIP Line, but service numbers should prefer a different outgoing line group, ARS can be used to distinguish between the two call patterns.

To add a new ARS route, right-click **ARS** in the Navigation Pane and select **New** (not shown). To view or edit an existing ARS route, expand ARS in the Navigation Pane and select a route name.

The following screen shows a sample ARS configuration for the route named ***50: Main***. The **In Service** parameter refers to the ARS form itself, not the Line Groups that may be referenced in the form. If the **In Service** box is un-checked, calls are routed to the ARS route name specified in the **Out of Service Route** parameter. IP Office short codes may also be defined to allow an ARS route to be disabled or enabled from a telephone. The configurable provisioning of an Out of Service Route and the means to manually activate the Out of Service Route can be helpful for scheduled maintenance or other known service-affecting events for the primary route.



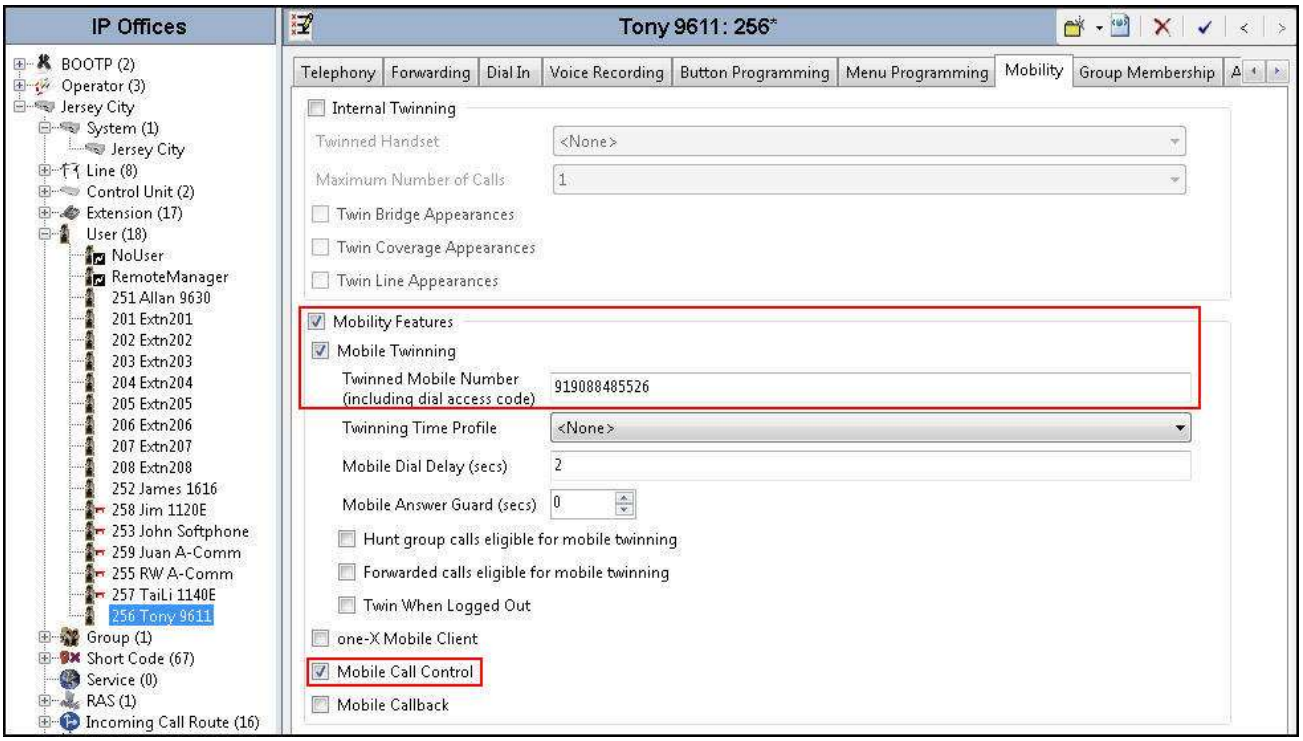
©2015 Avaya Inc. All Rights Reserved.

Assuming the primary route is in-service, the number passed from the short code used to access ARS (e.g., **8N;** in **Section 5.5**) can be further analyzed to direct the call to a specific Line Group ID. Per the example screen above, if the user dialed 8 plus any number, the processing for the short code **8N;** would direct the call via ARS to Line Group 17. A short code **911** can be configured to send the emergency call out using Line Group 1 when the user dials "911". If the primary route cannot be used, the call can automatically route to the route name specified in the **Alternate Route** field in the lower right of the screen (***51: Backup***). Since alternate routing is considered a privilege not available to all callers, IP Office can control access to the alternate route by comparing the calling user's priority, configured in the **User** tab of individual users, to the value in the **Alternate Route Priority Level** field.

5.9. Mobility

With Mobility configured for an Avaya IP Office user, an inbound call routed to this user automatically triggers an outbound call to the configured Mobile Twinning number for this user.

The following screen shows the **Mobility** tab for User "Tony 9611" at extension 256. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number for the twinned mobile telephone including the dial access code (short code), in this case ***919088485526*** (short code 9 plus the ensuing twinned mobile number). The **Mobile Call Control** option box is also checked so that an inbound call from the twinned mobile number (9088485526 in this example) to the Mobile Call Control application (see Incoming Call Route to "FNE31" in **Section 5.7**) will be delivered directly to an internal dial tone from the Avaya IP Office, allowing the caller to perform further dialing actions including making calls and activating Short Codes. Other options can be set according to customer requirements.



©2015 Avaya Inc. All Rights Reserved.

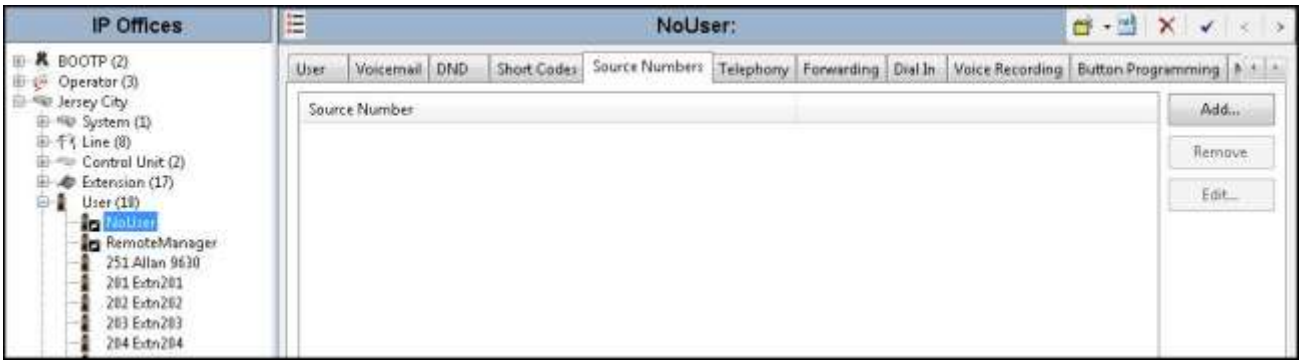
Note that when an inbound call is from the twinned mobile number to the Mobile Call Control application, the caller ID contained in the From header of the incoming INVITE must match the twinned mobile number (without the leading short code digit), otherwise the Avaya IP Office responds with a "486 Busy Here" message and the caller will hear busy tones (or be re-directed to a network-based messaging service as with the IDT test circuit used for the compliance test).

5.10. SIP Options

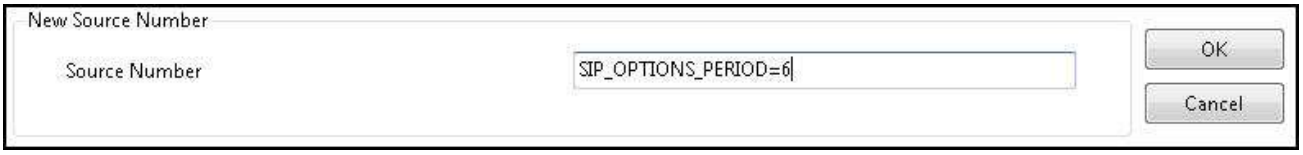
Avaya IP Office sends SIP OPTIONS messages periodically to determine if the SIP connection is active. By default, Avaya IP Office Release 9.1 sends out OPTIONS every 300 seconds. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time** (in seconds) set on the **Network Topology** tab in **Section 5.2.1** 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:

- To use the default value, set **Binding Refresh Time** to 300. OPTIONS will be sent at the 300 second frequency.
- To establish a period of less than 300 seconds, do not define the **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** setting.
- 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** settings.

To configure the **SIP_OPTIONS_PERIOD** parameter, navigate to **User → NoUser** in the Navigation Pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.

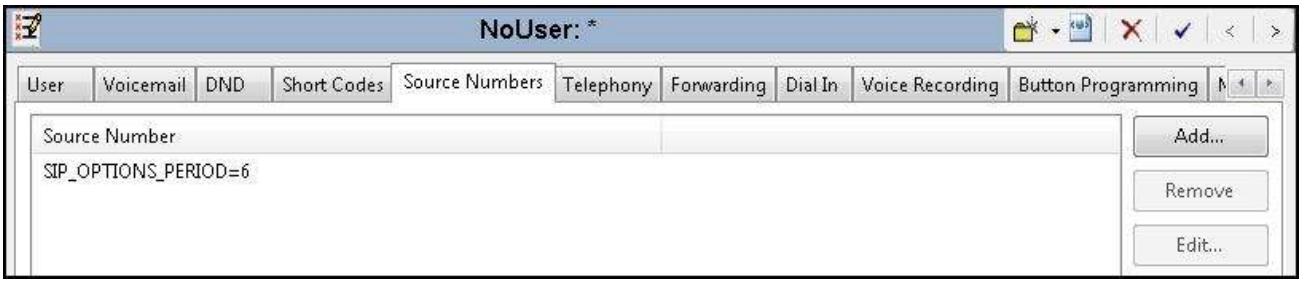


At the bottom of the Details Pane, the **Source Number** field will appear. Enter ***SIP_OPTIONS_PERIOD=X***, where ***X*** is the desired value in minutes. Click **OK**.



©2015 Avaya Inc. All Rights Reserved.

The **SIP_OPTIONS_PERIOD** parameter will appear in the list of Source Numbers as shown below. Click **OK** at the bottom of the screen (not shown).

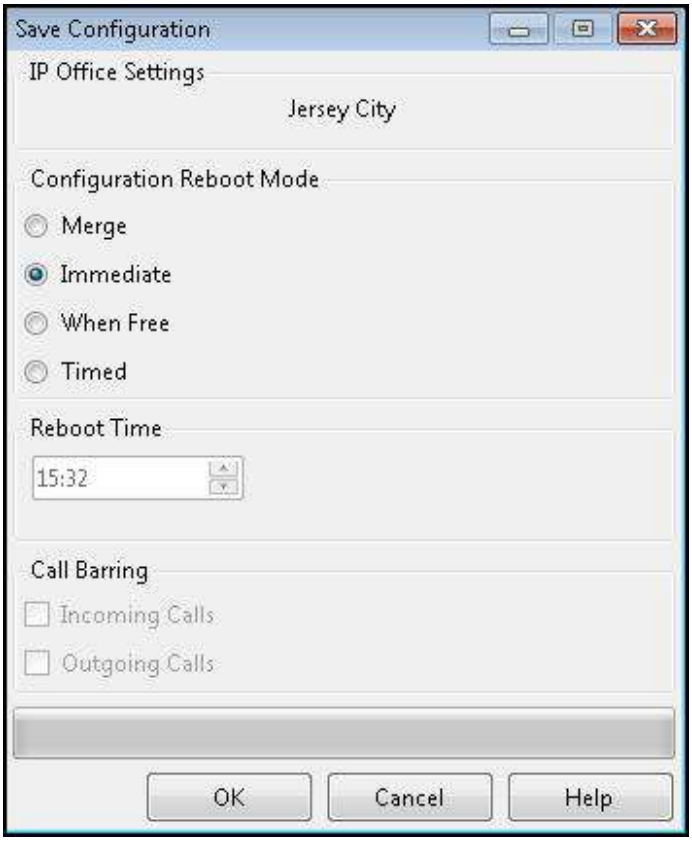


For the compliance test, an OPTIONS period of 2 minutes was desired. The **Binding Refresh Time** was set to ***120*** seconds in **Section 5.2.1**. Thus, there was no need to define **SIP_OPTIONS_PERIOD**.

5.11. Save Configuration

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

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



©2015 Avaya Inc. All Rights Reserved.

6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed, including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (i.e., A1 and B1). If the management interface has not been configured on a separate subnet, then contact your Avaya representative for guidance in correcting the configuration.

On all screens described in this section, it is to be assumed that parameters are left at their default values unless specified otherwise.

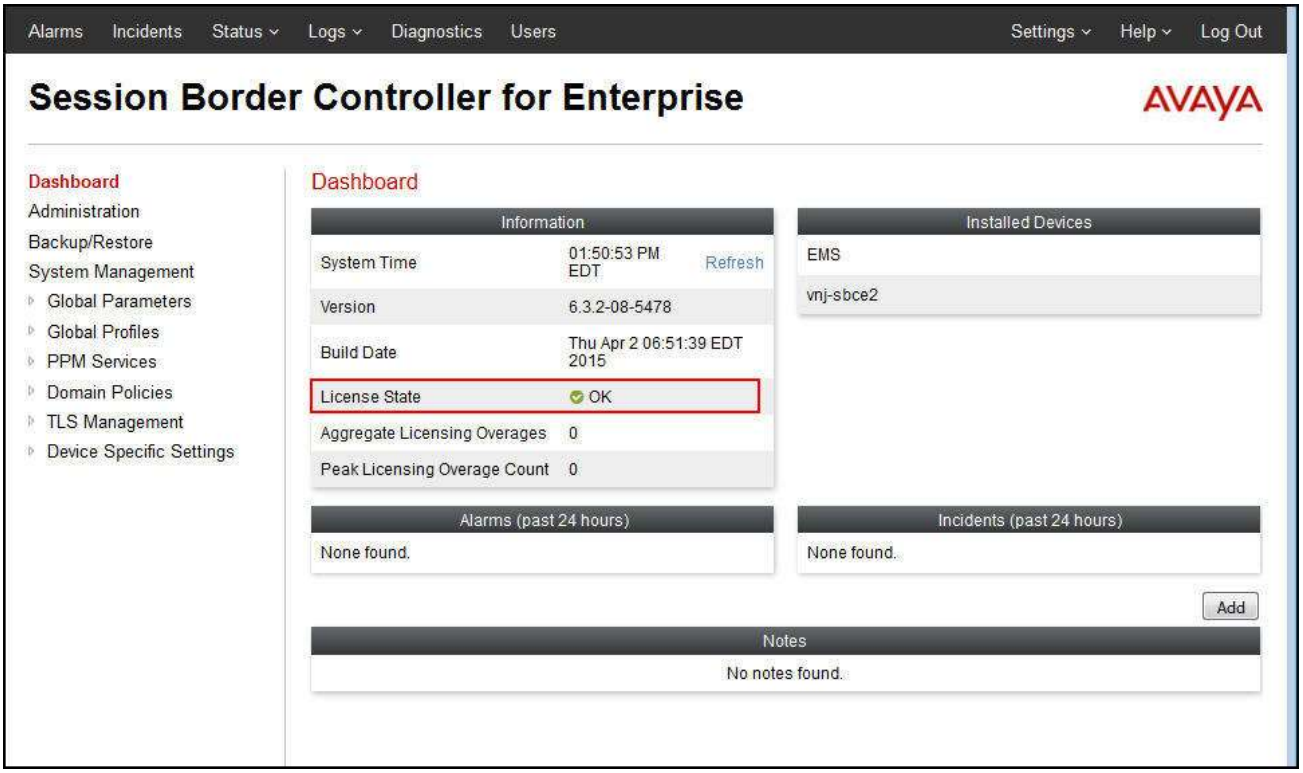
6.1. Access Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The Avaya SBCE login page will appear as shown below. Log in with the appropriate credentials.

©2015 Avaya Inc. All Rights Reserved.

After logging in, the Dashboard screen will appear as shown below. Verify that **License State** is **OK** as highlighted. The Avaya SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license if necessary.

All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

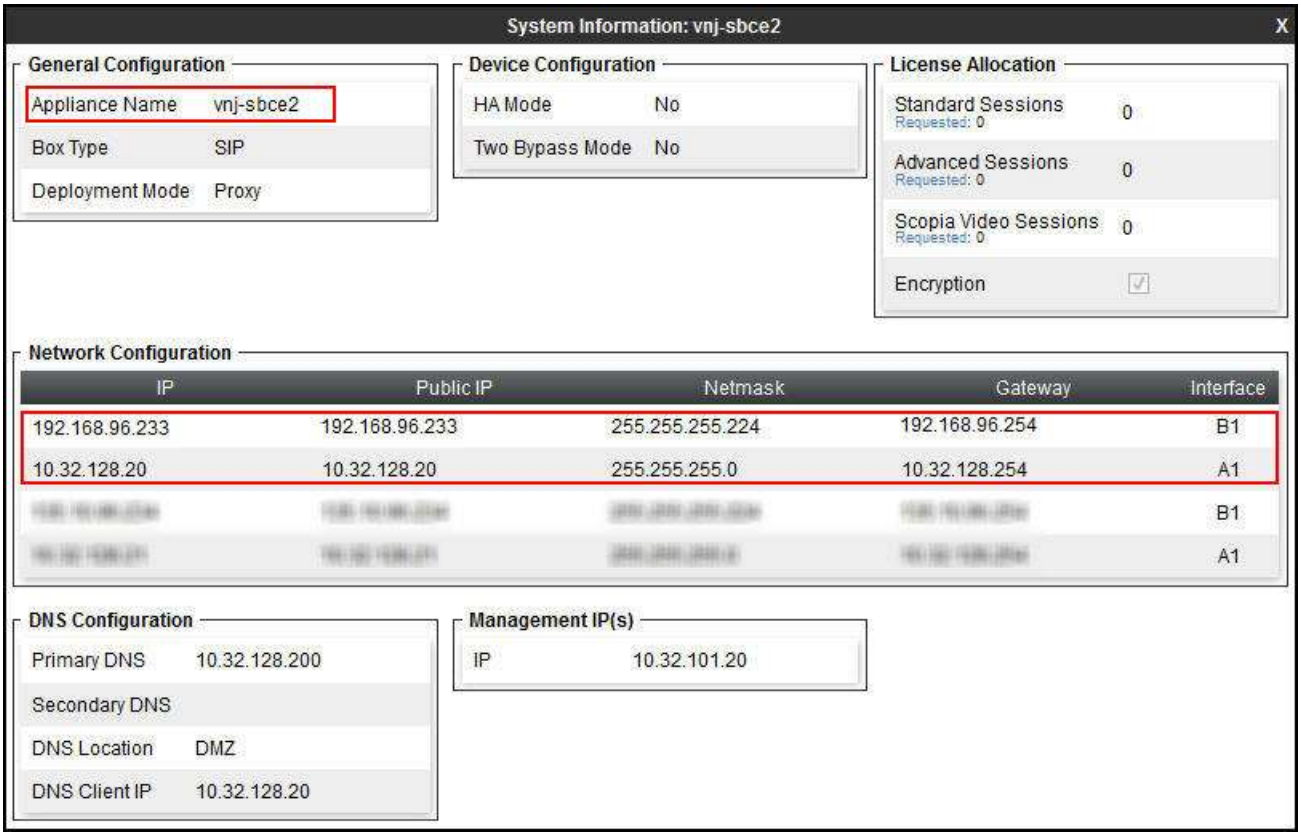


©2015 Avaya Inc. All Rights Reserved.

6.2. Verify Network Configuration and Enable Interfaces

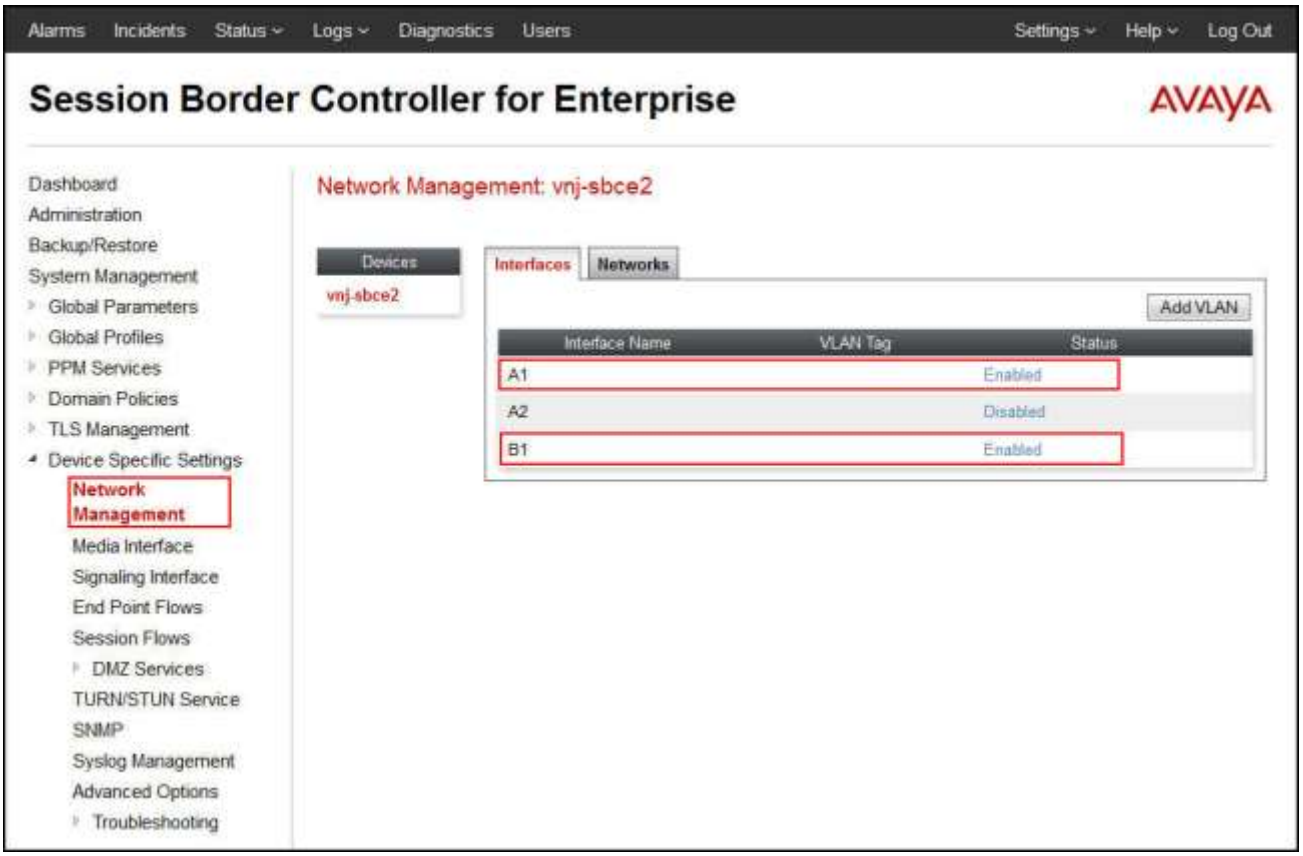
To view the network information provided during installation, navigate to **System Management**. In the right pane, click **View** as highlighted below.

A System Information page will appear showing the information provided during installation. The **Appliance Name** field is the name of the device (***vnj-sbce2***). This name will be referenced in other configuration screens. Interfaces **A1** and **B1** represent the private (or internal) and public (or external) interfaces of the Avaya SBCE. Each of these interfaces must be enabled after installation. Note that the **Management IP** is on a different subnet than either the A1 or B1 interfaces.



©2015 Avaya Inc. All Rights Reserved.

To enable the interfaces, first navigate to **Device Specific Settings → Network Management** in the left pane and select the device being managed in the center pane. In the right pane, in the **Interfaces** tab verify that **Status** is ***Enabled*** for both the **A1** and **B1** interfaces. If not, click on ***Disabled*** and confirm in the pop-up confirmation window to toggle to ***Enabled***.



©2015 Avaya Inc. All Rights Reserved.

6.3. Signaling Interface

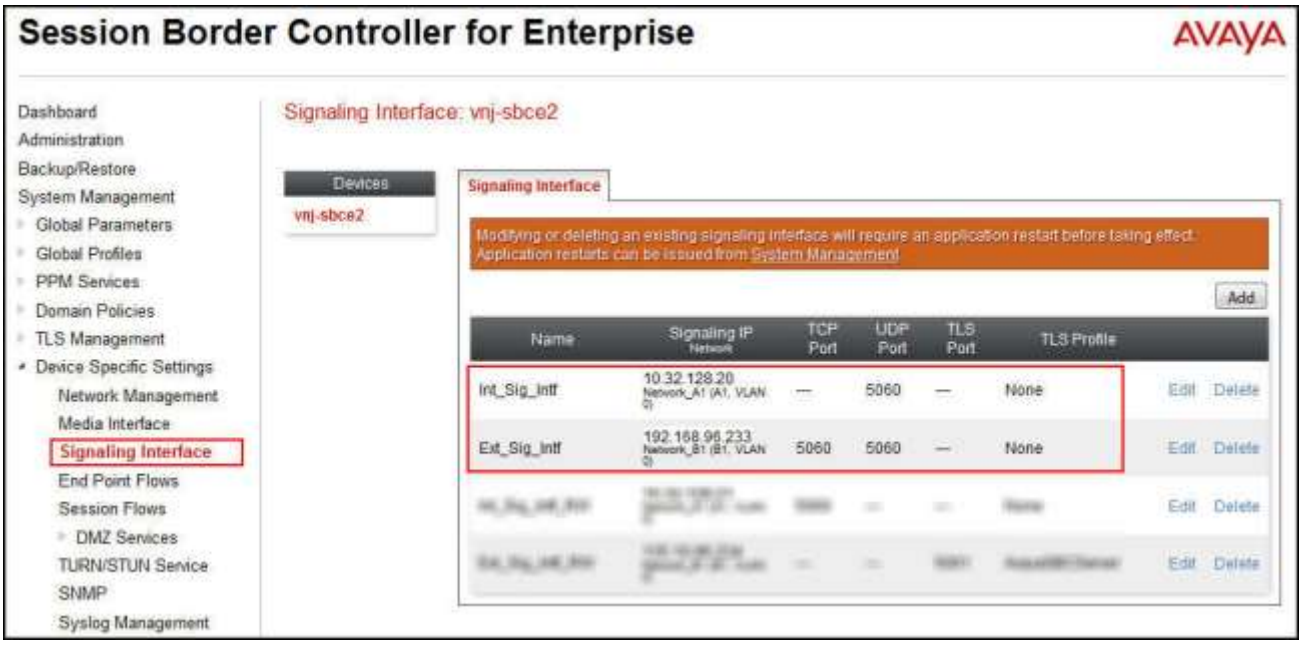
A signaling interface defines an IP address, transport protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear for configuring the name of the new interface as well as the interface parameters. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int_Sig_Intf** was created for the Avaya SBCE internal interface and signaling interface **Ext_Sig_Intf** was created for the Avaya SBCE external interface. These two signaling interfaces are highlighted below.

In the pop-up interface configuration window (not shown), configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the **IP Address** field, select the A1 interface and the IP address associated with the private interface (A1) shown in **Section 6.2**. For the external signaling interface, select the B1 interface and the IP address associated with the public interface (B1) shown in **Section 6.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port the Avaya SBCE will listen on for each transport protocol. For the internal interface, the Avaya SBCE was configured to listen for UDP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port 5060. Since the IDT SIP Trunking Services uses UDP, it would have been sufficient to simply configure the Avaya SBCE for UDP.



©2015 Avaya Inc. All Rights Reserved.

6.4. Media Interface

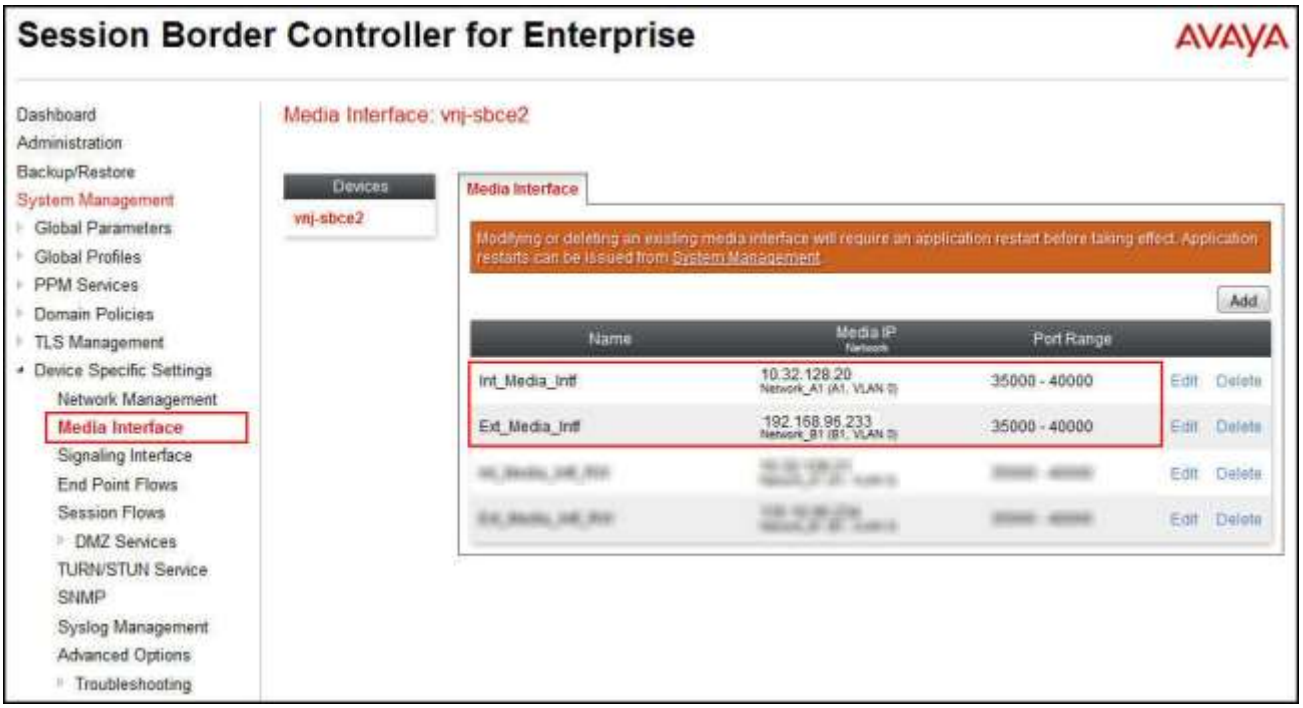
A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear for configuring the name of the new interface as well as the interface parameters. Once complete, the settings are shown in the far right pane.

For the compliance test, media interface **Int_Media_Intf** was created for the Avaya SBCE internal interface and media interface **Ext_Media_Intf** was created for the Avaya SBCE external interface. Both are highlighted below.

In the pop-up interface configuration window (not shown), configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the **IP Address** field, select the A1 interface and the IP address associated with the private interface (A1) shown in **Section 6.2**. For the external media interface, select the B1 interface and the IP address associated with the public interface (B1) shown in **Section 6.2**.
- Set **Port Range** to a range of ports acceptable to both the enterprise and the far end. For the compliance test, the default port range was used for both interfaces.



©2015 Avaya Inc. All Rights Reserved.

6.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create one server interworking profile for Avaya IP Office and another for the service provider SIP server. These profiles will be applied to the appropriate servers in **Section 6.6.1** and **6.6.2**.

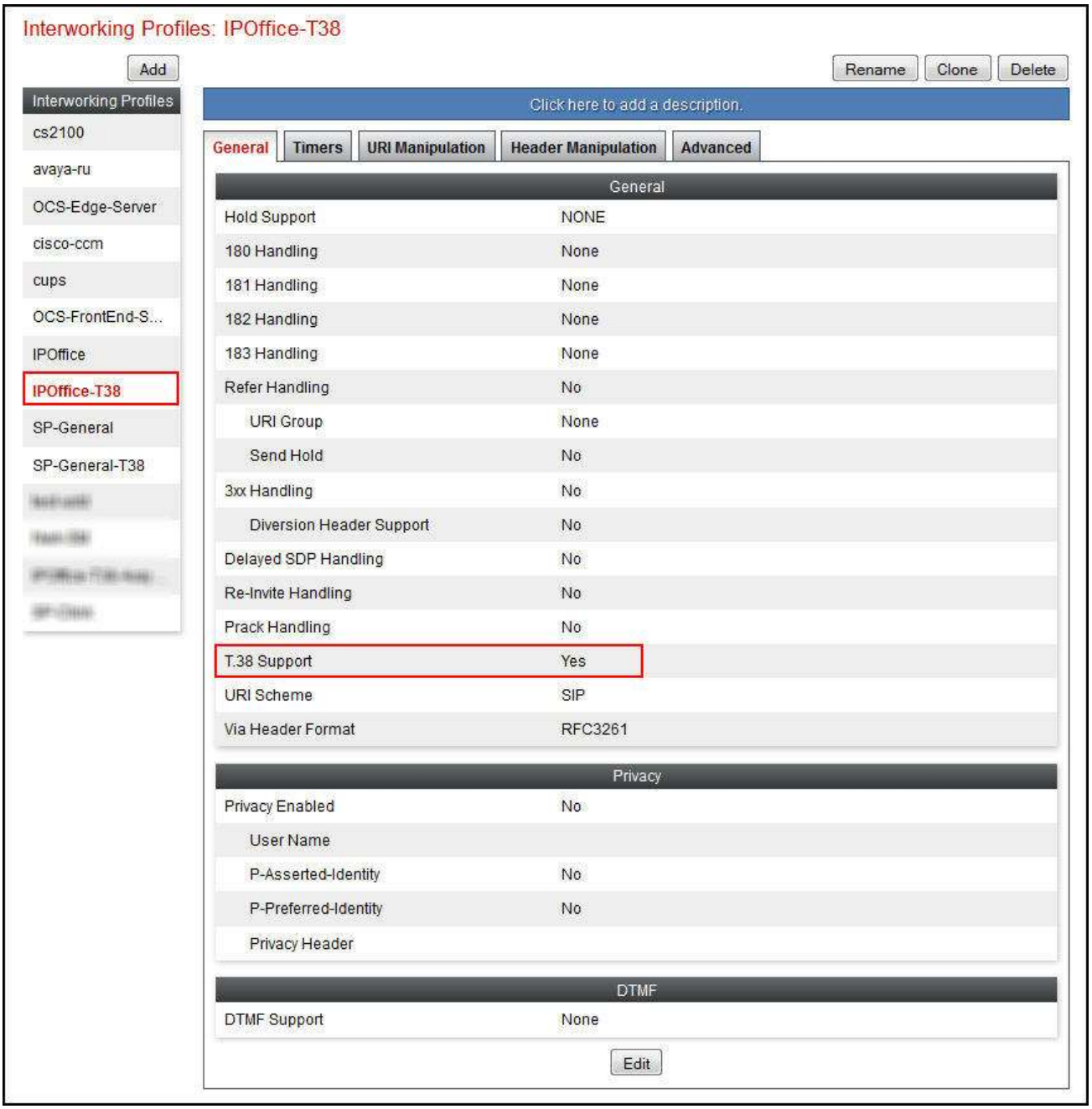
To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the user interface as described above, before creating the specific server interworking profiles used for the compliance test.

©2015 Avaya Inc. All Rights Reserved.

6.5.1. Server Interworking – Avaya IP Office

For the compliance test, the server interworking profile ***IPOffice-T38*** was created for Avaya IP Office. The **General** tab parameters are shown below. Note the setting for **T.38 Support**.



The **Timers**, **URI Manipulation** and **Header Manipulation** tabs have no configured entries.

©2015 Avaya Inc. All Rights Reserved.

The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to ***Yes***.

General | Timers | URI Manipulation | Header Manipulation | Advanced

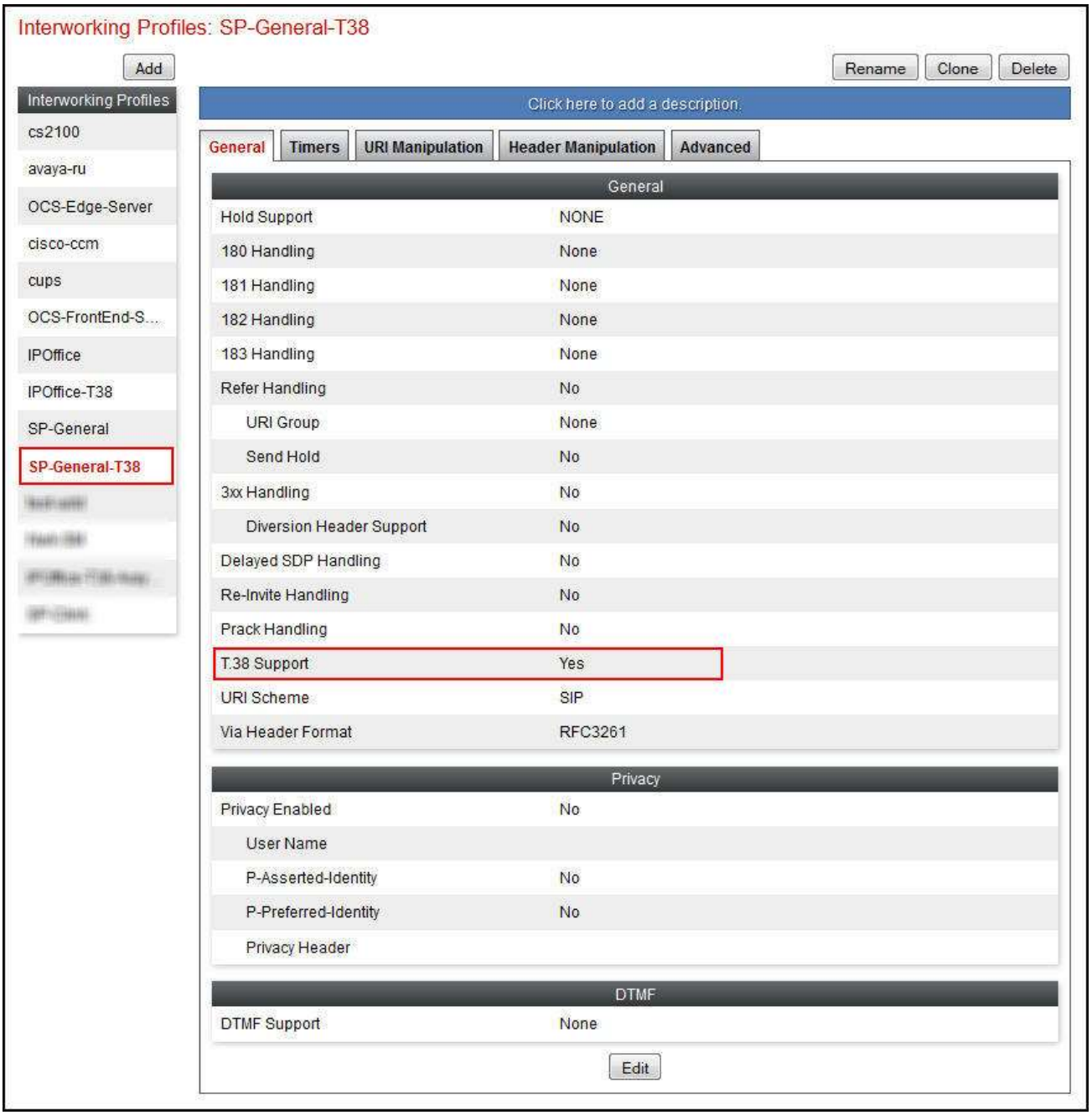
Record Routes	Both Sides
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	Yes
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on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

Edit

©2015 Avaya Inc. All Rights Reserved.

6.5.2. Server Interworking – IDT

For the compliance test, server interworking profile ***SP-General-T38*** was created for the IDT SIP server. The **General** tab parameters are shown below. Note the setting for **T.38 Support**.



The **Timers**, **URI Manipulation**, **Header Manipulation** tabs have no entries.

©2015 Avaya Inc. All Rights Reserved.

The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to ***No***.

General | Timers | URI Manipulation | Header Manipulation | Advanced

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

Edit

©2015 Avaya Inc. All Rights Reserved.

6.6. Server Configuration

A server configuration profile defines the attributes of the physical server. Create separate server configuration profiles for Avaya IP Office and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before the servers profiles were added for the compliance test.

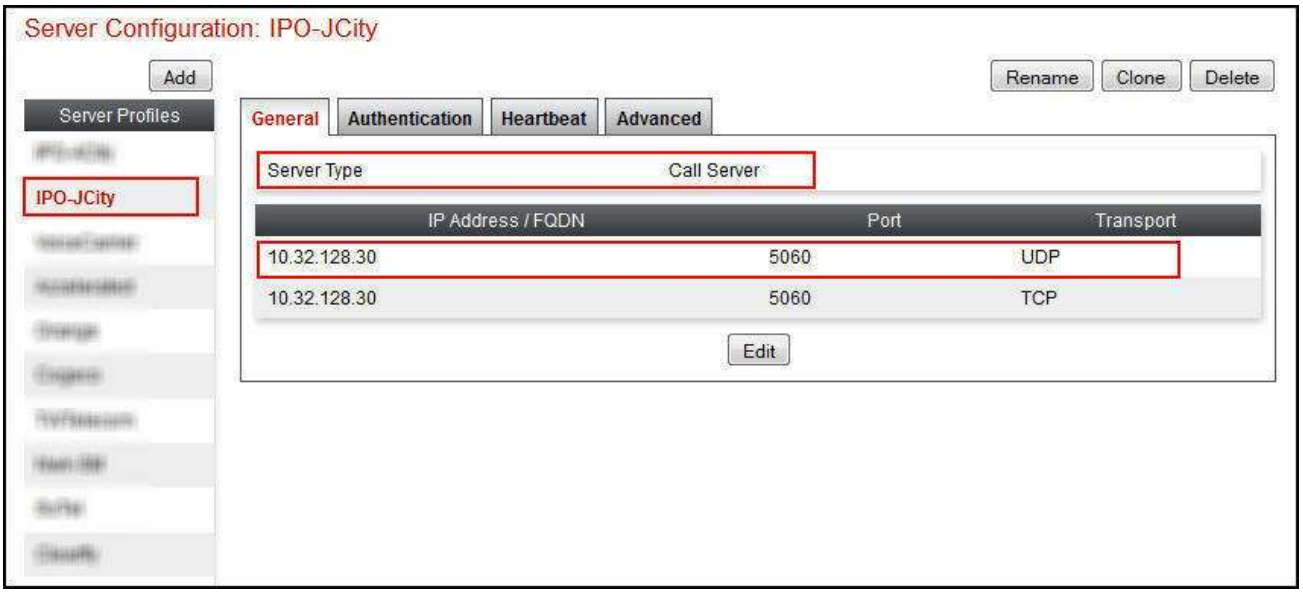
©2015 Avaya Inc. All Rights Reserved.

6.6.1. Server Configuration – Avaya IP Office

For the compliance test, the server configuration profile ***IPO-JCity*** was created for Avaya IP Office. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to ***Call Server***.
- Set **IP Addresses / FQDNs** to the IP address of the Avaya IP Office LAN1 port.
- Set **Transport** to ***UDP***, the transport protocol used for SIP signaling between Avaya IP Office and the Avaya SBCE.
- Set **Port** to the port Avaya IP Office will listen on for SIP requests from the Avaya SBCE.

Note that TCP was also set in the screen below, though UDP connectivity would have been sufficient.



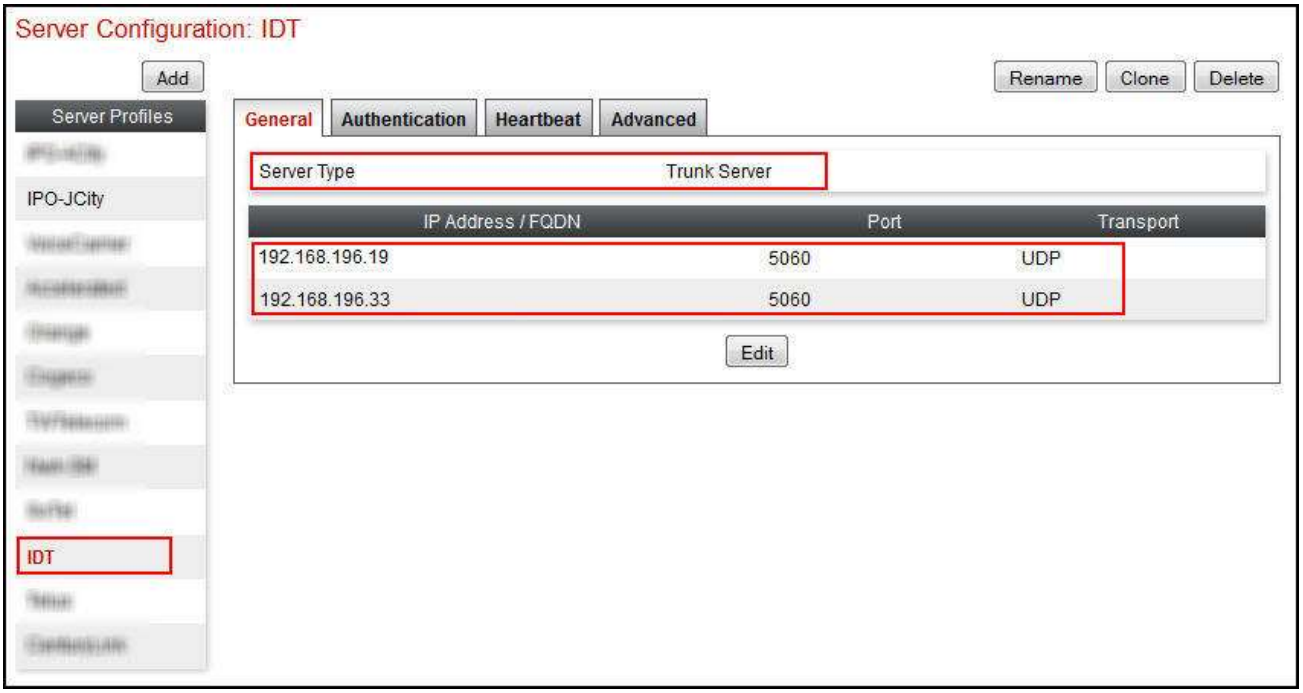
On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Avaya IP Office defined in **Section 6.5.1**.

©2015 Avaya Inc. All Rights Reserved.

6.6.2. Server Configuration – IDT

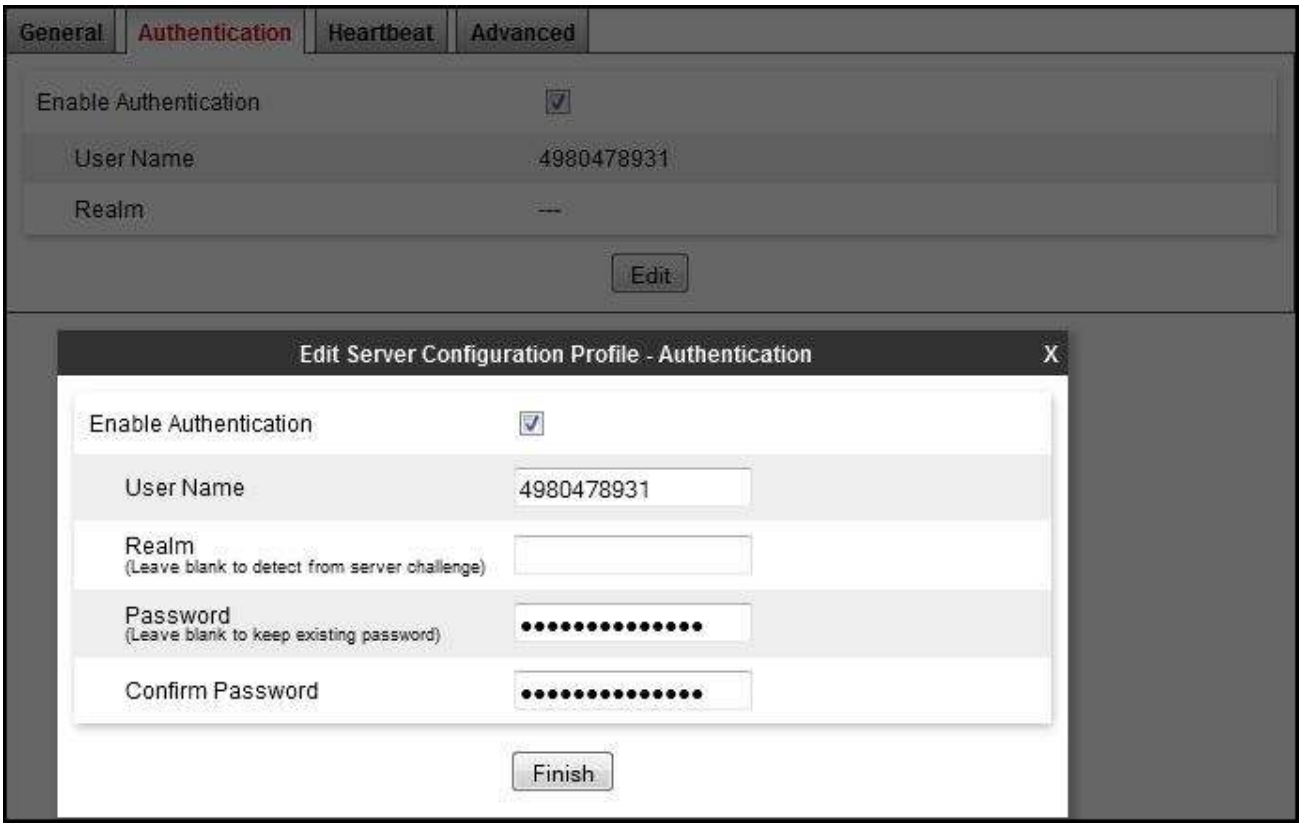
For the compliance test, server configuration profile ***IDT*** was created for IDT. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to ***Trunk Server***.
- Set **IP Addresses / FQDN** to the IP addresses of the IDT network access interface. Note that 2 entries were configured for the 2 border elements of the IDT SIP Trunking Service.
- Select the appropriate **Transport** protocol used for SIP signaling between IDT and the Avaya SBCE. In the compliance test, **UDP** was tested.
- Set **Port** to the standard SIP port of **5060**. This is the port the IDT SIP server will listen on for SIP messages from the Avaya SBCE.

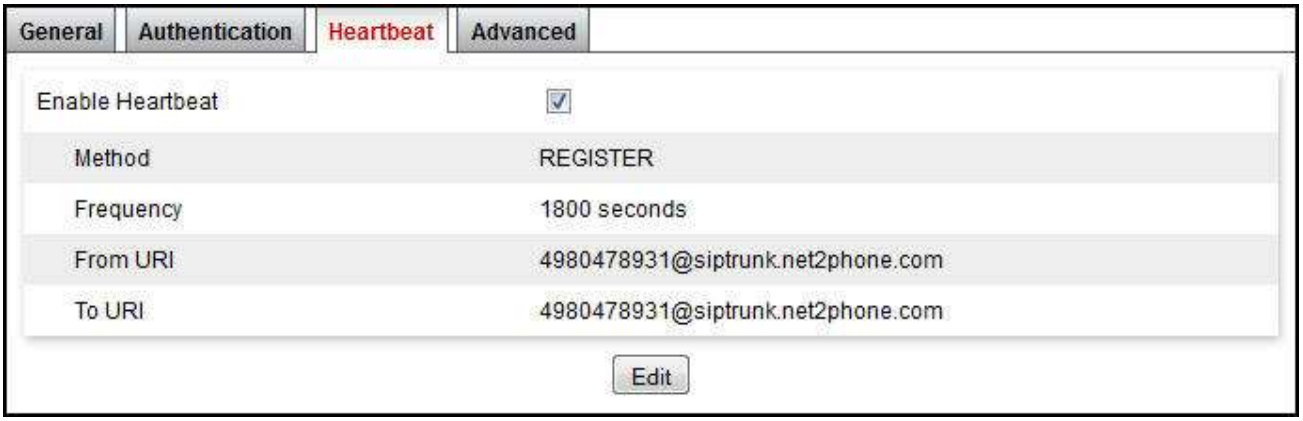


©2015 Avaya Inc. All Rights Reserved.

In the **Authentication** tab, check the **Enable Authentication** option box, and enter the SIP credentials (provided by IDT) for **User Name** and **Password**.

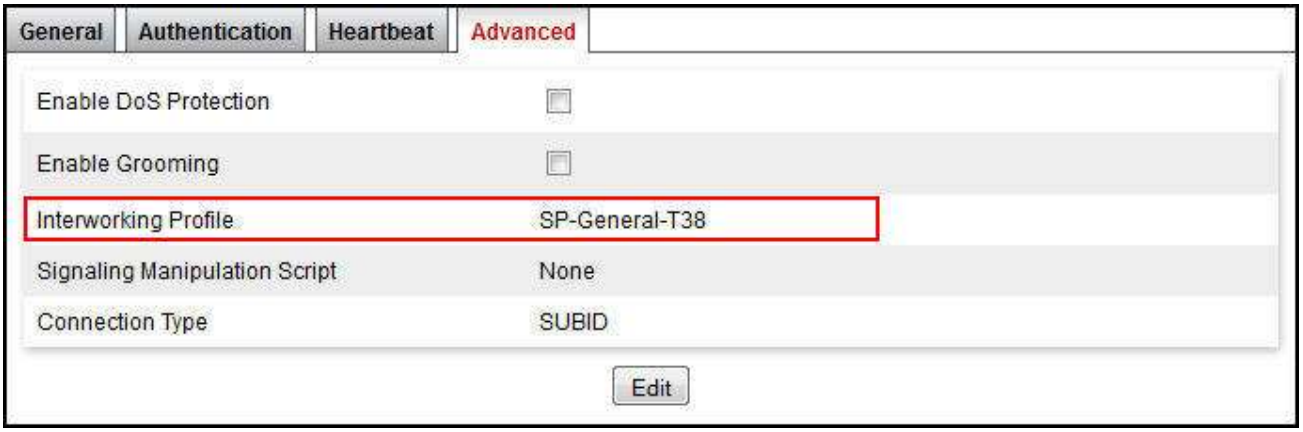


In the **Heartbeat** tab, check the **Enable Heartbeat** option box. Select ***REGISTER*** for **Method**, and enter the desired **Frequency** setting for the time interval at which the REGISTER message will be issued from the enterprise site. Finally enter the **From URI** and **To URI** settings: the user part of the URI's is the user name credential provided by the service provider for SIP trunk registration; the domain in the URI's is the domain for the IDP SIP Trunking Service as provided by IDT.



©2015 Avaya Inc. All Rights Reserved.

In the **Advanced** tab, select the **Interworking Profile** for IDT defined in **Section 6.5.2**.



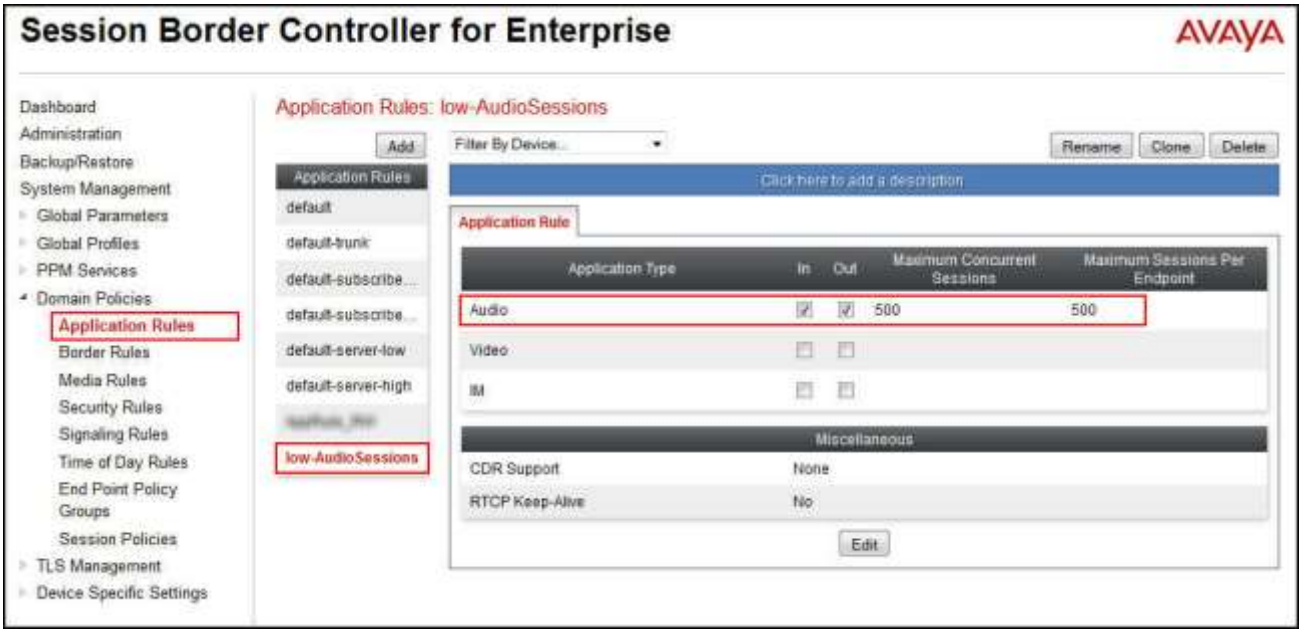
©2015 Avaya Inc. All Rights Reserved.

6.7. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 6.10**.

To view an existing rules profile, navigate to **Domain Policies → Application Rules** in the left pane. In the center pane, select the rules profile to be viewed. To add a new profile, click **Add** in the center pane. To clone from an existing profile, select a profile from the center pane, and then click **Clone** on the top of the right pane to provide a new profile name in the **Clone Rule** window (not shown). The cloned profile can then be selected for editing.

For the compliance test, the application rules profile named ***low-AudioSessions*** was cloned from the **default-trunk** profile in which the settings for both **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** were adjusted down to ***500*** (from 2000) for **Audio** in both call directions. This change was to accommodate the maximum capacity on the Avaya SBCE running on the Portwell CAD-0208 server. The ***low-AudioSessions*** application rules profile was used for both Avaya IP Office and the IDT SIP server.



©2015 Avaya Inc. All Rights Reserved.

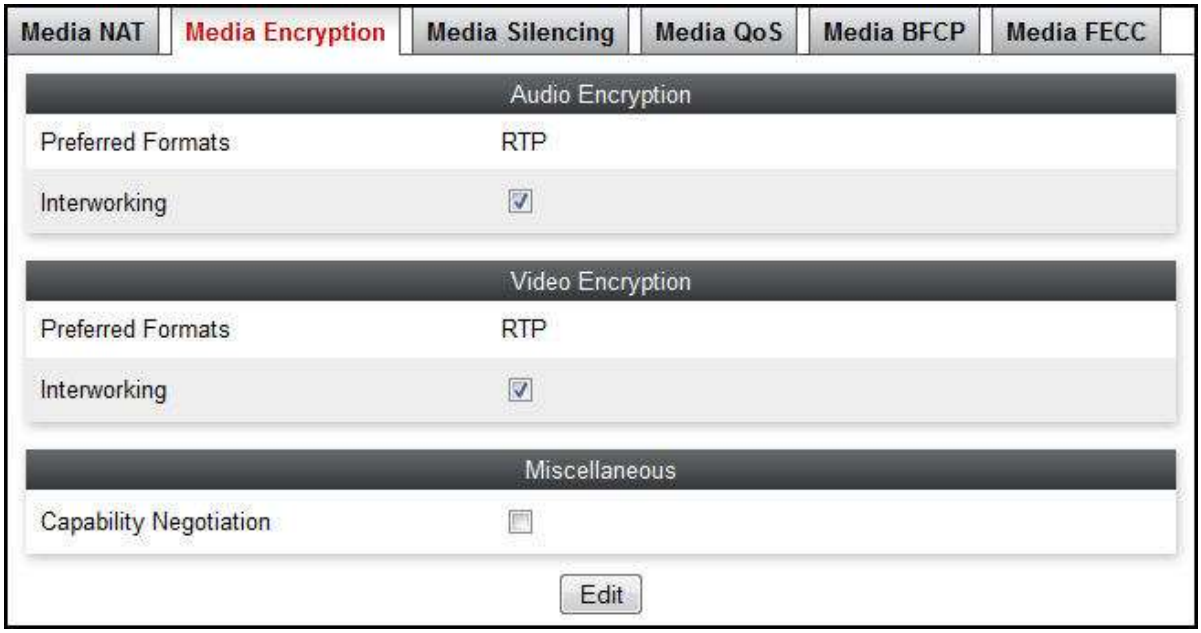
6.8. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger end point policy group defined in **Section 6.10**. For the compliance test, the pre-defined **default-low-med** media rule (shown below) was used for both Avaya IP Office and the IDT SIP server.

To view an existing rule, navigate to **Domain Policies → Media Rules** in the left pane. In the center pane, select the rule (e.g., **default-low-med**) to be viewed.

Each of the tabs of the **default-low-med** media rule is shown below (the **Media NAT** tab is shown above).

The **Media Encryption** tab indicates that no encryption was used.



©2015 Avaya Inc. All Rights Reserved.

The **Media Silencing** tab shows **Media Silencing** was disabled.

The **Media QoS** settings are shown below.

The **Media BFCP** tab is shown below.

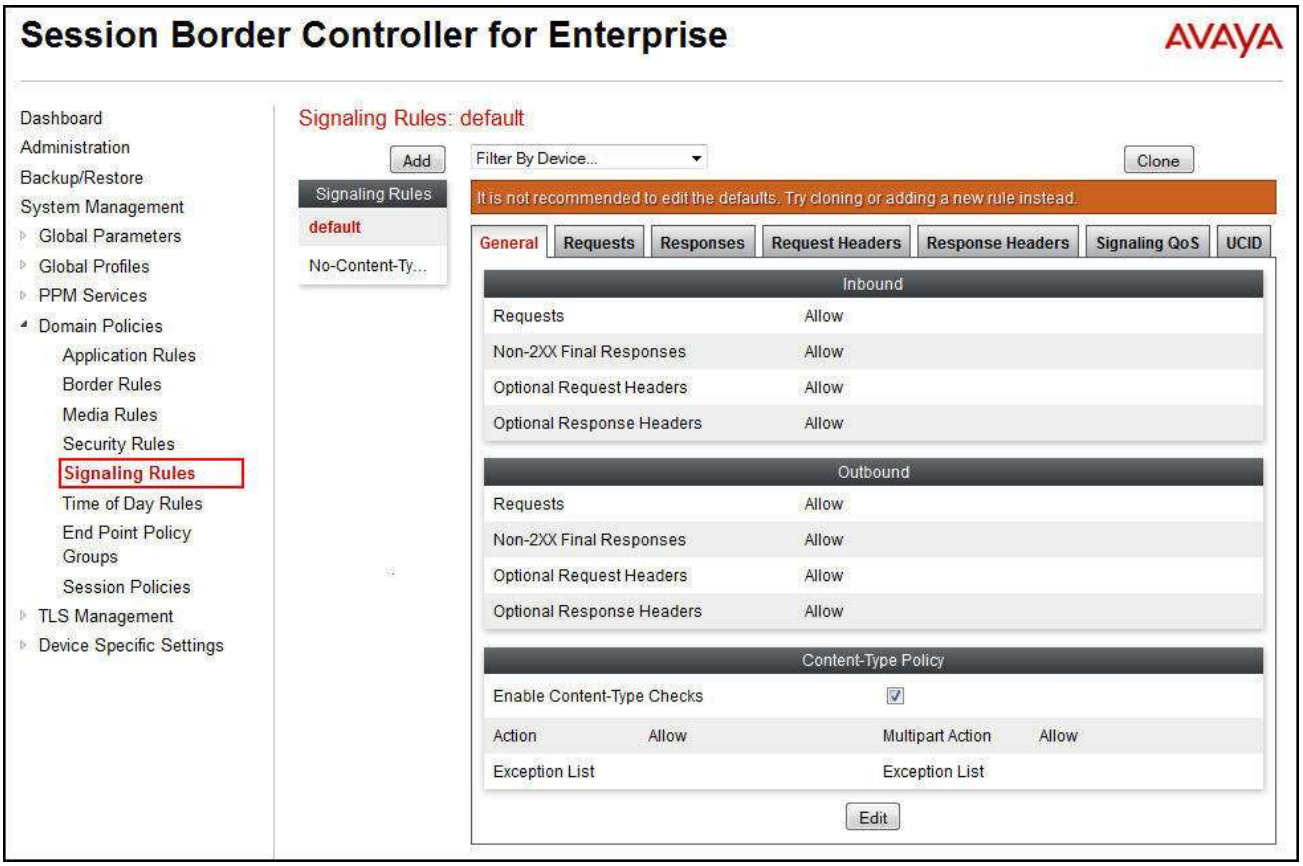
The **Media FECC** tab is shown below.

©2015 Avaya Inc. All Rights Reserved.

6.9. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger end point policy group defined in **Section 6.10**. For the compliance test, the pre-defined **default** signaling rule (shown below) was used for both Avaya IP Office and the IDT SIP server.

To view an existing rule, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select the rule (e.g., **default**) to be viewed. The **General** tab settings of the default signaling rule are shown below.



The **Requests**, **Responses**, **Request Headers, Response Headers** and **UCID** tabs have no entries. The **Signaling QoS** tab is shown below.

©2015 Avaya Inc. All Rights Reserved.

6.10. End Point Policy Groups

An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the service provider SIP server. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 6.13**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by a **Policy Group** window in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before specific endpoint policy groups were added for the compliance test.

©2015 Avaya Inc. All Rights Reserved.

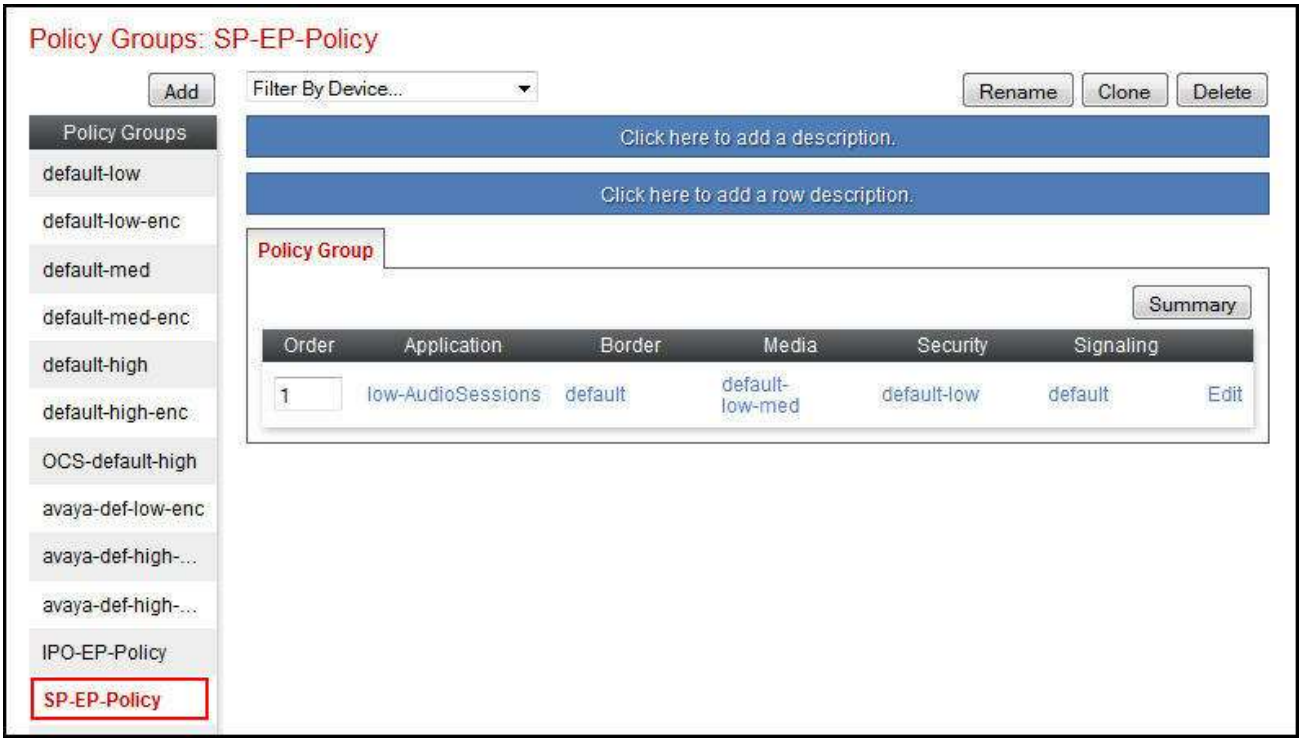
6.10.1. End Point Policy Group – Avaya IP Office

For the compliance test, the end point policy group ***IPO-EP-Policy*** was created for Avaya IP Office. Default values were used for each of the rules which comprise the group, except for the rule for **Application** (which was created in **Section 6.7**). The details of the settings for **Application**, **Media** and **Signaling** are shown in **Section 6.7**, **Section 6.8** and **Section 6.9** respectively.

©2015 Avaya Inc. All Rights Reserved.

6.10.2. End Point Policy Group – IDT

For the compliance test, the end point policy group ***SP-EP-Policy*** was created for the IDT SIP server. Default values were used for each of the rules which comprise the group, except for the rule for **Application** (which was created in **Section 6.7**). The **SP-EP-Policy** policy group is identical to the **IPO-EP-Policy** policy group created in **Section 6.10.1**.



©2015 Avaya Inc. All Rights Reserved.

6.11. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 6.13**. Create one routing profile for Avaya IP Office and another for the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a **Routing Profile** window in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

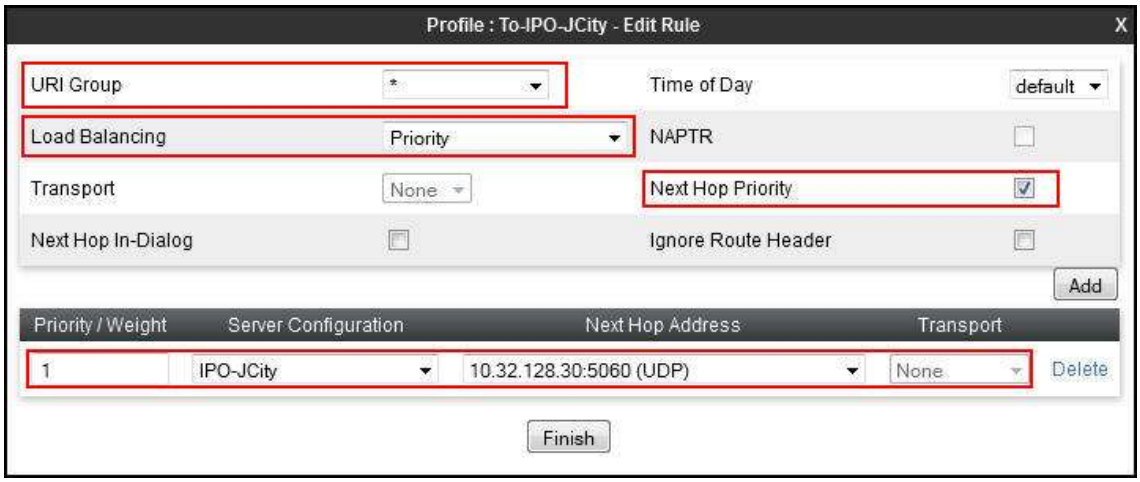
The screen below shows the GUI elements described above before specific routing profiles were added for the compliance test.

©2015 Avaya Inc. All Rights Reserved.

6.11.1. Routing – Avaya IP Office

For the compliance test, the routing profile ***To-IPO-JCity*** was created for Avaya IP Office. When creating the profile, configure the parameters as follows:

- Set **URI Group** to the wild card ***** to match on any URI.
- Select ***Priority*** for **Load Balancing**.
- Enable **Next Hop Priority**.
- When adding an entry for routing destination (Next Hop Address)
  - Enter ***1*** for **Priority/Weight**.
  - For **Server Configuration**, select the Server for Avaya IP Office as configured in **Section 6.6.1**. The selection will automatically populate the **Next Hop Address** field.



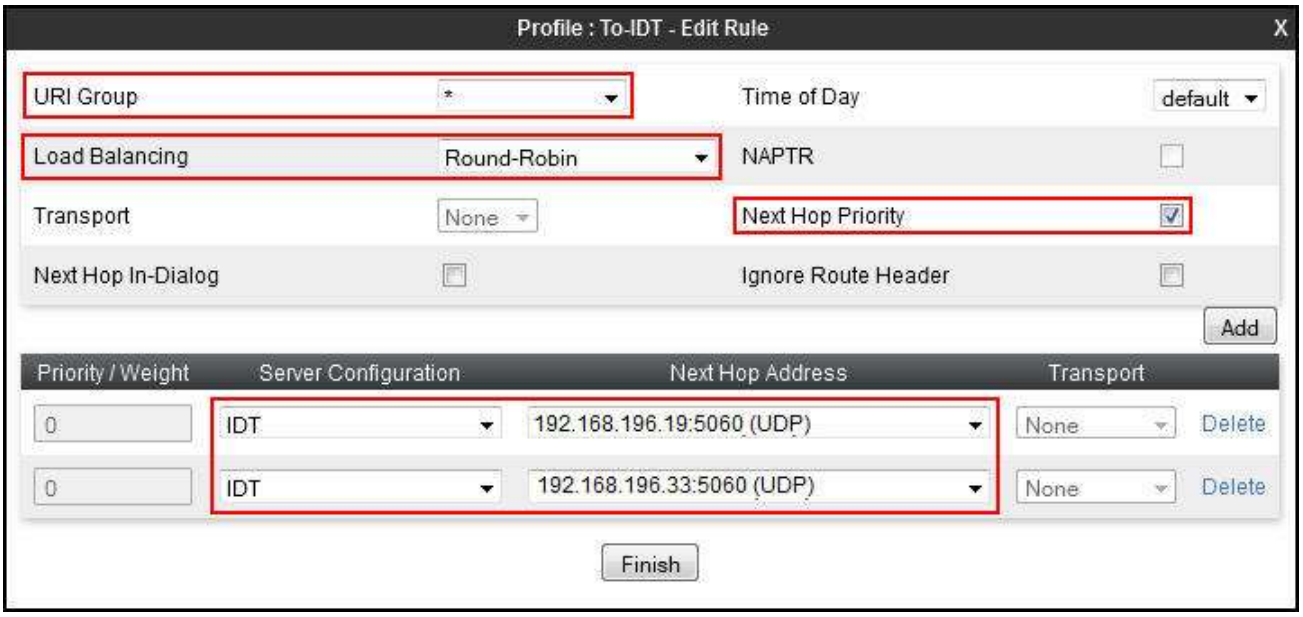
The following screen shows the routing profile for Avaya IP Office when configured.

©2015 Avaya Inc. All Rights Reserved.

6.11.2. Routing – IDT

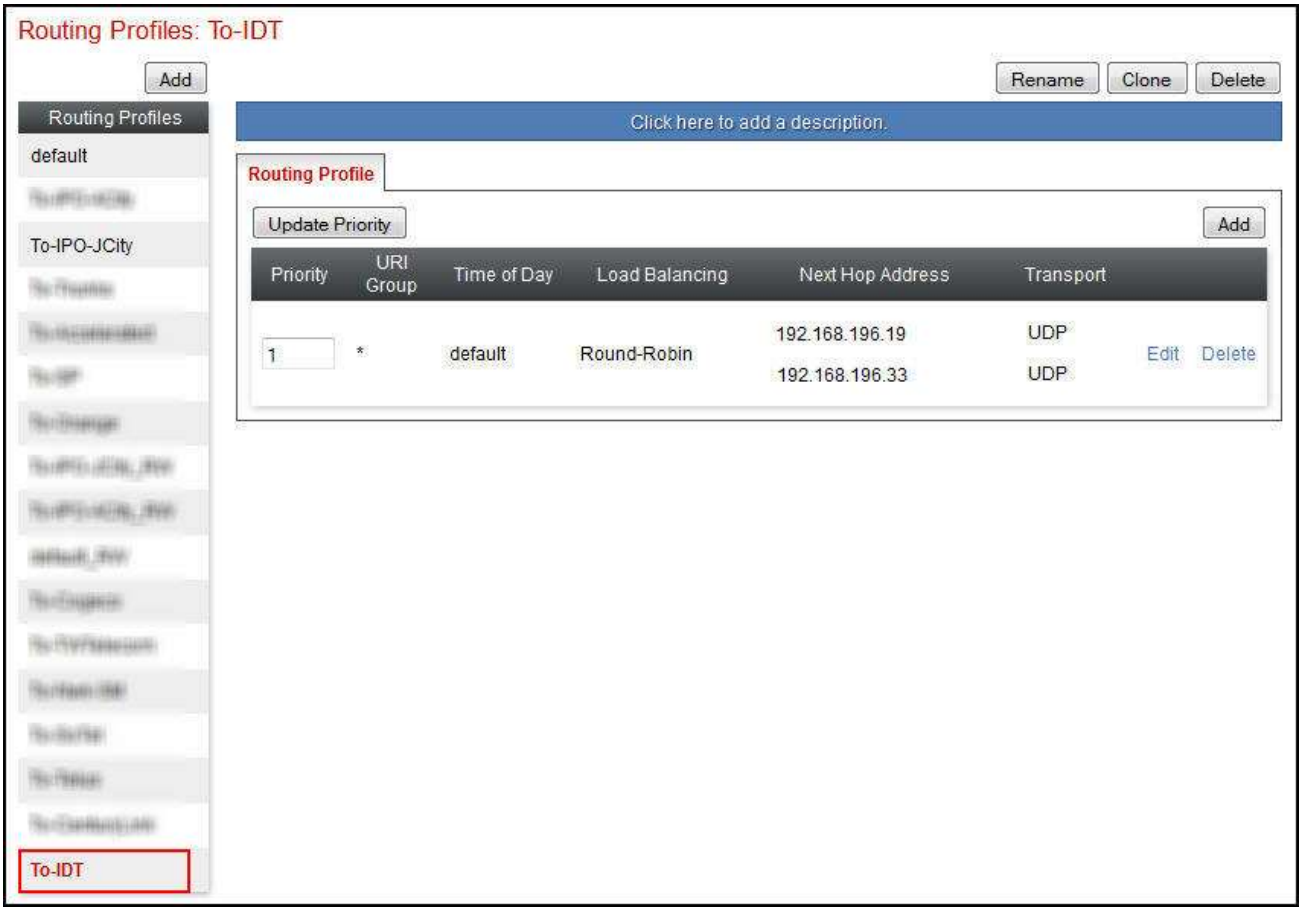
For the compliance test, routing profile ***To-IDT*** was created for routing calls to IDT. When creating the profile, configure the parameters as follows:

- Set **URI Group** to the wild card ***** to match on any URI.
- Select ***Round-Robin*** for **Load Balancing**. With this configuration, calls will be routed alternately to the route destinations defined below.
- Enable **Next Hop Priority**.
- Adding 1st entry for routing destination (Next Hop Address)
  - For **Server Configuration**, select the Server for IDT as configured in **Section 6.6.2**.
  - Select the 1st IP address, port, and transport for the **Next Hop Address** field.
- Adding 2nd entry for routing destination (Next Hop Address)
  - For **Server Configuration**, select the Server for IDT as configured in **Section 6.6.2**.
  - Select the 2nd IP address, port, and transport for the **Next Hop Address** field



©2015 Avaya Inc. All Rights Reserved.

The following screen shows the routing profile for IDT when configured.



©2015 Avaya Inc. All Rights Reserved.

6.12. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the end point flow in **Section 6.13**. For the compliance test, the pre-defined **default** topology hiding profile (shown below) was used for Avaya IP Office; an ***IDT-TH*** topology hiding profile was created for the IDT SIP server.

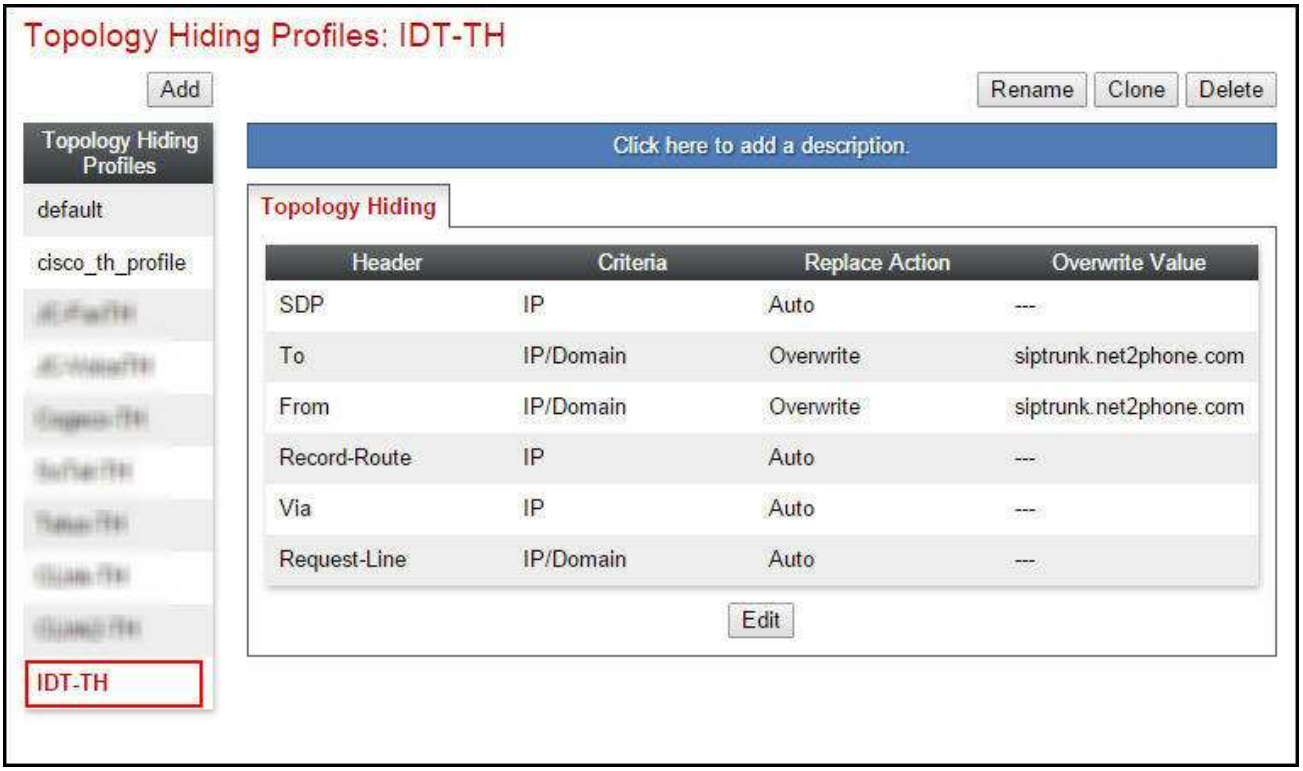
To add a new or view an existing profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add** to add a new profile, or select an existing profile (e.g., **default**) to be viewed.

For creating the topology hiding profile for IDT, navigate to **Global Profiles → Topology Hiding** in the left pane as shown above, and then click **Add** in the center pane. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a **Topology Hiding Profile** window in which the profile parameters can be configured.

©2015 Avaya Inc. All Rights Reserved.

Click the **Add Header** button in the **Topology Hiding Profile** window to add entries for various headers. Select for each entry the proper **Header**, **Criteria**, **Replace Action** and **Overwrite Value**. The screen below shows the added entries for the ***Request-Line***, ***From***, and ***To*** headers during the process for creating the profile:

The following screen shows the complete topology hiding profile for the IDT SIP server:

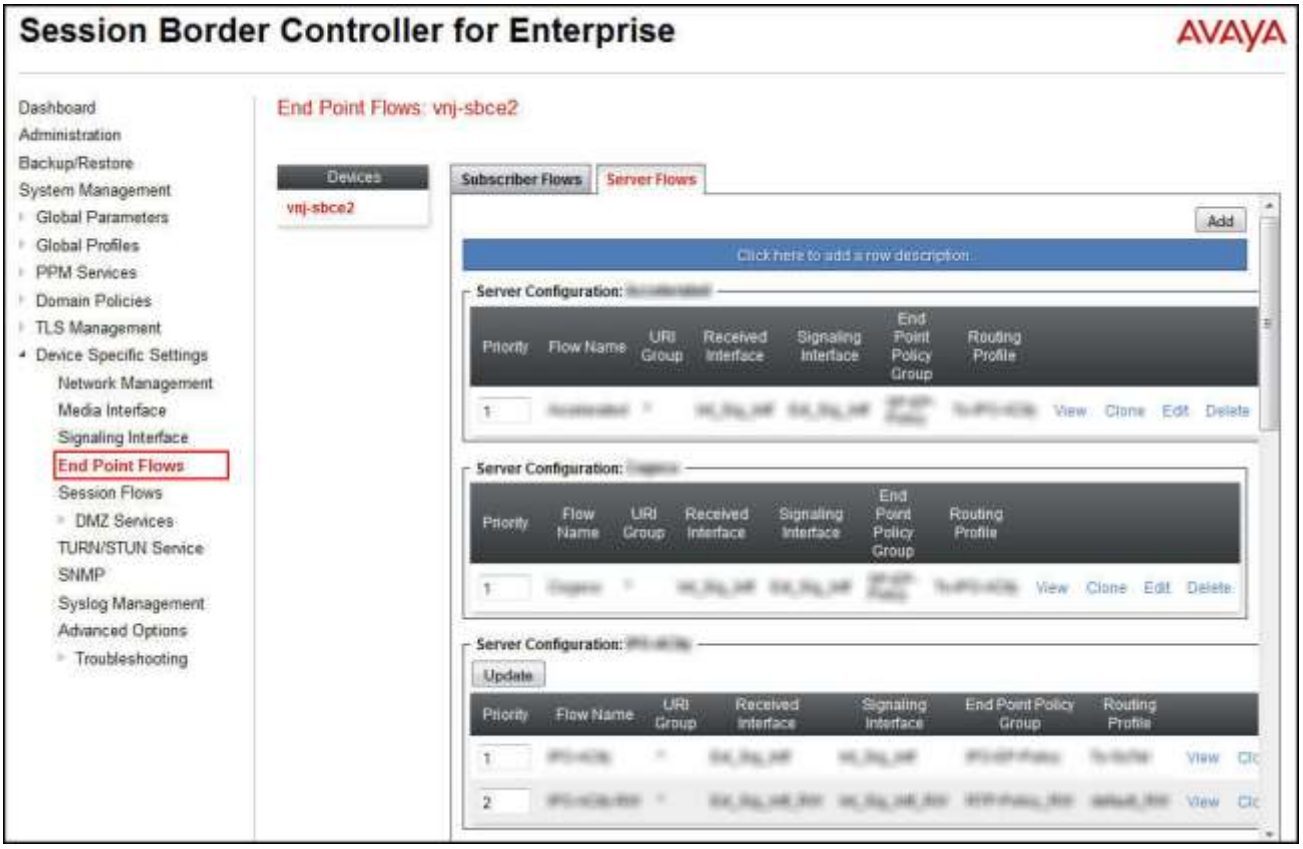


©2015 Avaya Inc. All Rights Reserved.

6.13. End Point Flows

End point flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at 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 policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source end point flow and the destination end point flow. In the case of the compliance test, the signaling endpoints are Avaya IP Office and the IDT SIP server.

To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device to be managed. In the right pane, select the **Server Flows** tab and click the **Add** button. A pop-up window (not shown) will appear requesting the name of the new flow and settings for the flow parameters. Once complete, the configured flow is shown in the far right pane under the server name listed by the **Server Configuration** heading.

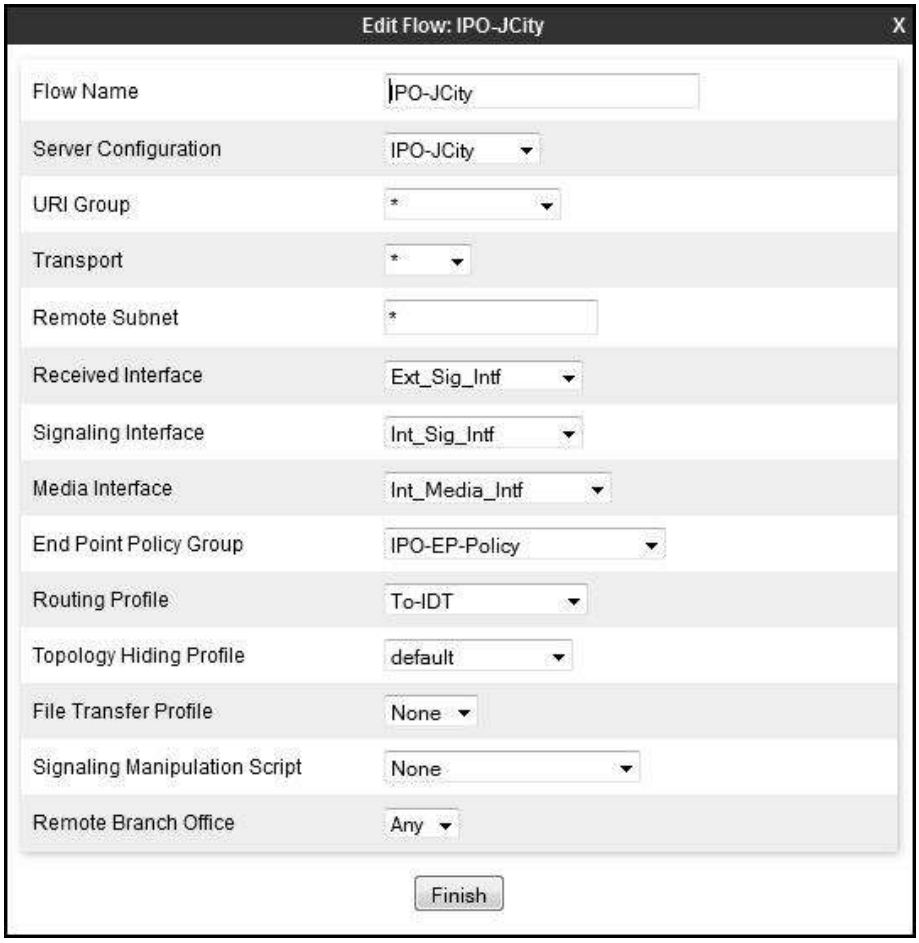


©2015 Avaya Inc. All Rights Reserved.

6.13.1. End Point Flow – Avaya IP Office

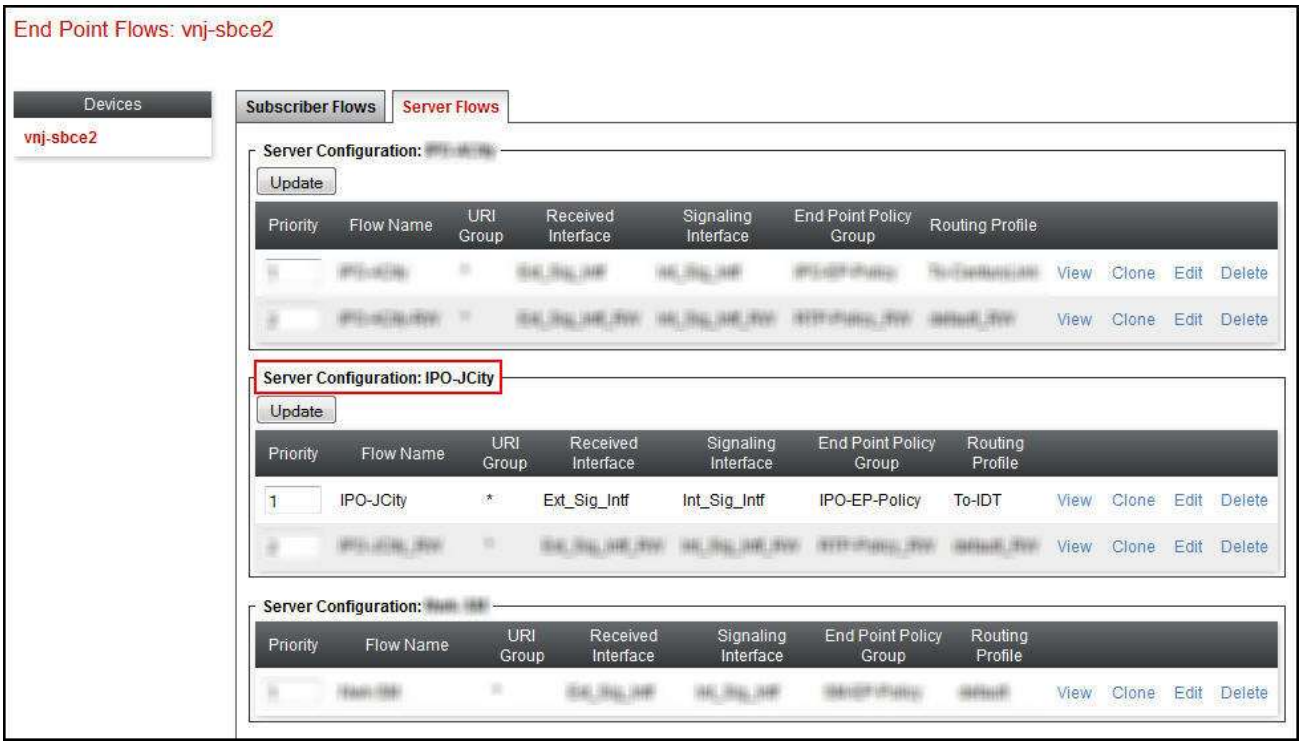
For the compliance test, the end point flow ***IPO-JCity*** was created for Avaya IP Office. All traffic from Avaya IP Office will match this flow as the source flow and use the specified routing profile ***To-IDT*** to determine the destination server and corresponding destination flow. The **End Point Policy Group** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Avaya IP Office server created in **Section 6.6.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set **Received Interface** to the external signaling interface.
- Set **Signaling Interface** to the internal signaling interface.
- Set **Media Interface** to the internal media interface.
- Set **End Point Policy Group** to the endpoint policy group defined for Avaya IP Office in **Section 6.10.1**.
- Set **Routing Profile** to the routing profile defined in **Section 6.11.2** used to direct traffic to the IDT SIP server.
- Set **Topology Hiding Profile** to the topology hiding profile specified for Avaya IP Office in **Section 6.12**.



©2015 Avaya Inc. All Rights Reserved.

The screen below shows the saved **IPO-JCity** configuration as a Server Flow. Note the server name by the **Server Configuration** heading.



©2015 Avaya Inc. All Rights Reserved.

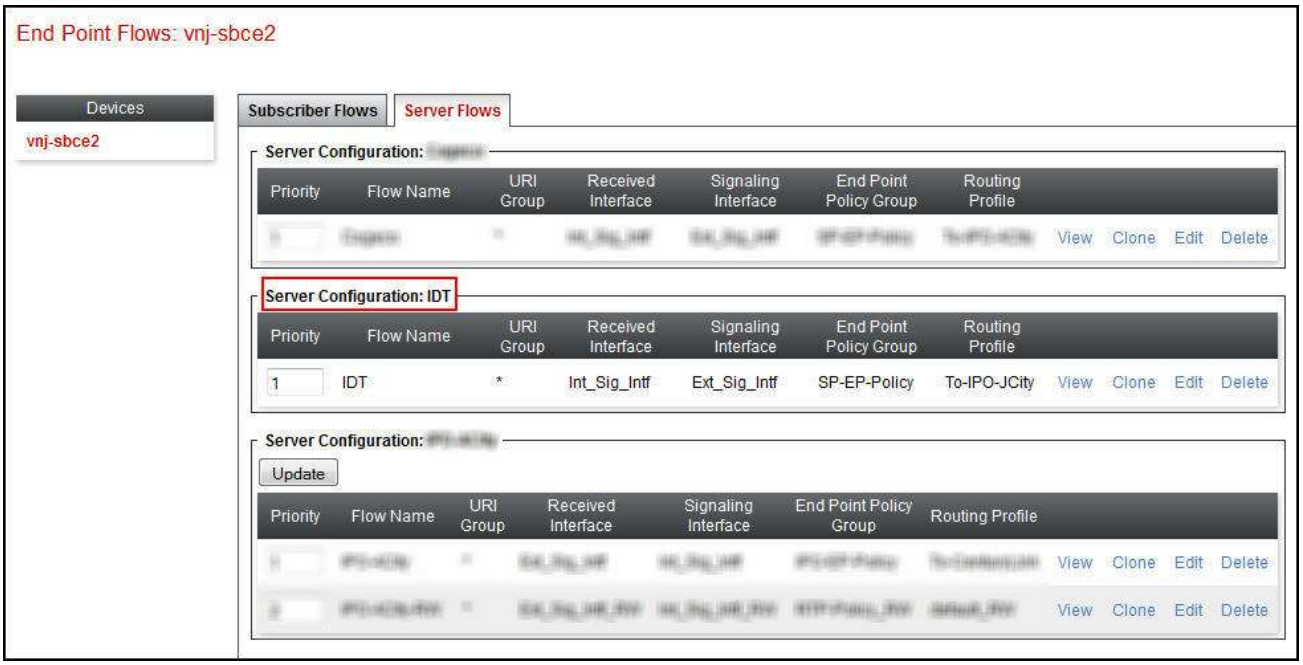
6.13.2. End Point Flow – IDT

For the compliance test, the end point flow ***IDT*** was created for the IDT SIP server. All traffic from IDT will match this flow as the source flow and use the specified routing profile ***To-IPO-JCity*** to determine the destination server and corresponding destination flow. The **End Point Policy Group** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the IDT SIP server created in **Section 6.6.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set **Received Interface** to the internal signaling interface.
- Set **Signaling Interface** to the external signaling interface.
- Set **Media Interface** to the external media interface.
- Set **End Point Policy Group** to the endpoint policy group defined for IDT in **Section 6.10.2**.
- Set **Routing Profile** to the routing profile defined in **Section 6.11.1** used to direct traffic to Avaya IP Office.
- Set **Topology Hiding Profile** to the topology hiding profile created for IDT in **Section 6.12**.

©2015 Avaya Inc. All Rights Reserved.

The screen below shows the saved **IDT** configuration as a Server Flow. Note the server name by the **Server Configuration** heading.



7. IDT SIP Trunking Service Configuration

IDT is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise site (i.e., the IP address of the public interface on the Avaya SBCE). IDT will provide the customer the necessary information to configure Avaya IP Office and Avaya SBCE, including:

- Access interface IP addresses of the IDT SIP Trunking Service.
- Transport and port for the IDT SIP connection to the Avaya SBCE at the enterprise.
- DID numbers to assign to users at the enterprise.
- Supported codecs and their preference order.

©2015 Avaya Inc. All Rights Reserved.

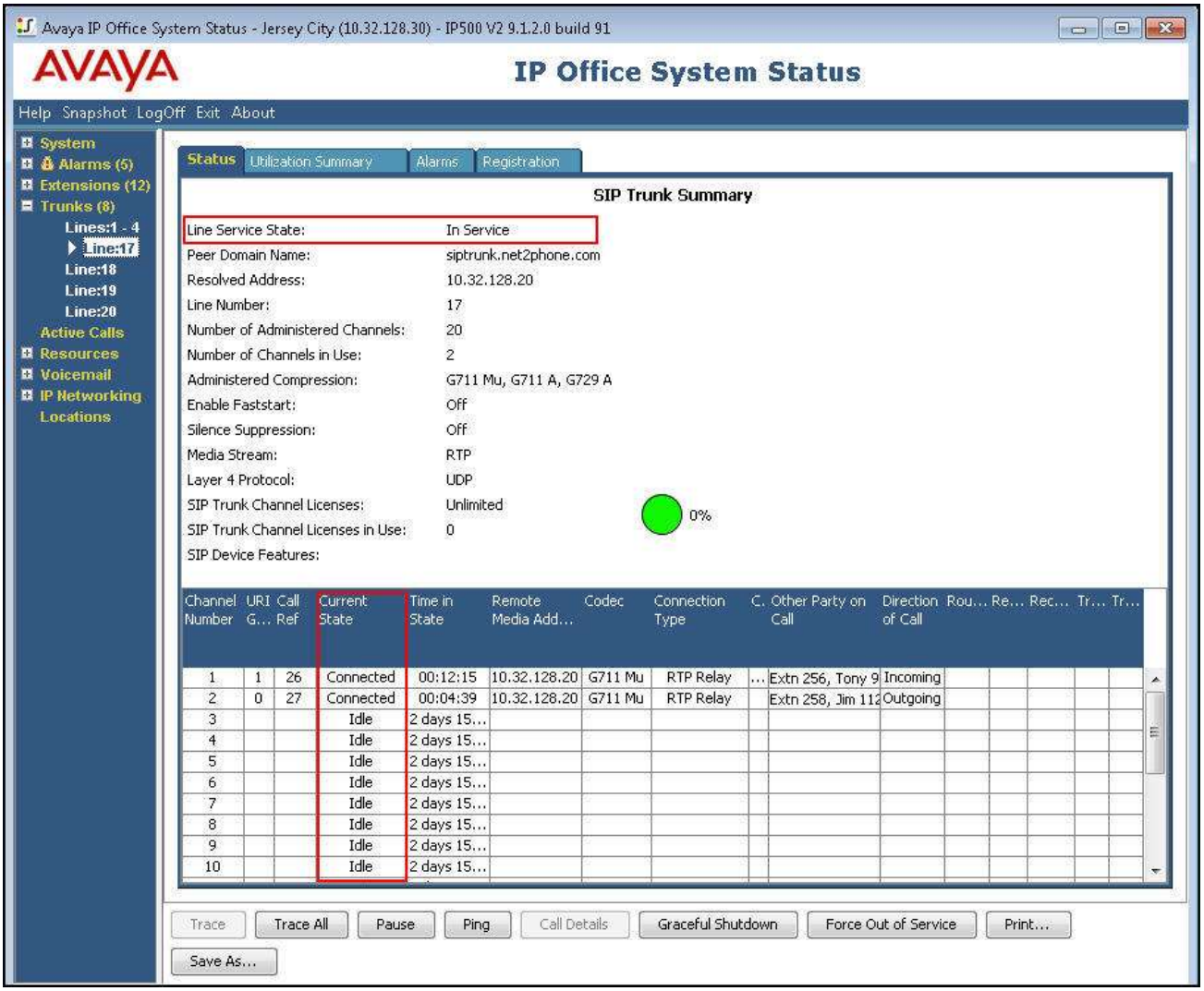
8. Verification Steps

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

8.1. Avaya IP Office System Status

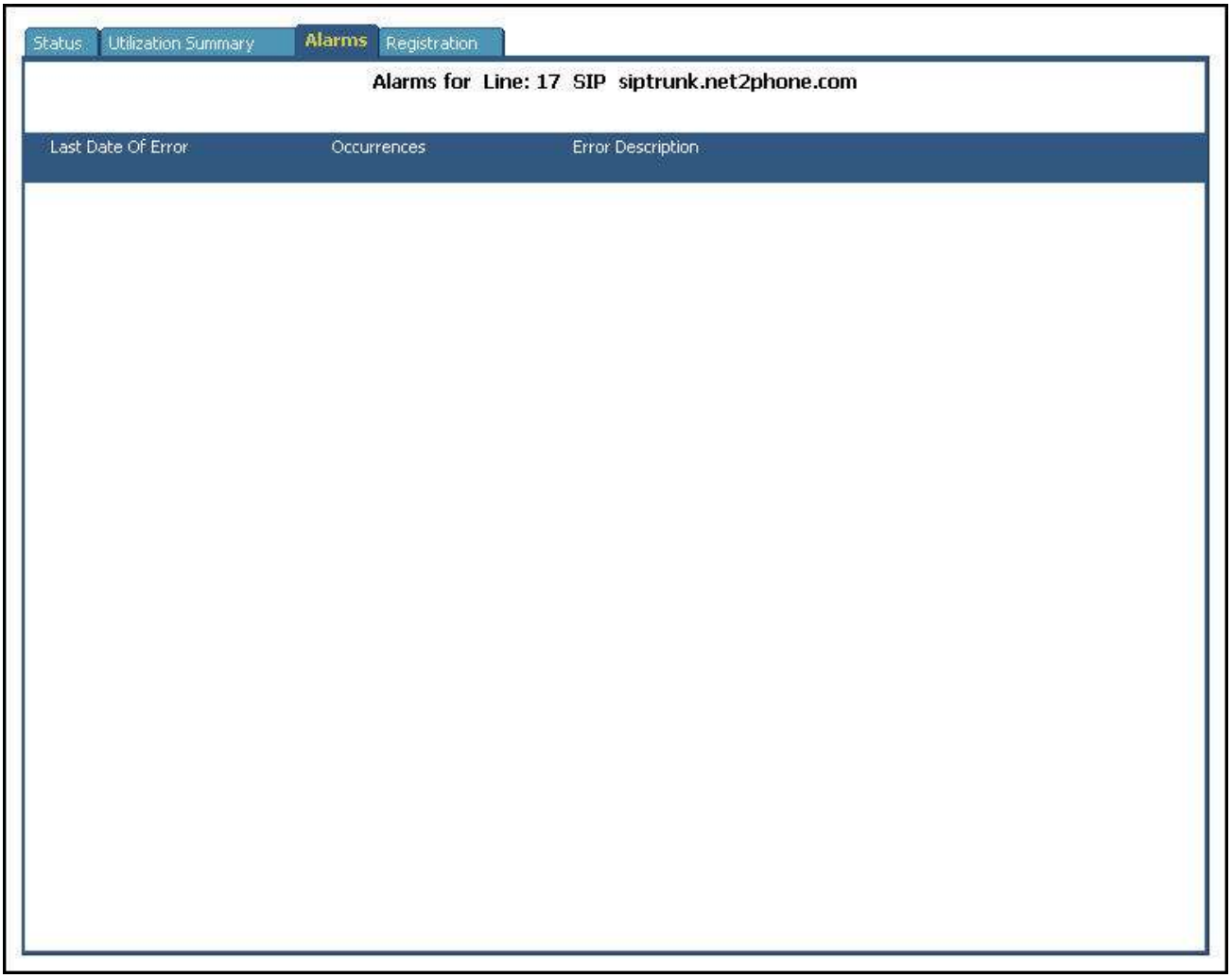
Use the Avaya IP Office System Status application to verify the service state and channels state of the SIP Line and to check alarms:

- Launch the application from **Start → Programs → IP Office → System Status** on the Avaya IP Office Manager PC. Select the SIP Line under **Trunks** from the left pane. On the **Status** tab in the right pane, verify **Line Service State** is shown as ***In Service***. Verify the **Current State** is ***Idle*** for channels where no active calls are currently in session; the state should be ***Connected*** for channels engaged in active calls.



©2015 Avaya Inc. All Rights Reserved.

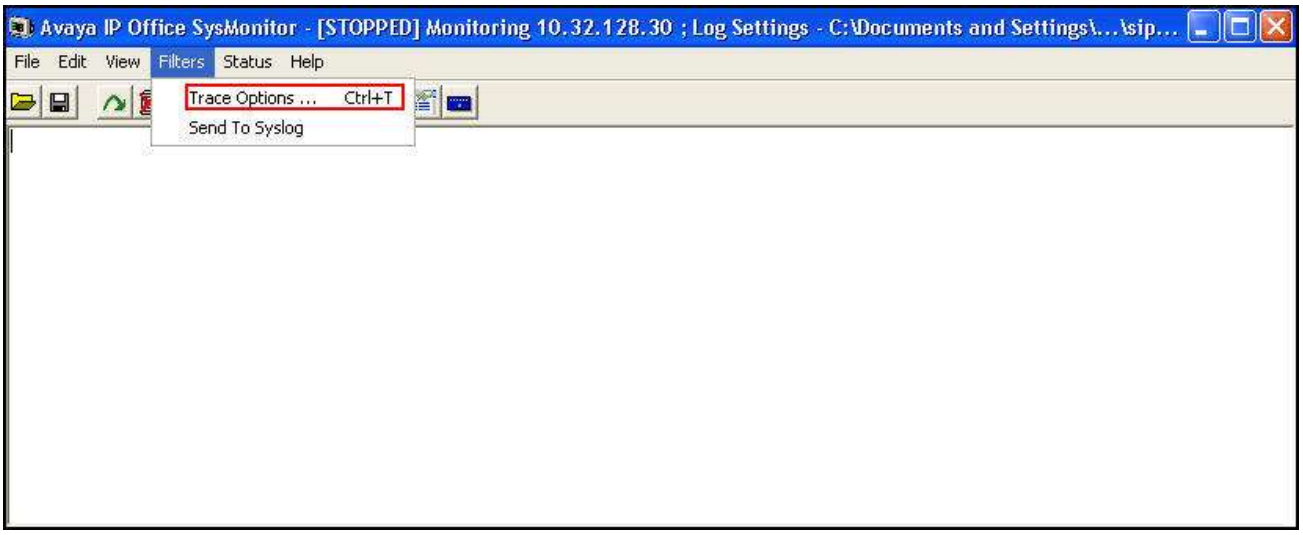
- Select the **Alarms** tab and verify that no alarms are active on the SIP Line.



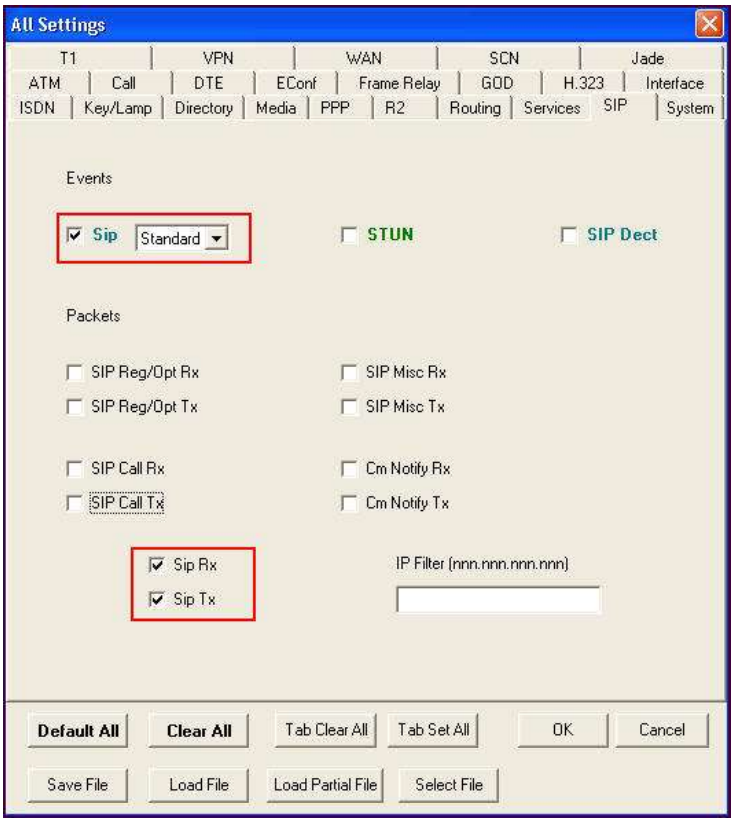
©2015 Avaya Inc. All Rights Reserved.

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.



©2015 Avaya Inc. All Rights Reserved.

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. In the **Packet Capture** tab, 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 press the **Start Capture** button to start the trace. The captured trace file can then be downloaded from the **Captures** tab for examination using a protocol sniffer application such as Wireshark.

The screen below shows the setup for capturing packets to and from the public interface of the Avaya SBCE (B1). The captured traffic will be capped at 10000 packets and be saved to a file named "SBCEToFromIDT.pcap".

9. Conclusion

The IDT Net2Phone SIP Trunking Service passed compliance testing with Avaya IP Office R91 and Avaya Session Border Controller for Enterprise R6.3. These Application Notes describe the configuration necessary to connect Avaya IP Office R9.1 and Avaya SBCE R6.3 to IDT as shown in **Figure 1**. Test results and observations are noted in **Section 2.2**.

©2015 Avaya Inc. All Rights Reserved.

10. Additional References

[1] *IP Office™ Platform 9.1, Deploying Avaya IP Office™ Platform IP500 V2,* Document Number 15-601042, Issue 30j, May 2015.
[2] *Administering Avaya IP Office™ Platform with Manager*, Release 9.1.2, Issue 10.07, March 2015.
[3] *IP Office ™ Platform 9.1, Administering Avaya IP Office™ Platform Voicemail Pro*, Document Number 15-601063, Issue 10e, May 2015.
[4] *IP Office™ Platform 9.1, Using IP Office System Monitor*, Document Number 15-601019, Issue 06e, May 2015.
[5] *IP Office™ Platform 9.1, Using Avaya IP Office™ Platform System Status*, Document Number 15-601758, Issue 10e, April 2015.
[6] *Using Avaya Communicator for Windows on IP Office*, Release 9.1.2, April 2015.
[7] *Deploying Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.
[8] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.
[9] *Application Notes for configuring Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.3 to support Remote Workers*, Issue 1.0, February 2015.

Additional IP Office documentation can be found at http://marketingtools.avaya.com/knowledgebase/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf_feed_template.html.

Product documentation for the IDT Net2Phone SIP Trunking Service is available from IDT. See **Section 2.3** on how to contact IDT.

©2015 Avaya Inc. All Rights Reserved.

©2015 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.