Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Clearfly Communications SIP Trunking Service with Avaya IP Office R9.1 and Avaya Session Border Controller for Enterprise R6.3 - 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 Clearfly Communications SIP Trunking Service. Clearfly Communications is a member of the Avaya DevConnect Service Provider program.

The Clearfly Communications SIP Trunking Service provides PSTN access via a SIP trunk between an enterprise site and the Clearfly Communications network as an alternative to legacy analog or digital trunks. This approach generally results in easier maintenance and lower cost for the business customer.

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

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

Table of Contents

1. Introduction

These Application Notes describe the procedures for configuring an enterprise solution using Avaya IP Office Release R9.1 and Avaya Session Border Controller for Enterprise (Avaya SBCE) R6.3 to inter-operate with the Clearfly Communications SIP Trunking Service.

In the sample configuration, the enterprise solution consists of an Avaya SBCE, an Avaya IP Office 500 V2 running Release 9.1 software, Avaya Preferred Edition (a.k.a Voicemail Pro) messaging application, Avaya H.323 and SIP deskphones, and the SIP-based Avaya Communicator softphone. Customers using this Avaya IP Office enterprise solution with the Clearfly Communications SIP Trunking Service are able to place and receive PSTN calls via a broadband WAN connection using SIP. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

For brevity, Clearfly Communications could be referred to as "Clearfly" in the remainder of this document. The term "service provider" was also used to refer to Clearfly Communications.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office to connect to Clearfly Communications via Avaya SBCE. The configuration shown in **Figure 1** was used to exercise the features and functionality tests listed in **Section 2.1**.

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

2.1. Interoperability Compliance Testing

To verify SIP Trunking interoperability, the following features and functionality were covered during the compliance test.

- SIP OPTIONS queries and responses.
- Incoming calls from the PSTN to H.323 and SIP telephones at the enterprise. All inbound calls from the PSTN were routed from the service provider across the SIP trunk to the enterprise.
- 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.
- Inbound and outbound calls to the Avaya Communicator for Windows (SIP soft client).
- Various call types including: local, long distance, toll-free, international, Local Directory Assistance, and Emergency 911 calls.
- G.711u and G.729a codecs.
- DTMF transmission using RFC 2833.

- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call transfer, conference, forwarding and mobility (mobile twinning).
- Use of the SIP REFER method for call redirection to the PSTN.
- Voicemail navigation for inbound and outbound calls, and voicemail Message Waiting Indicator (MWI).
- T.38 fax and G.711u pass-through fax.
- Inbound and outbound long-duration and long hold time call stability.
- Response to incomplete call attempts and trunk errors.
- 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 Clearfly SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **REFER Signaling –** When using the SIP REFER method for off-net call transfer, post-REFER signaling between Clearfly and the enterprise was sometimes not completely clean. Clearfly would issue BYE, immediately after accepting the REFER message from the enterprise, to terminate the call with the original enterprise caller. Due to timing, the enterprise could respond to the subsequent messages from Clearfly (to the enterprise caller) with "405 Method Not Allowed" or "481 Call Leg/Transaction does not exist" since the call was already terminated by the previous BYE. This problem did not negatively affect the call transfer itself – off-net call transfer to the PSTN was successfully verified in the compliance test.
- **T.38 Fax –** During compliance testing, inbound T.38 fax worked properly with Avaya IP Office issuing the reINVITE message towards Clearfly to re-negotiate to the T.38 codec after call connect. However, outbound T.38 faxes almost always fell back to G.711u pass-through (treating fax as regular voice calls with best effort). Clearfly passes fax call signaling straight through to/from its terminating carriers, and therefore does not guarantee codec re-negotiation to T.38 on outbound faxes from the service side.
- **Direct Media –** The Direct Media capability on IP Office allows IP endpoints to send RTP media directly to each other 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 by the Clearfly SIP Trunking Service included the following:

- **Operator Calls** – Clearfly does not support Operator (0) and Operator-Assisted (0 + 10-digits) calls.
- **Session Timer –** Session timer based on RFC 4028 is not supported by Clearfly. Instead, Clearfly uses a similar approach via reINVITE polling: Clearfly would re-INVITE an active SIP dialog every 15-minutes. During compliance testing, the enterprise sent session refresh UPDATE messages towards Clearfly with the configured session timer on Avaya IP Office.

2.3. Support

For support on the Clearfly SIP Trunking Service, please contact Clearfly Communications via the following:

- Web: https://www.clearfly.net/support/
- Phone: (866) 652-7520

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com.

3. Reference Configuration

Figure 1 illustrates the test configuration showing an enterprise site connected to the Clearfly SIP Trunking Service.

Located at the edge of the enterprise network is the Avaya SBCE. It has a public side that connects to the Clearfly network via the public Internet, and a private side that connects to the enterprise LAN 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.

Within the enterprise site is an Avaya IP Office 500 V2 running the Release 9.1 software. Endpoints include various Avaya IP Telephones (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.

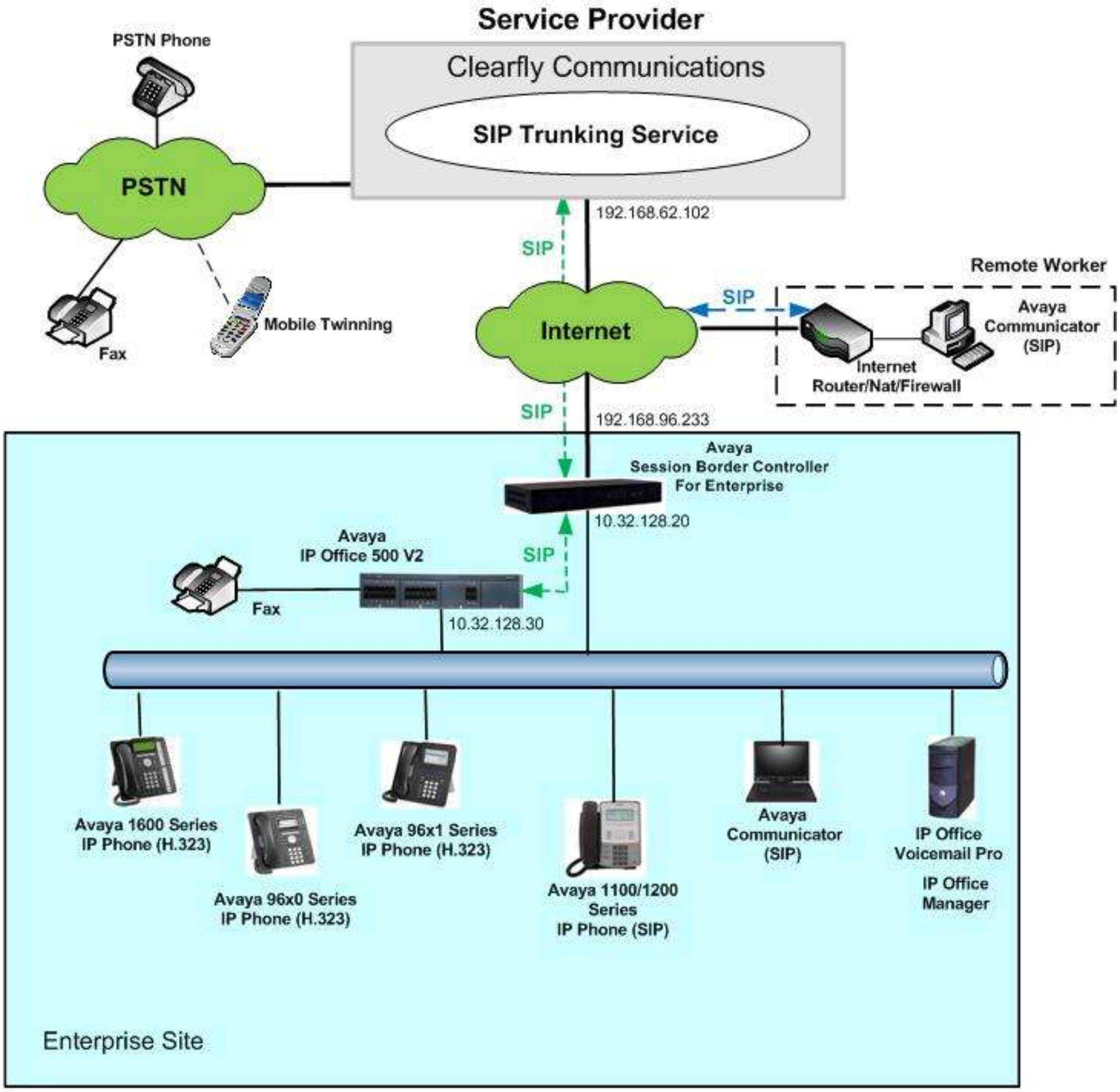


Figure 1: Avaya IP Office with Clearfly Communications SIP Trunking Service

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, enterprise 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 Clearfly. 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 To header of an outbound SIP INVITE message. Clearfly sent 10 digits in the Request URI and the To header of inbound SIP INVITE messages.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the 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 Preferred Edition (Voicemail Pro) messaging service and endpoints on Avaya IP Office is standard. Since these configuration tasks are not directly related to the inter-operation with the Clearfly SIP Trunking Service, they are not included in these Application Notes.

Remote Worker (which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise extensions) was tested as part of this solution. For configuration details on Avaya IP Office and Avaya SBCE to support Remote Worker, see [9] in **Section 10**.

4. Equipment and Software Validated

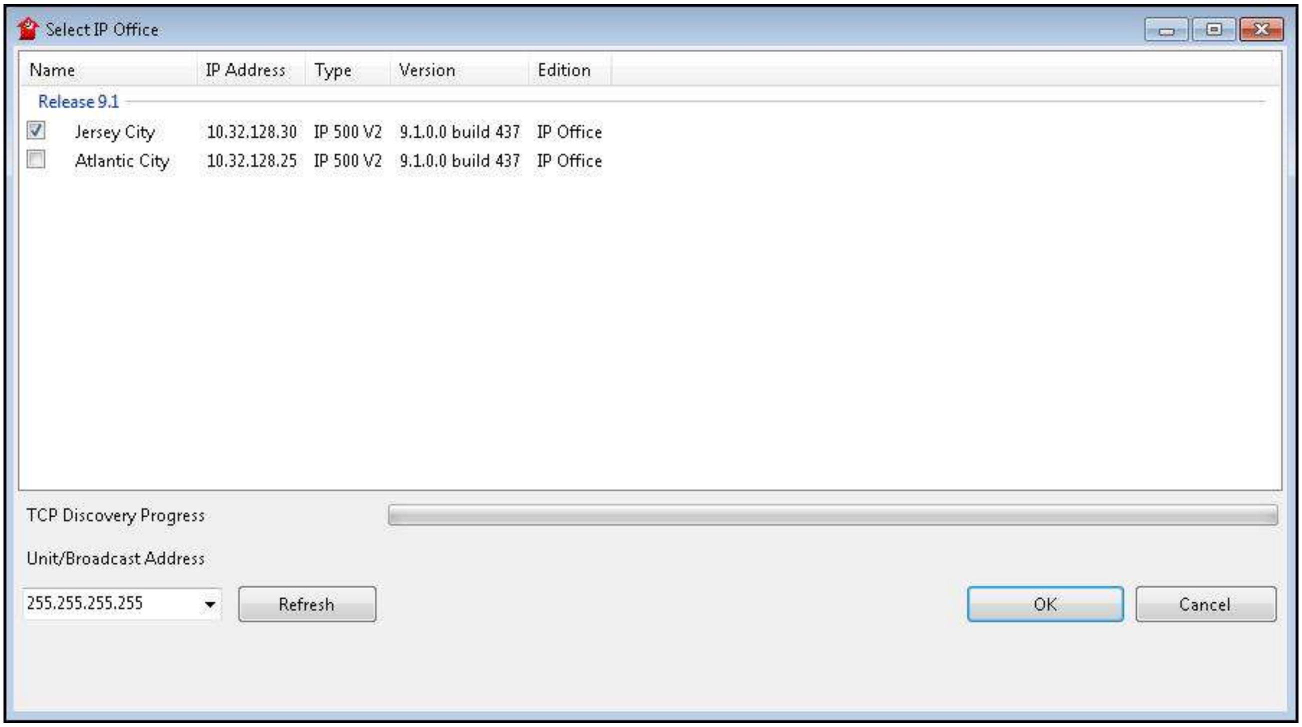
The following equipment and software/firmware were used for the sample configuration provided:

Avaya Telephony Components	
Equipment / Software	**Release / Version**
Avaya IP Office 500 V2	9.1.1.0 build 10
Avaya IP Office COMBO6210/ATM4 Module	9.1.1.0 build 10
Avaya IP Office Manager	9.1.1.0 build 10
Avaya Preferred Edition (a.k.a Voicemail Pro)	9.1.100.3
Avaya 1616 IP Telephones (H.323)	Avaya one-X® Deskphone 1.3 SP5
Avaya 9611G IP Telephones (H.323)	Avaya one-X® Deskphone 6.4.0.14_V452
Avaya 9630G IP Telephones (H.323)	Avaya one-X® Deskphone 3.2.2
Avaya 1120E IP Telephone (SIP)	4.04.18.00
Avaya Communicator for Windows	2.0.3.30
Avaya Session Border Controller for Enterprise running on Portwell CAD-0208 server	6.3.1-22-4653
Clearfly Communications Components	
Equipment / Software	**Release / Version**
Metaswitch Softswitch	v8.3
Metaswitch Perimeta Session Border Controller	v3.7

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 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 or 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.



Name	IP Address	Type	Version	Edition
Release 9.1				
☑ Jersey City	10.32.128.30	IP 500 V2	9.1.0.0 build 437	IP Office
□ Atlantic City	10.32.128.25	IP 500 V2	9.1.0.0 build 437	IP Office

TCP Discovery Progress

Unit/Broadcast Address: 255.255.255.255

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.

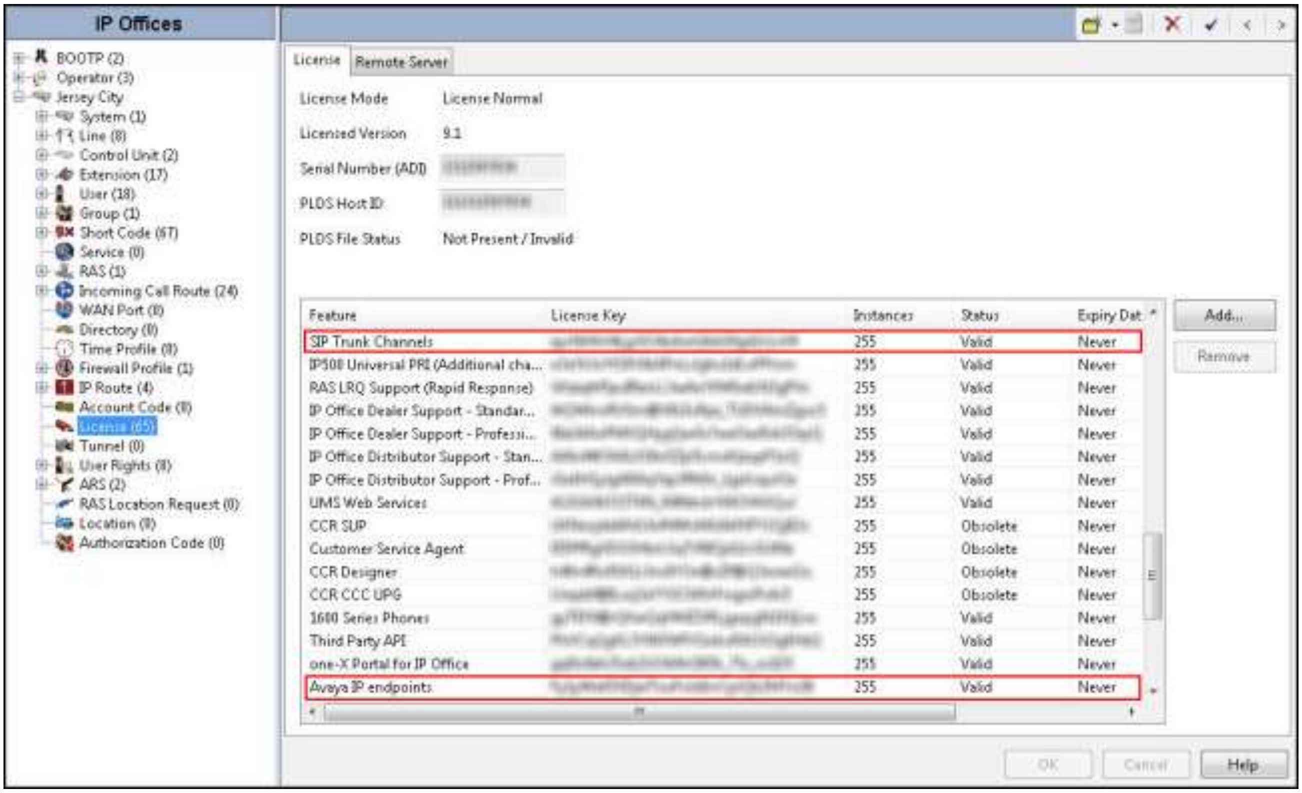
All licensing and feature configuration that is not directly related to the interface with the service provider (such as administering IP endpoints) is assumed to already be in place.

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.

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**.



License Mode: License Normal

Licensed Version: 9.1

Serial Number (ADI): [redacted]

PLDS Host ID: [redacted]

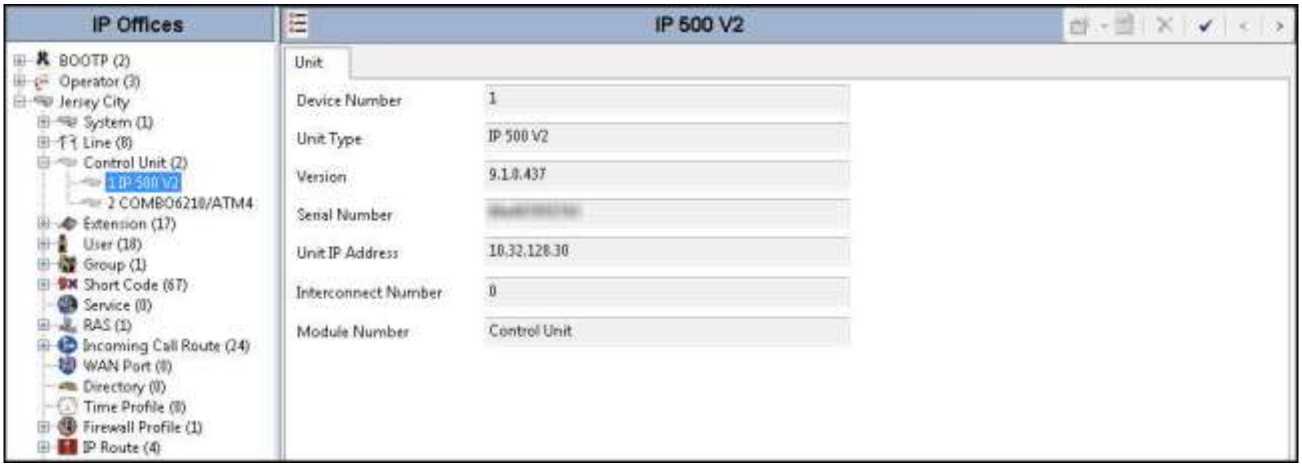
PLDS File Status: Not Present / Invalid

Feature	License Key	Instances	Status	Expiry Dat
SIP Trunk Channels	[redacted]	255	Valid	Never
IP500 Universal PRI (Additional cha...	[redacted]	255	Valid	Never
RAS LRQ Support (Rapid Response)	[redacted]	255	Valid	Never
IP Office Dealer Support - Standar...	[redacted]	255	Valid	Never
IP Office Dealer Support - Professi...	[redacted]	255	Valid	Never
IP Office Distributor Support - Stan...	[redacted]	255	Valid	Never
IP Office Distributor Support - Prof...	[redacted]	255	Valid	Never
UMS Web Services	[redacted]	255	Valid	Never
CCR SUP	[redacted]	255	Obsolete	Never
Customer Service Agent	[redacted]	255	Obsolete	Never
CCR Designer	[redacted]	255	Obsolete	Never
CCR CCC UPG	[redacted]	255	Obsolete	Never
1600 Series Phones	[redacted]	255	Valid	Never
Third Party API	[redacted]	255	Valid	Never
one-X Portal for IP Office	[redacted]	255	Valid	Never
Avaya IP endpoints	[redacted]	255	Valid	Never

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.

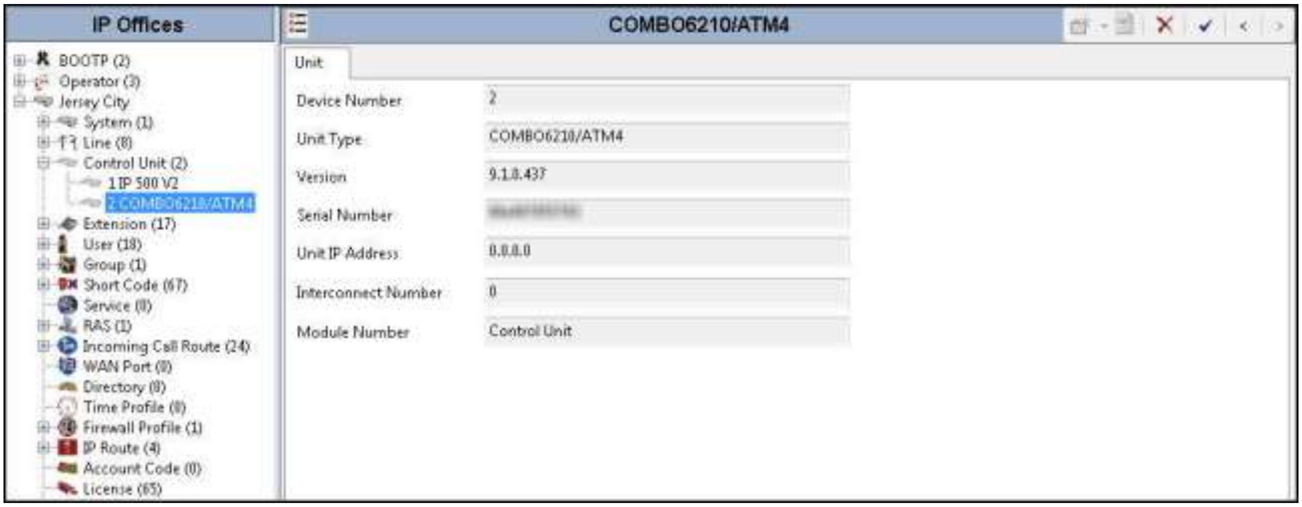
To view the details of the component, select the component in the Navigation Pane.

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



Device Number	1
Unit Type	IP 500 V2
Version	9.1.0.437
Serial Number	[redacted]
Unit IP Address	10.32.128.30
Interconnect Number	0
Module Number	Control Unit

The screen below shows the details of the Combination Card.



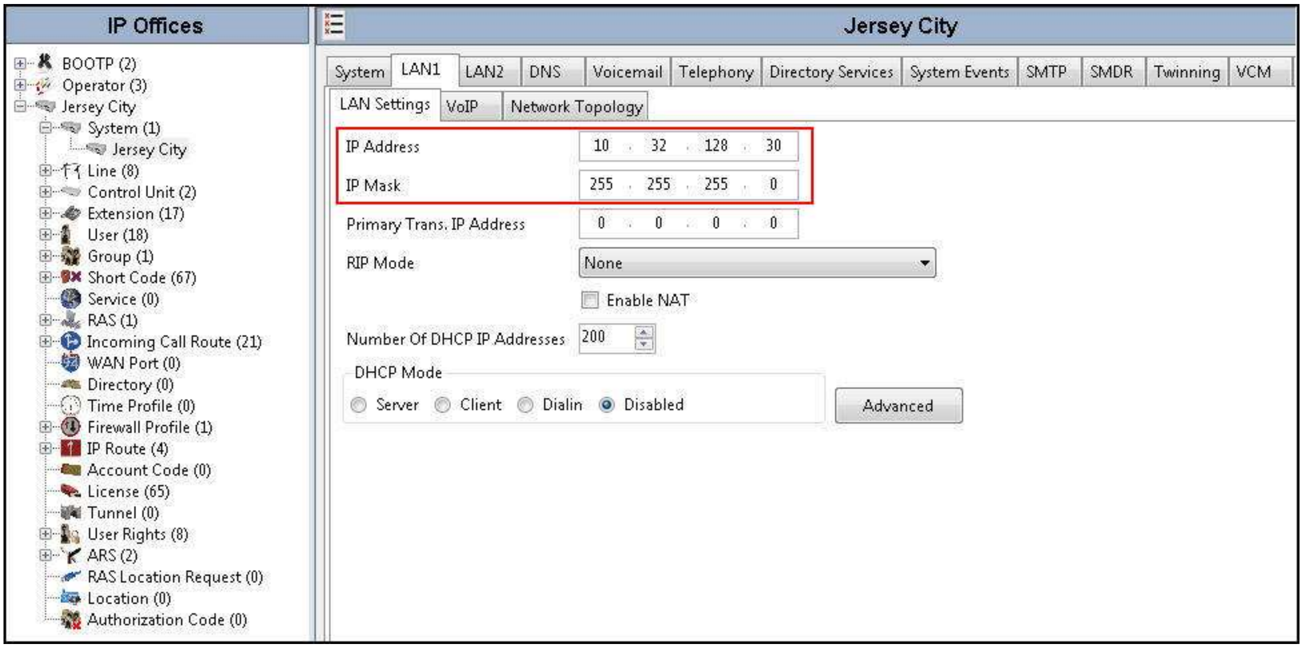
Device Number	2
Unit Type	COMBO6210/ATM4
Version	9.1.0.437
Serial Number	[redacted]
Unit IP Address	0.0.0.0
Interconnect Number	0
Module Number	Control Unit

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.



IP Address: 10 . 32 . 128 . 30

IP Mask: 255 . 255 . 255 . 0

Primary Trans. IP Address: 0 . 0 . 0 . 0

RIP Mode: None

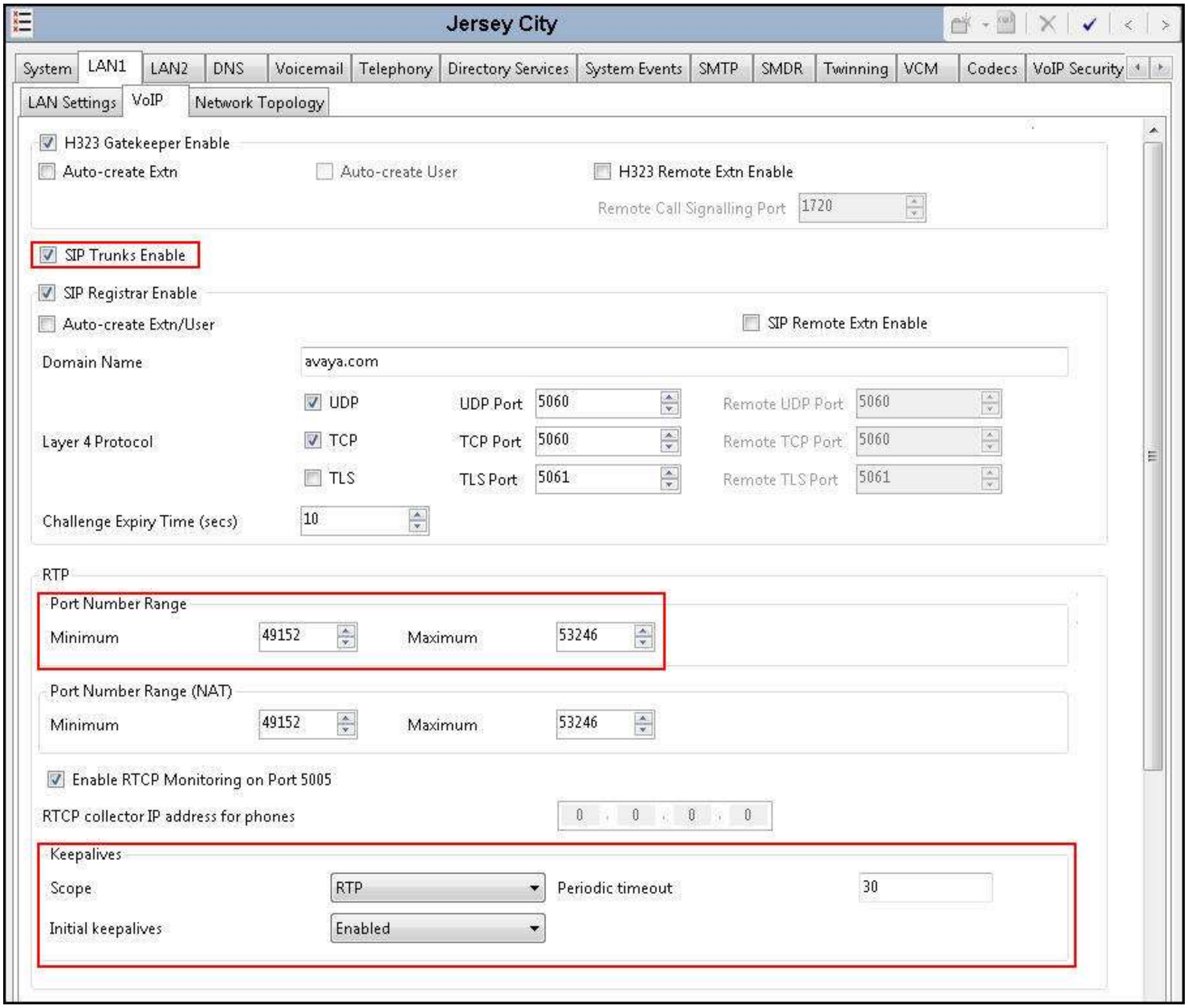
□ Enable NAT

Number Of DHCP IP Addresses: 200

DHCP Mode: ○ Server ○ Client ○ Dialin ● Disabled

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.



☑ H323 Gatekeeper Enable

☐ Auto-create Extn ☐ Auto-create User ☐ H323 Remote Extn Enable

Remote Call Signalling Port 1720

☑ SIP Trunks Enable

☑ SIP Registrar Enable

☐ Auto-create Extn/User ☐ SIP Remote Extn Enable

Domain Name avaya.com

Layer 4 Protocol

☑ UDP	UDP Port	5060	Remote UDP Port	5060
☑ TCP	TCP Port	5060	Remote TCP Port	5060
☐ TLS	TLS Port	5061	Remote TLS Port	5061

Challenge Expiry Time (secs) 10

RTP

Port Number Range

Minimum 49152 Maximum 53246

Port Number Range (NAT)

Minimum 49152 Maximum 53246

☑ Enable RTCP Monitoring on Port 5005

RTCP collector IP address for phones 0 . 0 . 0 . 0

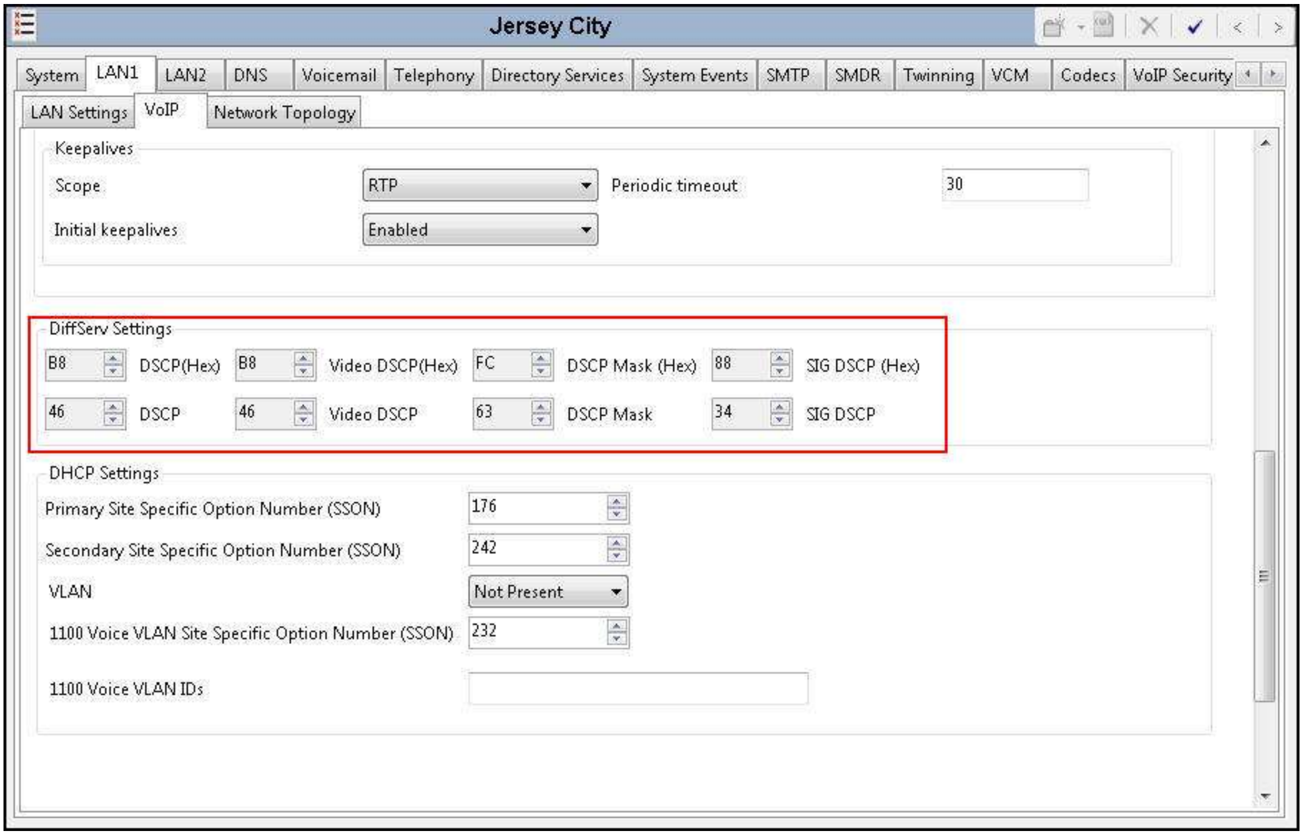
Keepalives

Scope RTP Periodic timeout 30

Initial keepalives Enabled

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.



Keepalives

Scope: RTP
Periodic timeout: 30
Initial keepalives: Enabled

DiffServ Settings

B8 DSCP(Hex) B8 Video DSCP(Hex) FC DSCP Mask (Hex) 88 SIG DSCP (Hex)

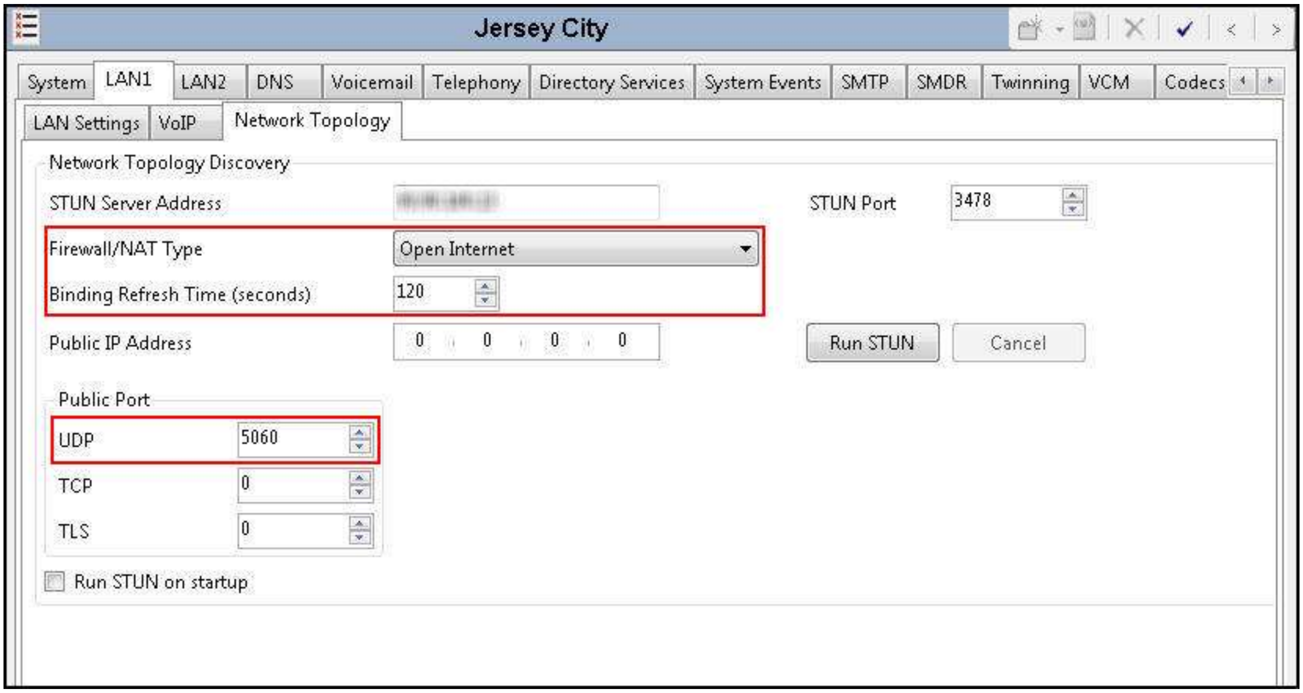
46 DSCP 46 Video DSCP 63 DSCP Mask 34 SIG DSCP

DHCP Settings

Primary Site Specific Option Number (SSON): 176
Secondary Site Specific Option Number (SSON): 242
VLAN: Not Present
1100 Voice VLAN Site Specific Option Number (SSON): 232
1100 Voice VLAN IDs:

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**.



Network Topology Discovery

STUN Server Address [redacted]

STUN Port 3478

Firewall/NAT Type Open Internet

Binding Refresh Time (seconds) 120

Public IP Address 0 . 0 . 0 . 0

Public Port

UDP 5060

TCP 0

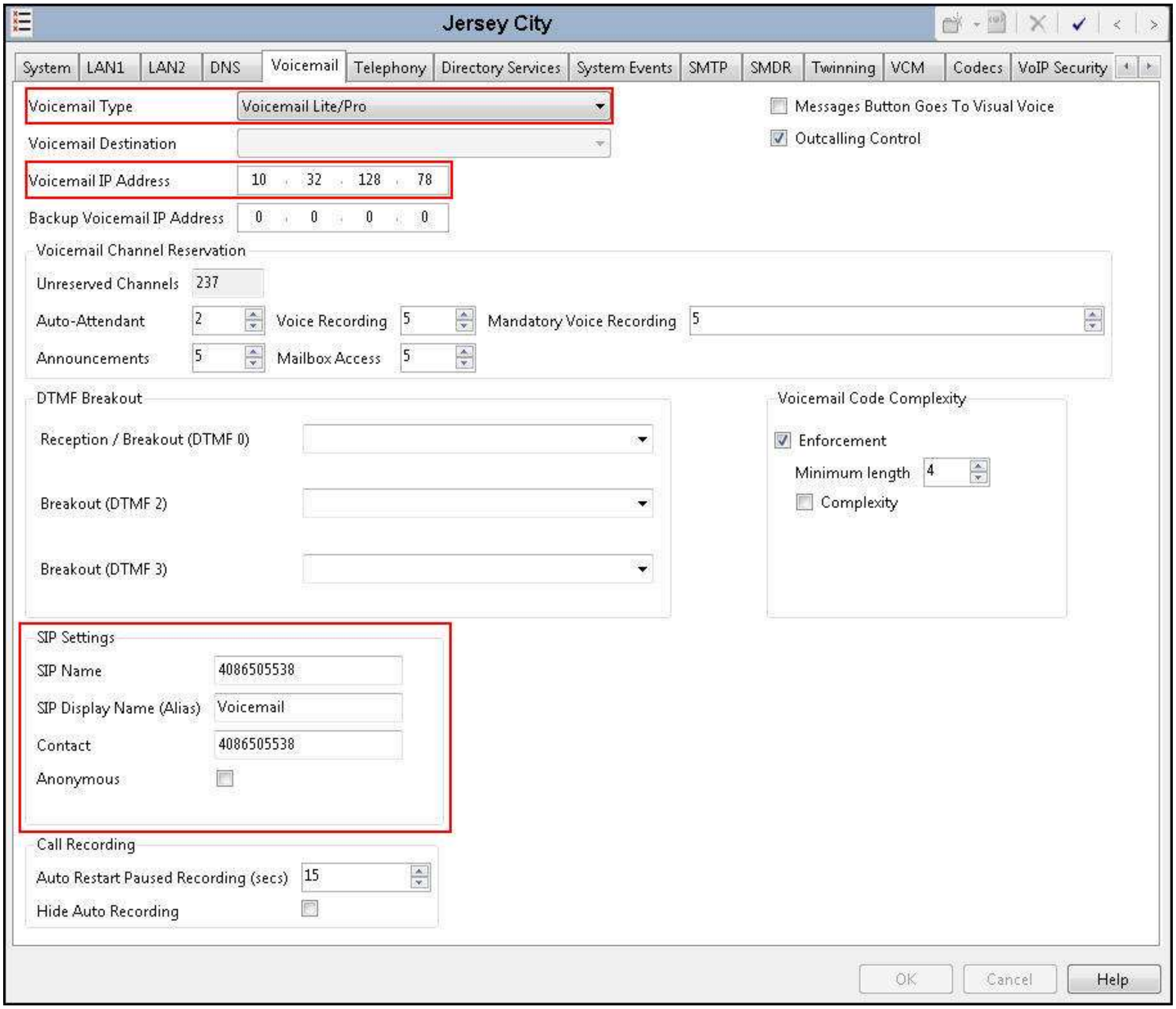
TLS 0

□ Run STUN on startup

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 Clearfly. 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).



Voicemail Type: Voicemail Lite/Pro
Voicemail Destination:
Voicemail IP Address: 10 . 32 . 128 . 78
Backup Voicemail IP Address: 0 . 0 . 0 . 0

□ Messages Button Goes To Visual Voice
☑ Outcalling Control

Voicemail Channel Reservation
Unreserved Channels: 237
Auto-Attendant: 2
Voice Recording: 5
Mandatory Voice Recording: 5
Announcements: 5
Mailbox Access: 5

DTMF Breakout
Reception / Breakout (DTMF 0):
Breakout (DTMF 2):
Breakout (DTMF 3):

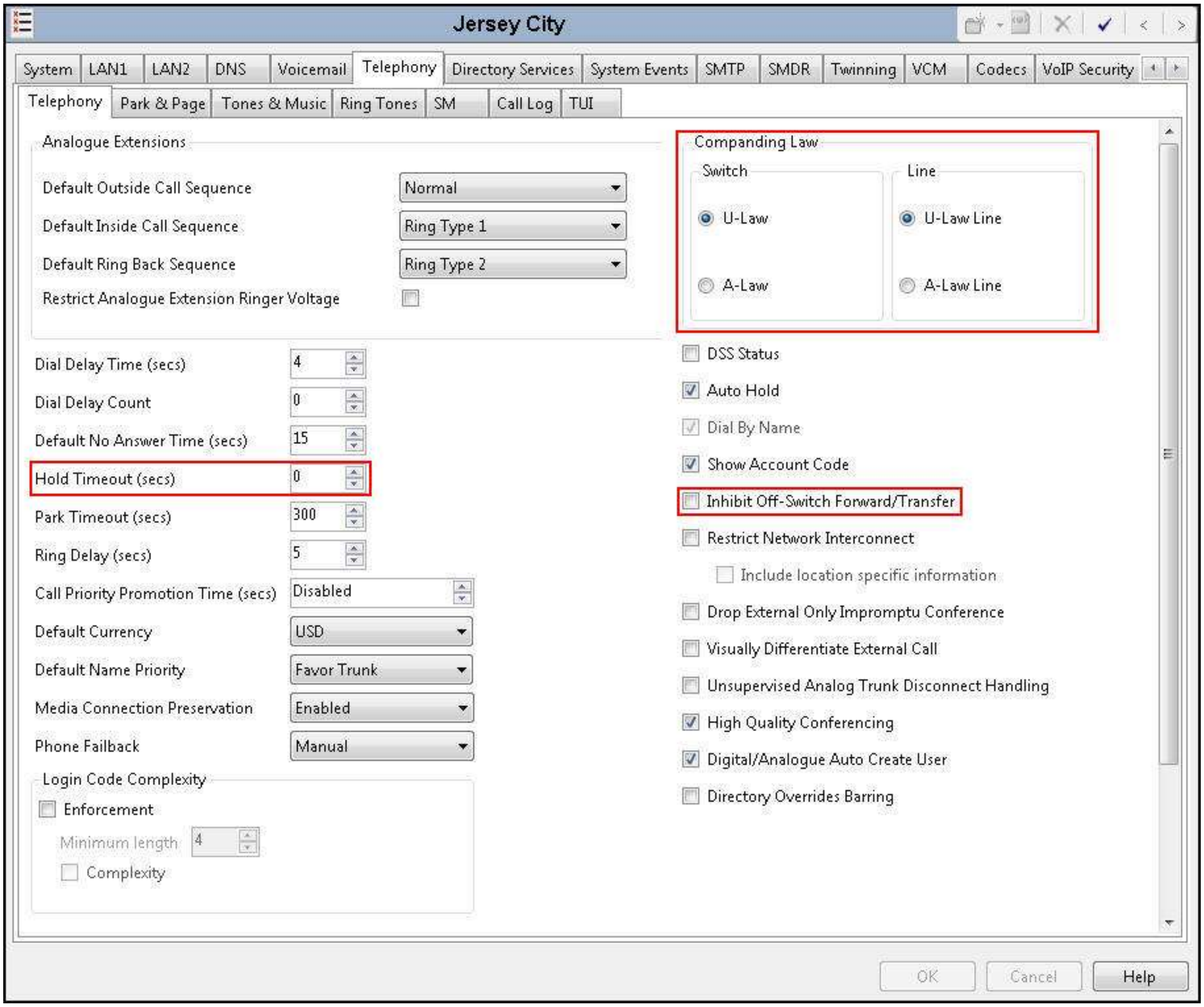
Voicemail Code Complexity
☑ Enforcement
Minimum length: 4
□ Complexity

SIP Settings
SIP Name: 4086505538
SIP Display Name (Alias): Voicemail
Contact: 4086505538
Anonymous: □

Call Recording
Auto Restart Paused Recording (secs): 15
Hide Auto Recording: □

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.



Jersey City

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | Twinning | VCM | Codecs | VoIP Security
Telephony | Park & Page | Tones & Music | Ring Tones | SM | Call Log | TUI

Analogue Extensions

Default Outside Call Sequence	Normal
Default Inside Call Sequence	Ring Type 1
Default Ring Back Sequence	Ring Type 2
Restrict Analogue Extension Ringer Voltage	□

Dial Delay Time (secs)	4
Dial Delay Count	0
Default No Answer Time (secs)	15
Hold Timeout (secs)	0
Park Timeout (secs)	300
Ring Delay (secs)	5
Call Priority Promotion Time (secs)	Disabled
Default Currency	USD
Default Name Priority	Favor Trunk
Media Connection Preservation	Enabled
Phone Failback	Manual

Login Code Complexity

□ Enforcement

Minimum length 4

□ Complexity

Companding Law

Switch: ● U-Law ○ A-Law

Line: ● U-Law Line ○ A-Law Line

□ DSS Status

☑ Auto Hold

☑ Dial By Name

☑ Show Account Code

□ Inhibit Off-Switch Forward/Transfer

□ Restrict Network Interconnect

□ Include location specific information

□ Drop External Only Impromptu Conference

□ Visually Differentiate External Call

□ Unsupervised Analog Trunk Disconnect Handling

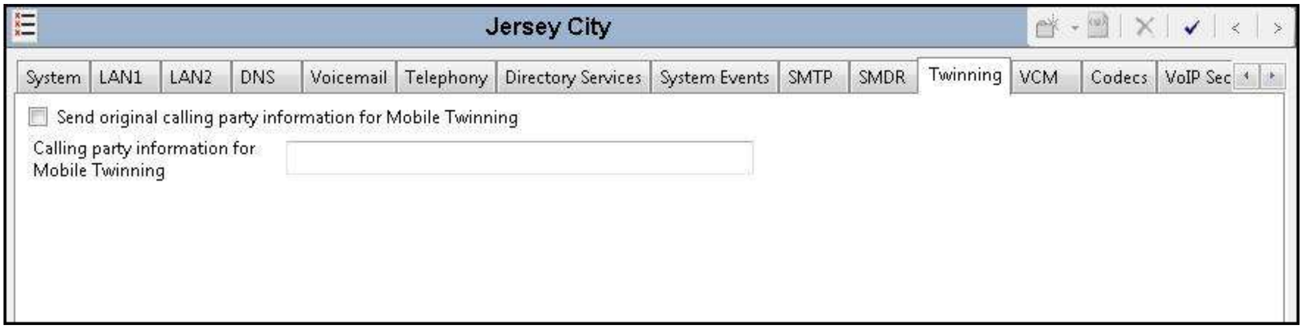
☑ High Quality Conferencing

☑ Digital/Analogue Auto Create User

□ Directory Overrides Barring

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.



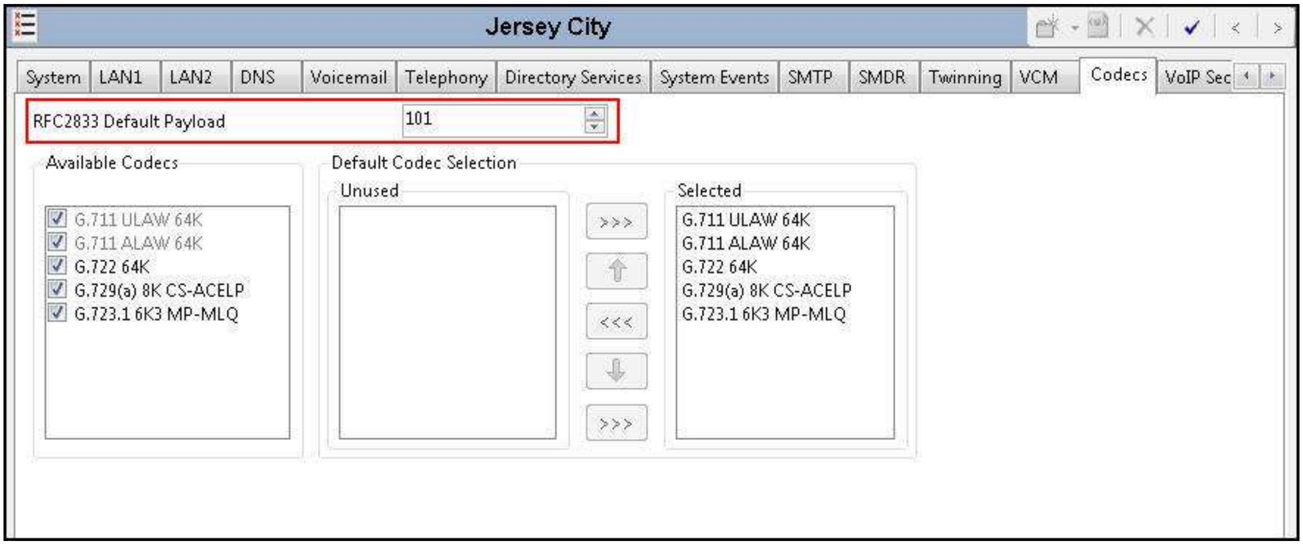
□ Send original calling party information for Mobile Twinning

Calling party information for Mobile Twinning

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 Clearfly 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 to be configured 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.



RFC2833 Default Payload: 101

Available Codecs
- ☑ G.711 ULAW 64K
- ☑ G.711 ALAW 64K
- ☑ G.722 64K
- ☑ G.729(a) 8K CS-ACELP
- ☑ G.723.1 6K3 MP-MLQ

Default Codec Selection

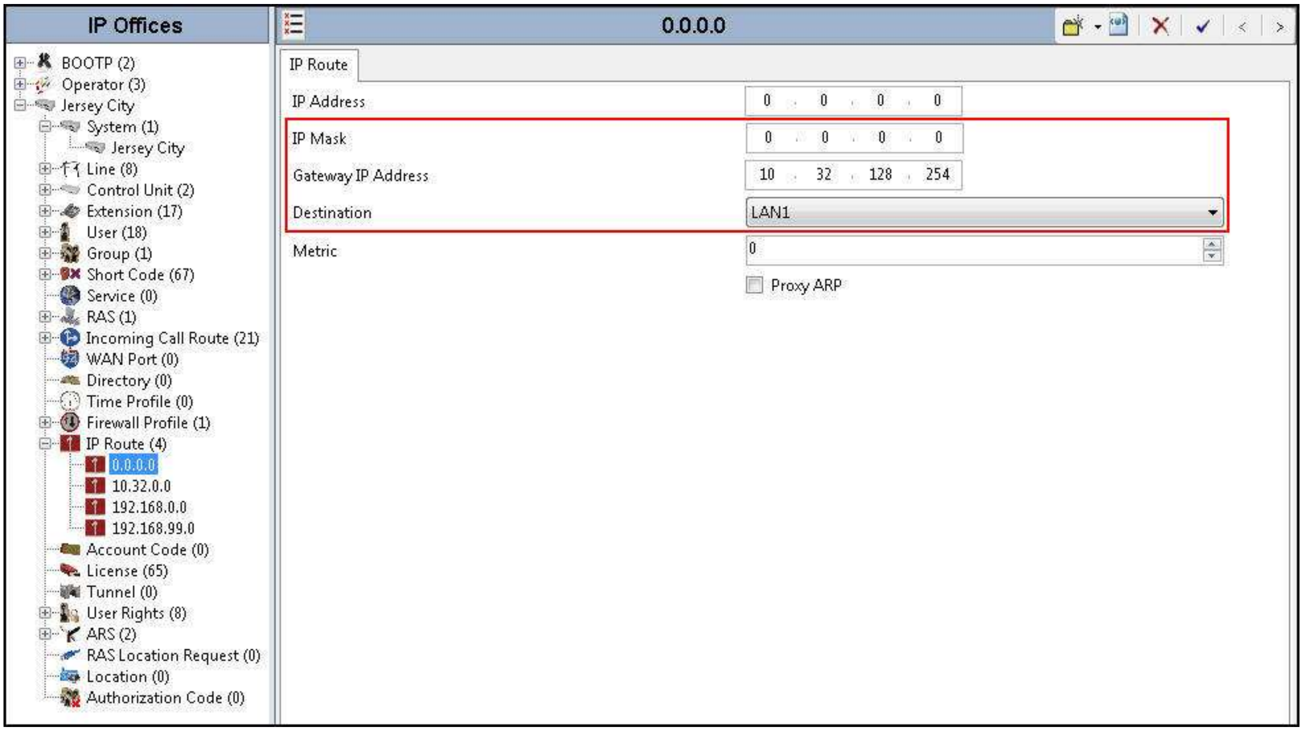
Unused

Selected
- G.711 ULAW 64K
- G.711 ALAW 64K
- G.722 64K
- G.729(a) 8K CS-ACELP
- G.723.1 6K3 MP-MLQ

5.3. IP Route

Navigate to **IP Route → 0.0.0.0** in the left Navigation Pane if a default route already exists. Otherwise, to create the default route, right-click 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.



IP Address: 0 . 0 . 0 . 0
IP Mask: 0 . 0 . 0 . 0
Gateway IP Address: 10 . 32 . 128 . 254
Destination: LAN1
Metric: 0
□ Proxy ARP

5.4. Administer SIP Line

A SIP Line is needed to establish the SIP connection between Avaya IP Office and the Clearfly 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 (500v2) 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 data 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.

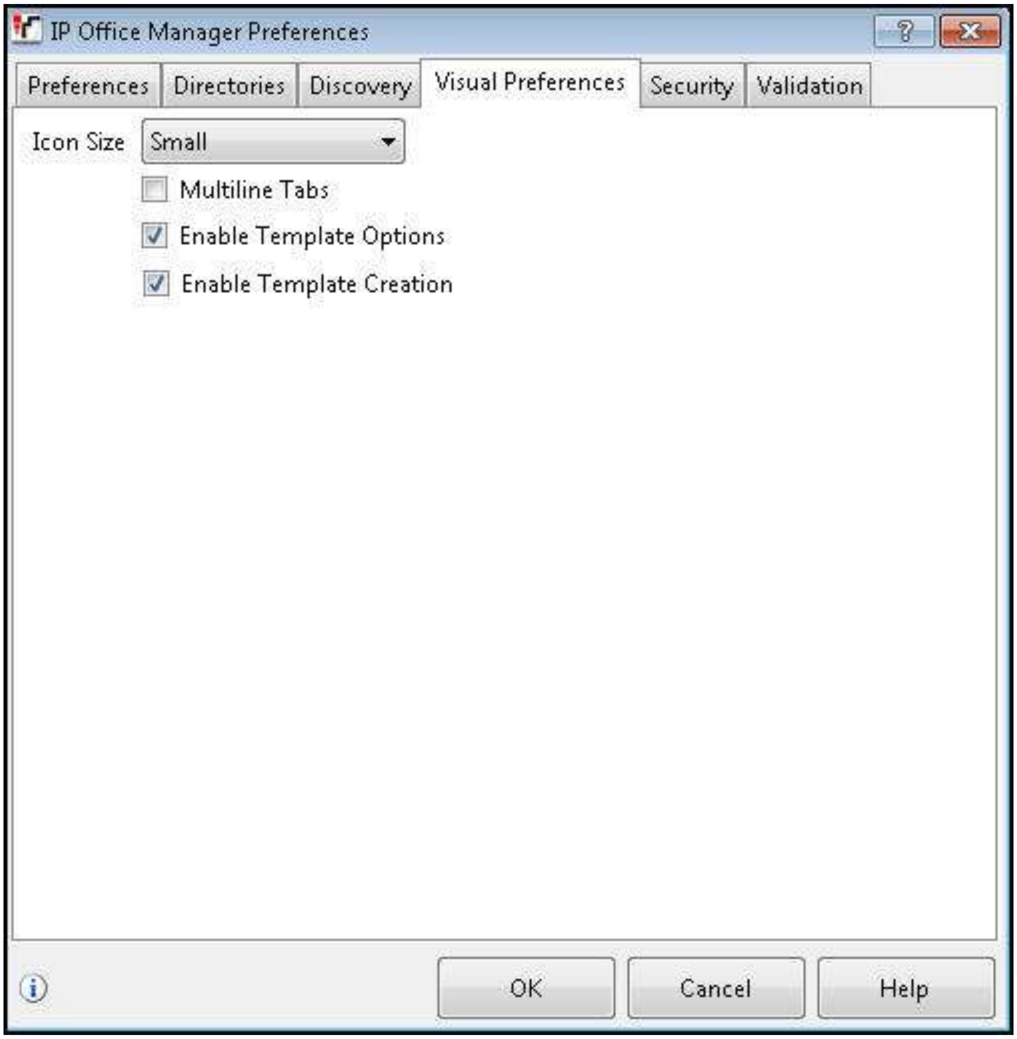
5.4.1. Create SIP Line From Template

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

   AF_Clearfly Communications_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**.



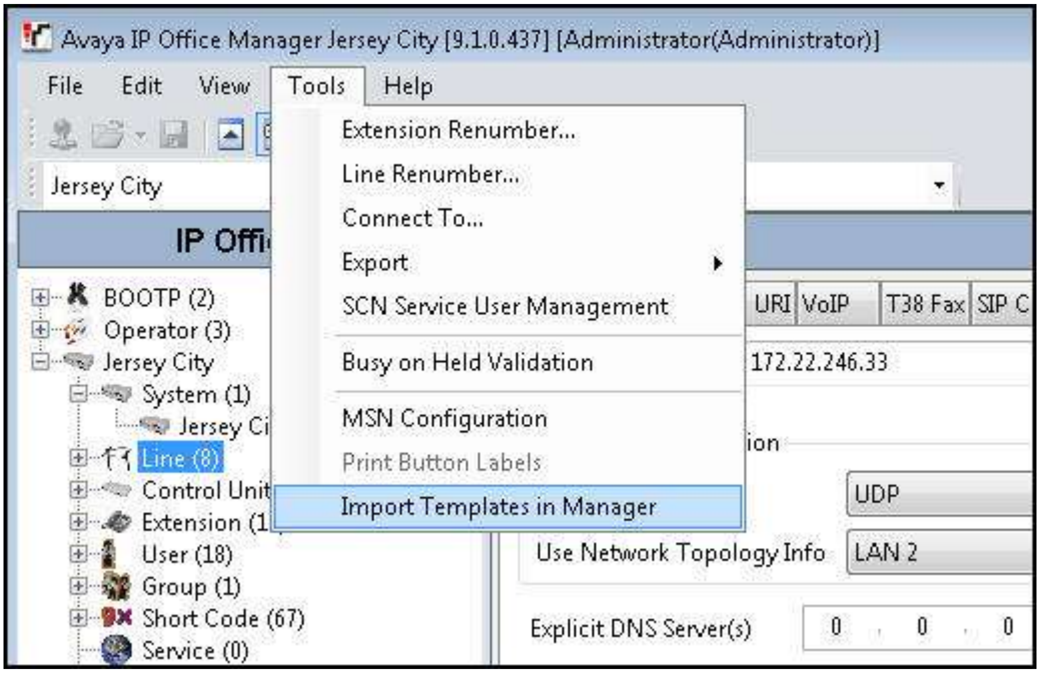
Icon Size: Small

□ Multiline Tabs

☑ Enable Template Options

☑ Enable Template Creation

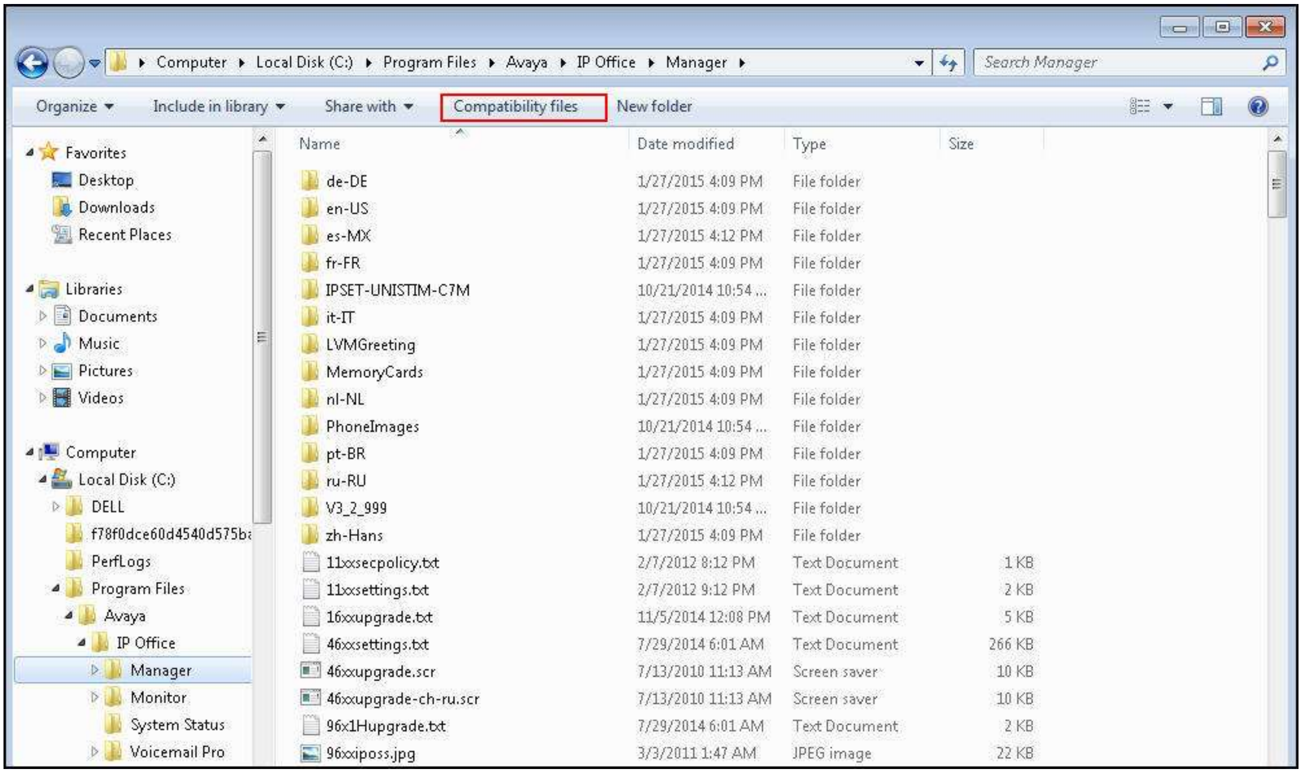
3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 4**. The default template 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.

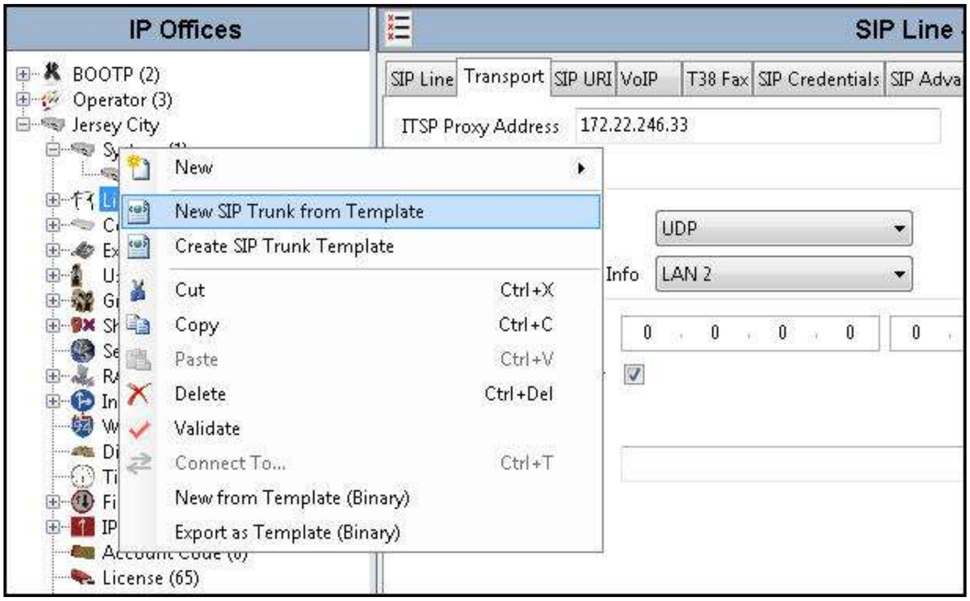
If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

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.



Name	Date modified	Type	Size
de-DE	1/27/2015 4:09 PM	File folder	
en-US	1/27/2015 4:09 PM	File folder	
es-MX	1/27/2015 4:12 PM	File folder	
fr-FR	1/27/2015 4:09 PM	File folder	
IPSET-UNISTIM-C7M	10/21/2014 10:54 ...	File folder	
it-IT	1/27/2015 4:09 PM	File folder	
LVMGreeting	1/27/2015 4:09 PM	File folder	
MemoryCards	1/27/2015 4:09 PM	File folder	
nl-NL	1/27/2015 4:09 PM	File folder	
PhoneImages	10/21/2014 10:54 ...	File folder	
pt-BR	1/27/2015 4:09 PM	File folder	
ru-RU	1/27/2015 4:12 PM	File folder	
V3_2_999	10/21/2014 10:54 ...	File folder	
zh-Hans	1/27/2015 4:09 PM	File folder	
11xxsecpolicy.txt	2/7/2012 8:12 PM	Text Document	1 KB
11xxsettings.txt	2/7/2012 9:12 PM	Text Document	2 KB
16xxupgrade.txt	11/5/2014 12:08 PM	Text Document	5 KB
46xxsettings.txt	7/29/2014 6:01 AM	Text Document	266 KB
46xxupgrade.scr	7/13/2010 11:13 AM	Screen saver	10 KB
46xxupgrade-ch-ru.scr	7/13/2010 11:13 AM	Screen saver	10 KB
96x1Hupgrade.txt	7/29/2014 6:01 AM	Text Document	2 KB
96xxiposs.jpg	3/3/2011 1:47 AM	JPEG image	22 KB

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



ITSP Proxy Address 172.22.246.33

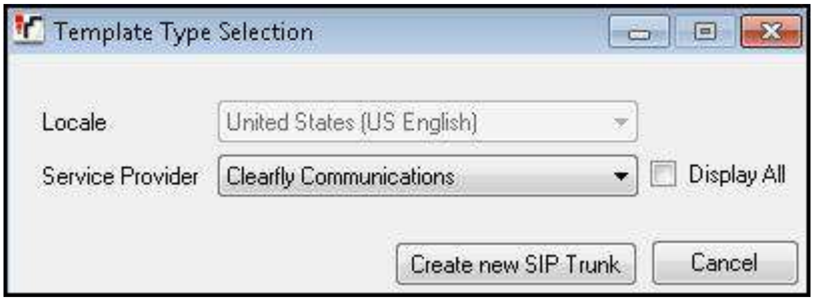
UDP

Info LAN 2

0 . 0 . 0 . 0

☑

In the subsequent **Template Type Selection** pop-up window, select ***Clearfly Communications*** 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.



Locale: United States (US English)

Service Provider: Clearfly Communications

□ Display All

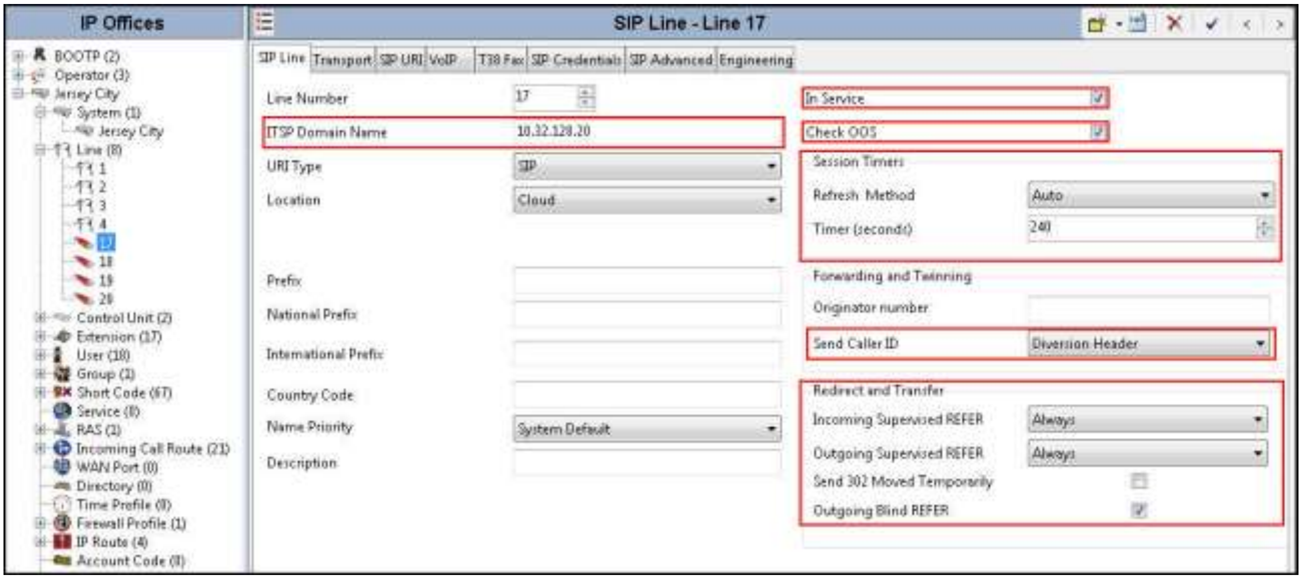
Note that the newly created SIP Line may not immediately appear in the Navigation pane until the configuration was saved, closed and reopened in IP Office Manager.

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**.

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 IP address of the internal signaling interface of the Avaya SBCE.
- 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 ***Always*** for **Incoming Supervised REFER** and **Outgoing Supervised REFER**. Clearfly supports use of the REFER method for supervised off-net call transfer. **Outgoing Blind REFER** is checked to enable use of REFER for blind transfers as well.



Line Number: 17
ITSP Domain Name: 10.32.128.20
URI Type: SIP
Location: Cloud
Prefix:
National Prefix:
International Prefix:
Country Code:
Name Priority: System Default
Description:

In Service ☑
Check OOS ☑

Session Timers
Refresh Method: Auto
Timer (seconds): 240

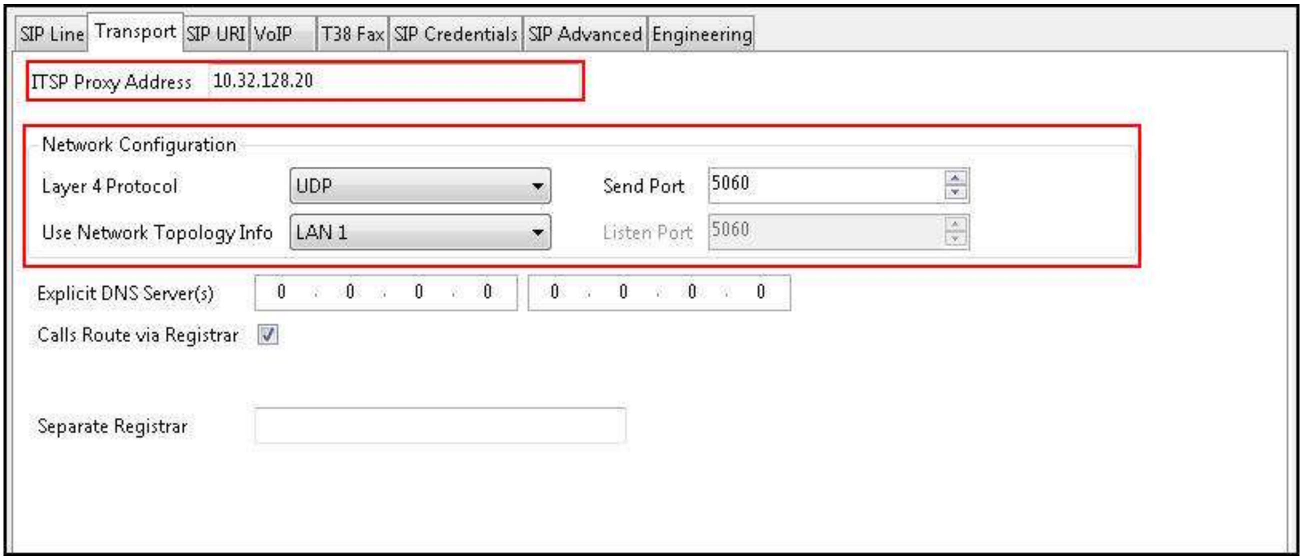
Forwarding and Twinning
Originator number:
Send Caller ID: Diversion Header

Redirect and Transfer
Incoming Supervised REFER: Always
Outgoing Supervised REFER: Always
Send 302 Moved Temporarily ☐
Outgoing Blind REFER ☑

5.4.3. 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***.



ITSP Proxy Address 10.32.128.20

Network Configuration

Layer 4 Protocol: UDP

Send Port: 5060

Use Network Topology Info: LAN 1

Listen Port: 5060

Explicit DNS Server(s): 0 . 0 . 0 . 0   0 . 0 . 0 . 0

Calls Route via Registrar ☑

Separate Registrar

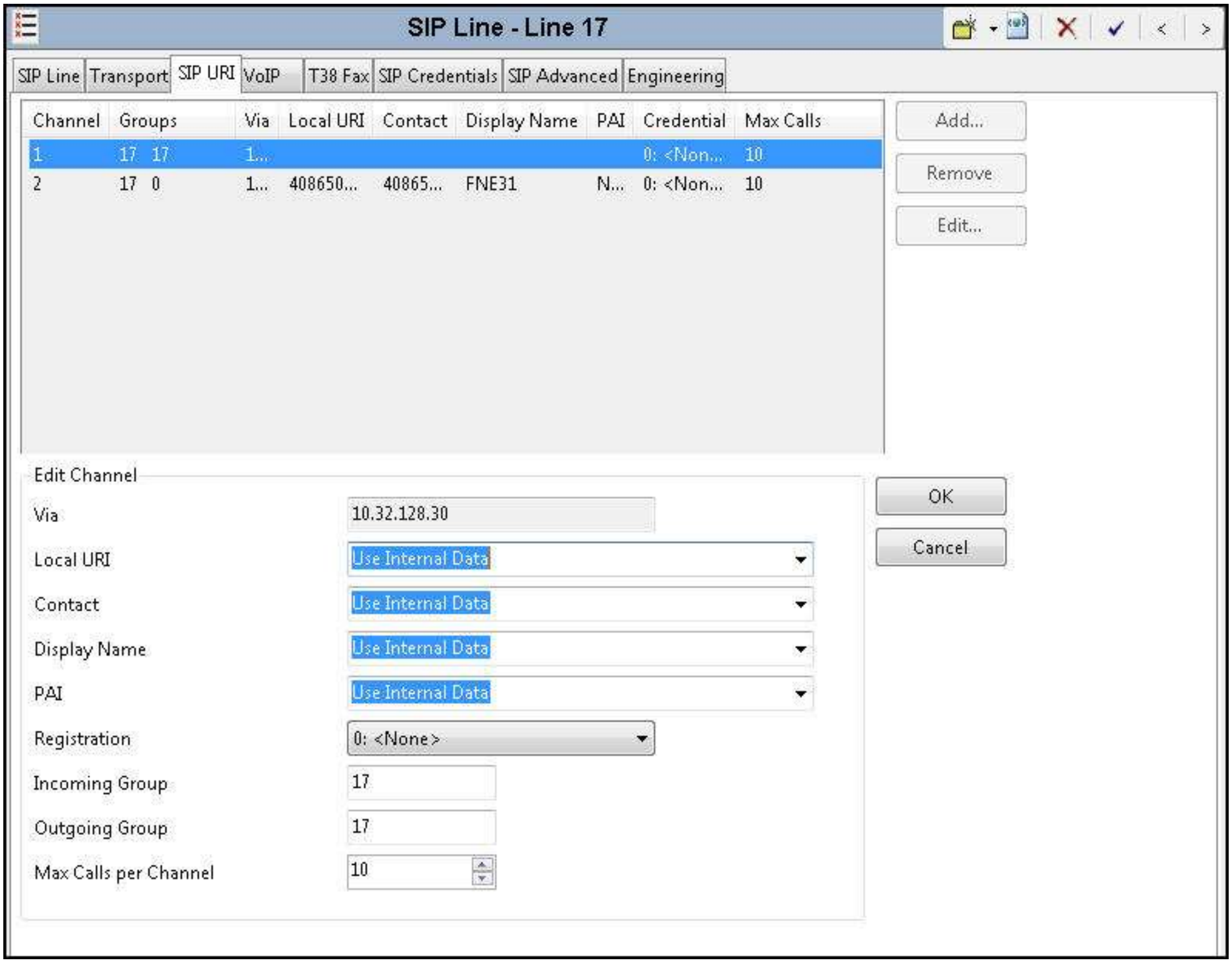
5.4.4. SIP Line – SIP URI Tab

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, a single SIP URI entry was created to match any DID number assigned to Avaya IP Office users. The following screen shows the edit window on this URI entry for the compliance test.

- 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**.
- Set **Contact** and **Display Name** to ***Use Internal Data***. This setting will cause the Contact and Display Name data for outbound messages to be set from the corresponding fields on the **SIP** tab of the individual **User** as shown in **Section 5.66**.
- Set **PAI** to ***Use Internal Data***. This setting directs Avaya IP Office to send the PAI (P-Asserted-Identity) header when appropriate. The PAI header will be populated from the data set in the **SIP** tab of the call initiating **User** as shown in **Section 5.66**.
- 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. Note that this group number can be different than the SIP Line number.

- Set **Max Calls per Channel** to the number of simultaneous SIP calls allowed using this SIP URI pattern.

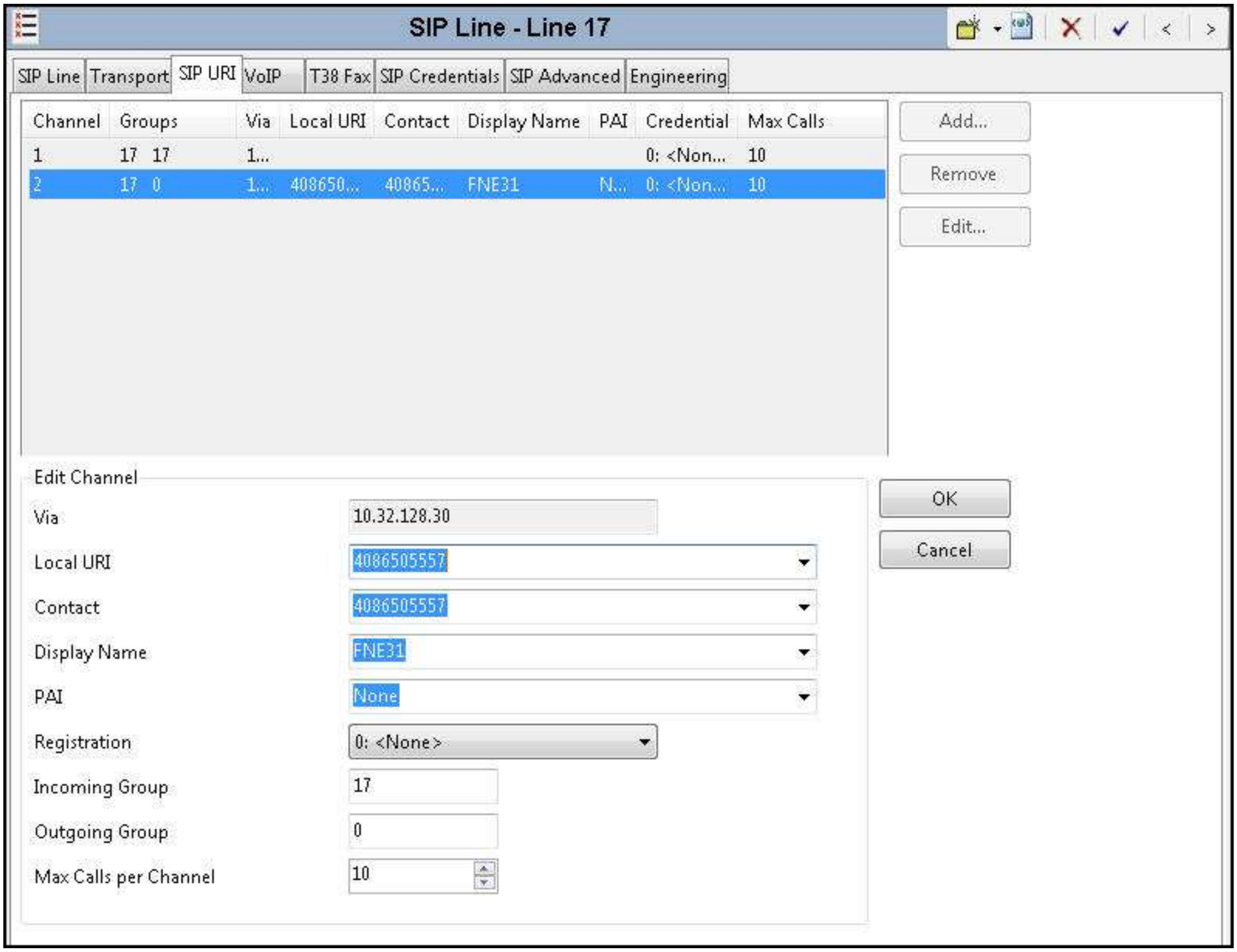


Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	17 17	1...					0: <Non...	10
2	17 0	1...	408650...	40865...	FNE31	N...	0: <Non...	10

Edit Channel

Via	10.32.128.30
Local URI	Use Internal Data
Contact	Use Internal Data
Display Name	Use Internal Data
PAI	Use Internal Data
Registration	0: <None>
Incoming Group	17
Outgoing Group	17
Max Calls per Channel	10

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**). The number ***4086505557*** 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.



Channel	Groups		Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	17	17	1...					0: <Non...	10
2	17	0	1...	408650...	40865...	FNE31	N...	0: <Non...	10

Edit Channel

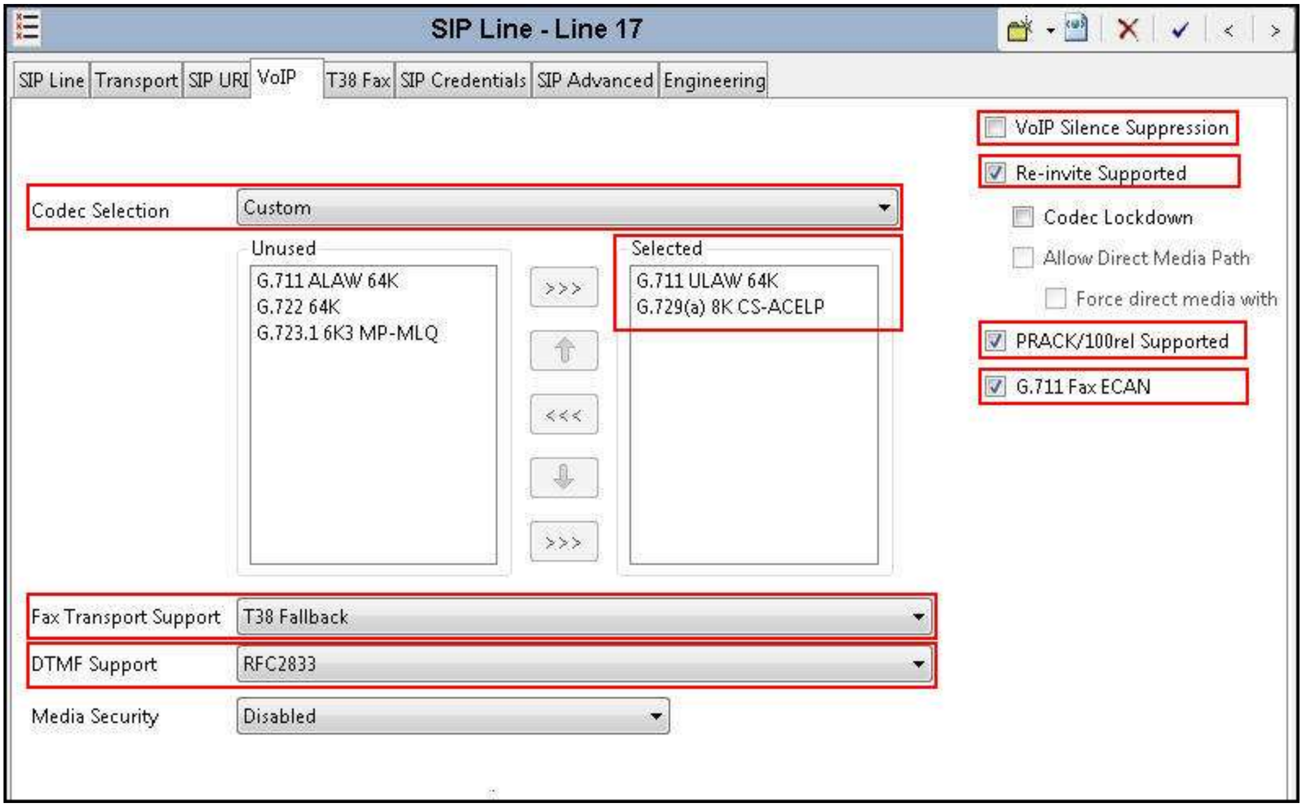
Via	10.32.128.30
Local URI	4086505557
Contact	4086505557
Display Name	FNE31
PAI	None
Registration	0: <None>
Incoming Group	17
Outgoing Group	0
Max Calls per Channel	10

Note that no line group number was configured for **Outgoing Group** for this SIP URI entry. This is because this SIP URI entry is used only for inbound calls to the Mobile Call Control application.

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*** and ***G.729(a) 8K CS-ACELP*** from the **Unused** box and move these two selections to the **Selected** box. Use the up and down arrows in the middle to order these 2 codes. The G.711u and G.729a codecs are supported by Clearfly. G.711u was configured as the preferred codec for the compliance test as shown below.
- Select ***T38 Fallback*** for **Fax Transport Support** to direct Avaya IP Office to use T.38 for fax calls and use G.711u pass-through for fax if the remote end does not support T.38.
- 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, reINVITE 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.
- Check **G.711 Fax ECAN**.



Codec Selection: Custom

Unused	Selected
G.711 ALAW 64K G.722 64K G.723.1 6K3 MP-MLQ	G.711 ULAW 64K G.729(a) 8K CS-ACELP

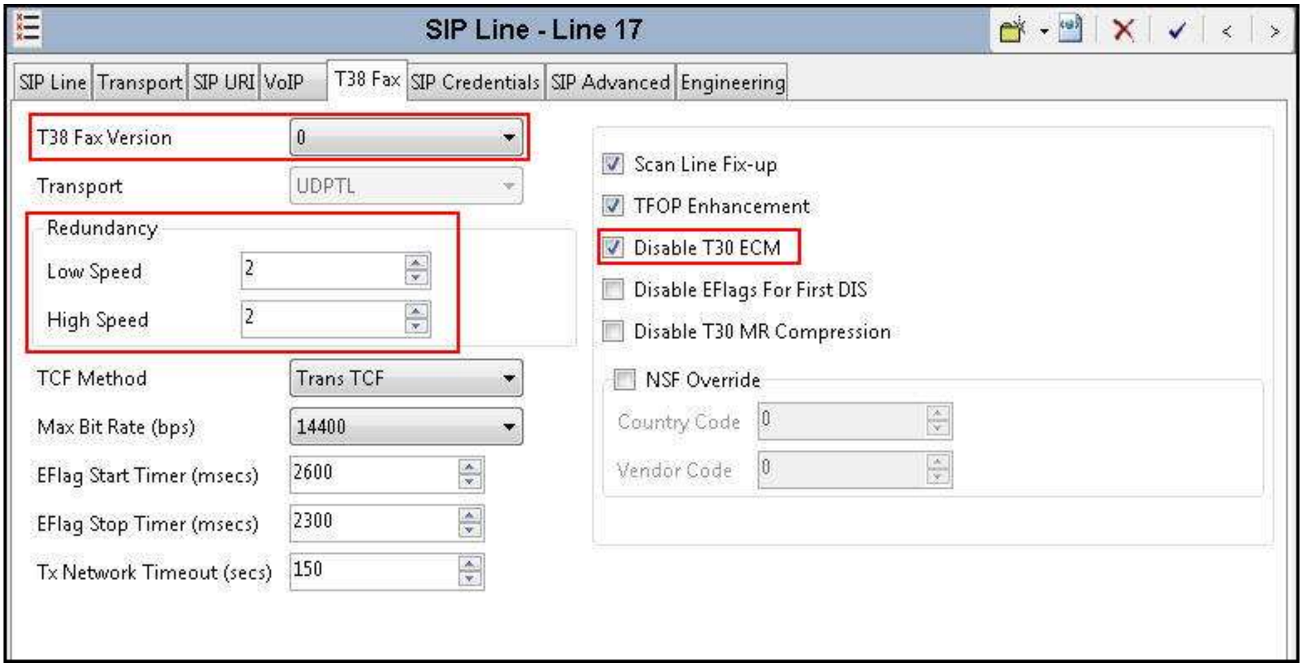
□ VoIP Silence Suppression
☑ Re-invite Supported
□ Codec Lockdown
□ Allow Direct Media Path
□ Force direct media with
☑ PRACK/100rel Supported
☑ G.711 Fax ECAN

Fax Transport Support: T38 Fallback
DTMF Support: RFC2833
Media Security: Disabled

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** must be checked or fax errors may be experienced when using T.38 Fax. When selected, it disables the T.30 Error Correction Mode used for fax transmission. All other values are left at default.



T38 Fax Version: 0

Transport: UDPTL

Redundancy

Low Speed: 2

High Speed: 2

TCF Method: Trans TCF

Max Bit Rate (bps): 14400

EFlag Start Timer (msecs): 2600

EFlag Stop Timer (msecs): 2300

Tx Network Timeout (secs): 150

☑ Scan Line Fix-up

☑ TFOP Enhancement

☑ Disable T30 ECM

☐ Disable EFlags For First DIS

☐ Disable T30 MR Compression

☐ NSF Override

Country Code: 0

Vendor Code: 0

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.

The Clearfly SIP Trunking Service does not require trunk registration or Digest Authentication for the compliance test. Therefore, this tab does not need to be visited.

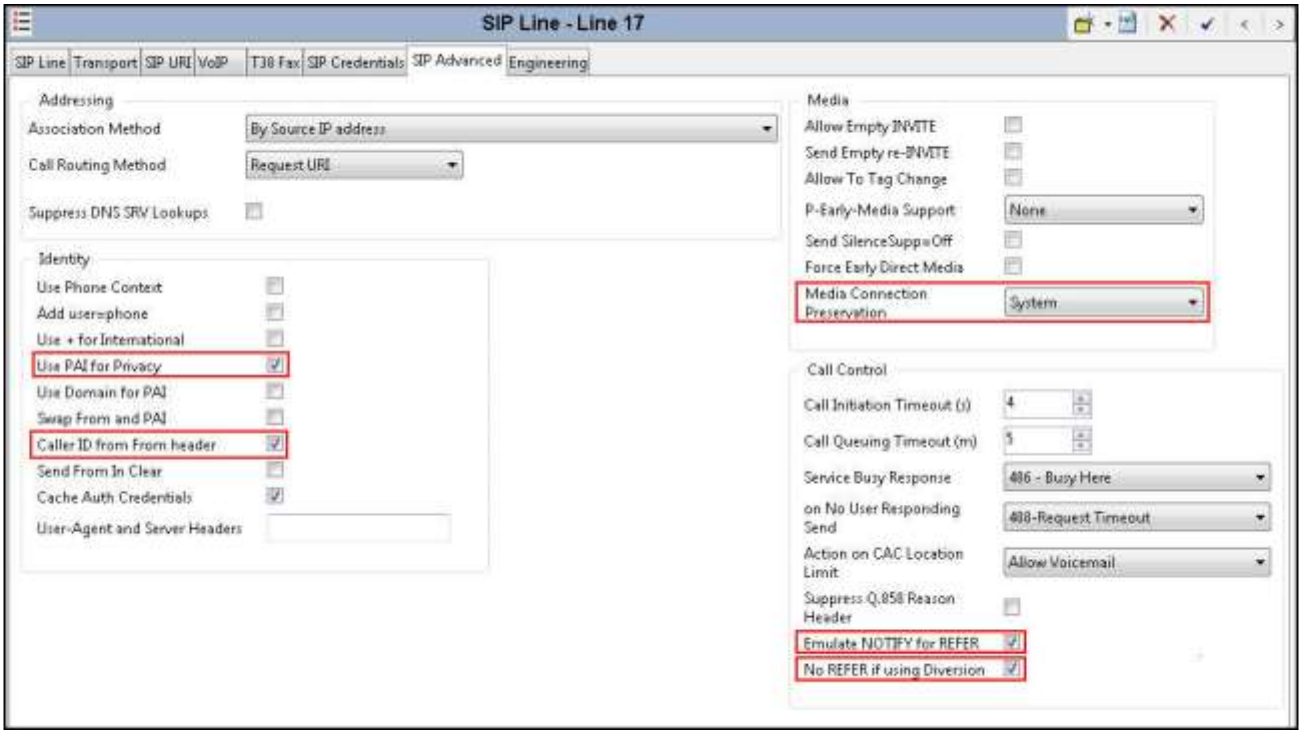
5.4.8. SIP Line – SIP Advanced Tab

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, **Emulate NOTIFY for REFER** is check. This is required for SIP endpoints that perform REFER-based transfers across the SIP line. **No REFER if using Diversion** is checked to prevent IP Office from using the SIP REFER method on call forward scenarios that use the Diversion SIP header.



Addressing

Association Method	By Source IP address
Call Routing Method	Request URI
Suppress DNS SRV Lookups	□

Identity

Use Phone Context	□
Add user=phone	□
Use + for International	□
Use PAI for Privacy	☑
Use Domain for PAI	□
Swap From and PAI	□
Caller ID from From header	☑
Send From In Clear	□
Cache Auth Credentials	☑
User-Agent and Server Headers	

Media

Allow Empty INVITE	□
Send Empty re-INVITE	□
Allow To Tag Change	□
P-Early-Media Support	None
Send SilenceSupp=Off	□
Force Early Direct Media	□
Media Connection Preservation	System

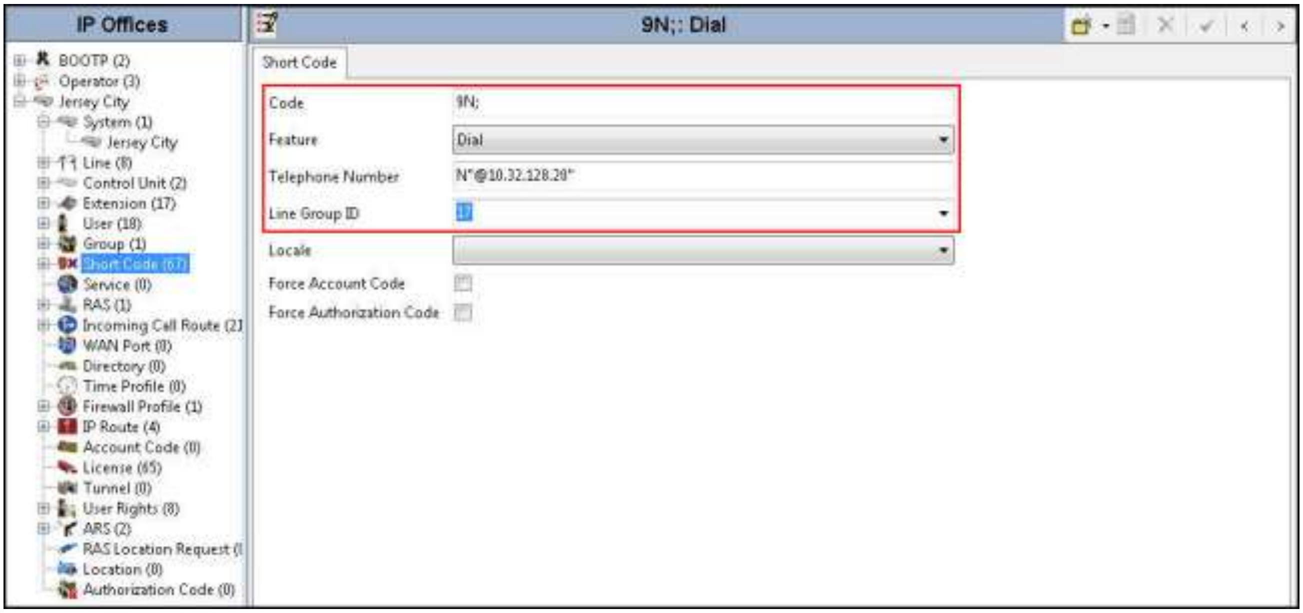
Call Control

Call Initiation Timeout (s)	4
Call Queuing Timeout (m)	5
Service Busy Response	486 - Busy Here
on No User Responding Send	408-Request Timeout
Action on CAC Location Limit	Allow Voicemail
Suppress Q.850 Reason Header	□
Emulate NOTIFY for REFER	☑
No REFER if using Diversion	☑

5.5. 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:

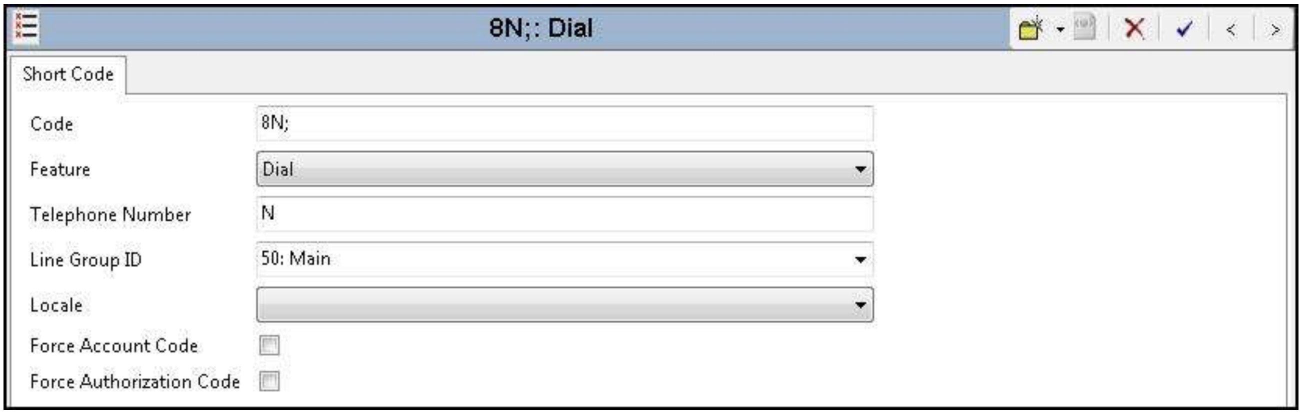
- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. The ***9N;*** short code, used for the compliance test, will be invoked when the user dials 9 followed by any number.
- Set **Feature** to ***Dial***. This is the action that the short code will perform.
- Set **Telephone Number** to ***N"@10.32.128.20"***. 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 IP address following the **@** sign is the IP address of the private interface of the Avaya SBCE.
- 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.



Code	9N;
Feature	Dial
Telephone Number	N"@10.32.128.20"
Line Group ID	17
Locale	
Force Account Code	□
Force Authorization Code	□

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.

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 example ARS route configuration.

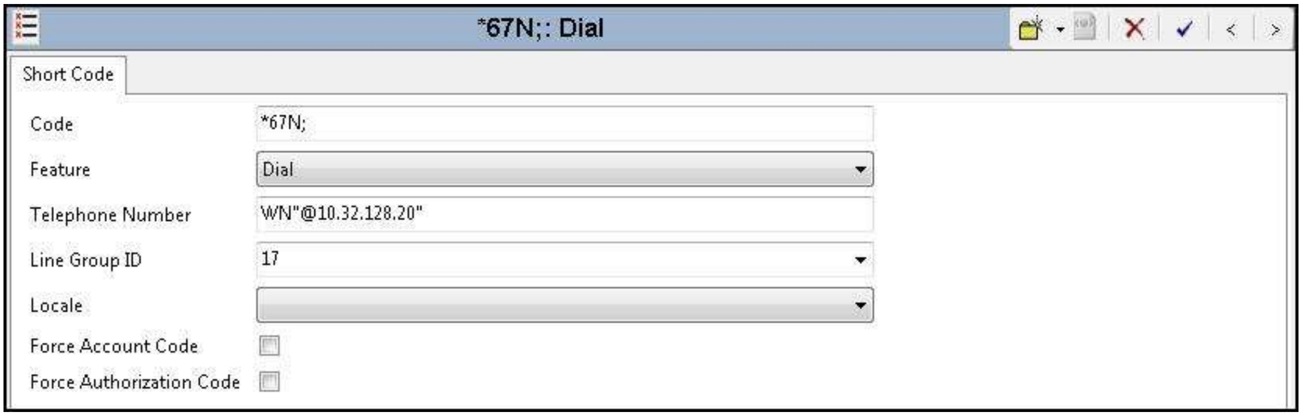


8N;: Dial

Short Code

Code	8N;
Feature	Dial
Telephone Number	N
Line Group ID	50: Main
Locale	
Force Account Code	□
Force Authorization Code	□

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 Clearfly would prevent presentation of the caller id to the called PSTN destination.

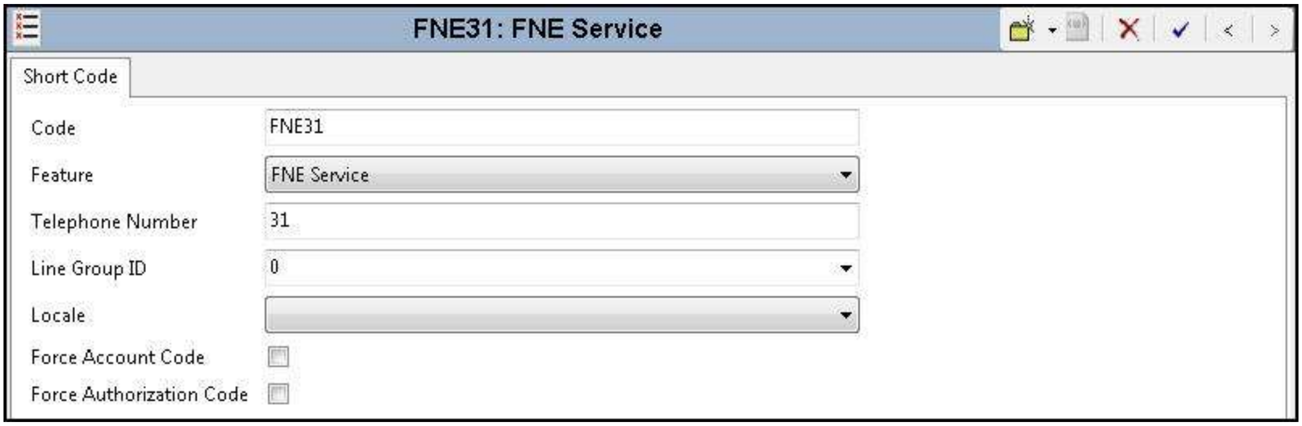


*67N;: Dial

Short Code

Code	*67N;
Feature	Dial
Telephone Number	WN"@10.32.128.20"
Line Group ID	17
Locale	
Force Account Code	□
Force Authorization Code	□

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.


FNE31: FNE Service

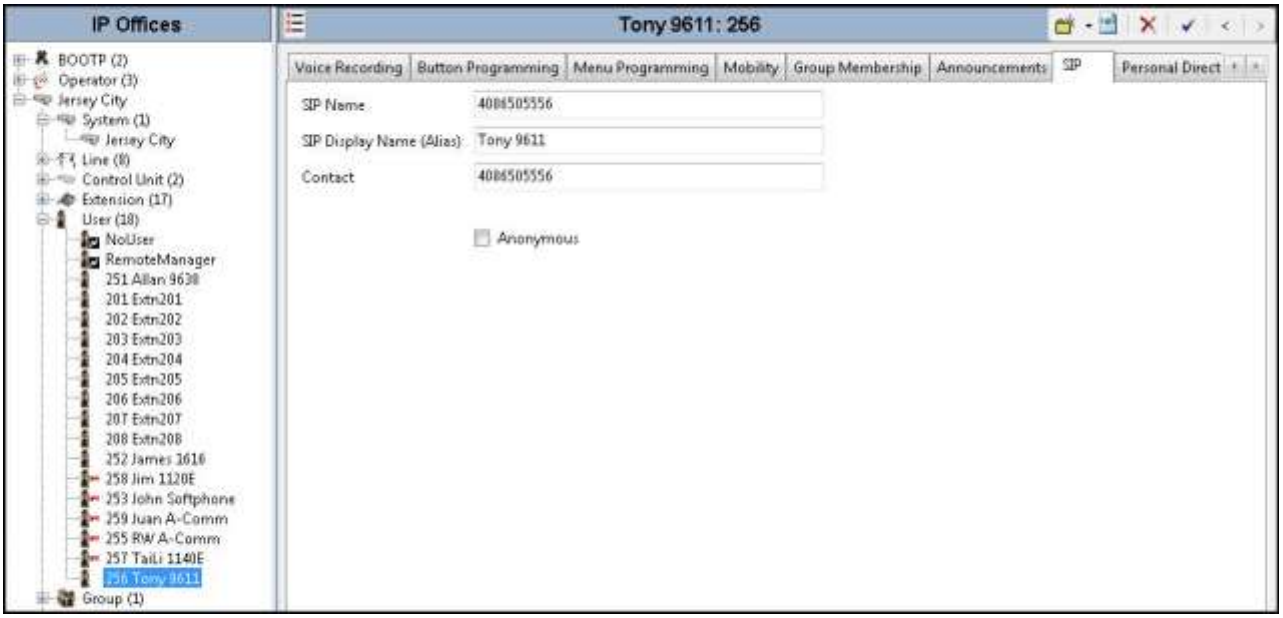
Short Code

Code	FNE31
Feature	FNE Service
Telephone Number	31
Line Group ID	0
Locale	
Force Account Code	□
Force Authorization Code	□

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 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 Clearfly. The **SIP Display Name (Alias)** can optionally be configured with a descriptive text string. The value entered for the **Contact** field will be used in the Contact header for outgoing SIP INVITE to the service provider. The value entered for the **SIP Name** is used as the user part of the SIP URI in the From header for outgoing SIP INVITE.

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**).



Tony 9611: 256

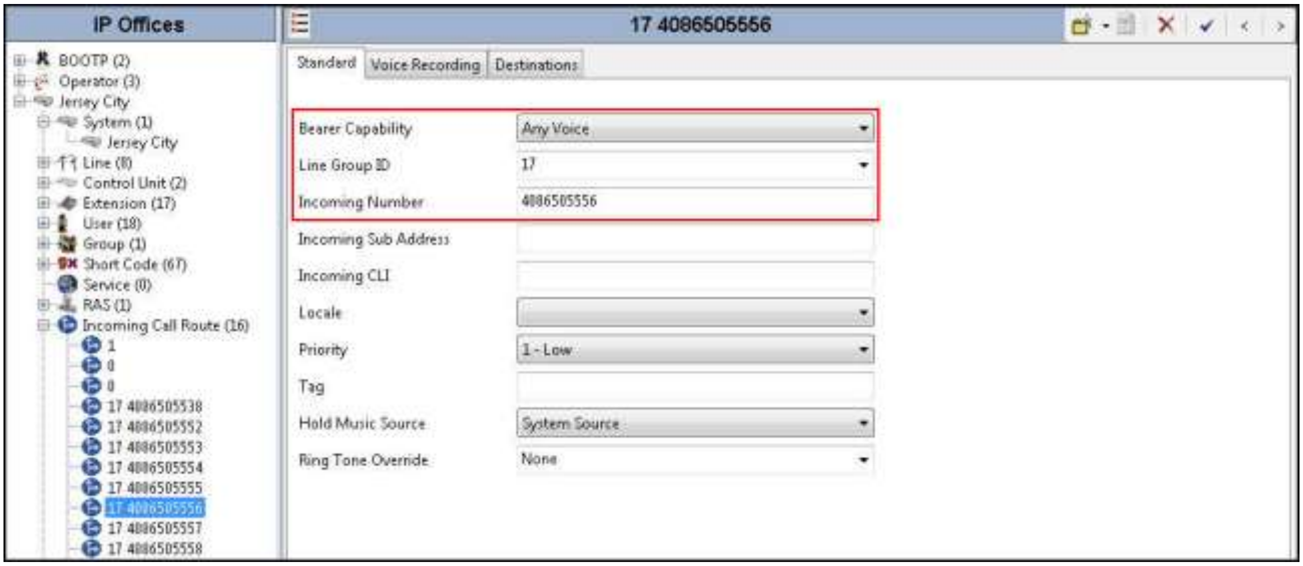
SIP Name	4086505556
SIP Display Name (Alias)	Tony 9611
Contact	4086505556

□ Anonymous

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 as shown below:

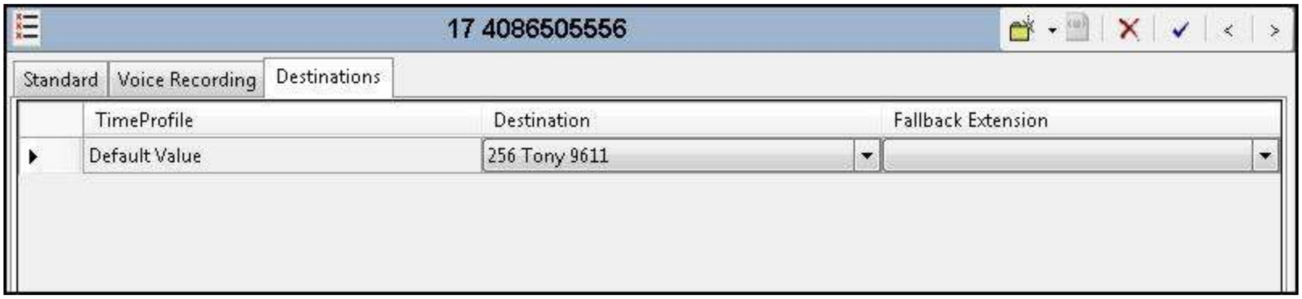
- Set the **Bearer Capacity** to ***Any Voice***.
- Set the **Line Group Id** to the **Incoming Group** of the SIP Line defined in **Section 5.4.4**.
- Set the **Incoming Number** to the incoming number on which this route should match.



17 4086505556

Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	4086505556
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

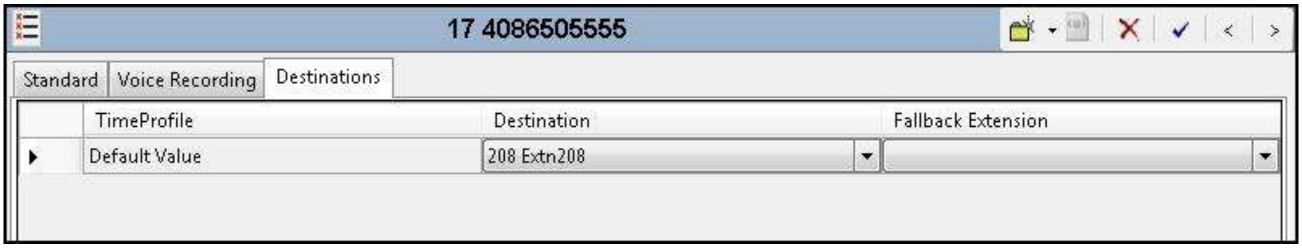
On the **Destinations** tab, select the destination from the pull-down list of the **Destination** field. In this example, incoming calls to 4086505556 on Incoming Group 17 are to be routed to the user "Tony 9611" at extension 256.



17 4086505556

TimeProfile	Destination	Fallback Extension
Default Value	256 Tony 9611	

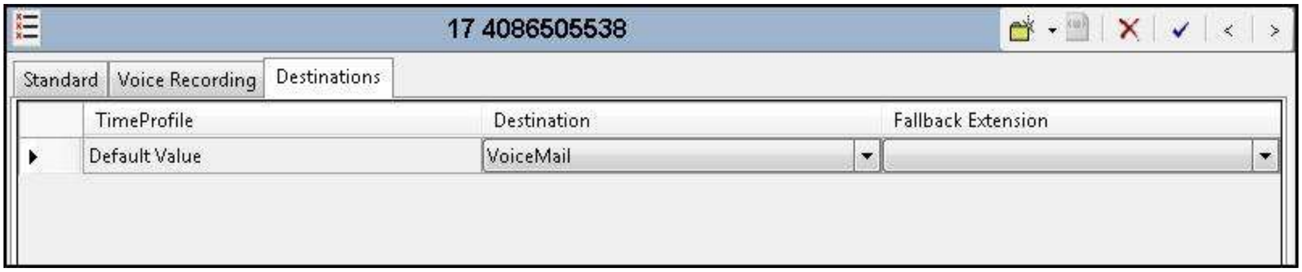
The screen below shows calls routed to the IP Office fax endpoint which is an analog extension (Extn 208).



17 4086505555

TimeProfile	Destination	Fallback Extension
Default Value	208 Extn208	

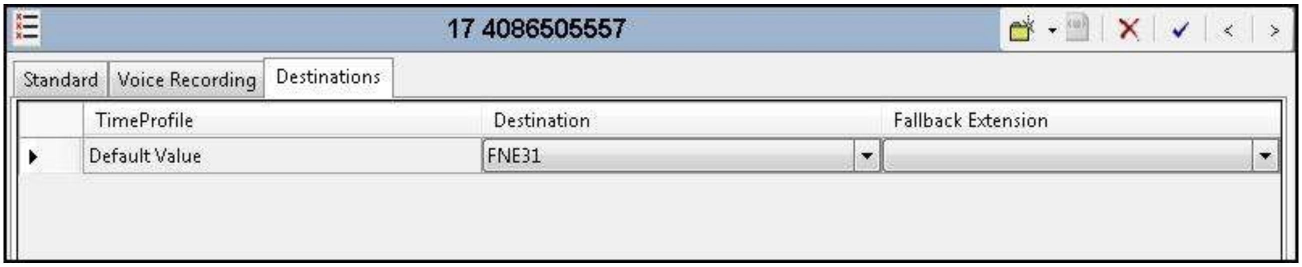
The screen below shows calls routed to IP Office Voicemail Pro for message retrieval. Note that the DID 4086505538 was assigned to Voicemail in **Section 5.2.2**.



17 4086505538

TimeProfile	Destination	Fallback Extension
Default Value	VoiceMail	

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 4086505557 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.



17 4086505557

TimeProfile	Destination	Fallback Extension
Default Value	FNE31	

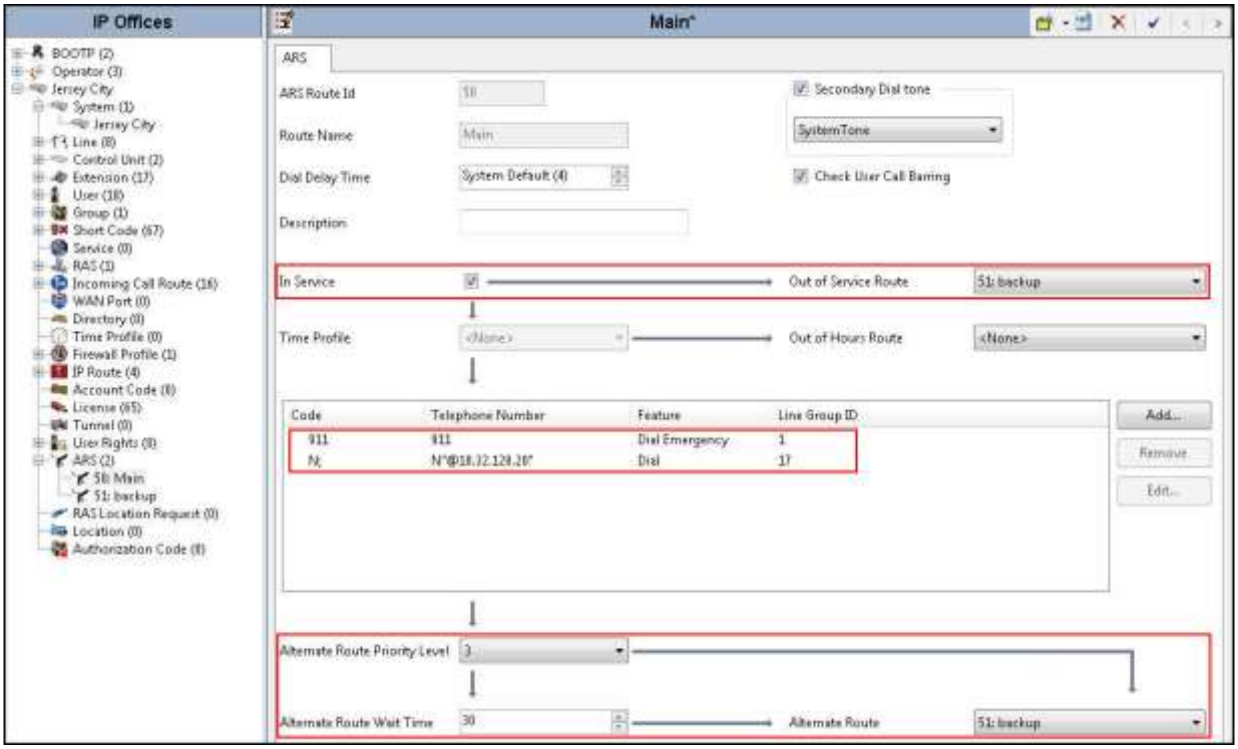
5.8. ARS and Alternate Routing

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. ARS is shown here mainly to illustrate alternate routing should the SIP Line be out of service or temporarily not responding.

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 an example 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.



ARS Route Id: 50
Route Name: Main
Dial Delay Time: System Default (4)
Description:
☑ Secondary Dial tone
SystemTone
☑ Check User Call Barring
In Service ☑ → Out of Service Route: 51: backup
Time Profile: <None> → Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
911	911	Dial Emergency	1
N;	N"@10.32.128.20"	Dial	17

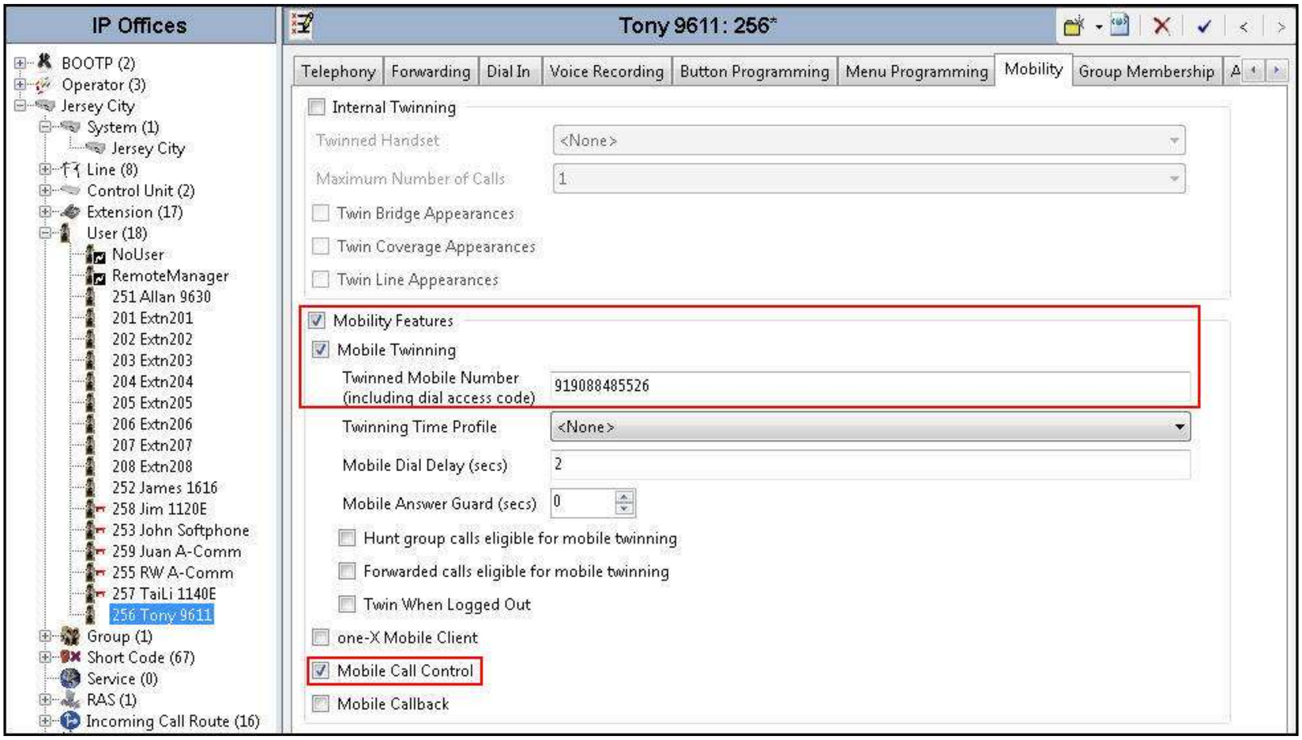
Alternate Route Priority Level: 3
Alternate Route Wait Time: 30 → Alternate Route: 51: backup

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 all 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.



Tony 9611: 256*

□ Internal Twinning
Twinned Handset: <None>
Maximum Number of Calls: 1
□ Twin Bridge Appearances
□ Twin Coverage Appearances
□ Twin Line Appearances
☑ Mobility Features
☑ Mobile Twinning
Twinned Mobile Number (including dial access code): 919088485526
Twinning Time Profile: <None>
Mobile Dial Delay (secs): 2
Mobile Answer Guard (secs): 0
□ Hunt group calls eligible for mobile twinning
□ Forwarded calls eligible for mobile twinning
□ Twin When Logged Out
□ one-X Mobile Client
☑ Mobile Call Control
□ Mobile Callback

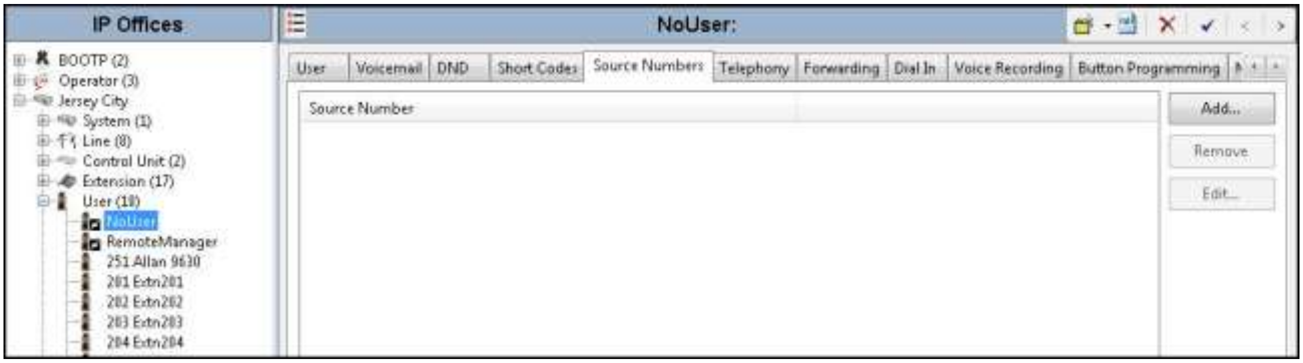
Note that when an inbound call is from the twinned mobile number to the Mobile Call Control application, the caller ID contained in the From header of the incoming INVITE must match the twinned mobile number (without the leading short code digit and the PSTN access code 1 for the North American Numbering Plan), otherwise the Avaya IP Office responds with a “486 Busy Here” message and the caller will hear busy tones.

5.10. SIP Options

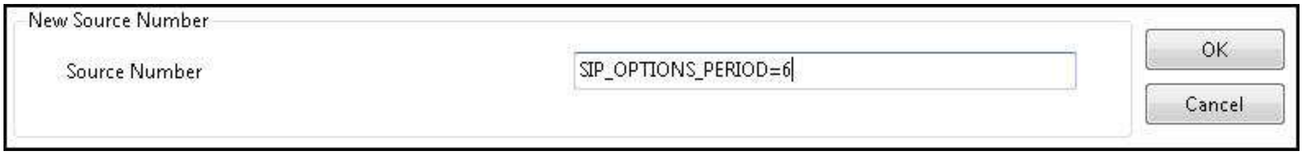
Avaya IP Office sends SIP OPTIONS messages periodically to determine if the SIP connection is active. By default, Avaya IP Office Release 9.1 sends out OPTIONS every 300 seconds. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time** (in seconds) set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

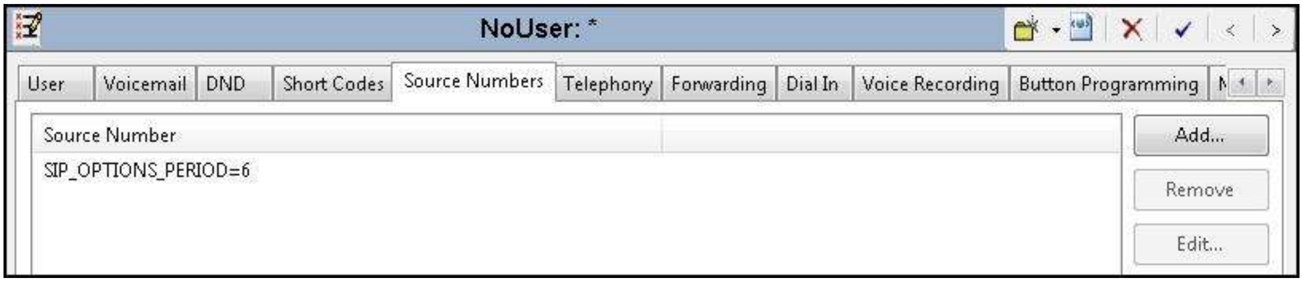


At the bottom of the Details Pane, the **Source Number** field will appear. Enter ***SIP_OPTIONS_PERIOD=X***, where ***X*** is the desired value in minutes. Click **OK**.


New Source Number

Source Number: SIP_OPTIONS_PERIOD=6

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).



NoUser: *

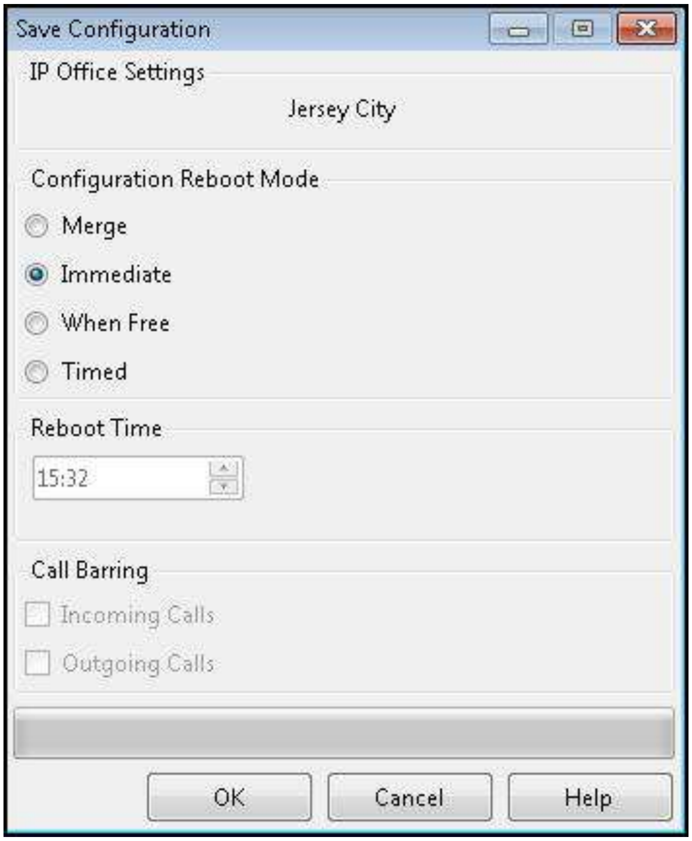
Source Number
SIP_OPTIONS_PERIOD=6

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.



Save Configuration

IP Office Settings

Jersey City

Configuration Reboot Mode

○ Merge

● Immediate

○ When Free

○ Timed

Reboot Time

15:32

Call Barring

□ Incoming Calls

□ Outgoing Calls

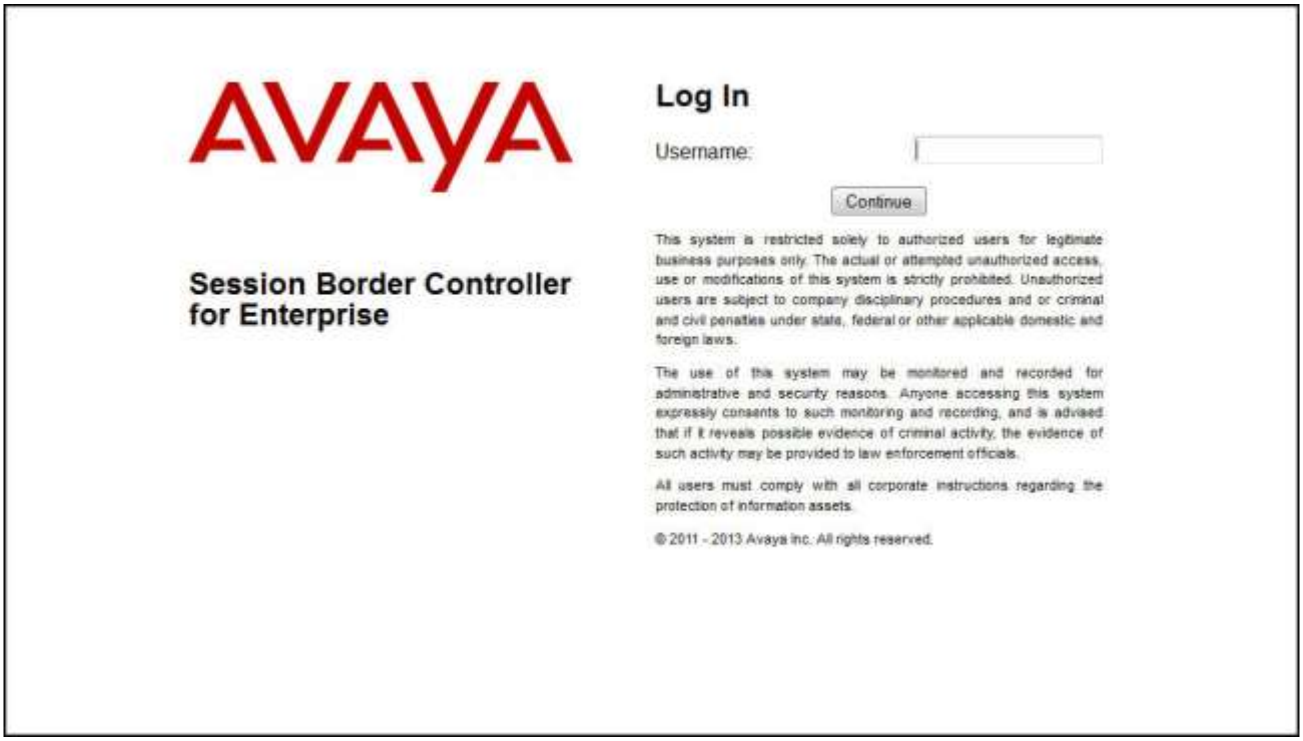
6. Configure Avaya Session Border Controller for Enterprise

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.



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

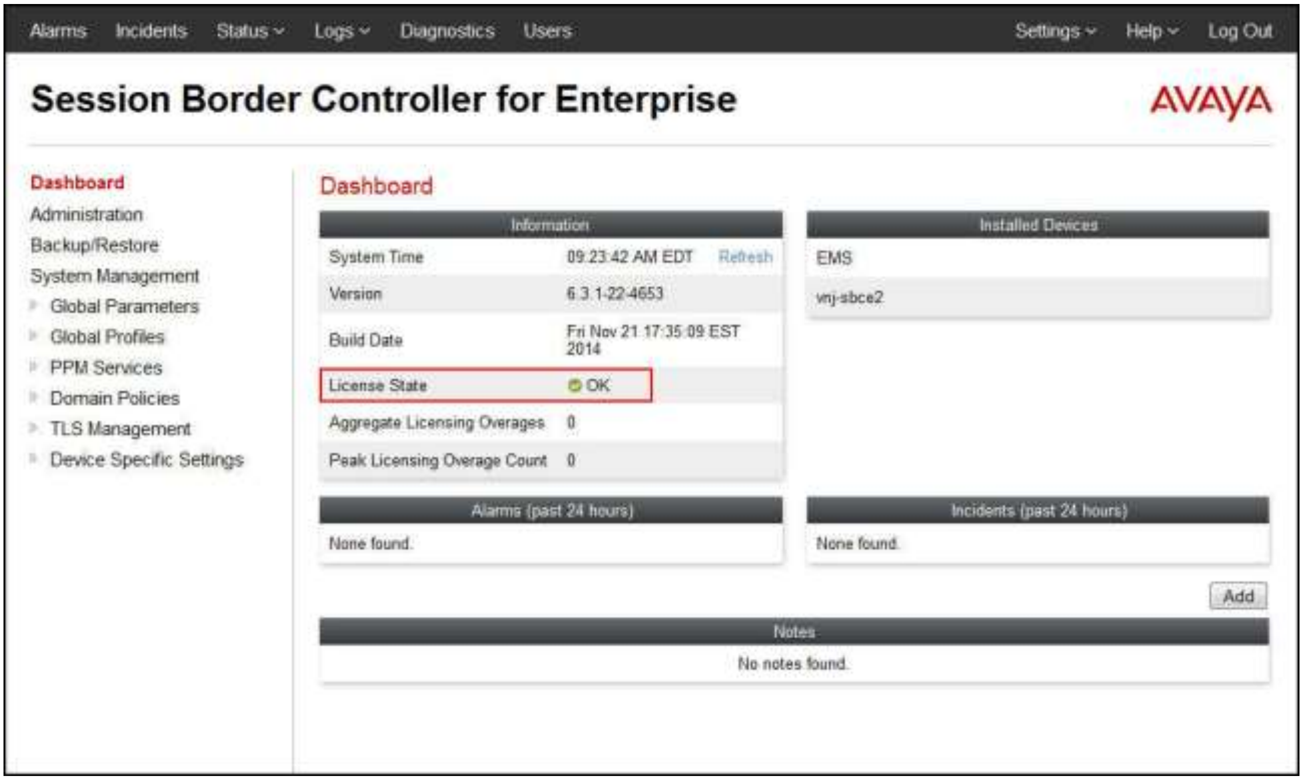
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law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

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

© 2011 - 2013 Avaya Inc. All rights reserved.

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.



Dashboard

Information	
System Time	09:23:42 AM EDT Refresh
Version	6.3.1-22-4653
Build Date	Fri Nov 21 17:35:09 EST 2014
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0

Installed Devices
EMS
vnj-sbce2

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

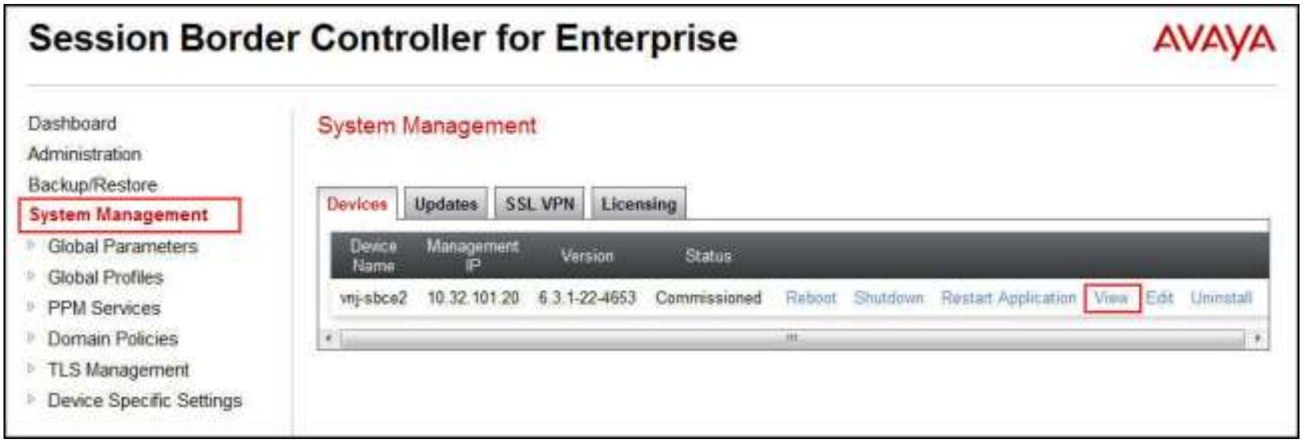
None found.

Notes

No notes found.

6.2. Verify Network Configuration and Enable Interfaces

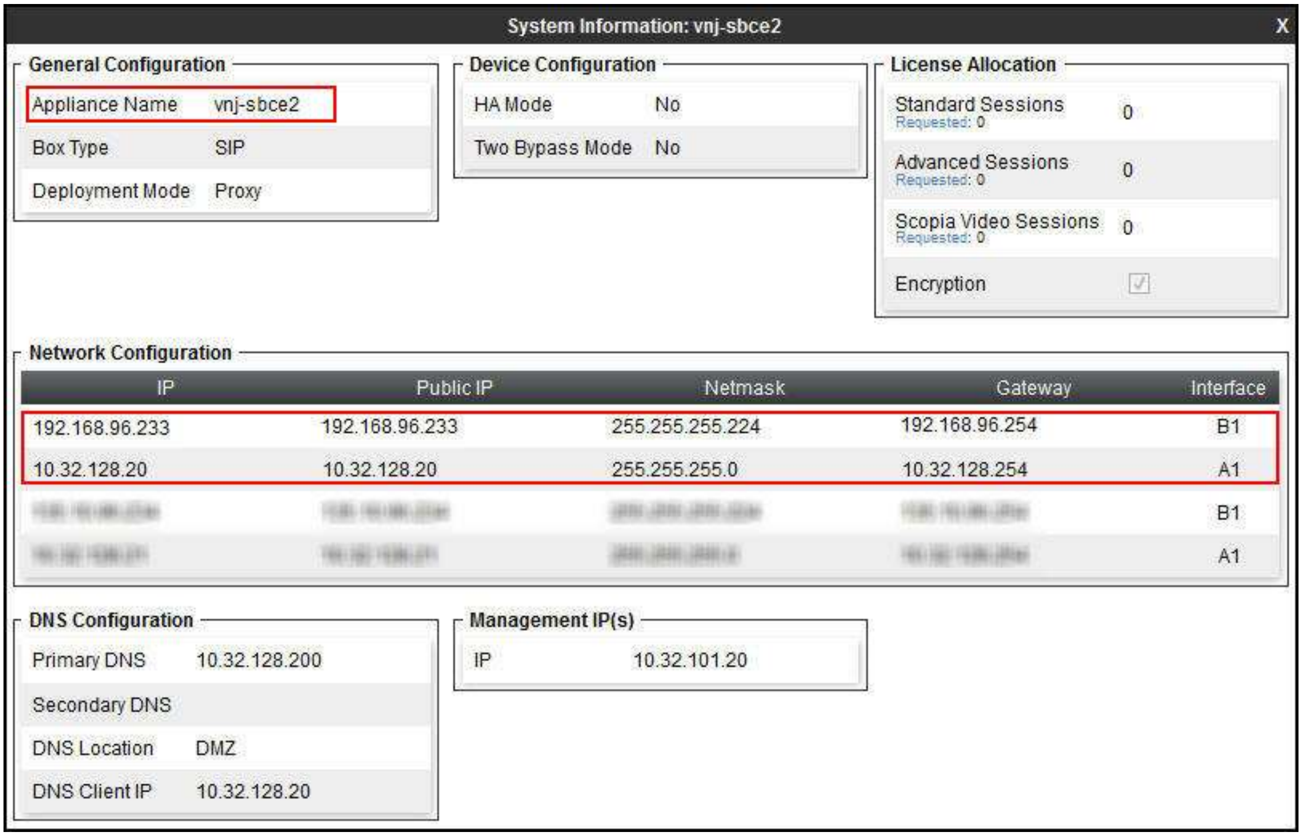
To view the network information provided during installation, navigate to **System Management**. In the right pane, click **View** highlighted below.



Session Border Controller for Enterprise

Device Name	Management IP	Version	Status						
vnj-sbce2	10.32.101.20	6.3.1-22-4653	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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.



System Information: vnj-sbce2

General Configuration

Appliance Name	vnj-sbce2
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 0	0
Advanced Sessions Requested: 0	0
Scopia Video Sessions Requested: 0	0
Encryption	☑

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
192.168.96.233	192.168.96.233	255.255.255.224	192.168.96.254	B1
10.32.128.20	10.32.128.20	255.255.255.0	10.32.128.254	A1
[redacted]	[redacted]	[redacted]	[redacted]	B1
[redacted]	[redacted]	[redacted]	[redacted]	A1

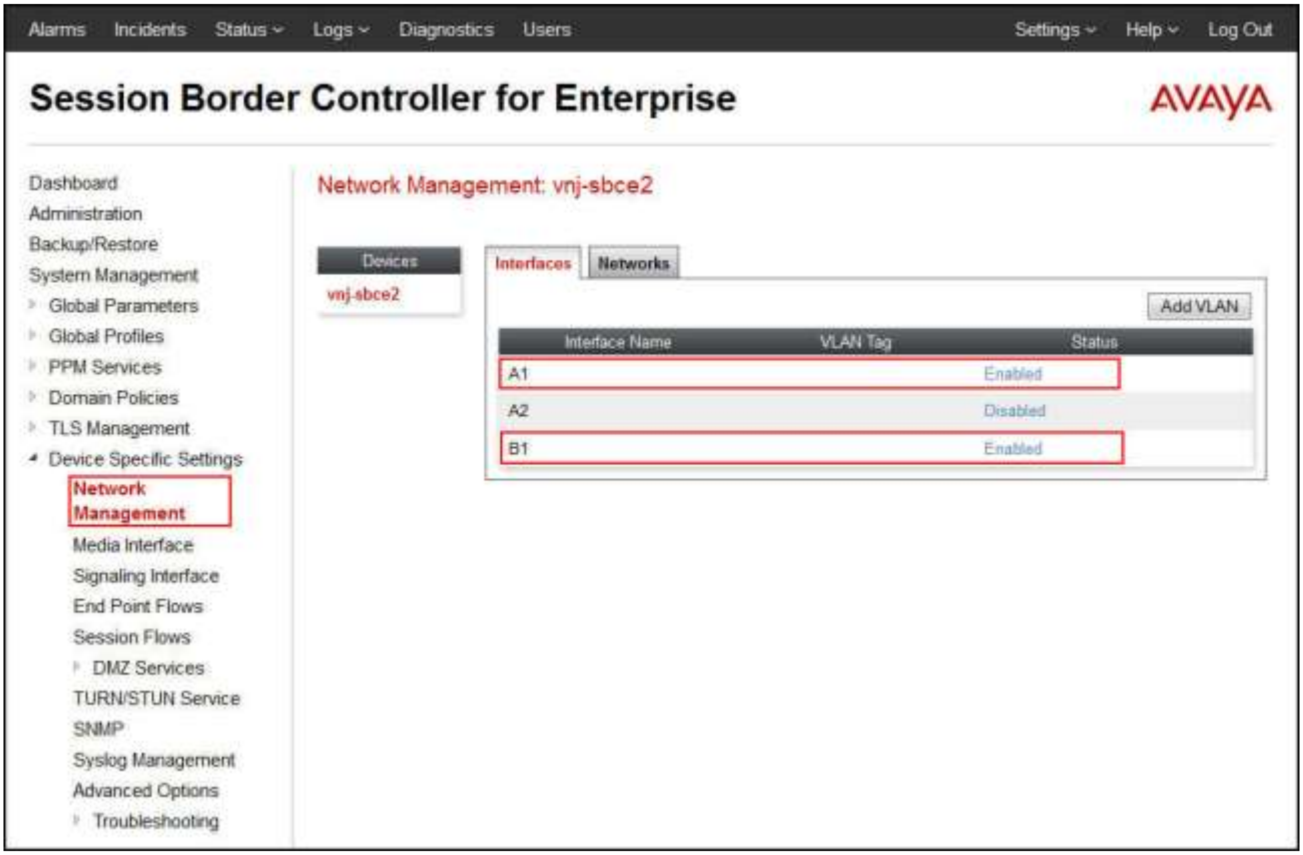
DNS Configuration

Primary DNS	10.32.128.200
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.32.128.20

Management IP(s)

IP	10.32.101.20

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**.



Network Management: vnj-sbce2

Device: vnj-sbce2

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled

6.3. Signaling Interface

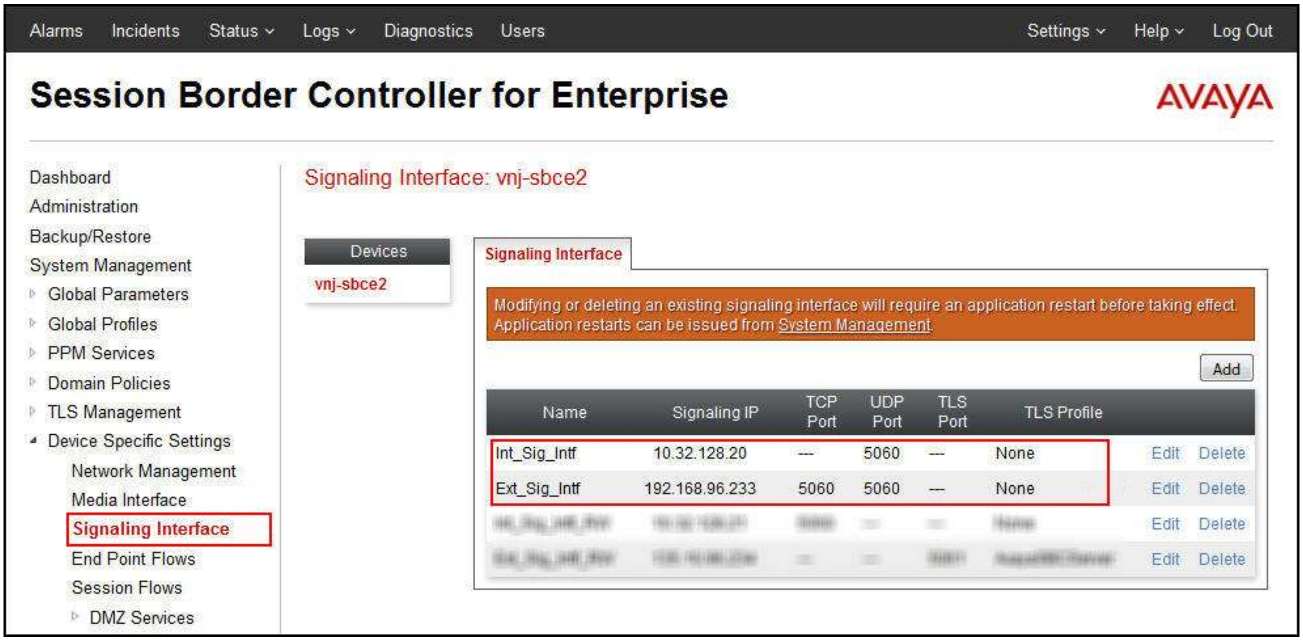
A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

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 requesting the name of the new interface, followed by a series of pop-up windows in which the interface parameters can be configured. 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.

When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Signaling IP** to the IP address associated with the private interface (A1) shown in **Section 6.2**. For the external interface, set the **Signaling IP** to 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 Clearfly SIP Trunking Services uses UDP, it would have been sufficient to simply configure the Avaya SBCE for UDP.



Signaling Interface: vnj-sbce2

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

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Int_Sig_Intf	10.32.128.20	---	5060	---	None	Edit	Delete
Ext_Sig_Intf	192.168.96.233	5060	5060	---	None	Edit	Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Edit	Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Edit	Delete

6.4. Media Interface

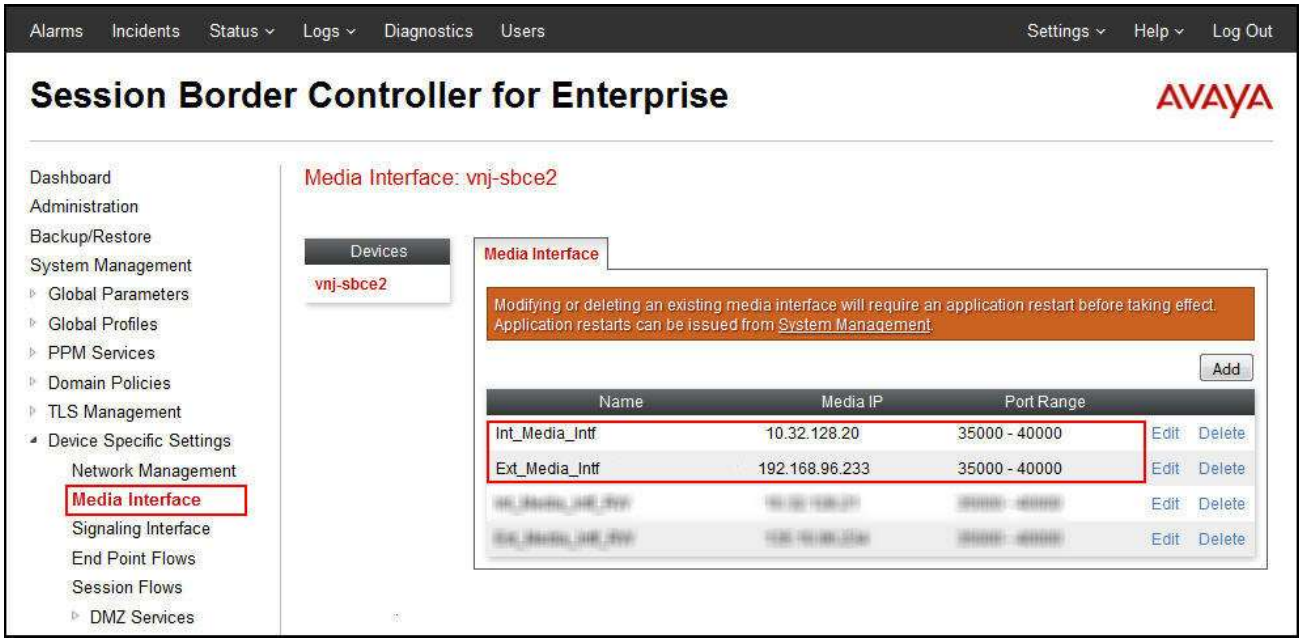
A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

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 requesting the name of the new interface, followed by a series of pop-up windows in which the interface parameters can be configured. 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.

When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Media IP** to the IP address associated with the private interface (A1) shown in **Section 6.2**. For the external interface, set the **Media IP** to 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.



Media Interface: vnj-sbce2

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

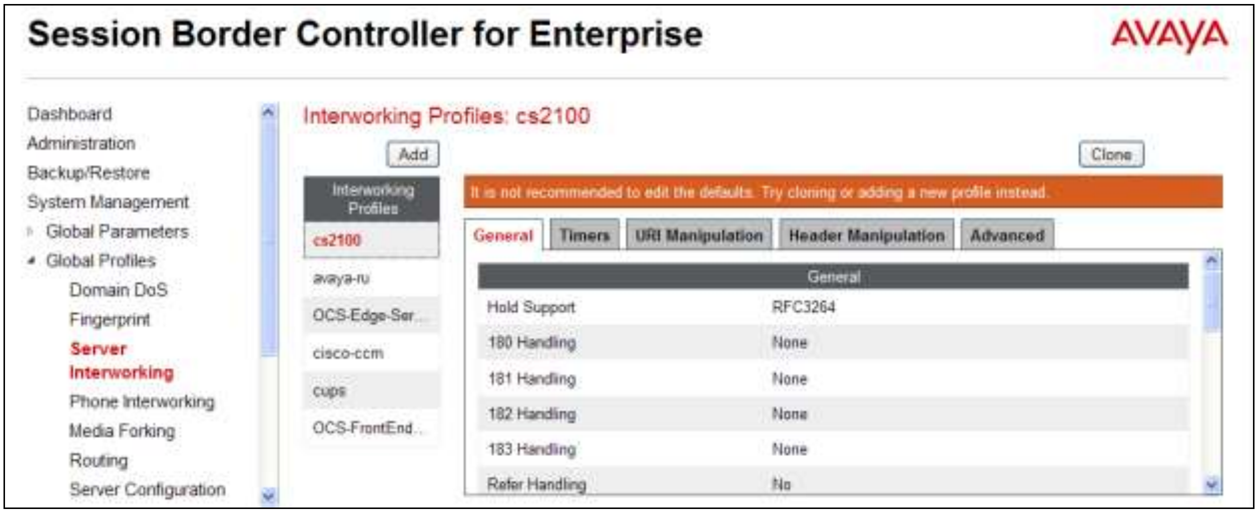
Name	Media IP	Port Range		
Int_Media_Intf	10.32.128.20	35000 - 40000	Edit	Delete
Ext_Media_Intf	192.168.96.233	35000 - 40000	Edit	Delete
[redacted]	[redacted]	[redacted]	Edit	Delete
[redacted]	[redacted]	[redacted]	Edit	Delete

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.

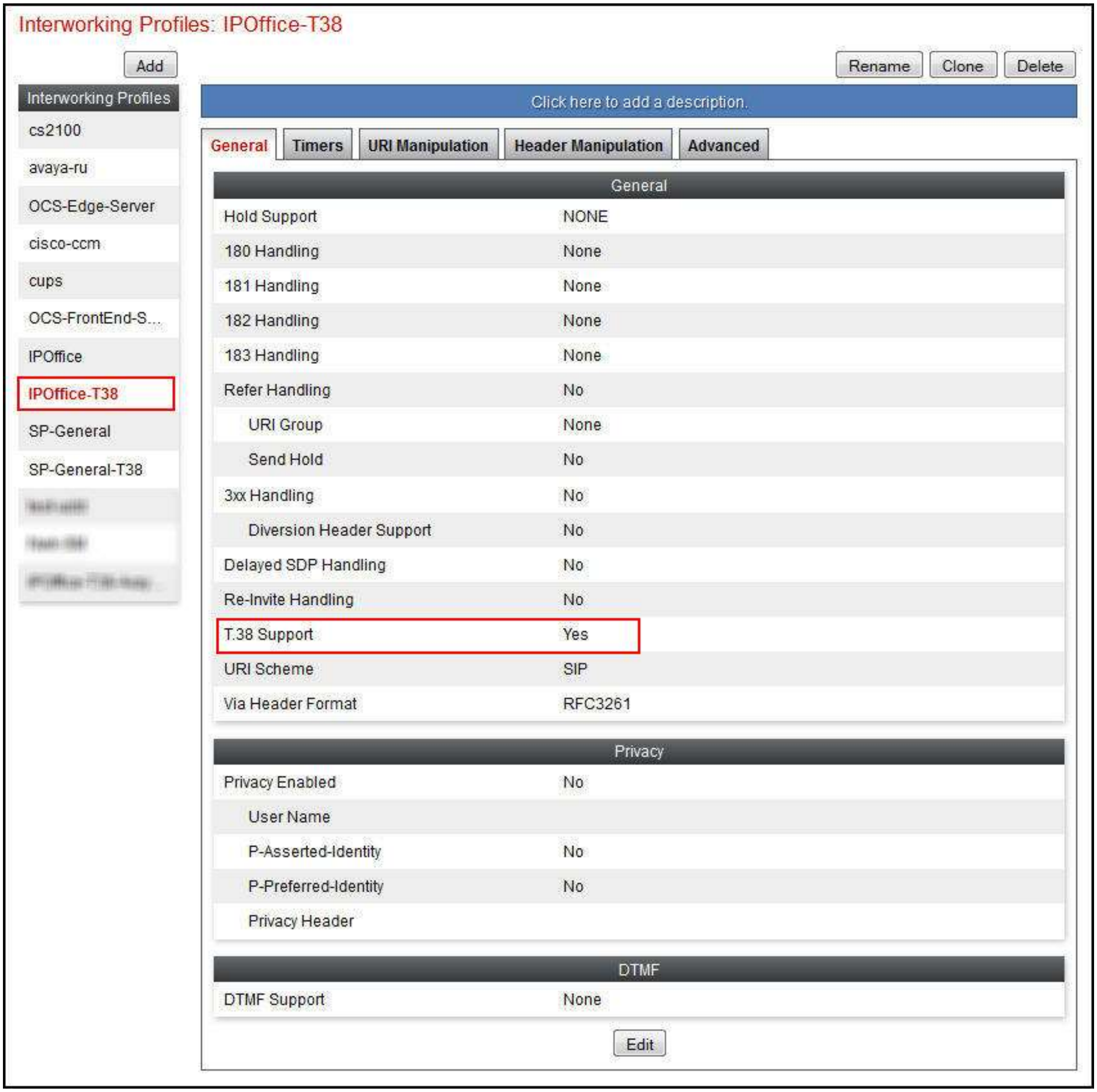


It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No

6.5.1. Server Interworking – Avaya IP Office

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



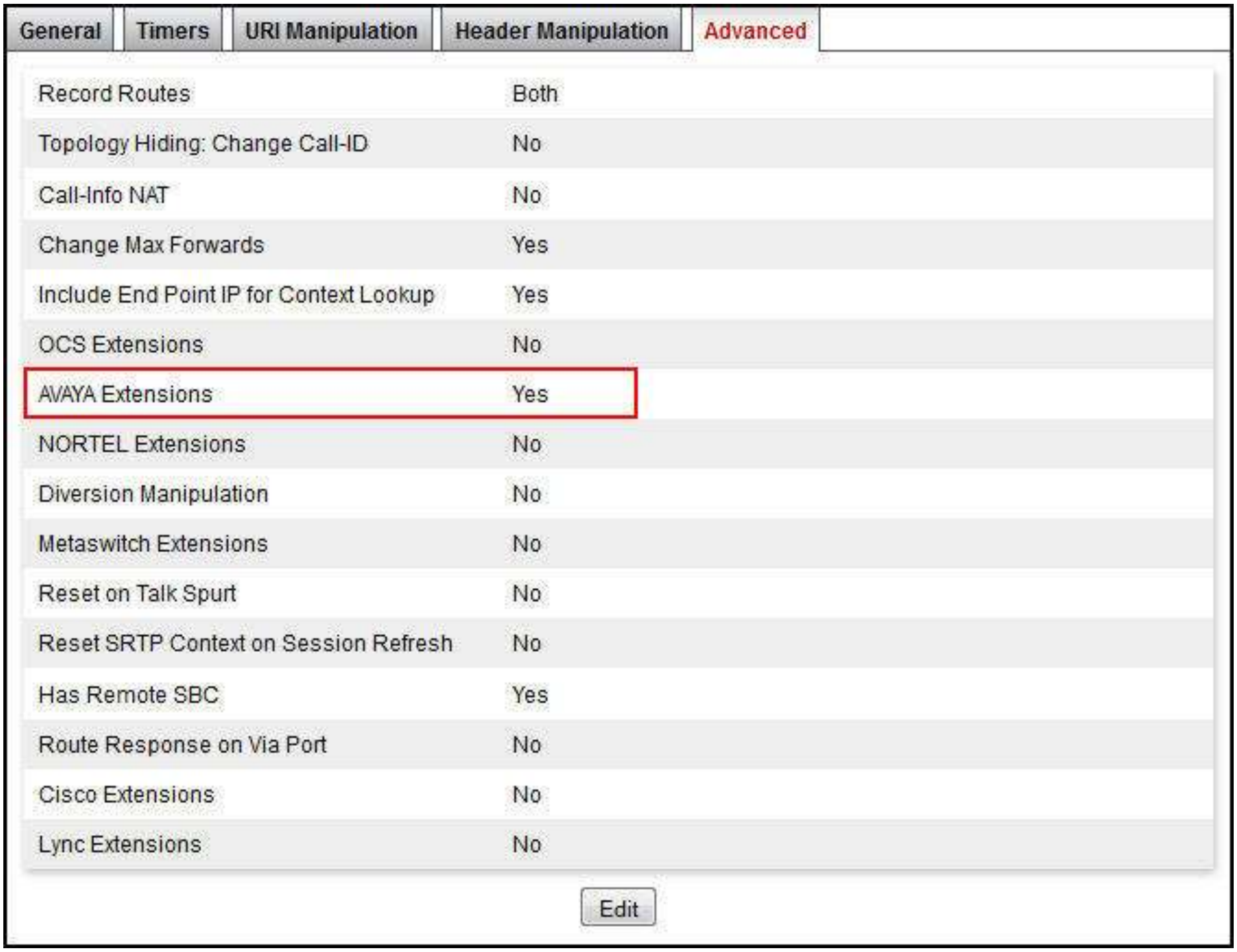
Interworking Profiles: IPOffice-T38

Interworking Profiles
- cs2100
- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- OCS-FrontEnd-S...
- IPOffice
- IPOffice-T38
- SP-General
- SP-General-T38
- [redacted]

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

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

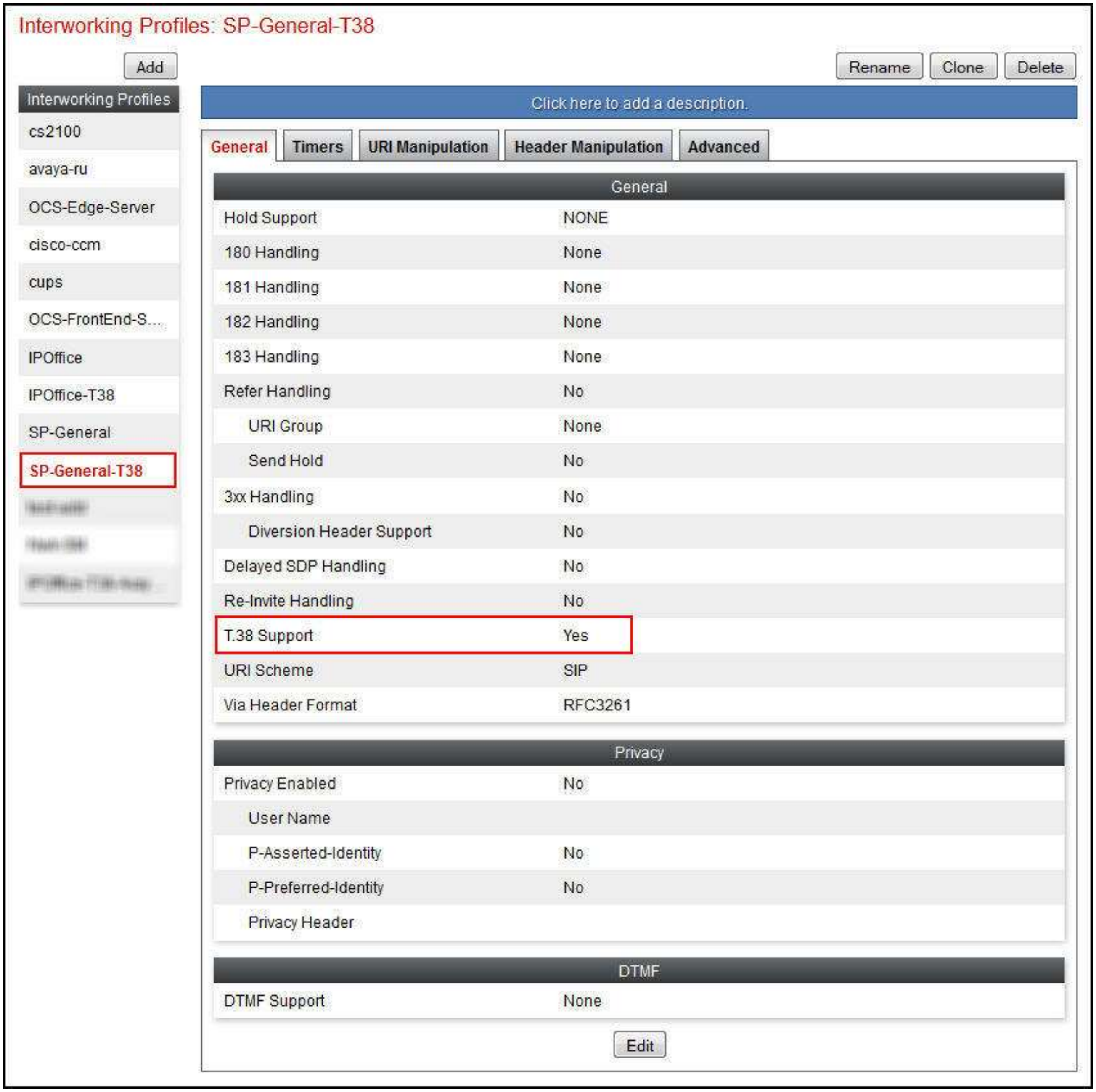
The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to ***Yes***.



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

6.5.2. Server Interworking – Clearfly Communications

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



Interworking Profiles
- cs2100
- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- OCS-FrontEnd-S...
- IPOffice
- IPOffice-T38
- SP-General
- SP-General-T38
- [redacted]
- [redacted]
- [redacted]

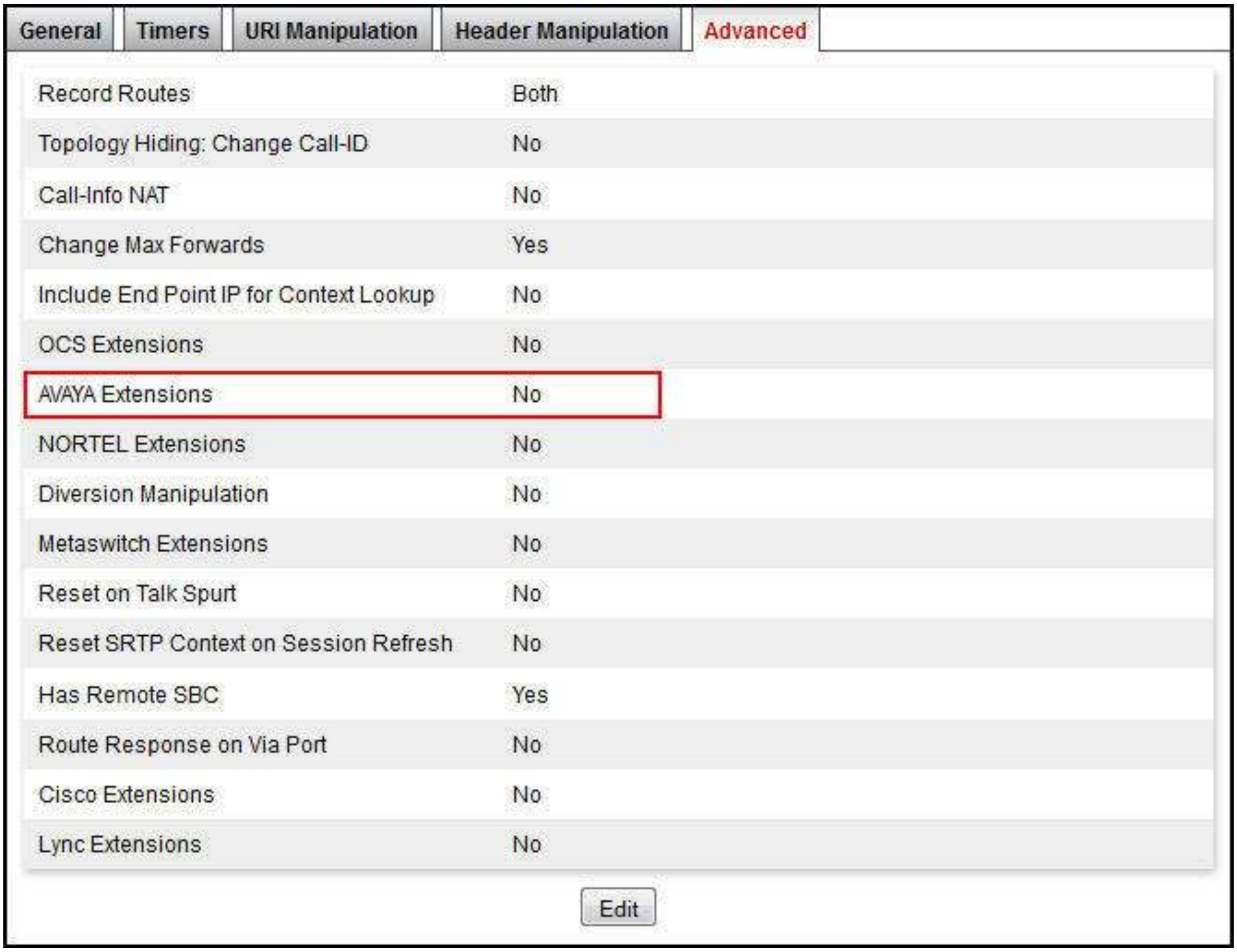
General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

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

DTMF	
DTMF Support	None

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

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



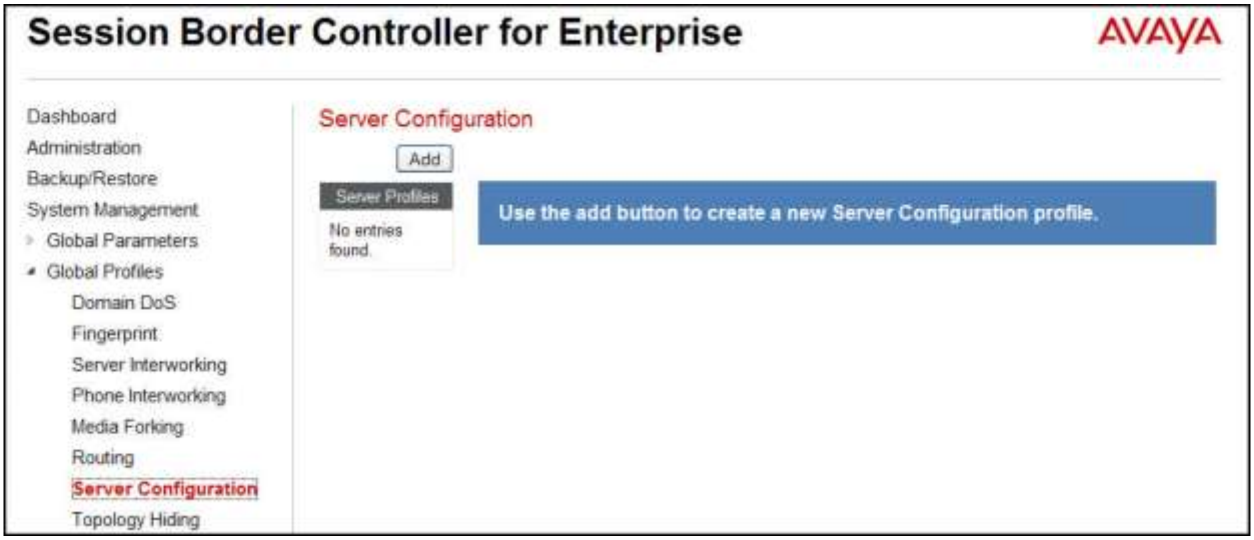
Record Routes	Both
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session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

6.6. 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.



No entries found.

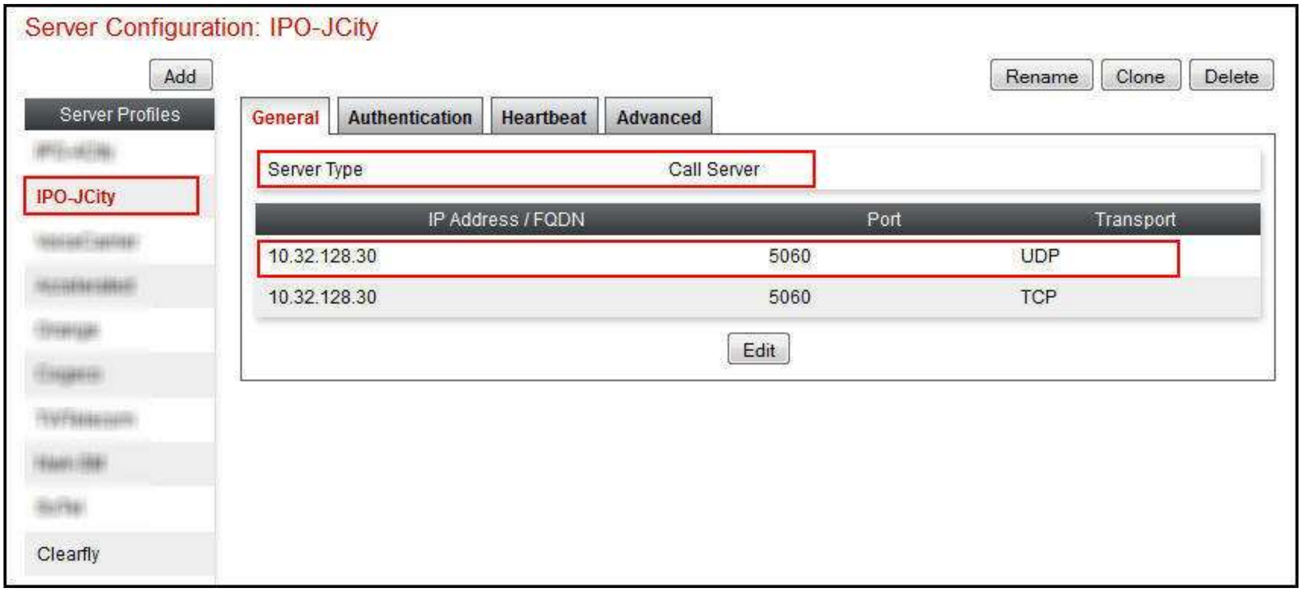
Use the add button to create a new Server Configuration profile.

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.



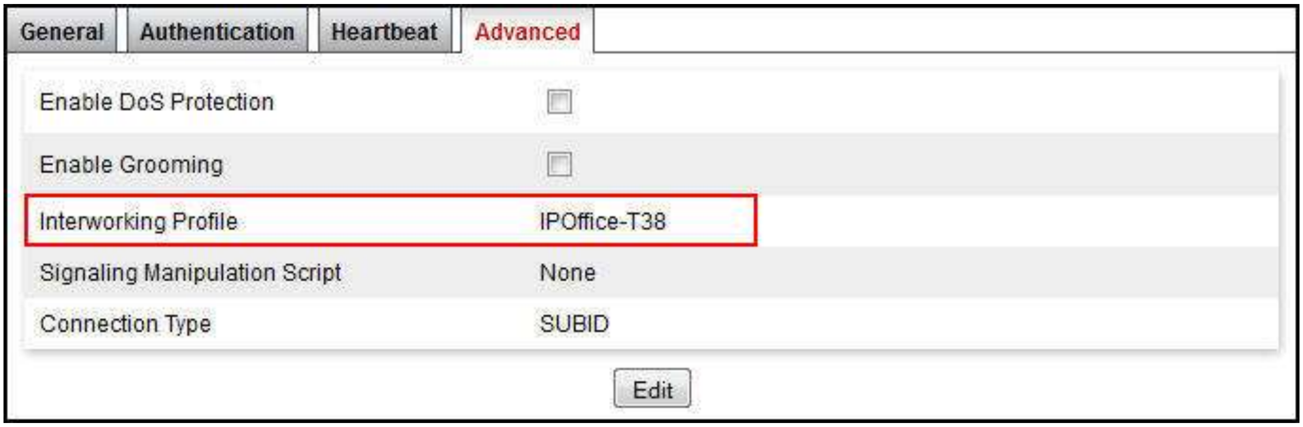
Server Configuration: IPO-JCity

Server Profiles
[redacted]
IPO-JCity
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
Clearfly

Server Type Call Server

IP Address / FQDN	Port	Transport
10.32.128.30	5060	UDP
10.32.128.30	5060	TCP

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

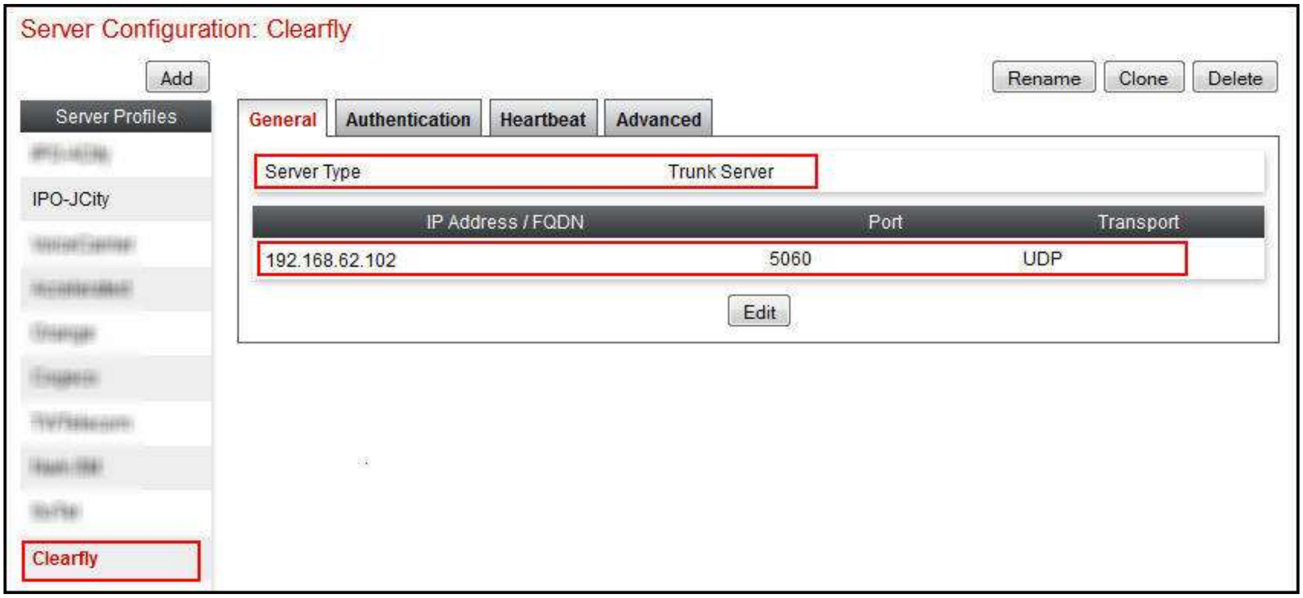


Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	IPOffice-T38
Signaling Manipulation Script	None
Connection Type	SUBID

6.6.2. Server Configuration – Clearfly Communications

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

- Set **Server Type** to ***Trunk Server***.
- Set **IP Addresses / FQDNs** to the IP address of the Clearfly network access interface as shown in **Figure 1**.
- Select the appropriate **Transport** protocol used for SIP signaling between Clearfly 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 Clearfly SIP server will listen on for SIP messages from the Avaya SBCE.

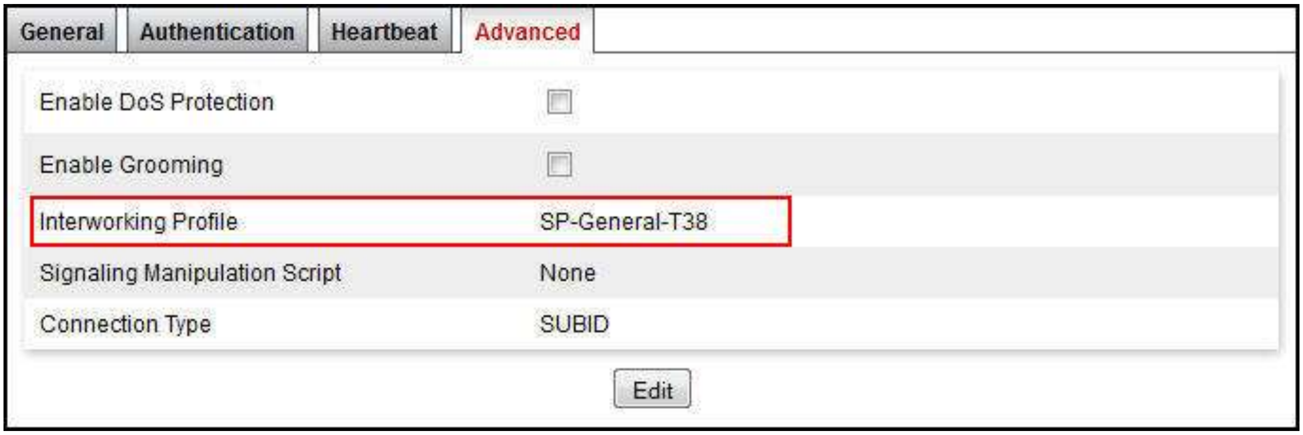

Server Configuration: Clearfly

Server Profiles
- [redacted]
- IPO-JCity
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Clearfly

Server Type	Trunk Server

IP Address / FQDN	Port	Transport
192.168.62.102	5060	UDP

On the **Advanced** tab, select the **Interworking Profile** for Clearfly Communications defined in **Section 6.5.2**.

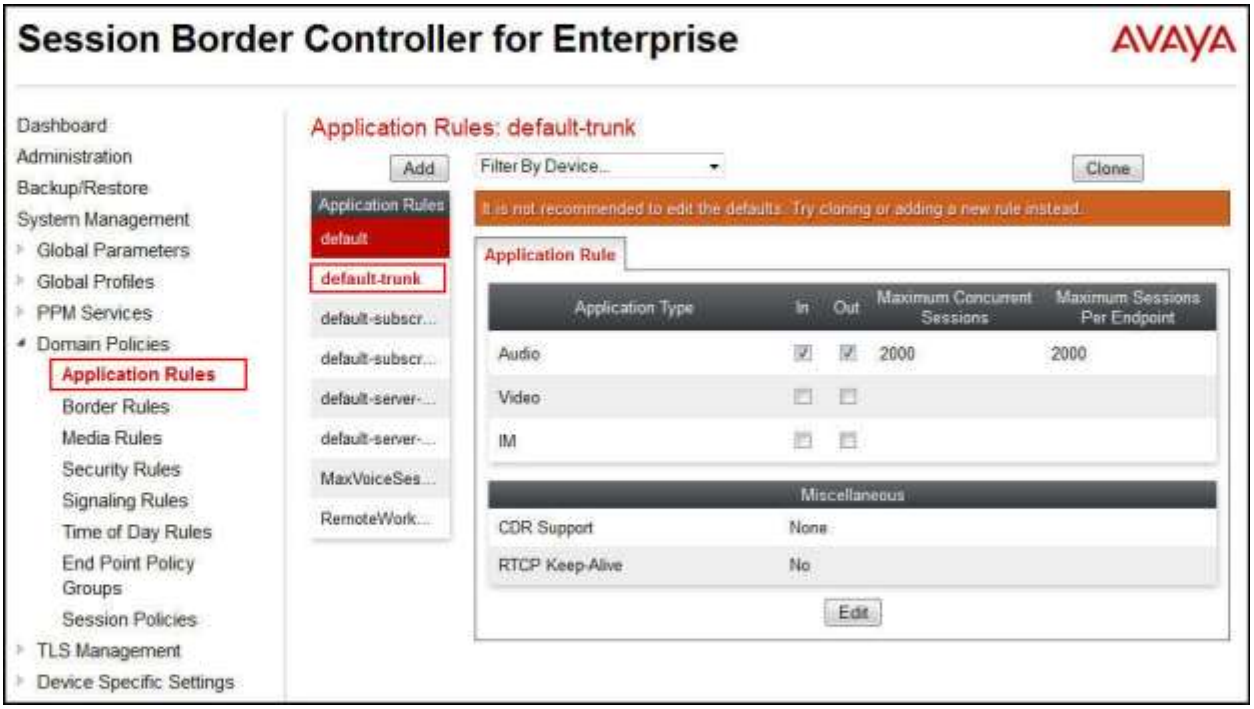


Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	SP-General-T38
Signaling Manipulation Script	None
Connection Type	SUBID

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**. For the compliance test, the predefined **default-trunk** application rule (shown below) was used for both Avaya IP Office and the Clearfly SIP server.

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



Application Rules: default-trunk

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

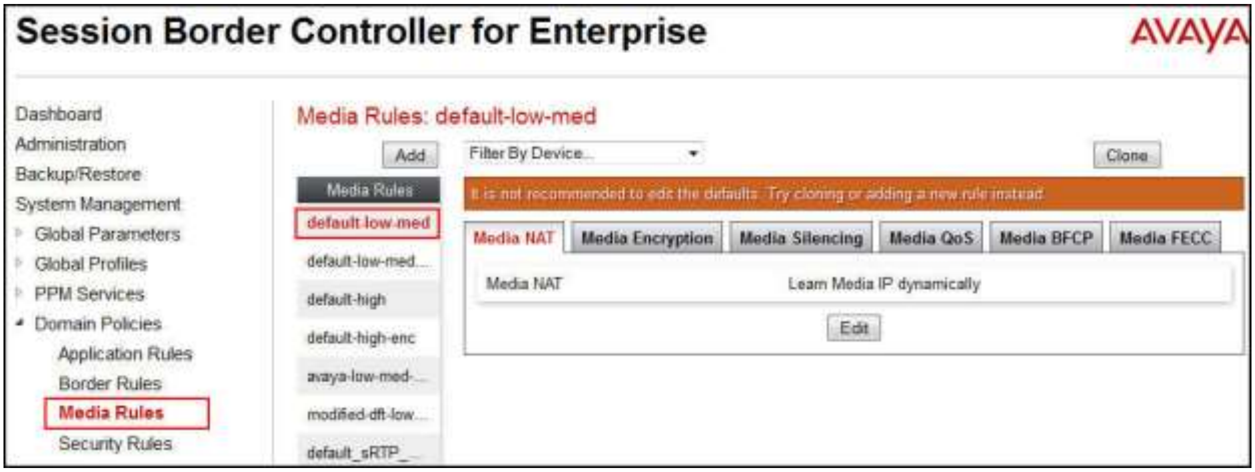
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	2000	2000
Video	□	□		
IM	□	□		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

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 predefined **default-low-med** media rule (shown below) was used for both Avaya IP Office and the Clearfly 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.



Session Border Controller for Enterprise

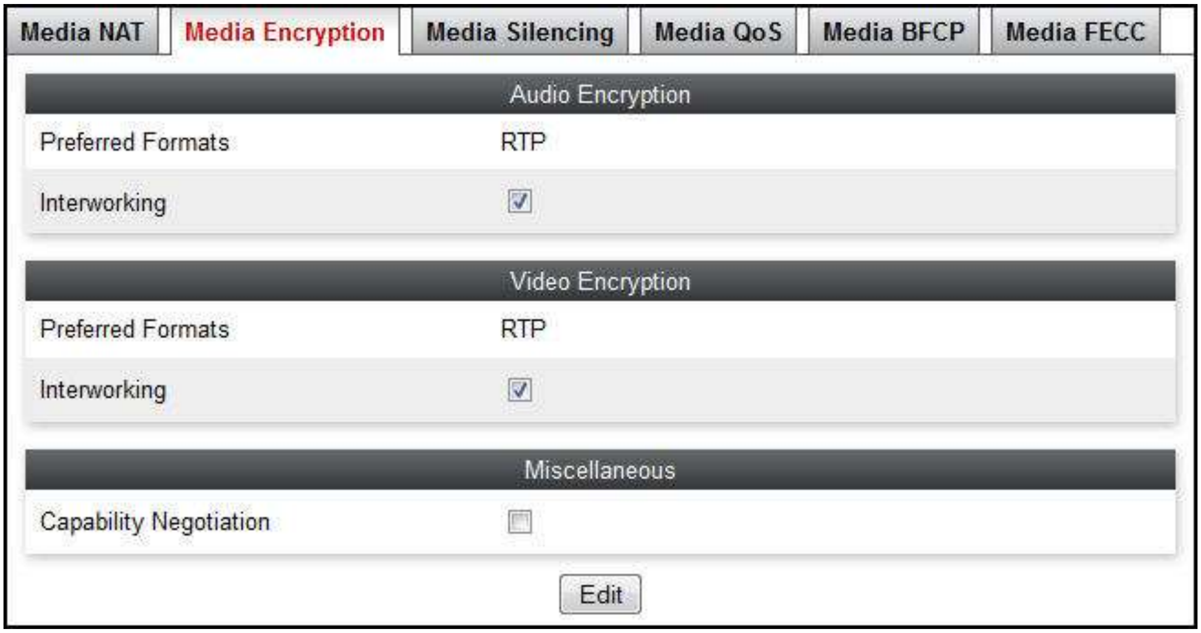
Media Rules: default-low-med

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Media NAT	Learn Media IP dynamically

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.

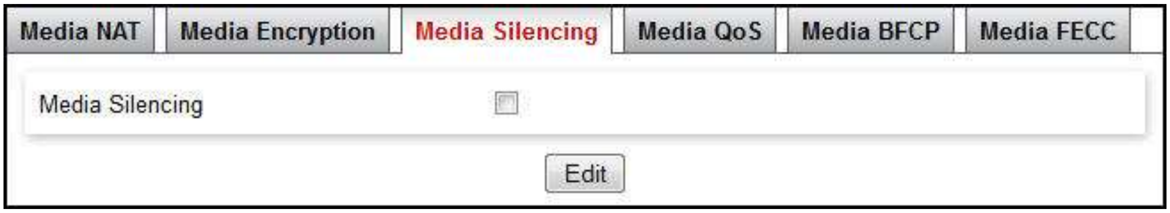


Audio Encryption	
Preferred Formats	RTP
Interworking	☑

Video Encryption	
Preferred Formats	RTP
Interworking	☑

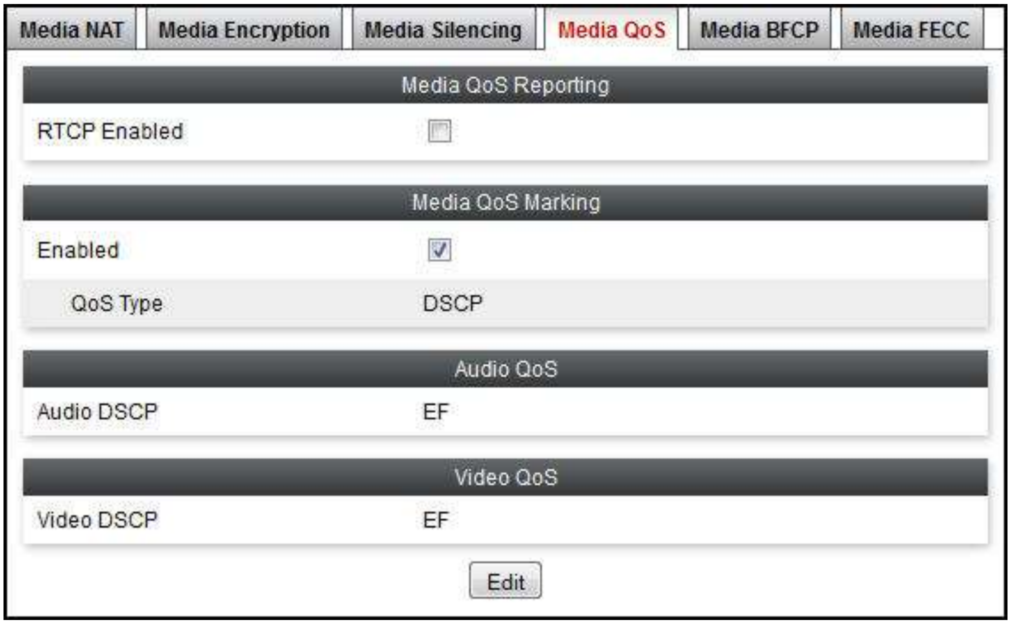
Miscellaneous	
Capability Negotiation	☐

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



Media Silencing ☐

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



Media QoS Reporting

RTCP Enabled ☐

Media QoS Marking

Enabled ☑

QoS Type DSCP

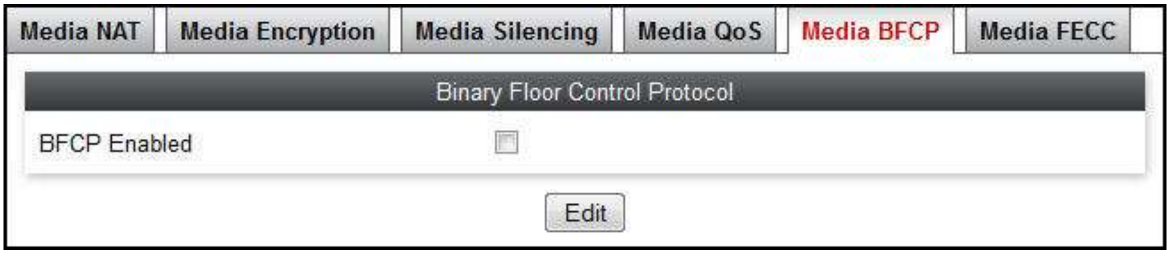
Audio QoS

Audio DSCP EF

Video QoS

Video DSCP EF

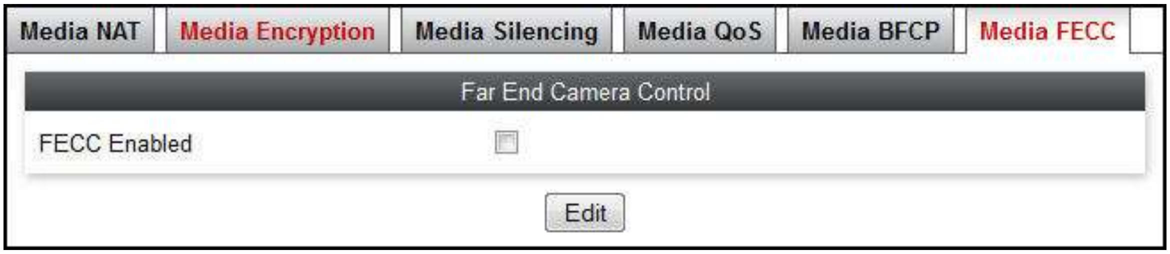
The **Media BFCP** tab is shown below.



Binary Floor Control Protocol

BFCP Enabled ☐

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



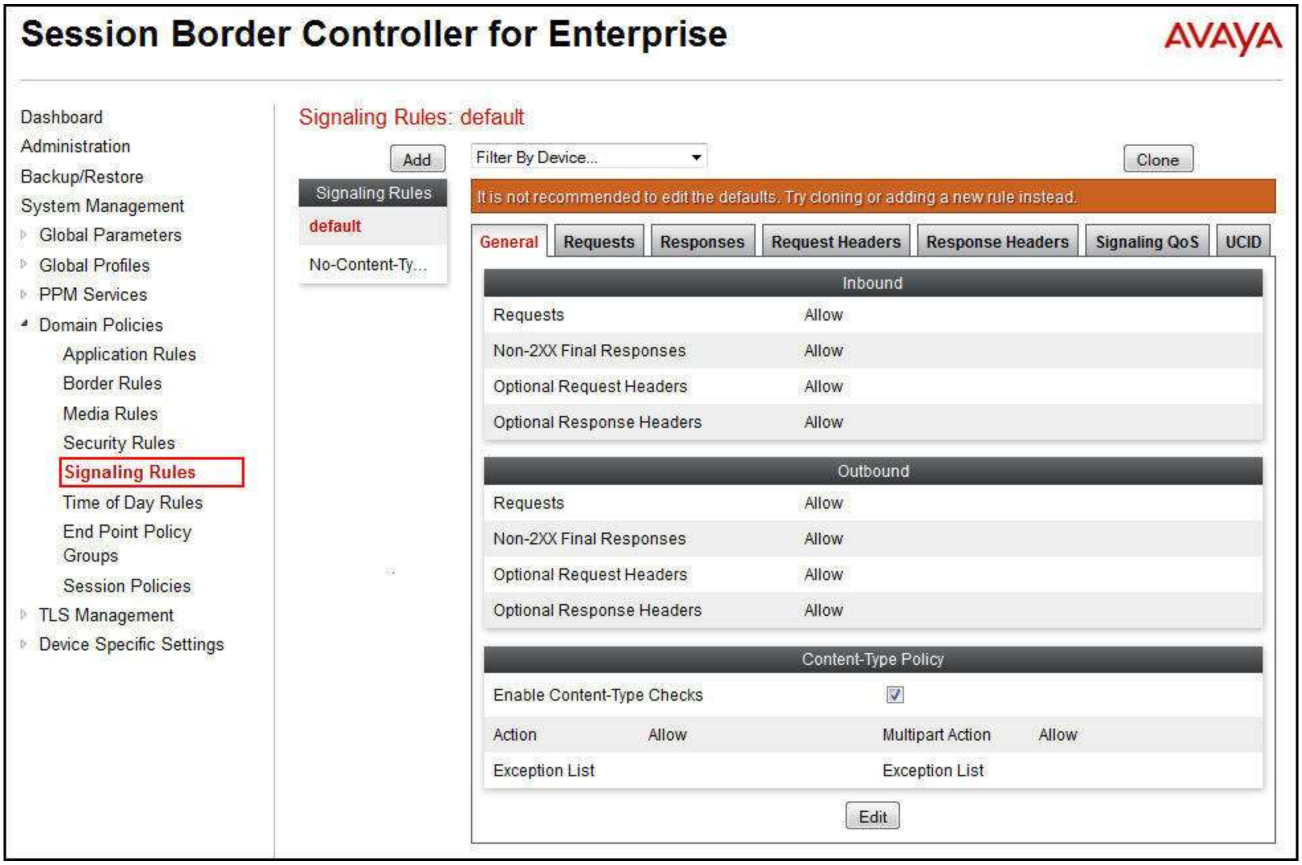
Far End Camera Control

FECC Enabled ☐

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 predefined **default** signaling rule (shown below) was used for both Avaya IP Office and the Clearfly 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.



Signaling Rules: default

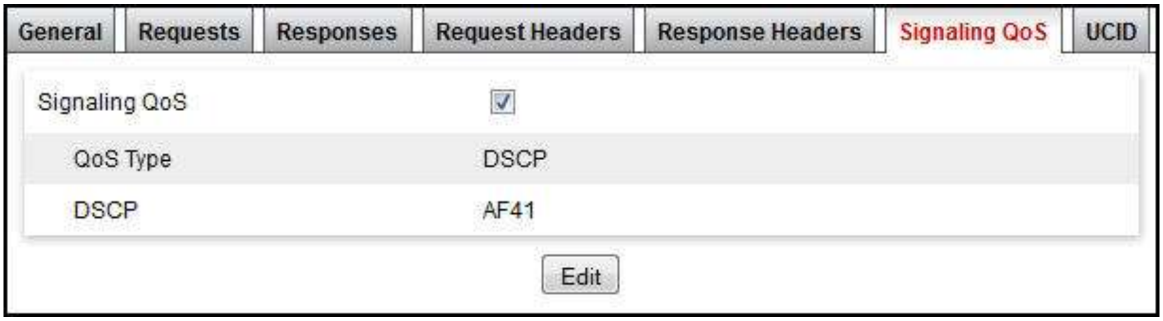
It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks		☑	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

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



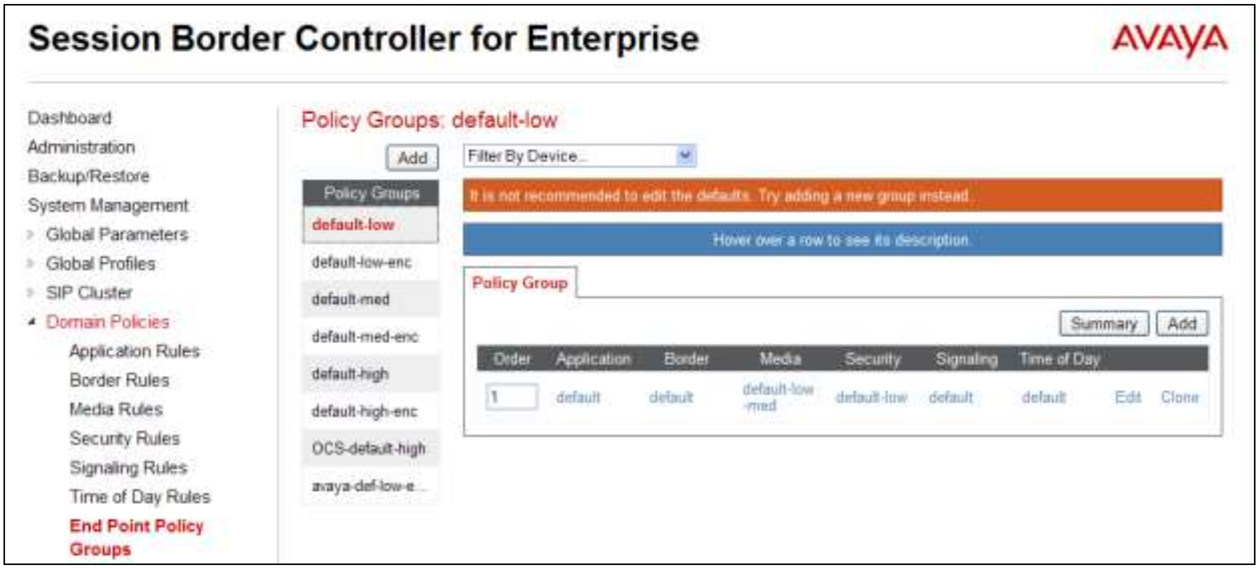
Signaling QoS	☑
QoS Type	DSCP
DSCP	AF41

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 series of pop-up windows 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.



Policy Groups: default-low

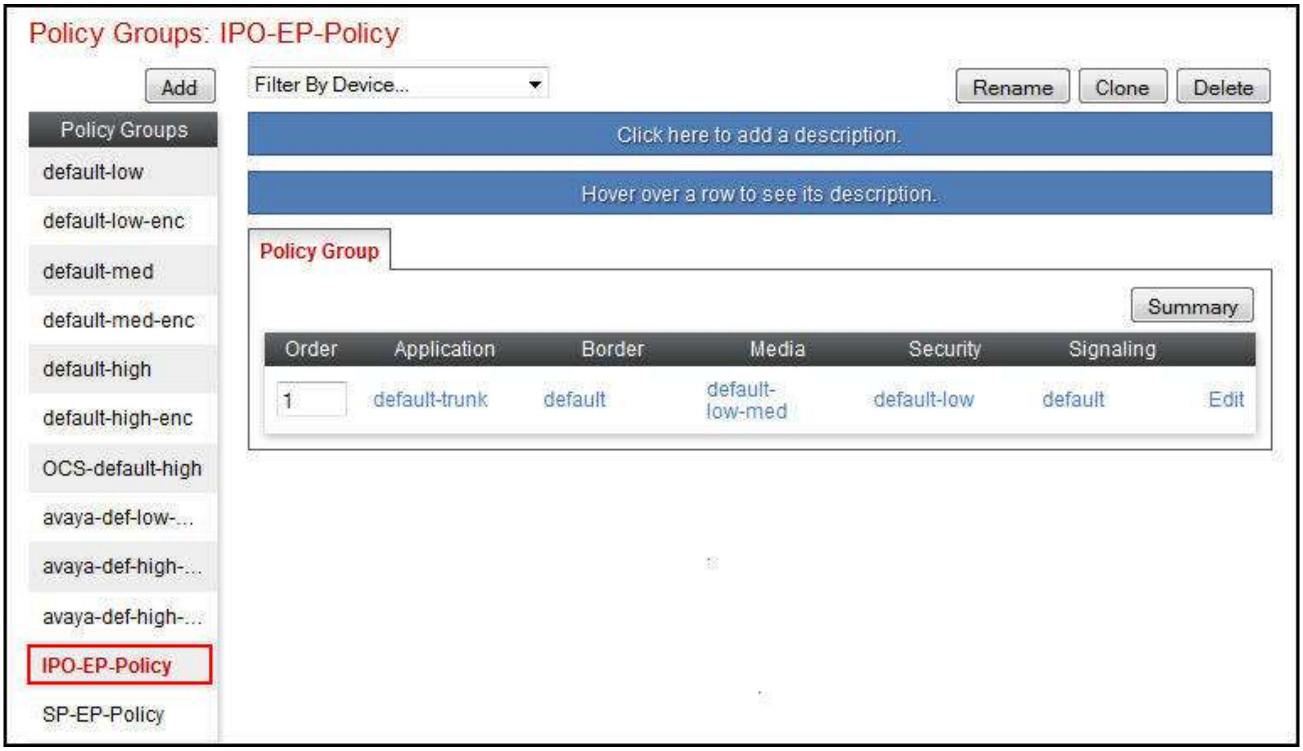
It is not recommended to edit the defaults. Try adding a new group instead.

Hover over a row to see its description.

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

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. The details of the default settings for **Application**, **Media** and **Signaling** are shown in **Section 6.7**, **Section 6.8** and **Section 6.9** respectively.

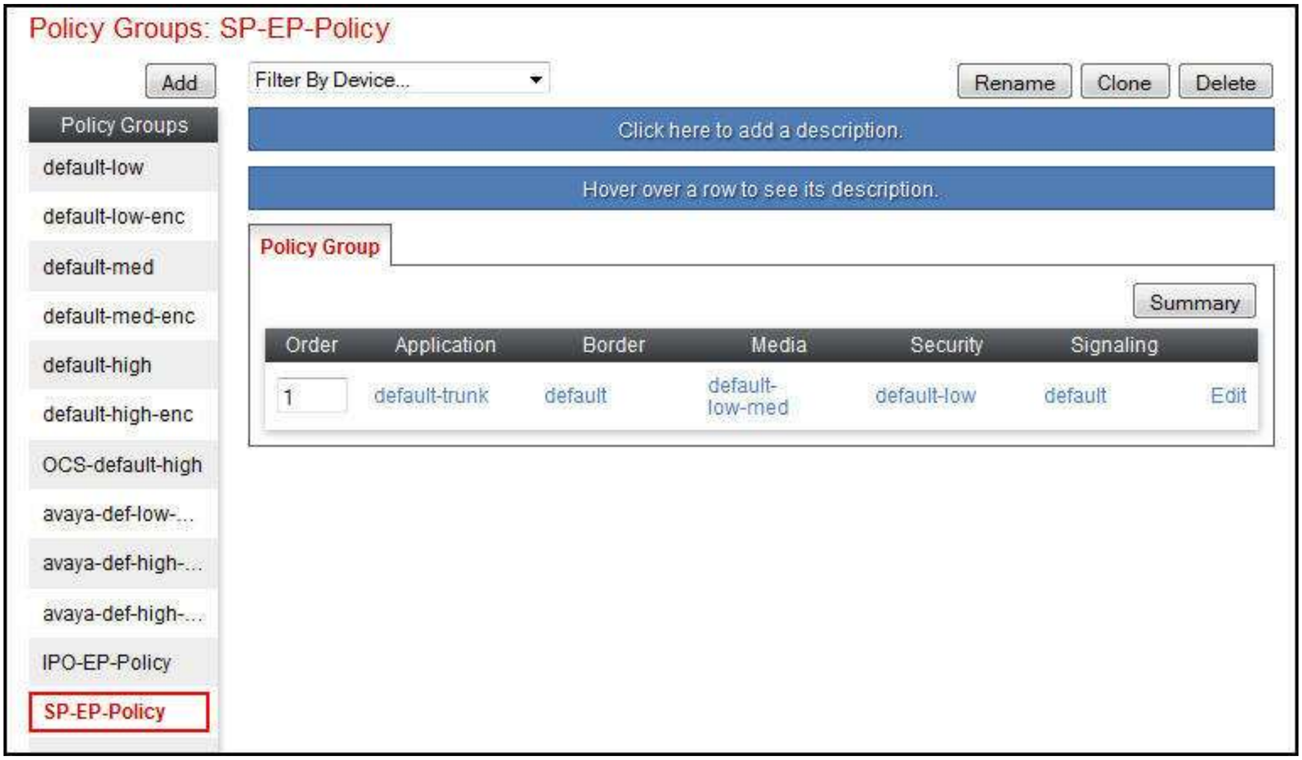


Policy Groups: IPO-EP-Policy

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

6.10.2. End Point Policy Group – Clearfly Communications

For the compliance test, the end point policy group ***SP-EP-Policy*** was created for the Clearfly SIP server. Same default values were used for each of the rules which comprise the group. Thus, the **SP-EP-Policy** is identical to the **IPO-EP-Policy** created in **Section 6.10.1**.



Policy Groups: SP-EP-Policy

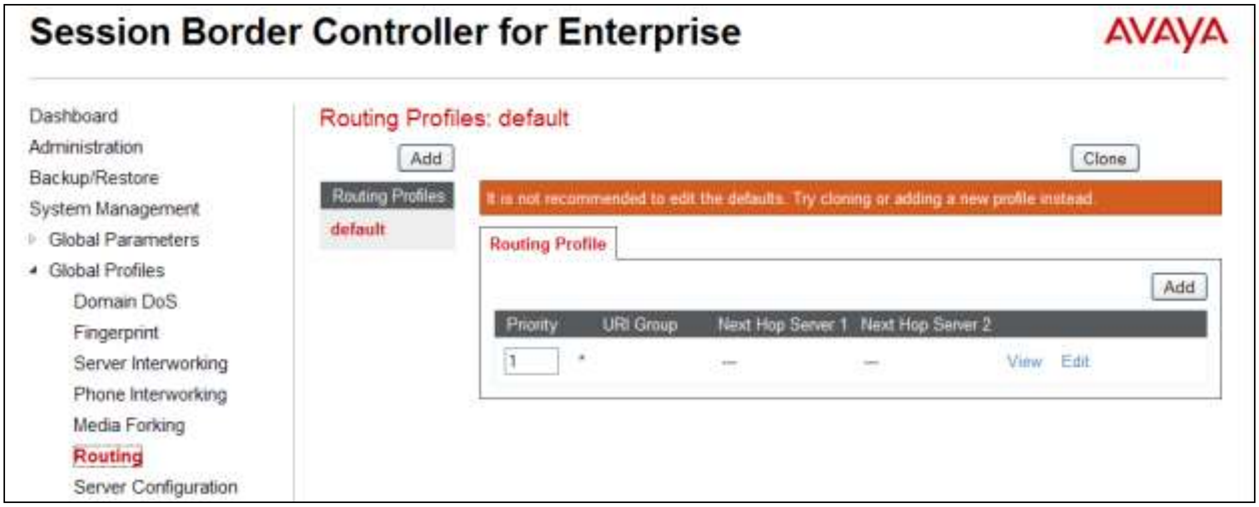
Order	Application	Border	Media	Security	Signaling	
1	default-trunk	default	default-low-med	default-low	default	Edit

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 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 specific routing profiles were added for the compliance test.



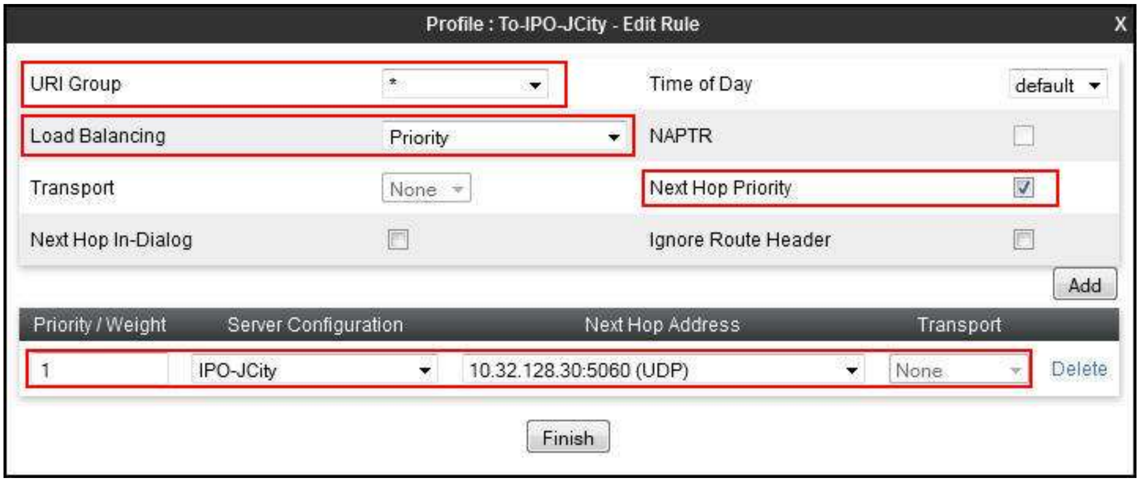
It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	--	--	View Edit

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**.
  - Set **Next Hop Address** to the IP address of Avaya IP Office LAN1 port.
  - Select ***UDP*** for **Transport** (the transport will be displayed in the Next Hop Address field once the entry is added).

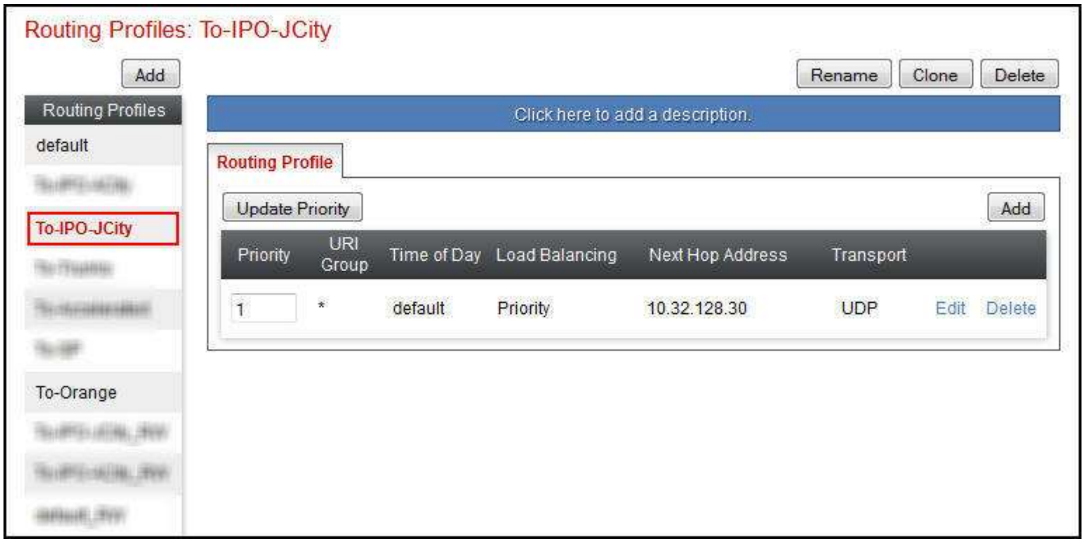


Profile : To-IPO-JCity - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	□	Ignore Route Header	□

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	IPO-JCity	10.32.128.30:5060 (UDP)	None	Delete

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



Routing Profiles: To-IPO-JCity

Routing Profiles
- default
- [redacted]
- To-IPO-JCity
- [redacted]
- [redacted]
- [redacted]
- To-Orange
- [redacted]
- [redacted]
- [redacted]

Click here to add a description.

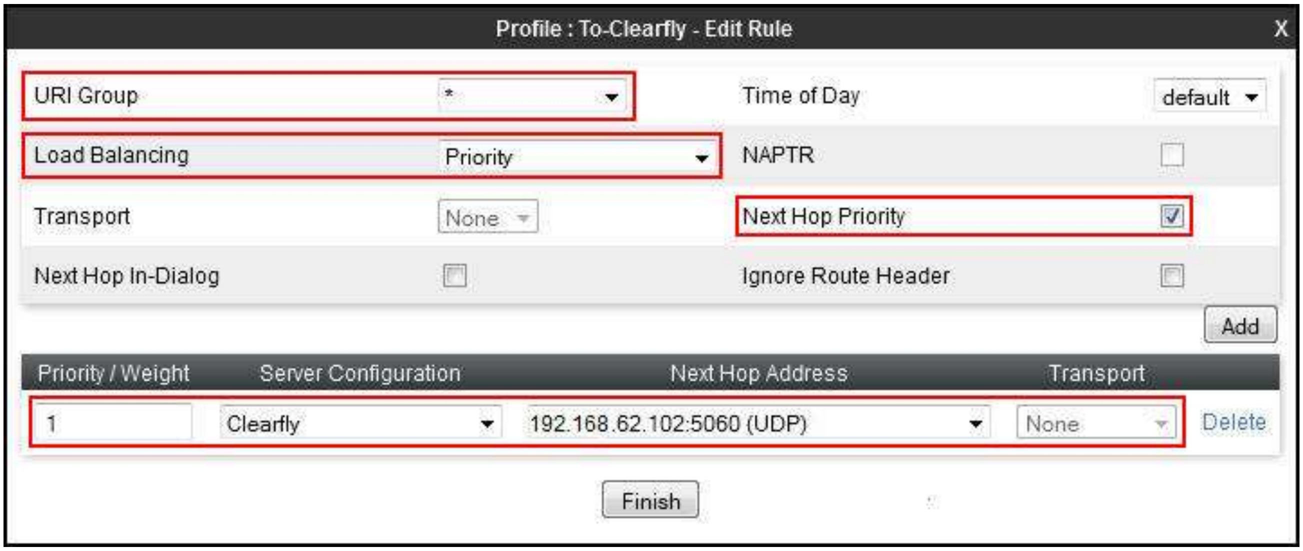
Routing Profile

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport		
1	*	default	Priority	10.32.128.30	UDP	Edit	Delete

6.11.2. Routing – Clearfly Communications

For the compliance test, routing profile ***To-Clearfly*** was created for routing calls to Clearfly Communications. 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 a sequential number starting with ***1*** for **Priority/Weight**.
  - For **Server Configuration**, select the Server for Clearfly as configured in **Section 6.6.2**.
  - Set **Next Hop Address** to the IP address of the Clearfly SIP server as configured in **Section 6.6.2**.
  - Select ***UDP*** for **Transport** (the transport will be displayed in the Next Hop Address field once the entry is added).

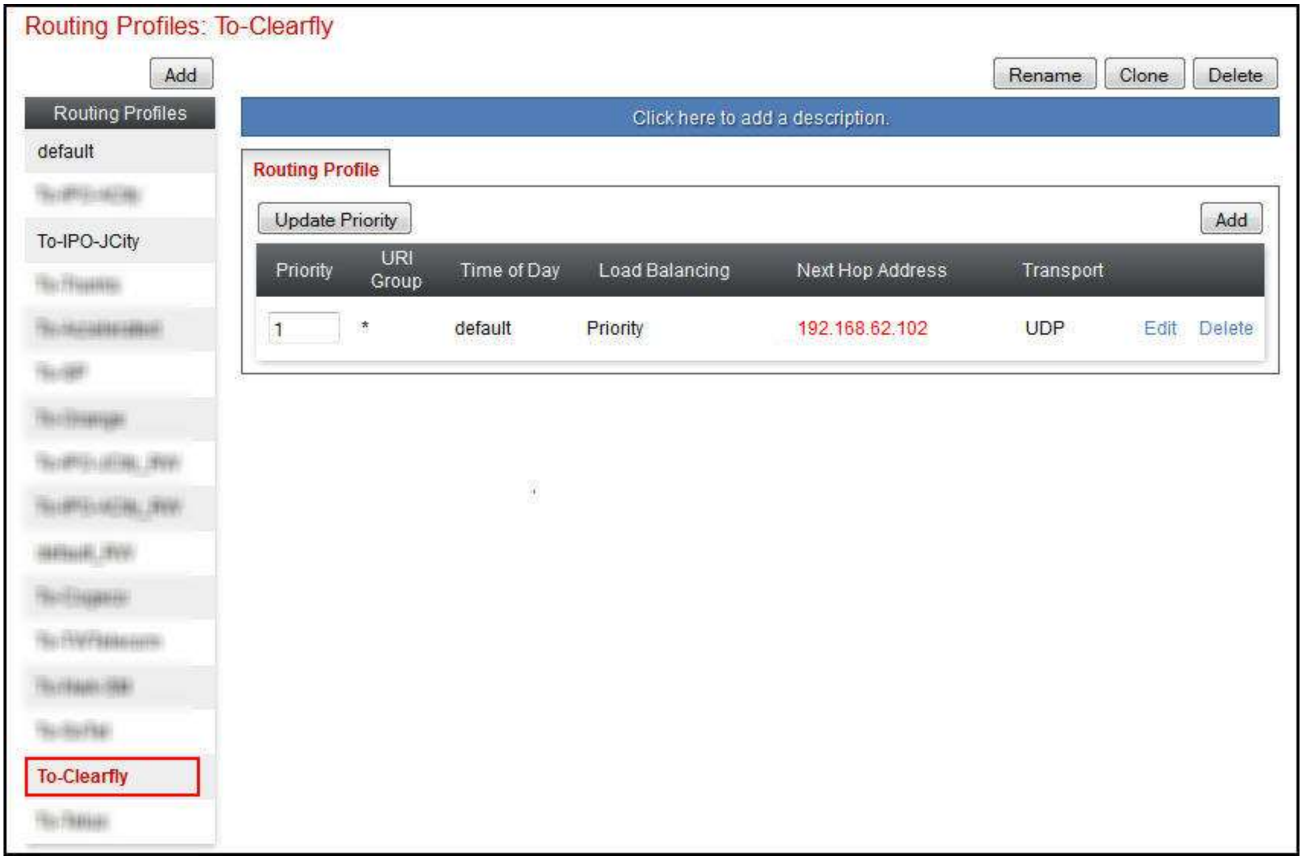


Profile : To-Clearfly - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	□	Ignore Route Header	□

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Clearfly	192.168.62.102:5060 (UDP)	None	Delete

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



Routing Profiles: To-Clearfly

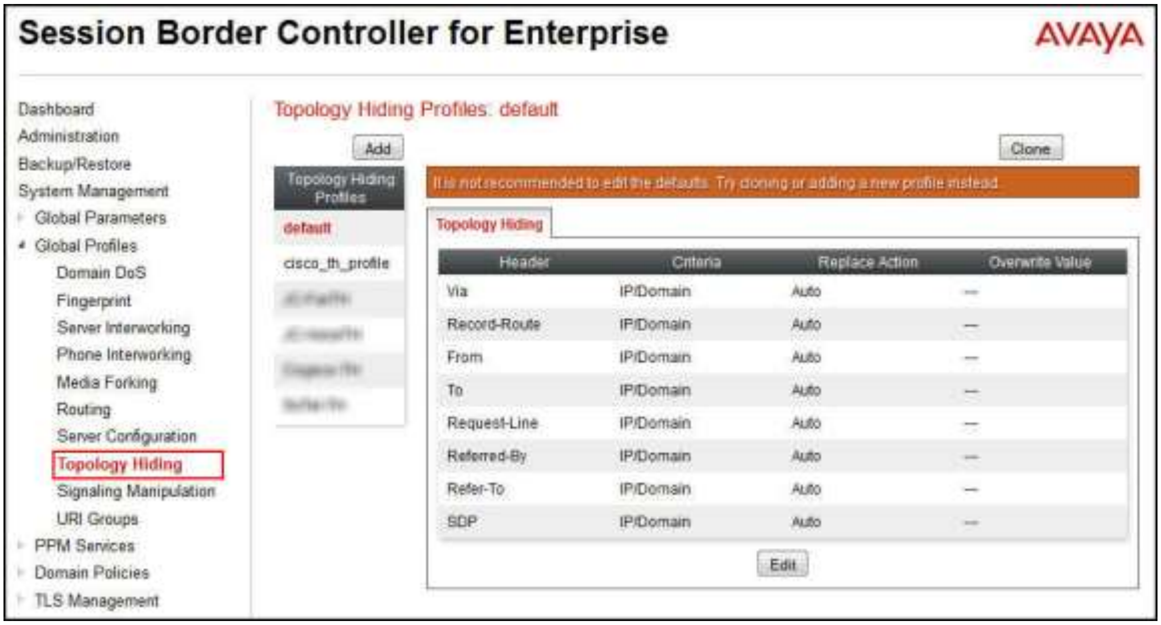
Routing Profiles
- default
- [redacted]
- To-IPO-JCity
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- To-Clearfly
- [redacted]

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport		
1	*	default	Priority	192.168.62.102	UDP	Edit	Delete

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 predefined **default** topology hiding profile (shown below) was used for both Avaya IP Office and the Clearfly SIP servers.

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.



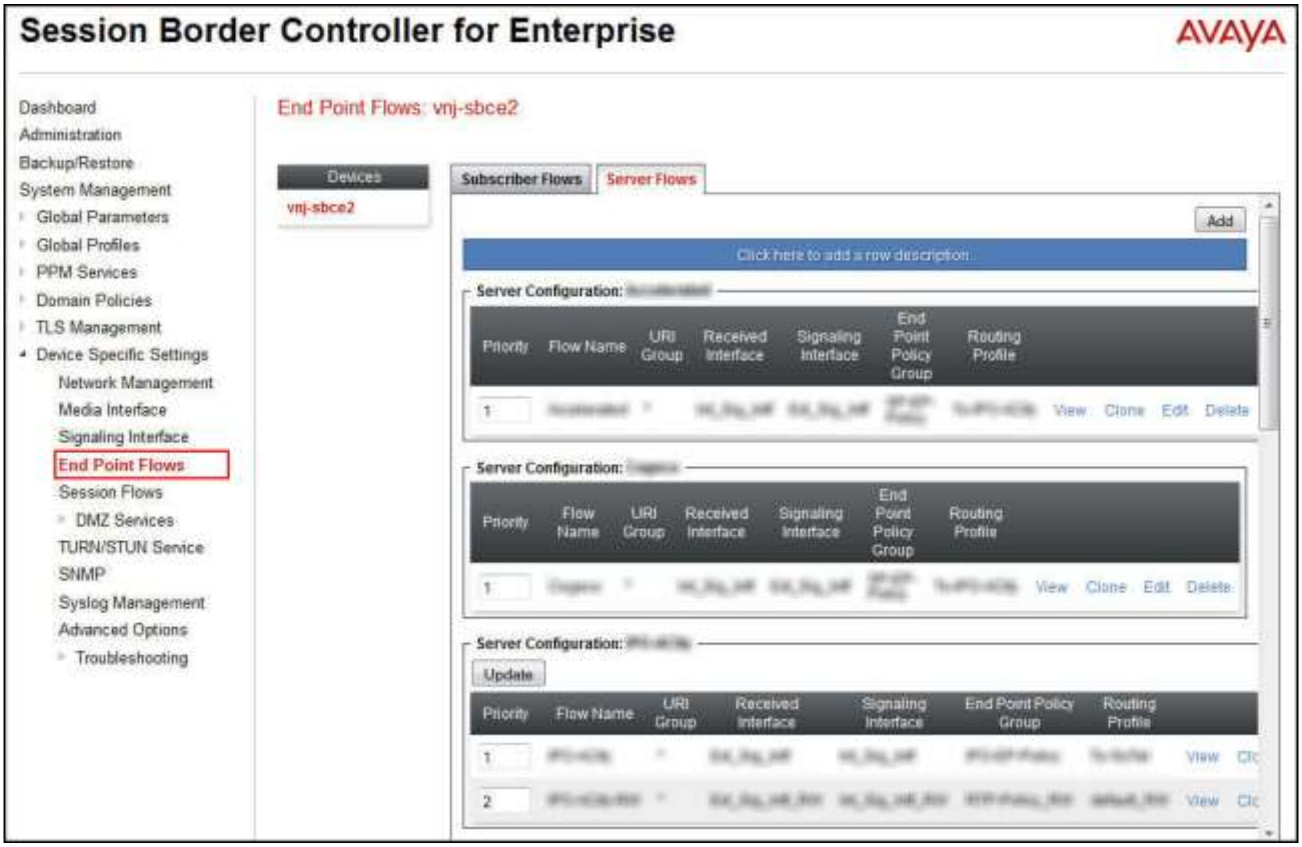
It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

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

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 Clearfly 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 the flow parameters. Once complete, the configured flow is shown in the far right pane under the server name listed beside the **Server Configuration** heading.



End Point Flows: vnj-sbce2

Server Configuration: [illegible]

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	[illegible]	*	[illegible]	[illegible]	[illegible]	[illegible]	View	Clone	Edit	Delete

Server Configuration: [illegible]

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	[illegible]	*	[illegible]	[illegible]	[illegible]	[illegible]	View	Clone	Edit	Delete

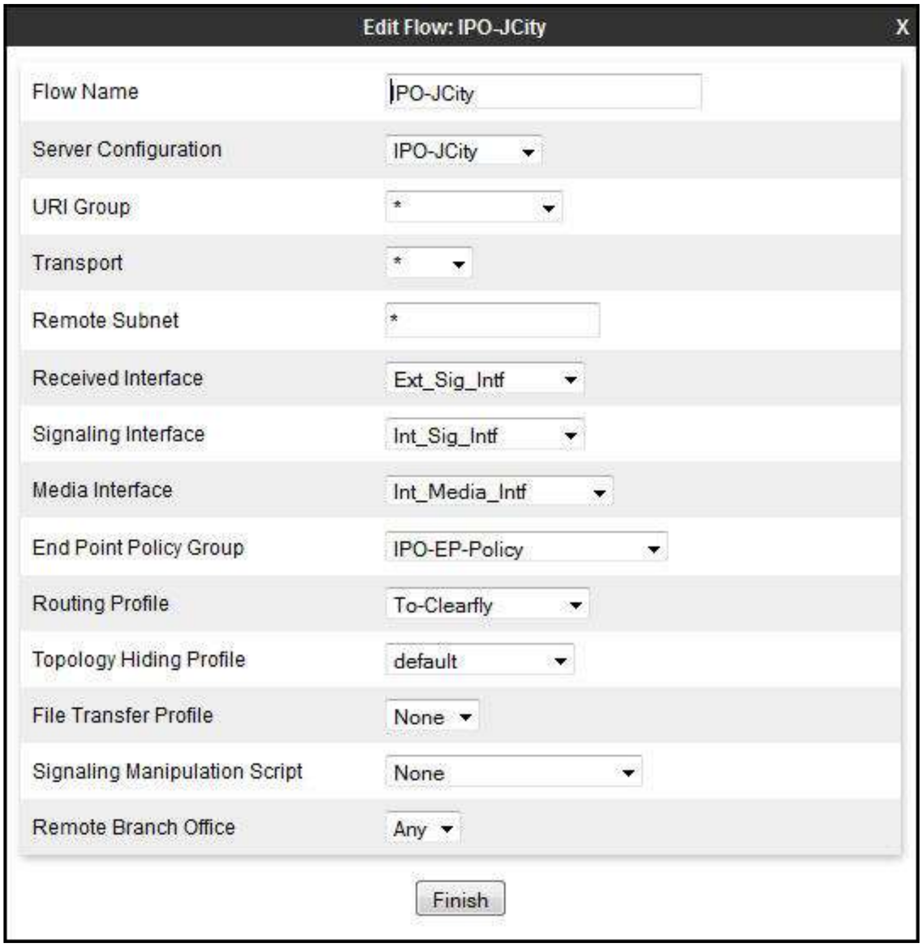
Server Configuration: [illegible]

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile		
1	[illegible]	*	[illegible]	[illegible]	[illegible]	[illegible]	View	Clo
2	[illegible]	*	[illegible]	[illegible]	[illegible]	[illegible]	View	Clo

6.13.1. End Point Flow – Avaya IP Office

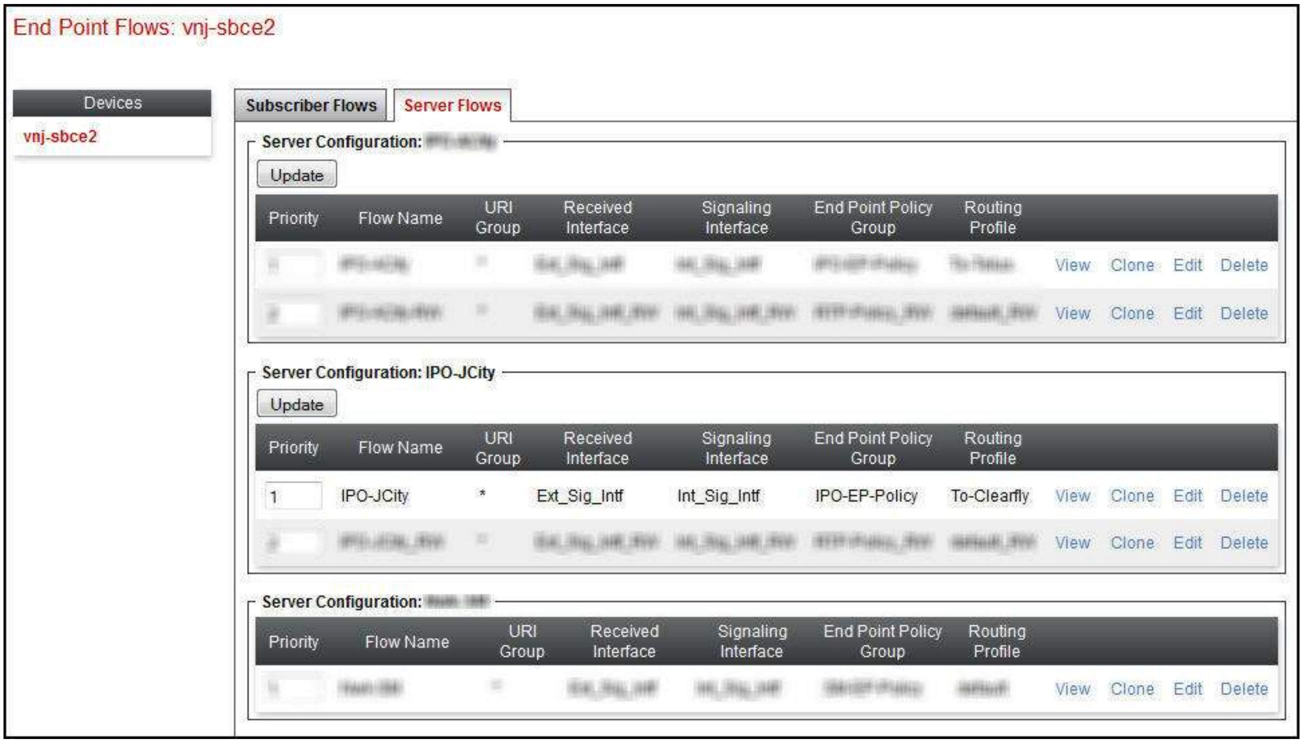
For the compliance test, the end point flow ***IPO-JCity*** was created for Avaya IP Office. All traffic from Avaya IP Office will match this flow as the source flow and use the specified routing profile ***To-Clearfly*** to determine the destination server and corresponding destination flow. The **End 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 Clearfly SIP server.
- Set **Topology Hiding Profile** to the topology hiding profile specified for Avaya IP Office in **Section 6.12**.



Flow Name	IPO-JCity
Server Configuration	IPO-JCity
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig_Intf
Signaling Interface	Int_Sig_Intf
Media Interface	Int_Media_Intf
End Point Policy Group	IPO-EP-Policy
Routing Profile	To-Clearfly
Topology Hiding Profile	default
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

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



End Point Flows: vnj-sbce2

Server Configuration: [redacted]

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

Server Configuration: IPO-JCity

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	IPO-JCity	*	Ext_Sig_Intf	Int_Sig_Intf	IPO-EP-Policy	To-Clearfly	View	Clone	Edit	Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	View	Clone	Edit	Delete

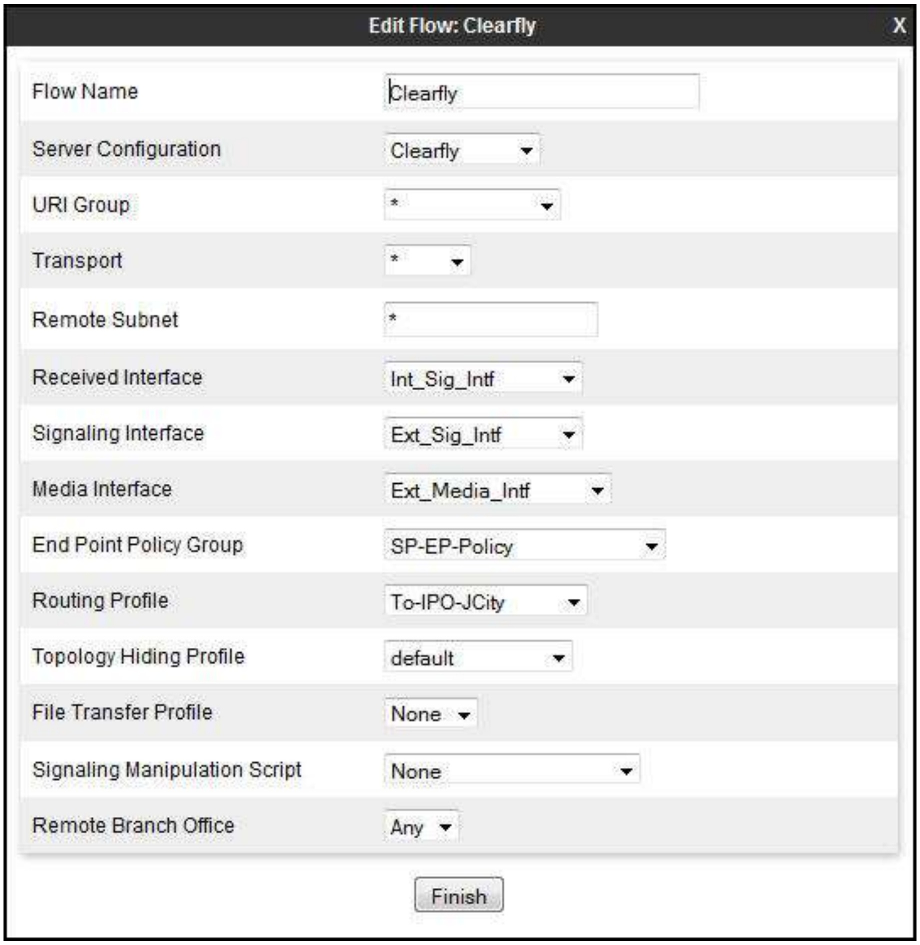
Server Configuration: [redacted]

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

6.13.2. End Point Flow – Clearfly Communications

For the compliance test, the end point flow ***Clearfly*** was created for the Clearfly SIP server. All traffic from Clearfly 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:

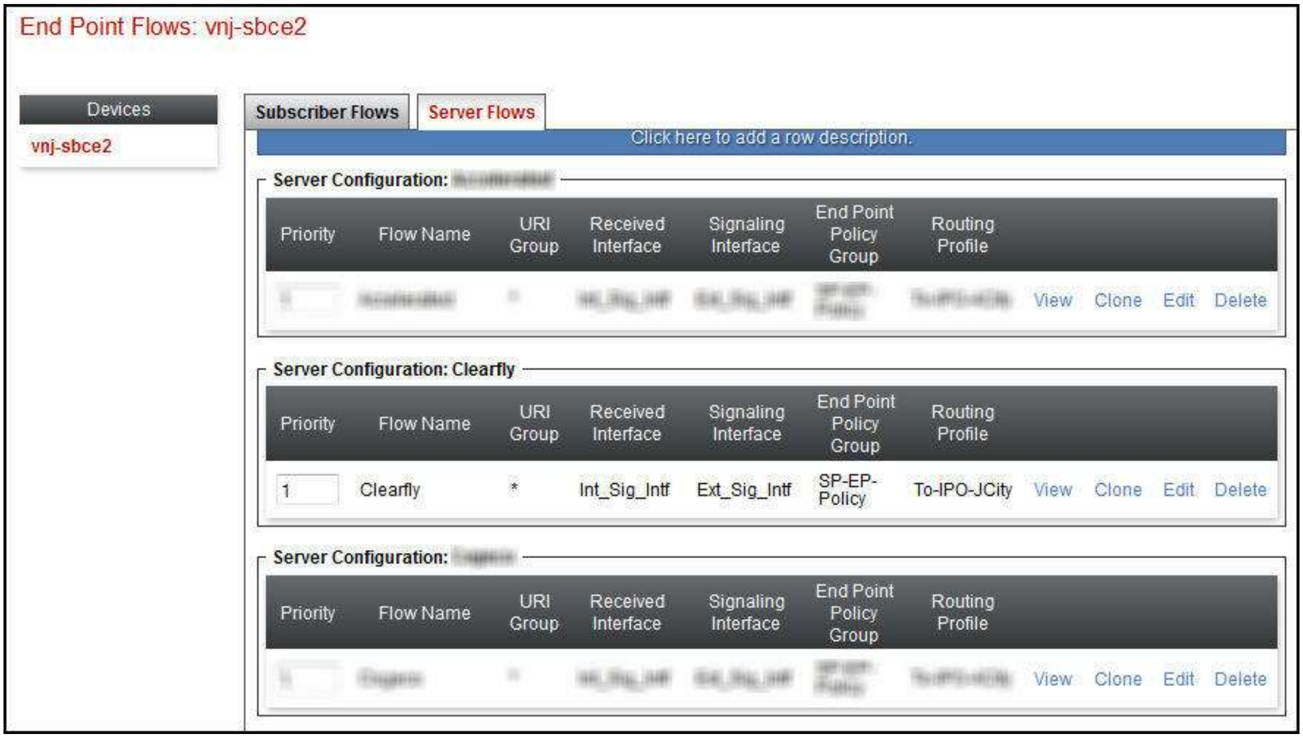
- For **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Clearfly SIP server created in **Section 6.6.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set **Received Interface** to the internal signaling interface.
- 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 Clearfly 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 specified for Clearfly in **Section 6.12**.



Edit Flow: Clearfly

Flow Name	Clearfly
Server Configuration	Clearfly
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_Intf
Signaling Interface	Ext_Sig_Intf
Media Interface	Ext_Media_Intf
End Point Policy Group	SP-EP-Policy
Routing Profile	To-IPO-JCity
Topology Hiding Profile	default
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

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


End Point Flows: vnj-sbce2
Devices
vnj-sbce2
Subscriber Flows
Server Flows
Click here to add a row description.

Server Configuration: [redacted]

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

Server Configuration: Clearfly

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Clearfly	*	Int_Sig_Intf	Ext_Sig_Intf	SP-EP-Policy	To-IPO-JCity	View	Clone	Edit	Delete

Server Configuration: [redacted]

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

7. Clearfly Communications SIP Trunking Configuration

Clearfly 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). Clearfly will provide the customer the necessary information to configure the Avaya IP Office and Avaya SBCE including:

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

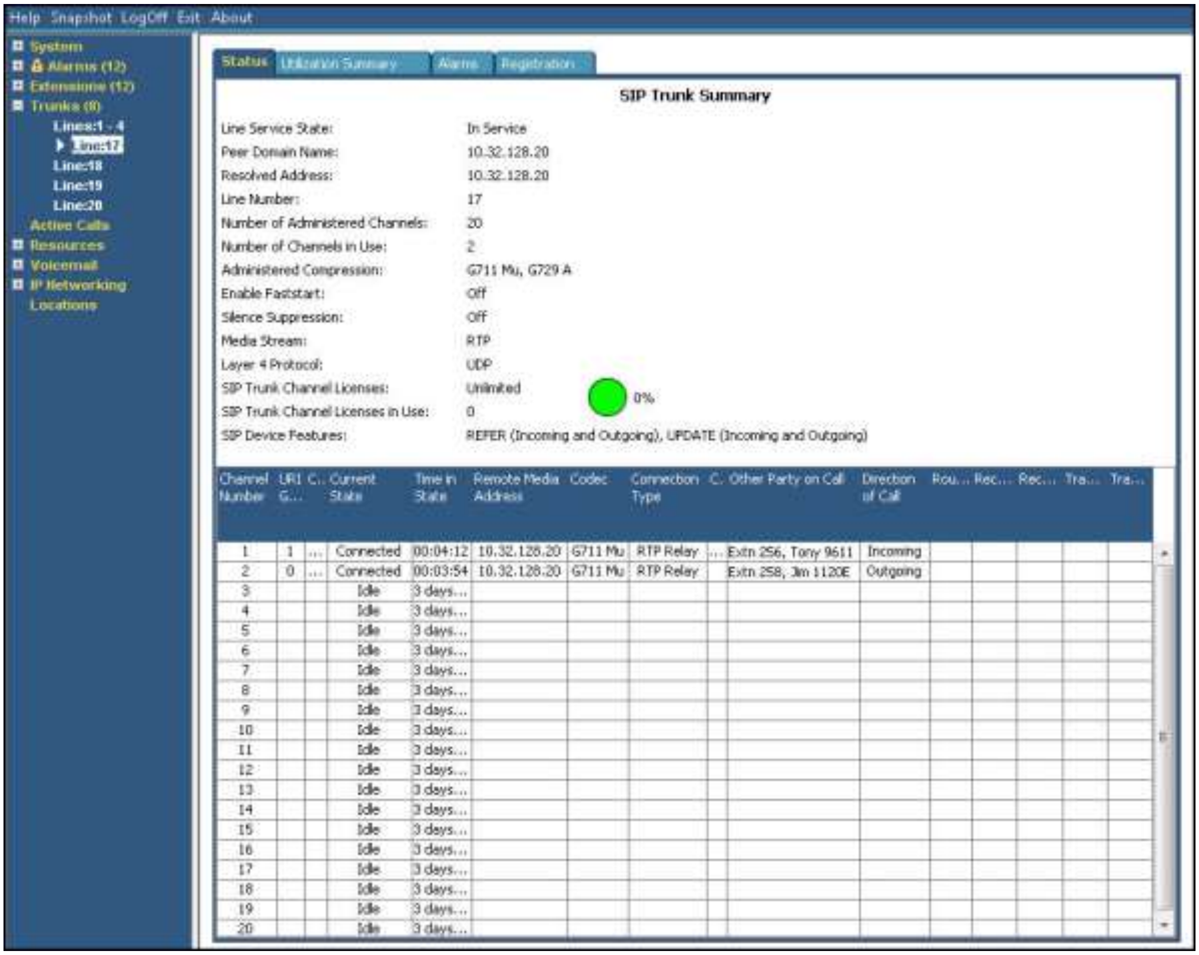
8. Verification Steps

This section provides verification steps that may be performed to verify the solution configuration.

8.1. Avaya IP Office System Status

Use the Avaya IP Office System Status application to check the SIP Line channels state and 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. In the **Status** tab in the right pane, verify the **Current State** is ***Idle*** for channels not taken by active calls; the state should be ***Connected*** for the channels engaged in active calls with the PSTN.

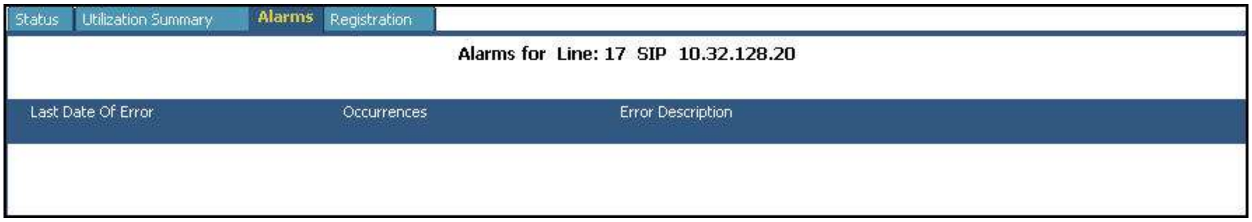


SIP Trunk Summary

Line Service State: In Service
Peer Domain Name: 10.32.128.20
Resolved Address: 10.32.128.20
Line Number: 17
Number of Administered Channels: 20
Number of Channels in Use: 2
Administered Compression: G711 Mu, G729 A
Enable Faststart: Off
Silence Suppression: Off
Media Stream: RTP
Layer 4 Protocol: UDP
SIP Trunk Channel Licenses: Unlimited
SIP Trunk Channel Licenses in Use: 0
SIP Device Features: REFER (Incoming and Outgoing), UPDATE (Incoming and Outgoing)

Channel Number	URI G...	C...	Current State	Time in State	Remote Media Address	Codec	Connection Type	C.	Other Party on Call	Direction of Call	Rou...	Rec...	Rec...	Tra...	Tra...
1	1	...	Connected	00:04:12	10.32.128.20	G711 Mu	RTP Relay	...	Extn 256, Tony 9611	Incoming					
2	0	...	Connected	00:03:54	10.32.128.20	G711 Mu	RTP Relay		Extn 258, Jim 1120E	Outgoing					
3			Idle	3 days...											
4			Idle	3 days...											
5			Idle	3 days...											
6			Idle	3 days...											
7			Idle	3 days...											
8			Idle	3 days...											
9			Idle	3 days...											
10			Idle	3 days...											
11			Idle	3 days...											
12			Idle	3 days...											
13			Idle	3 days...											
14			Idle	3 days...											
15			Idle	3 days...											
16			Idle	3 days...											
17			Idle	3 days...											
18			Idle	3 days...											
19			Idle	3 days...											
20			Idle	3 days...											

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

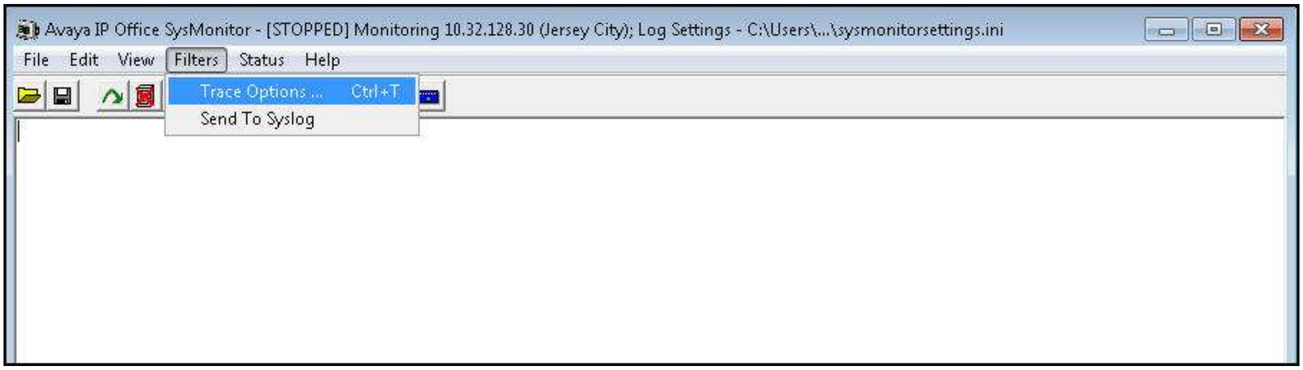


Alarms for Line: 17 SIP 10.32.128.20

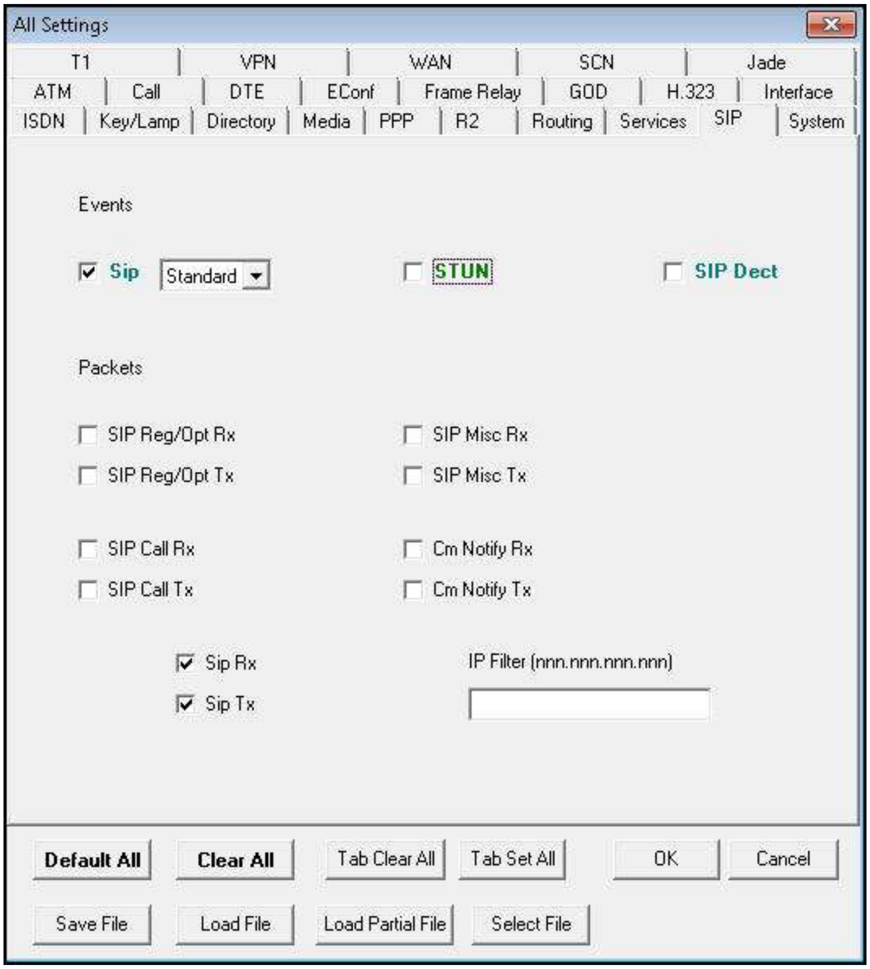
Last Date Of Error	Occurrences	Error Description

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 monitored information to be customized. To customize, select **Filters → Trace Options…** as shown below:


Avaya IP Office SysMonitor - [STOPPED] Monitoring 10.32.128.30 (Jersey City); Log Settings - C:\Users\...\sysmonitorsettings.ini
File
Edit
View
Filters
Status
Help
Trace Options ... Ctrl+T
Send To Syslog

The following screen shows the **SIP** tab of trace options. In this example, **Standard Sip Events** and the **Sip Rx** and **Sip Tx** boxes are checked.



Events

☑ Sip Standard

□ STUN

□ SIP Dect

Packets

□ SIP Reg/Opt Rx

□ SIP Reg/Opt Tx

□ SIP Misc Rx

□ SIP Misc Tx

□ SIP Call Rx

□ SIP Call Tx

□ Cm Notify Rx

□ Cm Notify Tx

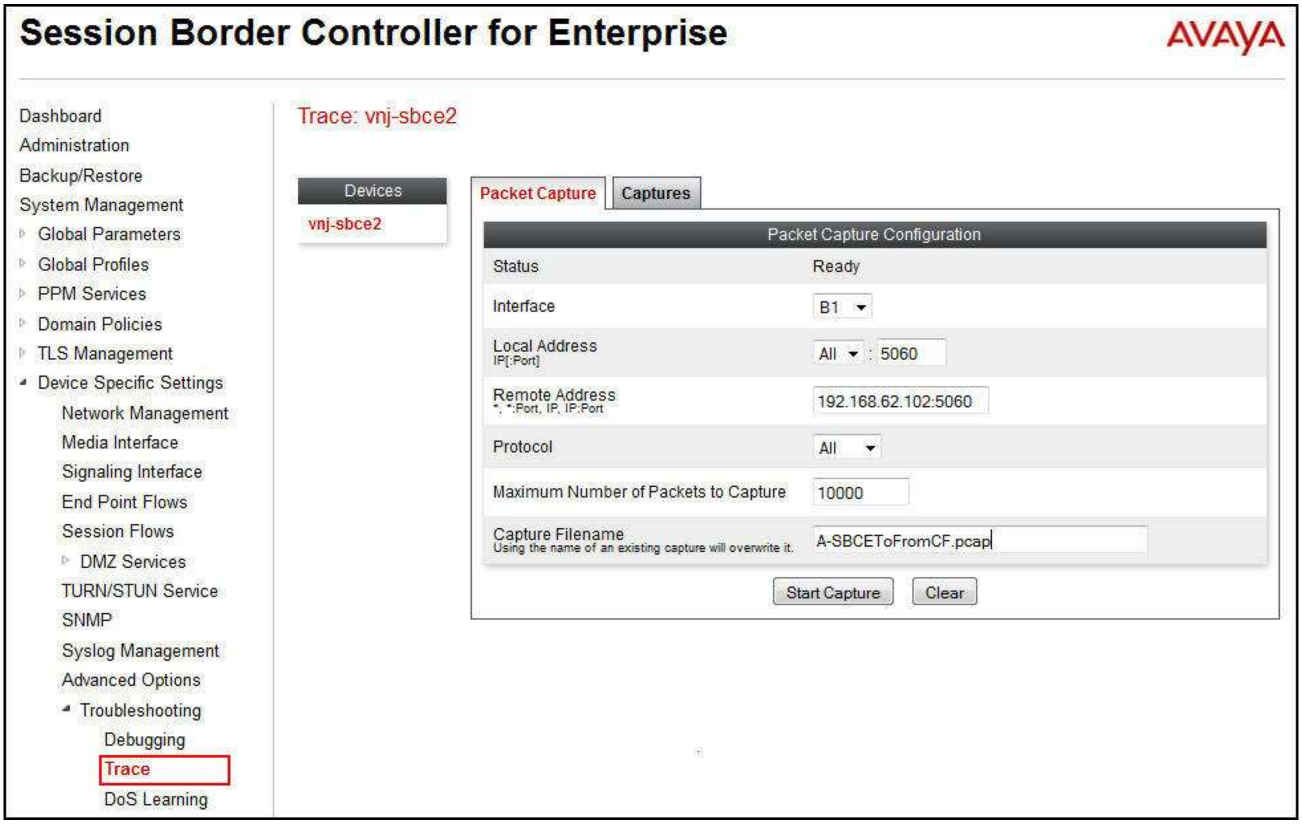
☑ Sip Rx

☑ Sip Tx

IP Filter (nnn.nnn.nnn.nnn)

8.3. Avaya SBCE Traces

The Avaya SBCE can take traces on specified interfaces. SIP signaling crossing both 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. After the trace capture has been stopped, the captured trace file can then be downloaded from the **Captures** tab for examination using a protocol sniffer application such as Wireshark.



Packet Capture Configuration

Status	Ready
Interface	B1
Local Address IP[:Port]	All : 5060
Remote Address *, *:Port, IP, IP:Port	192.168.62.102:5060
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename Using the name of an existing capture will overwrite it.	A-SBCEToFromCF.pcap

9. Conclusion

The Clearfly Communications SIP Trunking Service passed compliance testing with Avaya IP Office R9.1 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 Clearfly as shown in **Figure 1**. Test results and observations are noted in **Section 2.2**.

10. Additional References

[1] *IP Office™ Platform 9.1, Deploying Avaya IP Office™ Platform IP500 V2,* Document Number 15-601042, Issue 30g, January 2015.

[2] *Administering Avaya IP Office™ Platform with Manager*, Release 9.1, Issue 10.04, February 2015.

[3] *IP Office ™ Platform 9.1, Administering Avaya IP Office™ Platform Voicemail Pro*, Document Number 15-601063, Issue 10c, December 2014.

[4] *IP Office™ Platform 9.1, Using IP Office System Monitor*, Document Number 15-601019, Issue 06b, November 2014.

[5] *IP Office™ Platform 9.1, Using Avaya IP Office™ Platform System Status*, Document Number 15-601758, October 2014.

[6] *Using Avaya Communicator on IP Office*, Release 9.1, December 2014.

[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.

[10] RFC 3261 *SIP: Session Initiation Protocol*, http://www.ietf.org/.

[11] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/.

Product documentation for Avaya products may be found at http://support.avaya.com or http://marketingtools.avaya.com/knowledgebase/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf_feed_template.html.

Product documentation for Clearfly SIP Trunking Service is available from Clearfly Communications.

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.