



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Clearly Communications SIP Trunking Service with Avaya IP Office R9.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Avaya IP Office Release 9.1 to inter-operate with the Clearly Communications SIP Trunking Service. Clearly Communications is a member of the Avaya DevConnect Service Provider program..

The Clearly Communications SIP Trunking Service provides PSTN access via a SIP trunk between an enterprise site and the Clearly 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.

1. Introduction

These Application Notes describe the procedures for configuring an enterprise solution using Avaya IP Office Release R9.1 to inter-operate with the Clearfly Communications SIP Trunking Service.

In the sample configuration, the enterprise solution consists of 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 the public Internet. 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 transfers 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.

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.
- **Remote Worker** – Remote Worker (phones connected directly to the public Internet function as enterprise local extensions) is not supported by the combined Avaya/Clearfly solution as documented in these Application Notes since its setup requires the use of an Avaya Session Border Controller for Enterprise (Avaya SBCE) whereas in the tested solution the Avaya SBCE was not used.

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 via the public Internet.

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.

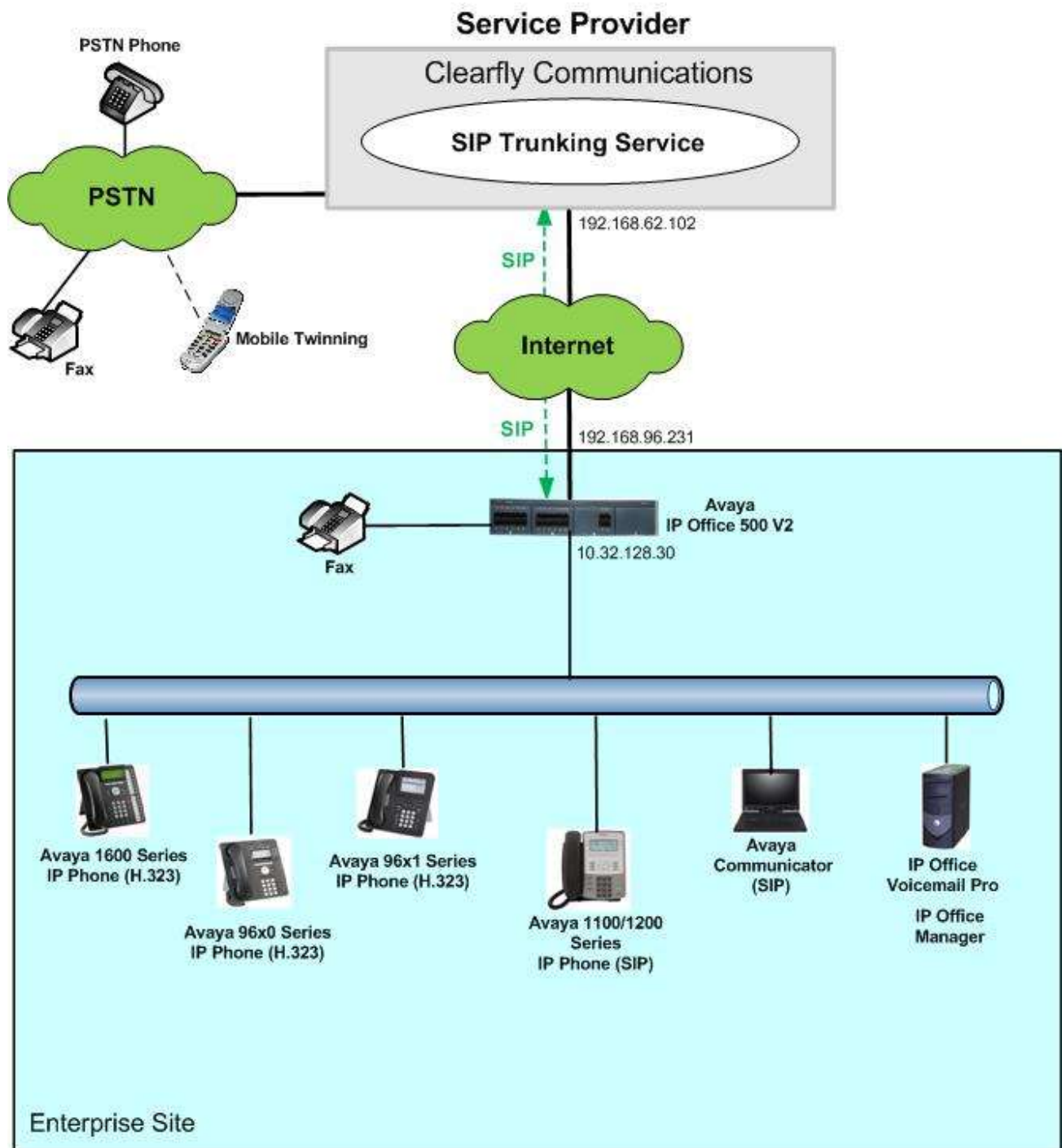


Figure 1: Avaya IP Office with Clearly Communications SIP Trunking Service

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 Clearly. 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. Clearly 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 Clearly SIP Trunking Service, they are not included in these Application Notes.

4. Equipment and Software Validated

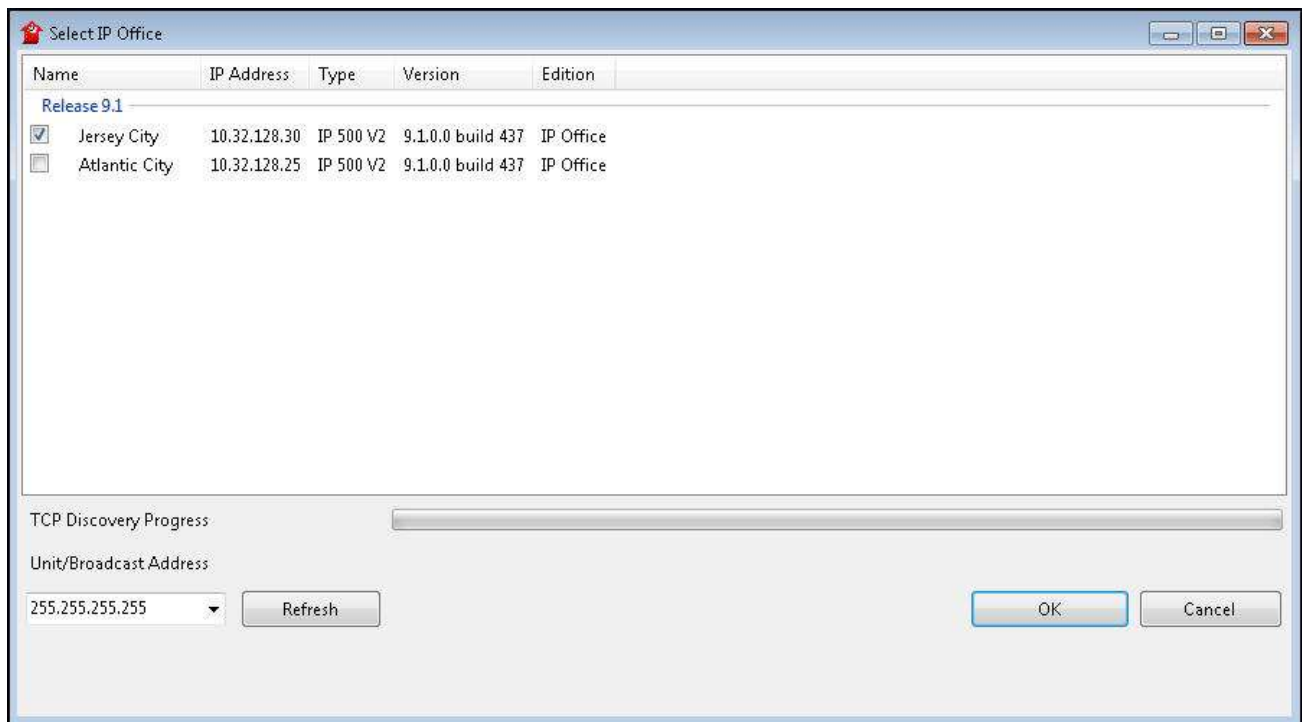
The following equipment and software/firmware were used for the sample configuration provided:

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
Clearly 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.



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.

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

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

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

The screenshot displays the Avaya IP Office configuration window. On the left, the 'IP Offices' navigation pane shows a tree structure with 'Control Unit (2)' expanded, and '1 IP 500 V2' selected. The main pane, titled 'IP 500 V2', shows the following details:

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

The screen below shows the details of the Combination Card.

The screenshot displays the Avaya IP Office configuration window. On the left, the 'IP Offices' navigation pane shows a tree structure with 'Control Unit (2)' expanded, and '2 COMBO6210/ATM4' selected. The main pane, titled 'COMBO6210/ATM4', shows the following details:

Unit	
Device Number	2
Unit Type	COMBO6210/ATM4
Version	9.1.0.437
Serial Number	XXXXXXXXXX
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 – LAN2 Tab

In the sample configuration, *Jersey City* was used as the system name and the WAN port (LAN2) was used to connect the Avaya IP Office to the public Internet (see **Figure 1**). The LAN2 settings correspond to the WAN interface on Avaya IP Office. To access the LAN2 settings, first navigate to **System → Jersey City** in the Navigation Pane and then navigate to the **LAN2 → LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office WAN port. Set the **IP Mask** field to the proper mask value.

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, showing a tree structure with 'Jersey City' selected. The main pane is titled 'Jersey City' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', 'System Events', 'SMTP', 'SMDR', 'Twinning', and 'VCM'. The 'LAN2' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The 'IP Address' field is set to '192 . 168 . 96 . 231' and the 'IP Mask' field is set to '255 . 255 . 255 . 224'. Other fields include 'Primary Trans. IP Address' (0 . 0 . 0 . 0), 'Firewall Profile' (set to '<None>'), 'RIP Mode' (set to 'None'), 'Enable NAT' (checked), 'Number Of DHCP IP Addresses' (200), and 'DHCP Mode' (set to 'Disabled'). An 'Advanced' button is located at the bottom right of the settings area.

Field	Value
IP Address	192 . 168 . 96 . 231
IP Mask	255 . 255 . 255 . 224
Primary Trans. IP Address	0 . 0 . 0 . 0
Firewall Profile	<None>
RIP Mode	None
Enable NAT	<input checked="" type="checkbox"/>
Number Of DHCP IP Addresses	200
DHCP Mode	Server <input type="radio"/> Client <input type="radio"/> Dialin <input type="radio"/> Disabled <input checked="" type="radio"/>

On the **VoIP** tab of LAN2 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 LAN2.
- 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.

The screenshot shows the Avaya IP Office configuration interface for Jersey City. The 'VoIP' tab is selected for LAN2. The 'SIP Trunks Enable' checkbox is checked and highlighted with a red box. Below it, the 'RTP' section is expanded, showing the 'Port Number Range' and 'Port Number Range (NAT)' settings, both with Minimum set to 49152 and Maximum set to 53246. The 'Keepalives' section is also expanded, showing 'Scope' set to RTP, 'Initial keepalives' set to Enabled, and 'Periodic timeout' set to 30. These three sections are highlighted with red boxes.

Jersey City

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | Twinning | VCM | Codecs | VoIP

LAN Settings | VoIP | Network Topology

☐ 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:

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

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.

The screenshot shows the Avaya IP Office configuration interface for 'Jersey City'. The 'VoIP' tab is selected, and the 'Network Topology' sub-tab is active. The 'DiffServ Settings' section is highlighted with a red box. Below it, the 'DHCP Settings' section is visible.

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 LAN2 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 IP Address** to the IP address of the Avaya IP Office WAN port.
- Set **Public Port** to **5060** for **UDP**.

The screenshot shows the 'Jersey City' VoIP configuration interface. The 'Network Topology' tab is selected under the 'LAN2' section. The 'Network Topology Discovery' panel contains the following settings:

- STUN Server Address:** 192.168.96.231
- STUN Port:** 3478
- Firewall/NAT Type:** Open Internet (highlighted with a red box)
- Binding Refresh Time (seconds):** 120
- Public IP Address:** 192 . 168 . 96 . 231
- Public Port:**
 - UDP:** 5060 (highlighted with a red box)
 - TCP:** 0
 - TLS:** 0
- ☐ Run STUN on startup

Buttons for 'Run STUN' and 'Cancel' are located to the right of the configuration fields.

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).

The screenshot shows the 'Jersey City' configuration window for the 'Voicemail' tab. The 'Voicemail Type' is set to 'Voicemail Lite/Pro'. The 'Voicemail IP Address' is set to 10.32.128.78. The 'SIP Settings' section is highlighted with a red box, showing 'SIP Name' as 4086505538, 'SIP Display Name (Alias)' as Voicemail, 'Contact' as 4086505538, and the 'Anonymous' checkbox is unchecked. Other settings include 'Auto-Attendant' set to 2, 'Voice Recording' set to 5, 'Mandatory Voice Recording' set to 5, 'Announcements' set to 5, 'Mailbox Access' set to 5, 'DTMF Breakout' set to Reception / Breakout (DTMF 0), 'Breakout (DTMF 2)' set to Breakout (DTMF 2), 'Breakout (DTMF 3)' set to Breakout (DTMF 3), 'Voicemail Code Complexity' set to Enforcement with a minimum length of 4, and 'Call Recording' set to Auto Restart Paused Recording (secs) 15. The 'Outcalling Control' checkbox is checked.

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.

The screenshot shows the 'Jersey City' configuration window with the 'Telephony' tab selected. The 'Telephony' sub-tab is also active. The 'Hold Timeout (secs)' field is set to 0. The 'Companding Law' section shows 'U-Law' selected for both 'Switch' and 'Line'. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked. Other settings include 'Default Outside Call Sequence' set to 'Normal', 'Default Inside Call Sequence' set to 'Ring Type 1', 'Default Ring Back Sequence' set to 'Ring Type 2', 'Restrict Analogue Extension Ringer Voltage' unchecked, 'Dial Delay Time (secs)' set to 4, 'Dial Delay Count' set to 0, 'Default No Answer Time (secs)' set to 15, 'Park Timeout (secs)' set to 300, 'Ring Delay (secs)' set to 5, 'Call Priority Promotion Time (secs)' set to 'Disabled', 'Default Currency' set to 'USD', 'Default Name Priority' set to 'Favor Trunk', 'Media Connection Preservation' set to 'Enabled', 'Phone Failback' set to 'Manual', 'Login Code Complexity' set to 'Enforcement' with 'Minimum length' set to 4, and 'Complexity' unchecked. The 'DSS Status' checkbox is unchecked, 'Auto Hold' is checked, 'Dial By Name' is checked, 'Show Account Code' is checked, 'Restrict Network Interconnect' is checked, 'Include location specific information' is unchecked, 'Drop External Only Impromptu Conference' is unchecked, 'Visually Differentiate External Call' is unchecked, 'Unsupervised Analog Trunk Disconnect Handling' is unchecked, 'High Quality Conferencing' is checked, 'Digital/Analogue Auto Create User' is checked, and 'Directory Overrides Barring' is unchecked. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

5.2.4. System - Twinning Tab

To view or change the System Twinning settings, navigate to the **Twining** 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.

The screenshot shows the 'Jersey City' system configuration window with the 'Twining' tab selected. The 'Send original calling party information for Mobile Twinning' checkbox is unchecked. Below it, the 'Calling party information for Mobile Twinning' text box is empty.

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.

The screenshot shows the 'Jersey City' system configuration window with the 'Codecs' tab selected. The 'RFC2833 Default Payload' dropdown is set to '101'. Below this, the 'Available Codecs' list on the left has all five items checked: G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, G.729(a) 8K CS-ACELP, and G.723.1 6K3 MP-MLQ. The 'Default Codec Selection' area in the center has an empty 'Unused' list and a 'Selected' list containing the same five codecs. Navigation buttons (right arrow, up arrow, down arrow, left arrow) are located between the lists.

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 gateway for the public Internet to which the IP Office WAN port is connected.
- Set **Destination** to **LAN2** from the drop-down list.

The screenshot displays the IP Office configuration interface. On the left is the 'IP Offices' navigation pane, showing a tree structure with various configuration categories like BOOTP, Operator, Jersey City, System, Line, Control Unit, Extension, User, Group, Short Code, Service, RAS, Incoming Call Route, WAN Port, Directory, Time Profile, Firewall Profile, IP Route (4), Account Code, License, Tunnel, User Rights, ARS, RAS Location Request, Location, and Authorization Code. The 'IP Route' category is expanded, and the '0.0.0.0' route is selected. The main configuration area on the right is titled '0.0.0.0*' and contains the following fields:

IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	192 . 168 . 96 . 254
Destination	LAN2
Metric	0
<input type="checkbox"/> 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 (500 V2) and IP Office Server Edition systems.

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

- IP addresses.
- SIP Credentials (if applicable).
- SIP URI entries.
- Setting of the **Use Network Topology Info** field on the SIP Line **Transport** tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated after the SIP Line is created via the template. The resulting SIP Line 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.

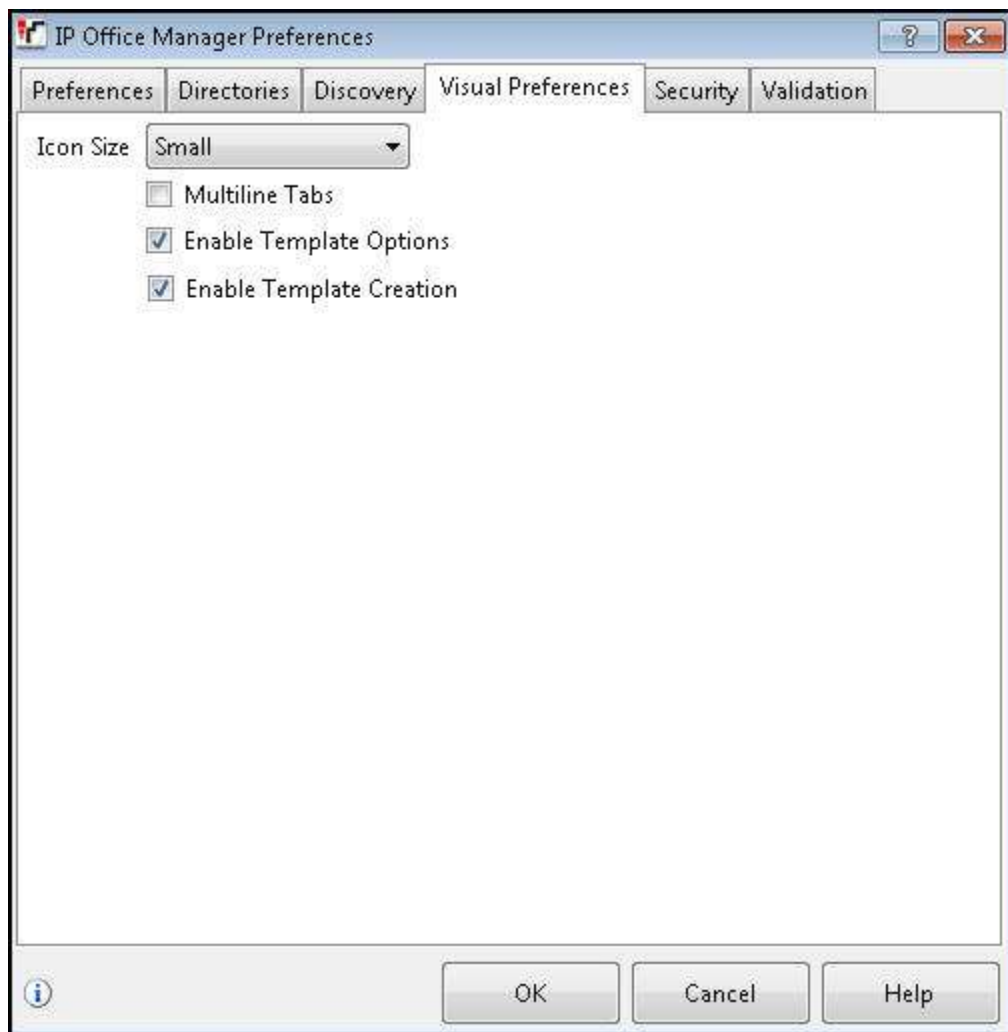
5.4.1. Create SIP Line From Template

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

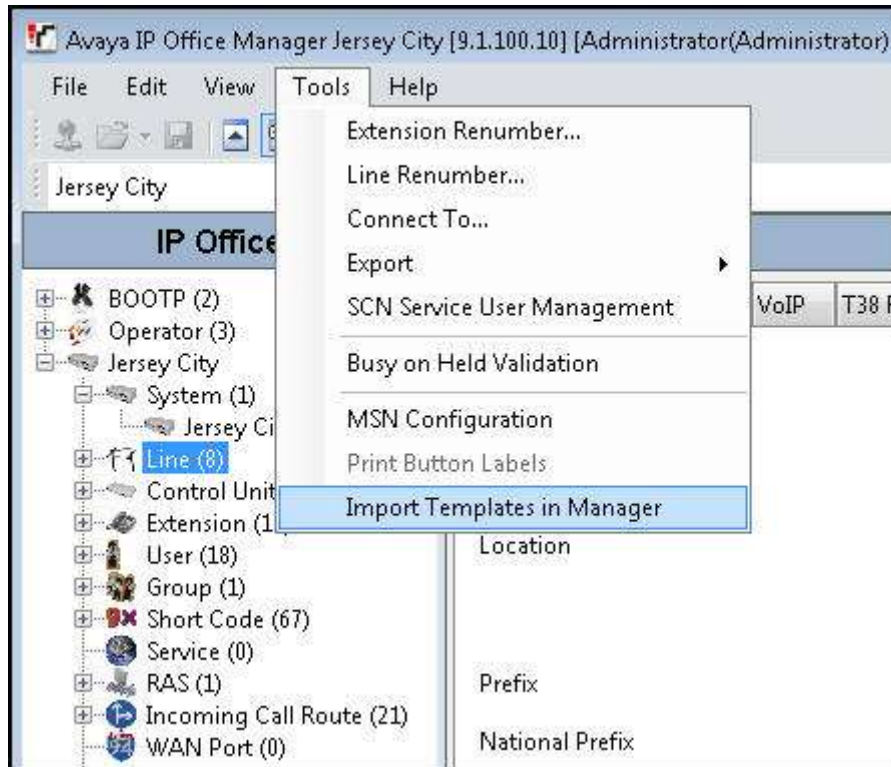
AF_Clearfly Communications_SIPTrunk.xml.

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**.



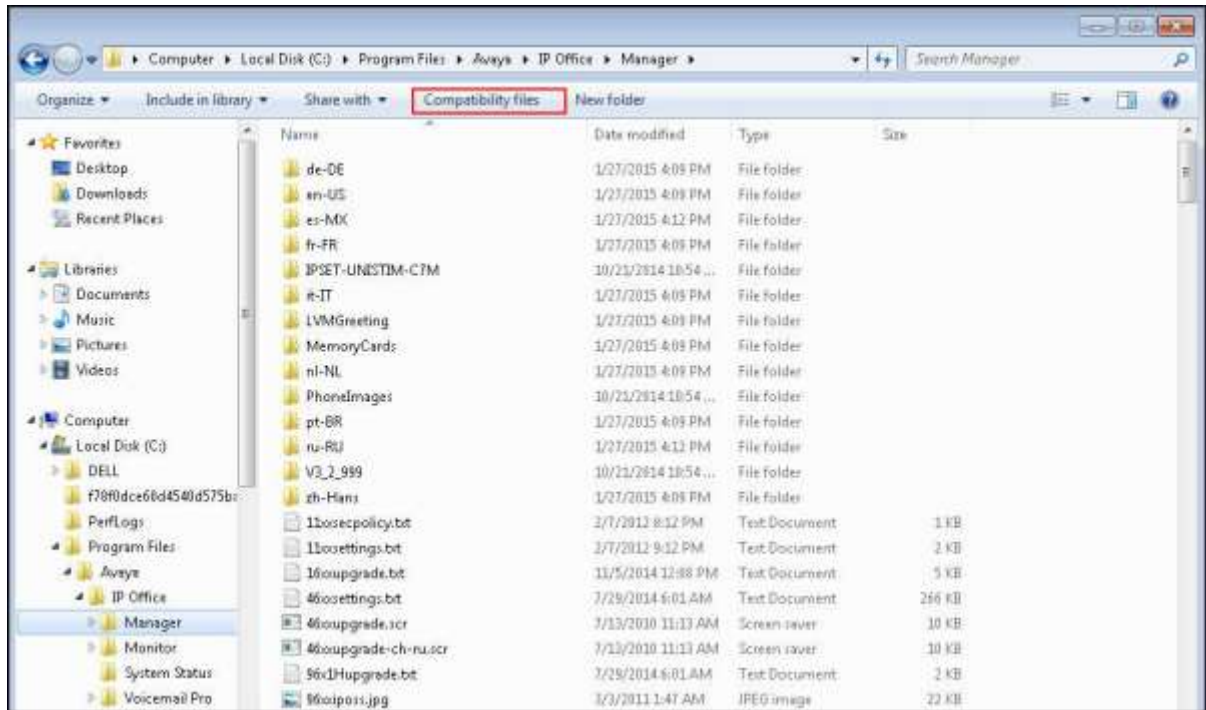
3. Import the template into IP Office Manager. From IP Office Manager, select **Tools** → **Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 4**. The default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



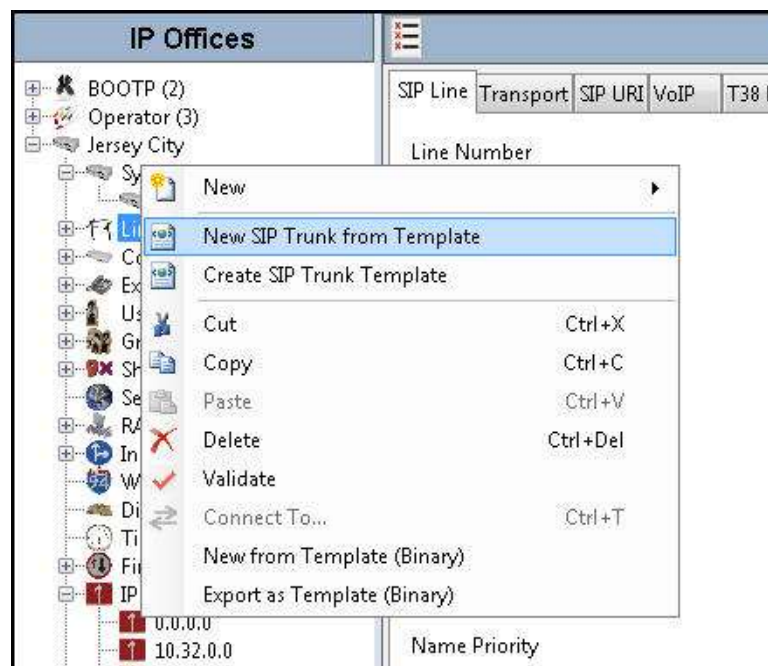
In the pop-up window that appears (not shown), select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue.

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.



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



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



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 service provider SIP Trunking access interface (provided by the service provider) which the SIP Line is connecting to.
- 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**. Clearly 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.

The screenshot displays the Avaya IP Office configuration window for 'SIP Line - Line 17'. The left sidebar shows a tree view of system components, with 'Line 17' selected. The main pane shows the 'SIP Line' tab with various configuration fields. Red boxes highlight the following settings:

- Line Number:** 17
- In Service:** ☒
- ITSP Domain Name:** 192.168.62.102
- Check OOS:** ☒
- Session Timers:**
 - Refresh Method:** Auto
 - Timer (seconds):** 240
- Forwarding and Twinning:**
 - 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 service provider SIP Trunking access interface (provided by the service provider) which the SIP Line is connecting to.
- 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**.

The screenshot shows the 'SIP Line - Line 17*' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '192.168.62.102'. The 'Network Configuration' section shows 'Layer 4 Protocol' set to 'UDP', 'Send Port' set to '5060', 'Use Network Topology Info' set to 'LAN 2', and 'Listen Port' set to '5060'. The 'Explicit DNS Server(s)' are set to '0.0.0.0'. The 'Calls Route via Registrar' checkbox is checked. The 'Separate Registrar' field is empty.

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...	1...	1...	1...	1...	0: <Non...	10
2	17 0	1...	408650...	40865...	FNE31	N...	0: <Non...	10

Edit Channel

Via: 192.168.96.231

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		OK	Cancel
Via	192.168.96.231		
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 Clearly. 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**.

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.

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'T38 Fax' tab selected. The window has a menu bar with 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'T38 Fax' tab contains the following settings:

- T38 Fax Version:** A dropdown menu set to '0'.
- Transport:** A dropdown menu set to 'UDPTL'.
- Redundancy:** A section containing two spinners: 'Low Speed' set to '2' and 'High Speed' set to '2'.
- TCF Method:** A dropdown menu set to 'Trans TCF'.
- Max Bit Rate (bps):** A dropdown menu set to '14400'.
- EFlag Start Timer (msecs):** A spinner set to '2600'.
- EFlag Stop Timer (msecs):** A spinner set to '2300'.
- Tx Network Timeout (secs):** A spinner set to '150'.
- Checkboxes:** 'Scan Line Fix-up' (checked), 'TFOP Enhancement' (checked), 'Disable T30 ECM' (checked), 'Disable EFlags For First DIS' (unchecked), 'Disable T30 MR Compression' (unchecked), and 'NSF Override' (unchecked).
- Country Code:** A spinner set to '0'.
- Vendor Code:** A spinner set to '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 Control** area, **Emulate NOTIFY for REFER** is checked. 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.

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'SIP Advanced' tab selected. The window is divided into several sections: Addressing, Identity, Media, and Call Control. In the Identity section, 'Use PAI for Privacy' and 'Caller ID from From header' are checked. In the Media section, 'Media Connection Preservation' is set to 'System'. In the Call Control section, 'Emulate NOTIFY for REFER' and 'No REFER if using Diversion' are checked. Red boxes highlight these specific settings.

Section	Parameter	Value/Status
Addressing	Association Method	By Source IP address
	Call Routing Method	Request URI
Identity	Suppress DNS SRV Lookups	<input type="checkbox"/>
	Use Phone Context	<input type="checkbox"/>
	Add user=phone	<input type="checkbox"/>
	Use + for International	<input type="checkbox"/>
	Use PAI for Privacy	<input checked="" type="checkbox"/>
	Use Domain for PAI	<input type="checkbox"/>
	Swap From and PAI	<input type="checkbox"/>
Media	Media Connection Preservation	System
	Force Early Direct Media	<input type="checkbox"/>
Call Control	Call Initiation Timeout (s)	4
	Call Queuing Timeout (m)	5
	Service Busy Response	406 - Busy Here
	on No User Responding Send	408-Request Timeout
	Action on CAC Location Limit	Allow Voicemail
	Suppress Q.858 Reason Header	<input type="checkbox"/>
	Emulate NOTIFY for REFER	<input checked="" type="checkbox"/>
	No REFER if using Diversion	<input checked="" type="checkbox"/>
	Send From In Clear	<input type="checkbox"/>
	Cache Auth Credentials	<input checked="" type="checkbox"/>

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"@192.168.62.102"**. 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 service provider network access interface towards which the outbound call is sent.
- 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.

Short Code	
Code	9N;
Feature	Dial
Telephone Number	N"@192.168.62.102"
Line Group ID	17
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

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.

The screenshot shows a configuration window titled "8N;: Dial". It contains the following fields and options:

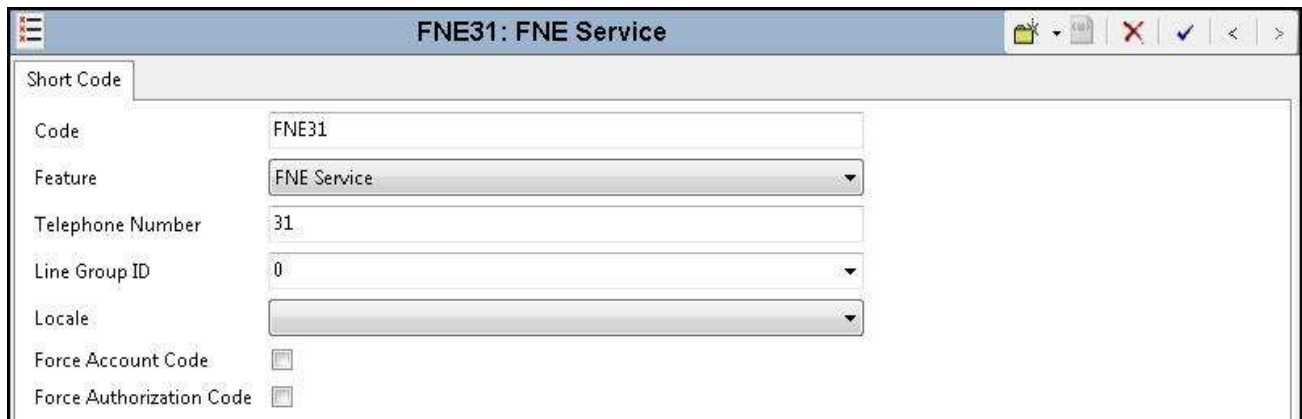
- Code:** 8N;
- Feature:** Dial (selected from a dropdown menu)
- Telephone Number:** N
- Line Group ID:** 50: Main (selected from a dropdown menu)
- Locale:** (empty dropdown menu)
- Force Account Code:** ☐
- Force Authorization Code:** ☐

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

The screenshot shows a configuration window titled "*67N;: Dial*". It contains the following fields and options:

- Code:** *67N;
- Feature:** Dial (selected from a dropdown menu)
- Telephone Number:** WN"@192.168.62.102"
- Line Group ID:** 17 (selected from a dropdown menu)
- Locale:** (empty dropdown menu)
- 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.

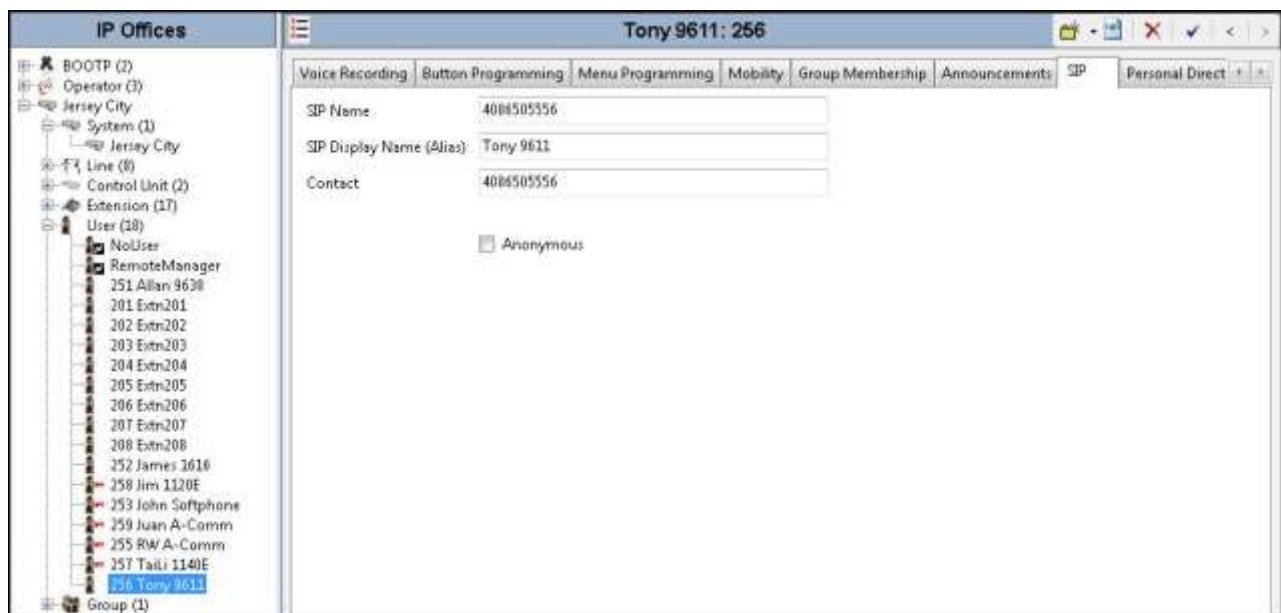


Short Code	
Code	FNE31
Feature	FNE Service
Telephone Number	31
Line Group ID	0
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

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 Clearly. 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**).



IP Offices	
<ul style="list-style-type: none"> BOOTP (2) Operator (3) Jersey City <ul style="list-style-type: none"> System (1) Jersey City <ul style="list-style-type: none"> Line (6) Control Unit (2) Extension (17) User (18) <ul style="list-style-type: none"> NoUser RemoteManager 251 Allan 9638 201 Extn201 202 Extn202 203 Extn203 204 Extn204 205 Extn205 206 Extn206 207 Extn207 208 Extn208 252 James 3616 258 Jim 1120E 253 John Softphone 259 Juan A-Comm 255 RW A-Comm 257 Tai Li 1140E 256 Tony 9611 Group (1) 	<div> <div>Tony 9611: 256</div> <div> Voice Recording Button Programming Menu Programming Mobility Group Membership Announcements SIP Personal Direct </div> </div> <div> SIP Name: 4084505556 SIP Display Name (Alias): Tony 9611 Contact: 4084505556 <input type="checkbox"/> Anonymous </div>

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.

IP Offices

17 4086505556

Standard Voice Recording Destinations

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

Standard Voice Recording Destinations

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).

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**.

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.

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.

The screenshot shows the IP Office configuration interface for the ARS route named 'Main'. The left pane shows the navigation tree with 'ARS' expanded. The main pane displays the configuration for the 'Main' route. The 'ARS Route Id' is 50, 'Route Name' is 'Main', 'Dial Delay Time' is 'System Default (4)', and 'Description' is empty. The 'In Service' checkbox is checked. The 'Out of Service Route' is set to '50: backup'. The 'Time Profile' is set to '<None>'. The 'Out of Hours Route' is set to '<None>'. Below these, there is a table for 'Code', 'Telephone Number', 'Feature', and 'Line Group ID'. The table has two rows: one for '911' with 'Dial Emergency' feature and '1' line group, and another for 'N' with 'Dial' feature and '17' line group. At the bottom, the 'Alternate Route Priority Level' is set to '3' and the 'Alternate Route Wait Time' is set to '30'. The 'Alternate Route' is set to '50: backup'.

Code	Telephone Number	Feature	Line Group ID
911	911	Dial Emergency	1
N	N*0162.168.62.102*	Dial	17

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

5.9. Mobility

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view shows the hierarchy: IP Offices > Jersey City > System (1) > Jersey City > Line (8) > Control Unit (2) > Extension (17) > User (18). The user '256 Tony 9611' is selected. The main configuration area is titled 'Tony 9611: 256*' and has tabs for Telephony, Forwarding, Dial In, Voice Recording, Button Programming, Menu Programming, Mobility, and Group Membership. The 'Mobility' tab is active. It contains sections for 'Internal Twinning' (Twinned Handset, Maximum Number of Calls), 'Mobility Features' (checked), 'Mobile Twinning' (checked), and 'Mobile Call Control' (checked). The 'Twinned Mobile Number (including dial access code)' is set to '919088485526'. Other settings include Twinned Time Profile, Mobile Dial Delay, Mobile Answer Guard, and checkboxes for Hunt group calls, Forwarded calls, Twin When Logged Out, one-X Mobile Client, and 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

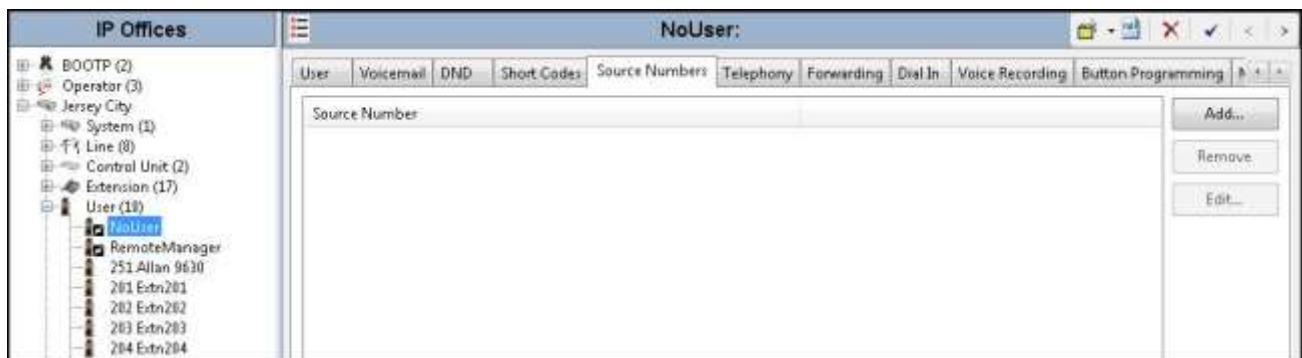
twinned mobile number (without the leading short code digit and the PSTN access code 1 for the North American Numbering Plan), otherwise the Avaya IP Office responds with a “486 Busy Here” message and the caller will hear busy tones.

5.10. SIP Options

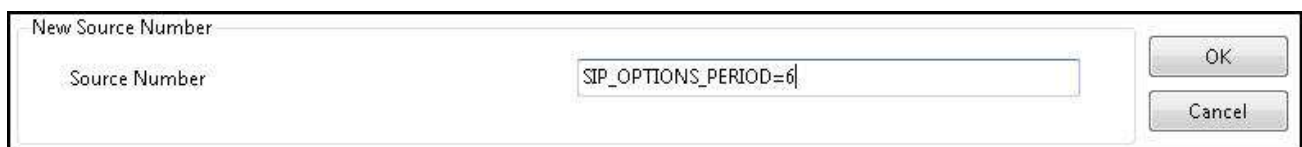
Avaya IP Office sends SIP OPTIONS messages periodically to determine if the SIP connection is active. By default, Avaya IP Office Release 9.1 sends out OPTIONS every 300 seconds. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time** (in seconds) set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

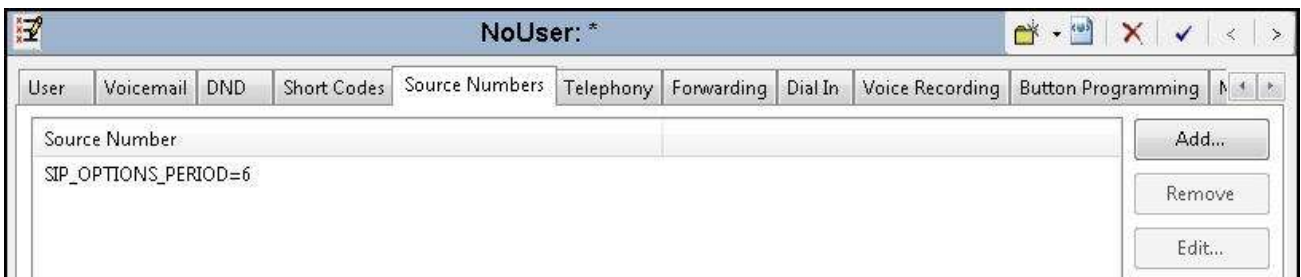
To configure the **SIP_OPTIONS_PERIOD** parameter, navigate to **User → NoUser** in the Navigation Pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.



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**.



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

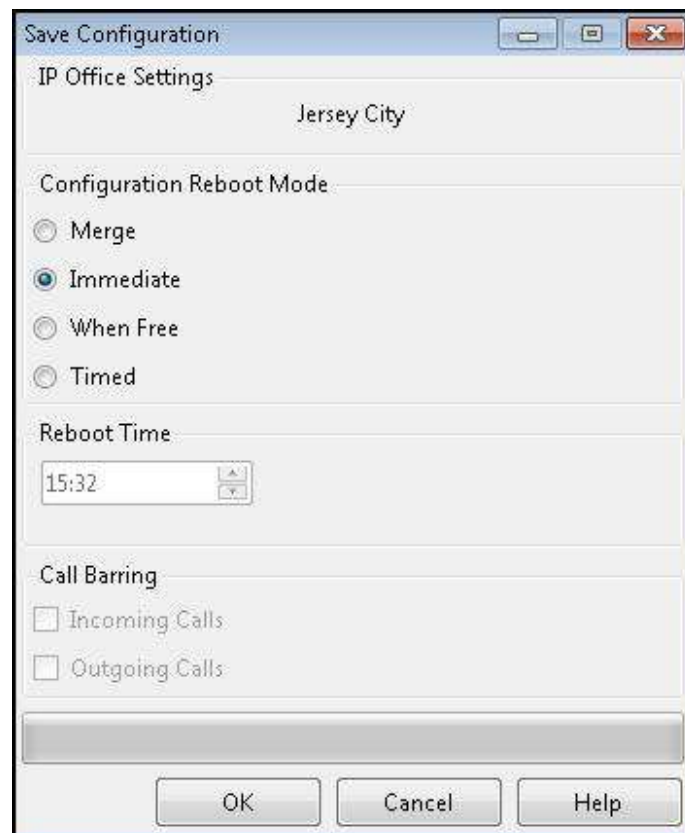


For the compliance test, an OPTIONS period of 2 minutes was desired. The **Binding Refresh Time** was set to **120** seconds in **Section 5.2.1**. Thus, there was no need to define **SIP_OPTIONS_PERIOD**.

5.11. Save Configuration

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

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



6. Clearly Communications SIP Trunking Configuration

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

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

7. Verification Steps

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

7.1. 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.

The screenshot shows the Avaya IP Office System Status application. The left pane displays a tree view with categories: System, Alarms (0), Extensions (12), Trunks (8), Active Calls, Resources, Voicemail, IP Networking, and Locations. Under Trunks, 'Line:17' is selected. The right pane shows the 'Status' tab for 'Line:17'. The 'SIP Trunk Summary' section displays the following information:

- Line Service State: In Service
- Peer Domain Name: 192.168.62.102
- Resolved Address: 192.168.62.102
- 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: UPDATE (Incoming and Outgoing)

A green circle indicates 0% utilization. Below the summary is a table showing the status of 20 channels:

Channel Number	URI	C. G.	Current State	Time in State	R. Codec	Connection Type	C. Other Party on Call	Direction of Call	Round Trip D...	Receive Jitter	Receive Packet...	Transmit Jitter	Transmit Packet...
1		1	Connected	00:04:46	G711 Mu	RTP Relay	Extn 256, Tony 9611	Incoming					
2		0	Connected	00:04:30	G711 Mu	RTP Relay	Extn 258, Jim 1120E	Outgoing					
3			Idle	06:29:46									
4			Idle	06:37:37									
5			Idle	06:37:37									
6			Idle	06:37:37									
7			Idle	06:37:37									
8			Idle	06:37:37									
9			Idle	06:37:37									
10			Idle	06:37:37									
11			Idle	06:37:37									
12			Idle	06:37:37									
13			Idle	06:37:37									
14			Idle	06:37:37									
15			Idle	06:37:37									
16			Idle	06:37:37									
17			Idle	06:37:37									
18			Idle	06:37:37									
19			Idle	06:37:37									
20			Idle	06:37:37									

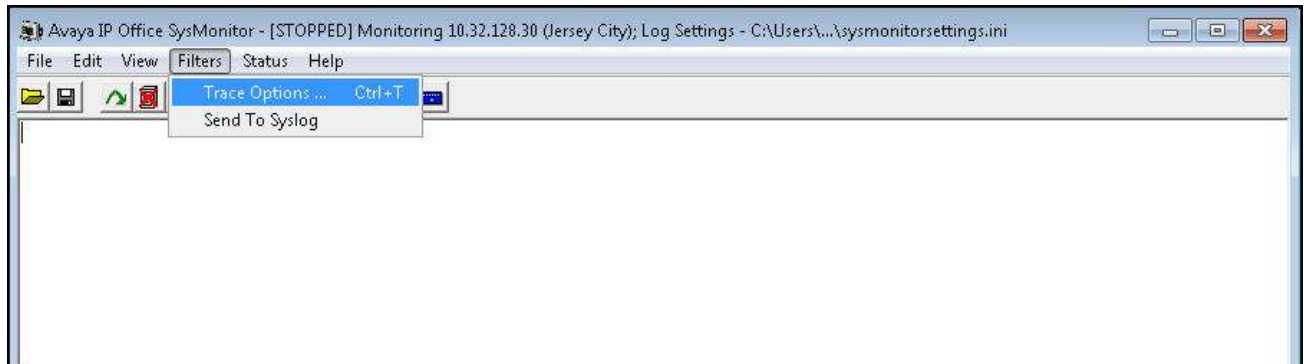
- Select the **Alarms** tab and verify that no alarms are active on the SIP Line.

The screenshot shows the 'Alarms' tab in the Avaya IP Office System Status application. The title bar indicates 'Alarms for Line: 17 SIP 192.168.62.102'. The table below shows the alarm history:

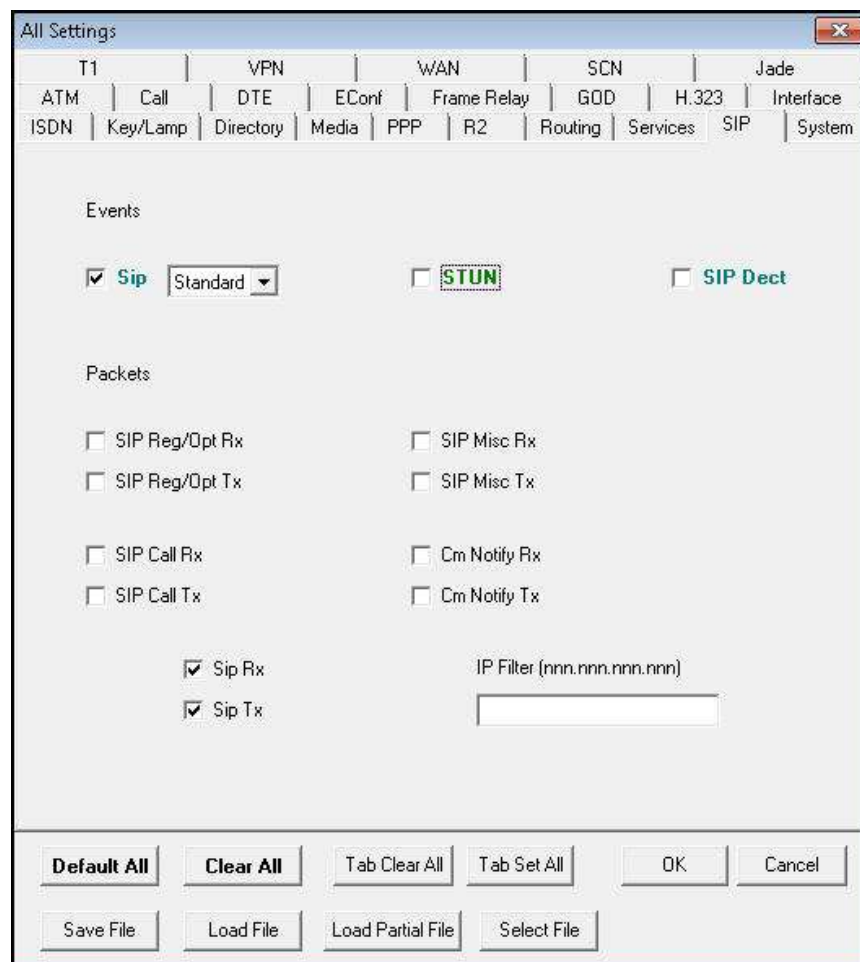
Last Date Of Error	Occurrences	Error Description
--------------------	-------------	-------------------

7.2. 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:



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.



8. Conclusion

The Clearfly Communications SIP Trunking Service passed compliance testing with Avaya IP Office R9.1. These Application Notes describe the configuration necessary to connect Avaya IP Office R9.1 to Clearfly as shown in **Figure 1**. Test results and observations are noted in **Section 2.2**.

9. 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] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>.
- [8] 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.

©2015 Avaya Inc. All Rights Reserved.

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

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