



## Avaya Solution & Interoperability Test Lab

# **Application Notes for Configuring Avaya IP Office Release 11.1 to support Clearly Communications SIP Trunking Service using Trunk Registration - Issue 1.0**

### **Abstract**

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 11.1 to support Clearly Communications SIP Trunking Service using Trunk Registration. These Application Notes update previously published Application Notes with a newer software version of Avaya IP Office.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consultative), conference, and voice mail. The calls were placed to and from the public switched telephone network (PSTN) with various Avaya endpoints.

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 steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Clearfly Communications and an Avaya SIP-enabled enterprise solution.

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of an Avaya IP Office Server Edition, two Avaya IP Office 500 V2 as expansion systems running software release 11.1 (hereafter referred to as IP Office) and various Avaya endpoints, listed in **Section 4**.

The Clearfly Communications SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the IP Office solution are able to place and receive PSTN calls via a broadband wide area network (WAN) connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

The terms “service provider”, “Clearfly Communications” or “Clearfly” will be used interchangeably throughout these Application Notes.

## 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Clearfly Communications network via the public Internet, as depicted in **Figure 1**, and exercise the features and functionalities 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

## 2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability the following features and functionalities were exercised during the interoperability compliance test:

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, Digital and Analog telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323, Digital and Analog telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider network.
- Incoming and outgoing PSTN calls to/from Avaya IX™ Workplace Client for Windows (SIP).
- Dialing plans including local calls, outbound toll-free, etc.
- Caller ID presentation.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two-way speech-path. Testing was performed with codecs: G.711MU and G.729A, Clearly Communications preferred codec order.
- Proper response to no matching codecs.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- SIP REFER method for call re-direction from the enterprise to the PSTN.
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.
- T.38 Fax.

Items not supported or not tested included the following:

- Clearly does not support Operator (0) and Operator Assisted (0+10 digits) calls.
- 911 Emergency calls were not tested.

## 2.2. Test Results

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

- **Extra SIP messages sent during Call Transfers to the PSTN** – After a call from the PSTN to the enterprise was successfully transferred back out to another PSTN party using the SIP REFER method, Clearfly accepted the SIP REFER messages sent by IP Office with “202 Accepted”, which resulted in successful call completion between the two PSTN parties and the release of the SIP trunk channel resources, as expected. It was observed that during the SIP trunk channel resource release process there were additional SIP messages being exchanged that did not have any negative impact on the call/user, it’s being mentioned here simply as an observation
- **Outbound call from an enterprise extension to a busy PSTN number** – Clearfly Communications did not send a “486 Busy Here” message on an outbound call to a PSTN number that was busy, as it was expected on this condition. There was no direct impact to the user, who heard busy tone.

## 2.3. Support

For support on Clearfly Communications systems visit the corporate Web page at: <https://www.clearfly.net/> or call (866) 652-7520.

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

### 3. Reference Configuration

**Figure 1** illustrates the test configuration used for the DevConnect compliance testing. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the Clearly Communications SIP Trunking Service through the public Internet.

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

- IP Office Server Edition running in VMware environment.
  - Avaya IP Office Voicemail Pro.
- Two Avaya IP Office 500 V2 as expansion systems.
- Avaya 96x1 Series IP Deskphones (H.323).
- Avaya J179 IP Deskphones (H.323).
- Avaya 1100 Series IP Deskphones (SIP).
- Avaya J129 IP Deskphones (SIP).
- Avaya 1400 Series Digital Deskphones.
- Analog Deskphones.
- Avaya IX™ Workplace Client for Windows (SIP).

Avaya IP Office provides the voice communications services for the enterprise. In the reference configuration, Avaya IP Office runs on the Avaya IP Office Server Edition platform. Note that this solution is extensible to deployments using the standalone IP500 V2 platform as well.

In the sample configuration, the Primary server runs the Avaya IP Office Server Edition Linux software. Avaya Voicemail Pro runs as a service on the Primary Server. The LAN1 port of the Primary Server is connected to the enterprise LAN. The LAN2 port was used to connect to the public network.

The Expansion Systems (IP500 V2) were used for the support of digital, analog and additional IP stations. The Avaya IP Office 500 V2s are equipped with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module). The LAN1 port of the Avaya IP Office IP500 V2 expansion systems was connected to the enterprise LAN, the LAN2 port was not used.

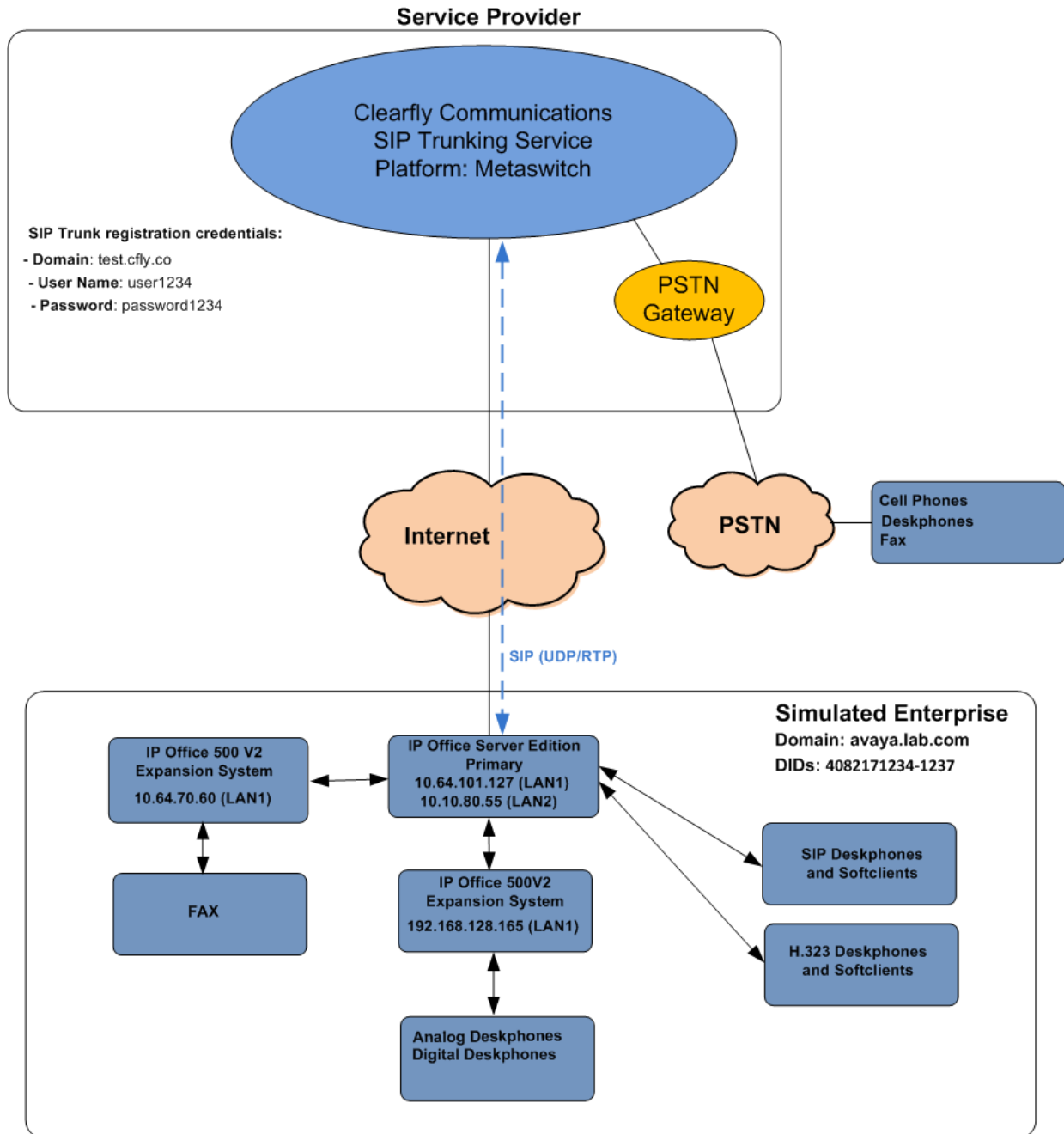
IP endpoints at the enterprise include 96x1 Series IP Deskphones (with H.323 firmware), Avaya 1100 and J100 Series IP Deskphones (with SIP firmware), Avaya 1400 Series Digital Deskphones, Analog Deskphones and Avaya IX™ Workplace Client for Windows (SIP). Some IP endpoints were registered to the Primary Server while others were registered to the Expansion Systems. Avaya 1400 Series Digital Deskphones and analog telephones are connected to media modules on the Expansion Systems. The site also has a Windows PC running Avaya IP Office Manager to configure and administer the system. Mobile Twinning is configured for some of the IP Office users so that calls to these user's extensions will also ring and can be answered at the configured mobile phones.

The transport protocols on the SIP trunk between IP Office and Clearfly Communications, across the public Internet, is UDP for signaling and RTP for media. The transport protocol between Avaya components inside the enterprise private IP network (LAN) is TLS for signaling and SRTP for media.

For the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to the Clearfly Communications network. The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Clearfly Communications network.

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

For confidentiality and privacy purposes, public IP addresses, domain names, and routable DID numbers used during the compliance testing have been masked.



**Figure 1: Avaya Interoperability Test Lab Configuration**



## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya IP Office Server Edition (Primary Server)	11.1.0.0.0 Build 237
• Avaya IP Office Voicemail Pro	11.1.0.0.0 Build 234
Avaya IP Office IP500 V2 (Expansion Systems)	11.1.0.0.0 Build 237
Avaya IP Office Manager	11.1.0.0.0 Build 237
Avaya 96x1 Series IP Deskphones (H.323)	6.8304
Avaya J179 IP Telephone (H.323)	6.8304
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.0.5.0.10
Avaya 1408 Digital Telephone	48.02
Avaya Equinox™ for Windows (SIP)	3.8.5.41.23
Analog Telephone	---
<b>Clearly Communications</b>	
Metaswitch Softswitch	v9.5
Metaswitch Perimeta Session Border Controller	V4.6

**Note:** 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. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints.

## 5. Avaya IP Office Primary Server Configuration

Avaya IP Office is configured through the Avaya IP Office Manager application. From the PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the Manager application. Log in using the appropriate credentials.

**Select IP Office**

Name	IP Address	Type	Version	Edition
Server Edition 11.1				
<input checked="" type="checkbox"/> IPOSE-Primary	10.64.101.127	IPO-Linux-PC	11.1.0.0.0 build 237	Server (Primary) Select

Configuration Service User Login

IP Office: IPOSE-Primary (Primary System - IPO-Linux-PC)

Service User Name:

Service User Password:

TCP Discovery Progress

Unit/Broadcast Address ☒ Open with Server Edition Manager

On Server Edition systems, the Solution View screen will appear, similar to the one shown below. All the Avaya IP Office configurable components are shown in the left pane, known as the Navigation Pane. Clicking the “plus” sign next to the Primary server system name, e.g., **IPOSE-Primary**, on the navigation pane will expand the menu on this server.

**Configuration**

- BOOTP (4)
- Operator (3)
- Solution
  - User(32)
  - Group(2)
  - Short Code(48)
  - Directory(0)
  - Time Profile(0)
  - Account Code(0)
  - User Rights(9)
  - Location(1)
  - IPOSE-Primary
  - IP500V2-One
  - IP500V2-Two

**Server Edition**

### Summary

Server Edition Primary

**Hardware Installed**

Control Unit: IPO-Linux-PC  
Secondary Server: NONE  
Expansion Systems: 192.168.128.165; 10.64.70.60  
System Identification: 8de6c6d337bc354d6ec88494533af87bb2d6e950

**System Settings**

IP Address: 10.64.101.127  
Sub-Net Mask: 255.255.255.0  
System Locale: United States (US English)  
System Location: 3: Thornton, CO  
Device ID: NONE  
Number of Extensions on System: 6

**Open...**

- Configuration
- System Status
- Voicemail Administration
- Resiliency Administration
- On-boarding
- IP Office Web Manager
- Help
- Set All Nodes License Source
- Set All Nodes to Subscription mode

**Add...**

- Secondary Server
- Expansion System

**Link...**

- Expansion System

Description	Name	Address	Primary Link	Secondary Link	Users Configured	Extensions Configured
Solution					32	54
Primary Server	IPOSE-Primary	10.64.101.127			6	6
Expansion System	IP500V2-One	192.168.128.165	Bothway		25	24
Expansion System	IP500V2-Two	10.64.70.60	Bothway		1	24



On Server Edition systems, the numbers of licenses to be assigned to the specific Server or Expansion Systems are reserved from the total pool of licenses present on the license server. On the screen below, 10 **SIP Trunk Sessions** licenses were reserved to be used by the Primary Server.

**Configuration**

- BOOTP (4)
- Operator (3)
- Solution
  - User(32)
  - Group(2)
  - Short Code(48)
  - Directory(0)
  - Time Profile(0)
  - Account Code(0)
  - User Rights(9)
  - Location(1)
  - IPOSE-Primary
    - System (1)
      - IPOSE-Primary
        - Line (3)
          - Control Unit (8)
          - Extension (6)
          - User (7)
          - Group (0)
          - Short Code (2)
          - Service (0)
          - Incoming Call Route (4)
          - IP Route (3)
          - License (6)
            - ARS (1)
            - Location (1)
            - Authorization Code (0)
          - IP500V2-One
          - IP500V2-Two

License Remote Server

Remote Server Configuration

License SourceWebLM

Domain Name (URL)10.64.101.127

PathWebLM/LicenseServer

Port Number52233

WebLM Client ID

WebLM Node ID-IPOSE-Primary

Reserved Licenses

SIP Trunk Sessions	10	Server Edition	1
SM Trunk Sessions	0	Avaya IP Endpoints	6
Voicemail Pro Ports	2	3rd Party IP Endpoints	0
VMPro Recordings Administrators	0	Receptionist	0
VMPro TTS Professional	0	Basic User	5
CTI Link Pro	0	Office Worker	0
UMS Web Services	0	Power User	1
Mac Softphones	0	Avaya Softphone	0
Avaya Contact Center Select	0	Web Collaboration	0
VM Media Manager	0		

## 5.2. System Settings

Configure the necessary system settings. The LAN2 tab settings correspond to the IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side).

### 5.2.1. System – LAN2 Tab

In the sample configuration, the LAN2 interface is used for the SIP trunk connection to Clearlyfly Communications.

#### 5.2.1.1 LAN2 - LAN Settings Tab

To view or configure the LAN2 IP address and subnet mask, select the **LAN2→ LAN Settings** tab, and enter the information as needed, according to the customer network requirements:

- **IP Address: 10.10.80.55** was used in the reference configuration, this is the public IP address assigned to IP Office.
- **IP Mask: 255.255.255.128** was used in the reference configuration.
- Other parameters on this screen are set to the defaults.

The screenshot displays the IPOSE-Primary configuration window. On the left is a tree view under 'Configuration' with various system components. The main area on the right is titled 'IPOSE-Primary' and contains several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, and SMTP. The 'LAN2' tab is selected, and within it, the 'LAN Settings' sub-tab is active. The configuration fields are as follows:

Field	Value
IP Address	10 . 10 . 80 . 55
IP Mask	255 . 255 . 255 . 128
Number Of DHCP IP Addresses	200
DHCP Mode	<input type="radio"/> Server <input type="radio"/> Client <input checked="" type="radio"/> Disabled

An 'Advanced' button is located at the bottom right of the LAN Settings section.

### 5.2.1.2 LAN2 VoIP Tab

- Select the **LAN2 → VoIP** tab in the Details Pane. Check the **SIP Trunks Enable** box to allow the configuration of SIP trunks. Since no SIP endpoints are to register on this interface, leave the **SIP Registrar Enable** box unchecked.

The screenshot shows the IPOSE-Primary configuration interface. On the left is a 'Configuration' tree with a hierarchy: BOOTP (4) → Operator (3) → Solution → User(32) → Group(2) → Short Code(48) → Directory(0) → Time Profile(0) → Account Code(0) → User Rights(9) → Location(1) → IPOSE-Primary → System (1) → IPOSE-Primary → Line (3) → Control Unit (8) → Extension (6) → User (7) → Group (0) → Short Code (2) → Service (0) → Incoming Call Route (4) → IP Route (3) → License (6) → ARS (1) → Location (1) → Authorization Code (0) → IP500V2-One → IP500V2-Two.

The main panel is titled 'IPOSE-Primary\*' and has tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and Contact Center. The 'LAN2' tab is selected, and within it, the 'VoIP' sub-tab is active. The 'Network Topology' section is expanded, showing the following settings:

- ☐ H.323 Gatekeeper Enable
- ☐ Auto-create Extension ☐ Auto-create User ☐ H.323 Remote Extension Enable
- H.323 Signaling over TLS: Disabled (dropdown)
- Remote Call Signaling Port: 1720 (spin box)
- ☒ SIP Trunks Enable
- ☐ SIP Registrar Enable
- ☐ Auto-create Extension/User ☐ SIP Remote Extension Enable
- Allowed SIP User Agents: Block blacklist only (dropdown)
- SIP Domain Name: (text field)
- SIP Registrar FQDN: (text field)
- 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 Expiration Time (sec): 10 (spin box)
- RTP: Port Number Range: Minimum 46750, Maximum 50750

Scroll down the page:

- Verify the **RTP Port Number Range**. Based on this setting, Avaya IP Office will request RTP media to be sent to a UDP port in the configurable range for calls using LAN2. The **Minimum** and **Maximum** port numbers were kept at their default values in the reference configuration.
- In the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. This is done to prevent possible issues with network firewalls closing idle RTP channels.
- In the **DiffServ Settings** section, 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 (QoS) policies for both signaling and media. The **DSCP** field is the value used for media, while the **SIG DSCP** is the value used for signaling. These settings should be set according to the customer's QoS policies in place. The default values used during the compliance test are shown.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view of the configuration hierarchy, with 'IPOSE-Primary' selected. The main panel on the right is titled 'IPOSE-Primary\*' and contains several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. The 'LAN2' tab is active, showing 'LAN Settings'. Within this tab, the 'VoIP' sub-tab is selected. The configuration includes sections for SIP settings (SIP Registrar Enable, SIP Domain Name, SIP Registrar FQDN), Layer 4 Protocol (UDP, TCP, TLS ports), RTP settings (Port Number Range, Port Number Range (NAT), Enable RTCP Monitoring on Port 5005, RTCP collector IP address for phones), Keepalives (Scope: RTP-RTCP, Periodic timeout: 30, Initial keepalives: Enabled), DiffServ Settings (DSCP, Video DSCP, DSCP Mask, SIG DSCP), and DHCP Settings (Primary Site Specific Option Number (SSON), Secondary Site Specific Option Number (SSON), VLAN).

Section	Parameter	Value
SIP Settings	SIP Registrar Enable	<input type="checkbox"/>
	SIP Domain Name	
	SIP Registrar FQDN	
	Challenge Expiration Time (sec)	10
Layer 4 Protocol	UDP Port	5060
	Remote UDP Port	5060
	TCP Port	5060
	Remote TCP Port	5060
RTP Settings	Port Number Range Minimum	46750
	Port Number Range Maximum	50750
	Port Number Range (NAT) Minimum	40750
	Port Number Range (NAT) Maximum	50750
Keepalives	Enable RTCP Monitoring on Port 5005	<input checked="" type="checkbox"/>
	RTCP collector IP address for phones	0 . 0 . 0 . 0
	Scope	RTP-RTCP
	Periodic timeout	30
DiffServ Settings	DSCP (Hex)	B8
	Video DSCP (Hex)	46
	DSCP Mask (Hex)	63
	SIG DSCP (Hex)	34
DHCP Settings	Primary Site Specific Option Number (SSON)	176
	Secondary Site Specific Option Number (SSON)	242
	VLAN	Not Present



**Note:** In the compliance test, the LAN1 interface was used to connect the Avaya IP Office to the enterprise site IP network (private network). The LAN1 interface configuration is not directly relevant to the interface with the Clearly Communications SIP Trunking Service, and therefore is not described in these Application Notes.

### 5.2.1.3 LAN2 - Network Topology Tab

On the **LAN2 Network Topology** tab in the Details pane, set the following:

- Select the **Firewall/NAT Type** from the pull-down menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used.
- Set **Binding Refresh Time (seconds)** to **180**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider.
- Set **Public Port** to **5060**.
- Default values were used for all other parameters.
- Click the **OK** button (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view under 'Configuration' showing a hierarchy of system components, with 'IPOSE-Primary' selected. The main panel is titled 'IPOSE-Primary\*' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', 'System Events', 'SMTP', 'SMDR', 'VoIP', and 'Contact Center'. The 'LAN2' tab is active, and within it, the 'Network Topology' sub-tab is selected. The 'Network Topology Discovery' section contains the following fields and controls:

- STUN Server Address:** An empty text input field.
- STUN Port:** A numeric spinner set to 3478.
- Firewall/NAT Type:** A dropdown menu currently showing 'Open Internet'.
- Binding Refresh Time (sec):** A numeric spinner set to 180.
- Public IP Address:** A field showing '0 . 0 . 0 . 0'.
- Public Port:** Three separate numeric spinners for UDP (5060), TCP (5060), and TLS (5061).
- Run STUN on startup:** An unchecked checkbox.

At the bottom of the 'Network Topology Discovery' section are two buttons: 'Run STUN' and 'Cancel'.

### 5.2.2. System - DNS Tab

Public DNS servers IP addresses are required to be configured; IP Office will retrieve Clearfly Communications Proxy IP Address via public DNS queries using Clearfly Communications ISTEP Domain Name configured under in **Section 5.4.2**. To access the System DNS settings, navigate to the **DNS** tab in the **Details** pane, configure the following parameters:

- Under DNS Server IP Address and Backup DNS Server IP Address enter the primary and backup public DNS servers IP addresses. These IP addresses should be provided by Clearfly Communications.
- Click **OK** to commit (not shown).

The screenshot displays the IP Office configuration interface. On the left is a tree view under the 'Configuration' header, listing various system components such as BOOTP (4), Operator (3), Solution, User(32), Group(2), Short Code(48), Directory(0), Time Profile(0), Account Code(0), User Rights(9), Location(1), IPOSE-Primary, System (1), IPOSE-Primary, Line (3), Control Unit (8), Extension (6), User (7), Group (0), Short Code (2), Service (0), Incoming Call Route (4), IP Route (3), License (6), ARS (1), Location (1), Authorization Code (0), IP500V2-One, and IP500V2-Two. The 'IPOSE-Primary' system is selected. The main pane on the right is titled 'IPOSE-Primary\*' and contains several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, and SMTP. The 'DNS' tab is active, showing the following configuration fields: 'DNS Server IP Address' with the value '8 . 8 . 8 . 8', 'Backup DNS Server IP' with the value '8 . 8 . 4 . 4', and 'DNS Domain' which is an empty text box.

### 5.2.3. Telephony Tab

To access the System Telephony settings, navigate to the **Telephony** → **Telephony** tab in the **Details** pane, configure the following parameters:

- Choose the **Companding Law** typical for the enterprise location; **U-Law** was used for the compliance test.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN. If for security reasons incoming calls should not be allowed to transfer back to the PSTN then leave this setting checked.
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

**Configuration**

- BOOTP (4)
- Operator (3)
- Solution
  - User(32)
  - Group(2)
  - Short Code(48)
  - Directory(0)
  - Time Profile(0)
  - Account Code(0)
  - User Rights(9)
  - Location(1)
  - IPOSE-Primary
    - System (1)
      - IPOSE-Primary
        - Line (3)
          - Control Unit (8)
          - Extension (6)
            - User (7)
            - Group (0)
            - Short Code (2)
            - Service (0)
            - Incoming Call Route (4)
            - IP Route (3)
            - License (6)
            - ARS (1)
            - Location (1)
            - Authorization Code (0)
            - IP500V2-One
            - IP500V2-Two

**IPOSE-Primary\***

System LAN1 LAN2 DNS Voicemail **Telephony** Directory Services System Events SMTP SMDR VoIP Contact Center

Telephony Park & Page Tones & Music Ring Tones SM Call Log TUI

Dial Delay Time (sec) 4

Dial Delay Count 0

Default No Answer Time (sec) 15

Hold Timeout (sec) 0

Park Timeout (sec) 300

Ring Delay (sec) 5

Call Priority Promotion Time (sec) Disabled

Default Currency USD

Default Name Priority Favor Directory

Media Connection Preservation Enabled

Phone Failback Automatic

Login Code Complexity

☒ Enforcement

Minimum length 6

☒ Complexity

RTCP Collector Configuration

☐ Send RTCP to an RTCP Collector

Server Address 0 . 0 . 0 . 0

UDP Port Number 5005

RTCP reporting interval (sec) 5

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

☒ High Quality Conferencing

☒ Directory Overrides Barring

☐ Advertise Callee State To Internal Callers

☐ Internal Ring on Transfer

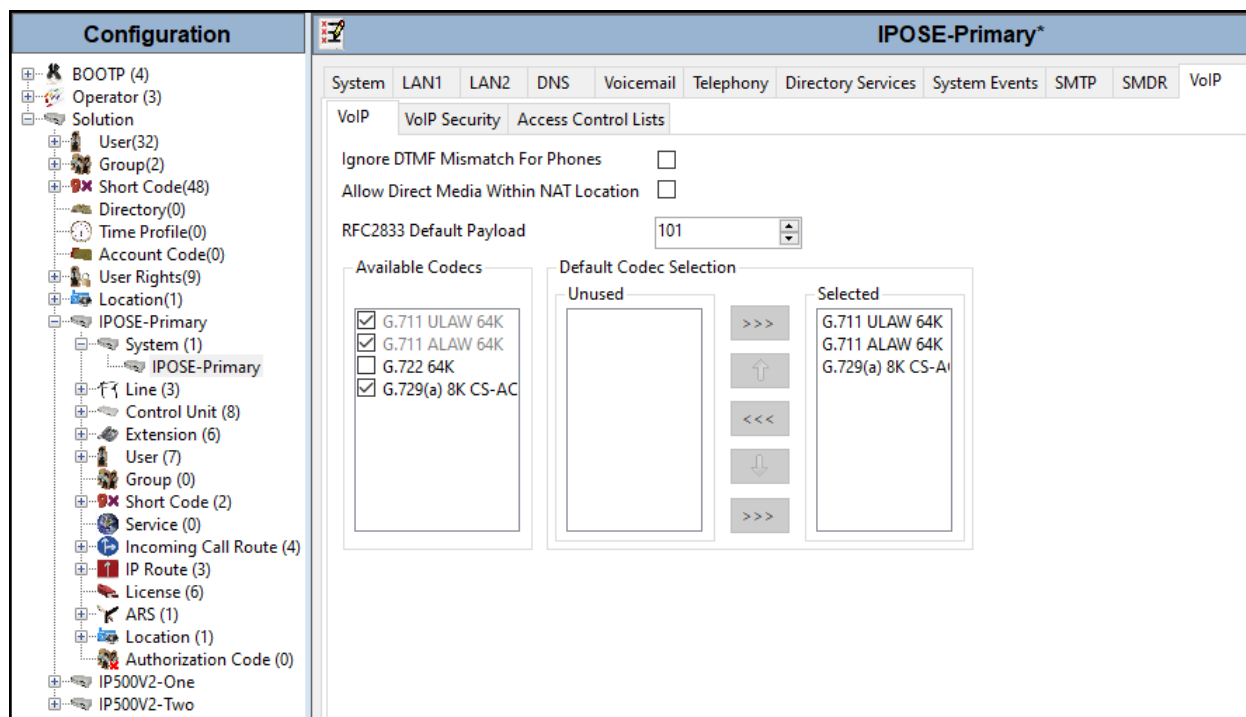
## 5.2.4. VoIP Tab

Navigate to the **VoIP** tab in the Details pane to view or change the system codecs and VoIP security settings.

### 5.2.4.1 VoIP - VoIP Tab

Select the **VoIP → VoIP** tab, configure the following parameters:

- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used.
- For codec selection, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order were used.
- Click **OK** to commit (not shown).



**Note:** The codec selections defined under this section (VoIP – VoIP Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.6** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

### 5.2.4.2 VoIP – VoIP Security Tab

Secure Real-Time Transport Protocol (SRTP) refers to the application of additional encryption and or authentication to VoIP calls (SIP and H.323). SRTP can be applied between telephones, between ends of an IP trunk or in various other combinations.

Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

- Disabled (default).
- Preferred.
- Enforced.

When enabling SRTP on the system, the recommended setting is **Preferred**. In this scenario, IP Office uses SRTP if supported by the far-end, otherwise uses RTP. If the **Enforced** setting is used, and SRTP is not supported by the far-end, the call is not established.

To configure the use of SRTP, select the **VoIP → VoIP Security** tab on the Details pane.

- Set the **Media Security** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption.
- Verify **Strict SIPS** is not checked.
- Under **Media Security Options**, select **RTP** for the **Encryptions** and **Authentication** fields.
- Under **Crypto Suites**, select **SRTP\_AES\_CM\_128\_SHA1\_80**.
- Click **OK** to commit (not shown).

The screenshot displays the IPOSE-Primary configuration window. The left sidebar shows a tree view of the configuration hierarchy, with 'IPOSE-Primary' selected. The main pane shows the 'VoIP Security' tab. The 'Default Extension Password' and 'Confirm Default Extension Password' fields are empty. The 'Media' dropdown is set to 'Preferred', and the 'Strict SIPS' checkbox is unchecked. Under 'Media Security Options', the 'Encryptions' and 'Authentication' sections both have 'RTP' and 'RTCP' checked. The 'Replay Protection' section is empty. The 'SRTP Window Size' is set to 64. Under 'Crypto Suites', 'SRTP\_AES\_CM\_128\_SHA1\_80' is checked, and 'SRTP\_AES\_CM\_128\_SHA1\_32' is unchecked.

### 5.3. IP Route

Create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to route calls to Clearlyfly Communications network.

Navigate to **IP Route**, right-click on **IP Route** and select **New**. The values used during the compliance test are shown below:

- Set the **IP Address** and **IP Mask** to **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP address of the gateway/router used to route calls to the public network, e.g., **10.10.80.1**.
- Set **Destination** to **LAN2** from the pull-down menu.
- Click **OK** to commit (not shown).

Configuration		0.0.0.0*	
IP Route			
IP Address		0 . 0 . 0 . 0	
IP Mask		0 . 0 . 0 . 0	
Gateway IP Address		10 . 10 . 80 . 1	
Destination		LAN2	
Metric		0	

## 5.4. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Clearly Communications. 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 **Sections 5.4.1** to create the SIP Line from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary, after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.4.2** to **5.4.7**.

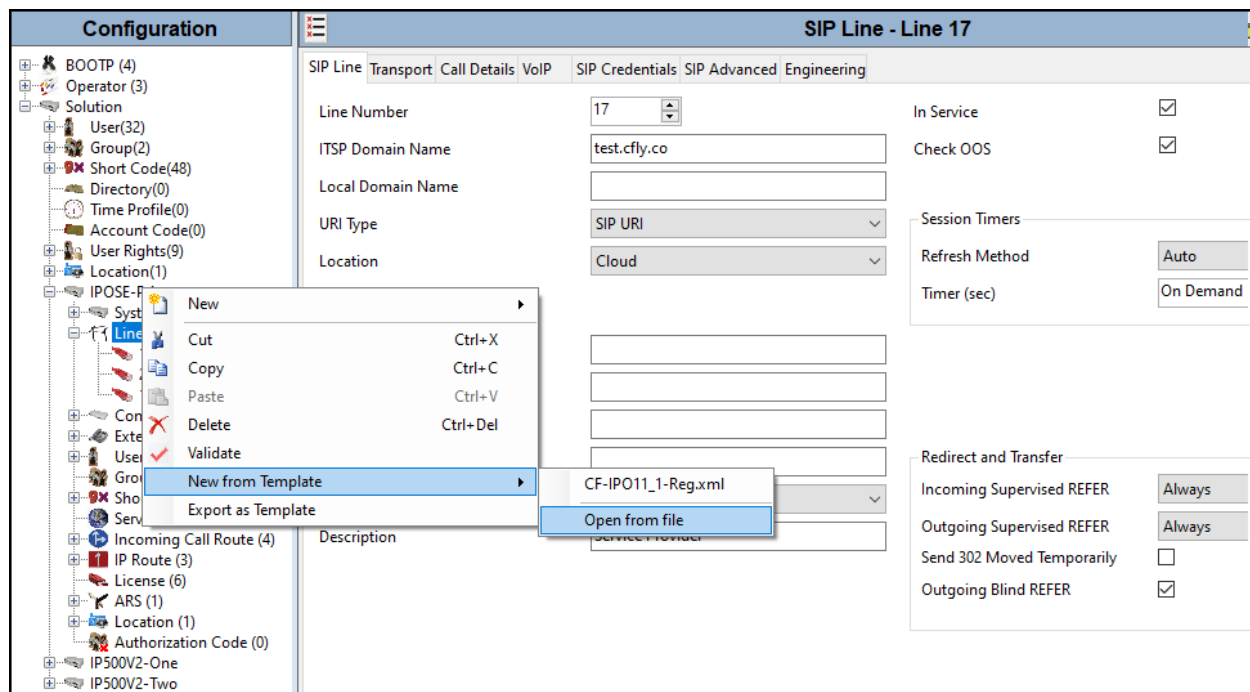
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.7**.

### 5.4.1. Creating a SIP Trunk from an XML Template

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. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

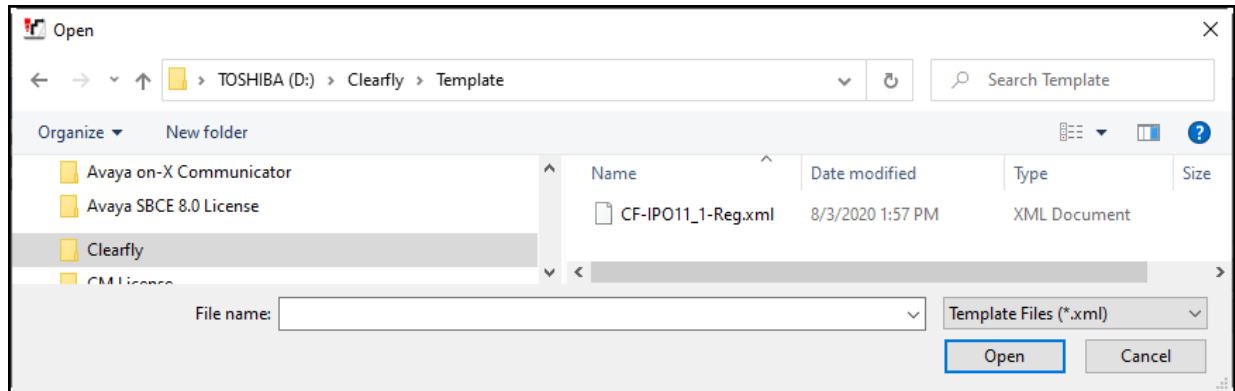
Copy a previously created template file to a location (e.g., *\Temp*) on the same computer where IP Office Manager is installed.

To create the SIP Trunk from the template, from the **Primary** server (**IPOSE-Primary**), right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template → Open from file**.

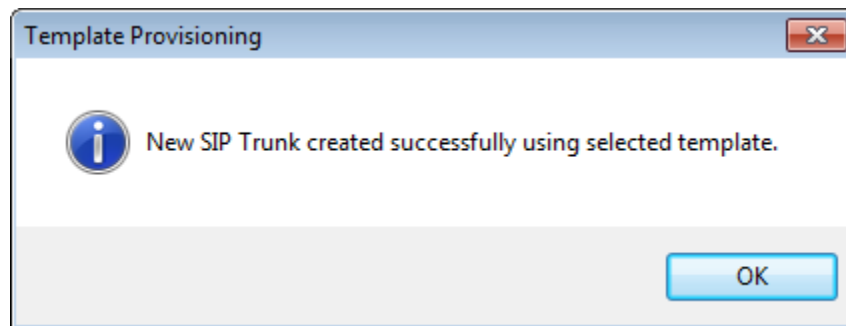




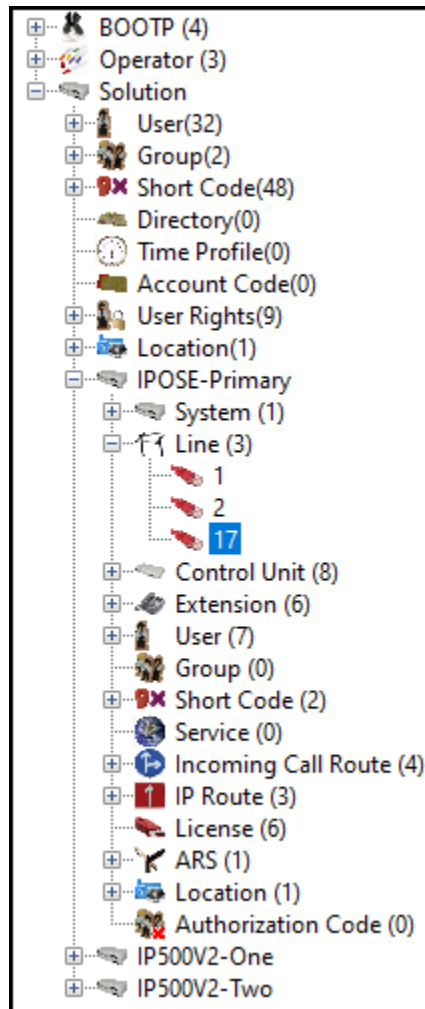
Navigate to the directory on the local machine where the template was copied and select the template.



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



The newly created SIP Line will appear in the Navigation pane (e.g., SIP Line **17**).



It is important that the SIP Line configuration be reviewed and updated if necessary, after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2 to 5.4.7**.

### 5.4.2. SIP Line – SIP Line Tab

On the **SIP Line** tab in the **Details** pane, configure or verify the parameters as shown below:

- Set **ITSP Domain Name** to **test.cfly.co**, the domain name provided by Clearly Communications.
- Verify that **In Service** box is checked, the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (sec)** is set to **On Demand**.
- For the compliance test REFER support was enabled. Thus, **Incoming Supervised REFER** and **Outgoing Supervised REFER** should be set to **Always**. Click **OK** to commit (not shown).
- Outgoing **Blind REFER** is checked to enable use of REFER for blind transfers as well.

The screenshot displays the 'SIP Line - Line 17\*' configuration window. On the left is a 'Configuration' tree showing a hierarchy from 'BOOTP (4)' down to 'IP500V2-Two'. The main panel has tabs for 'SIP Line', 'Transport', 'Call Details', 'VoIP', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'SIP Line' tab is active, showing fields for 'Line Number' (17), 'ITSP Domain Name' (test.cfly.co), 'Local Domain Name', 'URI Type' (SIP URI), 'Location' (Cloud), 'Prefix', 'National Prefix', 'International Prefix', 'Country Code', 'Name Priority' (System Default), and 'Description' (Service Provider). On the right, there are checkboxes for 'In Service' and 'Check OOS', both checked. Below these are 'Session Timers' with 'Refresh Method' set to 'Auto' and 'Timer (sec)' set to 'On Demand'. At the bottom, the 'Redirect and Transfer' section has 'Incoming Supervised REFER' and 'Outgoing Supervised REFER' set to 'Always', 'Send 302 Moved Temporarily' unchecked, and 'Outgoing Blind REFER' checked.

Field	Value	Field	Value
Line Number	17	In Service	<input checked="" type="checkbox"/>
ITSP Domain Name	test.cfly.co	Check OOS	<input checked="" type="checkbox"/>
Local Domain Name		Session Timers	
URI Type	SIP URI	Refresh Method	Auto
Location	Cloud	Timer (sec)	On Demand
Prefix		Redirect and Transfer	
National Prefix		Incoming Supervised REFER	Always
International Prefix		Outgoing Supervised REFER	Always
Country Code		Send 302 Moved Temporarily	<input type="checkbox"/>
Name Priority	System Default	Outgoing Blind REFER	<input checked="" type="checkbox"/>
Description	Service Provider		

### 5.4.3. SIP Line - Transport Tab

Select the **Transport** tab. Set or verify the parameters as shown below:

- Leave the **ITSP Proxy Address** blank (IP Office will retrieve the ITSP Proxy Address via public DNS queries using the ISTP Domain Name provided under in **Section 5.4.2**). The public DNS IP addresses were configured under **Section 5.2.2**.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **None** (refer to the note below).
- Set the **Send Port** and **Listen Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view under the 'Configuration' header, showing a hierarchy of system components including BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System (1), Line (3) (with sub-items 1, 2, and 17), Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, and two IP500V2-One devices. The main panel on the right is titled 'SIP Line - Line 17' and contains several tabs: 'SIP Line', 'Transport' (which is selected), 'Call Details', 'VoIP', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'Transport' tab shows the following settings: 'ITSP Proxy Address' is an empty text field. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'UDP' and 'Send Port' is '5060'. 'Use Network Topology Info' is set to 'None' and 'Listen Port' is '5060'. 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0' for both addresses. 'Calls Route via Registrar' is checked. 'Separate Registrar' is an empty text field.

**Note** – For the compliance testing, the **Use Network Topology Info** field was set to **None**, since no NAT was used in the test configuration. If a NAT is used between Avaya IP Office and the other end of the trunk, then the **Use Network Topology Info** field should be set to the LAN interface (LAN1 or LAN2) used by the trunk and the **System → LAN1 (or 2) → Network Topology** tab needs to be configured with the details of the NAT device.

#### 5.4.4. SIP Line – SIP Credentials Tab

Select the **SIP Credentials** tab, and then click the **Add** button to add the SIP Trunk registration credentials. Set the parameters as show below:

- For **User name**, **Authentication Name** and **Contact** enter the user name credential provided by Clearlyfly Communications for SIP Trunk registration.
- For **Password** and **Confirm Password**, add the password credential provided by Clearlyfly Communications for SIP Trunk registration.
- Set **Expiry (mins)** to a value acceptable to the enterprise. This setting defines how often registration with Clearlyfly Communications is required following any previous registration. For the compliance test **60** minutes was used. This value should be chosen in consultation with the service provider.
- Verify that **Registration required** is checked.
- Click the OK to commit (not shown).

The screenshot displays the 'SIP Line - Line 17' configuration window. The left sidebar shows a tree view of the system configuration, with 'Line (3)' expanded to show 'Line 17'. The main window has tabs for 'SIP Line', 'Transport', 'Call Details', 'VoIP', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'SIP Credentials' tab is active, showing a table with the following data:

Index	User Name	Authentication Name	Contact	Expiration (mins)	Register
1	user1234	user1234	user1234	60	True

Below the table is the 'Edit SIP Credentials' dialog box with the following fields:

- User name: user1234
- Authentication Name: user1234
- Contact: user1234
- Password: [masked]
- Confirm Password: [masked]
- Expiration (mins): 60
- Registration required: ☒

Buttons for 'Add...', 'Remove', 'Edit...', 'OK', and 'Cancel' are visible on the right side of the window.

### 5.4.5. SIP Line – Call Details Tab

Select the **Call Details** tab, and then click the **Add...** button (not shown) and the screen shown below will appear. To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button. In the example screen below a new entry was created with the parameters shown below:

- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Under **Credentials**, select **1: user123** from the pull-down menu (this field will default to the **User Name** used under the **SIP Credentials** tab in **Section 5.4.4**).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Check the **P Asserted ID** and **Diversion Header**.
- Set the **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** fields to the values shown in the screenshot below.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.

SIP Line - 17 | Call Details | SIP URI

New URI

Incoming Group: 17 Max Sessions: 10

Outgoing Group: 17

Credentials: 1: user1234

	Display	Content	Field meaning		
			Outgoing Calls	Forwarding/Twinning	Incoming Calls
Local URI	Auto	Auto	Caller	Original Caller	Called
Contact	Auto	Auto	Caller	Original Caller	Called
P Asserted ID	<input checked="" type="checkbox"/> Auto	Auto	Caller	Original Caller	Called
P Preferred ID	<input type="checkbox"/> None	None	None	None	None
Diversion Header	<input checked="" type="checkbox"/> Auto	Auto	None	Caller	None
Remote Party ID	<input type="checkbox"/> None	None	None	None	None

OK Cancel Help

### 5.4.6. SIP Line - VoIP Tab

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

- The **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line, as shown. Clearly Communications supports codecs **G.711ULAW** and **G.729(a)** for audio.
- Select **T38 Fallback** for **Fax Transport Support**. Clearly Communications supports T.38 fax, with this setting G.711 pass-through fax will be used if the attempt to use T.38 fails.
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).

The screenshot shows the Avaya IP Office Configuration window for SIP Line - Line 17. The left sidebar shows the Configuration tree with various nodes like BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line, Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, IP500V2-One, and IP500V2-Two. The main area is titled 'SIP Line - Line 17' and has tabs for SIP Line, Transport, Call Details, VoIP, SIP Credentials, SIP Advanced, and Engineering. The VoIP tab is selected. The Codec Selection is set to Custom. The Unused list contains G.711 ALAW 64K. The Selected list contains G.711 ULAW 64K and G.729(a) 8K CS-ACELP. The Fax Transport Support is set to T38 Fallback. The DTMF Support is set to RFC2833/RFC4733. The Media Security is set to Disabled. On the right, there are checkboxes for Local Hold Music, Re-invite Supported, Codec Lockdown, Allow Direct Media Path, Force direct media with phones, and PRACK/100rel Supported.

**Note:** The codec selections defined under this section are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.4.1** are the codecs selected for the IP phones/extension (H.323 and SIP).

### 5.4.7. SIP Line – SIP Advanced Tab

In the **Addressing** area:

- Select **Request URI** for **Call Routing Method**.

In the **Identity** area:

- The **Use PAI for Privacy** box is checked.
- The **Caller ID from From header** box is checked. Incoming calls can include caller ID information in both the From field and in the PAI fields. When this option is selected, the caller ID information in the From field is used rather than that in the PAI fields.
- Verify that **Cache Auth Credentials** box is checked (Default = On). When set to On, allows the **credentials** challenge and response from a registration transaction to be automatically inserted into later SIP messages without waiting for a subsequent challenge.

In the **Call Control** area:

- **Emulate NOTIFY for REFER** is checked. Use for SIP providers that do not send NOTIFY messages. When set to On, after IP Office issues a REFER, and the provider responds with 202 ACCEPTED, IP Office will assume the transfer is complete and issue a BYE.
- **No REFER if using Diversion** box is checked. Applies to Forwards and Twinning to prevent IP Office from using the SIP REFER method on call forward scenarios that use the Diversion SIP header.
- Click **OK** to commit (not shown).

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'SIP Advanced' tab selected. The left sidebar shows a tree view of the configuration hierarchy, including BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line, Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, and IP500V2-One/Two.

The main configuration area is divided into three sections:

- Addressing:**
  - Association Method: By Source IP address
  - Call Routing Method: Request URI
  - Use P-Called-Party: ☐
  - Suppress DNS SRV Lookups: ☐
- Identity:**
  - Use "phone-context": ☐
  - Add user=phone: ☐
  - Use + for International: ☐
  - Use PAI for Privacy: ☒
  - Use Domain for PAI: ☐
  - Caller ID from From header: ☒
  - Send From In Clear: ☐
  - Cache Auth Credentials: ☒
  - User-Agent and Server Headers:
  - Send Location Info: Never
  - Add UUI header: ☐
  - Add UUI header to redirected calls: ☐
- 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: Disabled
  - Indicate HOLD: ☐
- Call Control:**
  - Call Initiation Timeout (s): 4
  - Call Queuing Timeout (mins): 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. Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.4**. To configure these settings, first navigate to **User** → *Name* in the Navigation Pane where *Name* is the name of the user to be modified. In the example below, the name of the user is **Ext3041 H323**. Select the **SIP** tab in the Details Pane. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Clearly Communications. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network. This can also be accomplished by activating Withhold Number on H.323 Deskphones (not shown). Click the **OK** to commit (not shown).

### Configuration

- BOOTP (4)
- Operator (3)
- Solution
  - User (32)
  - Group(2)
  - Short Code(48)
  - Directory(0)
  - Time Profile(0)
  - Account Code(0)
  - User Rights(9)
  - Location(1)
  - IPOSE-Primary
    - System (1)
    - Line (3)
    - Control Unit (8)
    - Extension (6)
    - User (7)
      - NoUser
      - 3050 3050
      - 3040 Ext3040 H323
      - 3041 Ext3041 H323
      - 3042 Ext3042 H323
      - 3047 Ext3047 SIPSoft
      - 3051 Ext3051 Deskpho
    - Group (0)
    - Short Code (2)
    - Service (0)
    - Incoming Call Route (4)
    - IP Route (3)
    - License (6)
    - ARS (1)
    - Location (1)
    - Authorization Code (0)
  - IP500V2-One
  - IP500V2-Two

### Ext3041 H323: 3041

Dial In

Voice Recording

Button Programming

Menu Programming

Mobility

Group Membership

Announcements

SIP

SIP Name

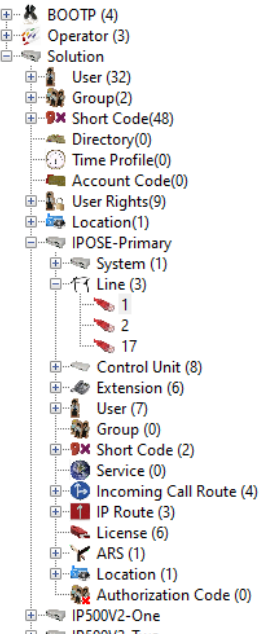
SIP Display Name (Alias)

Contact

☐ Anonymous

## 5.6. IP Office Line – Primary Server

In IP Office Server Edition systems, IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate line to be configured in the Group pane. The screen below shows the IP Office Line to the IP500V2-One Expansion System.

Configuration	IP Office Line - Line 1*	
	<div>Line   Short Codes   VoIP Settings</div> <div><div>Line Number: 1</div><div>Transport Type: WebSocket Server</div><div>Networking Level: SCN</div><div>Security: Medium</div><div>Gateway Address: 192 . 168 . 128 . 165</div><div>Location: 3: Thornton, CO</div><div>Password: .....</div><div>Confirm Password: .....</div><div>Description: </div></div> <div><div>Telephone Number: </div><div>Prefix: </div><div>Outgoing Group ID: 99999</div><div>Number of Channels: 250</div><div>Outgoing Channels: 250</div><div>SCN Resiliency Options<ul style="list-style-type: none"><li><input type="checkbox"/> Supports Resiliency<ul style="list-style-type: none"><li><input type="checkbox"/> Backs up my IP phones</li><li><input type="checkbox"/> Backs up my hunt groups</li><li><input type="checkbox"/> Backs up my voicemail</li><li><input type="checkbox"/> Backs up my IP DECT phones</li></ul></li></ul></div></div>	

The screen below shows the IP Office Line, **VoIP Settings** tab:

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **T38 Fallback** for **Fax Transport Support**. Clearly Communications supports T.38 fax, with this setting G.711 pass-through fax will be used if the attempt to use T.38 fails.
- Under **Media Security** verify **Same as System (Preferred)** is selected (default value).

**Configuration**

- BOOTP (4)
- Operator (3)
- Solution
  - User (32)
  - Group(2)
  - Short Code(48)
  - Directory(0)
  - Time Profile(0)
  - Account Code(0)
  - User Rights(9)
  - Location(1)
  - IPOSE-Primary
    - System (1)
    - Line (3)
      - 1
      - 2
      - 17
  - Control Unit (8)
  - Extension (6)
  - User (7)
    - Group (0)
    - Short Code (2)
    - Service (0)
  - Incoming Call Route (4)
  - IP Route (3)
  - License (6)
  - ARS (1)
  - Location (1)
  - Authorization Code (0)
  - IP500V2-One
  - IP500V2-Two

**IP Office Line - Line 1\***

Line Short Codes VoIP Settings

☒ Out Of Band DTMF  
☒ Allow Direct Media Path

Codec Selection: System Default

Unused: [Empty Box]

Selected: G.711 ULAW 64K, G.711 ALAW 64K, G.729(a) 8K CS-ACELP

Fax Transport Support: T38 Fallback

Call Initiation Timeout (s): 4

Media Security: Same as System (Preferred)

Advanced Media Security Options: ☒ Same As System

Encryptions: ☒ RTP, ☐ RTCP

Authentication: ☒ RTP, ☒ RTCP

Replay Protection: ☐

SRTP Window Size: 64

Crypto Suites: ☒ SRTP\_AES\_CM\_128\_SHA1\_80, ☐ SRTP\_AES\_CM\_128\_SHA1\_32

Repeat this process as needed to add additional Secondary server or Expansion Systems to the solution.

## 5.7. Incoming Call Route

Incoming call routes map inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system. To add an incoming call route, right click on **Incoming Call Route** in the **Navigation** pane and select **New** (not shown). On the Details Pane, under the **Standard** tab, set the parameters as show below:

- Set **Bearer Capacity** to **Any Voice**.
- The **Line Group ID** is set to **17**. This matches the **Incoming Group** field configured in the **Call Details** tab for the SIP Line on **Section 5.4.5**.
- On the **Incoming Number**, enter one of the DID numbers provided by Clearly Communications.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot shows the IP Office Configuration window. On the left is the 'Configuration' tree with a hierarchical view of system components. The 'Incoming Call Route (4)' folder is expanded, showing four entries: '17 4082171234' (selected), '17 4082171235', '17 4082171236', and '17 4082171237'. On the right is the 'Details' pane for the selected entry. It has tabs for 'Standard', 'Voice Recording', and 'Destinations'. The 'Standard' tab is active, displaying the following configuration parameters:

Parameter	Value
Bearer Capacity	Any Voice
Line Group ID	17
Incoming Number	4082171234
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

Select the **Destinations** tab. From the **Destination** drop-down menu, select the IP Office extension associated with this DID number. In the reference configuration, the DID number 4082171234 provided by Clearfly Communications was associated with the Avaya IP Office extension **3041 Ext3041 H323**.

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view under the 'Configuration' header, showing a hierarchy of system components. The 'Incoming Call Route' is expanded, showing several entries, including '17 4082171234'. On the right, the configuration details for '17 4082171234' are shown. The 'Destinations' tab is selected. Below the tab, a table lists the configuration details:

TimeProfile	Destination	Fallback Extension
Default Value	3041 Ext3041 H323	

Repeat this process as needed to assign incoming call routes to additional IP Office users, as well as for other Avaya IP Office destinations (Hunt Group, Voicemail, Short Codes, etc.).

## 5.8. Outbound Call Routing

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

### 5.8.1. Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code**, the **Navigation** pane and select **New**. The screen below shows the short code **9N** created (note that the semi-colon is not used here). In this case, when the IP Office user dials 9 plus any number **N**, instead of being directed to a specific Line Group ID, the call is directed to **Line Group 50: Main**, which is configurable via ARS.

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

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'Configuration' tree, and on the right is the '9N: Dial' configuration form.

**Configuration Tree (Left):**

- BOOTP (4)
- Operator (3)
- Solution
  - User (32)
  - Group(2)
  - Short Code(48)
    - Directory(0)
    - Time Profile(0)
    - Account Code(0)
    - User Rights(9)
    - Location(1)
    - IPOSE-Primary
      - System (1)
        - Line (3)
          - Control Unit (8)
          - Extension (6)
          - User (7)
          - Group (0)
          - Short Code (2)
            - \*66\*N#
            - 9N**
    - Service (0)
    - Incoming Call Route (4)
    - IP Route (3)
    - License (6)
    - ARS (1)
    - Location (1)
    - Authorization Code (0)

- IP500V2-One
- IP500V2-Two

**9N: Dial Configuration Form (Right):**

9N: Dial	
Short Code	
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	50: Main
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **Xs** used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office.

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

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **1** followed by **10 Xs** to represent the exact number of digits.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **1N**. The value **N** represents the additional number of digits dialed by the user after dialing **1** (The **9** will be stripped off).
- Set the **Line Group Id** to the Line Group number being used for the SIP Line, in this case **Line Group ID 17** was used.
- For **Locale**, **United States (US English)** was used
- Click **OK** to commit.

The following example shows the dial pattern for calls to the United States.



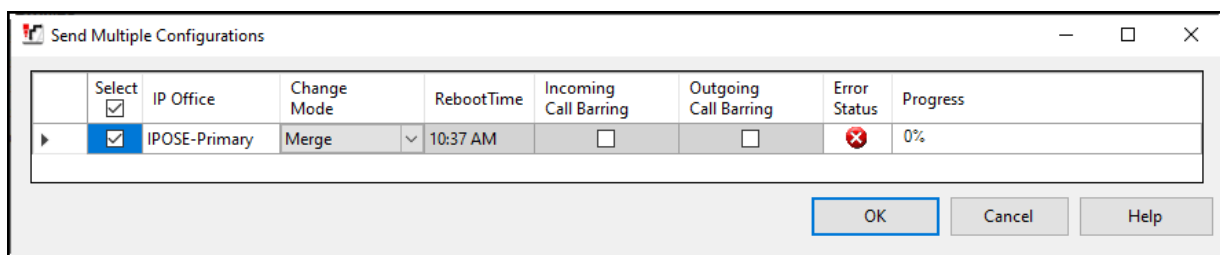
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

## 5.9. Save IP Office Primary Server Configuration

The provisioning changes made in Avaya IP Office Manager must be applied to the Avaya IP Office server in order for the changes to take effect. At the top of the Avaya IP Office Manager page, click **File → Save Configuration** (if that option is grayed out, no changes are pending).

A screen similar to the one below will appear, with either **Merge** or **Reboot** automatically selected, based on the nature of the configuration changes. The **Merge** option will save the configuration change with no impact to the current system operation. The **Immediate** option will save the configuration and cause the Avaya IP Office server to reboot.

Click **OK** to execute the save.





## 6. Avaya IP Office Expansion System Configuration

Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials. Clicking the “plus” sign next to IP Office Expansion system, in this case **IP500V2-One** was selected.

Configuration	System Inventory
<ul style="list-style-type: none"><li>BOOTP (4)</li><li>Operator (3)</li><li>Solution<ul style="list-style-type: none"><li>User (32)</li><li>Group(2)</li><li>Short Code(48)</li><li>Directory(0)</li><li>Time Profile(0)</li><li>Account Code(0)</li><li>User Rights(9)</li><li>Location(1)</li><li>IPOSE-Primary</li><li>IP500V2-One<ul style="list-style-type: none"><li>System (1)</li><li>Line (3)</li><li>Control Unit (4)</li><li>Extension (24)</li><li>User (27)</li><li>Group (1)</li><li>Short Code (12)</li><li>Service (0)</li><li>RAS (1)</li><li>Incoming Call Route (1)</li><li>WAN Port (0)</li><li>Firewall Profile (1)</li><li>IP Route (4)</li><li>License (2)</li><li>Tunnel (0)</li><li>ARS (2)</li><li>Location (1)</li><li>Authorization Code (0)</li></ul></li><li>IP500V2-Two</li></ul></li></ul>	<h3>Server Edition Expansion System</h3> <ul style="list-style-type: none"><li><b>Hardware Installed</b><ul style="list-style-type: none"><li>Control Unit: IP 500 V2</li><li>Internal Modules: VCM64/PRID U; PHONE8</li><li>Expansion Modules: DIG DCPx16 V2</li></ul></li><li><b>System Settings</b><ul style="list-style-type: none"><li>IP Address: 192.168.128.165</li><li>Sub-Net Mask: 255.255.255.0</li><li>System Locale: United States (US English)</li><li>System Location: 3: Thornton, CO</li><li>Device ID: NONE</li><li>Number of Extensions on System: 24</li></ul></li><li><b>Features Configured</b><ul style="list-style-type: none"><li>Licenses Installed: Server Edition(1); IP Office Select(1); Basic User(25)</li><li>Connected Extensions: 3043; 3044</li><li>Users NOT Configured for Voicemail: NONE</li><li>Users assigned as Ex-Directory: NONE</li><li>Users assigned for Twinning: NONE</li><li>Users barred from making Outgoing Calls: NONE</li><li>Music on Hold: WAV File</li></ul></li></ul>

## 6.1. Physical Hardware

In the sample configuration, the IP500 V2 Expansion System contained a PHONE8 analog card, for the support of analog extensions, a DIG DCPx16 V2, for support of digital extensions. Also included is a VCM64 (Voice Compression Module). The VCM64 cards provide voice compression channels to the control unit. Voice compression channels are needed to support VoIP calls, including IP extensions and or IP trunks.

Configuration

+

 BOOTP (4)

+

 Operator (3)

+

 Solution

+

 User (32)

+

 Group(2)

+

 Short Code(48)

+

 Directory(0)

+

 Time Profile(0)

+

 Account Code(0)

+

 User Rights(9)

+

 Location(1)

+

 IPOSE-Primary

+

 IP500V2-One

+

 System (1)

+

 Line (3)

+

 Control Unit (4)

+

 1 IP 500 V2

+

 2 VCM64/PRID U

+

 3 PHONE8

+

 6 DIG DCPx16 V2

+

 Extension (24)

+

 User (27)

+

 Group (1)

+

 Short Code (12)

+

 Service (0)

+

 RAS (1)

+

 Incoming Call Route (1)

+

 WAN Port (0)

+

 Firewall Profile (1)

+

 IP Route (4)

+

 License (2)

+

 Tunnel (0)

+

 ARS (2)

+

 Location (1)

+

 Authorization Code (0)

+

 IP500V2-Two

IP 500 V2

Unit

Device Number

1

Unit Type

IP 500 V2

Version

11.1.0.0.0 build 237

Serial Number

Unit IP Address

192.168.128.165

Interconnect Number

0

Module Number

Control Unit

## 6.2. LAN Settings

In the sample configuration, LAN1 is used to connect the Expansion System to the enterprise network. To view or configure the LAN1 IP address, select **System** on the Navigation pane. Select the **LAN1 → LAN Settings** tab on the Details pane, and enter the following:

- **IP Address:** 192.168.128.165 was used in the reference configuration.
- **IP Mask:** 255.255.255.0 was used in the reference configuration
- Click the **OK** button (not shown).

The screenshot displays the configuration interface for an IP500V2-One system. On the left is a 'Configuration' tree with a hierarchical list of components including BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, and IP500V2-One. The 'IP500V2-One' component is selected, and its sub-item 'System (1)' is highlighted. The main panel on the right is titled 'IP500V2-One' and contains several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, and System Events. The 'LAN1' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The configuration fields for LAN1 are as follows: IP Address is set to 192.168.128.165; IP Mask is set to 255.255.255.0; Primary Trans. IP Address is set to 0.0.0.0; RIP Mode is set to None; Enable NAT is unchecked; Number Of DHCP IP Addresses is set to 200; and DHCP Mode has four radio buttons: Server, Client, Dial In, and Disabled (which is selected). An 'Advanced' button is located at the bottom right of the DHCP Mode section.

Default values were used on the **VoIP** and **Network Topology** tabs (not shown).

### 6.3. IP Route

To create an IP route for the Expansion system, right-click on **IP Route** on the left Navigation pane. Select **New** (not shown).

- Enter **0.0.0.0** on the **IP Address** and **IP Mask** fields to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet. The default gateway in the reference configuration was **192.168.128.200**
- Set **Destination** to **LAN1** from the pull-down menu.

The screenshot displays the configuration interface for an IP Route. The left navigation pane shows a hierarchical tree of system components, with 'IP Route (4)' expanded to show four entries: 0.0.0.0, 10.64.101.0, 192.168.128.0, and 192.168.99.0. The right pane shows the configuration for the selected route (0.0.0.0\*). The configuration fields are as follows:

Field	Value
IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	192 . 168 . 128 . 200
Destination	LAN1
Metric	0

Below the configuration fields, there is a checkbox for 'Proxy ARP' which is currently unchecked.

## 6.4. IP Office Line – IP500 V2 Expansion System

In IP Office Server Edition systems, IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate line to be configured in the Group pane. The screen below shows the IP Office Line to the Primary server.

The screenshot displays the 'IP Office Line - Line 17' configuration window. On the left is a 'Configuration' navigation pane showing a tree structure of system components. The main area on the right is divided into tabs: 'Line', 'Short Codes', 'VoIP Settings', and 'T38 Fax'. The 'Line' tab is active, showing various configuration fields. The 'Gateway' section includes fields for Address, Location, Password, and Confirm Password. The 'SCN Resiliency Options' section contains three checkboxes: 'Supports Resiliency', 'Backs up my IP phones', 'Backs up my hunt groups', and 'Backs up my IP DECT phones'. The 'Description' field is at the bottom.

IP Office Line - Line 17	
Line Number	17
Transport Type	WebSocket Client
Networking Level	SCN
Security	Medium
Telephone Number	
Prefix	
Outgoing Group ID	99999
Number of Channels	250
Outgoing Channels	250
Gateway Address	10 . 64 . 101 . 127
Port	443
Location	3: Thornton, CO
Password	••••••••
Confirm Password	••••••••
SCN Resiliency Options	<input type="checkbox"/> Supports Resiliency <input type="checkbox"/> Backs up my IP phones <input type="checkbox"/> Backs up my hunt groups <input type="checkbox"/> Backs up my IP DECT phones
Description	

The screen below shows the IP Office Line, **VoIP Settings** tab:

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **T38 Fallback** for **Fax Transport Support**. Clearly Communications supports T.38 fax, with this setting G.711 pass-through fax will be used if the attempt to use T.38 fails.
- Under **Media Security Preferred** was selected.

**Configuration**

- BOOTP (4)
- Operator (3)
- Solution
  - User (32)
  - Group(2)
  - Short Code(48)
  - Directory(0)
  - Time Profile(0)
  - Account Code(0)
  - User Rights(9)
  - Location(1)
  - IPOSE-Primary
  - IP500V2-One
    - System (1)
    - Line (3)
      - 1
      - 2
      - 17
  - Control Unit (24)
  - Extension (24)
  - User (27)
  - Group (1)
  - Short Code (12)
  - Service (0)
  - RAS (1)
  - Incoming Call Route (1)
  - WAN Port (0)
  - Firewall Profile (1)
  - IP Route (4)
  - License (2)
  - Tunnel (0)
  - ARS (2)
  - Location (1)
  - Authorization Code (0)
  - IP500V2-Two

**IP Office Line - Line 17**

Line Short Codes VoIP Settings T38 Fax

**Codec Selection** System Default

Unused Selected

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

**Fax Transport Support** T38 Fallback

**Call Initiation Timeout (s)** 4

**Media Security** Preferred

**Advanced Media Security Options** ☒ Same As System

**Encryptions** ☒ RTP ☐ RTCP

**Authentication** ☒ RTP ☒ RTCP

**Replay Protection**

**SRTP Window Size** 64

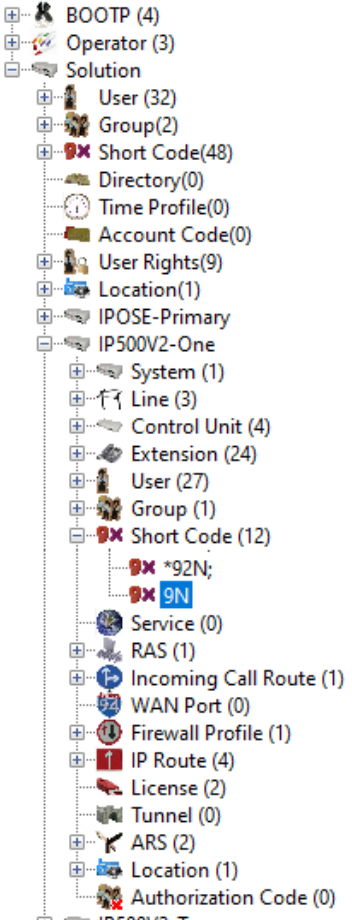
**Crypto Suites**

☒ SRTP\_AES\_CM\_128\_SHA1\_80  
☐ SRTP\_AES\_CM\_128\_SHA1\_32

☐ VoIP Silence Suppression  
☒ Out Of Band DTMF  
☒ Allow Direct Media Path

## 6.5. Short Codes

Similar to the configuration of the Primary server in **Section 5.8.1**, create a Short Code to access ARS. In the reference configuration, the **Line Group ID** is set to the ARS route illustrated in the next section.

Configuration	9N: Dial														
 <ul style="list-style-type: none"><li>BOOTP (4)</li><li>Operator (3)</li><li>Solution<ul style="list-style-type: none"><li>User (32)</li><li>Group(2)</li><li>Short Code(48)<ul style="list-style-type: none"><li>Directory(0)</li><li>Time Profile(0)</li><li>Account Code(0)</li><li>User Rights(9)</li><li>Location(1)</li><li>IPOSE-Primary</li><li>IP500V2-One<ul style="list-style-type: none"><li>System (1)</li><li>Line (3)</li><li>Control Unit (4)</li><li>Extension (24)</li><li>User (27)</li><li>Group (1)</li><li>Short Code (12)<ul style="list-style-type: none"><li>*92N;</li><li>9N</li></ul></li><li>Service (0)</li><li>RAS (1)</li><li>Incoming Call Route (1)</li><li>WAN Port (0)</li><li>Firewall Profile (1)</li><li>IP Route (4)</li><li>License (2)</li><li>Tunnel (0)</li><li>ARS (2)</li><li>Location (1)</li><li>Authorization Code (0)</li></ul></li><li>IP500V2-Two</li></ul></li></ul></li></ul>	<div>Short Code</div> <table><tr><td>Code</td><td>9N</td></tr><tr><td>Feature</td><td>Dial</td></tr><tr><td>Telephone Number</td><td>N</td></tr><tr><td>Line Group ID</td><td>51: To-Primary</td></tr><tr><td>Locale</td><td>United States (US English)</td></tr><tr><td>Force Account Code</td><td><input type="checkbox"/></td></tr><tr><td>Force Authorization Code</td><td><input type="checkbox"/></td></tr></table>	Code	9N	Feature	Dial	Telephone Number	N	Line Group ID	51: To-Primary	Locale	United States (US English)	Force Account Code	<input type="checkbox"/>	Force Authorization Code	<input type="checkbox"/>
Code	9N														
Feature	Dial														
Telephone Number	N														
Line Group ID	51: To-Primary														
Locale	United States (US English)														
Force Account Code	<input type="checkbox"/>														
Force Authorization Code	<input type="checkbox"/>														

## 6.6. Automatic Route Selection – ARS

The following screen shows an example ARS configuration for the route named “**To-Primary**” on the Expansion System. The **Telephone Number** is set to **9N**. The **Line Group ID** is set to “**99999**” matching the number of the **Outgoing Group ID** configured on the IP Office Line 17 to the Primary server (**Section 6.4**).

The screenshot displays the configuration window for an Automatic Route Selection (ARS) route named "To-Primary". The left sidebar shows a hierarchical tree of system components, with "ARS (2)" expanded to show "50: Main" and "51: To-Primary".

The main configuration area includes the following fields and options:

- ARS Route ID:** 51
- Route Name:** To-Primary
- Dial Delay Time:** System Default (4)
- Description:** (empty field)
- Secondary Dial tone:** ☐ (unchecked), dropdown menu showing "SystemTone"
- Check User Call Barring:** ☐ (unchecked)
- In Service:** ☒ (checked), linked to "Out of Service Route" dropdown (set to "<None>")
- Time Profile:** "<None>" dropdown, linked to "Out of Hours Route" dropdown (set to "<None>")

A table lists the route configuration:

Code	Telephone Number	Feature	Line Group ID
N	9N	Dial	99999

Buttons: Add..., Remove, Edit...

Below the table, the "Alternate Route" configuration is shown:

- Alternate Route Priority Level:** 3
- Alternate Route Wait Time:** 30
- Alternate Route:** "<None>" dropdown

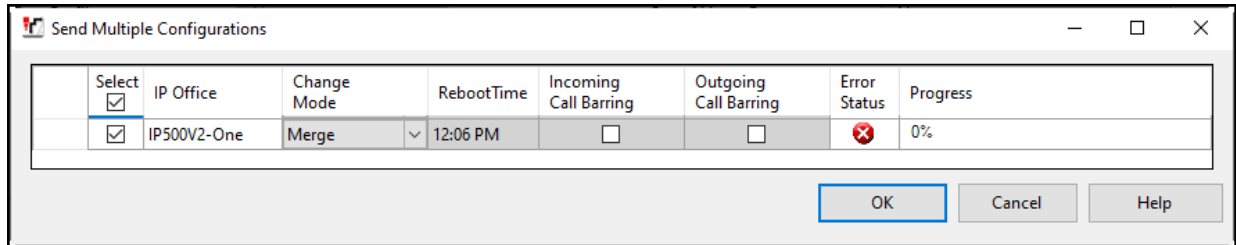
Repeat this process as needed to add additional Secondary server or Expansion Systems to the solution.



## 6.7. Save IP Office Expansion System Configuration

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

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



## 7. Clearfly Communications SIP Trunking Service Configuration

To use Clearfly Communications SIP Trunking Service, a customer must request the service from Clearfly Communications using the established sales processes. The process can be started by contacting Clearfly Communications via the corporate web site at: <https://www.clearfly.net/> or call (866) 652-7520.

During the signup process, Clearfly Communications and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Clearfly Communications network.

Clearfly Communications is responsible for the configuration of Clearfly Communications SIP Trunking Service. The customer will need to provide the public IP address used to reach the IP Office at the enterprise. In the case of the compliance test, this is the public IP address of the IP Office WAN port (LAN2) of the Primary server.

Clearfly Communications will provide the customer the necessary information to configure Avaya IP Office following the steps discussed in the previous sections, including:

- SIP Trunk registration credentials (User Name, Password, etc.).
- Clearfly Communications Domain Name.
- DID numbers.
- DNS IP addresses.
- Etc.

## 8. Verification Steps

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

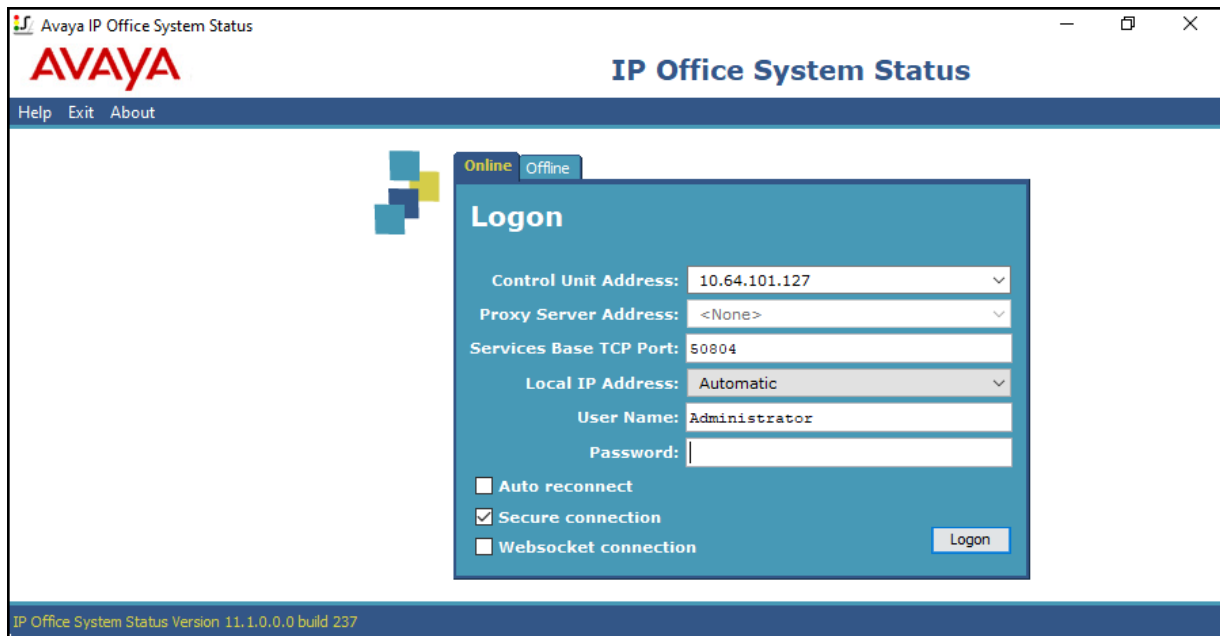
The following steps may be used to verify the configuration:

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

### 8.1. IP Office System Status

The following steps can also be used to verify the configuration.

Use the IP Office **System Status** application to verify the state of SIP connections. Launch the application from **Start → Programs → IP Office → System Status** on the PC where IP Office Manager is installed, log in with the proper credentials.



Select the SIP line under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current State** is **Idle** for each channel.

Avaya IP Office System Status - IPOSE-Primary (10.64.101.127) - IP Office Linux PC 11.1.0.0.0 build 237

## IP Office System Status

Help Snapshot LogOff Exit About

- System
- Alarms (35)
- Extensions (2)
- Trunks (3)
  - Line: 1
  - Line: 2
  - Line: 17
- Active Calls
- Resources
- Voicemail
- IP Networking
- Locations

Status
Utilization Summary
Alarms
Registration

### SIP Trunk Summary

Line Service State: In Service

Peer Domain Name: .cfly.co

Resolved Address:

Line Number: 17

Number of Administered Channels: 10

Number of Channels in Use: 0

Administered Compression: G711 Mu, G729 A

Enable Faststart: Off

Silence Suppression: Off


Media Stream: RTP

Layer 4 Protocol: UDP

SIP Trunk Channel Licenses: 10

SIP Trunk Channel Licenses in Use: 0

SIP Device Features: REFER (Incoming and Outgoing), UPDATE (Incoming and Outgoing)

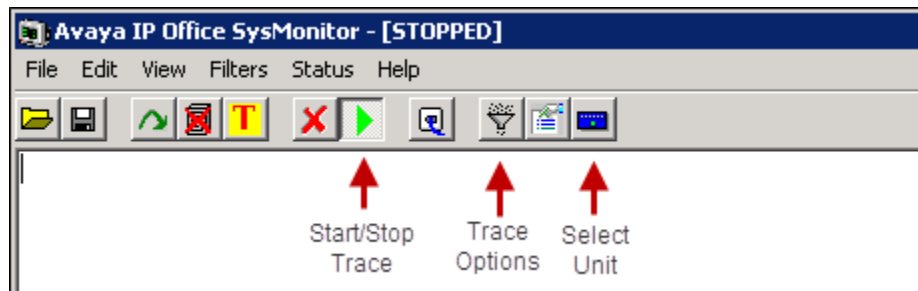
 0%

Channel Number	URI Gr...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call
1			Idle	16:18:56					
2			Idle	5 days 22:...					
3			Idle	6 days 21:...					
4			Idle	10 days 19...					
5			Idle	10 days 19...					
6			Idle	10 days 19...					
7			Idle	10 days 19...					
8			Idle	10 days 19...					
9			Idle	10 days 19...					
10			Idle	10 days 19...					

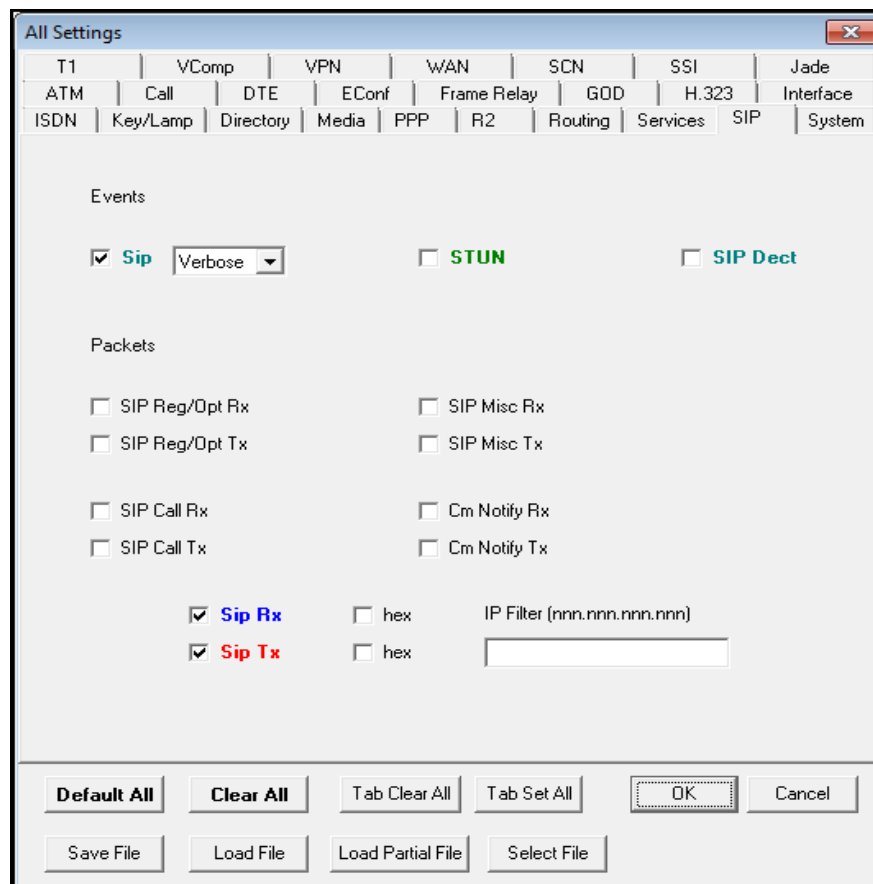
Trace
Trace All
Pause
Ping
Call Details
Graceful Shutdown
Force Out of Service
Print...

## 8.2. Monitor

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



Clicking the **Trace Options** icon on the taskbar, selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting the desired color.



## 9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office Release 11.1 to Clearfly Communications SIP Trunking Service using Trunk Registration. Clearfly Communications SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

## 10. Additional References

This section references the documentation relevant to these Application Notes. Product documentation for Avaya IP Office, including the following, is available at:

<http://support.avaya.com/>

- [1] *Deploying IP Office Server Edition*, Release 11.1, Issue 14, April 2020.
- [2] *IP Office Platform 11.0, Deploying Avaya IP Office Servers as Virtual Machines*, 15-601011 Issue 07d, June 9, 2020.
- [3] *IP Office Platform 11.0, Deploying Avaya IP Office Essential Edition (IP500 V2)*, 15-601042, Issue 35f, January 2020.
- [4] *Administering Avaya IP Office Platform with Manager*, Release 11.1 Issue 2, May 2020.
- [5] *Administering Avaya IP Office™ Platform with Web Manager*, Release 11.1 Issue 2, May 2020.
- [6] *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac and Windows*, Issue 1, Release 3.9, June 2020.
- [7] *Using Avaya IX™ Workplace Client for IP Office*, Release 11.1 Issue 9, June 2020.

Additional Avaya IP Office documentation can be found at:

<http://marketingtools.avaya.com/knowledgebase/>

---

**©2020 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](mailto:devconnect@avaya.com).