



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Configuring Avaya IP Office Release 9.1 to support Clearcom SIP Trunking Service using TLS - 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 9.1 to support Clearcom SIP Trunking Service using TLS.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the public switched telephone network (PSTN) with various Avaya endpoints. For privacy, Transport Layer Security (TLS) for Signaling was used.

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.

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

# 1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Clearcom and an Avaya SIP-enabled enterprise solution using Transport Layer Security (TLS).

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office 500v2 Release 9.1 (hereafter referred to as IP Office), Avaya Communicator for Windows and Avaya Deskphones, including SIP and H.323.

For privacy, TLS for Signaling, RTP for media was used outside of the enterprise (public network side, SRTP for media encryption was used inside of the enterprise (private network side).

The Clearcom SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the Avaya 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” or “Clearcom” 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 Clearcom’s 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.

### 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 and H.323 telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP Trunk from the service provider networks.

- Outgoing PSTN calls from Avaya endpoints including SIP and H.323 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 Communicator for Windows Softphone.
- Dialing plans including local calls (within Mexico), international, 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.729A, G.711A and G.711U, Clearcom's 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).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.

Items not supported or not tested included the following:

- REFER message for call redirection is supported by Clearcom but was not tested for reasons noted under **Section 2.2**.
- T.38 and G.711 fax pass-through was not tested for reasons noted under **Section 2.2**.
- Inbound toll-free call was not tested.
- 0, 0+10 digits, 411 Directory Assistance, 911 Emergency were not tested.

## 2.2. Test Results

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

- **Secure Real-time Transport Protocol (SRTP):** SRTP supports RTP media protection on a point to point basis providing confidentiality, message authentication, and replay protection. As SRTP is point to point, all individual links involved in the VoIP call, including key exchange/signaling, must be secure for the call to be secure from end to end. During the compliance test, it was observed that RTP, instead of SRTP, was always used outside of the enterprise (public network side). This behavior may be caused by the far-end not supporting SRTP. Thus **Best Effort** was used during the compliance test, allowing IP Office to use SRTP on the public network side if supported by the far-end, otherwise it defaults to RTP. SRTP for media encryption was used inside of the enterprise (private network side).
- **Call transfer to the PSTN using REFER:** PSTN calls that were transferred back to the PSTN network using REFER messages did not work properly. Calls that were blind transferred dropped. On attended transfers, the REFER message was accepted by Clearcom with a 202 message, but the trunks were not released. Due to these reasons, REFER was left disabled in the Avaya IP Office for the tests. With REFER disabled, blind and attended call transfers to the PSTN were allowed to complete, with the caveat that the IP Office was not released from the call path, and two trunks circuits remained seized for the duration of the call.
- **Outbound Calling Party Number (CPN) Block:** Clearcom did not allow outbound calls with privacy enabled. When an IP Office user activated “Withhold Number” to enable user privacy on an outbound call, IP Office sent “anonymous” in the “From” header and the “Privacy:id” header, while the caller information was still being sent in the “P-Asserted-Identity” header. Clearcom responded with a “403 PSTN calls are forbidden” message and the call was rejected.
- **Caller ID on inbound calls:** On inbound calls made from the test lab in the U.S., the Caller ID shown on the enterprise extensions occasionally showed “Unavailable”, while in other cases showed numbers corresponding to local PSTN numbers in Mexico, not the number of the original caller. Calls made from a local test number in Mexico showed the correct caller ID.
- **Caller ID on outbound calls:** On calls originating from IP Office extensions to PSTN telephones, the caller ID number displayed on the PSTN endpoint was always the main DID number assigned by Clearcom to the SIP trunk, not the specific DID assigned to the extension originating the call. This includes calls to “twinned” mobile phones, and calls that were forwarded or transferred back on the SIP trunk to the PSTN, where the number displayed on the PSTN endpoint was the main DID number on the trunk, not the originator’s caller’s ID. This may be a requirement of the Clearcom service for all outbound calls, it is listed here simply as an observation.
- **Fax support:** Fax calls using the T.38 protocol failed during the test. G.711 fax was also tested, but it behaved unreliably. Fax should not be used in this solution.

## 2.3. Support

For support on Clearcom systems visit the corporate Web page at: <http://www.clearcom.mx/>

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 Clearcom SIP trunk service through the public Internet.

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

- Avaya IP Office 500v2.
- Avaya Voicemail Pro for IP Office.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 1100 Series SIP IP Deskphones.
- Avaya Communicator for Windows Softphone.

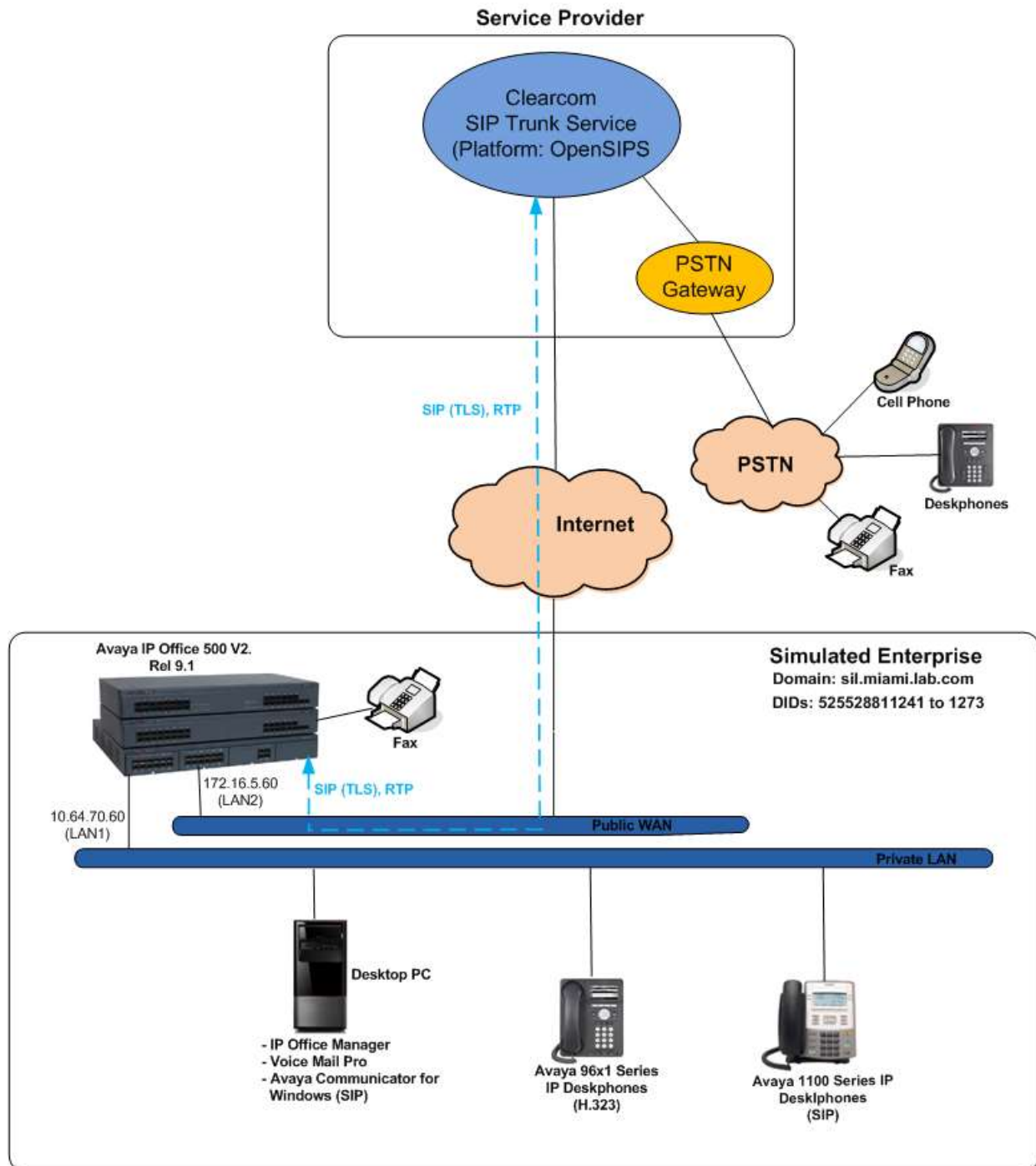
The enterprise site contains the Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codecs. The **LAN1** port of Avaya IP Office is connected to the enterprise LAN (private network) while the **LAN2** port is connected to the public network. Endpoints include Avaya 96x1 Series IP Deskphones (with H.323 firmware), Avaya 1100 IP Deskphones (with SIP firmware) and PC running Avaya Communicator for Windows Softphone. The site also has a Windows PC running Avaya IP Office Manager to configure and administer the Avaya IP Office system, and Avaya Voicemail Pro providing voice messaging service to the Avaya IP Office users. Mobile Twinning is configured for some of the Avaya IP Office users so that calls to these user's extensions will also ring and can be answered at the configured mobile phones.

For privacy, TLS for Signaling, RTP for media was used outside of the enterprise (public network side). SRTP for media encryption was used inside of the enterprise (private network side).

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Clearcom. The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to the network. Refer to **Section 5.6**.

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

For confidentiality and privacy purposes, public IP addresses 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 500v2	9.1.7.0 Build 163
Avaya IP Office DIG DCPx16 V2	9.1.7.0 Build 163
Avaya IP Office Manager	9.1.7.0 Build 163
Avaya Voicemail Pro Client	9.1.7.0 Build 5
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.115
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya Communicator for Windows	2.0.3.45
<b>Clearcom</b>	
OpenSIPS	1.9
OpenSIPS	1.9

*Testing was performed with Avaya IP Office 500 V2, but this testing also applies to Avaya IP Office Server Edition running the same software release. Note that Avaya IP Office Server Edition requires an Expansion IP Office 500 V2 R9 to support analog or digital endpoints or trunks.*



## 5. Configure Avaya IP Office

This section describes the IP Office configuration required to interwork with Clearcom SIP Trunking service. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP Office Manager. Navigate to **File → Open Configuration**, select the proper IP Office from the pop-up window, and log in with the appropriate credentials. A management window will appear as shown in the next sections. The appearance of IP Office Manager can be customized using the **View** menu (not shown). In the screenshots presented in this section, the **View** menu was configured to show the **Navigation Pane** on the left side and the **Details Pane** on the right side. These panes will be referenced throughout these Application Notes.

These Application Notes assume the basic installation and configuration of IP Office have already been completed and are not discussed here. For further information on IP Office, please consult **Error! Reference source not found.** in Section 9.

### 5.1. Licensing and Physical Hardware

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

To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License**, then from the license tab, locate **SIP Trunk Channels**. Confirm that there is a valid license with sufficient “Instances” (trunk channels) in the Details pane. Note that the full License Keys in the screen below is not shown for security purposes.

Feature	License Key	Instances	Status	Expiry Date	Source
IP Office Distributor Support - Stan...	RtQ42ReVV...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Prof...	FXCf8ToXt...	255	Valid	Never	ADI Nodal
UMS-Web Services	3tz3yXvcvt...	255	Valid	Never	ADI Nodal
Customer Service Agent	PtOp8LyjvS...	255	Obsolete	Never	ADI Nodal
Third Party API	Eg9W6a5s...	255	Valid	Never	ADI Nodal
one-X Portal for IP Office	qn8huAM6v...	255	Valid	Never	ADI Nodal
Avaya IP endpoints	4mh6b66b...	255	Valid	Never	ADI Nodal
Customer Service Supervisor	YnTLUnt5A...	255	Obsolete	Never	ADI Nodal
Advanced Edition	nIc966bYvL...	255	Valid	Never	ADI Nodal
Office Worker	zUWRyQ@...	255	Valid	Never	ADI Nodal
Small Site Software Upgrade 8 (R8.1)	KSVuShTD...	1	Valid	Never	ADI Nodal
Centralized Endpoints	a42SaNhoS...	255	Valid	Never	ADI Nodal
Software Upgrade 8 (R8.1)	s@KWBmMy...	1	Valid	Never	ADI Nodal
Essential Edition	fBudoHs8K...	255	Valid	Never	ADI Nodal
Avaya SIP Softphone	Virtual Ava...	254	Valid	Never	Virtual
Avaya IP endpoints	Virtual Ava...	255	Valid	Never	Virtual
<b>SIP Trunk Channels</b>	N/A	30	Valid	Never	PLDS Nodal

To view the physical hardware comprising Avaya IP Office, expand the components under the **Control Unit** in the Navigation pane. In the sample configuration, the Avaya IP Office 500v2 is equipped with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for 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 following screen shows the details of the **IP 500 V2**.

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, and on the right is the 'IP 500 V2' details pane.

**IP Offices Navigation Pane:**

- BOOTP (5)
- Operator (3)
- IP500V2 Main (selected)
- System (1)
  - IP500V2 Main
- Line (25)
  - Control Unit (4) (selected)
    - 1 IP 500 V2 (selected)
    - 2 VCM64/PRID U
    - 3 PHONE8
    - 6 DIG DCPx16 V2
- Extension (48)
- User (50)
- Group (1)
- Short Code (68)
- Service (0)
- RAS (1)
- Incoming Call Route (3)
- WAN Port (0)
- Directory (0)
- Time Profile (0)
- Firewall Profile (1)
- IP Route (11)
- Account Code (0)
- License (63)
- Tunnel (0)
- User Rights (8)
- ARS (2)
- RAS Location Request (0)
- Location (0)
- Authorization Code (0)

**IP 500 V2 Details Pane:**

Unit	
Device Number	1
Unit Type	IP 500 V2
Version	9.1.700.163
Serial Number	
Unit IP Address	10.64.70.60
Interconnect Number	0
Module Number	Control Unit

## 5.2. System

Configure the necessary system settings. In an Avaya IP Office the LAN2 tab settings correspond to the Avaya 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 Avaya IP Office WAN port was used to connect to Clearcom. The LAN2 settings correspond to the WAN port on the Avaya IP Office 500 V2. To access the LAN2 settings, first navigate to **System** → <Name>, where <Name> is the system name assigned to the Avaya IP Office. In this compliance test, the system name is **IP500V2 Main**. Next, navigate to the **LAN2** → **LAN Settings** tab in the Details Pane, configure the following parameters:

- Set the **IP Address** field to the public IP address assigned to the Avaya IP Office WAN port.
- Set the **IP Mask** field to the mask used with the public IP address. All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' tree shows the hierarchy: BOOTP (5), Operator (3), IP500V2 Main, System (1), and IP500V2 Main. The 'IP500V2 Main' system is selected. The main pane shows the 'IP500V2 Main' configuration tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, and SMTP. The 'LAN2' tab is active, and the 'LAN Settings' sub-tab is selected. The 'IP Address' field is set to 192 . 168 . 80 . 52, and the 'IP Mask' field is set to 255 . 255 . 255 . 128. Other fields include 'Primary Trans. IP Address' (0 . 0 . 0 . 0), 'Firewall Profile' (<None>), 'RIP Mode' (None), 'Enable NAT' (unchecked), 'Number Of DHCP IP Addresses' (200), and 'DHCP Mode' (Disabled). An 'Advanced' button is visible at the bottom right.

Field	Value
IP Address	192 . 168 . 80 . 52
IP Mask	255 . 255 . 255 . 128
Primary Trans. IP Address	0 . 0 . 0 . 0
Firewall Profile	<None>
RIP Mode	None
Enable NAT	<input type="checkbox"/>
Number Of DHCP IP Addresses	200
DHCP Mode	<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dialin <input checked="" type="radio"/> Disabled

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

- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Clearcom.
- Enter the Domain Name of the enterprise under **Domain Name**.
- Verify the **UDP Port**, **TCP Port** numbers under **Layer 4 Protocol** are set to **5060** and **TLS** port is set to **5061**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.

The screenshot displays the 'IP500V2 Main' configuration window. On the left, the 'IP Offices' tree shows the hierarchy: BOOTP (5), Operator (3), IP500V2 Main, System (1), IP500V2 Main, Line (25), Control Unit (4), Extension (48), User (50), Group (1), Short Code (68), Service (0), RAS (1), Incoming Call Route (3), WAN Port (0), Directory (0), Time Profile (0), Firewall Profile (1), IP Route (11), Account Code (0), License (63), Tunnel (0), User Rights (8), ARS (2), RAS Location Request (0), Location (0), and Authorization Code (0). The 'IP500V2 Main' item is selected and highlighted with a red box.

The main configuration area is titled 'IP500V2 Main' and has tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, and VCM. The 'LAN2' tab is active, and the 'VoIP' sub-tab is selected. The 'VoIP' sub-tab has three sections: 'LAN Settings', 'SIP', and 'Network Topology'. The 'SIP' section is expanded, showing the following settings:

- ☐ 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: sil.miami.avaya.com
- Layer 4 Protocol:
  - ☒ UDP: UDP Port 5060, Remote UDP Port 5060
  - ☒ TCP: TCP Port 5060, Remote TCP Port 5060
  - ☒ TLS: TLS Port 5061, Remote TLS Port 5061
- Challenge Expiry Time (secs): 10
- RTP:
  - Port Number Range: Minimum 49152, Maximum 53246
  - Port Number Range (NAT): Minimum 49152, Maximum 53246

The 'SIP Trunks Enable', 'SIP Registrar Enable', and the 'Layer 4 Protocol' section are highlighted with red boxes. The 'RTP' section is also highlighted with a red box.

Scroll down the page:

- In the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the periodic timeout to **30** and the **Initial Keepalives** parameter to **Enabled**. These settings will cause Avaya 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 to see media from the other, as well as helping to keep firewall ports open for the duration of the call.
- In the **DiffServ Settings** section, Avaya IP Office can also 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 example below and are also the default values. For a customer installation, if the default values are not sufficient, appropriate values will be provided by the customer.
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface for the 'IP500V2 Main' system. On the left, a tree view shows the system hierarchy, with 'IP500V2 Main' and its sub-items like 'System (1)' and 'IP500V2 Main' highlighted. The main panel shows the 'LAN2' tab selected, with the 'VoIP' sub-tab active. The 'VoIP' settings are divided into several sections: 'RTCP Monitoring on Port 5005' (checked), 'Keepalives' (Scope: RTP-RTCP, Periodic timeout: 30, Initial keepalives: Enabled), 'DiffServ Settings' (B8 DSCP, 46 DSCP, B8 Video DSCP, 46 Video DSCP, FC DSCP Mask, 63 DSCP Mask, 88 SIG DSCP, 34 SIG DSCP), and 'DHCP Settings' (Primary Site Specific Option Number: 176, Secondary Site Specific Option Number: 242, VLAN: Not Present, 1100 Voice VLAN Site Specific Option Number: 232, 1100 Voice VLAN IDs: empty). The 'LAN2' tab is highlighted with a red box, and the 'VoIP' sub-tab is also highlighted with a red box. The 'DiffServ Settings' section is also highlighted with a red box.

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

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. Since no firewall or network address translation (NAT) device was used between the Avaya IP Office and the Clearcom, the parameter was set to **Open Internet**.
- Set the **Binding Refresh Time (seconds)** to a desired value, the value of **300 (or every 5 minutes)** was used during the compliance testing. This value is used to determine the **frequency** that IP Office will send OPTIONS heartbeat to the service provider.
- Set **Public IP Address** to the IP address of the Avaya IP Office WAN port.
- In the **Public Port** section, next to the transport protocol **TLS**, select the **TLS** port on which Avaya IP Office will listen, for TLS, the well-known port is **5061**.
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

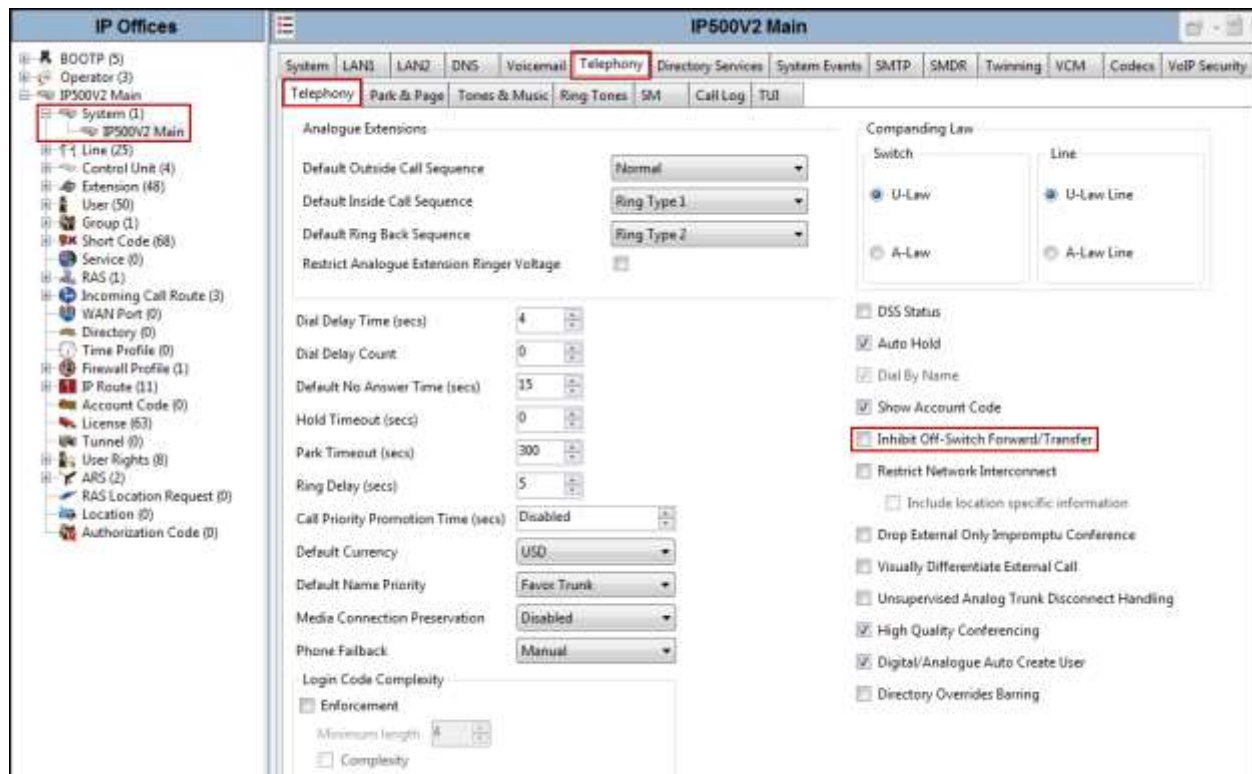
The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' tree shows the hierarchy: BOOTP (5), Operator (3), IP500V2 Main, System (1), and IP500V2 Main. The 'IP500V2 Main' configuration is selected. The main pane shows the 'IP500V2 Main' configuration with tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and Twinning. The 'LAN2' tab is active, and the 'Network Topology' sub-tab is selected. The 'Network Topology Discovery' section contains the following fields: STUN Server Address (69.90.168.13), STUN Port (3478), Firewall/NAT Type (Open Internet), Binding Refresh Time (seconds) (300), and Public IP Address (192 . 168 . 80 . 52). The 'Public Port' section includes UDP (5060), TCP (0), and TLS (5061). A checkbox for 'Run STUN on startup' is present. The 'Run STUN' and 'Cancel' buttons are at the bottom right.

**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 Clearcom SIP Trunk Service, and therefore is not described in these Application Notes.

## 5.2.2. System - Telephony Tab

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

- 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).

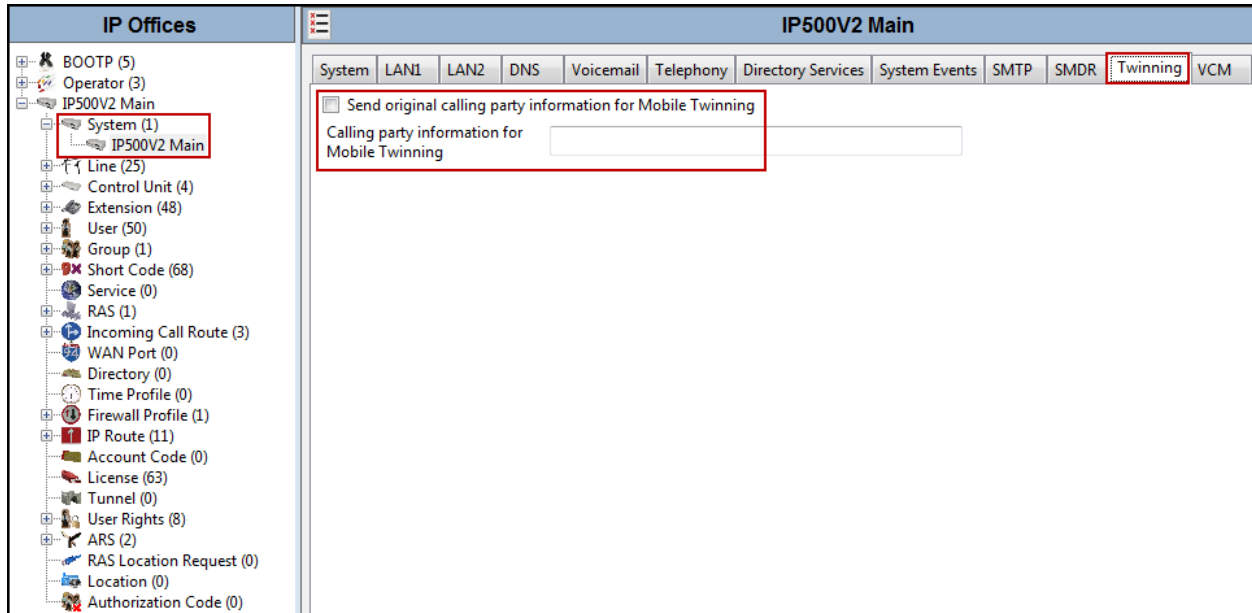




### 5.2.3. System - Twinning Tab

To view or change the System Twinning settings, navigate to the **Twinning** tab in the Details Pane as shown in the following screen, configure the following parameters:

- 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.
- Click **OK** to commit (not shown).

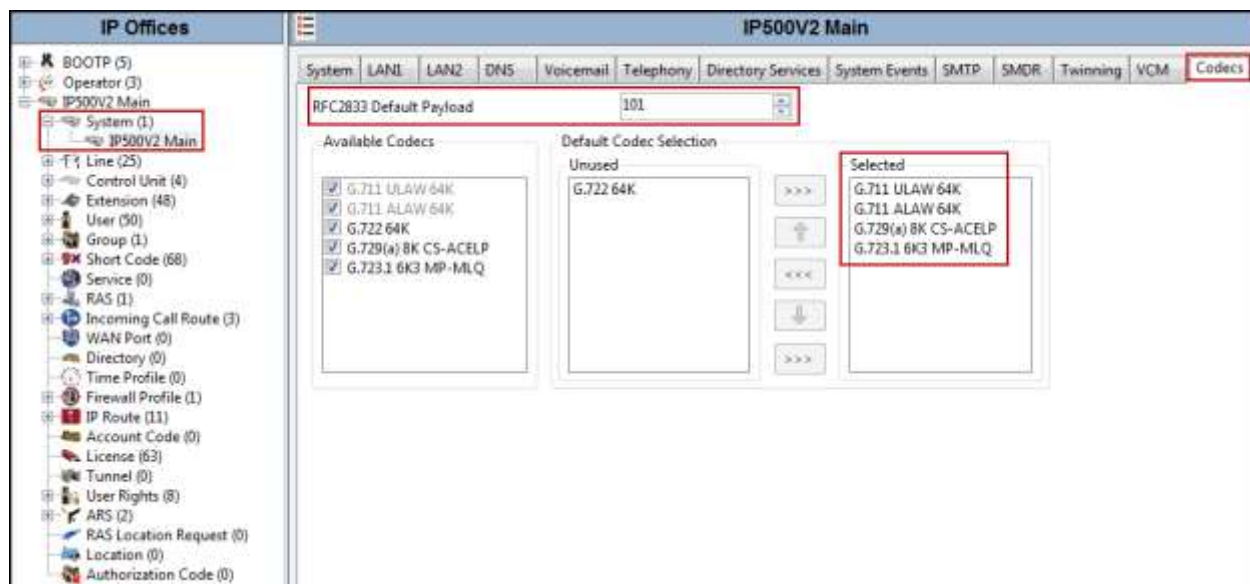




## 5.2.4. System - Codecs Tab

To view or change the System Codecs settings, navigate to the **Codecs** tab in the Details Pane as shown in the following screen, 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 was used.
- Click **OK** to commit (not shown).



### 5.2.5. System – 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.

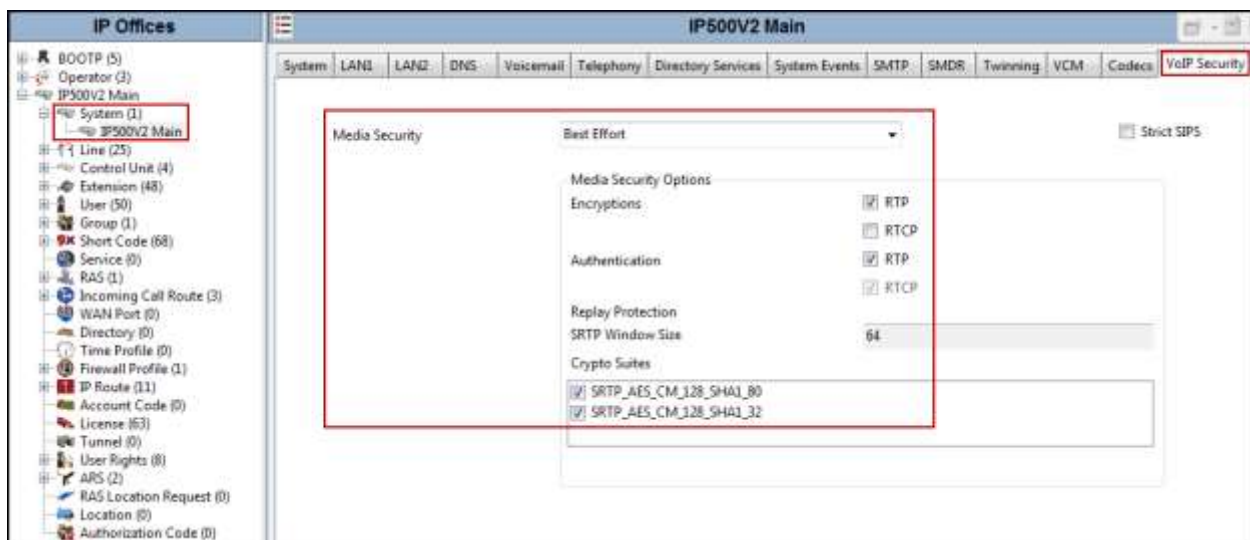
Configuring the use of SRTP at the system level is done on the **System→VoIP Security** tab using the Media Security setting. The options are:

- Best Effort
- Disabled (default)
- Enforced

When enabling SRTP on the system, the recommended setting is **Best Effort**. 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, navigate to the **VoIP Security** tab in the Details Pane as shown in the following screen, configure the following parameters:

- Under **Media Security** select **Best Effort** from the pull down menu.
- Under **Media Security Options** ensure that **RTP** is checked under **Encryptions** and **Authentication**.
- Under Crypto Suites ensure that **SRTP\_AES\_CM\_128\_SHA1\_80** and **SRTP\_AES\_CM\_128\_SHA1\_32** are checked.
- Verify that Strict **SIPS** is not checked.
- Click **OK** to commit (not shown).



### 5.2.6. 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 Clearcom's network.

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

- Set **IP Address** and **IP Mask** as needed.
- Set **Gateway IP Address** to the IP address of the default router for the public network where Avaya IP Office **LAN2** port is connected.
- Set **Destination** to **LAN2** from the drop-down list.
- Click the **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows various configuration categories, with 'IP Route (11)' highlighted. The main panel on the right is titled '172.16.179.0' and contains the 'IP Route' configuration form. The form fields are as follows:

172.16.179.0	
IP Route	
IP Address	172 . 16 . 179 . 0
IP Mask	255 . 255 . 255 . 128
Gateway IP Address	192 . 168 . 80 . 1
Destination	LAN2
Metric	0
<input type="checkbox"/> Proxy ARP	

## 5.3. SIP Line

A SIP Line is needed to establish the SIP connection between IP Office and Clearcom SIP Trunking Service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by Avaya IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.3.1** and **5.3.2** 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 trunk Registration Credentials.
- SIP URI entries.
- Setting of the Use Network Topology Info field on the Transport tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.3.3** to **5.3.8**.

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 5.3.3** to **5.3.8**.

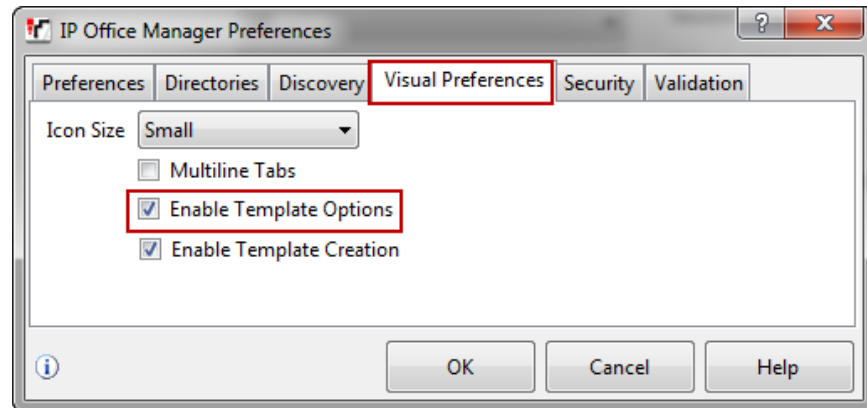
### 5.3.1. Importing a SIP Line Template

**Note:** DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500v2) and IP Office Server Edition systems. 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.

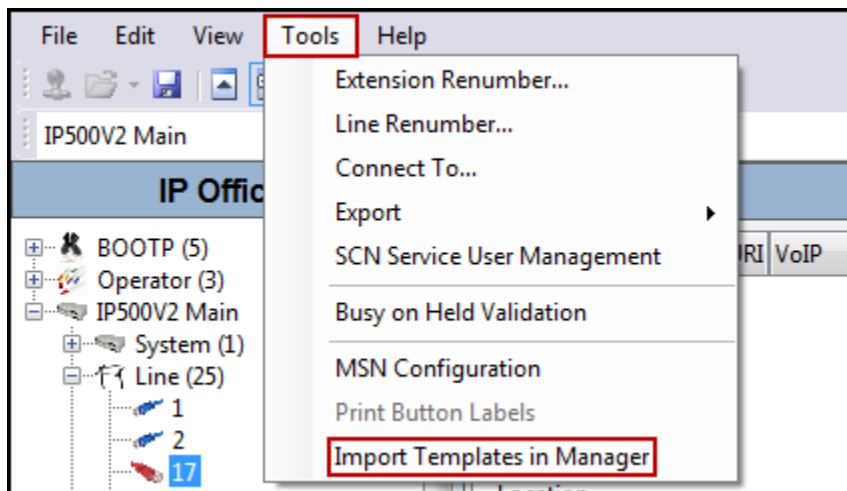
1. Copy a previously created template file to a location (e.g., C:\Temp) on the same computer where IP Office Manager is installed. By default, the template file name will have the format **AF\_<user supplied text>\_SIPTrunk.xml**, where the **<user supplied text>** portion is entered during template file creation.

**Note:** If necessary, the **<user supplied text>** portion of the template file name may be modified, however the **AF\_<user supplied text>\_SIPTrunk.xml** format of the file name must be maintained. For example, an original template file **AF\_TEST\_SIPTrunk.xml** could be changed to **AF\_Test1\_SIPTrunk.xml**. The template file name is selected in **Section 5.3.2, step 2**, to create a new SIP Line.

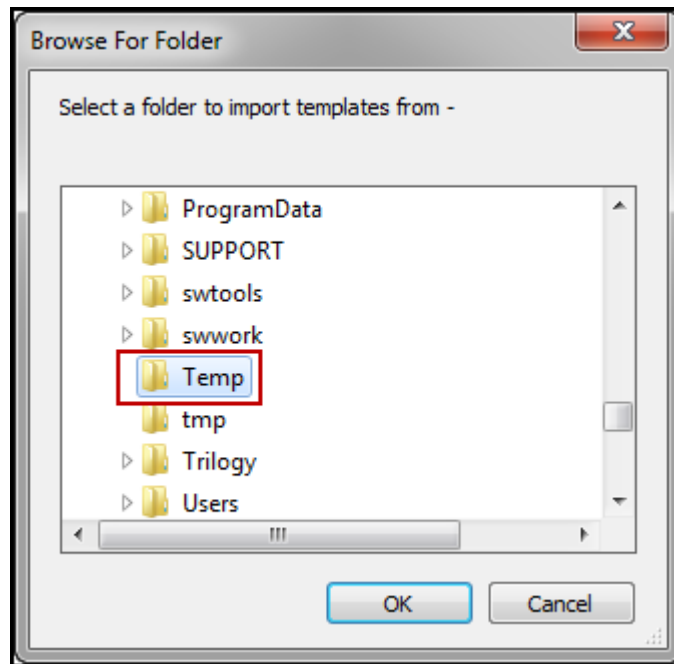
2. Verify that Template Options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the **Visual Preferences** tab. Check the box next to **Enable Template Options**. Click **OK**.



3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**.

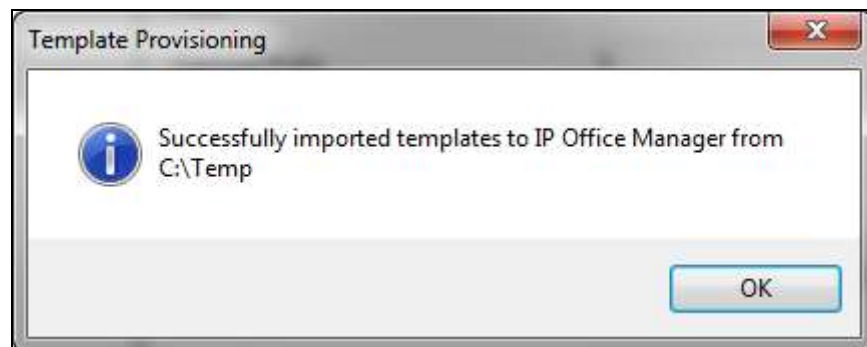


4. A folder browser will open. Select the directory used in **step 1** to store the template(s) (e.g., C:\Temp).

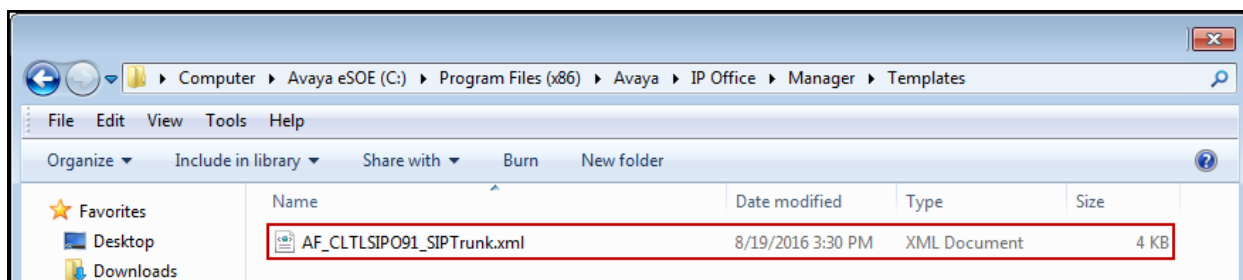
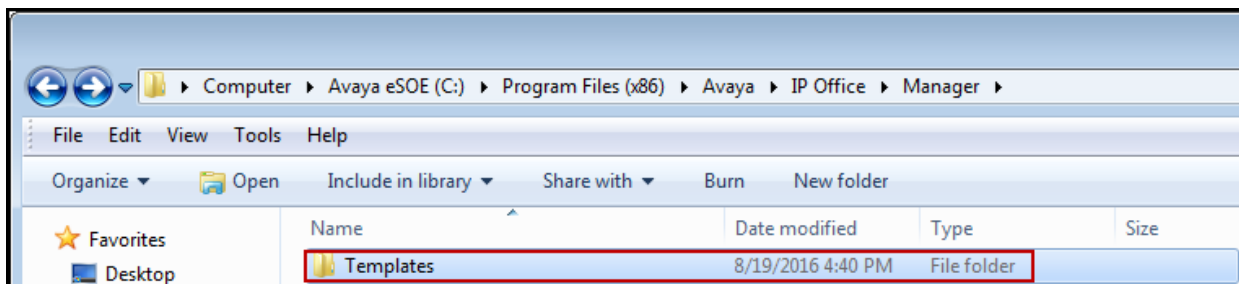
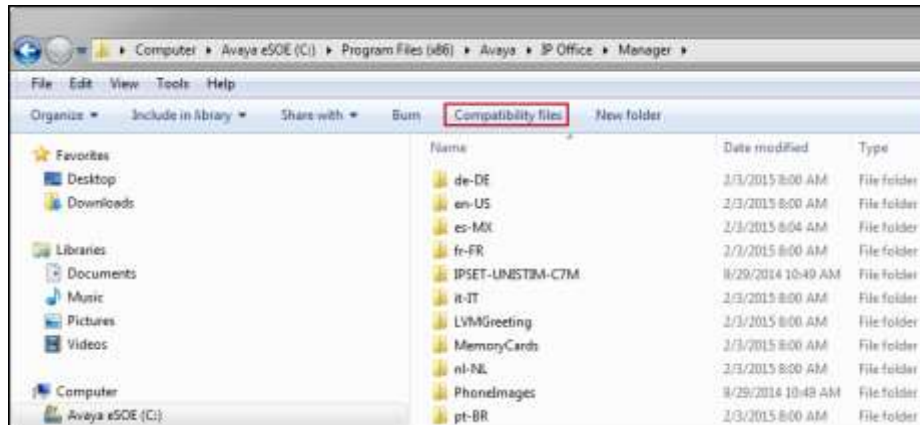


In the reference configuration, template files **AF\_CLTLSIPO91\_SIPTrunk.xml** was imported. The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.

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

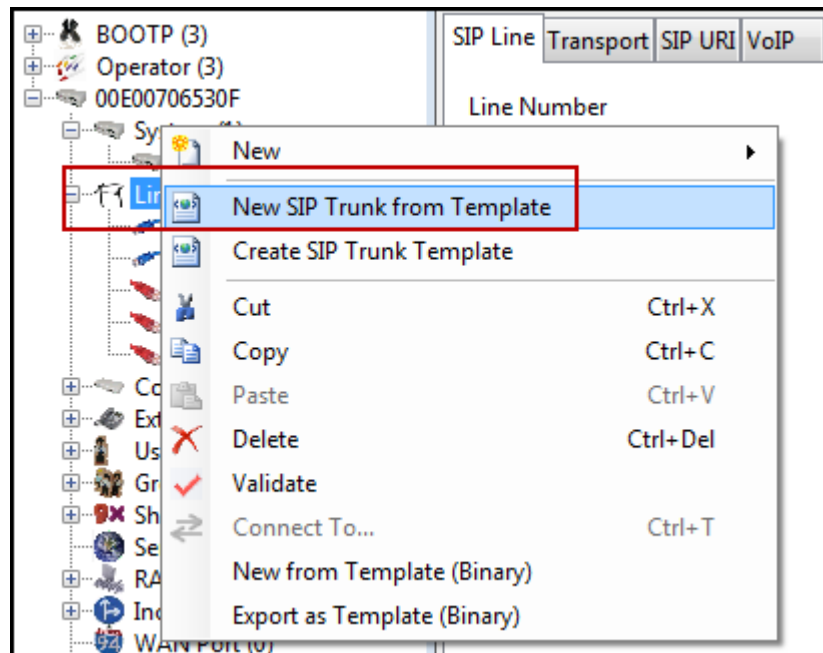


**Note:** Windows 7 (and later) locks the Avaya IP Office 9.1 **\Templates** directory, and it cannot be viewed. To enable browsing of the **\Templates** directory, open Windows Explorer, navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates** (or **C:\Program Files (x86)\Avaya\IP Office\Manager\Templates**), and then click on the **Compatibility files** option shown below. The **\Templates** directory and its contents can then be viewed.



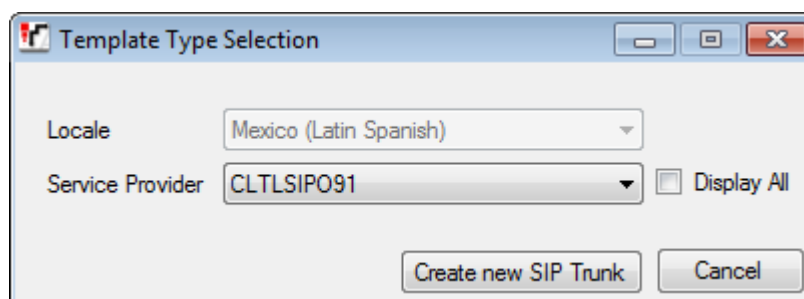
### 5.3.2. Creating a SIP Trunk from an XML Template

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



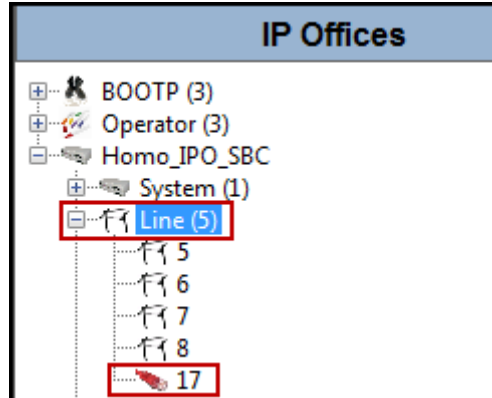
2. In the subsequent **Template Type Selection** pop-up window, from the **Service Provider** pull-down menu, select the XML template name from **Section 5.3.1**. Click **Create new SIP Trunk**.

**Note:** The drop down menu will display the *<user supplied text>* part of the template file name (see **Section 5.3.1**). If the **Display All** box is checked, then the full template file name is displayed.





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

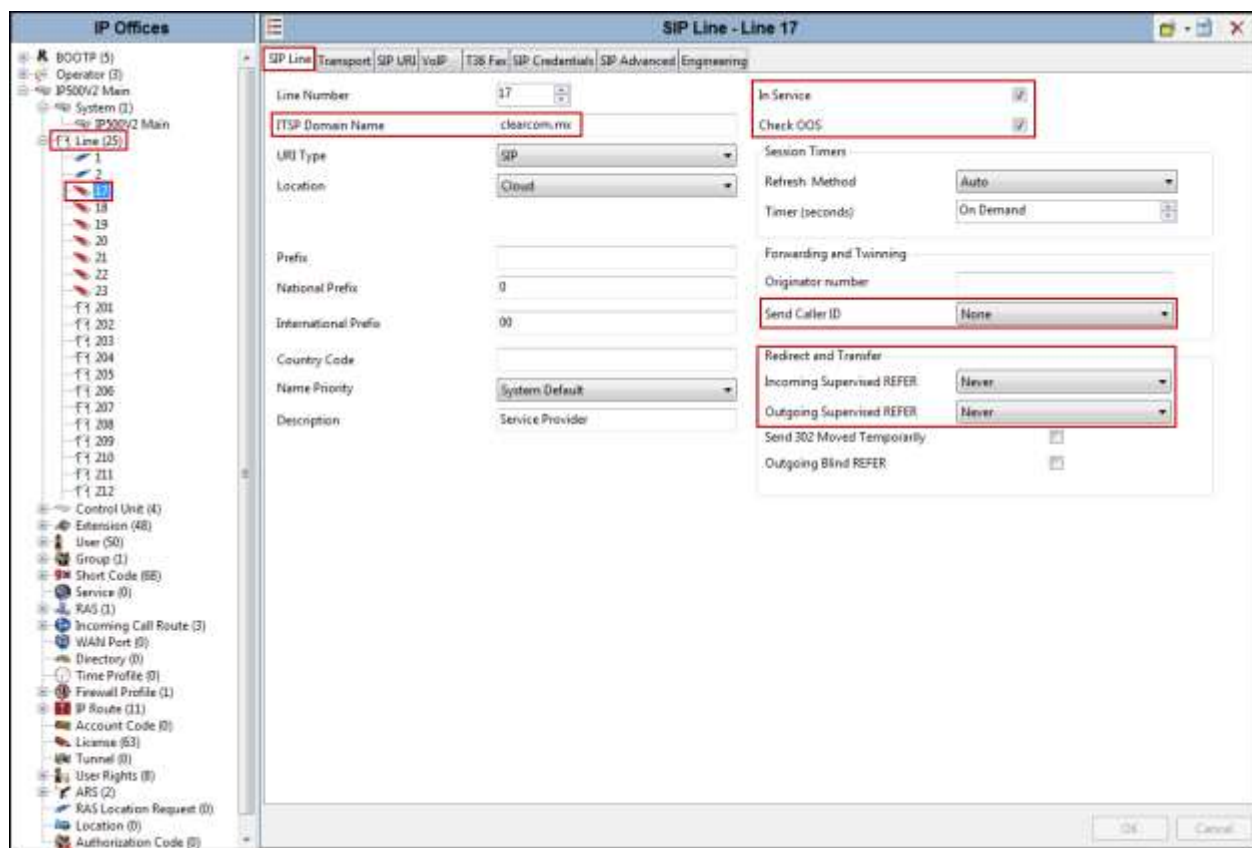


6. It is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.3.3 to 5.3.8**.

### 5.3.3. 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 **clearcom.mx**, the domain name for Clearcom.
- 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. Avaya IP Office will use the SIP OPTIONS method to periodically check the SIP Line. The time between SIP OPTIONS sent by Avaya IP Office will use the **Binding Refresh Time** for LAN2, as shown in **Section 5.2.1**.
- Verify that **Send Caller ID** is set to **None**, the default value.
- For the compliance test **REFER Support** was disabled. Thus, **Incoming Supervised REFER** and **Outgoing Supervised Refer** should be set to **Never**. Refer to **Section 2.2**.
- Click **OK** to commit.



### 5.3.4. 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 using public DNS queries).
- Set **Layer 4 Protocol** to **TLS**.
- Set **Use Network Topology Info** to **LAN2**, the network port used by the SIP line to access the far-end configured in **Section 5.2.1**.
- Set the **Send Port** to **5061**.
- Set **Explicit DNS Server(s)** to the IP addresses of the primary and secondary public DNS Servers used by the enterprise. This information should be provided by the local ISP. IP Office will use public DNS queries using Clearcom's domain name provided (clearcom.mx) to obtain the public IP of Clearcom.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the IP Office configuration interface. On the left, a tree view shows the hierarchy of components, with 'Line (25)' expanded and 'Line 17' selected. The main panel shows the configuration for 'SIP Line - Line 17', with the 'Transport' tab selected. The 'ITSP Proxy Address' field is empty. The 'Network Configuration' section shows 'Layer 4 Protocol' set to 'TLS', 'Send Port' set to '5061', 'Use Network Topology Info' set to 'LAN 2', 'Listen Port' set to '5061', and 'Explicit DNS Server(s)' set to '75.75.75.75' and '75.75.75.76'. The 'Calls Route via Registrar' checkbox is checked. The 'Separate Registrar' field is empty.

### 5.3.5. 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**, add the user name credential provided by Clearcom for SIP Trunk registration.
- For **Authentication Name**, add the authentication name credential provided by Clearcom for SIP Trunk registration, this should be the same as the **User name** above.
- For **Password** and **Confirm Password**, add the password credential provided by Clearcom for SIP Trunk registration.
- Set **Expiry (mins)** to a value acceptable to the enterprise. This setting defines how often registration with Clearcom is required following any previous registration. For the compliance test **2** minutes was used.
- Verify that **Registration required** is checked.
- Click the **OK** to commit.

The screenshot displays the 'SIP Line - Line 17\*' configuration window. The 'SIP Credentials' tab is selected, showing a table with the following data:

Index	UserName	Authentication Name	Contact	Expiry (mins)	Register
1	user123	user123		2	True

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

- User name: user123
- Authentication Name: user123
- Contact: (empty)
- Password: (masked with dots)
- Confirm Password: (masked with dots)
- Expiry (mins): 2
- Registration required: ☒

The 'OK' button is visible in the bottom right corner of the dialog.

### 5.3.6. SIP Line - SIP URI Tab

Two SIP URI entries must be created to match each outgoing number that Avaya IP Office will send on this line and incoming numbers that Avaya IP Office will accept on this line.

To set the SIP URI for outgoing numbers, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. The entry was created with the parameters shown below:

- Set **Local URI** to **Use Credentials User Name**.
- Set **Contact**, **Display Name** and **PAI** to **Use Internal Data**.
- Set **Registration** to **1: user123** (Note that this field will default to the **User Name** used under the **SIP Credentials** tab).
- Set **Incoming Group** to **0**.
- Set **Outgoing Group** to **17** (SIP Line number being used).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit.

The screenshot displays the Avaya IP Office configuration interface for a SIP Line. On the left, a tree view under 'IP Offices' shows 'Line 17' selected. The main pane is titled 'SIP Line - Line 17' and contains a tabbed interface with 'SIP URI' selected. A table lists two channels:

Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	0 17	1...	user123				1: user123	10
2	17 0	1...				N...	0: <Non...	10

Below the table is an 'Edit Channel' form. A red box highlights the following fields:

- Local URI: Use Credentials User Name
- Contact: Use Internal Data
- Display Name: Use Internal Data
- PAI: Use Internal Data
- Registration: 1: user123

Other fields in the form include:

- Via: 192.168.80.52
- Incoming Group: 0
- Outgoing Group: 17
- Max Calls per Channel: 10

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

To set the SIP URI for incoming numbers, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact**, and **Display Name** to **Use Internal Data**.
- Set **PAI** to **None**.
- Set **Registration** to **0: <None>**.
- Set **Incoming Group** to **17** (SIP Line number being used).
- Set **Outgoing Group** to **0**.
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit.
- Click **OK** to commit again (not shown).

**SIP Line - Line 17\***

SIP Line | Transport | SIP URI | VoIP | T38 Fax | SIP Credentials | SIP Advanced | Engineering

Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	0 17	1...	user123				1: user123	10
2	17 0	1...				N...	0: <Non...	10

**Edit Channel**

Via: 192.168.80.52

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

PAI: None

Registration: 0: <None>

Incoming Group: 17

Outgoing Group: 0

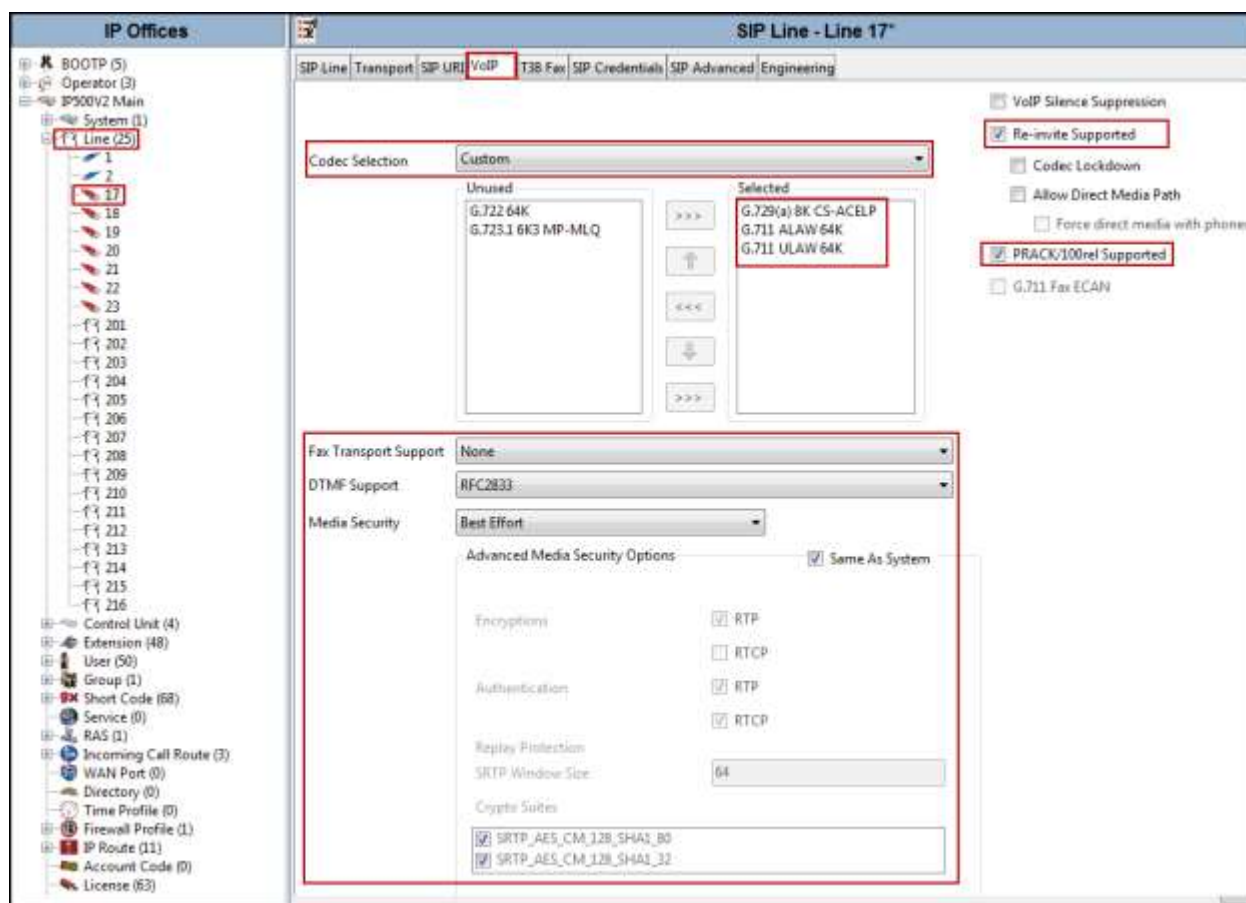
Max Calls per Channel: 10

OK Cancel

### 5.3.7. 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:

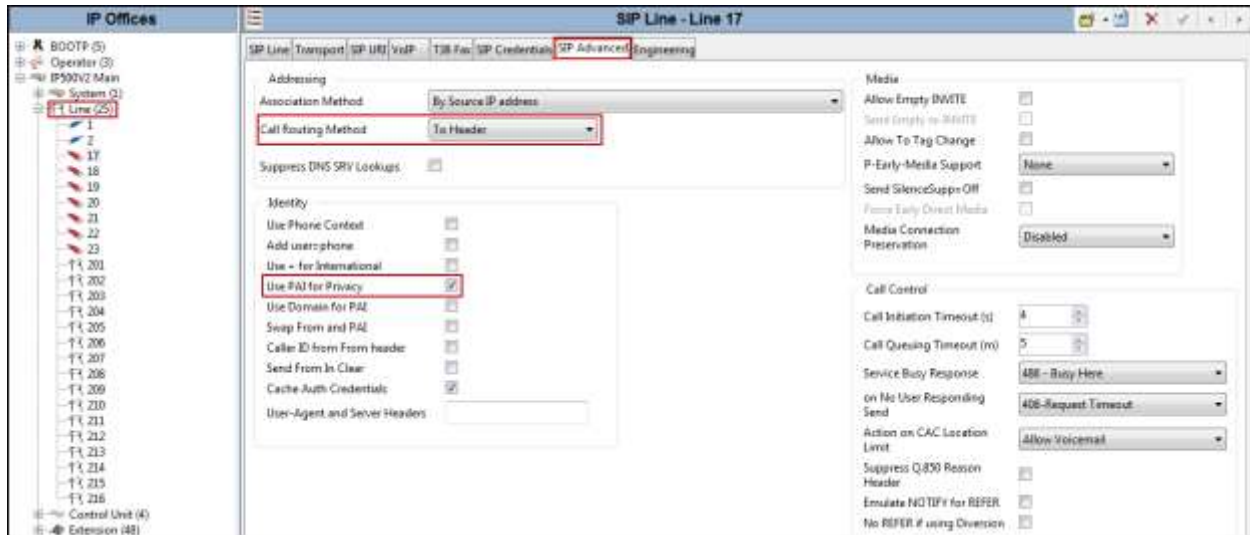
- For **Codec Selection**, select **System Default** from the pull-down menu to use the default list of codecs. A list of the codecs in their current order of preference will be shown on the right in the **Selected** column. To use a custom list of codecs, select **Custom** for **Codec Selection**. Next, move unwanted codecs from the **Selected** column to the **Unused** column. Lastly, move the codecs up or down the list in the **Selected** column to achieve the desired order of preference. The example below shows the codecs used for the compliance test (Note that **Custom** Codec Selection was used). The list must include G.729(a), G.711ALAW and G.711 ULAW which are the codecs supported by Clearcom. Codecs are listed in preferred codec order (from top to bottom).
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- Under **Media Security** select **Best Effort** from the pull-down menu.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).



### 5.3.8. SIP Line – SIP Advanced Tab

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

- Under **Call Routing Method** select **To Header** from the pull-down menu.
- Check the box for **Use PAI for Privacy**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).





## 5.4. Extension

In this section, an example of an Avaya IP Office extension will be illustrated. In the interests of brevity, not all users and extensions will be presented, since the configuration can be easily extrapolated to other users and extensions. To add an extension, right click on **Extension** then select **New** → **Select H323 or SIP**.

Select the **Extn** tab. Following is an example of extension **1540**; this extension corresponds to an H.323 extension.

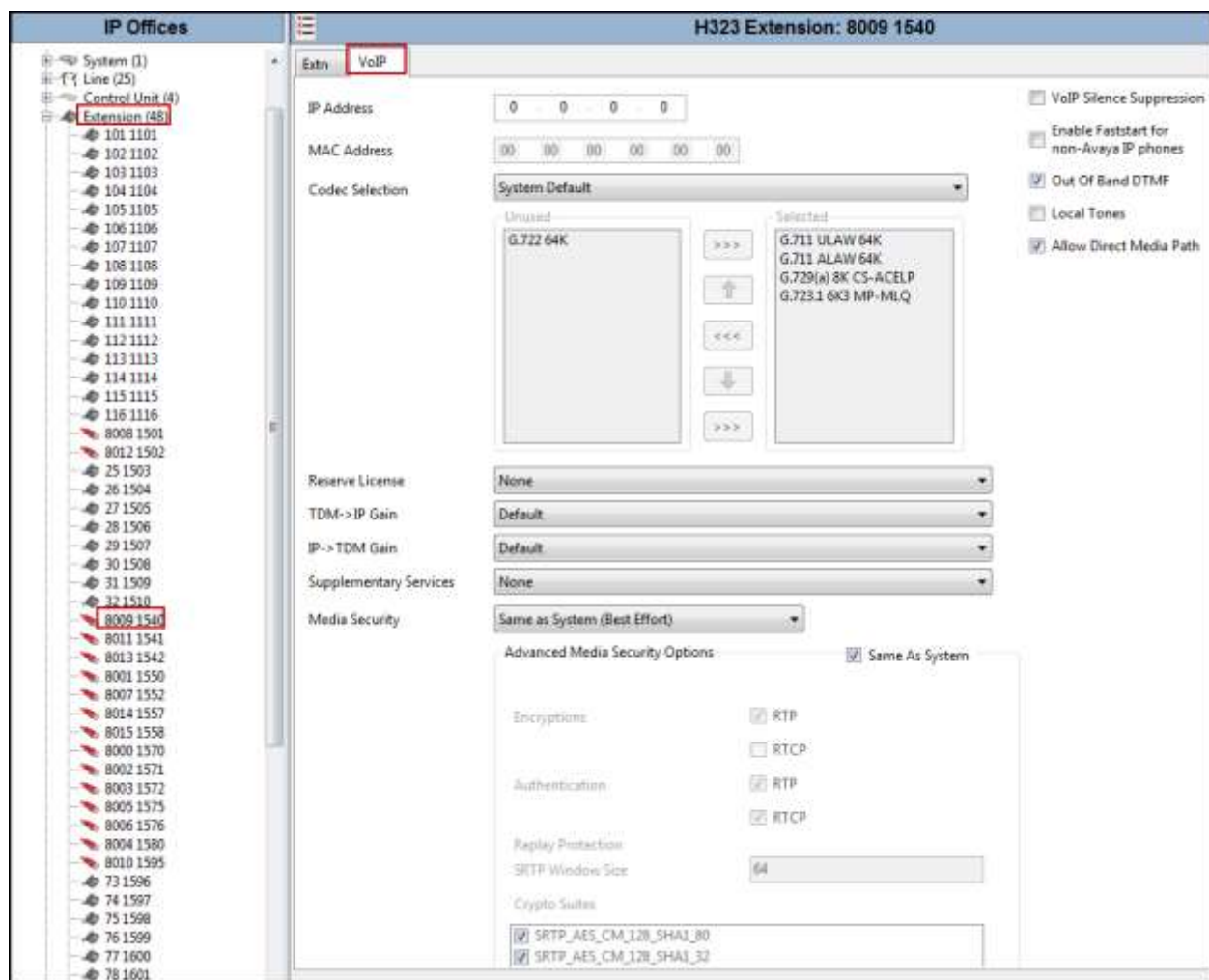
The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows a hierarchy: System (1) > Line (25) > Control Unit (4) > Extension (48). The 'Extension (48)' folder is selected, and a list of extensions is shown, including 101 1101 through 116 1116, 8008 1501, 8012 1502, 25 1503, 26 1504, 27 1505, 28 1506, 29 1507, 30 1508, 31 1509, 32 1510, 8009 1540 (highlighted with a red box), and 8011 1541. The main panel on the right is titled 'H323 Extension: 8009 1540' and contains two tabs: 'Extn' (selected) and 'VoIP'. The 'Extn' tab shows the following configuration fields:

Extension ID	8009
Base Extension	1540
Phone Password	
Confirm Phone Password	
Caller Display Type	On
Reset Volume After Calls	<input type="checkbox"/>
Device Type	Avaya 9641
Location	Automatic
Fallback As Remote Worker	Auto
Module	0
Port	0
Disable Speakerphone	<input type="checkbox"/>

Select the **VOIP** tab. Use default values on VoIP tab. Following is an example for extension 1540; this extension corresponds to an H.323 extension.

By default, all IP phones (SIP and H.323) will use the system default codec selection configured under the System Codecs tab (**Section 5.2.4**), unless configured otherwise for a specific extension by selecting **Custom** under **Codec Selection** on the screenshot shown below. The example below shows the codecs used for IP phones (SIP and H.323).

By default, all IP phones (SIP and H.323) will use the system default Media Security selection configured under the System **VoIP Security** tab (**Section 5.2.5**), unless configured otherwise for a specific extension by selecting **Media Security** under **VoIP** tab on the screenshot shown below. The **Media Security** field was set to **Same as System (Best Effort)**. The example below shows the Media Security used for IP phones (SIP and H.323).



## 5.5. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.3**. 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 **IP H323 1540**. Select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.3.6**). The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Clearcom. 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. Click the **OK** to commit (not shown).

The screenshot displays the Avaya User Configuration interface. On the left, the 'IP Offices' pane lists various users, with '1540 IP H323 1540' highlighted. The main pane shows the configuration for this user, with the 'SIP' tab selected. The 'SIP' tab contains the following fields:

Dial In	Voice Recording	Button Programming	Menu Programming	Mobility	Group Membership	Announcements	SIP
SIP Name 5528811242							
SIP Display Name (Alias) IP H323 1540							
Contact 5528811242							
<input type="checkbox"/> Anonymous							

## 5.6. 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.

### 5.6.1. Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code** on 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 Avaya 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.
- Click the **OK** to commit (not shown).


The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' navigation pane lists various short codes, with '9N' highlighted. The main configuration area on the right is titled '9N: Dial' and contains a 'Short Code' tab. A red rectangular box highlights the configuration fields for the short code:

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 **X**'s 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**.

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **001** followed by **10 X**'s 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 **001N**. The value **N** represents the additional number of digits dialed by the user after dialing **001** (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.
- Click **OK** to commit.



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

The first example highlighted below shows that for calls from Mexico to the North American numbering plan, the user dialed **9**, followed by **001** and **10** digits (represented by **10 X's**). The second example highlighted shows an eight digit number starting with a **28**, which is for local calls in Mexico, the user dialed **9**, followed by the local number (e.g., 28811234). In each case the **9** is stripped off, the remaining digits, including the **001** and **28** shown in the examples below, are included in the SIP INVITE message IP Office sends to Clearcom.

**IP Offices**

- BOOTP (3)
- Operator (3)
- 00E00706330F
- System (1)
- Line (3)
- Control Unit (4)
- Extension (37)
- User (32)
- Group (1)
- Short Code (55)
- Service (0)
- RAS (1)
- Incoming Call Route (2)
- WAN Port (0)
- Directory (0)
- Time Profile (0)
- Firewall Profile (1)
- IP Route (5)
- Account Code (0)
- License (74)
- Tunnel (0)
- User Rights (8)
- ARS (1)**
- RAS Location Request (0)
- Location (0)

**Main**

ARS

ARS Route Id: 10

Route Name: Main

Dial Delay Time: System Default (3)

In Service: ☒ Out of Service Route: <None>

Time Profile: <None> Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
001XXXXXXXXXX	001N	Dial	17
8XXXXXXXXXX	8N	Dial	17
1XXXXXXXXXX	1N	Dial	17
6XXXXXXXXXX	6N	Dial	17
3XXXXXXXXXX	3N	Dial	17
28XXXXXXX	28N	Dial	17
55XXXXXXXXXX	55N	Dial	17

Alternate Route Priority Level: 1

## 5.7. Incoming Call Route

An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system.

In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in IP Office. The routing decision for the call is based on the parameters previously configured for **Call Routing Method** and **SIP URI** (Section 5.3.6) and the users **SIP Name** and **Contact**, already populated with the assigned Clearcom DID numbers (Section 5.5).

### 5.7.1. Incoming Call Route – Standard Tab

On the **Standard** tab of the Details pane, enter the parameters as shown below:

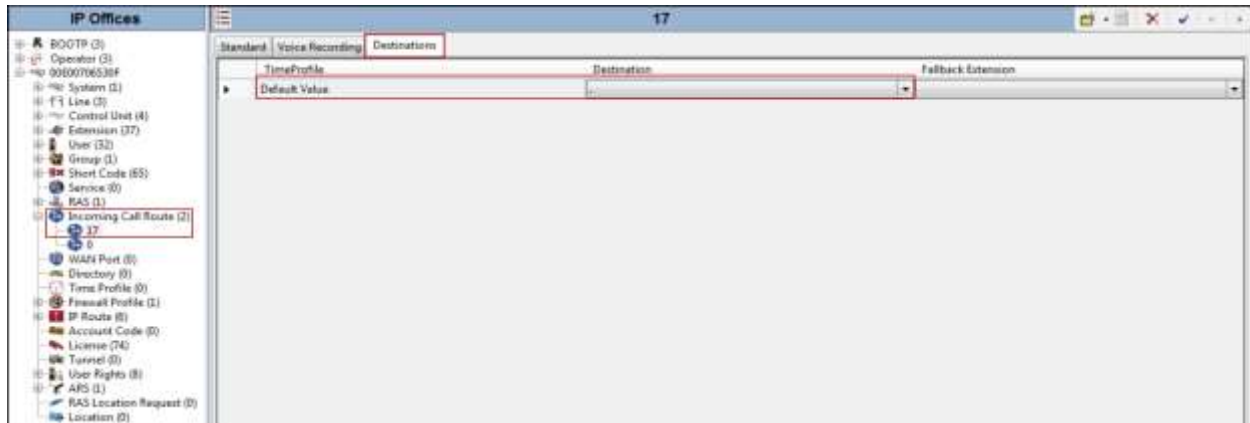
- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in Section 5.3, in this case **Line Group ID 17** was used.
- Default values can be used for all other fields.

The screenshot displays the IP Office configuration interface. On the left, a tree view under 'IP Offices' shows various system components, with 'Incoming Call Route (2)' and its sub-item '17' highlighted with a red box. On the right, the 'Standard' tab of the configuration pane is active, also highlighted with a red box. The configuration fields are as follows:

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

### 5.7.2. Incoming Call Route – Destinations Tab

Under the **Destinations** tab, enter “.” for the **Default Value**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of the **User**, which matches the number present on the user part of the “To” header on the incoming INVITE message received from Clearcom. Click **OK** to commit (not shown).



### 5.8. 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 will appear, with either **Merge** or **Immediate** 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.





## 6. Clearcom SIP Trunk Services Configuration

To use Clearcom's SIP Trunk service, a customer must request the service from Clearcom using the established sales processes. The process can be started by contacting Clearcom via the corporate web site at: <http://www.clearcom.mx/> and requesting information.

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

Clearcom is responsible for the configuration of Clearcom SIP Services. The customer will need to provide the public IP address used to reach the Avaya IP Office at the enterprise. In the case of the compliance test, this is the public IP address of the Avaya IP Office WAN port (LAN2). The customer will also need the IP addresses for the primary and the secondary public DNS servers, these addresses can be obtained from the local ISP in Mexico.

Clearcom 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.).
- Clearcom's Domain Name.
- DID numbers.

## 7. Verification Steps

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

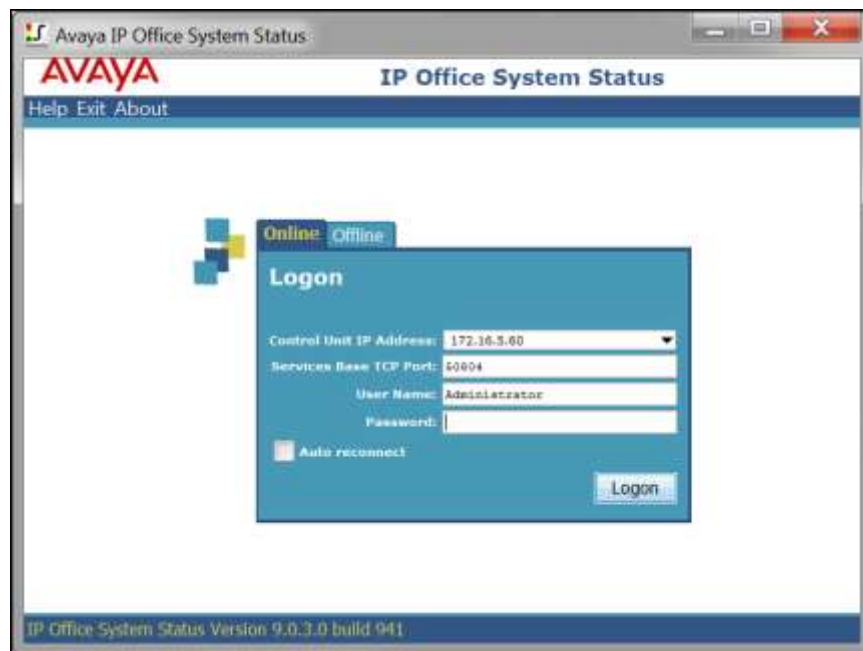
The following steps may be used to verify the configuration:

- 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.

### 7.1. IP Office System Status

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

Use the Avaya 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.

IP Office System Status

[Help](#)
[Snapshot](#)
[LogOff](#)
[Exit](#)
[About](#)

System
Alarms (35)
Extensions (26)
Trunks (9)
Line:1
Line:2
Line:17
Line:18
Line:19
Line:20
Line:21
Line:22
Line:23
Active Calls
Resources
Voicemail
IP Networking
Locations

Status

Utilization Summary

Alarms

SIP Trunk Summary

Line Service State: In Service  
Peer Domain Name: clearcom.mx  
Resolved Address: , 179.79  
Line Number: 17  
Number of Administered Channels: 20  
Number of Channels in Use: 0  
Administered Compression: G729 A, G711 A, G711 Mu  
Enable Faststart: Off  
Silence Suppression: Off  
Media Stream: Best Effort  
Layer 4 Protocol: TLS  
SIP Trunk Channel Licenses: 30  
SIP Trunk Channel Licenses in Use: 0  
SIP Device Features:

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	3 days 02:...					
2			Idle	5 days 01:...					
3			Idle	6 days 02:...					
4			Idle	6 days 02:...					
5			Idle	10 days 01:...					
6			Idle	10 days 04:...					
7			Idle	10 days 04:...					
8			Idle	10 days 04:...					
9			Idle	10 days 04:...					
10			Idle	10 days 04:...					
11			Idle	10 days 04:...					
12			Idle	10 days 04:...					
13			Idle	10 days 04:...					
14			Idle	10 days 04:...					
15			Idle	10 days 04:...					
16			Idle	10 days 04:...					
17			Idle	10 days 04:...					
18			Idle	10 days 04:...					
19			Idle	10 days 04:...					
20			Idle	10 days 04:...					

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

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

**AVAYA** IP Office System Status

Help Snapshot LogOff Exit About

System  
Alarms (35)  
Extensions (26)  
Trunks (9)  
Line:1  
Line:2  
Line:17  
Line:18  
Line:19  
Line:20  
Line:21  
Line:22  
Line:23  
Active Calls  
Resources  
Voicemail  
IP Networking  
Locations

Status Utilization Summary **Alarms**

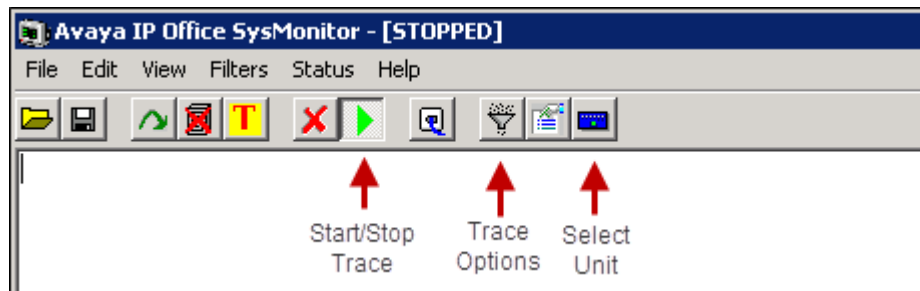
Alarms for Line: 17 SIP clearcom.mx

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

Ping Clear Clear All Graceful Shutdown Force Out of Service Print... Save As...

## 7.2. 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 Avaya 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.



## 8. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office Release 9.1 to Clearcom SIP Trunk Services using TLS. Clearcom SIP Trunk Services 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. Clearcom SIP Trunk Services passed compliance testing with the observations/limitations listed under **Section 2.2**.

## 9. 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] *IP Office Release 9.1 Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 30ze, 16 May, 2016.
- [2] *Administering Avaya IP Office Platform with Manager Release 9.1.2*, Issue 10.38, February 2016.
- [3] *IP Office Release 9.1 Using Avaya IP Office Platform System Status*, Document Number 15-601758, Issue 10f, August 11, 2015.
- [4] *IP Office Release 9.1 Administering Voicemail Pro*, Document Number 15-601063, Issue 10o, May 16, 2016.
- [5] *IP Office Release 9.1 Using IP Office System Monitor*, Document Number 15-601019, Issue 06h, May 17, 2016.

Additional Avaya IP Office documentation can be found at:

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

---

**©2016 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).