



Application Notes for Configuring Avaya IP Office Release 10.1 to support Clearcom SIP Trunking Service - 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 10.1 to support Clearcom SIP Trunking Service.

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.

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 Clearcom and an Avaya SIP-enabled enterprise solution.

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office 500 V2 Release 10.1 (hereafter referred to as IP Office) and various Avaya endpoints, listed in **Section 4**.

The Clearcom 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” 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 network.
- 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.
- 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.
- Fax.
- 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).
- 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 and 911 Emergency were not tested.

2.2. Test Results

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

- **Call transfer to the PSTN using REFER:** PSTN calls that were transferred back to the PSTN network using REFER message 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.
- **Outbound call from an enterprise extension to a busy PSTN number:** Clearcom 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.
- **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 Trunking Service through the public Internet.

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

- Avaya IP Office 500 V2.
- Avaya IP Office Application Server running Avaya Voicemail Pro.
- 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 500 V2 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 a PC running Avaya Communicator for Windows. The site also has a Windows PC running Avaya IP Office Manager to configure and administer the IP Office system, and an Avaya IP Office Application Server running Avaya Voicemail Pro, providing voice messaging service to the IP Office users. 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.

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. 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.

For the testing associated with this Application Note, the interface between the Avaya system and the Clearcom network did not include the use of any specific encryption features.

The transport protocol between IP Office and Clearcom, across the public Internet, is SIP over UDP. The transport protocol between Avaya endpoints and IP Office, inside the enterprise private IP network (LAN), is SIP over TLS.

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 IP Office but the remaining N digits were sent unaltered to the network. Refer to **Section 5.5** for configuration.

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.

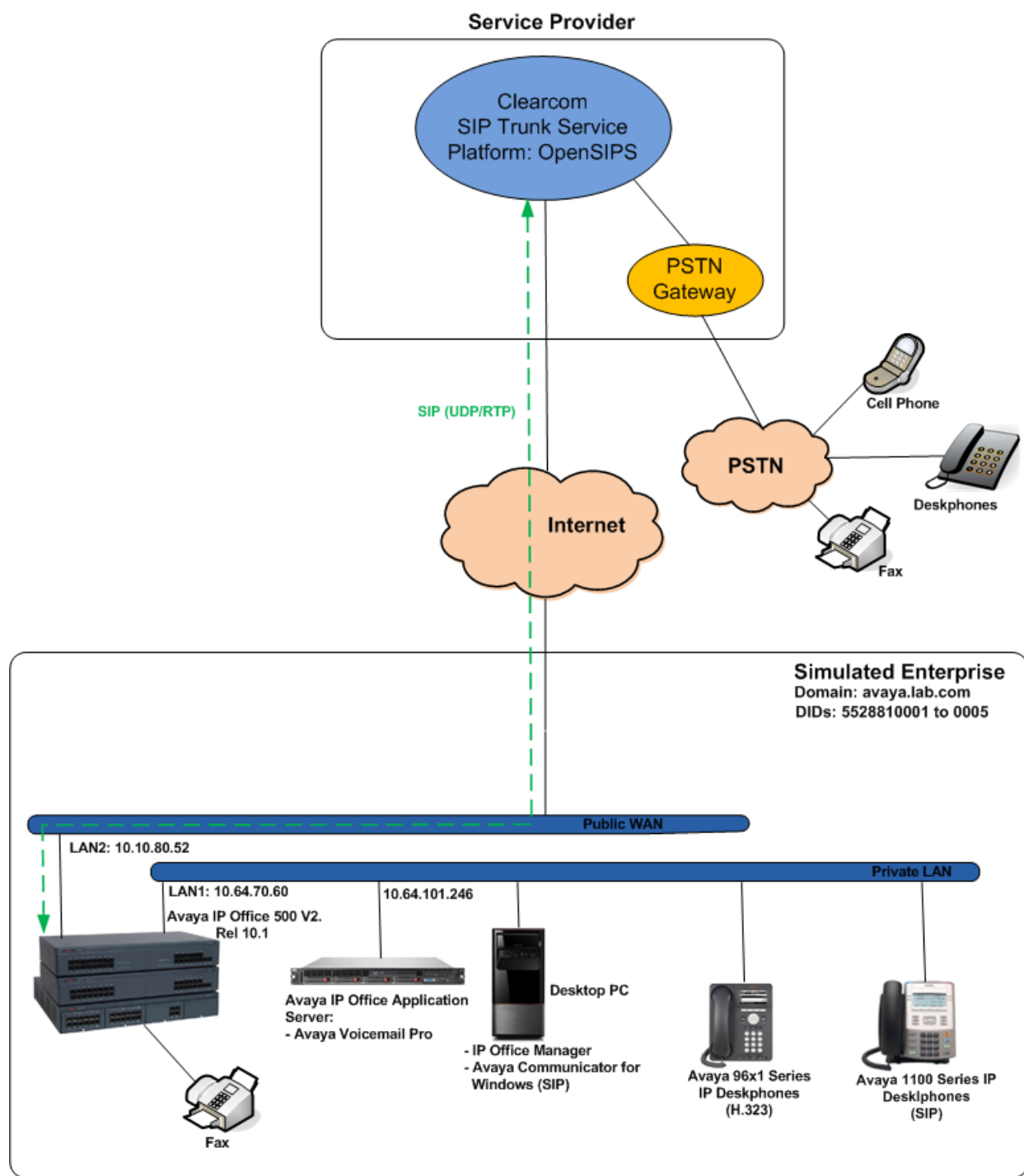


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	10.1.0.1.0 Build 3
Avaya IP Office DIG DCPx16 V2	10.1.0.1.0 Build 3
Avaya IP Office Manager	10.1.0.1.0 Build 3
Avaya IP Office Application Server	10.1.0.1.0 Build 3
▪ Voicemail Pro	10.1.0.1.0 build 6
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.2.1.0-05-14222
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6506
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya Communicator for Windows	2.1.4.274
Clearcom	
OpenSIPS Softswitch	1.9
OpenSIPS Session Border Controller	1.9

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.

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.

The screenshot displays the Avaya IP Office Manager interface. On the left is the 'IP Offices' navigation pane, where 'IP500V2 Main' is selected. The main area is divided into two tabs: 'License' (active) and 'Remote Server'. The 'License' tab shows license details for 'License Mode: License Normal', 'Licensed Version: 10.0', 'PLDS Host ID', and 'PLDS File Status: Valid'. Below this is a table of features.

Feature	Key	Instances	Status	Expiration Date	Source
Software Upgrade 8 (R9.1)	s@KWbMyld...	1	Obsolete	Never	ADI Nodal
Essential Edition	fludo0hStKO...	255	Obsolete	Never	ADI Nodal
Receptionist	N/A	4	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	N/A	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	N/A	1	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	N/A	4	Valid	Never	PLDS Nodal
VMPro TTS (Generic)	N/A	40	Valid	Never	PLDS Nodal
Teleworker	N/A	384	Valid	Never	PLDS Nodal
Mobile Worker	N/A	384	Valid	Never	PLDS Nodal
Office Worker	N/A	384	Valid	Never	PLDS Nodal
Avaya Softphone Licence	N/A	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	N/A	40	Valid	Never	PLDS Nodal
VMPro TTS Professional	N/A	40	Valid	Never	PLDS Nodal
IPSec Tunneling	N/A	1	Valid	Never	PLDS Nodal
Power User	N/A	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	N/A	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	N/A	32	Valid	Never	PLDS Nodal
SIP Trunk Channels	N/A	128	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	N/A	100	Valid	Never	PLDS Nodal
CTI Link Pro	N/A	1	Valid	Never	PLDS Nodal

To view the physical hardware comprising IP Office, expand the components under the **Control Unit** in the **Navigation** pane. In the sample configuration, the Avaya IP Office 500 V2 is equipped with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codecs. An 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 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 (6)
- Operator (3)
- IP500V2 Main (highlighted with a red box)
- System (1)
- Line (25)
- Control Unit (4)
 - 1 IP 500 V2 (highlighted with a red box)
 - 2 VCM64/PRID U
 - 3 PHONE8
 - 6 DIG DCPx16 V2
- Extension (48)
- User (50)
- Group (1)
- Short Code (69)
- Service (0)

IP 500 V2 Details Pane:

Unit	
Device Number	1
Unit Type	IP 500 V2
Version	10.1.0.1.0 build 3
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 IP Office 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 IP Office WAN port was used to connect to Clearcom. The LAN2 settings correspond to the WAN port on the IP Office 500 V2. To access the LAN2 settings, first navigate to **System** → <Name>, where <Name> is the system name assigned to 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 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 IP Office configuration interface. On the left, the 'IP Offices' tree shows a hierarchy where 'IP500V2 Main' is selected under 'System (1)'. The main panel is titled 'IP500V2 Main' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', 'System Events', and 'SMTP'. The 'LAN2' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The 'LAN Settings' sub-tab contains the following fields and values:

Field	Value
IP Address	10 . 10 . 80 . 52
IP Mask	255 . 255 . 255 . 0
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"/> Dial In <input checked="" type="radio"/> Disabled

An 'Advanced' button is located at the bottom right of the 'LAN Settings' sub-tab.

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.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Minimum** and **Maximum** values were kept as default.

The screenshot displays the configuration interface for IP500V2 Main. The left sidebar shows a tree view of configuration categories, with 'IP500V2 Main' and its sub-items highlighted. The main panel shows the 'VoIP' tab selected, with 'SIP Trunks Enable' checked. Below this, the 'RTP' section is highlighted, showing 'Port Number Range' and 'Port Number Range (NAT)' settings, both with Minimum and Maximum values set to 49152 and 53246 respectively.

IP500V2 Main												
System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	VCN	VoIP	VoIP Security
<div> <div>LAN Settings</div> <div>VoIP</div> <div>Network Topology</div> </div>												
<div> <input type="checkbox"/> H.323 Gatekeeper Enable <input type="checkbox"/> Auto-create Extension <input type="checkbox"/> Auto-create User <input type="checkbox"/> H.323 Remote Extension Enable </div> <div> H.323 Signaling over TLS: Disabled Remote Call Signaling Port: 1720 </div> <div> <input checked="" type="checkbox"/> SIP Trunks Enable </div> <div> <input type="checkbox"/> SIP Registrar Enable <input type="checkbox"/> Auto-create Extension/User <input type="checkbox"/> SIP Remote Extension Enable </div> <div> SIP Domain Name: sil.miami.avaya.com SIP Registrar FQDN: sil.miami.avaya.com </div> <div> <div> <input checked="" type="checkbox"/> UDP UDP Port: 5060 Remote UDP Port: 5060 </div> <div> <input checked="" type="checkbox"/> TCP TCP Port: 5060 Remote TCP Port: 5060 </div> <div> <input checked="" type="checkbox"/> TLS TLS Port: 5061 Remote TLS Port: 5061 </div> </div> <div> Layer 4 Protocol: </div> <div> Challenge Expiration Time (sec): 10 </div> <div> <div> RTP </div> <div> Port Number Range Minimum: 49152 Maximum: 53246 </div> <div> Port Number Range (NAT) Minimum: 49152 Maximum: 53246 </div> </div>												

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 IP Office to send a RTP and RTCP keepalive packet starting at the time of initial connection and every 30 seconds thereafter if no other RTP/RTCP 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, 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 shows the IP500V2 Main configuration window. The left sidebar lists various configuration categories, with 'IP500V2 Main' selected. The main window has tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VCM, and VoIP. The 'VoIP' tab is active, showing the 'LAN Settings' section. The 'RTP' section includes 'Port Number Range' (Minimum: 49152, Maximum: 53246) and 'Port Number Range (NAT)' (Minimum: 49152, Maximum: 53246). The 'Enable RTCP Monitoring on Port 5005' checkbox is checked. The 'RTCP collector IP address for phones' is set to 0.0.0.0. The 'Keepalives' section shows 'Scope' set to 'RTP-RTCP' and 'Periodic timeout' set to 30. The 'Initial keepalives' dropdown is set to 'Enabled'. The 'DiffServ Settings' section shows the following values: DSCP (Hex) 88, Video DSCP (Hex) 88, FC 63, DSCP Mask (Hex) 88, SIG DSCP (Hex) 46, DSCP 46, Video DSCP 63, DSCP Mask 34, and SIG DSCP 34.

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 Trunking 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:

- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used for the compliance test, **A-Law** could have been selected instead.
- 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).

The screenshot displays the 'IP500V2 Main' configuration window. On the left, the 'IP Offices' tree shows a hierarchy where 'IP500V2 Main' is selected, and its sub-item 'System (1)' is highlighted with a red box. The main panel on the right is titled 'IP500V2 Main' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony' (which is selected and highlighted with a red box), 'Directory Services', 'System Events', 'SMTP', 'SMDR', 'VCM', 'VoIP', and 'VoIP Security'. Below the 'Telephony' tab, there are sub-tabs: 'Telephony', 'Park & Page', 'Tones & Music', 'Ring Tones', 'SM', 'Call Log', and 'TUI'. The 'Telephony' sub-tab is active. It contains two main sections. The 'Analogue Extensions' section on the left includes dropdown menus for 'Default Outside Call Sequence' (set to 'Normal'), 'Default Inside Call Sequence' (set to 'Ring Type 1'), and 'Default Ring Back Sequence' (set to 'Ring Type 2'). Below these are input fields for '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), and 'Default Currency' (USD). The 'Companding Law' section on the right has two columns: 'Switch' and 'Line'. Both columns have radio buttons for 'U-Law' (selected) and 'A-Law'. The 'Line' column also has radio buttons for 'U-Law Line' (selected) and 'A-Law Line'. Below this, there are several checkboxes: 'DSS Status' (unchecked), 'Auto Hold' (checked), 'Dial By Name' (checked), 'Show Account Code' (checked), 'Inhibit Off-Switch Forward/Transfer' (unchecked and highlighted with a red box), 'Restrict Network Interconnect' (unchecked), 'Include location specific information' (unchecked), 'Drop External Only Impromptu Conference' (unchecked), and 'Visually Differentiate External Call' (unchecked).

5.2.3. System - VoIP Tab

To view or change the System Codecs settings, navigate to the **VoIP** 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).

The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' tree shows 'IP500V2 Main' selected. The main panel is titled 'IP500V2 Main' and has several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VCM, and VoIP (which is highlighted with a red box). Under the VoIP tab, there are two checkboxes: 'Ignore DTMF Mismatch For Phones' and 'Allow Direct Media Within NAT Location', both of which are unchecked. Below these is the 'RFC2833 Default Payload' field, which contains the value '101' and is highlighted with a red box. The 'Default Codec Selection' section contains two lists: 'Available Codecs' and 'Unused'. The 'Available Codecs' list includes G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, G.729(a) 8K CS-ACELP, and G.723.1 6K3 MP-MLQ. The 'Unused' list contains G.722 64K. Between these lists are buttons for moving codecs (>>>, <<<, <-, >=) and buttons for changing the order (up and down arrows). The 'Selected' list on the right contains G.711 ULAW 64K, G.711 ALAW 64K, G.729(a) 8K CS-ACELP, and G.723.1 6K3 MP-MLQ, and is highlighted with a red box.

Note: The codec selections defined under this section (System – VoIP Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.3.6** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.2.4. System - DNS Tab

Public DNS servers IP addresses are required to be configured, IP Office will retrieve Clearcom's Proxy IP Address via public DNS queries using Clearcom's ISTP Domain Name configured under in **Section 5.3.2**. 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 Clearcom.
- Click **OK** to commit (not shown).

The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' tree shows a hierarchy: BOOTP (6), Operator (3), IP500V2 Main (selected), System (1), and IP500V2 Main. The main panel on the right is titled 'IP500V2 Main' and contains several tabs: System, LAN1, LAN2, DNS (selected), Voicemail, Telephony, Directory Services, and System Events. The 'DNS' tab is active, showing the following configuration fields:

Field	Value
DNS Server IP Address	8 . 8 . 8 . 8
Backup DNS Server IP Address	75 . 75 . 75 . 75
DNS Domain	
WINS Server IP Address	0 . 0 . 0 . 0
Backup WINS Server IP Address	0 . 0 . 0 . 0
WINS Scope	

5.2.5. 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 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).

The screenshot displays the IP Office configuration interface. On the left, a tree view under 'IP Offices' shows various components, with 'IP Route (7)' highlighted. The main pane shows the 'IP Route' configuration for the selected item. The configuration fields are as follows:

0.0.0.0*	
IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	10 . 10 . 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 Avaya IP Office and Clearcom. 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 5.3.1** 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 5.3.2** to **5.3.7**.

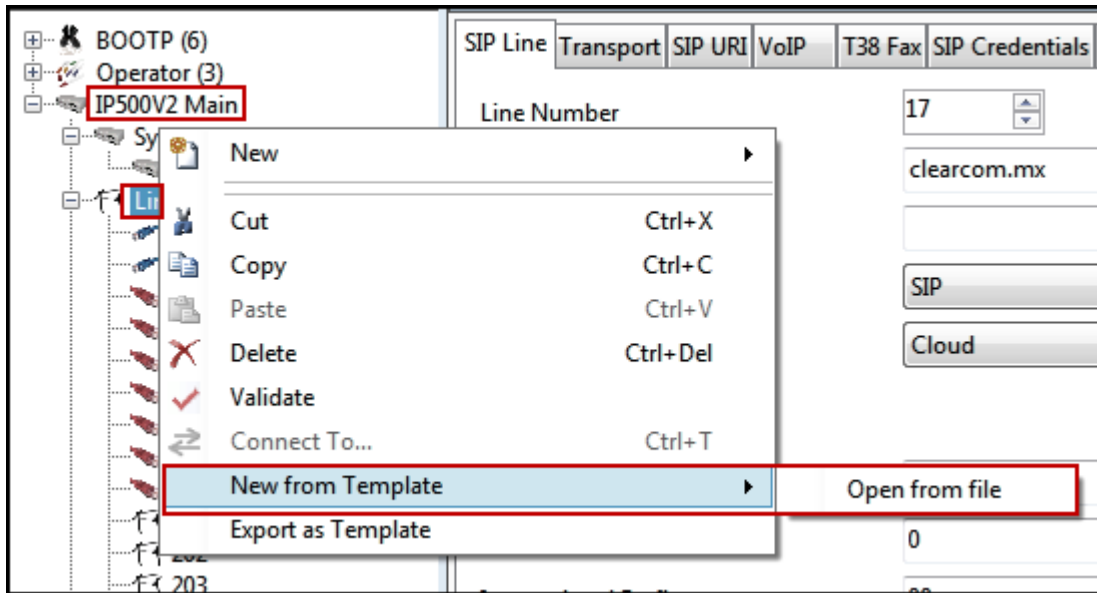
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.3.2** to **5.3.7**.

5.3.1. Creating a SIP Trunk from an XML Template

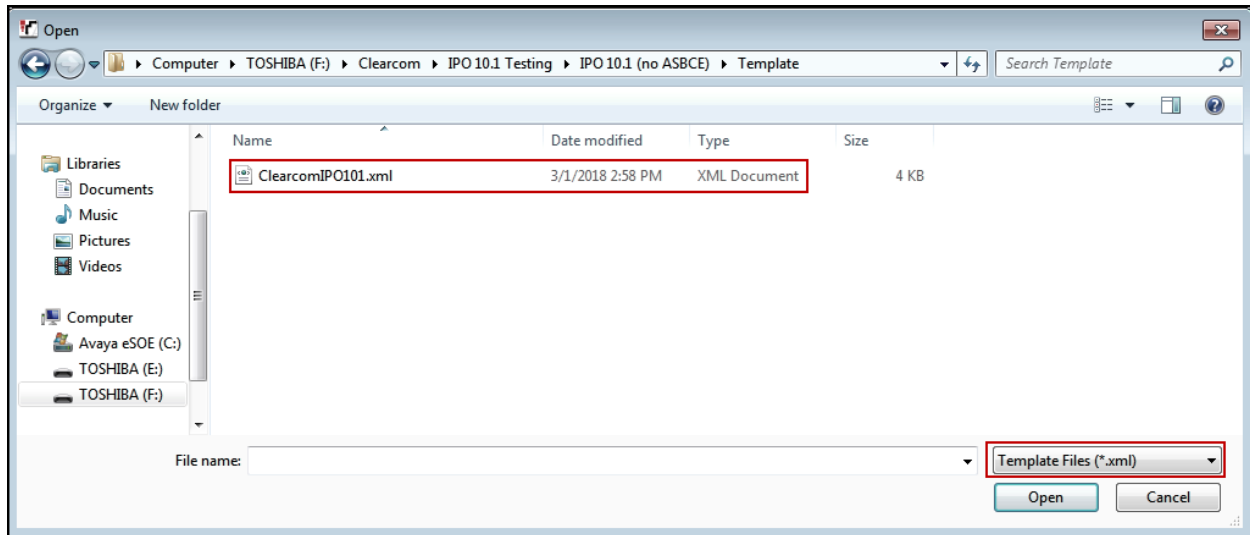
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and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

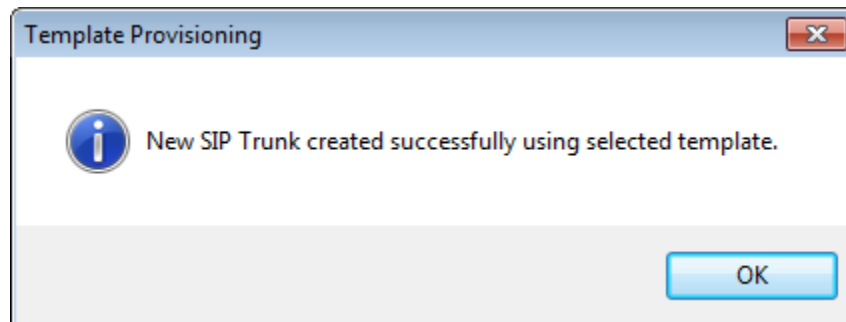
To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template→Open from file**.



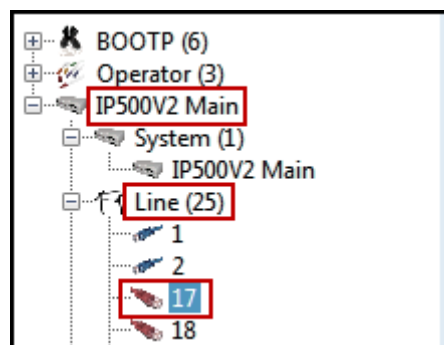
Navigate to the directory on the local machine where the template was copied and select the template.



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 5.3.2 to 5.3.7**.

5.3.2. 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 **clearcom.mx**, the domain name provided by 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. 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 disabled. Thus, **Incoming Supervised REFER** and **Outgoing Supervised REFER** should be set to **Never**. Refer to **Sections 2.1 and 2.2** for the reason this field was disabled.
- Click **OK** to commit (not shown).

SIP Line - Line 17							
SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials	SIP Advanced	Engineering
Line Number	17						
ITSP Domain Name	clearcom.mx						
Local Domain Name							
URI Type	SIP						
Location	Cloud						
Prefix							
National Prefix	0						
International Prefix	00						
Country Code							
Name Priority	System Default						
Description	Service Provider						
In Service	<input checked="" type="checkbox"/>						
Check OOS	<input checked="" type="checkbox"/>						
Session Timers							
Refresh Method	Auto						
Timer (sec)	On Demand						
Redirect and Transfer							
Incoming Supervised REFER	Never						
Outgoing Supervised REFER	Never						
Send 302 Moved Temporarily	<input type="checkbox"/>						
Outgoing Blind REFER	<input type="checkbox"/>						

5.3.3. 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 5.3.2**). The public DNS IP addresses were configured under **Section 5.2.4**.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **None** (refer to the note below).
- Set the **Send Port** and **Listening 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, the 'IP Offices' tree shows a hierarchy: BOOTP (6), Operator (3), IP500V2 Main, System (1), IP500V2 Main, and Line (25). Line 17 is selected. The main panel is titled 'SIP Line - Line 17' and contains several tabs: SIP Line, Transport (selected), SIP URI, VoIP, T38 Fax, SIP Credentials, SIP Advanced, and Engineering. The 'Transport' tab is active, showing the 'ITSP Proxy Address' field, which is empty. Below this is the 'Network Configuration' section, which includes a 'Layer 4 Protocol' dropdown set to 'UDP', a 'Send Port' field set to '5060', a 'Use Network Topology Info' dropdown set to 'None', and a 'Listen Port' field set to '5060'. There are also fields for 'Explicit DNS Server(s)' (both set to 0.0.0.0) and a 'Calls Route via Registrar' checkbox (checked). At the bottom, there is a 'Separate Registrar' 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. In addition, it was not necessary to configure the **System → LAN2 → Network Topology** tab for the purposes of SIP trunking. 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.

5.3.4. 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**, 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. For the compliance test the same value used under **User Name** was used.
- Leave the **Contact** blank.
- 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 (not shown).

The screenshot displays the 'SIP Line - Line 17*' configuration window. On the left, the 'IP Offices' tree shows a hierarchy with 'Line (25)' selected, and 'Line 17' highlighted. The main panel shows the 'SIP Credentials' tab. A table lists the SIP line configuration:

Index	User Name	Authentication Name	Contact	Expiration (mins)	Register
1	user123	user123		2	True

Below the table, the 'Edit SIP Credentials' form is shown with the following fields:

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

5.3.5. 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 Credential User Name**, the user name associated with the SIP trunk credentials provided by Clearcom. Clearcom required the user name to be sent in the “From” header.
- Set **Contact** and **Display Name** to **Use Internal Data**
- Set **Identity** under **Identity** to **None**.
- Set **Header** under **Identity** to **P Asserted ID**.
- Set **Originator Number** under **Forwarding and Twinning** to the user name associated with the SIP trunk registration credentials provided by Clearcom.
- Set **Send Caller ID** under **Forwarding and Twinning** to **Diversion Header**.
- Set **Diversion Header** to **Auto**.
- Under **Registration**, select **1: user123** from the pull-down menu (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 Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit (not shown).
- Click **OK** to commit again (not shown).

IP Offices

- BOOTP (6)
- Operator (3)
- IP500V2 Main
 - System (1)
 - IP500V2 Main
 - Line (25)
 - 1
 - 2
 - 17
 - 18
 - 19
 - 20
 - 21
 - 22
 - 23
 - 201
 - 202
 - 203
 - 204
 - 205
 - 206
 - 207
 - 208
 - 209
 - 210
 - 211
 - 212
 - 213
 - 214
 - 215
 - 216
- Control Unit (4)
- Extension (48)
- User (50)
- Group (1)
- Short Code (69)
- Service (0)
- RAS (1)
- Incoming Call Route (3)
- WAN Port (0)
- Directory (0)
- Time Profile (0)
- Firewall Profile (1)

SIP Line - Line 17

SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials	SIP Advanced	Engineering
1	0	17	user123	<Internal>	<Internal>	None	PAI
2	17	0	<Internal>	<Internal>	<Internal>	None	PAI

Edit URI

Local URI: Use Credentials User Name

Contact: Use Internal Data

Display Name: Use Internal Data

Identity: None

Header: P Asserted ID

Forwarding And Twinning

Originator Number: user123

Send Caller ID: Diversion Header

Diversion Header: Auto

Registration: 1: user123

Incoming Group: 0

Outgoing Group: 17

Max Sessions: 10

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**. This setting allows calls on this line that have a SIP URI that matches the number set in the **SIP** tab of any user as shown later in **Section 5.4**.
- Set **Identity** under **Identity** to **None**.
- Set **Header** under **Identity** to **P Asserted ID**.
- Set **Send Caller ID** under **Forwarding and Twinning** to **None**.
- Set **Diversion Header** to **None**.
- Under **Registration**, select **0: <None>** from the pull-down menu.
- Set **Incoming Group** to **17** (SIP Line number being used).
- Set **Outgoing Group** to **0**.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit (not shown).
- Click **OK** to commit again (not shown).

SIP Line - Line 17

SIP Line	Transport	SIP URI	VolP	T38 Fax	SIP Credentials	SIP Advanced	Engineering
1	0	17	user123	<Internal>	<Internal>	None	PAI
2	17	0	<Internal>	<Internal>	<Internal>	None	PAI

Edit URI

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

Identity: None

Header: P Asserted ID

Forwarding And Twinning

Originator Number:

Send Caller ID: None

Diversion Header: None

Registration: 0: <None>

Incoming Group: 17

Outgoing Group: 0

Max Sessions: 10

5.3.6. 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. Clearcom supports codec **G.729(a)**, **G.711ALAW** and **G.711ULAW** for audio, with G.729(a) being the preferred codec.
- Select **None** for **Fax Transport Support** (Refer to **Sections 2.1** and **2.2**).
- Set the **DTMF Support** field to **RFC2833**. 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 displays the Avaya IP Office configuration interface for 'SIP Line - Line 17'. The left sidebar shows a tree view of IP Offices, with 'Line (25)' selected. The main configuration area has tabs for 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'VoIP' tab is active, showing the following settings:

- Codec Selection:** Set to 'Custom'. The 'Unused' list contains 'G.722 64K' and 'G.723.1 6K3 MP-MLQ'. The 'Selected' list contains 'G.729(a) 8K CS-ACELP', 'G.711 ALAW 64K', and 'G.711 ULAW 64K'.
- Fax Transport Support:** Set to 'None'.
- DTMF Support:** Set to 'RFC2833'.
- Media Security:** Set to 'Disabled'.
- Checkboxes:** 'VoIP Silence Suppression' is checked. 'Local Hold Music' is unchecked. 'Re-invite Supported' is checked. 'Codec Lockdown' is unchecked. 'Allow Direct Media Path' is unchecked. 'Force direct media with phones' is unchecked. 'PRACK/100rel Supported' is checked. 'G.711 Fax ECAN' is unchecked.

Note: The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.3** (System – VoIP tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

5.3.7. 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).

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'SIP Advanced' tab selected. The left sidebar shows a tree view of IP Offices, with 'Line (25)' selected. The main configuration area is divided into three sections: Addressing, Identity, and Media. The 'Addressing' section has 'Association Method' set to 'By Source IP address' and 'Call Routing Method' set to 'To Header'. The 'Identity' section has 'Use PAI for Privacy' checked. The 'Media' section has 'Allow Empty INVITE' checked, 'Send Empty re-INVITE' checked, 'Allow To Tag Change' checked, 'P-Early-Media Support' set to 'None', 'Send SilenceSupp=Off' checked, 'Force Early Direct Media' checked, 'Media Connection Preservation' set to 'Disabled', and 'Indicate HOLD' checked. The 'Call Control' section has 'Call Initiation Timeout (s)' set to 4, 'Call Queuing Timeout (mins)' set to 5, 'Service Busy Response' set to '486 - Busy Here', 'on No User Responding Send' set to '408-Request Timeout', 'Action on CAC Location Limit' set to 'Allow Voicemail', 'Suppress Q.850 Reason Header' checked, 'Emulate NOTIFY for REFER' checked, and 'No REFER if using Diversion' checked.

Section	Parameter	Value
Addressing	Association Method	By Source IP address
	Call Routing Method	To Header
Identity	Suppress DNS SRV Lookups	<input type="checkbox"/>
	Use "phone-context"	<input type="checkbox"/>
	Add user=phone	<input type="checkbox"/>
	Use + for International	<input type="checkbox"/>
	Use PAI for Privacy	<input checked="" type="checkbox"/>
	Use Domain for PAI	<input type="checkbox"/>
	Swap From and PAI/Diversion	<input type="checkbox"/>
	Caller ID from From header	<input type="checkbox"/>
	Send From In Clear	<input type="checkbox"/>
	Cache Auth Credentials	<input checked="" type="checkbox"/>
Media	Allow Empty INVITE	<input checked="" type="checkbox"/>
	Send Empty re-INVITE	<input checked="" type="checkbox"/>
	Allow To Tag Change	<input checked="" type="checkbox"/>
	P-Early-Media Support	None
	Send SilenceSupp=Off	<input checked="" type="checkbox"/>
Call Control	Force Early Direct Media	<input checked="" type="checkbox"/>
	Media Connection Preservation	Disabled
	Indicate HOLD	<input checked="" type="checkbox"/>
	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	<input checked="" type="checkbox"/>
	Emulate NOTIFY for REFER	<input checked="" type="checkbox"/>
No REFER if using Diversion	<input checked="" type="checkbox"/>	

5.4. 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 1502**. 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).

H323 ext 1502: 1502*							
Dial In	Voice Recording	Button Programming	Menu Programming	Mobility	Group Membership	Announcements	SIP
SIP Name		5528810001					
SIP Display Name (Alias)		H323 ext 1502					
Contact		5528810001					
<input type="checkbox"/> Anonymous							

5.5. 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.

5.5.1. 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 **Locale**, **United States (US English)** was used.
- Click the **OK** to commit (not shown).

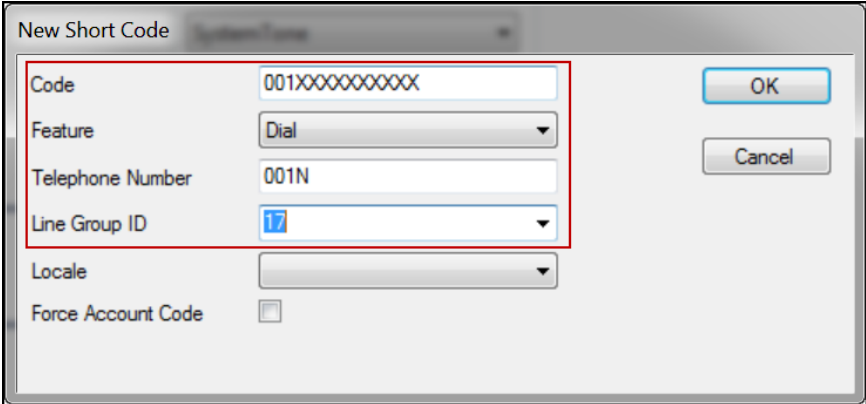
The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' pane lists various short codes, with '9N' highlighted. On the right, the '9N: Dial' configuration window is open, showing the following settings:

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 X's**. The **9** is stripped off, the remaining digits, including the **001** shown in the examples below, are included in the SIP INVITE message IP Office sends to Clearcom.

IP Offices

- BOOTP (6)
- Operator (3)
- IP500V2 Main**
- System (1)
- Line (25)
- Control Unit (4)
- Extension (48)
- User (50)
- Group (1)
- Short Code (69)
- Service (0)
- RAS (1)
- Incoming Call Route (3)
- WAN Port (0)
- Directory (0)
- Time Profile (0)
- Firewall Profile (1)
- IP Route (7)
- Account Code (0)
- License (90)
- Tunnel (0)
- User Rights (8)
- ARS (2)**
 - 50: Main**
 - 31: Outbound Fax
- Location (0)
- Authorization Code (0)

Main

ARS

ARS Route ID: 50

Route Name: Main

Dial Delay Time: System Default (4)

Description:

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

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

Code	Telephone Number	Feature	Line Group ID
001XXXXXXXXX	001N	Dial	17
01800XXXXXX	01800N	Dial	17
01XXXXXXX	01N	Dial	23
03XXXXXXX	03N	Dial	17
04XXXXXXX	04N	Dial	17
0800XXXXXX	0800N	Dial	17
11	911	Dial Emergency	17

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

Alternate Route: <None>

5.6. 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 5.3.5)** and the users **SIP Name** and **Contact**, already populated with the assigned Clearcom DID numbers (**Section 5.4**).

5.6.1. 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 **17** was used.
- Default values can be used for all other fields.

The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' tree shows a hierarchy with 'Incoming Call Route (3)' selected, and '17' highlighted. The main pane shows the 'Standard' tab of the 'Details' pane for '17'. The configuration fields are as follows:

Field	Value
Bearer Capability	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

5.6.2. 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).

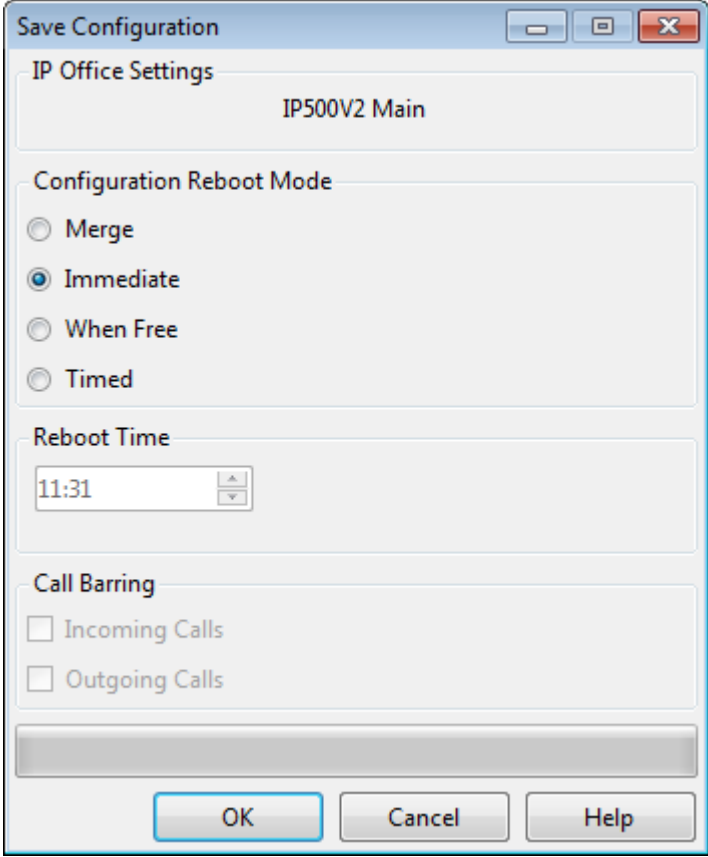
The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows the hierarchy: BOOTP (5), Operator (3), IP500V2 Main, System (1), Line (26), Control Unit (4), Extension (48), User (50), Group (1), Short Code (69), Service (0), RAS (1), Incoming Call Route (3), and 17. The 'Incoming Call Route (3)' and '17' are highlighted with a red box. The main panel on the right shows the configuration for '17' with tabs for Standard, Voice Recording, and Destinations. The 'Destinations' tab is active, showing a table with columns: TimeProfile, Destination, and Fallback Extension. The first row has 'Default Value' in the TimeProfile column and a period '.' in the Destination column.

TimeProfile	Destination	Fallback Extension
Default Value	.	

5.7. 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.



The image shows a 'Save Configuration' dialog box with a title bar containing minimize, maximize, and close buttons. The dialog is divided into several sections. The first section, 'IP Office Settings', displays 'IP500V2 Main'. The second section, 'Configuration Reboot Mode', contains four radio buttons: 'Merge', 'Immediate' (which is selected), 'When Free', and 'Timed'. The third section, 'Reboot Time', features a time selection control showing '11:31'. The fourth section, 'Call Barring', has two unchecked checkboxes for 'Incoming Calls' and 'Outgoing Calls'. At the bottom of the dialog is a horizontal separator line, and below it are three buttons: 'OK', 'Cancel', and 'Help'.

6. Clearcom SIP Trunking Service Configuration

To use Clearcom's SIP Trunking 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 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).

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

- SIP Trunk registration credentials (User Name, Password, etc.).
- Clearcom's Domain Name.
- DID numbers, etc.

7. Verification Steps

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

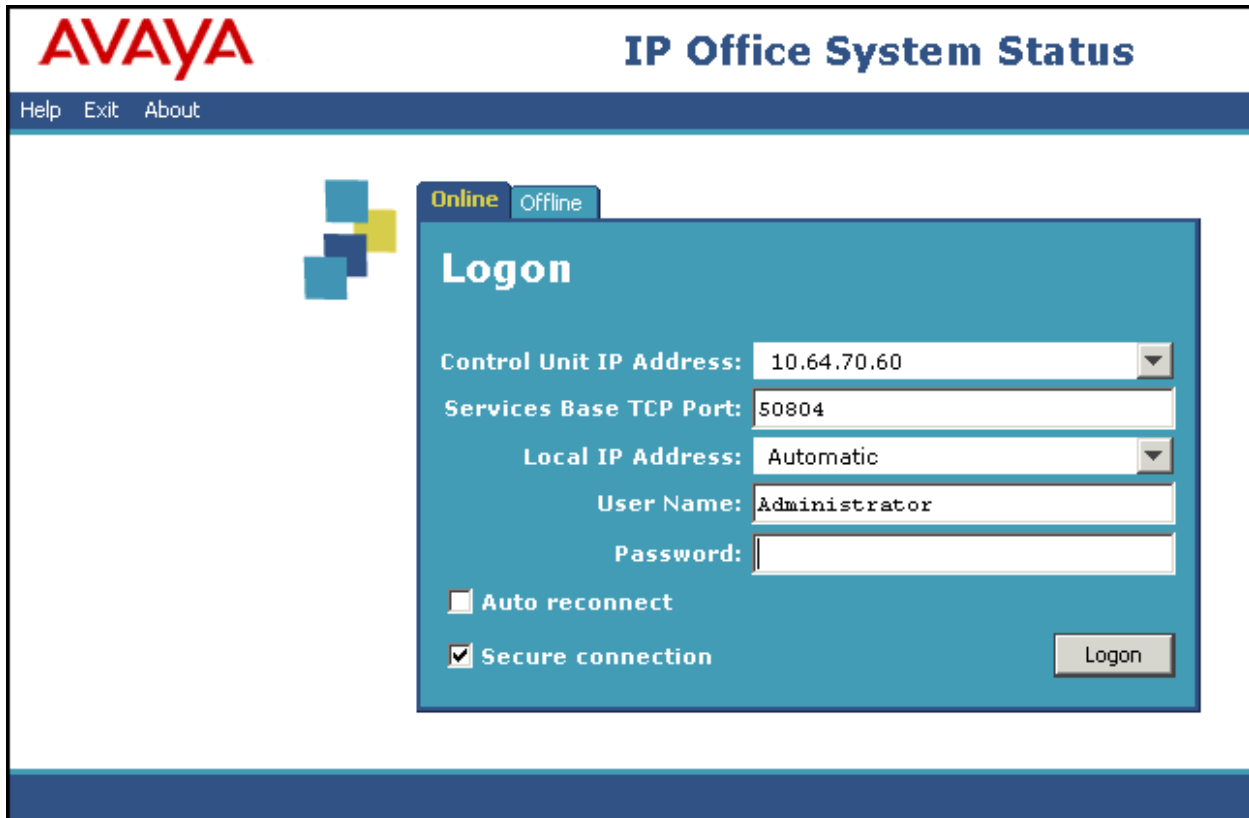
The following steps may be used to verify the configuration:

- 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 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.



The screenshot shows the AVAYA IP Office System Status application. The window title is "IP Office System Status". The menu bar includes "Help", "Exit", and "About". The main area displays a "Login" dialog box with the following fields and options:

- Control Unit IP Address:** 10.64.70.60
- Services Base TCP Port:** 50804
- Local IP Address:** Automatic
- User Name:** Administrator
- Password:** (empty field)
- ☐ Auto reconnect
- ☒ Secure connection
- Logon** button

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

Help Snapshot LogOff Exit About

System
Alarms (22)
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 Registration

SIP Trunk Summary

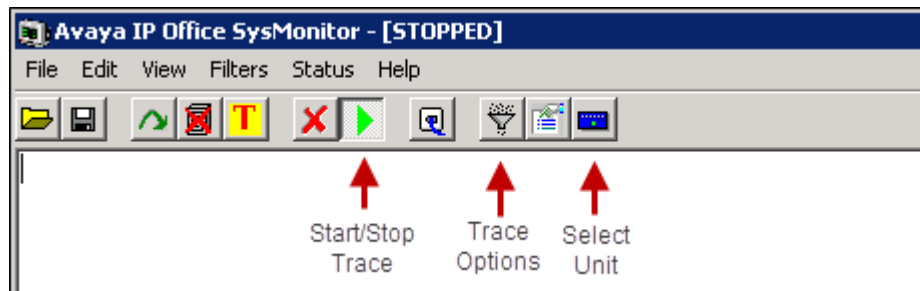
Line Service State: In Service
 Peer Domain Name: clearcom.mx
 Resolved Address: .179.79
 Line Number: 17
 Number of Administered Channels: 20
 Number of Channels in Use: 0
 Administered Compression: G729 A, G711 A, G711 Mu
 Enable Faststart: Off
 Silence Suppression: On
 Media Stream: RTP
 Layer 4 Protocol: UDP
 SIP Trunk Channel Licenses: 128
 SIP Trunk Channel Licenses in Use: 0 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	Direction of Call	Round Trip Delay	F
1			Idle	19:34:23								
2			Idle	19:38:08								

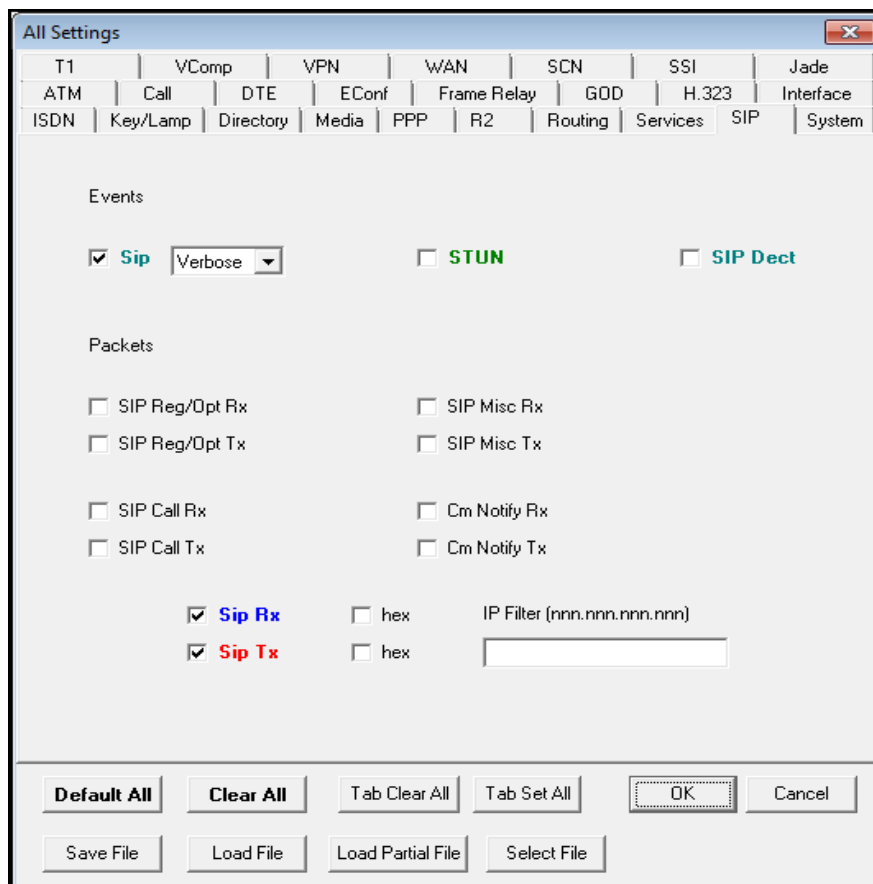
Trace Trace All Pause Ping Call Details Graceful Shutdown Force Out of Service Print... Save As...

7.2. Monitor

The Avaya IP Office SysMonitor 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.



8. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office Release 10.1 to Clearcom SIP Trunking Services. Clearcom SIP Trunking 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.

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**.

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] *Avaya IP Office Platform Solution Description, Release 10.1, Issue 1.2, September 2017.*
- [2] *Avaya IP Office Platform Feature Description, Release 10.1, Issue 1a, September 2017.*
- [3] *Deploying Avaya IP Office Platform IP500 V2, Document Number 15-601042, Issue 32m, January 22, 2017.*
- [4] *Administering Avaya IP Office Platform with Manager, Release 10.1, Issue 14, July 2017*
- [5] *Using Avaya Communicator for Windows on IP Office, Release 10, August 2016.*
- [6] *Administering Avaya Communicator on IP Office, Release 10.0, Issue 01.01, August 2016.*
- [7] *Avaya IP Office Platform Security Guidelines, Release 10. Issue 01e, May 8, 2017.*
- [8] *IP Office Technical Bulletin number 175*
(<http://www.ipofficeinfo.com/TechBulletins/tb175.pdf>)

Additional Avaya IP Office documentation can be found at:

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

©2018 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.