



## **Application Notes for Configuring Avaya IP Office Release 11.1 to support Avaya SIP Trunking Service using UDP Transport - Issue 1.0**

### **Abstract**

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 11.1 to support Avaya SIP Trunking Service using UDP transport on the public side.

The Avaya SIP Trunking service offer referenced within these Application Notes provides customers with PSTN access via a SIP trunk between the enterprise and the service provider network. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly as an alternative to legacy analog or digital trunks. The Avaya SIP Trunking service provides you with a cost effective and flexible way to connect your business to the outside world. It helps your business use the internet bandwidth you already pay for in a more flexible way.

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.

# 1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the Avaya SIP Trunking service offering and a simulated Avaya enterprise solution. User Datagram Protocol (UDP) transport was used to connect the simulated enterprise solution to the Avaya SIP Trunking service offering (public side network side).

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

The Avaya 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 “Avaya network” or “service provider” will be used interchangeably throughout these Application Notes to represent the far-end/service provider side of the Avaya SIP Trunking service offering handling calls to/from the PSTN across the SIP trunk. The terms “enterprise” or “Avaya enterprise” will be used interchangeably throughout these Application Notes to represent the Customer-Premises-Equipment site containing all the equipment for the Avaya enterprise solution.

## 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Avaya SIP Trunking network via the public Internet, as depicted in **Figure 1**, and exercise the features and functionalities listed in **Section 2.1**.

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

For the testing associated with this Application Note, the interface between the simulated enterprise site (private network) and the Avaya network (public network) did not include the use of any specific encryption features, UDP/RTP was used.

Encryption (TLS/sRTP) was used internal to the enterprise between Avaya products wherever possible.

## 2.1. Interoperability Compliance Testing

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

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

Items that were not tested for not being available at the time of testing includes the following:

- 0, 0+10 digits and 411 calls were not tested.

## 2.2. Test Results

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

- **T.38 Fax** – IP Office negotiates the use of T.38 for fax by sending a re-INVITE message with two media lines in the SDP, with the first media line set for audio, with the port set to 0, and the second media line set for T.38, with a valid port number, thus deactivating audio transmission for the call. The Service Provider responded to this re-INVITE message sent by Avaya IP Office with "488 Not Acceptable Here". With IP Office configured to use T.38, the "488 Not Acceptable Here" response sent by the Service Provider did not have any impact on the fax transmission, both, inbound and outbound fax were successful transmitted via T.38. It's being mentioned here simply as an observation. The setting of T.38 Fall-Back in IP Office caused fax transmissions to fail intermittently, thus only the setting of T.38 is recommended for fax transmission.
- **Outbound Calling Party Number (CPN) Block** – When the IP Office user activated "Withhold Number" to enable user privacy on outbound calls, IP Office sent "anonymous" in the "From" header, included the "Privacy:id" header, while the caller information (DID number) was included in the "P-Asserted-Identity" header of the outbound INVITE message. The Service Provider did not respond to the INVITE message sent by IP Office with "anonymous" in the "From" header, resulting on the call failing. This issue is being investigated by Avaya.
- **SIP Trunk registrations** – After each successful SIP Trunk registration attempt the service provider would send a "484 Address Incomplete" message response to the enterprise. This behaviour did not have any service impact, registrations were successful, it's being mentioned here simply as an observation.
- **SIP OPTIONS Messages** – During the compliance test Avaya did not send SIP OPTIONS messages to IP Office, IP Office did send SIP OPTIONS messages to Avaya, this was sufficient to keep the SIP trunk up in service.
- **SIP endpoints may indicate that a transfer failed even when it is successful** – Occasionally on a transfer operation, Avaya IP Office SIP endpoints (Avaya 1100 Series Deskphones) may indicate on the local call display that the transfer failed even though it was successful. The frequency of this behavior can be reduced by enabling "**Emulate Notify for REFER**" on the IP Office SIP Line (**Section 5.4.7**).

### **2.3. Support**

For information on Avaya SIP Trunking service go to: <https://www.avaya.com/en/documents/fs-sip-uc8179en.pdf>

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 compliance testing. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the Avaya SIP Trunking Service through the public Internet.

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

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

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

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

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

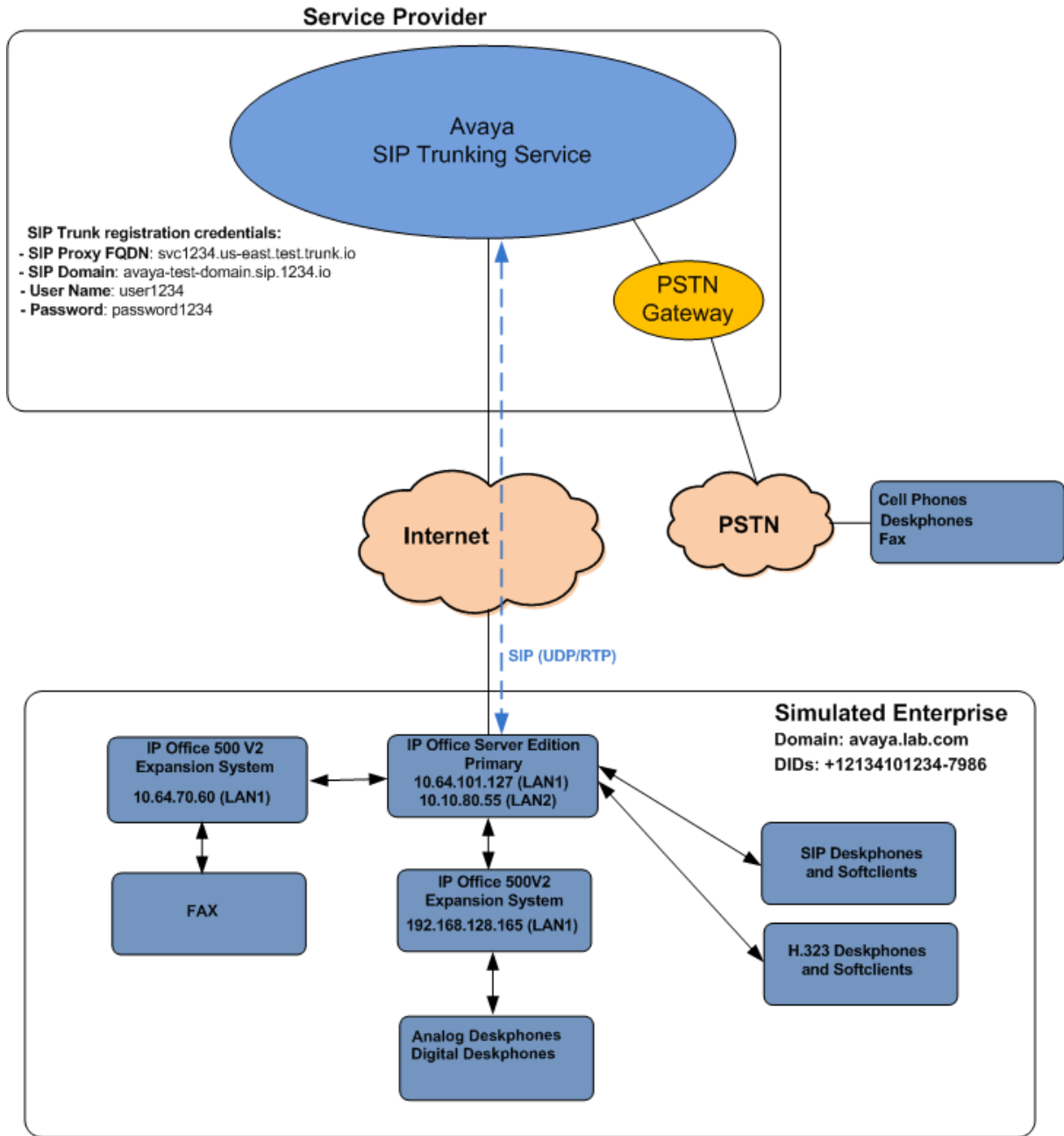
IP endpoints at the enterprise included Avaya 96x1 Series IP Deskphones (with H.323 firmware), Avaya 1100 Series IP Deskphones (with SIP firmware), Avaya J100 Series IP Deskphones (with SIP and H.323 firmware), Avaya Workplace Client for Windows (SIP), Avaya Digital and Analog Deskphones. IP endpoints were registered to the Primary Server; non-IP endpoints (analog and digital) were registered to the Expansion Systems. The site also has a Windows PC running Avaya IP Office Manager to configure and administer the system. Mobile Twinning is configured for some of the IP Office users so that calls to these user's extensions will also ring and can be answered at the configured mobile phones.

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

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

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

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



**Figure 1: Avaya simulated enterprise site connected to the Avaya SIP Trunking service offering**



## 4. Equipment and Software Validated

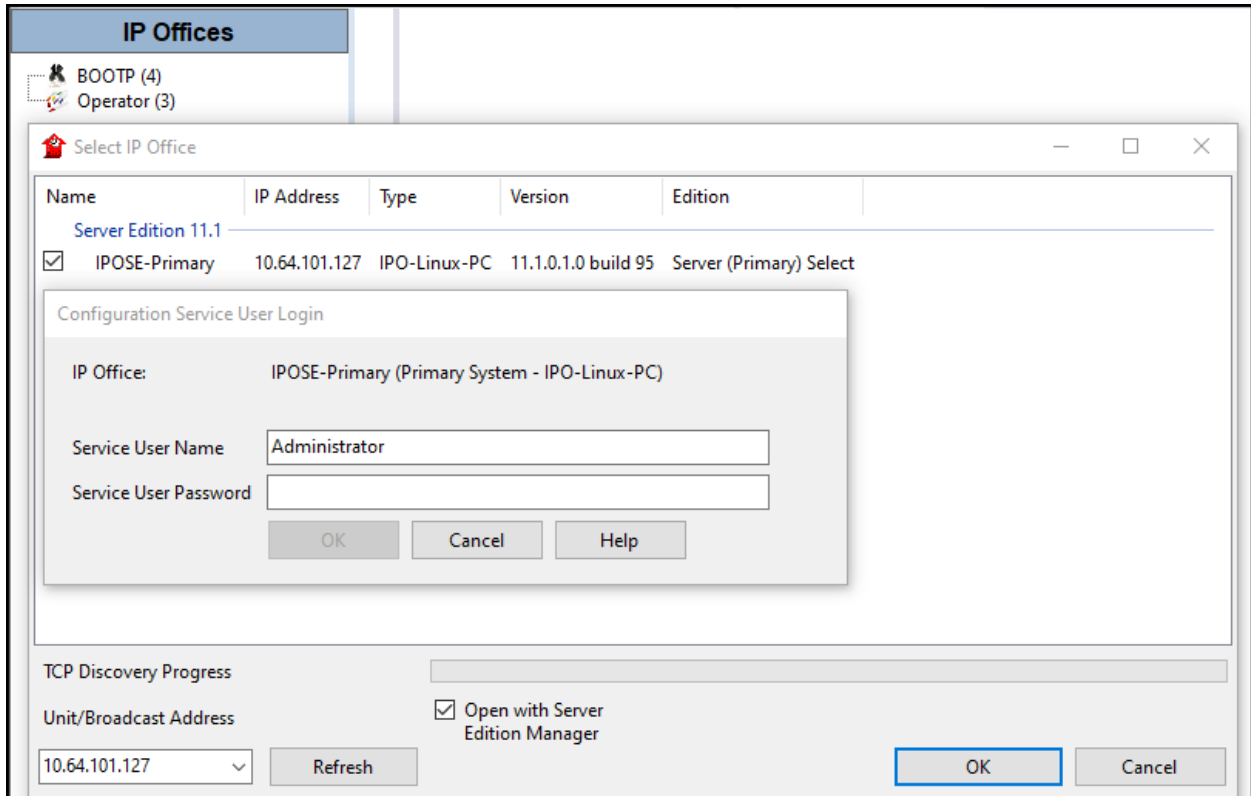
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya IP Office Server Edition (Primary Server)	11.1.0.1 Build 95
• Avaya IP Office Voicemail Pro	11.1.0.1 Build 10
Avaya IP Office IP500 V2 (Expansion Systems)	11.1.0.1 Build 95
Avaya IP Office Manager	11.1.0.1 Build 95
Avaya 96x1 Series IP Deskphones (H.323)	6.8304
Avaya J179 IP Telephone (H.323)	6.8304
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.0.6.0.8
Avaya 1408 Digital Telephone	48.02
Avaya Workplace Client for Windows (SIP)	3.11.0.44.25
Analog Telephone	---

**Note:** Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints.

## 5. Avaya IP Office Primary Server Configuration

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



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

**Configuration** | **Server Edition**

**Summary**  
Server Edition Primary

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

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

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



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

The screenshot displays the Avaya configuration interface. On the left is a tree view under 'Configuration' showing various system components like BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line, Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, and IP500V2-One/Two.

The main area is titled 'License Remote Server' and contains two sections:

- Remote Server Configuration:**
  - License Source: WebLM
  - Domain Name (URL): 10.64.101.127
  - Path: WebLM/LicenseServer
  - Port Number: 52233
  - WebLM Client ID: (empty)
  - WebLM Node ID: -IPOSE-Primary
- Reserved Licenses:**

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

## 5.2. System Settings

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

### 5.2.1. System – LAN2 Tab

In the sample configuration, the LAN2 interface is used for the SIP trunk connection to the Avaya network.

#### 5.2.1.1 LAN2 – LAN Settings Tab

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view under 'Configuration' with 'IPOSE-Primary' selected. The main area shows the 'IPOSE-Primary' configuration page with tabs for 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', and 'System Events'. The 'LAN2' tab is active, and the 'LAN Settings' sub-tab is selected. The configuration fields are as follows:

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

An 'Advanced' button is visible at the bottom right of the configuration area.

### 5.2.1.2 LAN2 – VoIP Tab

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

The screenshot displays the Avaya IPOSE-Primary configuration interface. On the left is a tree view under 'Configuration' with 'IPOSE-Primary' selected. The main pane shows the 'LAN2' tab with sub-tabs for 'LAN Settings', 'VoIP', and 'Network Topology'. The 'VoIP' sub-tab is active, showing the following settings:

- H.323 Gatekeeper Enable
  - Auto-create Extension
  - Auto-create User
  - H.323 Remote Extension Enable
- H.323 Signaling over TLS: Disabled (dropdown)
- Remote Call Signaling Port: 1720 (dropdown)
- SIP Trunks Enable
- SIP Registrar Enable
  - Auto-create Extension/User
  - SIP Remote Extension Enable
  - Allowed SIP User Agents: Block blacklist only
- SIP Domain Name: [Empty text box]
- SIP Registrar FQDN: [Empty text box]
- Layer 4 Protocol:
  - UDP: UDP Port 5060, Remote UDP Port 5060
  - TCP: TCP Port 5060, Remote TCP Port 5060
  - TLS: TLS Port 5061, Remote TLS Port 5061
- Challenge Expiration Time (sec): 10 (dropdown)
- RTP:
  - Port Number Range: Minimum 46750, Maximum 50750

Scroll down the page:

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

The screenshot displays the configuration page for 'IPOSE-Primary' in the Avaya IP Office system. The left sidebar shows a tree view of the configuration hierarchy, with 'IPOSE-Primary' selected. The main content area is divided into several sections:

- LAN Settings:** Includes tabs for LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. Under the LAN2 tab, there are settings for SIP Registrar FQDN, Layer 4 Protocol (with checkboxes for UDP, TCP, and TLS), and Challenge Expiration Time (set to 10 seconds).
- RTP:** Contains 'Port Number Range' (Minimum: 46750, Maximum: 50750) and 'Port Number Range (NAT)' (Minimum: 40750, Maximum: 50750). It also has a checkbox for 'Enable RTCP Monitoring on Port 5005' and an 'RTCP collector IP address for phones' field set to 0.0.0.0.
- Keepalives:** Shows 'Scope' set to 'RTP-RTCP' and 'Periodic timeout' set to 30. 'Initial keepalives' is set to 'Enabled'.
- DiffServ Settings:** A grid of DSCP values for various traffic types:
 

B8	DSCP(Hex)	B8	Video DSCP (Hex)	FC	DSCP Mask (Hex)	88	SIG DSCP (Hex)
46	DSCP	46	Video DSCP	63	DSCP Mask	34	SIG DSCP
- DHCP Settings:** Includes 'Primary Site Specific Option Number (SSON)' (176), 'Secondary Site Specific Option Number (SSON)' (242), 'VLAN' (Not Present), and '1100 Voice VLAN Site Specific Option Number (SSON)' (232).

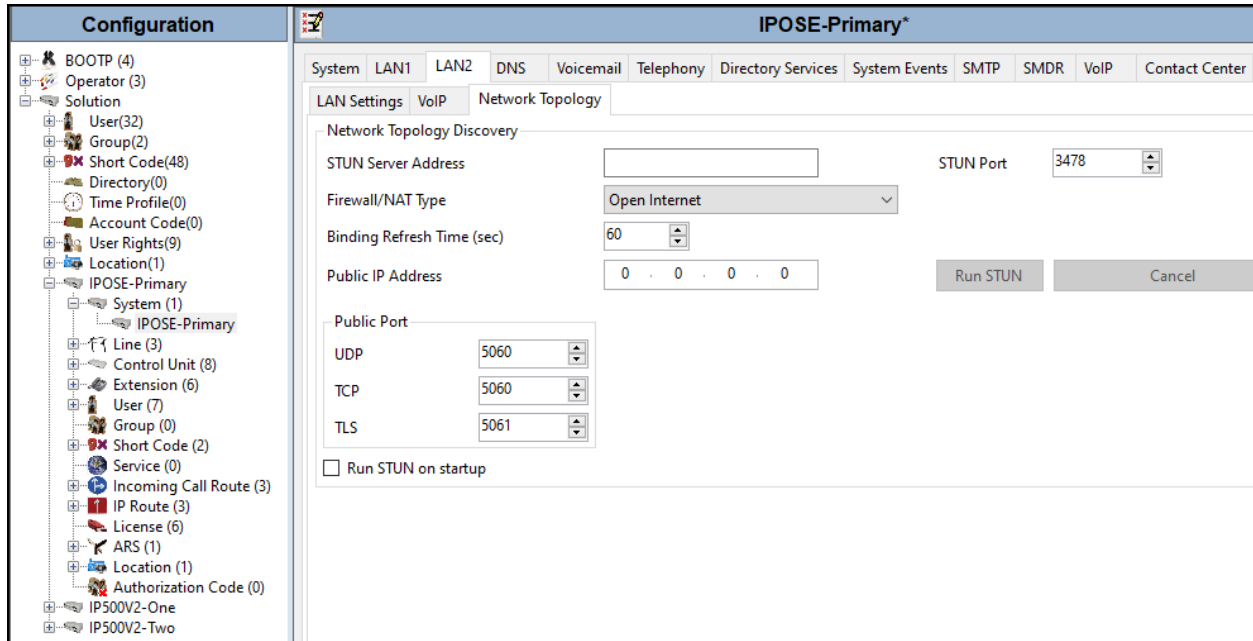


**Note:** In the compliance test, the LAN1 interface was used to connect the Avaya IP Office to the enterprise site IP network (private network). The LAN1 interface configuration is not directly relevant to the interface with the Avaya SIP Trunking Service, and therefore is not described in these Application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

### 5.2.1.3 LAN2 – Network Topology Tab

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

- Select the **Firewall/NAT Type** from the pull-down menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used.
- Set **Binding Refresh Time (seconds)** to **60**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider.
- Set **Public Port / UDP** to **5060**.
- Default values were used for all other parameters.
- Click the **OK** button (not shown).



## 5.2.2. System – DNS Tab

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view under the 'Configuration' header, showing a hierarchy of system components. The 'IPOSE-Primary' system is selected, and its 'System' sub-component is expanded. On the right, the 'IPOSE-Primary' details pane is shown with the 'DNS' tab selected. The configuration fields are as follows:

System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events
DNS Server IP Address			75 . 75 . 75 . 75				
Backup DNS Server IP Address			75 . 75 . 76 . 76				
DNS Domain							

### 5.2.3. 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.
- 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 configuration interface for IPOSE-Primary, specifically the Telephony tab. The left sidebar shows a tree view of the configuration hierarchy, with 'IPOSE-Primary' selected. The main panel is divided into several sections:

- System Tab:** Includes settings for Dial Delay Time (4), Dial Delay Count (0), Default No Answer Time (15), Hold Timeout (0), Park Timeout (300), Ring Delay (5), Call Priority Promotion Time (Disabled), Default Currency (USD), Default Name Priority (Favor Directory), Media Connection Preservation (Enabled), and Phone Failback (Automatic).
- Companding Law:** A sub-section with two columns: 'Switch' and 'Line'. Under 'Switch', the 'U-Law' radio button is selected. Under 'Line', the 'U-Law Line' radio button is selected.
- Other Settings:** Includes checkboxes for DSS Status, Auto Hold, Dial By Name (checked), Show Account Code (checked), Inhibit Off-Switch Forward/Transfer (unchecked), Restrict Network Interconnect (unchecked), and Include location specific information (unchecked).
- Drop External Only Impromptu Conference:** Checked.
- Visually Differentiate External Call:** Unchecked.
- High Quality Conferencing:** Checked.
- Directory Overrides Barring:** Checked.
- Advertise Callee State To Internal Callers:** Unchecked.
- Internal Ring on Transfer:** Unchecked.
- RTCP Collector Configuration:** Includes a checkbox for 'Send RTCP to an RTCP Collector' (unchecked), a 'Server Address' field (0.0.0.0), a 'UDP Port Number' field (5005), and an 'RTCP reporting interval (sec)' field (5).

## 5.2.4. System – VoIP Tab

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

### 5.2.4.1 VoIP – VoIP Tab

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

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

The screenshot displays the configuration interface for IPOSE-Primary, specifically the VoIP tab. The left sidebar shows a tree view of the configuration hierarchy, with 'IPOSE-Primary' selected. The main area shows the 'VoIP' configuration page. Under the 'VoIP' tab, there are sections for 'VoIP Security' and 'Access Control Lists'. The 'Ignore DTMF Mismatch For Phones' and 'Allow Direct Media Within NAT Location' checkboxes are both unchecked. The 'RFC2833 Default Payload' is set to '101'. Below this, there are three columns: 'Available Codecs', 'Default Codec Selection' (with 'Unused' and 'Selected' sub-sections), and 'Selected'. The 'Available Codecs' list includes G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, and G.729(a) 8K CS-AC. The 'Selected' list includes G.711 ULAW 64K, G.711 ALAW 64K, and G.729(a) 8K CS-AC. Navigation buttons (right arrow, up arrow, down arrow, left arrow) are located between the 'Unused' and 'Selected' lists.

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

### 5.2.4.2 VoIP – VoIP Security Tab

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

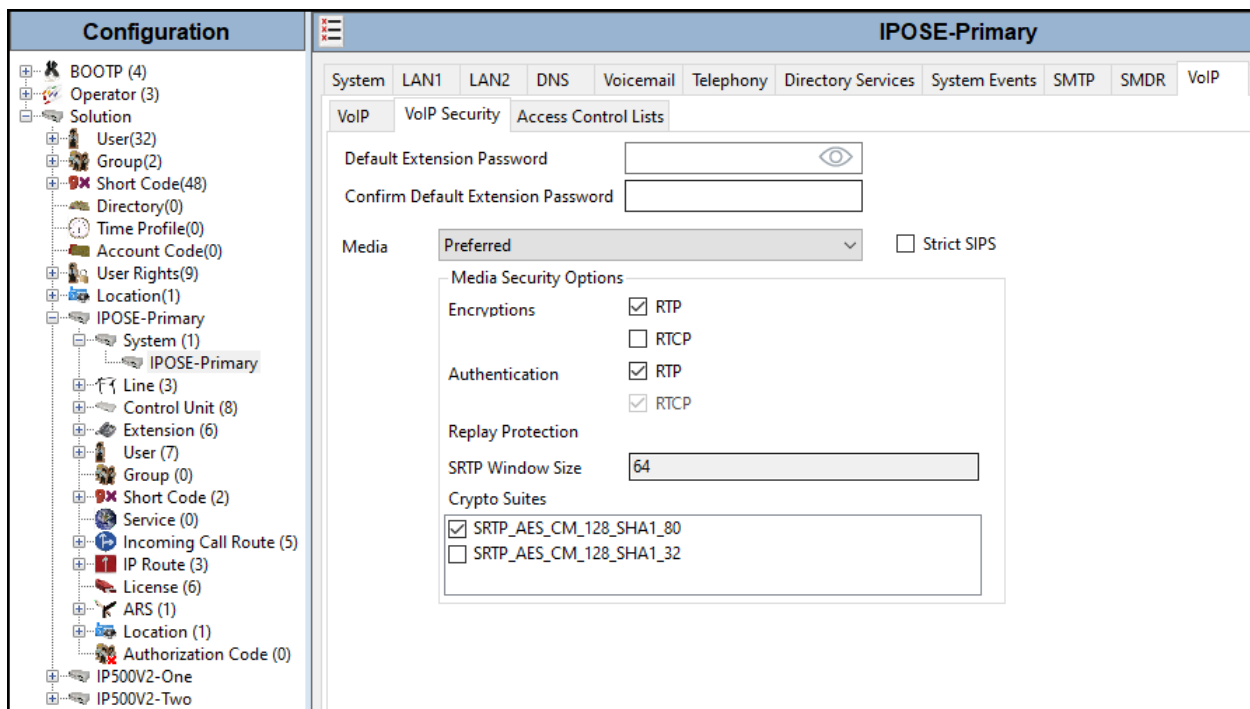
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

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

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

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

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



### 5.3. IP Route

Create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to route calls to the Avaya 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 Avaya IP Office configuration interface. On the left is a tree view under 'Configuration' with various categories like BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line, Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route (3), License, ARS, Location, Authorization Code, and IP500V2-One/Two. The 'IP Route' category is expanded, showing three entries: '0.0.0.0' (highlighted in blue), '10.64.70.0', and '192.168.128.0'. The main pane shows the configuration for the selected '0.0.0.0' route. The title bar indicates '0.0.0.0\*'. The configuration fields are: IP Address (0 . 0 . 0 . 0), IP Mask (0 . 0 . 0 . 0), Gateway IP Address (10 . 10 . 80 . 1), Destination (LAN2), and Metric (0).

Field	Value
IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	10 . 10 . 80 . 1
Destination	LAN2
Metric	0

## 5.4. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Avaya network. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.4.1** to create the SIP Line from the template.

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

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

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

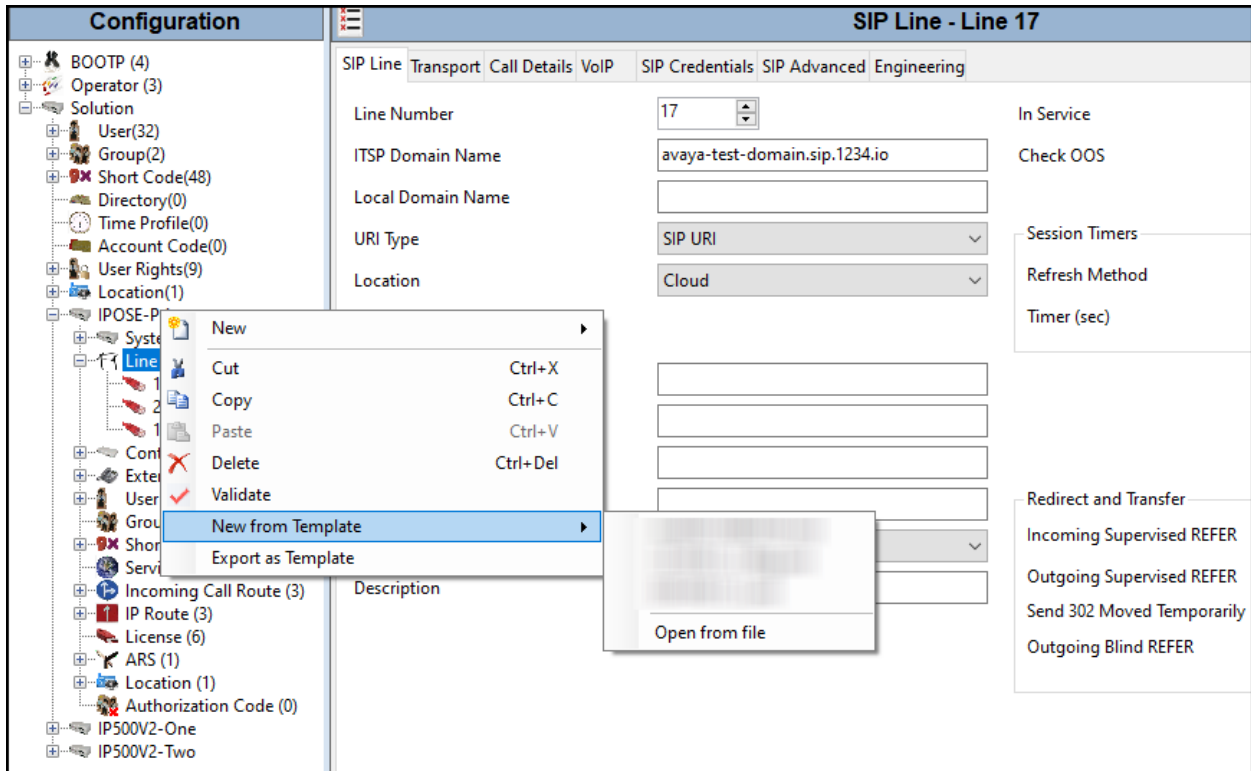
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.7**.

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

SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

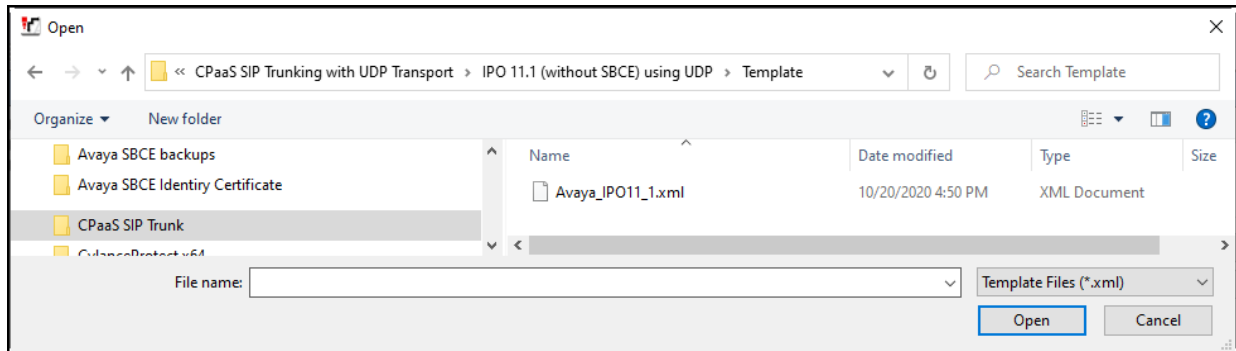
Copy a previously created template file to a location (e.g., *Temp*) on the same computer where IP Office Manager is installed.

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

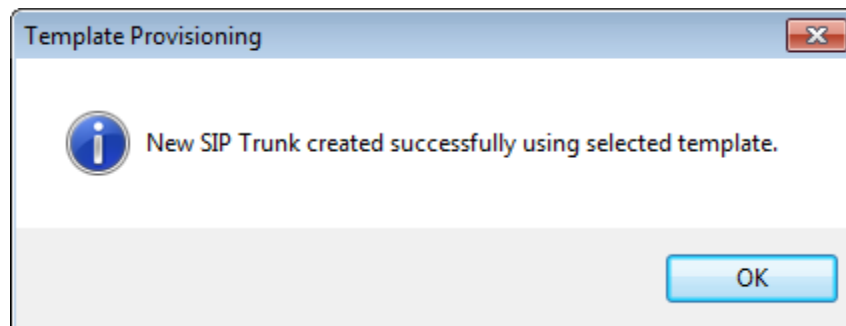




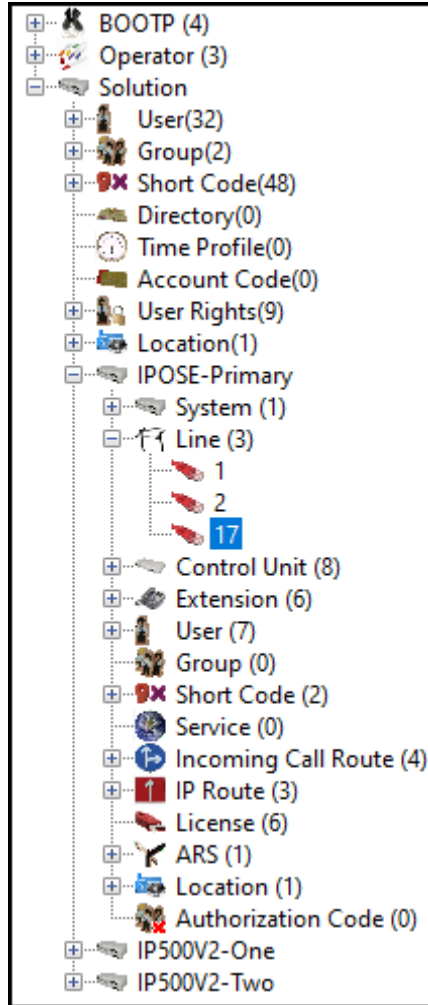
Navigate to the directory on the local machine where the template was copied and select the template.



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



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



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

## 5.4.2. SIP Line – SIP Line Tab

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

- Set **ITSP Domain Name** to **avaya-test-domain.sip.1234.io**, the domain name provided by Avaya. **Note:** The Domain Name shown here and throughout this document has been masked for confidentiality and privacy purposes. Set ITSP Domain Name to the domain name provided by Avaya instead of the domain shown here.
- 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**.
- Set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Always**.
- Check **Outgoing Blind REFER** parameter to enable the use of REFER for blind transfers.
- Click **OK** to commit (not shown).

Configuration		SIP Line - Line 17	
BOOTP (4)		SIP Line	Transport Call Details VoIP SIP Credentials SIP Advanced Engineering
Operator (3)		Line Number	17 <input type="checkbox"/> In Service
Solution		ITSP Domain Name	avaya-test-domain.sip.1234.io <input type="checkbox"/> Check OOS
User(32)		Local Domain Name	<input type="text"/>
Group(2)		URI Type	SIP URI
Short Code(48)		Location	Cloud
Directory(0)		Prefix	<input type="text"/>
Time Profile(0)		National Prefix	<input type="text"/>
Account Code(0)		International Prefix	<input type="text"/>
User Rights(9)		Country Code	<input type="text"/>
Location(1)		Name Priority	System Default
IPOSE-Primary		Description	Service Provider
System (1)			
Line (3)			
1			
2			
17			
Control Unit (8)			
Extension (6)			
User (7)			
Group (0)			
Short Code (2)			
Service (0)			
Incoming Call Route (3)			
IP Route (3)			
License (6)			
ARS (1)			
Location (1)			
Authorization Code (0)			
IP500V2-One			
IP500V2-Two			

### 5.4.3. SIP Line – Transport Tab

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

- Set the **ITSP Proxy Address** to **svc1234.us-east.test.trunk.io**, the ITSP Proxy Address provided by Avaya. **Note:** The ITSP Proxy Address shown here and throughout this document has been masked for confidentiality and privacy purposes. Set ITSP Proxy Address to the SIP proxy name provided by Avaya instead of the name shown here.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **None** (refer to the note below).
- Set the **Send Port** and **Listen Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya configuration interface for a SIP Line. On the left is a tree view under 'Configuration' showing various system components like BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line (1, 2, 17), Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, and IP500V2-One/Two. The main panel is titled 'SIP Line - Line 17' and has several tabs: SIP Line, Transport, Call Details, VoIP, SIP Credentials, SIP Advanced, and Engineering. The 'Transport' tab is active, showing the following configuration:

- ITSP Proxy Address: svc1234.us-east.test.trunk.io
- Network Configuration:
  - Layer 4 Protocol: UDP
  - Send Port: 5060
  - Use Network Topology Info: None
  - Listen Port: 5060
- Explicit DNS Server(s): 0 . 0 . 0 . 0 and 0 . 0 . 0 . 0
- Calls Route via Registrar:
- Separate Registrar: [Empty text box]

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

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

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

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

The screenshot shows the Avaya IP Office configuration interface. On the left is a tree view of the configuration hierarchy. The main window is titled "SIP Line - Line 17\*" and has several tabs: SIP Line, Transport, Call Details, VoIP, SIP Credentials (selected), SIP Advanced, and Engineering. Below the tabs is a table with the following data:

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

Below the table is an "Edit SIP Credentials" form with the following fields:

- User name: user1234
- Authentication Name: user1234
- Contact: (empty)
- Password: (masked with dots)
- Confirm Password: (masked with dots)
- Expiration (mins): 60
- Registration required:

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

### 5.4.5. SIP Line – Call Details Tab

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

- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Under **Credentials**, select **1: user1234** from the pull-down menu (this field will default to the **User Name** used under the **SIP Credentials** tab in **Section 5.4.4**).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Check the **P Asserted ID** and **Diversion Header**.
- Set the **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** fields to the values shown in the screenshot below.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.

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

## 5.4.6. SIP Line – VoIP Tab

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

- The **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line, as shown. Avaya supports codecs **G.711ULAW**, **G.711ALAW** and **G.729(a)** for audio.
- Select **T38** for **Fax Transport Support** (refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).

The screenshot shows the configuration interface for SIP Line - Line 17, specifically the VoIP tab. The left sidebar displays a tree view of the system configuration, including sections for BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line (with sub-items 1, 2, and 17), Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, and IP500V2-One/Two. The main configuration area is titled 'SIP Line - Line 17' and includes tabs for SIP Line, Transport, Call Details, VoIP, SIP Credentials, SIP Advanced, and Engineering. The VoIP tab is active, showing the following settings:

- Codec Selection:** Custom (dropdown). Below this are two lists: 'Unused' (empty) and 'Selected' (containing G.711 ULAW 64K, G.711 ALAW 64K, and G.729(a) 8K CS-ACELP). Navigation buttons (>>>, <<<, <<<<, >>>>) are present between the lists.
- Fax Transport Support:** T38 (dropdown).
- DTMF Support:** RFC2833/RFC4733 (dropdown).
- Media Security:** Disabled (dropdown).
- Local Hold Music:**
- Re-invite Supported:**
- Codec Lockdown:**
- Allow Direct Media Path:**
- Force direct media with phones:**
- PRACK/100rel Supported:**

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

## 5.4.7. SIP Line – SIP Advanced Tab

In the **Addressing** area:

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

In the **Identity** area:

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

In the **Call Control** area:

- Check **Emulate NOTIFY for REFER** (Refer to **Section 2.2**).
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the configuration interface for SIP Line - Line 17, specifically the SIP Advanced tab. The interface is divided into three main sections: Addressing, Identity, and Call Control.

**Addressing Section:**

- Association Method: By Source IP address (dropdown)
- Call Routing Method: Request URI (dropdown)
- Use P-Called-Party:
- Suppress DNS SRV Lookups:

**Identity Section:**

- Use "phone-context":
- Add user=phone:
- Use + for International:
- Use PAI for Privacy:
- Use Domain for PAI:
- Caller ID from From header:
- Send From In Clear:
- Cache Auth Credentials:
- User-Agent and Server Headers:
- Send Location Info: Never (dropdown)
- Add UUI header:
- Add UUI header to redirected calls:

**Call Control Section:**

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

**Media Section:**

- Allow Empty INVITE:
- Send Empty re-INVITE:
- Allow To Tag Change:
- P-Early-Media Support: None (dropdown)
- Send SilenceSupp=Off:
- Force Early Direct Media:
- Media Connection Preservation: System (dropdown)
- Indicate HOLD:



## 5.5. Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.4**. To configure these settings, first navigate to **User** → *Name* in the Navigation Pane where *Name* is the name of the user to be modified. In the example below, the name of the user is **Ext3041 H323**. Select the **SIP** tab in the Details Pane. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Avaya. Note the DID number is preceded by +1 since its required in order to conform with the E.164 numbering format. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network. This can also be accomplished by activating Withhold Number on H.323 Deskphones (not shown). Click the **OK** to commit (not shown).

The screenshot displays the Avaya configuration interface for user **Ext3041 H323: 3041**. The interface is divided into two main sections: a left-hand **Configuration** pane and a right-hand **Details** pane.

**Configuration Pane:** Shows a hierarchical tree structure. The **User** category is expanded to show a list of users, including **3041 Ext3041 H323**, which is selected.

**Details Pane:** The **SIP** tab is active. It contains the following configuration fields:

- SIP Name:** +12134101234
- SIP Display Name (Alias):** Ext3041 H323
- Contact:** +12134101234
- Anonymous:**

## 5.6. Mobility

Select the **Mobility** tab for the user. In the sample configuration user 3041 was one of the users configured to test the Mobile Twinning feature. The following screen shows the Mobility tab for user 3041. The Mobility Features, Mobile Twinning and Mobile Call Control boxes are checked. The Twinned Mobile Number field is configured with the number to dial to reach the twinned telephone, including the dial access code “9”, in this case 917864571234. Other options can be set according to customer requirements.

**Note:** Checking the Mobile Call Control box allows a user receiving a call on their twinned device to access system dial tone and then perform dialing action including making calls and activating short codes.

The screenshot displays the Avaya Configuration Manager interface for user 3041. The left-hand navigation tree shows a hierarchy of system components, with 'User (7)' expanded to show '3041 Ext3041 H323'. The main configuration area is titled 'Ext3041 H323: 3041' and has the 'Mobility' tab selected. The 'Internal Twinning' section is unchecked. The 'Mobility Features' section is checked, and 'Mobile Twinning' is also checked. The 'Twinned Mobile Number (including dial access code)' field is set to '917864571234'. The 'Twinning Time Profile' is set to '<None>'. The 'Mobile Dial Delay (sec)' is set to '2'. The 'Mobile Answer Guard (sec)' is set to '0'. Other options like 'Fallback Twinning', 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', 'Twin When Logged Out', 'one-X Mobile Client', and 'Mobile Call Control' are also visible, with 'Mobile Call Control' being checked.

## 5.7. IP Office Line – Primary Server

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

The screenshot displays the configuration interface for an IP Office Line. On the left is a navigation tree under 'Configuration', showing a hierarchy from 'Solution' down to 'IP500V2-One' and 'IP500V2-Two'. The main area is titled 'IP Office Line - Line 1' and contains several configuration sections:

- Line Settings:** Line Number (1), Transport Type (WebSocket Server), Networking Level (SCN), Security (Medium), Telephone Number, Prefix, Outgoing Group ID (99999), Number of Channels (250), and Outgoing Channels (250).
- Gateway:** Address (192 . 168 . 128 . 165), Location (3: Thornton, CO), Password, and Confirm Password.
- SCN Resiliency Options:** Includes a 'Supports Resiliency' checkbox and four sub-options: 'Backs up my IP phones', 'Backs up my hunt groups', 'Backs up my voicemail', and 'Backs up my IP DECT phones'.
- Description:** A text input field for the line's description.

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

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **T38** for **Fax Transport Support** (refer to **Section 2.2**).
- Under **Media Security** verify **Same as System (Preferred)** is selected (default value).

The screenshot displays the configuration page for 'IP Office Line - Line 1'. The left sidebar shows a hierarchical tree of system components, with 'Line (3)' expanded to show 'Line 1', '2', and '17'. The main configuration area is divided into several sections:

- Line**: Tabbed interface with 'VoIP Settings' selected.
- Codec Selection**: A dropdown menu set to 'System Default'. Below it are two lists: 'Unused' (empty) and 'Selected' (containing G.711 ULAW 64K, G.711 ALAW 64K, and G.729(a) 8K CS-ACELP). Navigation buttons (>>>, <<<, <-, >-, >>>) are present between the lists.
- Fax Transport Support**: A dropdown menu set to 'T38'.
- Call Initiation Timeout (s)**: A numeric input field set to '4'.
- Media Security**: A dropdown menu set to 'Same as System (Preferred)'. Below it is an 'Advanced Media Security Options' section with a 'Same As System' checkbox checked. This section includes:
  - Encryptions**: RTP (checked), RTCP (unchecked).
  - Authentication**: RTP (checked), RTCP (checked).
  - Replay Protection**: SRTP Window Size set to '64'.
  - Crypto Suites**: SRTP\_AES\_CM\_128\_SHA1\_80 (checked), SRTP\_AES\_CM\_128\_SHA1\_32 (unchecked).
- Out Of Band DTMF** and **Allow Direct Media Path**: Both checkboxes are checked.

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

## 5.8. Incoming Call Route

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

- Set **Bearer Capability** to **Any Voice**.
- The **Line Group ID** is set to **17**. This matches the **Incoming Group** field configured in the **Call Details** tab for the SIP Line on **Section 5.4.5**.
- On the **Incoming Number**, enter one of the DID numbers provided by Avaya. Note the DID number is preceded by **+1** since its required in order to conform with the E.164 numbering format.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office Configuration interface. On the left is the 'Configuration' tree, and on the right is the configuration details pane for the selected item '17 +12134101234'.

**Configuration Tree (Left):**

- BOOTP (4)
- Operator (3)
- Solution
  - User (32)
  - Group(2)
  - Short Code(48)
  - Directory(0)
  - Time Profile(0)
  - Account Code(0)
  - User Rights(9)
  - Location(1)
  - IPOSE-Primary
    - System (1)
    - Line (3)
    - Control Unit (8)
    - Extension (6)
    - User (7)
    - Group (0)
    - Short Code (2)
    - Service (0)
    - Incoming Call Route (3)
      - 17 +12134101234**
      - 17 +12134231234
      - 17 +12134235678
    - IP Route (3)
    - License (6)
    - ARS (1)
    - Location (1)
    - Authorization Code (0)
  - IP500V2-One
  - IP500V2-Two

**Configuration Details Pane (Right):**

Standard | Voice Recording | Destinations

Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	+12134101234
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

Select the **Destinations** tab. From the **Destination** drop-down menu, select the IP Office extension associated with this DID number. In the reference configuration, the DID number +12134101234 provided by Avaya was associated with the Avaya IP Office extension **3041 Ext3041 H323**.

The screenshot shows the Avaya IP Office configuration interface. On the left is a navigation tree under the 'Configuration' tab, with 'Solution' expanded to show 'Incoming Call Route (3)'. The selected route is '17 +12134101234'. The main area shows the configuration for this route, with the 'Destinations' tab selected. A table lists the destinations for this route.

TimeProfile	Destination	Fallback Extension
Default Value	3041 Ext3041 H323	

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

## 5.9. 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.

### 5.9.1. 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 Avaya IP Office configuration interface. On the left is a navigation tree with categories like BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line, Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, and IP500V2-One/Two. The 'Short Code' category is expanded, showing a list of short codes including '\*66\*N#' and '9N'. The '9N' short code is selected. On the right, the configuration details for '9N: Dial' are shown in a form. The fields are: Code (9N), Feature (Dial), Telephone Number (N), Line Group ID (50: Main), and Locale (United States (US English)). There are also checkboxes for Force Account Code and Force Authorization Code, both of which are unchecked.

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

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

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

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **1** followed by **10 Xs** to represent the exact number of digits.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **+1N**. The value **N** represents the additional number of digits dialed by the user after dialing **1** (The **9** will be stripped off). With this setting, the 10 digits dialed number, preceded by prefix **+1** will be sent to the SIP trunk, required to conform with the E.164 numbering format.
- Set the **Line Group Id** to the Line Group number being used for the SIP Line, in this case **Line Group ID 17** was used.
- For **Locale**, **United States (US English)** was used
- Click **OK** to commit.

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

The screenshot shows a dialog box titled "Edit Short Code". It contains the following fields and controls:

- Code:** A text input field containing "1XXXXXXXXXX".
- Feature:** A dropdown menu with "Dial" selected.
- Telephone Number:** A text input field containing "+1N".
- Line Group ID:** A dropdown menu with "17" selected.
- Locale:** A dropdown menu with "United States (US English)" selected.
- Force Account Code:** A checkbox that is unchecked.
- Force Authorization Code:** A checkbox that is unchecked.
- Buttons:** "OK" and "Cancel" buttons are located on the right side of the dialog.

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

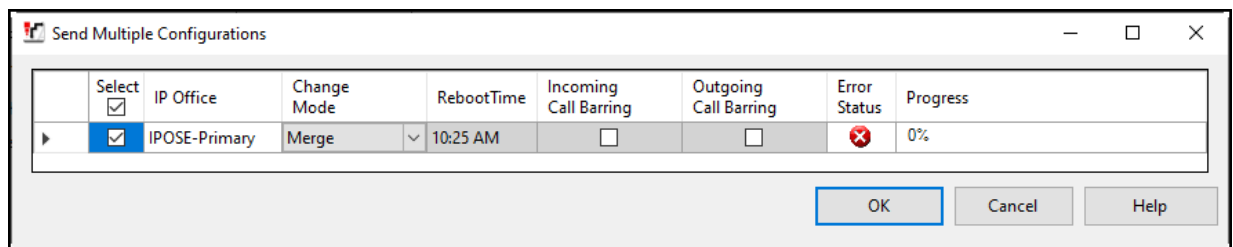


## 5.10. Save IP Office Primary Server Configuration

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

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

Click **OK** to execute the save.



## 6. Avaya IP Office Expansion System Configuration

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

Configuration	System Inventory
<ul style="list-style-type: none"> <li>⊕ BOOTP (4)</li> <li>⊕ Operator (3)</li> <li>⊖ Solution           <ul style="list-style-type: none"> <li>⊕ User(32)</li> <li>⊕ Group(2)</li> <li>⊕ Short Code(48)</li> <li>⊕ Directory(0)</li> <li>⊕ Time Profile(0)</li> <li>⊕ Account Code(0)</li> <li>⊕ User Rights(9)</li> <li>⊕ Location(1)</li> <li>⊕ IPOSE-Primary</li> <li>⊖ IP500V2-One               <ul style="list-style-type: none"> <li>⊕ System (1)</li> <li>⊕ Line (3)</li> <li>⊕ Control Unit (4)</li> <li>⊕ Extension (24)</li> <li>⊕ User (27)</li> <li>⊕ Group (1)</li> <li>⊕ Short Code (12)</li> <li>⊕ Service (0)</li> <li>⊕ RAS (1)</li> <li>⊕ Incoming Call Route (1)</li> <li>⊕ WAN Port (0)</li> <li>⊕ Firewall Profile (1)</li> <li>⊕ IP Route (4)</li> <li>⊕ License (2)</li> <li>⊕ Tunnel (0)</li> <li>⊕ ARS (2)</li> <li>⊕ Location (1)</li> <li>⊕ Authorization Code (0)</li> </ul> </li> <li>⊕ IP500V2-Two</li> </ul> </li> </ul>	<div style="border: 1px solid #ccc; padding: 5px;"> <h3 style="margin: 0;">Server Edition Expansion System</h3> <ul style="list-style-type: none"> <li>⊖ <b>Hardware Installed</b> <ul style="list-style-type: none"> <li>Control Unit: IP 500 V2</li> <li>Internal Modules: VCM64/PRID U; PHONE8</li> <li>Expansion Modules: DIG DCPx16 V2</li> </ul> </li> <li>⊖ <b>System Settings</b> <ul style="list-style-type: none"> <li>IP Address: 192.168.128.165</li> <li>Sub-Net Mask: 255.255.255.0</li> <li>System Locale: United States (US English)</li> <li>System Location: 3: Thornton, CO</li> <li>Device ID: NONE</li> <li>Number of Extensions on System: 24</li> </ul> </li> <li>⊖ <b>Features Configured</b> <ul style="list-style-type: none"> <li>Licenses Installed: Server Edition(1); IP Office Select(1); Basic User(25)</li> <li>Connected Extensions: 3043; 3044</li> <li>Users NOT Configured for Voicemail: NONE</li> <li>Users assigned as Ex-Directory: NONE</li> <li>Users assigned for Twinning: NONE</li> <li>Users barred from making Outgoing Calls: NONE</li> <li>Music on Hold: WAV File</li> </ul> </li> </ul> </div>

## 6.1. Physical Hardware

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

Configuration	IP 500 V2																
<ul style="list-style-type: none"> <li>BOOTP (4)</li> <li>Operator (3)</li> <li>Solution           <ul style="list-style-type: none"> <li>User(32)</li> <li>Group(2)</li> <li>Short Code(48)</li> <li>Directory(0)</li> <li>Time Profile(0)</li> <li>Account Code(0)</li> <li>User Rights(9)</li> <li>Location(1)</li> <li>IPOSE-Primary</li> <li>IP500V2-One               <ul style="list-style-type: none"> <li>System (1)</li> <li>Line (3)</li> <li>Control Unit (4)                   <ul style="list-style-type: none"> <li><b>1 IP 500 V2</b></li> <li>2 VCM64/PRID U</li> <li>3 PHONE8</li> <li>6 DIG DCPx16 V2</li> </ul> </li> </ul> </li> </ul> </li> <li>Extension (24)</li> <li>User (27)</li> <li>Group (1)</li> <li>Short Code (12)</li> <li>Service (0)</li> <li>RAS (1)</li> <li>Incoming Call Route (1)</li> <li>WAN Port (0)</li> <li>Firewall Profile (1)</li> <li>IP Route (4)</li> <li>License (2)</li> <li>Tunnel (0)</li> <li>ARS (2)</li> <li>Location (1)</li> <li>Authorization Code (0)</li> <li>IP500V2-Two</li> </ul>	<table border="1"> <thead> <tr> <th colspan="2">Unit</th> </tr> </thead> <tbody> <tr> <td>Device Number</td> <td>1</td> </tr> <tr> <td>Unit Type</td> <td>IP 500 V2</td> </tr> <tr> <td>Version</td> <td>11.1.0.1.0 build 95</td> </tr> <tr> <td>Serial Number</td> <td></td> </tr> <tr> <td>Unit IP Address</td> <td>192.168.128.165</td> </tr> <tr> <td>Interconnect Number</td> <td>0</td> </tr> <tr> <td>Module Number</td> <td>Control Unit</td> </tr> </tbody> </table>	Unit		Device Number	1	Unit Type	IP 500 V2	Version	11.1.0.1.0 build 95	Serial Number		Unit IP Address	192.168.128.165	Interconnect Number	0	Module Number	Control Unit
Unit																	
Device Number	1																
Unit Type	IP 500 V2																
Version	11.1.0.1.0 build 95																
Serial Number																	
Unit IP Address	192.168.128.165																
Interconnect Number	0																
Module Number	Control Unit																

## 6.2. LAN Settings

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

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

The screenshot displays the configuration interface for an IP500V2-One system. On the left is a navigation tree under 'Configuration' with 'IP500V2-One' selected. The main pane shows the 'LAN1' configuration tab. Under the 'LAN Settings' sub-tab, the following fields are visible:

- IP Address: 192 . 168 . 128 . 165
- IP Mask: 255 . 255 . 255 . 0
- Primary Trans. IP Address: 0 . 0 . 0 . 0
- RIP Mode: None (dropdown menu)
- Enable NAT
- Number Of DHCP IP Addresses: 200 (spinner)
- DHCP Mode:  Server  Client  Dial In  Disabled
- Advanced button

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

### 6.3. IP Route

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

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

Configuration		0.0.0.0*	
IP Route			
IP Address		0 . 0 . 0 . 0	
IP Mask		0 . 0 . 0 . 0	
Gateway IP Address		192 . 168 . 128 . 200	
Destination		LAN1	
Metric		0	
		<input type="checkbox"/> Proxy ARP	

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

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

The screenshot displays the configuration interface for an IP Office Line. On the left is a navigation tree under the 'Configuration' header, showing a hierarchy from Solution down to IP500V2-One and then to Line 17. The main area is titled 'IP Office Line - Line 17' and contains several tabs: 'Line', 'Short Codes', 'VoIP Settings', and 'T38 Fax'. The 'Line' tab is active, showing the following configuration fields:

- Line Number: 17
- Transport Type: WebSocket Client
- Networking Level: SCN
- Security: Medium
- Telephone Number: [Empty]
- Prefix: [Empty]
- Outgoing Group ID: 99999
- Number of Channels: 250
- Outgoing Channels: 250
- Gateway Address: 10 . 64 . 101 . 127
- Port: 443
- Location: 3: Thornton, CO
- Password: [Masked]
- Confirm Password: [Masked]
- Description: [Empty]

Under the 'SCN Resiliency Options' section, there are three checkboxes, all of which are unchecked:

- Supports Resiliency
- Backs up my IP phones
- Backs up my hunt groups
- Backs up my IP DECT phones



The screen below shows the IP Office Line, **T38 Fax** tab:

- Uncheck the **Use Default Values** at the bottom of the screen.
- Set the **T.38 Fax Version** to **0**.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).

The screenshot displays the configuration interface for the T38 Fax tab. The interface is organized into several sections:

- Top Navigation:** Line, Short Codes, VoIP Settings, T38 Fax (selected).
- Left Column:**
  - T38 Fax Version: 0 (dropdown)
  - Transport: UDPTL (dropdown)
  - Redundancy section:
    - Low Speed: 0 (spinner)
    - High Speed: 0 (spinner)
  - TCF Method: Trans TCF (dropdown)
  - Max Bit Rate (bps): 14400 (dropdown)
  - EFlag Start Timer (ms): 2600 (spinner)
  - EFlag Stop Timer (ms): 2300 (spinner)
  - Tx Network Timeout (sec): 150 (spinner)
- Right Column:**
  - Scan Line Fix-up:
  - TFOP Enhancement:
  - Disable T30 ECM:
  - Disable EFlags For First DIS:
  - Disable T30 MR Compression:
  - NSF Override:
  - Country Code: 0 (spinner)
  - Vendor Code: 0 (spinner)
- Bottom:**  Use Default Values



## 6.5. Short Codes

Similar to the configuration of the Primary server in **Section 5.9.1**, create a Short Code to access ARS. In the reference configuration, the **Line Group ID** is set to the ARS route illustrated in the next section.

The screenshot displays the Avaya configuration interface. On the left is a tree view under the 'Configuration' header, showing a hierarchy of system components. The 'Short Code' component is expanded, showing a list of short codes including '\*92N;' and '9N'. On the right, the configuration details for the selected '9N: Dial' short code are shown. The fields are as follows:

9N: Dial	
Short Code	
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	51: To-Primary
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

## 6.6. Automatic Route Selection – ARS

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

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

The main configuration area includes the following fields and options:

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

A table lists the route configuration:

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

Additional configuration options include:

- Alternate Route Priority Level: 3 (linked to Alternate Route: <None>)
- Alternate Route Wait Time: 30 (linked to Alternate Route: <None>)

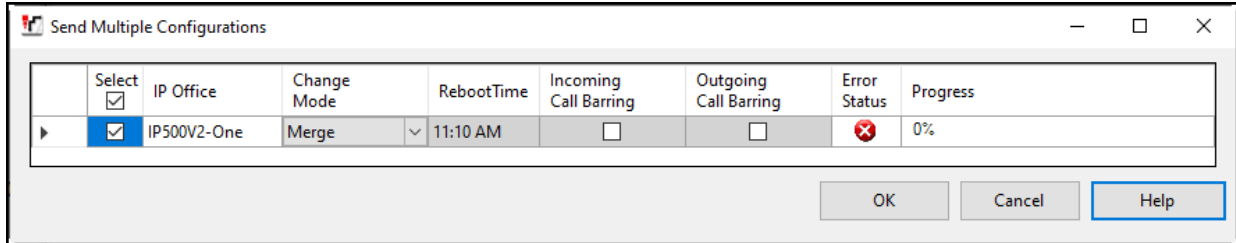
Buttons for "Add...", "Remove", and "Edit..." are visible next to the route table.

Repeat the process described in **Section 6** on any additional Secondary server or Expansion Systems in the solution, as required.

## 6.7. Save IP Office Expansion System Configuration

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

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



## 7. Avaya SIP Trunking Service Configuration

To use Avaya SIP Trunking Service, a customer must request the service from Avaya using the established sales processes. The process can be started by contacting Avaya SIP Trunking via the corporate web site at: <https://www.avaya.com/en/documents/fs-sip-uc8179en.pdf>

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

Avaya will provide the following information:

- SIP Proxy FQDN.
- SIP domain name.
- SIP Trunk registration credentials (User Name, Password, etc.).
- DID numbers.
- Public DNS IP addresses.
- Etc.

**Note:** The SIP Trunk registration credentials, Domain Name, DIDs, etc., shown in this document, were masked for confidentiality and privacy purposes. During the signup process Avaya will provide the customer the necessary information to configure Avaya IP Office.

## 8. Verification Steps

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

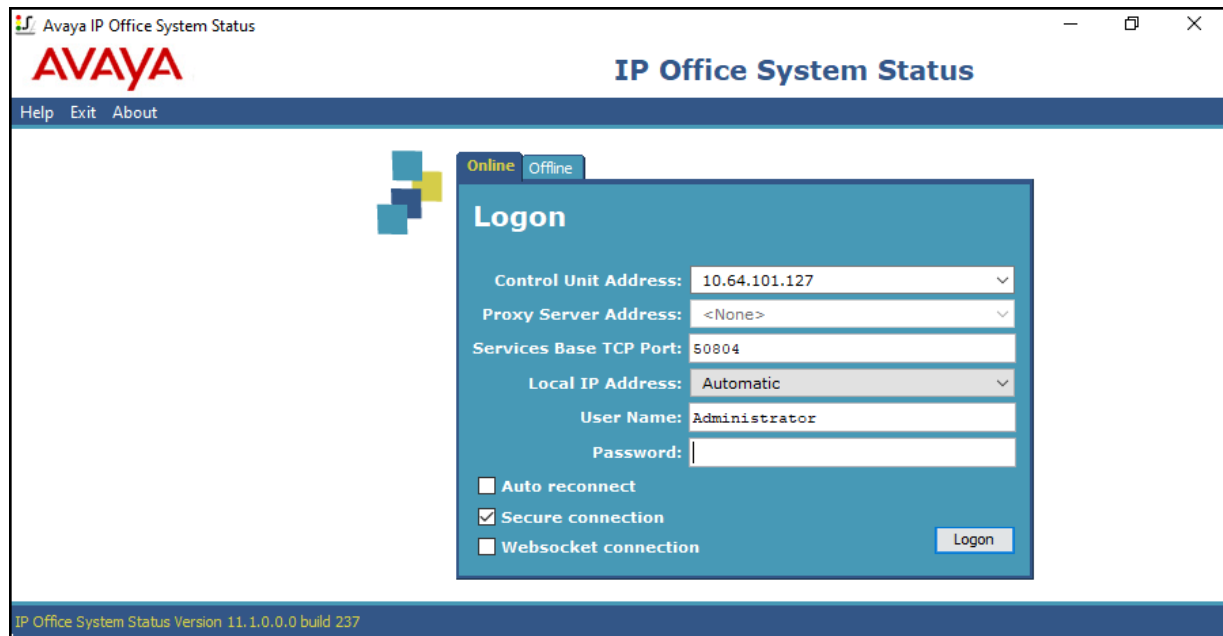
The following steps may be used to verify the configuration:

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

### 8.1. IP Office System Status

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

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



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

The screenshot shows the Avaya IP Office System Status interface. The left pane is expanded to 'Trunks (3)' and 'Line: 17' is selected. The right pane shows the 'Status' tab for the selected trunk. The 'SIP Trunk Summary' section displays various configuration details. Below this is a table with 10 channels, all of which are in an 'Idle' state. At the bottom of the interface, there are several control buttons for tracing, pausing, and managing the trunk's service state.


**AVAYA IP Office System Status**

Help Snapshot LogOff Exit About

**System**  
**Alarms (23)**  
**Extensions (3)**  
**Trunks (3)**  
 Line: 1  
 Line: 2  
**Line: 17**  
 Active Calls  
**Resources**  
**Voicemail**  
**IP Networking**  
 Locations

**Status** Utilization Summary Alarms

**SIP Trunk Summary**

Line Service State: In Service  
 Peer Domain Name:   
 Resolved Address: 251.179  
 Line Number: 17  
 Number of Administered Channels: 10  
 Number of Channels in Use: 0  
 Administered Compression: G711 Mu, G711 A, G729 A  
 Enable Faststart: Off  
 Silence Suppression: Off  
 Media Stream: RTP  
 Layer 4 Protocol: UDP  
 SIP Trunk Channel Licenses: 10  
 SIP Trunk Channel Licenses in Use: 0  0%  
 SIP Device Features: REFER (Incoming and Outgoing), UPDATE (Incoming and Outgoing)

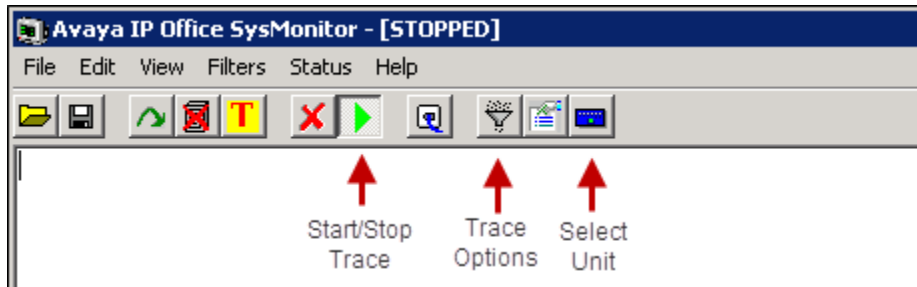
Cha...	U..	Call	Curr...	Time in	Remote	C...	Con...	Caller	Other	Dire...	Round	Rec...	Rec...	Tran...	Tran...
	Ref		State	Media...				ID o...	Party on...		Trip ...				
1			Idle	01:4...											
2			Idle	5 da...											
3			Idle	5 da...											
4			Idle	5 da...											
5			Idle	5 da...											
6			Idle	5 da...											
7			Idle	5 da...											
8			Idle	5 da...											
9			Idle	5 da...											
10			Idle	5 da...											

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

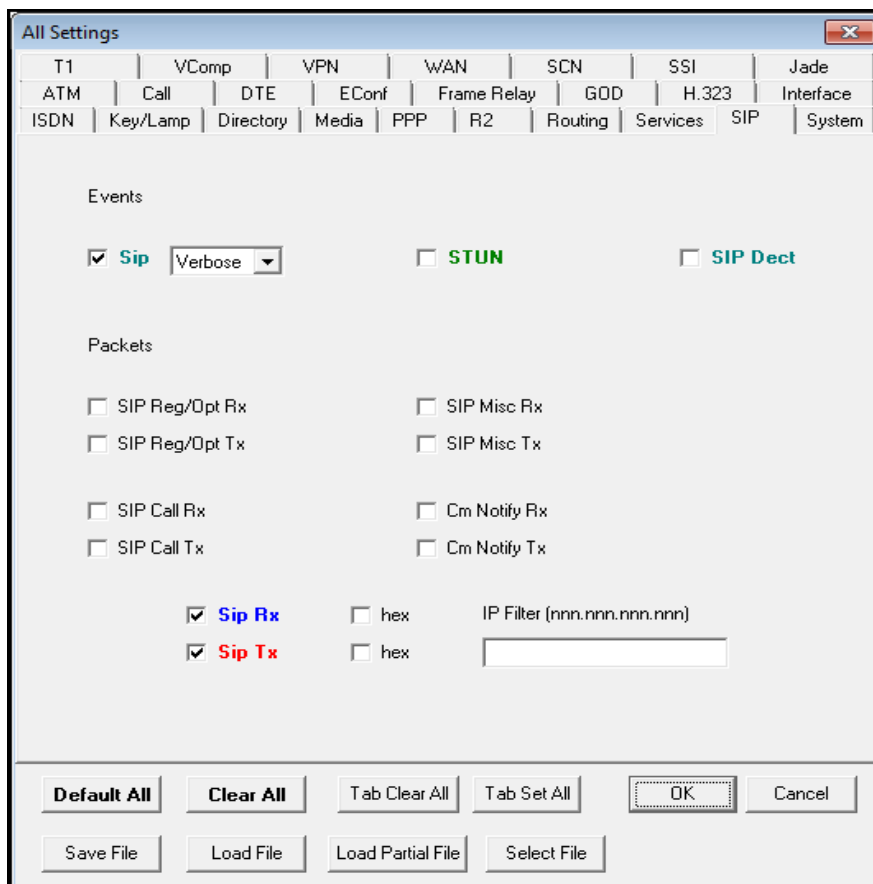
Print... Save As...

## 8.2. Monitor

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



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



## 9. Conclusion

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

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

## 10. Additional References

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

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

- [1] *Deploying IP Office Platform Server Edition, Release 11.1, Issue 14, April 2020*
- [2] *IP Office Platform 11.1, Deploying Avaya IP Office Servers as Virtual Machines, August 2020*
- [3] *Avaya IP Office Platform Server Edition Reference Configuration Release 11.1, Issue 2, May 2020*
- [4] *IP Office Platform 11.1, Deploying an IP500 V2 IP Office Basic Edition System, Issue 36g, September 10, 2020*
- [5] *IP Office Platform 11.1, Deploying an IP500 V2 IP Office Essential Edition System, Issue 36g, September 10, 2020*
- [6] *Administering Avaya IP Office Platform with Manager, Release 11.1 SP1, July 2020.*
- [7] *Administering Avaya IP Office Platform with Web Manager, Release 11.1 SP1, Issue 22, July 2020.*
- [8] *Avaya IP Office Platform Feature Description, Release 11.1, Issue 2, May 2020.*
- [9] *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac and Windows, August 2020*
- [10] *Using Avaya Avaya IX™ Workplace Client for Android, iOS, Mac and Windows, August 2020*

Additional Avaya IP Office documentation can be found at:

<https://ipofficekb.avaya.com/>



---

**©2020 Avaya Inc. All Rights Reserved.**

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interopnotesdl@avaya.com](mailto:interopnotesdl@avaya.com)