



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.1 to support BT Wholesale Hosted 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 11.1 to support BT Wholesale Hosted SIP Trunking Service. These Application Notes update previously published Application Notes with a newer software version of Avaya IP Office.

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

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between BT Wholesale Hosted SIP Trunking Service and an Avaya SIP-enabled enterprise solution.

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

The BT Wholesale Hosted 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”, “BT” or “BT Wholesale Hosted SIP Trunking Service” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the BT’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.

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

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

2.1. Interoperability Compliance Testing

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

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, Digital and Analog telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323, Digital and Analog telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider network.
- Incoming and outgoing PSTN calls to/from Avaya Workplace Client for Windows (SIP).
- 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.722 64K, G.711A, G.729(a) and G.711U, BT's preferred codec order.
- Proper response to no matching codecs.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- 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.
- Outbound calls to the BT SIP platform using Class 5 CLIP.
- Voice Recording.
- Auto Attendant.

Items not supported or not tested included the following:

- REFER message for call redirection was not tested for reasons noted under **Section 2.2**.
- T.38 and G.711 passthrough fax are supported but were not tested.
- Inbound and Outbound toll-free calls were not tested.
- 0, 0+10 digits, 411 Directory Assistance and 911 Emergency calls were not tested.
- Outbound international calls were not tested.

2.2. Test Results

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

- **Call transfers using the SIP REFER method:** Calls that were transferred to the network enforcing the use of the SIP REFER method did not work properly (with SIP REFER set to **Always**). The compliance test was done with SIP REFER set to **Auto** in Avaya IP Office. With the SIP REFER method set to **Auto** (**Section 5.4.2**), the **Allow** header of the OPTIONS response message is used to determine if the endpoint supports REFER. With it set to **Auto** SIP REFER was not used, call transfers worked properly.
- **DNS-SRV – Failover is not supported:** With IP Office configured to use DNS/SRV record queries (FQDN under **Line→Transport→ITSP Proxy Address**), it was observed that IP Office would not failover to the secondary SIP server when a fault was introduced into the primary SIP server, as expected. It was observed that IP Office would only failover to the secondary server if the IPs for the primary and secondary SIP servers are added under **Line→Transport→ITSP Proxy Address**, separated by commas. This issue is under investigation by Avaya.
- **DNS-SRV – IP Office did not attempt to fall back to the secondary SIP server when receiving 503 Service Unavailable response:** With IP Office configured to use DNS/SRV record queries (FQDN under **Line→Transport→ITSP Proxy Address**) or with the IPs for the primary and secondary SIP servers under **Line→Transport→ITSP Proxy Address**, separated by commas, IP Office did not attempt to fall back to the secondary SIP server after receiving **503 Service Unavailable** response to SIP INVITE messages. This issue is under investigation by Avaya.
- **DNS-SRV – Failover is supported but no fall back to primary SIP server:** With IP Office configured to use DNS/SRV record queries (FQDN under **Line→Transport→ITSP Proxy Address**) or with the IPs for the primary and secondary SIP servers under **Line→Transport→ITSP Proxy Address**, separated by commas, it was observed that IP Office would failover to the secondary SIP server when a fault was introduced into the primary SIP server, as expected, but no fall back to the primary SIP server was attempted after the primary SIP server was back in service, IP Office would fallback to primary only when secondary goes Out Of Service. This issue is under investigation by Avaya.
- **DNS-SRV – SIP INVITE did not trigger fail-over:** With IP Office configured to use DNS/SRV record queries (FQDN under **Line→Transport→ITSP Proxy Address**) or with the IPs for the primary and secondary SIP servers under **Line→Transport→ITSP Proxy Address**, separated by commas, it was observed that SIP INVITEs did not triggered the fail-over to occur, IP Office would only fail-over when the register timer expired. This issue is under investigation by Avaya.
- **SIP OPTIONS Messages:** During the compliance test BT did not send SIP OPTIONS messages to IP Office, IP Office did send SIP OPTIONS messages to BT. This was sufficient to keep the SIP trunk up in-service.

2.3. Support

For support on BT Wholesale Hosted SIP Trunking Service visit the corporate Web page at:
<https://www.btwholesale.com/pages/static/home.htm>

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

The transport protocols on the SIP trunk between IP Office and BT, 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 BT's network. The short code 9 was stripped off by Avaya IP Office, but the remaining N digits were sent unaltered to BT's network.

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

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

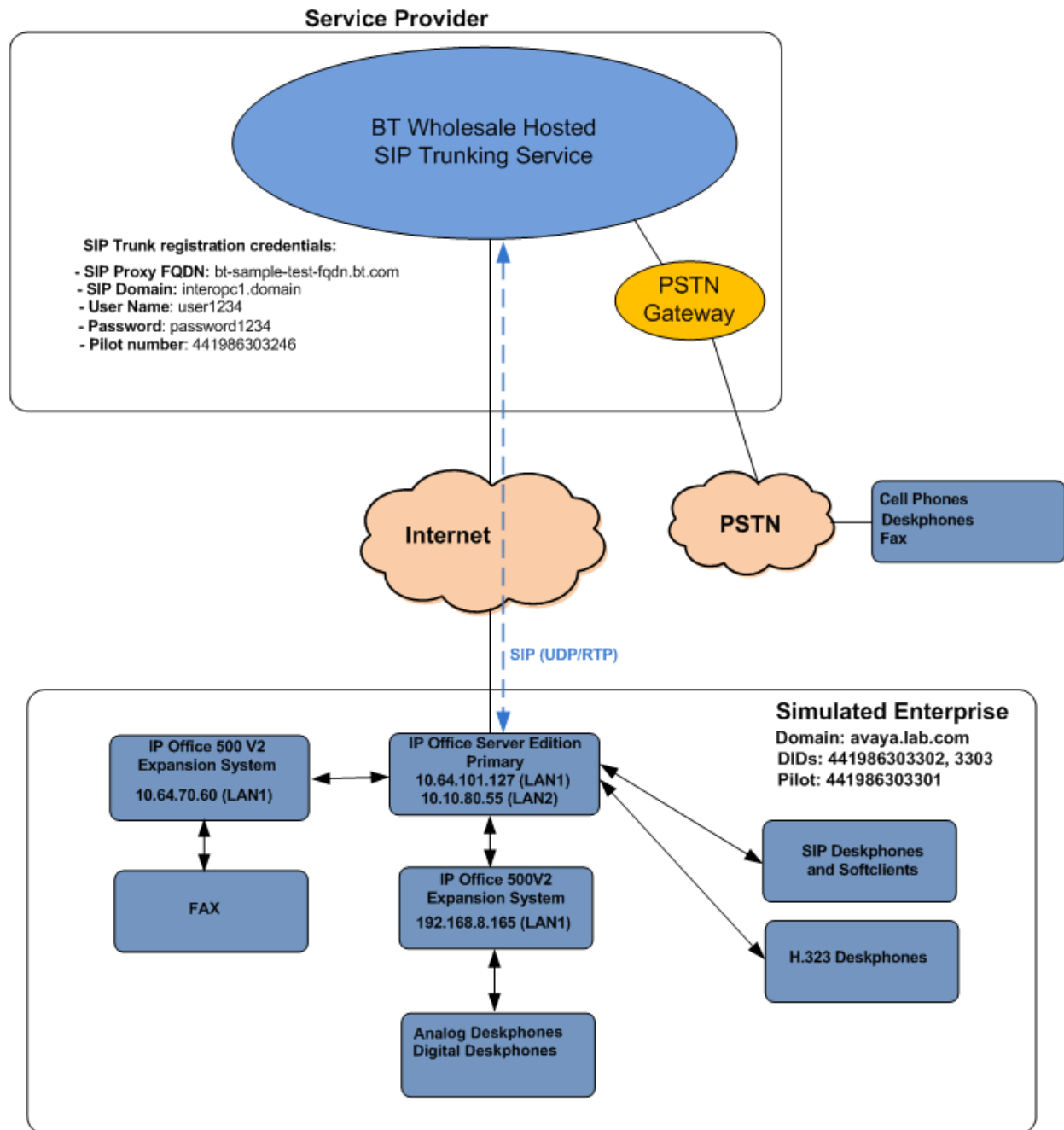


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server)	11.1.1.1.0 Build 18
• Avaya IP Office Voicemail Pro	11.1.1.1.0 Build 6
Avaya IP Office IP500 V2 (Expansion Systems)	11.1.1.1.0 Build 18
Avaya IP Office Manager	11.1.1.1.0 Build 18
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)	4.0.7.0.7
Avaya 1408 Digital Telephone	48.02
Avaya Workplace Client for Windows (SIP)	3.22.0.64
Analog Telephone	---
BT Wholesale Hosted SIP Trunking Service	
Acme Packet 6350	SCZ8.4p7k
OpenSIPS Session Border Controller	22

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.

The screenshot displays the Avaya IP Office Manager application interface. At the top, there is a table with columns: Name, IP Address, Type, Version, and Edition. Below the table, a modal dialog box titled "Configuration Service User Login" is open. The dialog contains the following fields and controls:

- IP Office:** IPOSE-Primary (Primary System - IPO-Linux-PC)
- Service User Name:** Administrator
- Service User Password:** (Empty text box)
- Buttons:** OK, Cancel, Help

Below the dialog, the main application window shows a "TCP Discovery Progress" bar and a "Unit/Broadcast Address" section. The "Unit/Broadcast Address" section includes a checkbox labeled "Open with Server Edition Manager" which is checked, a dropdown menu showing "10.64.101.127", a "Refresh" button, and "OK" and "Cancel" buttons at the bottom right.

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.

Avaya IP Office Select Manager for Server Edition IPOSE-Primary [11.1.1.1.0 build 18]

File Edit View Tools Help

Configuration

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

Server Edition

Summary

Server Edition Primary

Hardware Installed

- Control Unit: IPO-Linux-PC
- Secondary Server: NONE
- Expansion Systems: 10.64.70.60; 192.168.8.165
- System Identification: 8de6c6d337bc354d6ec88494533af87bb2d6e950

System Settings

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

Open...

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

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	192.168.8.165	Bothway		25	24
Expansion System	IP500V2-Two	10.64.70.60	Bothway		1	24

Ready

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, **100 SIP Trunk Sessions** licenses were reserved to be used by the Primary Server.

Configuration

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

License Remote Server

Remote Server Configuration

License SourceWebLM
Domain Name (URL)10.64.101.127
PathWebLM/LicenseServer
Port Number52233
WebLM Client ID
WebLM Node ID-IPOSE-Primary

Reserved Licenses

SIP Trunk Sessions	100	Server Edition	1
SM Trunk Sessions	0	Avaya IP Endpoints	6
Voicemail Pro Ports	152	3rd Party IP Endpoints	0
VMPRO Recordings Administrators	0	Receptionist	0
VMPRO TTS Professional	1	Basic User	5
CTI Link Pro	1	Office Worker	0
UMS Web Services	1	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 BT.

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 IP Office configuration interface. On the left is a tree view under the 'Configuration' header, listing various system components such as BOOTP (4), Operator (3), Solution, User (32), Group (2), Short Code (48), Directory (0), Time Profile (0), Account Code (0), User Rights (9), Location (1), IPOSE-Primary, System (1), IPOSE-Primary, Line (4), Control Unit (8), Extension (6), User (7), Group (0), Short Code (3), Service (0), Incoming Call Route (2), IP Route (4), License (9), ARS (2), Location (1), Authorization Code (0), IP500V2-One, and IP500V2-Two. The 'IPOSE-Primary' item is selected. On the right, the 'IPOSE-Primary' configuration panel is shown with tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, and System Events. The 'LAN2' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The 'IP Address' field is set to '10 . 10 . 80 . 55' and the 'IP Mask' field is set to '255 . 255 . 255 . 128'. The 'Number Of DHCP IP Addresses' is set to '200'. Under 'DHCP Mode', the 'Disabled' radio button is selected. An 'Advanced' button is located at the bottom right of the LAN Settings section.

5.2.1.2 LAN2 VoIP Tab

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

The screenshot shows the IPOSE-Primary configuration interface. On the left is a 'Configuration' tree with a hierarchy: BOOTP (4) → Operator (3) → Solution → User (32) → Group (2) → Short Code (48) → Directory (0) → Time Profile (0) → Account Code (0) → User Rights (9) → Location (1) → IPOSE-Primary → System (1) → IPOSE-Primary. The main pane is titled 'IPOSE-Primary*' and has tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. The 'LAN2' tab is selected, and within it, the 'VoIP' sub-tab is active. The 'LAN Settings' section includes checkboxes for 'H.323 Gatekeeper Enable', 'Auto-create Extension', 'Auto-create User', and 'H.323 Remote Extension Enable'. Below these is a dropdown for 'H.323 Signaling over TLS' set to 'Disabled' and a 'Remote Call Signaling Port' set to '1720'. The 'SIP Trunks Enable' checkbox is checked. Below this is the 'SIP Registrar Enable' checkbox, which is unchecked. There are also checkboxes for 'Auto-create Extension/User', 'SIP Remote Extension Enable', and a button for 'Allowed SIP User Agents' with a 'Block blacklist only' option. Fields for 'SIP Domain Name' and 'SIP Registrar FQDN' are present. The 'Layer 4 Protocol' section has checkboxes for 'UDP', 'TCP', and 'TLS'. For each, there are 'Port' and 'Remote Port' dropdowns: UDP (5060, 5060), TCP (5060, 5060), and TLS (5061, 5061). A 'Challenge Expiration Time (sec)' is set to '10'. The 'RTP' section has a 'Port Number Range' with 'Minimum' set to '40750' and 'Maximum' set to '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).

Configuration

IPOSE-Primary*

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

LAN Settings VoIP Network Topology

SIP Registrar FQDN

Layer 4 Protocol

Challenge Expiration Time (sec)

RTP

Port Number Range

Minimum 40750 Maximum 50750

Port Number Range (NAT)

Minimum 40750 Maximum 40750

Enable RTCP Monitoring on Port 5005

RTCP collector IP address for phones 0.0.0.0

Keepalives

Scope RTP-RTCP Periodic timeout 30

Initial keepalives Enabled

DiffServ Settings

B8 DSCP(Hex) B8 Video DSCP (Hex) FC DSCP Mask (Hex) 88 SIG DSCP (Hex)

46 DSCP 46 Video DSCP 63 DSCP Mask 34 SIG DSCP

DHCP Settings

Primary Site Specific Option Number (SSON) 176

Secondary Site Specific Option Number (SSON) 242

VLAN Not Present

1100 Voice VLAN Site Specific Option Number (SSON) 232

1100 Voice VLAN IDs

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 BT Wholesale Hosted 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).

The screenshot displays the Avaya IP Office 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, and IPOSE-Primary. The main pane is titled 'IPOSE-Primary*' and contains several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and Contact Center. The 'LAN2' tab is active, and within it, the 'Network Topology' sub-tab is selected. The 'Network Topology Discovery' section contains the following fields and controls:

- STUN Server Address:** An empty text input field.
- STUN Port:** A numeric input field set to 3478.
- Firewall/NAT Type:** A dropdown menu set to 'Open Internet'.
- Binding Refresh Time (sec):** A numeric input field set to 60.
- Public IP Address:** A text input field containing '0 . 0 . 0 . 0'.
- Public Port:** A section with three sub-fields: UDP (5060), TCP (5060), and TLS (5061).
- Run STUN on startup:** An unchecked checkbox.

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

5.2.2. System - DNS Tab

Public DNS servers IP addresses are required to be configured; IP Office will retrieve BT's Proxy IP Addresses via public DNS queries using BT's FQDN defined in **Section 5.4.3**. The FQDN should be provided by BT. 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 BT.
- Click **OK** to commit (not shown).

The screenshot shows the 'Configuration' window for 'IPOSE-Primary'. The left pane displays a tree view of the configuration hierarchy, with 'System (1)' > 'IPOSE-Primary' selected. The right pane shows the 'DNS' tab with the following fields:

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				<input type="text"/>			

5.2.3. Telephony Tab

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

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

The screenshot displays the IPOSE-Primary* Configuration window, specifically the Telephony tab. The left pane shows a tree view of the system configuration, including BOOTP (4), Operator (3), Solution, User (32), Group(2), Short Code(48), Directory(0), Time Profile(0), Account Code(0), User Rights(9), Location(1), IPOSE-Primary, System (1), IPOSE-Primary, Line (4), Control Unit (8), Extension (6), User (7), Group (0), Short Code (3), Service (0), Incoming Call Route (2), IP Route (4), License (9), ARS (2), Location (1), Authorization Code (0), IP500V2-One, and IP500V2-Two.

The main pane shows the following settings:

- System** tab selected.
- Telephony** sub-tab selected.
- Dial Delay Time (sec)**: 4
- Dial Delay Count**: 0
- Default No Answer Time (sec)**: 15
- Hold Timeout (sec)**: 0
- Park Timeout (sec)**: 300
- Ring Delay (sec)**: 5
- Call Priority Promotion Time (sec)**: Disabled
- Default Currency**: USD
- Default Name Priority**: Favor Directory
- Media Connection Preservation**: Enabled
- Phone Failback**: Automatic
- Login Code Complexity**:
 - ☒ Enforcement
 - Minimum length**: 6
 - ☒ Complexity
- RTCP Collector Configuration**:
 - ☐ Send RTCP to an RTCP Collector
 - Server Address**: 0 . 0 . 0 . 0
 - UDP Port Number**: 5005
 - RTCP reporting interval (sec)**: 5

The **Companding Law** section shows:

- Switch**:
 - ☒ U-Law
 - ☐ A-Law
- Line**:
 - ☒ U-Law Line
 - ☐ A-Law Line

Other settings include:

- ☐ DSS Status
- ☐ Auto Hold
- ☒ Dial By Name
- ☒ Show Account Code
- ☐ Inhibit Off-Switch Forward/Transfer
- ☐ Restrict Network Interconnect
 - ☐ Include location specific information
- ☒ Drop External Only Impromptu Conference
- ☐ Visually Differentiate External Call
- ☒ High Quality Conferencing
- ☒ Directory Overrides Barring
- ☐ Advertise Callee State To Internal Callers
- ☐ Internal Ring on Transfer

5.2.4. VoIP Tab

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

5.2.4.1 VoIP - VoIP Tab

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

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

The screenshot displays the IPOSE-Primary configuration window. The left-hand pane shows a hierarchical tree of configuration options, with 'IPOSE-Primary' expanded. The right-hand pane is titled 'IPOSE-Primary*' and contains several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. The 'VoIP' tab is active, showing sub-tabs for 'VoIP Security' and 'Access Control Lists'. Under 'VoIP Security', there are checkboxes for '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 is set to '101'. The 'Default Codec Selection' section contains two lists: 'Available Codecs' and 'Selected'. The 'Available Codecs' list has four items, all checked: G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, and G.729(a) 8K CS-A. The 'Selected' list also has four items: G.711 ALAW 64K, G.711 ULAW 64K, G.722 64K, and G.729(a) 8K CS-A. Between the two lists are five buttons: '>>>', '<<<', '<<<', '>>>', and '>>>'. The first and last buttons are disabled, while the middle three are active.

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

5.2.4.2 VoIP – VoIP Security Tab

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

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

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

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

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

- Set the **Media Security** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption.
- Verify **Strict SIPS** is not checked.
- Under **Media Security Options**, select **RTP** for the **Encryptions** and **Authentication** fields.
- Under **Crypto Suites**, select **SRTP_AES_CM_128_SHA1_80**.
- Click **OK** to commit (not shown).

The screenshot displays the IPOSE-Primary configuration window. On the left is a 'Configuration' tree with a hierarchy including BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line, Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, and IP500V2-One/Two. The main panel on the right is titled 'IPOSE-Primary*' and contains several tabs: LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. The 'VoIP' tab is active, and within it, the 'VoIP Security' sub-tab is selected. The 'Access Control Lists' sub-tab is also visible. The 'Default Extension Password' and 'Confirm Default Extension Password' fields are present. The 'Media' dropdown is set to 'Preferred', and the 'Strict SIPS' checkbox is unchecked. The 'Media Security Options' section includes 'Encryptions' (RTP checked, RTCP unchecked), 'Authentication' (RTP checked, RTCP checked), 'Replay Protection' (unchecked), and 'SRTP Window Size' (set to 64). The 'Crypto Suites' section shows 'SRTP_AES_CM_128_SHA1_80' checked and 'SRTP_AES_CM_128_SHA1_32' unchecked.

5.3. IP Route

Create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to route calls to BT'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).

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

5.4. SIP Line

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

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

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

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

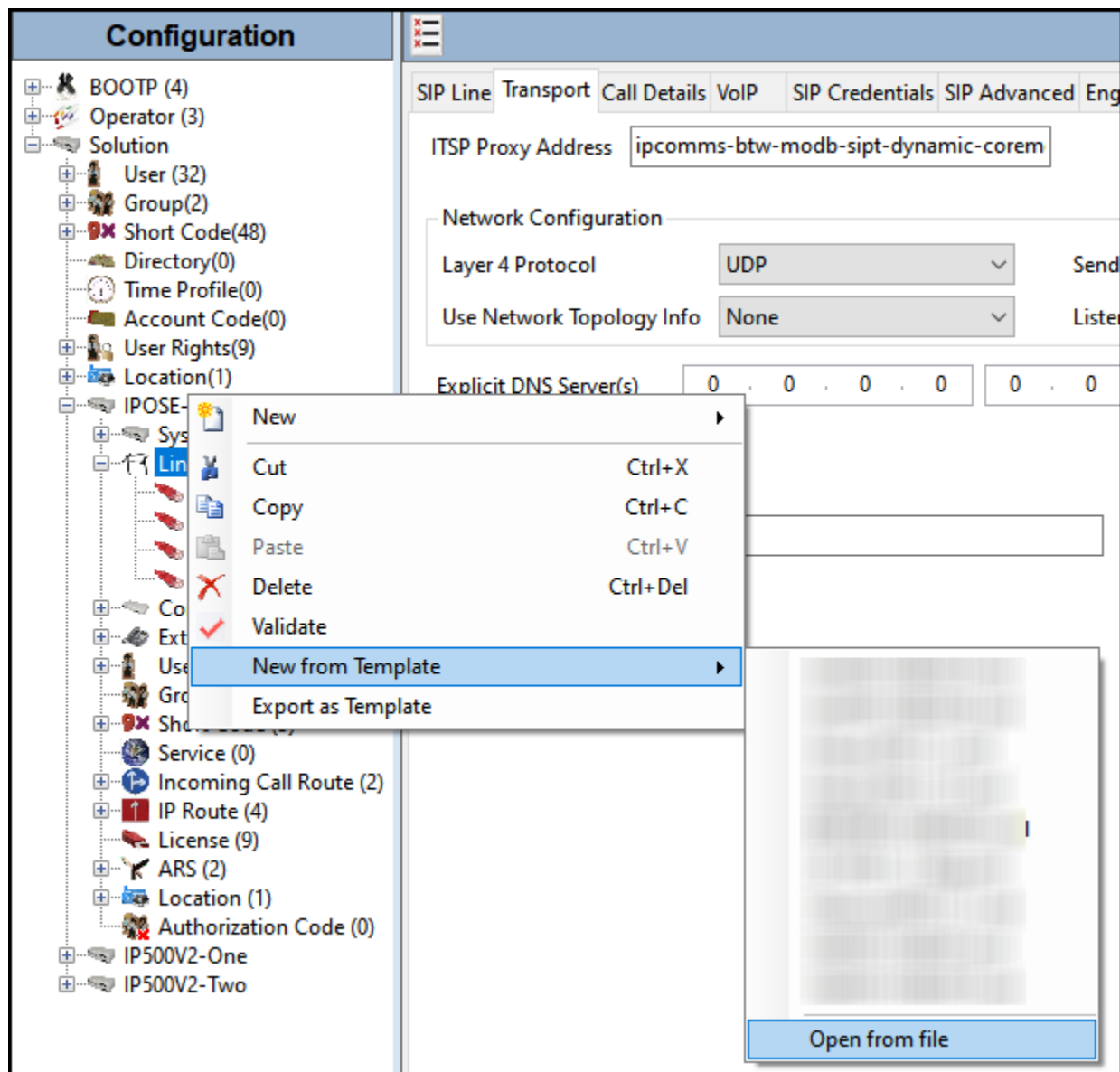
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.7**.

5.4.1. Creating a SIP Trunk from an XML Template

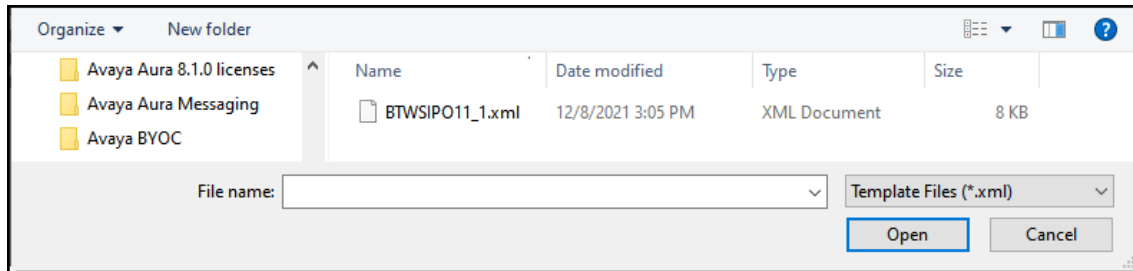
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and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

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

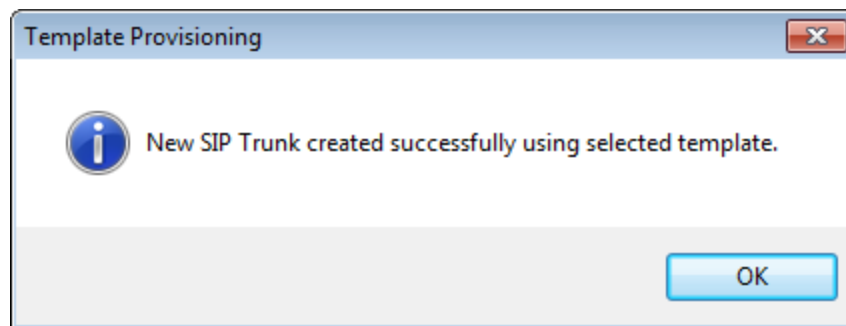
To create the SIP Trunk from the template, from the **Primary** server (**IPOSE-Primary**), right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template → Open from file**.



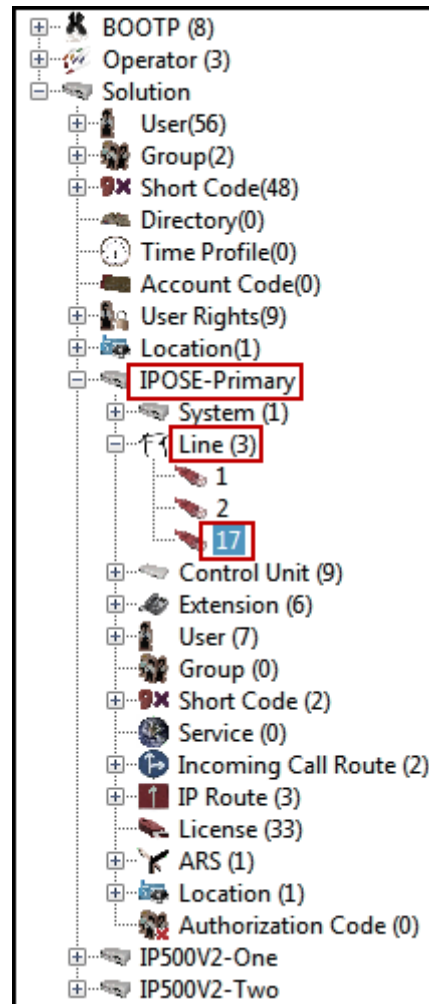
Navigate to the directory on the local machine where the template was copied and select the template.



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



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

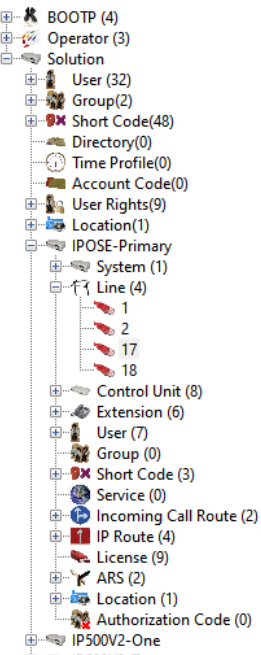


It is important that the SIP Line configuration be reviewed and updated if necessary, after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2 to 5.4.7**.

5.4.2. SIP Line – SIP Line Tab

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

- Set **ITSP Domain Name** to **interopc1.domain**, the domain name provided by BT.
- 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**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Auto** (refer to **Section 2.2**).
- Click **OK** to commit (not shown).

Configuration	SIP Line - Line 17	
	<div><div>SIP Line</div><div>Transport</div><div>Call Details</div><div>VoIP</div><div>SIP Credentials</div><div>SIP Advanced</div><div>Engineering</div></div> <div>Line Number: 17</div> <div>ITSP Domain Name: interopc1.domain</div> <div>Local Domain Name: </div> <div>URI Type: SIP URI</div> <div>Location: Cloud</div> <div>Prefix: 1</div> <div>National Prefix: </div> <div>International Prefix: </div> <div>Country Code: </div> <div>Name Priority: System Default</div> <div>Description: Service Provider</div>	<div>In Service: <input checked="" type="checkbox"/></div> <div>Check OOS: <input checked="" type="checkbox"/></div> <div>Session Timers</div> <div>Refresh Method: Auto</div> <div>Timer (sec): On Demand</div> <div>Redirect and Transfer</div> <div>Incoming Supervised REFER: Auto</div> <div>Outgoing Supervised REFER: Auto</div> <div>Send 302 Moved Temporarily: <input type="checkbox"/></div> <div>Outgoing Blind REFER: <input type="checkbox"/></div>

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 the FQDN to be used to retrieve BT's Proxy IP addresses via public DNS queries (**Sections 2.2** and **Section 5.2.2**). The FQDN should be provided by BT.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **None** (refer to the note below).
- Set the **Send Port** and **Listen Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view under the 'Configuration' header, showing a hierarchy of system components including BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line (with sub-items 1, 2, 17, 18), Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, and two IP500V2 endpoints. The main panel on the right is titled 'SIP Line - Line 17' and contains several tabs: 'SIP Line', 'Transport' (which is selected), 'Call Details', 'VoIP', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'Transport' tab shows the following configuration: 'ITSP Proxy Address' is set to 'bt-sample-test-fqdn.bt.com'; under 'Network Configuration', 'Layer 4 Protocol' is set to 'UDP' and 'Send Port' is '5060'; 'Use Network Topology Info' is set to 'None' and 'Listen Port' is '5060'; 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0'; 'Calls Route via Registrar' is checked; and 'Separate Registrar' is an empty text field.

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

5.4.4. SIP Line – SIP Credentials Tab

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

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

The screenshot displays the 'SIP Line - Line 17*' configuration window. The left sidebar shows a tree view of the system configuration, with 'Line (4)' selected. The main window has tabs for 'SIP Line', 'Transport', 'Call Details', 'VoIP', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'SIP Credentials' tab is active, showing a table with the following data:

Index	User Name	Authentication Name	Contact	Expiration (mins)	Register
1	user1234	auth_name	441986303246	60	True

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

- User name: user1234
- Authentication Name: auth_name
- Contact: 441986303246
- 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 window.

5.4.5. SIP Line – Call Details Tab

Select the **Call Details** tab, and then click the **Add...** button (not shown) and the screen shown below will appear. To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button. In the example screen below one new entry was added, for incoming calls and outgoing calls both.

The entry for calls from IP Office to the PSTN (outgoing calls) was created with the parameters shown below:

- Associate this entry 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 from this line. For the compliance test outgoing group **17** was used. The **Incoming Group** was also set as **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	Use Internal Data	Use Internal Data	Caller	Original Caller	Called
Contact	Use Internal Data	Use Internal Data	Caller	Original Caller	Called
P Asserted ID	<input checked="" type="checkbox"/> Use Internal Data	Use Internal Data	Caller	Original Caller	Called
P Preferred ID	<input type="checkbox"/> None	None	None	None	None
Diversion Header	<input checked="" type="checkbox"/> Use Internal Data	Use Internal Data	Caller	Original 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. BT supports codecs **G.722 64K**, **G.711ALAW**, **G.729(a)** and **G.711ULAW** for audio.
- Select **T.38** for **Fax Transport Support** (refer to **Section 2.1**).
- 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.
- Set the **Media Security** to **Disabled**.
- 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 window for 'SIP Line - Line 17*'. The 'VoIP' tab is active. On the left is a tree view of the system configuration. The main area contains the following settings:

- Codec Selection:** Set to 'Custom'. Below this are two lists: 'Unused' (empty) and 'Selected'. The 'Selected' list contains: G.722 64K, G.711 ALAW 64K, G.729(a) 8K CS-ACELP, and G.711 ULAW 64K. Arrows between the lists allow for reordering.
- Fax Transport Support:** Set to 'T38'.
- DTMF Support:** Set to 'RFC2833/RFC4733'.
- Media Security:** Set to 'Disabled'.
- Checkboxes on the right:**
 - ☐ 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:

- Check the box for **Use PAI for Privacy**.
- Check the box for **Use Domain for PAI**.
- Leave remaining fields as default.
- Click **OK** to commit (not shown).

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

The main configuration area is divided into three sections:

- Addressing:**
 - Association Method: By Source IP address (dropdown)
 - Call Routing Method: Request URI (dropdown)
 - Use P-Called-Party: ☐
 - Suppress DNS SRV Lookups: ☐
- Identity:**
 - Use "phone-context": ☐
 - Add user=phone: ☐
 - Use + for International: ☐
 - Use PAI for Privacy: ☒
 - Use Domain for PAI: ☒
 - Caller ID from From header: ☐
 - Send From In Clear: ☐
 - Cache Auth Credentials: ☒
 - User-Agent and Server Headers:
 - Send Location Info: Never (dropdown)
 - Add UUI header: ☐
 - Add UUI header to redirected calls: ☐
- Media:**
 - Allow Empty INVITE: ☐
 - Send Empty re-INVITE: ☐
 - Allow To Tag Change: ☐
 - P-Early-Media Support: None (dropdown)
 - Send SilenceSupp=Off: ☐
 - Force Early Direct Media: ☐
 - Media Connection Preservation: System (dropdown)
 - Indicate HOLD: ☐
- Call Control:**
 - 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: ☐

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 BT. 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. On the left, the 'Configuration' pane shows a hierarchical tree of system components. Under 'User (7)', the user '3041 Ext3041 H323' is selected. The right pane, titled 'Ext3041 H323: 3041', shows the configuration details for this user. The 'SIP' tab is active, displaying the following fields:

Dial In	Voice Recording	Button Programming	Menu Programming	Mobility	Group Membership
SIP Name					
441986303248					
SIP Display Name (Alias)					
Ext3041 H323					
Contact					
441986303248					
<input type="checkbox"/> Anonymous					

5.6. IP Office Line – Primary Server

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

The screenshot displays the 'IP Office Line - Line 1' configuration window. On the left is a 'Configuration' navigation pane showing a tree structure of system components. The main area on the right is divided into tabs: 'Line', 'Short Codes', and 'VoIP Settings'. The 'Line' tab is active, showing various configuration fields. The 'Gateway' section includes an 'Address' field with the value '192 . 168 . 8 . 165' and a 'Location' dropdown set to '3: Thornton, CO'. Below these are 'Password' and 'Confirm Password' fields, both masked with dots. To the right of the password fields is a 'SCN Resiliency Options' section with four checkboxes: 'Supports Resiliency', 'Backs up my IP phones', 'Backs up my hunt groups', and 'Backs up my voicemail'. The 'Outgoing Channels' field is set to '250'. At the bottom is a 'Description' field.

IP Office Line - Line 1	
Line Number	1
Transport Type	WebSocket Server
Networking Level	SCN
Security	Medium
Telephone Number	
Prefix	
Outgoing Group ID	99999
Number of Channels	250
Outgoing Channels	250
Gateway	
Address	192 . 168 . 8 . 165
Location	3: Thornton, CO
Password
Confirm Password
SCN Resiliency Options	
<input type="checkbox"/> Supports Resiliency	
<input type="checkbox"/> Backs up my IP phones	
<input type="checkbox"/> Backs up my hunt groups	
<input type="checkbox"/> Backs up my voicemail	
<input type="checkbox"/> Backs up my IP DECT phones	
Description	

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

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **T.38** for **Fax Transport Support** (refer to **Section 2.1**).
- Under **Media Security** verify **Same as System (Preferred)** is selected (default value).
- On the **Advanced Media Security Options** check **Same As System**.

Configuration

- BOOTP (4)
- Operator (3)
- Solution
 - User (32)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - System (1)
 - Line (4)
 - 1
 - 2
 - 17
 - 18
 - Control Unit (8)
 - Extension (6)
 - User (7)
 - Group (0)
 - Short Code (3)
 - Service (0)
 - Incoming Call Route (2)
 - IP Route (4)
 - License (9)
 - ARS (2)
 - Location (1)
 - Authorization Code (0)
 - IP500V2-One
 - IP500V2-Two

IP Office Line - Line 1

Line Short Codes VoIP Settings

Out Of Band DTMF ☒ Allow Direct Media Path ☒

Codec Selection System Default

Unused Selected

G.711 ALAW 64K
G.711 ULAW 64K
G.722 64K
G.729(a) 8K CS-ACELP

Fax Transport Support T38

Call Initiation Timeout (s) 4

Media Security Same as System (Preferred)

Advanced Media Security Options ☒ Same As System

Encryptions ☒ RTP ☐ RTCP

Authentication ☒ RTP ☒ RTCP

Replay Protection
SRTP Window Size 64

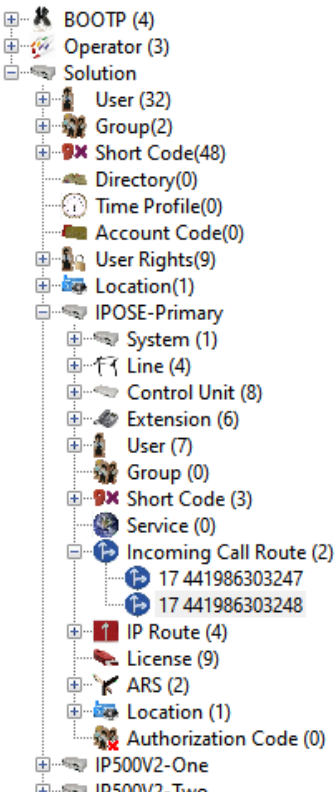
Crypto Suites
☒ SRTP_AES_CM_128_SHA1_80
☐ SRTP_AES_CM_128_SHA1_32

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

5.7. Incoming Call Route

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

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

Configuration	17 441986303248																				
	<div>Standard Voice Recording Destinations</div> <table><tr><td>Bearer Capability</td><td>Any Voice</td></tr><tr><td>Line Group ID</td><td>17</td></tr><tr><td>Incoming Number</td><td>441986303248</td></tr><tr><td>Incoming Sub Address</td><td></td></tr><tr><td>Incoming CLI</td><td></td></tr><tr><td>Locale</td><td></td></tr><tr><td>Priority</td><td>1 - Low</td></tr><tr><td>Tag</td><td></td></tr><tr><td>Hold Music Source</td><td>System Source</td></tr><tr><td>Ring Tone Override</td><td>None</td></tr></table>	Bearer Capability	Any Voice	Line Group ID	17	Incoming Number	441986303248	Incoming Sub Address		Incoming CLI		Locale		Priority	1 - Low	Tag		Hold Music Source	System Source	Ring Tone Override	None
Bearer Capability	Any Voice																				
Line Group ID	17																				
Incoming Number	441986303248																				
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 441986303248 provided by BT was associated with the Avaya IP Office extension **3041**.

The screenshot shows the Avaya IP Office configuration interface. On the left is a 'Configuration' tree with various nodes like BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line, Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, ARS, Location, Authorization Code, and IP500V2-One/Two. The 'Incoming Call Route' node is expanded, showing two entries: '17 441986303247' and '17 441986303248'. The '17 441986303248' entry is selected. On the right, the 'Destinations' tab is active for the selected entry. It shows a table with columns: TimeProfile, Destination, and Fallback Extension. The table has one row with 'Default Value' in the TimeProfile column, '3041 Ext3041 H323' in the Destination column, and a dropdown arrow in the Fallback Extension column.

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.).

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.

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.

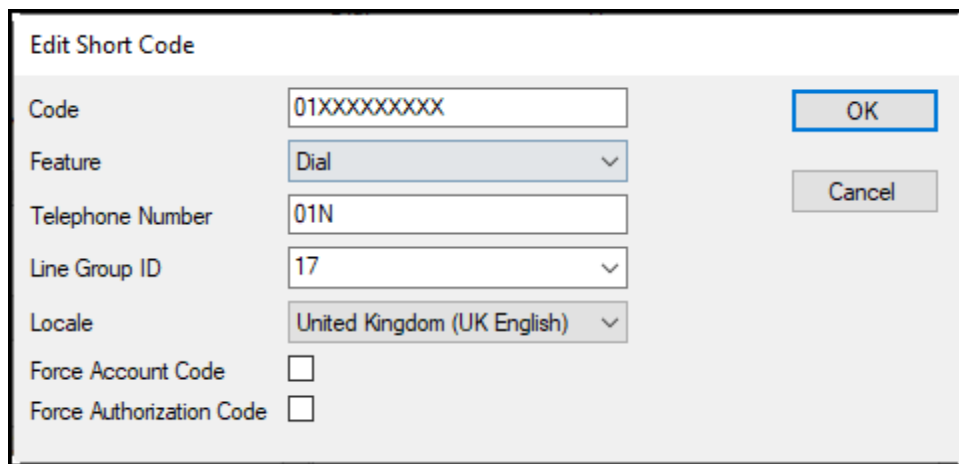
- | Configuration | | 9N: Dial Plan | | | | | | | | | | | | | | | |
|--|-----------------------------|---|--|------|----|---------|------|------------------|---|---------------|----------|--------|-----------------------------|--------------------|--------------------------|--------------------------|--------------------------|
| <ul style="list-style-type: none"> + BOOTP (4) + Operator (3) <ul style="list-style-type: none"> - Solution <ul style="list-style-type: none"> + User(32) + Group(2) + Short Code(48) <ul style="list-style-type: none"> - Directory(0) - Time Profile(0) - Account Code(0) + User Rights(9) - Location(1) - IPOSE-Primary <ul style="list-style-type: none"> - System (1) - Line (4) <ul style="list-style-type: none"> - Control Unit (8) - Extension (6) - User (7) - Group (0) - Short Code (3) <ul style="list-style-type: none"> - *66*N# - 8N - 9N - Service (0) - Incoming Call Route (2) - IP Route (4) - License (9) - ARS (2) - Location (1) - Authorization Code (0) - IP500V2-One - IP500V2-Two | | <p>Short Code</p> <table border="1"> <tr> <td>Code</td> <td>9N</td> </tr> <tr> <td>Feature</td> <td>Dial</td> </tr> <tr> <td>Telephone Number</td> <td>N</td> </tr> <tr> <td>Line Group ID</td> <td>50: Main</td> </tr> <tr> <td>Locale</td> <td>United Kingdom (UK English)</td> </tr> <tr> <td>Force Account Code</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Force Authorization Code</td> <td><input type="checkbox"/></td> </tr> </table> | | Code | 9N | Feature | Dial | Telephone Number | N | Line Group ID | 50: Main | Locale | United Kingdom (UK English) | Force Account Code | <input type="checkbox"/> | Force Authorization Code | <input type="checkbox"/> |
| Code | 9N | | | | | | | | | | | | | | | | |
| Feature | Dial | | | | | | | | | | | | | | | | |
| Telephone Number | N | | | | | | | | | | | | | | | | |
| Line Group ID | 50: Main | | | | | | | | | | | | | | | | |
| Locale | United Kingdom (UK English) | | | | | | | | | | | | | | | | |
| Force Account Code | <input type="checkbox"/> | | | | | | | | | | | | | | | | |
| Force Authorization Code | <input type="checkbox"/> | | | | | | | | | | | | | | | | |

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

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

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **01** followed by **9 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 **01N**. The value **N** represents the additional number of digits dialed by the user after dialing **01** (The **9** will be stripped off).
- Set the **Line Group Id** to the Line Group number being used for the SIP Line, in this case **Line Group ID 17** was used.
- For **Locale**, **United Kingdom (UK English)** was used. Click **OK** to commit.

The following example shows the dial pattern for calls within the UK.



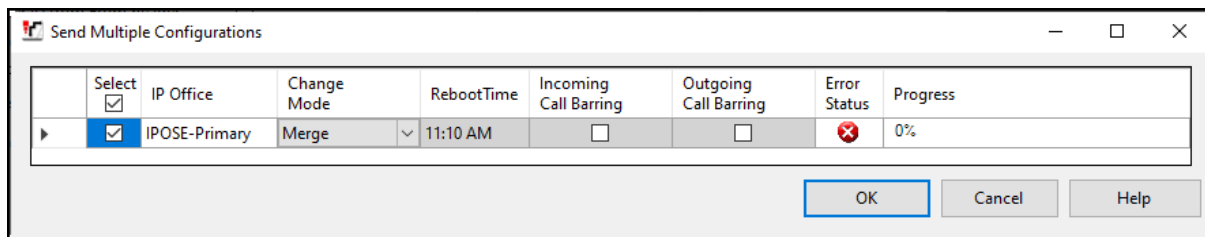
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

5.9. Save IP Office Primary Server Configuration

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

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

Click **OK** to execute the save.



6. Avaya IP Office Expansion System Configuration

Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials. Clicking the “plus” sign next to **IP500V2-One** on the left navigation pane will expand the menu on this server.

Configuration	System Inventory
<ul style="list-style-type: none">BOOTP (4)Operator (3)Solution<ul style="list-style-type: none">User(32)Group(2)Short Code (48)Directory(0)Time Profile(0)Account Code(0)User Rights(9)Location(1)IPOSE-PrimaryIP500V2-One<ul style="list-style-type: none">System (1)Line (3)Control Unit (4)Extension (24)User (27)Group (1)Short Code (12)Service (0)RAS (1)Incoming Call Route (1)WAN Port (0)Firewall Profile (1)IP Route (3)License (2)Tunnel (0)ARS (2)Location (1)Authorization Code (0)IP500V2-Two	<h3>Server Edition Expansion System</h3> <ul style="list-style-type: none">Hardware Installed<ul style="list-style-type: none">Control Unit: IP 500 V2Internal Modules: VCM64/PRID U; PHONE8Expansion Modules: DIG DCPx16 V2System Settings<ul style="list-style-type: none">IP Address: 192.168.8.165Sub-Net Mask: 255.255.255.0System Locale: United States (US English)System Location: 3: Thornton, CODevice ID: NONENumber of Extensions on System: 24Features Configured<ul style="list-style-type: none">Licenses Installed: Server Edition(1); IP Office Select(1); Basic User(25)Connected Extensions: 3043; 3044Users NOT Configured for Voicemail: NONEUsers assigned as Ex-Directory: NONEUsers assigned for Twinning: NONEUsers barred from making Outgoing Calls: NONEMusic on Hold: WAV File

6.1. Physical Hardware

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

Configuration

- BOOTP (4)
- Operator (3)
- Solution
 - User(32)
 - Group(2)
 - Short Code (48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - IP500V2-One
 - System (1)
 - Line (3)
 - Control Unit (4)
 - 1 IP 500 V2**
 - 2 VCM64/PRID U
 - 3 PHONE8
 - 6 DIG DCPx16 V2
 - Extension (24)
 - User (27)
 - Group (1)
 - Short Code (12)
 - Service (0)
 - RAS (1)
 - Incoming Call Route (1)
 - WAN Port (0)
 - Firewall Profile (1)
 - IP Route (3)
 - License (2)
 - Tunnel (0)
 - ARS (2)
 - Location (1)
 - Authorization Code (0)
- IP500V2-Two

IP 500 V2

Unit	
Device Number	1
Unit Type	IP 500 V2
Version	11.1.1.1.0 build 18
Serial Number	00e00706530f
Unit IP Address	192.168.8.165
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: 192.168.8.165** 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 the IP500V2-One system. On the left is a navigation pane titled 'Configuration' showing a tree structure of system components. The 'System' component is expanded, and 'IP500V2-One' is selected. The main pane on the right is titled 'IP500V2-One' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', and 'System Events'. The 'LAN1' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The configuration fields are as follows:

Field	Value
IP Address	192 . 168 . 8 . 165
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	0 . 0 . 0 . 0
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 configuration area.

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 **192.168.8.1**
- 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 . 8 . 1
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 'IP Office Line - Line 17' configuration window. On the left is a navigation tree under the 'Configuration' header, listing various system components like BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, IP500V2-One, System, Line, Control Unit, Extension, User, Group, Short Code, Service, RAS, Incoming Call Route, WAN Port, Firewall Profile, IP Route, License, Tunnel, ARS, Location, Authorization Code, and IP500V2-Two. The 'Line' component is selected, showing a sub-tree with lines 1, 17, and 17. The main configuration area on the right 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 fields for Line Number (17), Telephone Number, Transport Type (WebSocket Client), Prefix, Networking Level (SCN), Outgoing Group ID (99999), Security (Medium), Number of Channels (250), and Outgoing Channels (250). Below these are Gateway settings: Address (10 . 64 . 101 . 127), Port (443), Location (3: Thornton, CO), Password, and Confirm Password. A 'Description' field is also present. On the right side of the Gateway section, there are 'SCN Resiliency Options' with checkboxes for 'Supports Resiliency', 'Backs up my IP phones', 'Backs up my hunt groups', and 'Backs up my IP DECT phones'.

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

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

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **T.38** for **Fax Transport Support** (refer to Section 2.1).
- Under **Media Security Preferred** was selected.
- Under **Advanced Media Security Options Same as System** was selected.

Configuration

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

IP Office Line - Line 17

Line Short Codes VoIP Settings T38 Fax

Codec Selection: System Default

Unused:

Selected:

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

Fax Transport Support: T38

Call Initiation Timeout (s): 4

Media Security: Preferred

Advanced Media Security Options: ☒ Same As System

Encryptions:

- ☒ RTP
- ☐ RTCP

Authentication:

- ☒ RTP
- ☒ RTCP

Replay Protection:

SRTP Window Size: 64

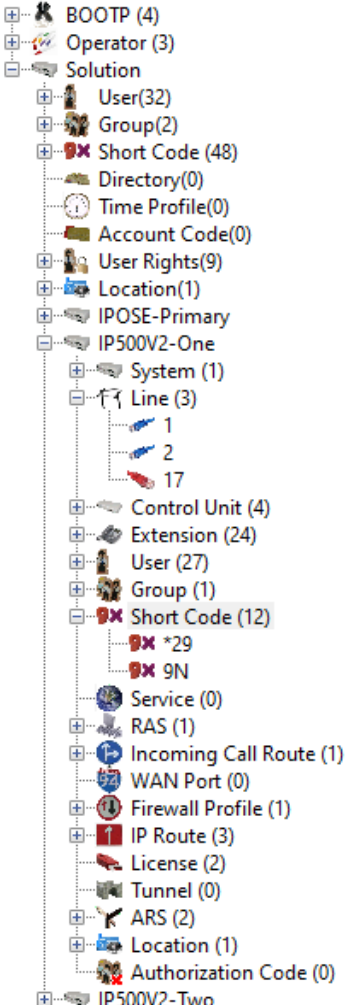
Crypto Suites:

- ☒ SRTP_AES_CM_128_SHA1_80
- ☐ SRTP_AES_CM_128_SHA1_32

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

6.5. Short Codes

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

Configuration	9N: Dial														
 <ul style="list-style-type: none">BOOTP (4)Operator (3)Solution<ul style="list-style-type: none">User(32)Group(2)Short Code (48)<ul style="list-style-type: none">Directory(0)Time Profile(0)Account Code(0)User Rights(9)Location(1)IPOSE-PrimaryIP500V2-One<ul style="list-style-type: none">System (1)<ul style="list-style-type: none">Line (3)<ul style="list-style-type: none">1217Control Unit (4)Extension (24)User (27)Group (1)Short Code (12)<ul style="list-style-type: none">*299NService (0)RAS (1)Incoming Call Route (1)WAN Port (0)Firewall Profile (1)IP Route (3)License (2)Tunnel (0)ARS (2)Location (1)Authorization Code (0)IP500V2-Two	<div>Short Code</div> <table><tr><td>Code</td><td>9N</td></tr><tr><td>Feature</td><td>Dial</td></tr><tr><td>Telephone Number</td><td>N</td></tr><tr><td>Line Group ID</td><td>51: To-Primary</td></tr><tr><td>Locale</td><td>United Kingdom (UK English)</td></tr><tr><td>Force Account Code</td><td><input type="checkbox"/></td></tr><tr><td>Force Authorization Code</td><td><input type="checkbox"/></td></tr></table>	Code	9N	Feature	Dial	Telephone Number	N	Line Group ID	51: To-Primary	Locale	United Kingdom (UK English)	Force Account Code	<input type="checkbox"/>	Force Authorization Code	<input type="checkbox"/>
Code	9N														
Feature	Dial														
Telephone Number	N														
Line Group ID	51: To-Primary														
Locale	United Kingdom (UK 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 interface for an Automatic Route Selection (ARS) system. On the left is a tree view of the system configuration, with 'ARS (2)' expanded to show '51: To-Primary'. The main panel is titled 'To-Primary' and contains the following settings:

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

Below these settings is a table for route entries:

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

Buttons for 'Add...', 'Remove', and 'Edit...' are located to the right of the table. Below the table, the following settings are visible:

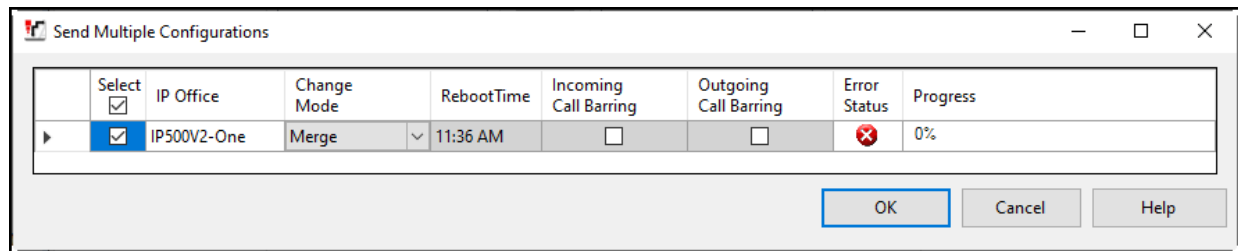
- Alternate Route Priority Level:** 3
- Alternate Route Wait Time:** 30
- Alternate Route:** <None>

Repeat this process described in **Section 6** on any additional Secondary servers 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. BT Wholesale Hosted SIP Trunking Service Configuration

To use BT Wholesale Hosted SIP Trunking Service, a customer must request the service from BT using the established sales processes. The process can be started by contacting BT via the corporate web site at <https://www.btwholesale.com/pages/static/home.htm> and requesting information.

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

BT is responsible for the configuration of BT Wholesale Hosted SIP Trunking Service. The customer will need to provide the public IP address used to reach the Avaya Session Border Controller for Enterprise at the enterprise, the public IP address assigned to IP Office LAN2.

BT will provide the customer the necessary information to configure Avaya IP Office and the Avaya Session Border Controller for Enterprise following the steps discussed in the previous sections, including:

BT will provide the following information:

- SIP Trunk registration credentials (User Name, Password, etc.).
- BT's Domain Name and SIP Proxy FQDN.
- DNS IP addresses.
- DID numbers, etc.

8. Verification Steps

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

The following steps may be used to verify the configuration:

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

8.1. IP Office System Status

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

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

Avaya IP Office System Status

AVAYA IP Office System Status

Help Exit About

Online Offline

Logon

Control Unit Address: 10.64.101.127

SCN Gateway Address: <None>

Services Base TCP Port: 50804

Local IP Address: Automatic

User Name: Administrator

Password:

☐ Auto reconnect

☒ Secure connection

☐ Websocket connection

Logon

IP Office System Status Version 11.1.1.1.0 build 18

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

IP Office System Status

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

System

Alarms (27)

Extensions (3)

Trunks (4)

Line: 1

Line: 2

Line: 17

Line: 18

Active Calls

Resources

Voicemail

IP Networking

Locations

Status

Utilization Summary

Alarms

Registration

SIP Trunk Summary

Line Service State:

In Service

Peer Domain Name:

interopc1.domain

Resolved Address:

Line Number:

17

Number of Administered Channels:

10

Number of Channels in Use:

0

Administered Compression:

G722, G711 A, G729 A, G711 Mu

Enable Faststart:

Off

Silence Suppression:

Off

Media Stream:

RTP

Layer 4 Protocol:

UDP

SIP Trunk Channel Licenses:

100

0%

SIP Trunk Channel Licenses in Use:

0

SIP Device Features:

UPDATE (Incoming and Outgoing)

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 Delay
1			Idle	03:43:59							
2			Idle	1 day 03:2...							
3			Idle	1 day 08:5...							
4			Idle	1 day 08:5...							
5			Idle	1 day 08:5...							
6			Idle	1 day 08:5...							
7			Idle	1 day 08:5...							
8			Idle	1 day 08:5...							
9			Idle	1 day 08:5...							
10			Idle	1 day 08:5...							

Trace

Trace All

Pause

Ping

Call Details

Graceful Shutdown

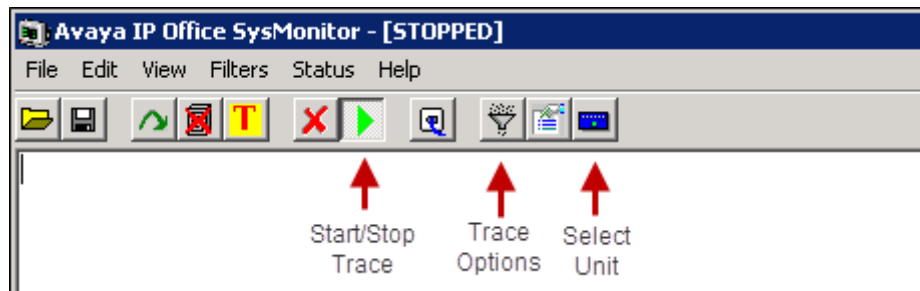
Force Out of Service

Print...

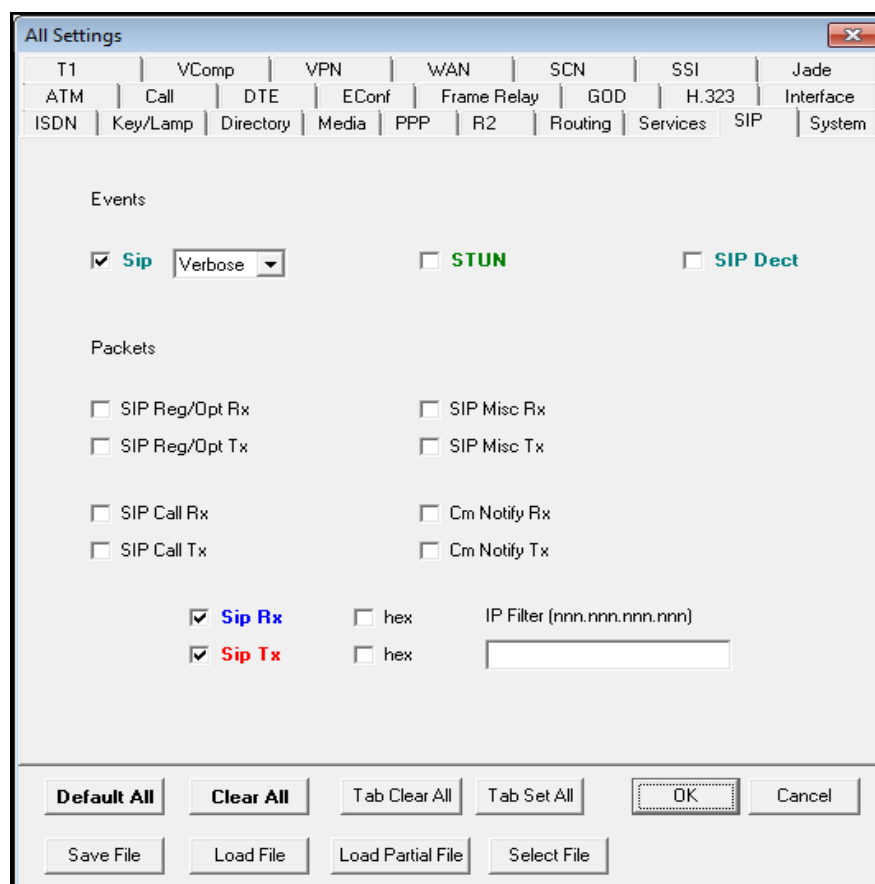
Save As...

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 BT Wholesale Hosted SIP Trunking Service. BT Wholesale Hosted SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

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

10. Additional References

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

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

[1] *Deploying IP Office Server Edition*, Release 11.1 FP1, Issue 16, February 2021

[2] *Administering Avaya IP Office with IP Office Manager*, November 15, 2021.

[3] *Administering Avaya IP Office with Web Manager*, August 2021.

Additional Avaya IP Office documentation can be found at:

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

11. Appendix A: Class 5 CLIP

During the compliance test, BT requested to test Class 5 CLIP PBX passthrough testing. This scenario is to verify if the PBX supports Class-5 CLIP. The PBX should be able to send a Class5 CLIP on outbound calls but accept incoming calls on BT DDIs configured in IP Office as per **Section 5.5**. The following configuration and screenshots explain the required configuration on IP Office to successfully test Class 5 CLIP PBX passthrough testing.

For this particular test scenario, two separate SIP URI entries were created, one was created to send Class-5 CLIP on outbound calls and one to accept incoming calls on BT DDIs configured in IP Office. The outbound entry was created with the parameters shown below:

- Associate this entry 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 from this line. For the compliance test outgoing group **17** was used. Leave the **Incoming Group** field as 0.
- Under **Credentials**, select **0: <None>** from the pull-down menu.
- 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. Notice that the Class 5 CLIP of 08001231234 provided by BT was configured under Content for the Local URI field, this is the call id that will be displayed on the terminating endpoint.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.

New URI	
Incoming Group	0
Outgoing Group	17
Credentials	0: <None>
Max Sessions	10

	Display	Content
Local URI	Use Internal Data	08001231234
Contact	Use Internal Data	Use Internal Data
P Asserted ID	<input checked="" type="checkbox"/> Use Internal Data	Use Internal Data
P Preferred ID	<input type="checkbox"/> None	None
Diversion Header	<input checked="" type="checkbox"/> Use Internal Data	Use Internal Data
Remote Party ID	<input type="checkbox"/> None	None

Field meaning		
Outgoing Calls	Forwarding/Twining	Incoming Calls
Caller	Original Caller	Called
Caller	Caller	Called
Caller	Caller	Called
None	None	None
Caller	Caller	None
None	None	None

OK Cancel Help

The entry for calls from the PSTN to IP Office (incoming calls) was created with the parameters shown below:

- Associate this entry to an incoming line group using the **Incoming Group** field. For the compliance test incoming group **17** was used. The **Outgoing Group** field was set to **100**, since it cannot be set to 0 in IP Office Server Edition systems, this is an arbitrary number.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Set the **Credentials** field to **0: <None>** (SIP Trunk registration is being done at the Avaya SBCE).
- For the **Local URI** and **Contact**, set the selections under the **Display** and **Content** columns to **Use Internal Data**.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.
- Click **OK** to commit again (not shown).

SIP Line - 17 | Call Details | SIP URI

New URI

Incoming Group: 17 Max Sessions: 10

Outgoing Group: 100

Credentials: 0: <None>

	Display	Content
Local URI	Use Internal Data	Use Internal Data
Contact	Use Internal Data	Use Internal Data
P Asserted ID	<input type="checkbox"/> None	None
P Preferred ID	<input type="checkbox"/> None	None
Diversion Header	<input type="checkbox"/> None	None
Remote Party ID	<input type="checkbox"/> None	None

Field meaning		
Outgoing Calls	Forwarding/Twinning	Incoming Calls
Caller	Original Caller	Called
Caller	Original Caller	Called
None	None	None
None	None	None
None	None	None
None	None	None

OK Cancel Help

The following screenshot shows the completed configuration.

The screenshot displays the Avaya SIP Line configuration interface. The left sidebar shows a hierarchical tree of configuration elements, including 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), IPSE-Primary, System (1), Line (4) (with sub-items 1, 2, 17, 18), Control Unit (8), Extension (6), User (7), Group (0), Short Code (3), Service (0), Incoming Call Route (2), IP Route (4), License (9), ARS (2), Location (1), Authorization Code (0), IP500V2-One, and IP500V2-Two.

The main panel is titled "SIP Line - Line 17" and contains several tabs: SIP Line, Transport, Call Details, VoIP, SIP Credentials, SIP Advanced, and Engineering. The "SIP Line" tab is active, showing a table of SIP URIs.

URI	Groups	Credential	Local URI	Contact	P Asserted ID	P Preferred ID	Diversion Header	Remote Party ID
1	0 17	0: <None>	08001231234	Use Internal Data	Use Internal Data		Use Internal Data	
2	17 100	0: <None>	Use Internal Data	Use Internal Data				

Below the table, there is a section for "SIP Line Appearances" with a checkbox and a table with columns: Line ID, Incoming ID, Outgoing ID, Groups, Credential, Local URI, Contact, P Asserted ID, P Preferred ID, Diversion Header, and Remote Party ID. The table is currently empty.

©2022 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.