



## **Application Notes for Configuring the XO Communications SIP Trunking Service with Avaya IP Office 10.0 – Issue 1.0**

### **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking for an enterprise solution using Avaya IP Office 10.0 to interoperate with the XO Communications SIP Trunking Service.

The XO Communications SIP Trunking Service provides PSTN access via a SIP trunk between the enterprise and the XO Communications network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise. XO Communications is a member of the Avaya DevConnect Service Provider program.

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 to configure Session Initiation Protocol (SIP) Trunking for an enterprise solution using Avaya IP Office 10.0 to interoperate with the XO Communications SIP Trunking Service.

The XO Communications SIP Trunking Service will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE).

## 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Avaya IP Office and various Avaya endpoints listed in **Section 4**.

The XO Communications SIP Trunking Service passed compliance testing with any observations or limitations described in **Section 2.2**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

### 2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Establishment of the SIP trunk
- SIP OPTIONS queries and responses
- Incoming PSTN calls (via the SIP trunk) to SIP and H.323 telephones at the enterprise
- Outgoing PSTN calls (via the SIP trunk) from SIP and H.323 telephones at the enterprise
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows and Avaya Communicator for Web
- Various call types including: local, long distance, inbound/outbound toll-free, international (00 + country code + number) operator, operator-assisted (0 + 10 digits), local directory assistance, and emergency calls (911)
- Codecs G.729A and G.711U
- Caller ID presentation and Caller ID restriction
- DTMF transmission using RFC 2833
- Response to incomplete call attempts and trunk errors
- Voicemail navigation using DTMF input for inbound and outbound calls
- Voicemail message waiting indicator (MWI)

- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and twinning (mobility)
- T.38 and G.711 fax
- Long duration calls and simultaneous active calls

## 2.2. Test Results

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

- **Outbound privacy calls failed:** Outbound privacy calls from Avaya IP Office failed because Avaya IP Office sends “Unknown” as the user portion of the SIP URI in the PAI header of the outbound INVITE instead of the DID assigned by the service provider to the caller. This causes XO Communications to reject the call. This only occurs if the SIP trunk on Avaya IP Office is configured with SIP URI **Identity** as **None (Section 5.4.5)**. This is an Avaya issue and is being investigated. A possible workaround is to set **Identity** to **PAI** but this has the side effect that the Caller ID is incorrect on inbound calls forwarded back to the PSTN and twinned calls.
- **Inbound and outbound G.711 fax calls failed:** These calls failed due to excessive jitter on the inbound media stream to Avaya IP Office. This prevented Avaya IP Office from being able to reliably detect the inbound fax tones from XO Communications and the call was disconnected. This is not an interoperability problem but instead is a network issue. This is not expected to be an issue with the XO Communications production environment but is the result of the limitations of the test environment.

## 2.3. Support

For technical support on the XO Communications Trunking Service, please contact XO Communications via the following:

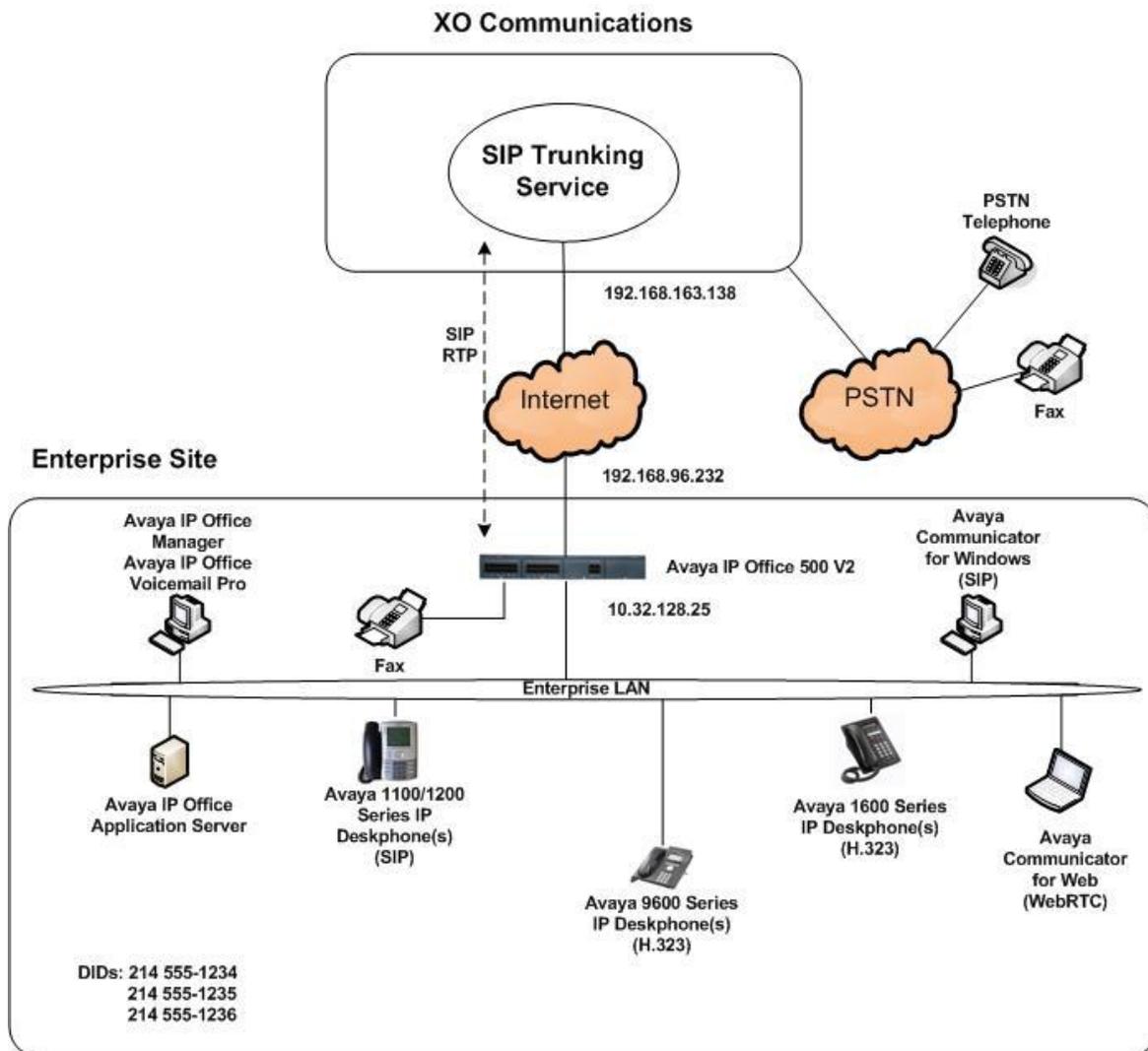
- Web: <http://www.xo.com> – visit Support link
- Phone: 800-421-3872

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 sample configuration used for the DevConnect compliance testing. The sample configuration shows an enterprise site connected to the XO Communications SIP Trunking Service.

The enterprise site contains an Avaya IP Office 500 V2 with various endpoints and a Windows PC running both Avaya IP Office Manager to configure Avaya IP Office and Avaya Voicemail Pro for voicemail. In addition, the Avaya IP Office Application Server is present to support use of Avaya Communicator for Web (WebRTC client). For the compliance test, Avaya IP Office is deployed in a 2-port configuration. The Avaya IP Office LAN1 port is connected to the private enterprise LAN and the WAN (LAN2) port is connected to the public network.



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

For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes. Instead, public IP addresses have been replaced with private addresses and all phone numbers have been replaced with numbers that are not routable by the PSTN.

For the purposes of the compliance test, users dialed a prefix digit 9 plus N digits to send an outbound call to the number N across the SIP trunk to the service provider. The short code of 9 was stripped off by Avaya IP Office and the remaining N digits were sent to the service provider network. Avaya IP Office sent the N digits in the Request URI and the To header of an outbound SIP INVITE message.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the enterprise network such as a 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 SIP and RTP traffic between the service provider and Avaya IP Office must be allowed to pass through these devices.

The administration of the Avaya Voicemail Pro messaging service and endpoints on Avaya IP Office are standard. Since these configuration tasks are not directly related to the interoperation with the XO Communications SIP Trunking Service, they are not included in these Application Notes.

## 4. Equipment and Software Validated

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

<b>Avaya Telephony Components</b>	
<b>Equipment</b>	<b>Software</b>
Avaya IP Office 500 v2	10.0 SP2 (10.0.0.2.0 Build 10)
Avaya IP Office Manager	10.0 SP2 (10.0.0.2.0 Build 10)
Avaya IP Office VoiceMail Pro	10.0 SP2 (10.0.0.2.0 Build 10)
Avaya IP Office Application Server <ul style="list-style-type: none"><li>• one-X® Portal</li><li>• WebRTC Gateway</li></ul>	10.0 SP2 (10.0.0.2.0 Build 10) (10.0.0.2.0 Build 13) (10.0.0.3.0 Build 07)
Avaya 1140E IP Deskphone (SIP)	4.4 SP4 (4.04.23)
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3.5 (1.3.50B)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.6.3 (6.6302)
Avaya Communicator for Windows	2.1.3 (2.1.3.237)
Avaya Communicator for Web	1.0.16.1718

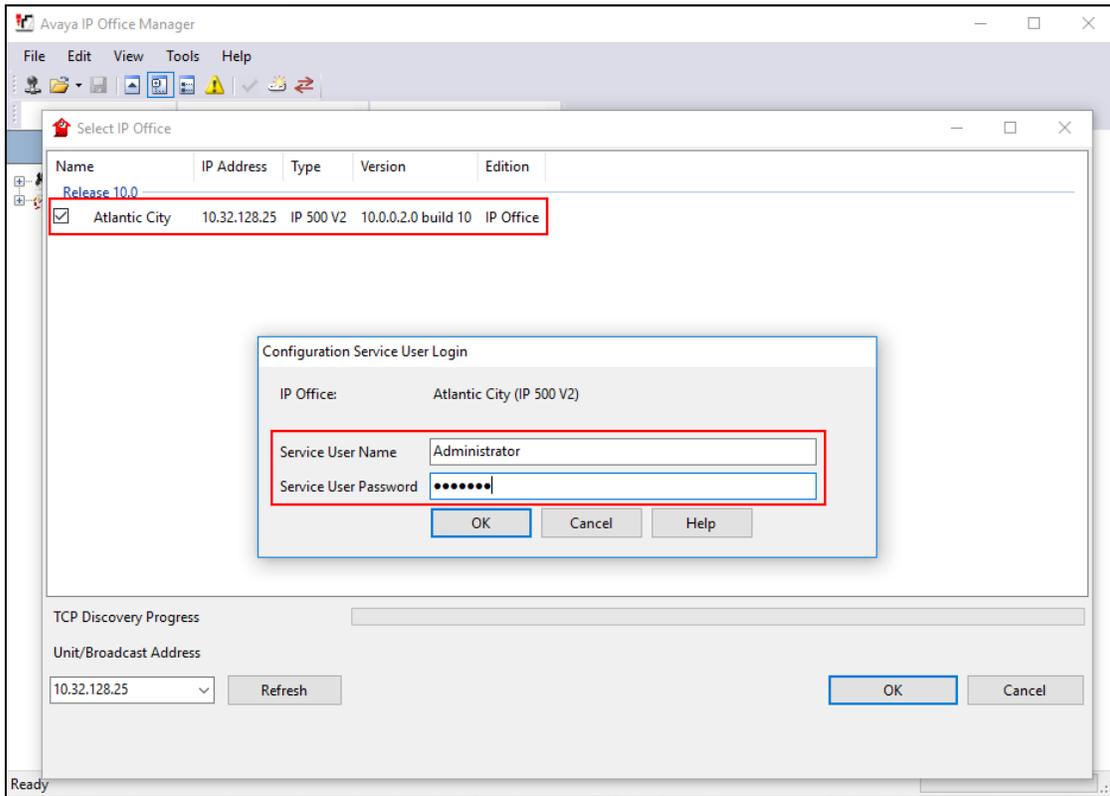
<b>XO Communications Components</b>	
<b>Equipment</b>	<b>Software</b>
Broadsoft Softswitch	Rel_20.sp1_1.606
Sonus GSX9000 SBC	V08.04.16 F003

Compliance Testing is applicable when the tested solution is deployed with a standalone Avaya IP Office 500 V2 and also when deployed with Avaya IP Office Server Edition in all configurations.

Avaya IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog/digital endpoints or analog/digital trunks.

## 5. Configure Avaya IP Office

Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the PC running Avaya IP Office Manager, select **Start** → **All Programs** → **IP Office** → **Manager** to launch the application. Select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials.



If the above screen does not appear, the configuration may be alternatively opened by navigating to **File** → **Open Configuration** at the top of the Avaya IP Office Manager window.

The appearance of the Avaya IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation pane on the left side, omit the Group pane in the center, and show the Details pane on the right side. Since the Group Pane has been omitted, its content is shown as submenus in the Navigation pane. The Navigation and Details panes will be referenced throughout the Avaya IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the service provider (such as twinning and Avaya Communicator support) is assumed to already be in place.

In the sample configuration, **Atlantic City** was used as the system name. All navigation described in the following sections (e.g., **License** → **SIP Trunk Channels**) appears as submenus underneath the system name **Atlantic City** in the Navigation Pane.

## 5.1. Licensing

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

To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License** in the Navigation pane. Confirm a valid license with sufficient **Instances** (trunk channels) appears in the Details pane.

The screenshot shows the Avaya IP Office web interface. On the left is a navigation tree under 'IP Offices' with 'License (30)' selected. The main content area is titled 'License Remote Server' and shows the following details:

- License Mode: License Normal
- Licensed Version: 10.0
- PLDS Host ID: [Redacted]
- PLDS File Status: Valid

Below these details is a table of installed licenses:

Feature	Instances	Status	Expiration Date	Source
Receptionist	4	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	1	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	4	Valid	Never	PLDS Nodal
VMPro TTS (Generic)	40	Valid	Never	PLDS Nodal
Teleworker	384	Valid	Never	PLDS Nodal
Mobile Worker	384	Valid	Never	PLDS Nodal
Office Worker	384	Valid	Never	PLDS Nodal
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	40	Valid	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	1	Valid	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Valid	Never	PLDS Nodal
SIP Trunk Channels	128	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Valid	Never	PLDS Nodal

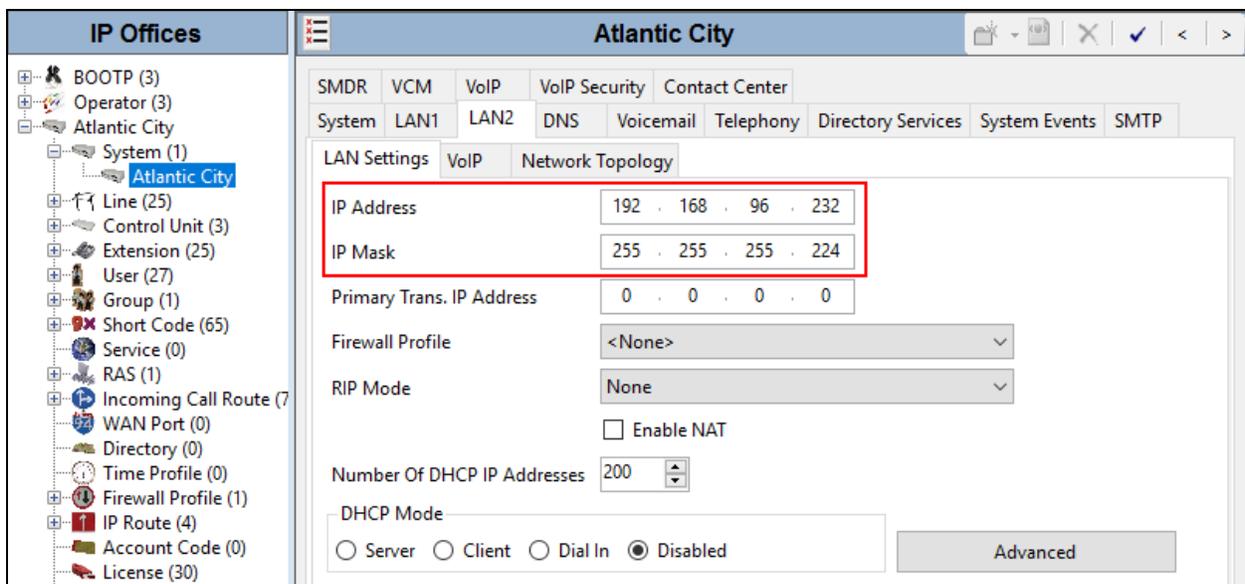
Buttons for 'Add...' and 'Remove' are visible on the right side of the table.

## 5.2. System

Configure the necessary system settings.

### 5.2.1. System – LAN2 Tab

In the sample configuration, the Avaya IP Office WAN port was used to connect to the public network. The LAN2 settings correspond to the WAN port on the Avaya IP Office 500 V2. To access the LAN2 settings, first navigate to **System** → *<Name>*, where *<Name>* is the system name assigned to the Avaya IP Office. In the case of the compliance test, the system name is **Atlantic City**. Next, navigate to the **LAN2** → **LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office WAN port on the public network. Set the **IP Mask** field to the mask used on the public network. All other parameters should be set according to customer requirements.



The screenshot displays the configuration interface for the 'Atlantic City' system. The left sidebar shows a tree view of system components, with 'Atlantic City' selected. The main pane shows the 'LAN2' settings tab, which is further divided into 'LAN Settings', 'VoIP', and 'Network Topology'. The 'LAN Settings' tab is active, and the 'IP Address' and 'IP Mask' fields are highlighted with a red box. The 'IP Address' is set to 192.168.96.232 and the 'IP Mask' is set to 255.255.255.224. Other settings include 'Primary Trans. IP Address' (0.0.0.0), 'Firewall Profile' (<None>), 'RIP Mode' (None), and 'DHCP Mode' (Disabled). The 'Advanced' button is visible at the bottom right of the settings pane.

Field	Value
IP Address	192 . 168 . 96 . 232
IP Mask	255 . 255 . 255 . 224
Primary Trans. IP Address	0 . 0 . 0 . 0
Firewall Profile	<None>
RIP Mode	None
Enable NAT	<input type="checkbox"/>
Number Of DHCP IP Addresses	200
DHCP Mode	<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dial In <input checked="" type="radio"/> Disabled

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

- Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks.
- The **RTP Port Number Range** can be customized to a specific range of ports that Avaya IP Office will use for RTP media. This port range will be used to select a destination port for incoming RTP and a source port for outgoing RTP for calls using LAN2.

The screenshot shows the Avaya IP Office configuration interface for 'Atlantic City'. The 'VoIP' tab is selected, and the 'LAN2' configuration is active. The 'SIP Trunks Enable' checkbox is checked and highlighted with a red box. Below it, the 'RTP' section is visible, with the 'Port Number Range' fields (Minimum: 49152, Maximum: 53246) also highlighted with a red box. Other settings include H.323 Gatekeeper Enable, Auto-create Extension, Auto-create User, H.323 Remote Extension Enable, H.323 Signaling over TLS (Disabled), Remote Call Signaling Port (1720), SIP Registrar Enable, Auto-create Extension/User, SIP Remote Extension Enable, SIP Domain Name, SIP Registrar FQDN, Layer 4 Protocol (UDP, TCP, TLS), and Challenge Expiration Time (10).

Scroll down the page.

- In the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the periodic timeout to **30** and the **Initial keepalives** parameter to **Enabled**. These settings will cause Avaya IP Office to send RTP and RTCP keepalive packets starting at the time of initial connection and every 30 seconds thereafter if no other RTP/RTCP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting to see media from the other, as well as helping to keep firewall ports open for the duration of the call.
- In the **DiffServ Settings** section, Avaya IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP header with specific values to support Quality of Services policies for both signaling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling. The specific values used for the compliance test were the Avaya IP Office default values and are shown in the screenshot below. Quality of Service (QoS) is not specifically tested as part of the compliance test.
- All other parameters should be set according to customer requirements.

The screenshot displays the configuration interface for 'Atlantic City'. The 'VoIP' tab is selected, and the 'Network Topology' sub-tab is active. The 'RTCP collector IP address for phones' is set to 0.0.0.0. The 'Keepalives' section is highlighted with a red box and contains the following settings: 'Scope' is set to 'RTP-RTCP', 'Periodic timeout' is set to 30, and 'Initial keepalives' is set to 'Enabled'. The 'DiffServ Settings' section is also highlighted with a red box and contains the following settings: 'DSCP (Hex)' is B8, 'Video DSCP (Hex)' is B8, 'DSCP Mask (Hex)' is FC, 'SIG DSCP (Hex)' is 88, 'DSCP' is 46, 'Video DSCP' is 46, 'DSCP Mask' is 63, and 'SIG DSCP' is 34. The 'DHCP Settings' section is visible below and includes 'Primary Site Specific Option Number (SSON)' set to 176, 'Secondary Site Specific Option Number (SSON)' set to 242, 'VLAN' set to 'Not Present', '1100 Voice VLAN Site Specific Option Number (SSON)' set to 232, and an empty field for '1100 Voice VLAN IDs'.

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

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. Since no firewall or network address translation (NAT) device was used between the Avaya IP Office and the service provider, the parameter was set to **Open Internet**. With the **Open Internet** setting, the **STUN Server Address** is not used.
- Set **Binding Refresh Time (sec)** to **300**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider.
- Set the **Public IP Address** to the IP address assigned to the Avaya IP Office WAN port in the **LAN2→LAN Settings** form earlier in this section.
- In the **Public Port** section, next to the transport protocol **UDP**, select the UDP port on which Avaya IP Office will listen.
- All other parameters should be set according to customer requirements.

The screenshot shows the configuration interface for Atlantic City. The 'Network Topology' tab is active, displaying the 'Network Topology Discovery' section. The 'Firewall/NAT Type' is set to 'Open Internet', 'Binding Refresh Time (sec)' is 300, and 'Public IP Address' is 192.168.96.232. The 'Public Port' section shows 'UDP' set to 5060, 'TCP' set to 0, and 'TLS' set to 0. A 'Run STUN' button is visible.

## 5.2.2. System - Telephony Tab

To access the System Telephony settings, navigate to the **Telephony** → **Telephony** tab in the Details Pane. Enter or select **0** for **Hold Timeout (sec)** so that calls on hold will not time out. Under Companding Law, set **Switch** to **U-Law** and **Line** to **U-Law Line**. 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.

The screenshot shows the 'Atlantic City' configuration window for the 'Telephony' tab. The 'Hold Timeout (sec)' field is highlighted with a red box and set to 0. The 'Companding Law' section is also highlighted with a red box, showing 'U-Law' selected for the Switch and 'U-Law Line' selected for the Line. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked. Other settings include 'Default Outside Call Sequence' (Normal), 'Default Inside Call Sequence' (Ring Type 1), 'Default Ring Back Sequence' (Ring Type 2), 'Restrict Analogue Extension Ringer Voltage' (unchecked), 'Dial Delay Time (sec)' (4), 'Dial Delay Count' (0), 'Default No Answer Time (sec)' (25), 'Park Timeout (sec)' (300), 'Ring Delay (sec)' (5), 'Call Priority Promotion Time (sec)' (Disabled), 'Default Currency' (USD), 'Default Name Priority' (Favor Trunk), 'Media Connection Preservation' (Disabled), 'Phone Failback' (Manual), and 'Login Code Complexity' (Enforcement unchecked, Minimum length 4). The 'DSS Status' checkbox is unchecked, and 'Auto Hold', 'Dial By Name', and 'Show Account Code' are checked. Other options like 'Restrict Network Interconnect', 'Include location specific information', 'Drop External Only Impromptu Conference', 'Visually Differentiate External Call', 'Unsupervised Analog Trunk Disconnect Handling', 'High Quality Conferencing', 'Digital/Analogue Auto Create User', 'Directory Overrides Barring', and 'Advertise Callee State To Internal Callers' are unchecked.

### 5.3. IP Route

A default route is needed so Avaya IP Office can reach network subnets other than the one where it resides. Navigate to **IP Route** → **0.0.0.0** in the left Navigation Pane if a default route already exists. Otherwise, to create the default route, right-click on **IP Route** and select **New**.

Create/verify a default route with the following parameters:

- Set **IP Address** and **IP Mask** to **0.0.0.0**.
- Set **Gateway IP Address** to the IP address of the default router on the public network where Avaya IP Office is connected.
- Set **Destination** to **LAN2** from the drop-down list.

Click the **OK** button at the bottom of the page (not shown).

The screenshot shows the Avaya IP Office configuration interface. On the left is a navigation pane titled "IP Offices" with a tree view containing various system components like BOOTP, Operator, Atlantic City, System, Line, Control Unit, Extension, User, Group, Short Code, Service, RAS, Incoming Call Route, WAN Port, Directory, Time Profile, Firewall Profile, and IP Route (4). The main window is titled "0.0.0.0" and displays the configuration for an IP Route. A red box highlights the following fields:

IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	192 . 168 . 96 . 254
Destination	LAN2
Metric	0

Below the Metric field, there is a checkbox labeled "Proxy ARP" which is currently unchecked.

## 5.4. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the XO Communications SIP Trunking Service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by Avaya IP Office Manager to create a SIP Line. Follow the steps in **Section 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 **Sections 5.4.2 – 5.4.8**.

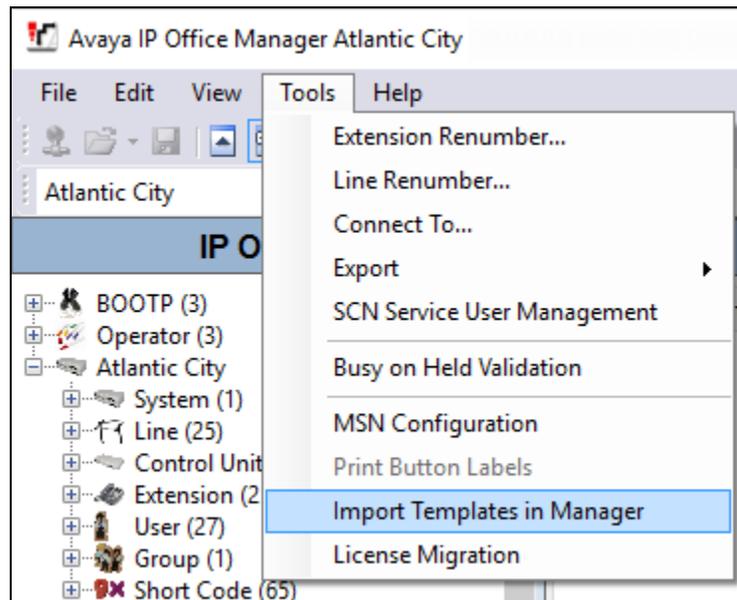
Also, the following SIP Line settings are not supported on Basic Edition:

- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required
- SIP Advanced
- Engineering

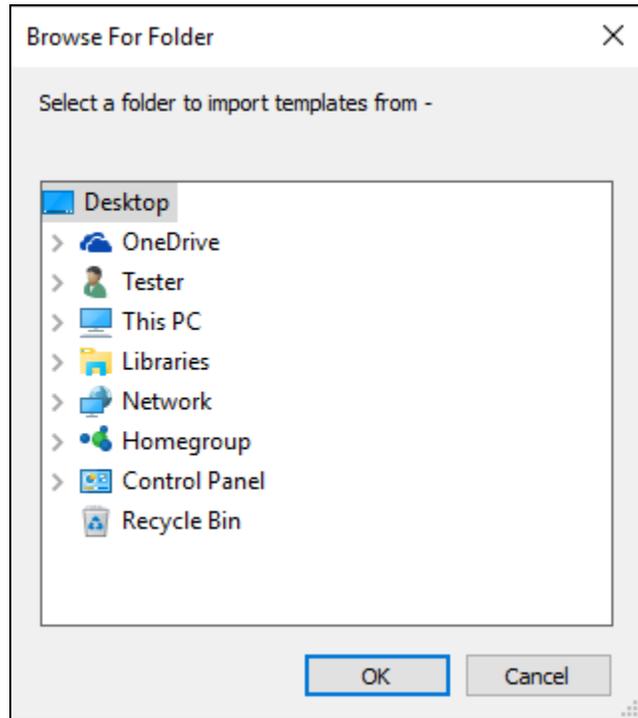
To create a SIP Line manually, right-click **Line** in the Navigation Pane and select **New → SIP Line**; then, follow the steps outlined in **Sections 5.4.2 – 5.4.8**.

### 5.4.1. SIP Line From Template

1. Copy the template file to the computer where Avaya IP Office Manager is installed. Place it in an empty directory. This is important because **Step 2** will import all templates located in this directory not just the template file associated with these Application Notes.
2. Import the template into Avaya IP Office Manager. From Avaya IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy all the template files located in the selected directory into the Avaya IP Office template directory and make the templates available in the Avaya IP Office Manager pull-down menus in **Step 3**.



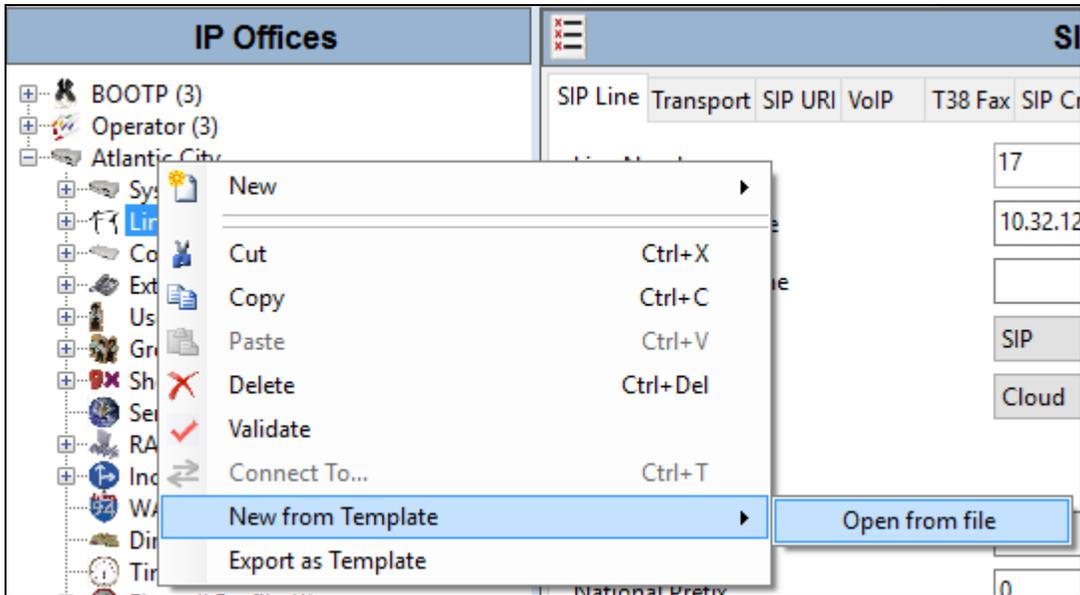
In the pop-up window that appears, select the directory where the template file was copied in **Step 1**, then click **OK**.



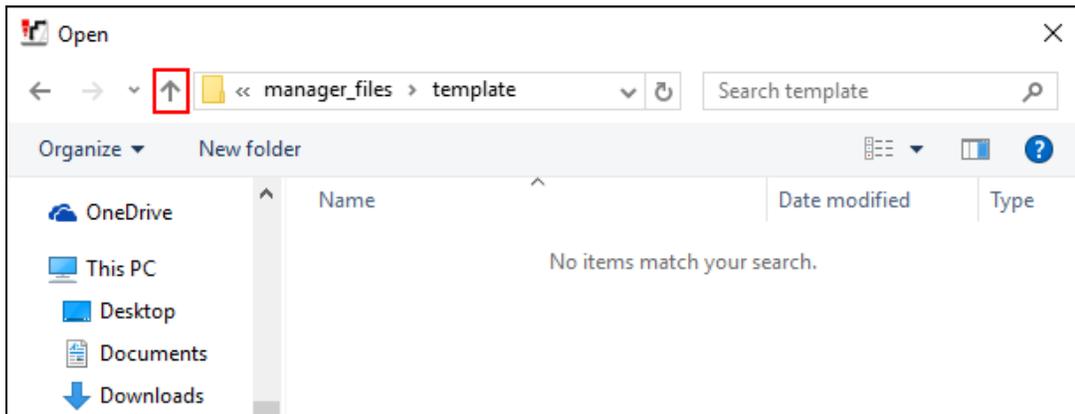
After the import is complete, a final import status pop-up window will appear stating success or failure (not shown). Click **OK** (not shown) to continue.

**Note** - Within Avaya IP Office Manager menus, the template directory may be accessed by navigating to **C:\Program Files\Avaya\IP Office\Manager\Templates**. However, the template directory is physically located in the User Access Control Virtual Store area of Windows. To view the directory from outside Avaya IP Office Manager (e.g., Windows Explorer), replace the **C:** portion of the template path above with **%UserProfile%\AppData\Local\VirtualStore**.

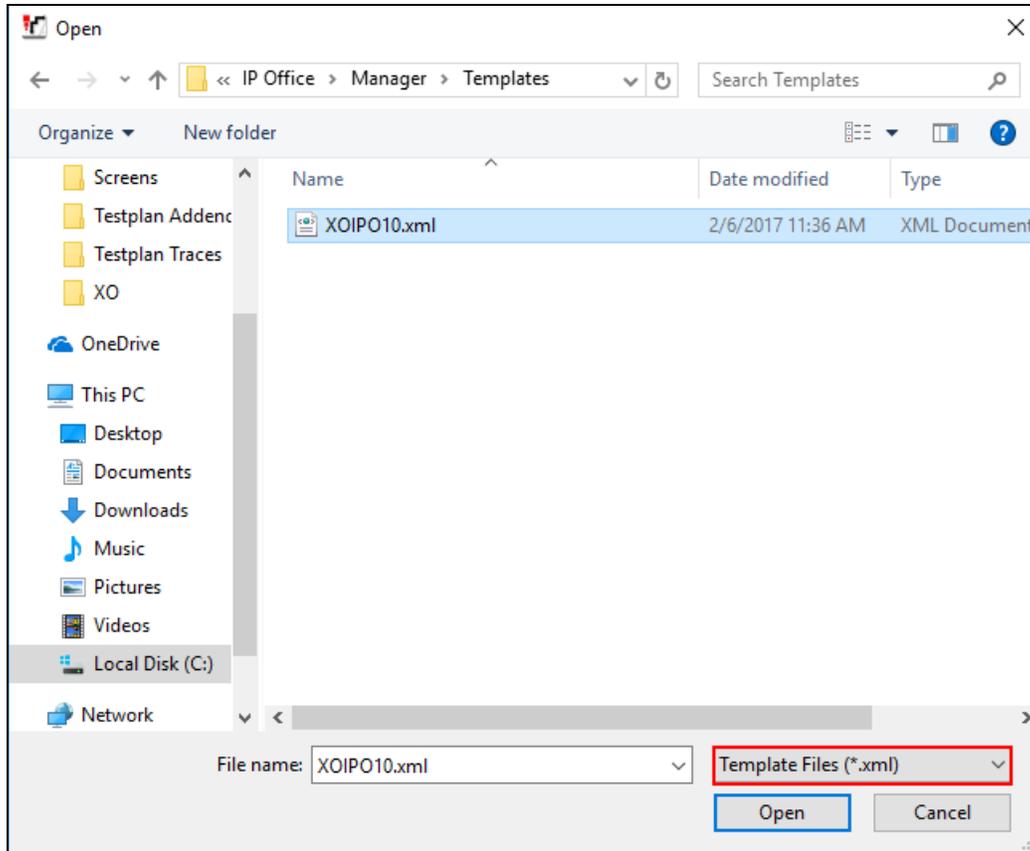
3. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, and select **New From Template** → **Open File**.



4. The subsequent pop-up window opens to **C:\Program Files\Avaya\IP Office\Manager\manager\_files\template**. Navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates**. The up arrow icon can be used to move up through the directory tree.



- Once reaching the correct directory, select **Template Files (.xml)** in the lower right corner to ensure that .xml template files are displayed. From the list of template files, select the one to be used and click **Open**.



A final status pop-up window will appear stating whether the trunk creation was a success or failure (not shown). Click **OK** (not shown) to continue.

- Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2 – 5.4.8**.

## 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 the **ITSP Domain Name** to the IP address of the XO Communications SIP proxy.
- Check the **In Service** box. This makes the trunk available to incoming and outgoing calls.
- Check the **Check OOS** box. Avaya IP Office will use the SIP OPTIONS method to periodically check the SIP Line. The time between SIP OPTIONS sent by Avaya IP Office will use the **Binding Refresh Time** for LAN2, as shown in **Section 5.2.1**.
- Set the **Refresh Method** to **Auto** and the **Timer (seconds)** to **300**. This will cause Avaya IP Office to send an UPDATE or INVITE message (depending on what the far-end supports) every 150 seconds (1/2 the **Timer** value) to check the state of each active session.
- Enter a **Description** for the trunk (optional).
- Use of REFER should be configured as per the needs of the customer. Call flows with and without REFER were tested as part of the compliance test. To enable REFER, set the **Incoming Supervised REFER** field and **Outgoing Supervised REFER** field to **Always**. To disable REFER, set these fields to **Never**.
- Default values may be used for all other parameters.

The screenshot displays the configuration for a SIP Line (Line 20) in the Avaya IP Office interface. The left sidebar shows a tree view of IP Offices and their components. The main area is titled "SIP Line - Line 20" and contains the following configuration fields and options:

- Line Number:** 20
- ITSP Domain Name:** 192.168.163.138
- Local Domain Name:** (empty)
- URI Type:** SIP
- Location:** Cloud
- Prefix:** (empty)
- National Prefix:** 0
- International Prefix:** 00
- Country Code:** (empty)
- Name Priority:** System Default
- Description:** XO Communications Trunk
- In Service:**
- Check OOS:**
- Session Timers:**
  - Refresh Method:** Auto
  - Timer (sec):** 300
- Redirect and Transfer:**
  - Incoming Supervised REFER:** Always
  - Outgoing Supervised REFER:** Always
  - Send 302 Moved Temporarily:**
  - Outgoing Blind REFER:**

### 5.4.3. SIP Line - Transport Tab

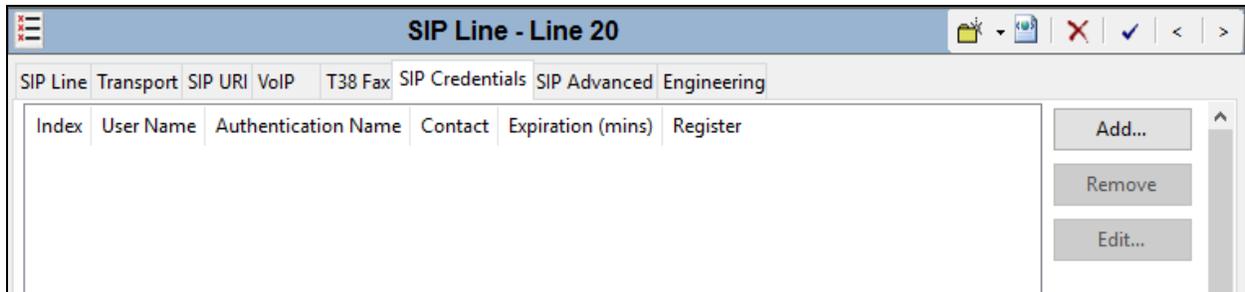
Select the **Transport** tab. Set or verify the parameters as shown below.

- Set the **ITSP Proxy Address** to the IP address of the XO Communications SIP proxy.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to the network port used by the SIP line to access the far-end and configured in **Section 5.2.1**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.

The screenshot shows the configuration window for 'SIP Line - Line 20' with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '192.168.163.138'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'UDP', 'Send Port' is '5060', 'Use Network Topology Info' is 'LAN 2', and 'Listen Port' is '5060'. 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0'. 'Calls Route via Registrar' is checked. 'Separate Registrar' is an empty field.

#### 5.4.4. SIP Line – SIP Credentials

The XO Communications SIP Trunking Service does not require SIP credentials for registration or authentication so the **SIP Credentials** tab has no entry.



### 5.4.5. SIP Line - SIP URI Tab

The set of SIP URI entries define which incoming calls will be accepted on the line and provide configuration control of various SIP headers for outbound calls.

For the compliance test, two SIP URIs were created: one for inbound calls and one for outbound calls.

To create the entry for inbound calls, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. The entry was created with the parameters shown below:

- Set **Local URI, Contact** and **Display Name** to **Auto**. This is equivalent to the wildcard \* used in previous releases. This setting will allow all inbound calls to be accepted. There is no matching performed on the inbound Request-URI.
- Under **Identity**, set **Identity** to **None**. This disables the sending of the P-Asserted-Identity (PAI) or P-Preferred-Identity (PPI) header in outgoing SIP requests or response messages.
- Under **Forwarding and Twinning**, set **Send Caller ID** to **Diversion Header**. This value was set to match the value needed on the outbound SIP URI described later.
- Set **Diversion Header** to **None**. This is the default value.
- For the **Registration** field, select **0: <None>** from the pull-down menu. XO Communications does not require registration or digest authentication.
- 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 in **Section 5.8.1**. For the compliance test, a new incoming group **20** was defined that only contained this line (line 20).
- Since this SIP URI is only for inbound calls, set the **Outgoing Group** field to an unused group (**0**).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

Click **OK**.

SIP Line - Line 20\*

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

URI	Groups	Local URI	Contact	Display Name	Identity	Header	Originator Number	Send Caller ID
Add...								
Remove								
Edit...								

New URI

Local URI Auto

Contact Auto

Display Name Auto

Identity

Identity None

Header P Asserted ID

Forwarding And Twinning

Originator Number

Send Caller ID Diversion Header

Diversion Header None

Registration 0: <None>

Incoming Group 20

Outgoing Group 0

Max Sessions 10

OK

Cancel

To create the entry for outbound calls, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. The entry was created with the parameters shown below:

- Set the **Local URI**, **Contact** and **Display Name** fields to **Internal Data**. These settings will populate the user portion of the From and Contact headers as well as the display name with the contents of the **User → SIP** tab (**Section 5.7**) of the user placing the call. The **User → SIP** tab is only present if a trunk in the system has a SIP URI using **Internal Data**.
- Under **Identity**, set **Identity** to **None**. This disables the sending of the P-Asserted-Identity (PAI) or P-Preferred-Identity (PPI) header in all outgoing SIP requests or response messages. By default, the PPI header will only be sent for privacy calls.
- Under **Forwarding and Twinning**, set **Send Caller ID** to **Diversion Header**. With this setting, Avaya IP Office will include the Diversion header for calls that are forwarded or directed via Mobile Twinning out the SIP Line. The Diversion header will contain the redirecting party which is a DID number provided by the service provider.
- Set **Diversion Header** to **None**. This disables the sending of the Diversion header in each outbound INVITE. The Diversion header is only sent for **Forwarding and Twinning** as described above.
- For the **Registration** field, select **0: <None>** from the pull-down menu. XO Communications does not require registration or digest authentication.
- Since this SIP URI is only for outbound calls, set the **Incoming Group** field to an unused line group (0).
- Associate this line with an outgoing line group by entering a line group number in the **Outgoing Group** field. The outgoing line group number is used in defining ARS entries for routing outbound traffic to this line in **Section 5.5**. For the compliance test, outgoing group **20** was defined that only contained this line (line 20).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

Click **OK**.

**SIP Line - Line 20\***

SIP Line Transport SIP URI VolP T38 Fax SIP Credentials SIP Advanced Engineering

URI	Groups	Local URI	Contact	Display Name	Identity	Header	Originator Number	Send Caller ID	Di
1	20 0	Auto	Auto	Auto	None	PAI		Diversion	N

Add...  
Remove  
Edit...

New URI

Local URI Use Internal Data

Contact Use Internal Data

Display Name Use Internal Data

Identity

Identity None

Header P Asserted ID

Forwarding And Twinning

Originator Number

Send Caller ID Diversion Header

Diversion Header None

Registration 0: <None>

Incoming Group 0

Outgoing Group 20

Max Sessions 10

OK  
Cancel

## 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.

- For **Codec Selection**, select **System Default** from the pull-down menu to use the default list of codecs. A list of the codecs in their current order of preference will be shown on the right in the **Selected** column. To use a custom list of codecs, select **Custom** for **Codec Selection**. Next, move unwanted codecs from the **Selected** column to the **Unused** column. Lastly, move the codecs up or down the list in the **Selected** column to achieve the desired order of preference. The example below shows the codecs used for the compliance test.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box. This enables support for Provisional Reliable Acknowledgement (PRACK).
- Set the **Fax Transport Support** to **T38 Fallback**. Using the **T38 Fallback** setting allows fax calls to fallback to G.711 fax if the request to use T.38 fax is not accepted.
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Default values may be used for all other parameters.

The screenshot displays the configuration interface for a SIP line, specifically the VoIP tab. The interface is titled "SIP Line - Line 20" and includes several tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax, SIP Credentials, SIP Advanced, and Engineering. The VoIP tab is active, showing various settings. A red box highlights the Codec Selection section, which includes a dropdown menu set to "Custom", an "Unused" column, a "Selected" column containing a list of codecs (G.729(a) 8K CS-ACELP, G.711 ULAW 64K, G.711 ALAW 64K, G.723.1 6K3 MP-MLQ, G.722 64K), and navigation buttons. Other settings include "VoIP Silence Suppression" (unchecked), "Local Hold Music" (unchecked), "Re-invite Supported" (checked), "Codec Lockdown" (unchecked), "Allow Direct Media Path" (unchecked), "Force direct media with phones" (unchecked), "PRACK/100rel Supported" (checked), "G.711 Fax ECAN" (unchecked), "Fax Transport Support" set to "T38 Fallback", "DTMF Support" set to "RFC2833", and "Media Security" set to "Disabled".

### 5.4.7. SIP Line – T38 Fax Tab

Select the **T38 Fax** tab. Leave the **Use Default Values** box checked at the bottom of the screen.

The screenshot shows the configuration window for 'SIP Line - Line 20'. The 'T38 Fax' tab is selected. The window contains several configuration fields and checkboxes. At the bottom left, the 'Use Default Values' checkbox is checked and highlighted with a red box.

Field	Value
T38 Fax Version	3
Transport	UDPTL
Redundancy	
Low Speed	0
High Speed	0
TCF Method	Trans TCF
Max Bit Rate (bps)	14400
EFlag Start Timer (ms)	2600
EFlag Stop Timer (ms)	2300
Tx Network Timeout (sec)	150

- Scan Line Fix-up
- TFOP Enhancement
- Disable T30 ECM
- Disable EFlags For First DIS
- Disable T30 MR Compression
- NSF Override

Field	Value
Country Code	0
Vendor Code	0

Use Default Values

## 5.4.8. SIP Line – SIP Advanced

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

- Set **Call Routing Method** to **Request-URI**. Avaya IP Office will route calls based on the contents of Request URI in the incoming INVITE.
- Check the **Emulate NOTIFY for REFER** box. With REFER enabled, the Avaya 1100 Series Deskphones and Avaya Communicator for Windows expects to receive a NOTIFY message to indicate that the referred (i.e., transferred) call was successful. If the NOTIFY is not received from the far-end, then the call display will indicate that the transfer failed even if the transfer was successful. If the **Emulate NOTIFY for REFER** box is checked, then Avaya IP Office will send a NOTIFY message (on behalf of the far-end) to the Avaya 1100 Series Deskphones and Avaya Communicator for Windows.
- The **No REFER if using Diversion** box is checked to prevent Avaya IP Office from using the SIP REFER method on call forward scenarios that use the Diversion SIP header.

Click the **OK** button at the bottom of the page (not shown).

The screenshot shows the 'SIP Line - Line 20' configuration window with the 'SIP Advanced' tab selected. The 'Call Routing Method' is set to 'Request URI'. The 'Emulate NOTIFY for REFER' and 'No REFER if using Diversion' checkboxes are checked. The 'Association Method' is set to 'By Source IP address'. The 'Suppress DNS SRV Lookups' checkbox is unchecked. The 'Identity' section has 'Cache Auth Credentials' checked. The 'Media' section has 'P-Early-Media Support' set to 'None' and 'Media Connection Preservation' set to 'Disabled'. The 'Call Control' section has 'Call Initiation Timeout (s)' set to 4, 'Call Queuing Timeout (mins)' set to 5, 'Service Busy Response' set to '486 - Busy Here', 'on No User Responding Send' set to '408-Request Timeout', and 'Action on CAC Location Limit' set to 'Allow Voicemail'. The 'Suppress Q,850 Reason Header' checkbox is unchecked.

## 5.5. Alternate Route Selection (ARS)

Alternate Route Selection (ARS) is used to route outbound traffic to the SIP line. To define a new ARS route, right-click **ARS** in the Navigation pane and select **New**. In the Details pane that appears, enter a name for the route in the **Route Name** field and a collection of matching patterns (similar to short codes) can be entered to route calls as shown below.

For the compliance test, two entries were created. The first entry matches on **0** and the second entry matches on any other number **N**.

To create an entry, click the **Add** button and enter the following in the pop-up window (not shown).

- In the **Code** field, enter the pattern to match the number passed to ARS from the short code in **Section 5.6**. The value **N;** will match any number.
- For **Code 0**, set **Telephone Number** to **0"@ipaddr"**, where *ipaddr* is the IP address of the XO Communications SIP proxy and used to configure the trunk in **Section 5.4.3**. Adding the IP address in this field was required to ensure that the correct Request-URI header appears in the outbound INVITE when dialing 0. This was not required when matching on any other dialed number as shown next.
- For **Code N;**, set **Telephone Number** to **N**. This field is used to construct the Request-URI and To headers in the outgoing SIP INVITE message. The value **N** represents the complete number passed to ARS.
- Set **Feature** to **Dial**. This is the action that the entry will perform.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4.5**. This entry will use this line group when placing the outbound call.

Click the **OK** button (not shown).

Code	Telephone Number	Feature	Line Group ID
0	0"@192.168.163.138"	Dial	20
N;	N	Dial	20

## 5.6. Short Codes

A short code is a dial pattern that triggers a specific function. A short code is used by the caller to route outbound traffic to ARS. To create a short code, right-click on **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as shown below.

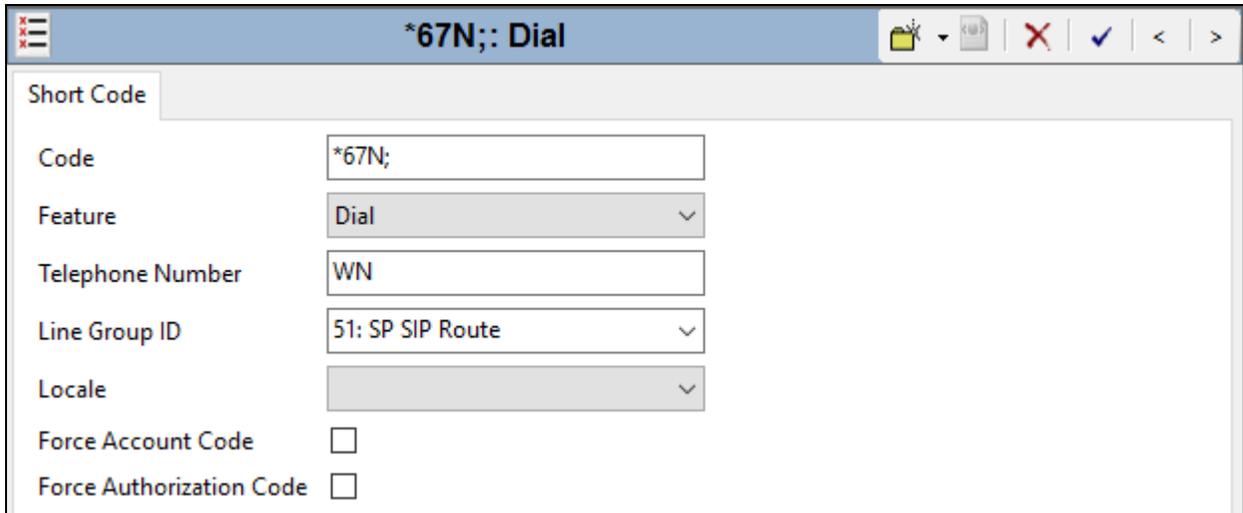
- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **9N;**. This short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone 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 the ARS route to be used (**Section 5.5**).

Click the **OK** button (not shown).

The screenshot shows the Avaya Management System interface. On the left is the 'IP Offices' navigation pane with a tree view including categories like BOOTP (3), Operator (3), Atlantic City, System (1), Line (25), Control Unit (3), Extension (25), User (27), Group (1), Short Code (65), Service (0), RAS (1), Incoming Call Ro, and WAN Port (0). The 'Short Code (65)' item is selected. The main pane is titled '9N;; Dial' and shows the configuration for a Short Code. The fields are: Code (9N;;), Feature (Dial), Telephone Number (N), Line Group ID (51: SP SIP Route), and Locale (dropdown). There are also checkboxes for Force Account Code and Force Authorization Code, both of which are unchecked. A red rectangular box highlights the Code, Feature, Telephone Number, and Line Group ID fields.

Optionally, add or edit a short code that can be used to access the SIP Line anonymously. In the screen shown below, the short code \*67N; is illustrated. This short code is similar to the 9N; short code except that the **Telephone Number** field begins with the letter **W**, which means “withhold the outgoing calling line identification”.

In the case of the SIP Line documented in these Application Notes, when a user dials \*67 plus the number, Avaya IP Office will include the calling number in the P-Preferred-Identity (PPI) header and will include the Privacy: Id header.

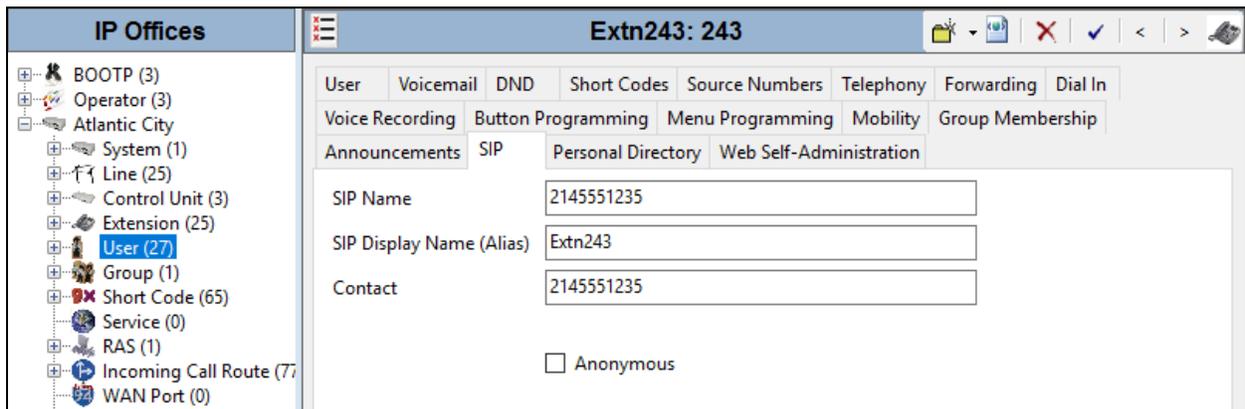


Short Code	
Code	*67N;
Feature	Dial
Telephone Number	WN
Line Group ID	51: SP SIP Route
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

## 5.7. User

If the SIP Line is configured to use **Internal Data** in **Section 5.4.5**, then configure the SIP parameters for each user that will be placing and receiving calls via the SIP line. 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 **Extn243**. Select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers for outgoing SIP trunk calls (**Section 5.4.5**). The example below shows the settings for user **Extn243**. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise from XO Communications. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network.

Click the **OK** button (not shown).



The screenshot displays the Avaya user configuration interface for user **Extn243: 243**. The left pane shows the navigation tree with **User (27)** selected. The right pane shows the configuration details for the selected user, with the **SIP** tab active. The configuration fields are as follows:

Field	Value
SIP Name	2145551235
SIP Display Name (Alias)	Extn243
Contact	2145551235

Below the fields, there is an **Anonymous** checkbox, which is currently unchecked.

## 5.8. Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by the service provider. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**.

### 5.8.1. Incoming Call Route – Standard Tab

On the **Standard** tab of the Details Pane, enter the parameters as shown below.

- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.4.5**.
- Set the **Incoming Number** to the incoming number on which this route should match.
- Default values can be used for all other fields.

The screenshot shows the configuration window for an Incoming Call Route. The left pane shows the navigation tree with 'Incoming Call Route (7)' selected. The right pane shows the 'Standard' tab with the following fields:

Bearer Capacity	Any Voice
Line Group ID	20
Incoming Number	2145551235
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

### 5.8.2. Incoming Call Route – Destinations Tab

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. Click the **OK** button (not shown). In this example, the incoming number on line 20 is routed to extension 243.

The screenshot shows the 'Destinations' tab of the configuration window. It contains a table with the following data:

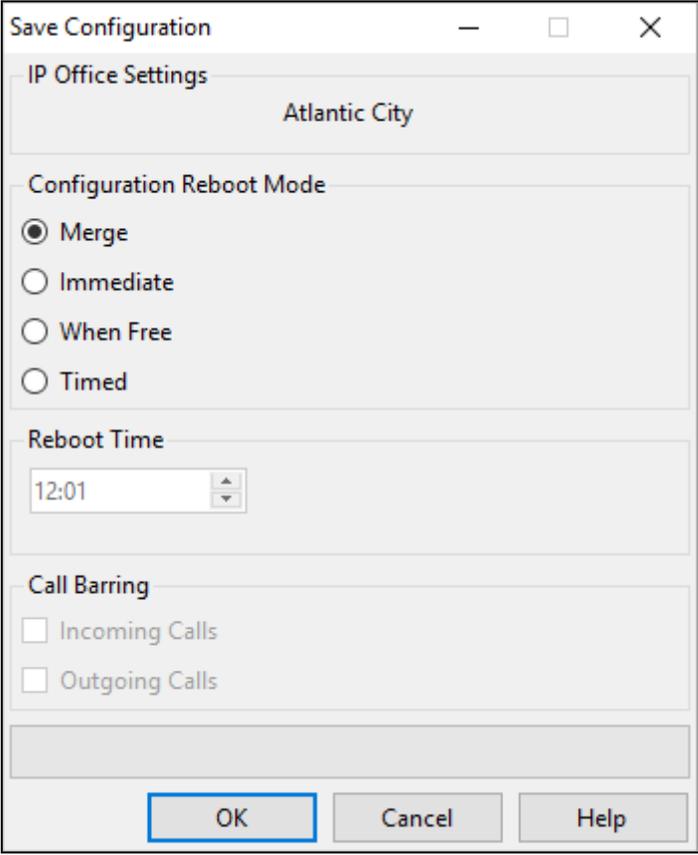
TimeProfile	Destination	Fallback Extension
Default Value	243 Extn243	

Incoming call routes for other direct mappings of DID numbers to Avaya IP Office users listed in **Figure 1** are omitted here, but can be configured in the same fashion. Incoming call routes can also be mapped to voicemail or short codes.

## 5.9. Save Configuration

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

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



The screenshot shows a 'Save Configuration' dialog box with the following sections:

- IP Office Settings**: Atlantic City
- Configuration Reboot Mode**:
  - Merge
  - Immediate
  - When Free
  - Timed
- Reboot Time**: 12:01 (with a time selection spinner)
- Call Barring**:
  - Incoming Calls
  - Outgoing Calls

At the bottom, there are three buttons: **OK** (highlighted with a blue border), **Cancel**, and **Help**.

## 6. XO Communications SIP Trunking Service Configuration

XO Communications is responsible for the configuration of the XO Communications SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise. In the case of the compliance test, this is the public IP address of the Avaya IP Office. XO Communications will provide the customer the necessary information to configure Avaya IP Office including:

- XO Communications SIP proxy IP address
- Supported codecs
- Transport protocol and port
- DID numbers

In addition, to configure any possible firewall/security devices at the enterprise, XO Communications will provide the IP address and port of any media sources that will need access to the enterprise.

## 7. Verification Steps

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

### 7.1. Avaya IP Office

#### 7.1.1. System Status

The System Status application is used to monitor and troubleshoot Avaya IP Office. Use the System Status application to verify the state of the SIP trunk. System Status can be accessed from **Start → All Programs → IP Office → System Status**.

The following screen shows an example **Logon** screen. Enter the Avaya IP Office IP address in the **Control Unit IP Address** field, and enter an appropriate **User Name** and **Password**. Click **Logon**.



The screenshot displays the Avaya IP Office System Status application window. The title bar reads "Avaya IP Office System Status". The main window features the Avaya logo and the text "IP Office System Status". Below this is a menu bar with "Help", "Exit", and "About". The main content area has a status indicator showing "Online" and "Offline" tabs. The "Logon" screen is active, featuring a blue background with the following fields and options:

- Control Unit IP Address:** A dropdown menu showing "10.32.128.25".
- Services Base TCP Port:** A text input field containing "50804".
- User Name:** A text input field containing "Administrator".
- Password:** A text input field.
- Auto reconnect
- Secure connection
- Logon** button

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

The screenshot shows the Avaya IP Office System Status interface. The left pane shows a tree view with 'Trunks (25)' expanded to 'Line: 20'. The right pane has tabs for 'Status', 'Utilization Summary', and 'Alarms'. The 'Status' tab is active, displaying the 'SIP Trunk Summary' for Line 20. Below the summary is a table with columns: Channel Number, U..., Call Ref, Current State, Time in State, Remote Media ..., Co..., Conn..., Caller ID or ..., Other Party on Call, Directi..., Round Trip ..., Receive Jitter, Receive Pack..., Trans..., and Trans... The table shows 7 channels, all with a 'Current State' of 'Idle' and a 'Time in State' of '2 day...'. At the bottom of the interface are buttons for 'Trace', 'Trace All', 'Pause', 'Ping', 'Call Details', 'Graceful Shutdown', 'Force Out of Service', 'Print...', and 'Save As...'. A green progress indicator shows 0% for SIP Trunk Channel Licenses in Use.

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

The screenshot shows the 'Alarms' tab selected in the Avaya IP Office System Status interface. The title is 'Alarms for Line: 20 SIP 192.168.163.138'. Below the title is a table with columns: 'Last Date Of Error', 'Occurrences', and 'Error Description'. The table is currently empty, indicating no active alarms.

## 7.1.2. Monitor

The Monitor application can also be used to monitor and troubleshoot Avaya IP Office. Monitor can be accessed from **Start → All Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select **Filters → Trace Options**.

The following screen shows the **SIP** tab, allowing configuration of SIP monitoring.

The screenshot shows the 'All Settings' dialog box with the 'SIP' tab selected. The dialog is organized into several sections:

- Events:** Includes checkboxes for 'Sip' (checked), 'STUN' (checked), and 'SIP Dect' (unchecked). A dropdown menu is set to 'Standard'.
- Packets:** Includes checkboxes for 'SIP Reg/Opt Rx', 'SIP Reg/Opt Tx', 'SIP Call Rx', 'SIP Call Tx', 'SIP Misc Rx', 'SIP Misc Tx', 'Cm Notify Rx', and 'Cm Notify Tx', all of which are currently unchecked.
- IP Filter:** A section with 'Sip Rx' (checked) and 'Sip Tx' (checked) checkboxes, followed by an 'IP Filter (nnn.nnn.nnn.nnn)' label and an empty text input field.
- Buttons:** A row of buttons at the bottom: 'Default All', 'Clear All', 'Tab Clear All', 'Tab Set All', 'OK', and 'Cancel'. Below this is another row: 'Save File', 'Load File', 'Load Partial File', and 'Select File'.

## 8. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office 10.0 to the XO Communications SIP Trunking Service. The XO Communications SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks. The XO Communications SIP Trunking Service passed compliance testing. Please refer to **Section 2.2** for any observations/exceptions.

## 9. Additional References

This section references documentation relevant to these Application Notes. In general, Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 31g, August 3, 2016.
- [2] *Administering Avaya IP Office Platform with Manager*, Release 10, September 2016.
- [3] *Using System Status*, Document Number 15-601758, Issue 11e, July 7, 2016.
- [4] *Administering Avaya IP Office Voicemail Pro*, Document Number 15-601063, Issue 11e, July 20, 2016.
- [5] *Using IP Office System Monitor*, Document Number 15-601019, Issue 07b, June 9, 2016.

Additional Avaya IP Office documentation can be found at:

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

---

**©2017 Avaya Inc. All Rights Reserved.**

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

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