



Application Notes for Configuring Avaya IP Office Release 11.0 to support G12 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 11.0 to support G12 SIP Trunking Service.

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

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

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

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between G12 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 and an Avaya IP Office 500 V2 expansion running software release 11.0 (hereafter referred to as IP Office) and various Avaya endpoints, listed in **Section 4**.

The G12 SIP Trunking Service within these Application Notes is designed for business customers. Customers using this service with the IP Office solution are able to place and receive PSTN calls via a broadband wide area network (WAN) connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

The terms “service provider” or “G12” 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 G12’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:

-
- 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 Equinox for Windows soft-client.
- Dialing plans including local calls, outbound toll-free, etc.
- Caller ID presentation.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two-way speech-path. Testing was performed with codecs: G.711MU and G.729A.
- Proper response to no matching codecs.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.
- T.38 and G.711 pass-through fax.

Items not supported or not tested included the following:

- Inbound toll-free calls were not tested.
- 911 Emergency call was not tested.

2.2. Test Results

Interoperability testing of G12 SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Outbound Anonymous Calls** – When privacy is enabled at the IP Office station (Withhold Number enabled), the SIP INVITE toward G12 does not include the “Privacy: id” header and the **From** header is masked out as “anonymous@anonymous.invalid”. This is causing G12 to drop the outbound privacy call because G12 authenticates the call based on the allowed IP address in the **From** header. To configure the outbound privacy call, set the PAI field of the **Call Details** to “**Use Internal Data**” (Section 5.4.4) and enable anonymous check box in the SIP tab of the user in Section 5.8.
- **OPTIONS** – G12 does not send OPTIONS messages to the Avaya enterprise network, but it does respond to OPTIONS messages received from the Avaya enterprise, this was sufficient to maintain the SIP trunk link up in service.
- **T.38 Fax** – G12 does not support the method in which IP Office negotiates the use of T.38 for fax, which consist of IP Office sending a re-INVITE message with two media lines in the SDP, with the first media line set for audio, with the port set to 0, and the second media line set for T.38, with a valid port number, thus de-activating audio transmission for the call. A SIP Line Custom String (SLIC) was added to the IP Office configuration used during the testing, as shown in Section 5.4.7. With the configuration shown in Section 5.4.7, IP Office will reverse the order of media line entries in the SDP, so that the active T.38 media line entry appears first, followed by the inactive audio media line entry, with the port set to 0. With the addition of the SIP Line Custom String (SLIC), G12 responded successfully to the re-INVITE message sent by Avaya IP Office with "200 OK" and the T.38 fax calls worked properly in both directions.

2.3. Support

For support on G12 SIP Trunking Service visit the corporate Web page at:
<https://www.g12com.com/advanced-sip-trunking/>

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 G12 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 Virtualized environment.
 - Avaya IP Office Voicemail Pro.
- Two Avaya IP Office 500 V2 as expansion systems.
- Avaya 96x1 Series IP Deskphones (H.323).
- Avaya 1100 Series IP Deskphones (SIP).
- Avaya J129 IP Deskphones (SIP).
- Avaya 1400 Series Digital Deskphones.
- Analog Deskphones.
- Avaya Equinox™ for Windows softphone (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 system 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 Equinox™ for Windows Softphones (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 G12, 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 G12 network. The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to G12 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.

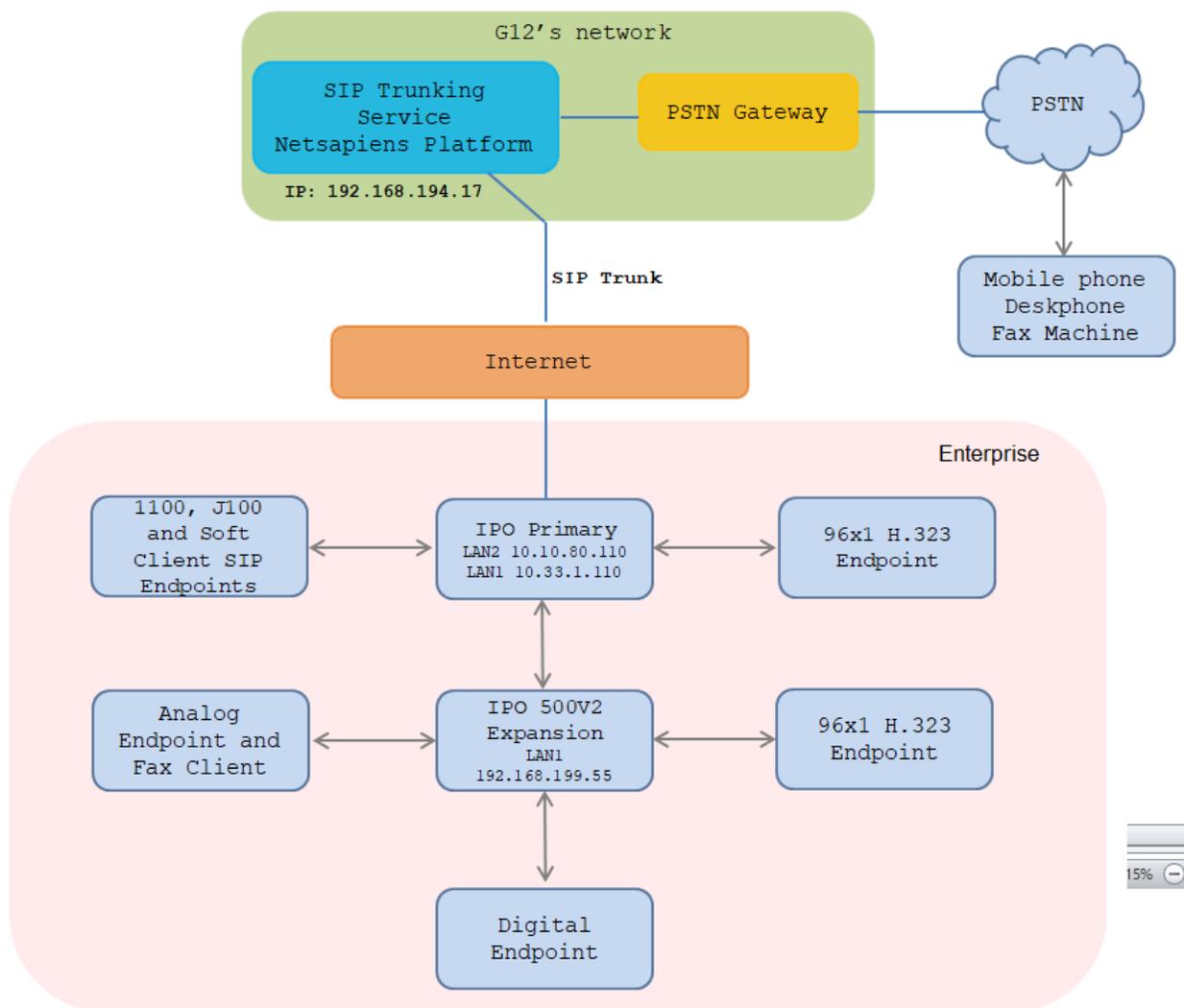


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

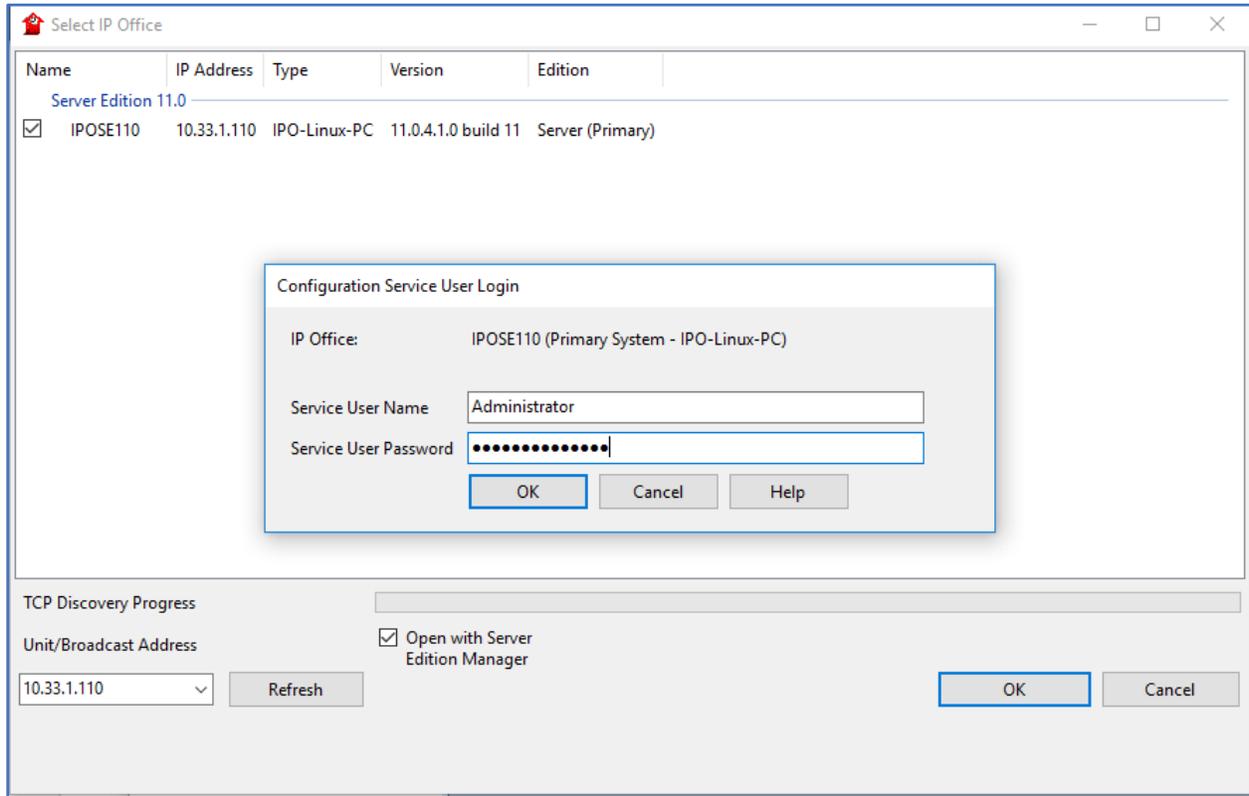
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server) <ul style="list-style-type: none">• Avaya IP Office Voicemail Pro	11.0.4.1.0 Build 11 11.0.4.1.0 Build 2
Avaya IP Office IP500 V2 (Expansion Systems)	11.0.4.1.0 Build 11
Avaya IP Office Manager	11.0.4.1.0 Build 11
Avaya 96x1 Series IP Deskphones (H.323)	6.8002
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.0.0.0.21
Avaya 1408 Digital Telephone	48.02
Avaya Equinox™ for Windows (SIP)	3.6.0.153.36
Analog Telephone	---
G12	
Netsapiens	Version 40

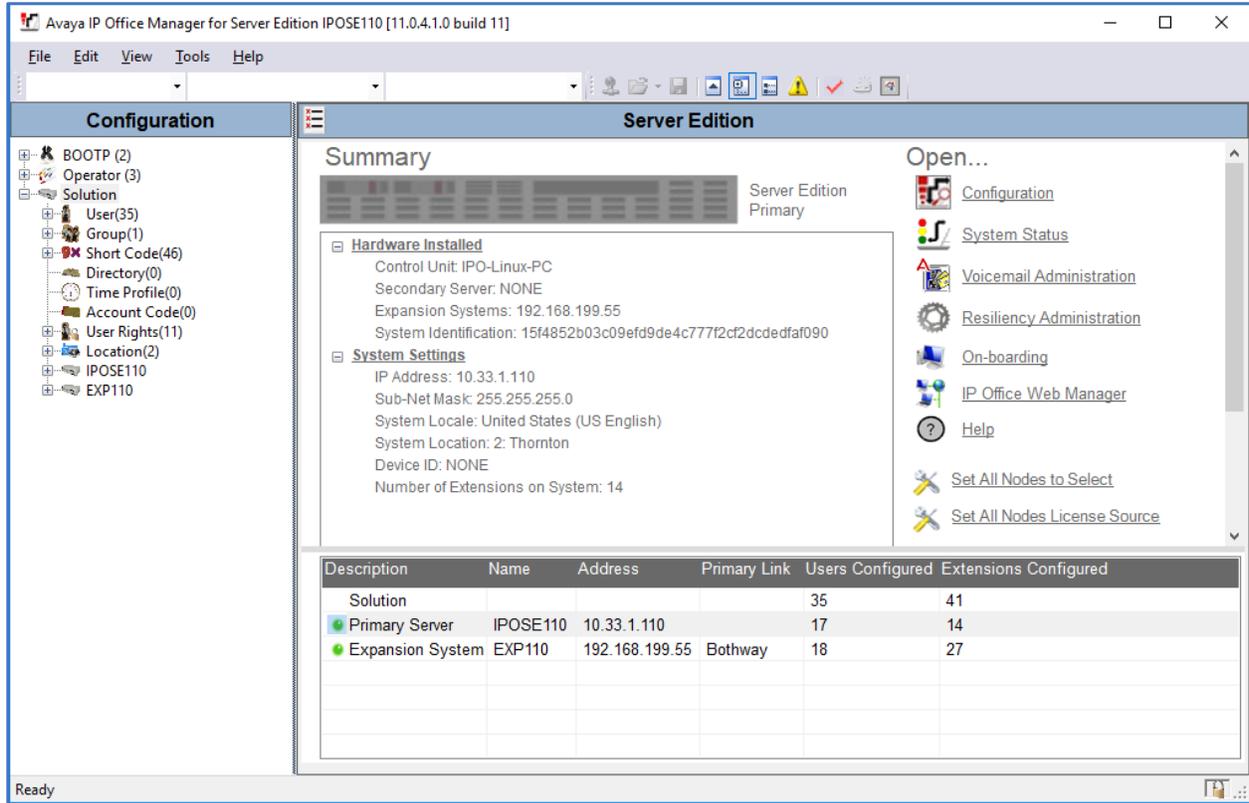
Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints.

5. Avaya IP Office Primary Server Configuration

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



On Server Edition systems, the Solution View screen will appear, similar to the one shown below. All the Avaya IP Office configurable components are shown in the left pane, known as the Navigation Pane. Clicking the “plus” sign next to the Primary server system name, e.g., **IPOSE110**, on the navigation pane will expand the menu on this server.



In the screens presented in the following sections, the View menu was configured to show the Navigation pane on the left side and the Details pane on the right side. These panes will be referenced throughout the rest of this document.

Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

5.1. Licensing

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

In the reference configuration, **IPOSE110** was used as the system name of the Primary Server and **EXP500** was used as the system name of the Expansion System. All navigation described in the following sections (e.g., **License**) appears as submenus underneath the system name in the Navigation Pane.

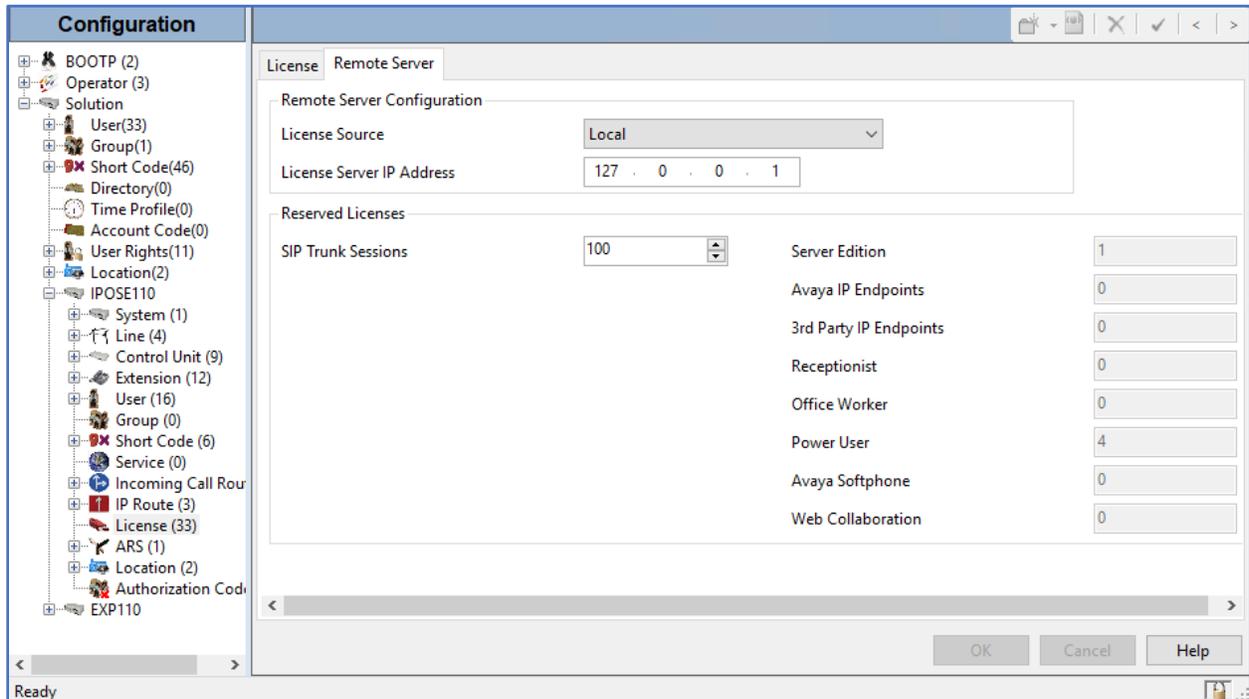
Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of channels provisioned for the SIP trunk.

The screenshot shows the Avaya IP Office Configuration Manager interface. On the left is the 'Configuration' navigation pane with a tree view. The 'License' option is selected under the 'IPOSE110' system. The main pane displays a table of licenses for the 'Remote Server'.

Feature	Instances	Status	Expiration Date	Source
Teleworker	384	Obsolete	Never	PLDS Nodal
Mobile Worker	384	Obsolete	Never	PLDS Nodal
Office Worker	384	Never	Never	PLDS Nodal
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	40	Obsolete	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	10	Obsolete	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal
SIP Trunk Channels	512	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	10	Valid	Never	PLDS Nodal
Wave User	16	Obsolete	Never	PLDS Nodal
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal
Essential Edition	10	Obsolete	Never	PLDS Nodal
R8+ Preferred Edition (VM Pro)	10	Obsolete	Never	PLDS Nodal
Server Edition	5	Valid	Never	PLDS Nodal
HIMS Web Services	100	Valid	Never	PLDS Nodal

The interface includes an 'Add...' button and a 'Remove' button on the right side of the table. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

On Server Edition systems, the number 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. Note that if **SIP Trunk Sessions** is not set in the **Reserved Licenses** section, the incoming call to IPO via SIP trunk will be rejected with the error “503 Service Not Available”.



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).

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 G12 SIP Trunking Service, and therefore is not described in these Application Notes.

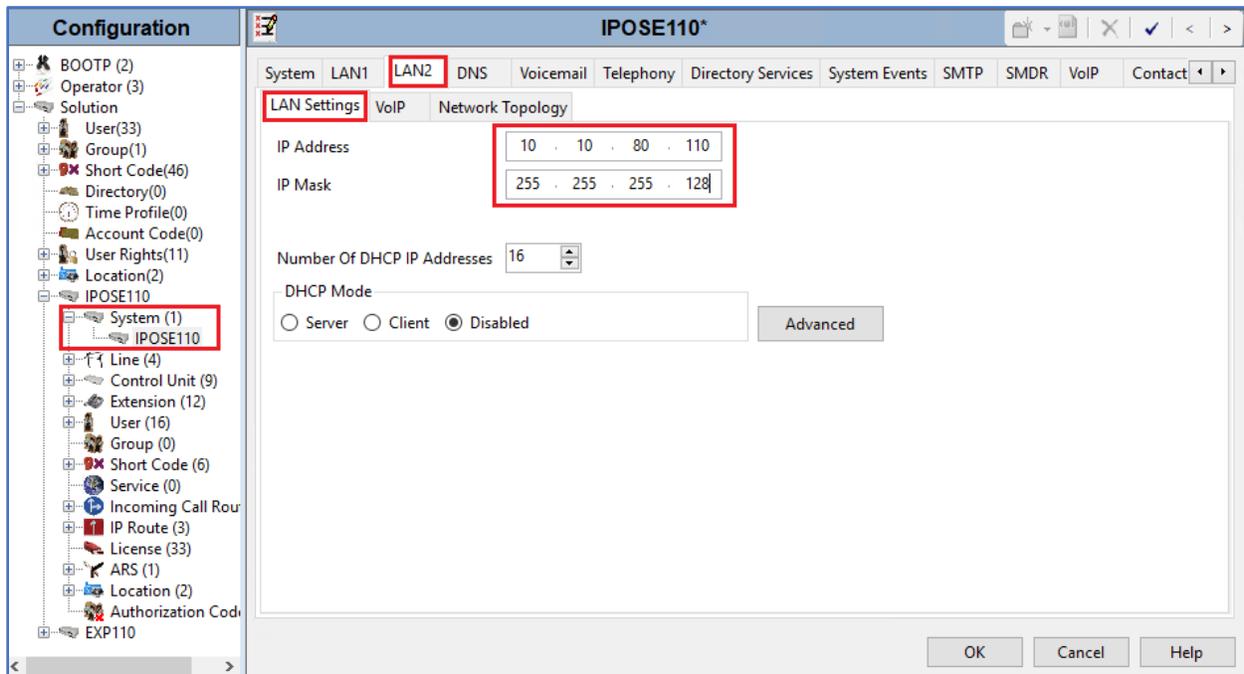
5.2.1. System – LAN2 Tab

In the sample configuration, the LAN2 interface is used for the SIP trunk connection to G12.

5.2.1.1 LAN2 - LAN Settings Tab

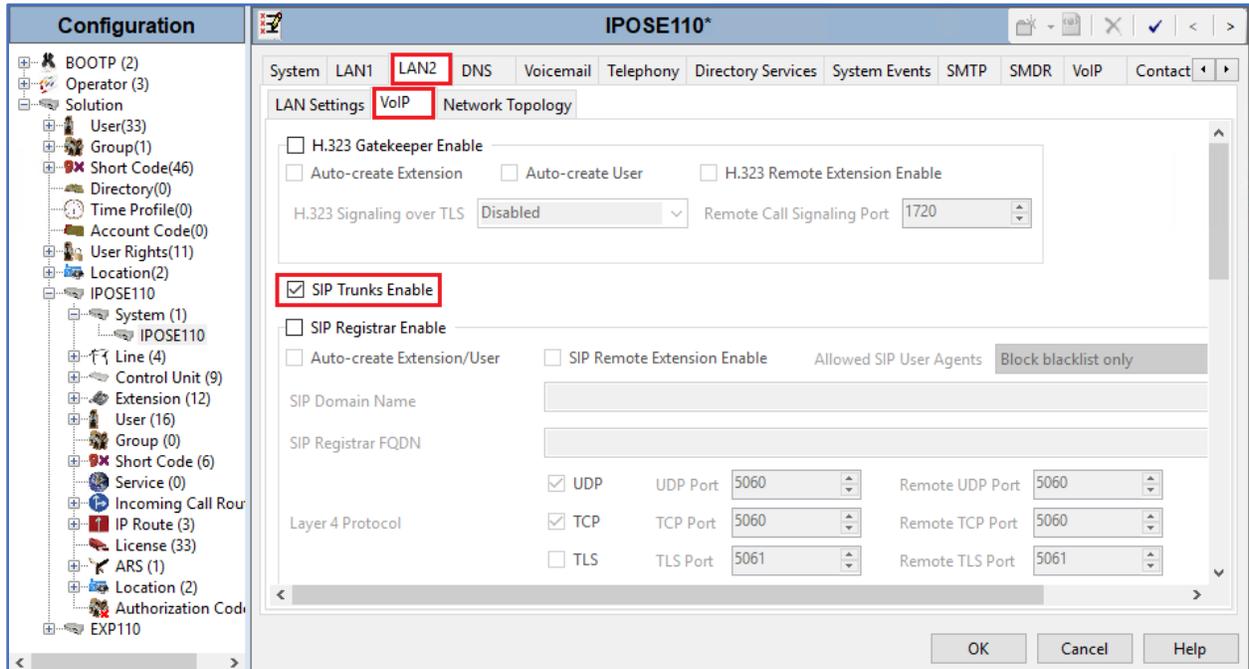
To view or configure the LAN2 IP address and subnet mask, select the **LAN2 → LAN Settings** tab, and enter the information as needed, according to the customer network requirements:

- **IP Address: 10.10.80.110** 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.



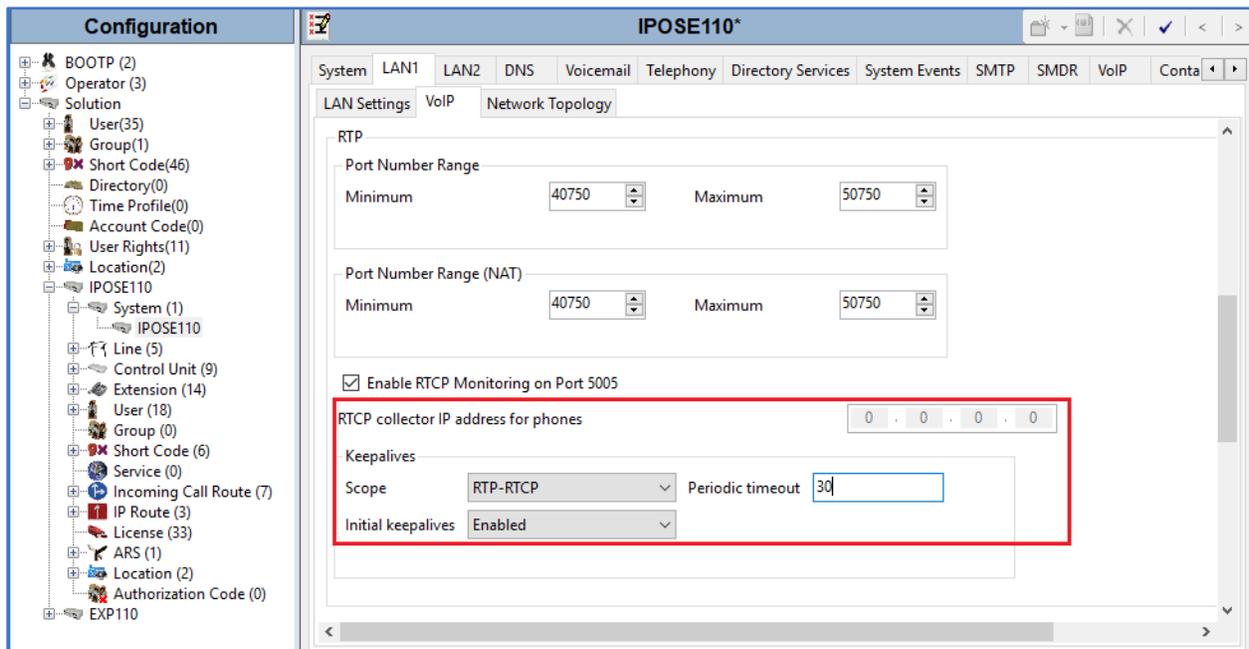
5.2.1.2 LAN2 VoIP Tab

- 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.



Scroll down the page:

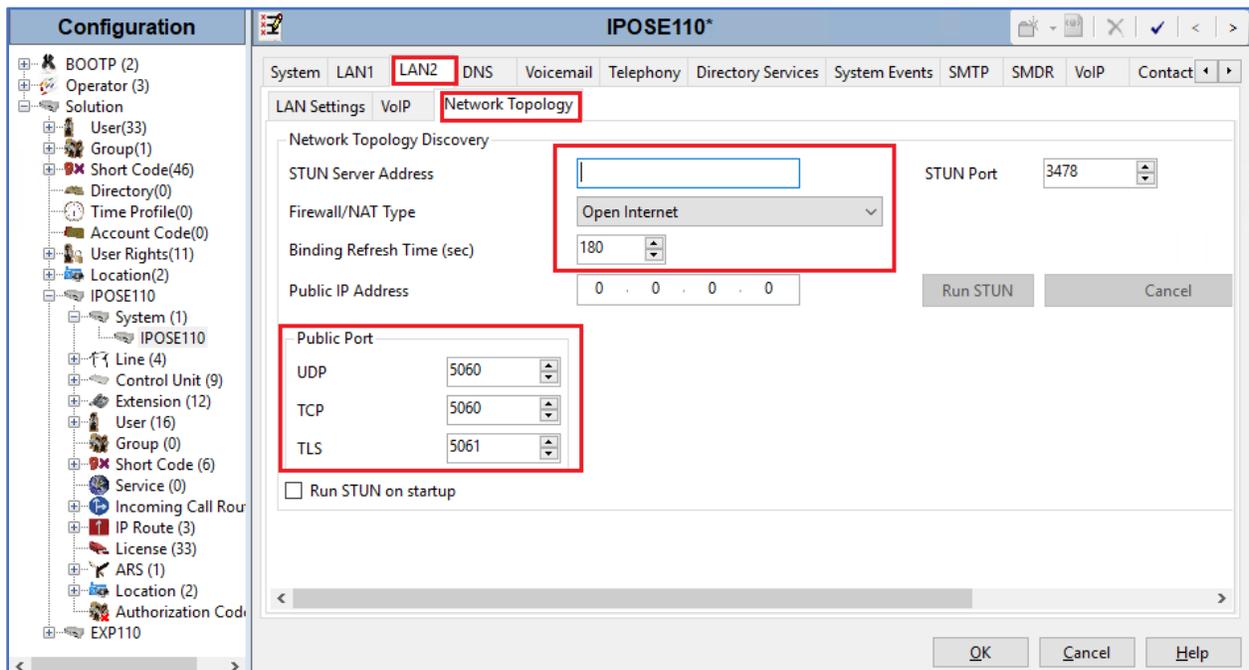
- Verify the **RTP Port Number Range**. Based on this setting, Avaya IP Office will request RTP media to be sent to a UDP port in the configurable range for calls using LAN2. The **Minimum** and **Maximum** port numbers were kept at their default values in the reference configuration.
- In the **Keepalives** 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).



5.2.1.3 LAN2 - Network Topology Tab

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

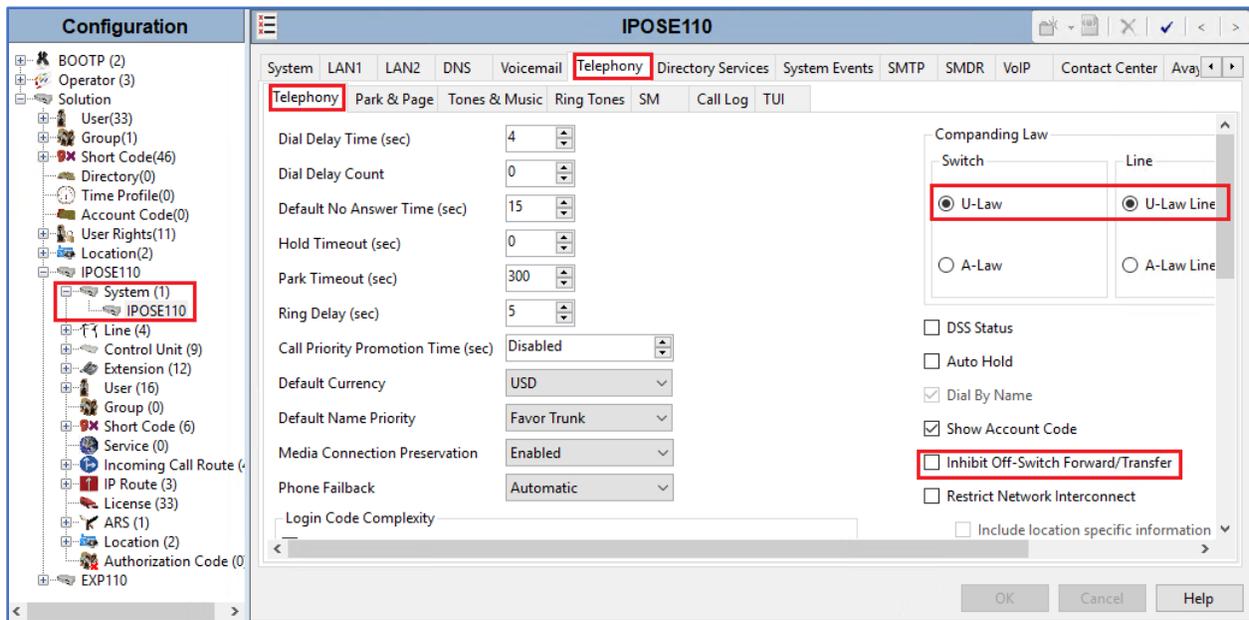
- Select the **Firewall/NAT Type** from the pull-down menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used.
- Set **Binding Refresh Time (seconds)** to **180**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider.
- Set **Public Port** to **5060** for **UDP**.
- Default values were used for all other parameters.
- Click the **OK** button (not shown).



5.2.2. 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).



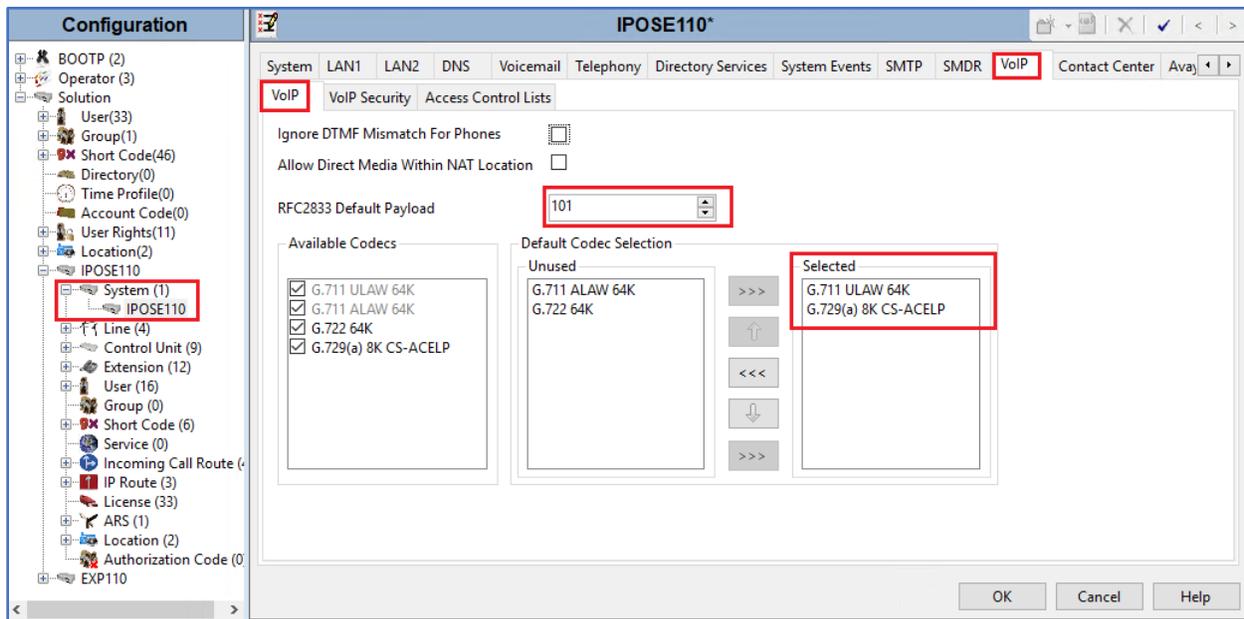
5.2.3. VoIP Tab

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

5.2.3.1 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).



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 5.4.5** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.2.3.2 VoIP – VoIP Security Tab

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

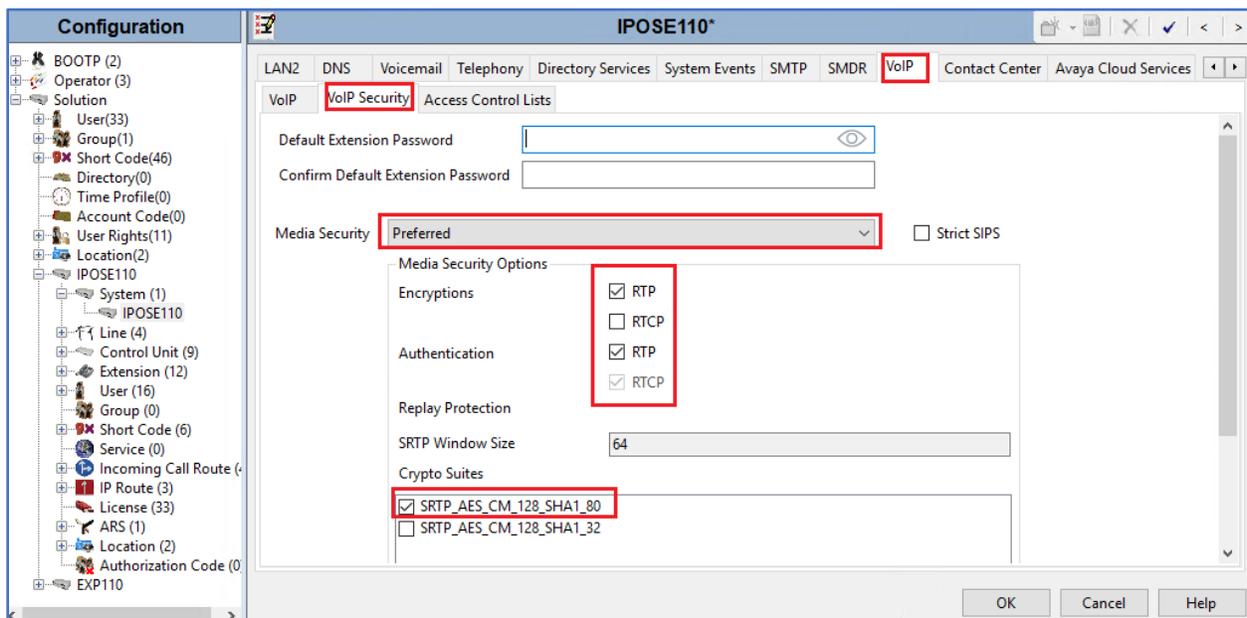
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

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

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

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

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

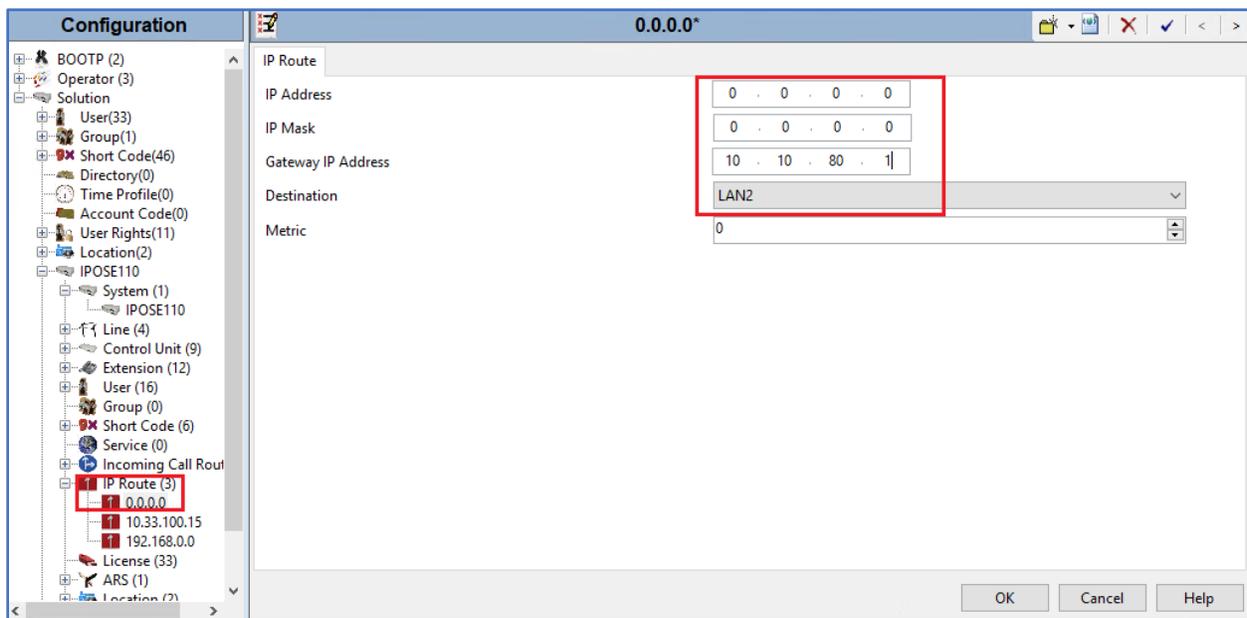


5.3. IP Route

Create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to route calls to G12 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).



5.4. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and G12. 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**.

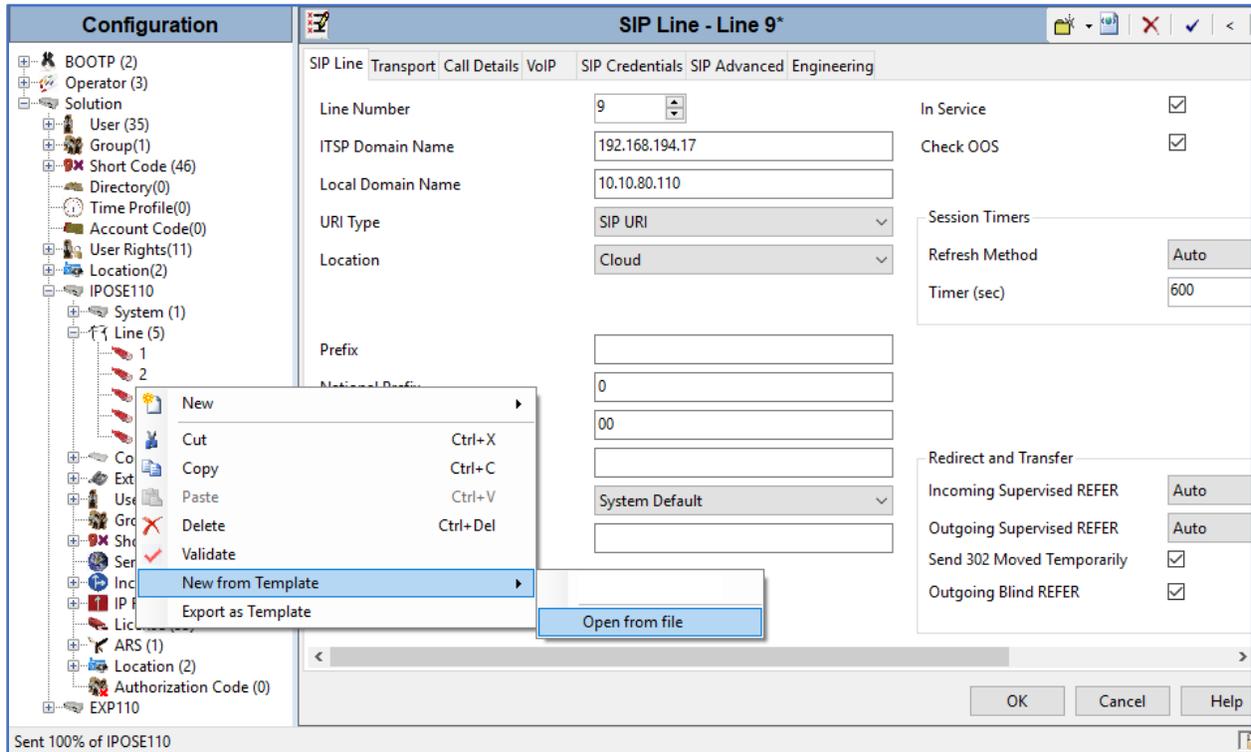
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.7**.

5.4.1. Creating a SIP Trunk from an XML Template

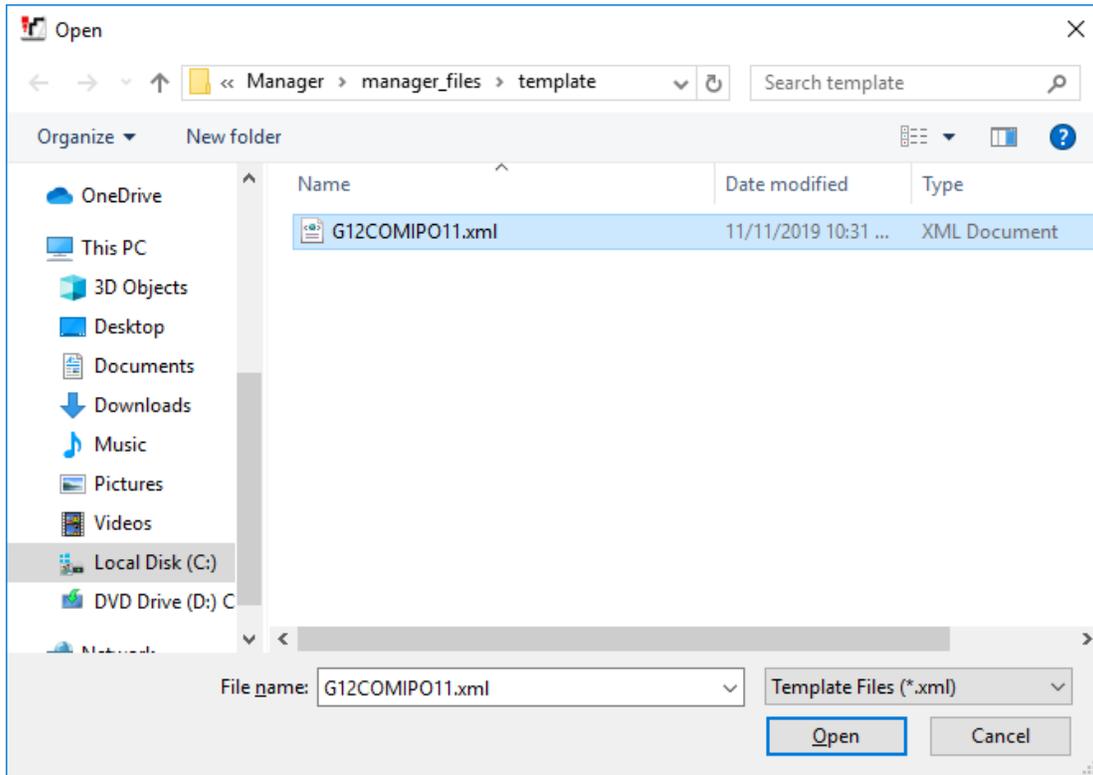
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and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

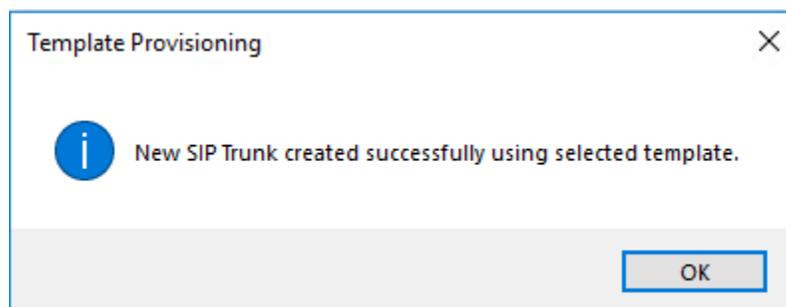
To create the SIP Trunk from the template, from the **Primary** server (**IPOSE110**), right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template → Open from file**.



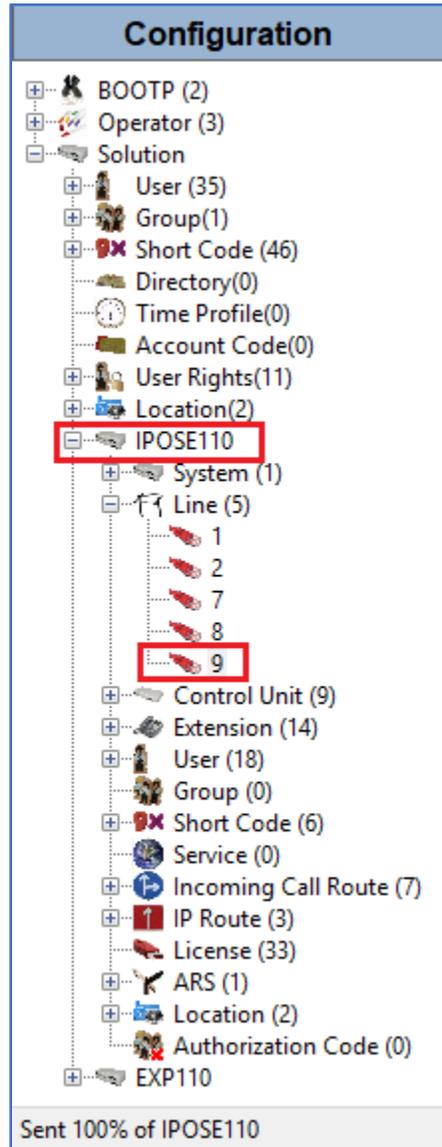
Navigate to the directory on the local machine where the template was copied and select the template.



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 7).



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 the IP address of G12 SIP Trunking service.
- Set **Local Domain Name** to the LAN2 IP address of IPO.
- Verify that **In Service** box is checked, the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (sec)** is set to **On Demand**.
- For the compliance test **Incoming Supervised REFER** and **Outgoing Supervised REFER** was set to **Auto**. G12 supports the SIP REFER and RE-Invite methods for call transfers to the PSTN but the REFER method was used for the testing.
- Click **OK** to commit (not shown).

The screenshot displays the configuration window for a SIP Line, titled "SIP Line - Line 9". The window is divided into a left-hand navigation pane and a main configuration area. The navigation pane shows a tree structure of system components, with "Line 9" selected. The main configuration area is titled "SIP Line" and contains several tabs: "SIP Line", "Transport", "Call Details", "VoIP", "SIP Credentials", "SIP Advanced", and "Engineering". The "SIP Line" tab is active, showing the following configuration fields and options:

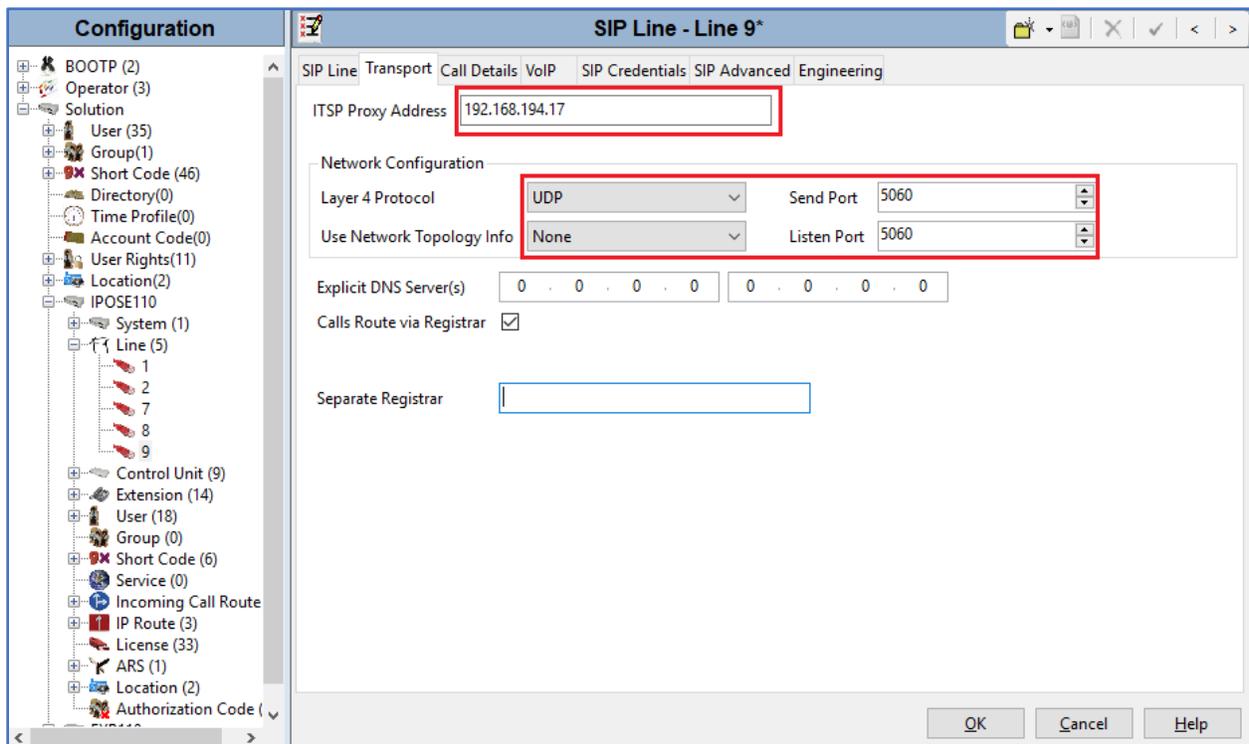
- Line Number:** 9
- ITSP Domain Name:** 192.168.194.17
- Local Domain Name:** 10.10.80.110
- URI Type:** SIP URI
- Location:** Cloud
- Prefix:** (empty)
- National Prefix:** 0
- International Prefix:** 00
- Country Code:** (empty)
- Name Priority:** System Default
- Description:** (empty)
- In Service:**
- Check OOS:**
- Session Timers:**
 - Refresh Method:** Auto
 - Timer (sec):** On Demand
- Redirect and Transfer:**
 - Incoming Supervised REFER:** Auto
 - Outgoing Supervised REFER:** Auto
 - Send 302 Moved Temporarily:**
 - Outgoing Blind REFER:**

At the bottom of the window, there are three buttons: "OK", "Cancel", and "Help".

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 SIP Proxy IP address provided by G12, **192.168.194.17** was used during the compliance test.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **None** (refer to the note below).
- Set the **Send Port** to **5060** (G12 uses the standard UDP port 5060).
- Set the **Listen Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



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 – 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 compliance test, two entries were created: one for incoming call and one for outgoing call.

The entry for incoming and outgoing calls was created with the parameters shown below:

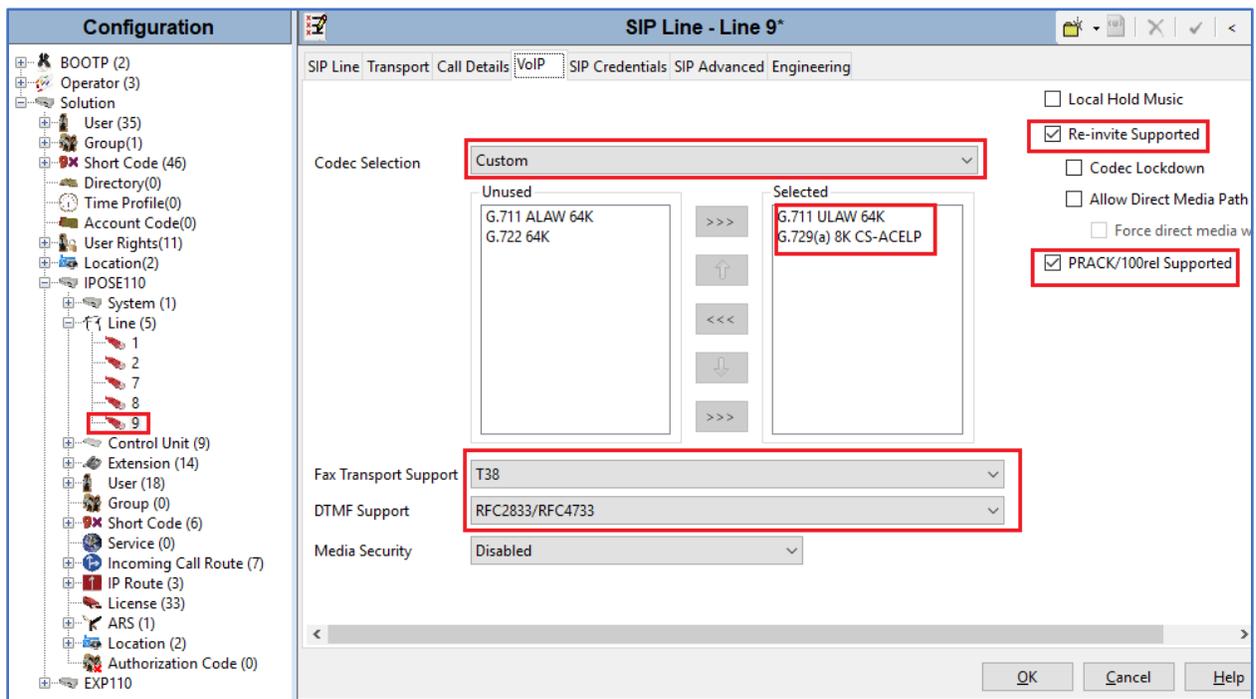
- Associate this line with an incoming line group by entering the line group number (line 9) in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line.
- Associate the line to an outgoing line group using the **Outgoing Group** field. In the compliance test, the entry for outgoing call was used to create short codes.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Leave the **Credentials** field as blank.
- Check the **P Asserted ID** and set the **Content** field as “**Use Internal Data**”, refer the test results in **Section 2.2** for more detail.
- Set the **Local URI**, **Contact** and **P Asserted ID** as shown in the screenshot below, these settings are default values.
- Click **OK**.
- Click **OK** to commit again (not shown).

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

5.4.5. 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. G12 supports codecs **G.711ULAW** and **G729(a)** for audio.
- Select **T.38** for **Fax Transport Support** (refer to **Section 2.2** for fax limitations).
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).



Note: The codec selections defined under this section are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.3.1** are the codecs selected for the IP phones/extension (H.323 and SIP).

5.4.6. SIP Line – SIP Advanced Tab

In the **Addressing** area:

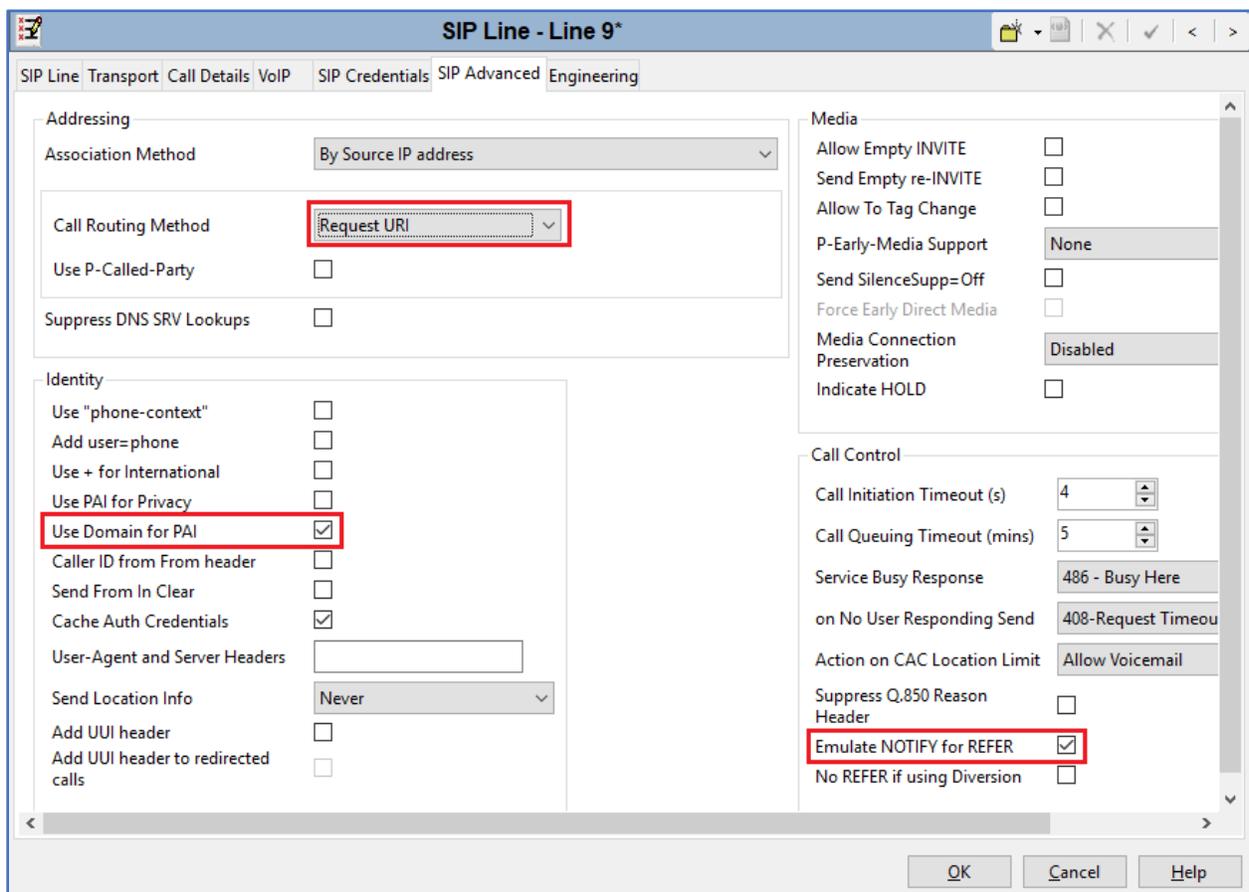
- Select **Request URI** for **Call Routing Method**.

In the **Identity** area:

- Check the box for **Use PAI for Privacy**.

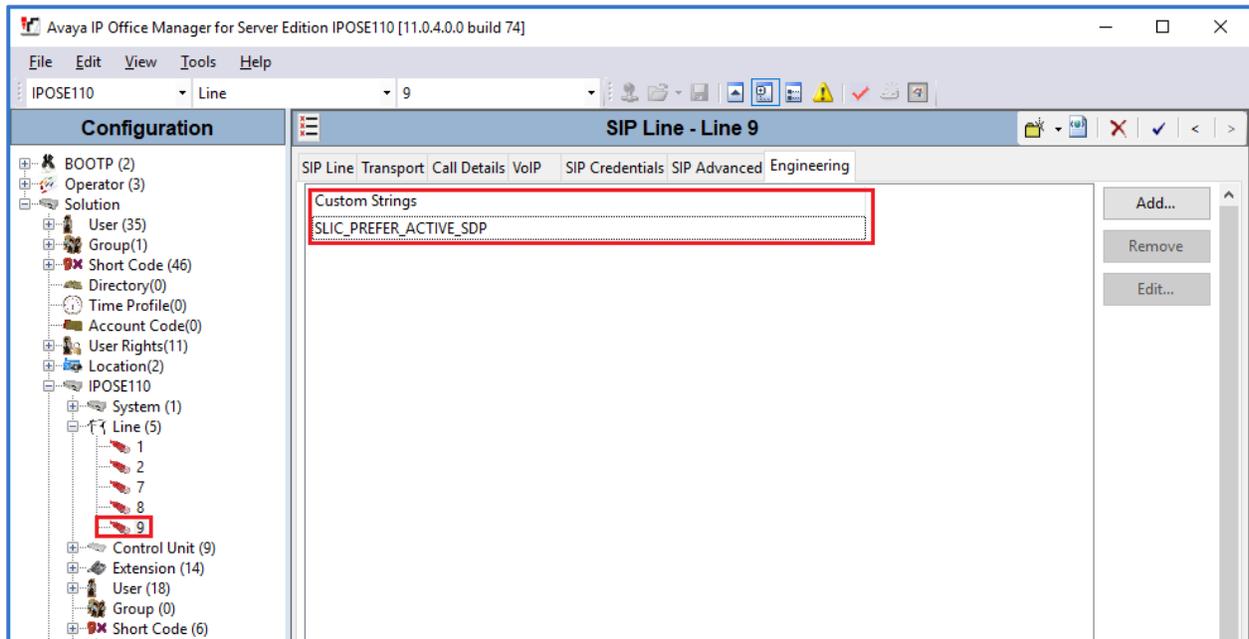
In the **Call Control** area:

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



5.4.7. SIP Line – Engineering

Select the **Engineering** tab, select Add button and add a custom string “*SLIC_PREFER_ACTIVE_SDP*” as shown in the screenshot. This custom string will help to overcome the T.38 fax issue as described in **Section 2.2**.



5.5. 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 EXP110 System.

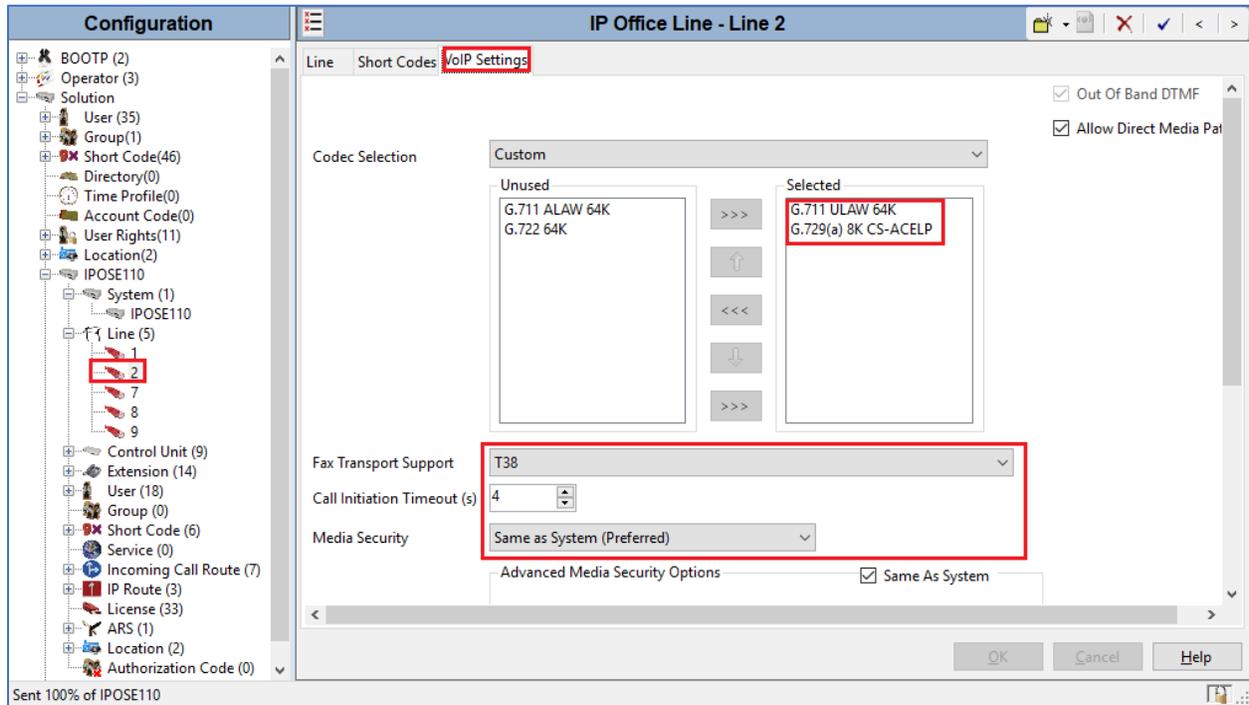
The screenshot displays the configuration window for 'IP Office Line - Line 2'. The left-hand 'Configuration' pane shows a tree view with 'IPOSE110' and 'Line (4)' highlighted. The main configuration area is divided into several sections:

- Line Settings:** Line Number (2), Transport Type (WebSocket Server), Networking Level (SCN), Security (Medium), Telephone Number, Prefix, and Outgoing Group ID (99001).
- Channels:** Number of Channels (250) and Outgoing Channels (250).
- Gateway:** Address (192 . 168 . 199 . 55), Location (2: Thornton), Password, and Confirm Password.
- SCN Resiliency Options:** Includes checkboxes for 'Supports Resiliency', 'Backs up my IP phones', 'Backs up my hunt groups', and 'Backs up my IP DECT phones'.
- Description:** A text input field.

At the bottom right, there are 'OK', 'Cancel', and 'Help' buttons.

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

- Under **Codec Selection** verify **G.711Mu** and **G.729(a)** are selected.
- Select **T.38** for **Fax Transport Support** (refer to **Section 2.2**).
- Under **Media Security** verify **Same as System (Preferred)** is selected (default value).



5.6. Incoming Call Route

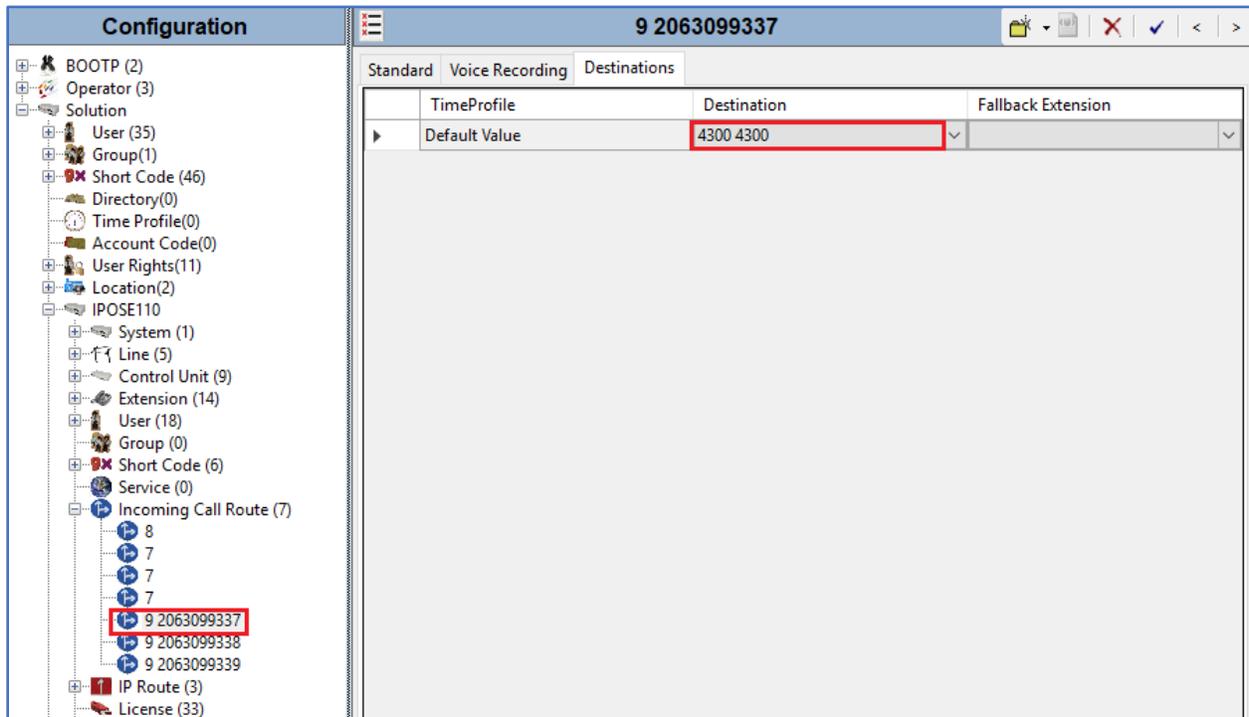
Incoming call routes map inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system. To add an incoming call route, right click on **Incoming Call Route** in the **Navigation** pane and select **New** (not shown). On the Details Pane, under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

- Set **Bearer Capacity** to **Any Voice**.
- The **Line Group ID** is set to **9**. This matches the **Incoming Group** field configured in the **Call Details** tab for the SIP Line on **Section 5.4.4**.
- On the **Incoming Number**, enter one of the DID numbers provided by G12. When the destination is a user's extension, the **Incoming Number** can be used to construct the "From" and "Contact" headers to be used in place of the extension number in the outgoing SIP INVITE for that user.
- Default values may be used for all other parameters.

The screenshot displays the IP Office configuration interface. On the left is the 'Configuration' tree, and on the right is the configuration details pane for the selected item '9 2063099337'. The 'Standard' tab is active, showing various configuration fields. A red box highlights the 'Line Group ID' field, which is set to '9', and the 'Incoming Number' field, which is set to '2063099337'. The 'Incoming Call Route' entry in the left tree is also highlighted with a red box.

Field	Value
Bearer Capacity	Any Voice
Line Group ID	9
Incoming Number	2063099337
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 **2063099337** provided by G12 was associated with the Avaya IP Office extension **4300**.



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

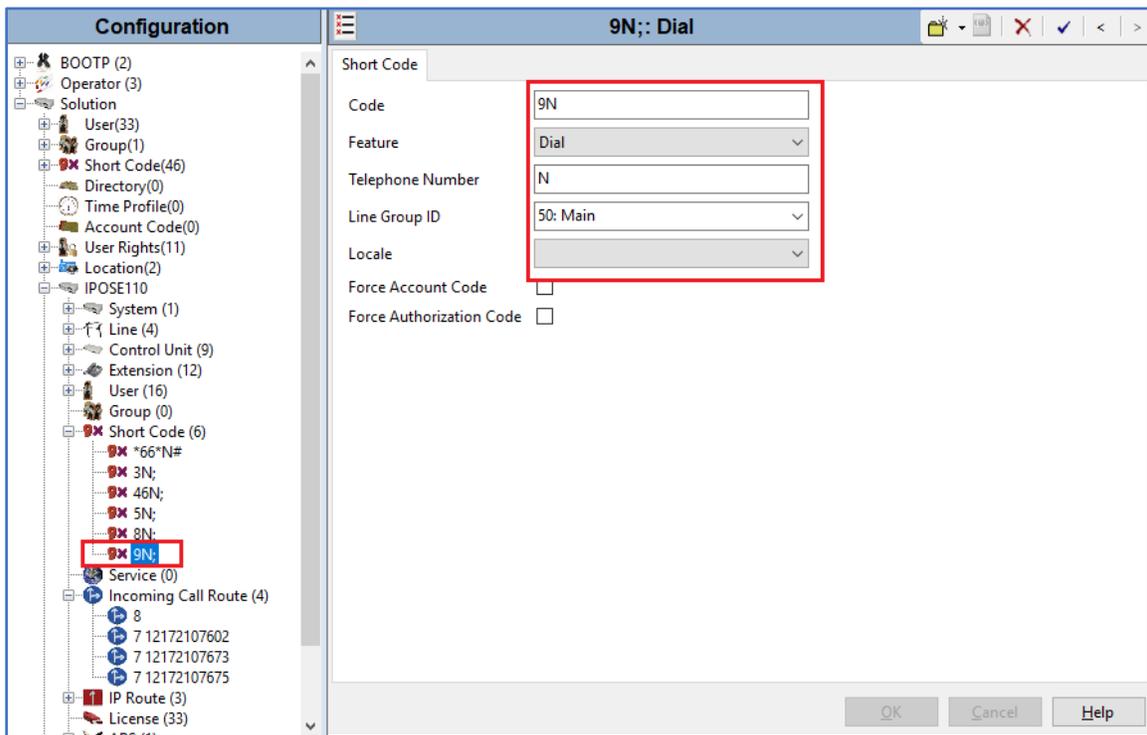
5.7. Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. While detailed coverage of ARS is beyond the scope of these Application Notes, and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance testing.

5.7.1. Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code**, the **Navigation** pane and select **New**. The screen below shows the short code **9N** created (note that the semi-colon is not used here). In this case, when the IP Office user dials 9 plus any number **N**, instead of being directed to a specific Line Group ID, the call is directed to **Line Group 50: Main**, which is configurable via ARS.

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **9N** was used (note that the semi-colon is not used here).
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value is passed to ARS.
- Set the **Line Group ID** to **50: Main** to be directed to **Line Group 50: Main**, this is configurable via ARS.
- For **Locale**, **United States (US English)** was used.
- Click the **OK** to commit (not shown).



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

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

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

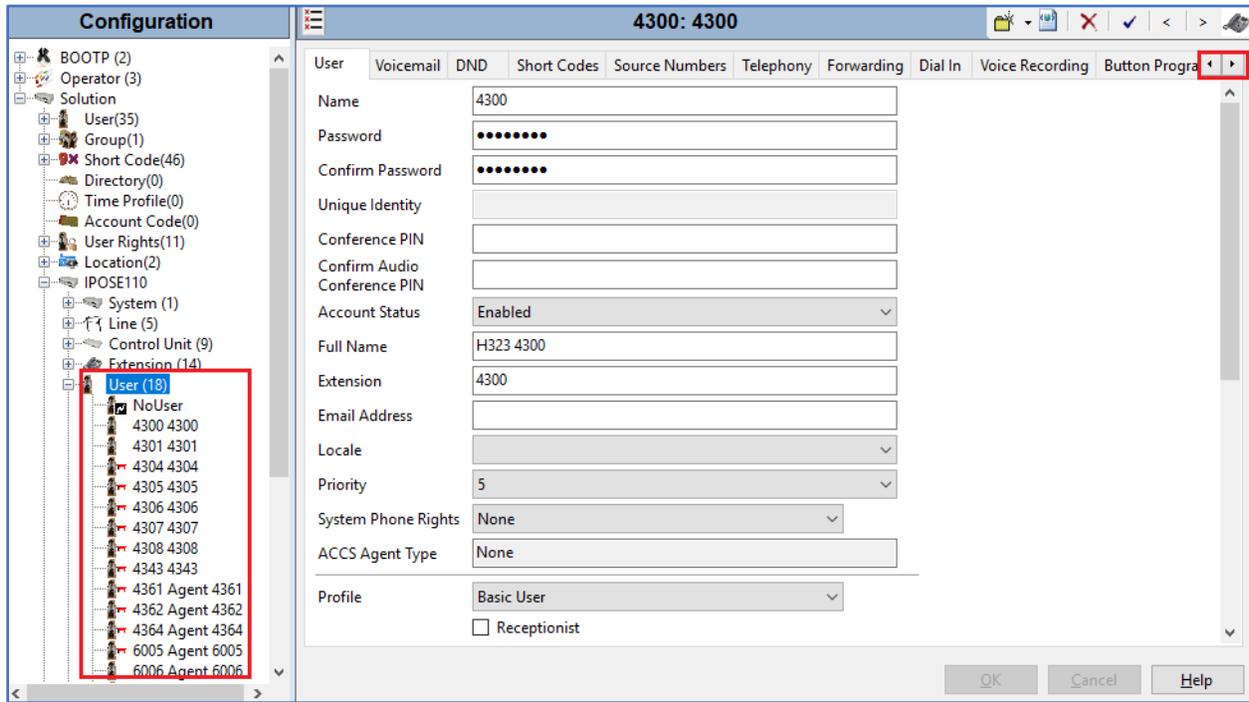
The following example shows the dial pattern for calls within the United States.

Edit Short Code	
Code	1XXXXXXXXXX
Feature	Dial
Telephone Number	1N
Line Group ID	9
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

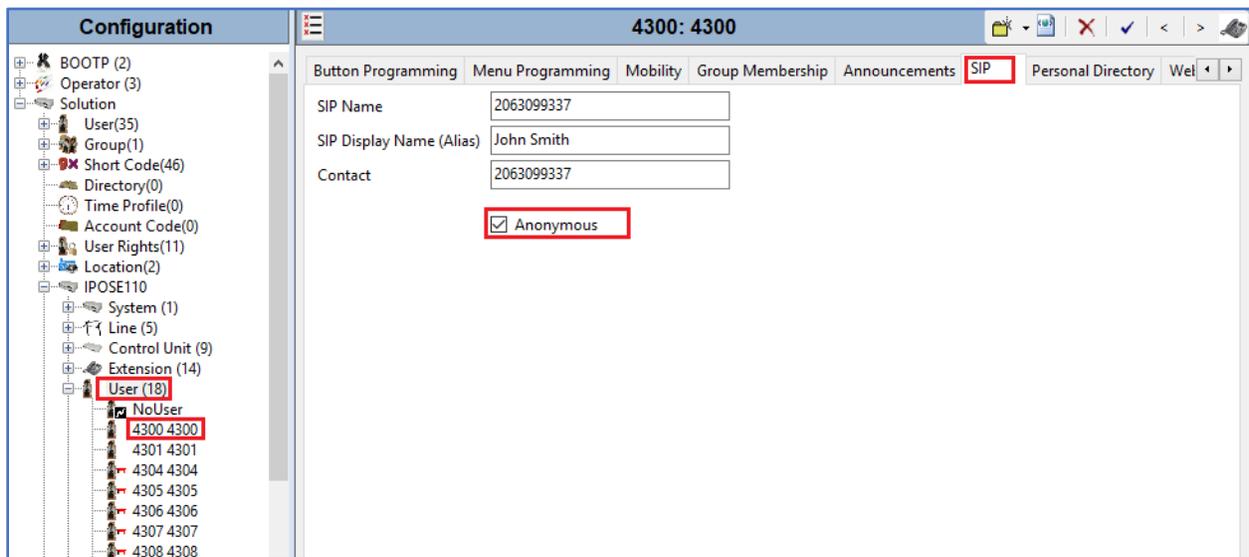
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

5.8. User

A user can be newly added as new or edit by selecting **User** in the left pane. The screen below shows the user 4300 that was previously created.



Click on the left arrow button in the top right corner as highlighted in red to navigate other tabs, select **SIP** tab. In the **SIP** tab, check the **Anonymous** box to enable privacy for this user as placing outbound call.

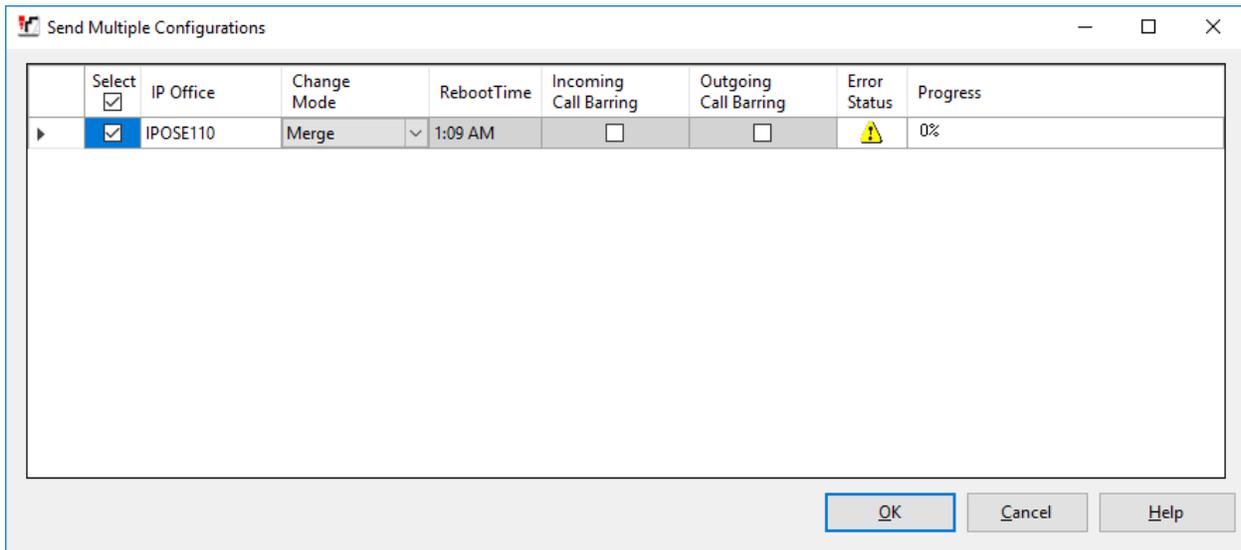


5.9. Save IP Office Primary Server Configuration

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 **Reboot** option will save the configuration and cause the Avaya IP Office server to reboot.

Click **OK** to execute the save.



6. Avaya IP Office Expansion System Configuration

Navigate to **File** → **Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials. Clicking the “plus” sign next to IP Office Expansion system, in this case **EXP110** was selected.

The screenshot displays the Avaya IP Office configuration interface, divided into two main panes: **Configuration** and **System Inventory**.

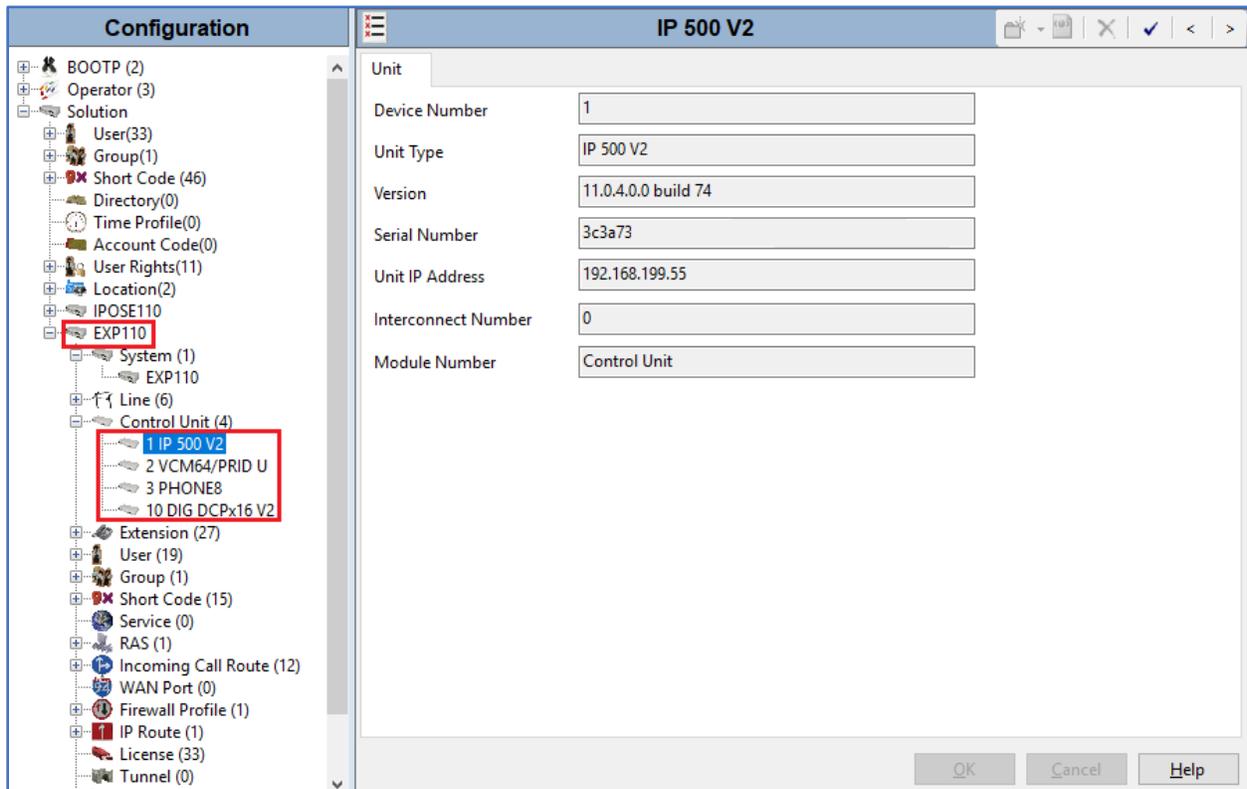
Configuration Pane: A tree view on the left shows the system hierarchy. The **EXP110** system is highlighted with a red box. The tree includes categories such as BOOTP (2), Operator (3), Solution, User (33), Group (1), Short Code (46), Directory (0), Time Profile (0), Account Code (0), User Rights (11), Location (2), IPOSE110, and EXP110. Below EXP110, various system components are listed, including System (1), Line (6), Control Unit (4), Extension (27), User (19), Group (1), Short Code (15), Service (0), RAS (1), Incoming Call Route (12), WAN Port (0), Firewall Profile (1), IP Route (1), License (33), Tunnel (0), ARS (2), Location (2), and Authorization Code (1).

System Inventory Pane: The right pane shows the details for the selected **Server Edition Primary** system. It is organized into sections:

- Hardware Installed:**
 - Control Unit: IPO-Linear-PC
 - Secondary Server: NONE
 - Expansion Systems: 192.168.199.55
 - System Identification: 15f4852b03c09efd9de4c777f2cf2dcdedfaf090
- System Settings:**
 - IP Address: 10.33.1.110
 - Sub-Net Mask: 255.255.255.0
 - System Locale: United States (US English)
 - System Location: 2: Thornton
 - Device ID: NONE
 - Number of Extensions on System: 12
- Features Configured:**
 - Licenses Installed: Receptionist(4); Additional Voicemail Pro Ports(152); VMPro Recordings Adminis
 - Connected Extensions: 4300; 4304; 4305
- Hunt Group Extensions**
- Incoming Call Routes**
 - Time Profiles:**
 - Users NOT Configured for Voicemail: 4300; 4343; Agent 6007; Agent 6010
 - Users assigned as Ex-Directory: NONE
 - Users assigned for Twinning: NONE
 - Users barred from making Outgoing Calls: NONE
 - Music 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.



6.2. LAN Settings

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

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

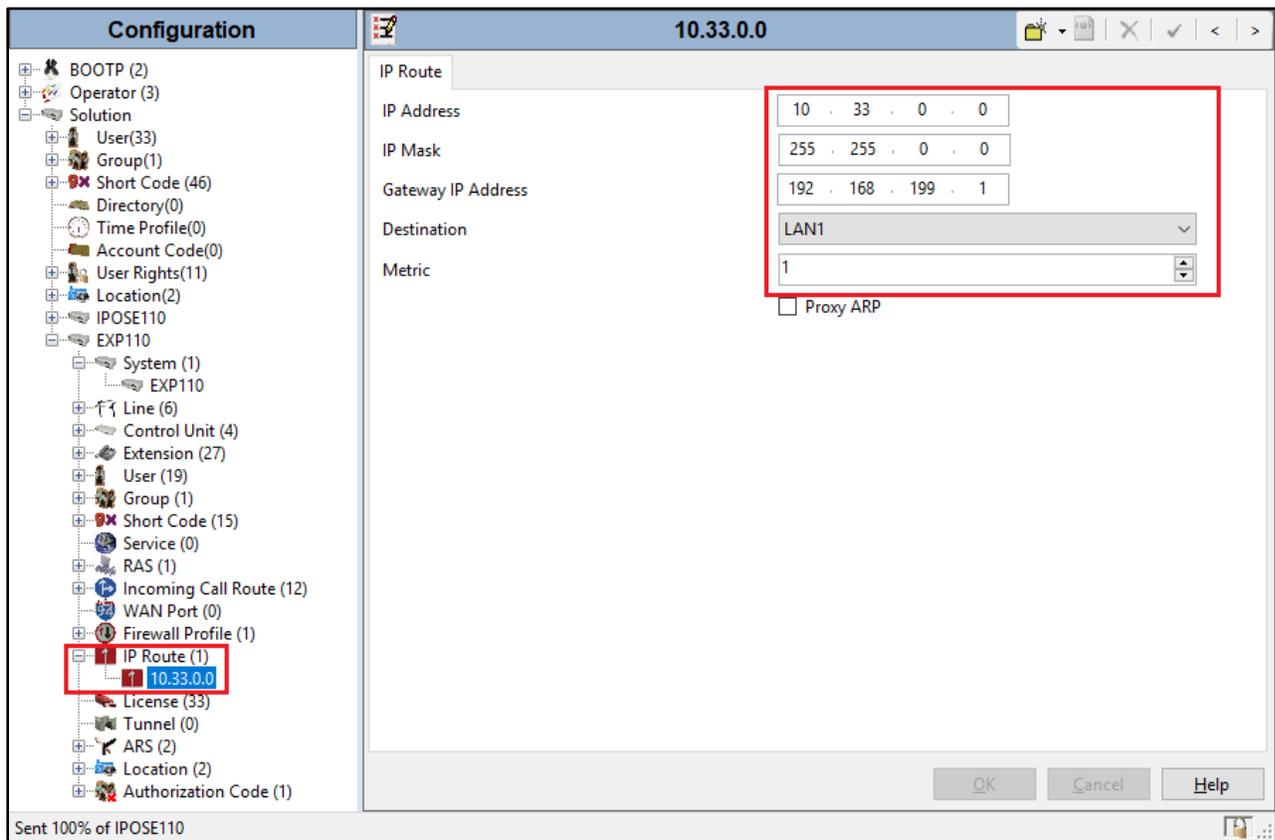
The screenshot displays the Avaya Configuration Manager interface for the system 'EXP110'. The left-hand 'Configuration' pane shows a tree view where 'System (1)' is selected and highlighted with a red box. The right-hand 'Details' pane is set to the 'LAN Settings' tab, also highlighted with a red box. The 'IP Address' field is set to '192 . 168 . 199 . 55' and the 'IP Mask' field is set to '255 . 255 . 255 . 0', both fields being highlighted with red boxes. Other visible settings include 'Primary Trans. IP Address' (0 . 0 . 0 . 0), 'RIP Mode' (None), 'Number Of DHCP IP Addresses' (1), and 'DHCP Mode' (Disabled). The interface includes standard navigation buttons like 'OK', 'Cancel', and 'Help' at the bottom right.

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

6.3. IP Route

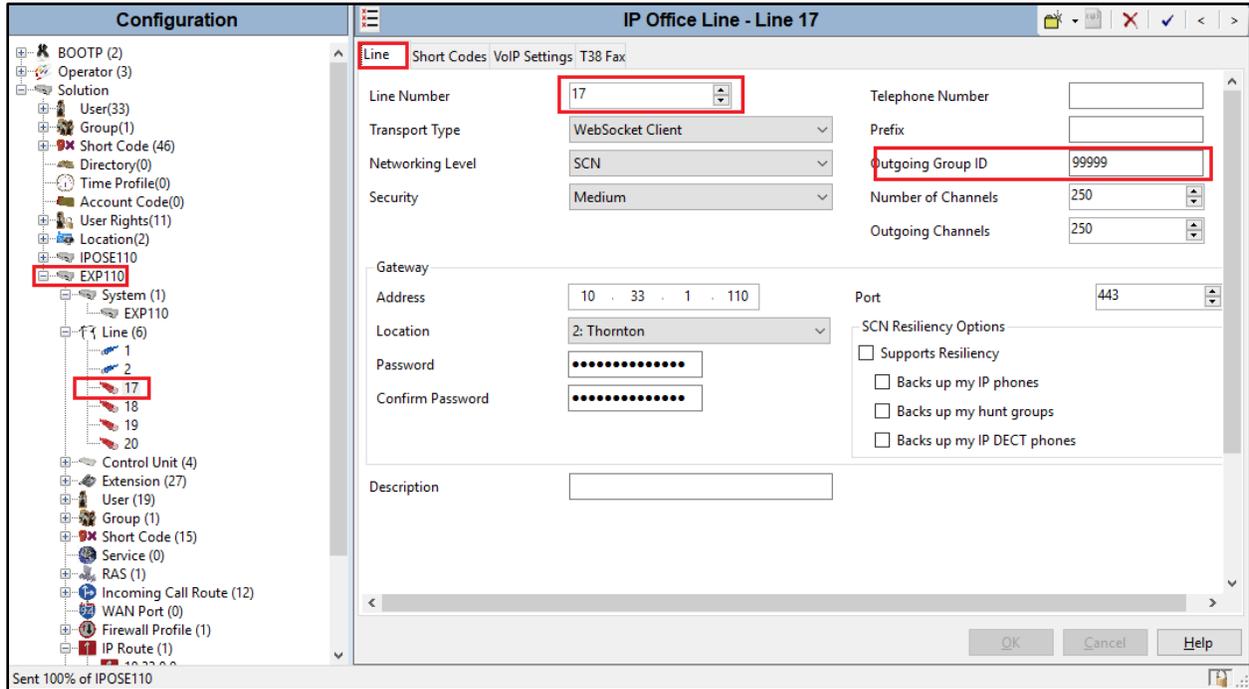
To create an IP route for the Expansion system, right-click on **IP Route** on the left Navigation pane. Select **New** (not shown).

- Enter **10.10.0.0** on the **IP Address** and **IP Mask 255.255.0.0** 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 **192.168.199.1**.
- Set **Destination** to **LAN1** from the pull-down menu.



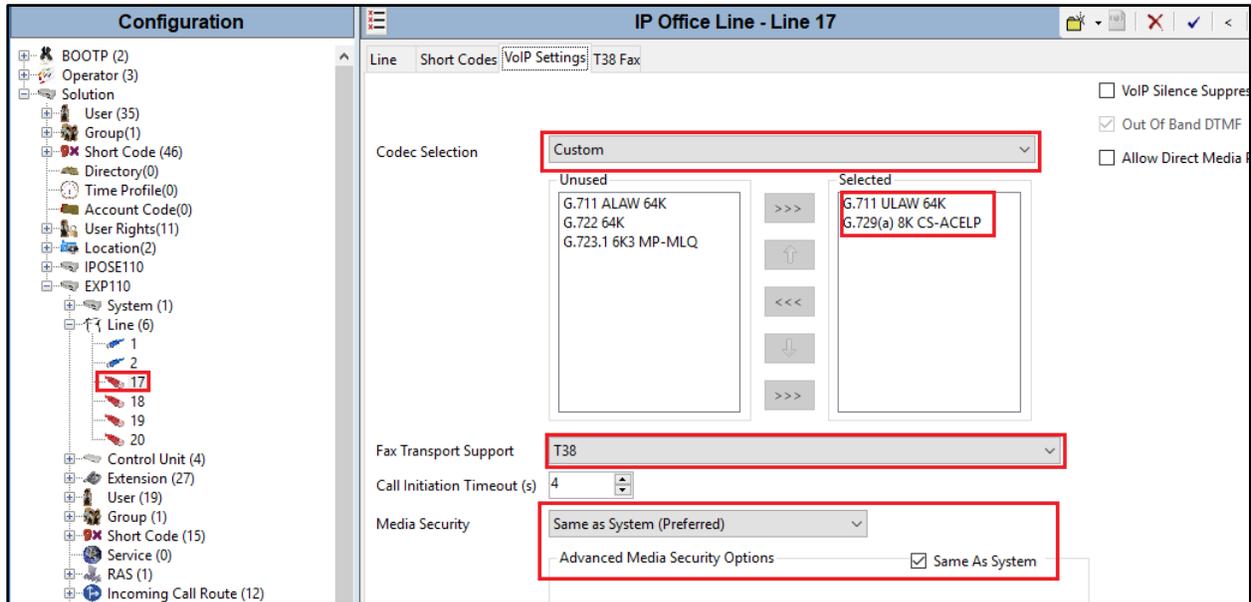
6.4. IP Office Line – IP500 V2 Expansion System

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.



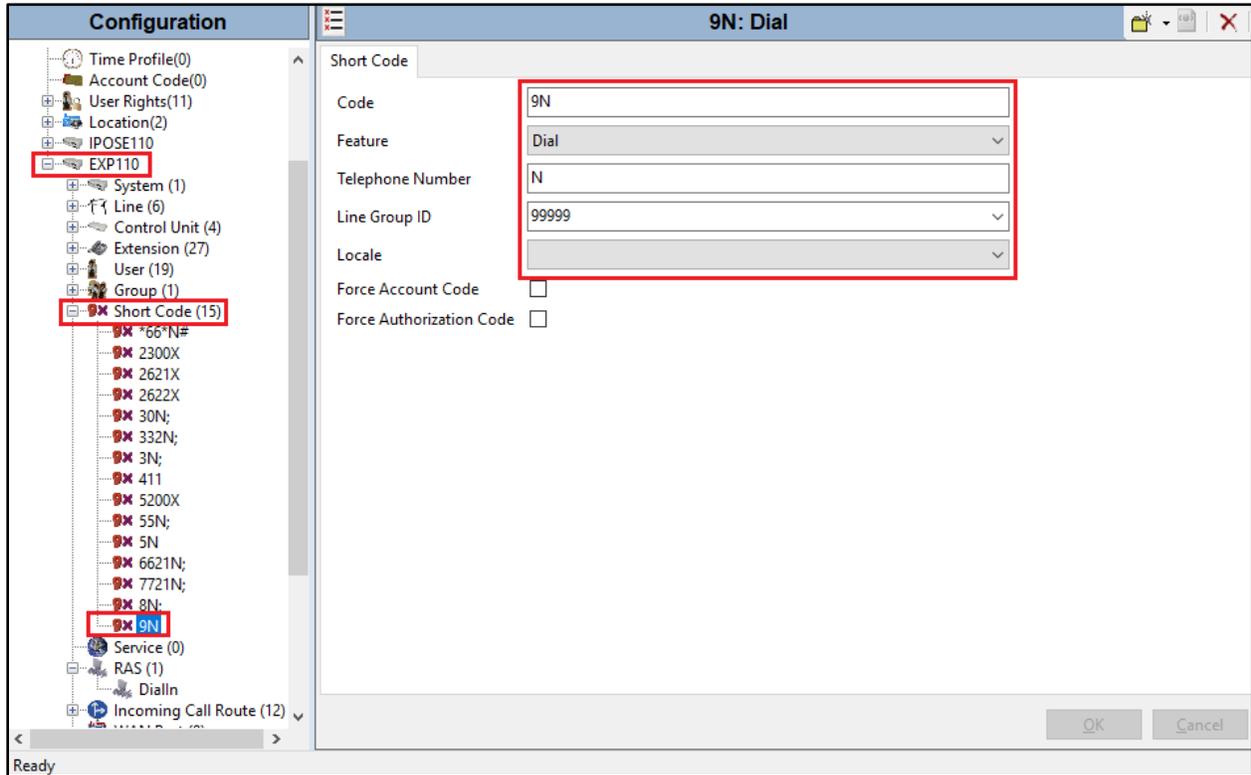
The screen below shows the IP Office Line, **VoIP Settings** tab:

- Under **Codec Selection** verify **G.711Mu** and **G.729(a)** are selected.
- Select **T.38** for **Fax Transport Support**.
- Under **Media Security Preferred** was selected.



6.5. Short Codes

Similar to the configuration of the Primary server in **Section 5.7**, 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.



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 shows the configuration window for the ARS route named "To-Primary". The left sidebar shows a tree view of the configuration hierarchy, with "51: To-Primary" selected under the ARS (2) folder. The main configuration area includes the following fields:

- Route Name: To-Primary
- Dial Delay Time: System Default (4)
- Description: (empty)
- In Service: (checked)
- Time Profile: <None>
- Out of Service Route: <None>
- Out of Hours Route: <None>

Below these fields is a table with the following data:

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

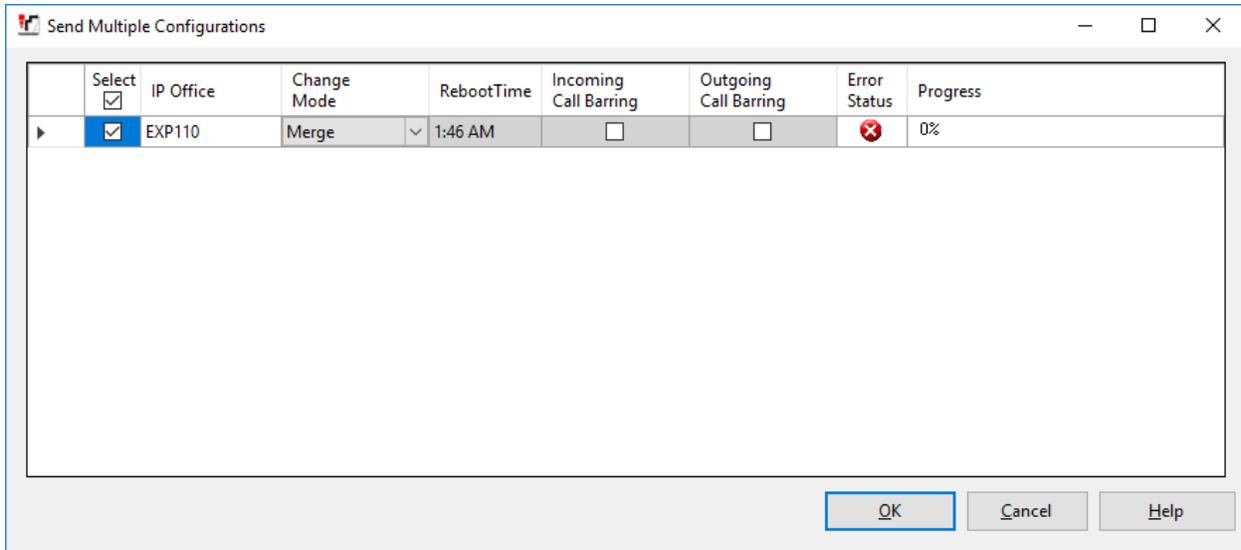
The table has buttons for "Add...", "Remove", and "Edit..." on the right side. At the bottom of the window are "OK", "Cancel", and "Help" buttons.

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

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. G12 SIP Trunking Service Configuration

To use G12 SIP Trunking Service, a customer must request the service from G12 using the established sales processes. The process can be started by contacting G12 via the corporate web site and requesting information.

During the signup process, G12 and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to G12 network.

G12 is responsible for the configuration of G12 SIP Trunking Service. The customer will need to provide the public IP address used to reach the IP Office at the enterprise. In the case of the compliance test, this is the public IP address of the IP Office WAN port (LAN2) of the Primary server.

G12 will provide the customer the necessary information to configure Avaya IP Office following the steps discussed in the previous sections, including:

- SIP Proxy IP address.
- DID numbers, etc.

8. Verification Steps

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

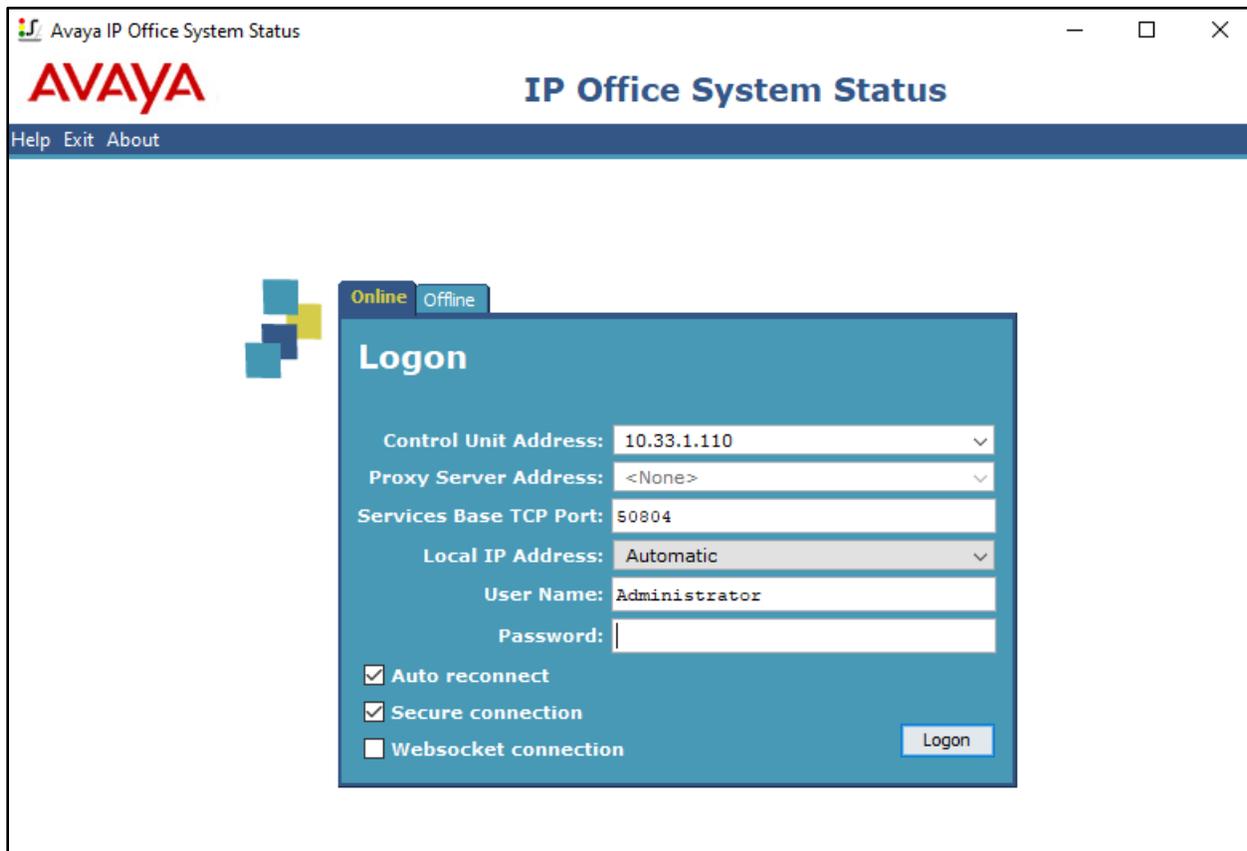
The following steps may be used to verify the configuration:

- 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.



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 application. The left pane shows a tree view with 'Trunks (5)' expanded to 'Line: 9'. The main pane shows the 'Status' tab for the selected trunk. The 'SIP Trunk Summary' section displays various configuration details. Below this is a table showing the status of 10 channels, all of which are in an 'Idle' state.

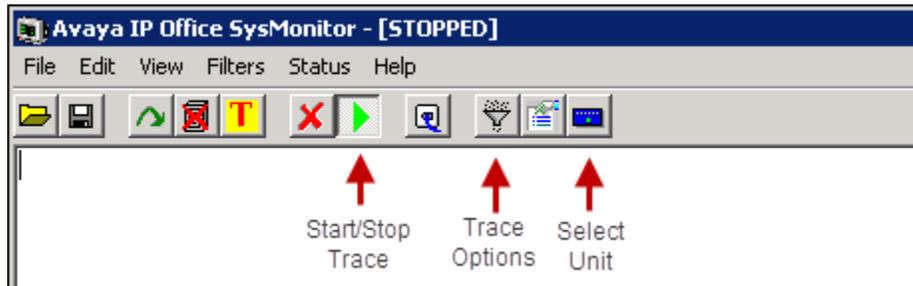
SIP Trunk Summary

Line Service State: In Service
 Peer Domain Name: 192.168.194.17
 Resolved Address: 192.168.194.17
 Line Number: 9
 Number of Administered Channels: 10
 Number of Channels in Use: 0
 Administered Compression: G711 Mu, G729 A
 Enable Faststart: Off
 Silence Suppression: Off
 Media Stream: RTP
 Layer 4 Protocol: UDP
 SIP Trunk Channel Licenses: 512 0%
 SIP Trunk Channel Licenses in Use: 0
 SIP Device Features: REFER (Incoming and Outgoing)

Channel Number	URI G...	Call Ref	Current State	Time in State	Remote Media A...	Co...	Conne...	Caller ID or Dial...	Other Party on Call	Direction of Call	Round Trip D...	Receive Jitter	Receive Packet...	Transmit Jitter	Transmit Packet...
1			Idle	02:49:14											
2			Idle	6 days...											
3			Idle	9 days...											
4			Idle	14 day...											
5			Idle	14 day...											
6			Idle	14 day...											
7			Idle	14 day...											
8			Idle	14 day...											
9			Idle	14 day...											
10			Idle	14 day...											

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 11.0 to G12 SIP Trunking Service. G12 SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

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

10. Additional References

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

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

- [1] *Deploying IP Office Platform Server Edition Solution*, Release 11.0, May 2018
- [2] *IP Office Platform 11.0, Deploying Avaya IP Office Servers as Virtual Machines*, January 2019
- [3] *IP Office Platform 11.0, Deploying Avaya IP Office Essential Edition (IP500 V2)*, February 2019.
- [4] *Administering Avaya IP Office Platform with Manager, Release 11.0 FP4*, February 2019.
- [5] *Administering Avaya IP Office™ Platform with Web Manager, Release 11.0 FP4*, February 2019.
- [6] *Planning for and Administering Avaya Equinox for Android, iOS, Mac and Windows, Release 3.4.8, November 2018*
- [7] *Using Avaya Equinox for IP Office, Release 11.0 FP4*, February 2019

Additional Avaya IP Office documentation can be found at:

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

©2019 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.