



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.1 to support Cincinnati Bell SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 11.1 to support Cincinnati Bell SIP Trunking Service. These Application Notes update previously published Application Notes with a newer software version of Avaya IP Office.

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

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

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

1. Introduction

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

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

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

The terms “service provider”, “Cincinnati Bell”, “Cincinnati Bell Business” or “CBTS” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Cincinnati Bell 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:

- Static IP SIP Trunk authentication.
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, Digital and Analog telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323, Digital and Analog telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider network.
- Incoming and outgoing PSTN calls to/from Avaya Workplace Client for Windows (SIP).
- Dialing plans including local calls, outbound toll-free, etc.
- Caller ID presentation.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two-way speech-path. Testing was performed with codec: G.711MU (Note: Other audio codecs may be supported by Cincinnati Bell, G.711MU was the only codec being offered by Cincinnati Bell during the compliance test).
- Proper response to no matching codecs.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.
- Simultaneous active calls.
- Long duration calls (over one hour).

Items not supported or not tested included the following:

- Inbound toll-free calls, outbound Toll-Free calls, 911 calls (emergency), “0” calls (Operator), local directory assistance and international calls were not tested.

2.2. Test Results

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

- **Fax support** – Fax calls using the T.38 protocol failed during the compliance test. G.711 pass-through fax was also tested, but it behaved unreliably. The issue related to G.711 pass-through fax failing during the compliance test may be related to the unpredictability of G.711 pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay. The issue related to T.38 fax calls failing is related to the PSTN carriers used by Cincinnati Bell to route calls to the PSTN, not all PSTN carriers used by Cincinnati Bell support T.38. This issue could be solved by Cincinnati Bell selecting and routing T.38 fax traffic via PSTN carriers that support T.38.
- **Cincinnati Bell does not support REFER for call forward** – Cincinnati Bell supports REFER for call transfers to the PSTN but does not support REFER for call forward to the PSTN. The call scenario in which Cincinnati Bell does not support REFER is for inbound calls from the PSTN to IP Office which are then forwarded to another PSTN endpoint. In this scenario, if REFER is enabled (**Section 5.4.2**), Cincinnati Bell responds with a “403 Forbidden” message in response to the REFER message sent by IP Office. This issue was solved by enabling “**No REFER if using Diversion**” on the IP Office SIP Line, which resulted in IP Office sending REFER during call transfers to the PSTN and not send it during call forwards to the PSTN (**Section 5.4.6**).

2.3. Support

For support of Cincinnati Bell SIP Trunking Service visit the corporate Web page at:
<https://www.altafiber.com/business/support/sip-trunking-support>

For technical support on the Avaya products described in these Application Notes visit
<http://support.avaya.com>

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 Cincinnati Bell SIP Trunking Service through the public Internet.

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

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

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

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

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

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

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

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

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

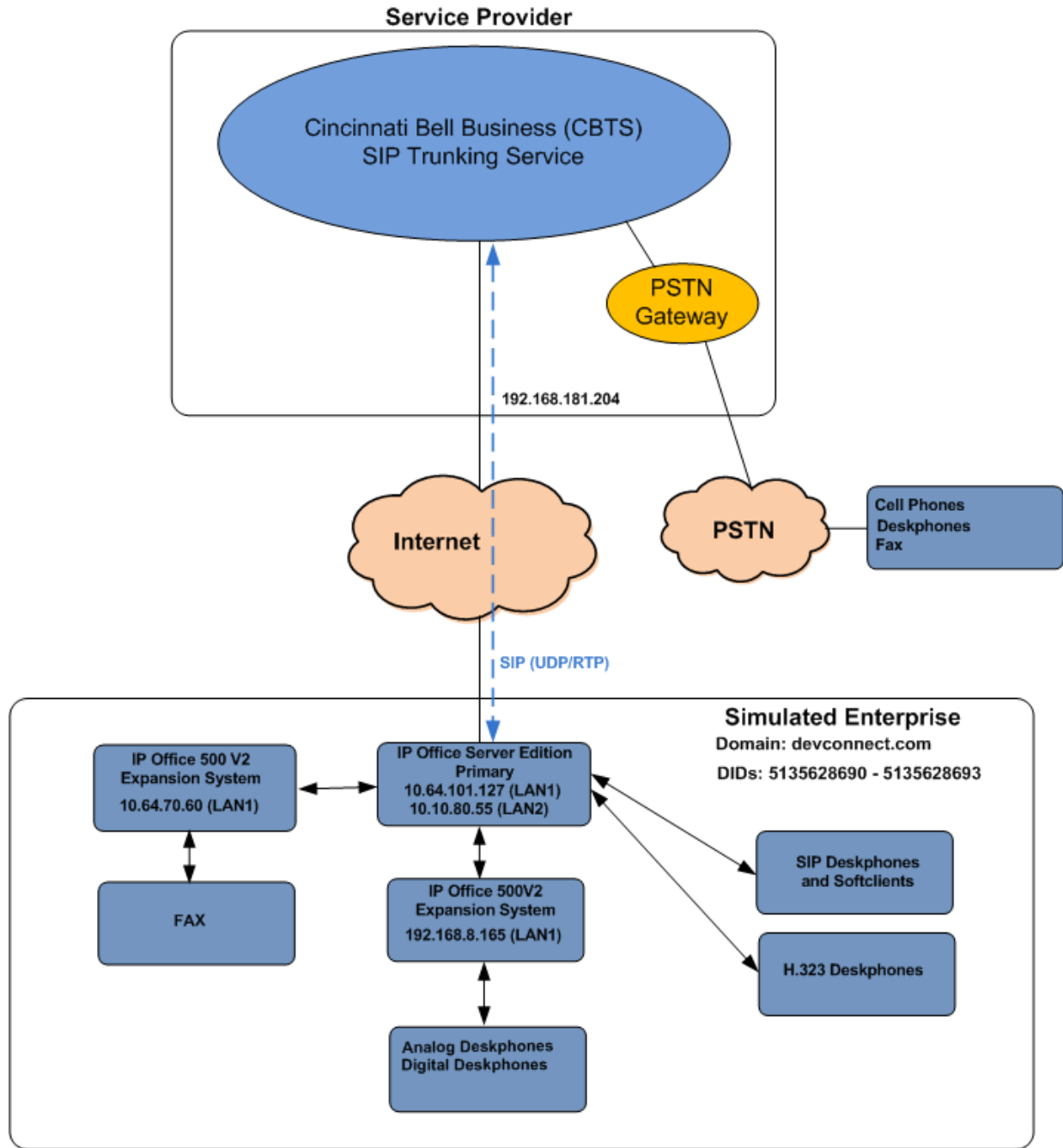


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

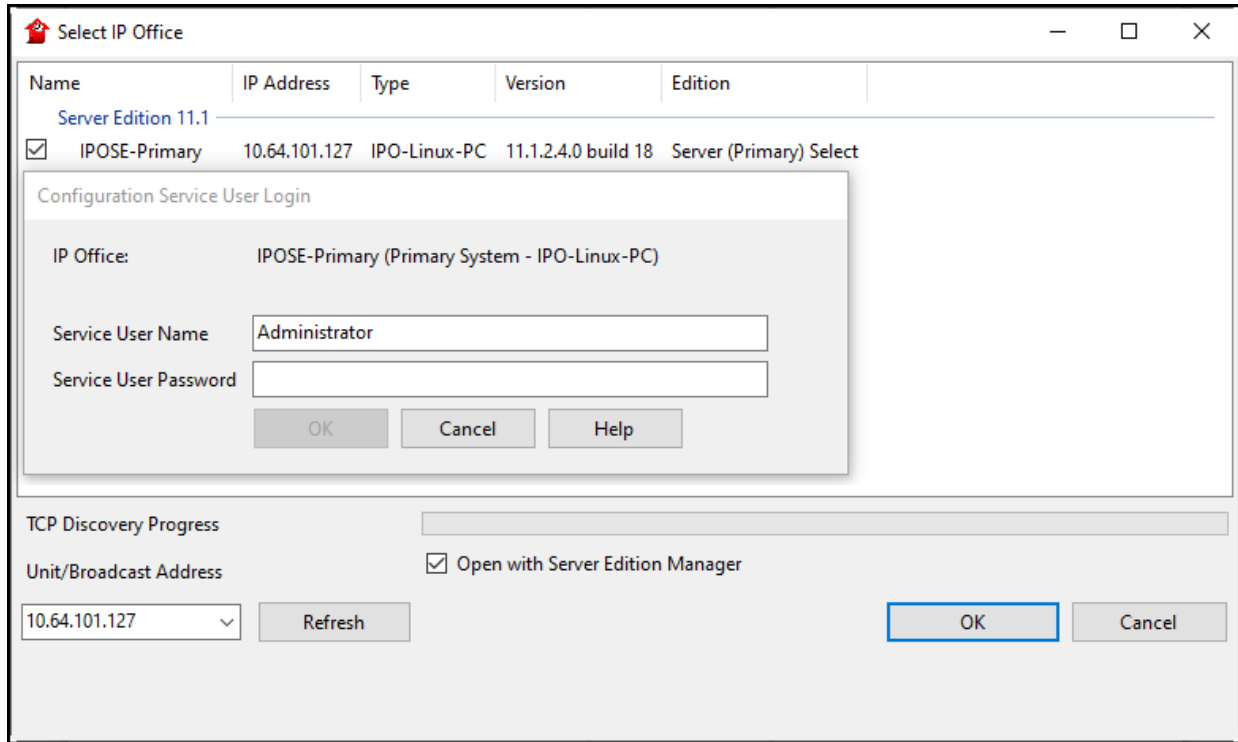
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server)	11.1.2.4.0 Build 18
• Avaya IP Office Voicemail Pro	11.1.2.4.0 Build 2
Avaya IP Office IP500 V2 (Expansion Systems)	11.1.2.4.0 Build 18
Avaya IP Office Manager	11.1.2.4.0 Build 18
Avaya J179 IP Telephone (H.323)	6.8.5.2.3
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya 96x1 IP Deskphone (SIP)	Version 7.1.15.2.1
Avaya J129 IP Deskphones (SIP)	Version 4.1.0.0.7
Avaya 1408 Digital Telephone	48.02
Avaya Workplace Client for Windows (SIP)	3.32.0.75
Analog Telephone	---
Cincinnati Bell	
Cisco Broadworks	R24
Ribbon SBC	09.02.04R002

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

5. Avaya IP Office Primary Server Configuration

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



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

Configuration

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

Server Edition

Summary

Server Edition Primary

Hardware Installed

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

System Settings

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

Open...

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

Add...

- Secondary Server
- Expansion System

Link...

- Expansion System

Description	Name	Address	Primary Link	Secondary Link	Users Configured	Extensions Configured
Solution					32	54
Primary Server	IPOSE-Primary	10.64.101.127			6	6
Expansion System	IP500V2-One	192.168.8.165	Bothway		25	24
Expansion System	IP500V2-Two	10.64.70.60	Bothway		1	24

Ready

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, **IPOSE-Primary** was used as the system name of the Primary Server and **IP500V2-One** and **IP500V2-Two** were used as the system names of the Expansion Systems. 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 Configuration Manager interface. The left pane shows a tree view with 'License' selected under 'IPOSE-Primary'. The right pane shows the 'License Remote Server' configuration. The 'License Mode' is 'License Normal' and 'Licensed Version' is '11.0'. Below this is a table of installed features.

Feature	Instances	Status	Expiration Date	Source
Office Worker	1000	Valid	Never	PLDS Nodal
VMPPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	1	Obsolete	Never	PLDS Nodal
Power User	1000	Valid	Never	PLDS Nodal
Customer Service Agent	5	Dormant	Never	PLDS Nodal
Customer Service Supervisor	5	Dormant	Never	PLDS Nodal
Avaya IP endpoints	1000	Valid	Never	PLDS Nodal
SIP Trunk Channels	256	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	1	Valid	Never	PLDS Nodal
Wave User	16	Obsolete	Never	PLDS Nodal
3rd Party IP Endpoints	1000	Valid	Never	PLDS Nodal
Server Edition	150	Valid	Never	PLDS Nodal
UMS Web Services	1000	Valid	Never	PLDS Nodal
Avaya Mac Softphone	1000	Valid	Never	PLDS Nodal
Avaya Softphone Licence	1000	Valid	Never	PLDS Nodal
SM Trunk Channels	128	Valid	Never	PLDS Nodal
Web Collaboration	64	Valid	Never	PLDS Nodal
Avaya Contact Center Select	1	Valid	Never	PLDS Nodal
Allow Virtualization	10	Valid	Never	PLDS Nodal
Devlink3 External Recorder	1	Valid	Never	PLDS Nodal
Basic User	1000	Obsolete	Never	PLDS Nodal

5.2. System Settings

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

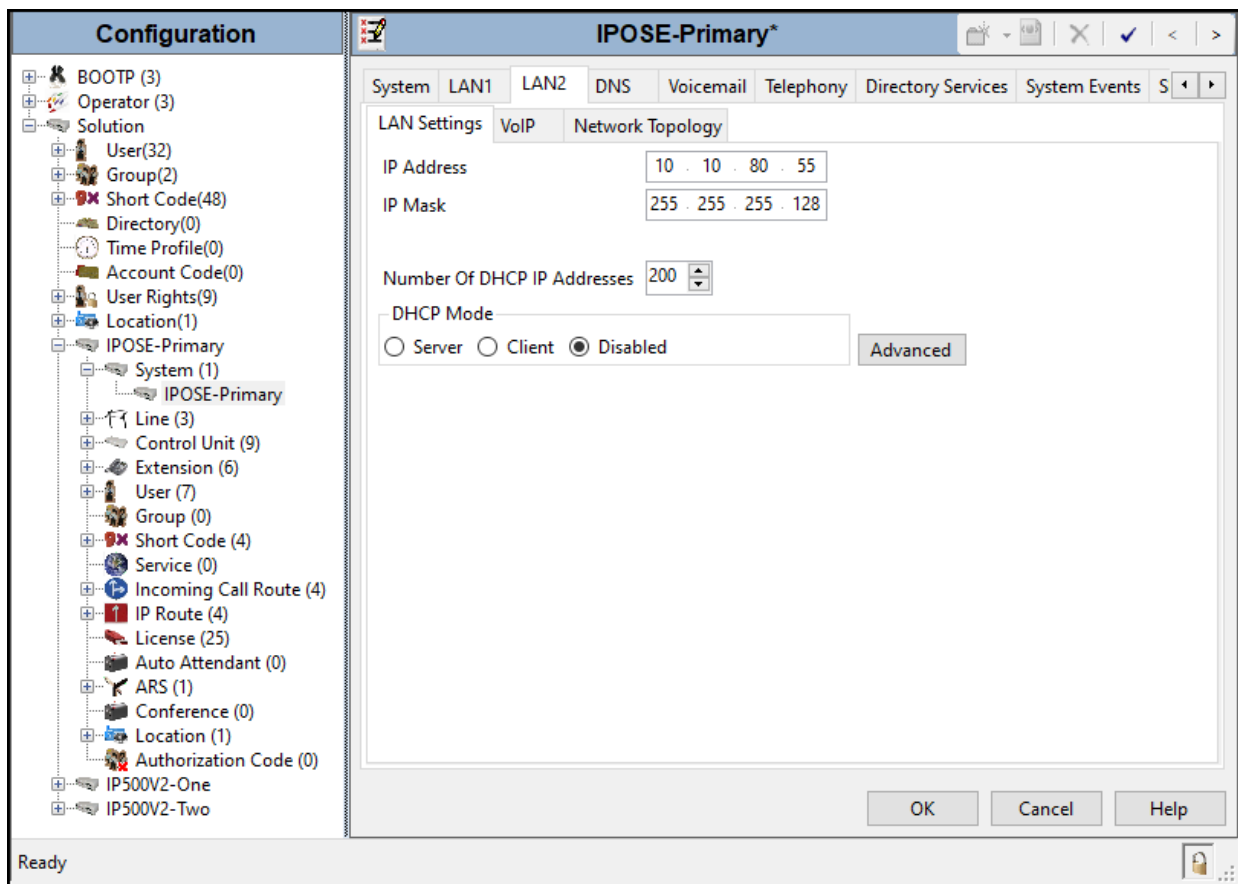
5.2.1. System – LAN2 Tab

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

5.2.1.1 LAN2 - LAN Settings Tab

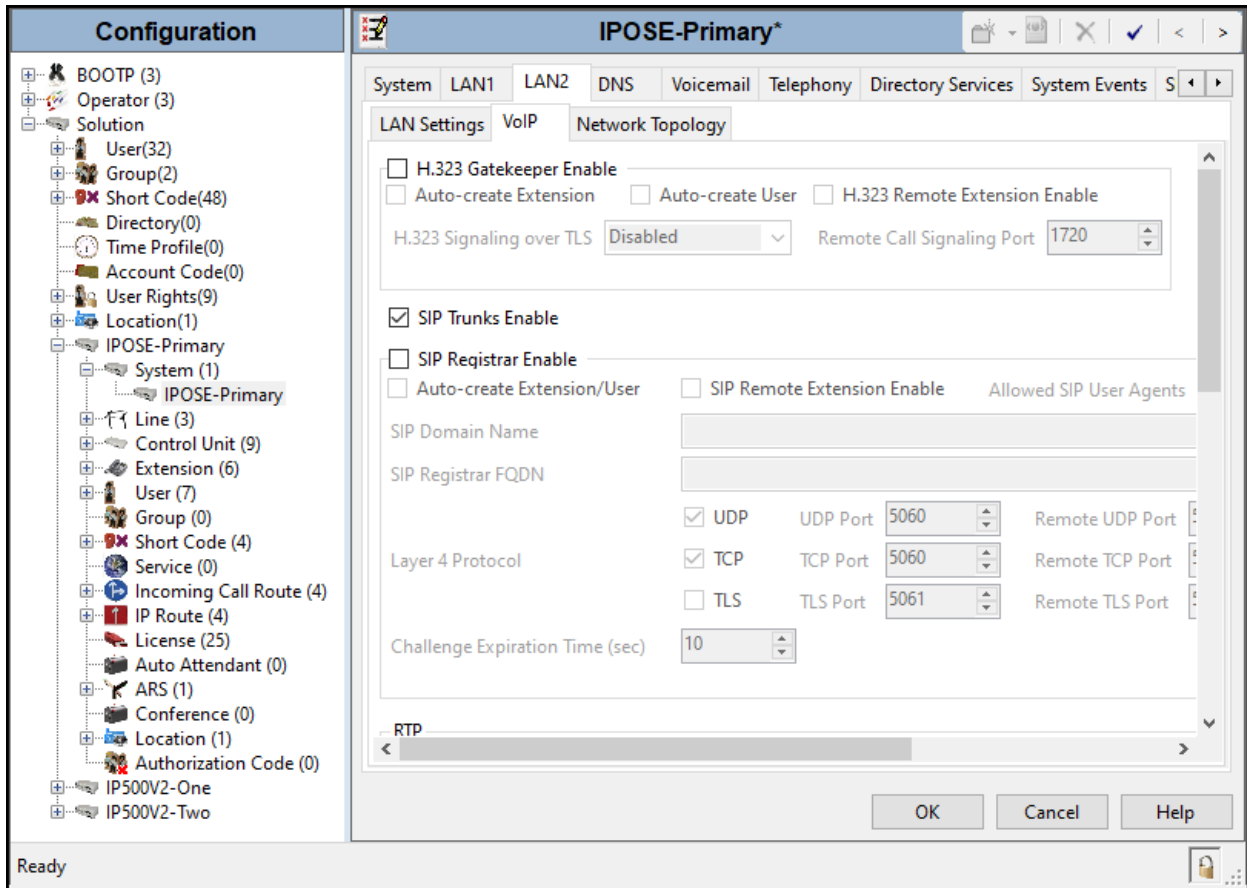
To view or configure the LAN2 IP address and subnet mask, select the **LAN2** → **LAN Settings** tab, and enter the information as needed, according to the customer network requirements:

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



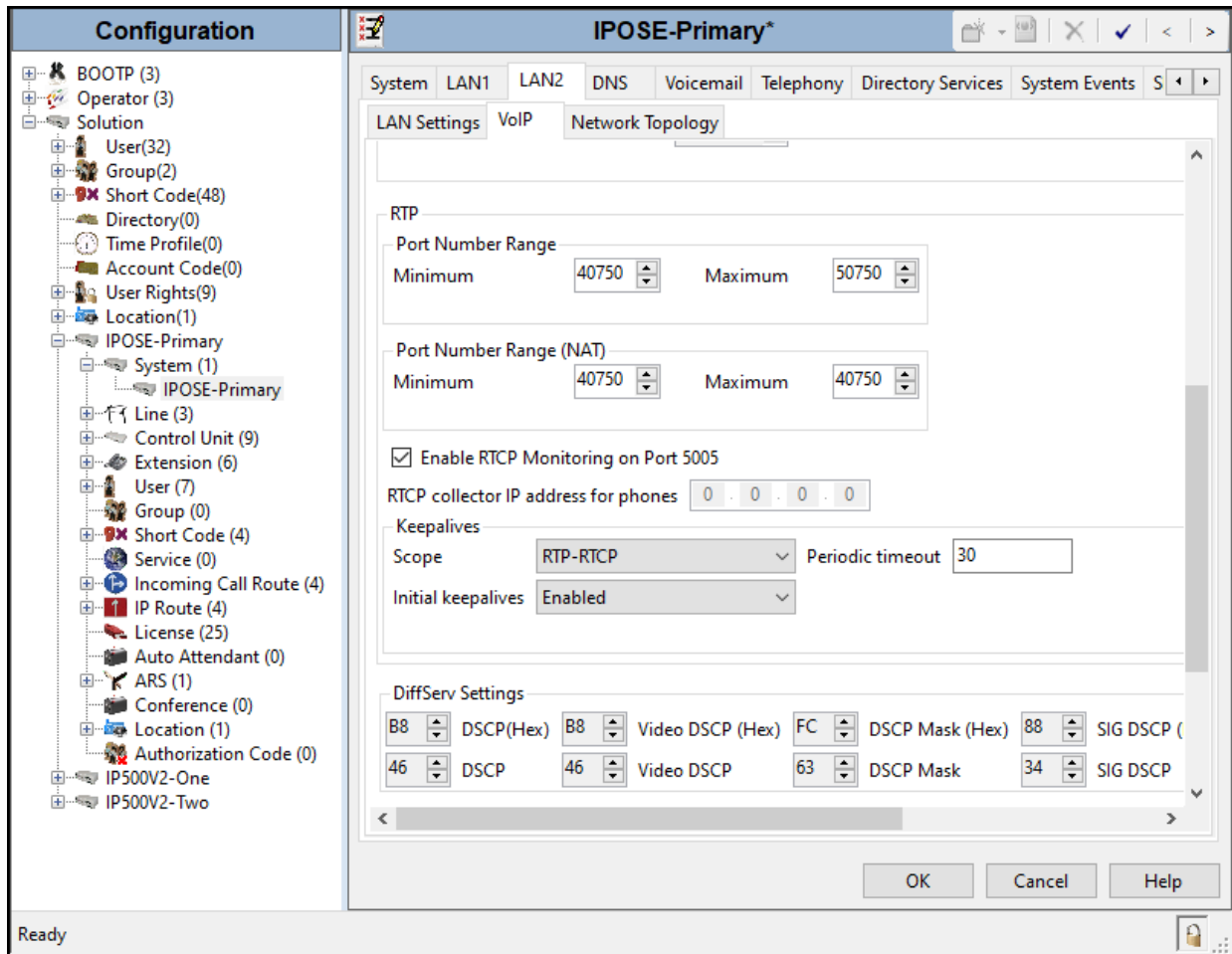
5.2.1.2 LAN2 VoIP Tab

- 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.

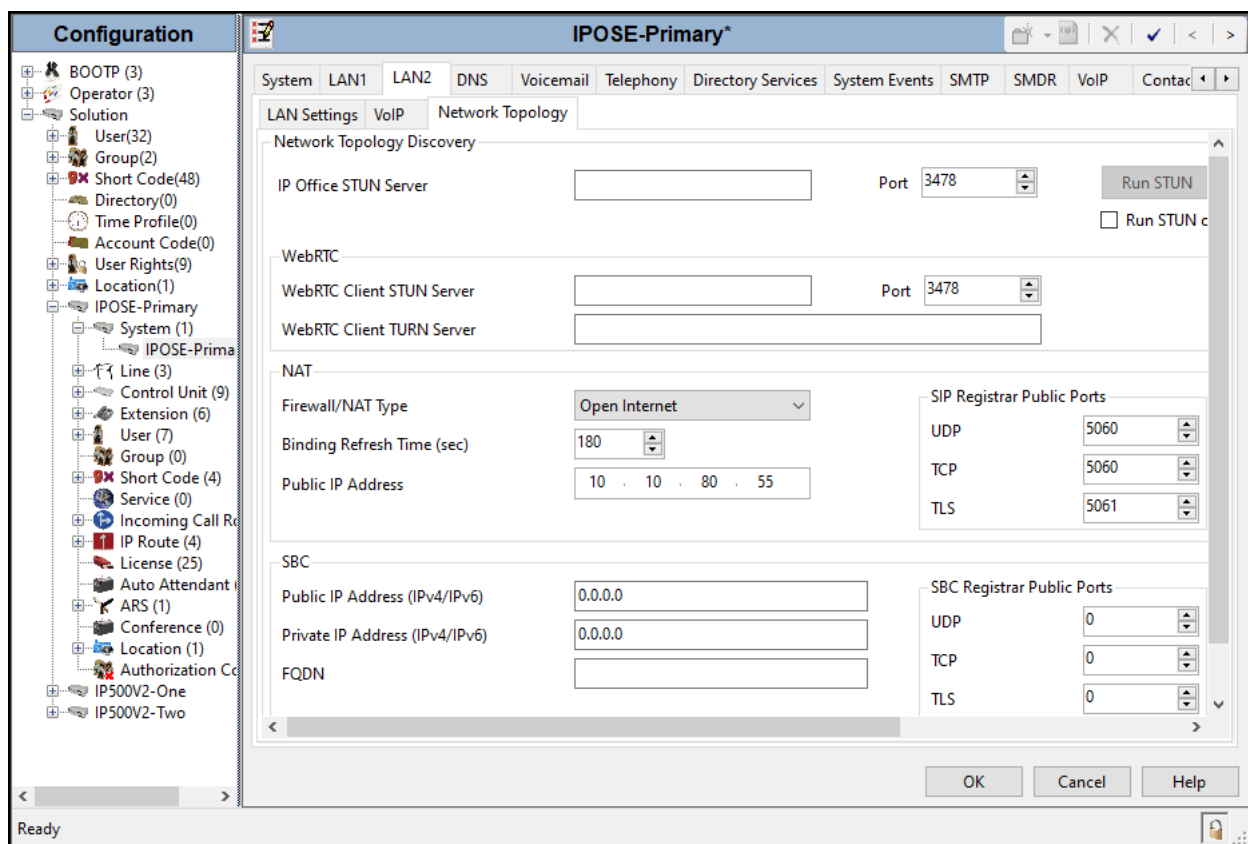


Note: In the compliance test, the LAN1 interface was used to connect the Avaya IP Office to the enterprise site IP network (private network). The LAN1 interface configuration is not directly relevant to the interface with the Cincinnati Bell SIP Trunking Service, and therefore is not described in these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

5.2.1.3 LAN2 - Network Topology Tab

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

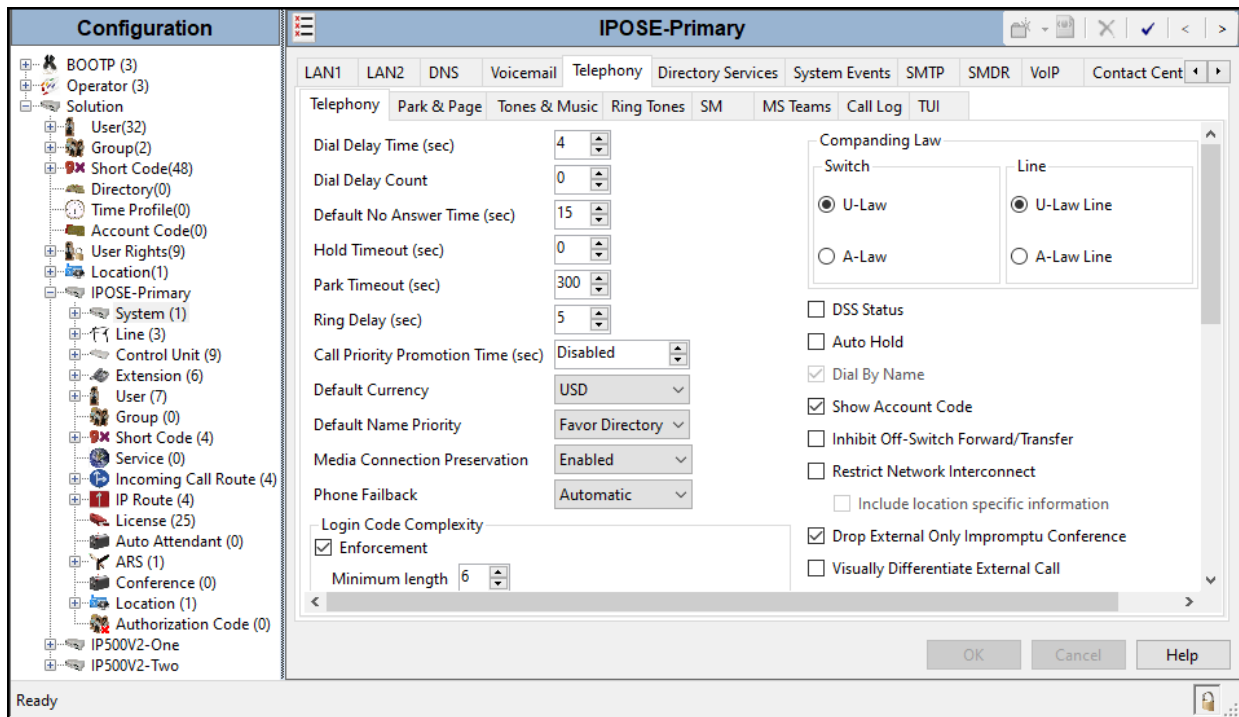
- Select the **Firewall/NAT Type** from the pull-down menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used.
- Set **Binding Refresh Time (seconds)** to **180**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider.
- Set **Public IP Address** to the same public IP address assigned to the Avaya IP Office **LAN2 (Section 5.2.1.1)**.
- Set **Public Port / UDP** to **5060**.
- Default values were used for all other parameters.
- Click the **OK** button.



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.



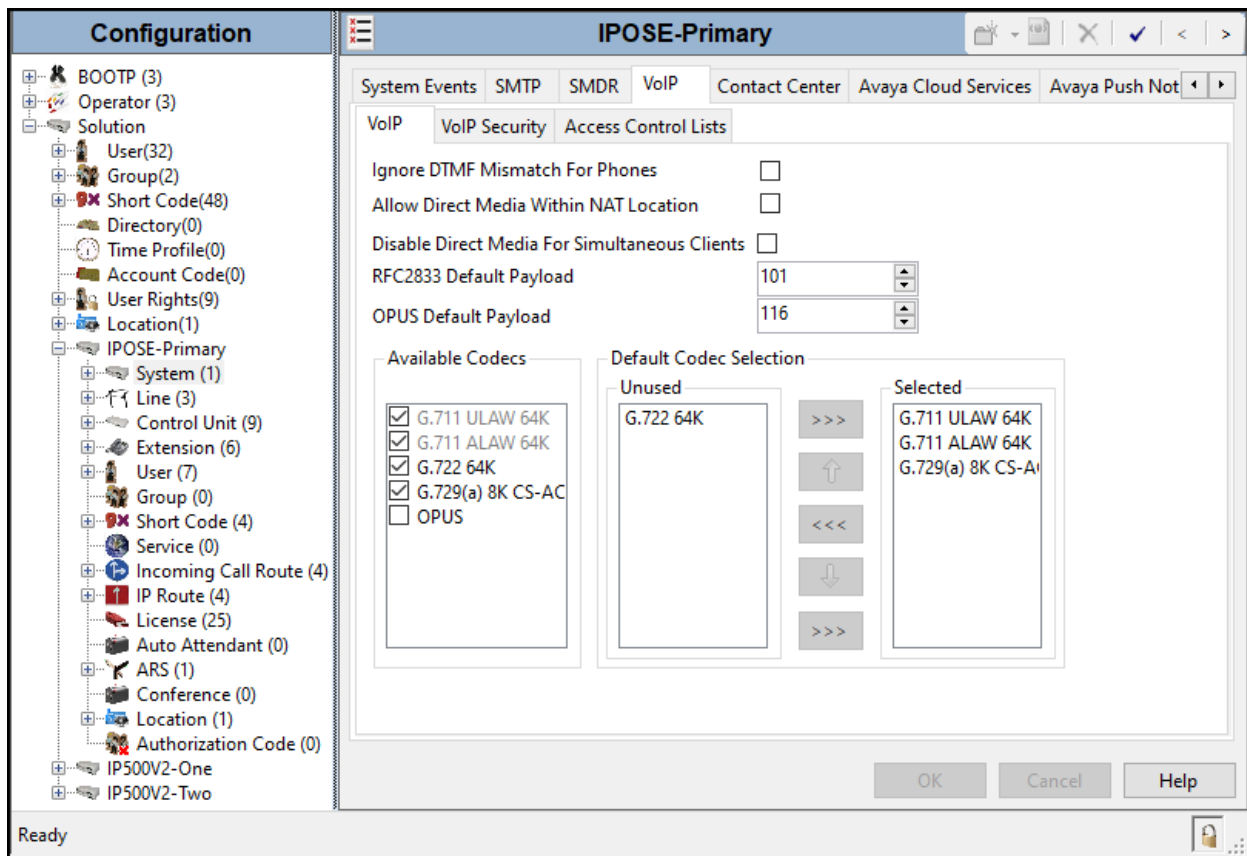
5.2.3. VoIP Tab

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.



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.

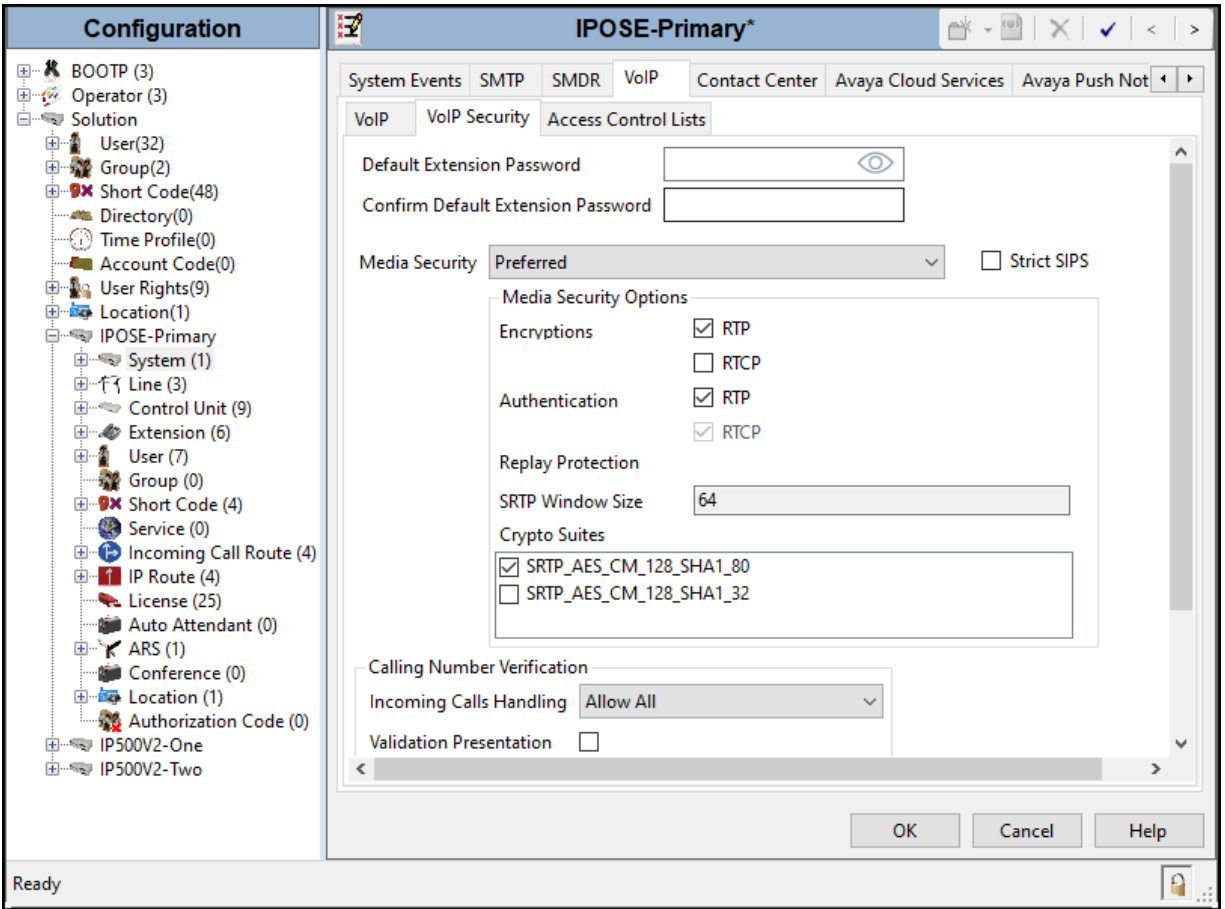
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

- 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.

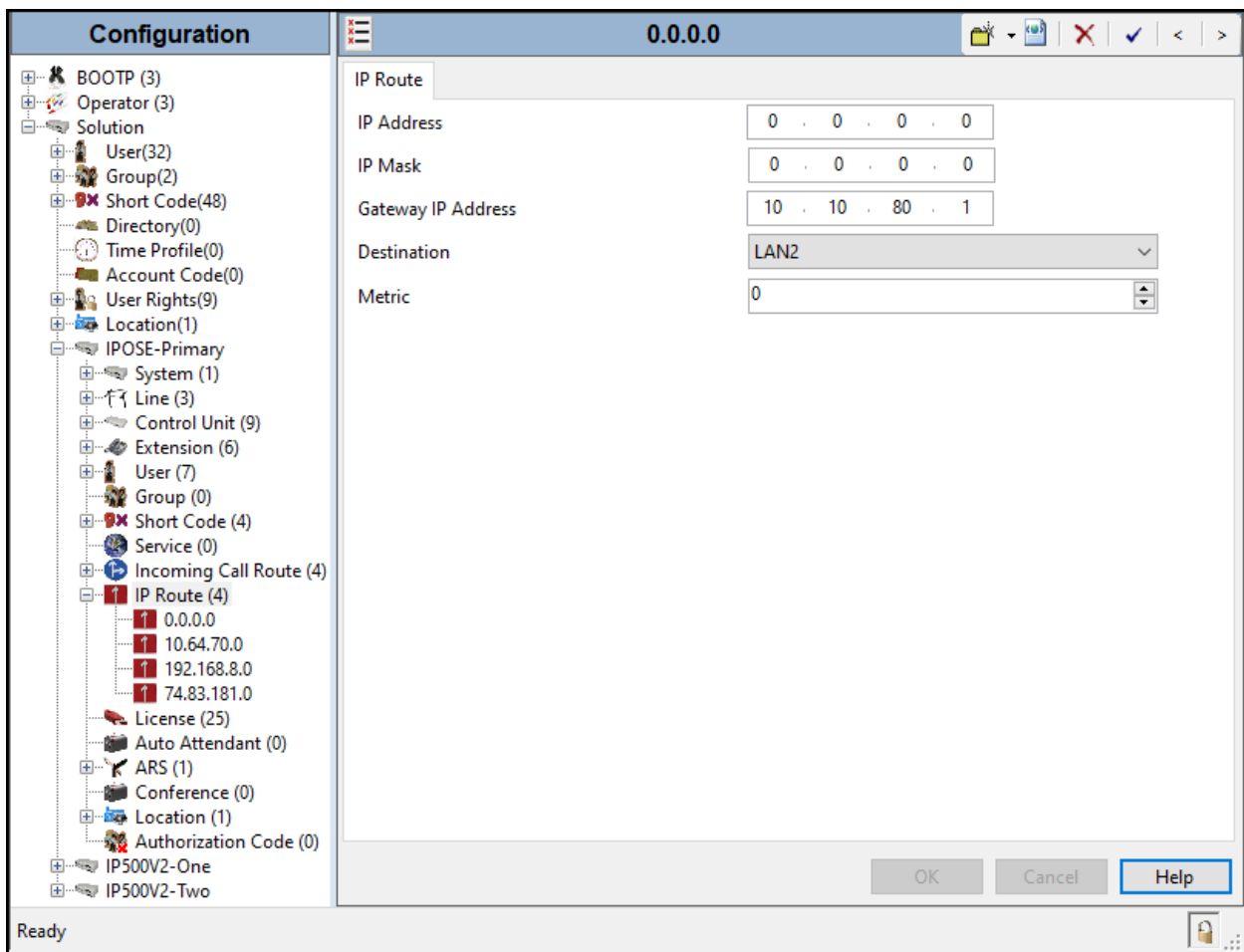


5.3. IP Route

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 Cincinnati Bell 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.



5.4. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Cincinnati Bell. 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 **5.4.6**.

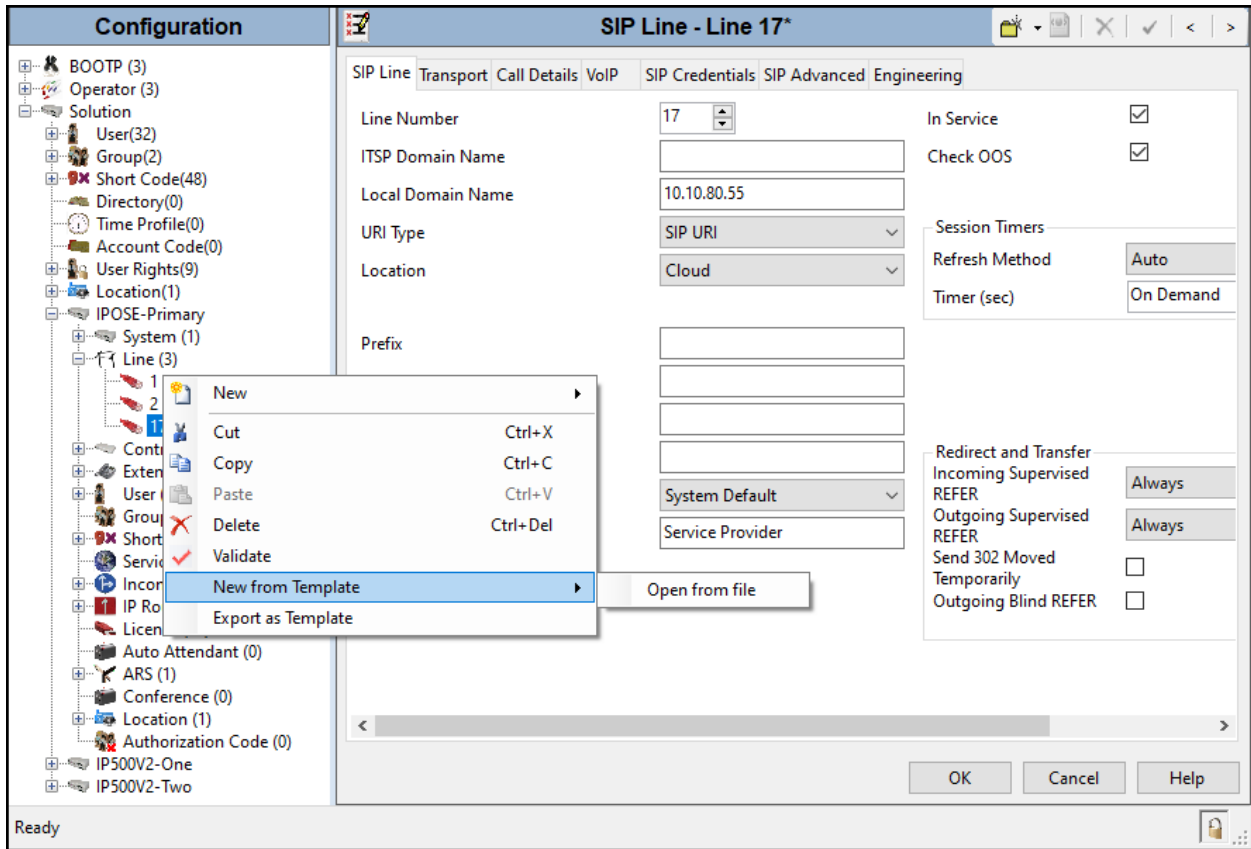
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.6**.

5.4.1. Creating a SIP Trunk from an XML Template

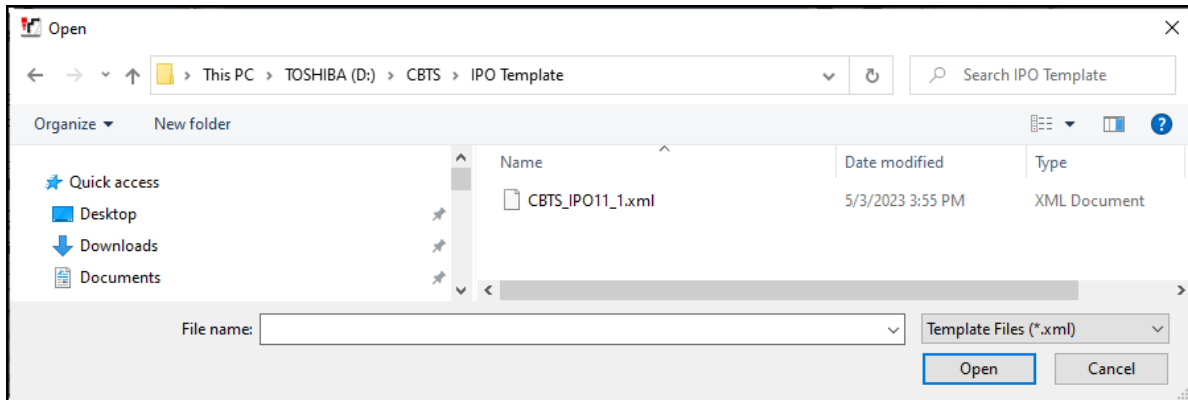
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and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

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

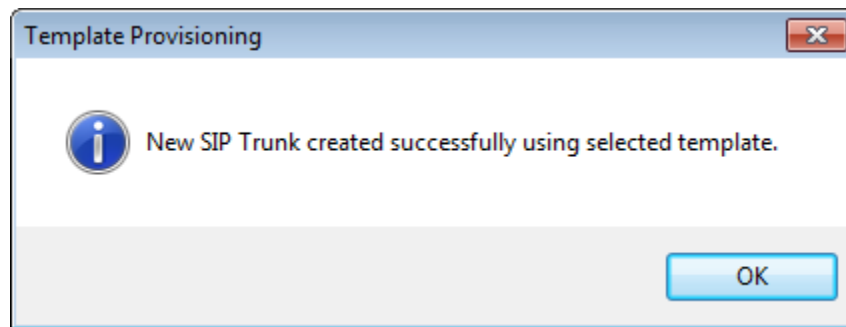
To create the SIP Trunk from the template, from the **Primary** server (**IPOSE-Primary**), right-click on **Line** in the Navigation Pane, then navigate to **New** → **New from Template** → **Open from file**.



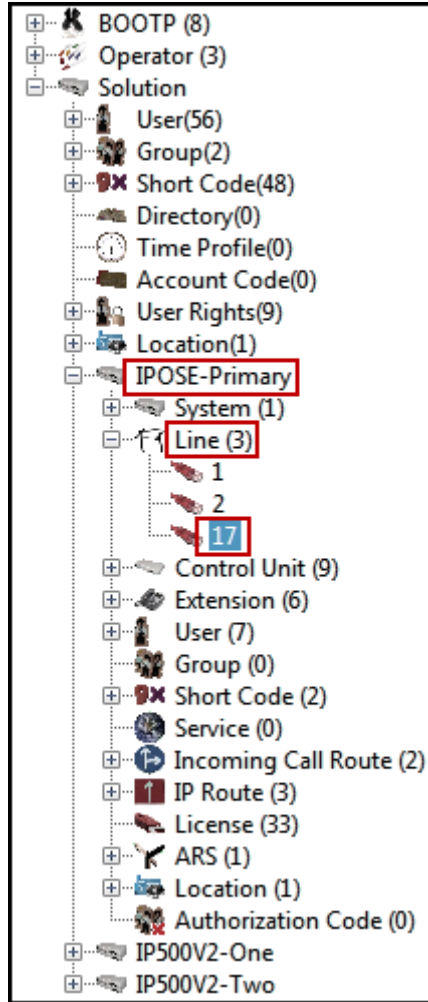
Navigate to the directory on the local machine where the template was copied and select the template.



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



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

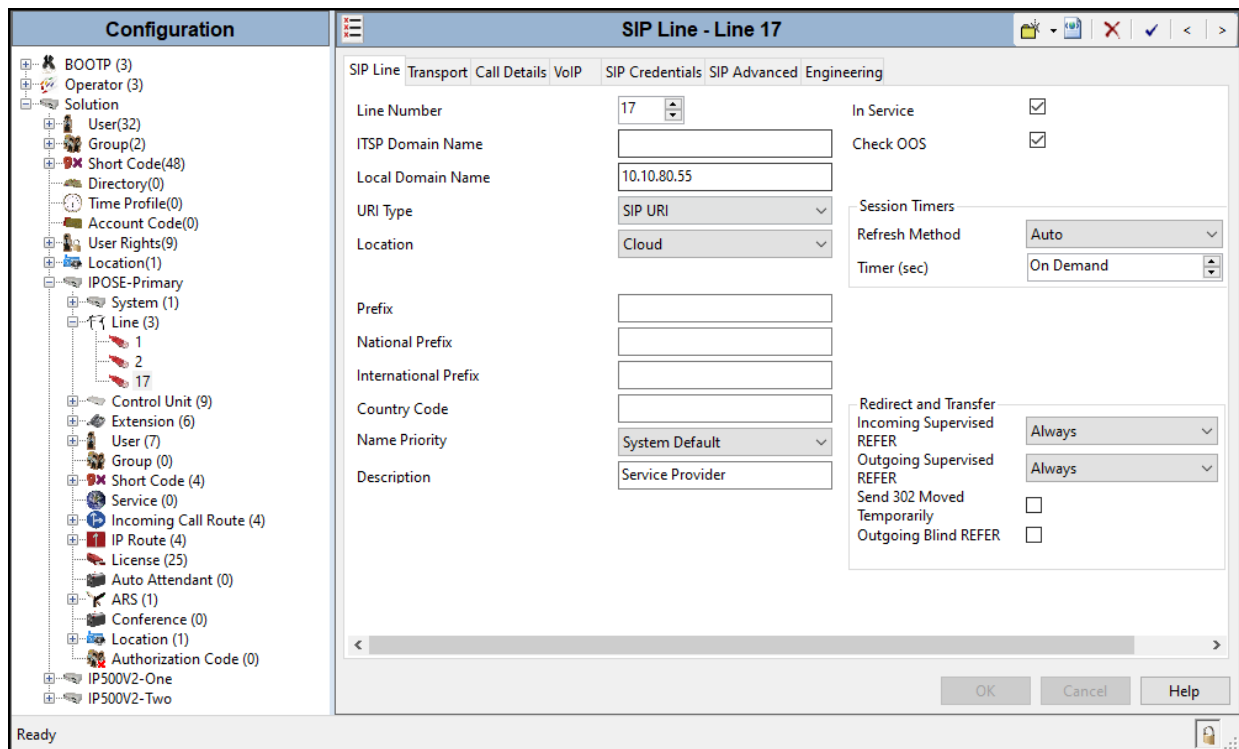


It is important that the SIP Line configuration be reviewed and updated, if necessary, after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2 to 5.4.6**.

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:

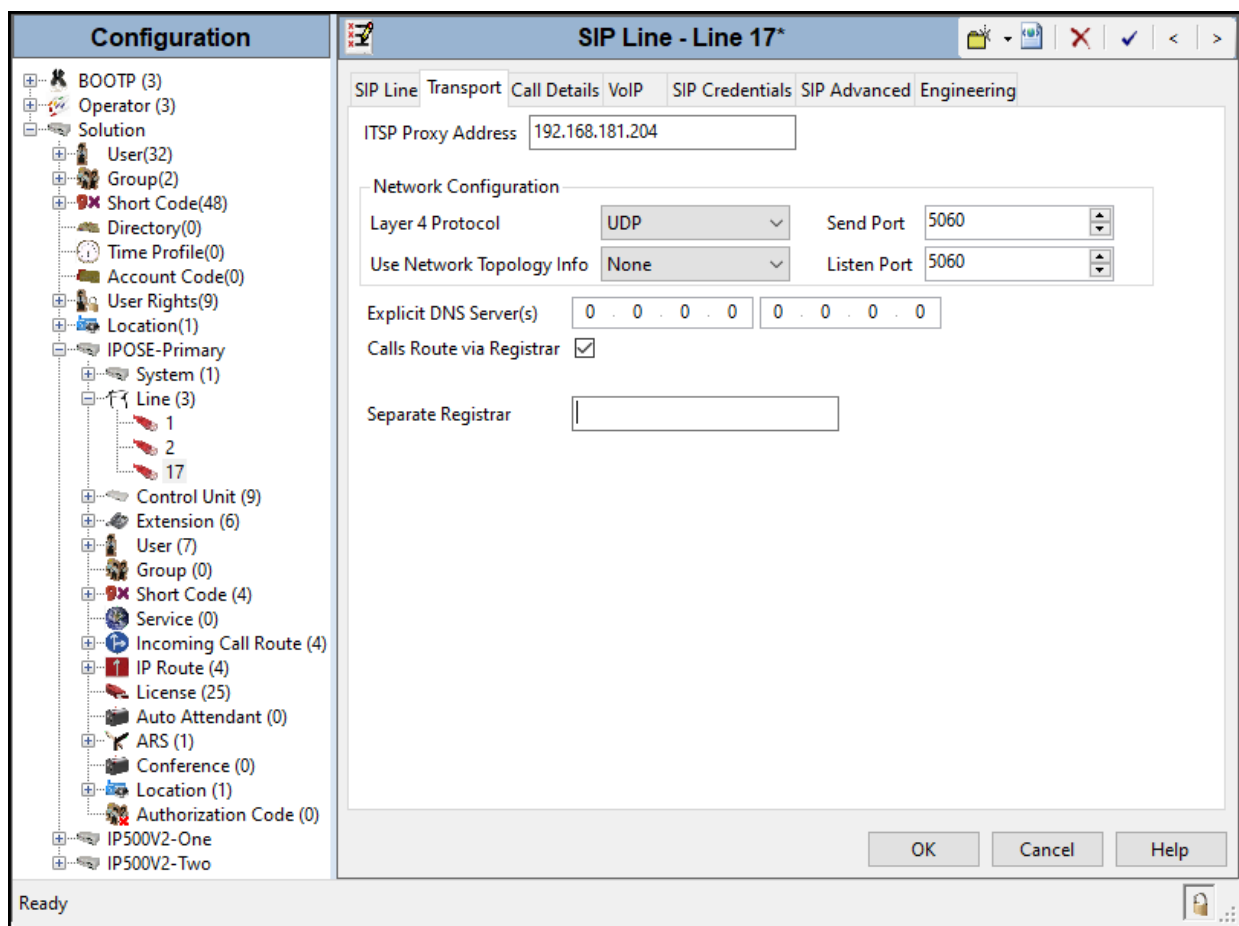
- The **ITSP Domain Name** is left blank.
- The Local Domain Name is set to the IP address of the LAN2 interface configured in **Section 5.2.1.1**.
- Verify that **In Service** box is checked, the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (sec)** is set to **On Demand**.
- For the compliance test REFER support was enabled. Thus, **Incoming Supervised REFER** and **Outgoing Supervised REFER** was set to **Always**.
- Click **OK** to commit.



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 proxy IP address provided by Cincinnati Bell, as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **None** (refer to the note below).
- Set the **Send Port** and **Listen Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit.



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 example screen below one new entry was added for both, incoming and outgoing calls.

The entry was created with the parameters shown below:

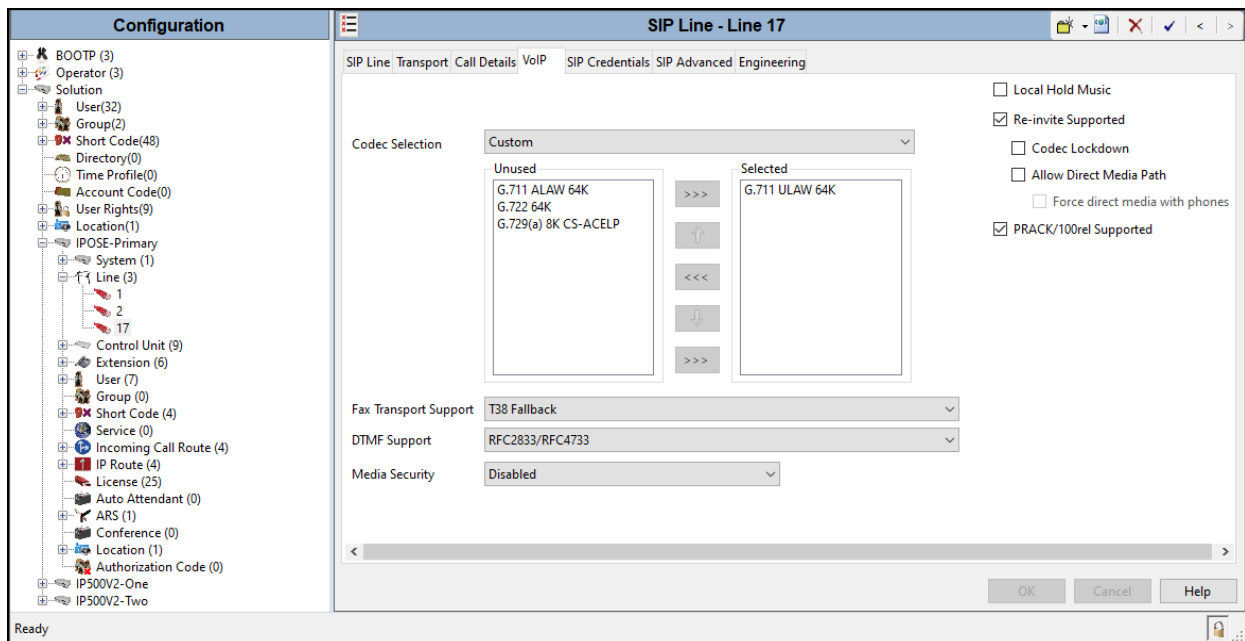
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Set the **Credentials** field to **0: <None>**.
- Check the **P Asserted ID** and **Diversion Header**.
- Set the **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** as shown in the screenshot below.
- Click **OK**.
- Click **OK** to commit again.

	Display	Content	Field meaning		
			Outgoing Calls	Forwarding/Twinning	Incoming Calls
Local URI	Auto	Auto	Caller	Original Caller	Called
Contact	Auto	Auto	Caller	Original Caller	Called
P Asserted ID	<input checked="" type="checkbox"/> Auto	Auto	Caller	Original Caller	Called
P Preferred ID	<input type="checkbox"/> None	None	None	None	None
Diversion Header	<input checked="" type="checkbox"/> Auto	Auto	Caller	Caller	None
Remote Party ID	<input type="checkbox"/> None	None	None	None	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. Only codec **G.711ULAW** was used during the compliance. Other audio codecs may be supported by Cincinnati Bell.
- Select **T38 Fallback** for **Fax Transport Support** (refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- Default values may be used for all other parameters.
- Click the **OK** to commit.



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).

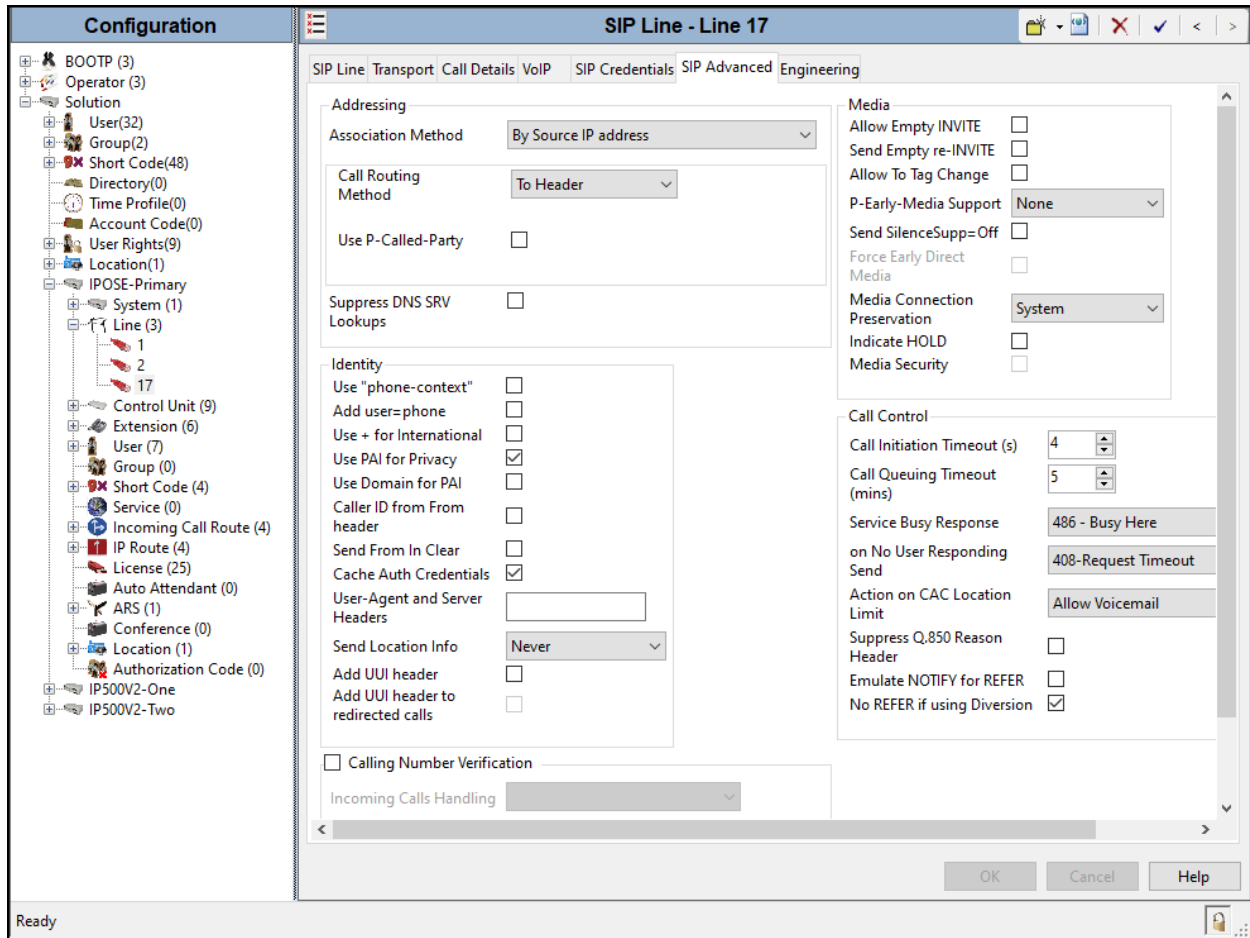
5.4.6. SIP Line – SIP Advanced Tab

In the **Addressing** area:

- Select **To Header** for **Call Routing Method**.

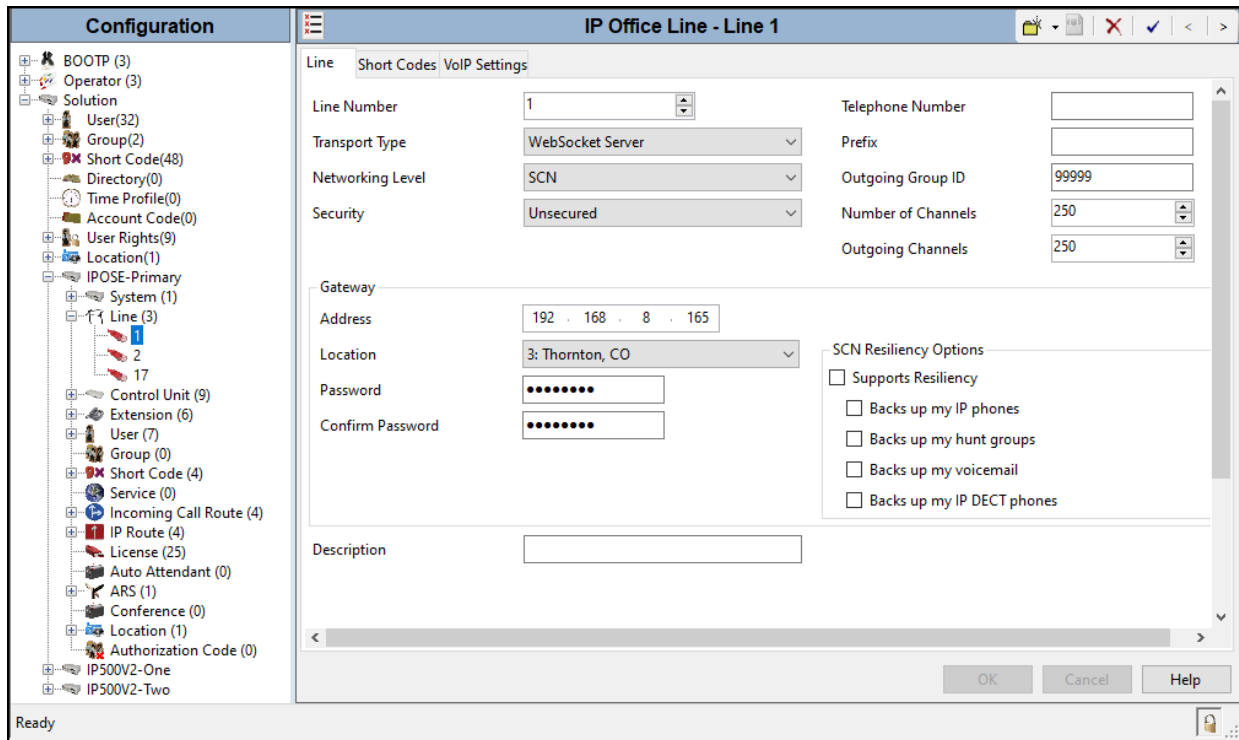
In the **Identity** area:

- Check the box for **Use PAI for Privacy**.
- Check the box for **No REFER if using Diversion** (refer to **Section 2.2**).
- Click **OK** to commit.



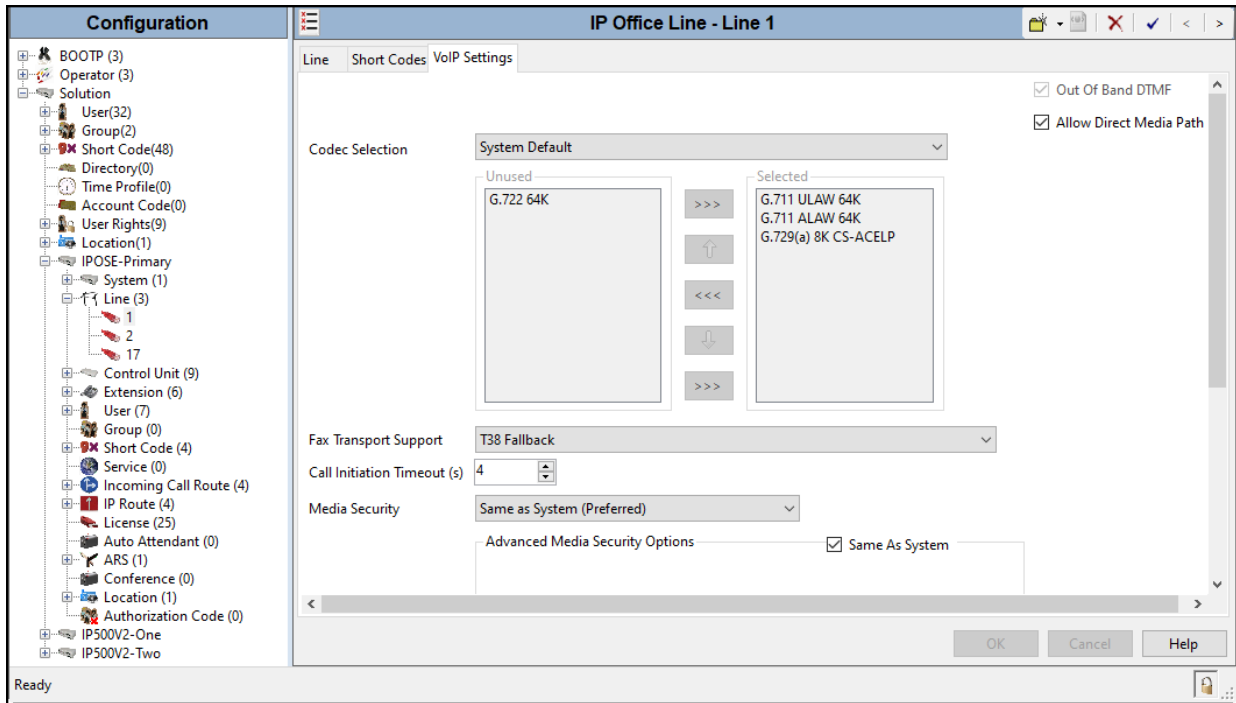
5.5. IP Office Line – Primary Server

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 IP500V2-One Expansion System.



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

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

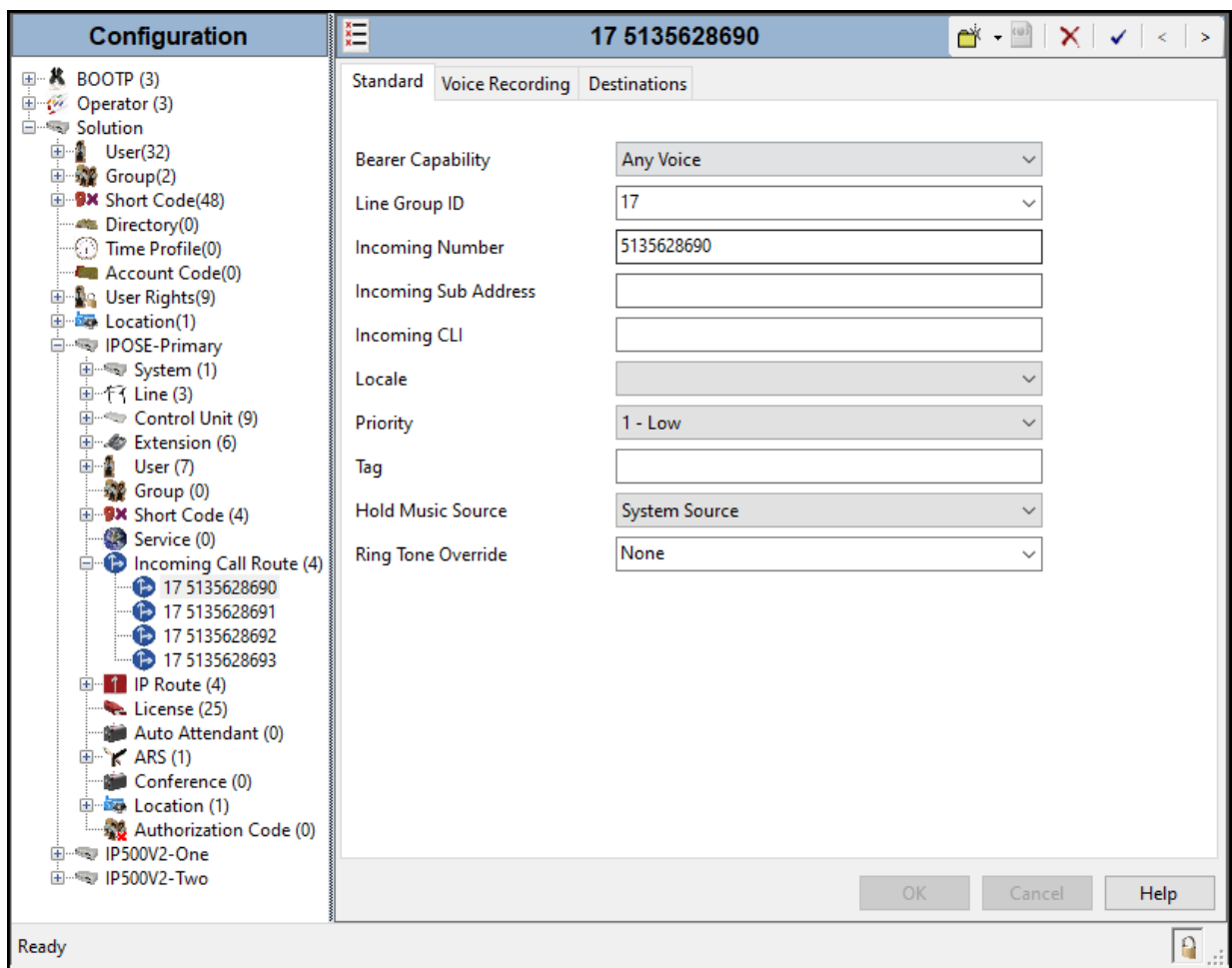


Repeat this process as needed to add additional Secondary server or Expansion Systems to the solution.

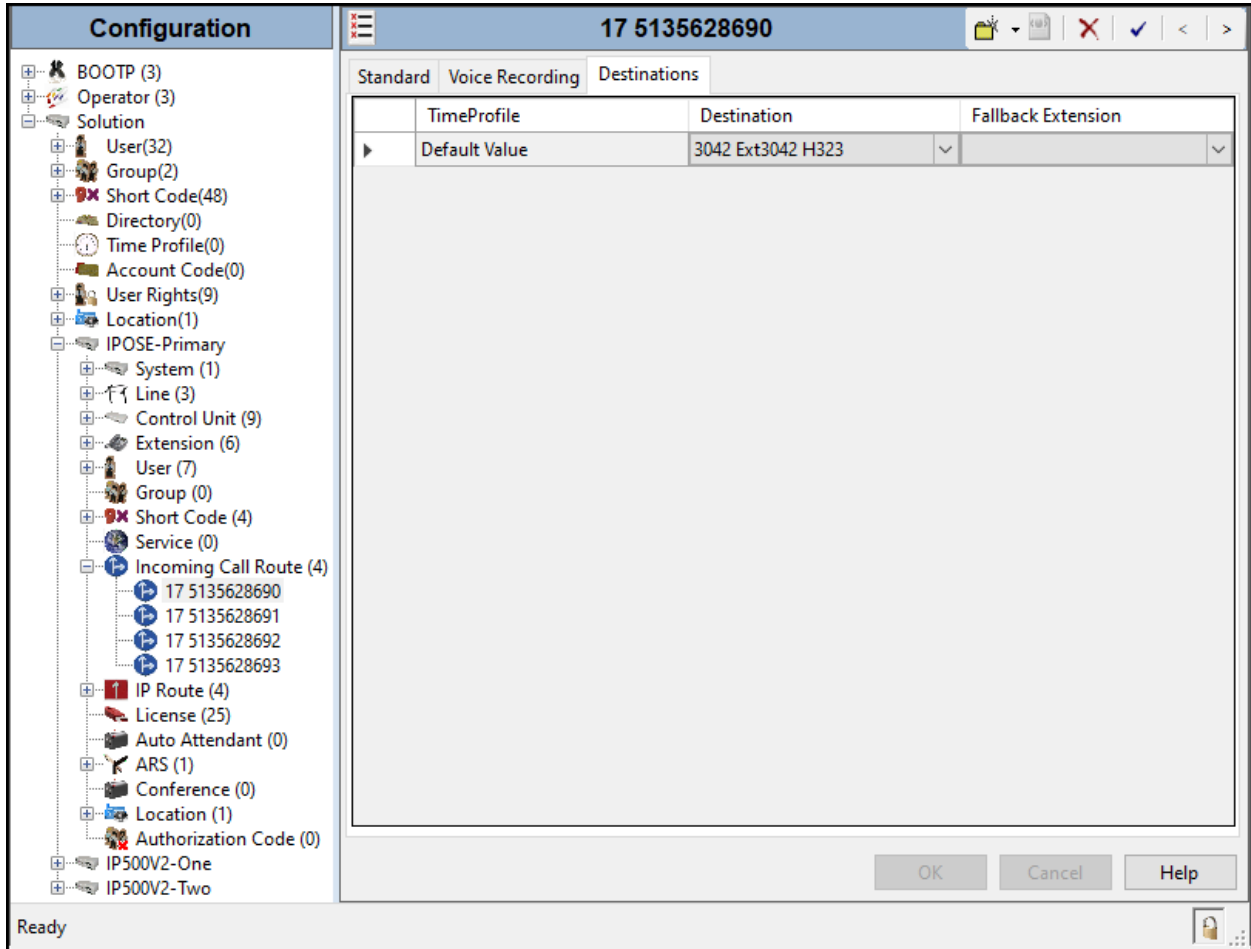
5.6. Incoming Call Route

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 Capability** to **Any Voice**.
- The **Line Group ID** is set to **17**. This matches the **Incoming Group** field configured in the **Call Details** tab for the SIP Line on **Section 5.4.4**.
- On the **Incoming Number**, enter one of the DID numbers provided by Cincinnati Bell.
- Default values may be used for all other parameters.
- Click **OK** to commit.



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 **5135628690** provided by Cincinnati Bell was associated with the Avaya IP Office extension **3042**.



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.).

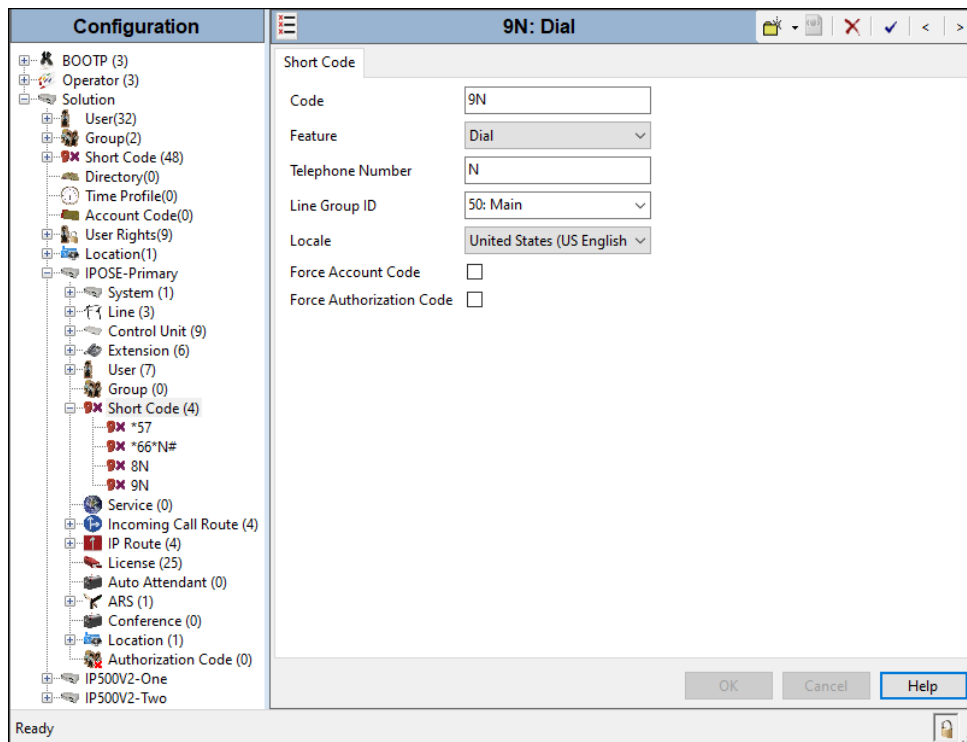
5.7. Outbound Call Routing

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 **United States (US English)** was used.
- Click the **OK** to commit.

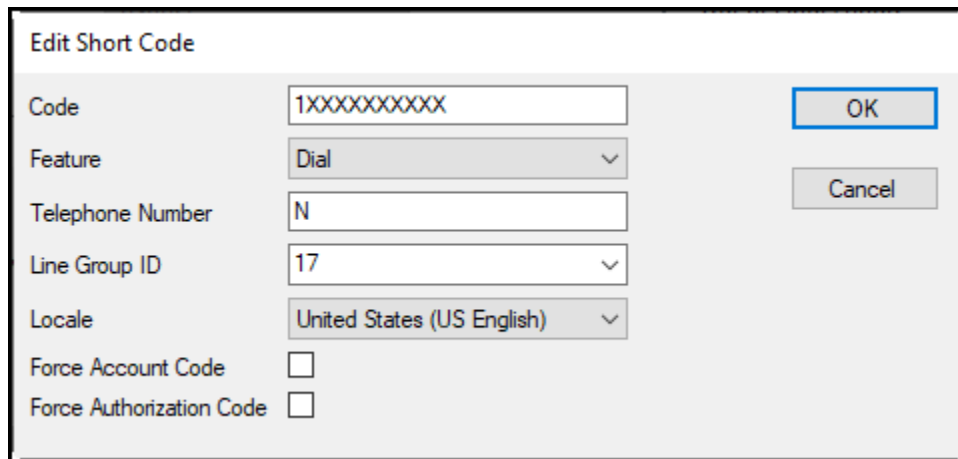


The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **Xs** used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string. This type of setting results 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 **N**. 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 17** was used.
- For **United States (US English)** was used
- Click **OK** to commit.

The following example shows the dial pattern for calls within the North America dialing plan.



Code	1XXXXXXXXXX	OK
Feature	Dial	Cancel
Telephone Number	N	
Line Group ID	17	
Locale	United States (US English)	
Force Account Code	<input type="checkbox"/>	
Force Authorization Code	<input type="checkbox"/>	

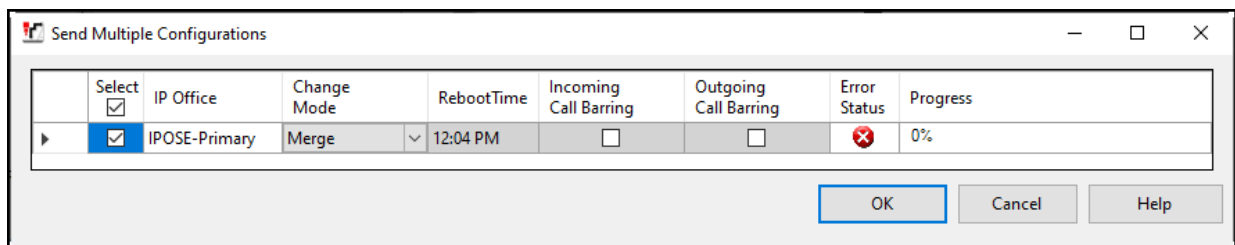
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

5.8. Save IP Office Primary Server Configuration

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

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

Click **OK** to execute the save.



6. Avaya IP Office Expansion System Configuration

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

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

Configuration Pane: Shows a hierarchical tree structure of system components. The selected system is **IP500V2-One**, which is expanded to show its sub-components: **System (1)**, **IP500V2-One**, **Line (3)**, **Control Unit (4)**, **Extension (24)**, **User (27)**, **Group (1)**, **Short Code (12)**, **Service (0)**, **RAS (1)**, **Incoming Call Route (1)**, **WAN Port (0)**, **Firewall Profile (1)**, **IP Route (2)**, **License (2)**, **Tunnel (0)**, **ARS (2)** (with sub-items **50: Main** and **51: To-Primary**), **Location (1)**, **Authorization Code (0)**, and **IP500V2-Two**.

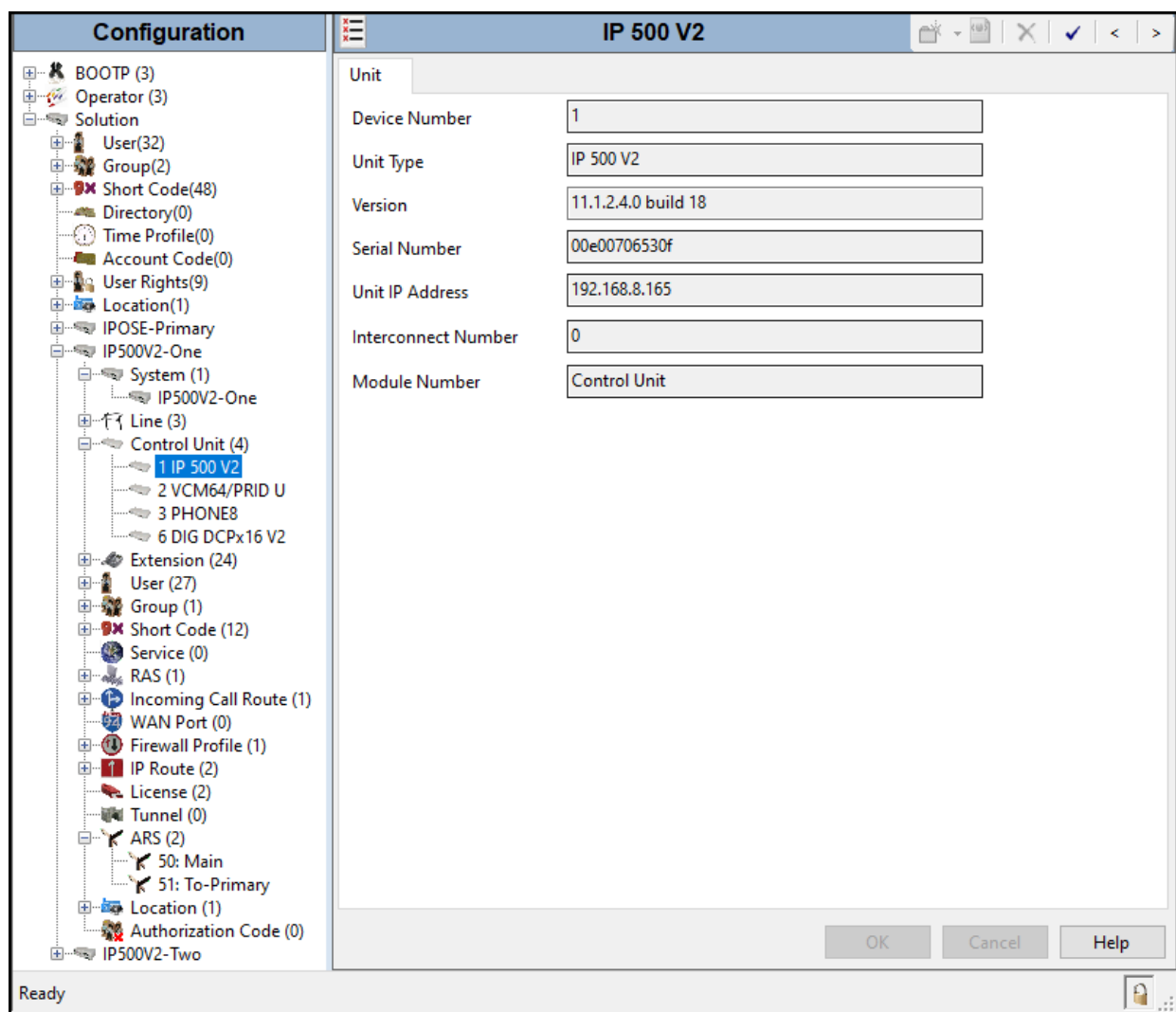
System Inventory Pane: Displays the configuration details for the selected system, titled **Server Edition Expansion System**. The details are organized into three sections:

- Hardware Installed:**
 - Control Unit: IP 500 V2
 - Internal Modules: VCM64/PRID U; PHONE8
 - Expansion Modules: DIG DCPx16 V2
- System Settings:**
 - IP Address: 192.168.8.165
 - Sub-Net Mask: 255.255.255.0
 - System Locale: United States (US English)
 - System Location: 3: Thornton, CO
 - Device ID: NONE
 - Number of Extensions on System: 24
- Features Configured:**
 - Licenses Installed: Server Edition(1); IP Office Select(1); SIP Trunk Channels(10)
 - Connected Extensions: 3043; 3044
 - Users NOT Configured for Voicemail: Ext3049 Fax
 - Users assigned as Ex-Directory: NONE
 - Users assigned for Twinning: NONE
 - Users barred from making Outgoing Calls: NONE
 - Music on Hold: WAV File

The status bar at the bottom left indicates **Ready**, and a small system tray icon is visible at the bottom right.

6.1. Physical Hardware

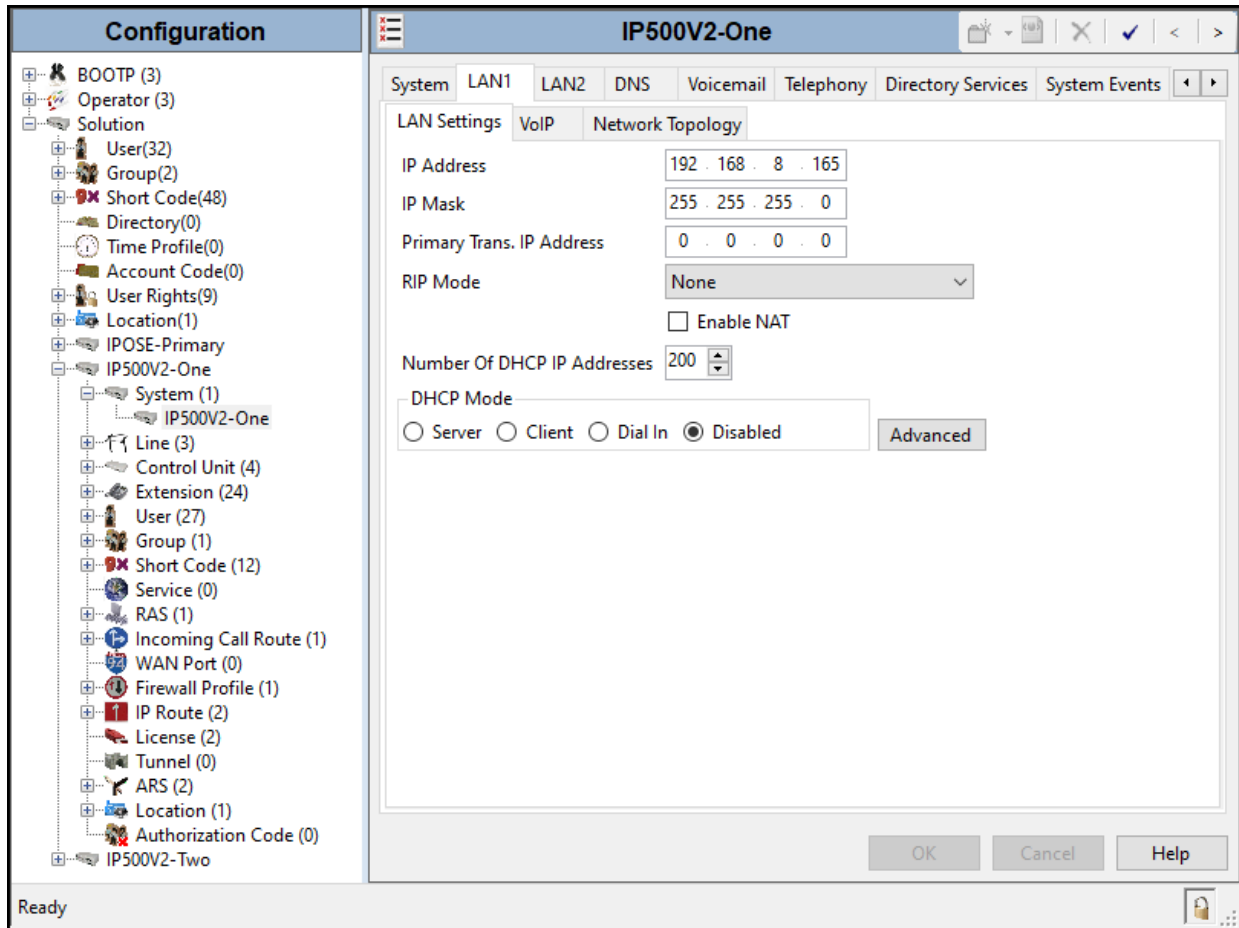
In the sample configuration, the IP500 V2 Expansion System contained a PHONE8 analog card, for the support of analog extensions, a DIG DCPx16 V2, for support of digital extensions. Also included is a VCM64 (Voice Compression Module). The VCM64 cards provide voice compression channels to the control unit. 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: 192.168.8.165** was used in the reference configuration.
- **IP Mask: 255.255.255.0** was used in the reference configuration.
- Click the **OK** button.

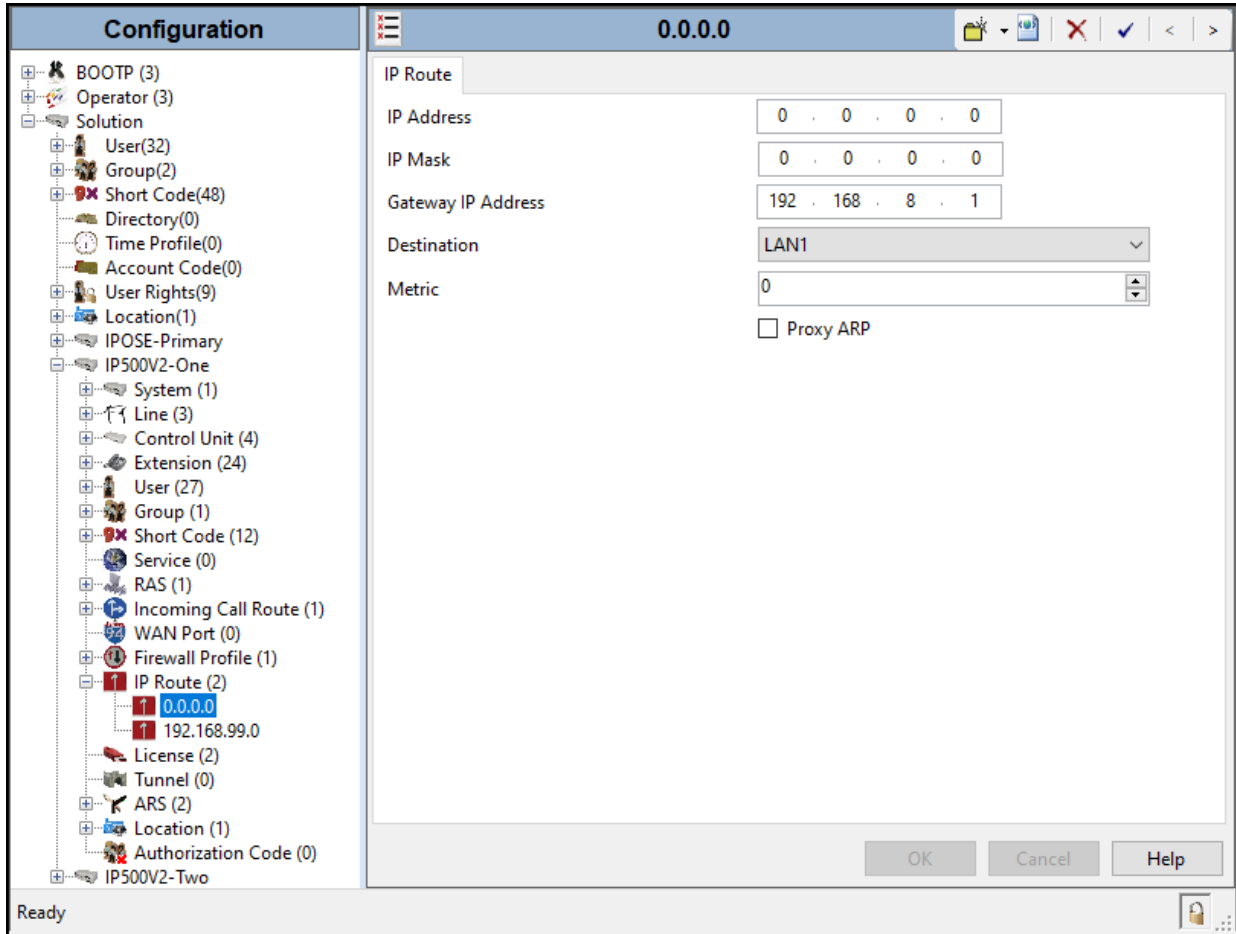


Default values were used on the **VoIP** and **Network Topology** tabs (not shown).

6.3. IP Route

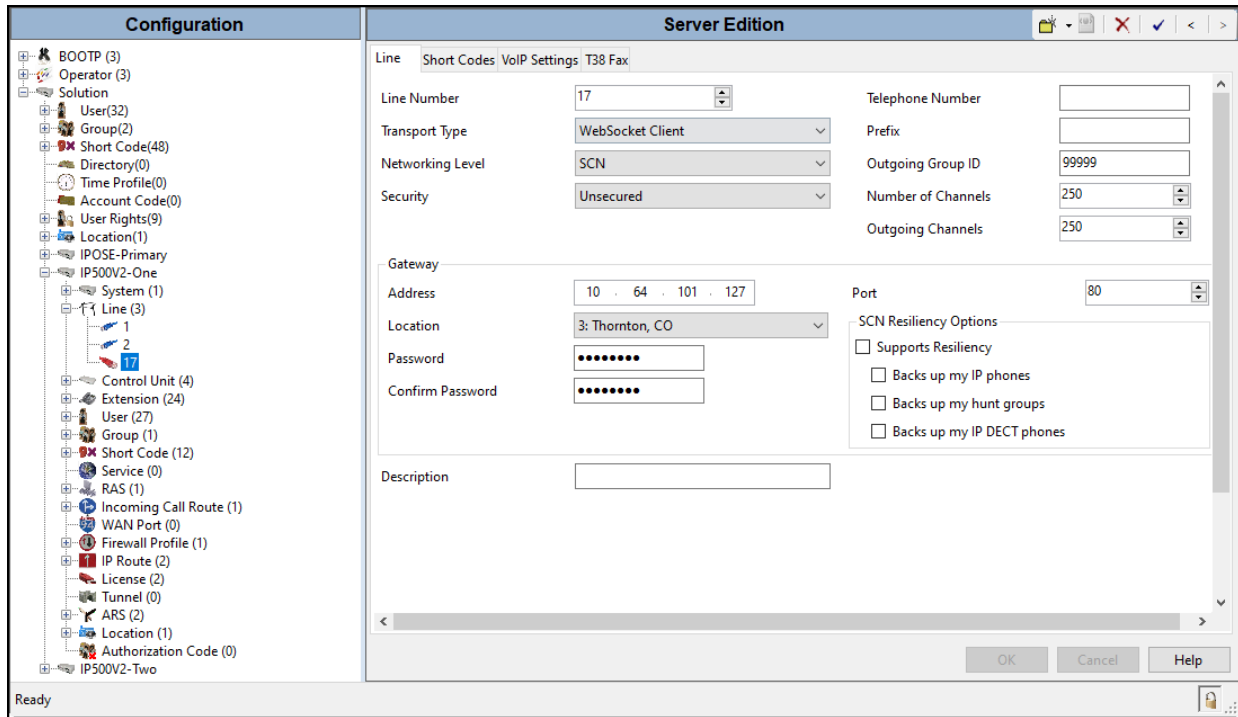
To create an IP route for the Expansion system, right-click on **IP Route** on the left Navigation pane. Select **New** (not shown).

- Enter **0.0.0.0** on the **IP Address** and **IP Mask** fields to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet. The default gateway in the reference configuration was **192.168.8.1**
- Set **Destination** to **LAN1** from the pull-down menu.



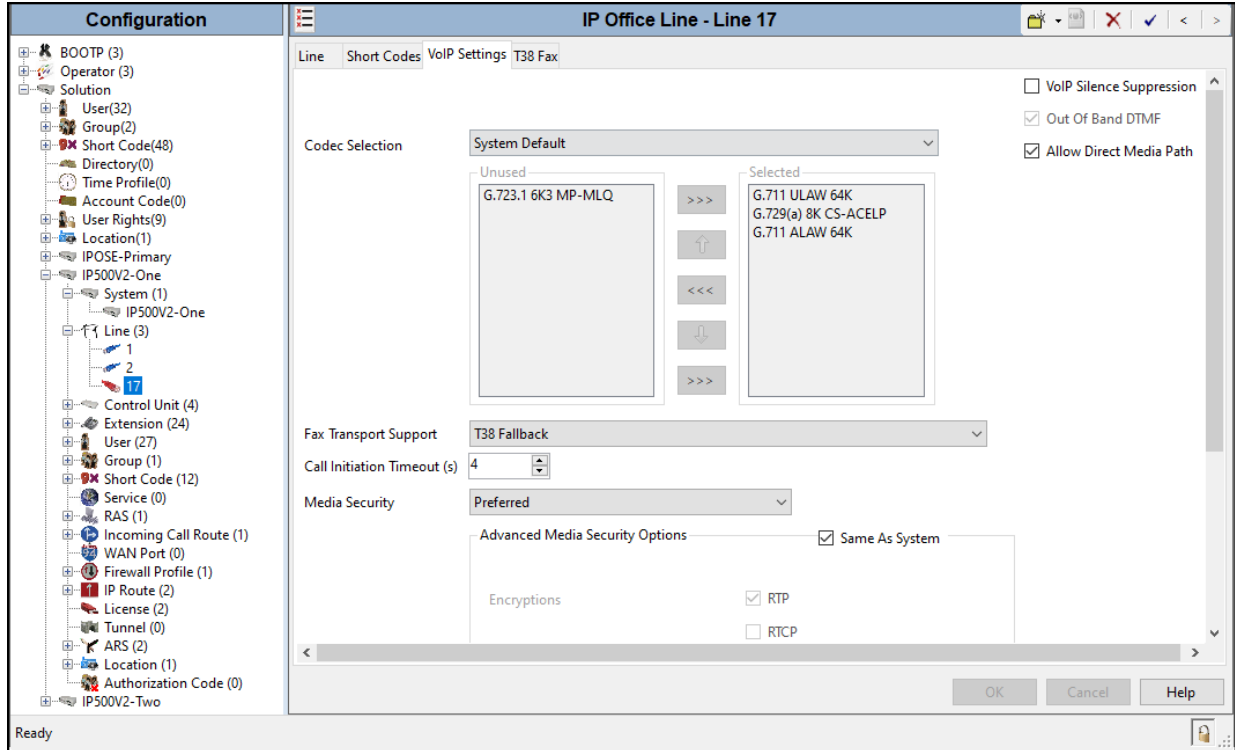
6.4. IP Office Line – IP500 V2 Expansion System

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:

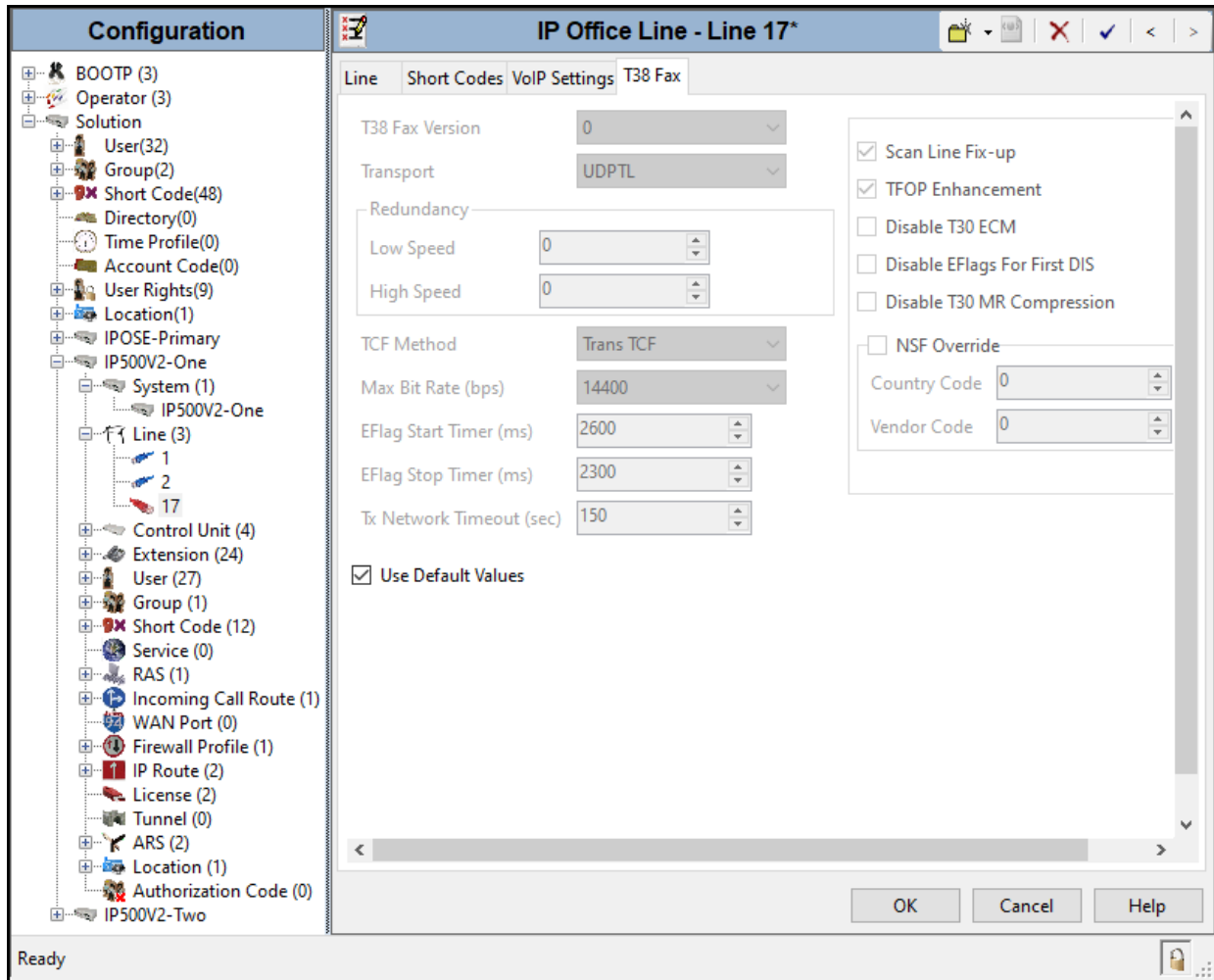
- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **T38 Fallback** for **Fax Transport Support** (refer to Section 2.2).
- Under **Media Security** verify **Same as System (Preferred)** is selected (default value).



Select the **T38 Fax** tab, to set the Fax over Internet Protocol parameters of the SIP Line. Set or verify the parameters as shown below:

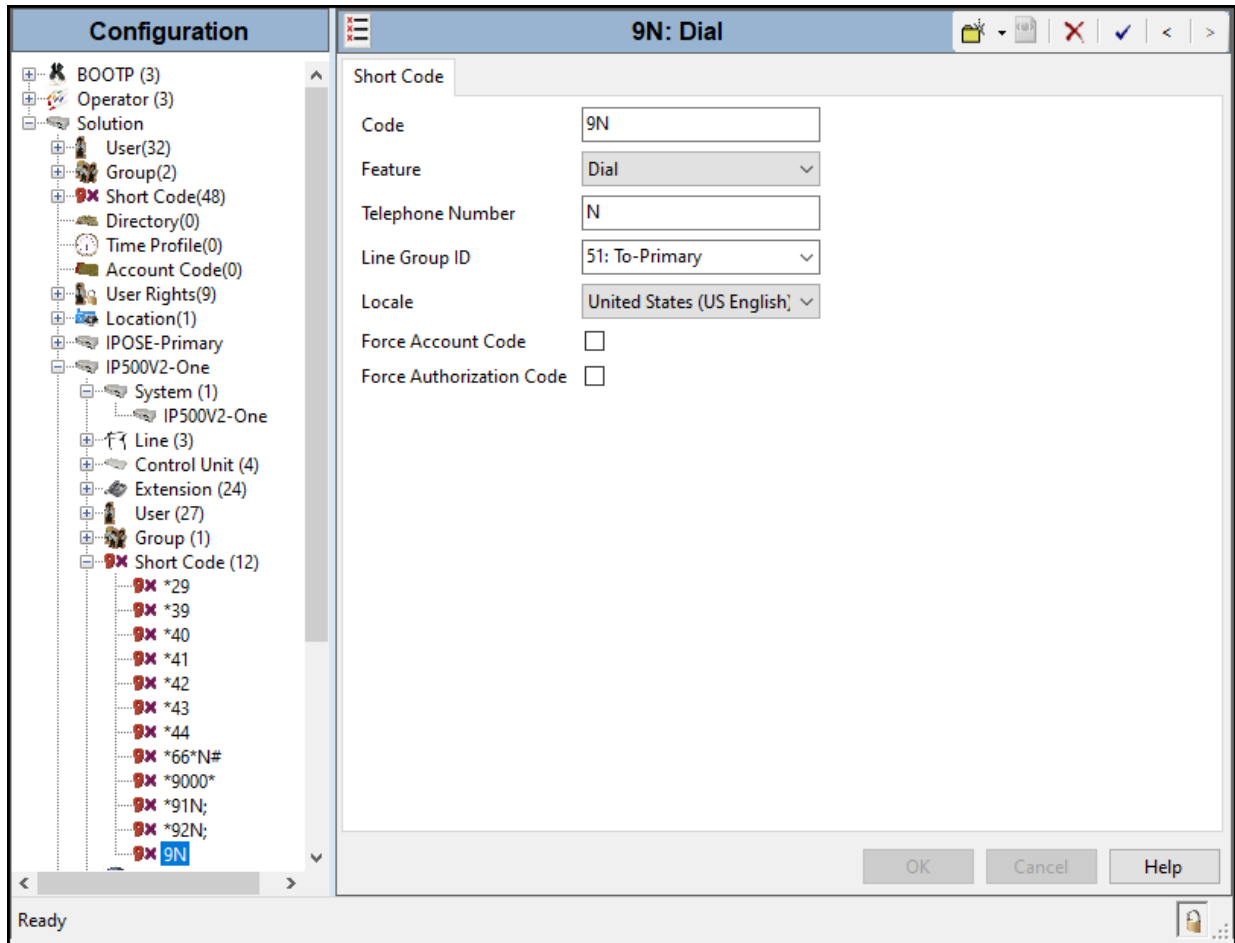
- check the **Use Default Values** at the bottom of the screen.

Note: T.38 fax was not tested for reasons noted in **Section 2.2**. The T.38 fax settings shown below may need to be adjusted if changes are made by Cincinnati Bell to route T.38 fax calls via a PSTN carrier that supports T.38 fax.



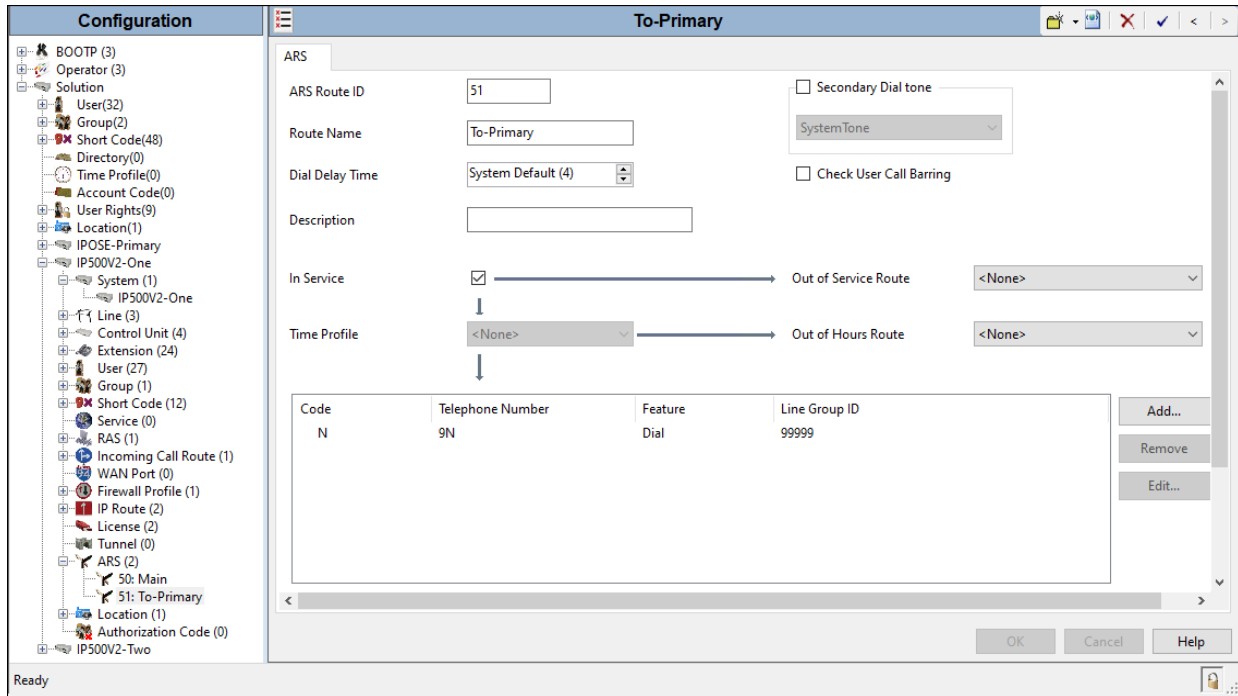
6.5. Short Codes

Similar to the configuration of the Primary server in **Section 5.7.1**, create a Short Code to access ARS. In the reference configuration, the **Line Group ID** is set to the ARS route illustrated in the next section.



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**).

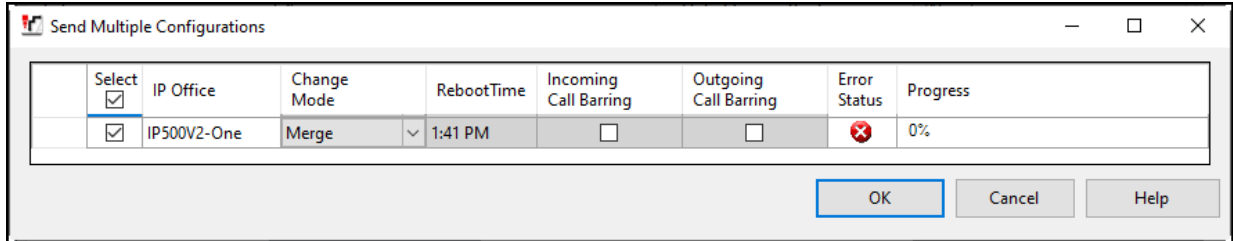


Repeat this process described in **Section 6** on any additional Secondary servers or Expansion Systems in the solution as required.

6.7. Save IP Office Expansion System Configuration

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

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



7. Cincinnati Bell SIP Trunking Service Configuration

To use Cincinnati Bell SIP Trunking Service, a customer must request the service from Cincinnati Bell using the established sales processes. The process can be started by contacting Cincinnati Bell via the corporate web site at <https://www.altafiber.com/business/support/sip-trunking-support> and requesting information.

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

Cincinnati Bell is responsible for the configuration of Cincinnati Bell 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.

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

- Cincinnati Bell's SIP Proxy IP address.
- DID numbers.
- DNS IP addresses.
- Voice codecs supported.
- Etc.

8. Verification Steps

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

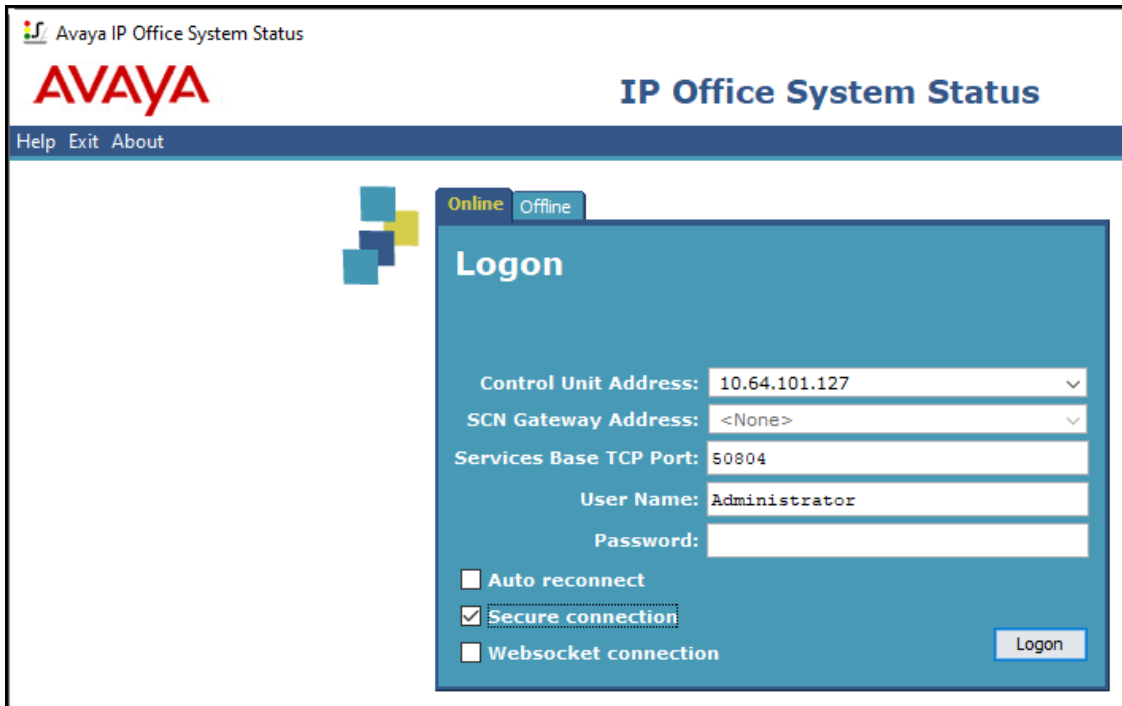
The following steps may be used to verify the configuration:

- 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.



The screenshot shows the Avaya IP Office System Status application interface. At the top left is the Avaya logo and the text "Avaya IP Office System Status". To the right is the title "IP Office System Status". Below the title is a menu bar with "Help", "Exit", and "About". The main content area features a "Logon" dialog box with the following fields and options:

- Control Unit Address: 10.64.101.127 (dropdown)
- SCN Gateway Address: <None> (dropdown)
- Services Base TCP Port: 50804 (text field)
- User Name: Administrator (text field)
- Password: (password field)
- Auto reconnect
- Secure connection
- Websocket 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 displays the Avaya IP Office System Status interface. The left sidebar contains a navigation menu with the following items: System, Alarms (9), Extensions (0), Trunks (3) (with sub-items Line: 1, Line: 2, and Line: 17 selected), Active Calls, Resources, Voicemail, IP Networking, and Locations. The main content area is titled "IP Office System Status" and has tabs for Status, Utilization Summary, and Alarms. The "Status" tab is active, showing a "SIP Trunk Summary" section with the following details:

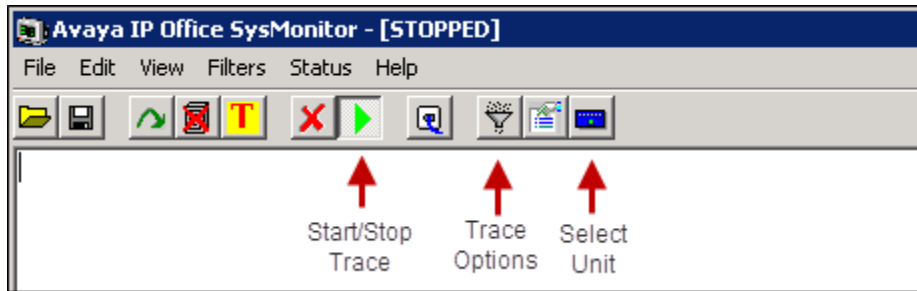
- Line Service State: In Service
- Peer Domain Name: sip://.181.204
- Resolved Address: 181.204
- Line Number: 17
- Number of Administered Channels: 10
- Number of Channels in Use: 0
- Administered Compression: G711 Mu
- Silence Suppression: Off
- Media Stream: RTP
- Layer 4 Protocol: UDP
- SIP Trunk Channel Licenses: 256
- SIP Trunk Channel Licenses in Use: 0 (indicated by a green circle and 0%)
- SIP Device Features: REFER (Incoming and Outgoing), UPDATE (Incoming and Outgoing)

Below the summary is a table with the following columns: Cha... U., Call Ref, Cur... in S..., Time, Rem..., C..., Con..., Caller ID ..., Other Party ..., Dire..., Rou..., Rec..., Rec..., Tra..., Tra... The table contains 10 rows, all with "Idle" in the "Cur... in S..." column and "27 ..." in the "Time" column.

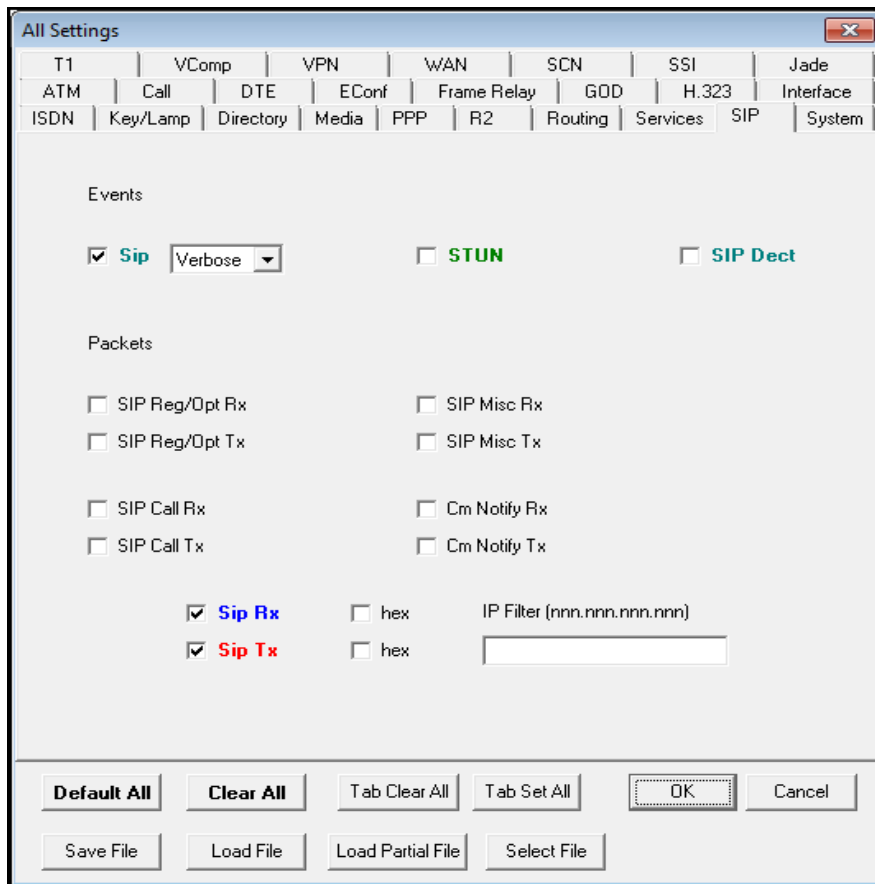
At the bottom of the interface, there are several control buttons: Trace, Trace All, Pause, Ping, Call Details, Graceful Shutdown, Force Out of Service, Print..., and Save As... The status bar at the bottom right shows the time "2:52:42 PM" and the status "Online".

8.2. Monitor

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



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



9. Conclusion

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

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

10. Additional References

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

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

- [1] *Deploying IP Office Platform Server Edition, Release 11.1 FP2, Issue 26, January 2023.*
- [2] *IP Office Platform 11.1.2.4, Deploying Avaya IP Office Servers as Virtual Machines, Issue 13, January 2023.*
- [3] *Avaya IP Office Platform Server Edition Reference Configuration Release 11.1 FP2, Issue 18, January 2023.*
- [4] *IP Office Platform 11.1 FP2, Deploying an IP500 V2 IP Office Essential Edition System, Issue 39b, March 3, 2023.*
- [5] *Administering Avaya IP Office using Manager, Release 11.1.2.4, Issue 43, March 2023.*
- [6] *Avaya IP Office Platform Feature Description, Release 11.1 FP2, Issue 18, January 2023.*

Additional Avaya IP Office documentation can be found at:

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

©2023 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.