Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.0 to support CenturyLink IQ® SIP Trunking Service on the Broadsoft Platform - 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 CenturyLink IQ® SIP Trunking Service on the Broadsoft Platform.

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 CenturyLink 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 11.0 (hereafter referred to as IP Office) and various Avaya endpoints, listed in **Section 4**.

The CenturyLink IQ® SIP Trunking Service on the Broadsoft Platform 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” or “CenturyLink” 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 CenturyLink’s network via the public Internet, as depicted in **Figure 1**, and exercise the features and functionalities listed in **Section 2.1**.

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

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

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

2.1. Interoperability Compliance Testing

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

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, Digital and Analog telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323, Digital and Analog telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider network.
- Incoming and outgoing PSTN calls to/from Avaya 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 and international calls were not tested.

2.2. Test Results

Interoperability testing of CenturyLink IQ® SIP Trunking Service on the Broadsoft Platform 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 CenturyLink does not include the "Privacy: id" header. This is causing the far-end to still see the number presented in the P-Asserted Identity header. This is currently being investigated by IP Office development team. For Outbound Anonymous Calls, CenturyLink requires the domain name (voip.centurylink.com) to be present in the P-Asserted Identity header or it will reject the call with a "604 Does Not Exist Anywhere" message. This was accomplished by enabling the field "**Use Domain for PAI**" in the SIP Line Advanced tab as shown in **Section 5.4.7**.
- **OPTIONS –** CenturyLink 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.
- **Outbound T.38 Fax issue with codec G.729A –** CenturyLink supports codecs G.711ULAW and G.729A, for T.38 fax calls from IP Office to the PSTN, the initial voice call was always set up with codec G.729A instead of G.711MU, IP Office was unable to detect fax tone from the far end with codec G.729A, causing IP Office not to send a re-INVITE for T.38. In addition, a re-INVITE for T.38 was never sent by CenturyLink. This behavior resulted in outbound T.38 fax call attempts failing. This behavior did not affect inbound T.38 fax calls (calls from the PSTN to IP Office), inbound T.38 fax calls were transmitted successfully. The solution/work around for this issue is to configure the SIP Trunk to CenturyLink with codec **G.711ULAW only**, as noted in **Section 5.4.6**. Note that the testing was done with the SIP Trunk configured with both codecs, G.711ULAW and G.729A, as shown in **Sections 5.4.6**.
- **G.711 pass-through fax –** The G.711 pass-through fax method was also tested, inbound and outbound G.711 pass-through fax calls worked intermittently. This may be due 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, G.711 fax pass-through is delivered on a "best effort" basis; its success is not guaranteed, and it should be used at the customer's discretion. Fax Transport Support was configured in IP Office as **T.38 Fallback** (refer to **Sections 5.4.6**, **5.5** and **6.4**), with this setting IP Office will first attempt to use T.38, and then it will attempt to use G.711 pass-through if T.38 fails. Note that for T.38 fax to work the SIP Trunk to CenturyLink needs to be configured with codec **G.711ULAW only**, as noted in **Section 5.4.6**.
- **Voice/Audio codecs supported by CenturyLink –** CenturyLink supports voice/audio codecs G.711ULAW and G.729A. During the compliance test the preferred codec order offered by CenturyLink for calls from the PSTN to IP Office was "**0 18**" respectively, which represent codecs G.711ULAW as the first choice and G.729A as the second choice, with G.711ULAW as the preferred codec. The codec order in IP Office was configured to match this codec order, resulting in IP Office prioritizing the codec order for calls from the PSTN to IP Office and selecting codec G.711ULAW for voice/audio,

as expected. It was observed that for calls from IP Office to the PSTN the voice/audio codec selected by CenturyLink was always G.729A instead of G.711ULAW, the expectation was that codec G.711ULAW would be selected since the codec order for these calls contained codecs "**0 18**" respectively, which represent G.711ULAW as the first choice and G.729A as the second choice, with G.711ULAW as the preferred codec. This behaviour had no negative impact, it's being mentioned here simply as an observation.

- **Disable Error Correction Mode (ECM) for T.38 fax** – CenturyLink does not support ECM for T.38; however, CenturyLink sets the ECM bit in the facsimile control field describing its capabilities in the T.30 signaling. Thus, for interoperability, ECM should be disabled on Avaya IP Office so the resulting call will negotiate to not use ECM (**Section 6.4**).
- **Extra SIP messages sent during Call Transfers and call forward to the PSTN** – After a call from the PSTN to the enterprise was successfully transferred back out to another PSTN party using the SIP REFER method, CenturyLink accepted the SIP REFER messages sent by IP Office with "202 Accepted", which resulted in successful call completion between the two PSTN parties and the release of the SIP trunk channel resources, as expected. It was observed that during the SIP trunk channel resource release process there were additional SIP messages being exchanged that did not have any negative impact on the call/user, it's being mentioned here simply as an observation.
- **SIP endpoints may indicate that a transfer failed even when it is successful** – Occasionally on a transfer operation, Avaya IP Office SIP endpoints (Avaya 1100 Series Deskphones) may indicate on the local call display that the transfer failed even though it was successful. The frequency of this behavior can be reduced by enabling "**Emulate Notify for REFER**" on the IP Office SIP Line (**Section 5.4.7**).
- **CenturyLink does not support REFER for call forward** – CenturyLink supports REFER for call transfers to the PSTN but does not support REFER for call forward to the PSTN. The call scenario in which CenturyLink 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**), CenturyLink does not return "202 Accepted" message in response to the REFER message sent by IP Office, causing IP Office to send several REFER messages to CenturyLink, the call eventually drops. 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 5.4.7.**).

2.3. Support

For support on CenturyLink systems visit the corporate Web page at:
http://www.centurylink.com/business/voice/sip-trunk.html

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 CenturyLink IQ® SIP Trunking Service on the Broadsoft Platform through the public Internet.

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

- IP Office Server Edition running in VMware environment.
  - Avaya IP Office Voicemail Pro.
- Two Avaya IP Office 500 V2 as expansion systems.
- Avaya 96x1 Series IP Deskphones (H.323).
- Avaya J179 IP Deskphones (H.323).
- Avaya 1100 Series IP Deskphones (SIP).
- Avaya J129 IP Deskphones (SIP).
- Avaya 1400 Series Digital Deskphones.
- Analog Deskphones.
- Avaya 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 systems was connected to the enterprise LAN, the LAN2 port was not used.

IP endpoints at the enterprise include 96x1 Series IP Deskphones (with H.323 firmware), Avaya 1100 and J100 Series IP Deskphones (with SIP firmware), Avaya 1400 Series Digital Deskphones, Analog Deskphones and Avaya 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 CenturyLink, 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 CenturyLink network. The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to CenturyLink 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.

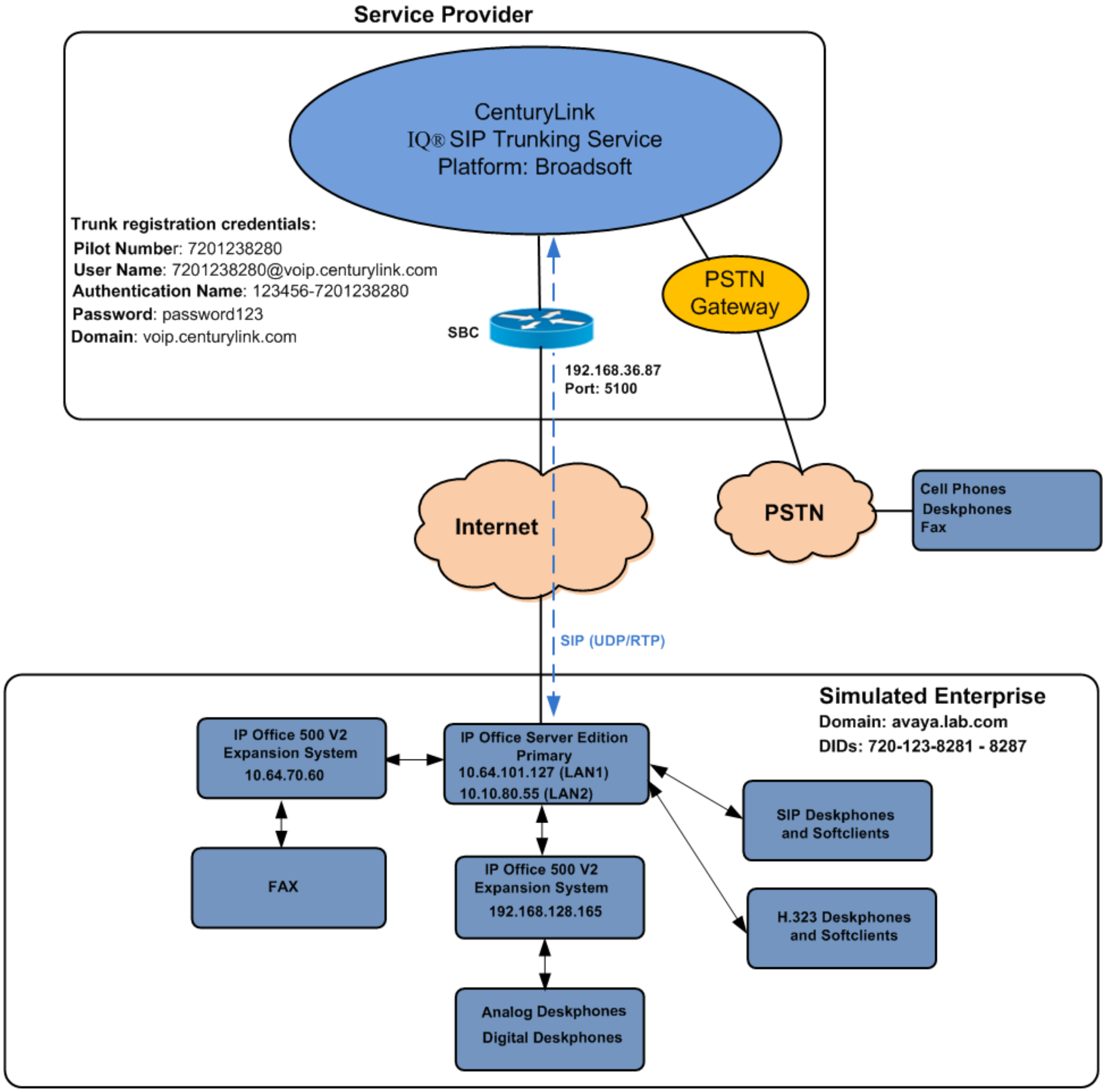


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

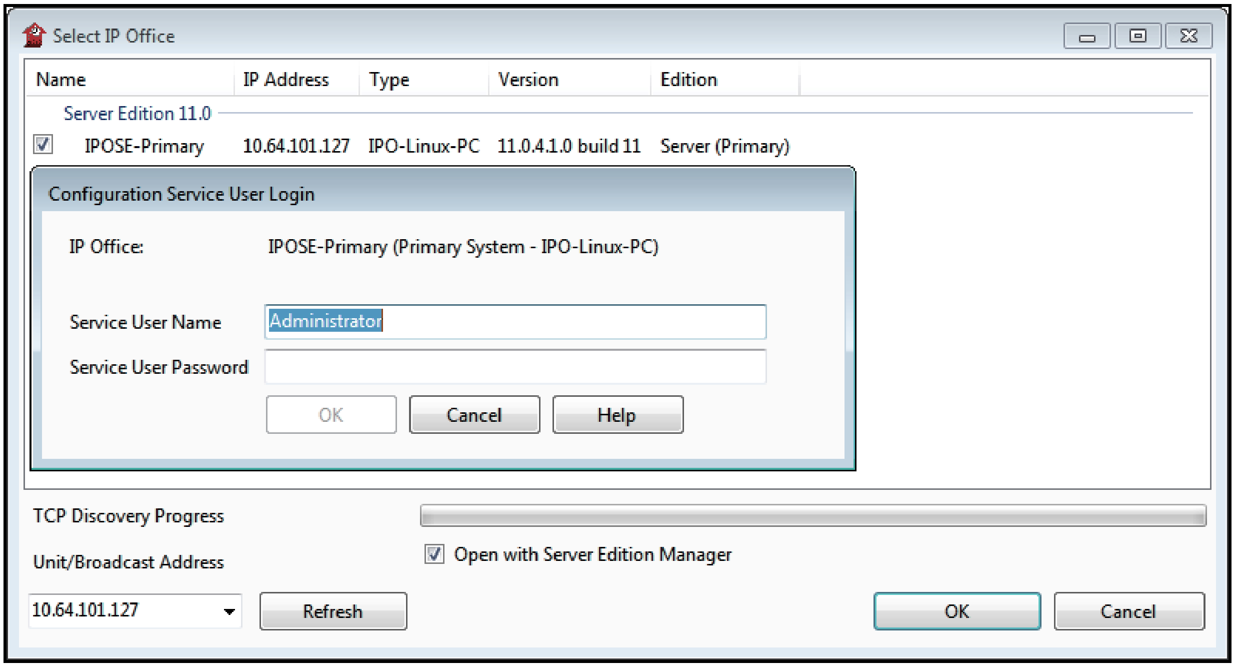
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server) • 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 J179 IP Telephone (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	---
CenturyLink	
BroadSoft BroadWorks	R21.SP1
Metaswitch Perimeta SBC	V4.1.40_SU15_P01.02

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.



Name	IP Address	Type	Version	Edition
Server Edition 11.0				
☑ IPOSE-Primary	10.64.101.127	IPO-Linux-PC	11.0.4.1.0 build 11	Server (Primary)

IP Office: IPOSE-Primary (Primary System - IPO-Linux-PC)

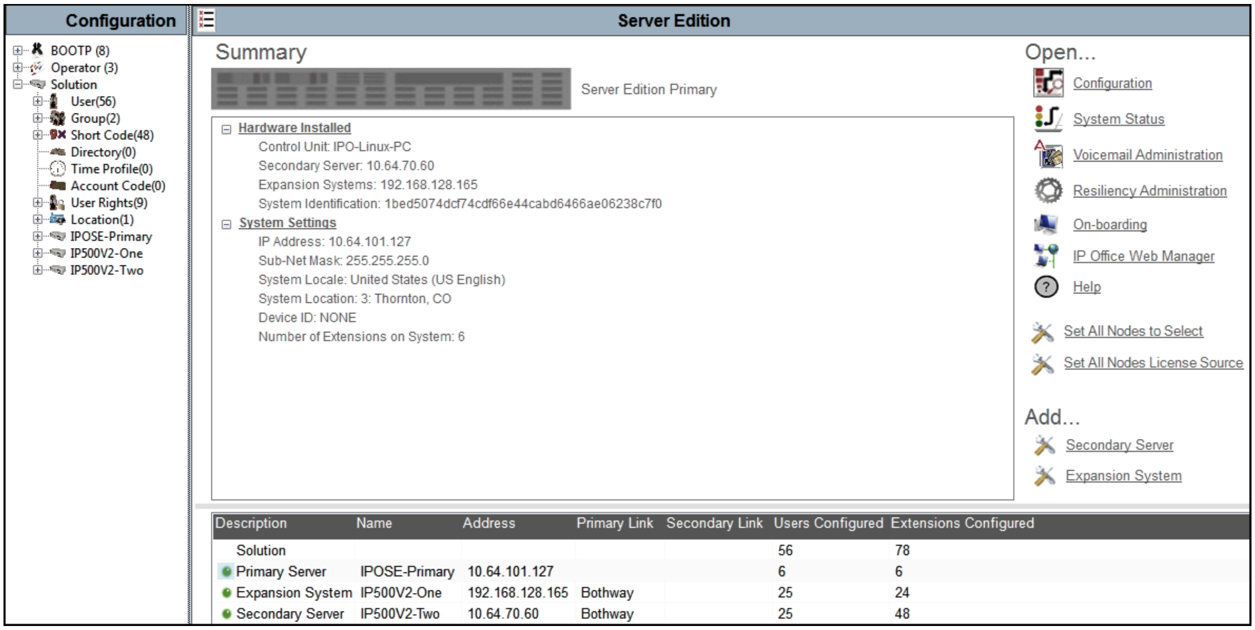
Service User Name: Administrator

Service User Password:

Unit/Broadcast Address: 10.64.101.127

☑ Open with Server Edition Manager

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.



Hardware Installed

Control Unit: IPO-Linux-PC
Secondary Server: 10.64.70.60
Expansion Systems: 192.168.128.165
System Identification: 1bed5074dcf74cdf66e44cabd6466ae06238c7f0

System Settings

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

Description	Name	Address	Primary Link	Secondary Link	Users Configured	Extensions Configured
Solution					56	78
● Primary Server	IPOSE-Primary	10.64.101.127			6	6
● Expansion System	IP500V2-One	192.168.128.165	Bothway		25	24
● Secondary Server	IP500V2-Two	10.64.70.60	Bothway		25	48

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.

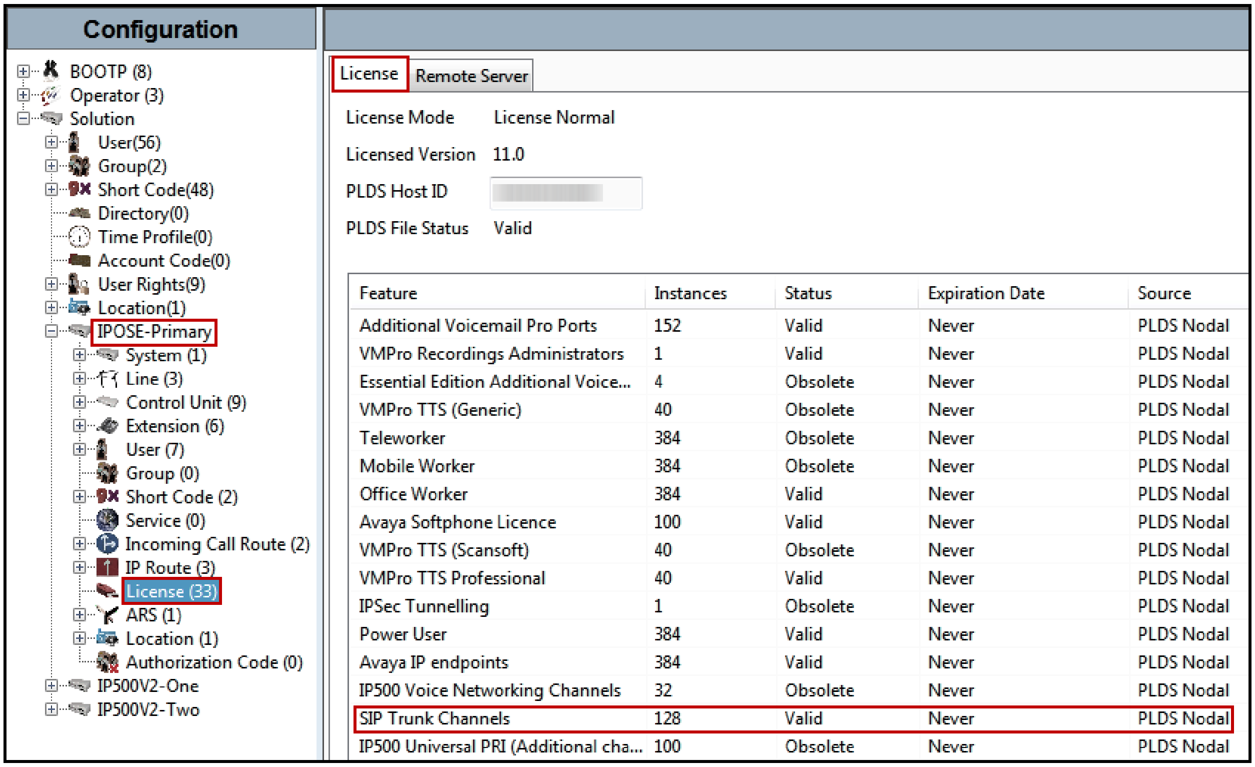
Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

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.



License Mode License Normal

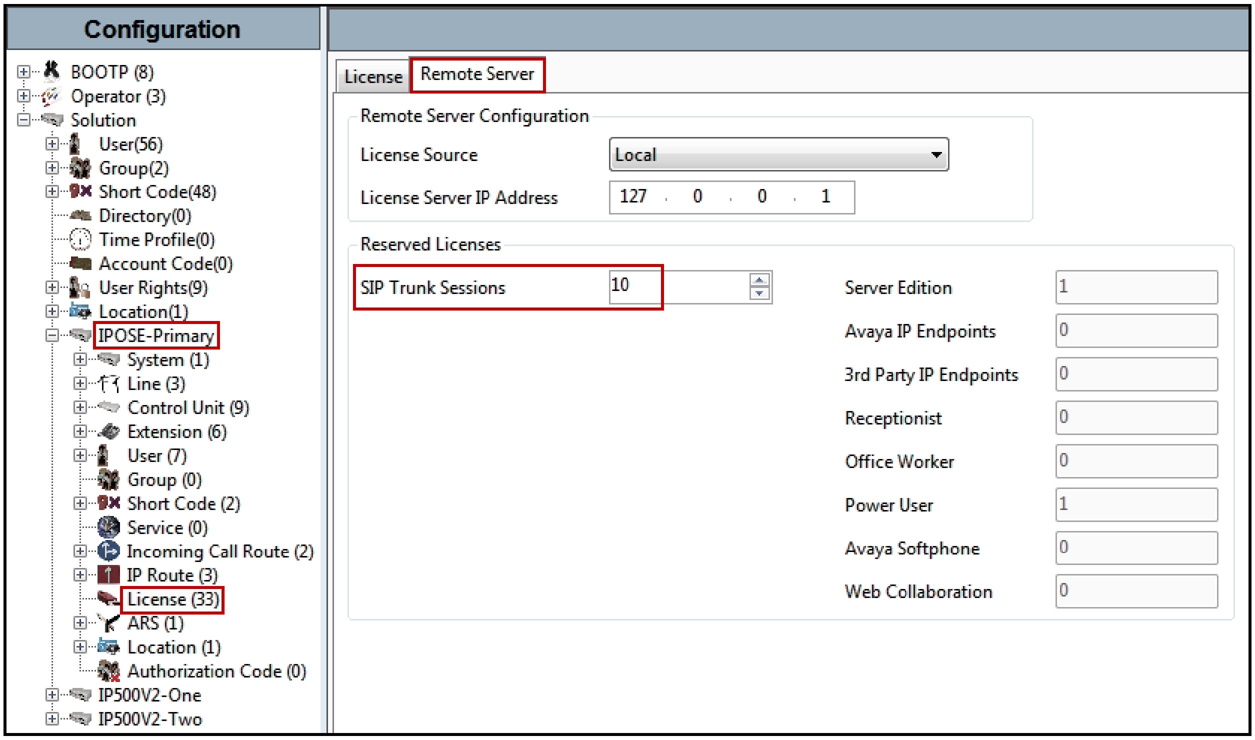
Licensed Version 11.0

PLDS Host ID [redacted]

PLDS File Status Valid

Feature	Instances	Status	Expiration Date	Source
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	1	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	4	Obsolete	Never	PLDS Nodal
VMPro TTS (Generic)	40	Obsolete	Never	PLDS Nodal
Teleworker	384	Obsolete	Never	PLDS Nodal
Mobile Worker	384	Obsolete	Never	PLDS Nodal
Office Worker	384	Valid	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	1	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	128	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal

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



Remote Server Configuration

License Source: Local

License Server IP Address: 127 . 0 . 0 . 1

Reserved Licenses

SIP Trunk Sessions	10
Server Edition	1
Avaya IP Endpoints	0
3rd Party IP Endpoints	0
Receptionist	0
Office Worker	0
Power User	1
Avaya Softphone	0
Web Collaboration	0

5.2. System Settings

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

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 CenturyLink IQ® SIP Trunking Service on the Broadsoft Platform, and therefore is not described in these Application Notes.

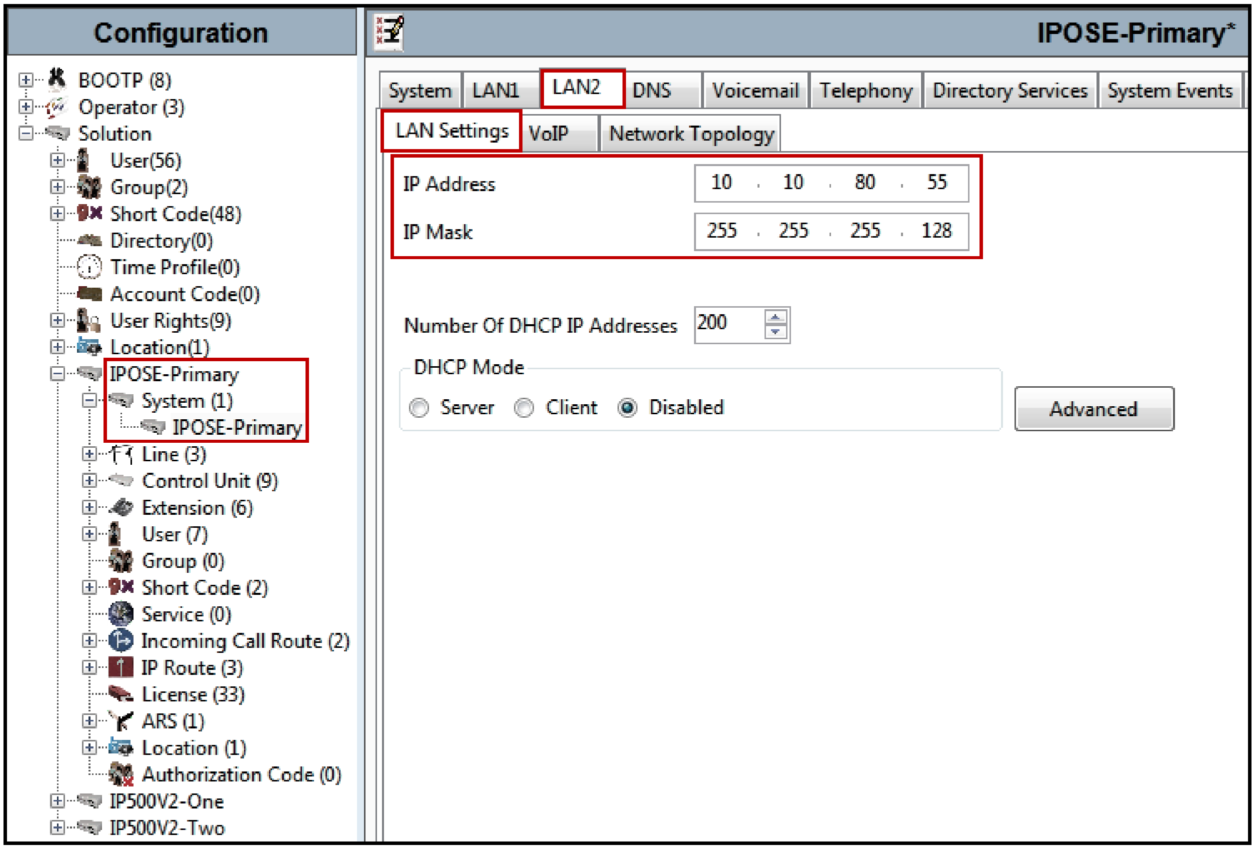
5.2.1. System – LAN2 Tab

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

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.



IP Address: 10 . 10 . 80 . 55

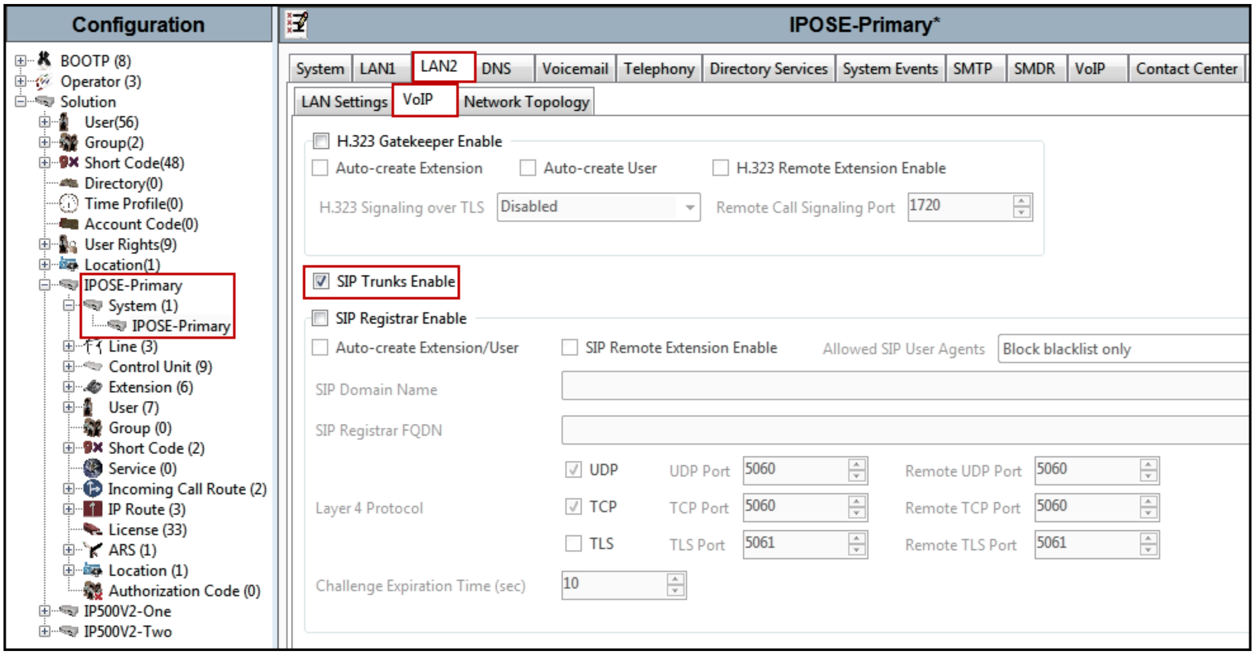
IP Mask: 255 . 255 . 255 . 128

Number Of DHCP IP Addresses: 200

DHCP Mode: ○ Server ○ Client ● Disabled

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.



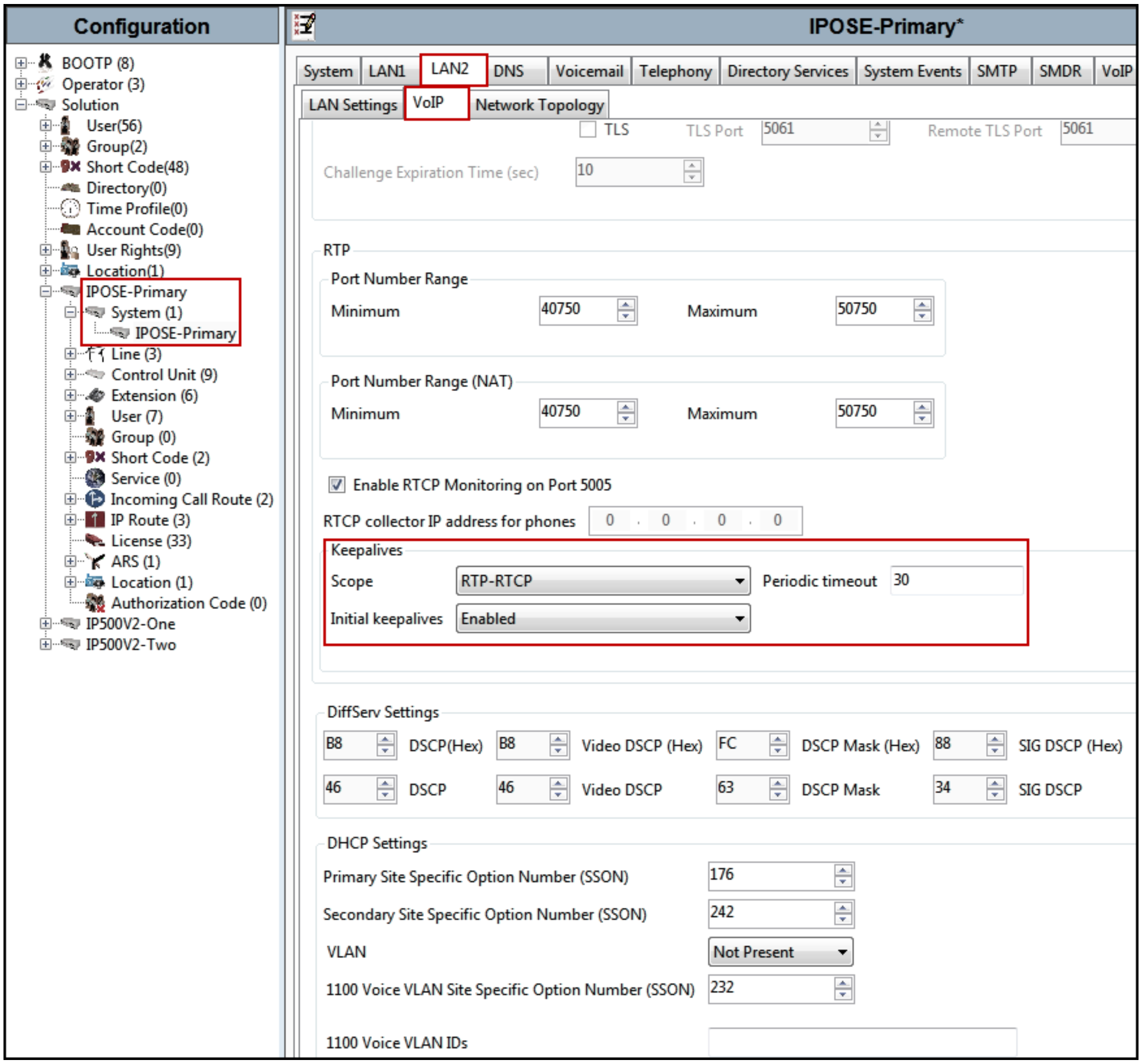
☐ H.323 Gatekeeper Enable
☐ Auto-create Extension
☐ Auto-create User
☐ H.323 Remote Extension Enable
H.323 Signaling over TLS: Disabled
Remote Call Signaling Port: 1720

☑ SIP Trunks Enable

☐ SIP Registrar Enable
☐ Auto-create Extension/User
☐ SIP Remote Extension Enable
Allowed SIP User Agents: Block blacklist only
SIP Domain Name:
SIP Registrar FQDN:
Layer 4 Protocol:
☑ UDP UDP Port: 5060 Remote UDP Port: 5060
☑ TCP TCP Port: 5060 Remote TCP Port: 5060
☐ TLS TLS Port: 5061 Remote TLS Port: 5061
Challenge Expiration Time (sec): 10

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).



☐ TLS

TLS Port: 5061

Remote TLS Port: 5061

Challenge Expiration Time (sec): 10

RTP

Port Number Range

Minimum: 40750

Maximum: 50750

Port Number Range (NAT)

Minimum: 40750

Maximum: 50750

☑ Enable RTCP Monitoring on Port 5005

RTCP collector IP address for phones: 0 . 0 . 0 . 0

Keepalives

Scope: RTP-RTCP

Periodic timeout: 30

Initial keepalives: Enabled

DiffServ Settings

B8	DSCP(Hex)	B8	Video DSCP (Hex)	FC	DSCP Mask (Hex)	88	SIG DSCP (Hex)
46	DSCP	46	Video DSCP	63	DSCP Mask	34	SIG DSCP

DHCP Settings

Primary Site Specific Option Number (SSON): 176

Secondary Site Specific Option Number (SSON): 242

VLAN: Not Present

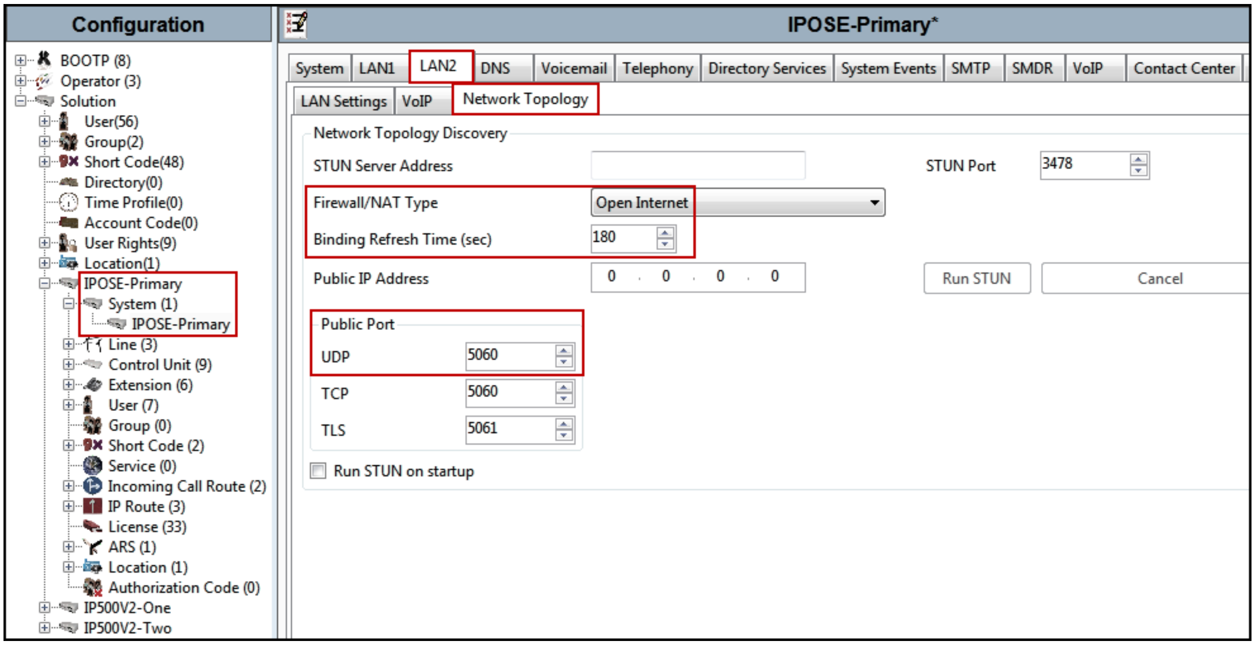
1100 Voice VLAN Site Specific Option Number (SSON): 232

1100 Voice VLAN IDs

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**.
- Default values were used for all other parameters.
- Click the **OK** button (not shown).



Network Topology Discovery

STUN Server Address

STUN Port 3478

Firewall/NAT Type Open Internet

Binding Refresh Time (sec) 180

Public IP Address 0 . 0 . 0 . 0

Public Port

UDP 5060

TCP 5060

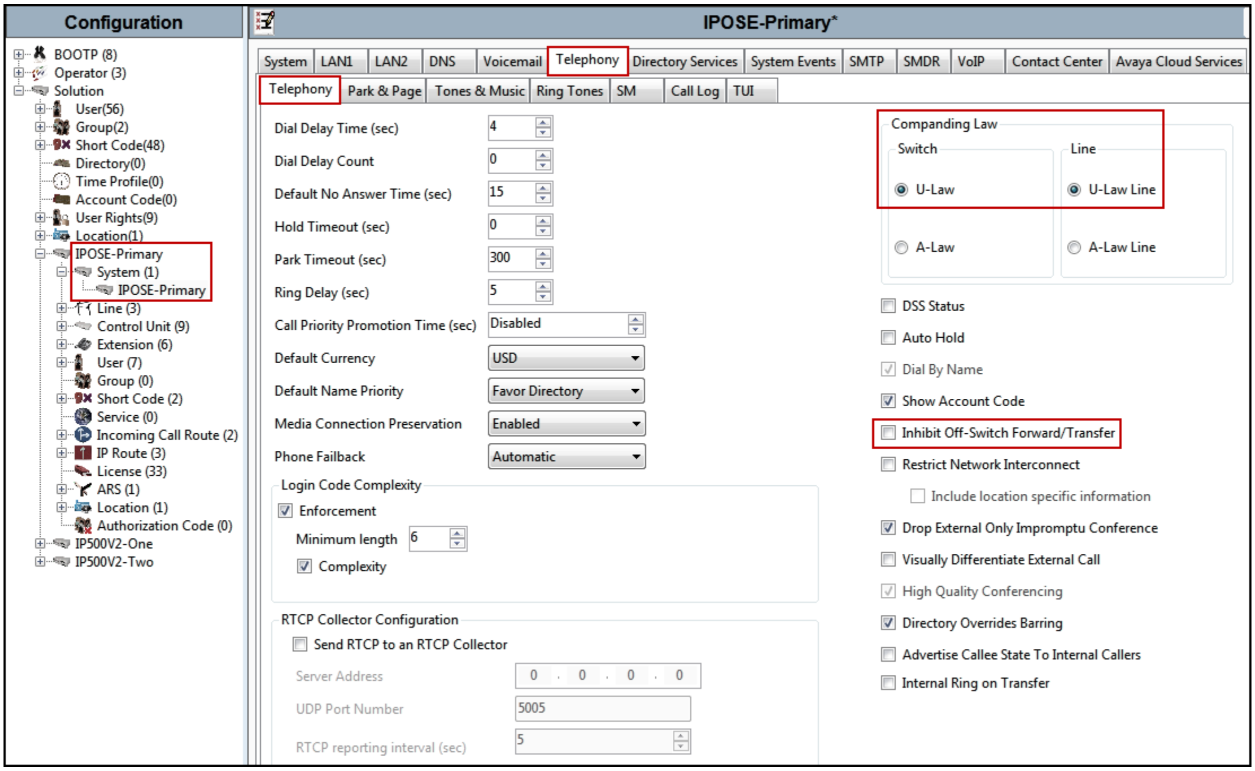
TLS 5061

☐ Run STUN on startup

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).



Dial Delay Time (sec): 4
Dial Delay Count: 0
Default No Answer Time (sec): 15
Hold Timeout (sec): 0
Park Timeout (sec): 300
Ring Delay (sec): 5
Call Priority Promotion Time (sec): Disabled
Default Currency: USD
Default Name Priority: Favor Directory
Media Connection Preservation: Enabled
Phone Failback: Automatic

Login Code Complexity
☑ Enforcement
Minimum length: 6
☑ Complexity

RTCP Collector Configuration
☐ Send RTCP to an RTCP Collector
Server Address: 0 . 0 . 0 . 0
UDP Port Number: 5005
RTCP reporting interval (sec): 5

Companding Law
Switch: ● U-Law ○ A-Law
Line: ● U-Law Line ○ A-Law Line

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

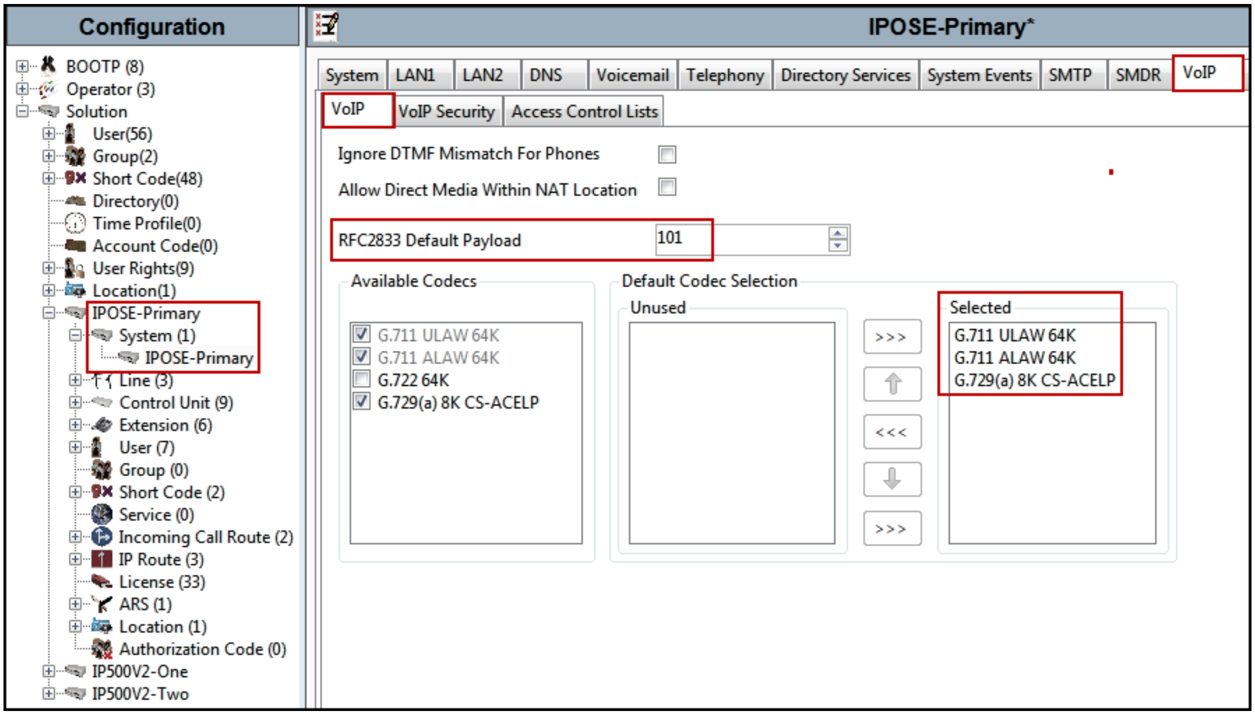
5.2.3. VoIP Tab

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).



Ignore DTMF Mismatch For Phones ☐

Allow Direct Media Within NAT Location ☐

RFC2833 Default Payload: 101

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

Default Codec Selection

Unused

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

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

5.2.3.2 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.

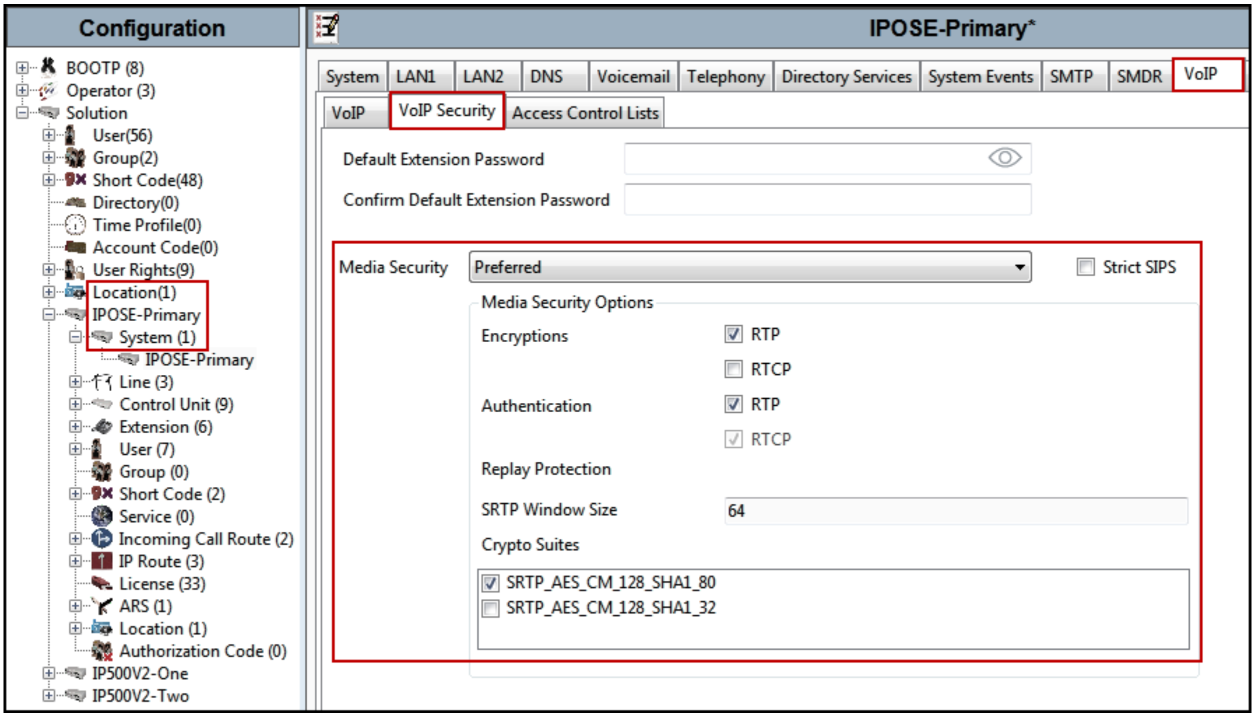
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

- 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).



Default Extension Password

Confirm Default Extension Password

Media Security: Preferred

☐ Strict SIPS

Media Security Options

Encryptions: ☑ RTP ☐ RTCP

Authentication: ☑ RTP ☑ RTCP

Replay Protection

SRTP Window Size: 64

Crypto Suites

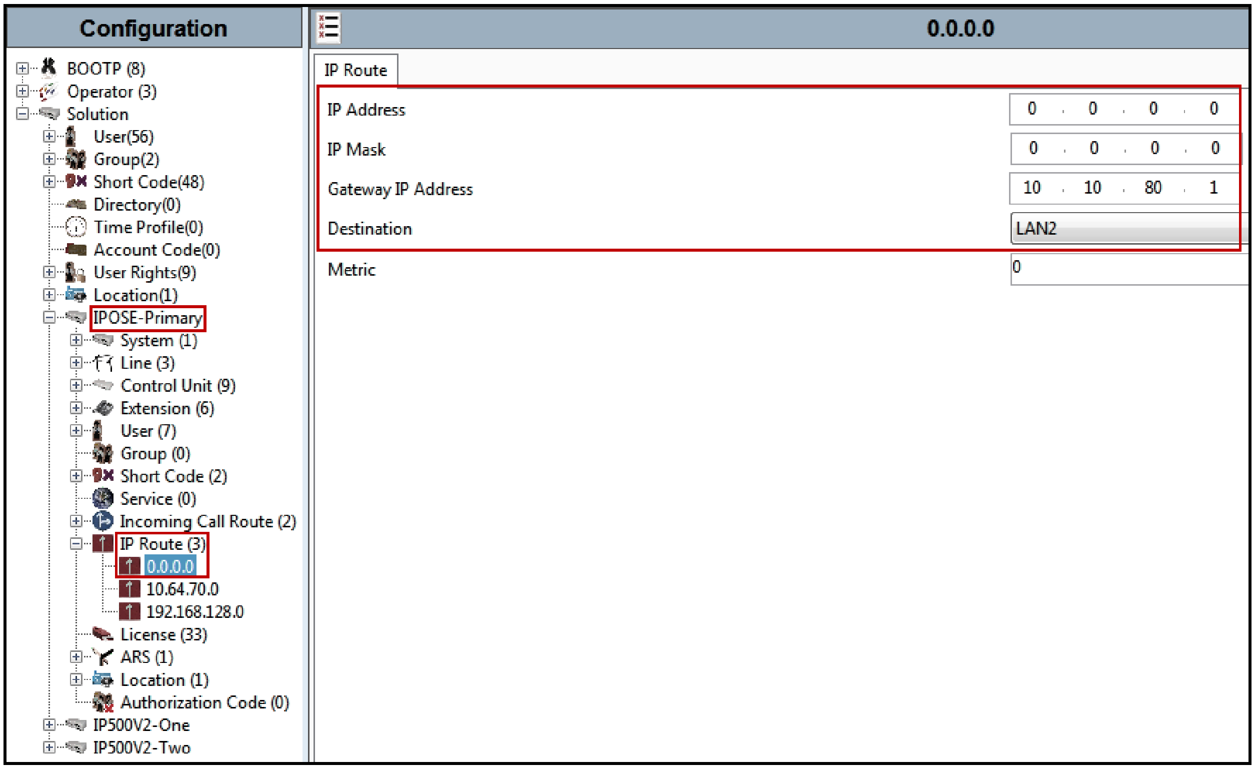
☑ SRTP_AES_CM_128_SHA1_80
☐ SRTP_AES_CM_128_SHA1_32

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 CenturyLink 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).



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

5.4. SIP Line

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

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

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

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

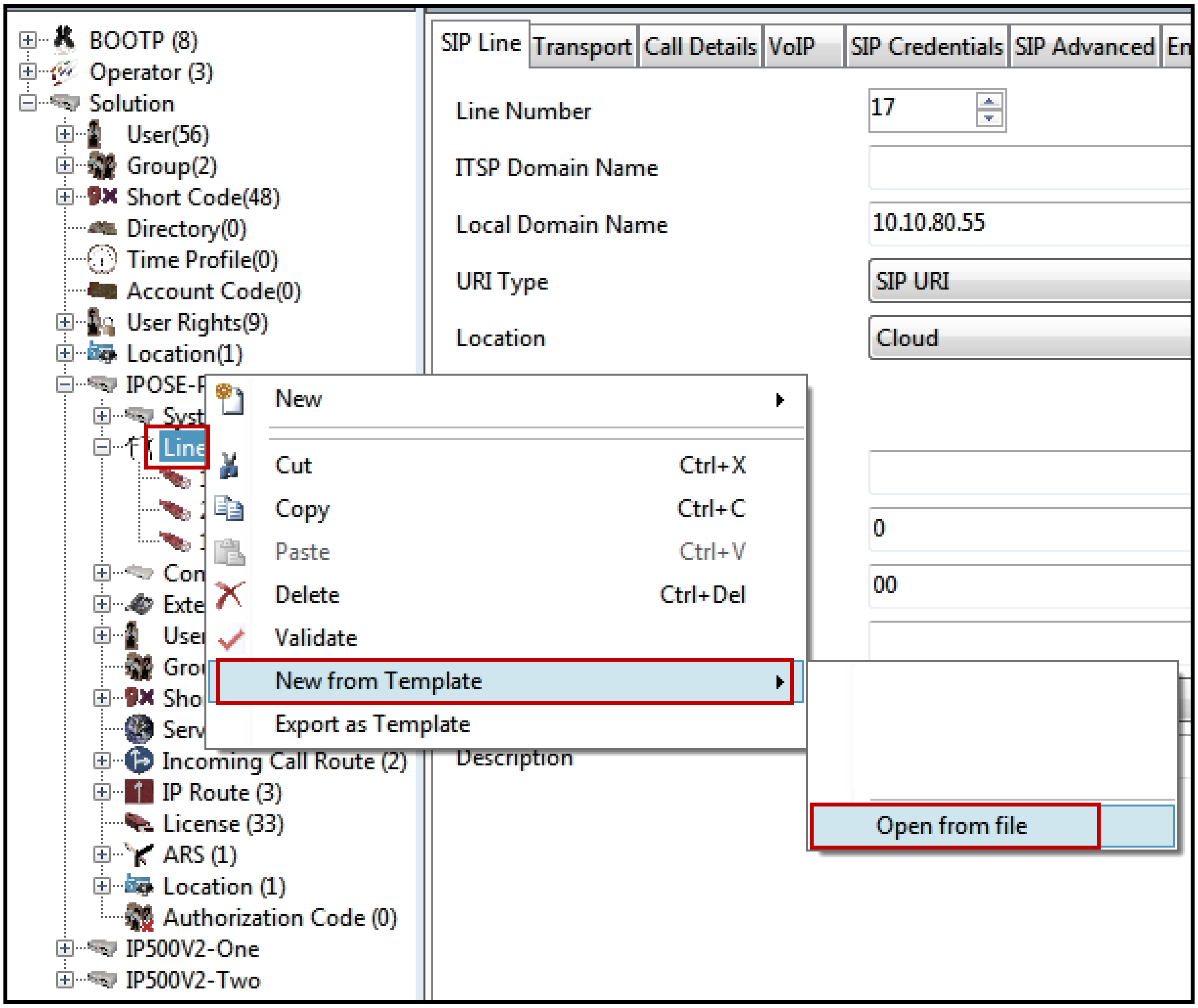
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.7**.

5.4.1. Creating a SIP Trunk from an XML Template

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

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

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



Line Number 17

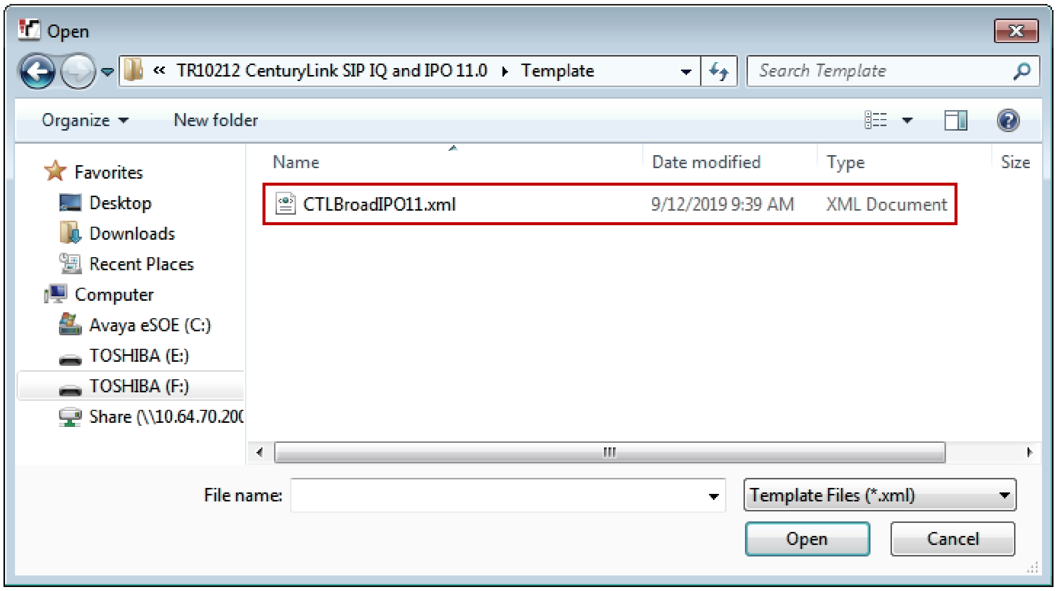
ITSP Domain Name

Local Domain Name 10.10.80.55

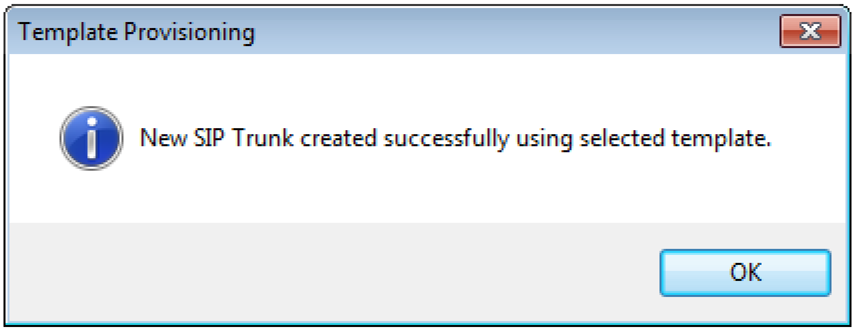
URI Type SIP URI

Location Cloud

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

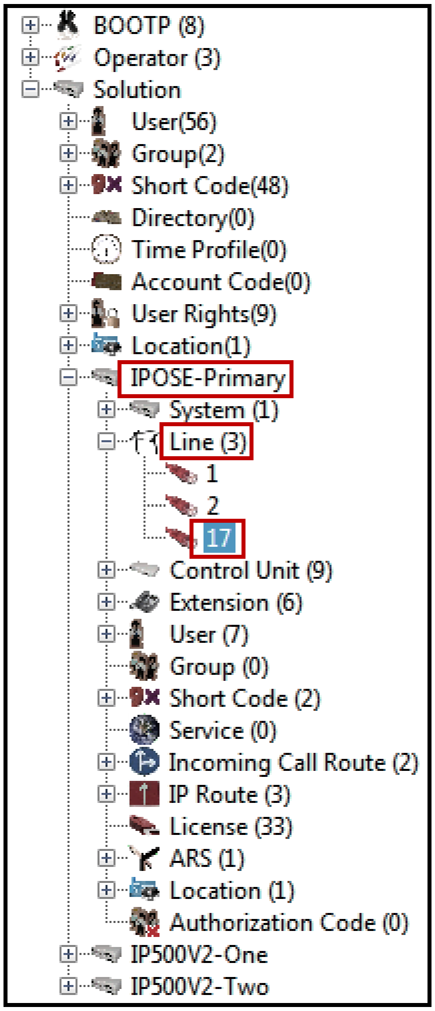


After the import is complete, a final import status pop-up window will open stating success or failure. Click **OK**.



New SIP Trunk created successfully using selected template.

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

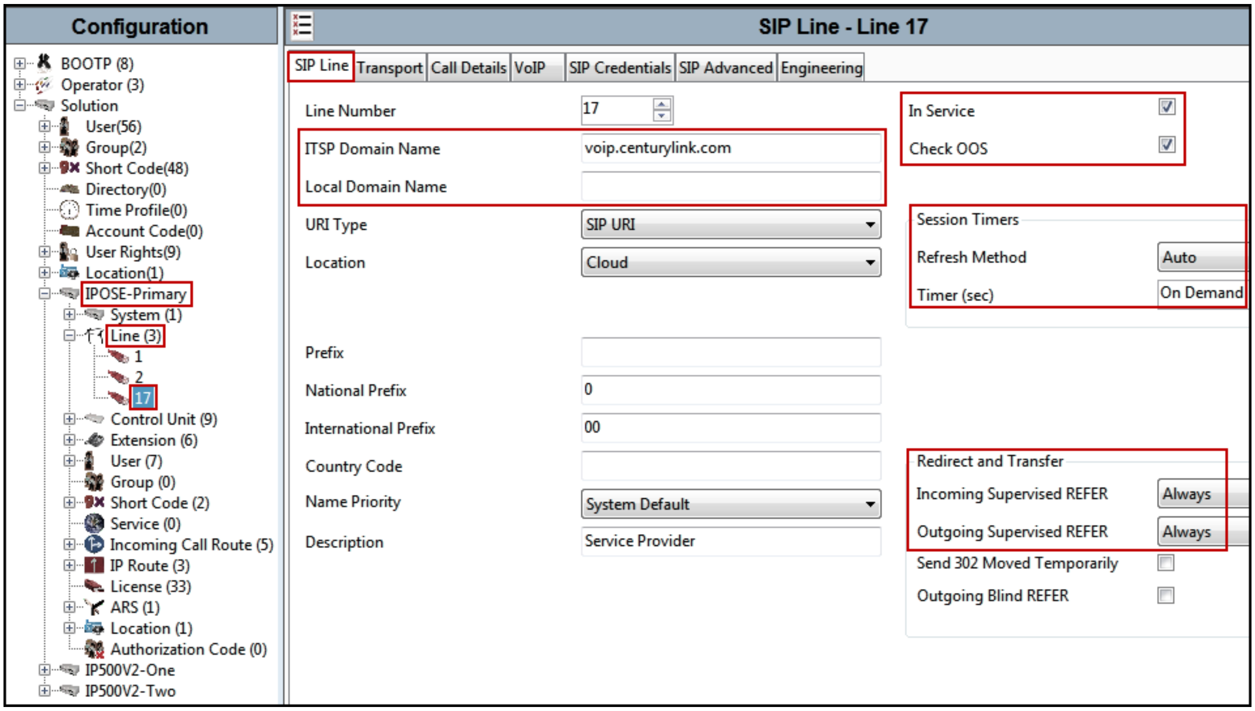


It is important that the SIP Line configuration be reviewed and updated if necessary, after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2** to **5.4.7**.

5.4.2. SIP Line – SIP Line Tab

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

- Under the **ITSP Domain Name** enter the domain name provided by CenturyLink, **voip.CenturyLink.com** was used during the compliance test.
- Leave the **Local Domain Name** blank.
- 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 **Always**. CenturyLink supports the SIP REFER method for call transfers to the PSTN.
- Click **OK** to commit (not shown).



Line Number: 17
ITSP Domain Name: voip.centurylink.com
Local Domain Name:
URI Type: SIP URI
Location: Cloud
Prefix:
National Prefix: 0
International Prefix: 00
Country Code:
Name Priority: System Default
Description: Service Provider

In Service ☑
Check OOS ☑

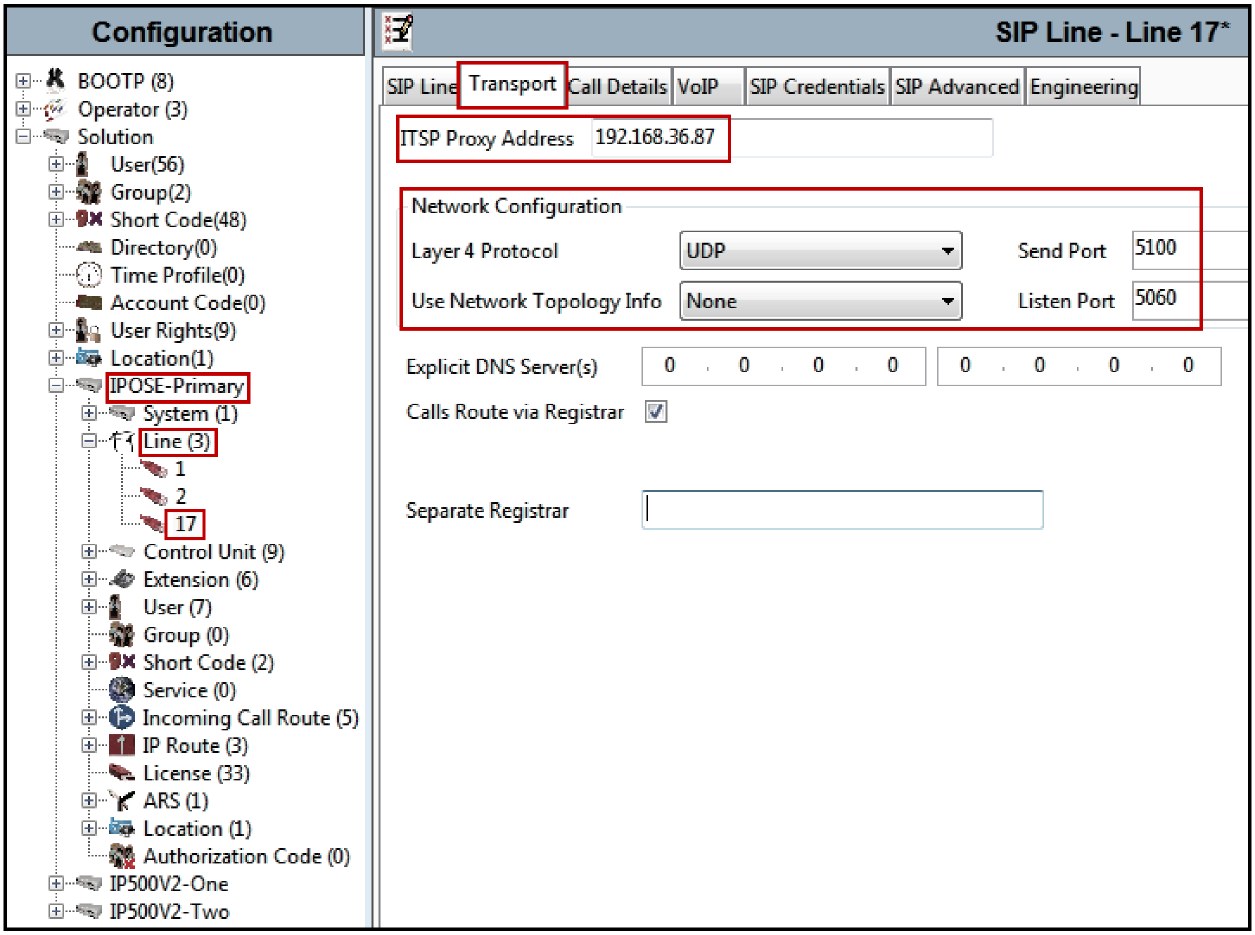
Session Timers
Refresh Method: Auto
Timer (sec): On Demand

Redirect and Transfer
Incoming Supervised REFER: Always
Outgoing Supervised REFER: Always
Send 302 Moved Temporarily ☐
Outgoing Blind REFER ☐

5.4.3. SIP Line - Transport Tab

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

- Set the **ITSP Proxy Address** to the SIP Proxy IP address provided by CenturyLink, **192.168.36.87** 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 **5100** (this information was provided by CenturyLink, this is the port number that CenturyLink will listen for traffic, instead of 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).



ITSP Proxy Address: 192.168.36.87

Layer 4 Protocol: UDP

Send Port: 5100

Use Network Topology Info: None

Listen Port: 5060

Explicit DNS Server(s): 0 . 0 . 0 . 0 | 0 . 0 . 0 . 0

Calls Route via Registrar: ☑

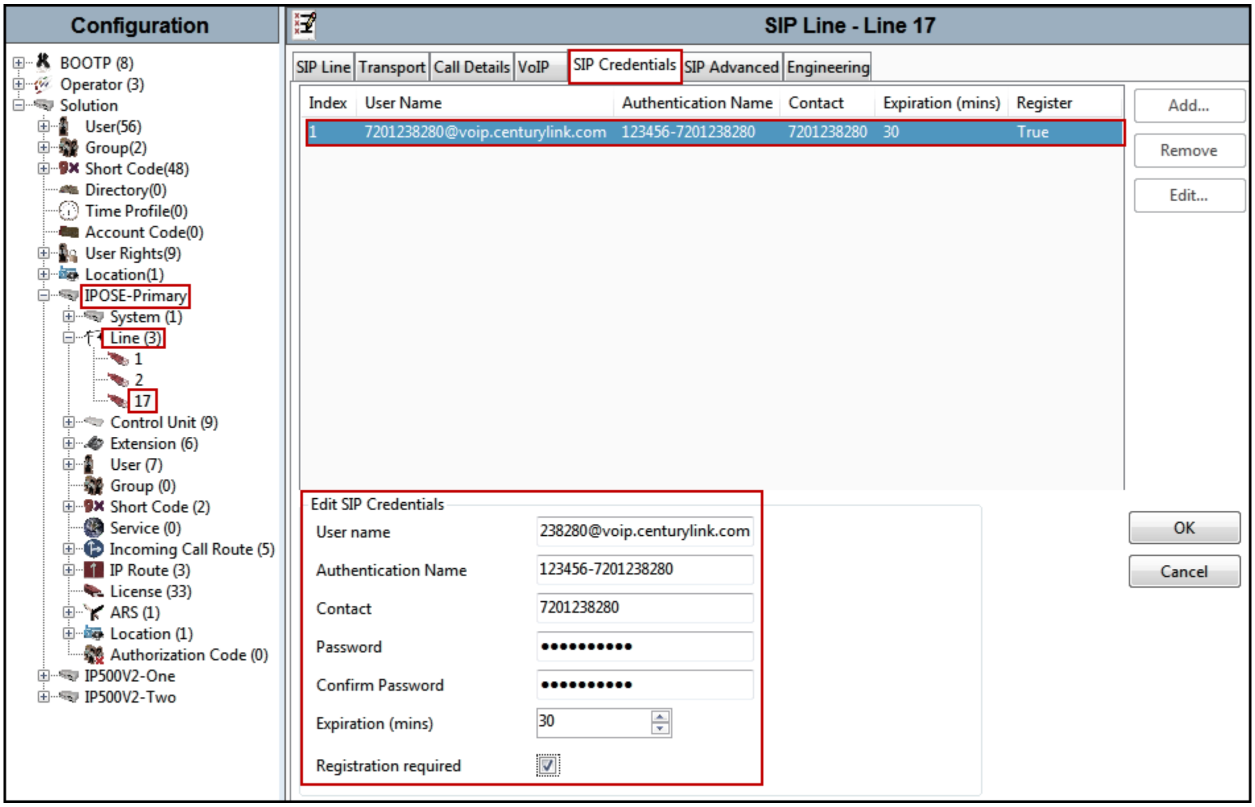
Separate Registrar:

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

5.4.4. SIP Line – SIP Credentials Tab

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

- For **User name**, enter the user name credential provided by CenturyLink for SIP Trunk registration. For the compliance test **7201238280@voip.centurylink.com**, which included the pilot number associated with the SIP trunk and the domain name, were used.
- For **Authentication Name**, enter the authentication name credential provided by CenturyLink for SIP Trunk registration. For the compliance test **123456-7201238280**, which represents the "**Group SIP ID**" provided by CenturyLink, was used.
- For **Contact** enter the pilot number provided by CenturyLink. For the compliance test **7201238280** was used.
- For **Password** and **Confirm Password**, enter the password credential provided by CenturyLink for SIP Trunk registration.
- Set **Expiry (mins)** to a value acceptable to the enterprise. This setting defines how often registration with CenturyLink is required following any previous registration. For the compliance test 30 minutes was used. This value should be chosen in consultation with the service provider.
- Verify that **Registration required** is checked.
- Click the **OK** to commit (not shown).



Index	User Name	Authentication Name	Contact	Expiration (mins)	Register
1	7201238280@voip.centurylink.com	123456-7201238280	7201238280	30	True

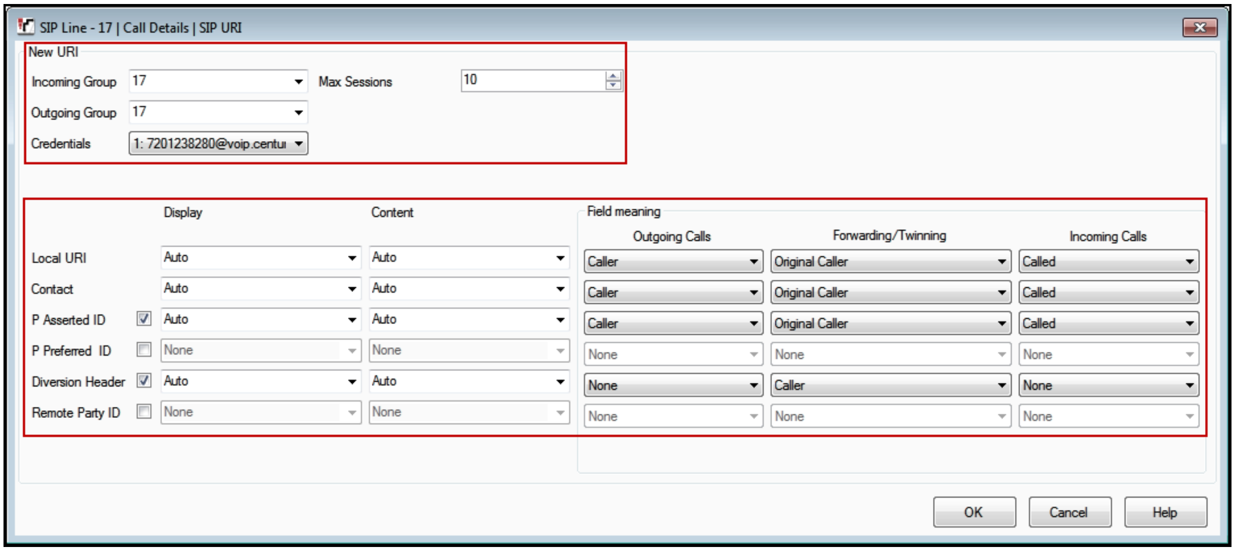
Edit SIP Credentials

User name	238280@voip.centurylink.com
Authentication Name	123456-7201238280
Contact	7201238280
Password	••••••••••
Confirm Password	••••••••••
Expiration (mins)	30
Registration required	☑

5.4.5. SIP Line – Call Details Tab

Select the **Call Details** tab, and then click the **Add…** button (not shown) and the screen shown below will appear. To edit an existing entry, click an entry in the list at the top, and click the **Edit…** button. In the example screen below a new entry was added. 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 **1: 7201238280@voip.centurylink.com** (SIP Trunk registration credentials defined under **Section 5.4.4**).
- 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, these settings are default values.
- Click **OK**.
- Click **OK** to commit again (not shown).



Incoming Group: 17
Max Sessions: 10
Outgoing Group: 17
Credentials: 1: 7201238280@voip.centu

		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	☑	Auto	Auto	Caller	Original Caller	Called
P Preferred ID	☐	None	None	None	None	None
Diversion Header	☑	Auto	Auto	None	Caller	None
Remote Party ID	☐	None	None	None	None	None

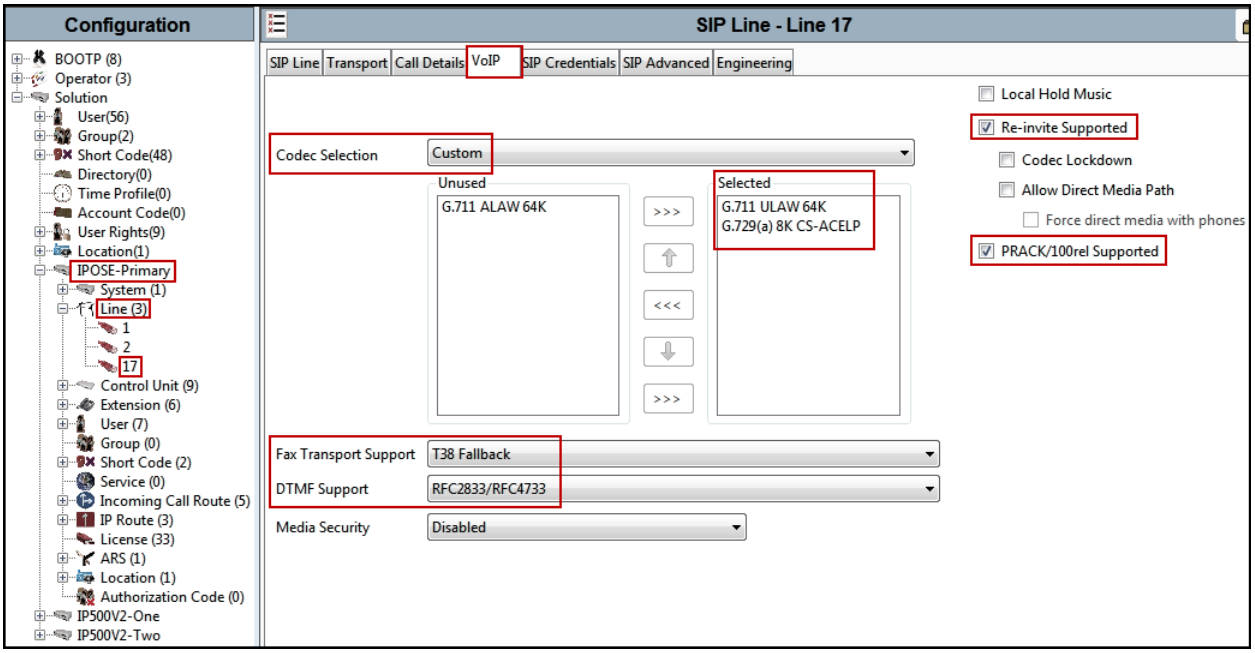
5.4.6. SIP Line - VoIP Tab

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

- The **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line, as shown. CenturyLink supports codecs **G.711ULAW** and **G729(a)** for audio.

> **Note**: Set the codec selection to **G.711ULAW only** if T.38 fax is required. refer to **Section 2.2**).

- Select **T.38 Fallback** 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).



Codec Selection: Custom

Unused: G.711 ALAW 64K

Selected:
G.711 ULAW 64K
G.729(a) 8K CS-ACELP

Fax Transport Support: T38 Fallback

DTMF Support: RFC2833/RFC4733

Media Security: Disabled

☐ Local Hold Music
☑ Re-invite Supported
☐ Codec Lockdown
☐ Allow Direct Media Path
☐ Force direct media with phones
☑ PRACK/100rel Supported

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

5.4.7. SIP Line – SIP Advanced Tab

In the **Addressing** area:

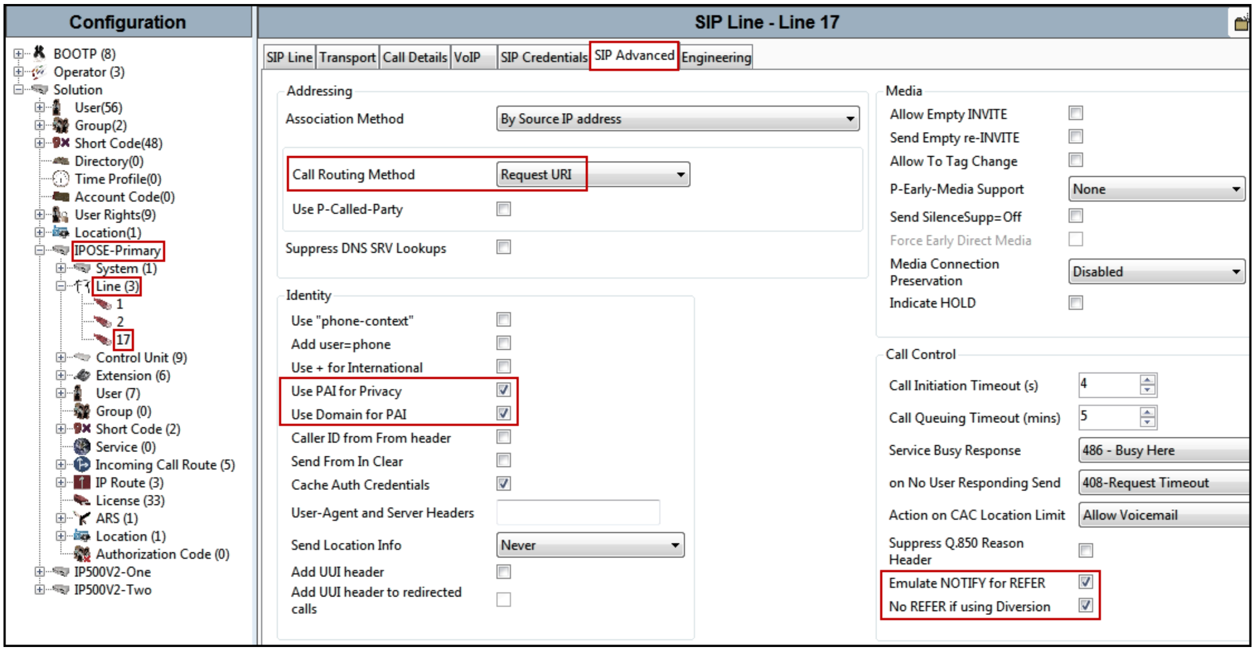
- Select **Request URI** for **Call Routing Method**.

In the **Identity** area:

- Check the box for **Use PAI for Privacy**.
- Check the box for **Use Domain for PAI** (refer to **Section 2.2)**.

In the **Call Control** area:

- Check the box **Emulate NOTIFY for REFER** (refer to **Section 2.2)**.
- Check the box **No REFER if using Diversion** (refer to **Section 2.2)**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



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

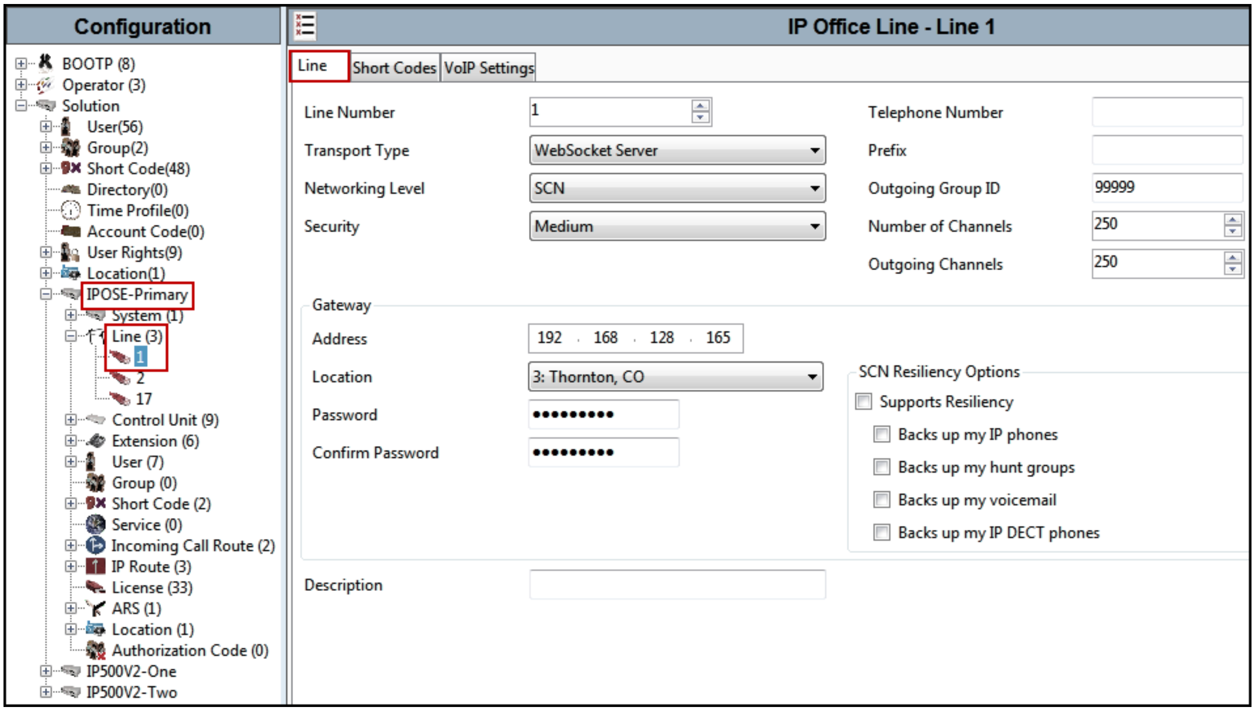
Identity
Use "phone-context" ☐
Add user=phone ☐
Use + for International ☐
Use PAI for Privacy ☑
Use Domain for PAI ☑
Caller ID from From header ☐
Send From In Clear ☐
Cache Auth Credentials ☑
User-Agent and Server Headers:
Send Location Info: Never
Add UUI header ☐
Add UUI header to redirected calls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

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

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

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.



Line Number: 1
Transport Type: WebSocket Server
Networking Level: SCN
Security: Medium
Telephone Number:
Prefix:
Outgoing Group ID: 99999
Number of Channels: 250
Outgoing Channels: 250

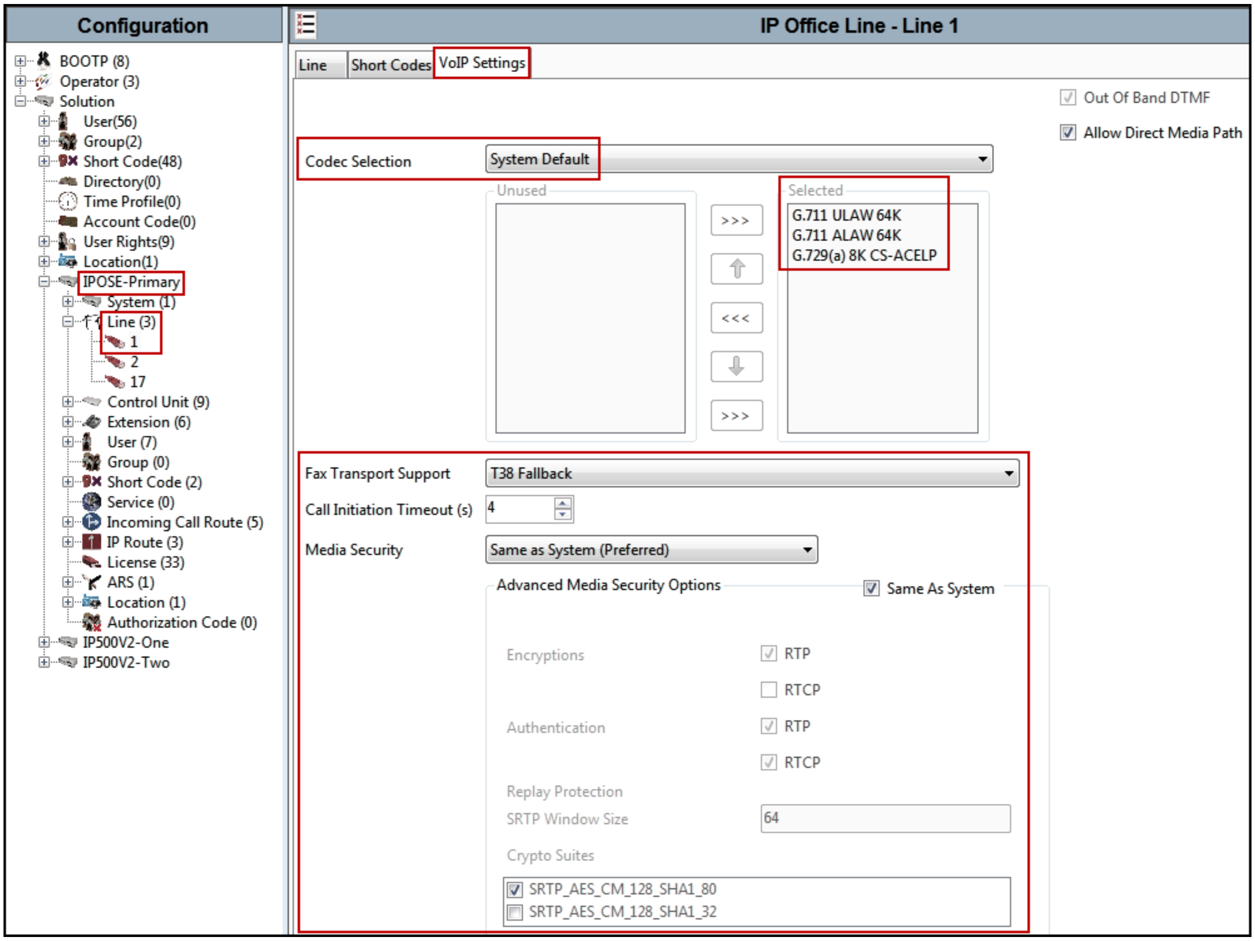
Gateway
Address: 192 . 168 . 128 . 165
Location: 3: Thornton, CO
Password: •••••••••
Confirm Password: •••••••••

SCN Resiliency Options
☐ Supports Resiliency
☐ Backs up my IP phones
☐ Backs up my hunt groups
☐ Backs up my voicemail
☐ Backs up my IP DECT phones

Description:

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

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



☑ Out Of Band DTMF

☑ Allow Direct Media Path

Codec Selection: System Default

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

Fax Transport Support: T38 Fallback

Call Initiation Timeout (s): 4

Media Security: Same as System (Preferred)

Advanced Media Security Options ☑ Same As System

Encryptions ☑ RTP ☐ RTCP

Authentication ☑ RTP ☑ RTCP

Replay Protection

SRTP Window Size: 64

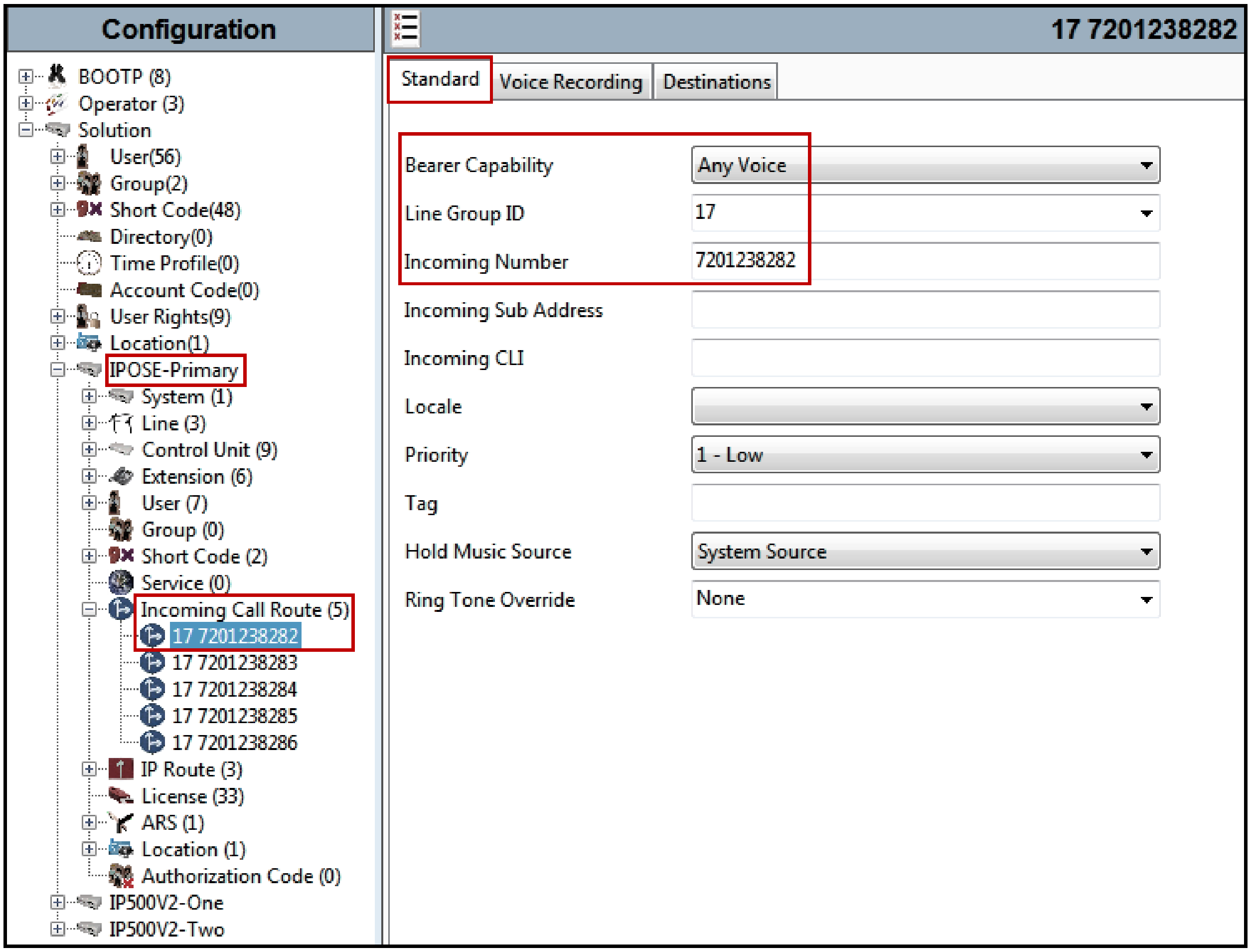
Crypto Suites
☑ SRTP_AES_CM_128_SHA1_80
☐ SRTP_AES_CM_128_SHA1_32

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

5.6. Incoming Call Route

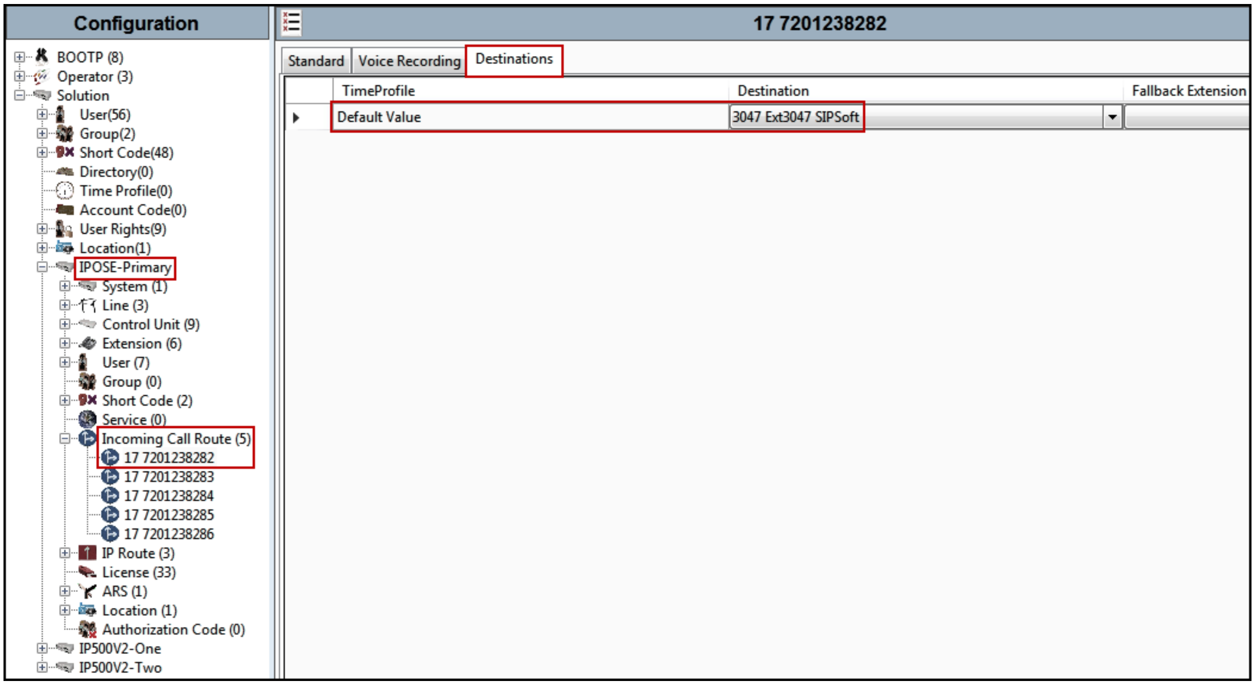
Incoming call routes map inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system. To add an incoming call route, right click on **Incoming Call Route** in the the **Navigation** pane and select **New** (not shown). On the Details Pane,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

- Set **Bearer Capacity** to **Any Voice**.
- The **Line Group ID** is set to **17**. This matches the **Incoming Group** field configured in the **Call Details** tab for the SIP Line on **Section 5.4.5**.
- On the **Incoming Number**, enter one of the DID numbers provided by CenturyLink. 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.



Bearer Capability: Any Voice
Line Group ID: 17
Incoming Number: 7201238282
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 **7201238282** provided by CenturyLink was associated with the Avaya IP Office extension **3047**.



TimeProfile	Destination	Fallback Extension
Default Value	3047 Ext3047 SIPSoft	

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.).

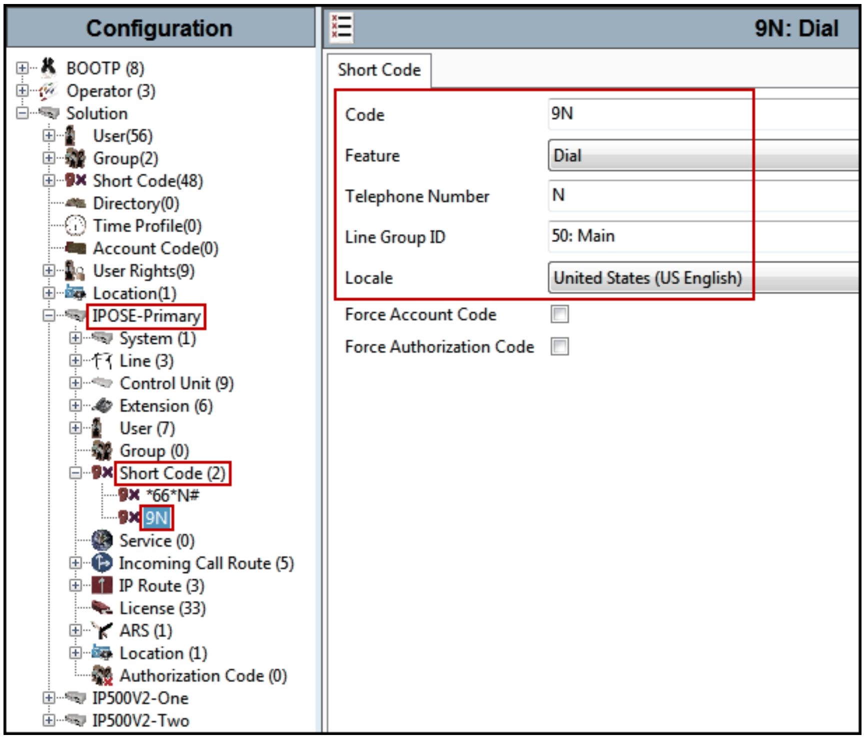
5.7. Outbound Call Routing

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).



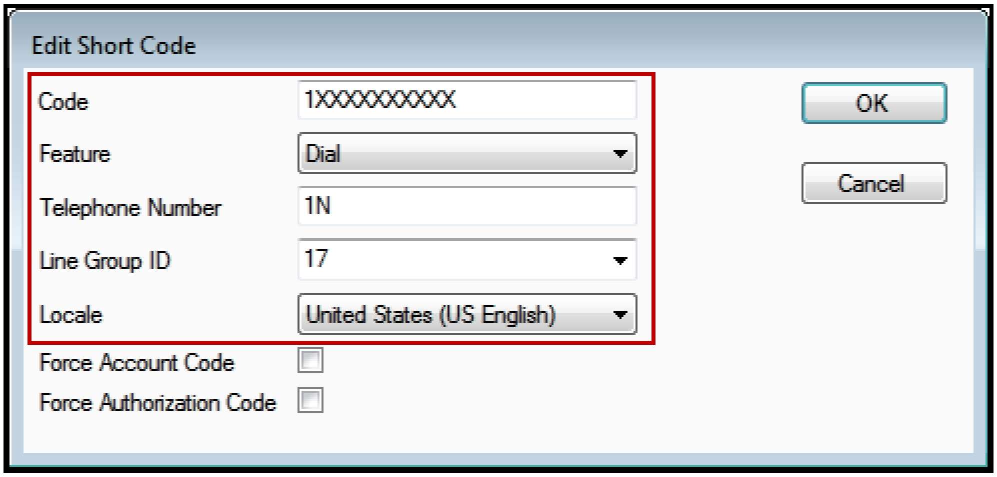
Code: 9N
Feature: Dial
Telephone Number: N
Line Group ID: 50: Main
Locale: United States (US English)
Force Account Code ☐
Force Authorization Code ☐

The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **X**s 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 17** 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: 17
Locale: United States (US English)
Force Account Code ☐
Force Authorization Code ☐

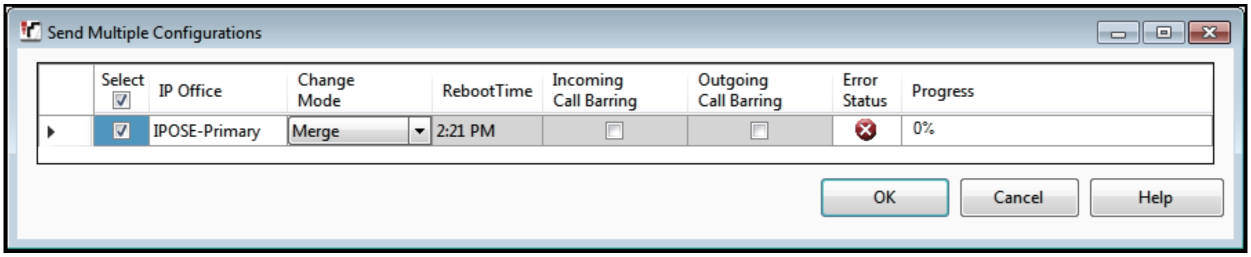
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

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

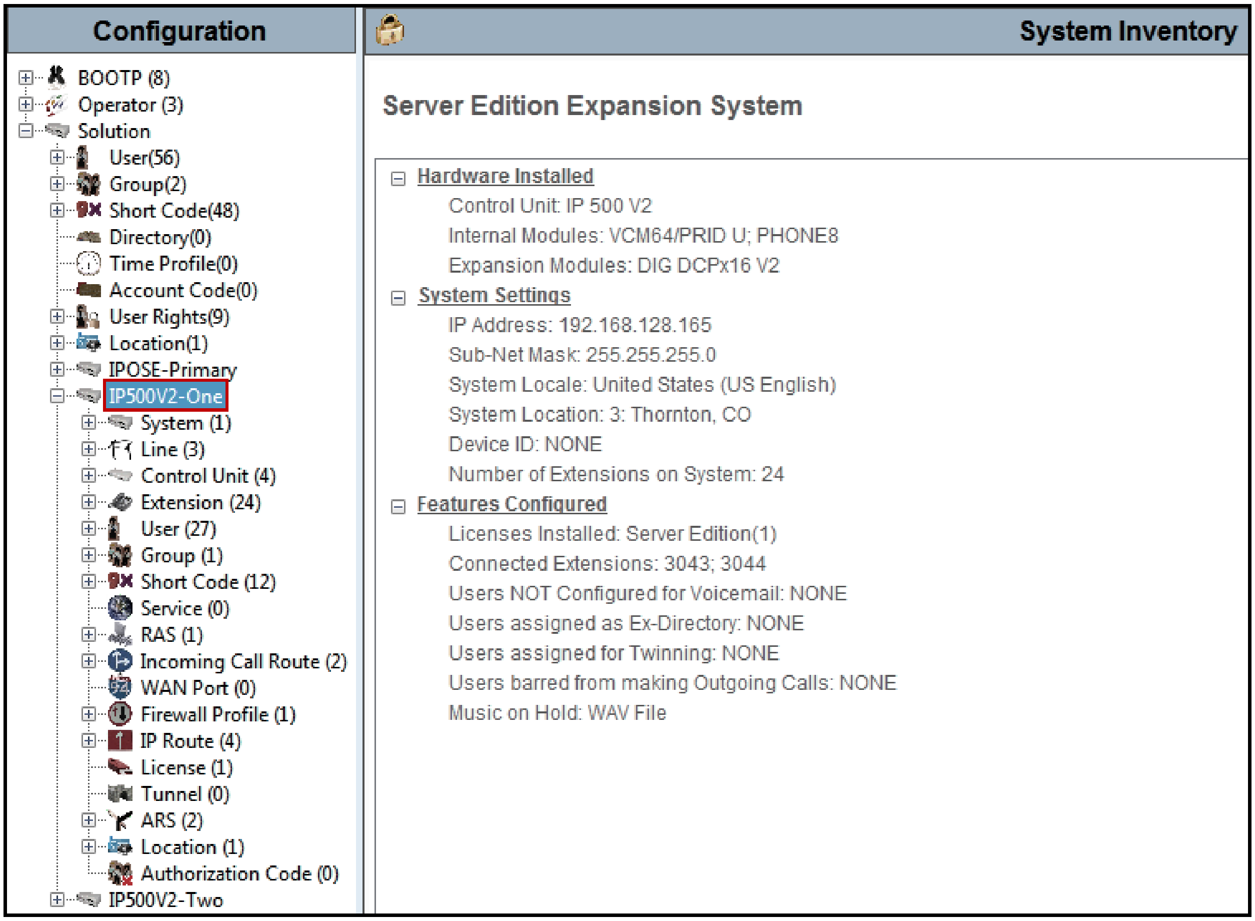
Click **OK** to execute the save.



	Select ☑	IP Office	Change Mode	RebootTime	Incoming Call Barring	Outgoing Call Barring	Error Status	Progress
▸	☑	IPOSE-Primary	Merge	2:21 PM	☐	☐	☒	0%

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.



Server Edition Expansion System

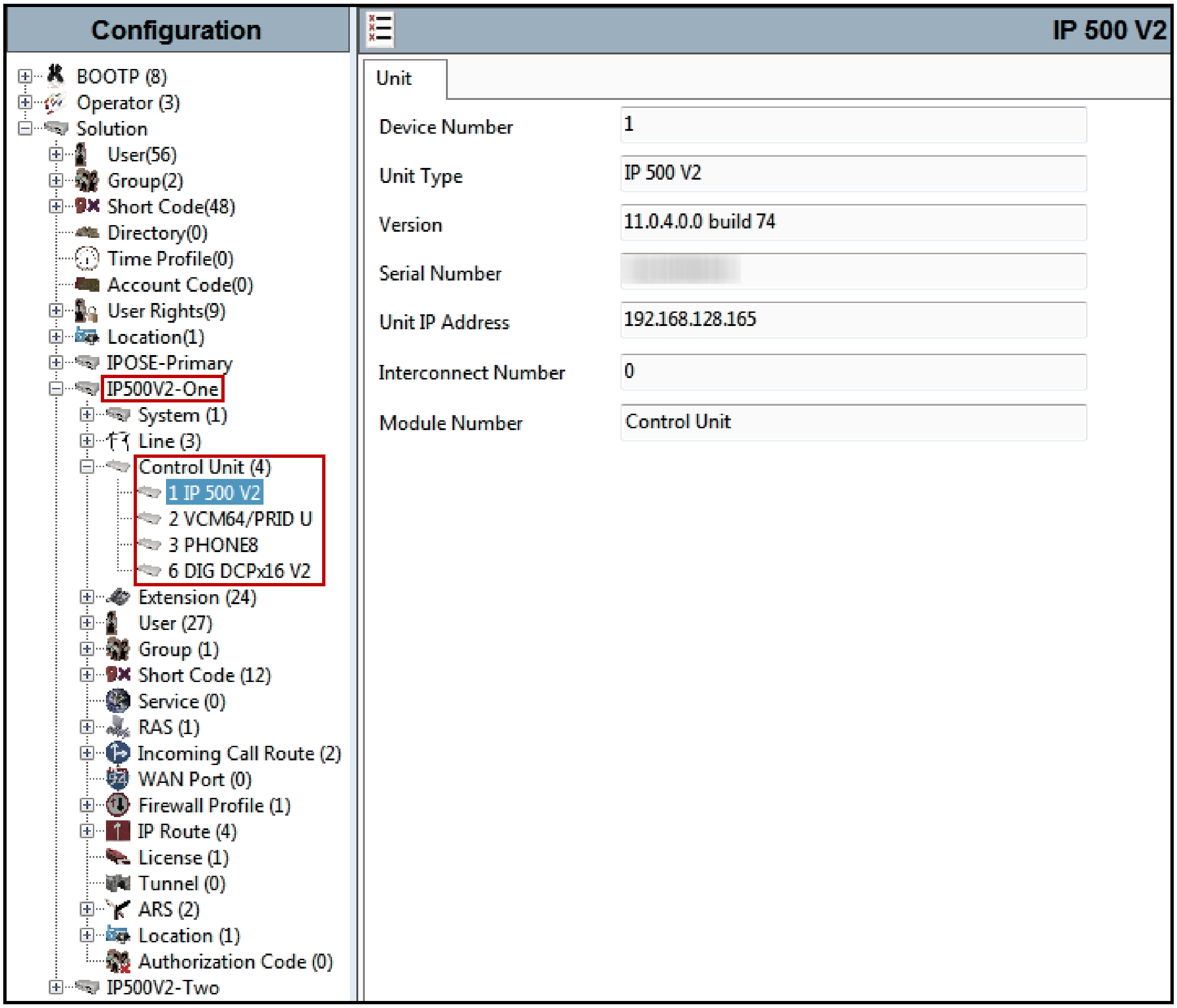
Hardware Installed
Control Unit: IP 500 V2
Internal Modules: VCM64/PRID U; PHONE8
Expansion Modules: DIG DCPx16 V2

System Settings
IP Address: 192.168.128.165
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)
Connected Extensions: 3043; 3044
Users NOT Configured for Voicemail: NONE
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.

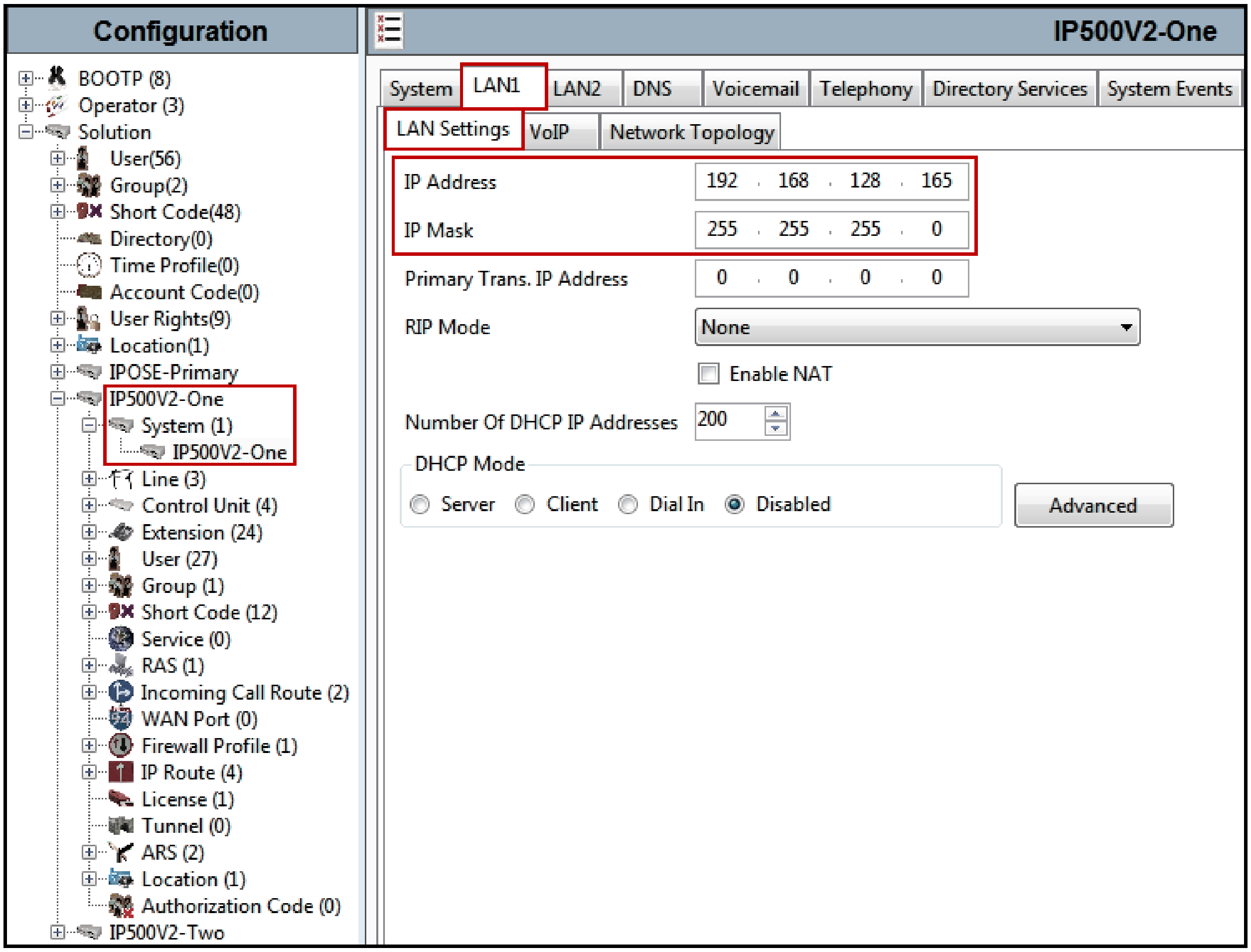


Device Number: 1
Unit Type: IP 500 V2
Version: 11.0.4.0.0 build 74
Serial Number: [redacted]
Unit IP Address: 192.168.128.165
Interconnect Number: 0
Module Number: Control Unit

6.2. LAN Settings

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

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



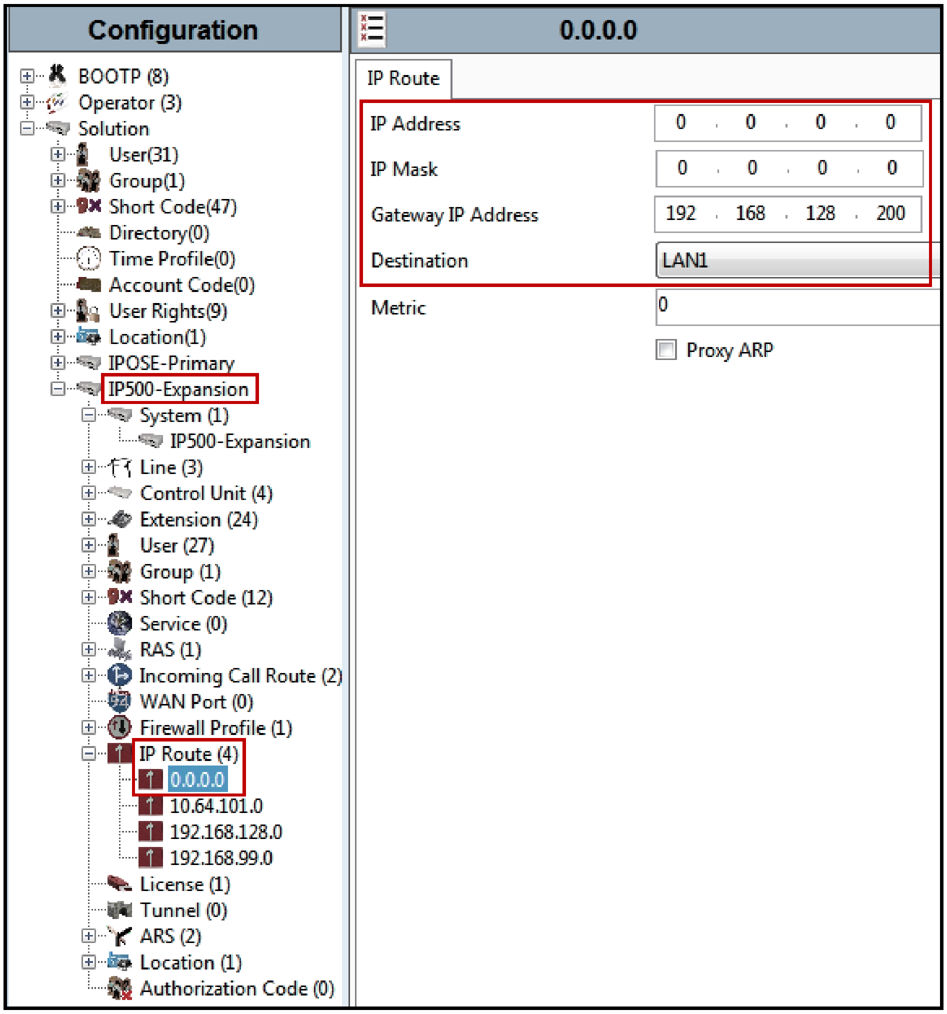
IP Address: 192 . 168 . 128 . 165
IP Mask: 255 . 255 . 255 . 0
Primary Trans. IP Address: 0 . 0 . 0 . 0
RIP Mode: None
☐ Enable NAT
Number Of DHCP IP Addresses: 200
DHCP Mode: ○ Server ○ Client ○ Dial In ● Disabled

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

6.3. IP Route

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

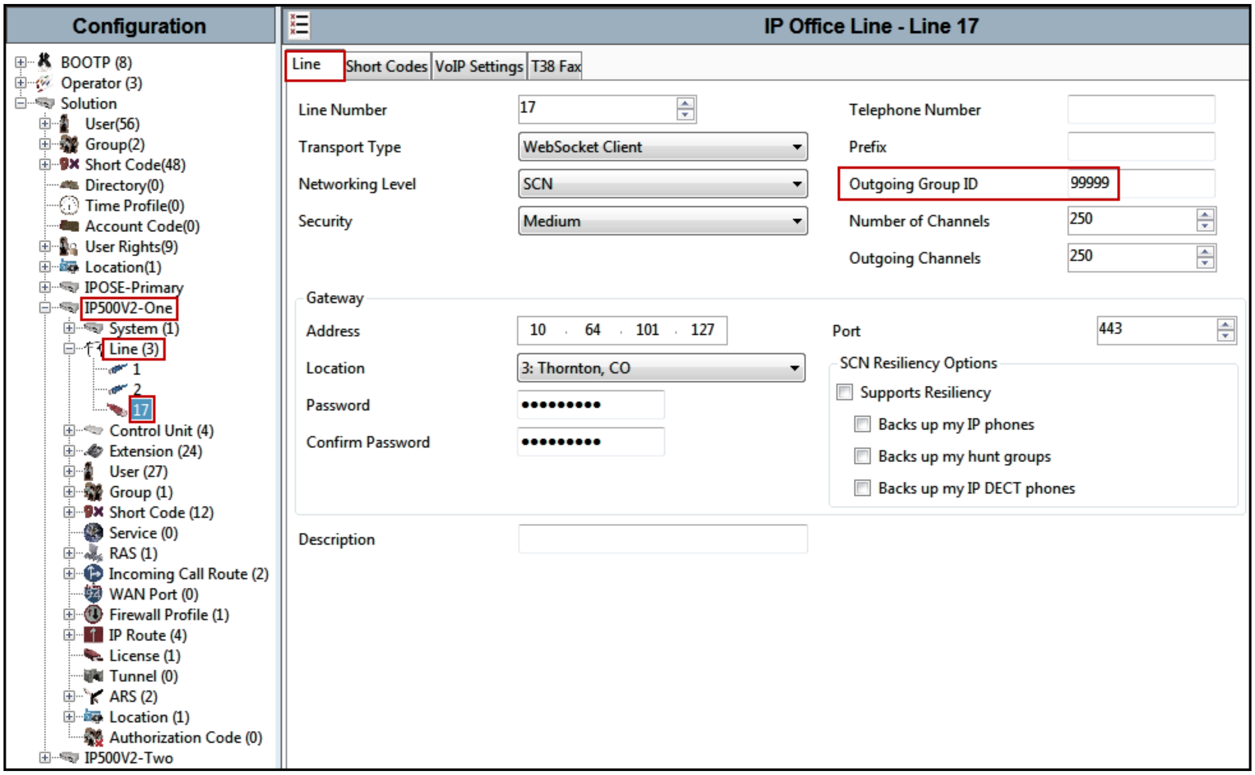
- Enter **0.0.0.0** on the **IP Address** and **IP Mask** fields to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet. The default gateway in the reference configuration was **192.168.128.200**.
- Set **Destination** to **LAN1**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



IP Address: 0 . 0 . 0 . 0
IP Mask: 0 . 0 . 0 . 0
Gateway IP Address: 192 . 168 . 128 . 200
Destination: LAN1
Metric: 0
☐ Proxy ARP

6.4. IP Office Line – IP500 V2 Expansion System

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



Line Number: 17
Transport Type: WebSocket Client
Networking Level: SCN
Security: Medium
Telephone Number:
Prefix:
Outgoing Group ID: 99999
Number of Channels: 250
Outgoing Channels: 250

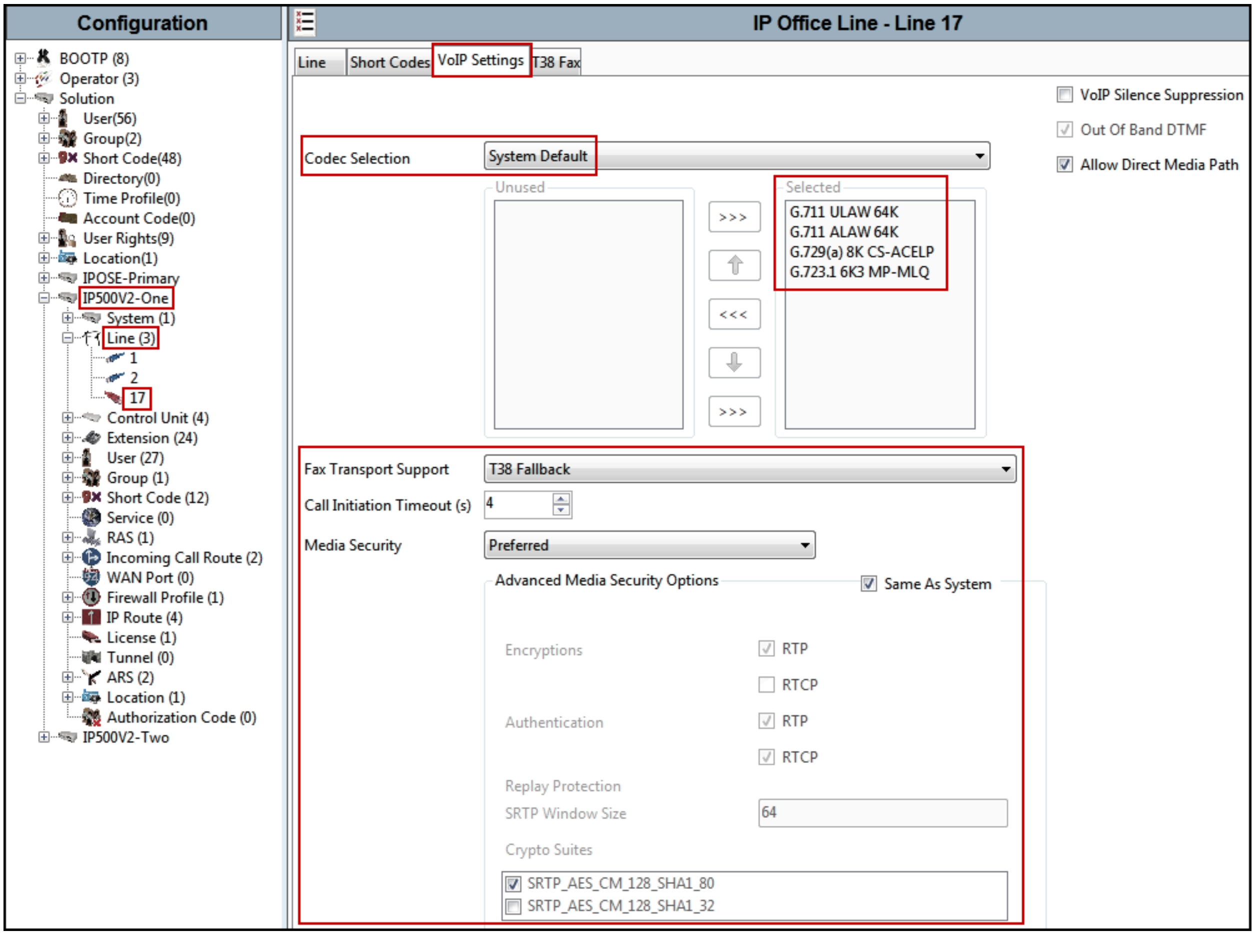
Gateway
Address: 10 . 64 . 101 . 127
Port: 443
Location: 3: Thornton, CO
Password: ••••••••••
Confirm Password: ••••••••••

SCN Resiliency Options
☐ Supports Resiliency
☐ Backs up my IP phones
☐ Backs up my hunt groups
☐ Backs up my IP DECT phones

Description:

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

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



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

Codec Selection: System Default

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

Fax Transport Support: T38 Fallback

Call Initiation Timeout (s): 4

Media Security: Preferred

Advanced Media Security Options ☑ Same As System

Encryptions: ☑ RTP ☐ RTCP

Authentication: ☑ RTP ☑ RTCP

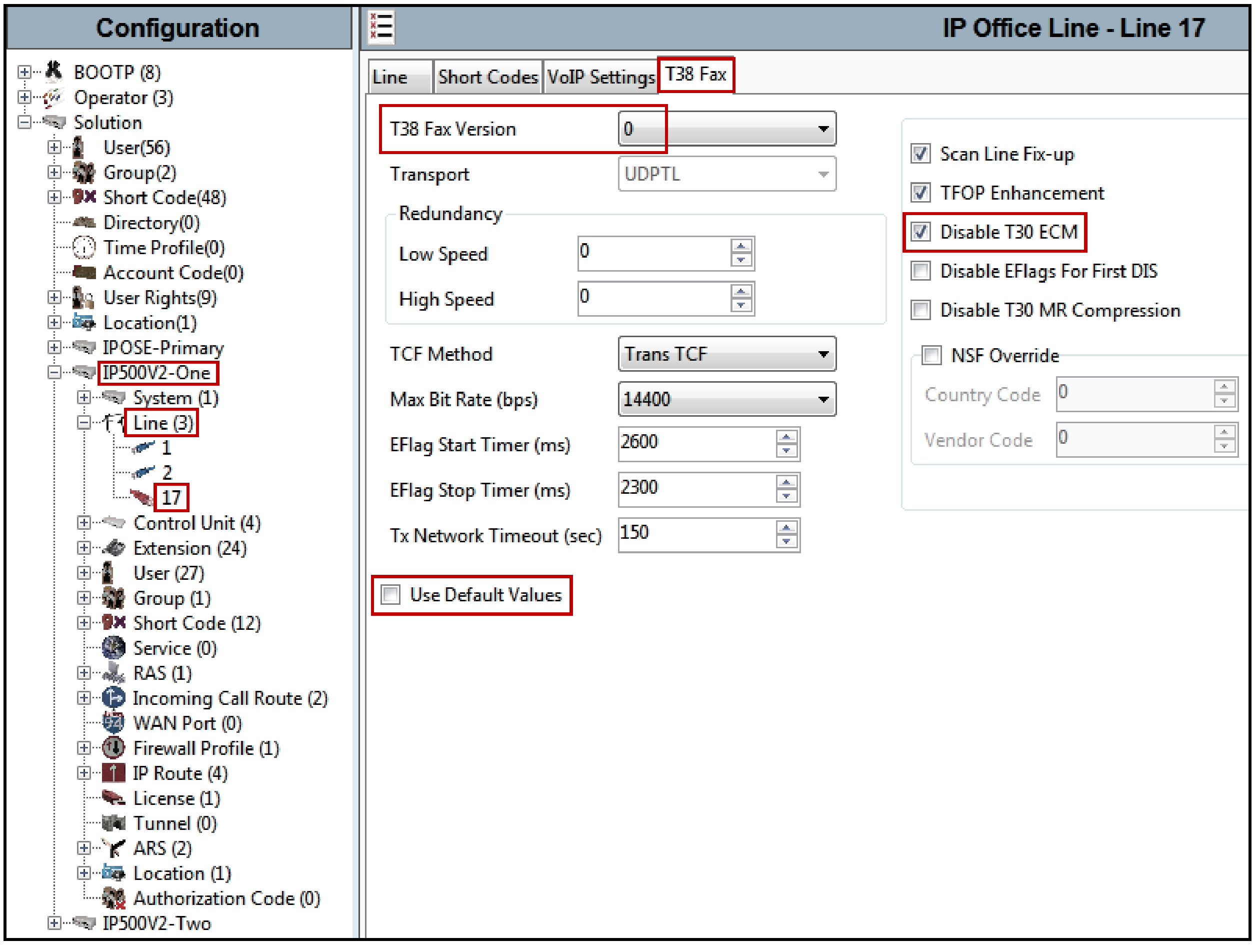
Replay Protection

SRTP Window Size: 64

Crypto Suites:
☑ SRTP_AES_CM_128_SHA1_80
☐ SRTP_AES_CM_128_SHA1_32

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:

- Uncheck the **Use Default Values** at the bottom of the screen.
- Set the **T.38 Fax Version** to **0**, CenturyLink supports T.38 fax version 0.
- Check **Disable T30 ECM** (refer to **Section 2.2**).
- Default values may be used for all other parameters.



T38 Fax Version: 0

Transport: UDPTL

Redundancy

Low Speed: 0

High Speed: 0

TCF Method: Trans TCF

Max Bit Rate (bps): 14400

EFlag Start Timer (ms): 2600

EFlag Stop Timer (ms): 2300

Tx Network Timeout (sec): 150

☐ Use Default Values

☑ Scan Line Fix-up

☑ TFOP Enhancement

☑ Disable T30 ECM

☐ Disable EFlags For First DIS

☐ Disable T30 MR Compression

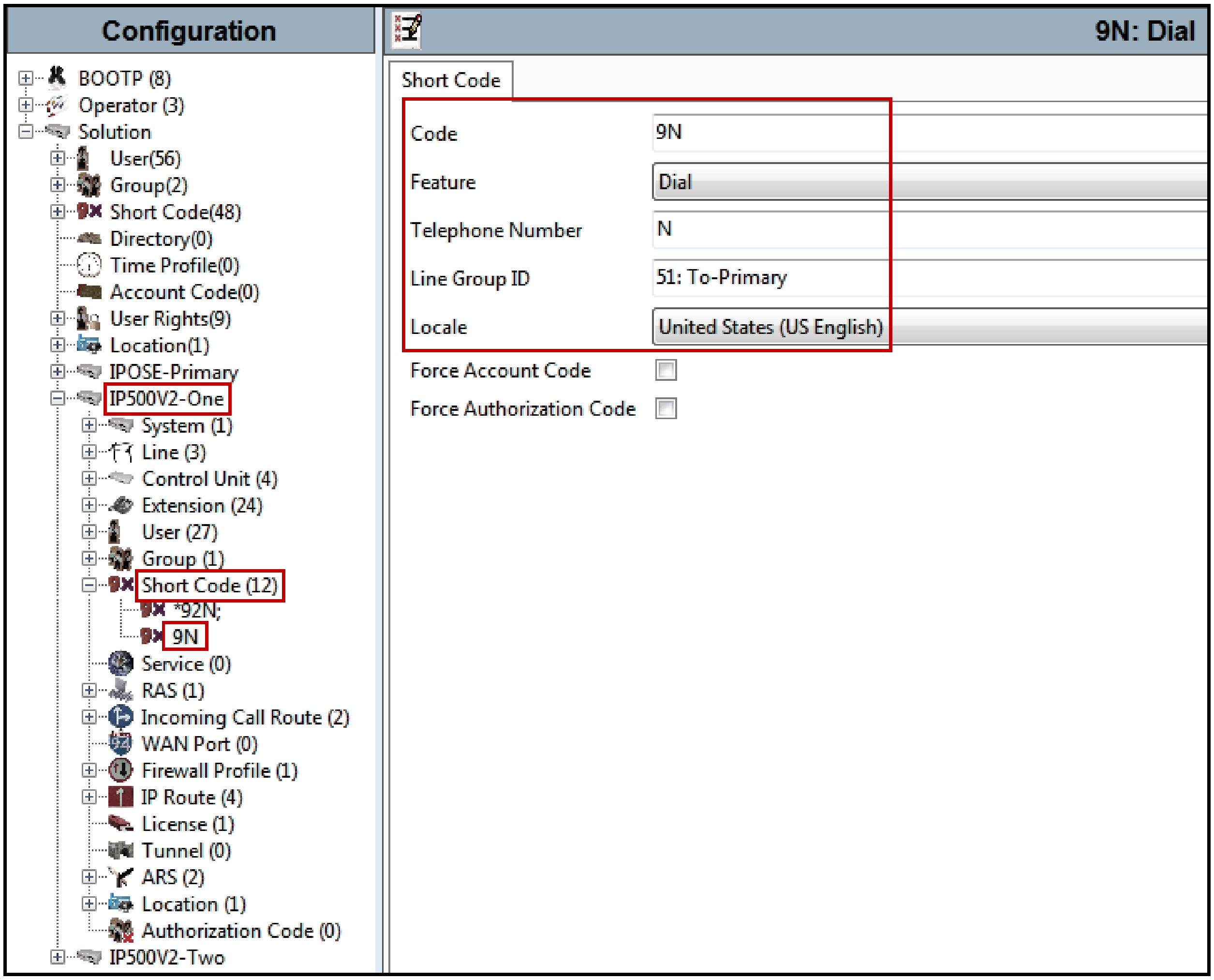
☐ NSF Override

Country Code: 0

Vendor Code: 0

6.5. Short Codes

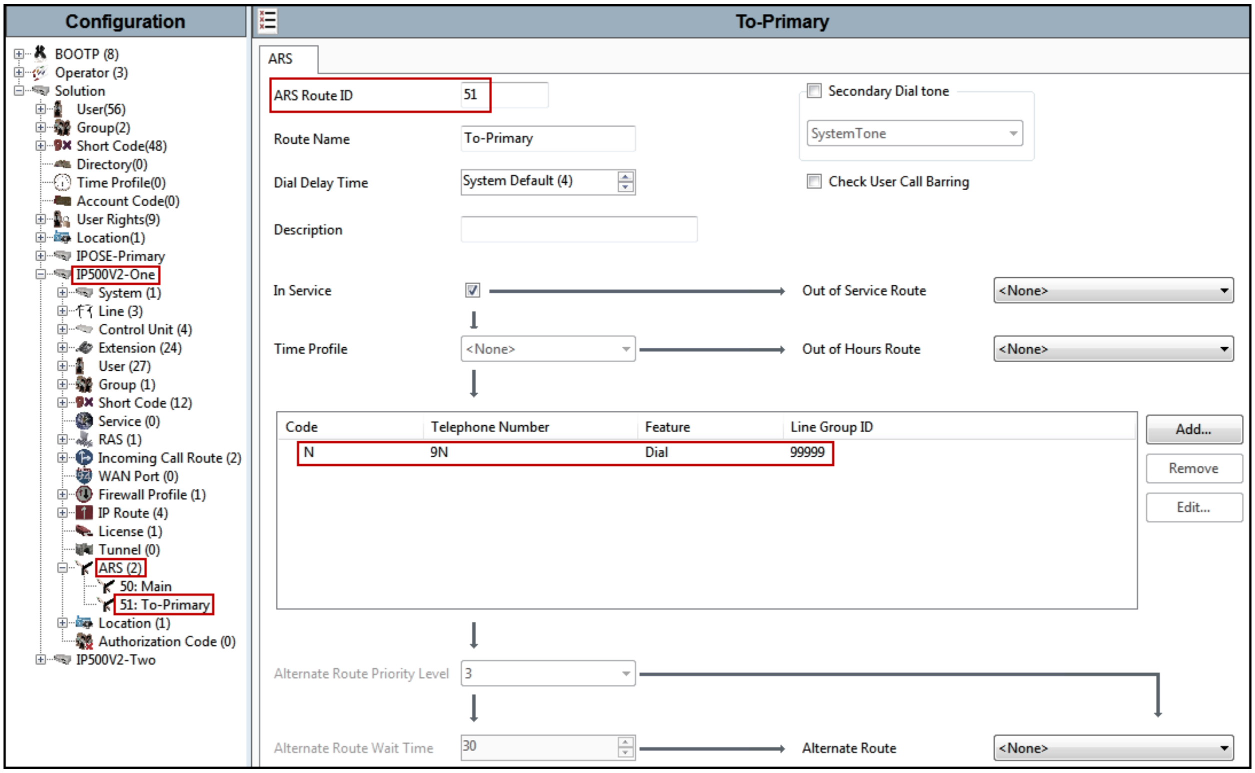
Similar to the configuration of the Primary server in **Section 5.7**, create a Short Code to access ARS. In the reference configuration, the **Line Group ID** is set to the ARS route illustrated in the next section.



Code: 9N
Feature: Dial
Telephone Number: N
Line Group ID: 51: To-Primary
Locale: United States (US English)
Force Account Code ☐
Force Authorization Code ☐

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**).



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

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

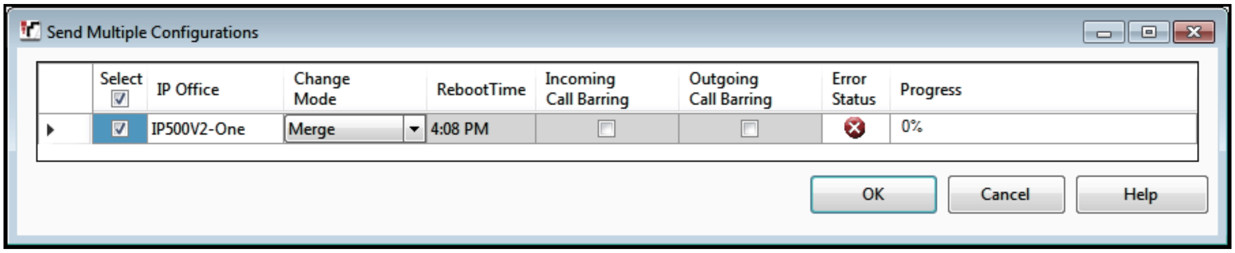
Alternate Route Priority Level: 3
Alternate Route Wait Time: 30
Alternate Route: <None>

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.



Select ☑	IP Office	Change Mode	RebootTime	Incoming Call Barring	Outgoing Call Barring	Error Status	Progress
☑	IP500V2-One	Merge	4:08 PM	☐	☐	✗	0%

7. CenturyLink IQ® SIP Trunking Service on the Broadsoft Platform Configuration

To use CenturyLink IQ® SIP Trunking Service on the Broadsoft Platform, a customer must request the service from CenturyLink using the established sales processes. The process can be started by contacting CenturyLink via the corporate web site at: http://www.centurylink.com/business/voice/sip-trunk.html and requesting information.

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

CenturyLink is responsible for the configuration of CenturyLink IQ® SIP Trunking Service on the Broadsoft Platform. 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.

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

- SIP Trunk registration credentials.
- SIP Proxy IP address.
- Domain Name.
- DID numbers, etc.

8. Verification Steps

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

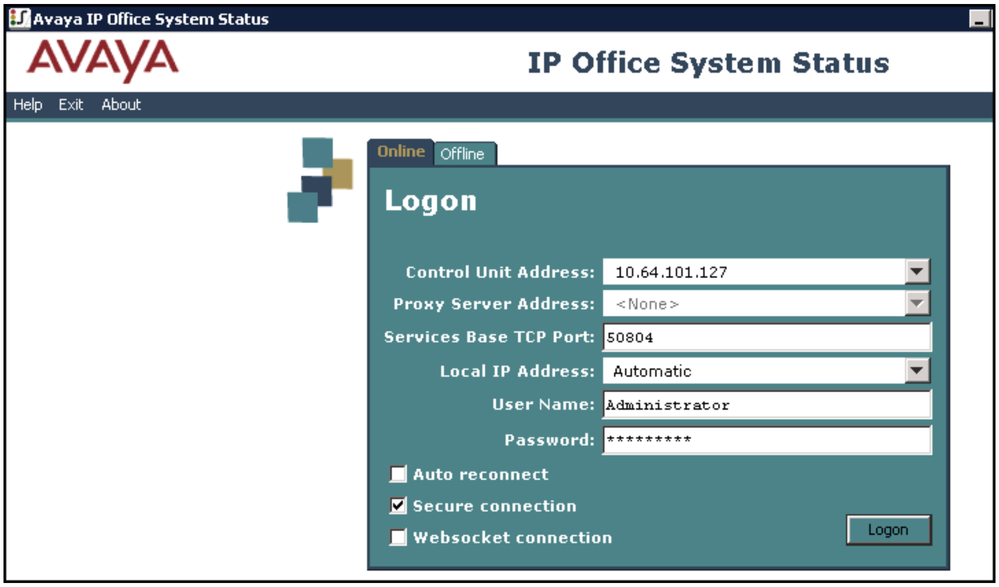
The following steps may be used to verify the configuration:

- 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

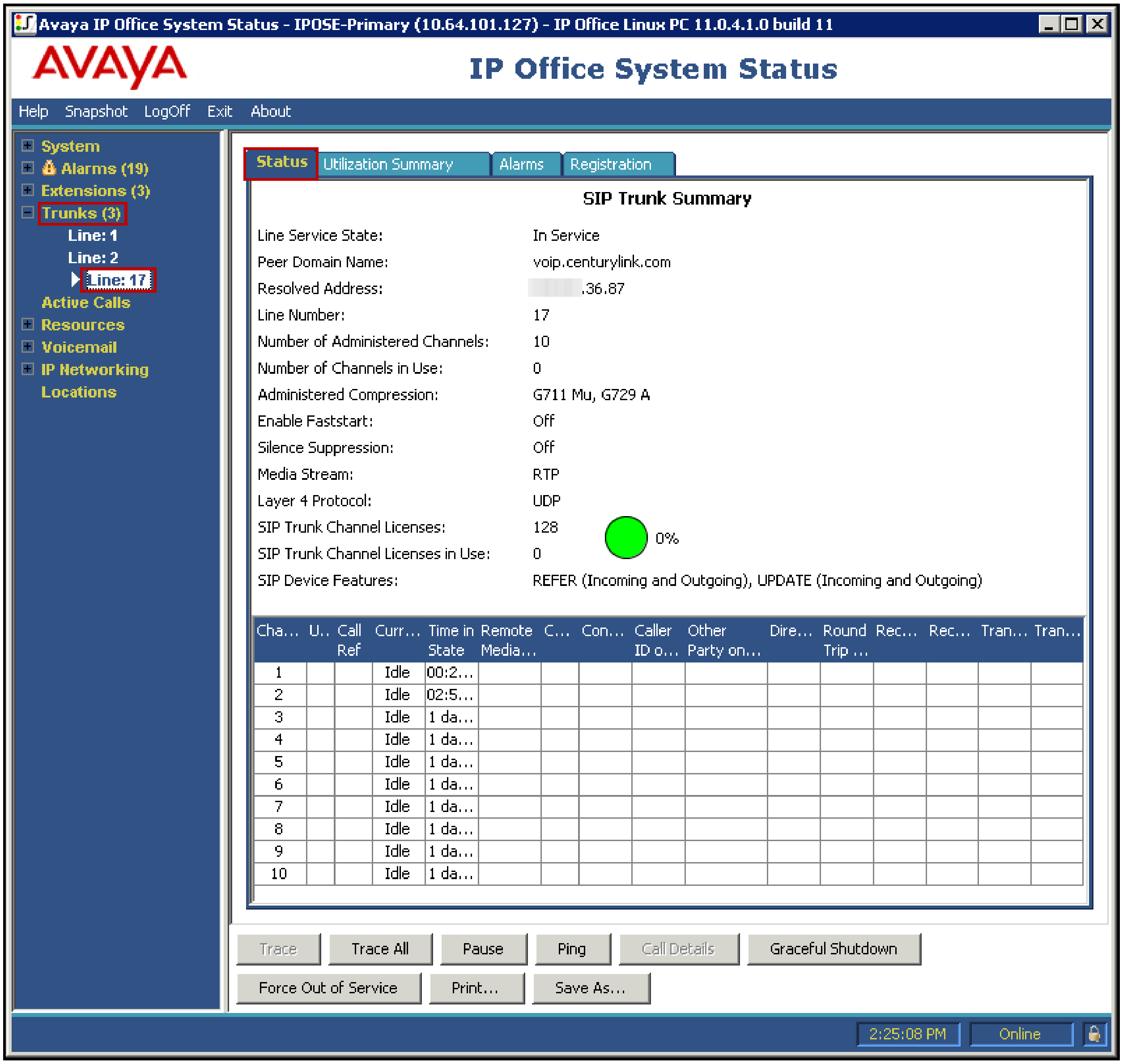
The following steps can also be used to verify the configuration.

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.



Control Unit Address: 10.64.101.127
Proxy Server Address: <None>
Services Base TCP Port: 50804
Local IP Address: Automatic
User Name: Administrator
Password: *********
☐ Auto reconnect
☑ Secure connection
☐ Websocket connection

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.



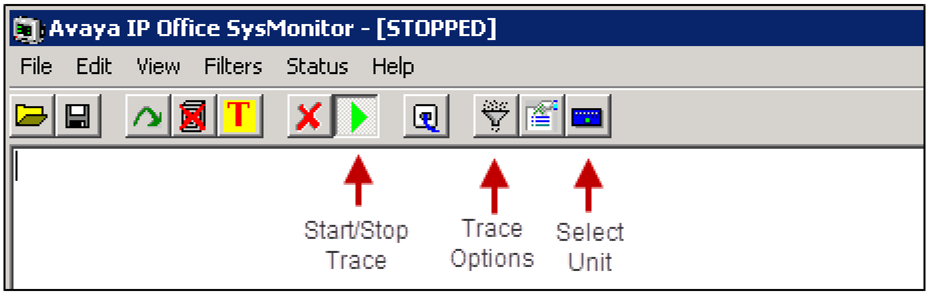
SIP Trunk Summary

Line Service State:	In Service
Peer Domain Name:	voip.centurylink.com
Resolved Address:	[redacted].36.87
Line Number:	17
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:	128 🟢 0%
SIP Trunk Channel Licenses in Use:	0
SIP Device Features:	REFER (Incoming and Outgoing), UPDATE (Incoming and Outgoing)

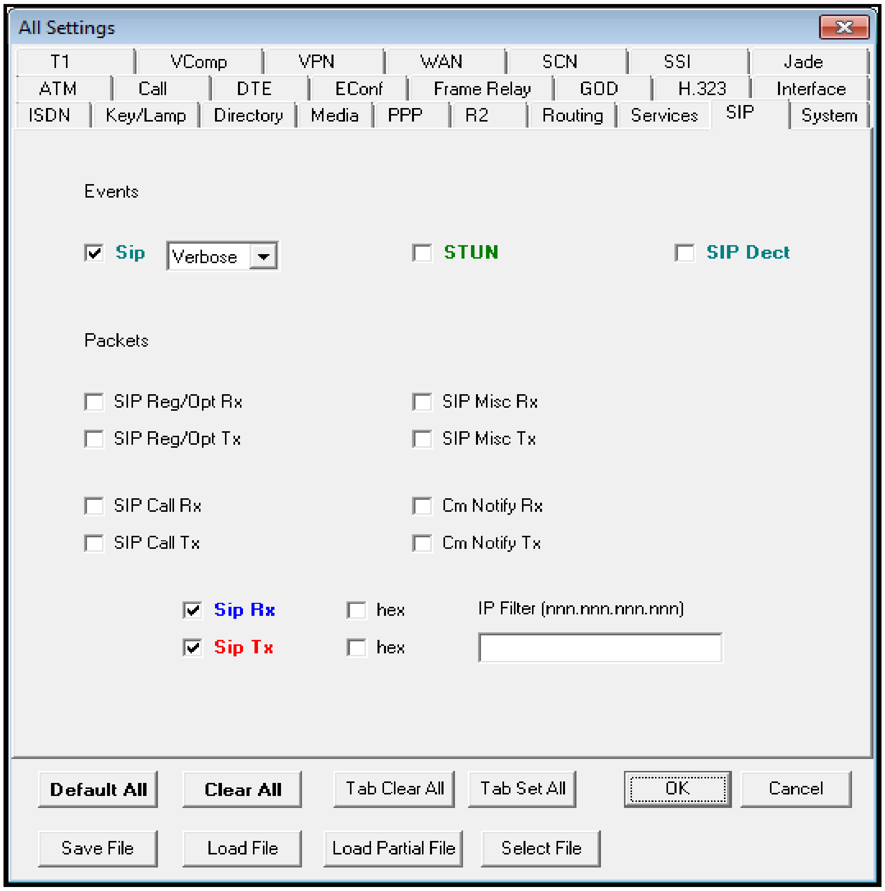
Cha...	U..	Call Ref	Curr...	Time in State	Remote Media...	C...	Con...	Caller ID o...	Other Party on...	Dire...	Round Trip ...	Rec...	Rec...	Tran...	Tran...
1			Idle	00:2...											
2			Idle	02:5...											
3			Idle	1 da...											
4			Idle	1 da...											
5			Idle	1 da...											
6			Idle	1 da...											
7			Idle	1 da...											
8			Idle	1 da...											
9			Idle	1 da...											
10			Idle	1 da...											

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.



Events

☑ Sip Verbose
☐ STUN
☐ SIP Dect

Packets

☐ SIP Reg/Opt Rx
☐ SIP Reg/Opt Tx
☐ SIP Call Rx
☐ SIP Call Tx
☐ SIP Misc Rx
☐ SIP Misc Tx
☐ Cm Notify Rx
☐ Cm Notify Tx

☑ Sip Rx ☐ hex
☑ Sip Tx ☐ hex

IP Filter (nnn.nnn.nnn.nnn)

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office Release 11.0 to CenturyLink IQ® SIP Trunking Service on the Broadsoft Platforms. CenturyLink IQ® SIP Trunking Service on the Broadsoft Platforms 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/

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.