



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.0 to support CenturyLink Voice Complete 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 Voice Complete 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 Voice Complete 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:

- 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 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, G.711A 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.
- CenturyLink does not support the SIP REFER method for call transfers to the PSTN, the testing was done with REFER disabled in IP Office (refer to **Section 5.4.2**).

2.2. Test Results

Interoperability testing of CenturyLink Voice Complete 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.

- **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 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 caused the far-end to still see the number presented in the P-Asserted Identity header (the originating calling number was not blocked). This is currently being investigated by IP Office development team.

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 Voice Complete 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.

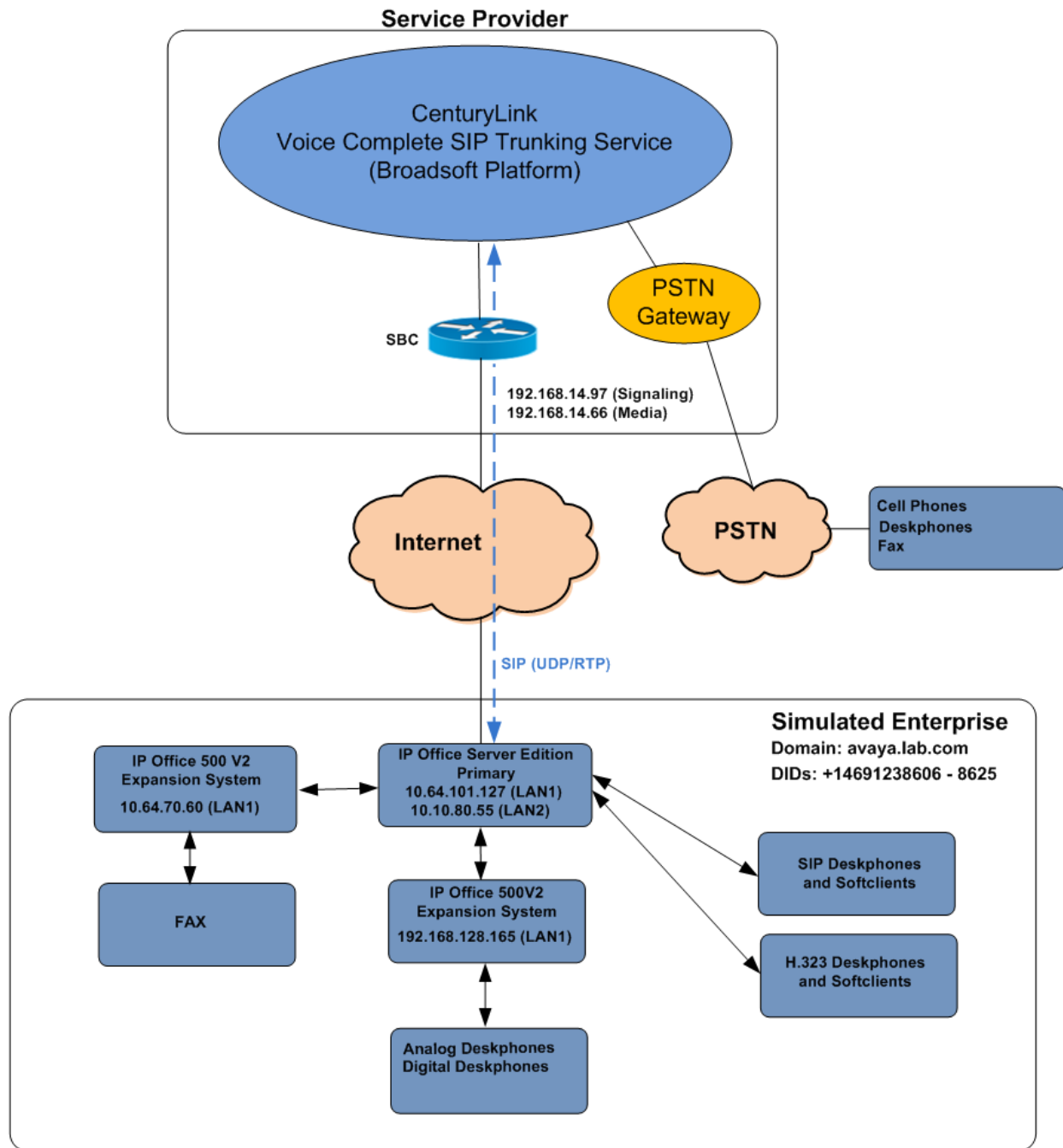


Figure 1: Avaya Interoperability Test Lab Configuration

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)	11.0.4.1.0 Build 11
• Avaya IP Office Voicemail Pro	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)	3.6.4.31.2
Analog Telephone	---
CenturyLink	
BroadSoft BroadWorks	R21.SP1
Sonus (Ribbon) SBC 7000	5.1.3

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.

Select IP Office

Name	IP Address	Type	Version	Edition
Server Edition 11.0				
<input checked="" type="checkbox"/> IPOSE-Primary	10.64.101.127	IPO-Linux-PC	11.0.4.1.0 build 11	Server (Primary)

Configuration Service User Login

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

Service User Name:

Service User Password:

TCP Discovery Progress

Unit/Broadcast Address ☒ 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.

Configuration

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - 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: 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

Open...

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

Add...

- Secondary Server
- Expansion System

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.

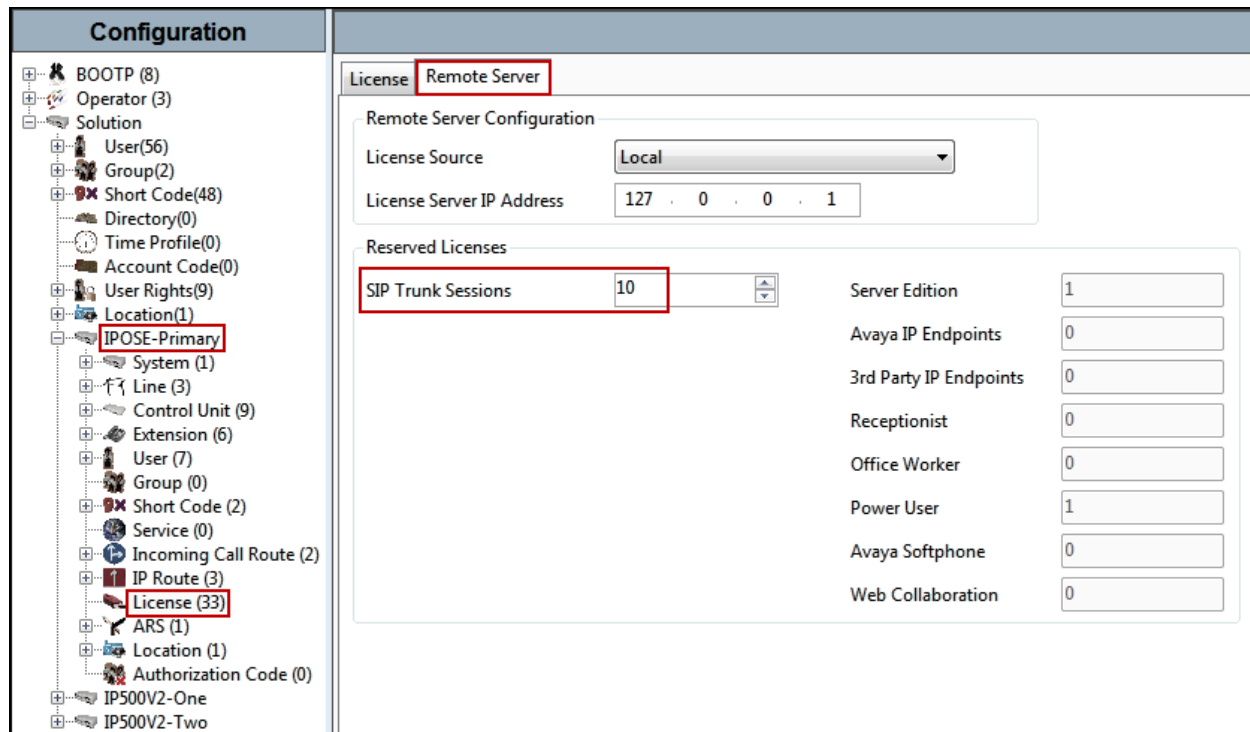
The screenshot shows the Avaya IP Office Configuration interface. On the left is the 'Configuration' navigation pane with a tree view. The 'License (33)' item under the 'IPOSE-Primary' system is selected and highlighted with a red box. On the right is the 'Details' pane, which has two tabs: 'License' (selected) and 'Remote Server'. The 'License' tab displays the following information:

- License Mode: License Normal
- Licensed Version: 11.0
- PLDS Host ID: [Empty field]
- PLDS File Status: Valid

Below this information is a table listing various features, their instance counts, status, expiration dates, and sources. The 'SIP Trunk Channels' row is highlighted with a red box.

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 numbers of licenses to be assigned to the specific Server or Expansion Systems are reserved from the total pool of licenses present on the license server. On the screen below, 10 **SIP Trunk Sessions** licenses were reserved to be used by the Primary Server.



Configuration

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - System (1)
 - Line (3)
 - Control Unit (9)
 - Extension (6)
 - User (7)
 - Group (0)
 - Short Code (2)
 - Service (0)
 - Incoming Call Route (2)
 - IP Route (3)
 - License (33)
 - ARS (1)
 - Location (1)
 - Authorization Code (0)
- IP500V2-One
- IP500V2-Two

License Remote 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 Voice Complete 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.

The screenshot displays the IPOSE-Primary configuration window. On the left is a tree view under 'Configuration' with various system components. The 'IPOSE-Primary' section is expanded, showing 'System (1)' and 'IPOSE-Primary'. The main panel on the right has tabs for 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', and 'System Events'. The 'LAN2' tab is selected. Within this tab, there are sub-tabs for 'LAN Settings', 'VoIP', and 'Network Topology'. The 'LAN Settings' sub-tab is active. It contains fields for 'IP Address' (10 . 10 . 80 . 55) and 'IP Mask' (255 . 255 . 255 . 128), both of which are highlighted with a red box. Below these are 'Number Of DHCP IP Addresses' (200) and 'DHCP Mode' (Server, Client, Disabled). The 'Disabled' radio button is selected. An 'Advanced' button is located at the bottom right of the DHCP settings.

5.2.1.2 LAN2 VoIP Tab

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

The screenshot displays the IPOSE-Primary configuration interface. On the left is a 'Configuration' tree with various system components. The 'LAN2' tab is selected in the top navigation bar, and the 'VoIP' sub-tab is active. The main configuration area shows settings for SIP trunks and registration. The 'SIP Trunks Enable' checkbox is checked, while 'SIP Registrar Enable' is unchecked. Below these, there are fields for SIP Domain Name and SIP Registrar FQDN. The 'Layer 4 Protocol' section shows UDP and TCP ports (5060) and Remote ports (5060) for both protocols, and TLS ports (5061) and Remote ports (5061). The 'Challenge Expiration Time (sec)' is set to 10. The 'H.323 Gatekeeper Enable' section is also visible at the top, with 'Auto-create Extension', 'Auto-create User', and 'H.323 Remote Extension Enable' all unchecked. The 'H.323 Signaling over TLS' is set to 'Disabled' and the 'Remote Call Signaling Port' is 1720.

System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	VoIP	Contact Center
LAN Settings VoIP Network Topology											
<input type="checkbox"/> H.323 Gatekeeper Enable											
<input type="checkbox"/> Auto-create Extension <input type="checkbox"/> Auto-create User <input type="checkbox"/> H.323 Remote Extension Enable											
H.323 Signaling over TLS Disabled Remote Call Signaling Port 1720											
<input checked="" type="checkbox"/> SIP Trunks Enable											
<input type="checkbox"/> SIP Registrar Enable											
<input type="checkbox"/> Auto-create Extension/User <input type="checkbox"/> SIP Remote Extension Enable Allowed SIP User Agents Block blacklist only											
SIP Domain Name											
SIP Registrar FQDN											
<input checked="" type="checkbox"/> UDP UDP Port 5060 Remote UDP Port 5060											
<input checked="" type="checkbox"/> TCP TCP Port 5060 Remote TCP Port 5060											
<input type="checkbox"/> 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).

Configuration

IPOSE-Primary*

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

LAN Settings **VoIP** Network Topology

☐ 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).

The screenshot displays the IPOSE-Primary configuration window. The left sidebar shows a tree view of configuration elements, with 'IPOSE-Primary' and its sub-items 'System (1)' and 'IPOSE-Primary' highlighted. The main pane is titled 'IPOSE-Primary*' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', 'System Events', 'SMTP', 'SMDR', 'VoIP', and 'Contact Center'. The 'LAN2' tab is active, and within it, the 'Network Topology' sub-tab is selected. The 'Network Topology Discovery' section contains the following settings: 'STUN Server Address' (empty), 'STUN Port' (3478), 'Firewall/NAT Type' (Open Internet), 'Binding Refresh Time (sec)' (180), 'Public IP Address' (0.0.0.0), and 'Public Port' (UDP: 5060, TCP: 5060, TLS: 5061). A 'Run STUN' button and a 'Cancel' button are visible. At the bottom, there is a checkbox for 'Run STUN on startup' which is currently unchecked.

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).

The screenshot displays the IPOSE-Primary configuration window. On the left is a tree view of the configuration hierarchy, with 'IPOSE-Primary' and its sub-items highlighted. The main area is divided into tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony (selected), Directory Services, System Events, SMTP, SMDR, VoIP, Contact Center, and Avaya Cloud Services. The 'Telephony' tab is active, showing various settings. A red box highlights the 'Companding Law' section, where 'U-Law' is selected for both 'Switch' and 'Line'. Another red box highlights the 'Inhibit Off-Switch Forward/Transfer' checkbox, which is currently checked. Other visible settings include Dial Delay Time (4), Hold Timeout (0), Park Timeout (300), Ring Delay (5), and Login Code Complexity (Enforcement and Complexity checked).

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).

The screenshot displays the configuration interface for IPOSE-Primary. On the left, a tree view shows the configuration hierarchy, with 'IPOSE-Primary' selected. The main pane on the right is titled 'IPOSE-Primary*' and contains several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. The 'VoIP' tab is active, showing options for 'VoIP Security' and 'Access Control Lists'. The 'RFC2833 Default Payload' is set to 101. Below this, the 'Default Codec Selection' section shows two lists: 'Available Codecs' and 'Selected'. The 'Available Codecs' list includes G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, and G.729(a) 8K CS-ACELP. The 'Selected' list contains G.711 ULAW 64K, G.711 ALAW 64K, and G.729(a) 8K CS-ACELP. Buttons for moving codecs between lists and changing their order are also visible.

Note: The codec selections defined under this section (VoIP – VoIP Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.5** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.2.3.2 VoIP – VoIP Security Tab

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

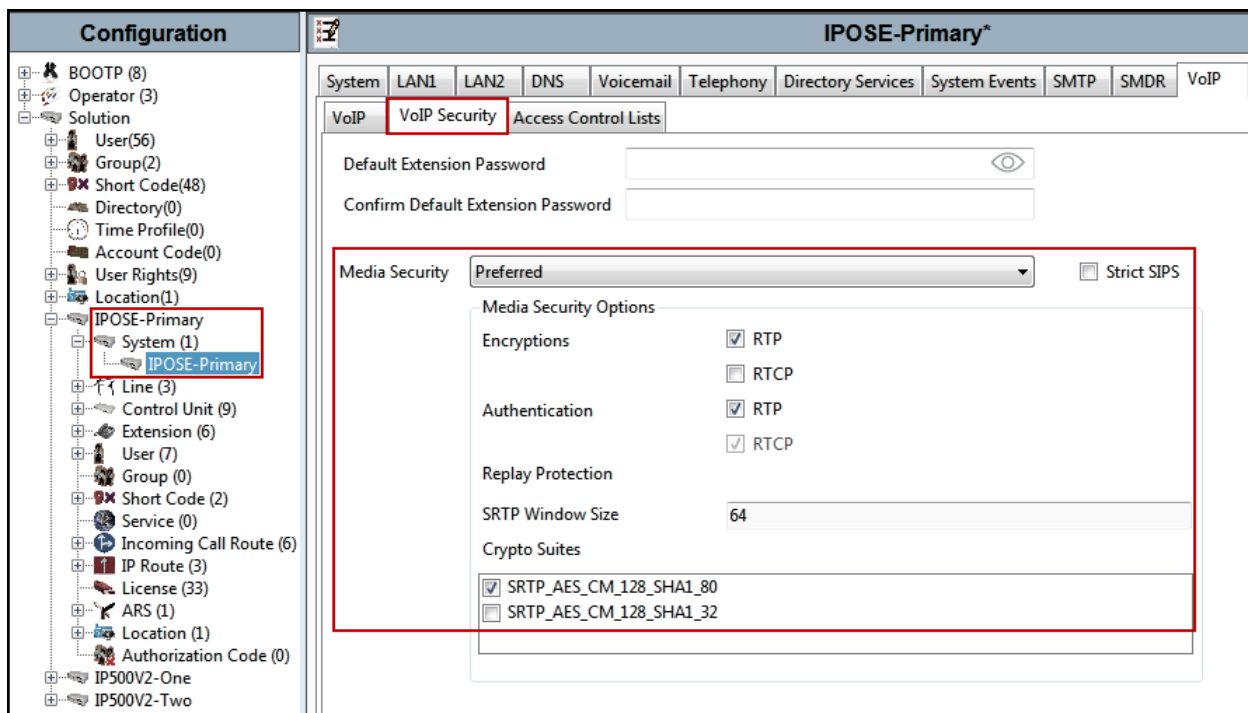
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

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

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

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

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



5.3. IP Route

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

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

5.4. SIP Line

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

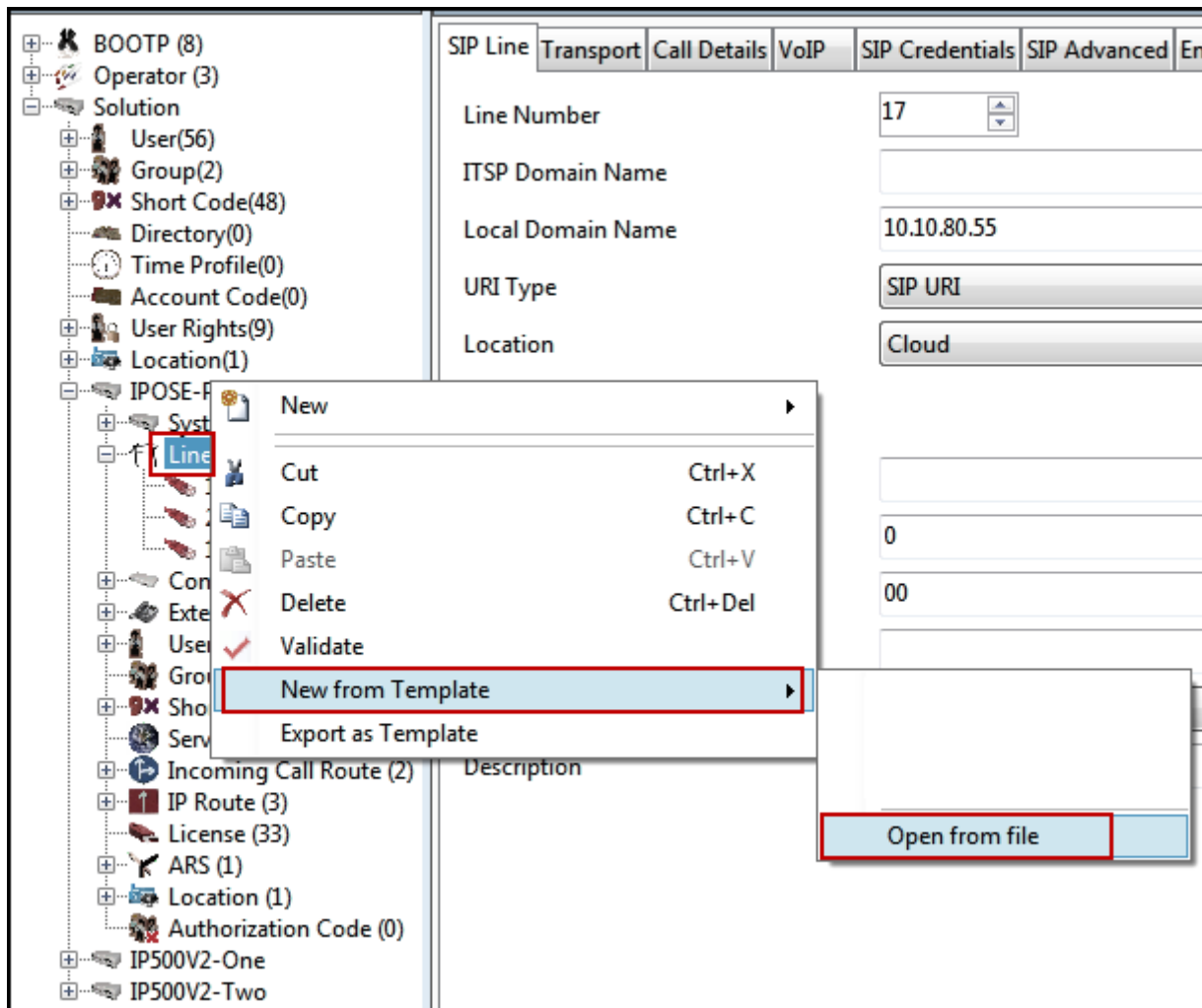
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.6**.

5.4.1. Creating a SIP Trunk from an XML Template

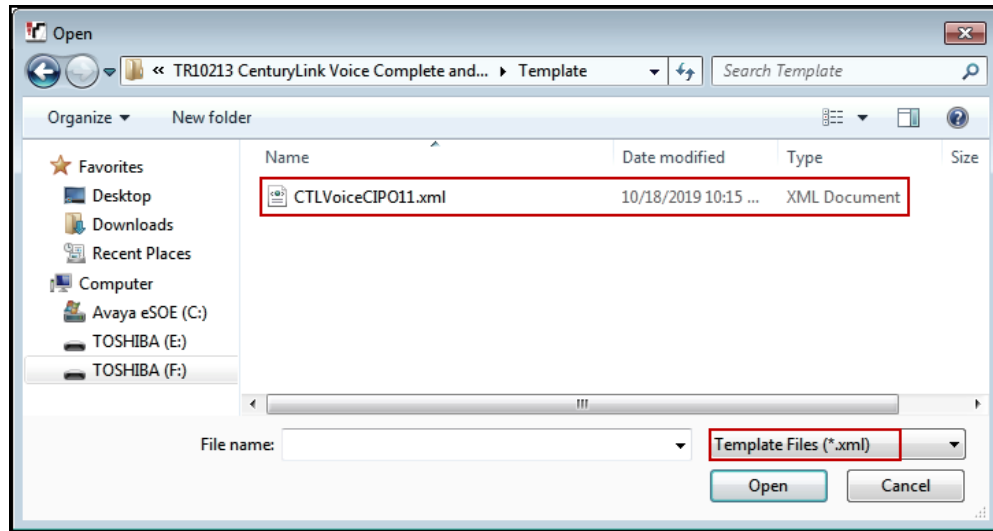
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and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

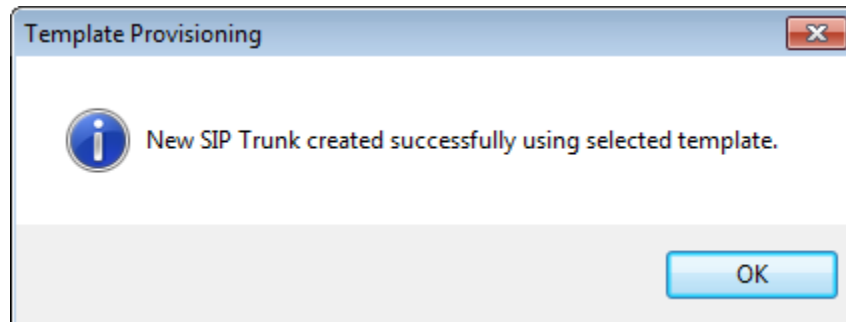
To create the SIP Trunk from the template, from the **Primary** server (**IPOSE-Primary**), right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template → Open from file**.



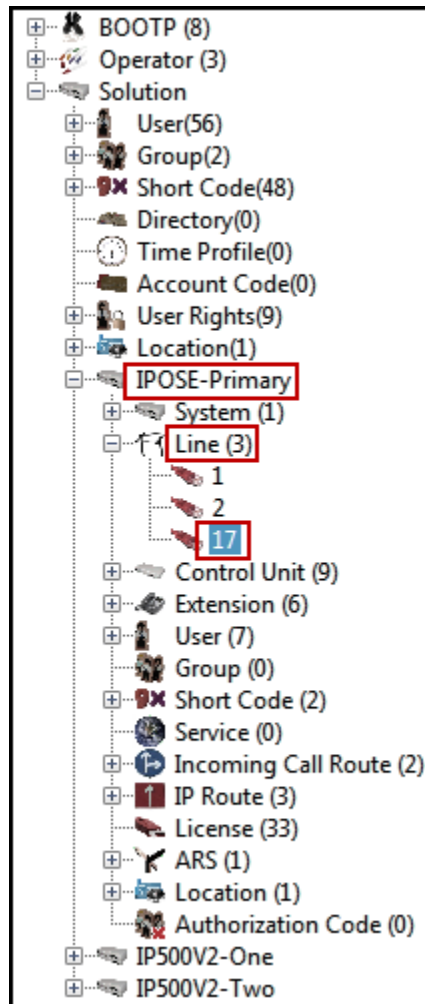
Navigate to the directory on the local machine where the template was copied and select the template.



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:

- Leave the **ITSP Domain Name** blank. Note that if this field is left blank, then IP Office inserts the ITSP Proxy Address from the Transport tab as the ITSP Domain in the SIP messaging.
- Set the **Local Domain Name** to the public IP address of **LAN2**, refer to **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 **Incoming Supervised REFER** and **Outgoing Supervised REFER** was set to **Never**. CenturyLink does not support the SIP REFER method for call transfers to the PSTN (refer to **Section 2.1**).
- Click **OK** to commit (not shown).

Configuration

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary**
 - System (1)
 - Line (3)**
 - 1
 - 2
 - 17**
 - Control Unit (9)
 - Extension (6)
 - User (7)
 - Group (0)
 - Short Code (2)
 - Service (0)
 - Incoming Call Route (6)
 - IP Route (3)
 - License (33)
 - ARS (1)
 - Location (1)
 - Authorization Code (0)
- IP500V2-One
- IP500V2-Two

SIP Line - Line 17

SIP Line | Transport | Call Details | VoIP | SIP Credentials | SIP Advanced | Engineering

Line Number: 17

ITSP Domain Name:

Local Domain Name: 10.10.80.55

URI Type: SIP URI

Location: Cloud

Prefix:

National Prefix:

International Prefix:

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: Never

Outgoing Supervised REFER: Never

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, **192.168.14.97** was used during the compliance test.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **None** (refer to the note below).
- Set the **Send Port** to **5060**.
- Set the **Listen Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view shows the configuration hierarchy, with 'Line (3)' selected under 'IPOSE-Primary'. The main window shows the 'SIP Line - Line 17' configuration. The 'Transport' tab is active. The 'ITSP Proxy Address' is set to '192.168.14.97'. The 'Network Configuration' section is highlighted with a red box, showing 'Layer 4 Protocol' set to 'UDP', 'Send Port' set to '5060', 'Use Network Topology Info' set to 'None', and 'Listen Port' set to '5060'. Below this, 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0', 'Calls Route via Registrar' is checked, and 'Separate Registrar' is empty.

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 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 **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, these settings are default values.
- Click **OK**.
- Click **OK** to commit again (not shown).

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	None	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. CenturyLink supports codecs **G.711 ULAW**, **G.711 ALAW** and **G.729(a)** for audio.
- Select **T.38 Fallback** for **Fax Transport Support**.
- 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).

The screenshot shows the Avaya IP Office configuration interface for 'SIP Line - Line 17'. The 'VoIP' tab is selected. The left sidebar shows a tree view with 'Line 17' highlighted. The main configuration area includes:

- Codec Selection:** Set to 'Custom'. Below it, an 'Unused' list is empty, and a 'Selected' list contains 'G.711 ULAW 64K', 'G.711 ALAW 64K', and 'G.729(a) 8K CS-ACELP'.
- Fax Transport Support:** Set to 'T38 Fallback'.
- DTMF Support:** Set to 'RFC2833/RFC4733'.
- Media Security:** Set to 'Disabled'.
- Checkboxes on the right:**
 - ☐ Local Hold Music
 - ☒ Re-invite Supported
 - ☐ Codec Lockdown
 - ☐ Allow Direct Media Path
 - ☐ Force direct media with phones
 - ☒ PRACK/100rel Supported

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

5.4.6. SIP Line – SIP Advanced Tab

In the **Addressing** area:

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

In the **Identity** area:

- Check the box for **Use PAI for Privacy**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'SIP Advanced' tab selected. The left sidebar shows a tree view of the configuration hierarchy, with 'Line (3)' selected. The main area is divided into three sections: Addressing, Identity, and Media. The 'Addressing' section has 'Association Method' set to 'By Source IP address' and 'Call Routing Method' set to 'Request URI'. The 'Identity' section has 'Use PAI for Privacy' checked. The 'Media' section has 'Allow Empty INVITE', 'Send Empty re-INVITE', 'Allow To Tag Change', 'P-Early-Media Support', 'Send SilenceSupp=Off', 'Force Early Direct Media', 'Media Connection Preservation', and 'Indicate HOLD' all disabled. The 'Call Control' section has 'Call Initiation Timeout (s)' set to 4, 'Call Queuing Timeout (mins)' set to 5, 'Service Busy Response' set to '486 - Busy Here', 'on No User Responding Send' set to '408-Request Timeout', 'Action on CAC Location Limit' set to 'Allow Voicemail', 'Suppress Q.850 Reason Header' unchecked, 'Emulate NOTIFY for REFER' unchecked, and 'No REFER if using Diversion' unchecked.

Section	Parameter	Value
Addressing	Association Method	By Source IP address
	Call Routing Method	Request URI
Identity	Use "phone-context"	<input type="checkbox"/>
	Add user=phone	<input type="checkbox"/>
	Use + for International	<input type="checkbox"/>
	Use PAI for Privacy	<input checked="" type="checkbox"/>
	Use Domain for PAI	<input type="checkbox"/>
	Caller ID from From header	<input type="checkbox"/>
	Send From In Clear	<input type="checkbox"/>
	Cache Auth Credentials	<input checked="" type="checkbox"/>
	User-Agent and Server Headers	
	Send Location Info	Never
Media	Allow Empty INVITE	<input type="checkbox"/>
	Send Empty re-INVITE	<input type="checkbox"/>
	Allow To Tag Change	<input type="checkbox"/>
	P-Early-Media Support	None
	Send SilenceSupp=Off	<input type="checkbox"/>
	Force Early Direct Media	<input type="checkbox"/>
	Media Connection Preservation	Disabled
	Indicate HOLD	<input type="checkbox"/>
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	<input type="checkbox"/>
	Emulate NOTIFY for REFER	<input type="checkbox"/>
No REFER if using Diversion	<input type="checkbox"/>	

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 screenshot displays the IP Office configuration interface. On the left, the 'Configuration' pane shows a tree structure where 'IPOSE-Primary' and 'Line (3)' are selected. The main area is titled 'IP Office Line - Line 1' and contains the following configuration fields:

Line		Short Codes		VoIP Settings	
Line Number	1	Telephone Number			
Transport Type	WebSocket Server	Prefix			
Networking Level	SCN	Outgoing Group ID	99999		
Security	Medium	Number of Channels	250		
		Outgoing Channels	250		
Gateway					
Address	192 . 168 . 128 . 165				
Location	3: Thornton, CO				
Password				
Confirm Password				
SCN Resiliency Options					
<input type="checkbox"/> Supports Resiliency					
<input type="checkbox"/> Backs up my IP phones					
<input type="checkbox"/> Backs up my hunt groups					
<input type="checkbox"/> Backs up my voicemail					
<input type="checkbox"/> Backs up my IP DECT phones					
Description					

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

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

Configuration

IP Office Line - Line 1

Line Short Codes **VoIP Settings**

Out Of Band DTMF ☒ Allow Direct Media Path ☒

Codec Selection **System Default**

Unused

Selected

G.711 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

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 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 5.4.4**.
- On the **Incoming Number**, enter one of the DID numbers provided by CenturyLink, notice the DID number is preceded with “+1”. When the destination is a user’s extension, the **Incoming Number** can be used to construct the “From” and “Contact” headers to be used in place of the extension number in the outgoing SIP INVITE for that user.
- Default values may be used for all other parameters.

The screenshot displays the IP Office Configuration interface. On the left is the 'Configuration' tree, and on the right is the 'Details' pane for the selected item.

Configuration Tree (Left):

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - System (1)
 - Line (3)
 - Control Unit (9)
 - Extension (6)
 - User (7)
 - Group (0)
 - Short Code (2)
 - Service (0)
 - Incoming Call Route (6)**
 - 17 +14691238606** (highlighted with a red box)
 - 17 +14691238607
 - 17 +14691238608
 - 17 +14691238609
 - 17 +14691238610
 - 17 +14691238611
 - IP Route (3)
 - License (33)
 - ARS (1)
 - Location (1)
 - Authorization Code (0)
 - IP500V2-One
 - IP500V2-Two

Details Pane (Right):

The title bar shows '17 +14691238606'. The 'Standard' tab is selected. The following fields are visible:

- Bearer Capacity:** Any Voice (dropdown menu)
- Line Group ID:** 17 (dropdown menu)
- Incoming Number:** +14691238606 (text field)
- Incoming Sub Address:** (empty text field)
- Incoming CLI:** (empty text field)
- Locale:** (empty dropdown menu)
- Priority:** 1 - Low (dropdown menu)
- Tag:** (empty text field)
- Hold Music Source:** System Source (dropdown menu)
- Ring Tone Override:** None (dropdown menu)

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 **+14691238606** provided by CenturyLink was associated with the Avaya IP Office extension **3041**.

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view of the configuration hierarchy. The 'Incoming Call Route (6)' folder is expanded, and the entry '17 +14691238606' is selected and highlighted with a red box. On the right, the configuration details for this route are shown. The 'Destinations' tab is active and highlighted with a red box. Below the tab is a table with the following data:

TimeProfile	Destination	Fallback Extension
Default Value	3041 Ext3041 H323	

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

5.7. Outbound Call Routing

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

5.7.1. Short Codes and Automatic Route Selection

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'Configuration' tree, and on the right is the '9N: Dial' configuration panel.

Configuration Tree (Left):

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary**
 - System (1)
 - Line (3)
 - Control Unit (9)
 - Extension (6)
 - User (7)
 - Group (0)
 - Short Code (2)**
 - 9N**
 - Service (0)
 - Incoming Call Route (5)
 - IP Route (3)
 - License (33)
 - ARS (1)
 - Location (1)
 - Authorization Code (0)
 - IP500V2-One
 - IP500V2-Two

9N: Dial Configuration Panel (Right):

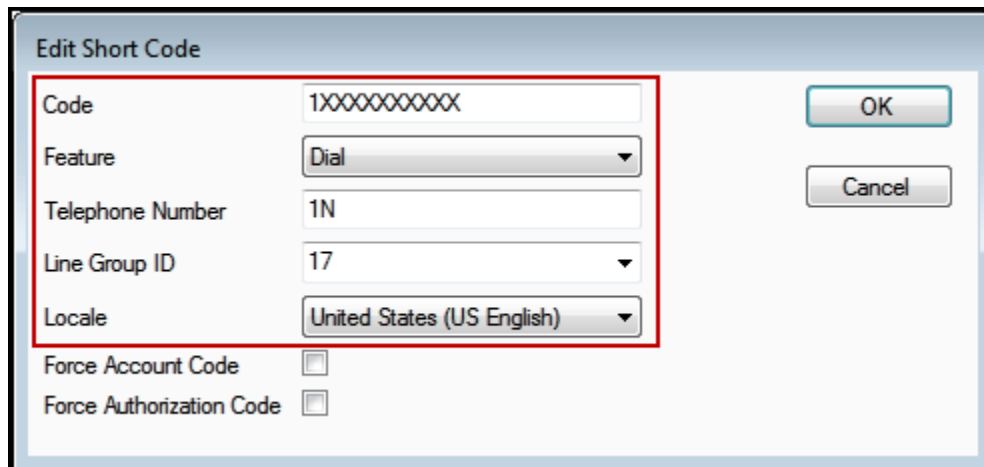
Short Code	
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	50: Main
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

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

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

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **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.



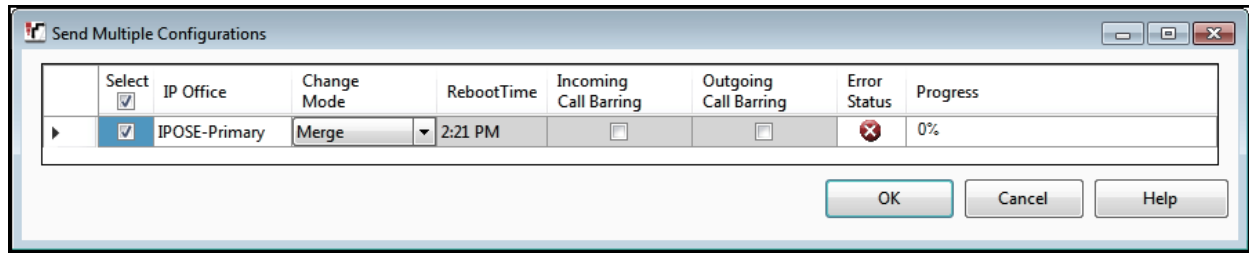
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

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.



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.

Configuration	System Inventory
<ul style="list-style-type: none">BOOTP (8)Operator (3)Solution<ul style="list-style-type: none">User(56)Group(2)Short Code(48)Directory(0)Time Profile(0)Account Code(0)User Rights(9)Location(1)IPOSE-PrimaryIP500V2-OneSystem (1)Line (3)Control Unit (4)Extension (24)User (27)Group (1)Short Code (12)Service (0)RAS (1)Incoming Call Route (2)WAN Port (0)Firewall Profile (1)IP Route (4)License (1)Tunnel (0)ARS (2)Location (1)Authorization Code (0)IP500V2-Two	<h3>Server Edition Expansion System</h3> <ul style="list-style-type: none">Hardware Installed<ul style="list-style-type: none">Control Unit: IP 500 V2Internal Modules: VCM64/PRID U; PHONE8Expansion Modules: DIG DCPx16 V2System Settings<ul style="list-style-type: none">IP Address: 192.168.128.165Sub-Net Mask: 255.255.255.0System Locale: United States (US English)System Location: 3: Thornton, CODevice ID: NONENumber of Extensions on System: 24Features Configured<ul style="list-style-type: none">Licenses Installed: Server Edition(1)Connected Extensions: 3043; 3044Users NOT Configured for Voicemail: NONEUsers assigned as Ex-Directory: NONEUsers assigned for Twinning: NONEUsers barred from making Outgoing Calls: NONEMusic on Hold: WAV File

6.1. Physical Hardware

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

Configuration

- BOOTP (8)
- Operator (3)
- Solution
 - User(56)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - IP500V2-One
 - System (1)
 - Line (3)
 - Control Unit (4)
 - 1 IP 500 V2
 - 2 VCM64/PRID U
 - 3 PHONE8
 - 6 DIG DCPx16 V2
 - Extension (24)
 - User (27)
 - Group (1)
 - Short Code (12)
 - Service (0)
 - RAS (1)
 - Incoming Call Route (2)
 - WAN Port (0)
 - Firewall Profile (1)
 - IP Route (4)
 - License (1)
 - Tunnel (0)
 - ARS (2)
 - Location (1)
 - Authorization Code (0)
- IP500V2-Two

IP 500 V2

Unit

Device Number	1
Unit Type	IP 500 V2
Version	11.0.4.1.0 build 11
Serial Number	
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).

The screenshot displays the configuration interface for the IP500V2-One system. On the left is the 'Configuration' navigation pane, which lists various system components. The 'IP500V2-One' component is selected, and its sub-item 'System (1)' is highlighted. The main area on the right shows the 'IP500V2-One' configuration details. The 'LAN1' tab is active, and the 'LAN Settings' sub-tab is selected. The 'IP Address' is set to 192.168.128.165 and the 'IP Mask' is set to 255.255.255.0. Other settings include 'Primary Trans. IP Address' (0.0.0.0), 'RIP Mode' (None), 'Enable NAT' (unchecked), 'Number Of DHCP IP Addresses' (200), and 'DHCP Mode' (Disabled). An 'Advanced' button is visible at the bottom right of the configuration area.

IP500V2-One							
System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events
LAN Settings		VoIP	Network Topology				
IP Address	192 . 168 . 128 . 165						
IP Mask	255 . 255 . 255 . 0						
Primary Trans. IP Address	0 . 0 . 0 . 0						
RIP Mode	None						
<input type="checkbox"/> Enable NAT							
Number Of DHCP IP Addresses	200						
DHCP Mode							
<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dial In <input checked="" type="radio"/> Disabled							
<button>Advanced</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 **192.168.128.200**
- Set **Destination** to **LAN1** from the pull-down menu.

Configuration	
0.0.0.0	
IP Route	
IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	192 . 168 . 128 . 200
Destination	LAN1
Metric	0
<input type="checkbox"/> Proxy ARP	

6.4. IP Office Line – IP500 V2 Expansion System

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

The screenshot displays the 'IP Office Line - Line 17' configuration window. On the left is a 'Configuration' navigation pane with a tree view. The 'Line' tab is selected in the top navigation bar. The main configuration area is divided into several sections:

- Line Information:** Line Number (17), Telephone Number (empty), Transport Type (WebSocket Client), Prefix (empty), Networking Level (SCN), Security (Medium), and Outgoing Group ID (99999).
- Gateway:** Address (10 . 64 . 101 . 127), Port (443), Location (3: Thornton, CO), Password (masked), and Confirm Password (masked).
- SCN Resiliency Options:** Includes checkboxes for 'Supports Resiliency', 'Backs up my IP phones', 'Backs up my hunt groups', and 'Backs up my IP DECT phones'.
- Description:** A text field for the line's description.

The 'Configuration' pane on the left shows a hierarchy: BOOTP (8), Operator (3), Solution, User (56), Group (2), Short Code (48), Directory (0), Time Profile (0), Account Code (0), User Rights (9), Location (1), IPOSE-Primary, IP500V2-One, System (1), Line (3), Control Unit (4), Extension (24), User (27), Group (1), Short Code (12), Service (0), RAS (1), Incoming Call Route (2), WAN Port (0), Firewall Profile (1), IP Route (4), License (1), Tunnel (0), ARS (2), Location (1), Authorization Code (0), and IP500V2-Two. The 'Line (3)' item is highlighted.

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**.
- Under **Media Security Preferred** was selected.

The screenshot displays the 'IP Office Line - Line 17' configuration window, specifically the 'VoIP Settings' tab. The left sidebar shows a tree view of the configuration hierarchy, with 'Line (3)' selected. The main area contains several settings:

- Codec Selection:** A dropdown menu set to 'System Default'. Below it, a list of selected codecs is shown: G.711 ULAW 64K, G.711 ALAW 64K, G.729(a) 8K CS-ACELP, and G.723.1 6K3 MP-MLQ.
- Fax Transport Support:** A dropdown menu set to 'T38 Fallback'.
- Call Initiation Timeout (s):** A numeric field set to 4.
- Media Security:** A dropdown menu set to 'Preferred'.
- Advanced Media Security Options:** A section with several checkboxes and a text field:
 - Same As System:** Checked.
 - Encryptions:** RTP (checked), RTCP (unchecked).
 - Authentication:** RTP (checked), RTCP (checked).
 - Replay Protection:** SRTP Window Size set to 64.
 - Crypto Suites:** SRTP_AES_CM_128_SHA1_80 (checked), SRTP_AES_CM_128_SHA1_32 (unchecked).
- Other Settings:**
 - VoIP Silence Suppression:** Unchecked.
 - Out Of Band DTMF:** Checked.
 - Allow Direct Media Path:** Checked.

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.
- Default values may be used for all other parameters.

Configuration

IP Office Line - Line 17

Line Short Codes VoIP Settings **T38 Fax**

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.

The screenshot displays the Avaya configuration interface. On the left, a tree view shows the configuration hierarchy. The 'Short Code (12)' is selected under the 'IP500V2-One' node. On the right, the 'Short Code' configuration page is shown for '9N: Dial'. The configuration details are as follows:

Short Code	
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	51: To-Primary
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

6.6. Automatic Route Selection – ARS

The following screen shows an example ARS configuration for the route named “**To-Primary**” on the Expansion System. The **Telephone Number** is set to **9N**. The **Line Group ID** is set to “**99999**” matching the number of the **Outgoing Group ID** configured on the IP Office Line 17 to the Primary server (**Section 6.4**).

Configuration

To-Primary

ARS

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

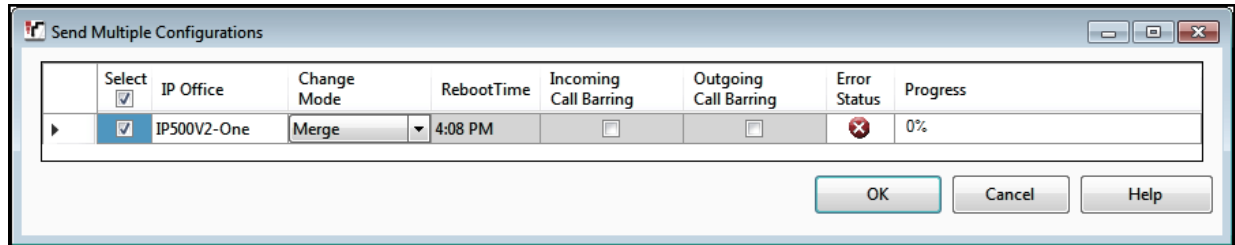
Alternate Route: <None>

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.



7. CenturyLink Voice Complete SIP Trunking Service on the Broadsoft Platform Configuration

To use CenturyLink Voice Complete 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 Voice Complete 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:

- Public IP address of CenturyLink's SIP Proxy server.
- DID numbers, etc.

8. Verification Steps

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

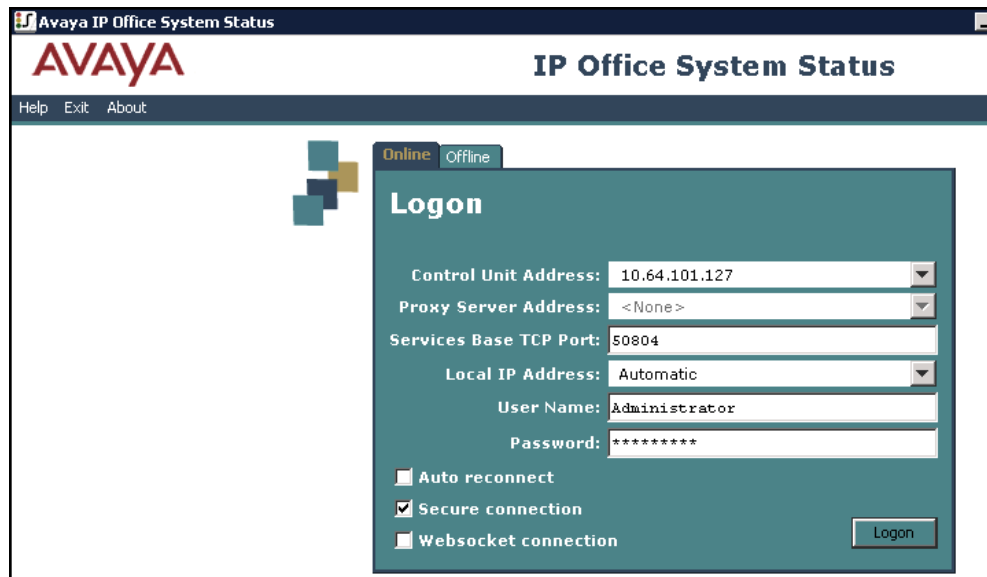
The following steps may be used to verify the configuration:

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

8.1. IP Office System Status

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

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



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

Avaya IP Office System Status - IPOSE-Primary (10.64.101.127) - IP Office Linux PC 11.0.4.1.0 build 11

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System
Alarms (15)
Extensions (4)
Trunks (3)
 Line: 1
 Line: 2
Line: 17
Active Calls
Resources
Voicemail
IP Networking
Locations

Status Utilization Summary Alarms

SIP Trunk Summary

Line Service State: In Service
 Peer Domain Name: sip:// 14.97
 Resolved Address: 14.97
 Line Number: 17
 Number of Administered Channels: 10
 Number of Channels in Use: 0
 Administered Compression: G711 Mu, G711 A, 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: 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	4 da...											
3			Idle	7 da...											
4			Idle	7 da...											
5			Idle	7 da...											
6			Idle	7 da...											
7			Idle	7 da...											
8			Idle	7 da...											
9			Idle	7 da...											
10			Idle	7 da...											

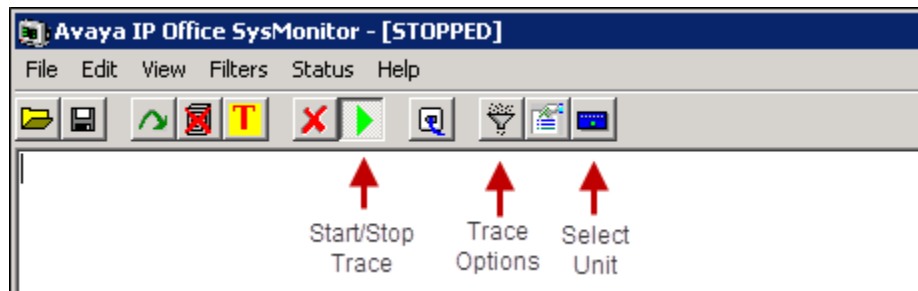
Trace Trace All Pause Ping Call Details Graceful Shutdown

Force Out of Service Print... Save As...

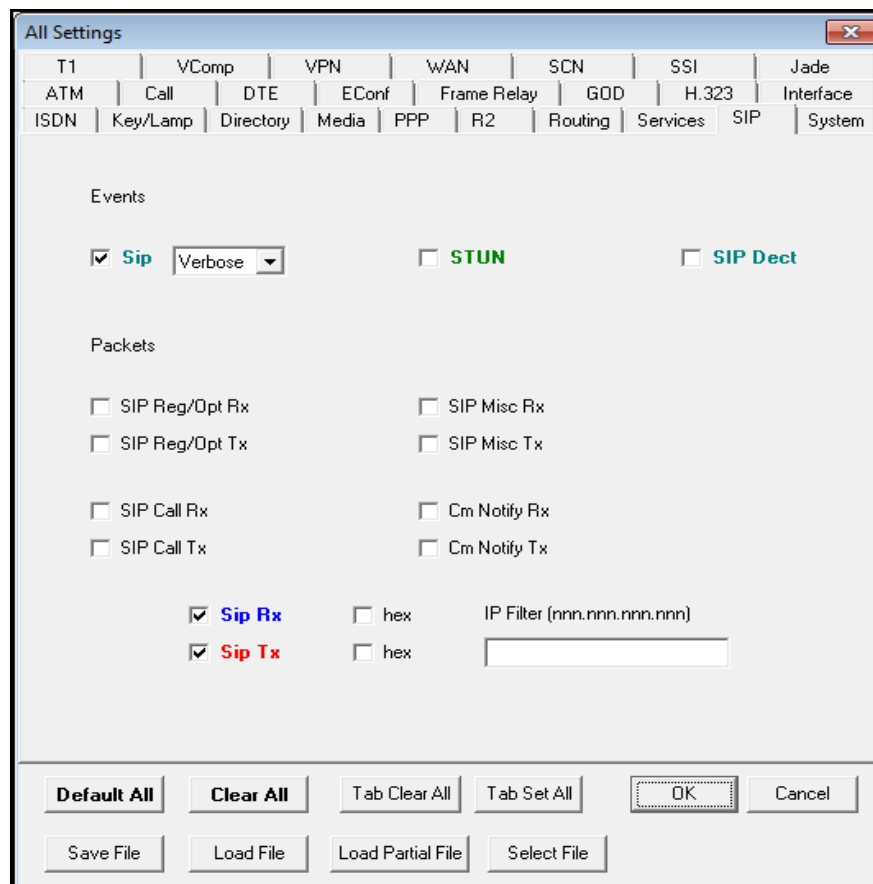
2:31:00 PM Online

8.2. Monitor

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



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



9. Conclusion

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

©2019 Avaya Inc. All Rights Reserved.

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

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