



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the CenturyLink IQ® SIP Trunk Service with Avaya IP Office Release 9.1 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking for an enterprise solution using Avaya IP Office Release 9.1 to interoperate with the CenturyLink IQ® SIP Trunk Service.

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

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

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking for an enterprise solution using Avaya IP Office Release 9.1 to interoperate the CenturyLink IQ® SIP Trunk Service.

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

2. General Test Approach and Test Results

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

The CenturyLink IQ® SIP Trunk Service passed compliance testing with any observations or limitations described in **Section 2.2**.

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

2.1. Interoperability Compliance Testing

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

- Establishment and registration of the SIP trunk
- Sending/receiving SIP OPTIONS queries to/from the service provider
- Incoming PSTN calls (via the CenturyLink SIP trunk) to SIP and H.323 telephones at the enterprise
- Outgoing PSTN calls (via the CenturyLink SIP trunk) from SIP and H.323 telephones at the enterprise
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows
- Various call types including: local (10 digits), long distance (1 + 10 digits), outbound toll-free, international (011 + country code + number) and local directory assistance (411)
- Codecs G.711MU and G.729A
- Caller ID presentation and Caller ID restriction
- DTMF transmission using RFC 2833
- Response to incomplete call attempts and trunk errors
- Voicemail navigation using DTMF input for inbound and outbound calls
- Voicemail message waiting indicator (MWI)

- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and twinning
- T.38 and G.711 fax

Emergency calls (911) and inbound toll-free calls are supported but were not tested as part of the compliance test.

2.2. Test Results

Interoperability testing of the CenturyLink IQ® SIP Trunk Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **CenturyLink does not support REFER for call forward:** The call scenario is an inbound call from the PSTN to Avaya IP Office which is then forwarded to another PSTN endpoint. In this scenario, if REFER is enabled (**Section 5.4.2**), CenturyLink returns a failure to the REFER message. The call is still successful because on receipt of the failure message, Avaya IP Office stays in the middle of the call. However, the Avaya IP Office trunk will not be released until the call is terminated.
- **Call forwarding of a privacy call fails:** The call scenario is the same as in the previous bullet item except the inbound call has calling party number block (aka privacy) enabled. CenturyLink sends a 403 Forbidden or a 606 Not Acceptable response on the forwarded call leg and the call is terminated. This occurs with REFER enabled or disabled. However, since the completion of this testing, CenturyLink has reported that this issue has been corrected.
- **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 5.4.7**).
- **SIP Line should be taken out of service before making changes:** Certain changes to the Avaya IP Office SIP Line configuration will cause the Avaya IP Office to unregister and reregister the SIP Line in rapid succession. Depending on the arrival of the messaging at the far-end, the trunk may end-up unregistered. As a workaround, the Avaya IP Office SIP Line should be taken out of service prior to making changes on the SIP Line and then placed back in service once the changes are complete. This is unrelated to CenturyLink interoperability.
- **SIP endpoints may indicate that a transfer failed even when it is successful:** Occasionally on performing a transfer operation, Avaya IP Office SIP endpoints (Avaya 1100 Series Deskphone and Avaya Communicator for Windows) 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 IPO SIP Line (**Section 5.4.8**).

2.3. Support

For technical support on the CenturyLink IQ® SIP Trunk Service, please contact CenturyLink via the following:

- Web: <http://www.centurylink.com>
- Enterprise Business Support: 1-888-638-6771

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The sample configuration shows an enterprise site connected to the CenturyLink IQ® SIP Trunk Service.

The enterprise site contains an Avaya IP Office 500 V2 with various endpoints and a Windows 7 PC running Avaya IP Office Manager to configure Avaya IP Office. This PC also runs Avaya VoiceMail Pro for voicemail. For the compliance test, Avaya IP Office is deployed in a 2-port configuration. The Avaya IP Office LAN1 port is connected to the private enterprise LAN and the WAN (LAN2) port is connected to the public network.

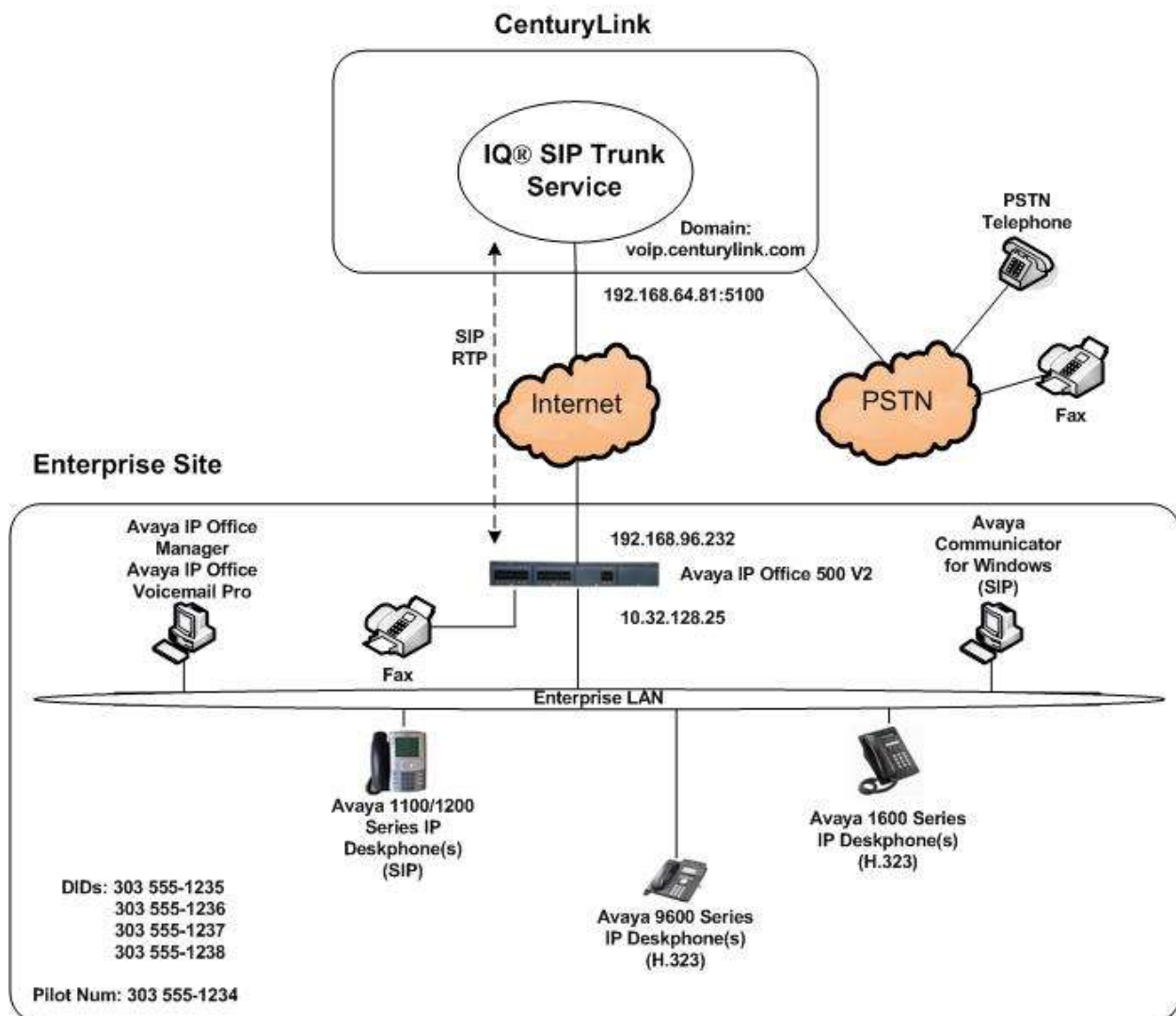


Figure 1: Avaya Interoperability Test Lab Configuration

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

For the purposes of the compliance test, users dialed a short code of 9 + N digits to send digits across the SIP trunk to CenturyLink. The short code of 9 is stripped off by Avaya IP Office and the remaining digits were sent unaltered to CenturyLink. CenturyLink accepts 11 digits in the Request-URI header for long distance and local calls. For inbound calls, CenturyLink sends 10 digits in the Request-URI.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment	Software
Avaya IP Office 500 v2	9.1 SP2 (9.1.2.0.91)
Avaya IP Office Manager	9.1 SP2 (9.1.2.0.91)
Avaya IP Office VoiceMail Pro	9.1 SP2 (9.1.2.0.61)
Avaya 1140E IP Deskphone (SIP)	4.4 SP2 (4.04.18)
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3.6 (1.3.60A)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.6.0 (6.6.0.29)
Avaya Communicator for Windows	2.0.3.30

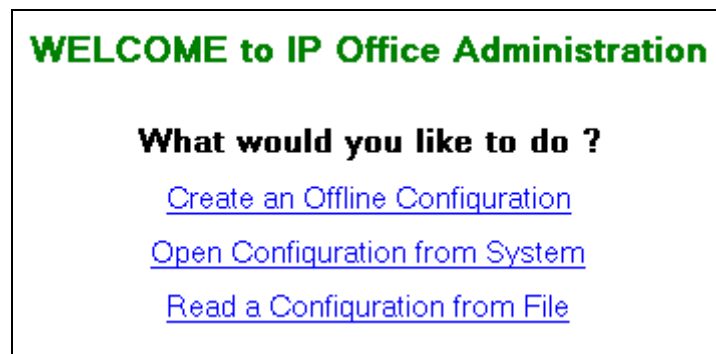
CenturyLink Components	
Equipment	Software
BroadSoft BroadWorks	20.0_1.606
Oracle Net-Net 6300 Session Border Controller	SCZ7.1.2 MR-3 GA (Build 359)

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 without T.38 Fax Service.

Avaya IP Office Server Edition requires an Expansion IP Office 500 V2 R9 to support analog/digital endpoints or analog/digital trunks.

5. Configure Avaya IP Office

Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the Avaya IP Office Manager PC, select **Start → All Programs → IP Office → Manager** to launch the application. A screen that includes the following may be displayed:



Select **Open Configuration from System**. If the above screen does not appear, the configuration may be alternatively opened by navigating to **File → Open Configuration** at the top of the Avaya IP Office Manager window. Select the proper Avaya IP Office system from the pop-up window and log in with the appropriate credentials.

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

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

5.1. Licensing and Physical Hardware

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, which lists various system components and their counts. The 'License' component is highlighted with a blue selection bar. The main area on the right is the 'License' details pane, which has a 'Remote Server' tab selected. This pane shows license information including 'License Mode' (License Normal), 'Licensed Version' (9.1), 'Serial Number (ADI)', 'PLDS Host ID', and 'PLDS File Status' (Not Present / Invalid). Below this information is a table listing installed features, their license keys, the number of instances, and their status. The 'SIP Trunk Channels' row is highlighted with a red border, showing 255 instances in a 'Valid' status. To the right of the table are 'Add...' and 'Remove' buttons.

Feature	License Key	Instances	Status
IP500 Voice Networking Channels	...	4	Valid
VCM Channel Migration	...	255	Valid
SIP Trunk Channels	...	255	Valid
VPN IP Extensions	...	255	Obsolete
IP500 Universal PRI (Additional cha...	...	255	Valid
RAS LRQ Support (Rapid Response)	...	255	Valid

To view the physical hardware comprising Avaya IP Office, expand the components under the **Control Unit** in the Navigation pane. In the sample configuration, the second component listed is a Combination Card. This module has 6 digital stations ports, two analog extension ports, 4 analog trunk ports and 10 VCM channels. The VCM is a Voice Compression Module supporting VoIP codecs. An Avaya IP Office hardware configuration with a VCM component is necessary to support SIP trunking.

To view the details of the component, select the component in the Navigation pane. The following screen shows the details of the **IP 500 V2**.

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, and on the right is the 'IP 500 V2' details pane.

IP Offices Navigation Pane:

- BOOTP (2)
- Operator (3)
- Atlantic City
 - System (1)
 - Line (21)
 - Control Unit (3)
 - 1 IP 500 V2** (selected)
 - 2 COMBO6210/ATM4
 - 3 DIGSTA8/ATM4
 - Extension (25)
 - User (27)
 - Group (1)
 - Short Code (64)
 - Service (0)
 - RAS (1)
 - Incoming Call Route (57)

IP 500 V2 Details Pane:

Unit	
Device Number	1
Unit Type	IP 500 V2
Version	9.1.200.91
Serial Number	
Unit IP Address	10.32.128.25
Interconnect Number	0
Module Number	Control Unit

5.2. System

Configure the necessary system settings.

5.2.1. System – LAN2 Tab

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

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view under 'IP Offices' containing various system components like BOOTP, Operator, Atlantic City, System, Line, Control Unit, Extension, User, Group, Short Code, Service, RAS, Incoming Call Route, WAN Port, Directory, Time Profile, Firewall Profile, IP Route, Account Code, and License. The main pane is titled 'Atlantic City' and contains several tabs: SMDR, Twinning, VCM, Codecs, VoIP Security, Contact Center, System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, and SMTP. The 'LAN2' tab is selected, and within it, the 'LAN Settings' sub-tab is active. The configuration fields are as follows:

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

An 'Advanced' button is located at the bottom right of the configuration area.

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

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

The screenshot displays the 'Atlantic City' configuration window with the 'VoIP' tab selected. The 'LAN Settings' sub-tab is active, showing various configuration options. The 'H323 Gatekeeper Enable' checkbox is checked, and the 'Remote Call Signalling Port' is set to 1720. The 'SIP Trunks Enable' checkbox is also checked. Below this, the 'SIP Registrar Enable' checkbox is checked, and the 'Auto-create Extn/User' checkbox is unchecked. The 'Domain Name' field is empty. The 'Layer 4 Protocol' section shows 'UDP' and 'TCP' both checked, with 'TLS' unchecked. The 'Challenge Expiry Time (secs)' is set to 10. The 'RTP' section shows the 'Port Number Range' and 'Port Number Range (NAT)' both set with a minimum of 49152 and a maximum of 53246. The 'Remote UDP Port', 'Remote TCP Port', and 'Remote TLS Port' are all set to 5060.

Section	Parameter	Value
H323 Gatekeeper	H323 Gatekeeper Enable	Checked
	Auto-create Extn	Unchecked
	Auto-create User	Unchecked
	H323 Remote Extn Enable	Unchecked
Remote Call Signalling	Remote Call Signalling Port	1720
SIP Trunks	SIP Trunks Enable	Checked
SIP Registrar	SIP Registrar Enable	Checked
	Auto-create Extn/User	Unchecked
SIP Remote Extn	SIP Remote Extn Enable	Unchecked
Domain Name	Domain Name	
Layer 4 Protocol	UDP	Checked
	TCP	Checked
	TLS	Unchecked
Challenge Expiry Time (secs)	Challenge Expiry Time (secs)	10
RTP Port Number Range	Minimum	49152
	Maximum	53246
RTP Port Number Range (NAT)	Minimum	49152
	Maximum	53246
Remote Ports	Remote UDP Port	5060
	Remote TCP Port	5060
	Remote TLS Port	5060

Scroll down the page.

- In the **Keepalives** section, set the **Scope** to **RTP**. Set the periodic timeout to **30** and the **Initial Keepalives** parameter to **Enabled**. These settings will cause Avaya IP Office to send a RTP keepalive packet starting at the time of initial connection and every 30 seconds thereafter if no other RTP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting to see media from the other, as well as helping to keep firewall ports open for the duration of the call.
- In the **DiffServ Settings** section, Avaya IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for both signaling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling. The specific values used for the compliance test were the Avaya IP Office default values and are shown in the screenshot below. Quality of Service (QoS) is not specifically tested as part of the compliance test. For a customer installation, the **DSCP** and **SIG DSCP** fields should be set to values provided by CenturyLink. CenturyLink uses a DSCP value of 40 (decimal) for media and a SIG DSCP value of 24 (decimal) for signaling.
- All other parameters should be set according to customer requirements.

Atlantic City

Contact Center

System LAN1 LAN2 DNS Voicemail Telephony Directory Services System Events SMTP SMDR Twinning VCM Codecs VoIP Security

LAN Settings VoIP Network Topology

☒ Enable RTCP Monitoring on Port 5005

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

Keepalives

Scope RTP 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

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

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. Since no firewall or network address translation (NAT) device was used between the Avaya IP Office and the public network, the parameter was set to **Open Internet**.
- Set **Binding Refresh Time (seconds)** to **300**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider.
- Set the **Public IP Address** to the IP address assigned to the Avaya IP Office WAN port in the **LAN2→LAN Settings** form earlier in this section.
- In the **Public Port** section, next to the transport protocol **UDP**, select the UDP port on which Avaya IP Office will listen.
- All other parameters should be set according to customer requirements.

The screenshot shows the Avaya IP Office configuration interface for a system named "Atlantic City". The "Network Topology" tab is selected. The "Network Topology Discovery" section contains the following fields and values:

- STUN Server Address: 10.90.168.13
- STUN Port: 3478
- Firewall/NAT Type: Open Internet
- Binding Refresh Time (seconds): 300
- Public IP Address: 192 . 168 . 96 . 232
- Public Port section:
 - UDP: 5060
 - TCP: 0
 - TLS: 0
- ☐ Run STUN on startup

Buttons for "Run STUN" and "Cancel" are located to the right of the Public IP Address field.

5.2.2. System - Telephony Tab

To access the System Telephony settings, navigate to the **Telephony** → **Telephony** tab in the Details Pane. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN. If for security reasons incoming calls should not be allowed to transfer back to the PSTN then leave this setting checked.

The screenshot displays the 'Atlantic City' system configuration window, specifically the 'Telephony' tab. The interface is divided into several sections:

- Analogue Extensions:** Includes dropdown menus for 'Default Outside Call Sequence' (Normal), 'Default Inside Call Sequence' (Ring Type 1), and 'Default Ring Back Sequence' (Ring Type 2). There is also a checkbox for 'Restrict Analogue Extension Ringer Voltage'.
- Comping Law:** Contains two sub-sections, 'Switch' and 'Line', each with radio buttons for 'U-Law' (selected) and 'A-Law'.
- System Parameters:** A list of settings with spinners or dropdowns, including 'Dial Delay Time (secs)' (4), 'Dial Delay Count' (0), 'Default No Answer Time (secs)' (25), 'Hold Timeout (secs)' (0), 'Park Timeout (secs)' (300), 'Ring Delay (secs)' (5), 'Call Priority Promotion Time (secs)' (Disabled), 'Default Currency' (USD), 'Default Name Priority' (Favor Trunk), 'Media Connection Preservation' (Disabled), and 'Phone Failback' (Manual).
- Login Code Complexity:** A section with checkboxes for 'Enforcement' and 'Complexity', and a 'Minimum length' spinner set to 4.
- Advanced Settings:** A list of checkboxes on the right side, including 'DSS Status', 'Auto Hold', 'Dial By Name', 'Show Account Code', 'Inhibit Off-Switch Forward/Transfer' (unchecked), 'Restrict Network Interconnect', 'Include location specific information', 'Drop External Only Impromptu Conference', 'Visually Differentiate External Call', 'Unsupervised Analog Trunk Disconnect Handling', 'High Quality Conferencing', 'Digital/Analogue Auto Create User', and 'Directory Overrides Barring'.

5.2.3. System - Twinning Tab

To view or change the System Twinning settings, navigate to the **Twinning** tab in the Details Pane as shown in the following screen. The **Send original calling party information for Mobile Twinning** box is not checked in the sample configuration, and the **Calling party information for Mobile Twinning** is left blank. Click the **OK** button at the bottom of the page (not shown).

The screenshot shows the 'Atlantic City' configuration window with the 'Twinning' tab selected. The 'Send original calling party information for Mobile Twinning' checkbox is unchecked. Below it, the 'Calling party information for Mobile Twinning' field is empty.

5.3. IP Route

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

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

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

The screenshot shows the 'IP Office' configuration window with the 'IP Route' tab selected for the route '0.0.0.0'. The 'IP Address' and 'IP Mask' fields are both set to '0 . 0 . 0 . 0'. The 'Gateway IP Address' field is set to '192 . 168 . 96 . 254'. The 'Destination' dropdown menu is set to 'LAN2'. The 'Metric' field is set to '0'. The 'Proxy ARP' checkbox is unchecked.

5.4. SIP Line

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

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2 – 5.4.8**.

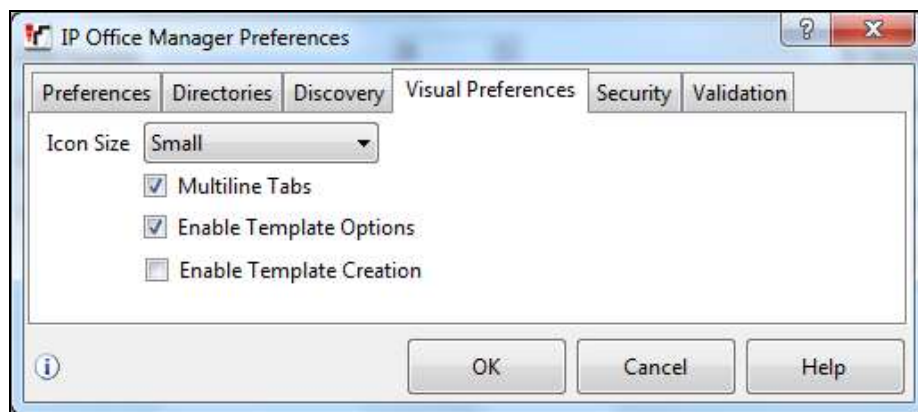
Also, the following SIP Line settings are not supported on Basic Edition:

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

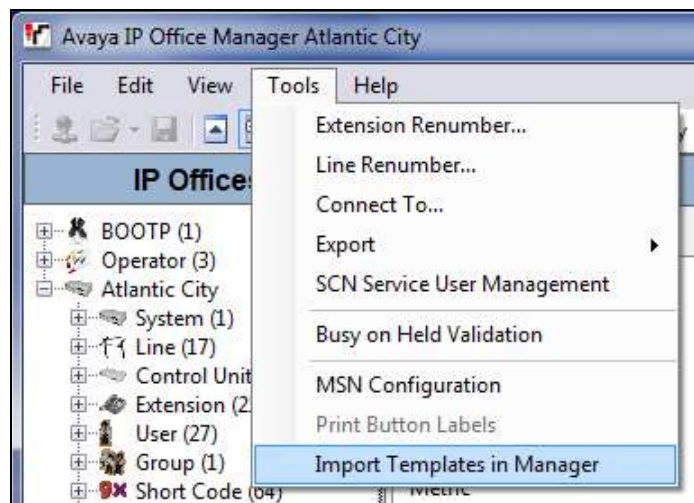
To create a SIP Line manually, right-click **Line** in the Navigation Pane and select **New → SIP Line**; then, follow the steps outlined in **Sections 5.4.2 – 5.4.8**.

5.4.1. SIP Line From Template

1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to a name with the following format **AF_<user_supplied_text>_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**. The example used in these Application Notes is **AF_CenturyLink-noSBCE_SIPTrunk.xml**.
2. Verify that template options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the Visual Preferences tab. Verify that the box is checked next to **Enable Template Options**. Click **OK**.

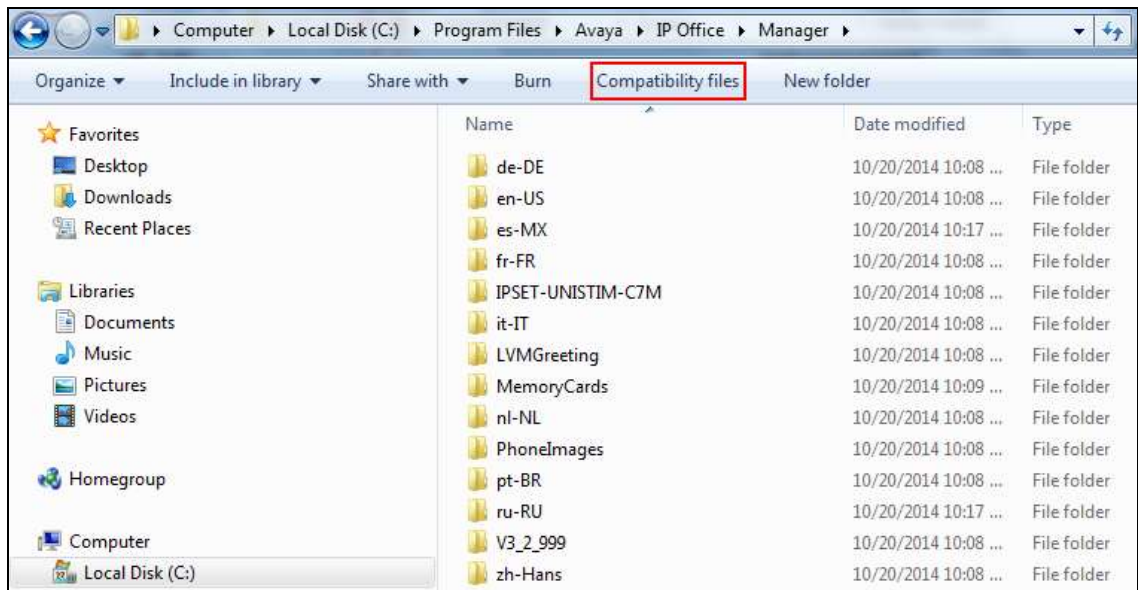


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.

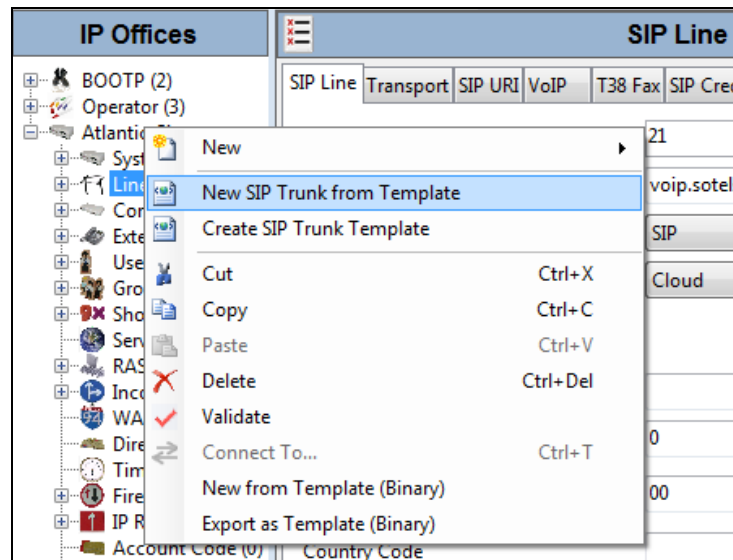


In the pop-up window that appears (not shown), select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window will appear stating success or failure (not shown). Click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

Note –Windows 7 (and later) locks the Avaya IP Office 9.1 \Templates directory, and it cannot be viewed. To enable browsing of the \Templates directory, open Windows Explorer, navigate to **C:\Program Files\Avaya\IP Office\Manager** (or *C:\Program Files (x86)\Avaya\IP Office\Manager*), and then click on the **Compatibility files** option shown below. The \Templates directory and its contents can then be viewed.



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



5. In the subsequent Template Type Selection pop-up window, use the **Service Provider** pull-down menu to select the XML template file created in **Step 1**. This menu will display the *<user_supplied_text>* portion of the file name of each template located in the directory. Select the entry that corresponds to the desired file name. In the case of this example, **CenturyLink-noSBCE** was selected, corresponding to a file name of **AF_CenturyLink-noSBCE_SIPTrunk.xml**. Click **Create new SIP Trunk** to finish creating the trunk.



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

5.4.2. SIP Line – SIP Line Tab

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

- Set **ITSP Domain Name** to the domain name provided by CenturyLink.
- Check the **In Service** box. This makes the trunk available to incoming and outgoing calls.
- Check the **Check OOS** box. Avaya IP Office will use the SIP OPTIONS method to periodically check the SIP Line. The time between SIP OPTIONS sent by Avaya IP Office will use the **Binding Refresh Time** for LAN2, as shown in **Section 5.2.1**.
- Set the **Refresh Method** to **Auto** and the **Timer (seconds)** to **600**. This will cause Avaya IP Office to send an UPDATE message every 300 seconds (1/2 the **Timer** value) to check the state of each active session.
- Set **Send Caller ID** to **Diversion Header**. With this setting and the related configuration in **Section 5.2.3**, Avaya IP Office will include the Diversion Header for calls that are directed via Mobile Twinning out the SIP Line to CenturyLink. It will also include the Diversion Header for calls that are call forwarded out the SIP Line.
- CenturyLink supports REFER except for call forward. REFER may still be enabled on Avaya IP Office; however, for call forwarding, the call will succeed but the Avaya IP Office SIP trunk will not be released until the call is terminated (**Section 2.2**). To enable REFER, under **Redirect and Transfer**, set the **Incoming Supervised REFER** field and **Outgoing Supervised REFER** field to **Always**. To disable, set these fields to **Never**.
- Default values may be used for all other parameters.

The screenshot shows the Avaya IP Office configuration window for 'SIP Line - Line 29'. The left pane shows a tree view of configuration objects. The right pane has tabs for 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'SIP Line' tab is active, showing the following configuration:

Field	Value
Line Number	29
ITSP Domain Name	voip.centurylink.com
URI Type	SIP
Location	Cloud
Prefix	
National Prefix	0
International Prefix	00
Country Code	
Name Priority	System Default
Description	
In Service	<input checked="" type="checkbox"/>
Check OOS	<input checked="" type="checkbox"/>
Session Timers	
Refresh Method	Auto
Timer (seconds)	600
Forwarding and Twinning	
Originator number	
Send Caller ID	Diversion Header
Redirect and Transfer	
Incoming Supervised REFER	Always
Outgoing Supervised REFER	Always
Send 302 Moved Temporarily	<input type="checkbox"/>
Outgoing Blind REFER	<input type="checkbox"/>

5.4.3. SIP Line - Transport Tab

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

- Set the **ITSP Proxy Address** to the IP address of the CenturyLink SIP proxy provided by CenturyLink.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to the network port used by the SIP line to access the far-end and configured in **Section 5.2.1**.
- Set the **Send Port** to **5100**. This port number was provided by CenturyLink.
- Default values may be used for all other parameters.

The screenshot shows the 'SIP Line - Line 29' configuration window with the 'Transport' tab selected. The window has a title bar with standard icons and a tabbed interface. The 'Transport' tab is active, showing the following settings:

- ITSP Proxy Address:** 192.168.64.81
- Network Configuration:**
 - Layer 4 Protocol:** UDP (selected from a dropdown)
 - Send Port:** 5100 (spin box)
 - Use Network Topology Info:** LAN 2 (selected from a dropdown)
 - Listen Port:** 5060 (spin box)
- Explicit DNS Server(s):** Two groups of IP address fields, each containing '0 . 0 . 0 . 0'.
- Calls Route via Registrar:** ☒
- Separate Registrar:** An empty text field.

5.4.4. SIP Line – SIP Credentials

SIP Credentials are provided by CenturyLink for registration and authentication of the enterprise. To enter the SIP Credentials, select the **SIP Credentials** tab and click **Add**. In the **New SIP Credentials** area that appears, enter the information as shown below.

- Set the **User name** and **Contact** to the pilot number provided by CenturyLink.
- Set the **Authentication Name** to the user name provided by CenturyLink.
- Set the **Password** and **Confirm Password** to the password provided by CenturyLink.
- Set **Expiry (mins)** to **60**. This is the value recommended by CenturyLink.
- Check the **Registration required** box.

Click **OK**.

The screenshot shows a software window titled "SIP Line - Line 29*". It has a tabbed interface with tabs for "SIP Line", "Transport", "SIP URI", "VoIP", "T38 Fax", "SIP Credentials" (which is selected), "SIP Advanced", and "Engineering". Below the tabs is a table with columns: "Index", "UserName", "Authentication Name", "Contact", "Expiry (mins)", and "Register". To the right of the table are buttons for "Add...", "Remove", and "Edit...". Below the table is a section titled "New SIP Credentials" containing several input fields: "User name" (3035551234), "Authentication Name" (255727-3035551234), "Contact" (3035551234), "Password" (masked with dots), "Confirm Password" (masked with dots), "Expiry (mins)" (60), and a "Registration required" checkbox which is checked. To the right of these fields are "OK" and "Cancel" buttons.

5.4.5. SIP Line - SIP URI Tab

A SIP URI entry must be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. 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 is created. The entry was created with the parameters shown below:

- Set **Local URI** to **Use Internal Data**. The **Local URI** parameter controls which calls will be accepted by the system on this SIP URI and also defines the contents of the From header for outbound calls. The setting of **Use Internal Data** will enable the **User → SIP** tab for each Avaya IP Office user where the SIP information can be configured. The setting of **Use Internal Data** will allow inbound calls whose user portion of the incoming Request-URI matches a value configured on the system for a user (**User → SIP**), hunt group (**Hunt Group → SIP**) or voicemail (**System → Voicemail**). For outbound calls, the From header is populated with the **SIP Name** configured for the user (**Section 5.7**).
- Set **Contact**, and **Display Name** to **Use Internal Data**. This setting will populate each of these headers with the corresponding value from the **User → SIP** tab of the Avaya IP Office user involved in the call. See **Section 5.7**.
- Set **PAI** to **Use Credentials User Name**. CenturyLink requires the pilot number to appear as the user part of the URI in the PAI header. The pilot number is configured as the SIP Credentials User Name in **Section 5.4.4**.
- For the **Registration** field, select the credentials created in **Section 5.4.4** from the pull-down menu.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line in **Section 5.8.1**. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining ARS entries for routing outbound traffic to this line in **Section 5.5**. For the compliance test, a new incoming and outgoing group **29** was defined that only contained this line (line 29).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

Click **OK**.

SIP Line - Line 29*

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

Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls

Buttons: Add... Remove Edit...

New Channel

Via: 192.168.96.232

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

PAI: Use Credentials User Name

Registration: 1: 3035551234

Incoming Group: 29

Outgoing Group: 29

Max Calls per Channel: 10

Buttons: OK Cancel

Additional SIP URIs may be required to allow inbound calls to numbers not associated with a user, such as a short code. These URIs are created in the same manner as shown above with the exception that the incoming DID number is entered directly in the **Local URI**, **Contact**, and **Display Name** fields (i.e., all fields set to **Use Internal Data**).

5.4.6. SIP Line - VoIP Tab

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

- For **Codec Selection**, select **Custom** from the pull-down menu to use a custom list of codecs. Next, move unwanted codecs from the **Selected** column to the **Unused** column if needed. Lastly, move the codecs up or down the list in the **Selected** column to achieve the desired order of preference. The example below shows the codecs used for the compliance test. This codec order was used to match the codec order used by CenturyLink as close as possible.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box.
- Set the **Fax Transport Support** to **T38 Fallback**. In general, CenturyLink supports T.38 fax but not necessarily on all media gateways in the network. Using the **T38 Fallback** setting will allow all fax calls to succeed, though some may use G.711 fax instead of T.38.
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Default values may be used for all other parameters.

The screenshot shows the 'SIP Line - Line 29' configuration window with the 'VoIP' tab selected. The window has a tabbed interface with 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'VoIP' tab is active, displaying various settings. On the left, the 'Codec Selection' section shows a 'Custom' dropdown menu. Below it are two columns: 'Unused' (empty) and 'Selected' (containing G.729(a) 8K CS-ACELP, G.711 ULAW 64K, G.711 ALAW 64K, and G.723.1 6K3 MP-MLQ). Between these columns are buttons for moving codecs (>>>, <<<, up, down) and a '>>>' button at the bottom. On the right, a list of checkboxes includes 'VoIP Silence Suppression' (unchecked), 'Re-invite Supported' (checked), 'Codec Lockdown' (unchecked), 'Allow Direct Media Path' (unchecked), 'Force direct media with phones' (unchecked), 'PRACK/100rel Supported' (checked), and 'G.711 Fax ECAN' (checked). At the bottom, three dropdown menus are visible: 'Fax Transport Support' set to 'T38 Fallback', 'DTMF Support' set to 'RFC2833', and 'Media Security' set to 'Disabled'.

5.4.7. SIP Line – T38 Fax Tab

Select the **T38 Fax** tab. Set the parameters as shown below.

- Uncheck the **Use Default Values** box at the bottom of the page.
- Set the **T38 Fax Version** to **0**.
- Check the **Disable T30 ECM** box.

The screenshot shows the 'SIP Line - Line 29' configuration window with the 'T38 Fax' tab selected. The window has a title bar with standard icons and a tabbed interface with tabs for SIP Line, Transport, SIP URI, VoIP, T38 Fax, SIP Credentials, SIP Advanced, and Engineering. The T38 Fax tab is active, displaying various configuration fields. On the left, there are fields for T38 Fax Version (set to 0), Transport (set to UDPTL), a Redundancy section with Low Speed and High Speed (both set to 0), TCF Method (set to Trans TCF), Max Bit Rate (bps) (set to 14400), EFlag Start Timer (msecs) (set to 2600), EFlag Stop Timer (msecs) (set to 2300), and Tx Network Timeout (secs) (set to 150). On the right, there is a list of checkboxes: Scan Line Fix-up (checked), TFOP Enhancement (checked), Disable T30 ECM (checked), Disable EFlags For First DIS (unchecked), and Disable T30 MR Compression (unchecked). Below these is an NSF Override section with Country Code (set to 0) and Vendor Code (set to 0). At the bottom left, there is an unchecked checkbox for 'Use Default Values'.

Field	Value
T38 Fax Version	0
Transport	UDPTL
Low Speed	0
High Speed	0
TCF Method	Trans TCF
Max Bit Rate (bps)	14400
EFlag Start Timer (msecs)	2600
EFlag Stop Timer (msecs)	2300
Tx Network Timeout (secs)	150
Scan Line Fix-up	Checked
TFOP Enhancement	Checked
Disable T30 ECM	Checked
Disable EFlags For First DIS	Unchecked
Disable T30 MR Compression	Unchecked
Country Code	0
Vendor Code	0
Use Default Values	Unchecked

5.4.8. SIP Line – SIP Advanced

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

- Check the **Use Domain for PAI** box. CenturyLink requires the CenturyLink SIP domain to appear in URI of the PAI header. Avaya IP Office sends the public IP address of the Avaya IP Office in the PAI header even if a SIP domain is configured on the SIP Line (**Section 5.4.2**). To change this behavior, the **Use Domain For PAI** needs to be enabled. Without this setting, outbound privacy calls will fail and the calling party number for call forwarding to the PSTN and twinning will incorrectly show the pilot number instead of the original PSTN caller.
- Check the **Emulate NOTIFY for REFER** box. With REFER enabled (**Section 5.4.2**), the Avaya 1100 Series Deskphones and Avaya Communicator for Windows expects to receive a NOTIFY message to indicate that the referred (i.e., transferred) call was successful. If the NOTIFY is not received from the far-end, then the call display will indicate that the transfer failed even if the transfer was successful. If the **Emulate NOTIFY for REFER** box is checked, then Avaya IP Office will send a NOTIFY message (on behalf of the far-end) to the Avaya 1100 Series Deskphones and Avaya Communicator for Windows.

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

The screenshot shows the 'SIP Line - Line 29' configuration window with the 'SIP Advanced' tab selected. The window is divided into several sections:

- Addressing:** Association Method is set to 'By Source IP address', Call Routing Method is 'Request URI', and Suppress DNS SRV Lookups is unchecked.
- Identity:** A list of checkboxes includes 'Use Phone Context', 'Add user=phone', 'Use + for International', 'Use PAI for Privacy', 'Use Domain for PAI' (checked), 'Swap From and PAI', 'Caller ID from From header', 'Send From In Clear', 'Cache Auth Credentials' (checked), and 'User-Agent and Server Headers' (empty text box).
- Media:** Includes checkboxes for 'Allow Empty INVITE', 'Send Empty re-INVITE', 'Allow To Tag Change', 'P-Early-Media Support' (set to 'None'), 'Send SilenceSupp=Off', 'Force Early Direct Media', and 'Media Connection Preservation' (set to 'Disabled').
- Call Control:** Includes 'Call Initiation Timeout (s)' (4), 'Call Queuing Timeout (m)' (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' (unchecked), 'Emulate NOTIFY for REFER' (checked), and 'No REFER if using Diversion' (unchecked).

5.5. ARS

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

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

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

- In the **Code** field, enter the pattern to match the number passed to ARS from the short code in **Section 5.6** followed by a semi-colon. The value **N** will match any number.
- Set **Feature** to **Dial**. This is the action that the entry will perform.
- For **Code 0**, set **Telephone Number** to **0"@domain"**, where *domain* is the SIP domain provided by CenturyLink and used to configure the trunk in **Section 5.4.2**. Adding the domain in this field was required to ensure that the correct domain appeared in the outbound Request-URI header when dialing 0. This was not required when matching on any other dialed number as shown next.
- For **Code N**, set **Telephone Number** to **N**. This field is used to construct the Request-URI and To headers in the outgoing SIP INVITE message. The value **N** represents the complete number passed to ARS.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4.5**. This entry will use this line group when placing the outbound call.

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

Code	Telephone Number	Feature	Line Group ID
0	0"@voip.centurylink.com"	Dial	29
N	N	Dial	29

5.6. Short Codes

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

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **9N;** was used. This short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value is passed to ARS.
- Set the **Line Group ID** to the ARS route to be used (**Section 5.5**).

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

9N;; Dial	
Short Code	
Code	9N;
Feature	Dial
Telephone Number	N
Line Group ID	58: CenturyLink
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

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

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

The screenshot shows a configuration window titled "*67N;; Dial". The window has a toolbar with icons for save, delete, add, and navigation. The main area is labeled "Short Code" and contains the following fields:

Code	*67N;
Feature	Dial
Telephone Number	WN
Line Group ID	58: CenturyLink
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

5.7. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.4**. To configure these settings, first navigate to **User** → *Name* in the Navigation Pane where *Name* is the name of the user to be modified. In the example below, the name of the user is **Extn243**. Select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers for outgoing SIP trunk calls and allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.4.5**). The example below shows the settings for user **Extn243**. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise from CenturyLink. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network.

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

IP Offices		Extn243: 243	
<ul style="list-style-type: none">BOOTP (2)Operator (3)Atlantic City<ul style="list-style-type: none">System (1)Line (22)Control Unit (3)Extension (25)User (27)Group (1)Short Code (64)Service (0)RAS (1)	<div>User Voicemail DND Short Codes Source Numbers Telephony Forwarding Dial In Voice Recording Button Programming</div> <div>Menu Programming Mobility Group Membership Announcements SIP Personal Directory Web Self-Administration</div> <div>SIP Name: 3035551235</div> <div>SIP Display Name (Alias): Extn243</div> <div>Contact: 3035551235</div> <div><input type="checkbox"/> Anonymous</div>		

5.8. Incoming Call Route

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

5.8.1. Incoming Call Route – Standard Tab

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

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

The screenshot shows the 'Incoming Call Route' configuration window with the 'Standard' tab selected. The title bar displays '29 3035551235'. The left navigation pane lists various system components, with 'Incoming Call Route (1)' highlighted. The main area contains the following fields:

Field	Value
Bearer Capability	Any Voice
Line Group ID	29
Incoming Number	3035551235
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

5.8.2. Incoming Call Route – Destinations Tab

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. Click the **OK** button (not shown). In this example, incoming calls to 3035551235 on line 29 are routed to extension 243.

The screenshot shows the 'Incoming Call Route' configuration window with the 'Destinations' tab selected. The title bar displays '29 3035551235'. The left navigation pane shows 'Destinations' selected. The main area contains a table with the following data:

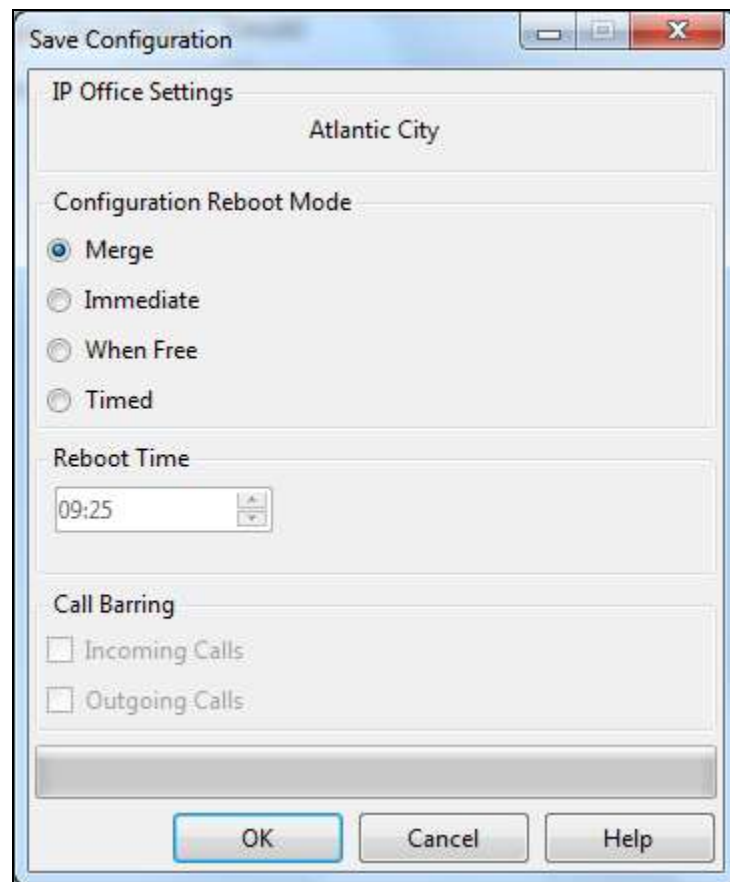
TimeProfile	Destination	Fallback Extension
Default Value	243 Extn243	

Incoming Call Routes for other direct mappings of DID numbers to Avaya IP Office users listed in **Figure 1** are omitted here, but can be configured in the same fashion.

5.9. Save Configuration

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

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



6. CenturyLink IQ® SIP Trunk Service Configuration

CenturyLink is responsible for the configuration of the CenturyLink IQ® SIP Trunk Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise. In the case of the compliance test, this is the public IP address of the Avaya IP Office WAN port. CenturyLink will provide the customer the necessary information to configure Avaya IP Office including:

- CenturyLink SIP proxy IP address
- Transport protocol and port
- SIP domain
- SIP credentials: user name and password
- Pilot number
- DID numbers

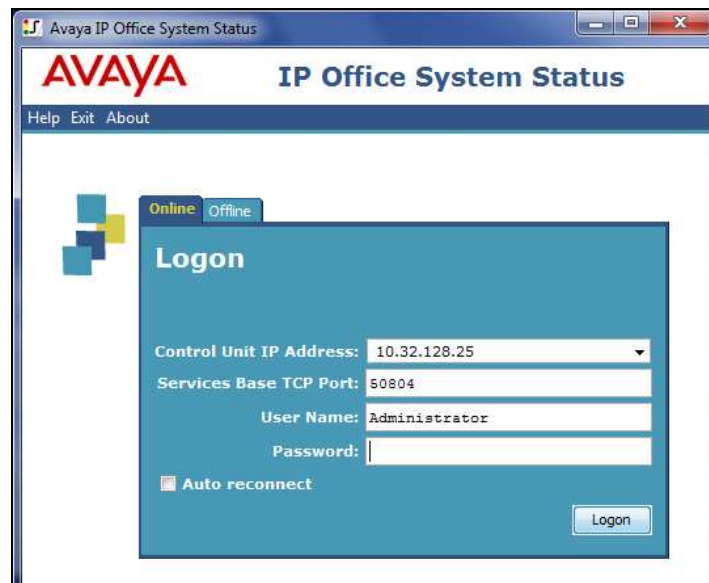
7. Verification Steps

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

7.1. System Status

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

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



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

Help Snapshot LogOff Exit About

System
Alarms (21)
Extensions (19)
Trunks (22)
 Lines:1 - 4
 Lines:5 - 8
 Line:17
 Line:18
 Line:19
 Line:20
 Line:21
 Line:22
 Line:23
 Line:24
 Line:25
 Line:26
 Line:27
 Line:28
 ▶ **Line:29**
 Line:30
Active Calls
Resources
Voicemail
IP Networking
Locations

Status Utilization Summary Alarms Registration

SIP Trunk Summary

Line Service State: In Service
 Peer Domain Name: voip.centurylink.com
 Resolved Address: 192.168.64.81
 Line Number: 29
 Number of Administered Channels: 10
 Number of Channels in Use: 0
 Administered Compression: G729 A, G711 Mu, G711 A, G7231
 Enable Faststart: Off
 Silence Suppression: Off
 Media Stream: RTP
 Layer 4 Protocol: UDP
 SIP Trunk Channel Licenses: Unlimited  0%
 SIP Trunk Channel Licenses in Use: 0
 SIP Device Features: REFER (Incoming and Outgoing)

Channel Number	U...	Call Ref	Current State	Time in State	Remote Media ...	Co...	Conne...	Caller ID or ...	Other Party on Call	Directi...	Round Trip D...	Receive Jitter	Receive Pack...	Trans...	Trans...
1			Idle	00:31:44											
2			Idle	00:31:50											
3			Idle	1 day 0...											
4			Idle	1 day 0...											
5			Idle	1 day 0...											
6			Idle	1 day 0...											
7			Idle	1 day 0...											
8			Idle	1 day 0...											
9			Idle	1 day 0...											
10			Idle	1 day 0...											

Trace Trace All Pause Ping Call Details Graceful Shutdown Force Out of Service Print... Save As...

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

Status Utilization Summary **Alarms** Registration

Alarms for Line: 29 SIP voip.centurylink.com

Last Date Of Error	Occurrences	Error Description
--------------------	-------------	-------------------

7.2. Monitor

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

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

The screenshot shows the 'All Settings' dialog box with the 'SIP' tab selected. The dialog has a tabbed interface with tabs for T1, VPN, WAN, SCN, and Jade. Under the 'SIP' tab, there are sub-tabs for ATM, Call, DTE, EConf, Frame Relay, GOD, H.323, Interface, ISDN, Key/Lamp, Directory, Media, PPP, R2, Routing, Services, SIP, and System. The 'SIP' sub-tab is active, showing configuration options for SIP monitoring.

Events

- ☒ **Sip** Standard
- ☒ **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
- ☒ Sip Tx

IP Filter (nnn.nnn.nnn.nnn)

Buttons: Default All, Clear All, Tab Clear All, Tab Set All, OK, Cancel, Save File, Load File, Load Partial File, Select File.

8. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office 9.1 to the CenturyLink IQ® SIP Trunk Service. The CenturyLink IQ® SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks. The CenturyLink IQ® SIP Trunk Service passed compliance testing. Please refer to **Section 2.2** for any observations/exceptions.

9. Additional References

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

- [1] *Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 30l, August 12, 2015.
- [2] *Administering Avaya IP Office Platform with Manager*, Issue 10.21, August 2015.
- [3] *Using System Status*, Document Number 15-601758, Issue 10f, August 11, 2015.
- [4] *Administering Avaya IP Office Voicemail Pro*, Document Number 15-601063, Issue 10f, July 10, 2015.
- [5] *Using IP Office System Monitor*, Document Number 15-601019, Issue 06e, May 19, 2015.

Additional Avaya IP Office documentation can be found at:
<http://marketingtools.avaya.com/knowledgebase/>

©2015 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.