Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 8.0.1 to support Alestra SIP Trunking Service on the Sonus 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 and Avaya Session Border Controller for Enterprise Release 8.0.1 to support Alestra SIP Trunking Service on the Sonus Platform. These Application Notes update previously published Application Notes with newer versions of Avaya software.

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

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

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

©2019 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction 4
2. General Test Approach and Test Results 4
   2.1. Interoperability Compliance Testing 5
   2.2. Test Results 6
   2.3. Support 8
3. Reference Configuration 8
4. Equipment and Software Validated 11
5. Avaya IP Office Primary Server Configuration 12
   5.1. Licensing 14
   5.2. System Settings 16
      5.2.1. System - LAN1 Tab 16
      5.2.2. System - Telephony Tab 19
      5.2.3. System - VoIP Tab 20
   5.3. IP Route 22
   5.4. SIP Line 23
      5.4.1. Creating a SIP Trunk from an XML Template 23
      5.4.2. SIP Line – SIP Line Tab 27
      5.4.3. SIP Line - Transport Tab 28
      5.4.4. SIP Line – Call Details Tab 29
      5.4.5. SIP Line - VoIP Tab 31
      5.4.6. SIP Line – SIP Advanced Tab 32
   5.5. Users 33
   5.6. IP Office Line – Primary Server 34
   5.7. Incoming Call Route 36
   5.8. Outbound Call Routing 38
      5.8.1. Short Codes and Automatic Route Selection 38
   5.9. Save IP Office Primary Server Configuration 40
6. Avaya IP Office Expansion System Configuration 41
   6.1. Physical Hardware 42
   6.2. LAN Settings 43
   6.3. IP Route 44
   6.4. IP Office Line – IP500 V2 Expansion System 45
   6.5. Short Codes 47
   6.6. Automatic Route Selection – ARS 48
   6.7. Save IP Office Expansion System Configuration 49
7. Configure Avaya Session Border Controller for Enterprise 50
   7.1. Log in Avaya SBCE 50
   7.2. Device Management 52
   7.3. TLS Management 54
   7.4. Configuration Profiles 54
      7.4.1. Server Interworking – Avaya-IPO 54
      7.4.2. Server Interworking - SP-General 58

©2019 Avaya Inc. All Rights Reserved.

7.4.3. Signaling Manipulation 61
7.4.4. SIP Server Configuration 63
7.4.5. Routing Profiles 68
7.4.6. Topology Hiding 72
7.5. Domain Policies 74
7.5.1. Application Rules 74
7.5.2. Media Rules 76
7.5.3. End Point Policy Groups 78
7.6. Network & Flows Settings 82
7.6.1. Network Management 82
7.6.2. Media Interface 83
7.6.3. Signaling Interface 85
7.6.4. End Point Flows 87
8. Alestra SIP Trunking Service on the Sonus Platform Configuration 91
9. Verification Steps 92
9.1. IP Office System Status 92
9.2. Monitor 94
9.3. Avaya Session Border Controller for Enterprise 95
10. Conclusion 99
11. Additional References 99

©2019 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Alestra 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), an Avaya Session Border Controller for Enterprise Release 8.0.1 (hereafter referred to as Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The Alestra SIP Trunking Service on the Sonus 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 "Alestra" 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 Alestra 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.

©2019 Avaya Inc. All Rights Reserved.

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's 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's network.
- Incoming and outgoing PSTN calls to/from Avaya Equinox for Windows soft-client.
- Dialing plans including local calls, international 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.729, G.711A and G.711MU, Alestra preferred codec order.
- 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.

Note: Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

©2019 Avaya Inc. All Rights Reserved.

Items not supported or not tested included the following:

- Inbound toll-free calls were not tested.
- 0, 0+10 digits and 911 Emergency calls were not tested.

2.2. Test Results

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

- **Caller ID on outbound calls** – On calls originating from IP Office extensions to the PSTN, the caller ID number displayed at the PSTN endpoints was always of the main DID number (BDN number) associated with the SIP trunk, not of the DID number assigned to the IP Office extension originating the call. This included calls to "twinned" mobile phones, and calls that were forwarded or transferred back out on the SIP trunk to the PSTN. This is the expected behavior of the Alestra service for outbound calls on the SIP trunk; it is listed here simply as an observation.
- **Outbound call from an enterprise extension to a busy PSTN number** – Alestra did not send a "486 Busy Here" message on an outbound call to a PSTN number that was busy, as it was expected on this condition. There was no direct impact to the user, who heard busy tone.
- **SIP REFER method –** PSTN calls that were transferred back to the network using the SIP REFER method did not work properly. On blind transfers, the REFER message was accepted by Alestra with a 202 message, but the trunk channels were not released after the call transfer was completed successfully. For this reason, testing was done with REFER disabled in IP Office, refer to **Section 5.4.2**. With REFER disabled, blind and attended call transfers to the PSTN completed successfully, with the caveat that trunk channels were not released from the call path after the call was transferred, two trunks channels remained busy/connected for the entire duration of the call.
- **Outbound Calling Party Number (CPN) Blocking –** When privacy is enabled at the IP Office station (Withhold Number enabled), the SIP INVITE toward Alestra did not include the "Privacy: id" header. This can cause the far-end to still see the number presented in the P-Asserted Identity header. This is currently being investigated by the IP Office development team. The current work around to this issue is to add a Signaling Manipulation script (SigMa) to the Avaya SBCE to add "Privacy = id" to INVITE messages sent by IP Office on calls with privacy enabled in IP Office stations (**Sections 7.4.3**). Note that in the case of Alestra, the addition of the SigMa script did not make any difference, the main DID number (BDN number) associated with the SIP trunk was still displayed. Calling Party Number (CPN) blocking may not be supported in Mexico.
- **SIP OPTION Messages** – During the compliance test Alestra did not send SIP OPTION messages to IP Office, IP Office did send SIP OPTION messages to Alestra with Alestra responding with 200 OK, this was sufficient to keep the SIP trunk up in-service.
- **Fax support –** Fax calls using the T.38 protocol failed during the compliance test. G.711 pass-through fax was also tested, but it behaved unreliably. The issue related to G.711 pass-through fax failing during the compliance test may be related to the unpredictability of G.711 pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay. The issue related to T.38 fax calls failing may be

©2019 Avaya Inc. All Rights Reserved.

related to the PSTN carriers used by Alestra in Mexico to route calls to the PSTN, not all PSTN carriers used by Alestra in Mexico support T.38. This issue could be resolved by Alestra selecting specific PSTN carriers that do support T.38 and routing T.38 fax traffic via these PSTN carriers.

- **The Avaya SBCE responded with 481 Call/Transaction does Not Exist** – Outbound call from enterprise extensions to the PSTN that were cancelled at the originating enterprise extensions before the far end answered (cancelling by hanging-up) were causing the Avaya SBCE to respond with "481 Call/Transaction Does Not Exist" to the Cancel message sent by IP Office. The user impact is that the call at the originating enterprise telephone is release/drop but the call leg from the Avaya SBCE → Alestra →PSTN is not released/dropped. This behavior was causing the terminating PSTN telephone to keep ringing, since the BYE message sent by IP Office is never passed/forwarded to Alestra by the Avaya SBCE. This issue seems to be related to an UPDATE message sent by IP Office during the initial call establishment. The current work around is to disable "PRACK/100rel Support" on the IP Office Line (refer to **Section 5.4.5**). This issue is under investigation by Avaya.

©2019 Avaya Inc. All Rights Reserved.

2.3. Support

For support on Alestra systems visit the corporate Web page at: http://www.alestra.com.mx/

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 Alestra SIP Trunking Service on the Sonus 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 Session Border Controller for Enterprise.
- 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 not used.

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

Located at the edge of the enterprise is the Avaya SBCE. The Avaya SBCE has two physical interfaces, interface **B1** is used to connect to the public network, interface **A1** is used to connect to the private network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. The Avaya SBCE provides network address translation at both the IP and SIP layers.

©2019 Avaya Inc. All Rights Reserved.

IP endpoints at the enterprise included Avaya 96x1 Series IP Deskphones (with H.323 firmware), Avaya 1100 Series IP Deskphones (with SIP firmware), Avaya J100 Series IP Deskphones (with SIP and H.323 firmware), Avaya Equinox™ for Windows Softphones, Avaya Digital and Analog Deskphones. IP endpoints were registered to the Primary Server; non IP endpoints (analog and digital) 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 protocol between the Avaya SBCE and Alestra, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network, is SIP over TLS.

For inbound calls, the calls flowed from Alestra network to the Avaya SBCE, then to IP Office.

Outbound calls to the PSTN were first processed by IP Office. Once IP Office selected the proper SIP trunk, the call was routed to the Avaya SBCE for egress to Alestra network.

For the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Alestra network. The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Alestra 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.

©2019 Avaya Inc. All Rights Reserved.

Figure 1: Avaya Interoperability Test Lab Configuration

©2019 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server) • Avaya IP Office Voicemail Pro	11.0.4.1.0 Build 11 11.0.4.1.0 Build 2
Avaya IP Office IP500 V2 (Expansion Systems)	11.0.4.1.0 Build 11
Avaya IP Office Manager	11.0.4.1.0 Build 11
Avaya Session Border Controller for Enterprise	ASBCE 8.0 8.0.1.0-10-17555
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	---
Alestra	
Sonus Soft switch	V09.03.02R000
AudioCodes SBC	7.20A.204.015
Lucent 5ESS	V16.1

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.

©2019 Avaya Inc. All Rights Reserved.

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.

©2019 Avaya Inc. All Rights Reserved.

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.

©2019 Avaya Inc. All Rights Reserved.

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, **IP500V2-One** and **IP500V2-Two** were used as the system name for the two 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.

©2019 Avaya Inc. All Rights Reserved.

On Server Edition systems, the number of licenses to be assigned to the specific Server or Expansion System is 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.

©2019 Avaya Inc. All Rights Reserved.

5.2. System Settings

Configure the necessary system settings. In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to connect IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.1. System - LAN1 Tab

In the sample configuration, **IPOSE-Primary** was used as the system name, the **LAN1** port connects to the inside interface (enterprise private network side) of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE connects to Alestra network via the public internet. To access the **LAN1** settings, navigate to **System (1) → IPOSE-Primary** in the Navigation Pane, then in the Details Pane navigate to the **LAN1→ LAN Settings** tab. The **LAN1** settings for the compliance testing were configured with following parameters:

- Set the **IP Address** field to the LAN IP address, e.g., **10.64.101.127**.
- Set the **IP Mask** field to the subnet mask of the enterprise private network, e.g., **255.255.255.0**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

©2019 Avaya Inc. All Rights Reserved.

5.2.1.1 LAN1 VoIP Tab

The **VoIP** tab as shown in the screenshot below was configured with following settings:

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Select **Preferred** under **H.323 Signaling over TLS**. When enabled, TLS is used to secure the registration and call signaling communication between IP Office and endpoints that support TLS. The H.323 phones that support TLS are 9608, 9611, 9621, 9641 running firmware version 6.6 or higher and the Avaya J100 Series IP Deskphones.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Alestra.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name of the enterprise under **SIP Domain Name**.
- Enter the SIP Registrar FQDN of the enterprise under **SIP Registrar FQDN**.
- Check TLS and verify the **TLS Port** numbers under **Layer 4 Protocol** are set to **5061**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP-RTCP**, **Periodic Timeout** to **30**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send RTP and RTCP keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP/RTCP traffic is present.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

©2019 Avaya Inc. All Rights Reserved.

Note: In the compliance test, the **LAN1** interface was used to connect IP Office to the enterprise private network (LAN), **LAN2** was not used.

©2019 Avaya Inc. All Rights Reserved.

5.2.2. System - 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).

©2019 Avaya Inc. All Rights Reserved.

5.2.3. System - VoIP Tab

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

5.2.3.1 VoIP - VoIP Tab

Select the **VoIP → VoIP** tab, configure the following parameters:

- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used.
- For codec selection, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order were used.
- Click **OK** to commit (not shown).

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

©2019 Avaya Inc. All Rights Reserved.

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).

©2019 Avaya Inc. All Rights Reserved.

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 Alestra 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., **10.64.101.1**.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).

©2019 Avaya Inc. All Rights Reserved.

5.4. SIP Line

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

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.

©2019 Avaya Inc. All Rights Reserved.

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

©2019 Avaya Inc. All Rights Reserved.

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**.

©2019 Avaya Inc. All Rights Reserved.

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**.

©2019 Avaya Inc. All Rights Reserved.

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.
- 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**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never** (refer to **Section 2.2)**.
- Click **OK** to commit (not shown).

©2019 Avaya Inc. All Rights Reserved.

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 inside IP Address of the Avaya SBCE or **10.64.101.243** as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **TLS**.
- Set **Use Network Topology Info** to **None** (see note below).
- Set the **Send Port** to **5061**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

Note – For the compliance testing, the **Use Network Topology Info** field was set to **None**, since no NAT was used in the test configuration. In addition, it was not necessary to configure the **System → LAN1 → Network Topology** tab for the purposes of SIP trunking. 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) used by the trunk and the **System → LAN1 → Network Topology** tab needs to be configured with the details of the NAT device.

©2019 Avaya Inc. All Rights Reserved.

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 two new entries were added, one for incoming calls and one for outgoing calls.

The entry for calls from IP Office to the PSTN (outgoing calls) was created with the parameters shown below:

- Associate this entry 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 from this line. For the compliance test outgoing group **17** was used. Leave the **Incoming Group** field as 0.
- 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** (SIP Trunk registration is being done at the Avaya SBCE).
- Check the **P Asserted ID** and **Diversion Header**.
- For the **Local URI**, **Contact, P Asserted ID** and **Diversion Header** set the selections under the **Display** and **Content** columns to **Use Internal Data**.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.

©2019 Avaya Inc. All Rights Reserved.

The entry for calls from the PSTN to IP Office (incoming calls) was created with the parameters shown below:

- Associate this entry to an incoming line group using the **Incoming Group** field. For the compliance test incoming group **17** was used. The **Outgoing Group** field was set to **17**, since it cannot be set to 0 in IP Office Server Edition systems.
- 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** (SIP Trunk registration is being done at the Avaya SBCE).
- For the **Local URI** and **Contact**, set the selections under the **Display** and **Content** columns to **Auto**.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.
- Click **OK** to commit again (not shown).

©2019 Avaya Inc. All Rights Reserved.

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. Alestra supports codecs **G.729(a)**, **G.711ALAW** and **G.711ULAW** for audio.
- Select **T38 Fallback** for **Fax Transport Support** (Refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set the **Media Security** field to **Same as System (Preferred)**.
- Check the **Re-invite Supported** box.
- Verify **PRACK/100rel Supported** box is unchecked (Refer to **Section 2.2**).
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).

Note: The codec selections defined under this section are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.3** are the codecs selected for the IP phones/extension (H.323 and SIP).

©2019 Avaya Inc. All Rights Reserved.

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).

©2019 Avaya Inc. All Rights Reserved.

5.5. Users

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 **Ext3041 H323**. Select the **SIP** tab in the Details Pane. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Alestra. Note that the full 10 digits number of the DID provided by Alestra is being used here, instead of only using the last 4 digits of the DID, as shown in **Section 5.7**. The full DID number provided by Alestra should be use here. 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. This can also be accomplished by activating Withhold Number on H.323 Deskphones (not shown). Click the **OK** to commit (not shown).

©2019 Avaya Inc. All Rights Reserved.

5.6. 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.

©2019 Avaya Inc. All Rights Reserved.

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

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

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

©2019 Avaya Inc. All Rights Reserved.

5.7. 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 Alestra. Note that in the case of Alestra only the last 4 digits of the DID numbers provided by Alestra were used for the **Incoming Number**, this is because Alestra was configured to only send the last 4 digits of the DID numbers to the enterprise.
- Default values may be used for all other parameters.

©2019 Avaya Inc. All Rights Reserved.

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 333001**6502** provided by Alestra was associated with the Avaya IP Office extension **3041**. Note that in the case of Alestra only the last 4 digits of the DID numbers provided by Alestra were used for the **Incoming Number**, as mentioned above.

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.).

©2019 Avaya Inc. All Rights Reserved.

5.8. 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.

5.8.1. 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**, **Mexico (Latin Spanish)** was used.
- Click the **OK** to commit (not shown).

©2019 Avaya Inc. All Rights Reserved.

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

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

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **001** 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 **001N**. The value **N** represents the additional number of digits dialed by the user after dialing **001** (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**, **Mexico (Latin Spanish)** was used
- Click **OK** to commit.

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

The following example shows the dial pattern for local calls within Mexico.

©2019 Avaya Inc. All Rights Reserved.

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

5.9. Save IP Office Primary Server Configuration

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

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

Click **OK** to execute the save.

©2019 Avaya Inc. All Rights Reserved.

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 **IP500V2-One** on the left navigation pane will expand the menu on this server.

©2019 Avaya Inc. All Rights Reserved.

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.

©2019 Avaya Inc. All Rights Reserved.

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).

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

©2019 Avaya Inc. All Rights Reserved.

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.

©2019 Avaya Inc. All Rights Reserved.

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.

©2019 Avaya Inc. All Rights Reserved.

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

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

©2019 Avaya Inc. All Rights Reserved.

6.5. Short Codes

Similar to the configuration of the Primary server in **Section 5.8**, 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.

©2019 Avaya Inc. All Rights Reserved.

6.6. Automatic Route Selection – ARS

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

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

©2019 Avaya Inc. All Rights Reserved.

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.

©2019 Avaya Inc. All Rights Reserved.

7. Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of the Avaya SBCE to connect to Alestra SIP Trunking Service on the Sonus Platform.

It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

7.1. Log in Avaya SBCE

Use a Web browser to access the Avaya SBCE Web interface. Enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the Avaya SBCE management IP address.

Enter the appropriate credentials and click **Log In**.

©2019 Avaya Inc. All Rights Reserved.

Once logged in, on the top left of the screen, under **Device:** select the device being managed, ***Avaya_SBCE*** in the sample configuration.

The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.

©2019 Avaya Inc. All Rights Reserved.

7.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named ***Avaya_SBCE*** is shown. The management IP address that was configured during installation is blurred out for security reasons, the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is ***Commissioned***, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings.

©2019 Avaya Inc. All Rights Reserved.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

The highlighted IP addresses in the **System Information** screen shown above are the ones used for the SIP trunk to Alestra and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBCE **A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

In the reference configuration, the private interface of the Avaya SBCE (10.64.101.243) was used to connect to the enterprise network, while its public interface (10.10.80.51) was used to connect to the public network. See **Figure 1**.

On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP

©2019 Avaya Inc. All Rights Reserved.

trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

7.3. TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

For the compliance testing, the transport protocol that was used between IP Office and the Avaya SBCE, across the enterprise private IP network (LAN), was SIP over TLS. SIP over UDP was used between the Avaya SBCE and Alestra, across the public Internet.

It is assumed that generation and installation of certificates and the creation of TLS Profiles on the Avaya SBCE have been previously completed, as it's not discussed in this document. Refer to item [**7**] in **Section 11**.

7.4. Configuration Profiles

The Configuration Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

7.4.1. Server Interworking – Avaya-IPO

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or "cloned". Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or "cloned". If needed, the profile can then be modified to meet specific requirements for the enterprise SIP-enabled solution. For Alestra, this profile was left with the **avaya-ru** default values.

On the left navigation pane, select **Configuration Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone** on top right of the screen (not shown).

Enter the new profile name in the **Clone Name** field, the name of ***Avaya-IPO*** was chosen in this example. Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

Click **Edit** on the newly cloned ***Avaya-IPO*** interworking profile:

- On the **General** tab, check ***T.38 Support***.
- Leave remaining fields with default values.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries.

The following screen capture shows the **General** tab of the newly created **Avaya-IPO** Server Interworking Profile.

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **Avaya-IPO** Server Interworking Profile.

©2019 Avaya Inc. All Rights Reserved.

7.4.2. Server Interworking - SP-General

A second Server Interworking profile named **SP-General** was created for the Service Provider.

On the left navigation pane, select **Configuration Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **Add** (not shown) (note that **Add** is being used to create the SP-General profile instead of cloning the avaya-ru profile).

Enter the new profile name, the name of ***SP-General*** was chosen in this example.

- Click **Next**.

©2019 Avaya Inc. All Rights Reserved.

On the **General** tab, check ***T.38 Support***, click **Next** until the last tab is reached then click **Finish** on the last tab leaving remaining fields with default values (not shown).

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the **General** tab of the newly created **SP-General** Server Interworking Profile.

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **SP-General** Server Interworking Profile.

7.4.3. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform granular header manipulations on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult reference **[7]** in the **References** section for more information on this topic.

A Sigma scripts was created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

- Calls from IP Office to the PSTN with “privacy” enabled do not include the privacy header (privacy = id) in the INVITE message sent to Alestra.

©2019 Avaya Inc. All Rights Reserved.

The scripts will later be applied to the SIP Server configuration profile corresponding to the service provider in **Section 7.4.4**.

To create the SigMa script to set the privacy header (privacy = id) in the INVITE message sent to Alestra, on the left navigation pane, select **Configuration Profiles → Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name ***Add_Privacy_Header*** was chosen in this example.
- Copy the complete script shown below.
- Click **Save**.

```
within session "INVITE"
{
 act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
  {
// fix anonymous
       if (%HEADERS["From"][1].URI.USER = "anonymous") then
       {
          if (exists(%HEADERS["Privacy"][1])) then
          {
             %do = "nothing";
             }
          else
          {
             %HEADERS["Privacy"][1] = "id";
             }
          }
       }
    }
```

©2019 Avaya Inc. All Rights Reserved.

7.4.4. SIP Server Configuration

SIP Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (IP Office) and the Trunk Server or SIP Proxy at the service provider's network.

To add the SIP Server profile for the Call Server, from the **Services** menu on the left-hand navigation pane, select **SIP Servers** (not shown). Click **Add** (not shown) and enter the profile name: ***IP Office-Thornton***.

- Click **Next**.

©2019 Avaya Inc. All Rights Reserved.

On the **Edit SIP Server Profile – General** window:

- **Server Type**: Select ***Call Server***.
- **IP Address / FQDN**: ***10.64.101.127*** (IP Address of IP Office).
- **Port**: ***5061*** (This port must match the port number defined in **Section 5.2.1**).
- **Transport**: Select ***TLS***.
- Select a **TLS Client Profile**.
- Click **Next**.

- Click **Next** until the **Add SIP Server Profile - Advanced** tab is reached (not shown).
- On the **Add SIP Server Profile - Advanced** tab:
- Verify that ***Enable Grooming*** is checked.
- Select ***Avaya-IPO*** from the **Interworking Profile** drop down menu (**Section 7.4.1**).
- Leave the **Signaling Manipulation Script** at the default ***None***.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the **General** tab of the newly created **IP Office-Thornton** SIP Server Configuration Profile.

The following screen capture shows the **Advanced** tab of the newly created **IP Office-Thornton** SIP Server Configuration Profile.

©2019 Avaya Inc. All Rights Reserved.

To add the SIP Server profile for the Trunk Server, from the **Services** menu on the left-hand navigation pane, select **SIP Servers** (not shown). Click **Add** (not shown) and enter the profile name: ***Service Provider UDP***.

- Click **Next**.

On the **Edit SIP Server Profile – General** window:

- **Server Type**: Select ***Trunk Server***.
- **IP Address / FQDN**: ***192.168.5.138*** (IP Address of the Service Provider SIP Proxy, this information is provided by the Service Provider.
- **Port**: ***5060***.
- **Transports**: Select ***UDP***.
- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).

©2019 Avaya Inc. All Rights Reserved.

On the **Add Server Configuration Profile – Advanced** tab:

- Uncheck ***Enable Grooming***.
- Select ***SP-General*** from the **Interworking Profile** drop-down menu (**Section 7.4.2**).
- Select the ***Add_Privacy_Header*** from the **Signaling Manipulation Script** drop down menu (**Sections 7.4.3**).
- Click **Finish**.

The following screen capture shows the **General** tab of the newly created **Service Provider UDP** SIP Server Configuration Profile.

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **Service Provider UDP** SIP Server Configuration Profile.

7.4.5. Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing profiles were created, one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

To create the inbound route, from the **Configuration Profiles** menu on the left-hand side (not shown):

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: ***Route_to_IPO_TLS***.
- Click **Next**.

©2019 Avaya Inc. All Rights Reserved.

On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: ***1***
- **Server Configuration**: Select ***IP Office Thornton***.
- **Next Hop Address** is populated automatically with ***10.64.101.127:5061 (TLS)*** (IP Office IP address, Port and Transport).
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

The following screen shows the newly created **Route_to_IPO_TLS** Routing Profile.

Similarly, for the outbound route:

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: ***Route_to_SP_UDP***.
- Click **Next**.

©2019 Avaya Inc. All Rights Reserved.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: ***1***
- **Server Configuration**: Select ***Service Provider UDP***.
- **Next Hop Address** is populated automatically with ***192.168.5.138:5060 (UDP)*** (Service Provider SIP Proxy IP address, Port and Transport).
- Click **Finish**.

The following screen capture shows the newly created **Route_to_SP_UDP** Routing Profile.

©2019 Avaya Inc. All Rights Reserved.

7.4.6. Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by IP Office and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Profile Name**: ***IP Office***.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly added **IP Office** Topology Hiding Profile. Note that for IP Office no values were overwritten (left with default values).

To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Profile Name**: ***Service_Provider***.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly added **Service_Provider** Topology Hiding Profile.

7.5. Domain Policies

Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.5.1. Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the Avaya SBCE will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

From the menu on the left-hand side, select **Domain Policies → Application Rules** (not shown).

- Click on the **Add** button to add a new rule (not shown).
- **Rule Name:** enter the name of the profile, e.g., ***500 Session***.
- Click **Next**.

©2019 Avaya Inc. All Rights Reserved.

- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values; the value of ***500*** was used in the sample configuration.
- Under **Video** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values; the value of ***100*** was used in the sample configuration.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **500 Sessions** Application Rule.

7.5.2. Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test one media rule was created toward IP Office, the existing ***default-low-med*** media rule was used toward the Service Provider.

To add a media rule in the IP Office direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter ***IPO_SRTP***.
- Click Next.

©2019 Avaya Inc. All Rights Reserved.

- Under Audio Encryption, **Preferred Format #1**, select ***SRTP_AES_CM_128_HMAC_SHA1_80***.
- Under Audio Encryption, **Preferred Format #2**, select ***RTP***.
- Under Audio Encryption**,** uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous check **Capability Negotiation**.
- Click **Next**.

- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **IPO_SRTP** Media Rule

7.5.3. End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups** (not shown).

- Click on the **Add** button to add a new policy group (not shown).
- **Group Name**: ***Enterprise***.
- Click **Next**.

- **Application Rule**: ***500 Sessions***.
- **Border Rule**: ***default***.
- **Media Rule**: ***IPO_SRTP*** (**Section 7.5.2**).

©2019 Avaya Inc. All Rights Reserved.

- **Security Rule**: ***default-low***.
- **Signaling Rule**: ***default***.
- Click **Finish**.

The following screen capture shows the newly created **Enterprise** End Point Policy Group.

©2019 Avaya Inc. All Rights Reserved.

Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk.

- Click on the **Add** button to add a new policy group (not shown).
- **Group Name**: ***Service Provider***.
- Click **Next**.

- **Application Rule**: ***500 Sessions***
- **Border Rule**: ***default.***
- **Media Rule**: ***default-low-med***.
- **Security Rule**: ***default-low***.
- **Signaling Rule**: ***default***.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **Service Provider** End Point Policy Group.

©2019 Avaya Inc. All Rights Reserved.

7.6. Network & Flows Settings

The **Network & Flows** settings allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

7.6.1. Network Management

The network information should have been previously completed. To verify the network configuration, from the **Network & Flows** on the left hand side, select **Network Management**. Select the **Networks** tab.

In the event that changes need to be made to the network configuration information, they can be entered here.

Use **Figure 1** as reference for IP address assignments.

Note: Only the highlighted entity items were created for the compliance test and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in these Application Notes.

©2019 Avaya Inc. All Rights Reserved.

On the Interfaces tab, click the **Status** control for interfaces **A1** and **B1** to change the status to ***Enabled***. It should be noted that the default state for all interfaces is ***Disabled***, so it is important to perform this step, or the Avaya SBCE will not be able to communicate on any of its interfaces.

7.6.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

From the **Network & Flows** menu on the left-hand side, select **Media Interface** (not shown).

- Select **Add** in the **Media Interface** area (not shown).
- **Name**: ***Private_med***.
- Under **IP Address** select: ***Network_A1 (A1, VLAN 0)***
- Select **IP Address**: ***10.64.101.243*** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **Port Range**: ***35000-40000***.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

- Select **Add** in the **Media Interface** area (not shown)**.**
- **Name**: ***Public_med***.
- Under **IP Address** select: ***Network_B1 (B1, VLAN 0)***
- Select **IP Address**: ***10.10.80.51*** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **Port Range**: ***35000-40000***.
- Click **Finish**.

The following screen capture shows the newly created Media Interfaces.

©2019 Avaya Inc. All Rights Reserved.

7.6.3. Signaling Interface

To create the Signaling Interface toward IP Office, from the **Network & Flows** menu on the left hand side, select **Signaling Interface** (not shown).

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name**: ***Private_sig***.
- Under **IP Address** select: ***Network_A1 (A1, VLAN 0)***
- Select **IP Address**: ***10.64.101.243*** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **TLS Port**: ***5061***.
- Select a **TLS Profile**.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name**: ***Public_sig***.
- Under **IP Address** select: ***Network_B1 (B1, VLAN 0)***
- Select **IP Address**: ***10.10.80.51*** (outside or public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port**: ***5060***.
- Click **Finish**.

The following screen capture shows the newly created Signaling Interfaces.

©2019 Avaya Inc. All Rights Reserved.

7.6.4. End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

©2019 Avaya Inc. All Rights Reserved.

The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward the Service Provider SIP trunk, from the **Network & Flows** menu, select **End Point Flows** (not shown**)**, then the **Server Flows** tab. Click **Add** (not shown).

- **Name**: ***SIP_Trunk_Flow_UDP***.
- **Server Configuration**: ***Service Provider UDP***.
- **URI Group**: ***
- **Transport**: ***
- **Remote Subnet**: ***
- **Received Interface**: ***Private_sig***.
- **Signaling Interface**: ***Public_sig***.
- **Media Interface**: ***Public_med***.
- **Secondary Media Interface**: **None**.
- **End Point Policy Group**: ***Service Provider***.
- **Routing Profile**: ***Route_to_IPO_TLS*** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile**: ***Service_Provider***.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

To create the call flow toward IP Office, click **Add** (not shown).

- **Name**: ***IP_Office_Flow***.
- **Server Configuration**: ***IP Office-Thornton***.
- **URI Group**: ***
- **Transport**: ***
- **Remote Subnet: ***
- **Received Interface**: ***Public_sig***.
- **Signaling Interface**: ***Private_sig***.
- **Media Interface**: ***Private_med***.
- **Secondary Media Interface**: ***None***.
- **End Point Policy Group**: ***Enterprise***.
- **Routing Profile**: ***Route_to_SP_UDP*** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile**: ***IP Office***.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **End Point Flows**.

©2019 Avaya Inc. All Rights Reserved.

8. Alestra SIP Trunking Service on the Sonus Platform Configuration

To use Alestra SIP Trunking Service on the Sonus Platform, a customer must request the service from Alestra using the established sales processes. The process can be started by contacting Alestra via the corporate web site at: http://www.alestra.com.mx/ and requesting information.

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

Alestra is responsible for the configuration of Alestra SIP Trunking Service on the Sonus Platform. The customer will need to provide the public IP address used to reach the Avaya Session Border Controller for Enterprise at the enterprise, the public IP address assigned to interface B1.

Alestra will provide the customer the necessary information to configure Avaya IP Office and the Avaya Session Border Controller for Enterprise following the steps discussed in the previous sections, including:

Alestra will provide the following information:

- SIP Proxy IP address (public IP address).
- DID numbers.
- Etc.

©2019 Avaya Inc. All Rights Reserved.

9. 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.

9.1. 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.

©2019 Avaya Inc. All Rights Reserved.

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.

©2019 Avaya Inc. All Rights Reserved.

9.2. Monitor

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

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

©2019 Avaya Inc. All Rights Reserved.

9.3. Avaya Session Border Controller for Enterprise

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

Alarms: Provides information about the health of the Avaya SBCE.

The following screen shows the **Alarm Viewer** page.

©2019 Avaya Inc. All Rights Reserved.

Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.

The following screen shows the Incident Viewer page.

©2019 Avaya Inc. All Rights Reserved.

Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

The following screen shows the Diagnostics page with the results of a ping test.

©2019 Avaya Inc. All Rights Reserved.

Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as pcap files. Navigate to **Monitor & Logging →** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

Once the capture is stopped, click on the **Captures** tab and select the proper pcap file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

©2019 Avaya Inc. All Rights Reserved.

Also, the **traceSBC** tool can be used to monitor the SIP signaling messages between the Service provider and the Avaya SBCE

10. Conclusion

These Application Notes describe the procedures required to configure Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 8.0.1 to connect to Alestra SIP Trunking Service on the Sonus Platform. Alestra SIP Trunking Service on the Sonus Platform 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**.

11. 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] *Deploying Avaya Session Border Controller* in a Virtualized Environment, Release 8.0, Issue 2, March 2019.
[7] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0, Issue 1, February 2019.
[8] *Planning for and Administering Avaya Equinox for Android, iOS, Mac and Windows, Release 3.4.8, November 2018*
[9] *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.

©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.