Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Line Systems SIP Trunk Service with Avaya IP Office 10.1 and Avaya Session Border Controller for Enterprise 7.2 using TLS/SRTP - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Line Systems and Avaya IP Office Release 10.1 and Avaya Session Border Controller for Enterprise Release 7.2 using TLS/SRTP.

Line Systems SIP Trunk Service provides PSTN access via a SIP trunk between the enterprise and the Line Systems network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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.

Line Systems is a member of the Avaya DevConnect Service Provider program. 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.

©2017 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 5
   2.3. Support 6
3. Reference Configuration 7
4. Equipment and Software Validated 10
5. Configure Avaya IP Office Solution 11
   5.1. Licensing 12
   5.2. System Tab 13
   5.3. LAN2 Settings 14
   5.4. System Telephony Settings 17
   5.5. System VoIP Settings 18
   5.6. Administer SIP Line 19
      5.6.1. Create SIP Line from Template 20
      5.6.2. Create SIP Line Manually 24
   5.7. Outgoing Call Routing 30
      5.7.1. Short Code 30
   5.8. User 32
   5.9. Incoming Call Route 34
   5.10. Save Configuration 35
6. Configure Avaya Session Border Controller for Enterprise 36
   6.1. Log in to the Avaya SBCE 36
   6.2. TLS Management 39
      6.2.1. Installing TLS Certificate 40
      6.2.2. TLS Client Profile 42
      6.2.3. TLS Server Profile 44
   6.3. Global Profiles 45
      6.3.1. Configure Server Interworking Profile – Avaya IP Office 45
      6.3.2. Configure Server Interworking Profile – Line Systems 46
      6.3.3. Configure Server – Avaya IP Office 47
      6.3.4. Configure Server – Line Systems 49
      6.3.5. Configure Routing – Avaya IP Office 51
      6.3.6. Configure Routing – Line Systems 52
      6.3.7. Configure Topology Hiding – Avaya IP Office 53
      6.3.8. Configure Topology Hiding – Line Systems 54
   6.4. Domain Policies 55
      6.4.1. Create Application Rules 55

©2017 Avaya Inc. All Rights Reserved.

6.4.2. Create Media Rules ... 56
6.4.3. Create Endpoint Policy Groups ... 57
6.5. Device Specific Settings ... 58
6.5.1. Manage Network Settings ... 58
6.5.2. Create Media Interfaces ... 61
6.5.3. Create Signaling Interfaces ... 62
6.5.4. Configuration Server Flows ... 63
7. Line Systems SIP Trunk Configuration ... 66
8. Verification Steps ... 67
9. Conclusion ... 69
10. Additional References ... 69
11. Appendix - Remote Worker Configuration via Avaya SBCE ... 70
11.1. Provisioning Avaya SBCE for Remote Worker ... 71
11.1.1. Network Management ... 71
11.1.2. Signaling Interfaces ... 72
11.1.3. Media Interface ... 73
11.1.4. Server Profile for Avaya IP Office ... 74
11.1.5. Routing Profiles ... 75
11.1.6. User Agent ... 77
11.1.7. Create Media Rules for Remote Worker ... 78
11.1.8. End Point Policy Groups ... 79
11.1.9. End Point Flows ... 80
11.2. Remote Worker Endpoint Configuration on Avaya IP Office ... 87
11.2.1. Extension and User Configuration ... 87
11.2.2. Incoming Call Route ... 88
11.3. Remote Worker - Avaya Communicator for Windows Settings ... 89

©2017 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between Line Systems and an Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of Avaya IP Office Release 10.1, Avaya embedded Voicemail, Avaya IP Office Application Server (with WebRTC and one-X Portal services enabled), Avaya Communicator for Windows (SIP mode), Avaya Communicator for Web, Avaya H.323, Avaya SIP, digital and analog deskphones. The enterprise solution connects to the Line Systems network via the Avaya Session Border Controller for Enterprise (Avaya SBCE).

The Line Systems referenced within these Application Notes is designed for business customers. The service enables local and long distance PSTN calling via standards-based SIP trunks as an alternative to legacy analog or digital trunks, without the need for additional TDM enterprise gateways and the associated maintenance costs.

.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office connecting to Line Systems via the Avaya SBCE.

This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**. **Note**: NAT devices added between Avaya SBCE and the Line Systems network should be transparent to the SIP signaling.

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. 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.

©2017 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

A simulated enterprise site with Avaya IP Office and Avaya SBCE was connected to Line Systems. To verify SIP trunking interoperability, the following features and functionality were exercised during the interoperability compliance test:

- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog phones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog phones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls from/to the Avaya Communicator for Windows (SIP)
- Inbound and outbound PSTN calls from/to the Avaya Communicator for Web with basic telephony transfer feature
- Inbound and outbound long hold time call stability
- Various call types including: local, long distance, international call, inbound toll-free, outbound toll-free, and 411 Directory Assistance
- SIP transport TLS/SRTP between Line Systems and the simulated Avaya enterprise site
- Codec G.711MU and G.729A
- Caller number/ID presentation
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls
- DTMF transmission using RFC 2833
- Voicemail navigation for inbound and outbound calls
- Telephony features such as hold and resume, transfer, and conference
- Fax G.711 pass-through mode
- Off-net call forwarding
- Off-net call transfer: Use of either SIP Re-Invite or SIP Refer
- Twinning to mobile phones on inbound calls
- Remote Worker. Avaya Communicator for Windows (SIP) was used to test remote worker functionality

Item not supported include the following:

- Registration/Authentication
- Operator assisted calls (0+10 digits)
- Outbound call to 911 service
- T.38 fax

2.2. Test Results

Interoperability testing of Line Systems was completed with successful results for all test cases with the exception of the limitation described below:

- On incoming calls from the PSTN to the enterprise, Line Systems only offered codec G.711MU, however, on outbound calls from the enterprise to the PSTN, Line Systems accepted codec G.729A, with codec G.711MU being the preferred codec of Line System.

©2017 Avaya Inc. All Rights Reserved.

2.3. Support

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

For technical support on the Line Systems SIP Trunk Service, please contact customer service at 1-888-808-6111 or visit: http://www.linesystems.com/services/voice/.

.

©2017 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to Line Systems through the public internet. For confidentiality and privacy purposes, actual public IP addresses and DID numbers used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

The Avaya components used to create the simulated customer site included:

- Avaya IP Office 500V2.
- Avaya micro Session Border Controller for Enterprise.
- Avaya embedded Voicemail for IP Office.
- Avaya Application Server (Enabled WebRTC and one-X Portal services)
- Avaya 9600 Series IP Deskphones (H.323).
- Avaya 11x0 Series IP Deskphones (SIP).
- Avaya 1408 Digital phones.
- Avaya Analog phones.
- Avaya Communicator for Windows (SIP).
- Avaya Communicator for Web (WebRTC)
- Avaya Communicator for Windows (SIP) for remote worker

Located at the enterprise site are an Avaya Session Border Controller for Enterprise (Avaya SBCE), an Avaya IP Office 500V2 with the MOD DGTL STA16 expansion module which provides connections for 16 digital stations to the PSTN, and the extension PHONE 8 card which provides connections for 8 analog stations to the PSTN as well as 64-channel VCM (Voice Compression Module) for supporting VoIP codecs. The voicemail service is embedded on Avaya IP Office. Endpoints include Avaya 9600 Series IP Telephone (with H.323 firmware), Avaya 1100 Series IP Telephone (with SIP firmware), Avaya 1408D Digital Telephones, Avaya Analog Telephone, and Avaya Communicator for Windows.

The LAN2 port of Avaya IP Office was connected to the enterprise LAN while the LAN1 port was not used during the compliance test. The Avaya SBCE internal interface was connected to LAN2 port of the Avaya IP Office, while the Avaya SBCE external interface was connected to public internet.

A separate Windows 10 Enterprise PC runs Avaya IP Office Manager to configure and administer Avaya IP Office system.

Mobility Twinning is configured for some of the Avaya IP Office users so that calls to these user's phones will also ring and can be answered at configured mobile phones.

©2017 Avaya Inc. All Rights Reserved.

Figure 1 - Test Configuration for Avaya IP Office with Line Systems SIP Trunk Service

For the purposes of the compliance test, Avaya IP Office users dialed a short code of 9 + N digits to send digits across the SIP trunk to Line Systems. The short code of 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Line Systems. For calls within the North American Numbering Plan (NANP), the user would dial 11 (1 + 10) digits. Thus for these NANP calls, Avaya IP Office would send 11 digits in the Request URI and the To field of an outbound SIP INVITE message. It was configured to send 10 digits in the From field. For inbound calls, Line Systems sent 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and Avaya SBCE, such as a data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes.

©2017 Avaya Inc. All Rights Reserved.

However, it should be noted that SIP and SRTP traffic between the service provider and Avaya SBCE must be allowed to pass through these devices.

©2017 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment	**Release**
Avaya IP Office solution • Avaya IP Office 500V2 • Embedded Voicemail • Avaya Web RTC Gateway • Avaya one-X Portal • Avaya IP Office Manager • Avaya IP Office Analogue PHONE 8 • Avaya IP Office VCM64/PRID U • Avaya IP Office DIG DCPx16 V2	 10.1.0.0.0 build 237 10.1.0.0.0 build 237 10.1.0.0.0 build 13 10.1.0.0.0 build 305 10.1.0.0.0 build 237 10.1.0.0.0 build 237 10.1.0.0.0 build 237 10.1.0.0.0 build 237
Avaya Session Border Controller for Enterprise	7.2.0.0-18-13712
Avaya 1140E IP Deskphone (SIP)	04.04.23
Avaya 9641G IP Deskphone (H.323)	6.6.4.01
Avaya 9621G IP Deskphone (H.323)	6.6.4.01
Avaya Communicator for Windows (SIP)	2.1.4.0 - 256
Avaya Communicator for Web	1.0.16.1718
Avaya 1408D Digital Deskphone	R46
Avaya Analog Deskphone	N/A
HP Officejet 4500 (fax)	N/A
Line Systems Components	
Equipment	**Release**
Metaswitch	V9.1.10

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500V2 and also when deployed with IP Office in all configurations.

©2017 Avaya Inc. All Rights Reserved.

5. Configure Avaya IP Office Solution

This section describes the Avaya IP Office solution configuration necessary to support connectivity to the Avaya SBCE. It is assumed that the initial installation and provisioning of the Avaya IP Office 500V2 has been previously completed and therefore is not covered in these Application Notes. For information on these installation tasks refer to Additional References **Section 10**.

This section describes the Avaya IP Office configuration required to support connectivity to the Avaya SBCE. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window and click **OK** button. Log in using appropriate credentials.

Figure 2 – Avaya IP Office Selection

©2017 Avaya Inc. All Rights Reserved.

5.1. Licensing

The configuration and features described in these Application Notes require the Avaya 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.

To verify that there is a SIP Trunk Channels license with sufficient capacity, select **IPOffice_1 → License** on the Navigation pane and **SIP Trunk Channels** in the Group pane. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the **Details** pane.

Figure 3 – Avaya IP Office License

©2017 Avaya Inc. All Rights Reserved.

5.2. System Tab

Navigate to **System (1)** under **IPOffice_1** on the left pane and select the **System** tab in the **Details** pane. The **Name** field can be used to enter a descriptive name for the system. In the reference configuration, **IPOffice_1** was used as the name in IP Office.

Figure 4 - Avaya IP Office System Configuration

©2017 Avaya Inc. All Rights Reserved.

5.3. LAN2 Settings

In the sample configuration, LAN2 is used to connect the enterprise network to Avaya SBCE.

To configure the LAN2 settings on the IP Office, complete the following steps. Navigate to **IPOffice_1 → System (1)** in the **Navigation** and **Group** panes and then 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 LAN2 port. Set the **IP Mask** field to the mask used on the private network. All other parameters should be set according to customer requirements. Click **OK** to submit the change.

Figure 5 - Avaya IP Office LAN2 Settings

©2017 Avaya Inc. All Rights Reserved.

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

- Check the **H323 Gatekeeper Enable** to allow Avaya IP deskphones/softphones using the H.323 protocol to register
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Line Systems via Avaya SBCE
- Check the **SIP Registrar Enable** to allow Avaya IP deskphones/softphones to register using the SIP protocol
- Input **SIP Domain Name** as **10.10.98.14**
- The **Layer 4 Protocol** uses **TLS** with **TLS Port** as **5061**
- Verify **Keepalives** to select **Scope** as **RTP-RTCP** with **Periodic timeout 60** and select **Initial keepalives** as **Enabled**
- All other parameters should be set according to customer requirements
- Click **OK** to submit the changes

©2017 Avaya Inc. All Rights Reserved.

Figure 6 - Avaya IP Office LAN2 VoIP

©2017 Avaya Inc. All Rights Reserved.

5.4. System Telephony Settings

Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes (not shown) and then navigate to the **Telephony → Telephony** tab in the **Details** pane. Choose the **Companding Law** typical for the enterprise location. For North America, **U-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the service provider across the SIP trunk. Set **Hold Timeout (sec)** to a valid number. Set **Default Name Priority** to **Favor Trunk**. Defaults were used for all other settings. Click **OK** to submit the changes.

Figure 7 - Avaya IP Office Telephony

©2017 Avaya Inc. All Rights Reserved.

5.5. System VoIP Settings

Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes and then navigate to the **VoIP** tab in the **Details** pane. Leave the **RFC2833 Default Payload** as default of **101**. Select codec **G.729(a) 8K CS-ACEL**P, **G.711 ULAW 64K** which Line Systems supports. Click **OK** to submit the changes.

Figure 8 - Avaya IP Office VoIP

Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes and then navigate to the **VoIP Security** tab in the **Details** pane. Select **Media** as **Preferred** and select **Media Security Options** as highlights. Click **OK** to submit the changes.

Figure 9 - Avaya IP Office VoIP Security

©2017 Avaya Inc. All Rights Reserved.

5.6. Administer SIP Line

A SIP Line is needed to establish the SIP connection between Avaya IP Office and Avaya SBCE. 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 Avaya IP Office Manager to create a SIP Line. Follow the steps in **Section 5.6.1** to create the SIP Line from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.6.2**.

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.

Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Section 5.6.2**.

For the compliance test, SIP Line 17 was used as trunk for both outgoing and incoming calls.

©2017 Avaya Inc. All Rights Reserved.

5.6.1. Create SIP Line from Template

This section describes the steps to create a SIP line from the template as follows:

1. Create a new folder in computer where Avaya IP Office Manager is installed (e.g. C:\Line Systems\Template). Copy the template file to this folder. The template file for the compliance test is **LSIPO101SBC72.xml** (for SIP Line 17).
2. Import the template into Avaya IP Office Manager: From Avaya IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file from step 1 into the IP Office template directory.

Figure 10 – Import Template for SIP Line

In the pop-up window (not shown) that appears, select the folder where the template file was copied in step 1. After the import is complete, a final import status pop-up window below will appear stating success (or failure). Then click **OK** to continue.

Figure 11 – Import Template for SIP Line successfully

©2017 Avaya Inc. All Rights Reserved.

3. Create the SIP Trunk from the template: Right-click on **Line** in the Navigation Pane, then navigate to **New from Template → Open from file**.

Figure 12 – Create SIP Line from Template

©2017 Avaya Inc. All Rights Reserved.

4. Select the **Template Files (*.xml)** and select the imported template from step 2 at IP Office template directory **C:\Program Files\Avaya\IP Office\Manager\Templates**. Click **Open** button to create a SIP line from template.

Figure 13 – Create SIP Line from IP Office Template directory

©2017 Avaya Inc. All Rights Reserved.

A pop-up window below will appear stating success (or failure). Then click **OK** to continue.

Figure 14 – Create SIP Line from Template successfully

5. Once the SIP Line is created, verify the configuration of the SIP Lines with the configuration shown in **Section 5.6.2**.

©2017 Avaya Inc. All Rights Reserved.

5.6.2. Create SIP Line Manually

To create a SIP line, begin by navigating to **Line** in the left Navigation Pane, then right-click in the Group Pane and select **New → SIP Line** (not shown).

On the **SIP Line** tab in the Details Pane, configure the parameters as shown below:

- Select available **Line Number**: **17**
- Set **ITSP Domain Name** to the IP address of Avaya SBCE internal interface. This field is used to specify the default host part of the SIP URI in the To, R-URI fields for outgoing calls
- Set **Local Domain Name** to IP address of Avaya IP Office LAN2 port. This field is used to specify the default host part of the SIP URI in the From field for outgoing calls
  Note: For the user making the call, the user part of the From SIP URI is determined by the settings of the SIP URI channel record being used to route the call (see SIP URI → Local URI). For the destination of the call, the user part of the To and R-URI fields are determined by dial short codes of the form 9N;/N"@10.10.97.174" where N is the user part of the SIP URI and "@10.10.97.174" can be used to override the host part of the To and R-URI
- Check the **In Service** and **Check OOS** boxes
- Set **URI Type** to **SIP**
- For **Session Timers**, set **Refresh Method** to **Re-invite** with **Timer (sec)** to **1200**
- Set **Name Priority** to **Favor Trunk**. As described in **Section 5.4**, the **Default Name Priority** parameter may retain the default **Favor Trunk** setting, or can be configured to **Favor Directory**. As shown below, the default **Favor Trunk** setting was used in the reference configuration
- For **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Auto**. Note: Line Systems supported either SIP re-Invite or SIP Refer for off-net call transfer call during the compliance testing
- Default values may be used for all other parameters
- Click **OK** to commit then press Ctrl + S to save

Figure 15 – SIP Line Configuration

©2017 Avaya Inc. All Rights Reserved.

On the **Transport** tab in the Details Pane, configure the parameters as shown below:

- The **ITSP Proxy Address** was set to the IP address of Avaya SBCE internal interface: **10.10.97.174** as shown in **Figure 1**
- In the **Network Configuration** area, **TLS** was selected as the **Layer 4 Protocol** and the **Send Por**t was set to **5061**
- The **Use Network Topology Info** parameter was set to **None**. The **Listen Port** was set to **5061**. Note: For the compliance testing, the **Use Network Topology Info** field was set to **None**, since no NAT was using in the test configuration. In addition, it was not necessary to configure the **System → LAN2 → 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 (**LAN2**) used by the trunk and the **System → LAN2 → Network Topology** tab needs to be configured with the details of the NAT device
- The **Calls Route via Registrar** was unchecked. In this certification testing, Line Systems did not support the dynamic Registration on the SIP Trunk
- Other parameters retain default values
- Click **OK** to commit then press Ctrl + S to save

Figure 16 – SIP Line Transport Configuration

©2017 Avaya Inc. All Rights Reserved.

The SIP URI entry must be created to match any DID number assigned to an Avaya IP Office user and Avaya IP Office will route the calls on this SIP line. Select the **SIP URI** tab; click the **Add** button and the **New Channel** area will appear at the bottom of the pane (not shown). To edit an existing entry, click an entry in the list at the top, and click **Edit…** button. In the example screen below, a previously configured entry is edited.

A SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact**, and **Display Name** to **Use Internal Data**. This setting allows calls on this line whose SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.8**
- For **Identity**, set **Identity** to **Auto** and **Header** to **P Asserted ID**
- For **Forwarding And Twinning**, set **Send Caller ID** to **Diversion Header**
  Note: When using the twinning feature, the calling party number displayed on the twinned phone is controlled by the **Send Caller ID** parameter
- Leave **Diversion Header** to **None** by default
- Set **Registration** to **0: <None>**
- Associate this line with an incoming line group in the **Incoming Group** field and an outgoing line group in the **Outgoing Group** field. This line group number will be used in defining incoming and outgoing call routes for this line. For the compliance test, a new line group **17** was defined that only contains this line (line 17)
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern
- Click **OK** to submit the changes

©2017 Avaya Inc. All Rights Reserved.

Figure 17 – SIP Line SIP URI Configuration

©2017 Avaya Inc. All Rights Reserved.

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

- The **Codec Selection** can be selected by choosing **Custom** from the pull-down menu, allowing an explicit ordered list of codecs to be specified. The **G.711 ULAW 64K** and **G.729(a) 8K CS –ACELP** codecs are selected. Avaya IP Office supports these codecs, which are sent to Line Systems, in the Session Description Protocol (SDP) offer, in that order
- Check the **Re-invite Supported** box
- Set **Fax Transport Support** to **G.711** from the pull-down menu. Note: Line Systems supported only Fax G.711 pass-through mode during the compliance testing
- Set the **DTMF Support** to **RFC2833** from the pull-down menu. This directs Avaya IP Office to send DTMF tones using SRTP events messages as defined in RFC2833.
- Set **Media Security** as **Preferred**. Check **Same As System** box
- Default values may be used for all other parameters
- Click **OK** to submit the changes

©2017 Avaya Inc. All Rights Reserved.

Figure 18 – SIP Line VoIP Configuration

©2017 Avaya Inc. All Rights Reserved.

5.7. Outgoing Call Routing

The following section describes the Short Code for outgoing calls to Line Systems via Avaya SBCE.

5.7.1. Short Code

Define a short code to route outbound traffic on the SIP line to Line Systems via Avaya SBCE. To create a short code, select **Short Code** in the left Navigation Pane, then right-click in the Group Pane and select **New** (not shown). On the **Short Code** tab in the Details Pane, configure the parameters for the new short code to be created. The screen below shows the details of the previously administered "**9N;**" short code used in the test configuration.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **9N;**, 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"@10.10.97.174"**. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value **N** represents the number dialed by the user. The host part following the "@" is IP address of the Avaya SBCE internal interface
- Set the **Line Group ID** to the **Outgoing Group 17** defined on the **SIP URI** tab on the **SIP Line** in **Section 5.6.2**. This short code will use this line group when placing the outbound call
- Set the **Locale** to **United States (US English)**
- Default values may be used for all other parameters
- Click **OK** to submit the changes

Figure 19 – Short Code 9N

©2017 Avaya Inc. All Rights Reserved.

The feature of incoming calls from mobility extension to idle-appearance FNE (Feature Name Extension) is hosted by Avaya IP Office. The Short Code **FNE00** was configured with following parameters:

- For **Code** field, enter FNE feature code as **FNE00** for dial tone
- Set **Feature** to **FNE Service**
- Set **Telephone Number** to **00**
- Set **Line Group ID** to **0**
- Set the **Locale** to **United States (US English)**
- Default values may be used for other parameters
- Click **OK** to submit the changes

Figure 20 – Short Code FNE

©2017 Avaya Inc. All Rights Reserved.

5.8. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.6**. To configure these settings, first select **User** in the left Navigation Pane, then select the name of the user to be modified in the center Group Pane. In the example below, the name of the user is **4901**. 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 accordingly for outgoing SIP trunk calls. They also allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line. The example below shows the settings for user **4901**. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise provided by Line Systems. 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.

Figure 21 – User Configuration

©2017 Avaya Inc. All Rights Reserved.

One of the H.323 IP Deskphones at the enterprise site uses the Mobile Twinning feature. The following screen shows the **Mobility** tab for User 4901. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone, in this case **91613XXX7497**. Check **Mobile Call Control** to allow incoming calls from mobility extension to access FNE00 (defined in **Section 5.7.1**). Other options can be set according to customer requirements.

Figure 22 – Mobility Configuration for User

©2017 Avaya Inc. All Rights Reserved.

5.9. 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 service provider. To create an incoming call route, select **Incoming Call Route** in the left Navigation Pane, then right-click in the center Group Pane and select **New** (not shown). 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 Group 17** defined on the **SIP URI** tab on the **SIP Line** in **Section 5.6.2**.
- Set the **Incoming Number** to the incoming DID number on which this route should match.
- Default values can be used for all other fields.

Figure 23 – Incoming Call Route Configuration

On the **Destination** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **4845554901** on line 17 are routed to **Destination 4901 4901** as below screenshot:

Figure 24 – Incoming Call Route for Destination 4901

©2017 Avaya Inc. All Rights Reserved.

For Feature Name Extension Service testing purpose, the incoming calls to DID number **4845554904** were configured to access **FNE00**. The **Destination** was appropriately defined as **FNE00** as below screenshot:

Figure 25 – Incoming Call Route for Destination FNE

For Voice Mail testing purpose, the incoming calls to DID number **4845554905** were configured to access **VoiceMail**. The **Destination** was appropriately defined as **VoiceMail** as below screenshot:

Figure 26 – Incoming Call Route for Destination VoiceMail

5.10. 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.

©2017 Avaya Inc. All Rights Reserved.

6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of Avaya SBCE necessary for interoperability with the Avaya IP Office and Line Systems SIP Trunk Service.

Avaya elements reside on the Private side and the Line Systems SIP Trunk Service resides on the Public side of the network, as illustrated in **Figure 1**.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see relevant product documentation references in **Section 10** of these Application Notes.

6.1. Log in to the Avaya SBCE

Access the web interface by typing "**https://x.x.x.x/sbc/**" (where x.x.x.x is the management IP address of the Avaya SBCE).

Enter the **Username** and **Password**.

Figure 27 – Avaya SBCE Login

The **Dashboard** main page will appear as shown below.

Figure 28 - Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance test, a single Device Name **mSBCE** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.

Figure 29 - Avaya SBCE System Management

©2017 Avaya Inc. All Rights Reserved.

The **System Information** screen shows **General Configuration**, **Device Configuration**, **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**.

Figure 30 - Avaya SBCE System Information

©2017 Avaya Inc. All Rights Reserved.

6.2. 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. Avaya security products utilize TLS primarily to facilitate secure communications with remote users.

The server authentication comes into play for encrypted connections, such as TLS. The client initiates a request to the server for secure session, the server then sends its identity certificate to the client. The client checks the received server identity certificate against the trusted Certification Authority (CA) certificates that are saved in its trust store, to verify that the server identity certificate is indeed signed by a CA that the client trusts. There has to be a trusted CA, which is used to create and sign the server identity certificate.

The client authentication is similar to server authentication, except that the roles are reversed. The client authentication comes into play for encrypted connections with mutual authentication, and applies in addition to server authentication. The server also sends a request to the client for the client identity certificate, the client then sends its identity certificate to the server, and the server checks the received client identity certificate against the CA certificates that are saved in its trust store, to verify that the client identity certificate is indeed signed by a CA that the server trusts.

The following section describes TLS certificate installation so that clients authenticate servers or, optionally, servers authenticate clients.

©2017 Avaya Inc. All Rights Reserved.

6.2.1. Installing TLS Certificate

To manage TLS parameters for Line Systems site:

- Avaya provided the root certificate to install on Line System as Certificate Authority (CA) certificate. Besides, Line Systems also provided root certificate to install on Avaya SBCE as Certificate Authority (CA) certificate
- Once these procedures are completed, create a client profile and a server profile

The following procedures show how to install the certificates:

From the left hand site menu, select **TLS Management → Certificates** and click on **Install** button located in the upper-right hand

- Select **Type**: **Certificate** for installing the Identity Certificate, or **CA Certificate** for installing the root certificates
- Enter **Name**: **AvayaSBC** for installing Avaya Identity Certificate, **Line_System_CA** for installing Line Systems CA Certificate
- Click on **Allow Weak Certificate/Key** box
- Click **Browse** button to navigate to the **Certificate File**. Choose the certificates accordingly
- Check **Upload Key File** button in **Key** section (This option is only for installing the Certificate) and click **Browse** button to navigate to the **Key File**. Choose the keys accordingly
- Click **Upload** and then click **Install**

Figure 31 – Certificate Installation

©2017 Avaya Inc. All Rights Reserved.

The following screen shows the installed certificates.

Figure 32 – The installed certificates

Note: To manage TLS parameters for Avaya enterprise site is not mentioned in this document. There has to be a trusted CA, which is used to create and sign the server identity certificate. During the compliance test in the lab environment, demo certificates are used and are not recommended for production use. Consult the appropriate Avaya product documentation for further information regarding security certificate and encryption capabilities supported by Avaya product.

©2017 Avaya Inc. All Rights Reserved.

6.2.2. TLS Client Profile

From the menu on the left-hand side, select **TLS Management → Client Profiles**

- Select **Add** to create a TLS client profile
- Enter **Profile Name**: **Line_Systems_Client**
- Select **Certificate**: **AvayaSBC.crt**
- The **Peer Verification** is always **Required**
- Select **Peer Certificate Authorities**: **Line_Systems_CA.crt** to peer with Line Systems
- Enter **Verification Depth**: **5**
- Click **Next** and then click **Finish**

©2017 Avaya Inc. All Rights Reserved.

Figure 33 – TLS Client Profile - Line Systems site

©2017 Avaya Inc. All Rights Reserved.

6.2.3. TLS Server Profile

From the menu on the left-hand side, select **TLS Management → Server Profiles**

- Select **Add** to create a TLS server profile
- Enter **Profile Name**: **AvayaSBCServer**
- Select **Certificate**: **AvayaSBC.crt**
- Select **Peer Verification**: **None**
- Click **Next** and then click **Finish**

Figure 34 – TLS Server Profile – Line Systems site

©2017 Avaya Inc. All Rights Reserved.

6.3. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

6.3.1. Configure Server Interworking Profile – Avaya IP Office

Server Interworking profile allows administrator to configure and manage various SIP call server-specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Global Profiles → Server Interworking**

- Select **avaya-ru** in **Interworking Profiles**
- Click **Clone**
- Enter **Clone Name**: **IPO_14** and click **Finish** (not shown)

The following screen shows that Avaya IP Office server interworking profile (named: **IPO_14**) was added.

Figure 35 - Server Interworking – Avaya

©2017 Avaya Inc. All Rights Reserved.

6.3.2. Configure Server Interworking Profile – Line Systems

From the menu on the left-hand side, select **Global Profiles → Server Interworking → Add**

- Enter **Profile Name**: **SP4** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)

The following screen shows that Line Systems server interworking profile (named: **SP4**) was added.

Figure 36 - Server Interworking – Line Systems

©2017 Avaya Inc. All Rights Reserved.

6.3.3. Configure Server – Avaya IP Office

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server-specific parameters such as TLS port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**

Enter **Profile Name**: **IPO_14** (not shown).
On **General** tab, enter the following:

- **Server Type**: Select **Call Server**
- **TLS Client Profile**: Select **Avaya_IPO14**. Note: During the compliance test in the lab environment, demo certificates are used and are not recommended for production use. Consult the appropriate Avaya product documentation for further information regarding security certificate and encryption capabilities supported by Avaya product
- **IP Address/FQDN**: **10.10.98.14** (Avaya IP Office IP LAN2 port IP address)
- **Port**: **5061**
- **Transport**: **TLS**
- Click **Finish** (not shown)

Figure 37 – Avaya Server Configuration – General

©2017 Avaya Inc. All Rights Reserved.

On the **Advanced** tab:

- Check **Enable Grooming** box
- Select **IPO_14** for **Interworking Profile** (see **Section 6.3.1**)
- Click **Finish** (not shown)

Figure 38 – Avaya Server Configuration – Advanced

©2017 Avaya Inc. All Rights Reserved.

6.3.4. Configure Server – Line Systems

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**

Enter **Profile Name**: **SP4** (not shown)
On **General** tab, enter the following:

- **Server Type**: Select **Trunk Server**
- **TLS Client Profile**: Select **Line_Systems_Client** (Defined in **Section 6.2.2**)
- Add **IP Address/FQDN**: **192.168.66.42** (Line Systems Signaling Server IP address
- **Port**: **5061**
- **Transport**: **TLS**
- Click **Finish** (not shown)

Figure 39 - Line Systems Server Configuration – General

©2017 Avaya Inc. All Rights Reserved.

On the **Advanced** tab, enter the following:

- Check **Enable Grooming** box
- **Interworking Profile**: Select **SP4** (see **Section 6.3.2**)
- Click **Finish** (not shown)

Figure 40 - Line Systems Server Configuration – Advanced

©2017 Avaya Inc. All Rights Reserved.

6.3.5. Configure Routing – Avaya IP Office

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

Enter **Profile Name**: **To_IPO_14** and click **Next** button (not shown)

- Select **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**
- **Server Configuration**: **IPO_14** (see **Section 6.3.3**). This selection will automatically populate the **Next Hop Address** field with **10.10.98.14:5061 (TLS)** (Avaya IP Office LAN2 port IP address)
- Click **Finish**

Figure 41 - Routing to Avaya IP Office

©2017 Avaya Inc. All Rights Reserved.

6.3.6. Configure Routing – Line Systems

From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

Enter **Profile Name**: **To_SP4** (not shown)

- **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
  - **Priority/Weight**: **1**, **Server Configuration**: **SP4** (see **Section 6.3.4**). This selection will automatically populate the **Next Hop Address** field drop-down menu. Select **192.16.66.42:5061 (TLS)** (Line Systems Signaling IP Address)
- Click **Finish**

Figure 42 - Routing to Line Systems

©2017 Avaya Inc. All Rights Reserved.

6.3.7. Configure Topology Hiding – Avaya IP Office

The **Topology Hiding** screen allows an administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name**: **To_IPO_14** and click **Finish** (not shown)
- Select **To_IPO_14** in **Topology Hiding Profiles** and click **Edit** button to modify as below:
  For the Header **Request-Line**,
  - In the **Criteria** column, select **IP/Domain**
  - In the **Replace Action** column, select Overwrite
  - In the **Overwrite Value** column, enter **10.10.98.14** (Avaya IP Office LAN2 port IP address)

  For the Header **To**,
  - In the **Criteria** column, select **IP/Domain**
  - In the **Replace Action** column, select **Overwrite**
  - In the **Overwrite Value** column, enter **10.10.98.14** (Avaya IP Office LAN2 port IP address)

  For the Header **From**,
  - In the **Criteria** column, select **IP/Domain**
  - In the **Replace Action** column, select **Overwrite**
  - In the Overwrite Value column, enter **10.10.97.174** (Avaya SBCE internal IP address)
- Click **Finish** (not shown)

Figure 43 - Topology Hiding Avaya IP Office

©2017 Avaya Inc. All Rights Reserved.

6.3.8. Configure Topology Hiding – Line Systems

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name**: **To_SP4** and click **Finish** (not shown)

Figure 44 - Topology Hiding Line Systems

©2017 Avaya Inc. All Rights Reserved.

6.4. Domain Policies

The Domain Policies feature allows administrator to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or an administrator can create a custom domain policy.

6.4.1. Create Application Rules

Application Rules allow one to define which types of Avaya applications will be passed. The Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, one can determine the maximum number of concurrent voice and video sessions so that the network will process to prevent resource exhaustion. For the compliance test, the **SP4_IPO_14** application rule (shown below) was used for the End Point Policy Group defined in **Section 6.4.3**.

From the menu on the left-hand side, select **Domain Policies → Application Rules**

- Select the **default** rule and click on **Clone** button
- Enter **Clone Name**: **SP4_IPO_14** and click **Finish** button (not shown)
- Select the **SP4_IPO_14** rule from the list of **Application Rules** and click on **Edit** button
- Set **Maximum Concurrent Sessions** to **500** and **Maximum Sessions Per Endpoint** to **500**
- Click **Finish** button (not shown) to save the changes

Figure 45 – Application Rule

©2017 Avaya Inc. All Rights Reserved.

6.4.2. Create Media Rules

Media Rules allow one to define SRTP 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. For the compliance test, the predefined **default-high-enc** media rule (shown below) was used to clone for media rule.

From the menu on the left-hand side, select **Domain Policies → Media Rules**

- Select the **default-high-enc** rule, click **Clone**. Enter **Clone Name**: **SP4_IPO_14**. Click **Finish** (not shown)
- Select **SP4_IPO_14** under the list of **Media Rules** and click on **Edit** button to modify. The **Encryption** tab indicates that **SRTP_AES_CM_128_HMAC_SHA1_80** and **SRTP_AES_CM_128_HMAC_SHA1_32** encryption were used. Make sure to check **Encrypted RTCP** and leave Lifetime as blank to match any values.

Figure 46 – Media Rule - Encryption

©2017 Avaya Inc. All Rights Reserved.

6.4.3. Create Endpoint Policy Groups

The End-Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, and signaling, each of which was created using the procedures contained in the previous sections. A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**

- Select **Add**
- Enter **Group Name**: **SP4_IPO_14**
  - **Application Rule**: **SP4_IPO_14** (See **Section 6.4.1**)
  - **Border Rule**: **default**
  - **Media Rule**: **SP4_IPO_14** (See **Section 6.4.2**)
  - **Security Rule**: **default-med**
  - **Signaling Rule**: **default**
- Select **Finish** (not shown)

Figure 47 – End Point Policy

©2017 Avaya Inc. All Rights Reserved.

6.5. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

6.5.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
  - **Name**: **Network_A1**
  - **Default Gateway**: **10.10.97.129**
  - **Network Prefix or Subnet Mask**: **255.255.255.192**
  - **Interface**: **A1** (This is the Avaya SBCE internal interface)
  - Click the **Add** button to add the **IP Address** for inside interface: **10.10.97.174**
  - Click the **Finish** button to save the changes

Figure 48 - Network Management – Inside Interface

©2017 Avaya Inc. All Rights Reserved.

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
  - **Name**: **Network_A1**
  - **Default Gateway**: **10.10.97.129**
  - **Network Prefix or Subnet Mask**: **255.255.255.192**
  - **Interface**: **A1** (This is the Avaya SBCE internal interface)
  - Click the **Add** button to add the **IP Address** for inside interface: **10.10.97.174**
  - Click the **Finish** button to save the changes

Figure 49 - Network Management – Inside Interface

©2017 Avaya Inc. All Rights Reserved.

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select **Networks** tab and click the **Add** button to add a network for the external interface as follows:
  - **Name**: **Network_B1**
  - **Default Gateway**: **10.10.98.97**
  - **Network Prefix or Subnet Mask**: **255.255.255.224**
  - **Interface**: **B1** (This is the Avaya SBCE outside interface)
  - Click the **Add** button to add the **IP Address** for external interface: **10.10.98.106**
  - Click the **Finish** button to save the changes

Figure 50 - Network Management – External Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select the **Interfaces** tab
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state

Figure 51 - Network Management – Interface Status

©2017 Avaya Inc. All Rights Reserved.

6.5.2. Create Media Interfaces

Media Interfaces define the type of media on the ports. The default media port range on the Avaya SBCE can be used for both inside and outside ports.

From the menu on the left-hand side, **Device Specific Settings → Media Interface**

- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **InsideMedia**
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.97.174** (Avaya SBCE internal IP address toward Avaya IP Office)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)
- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **OutsideMedia**
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.106** (Avaya SBCE external IP address toward Line Systems)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)

The screen below shows the configured media interfaces:

Figure 52 - Media Interface

©2017 Avaya Inc. All Rights Reserved.

6.5.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**

- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **InsideSIP**
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.97.174** (Avaya SBCE internal IP address toward Avaya IP Office)
  - **TLS Port**: **5061**
  - **TLS Profile: IPO14**. Note: During the compliance test in the lab environment, demo certificates are used and are not recommended for production use. Consult the appropriate Avaya product documentation for further information regarding security certificate and encryption capabilities supported by Avaya product
  - Click **Finish** (not shown)

From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**

- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **OutsideSIP**
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.106** (Avaya SBCE external IP address toward Line Systems)
  - **TLS Port**: **5061**
  - **TLS Profile: AvayaSBCServer**. Note: During the compliance test in the lab environment, demo certificates are used and are not recommended for production use. Consult the appropriate Avaya product documentation for further information regarding security certificate and encryption capabilities supported by Avaya product
  - Click **Finish** (not shown)

The screen below shows the configured signaling interfaces:

Figure 53 - Signaling Interface

©2017 Avaya Inc. All Rights Reserved.

6.5.4. Configuration Server Flows

Server Flows allow an administrator to categorize signaling and apply various policies.

6.5.4.1 Create End Point Flows – Avaya IP Office

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**

- Select the **Server Flows** tab
- Select **Add**, enter the followings:
  - **Flow Name**: **IPO Flow**
  - **Server Configuration**: **IPO_14** (see **Section 6.3.3**)
  - **URI Group**: *****
  - **Transport**: *****
  - **Remote Subnet**: *****
  - **Received Interface**: **OutsideSIP** (see **Section 6.5.3**)
  - **Signaling Interface**: **InsideSIP** (see **Section 6.5.3**)
  - **Media Interface**: **InsideMedia** (see **Section 6.5.2**)
  - **Secondary Media Interface**: **None**
  - **End Point Policy Group**: **SP4_IPO_14** (see **Section 6.4.3**)
  - **Routing Profile**: **To_SP4** (see **Section 6.3.6**)
  - **Topology Hiding Profile**: **To_IPO_14** (see **Section 6.3.7**)
  - Leave other options as default
  - Click **Finish**

©2017 Avaya Inc. All Rights Reserved.

Figure 54 - End Point Flow to Line Systems

6.5.4.2 Create End Point Flows – Line Systems

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**

- Select the **Server Flows** tab
- Select **Add**, enter the followings:
  - **Flow Name**: **SP4 Flow**
  - **Server Configuration**: **SP4** (see **Section 6.3.4**)
  - **URI Group**: *****
  - **Transport**: *****
  - **Remote Subnet**: *****
  - **Received Interface**: **InsideSIP** (see **Section 6.5.3**)
  - **Signaling Interface**: **OutsideSIP** (see **Section 6.5.3**)
  - **Media Interface**: **OutsideMedia** (see **Section 6.5.2**)
  - **Secondary Media Interface**: **None**
  - **End Point Policy Group**: **SP4_IPO_14** (see **Section 6.4.3**)
  - **Routing Profile**: **To_IPO_14** (see **Section 6.3.5**)

©2017 Avaya Inc. All Rights Reserved.

- **Topology Hiding Profile**: **To_SP4** (see **Section 6.3.8**)
- Leave other options as default
- Click **Finish**

Figure 55 - End Point Flow from Line Systems

©2017 Avaya Inc. All Rights Reserved.

7. Line Systems SIP Trunk Configuration

Line Systems is responsible for the configuration of Line Systems SIP Trunk Service. The customer must provide the IP address used to reach the Avaya SBCE at the enterprise. Line Systems will provide the customer necessary information to configure the SIP connection between Avaya SBCE and Line Systems. The provided information from Line Systems includes:

- IP address and port number used for signaling or media servers through any security devices
- DID numbers
- Line Systems SIP Trunk Specification (if applicable)

©2017 Avaya Inc. All Rights Reserved.

8. Verification Steps

The following steps may be used to verify the configuration:

- Use the Avaya IP Office System Status application to verify the state of the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select the SIP Line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** for each channel. (The below screen shot showed 2 active calls at the time.)

Figure 56 – SIP Trunk status

©2017 Avaya Inc. All Rights Reserved.

- Use the Avaya IP Office System Status application to verify that no alarms are active on the SIP line. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select **Alarm → Trunks** to verify that no alarms are active on the SIP line.

Figure 57 – SIP Trunk alarm

- Verify that a phone connected to the PSTN can successfully place a call to Avaya IP Office with two-way audio.
- Verify that a phone connected to Avaya IP Office can successfully place a call to the PSTN with two-way audio.
- Capture SIP call traces on Avaya SBCE by executing command via the Command Line Interface (CLI): Login Avaya SBCE with root user and enter the command: #traceSBC. The tool updates the database directly based on which trace mode is selected.

©2017 Avaya Inc. All Rights Reserved.

9. Conclusion

Line Systems passed compliance testing with the limitation listed in **Section** . These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 10.1 and the Avaya SBCE 7.2 to support Line Systems SIP Trunking service, as shown in **Figure 1**.

10. Additional References

[1] Administering Avaya IP Office Platform with Manager, Release 10.1, 15-601011, Issue 14, July 2017.

[2] Deploying Avaya IP Office™ Platform IP500V2, Release 10.1, 15-601042, Issue 32d, May 2017.

[3] Avaya IP Office™ Platform Release 10.1 - Release Notes / Technical Bulletin General Availability

[4] Avaya Session Border Controller for Enterprise 7.2 Release Notes, Issue 1, June 2017

Product documentation for Avaya products may be found at: http://support.avaya.com. Additional IP Office documentation can be found at:
http://marketingtools.avaya.com/knowledgebase/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf_feed_template.html

Product documentation for Line Systems SIP Trunking may be found at:
http://www.linesystems.com/services/voice/

©2017 Avaya Inc. All Rights Reserved.

11. Appendix - Remote Worker Configuration via Avaya SBCE

This section describes the process for connecting remote Avaya SIP endpoints on the public Internet to Avaya IP Office on the private enterprise network via the Avaya SBCE. The provisioning builds on the reference configuration described in previous sections of this document.

For more information, refer to **Section 10**.

Note – This Remote Worker configuration is based on provisioning the Avaya SBCE. It is not to be confused with "native" Avaya IP Office Remote Worker configurations.

In the configuration for the compliance test, Avaya Communicator for Windows (SIP mode) was used as the Remote Worker SIP endpoint.

The reference configuration for the compliance test, including the Remote Worker endpoint, is shown in **Figure 1** in **Section 3**.

©2017 Avaya Inc. All Rights Reserved.

11.1. Provisioning Avaya SBCE for Remote Worker

Provisioning of the Avaya SBCE to support Avaya IP Office SIP connection to the service provider is described in **Section 6**. The following sections build on that provisioning.

11.1.1. Network Management

This section shows the **Network Management** configuration of the Avaya SBCE to support Remote Worker. For this purpose, the Avaya SBCE is configured with a second outside IP address assigned to physical interface B1, and a second inside IP address assigned to physical interface A1.

The following IP addresses were used on the Avaya SBCE in the configuration used for the compliance test:

- **10.10.97.174** is the inside IP address previously provisioned for SIP Trunking with Avaya IP Office (see **Section 6.5.1**).
- **10.10.97.173** is the new inside IP address for Remote Worker.
- **10.10.98.106** is the outside IP address previously provisioned for SIP Trunking with Line Systems (see **Section 6.5.1**).
- **10.10.98.102** is the new outside IP address for Remote Worker.

On the **Networks** tab, select **Add** to create an entry for **10.10.97.173** on interface **A1**, then select **Save** (not shown).
On the **Networks** tab, select **Add** to create an entry for **10.10.98.102** on interface **B1**, then select **Save** (not shown).

Figure 58 – Remote Worker Network Management

©2017 Avaya Inc. All Rights Reserved.

11.1.2. Signaling Interfaces

Two new Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic. Both interfaces **InsideRW** and **OutsideRW** support **TLS Port 5061**.

From **Device Specific Settings** on the left-hand menu, select **Signaling Interface**. Click on the **Add** button to create Signaling Interface **InsideRW**

- **Signaling IP = 10.10.97.173**
- **TLS Port = 5061**
- **TLS Profile: IPO14**

From **Device Specific Settings** on the left-hand menu, select **Signaling Interface**. Click on the **Add** button to create Signaling Interface **OutsideRW**

- **Signaling IP = 10.10.98.102**
- **TLS Port = 5061**
- **TLS Profile: AvayaSBCServer**

Figure 59 – Remote Worker Signaling Interface

Signaling Interface **InsideRW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.9.2**). Signaling Interface **OutsideRW** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.9.1**), and in the Remote Worker Server Flow (Refer to **Section 11.1.9.2**).

©2017 Avaya Inc. All Rights Reserved.

11.1.3. Media Interface

Two new Media interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

From **Device Specific Settings** on the left-hand menu, select **Media Interface**. Click on the **Add** button to create Media Interface **InsideRW** using the parameters shown below:

- **Media IP** = **10.10.97.173**
- **Port Range** = **35000 – 40000**

From **Device Specific Settings** on the left-hand menu, select **Media Interface**. Click on the **Add** button to create Media Interface **OutsideRW** using the parameters shown below:

- **Media IP** = **10.10.98.102**
- **Port Range** = **35000 – 40000**

Figure 60 – Remote Worker Media Interface

Media Interface **InsideRW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.9.2**). Media Interface **OutsideRW** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.9.1**).

©2017 Avaya Inc. All Rights Reserved.

11.1.4. Server Profile for Avaya IP Office

The existing **IPO_14** Server Profile (see **Section 6.3.3**) is used for Remote Worker.

Figure 61 – Remote Worker Server Configuration

©2017 Avaya Inc. All Rights Reserved.

11.1.5. Routing Profiles

Two Routing Profiles are required to support Remote Worker
The existing **To_IPO_14** Routing (see **Section 6.3.5**) is used for Remote Worker.

Figure 62 – Remote Worker Routing

©2017 Avaya Inc. All Rights Reserved.

From the menu on the left-hand side, select **Global Profiles → Routing**, select the existing **default Routing Profiles** and click on the **Clone** button, and name it **default_RW** and click **Finish** (not shown) to submit the changes. The **default_RW** was created as below.

Figure 63 – Remote Worker Default Routing

The Routing Profile **To_IPO_14** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.9.1**). The Routing Profile **default_RW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.9.2**).

©2017 Avaya Inc. All Rights Reserved.

11.1.6. User Agent

User Agents are created for each type of Remote Worker endpoint used. In the compliance test, the Avaya Communicator for Windows (SIP) softphone was used, and its configuration is shown below. From the menu on the left-hand side, select **Global Parameters → User Agents**, and click **Add** button to create a new User Agent.

Enter the following:

- **Name** = **Avaya Communicator**
- **Regular Expression = Avaya Flare Engine.***

In this expression, "Avaya Flare Engine.*" will match any software version listed after the user agent name.

Figure 64 – Remote Worker User Agent

The **Avaya Communicator** User Agent is defined in the Remote Worker Subscriber Flow (see **Section 11.1.9.1**).

©2017 Avaya Inc. All Rights Reserved.

11.1.7. Create Media Rules for Remote Worker

From the menu on the left-hand side, select **Domain Policies → Media Rules**

- Select the **default-high-enc** rule, click **Clone**. Enter **Clone Name**: **SP4_IPO_14_RW**. Click **Finish** (not shown)
- Select **SP4_IPO_14_RW** under the list of **Media Rules** and click on **Edit** button to modify The **Encryption** tab indicates that **SRTP_AES_CM_128_HMAC_SHA1_80** and **SRTP_AES_CM_128_HMAC_SHA1_32**, and **RTP** were used as **Preferred Formats** Leave other parameters as default

Figure 65 – Media Rule - Encryption

©2017 Avaya Inc. All Rights Reserved.

11.1.8. End Point Policy Groups

The End Point Policy Group is defined for Remote Worker. Group **SP4_IPO_14_RW** is defined for the RW connection.

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**

- Select **Add** button to create a new End Point Policy Group
- Enter a name (e.g., **SP4_IPO_14_RW**), and click on **Next** (not shown)
- The **Policy Group** window will open. Select the information as shown in capture below

Figure 66 – Remote Worker Endpoint Policy Group

End Point Policy Group **SP4_IPO_14_RW** is used in the Subscriber Flow (Refer to **Section 11.1.9.1**) and in the Server Flow (Refer to **Section 11.1.9.2**).

©2017 Avaya Inc. All Rights Reserved.

11.1.9. End Point Flows

A Subscriber Flow and a Server Flow are created for Remote Worker.

11.1.9.1 Subscriber Flow

A **Subscriber Flow** is defined as follows:
From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**.
On **Subscriber Flows** tab, click on **Add** and the **Criteria** window will open.

- Enter **Flow Name** (e.g., **Avaya Communicator**).
- **URI Group** = *****
- **User Agent** = **Avaya Communicator** (Refer to **Section 11.1.6**)
- **Source Subnet** = ***** (default)
- **Via Host** = ***** (default)
- **Contact Host** = ***** (default)
- **Signaling Interface** = **OutsideRW** (Refer to **Section 11.1.2**)

Figure 67 – Remote Worker Subscriber Flow 1

©2017 Avaya Inc. All Rights Reserved.

Click on **Next** and the **Profile** window will open. Enter the followings:

- **Source** = **Subscriber**
- **Methods Allowed Before REGISTER**: Leave as default.
- **Media Interface** = **OutsideRW** (Refer to **Section 11.1.3**)
- **Secondary Media Interface = None**
- **Received Interface = None**
- **End Point Policy Group = SP4_IPO_14_RW** (Refer to **Section 11.1.8**)
- **Routing Profile = To_IPO_14** (Refer to **Section 11.1.5**)
- **TLS Client Profile** = **None**
- **Signaling Manipulation Script** = **None**
- **Presence Server Address** = **Blank**
- Click **Finish** to submit the changes.

©2017 Avaya Inc. All Rights Reserved.

Figure 68 – Remote Worker Subscriber Flow 2

©2017 Avaya Inc. All Rights Reserved.

The **Subscriber Flows** tab shown below displays the finished Subscriber Flow **Avaya Communicator**.

Figure 69 – Remote Worker Subscriber Flow 3

©2017 Avaya Inc. All Rights Reserved.

Click on the highlighted **View** link brings up the following **View Flow** window.

Figure 70 – Remote Worker Subscriber Flow 4

11.1.9.2 Server Flow

The following section shows the new **Server Flow** settings for Remote Worker. The new Remote Worker Server Flow (IPO_14_RW) is configured for the SIP traffic flow from Avaya IP Office to Remote Worker via Avaya SBCE.

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**

On **Server Flows** tab, click on **Add** to create a new server flow for Remote Worker

Enter the following:

- **Flow Name = IPO_14_RW**
- **Server Configuration** = **IPO_14** (Refer to **Section 11.1.4**)

©2017 Avaya Inc. All Rights Reserved.

- **URI Group** = ***** (default)
- **Transport** = ***** (default)
- **Remote Subnet** = ***** (default)
- **Received Interface** = **OutsideRW** (Refer to **Section 11.1.2**)
- **Signaling Interface** = **InsideRW** (Refer to **Section 11.1.2**)
- **Media Interface** = **InsideRW** (Refer to **Section 11.1.3**)
- **Secondary Media Interface = None**
- **End Point Policy Group** = **SP4_IPO_14_RW** (Refer to **Section 11.1.8**)
- **Routing Profile** = **default_RW** (Refer to **Section 11.1.5**)
- **Topology Hiding Profile** = **None**
- **Signaling Manipulation Script** = **None**
- **Remote Branch Office** = **Any**
- Click **Finish** to submit the changes

Figure 71 – Remote Worker Server Flow 1

©2017 Avaya Inc. All Rights Reserved.

If the Remote Worker server flow is listed ahead of the flow for SIP Trunking **IPO Flow** (defined in **Section 6.5.4.1**), enter **2** in the **Priority** box at the start of the Remote Worker flow entry and click the **Update** button under the server name. The completed flow should show up in the **Server Flows** tab as below.

Figure 72 – Remote Worker Server Flow 2

©2017 Avaya Inc. All Rights Reserved.

11.2. Remote Worker Endpoint Configuration on Avaya IP Office

The Remote Worker - Avaya Communicator for Windows endpoint is added to the Avaya IP Office **User** and **Extension** configuration.

11.2.1. Extension and User Configuration

No special configurations are required to create the Remote Worker extension and user in Avaya IP Office. Follow the same standard procedures for creating a local extension and user for Avaya Communicator for Windows.

The Remote Worker user provisioned is shown below. Note that since the Remote Worker endpoint used in the reference configuration is Avaya Communicator for Windows, the **Enable Softphone** and **Enable Communicator** options are selected.

Note: Do not check the **Enable Remote Worker** option. This is only enabled for Avaya IP Office "native" Remote Worker configurations, not for Remote Worker configurations utilizing the Avaya SBCE.

Figure 73 – Remote Worker User Configuration 1

©2017 Avaya Inc. All Rights Reserved.

The **SIP** tab for the Remote User is configured the same way as with a local Avaya IP Office user (see **Section 5.8**).

Figure 74 – Remote Worker User Configuration 2

11.2.2. Incoming Call Route

Follow the same procedures described in **Section 5.9** for defining an Incoming Call Route to the Remote Worker.

Figure 75 – Remote Worker Incoming Call Route

©2017 Avaya Inc. All Rights Reserved.

11.3. Remote Worker - Avaya Communicator for Windows Settings

The following screen illustrates Avaya Communicator for Windows administration settings for Remote Worker as used in the reference configuration.

After opening the Avaya Communicator for Windows application, select the **Settings** icon, select **Server** from the Settings menu, and enter the following:

- **Server address** = **10.10.98.102** (IP address of Remote Worker outside interface B1 on Avaya SBCE (see **Section 11.1.1**)
- **Server port** = **5061**
- **Transport type** = **TLS**
- **Domain** = **10.10.98.14** (SIP Domain Name was defined in LAN1→ VoIP tab in **Section 5.3**)
- Click **OK** the save the changes.

Figure 76 – Remote Worker - Avaya Communicator for Windows Settings

©2017 Avaya Inc. All Rights Reserved.

Note: For this compliance testing, only audio calls were tested with RTP media for Avaya Communicator for Windows.

©2017 Avaya Inc. All Rights Reserved.

©2017 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.