Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Cox Communications SIP Trunking with Avaya IP Office 11.1 and Avaya Session Border Controller for Enterprise 8.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking service between service provider Cox Communications and Avaya IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 8.1.

Cox Communications SIP Trunk Service provides PSTN access via a SIP trunk between the enterprise and the Cox Communications 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.

Cox Communications 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.

©2021 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 ... 6
3. Reference Configuration ... 7
4. Equipment and Software Validated ... 10
5. Configure Avaya IP Office Solution ... 11
   5.1. Licensing ... 13
   5.2. TLS Management ... 13
   5.3. System Settings ... 14
      5.3.1. System – LAN1 Tab ... 14
      5.3.2. System – Telephony Tab ... 18
      5.3.3. System – VoIP Tab ... 19
   5.4. IP Route ... 20
   5.5. Administer SIP Line ... 22
      5.5.1. Create SIP Line from an XML Template ... 23
      5.5.2. Create SIP Line Manually ... 26
   5.6. IP Office Line in Primary System ... 33
   5.7. IP Office Line in Expansion System ... 35
   5.8. Outbound Short Code ... 37
   5.9. User ... 40
   5.10. Incoming Call Route ... 43
   5.11. Save Configuration ... 44
6. Configure Avaya Session Border Controller for Enterprise ... 45
   6.1. Log in to the Avaya SBCE ... 45
   6.2. Server Interworking ... 48
      6.2.1. Configure Server Interworking Profile – Avaya IP Office ... 48
      6.2.2. Configure Server Interworking Profile – Cox Communications ... 49
   6.3. Configure SIP Server ... 50
      6.3.1. Configure SIP Server – Avaya Site ... 50
      6.3.2. Configure SIP Server – Cox Communications ... 53
   6.4. Routing ... 56
      6.4.1. Configure Routing – Avaya IP Office ... 56
      6.4.2. Configure Routing – Cox Communications ... 58
   6.5. Configure Topology Hiding ... 59
      6.5.1. Configure Topology Hiding – Avaya Site ... 59
      6.5.2. Configure Topology Hiding – Cox Communications ... 60
   6.6. Domain Policies ... 61
      6.6.1. Create Application Rules ... 61
      6.6.2. Create Media Rules ... 61
      6.6.3. Create Endpoint Policy Groups ... 63
   6.7. Network & Flows ... 65
      6.7.1. Manage Network Settings ... 65

©2021 Avaya Inc. All Rights Reserved.

6.7.2. Create Media Interfaces ... 68
6.7.3. Create Signaling Interfaces ... 69
6.7.4. Configure Server Flows ... 70
7. Cox Communications SIP Trunk Configuration ... 72
8. Verification Steps ... 73
9. Conclusion ... 75
10. Additional References ... 75
11. Appendix A - Remote Worker Configuration via Avaya SBCE ... 76
11.1. Network Management on Avaya SBCE ... 77
11.2. Media Interface on Avaya SBCE ... 78
11.3. Signaling Interface on Avaya SBCE ... 79
11.4. Routing Profile on Avaya SBCE ... 80
11.5. User Agent on Avaya SBCE ... 82
11.6. End Point Policy Groups on Avaya SBCE ... 84
11.7. End Point Flows on Avaya SBCE ... 85
11.7.1. Subscriber Flow ... 85
11.7.2. Server Flow ... 87
11.8. Remote Worker Endpoint Configuration on Avaya IP Office ... 91
11.8.1. Extension and User Configuration ... 91
11.8.2. Incoming Call Route ... 92
11.9. Remote Worker - Avaya Workplace for Windows Settings ... 93
12. Appendix B - Cox managed CPE Configuration ... 95
12.1. Cox managed CPE Login ... 96
12.2. Network Configuration ... 97
12.3. VLAN Configuration ... 99
12.4. VoIP Settings ... 100
12.5. ALG Trunking Configuration ... 102
12.6. SIP Routing Configuration ... 104

©2021 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking service between Cox Communications and an Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of Avaya IP Office Server Edition Release 11.1, Avaya IPO Voicemail Pro, Avaya IP Office Application Server (with WebRTC and one-X Portal services enabled), Avaya Workplace for Windows (SIP mode), 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 Cox Communications network via the Avaya Session Border Controller for Enterprise (Avaya SBCE).

The Cox Communications 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 Cox Communications 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 Cox Communications 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.

©2021 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

A simulated enterprise site with Avaya IP Office and Avaya SBCE was connected to Cox Communications via Cox managed CPE. 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 Workplace for Windows (SIP)
- 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 (WebRTC) 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, outbound call to 411 and 911 services
- SIP transport UDP/RTP between Cox Communications and the simulated Avaya enterprise site
- Codec G.711MU
- Caller number/ID presentation
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls
- DTMF transmission using RFC 2833
- SIP Registration and Authentication
- SIP OPTIONS queries and responses
- Voicemail navigation for inbound and outbound calls
- Telephony features such as hold and resume, transfer, and conference
- G.711 pass-through and T.38 fallback fax
- Off-net call forwarding
- Off-net call transfer
- Twinning to mobile phones on inbound calls
- Remote Worker. Avaya Workplace for Windows (SIP) was used to test remote worker functionality

Item not supported include the following:

- TLS/SRTP SIP transport to Cox Communications
- The implementation of STIR/SHAKEN by Cox Communications have yet to fully enable, therefore it was not tested during the compliance testing
- The SIP REFER in the off-net call redirection was not tested during the compliance testing because Cox Communications did not fully support it. Cox Communications confirmed that SIP REFER is only supported without sending a NOTIFY message. Therefore, the SIP RE-INVITE was tested in the off-net call redirection instead

©2021 Avaya Inc. All Rights Reserved.

2.2. Test Results

Interoperability testing of Cox Communications was completed with successful results for all test cases with the exception of the observation described below:

- The Cox managed CPE did not forward Diversion header (or PAI header) to Cox Communications network in off-net call forward - Although the Cox managed CPE did not forward Diversion header (or PAI header) to Cox Communications network in off-net call forward, the off-net call forward still worked successfully. As far as Cox Communications is aware, this issue should be fixed in new EdgeMarc firmware load (Potentially 15.7.0 and higher firmware)

2.3. Support

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

For technical support on Cox Communications SIP Trunking, contact Cox Communications at http://www.cox.com.

©2021 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to Cox Communications 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:

- IP Office Server Edition Primary Server
- IP Office Voicemail Pro
- IP Office Server Edition Expansion System (IP500 V2)
- WebRTC and one-X Portal services
- Avaya Session Border Controller for Enterprise
- Avaya 96x1 Series IP Deskphones (H.323)
- Avaya 11x0 Series IP Deskphones (SIP)
- Avaya J129 IP Deskphones (SIP)
- Avaya 1408 Digital phones
- Avaya Analog phones
- Avaya Communicator for Web
- Avaya Communicator for Windows (SIP)
- Avaya Workplace for Windows (SIP)
- Avaya Workplace for Windows (SIP) for remote worker

The Primary Server consists of a Dell PowerEdge R640 server, running the Avaya IP Office Server Edition Linux software Release 11.1. Avaya Voicemail Pro runs as a service on the Primary Server. The LAN1 port of Avaya IP Office is connected to Avaya SBCE internal interface. The Avaya SBCE external interface is connected to LAN port of the Cox managed CPE (This device is included as part of the Service Provider service and not as part of the CPE solution – See **Section** Error! Reference source not found. **Appendix B** in details). The WAN port of Cox managed CPE is connected to Cox Communications' network via public network.

The optional Expansion System (IP500 V2) is used for the support of digital, analog, fax, and additional IP stations. It consists of an Avaya IP Office IP500 V2 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.

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.

©2021 Avaya Inc. All Rights Reserved.

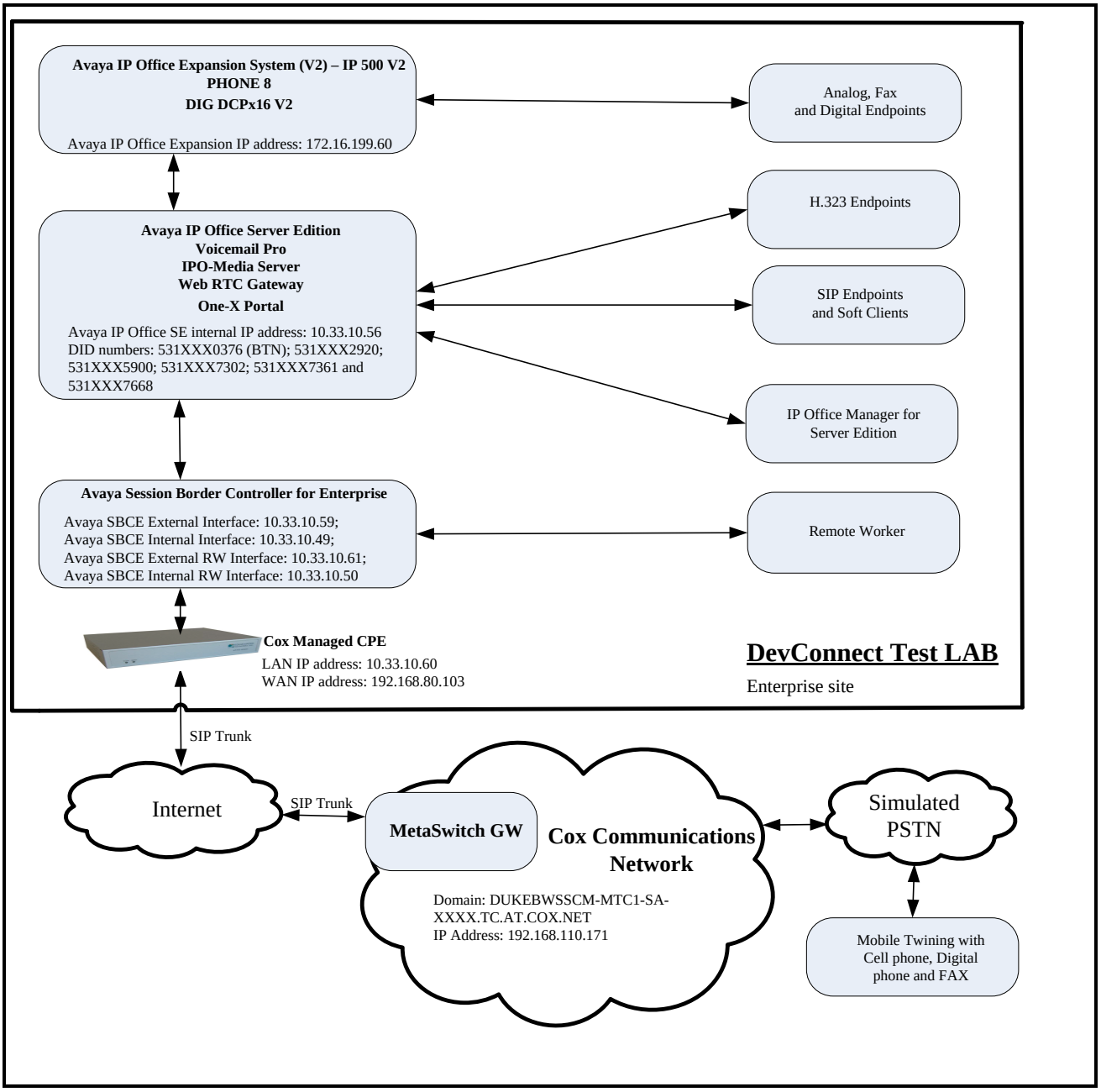


Figure 1 - Test Configuration for Avaya IP Office with Cox Communications SIP Trunk Service

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 Cox Communications. The short code of 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Cox Communications. 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

©2021 Avaya Inc. All Rights Reserved.

an outbound SIP INVITE message. It was configured to send 10 digits in the From field. For inbound calls, Cox Communications 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. However, it should be noted that SIP and RTP traffic between the service provider and Avaya SBCE must be allowed to pass through these devices.

©2021 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya IP Office Server Edition solution ▪ Primary Server Dell PowerEdge R640 – IPO-Linux-PC ▪ IPO-Media Server ▪ Voicemail Pro ▪ Web RTC Gateway ▪ one-X Portal ▪ IP Office Manager for Server Edition ▪ IP Office Expansion System (V2) – IP 500 V2 ▪ IP Office Analogue - PHONE 8 ▪ IP Office Digital - DIG DCPx16 V2	 11.1.1.0.0 build 209 11.1.1.0.0 build 209 11.1.1.0.0 build 152 11.1.1.0.0 build 8 11.1.1.0.0 build 111 11.1.1.0.0 build 209 11.1.1.0.0 build 209 11.1.1.0.0 build 209 11.1.1.0.0 build 209
Avaya Session Border Controller for Enterprise	8.1.2.0-31-19809
Avaya 1140E IP Deskphone (SIP)	04.04.33
Avaya 9641G IP Deskphone (H323)	6.8.5.02
Avaya 9621G IP Deskphone (H323)	6.8.5.02
Avaya J129 IP Deskphone (SIP)	4.0.7.1.5
Avaya Communicator for Windows	2.1.4.0 Build 324
Avaya Communicator for Web	1.0.20.1722
Avaya Workplace for Windows	3.15.0.64.17
Avaya 1408D Digital Deskphone	R48
Avaya Analog Deskphone	N/A
VentaFax	7.10.258.664
Cox Communications	
Cox managed CPE	14.9.7
MetaSwitch GW	4.7.40

©2021 Avaya Inc. All Rights Reserved.

5. Configure Avaya IP Office Solution

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

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

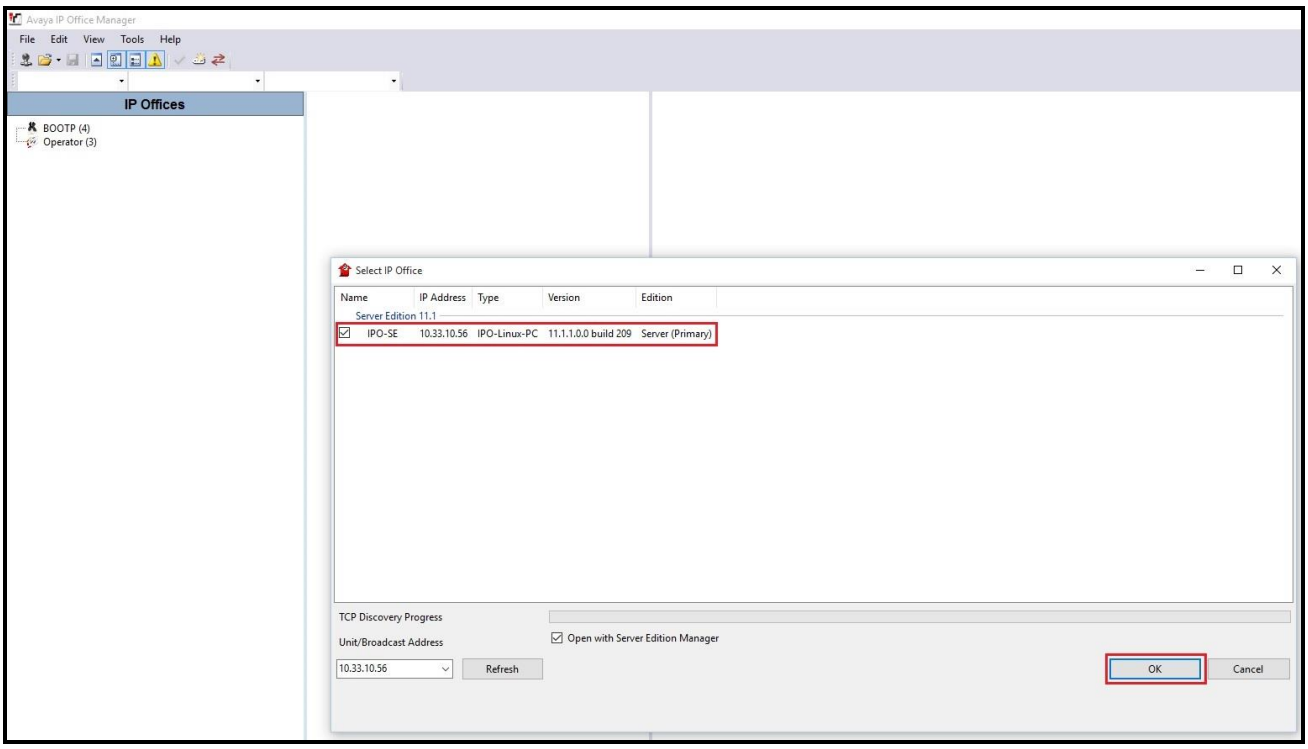


Figure 2 – Avaya IP Office Server Edition Selection

©2021 Avaya Inc. All Rights Reserved.

The appearance of the Avaya IP Office Server Edition Manager can be customized using the **View** menu. In the screens presented in this section, it includes the system inventory of the servers and links for administration and configuration tasks.

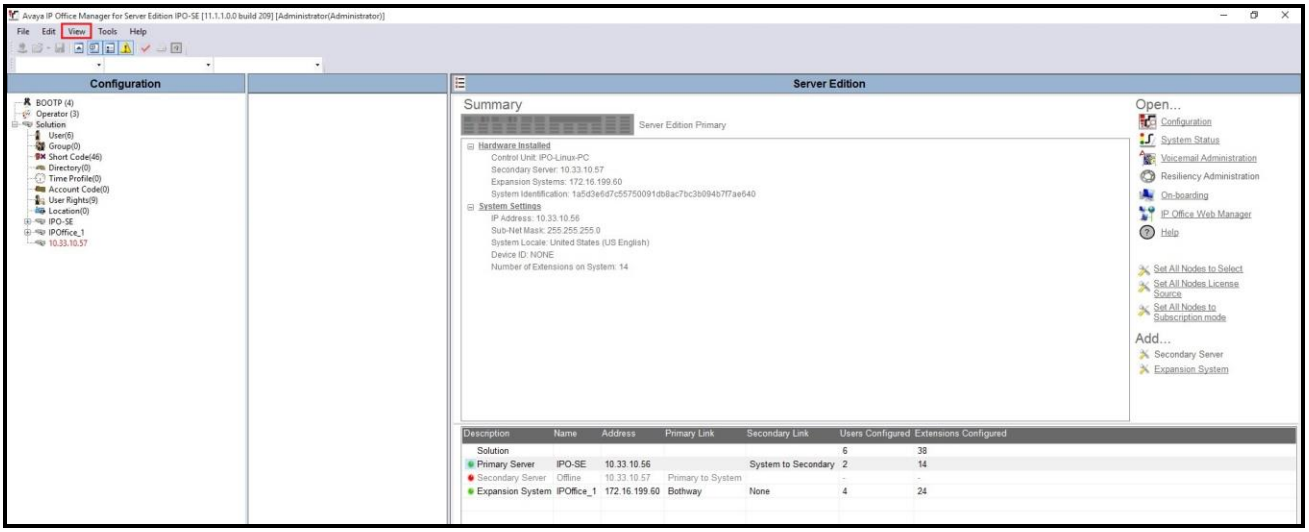


Figure 3 – Avaya IP Office Server Edition View Menu

©2021 Avaya Inc. All Rights Reserved.

5.1. Licensing

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

Licenses for an Avaya IP Office Server Edition solution are based on a combination of centralized licensing done through the Avaya IP Office Server Edition Primary Server, and server specific licenses that are entered into the configuration of the system requiring the feature. SIP Trunk Channels are centralized licenses, and they are entered into the configuration of the Primary Server. Note that when centralized licenses are used to enable features on other systems, such as SIP trunk channels, the Primary Server allocates those licenses to the other systems only after it has met its own license needs. To verify that there is a SIP Trunk Channels license with sufficient capacity, select **Solution → IPO-SE → 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. Note that the actual License Key in the screen below was edited for security purposes.

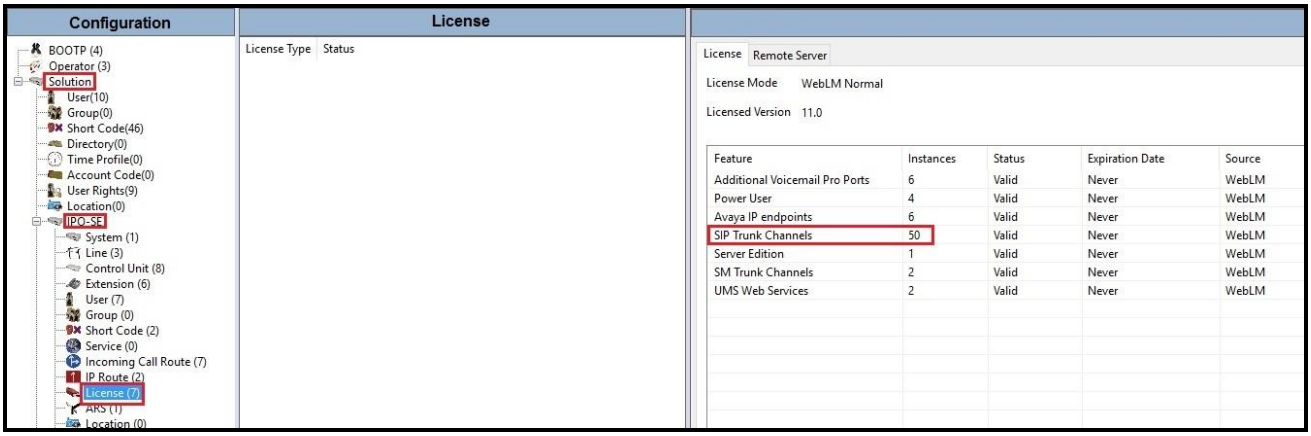


Figure 4 – Avaya IP Office Server Edition License

5.2. TLS Management

For the compliance test, the signaling on the SIP trunk between IP Office and the Avaya SBCE was secured using TLS. Testing was done using identity certificates signed by a local certificate authority, Avaya Aura® System Manager. The generation and installation of these certificates are beyond the scope of these Application Notes. However, once the certificates are available, they can be viewed on IP Office in the following manner.

To view the certificates currently installed on IP Office, navigate to **File → Advanced → Security Settings**. Log in with the appropriate security credentials (not shown). In the Security Settings window, navigate to **Security → System** and select the **Certificates** tab.

©2021 Avaya Inc. All Rights Reserved.

To verify the identity certificate, locate the **Identity Certificate** section and click **View** to see the details of the certificate.

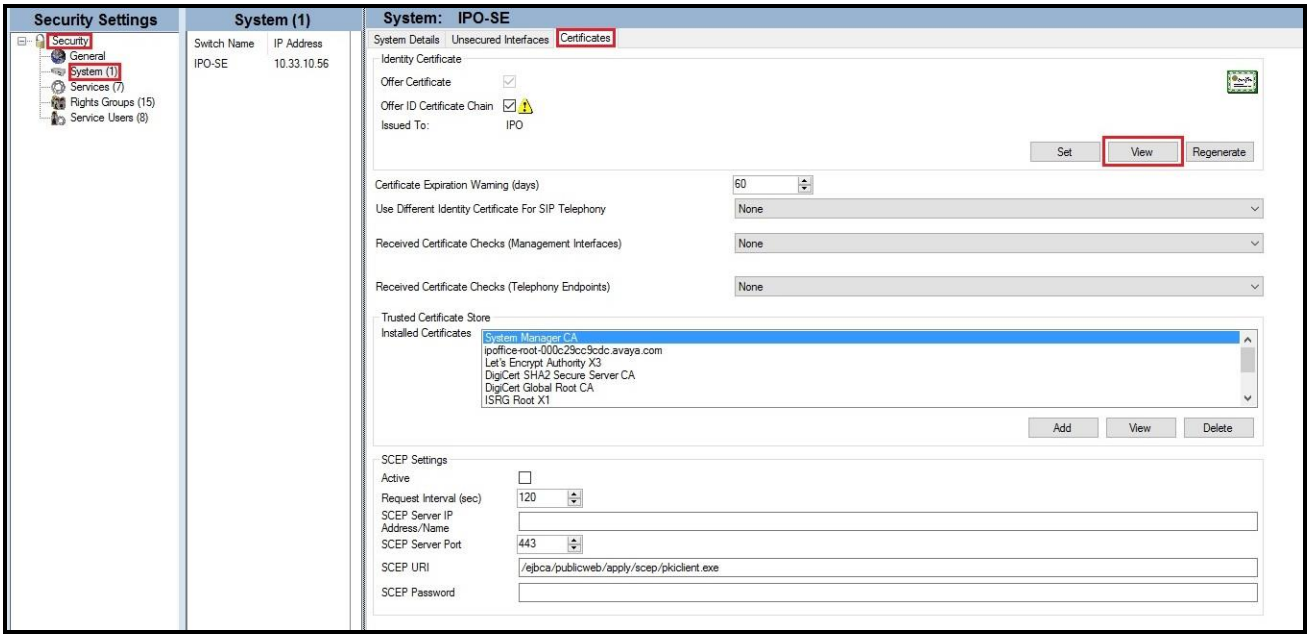


Figure 5 – Avaya IP Office Server Edition TLS Certificate

5.3. 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.

5.3.1. System – LAN1 Tab

In the sample configuration, **IPO-SE** was used as the Primary Server name and **IPOffice_1** was used as the Expansion System name. The **LAN1** port on the Primary Server (Eth0) connects to the inside interface (enterprise private network side) of the Avaya SBCE across the enterprise LAN (private) network. The LAN1 port on the Expansion System were used to connect to the enterprise LAN (private) network. The outside interface of the Avaya SBCE connects to the Cox managed CPE LAN interface. The Cox managed CPE WAN interface connects Cox Communications network via the public internet.

To configure the LAN1 settings on the Primary Server, complete the following steps. Navigate to **IPO-SE → System (1)** in the Navigation and Group Panes and then navigate to the **LAN1 → LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office Server Edition LAN1 port. Set the **IP Mask** field to the mask used on the public network. All other parameters should be set according to customer requirements. Click **OK** to submit the change.

©2021 Avaya Inc. All Rights Reserved.

Figure 6 - Avaya IP Office Primary Server LAN1 Settings

©2021 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 Avaya SBCE
- Check the **SIP Register Enable** to allow Avaya IP deskphones/softphones to register using the SIP protocol
- Input **SIP Domain Name** and **SIP Register FQDN** as **10.33.10.56**
- 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

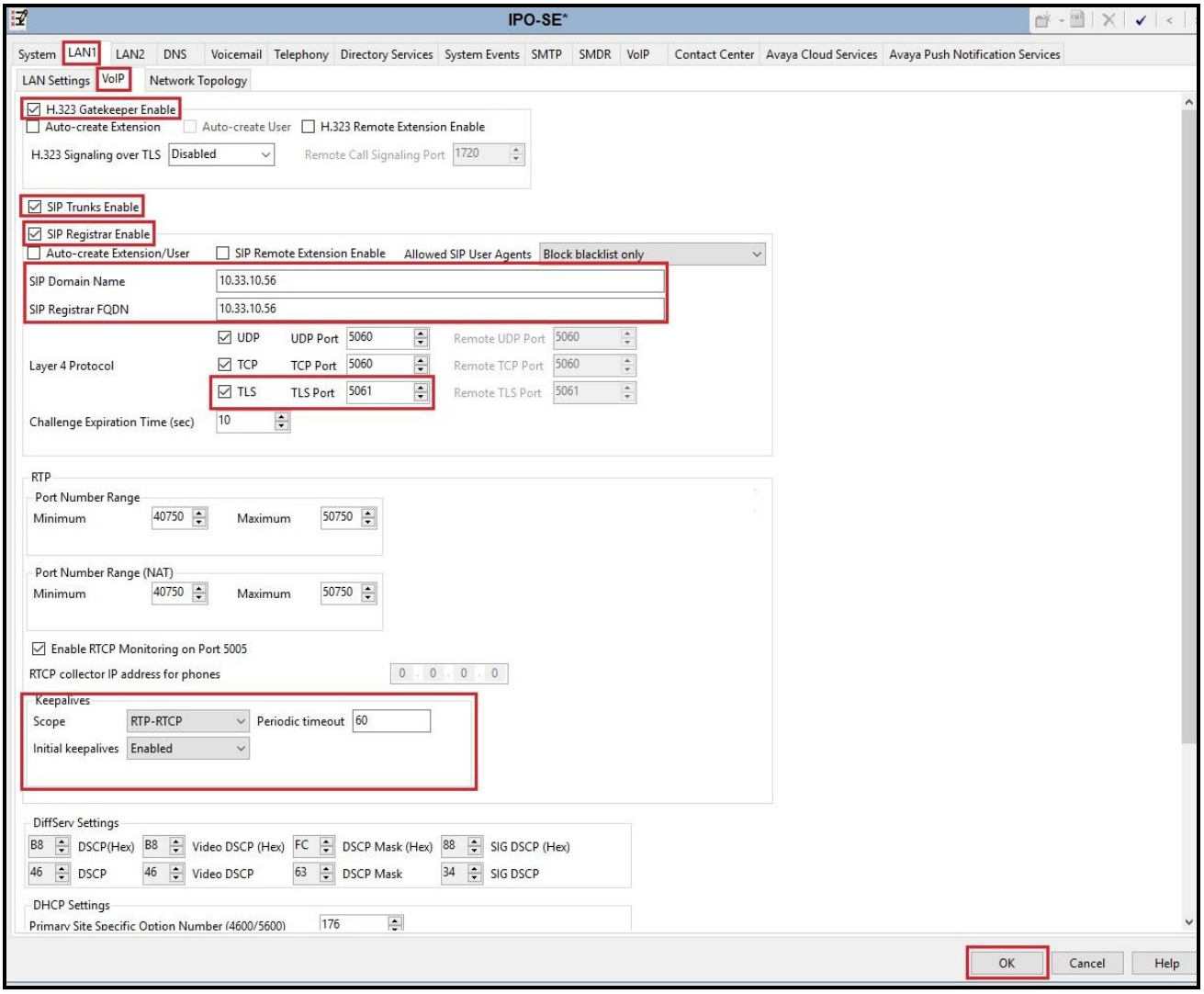


Figure 7 - Avaya IP Office Primary Server LAN1 VoIP

©2021 Avaya Inc. All Rights Reserved.

To configure the LAN1 settings tab for the Expansion System, navigate to **Solution → IPOffice_1 → System (1)** in the Navigation and Group Panes and then navigate to the **LAN1 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields should be populated with the values assigned during the Expansion System initial installation process. Verify the configuration or modify the values if needed. While DHCP was disabled during the compliance test, this parameter should be set according to customer requirements. Other settings were left at their default values. Click **OK** to submit the change.

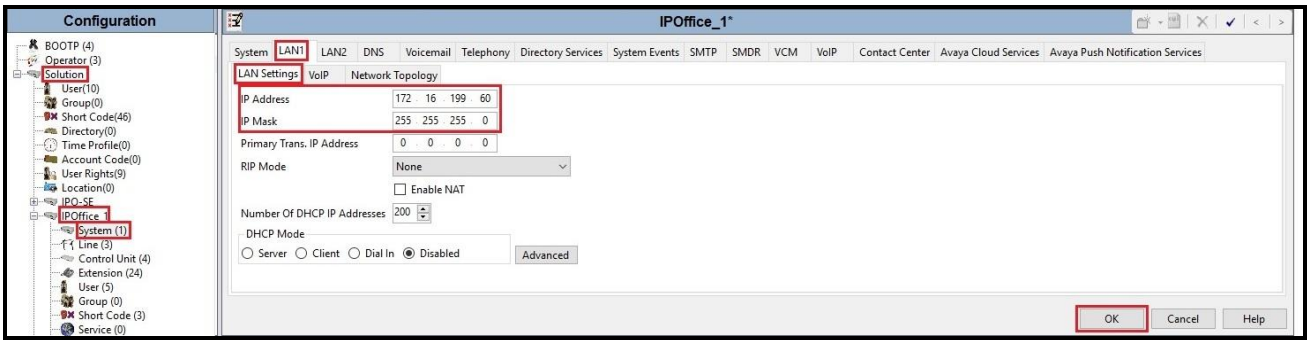


Figure 8 - Avaya IP Office Expansion Server LAN Settings

©2021 Avaya Inc. All Rights Reserved.

5.3.2. System – Telephony Tab

Navigate to **Solution → IPO-SE → 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. The **Hold Timeout (sec)** field controls how long calls remain on hold before being alerted to the user and should be set based on the customer's requirement. Set **Default Name Priority** to **Favor Trunk** to have IP Office display the name provided in the Caller ID from the SIP trunk. Defaults were used for all other settings. Click **OK** to submit the changes.

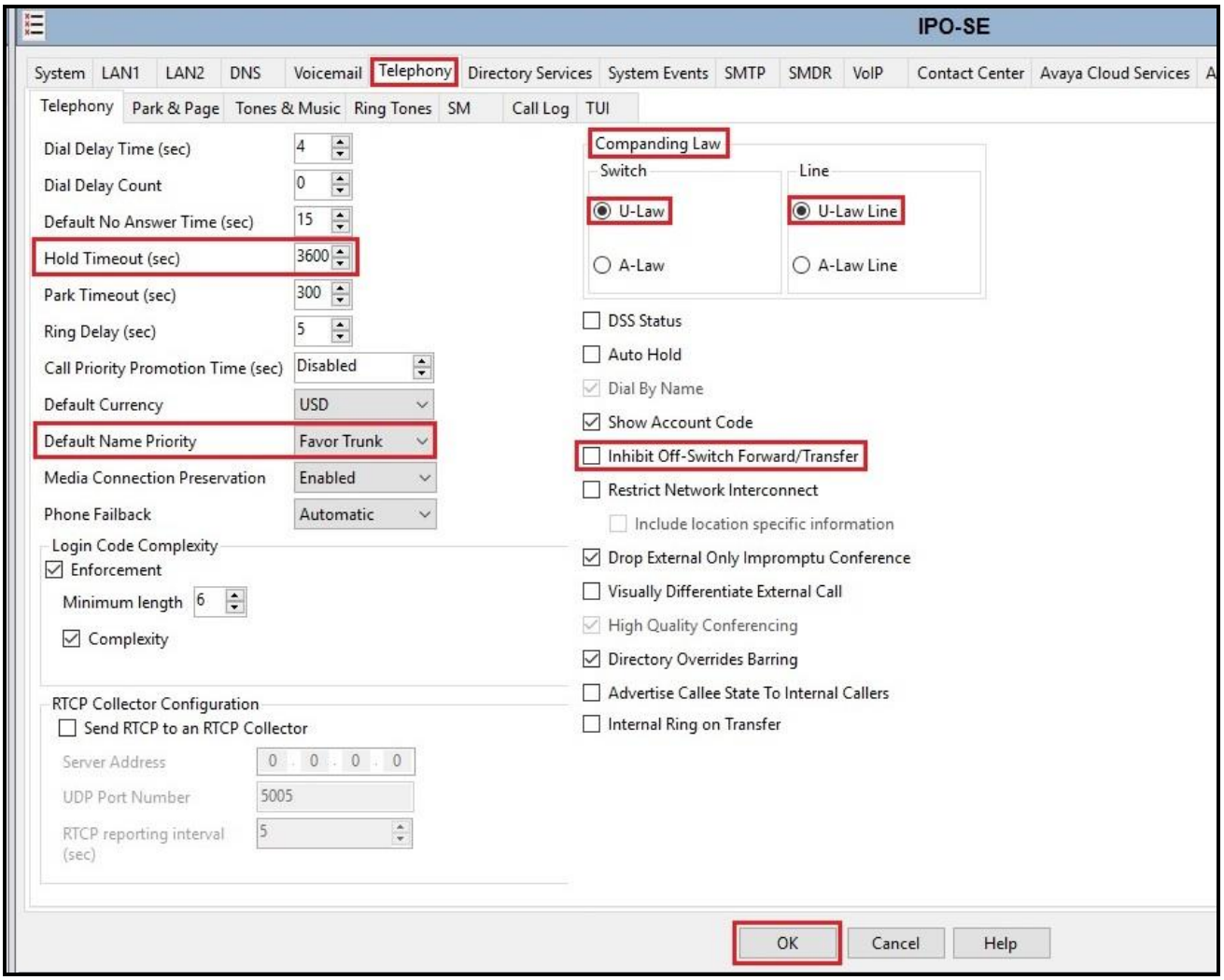


Figure 9 - Avaya IP Office Primary Server Telephony

Navigate to **Solution → IPOffice_1 → System (1)** (not shown) and repeat the steps above to configure the **Telephony** settings for the Expansion System.

©2021 Avaya Inc. All Rights Reserved.

5.3.3. System – VoIP Tab

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

Navigate to **Solution → IPO-SE → 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 the default value of **101**. 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 submit the changes.

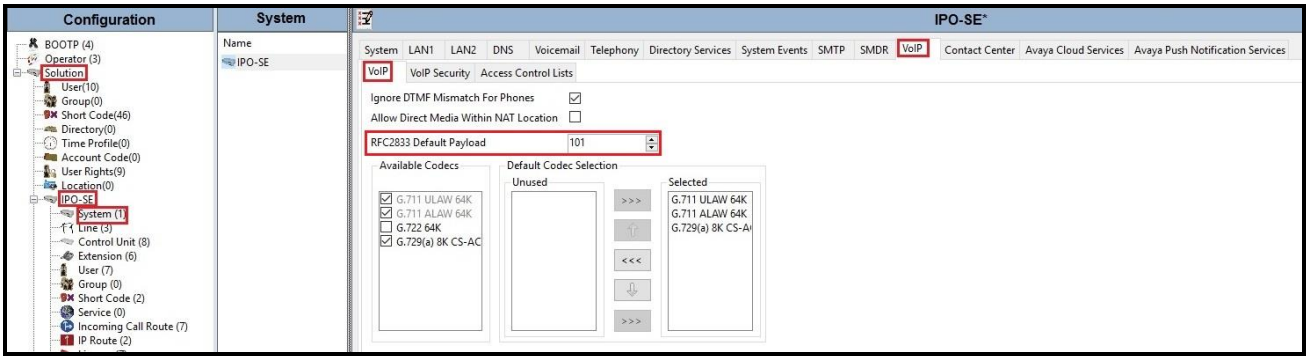


Figure 10 - Avaya IP Office Primary Server VoIP

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 5.5.2** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

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.

©2021 Avaya Inc. All Rights Reserved.

To configure the use of SRTP, navigate to **Solution → IPO-SE → System (1)** in the Navigation and Group Panes and then navigate to **VoIP → VoIP Security** tab on the Details pane.
Set the **Media** 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

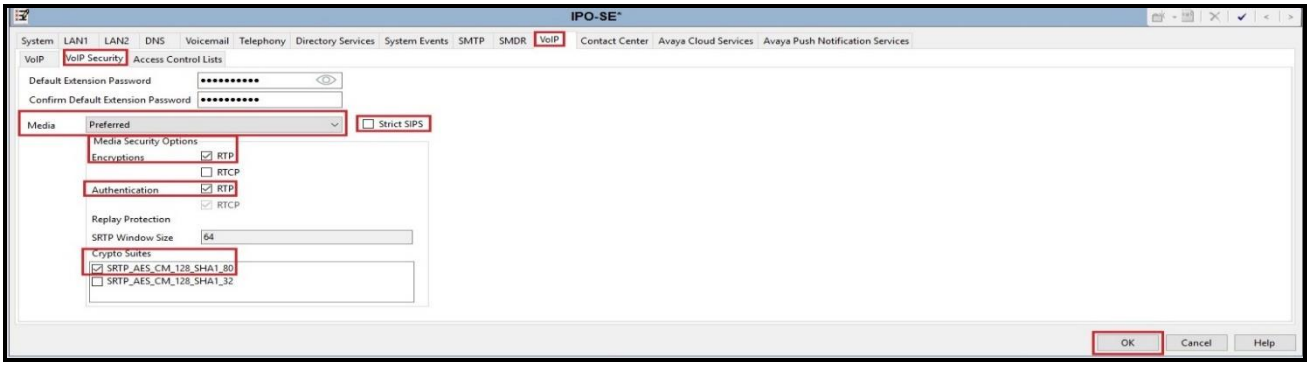


Figure 11 - Avaya IP Office Primary Server VoIP Security

5.4. 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 create an IP route for the Primary system, navigate to **Solution → IPO-SE → IP Route**, right-click on **IP Route** and select **New** (Not shown). 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 Avaya SBCE, e.g., **10.33.10.1**
- Set **Destination** to **LAN1** from the pull-down menu
- Click **OK** to commit

©2021 Avaya Inc. All Rights Reserved.

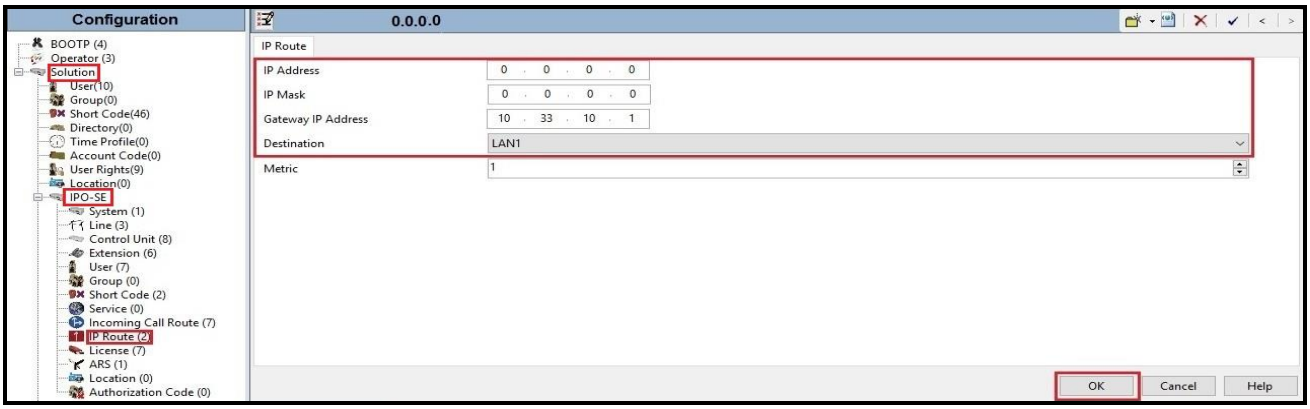


Figure 12 - Avaya IP Office Primary Server IP Route

To create an IP route for the Expansion system, navigate to **Solution → IPOffice_1 → IP Route**, right-click on **IP Route** and select **New** (Not shown). 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 Avaya IP Office SE, e.g., **172.16.199.1**
- Set **Destination** to **LAN1** from the pull-down menu
- Click **OK** to commit

Figure 13 - Avaya IP Office Expansion Server IP Route

©2021 Avaya Inc. All Rights Reserved.

5.5. Administer SIP Line

A SIP Line is needed to establish the SIP connection between Avaya IP Office Server Edition 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 Server Edition Manager to create a SIP Line. Follow the steps in **Section 5.5.1** 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 5.5.2**.

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 5.5.2**.
For the compliance test, SIP Line 17 was used as trunk for both outgoing and incoming calls.

©2021 Avaya Inc. All Rights Reserved.

5.5.1. Create SIP Line from an XML Template

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

Create a new folder in a location where Avaya IP Office Server Edition Manager is installed (e.g., C:\Cox Communications\Template). Copy the template file to this folder and rename the template file to **CoxIPO111SBCE81.xml** (for SIP Line 17).

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

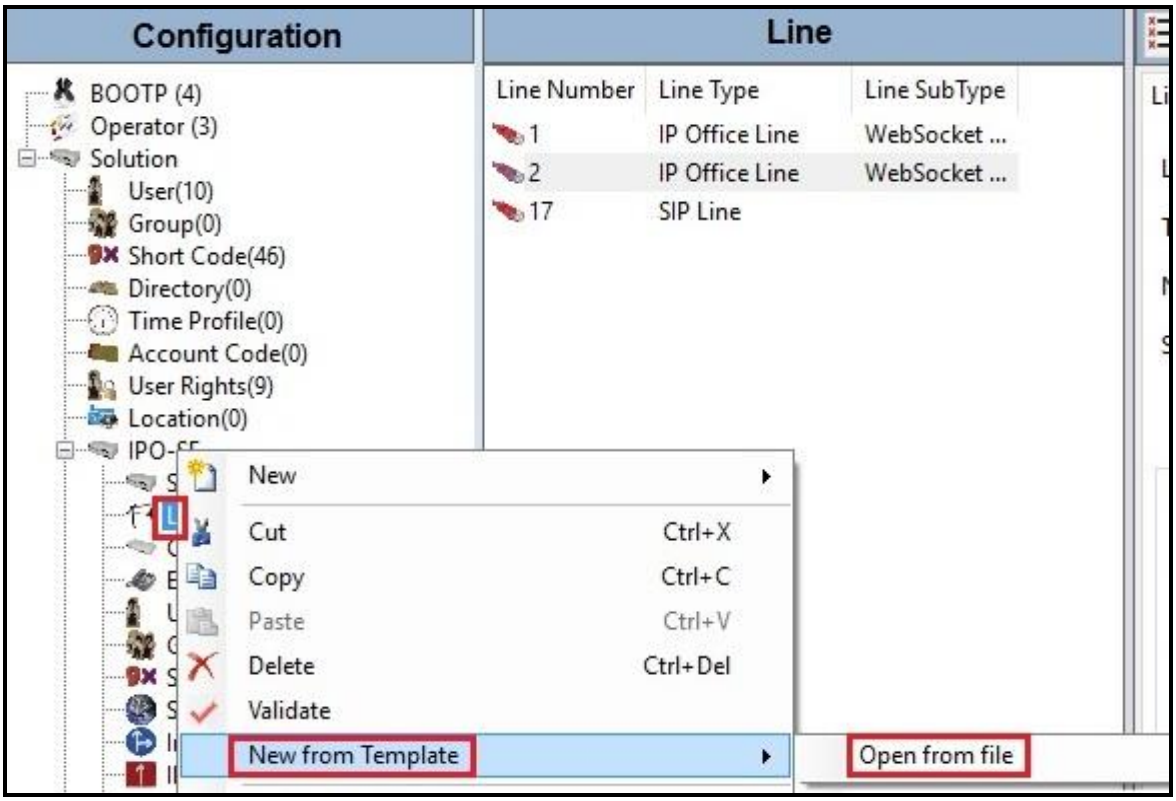


Figure 14 – Create SIP Line from Template

©2021 Avaya Inc. All Rights Reserved.

Select the **Template Files (*.xml)** and select the copied template at folder (e.g., C:\Cox Communications\Template). Click **Open** button to create a SIP line from template.

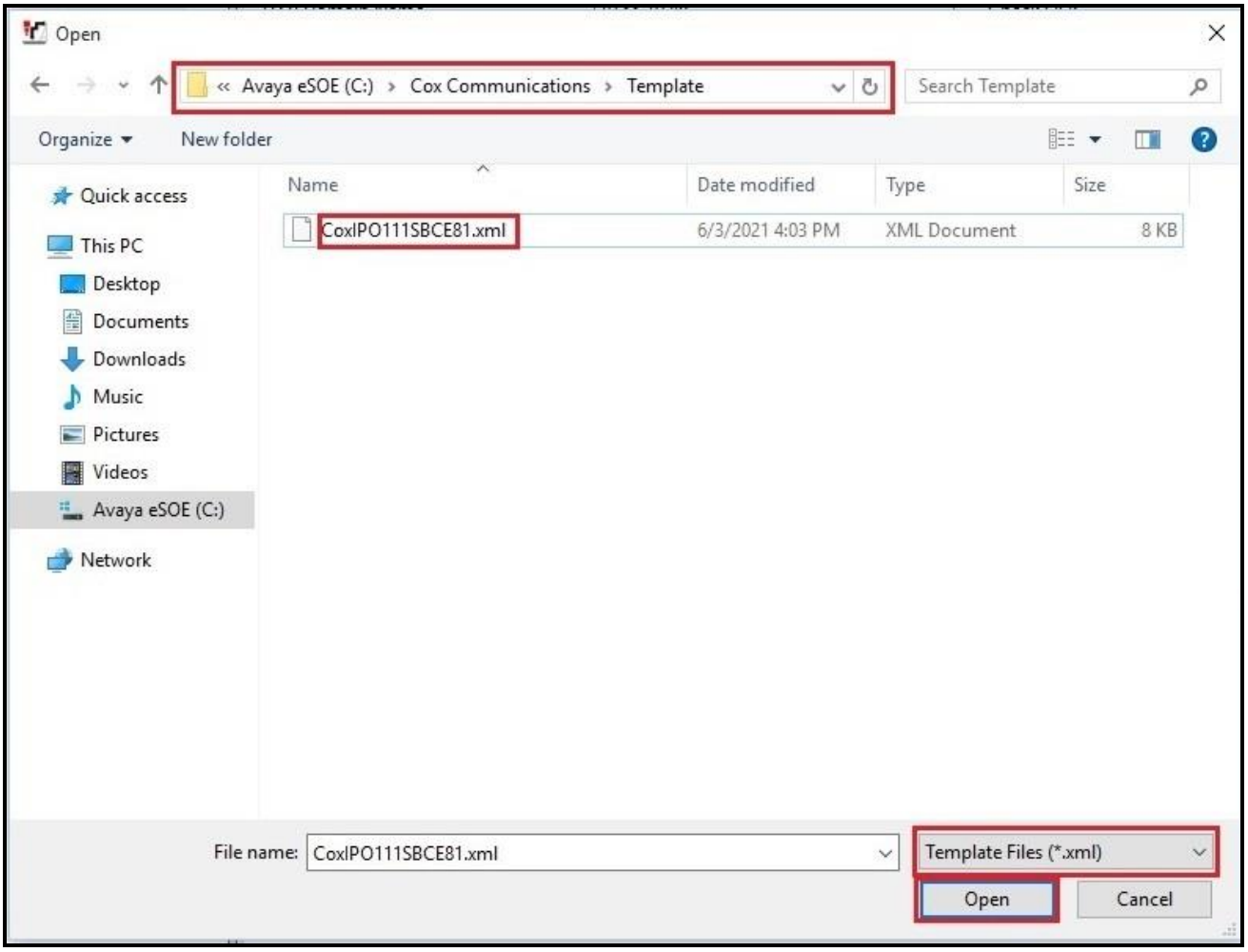


Figure 15 – Create SIP Line from directory

©2021 Avaya Inc. All Rights Reserved.

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

Figure 16 – Create SIP Line from Template successfully

Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Section 5.5.2**.

©2021 Avaya Inc. All Rights Reserved.

5.5.2. 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**
- Check the **In Service** and **Check OOS** box
- Input **ITSP Domain Name**: **10.33.10.49** (This is Avaya SBCE internal IP address)
- Input **Local Domain Name**: **10.33.10.56** (This is Avaya IP Office SE LAN1 IP address)
- Set **URI Type** to **SIP URI**
- For **Session Timers**, set **Refresh Method** to **Auto** with **Timer (sec)** to **On Demand**
- Set **Name Priority** to **Favor Trunk**. As described in **Section 5.3.2**, 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 **NEVER**. Note: Cox Communications does not fully support SIP Refer in off-net call redirection during the compliance testing (See **Section 2.1** for item not supported in detail). Therefore, the SIP RE-INVITE was tested in the off-net call redirection instead
- Default values may be used for all other parameters
- Click **OK** to commit then press Ctrl + S to save

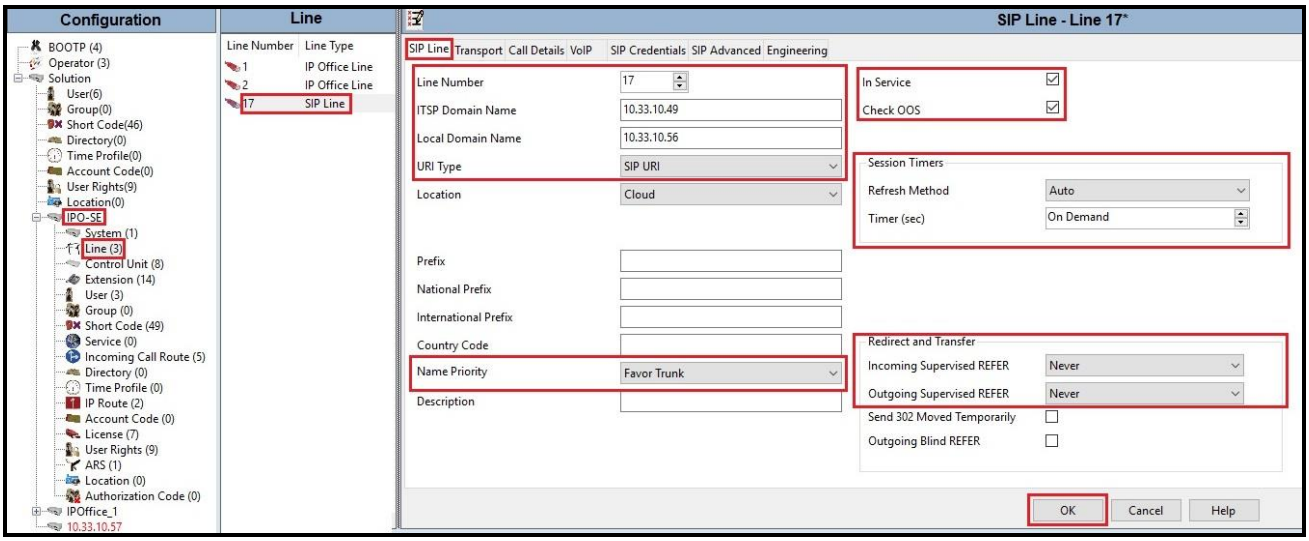


Figure 17 – SIP Line Configuration

©2021 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: **10.33.10.49** as shown in **Figure 1**. This is the SIP Proxy address used for outgoing SIP calls
- 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 → 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
- The **Calls Route via Registrar** was unchecked as Cox Communications 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

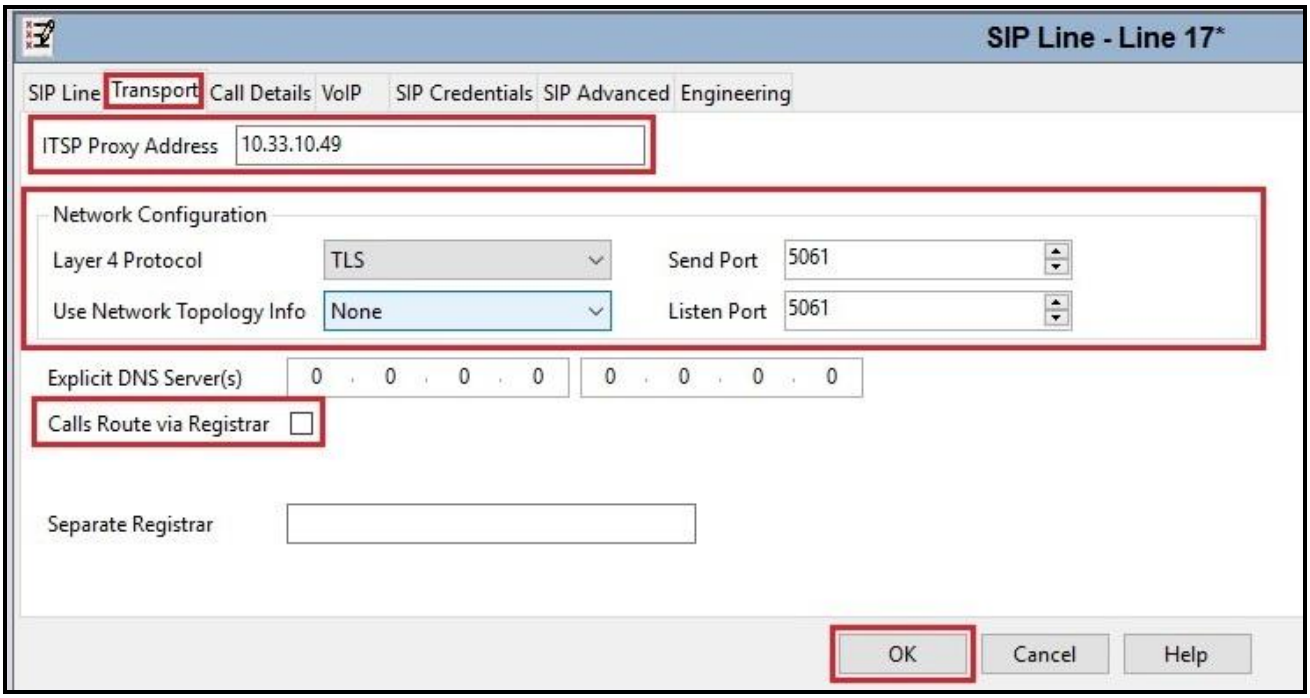


Figure 18 – SIP Line Transport Configuration

©2021 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 **Call Details** 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:

- Associate this SIP 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
- Select **Credentials** to **0: <None>**
- Check **P Asserted ID** and **Diversion Header** options (See **Section 2.2** for Diversion/PAI headers issue)
- Set the **Display** and **Content** of **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** to **Auto**
- In **Field meaning**: Set **Forwarding/Twinning** of **Local URI**, **Contact**, **P Asserted ID, Diversion Header** to **Original Caller**
- Set all remaining fields as shown on the screenshot below
- Click **OK** to submit the changes

©2021 Avaya Inc. All Rights Reserved.

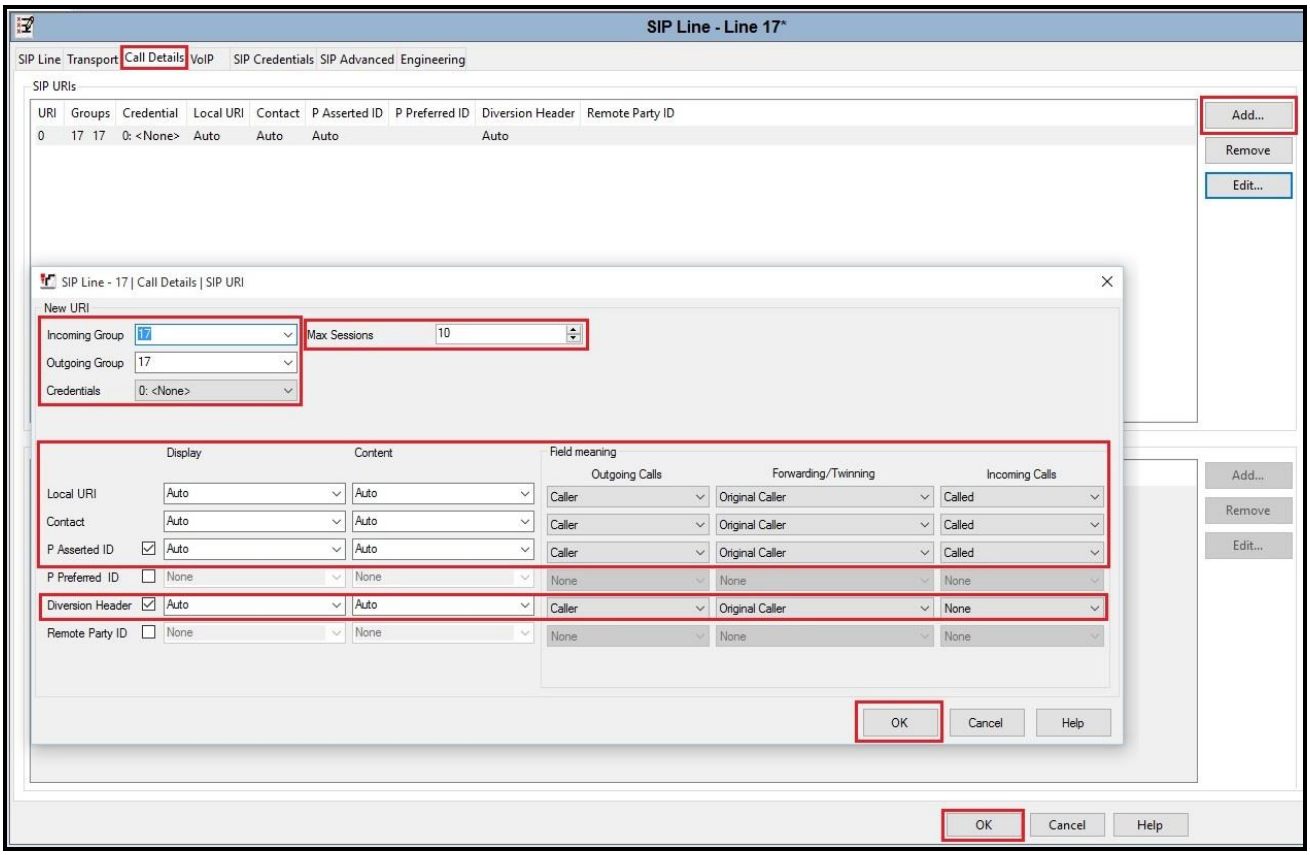


Figure 19 – SIP Line Call Details Configuration

©2021 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** codec is selected. Avaya IP Office Server Edition supports the codec, which is sent to the Cox Communications, in the Session Description Protocol (SDP) offer
- Check the **Re-invite Supported** box
- Set **Fax Transport Support** to **G.711** or **T38 Fallback** from the pull-down menu. Note: Cox Communications supports both G.711 pass through and T.38 FAX during the compliance testing
- Set the **DTMF Support** to **RFC2833/RFC4733** from the pull-down menu. This directs Avaya IP Office Server Edition to send DTMF tones using RTP events messages as defined in RFC2833 and RFC4733
- Set the **Media Security** field to **Same as System (Preferred)**
- Default values may be used for all other parameters
- Click **OK** to submit the changes

©2021 Avaya Inc. All Rights Reserved.

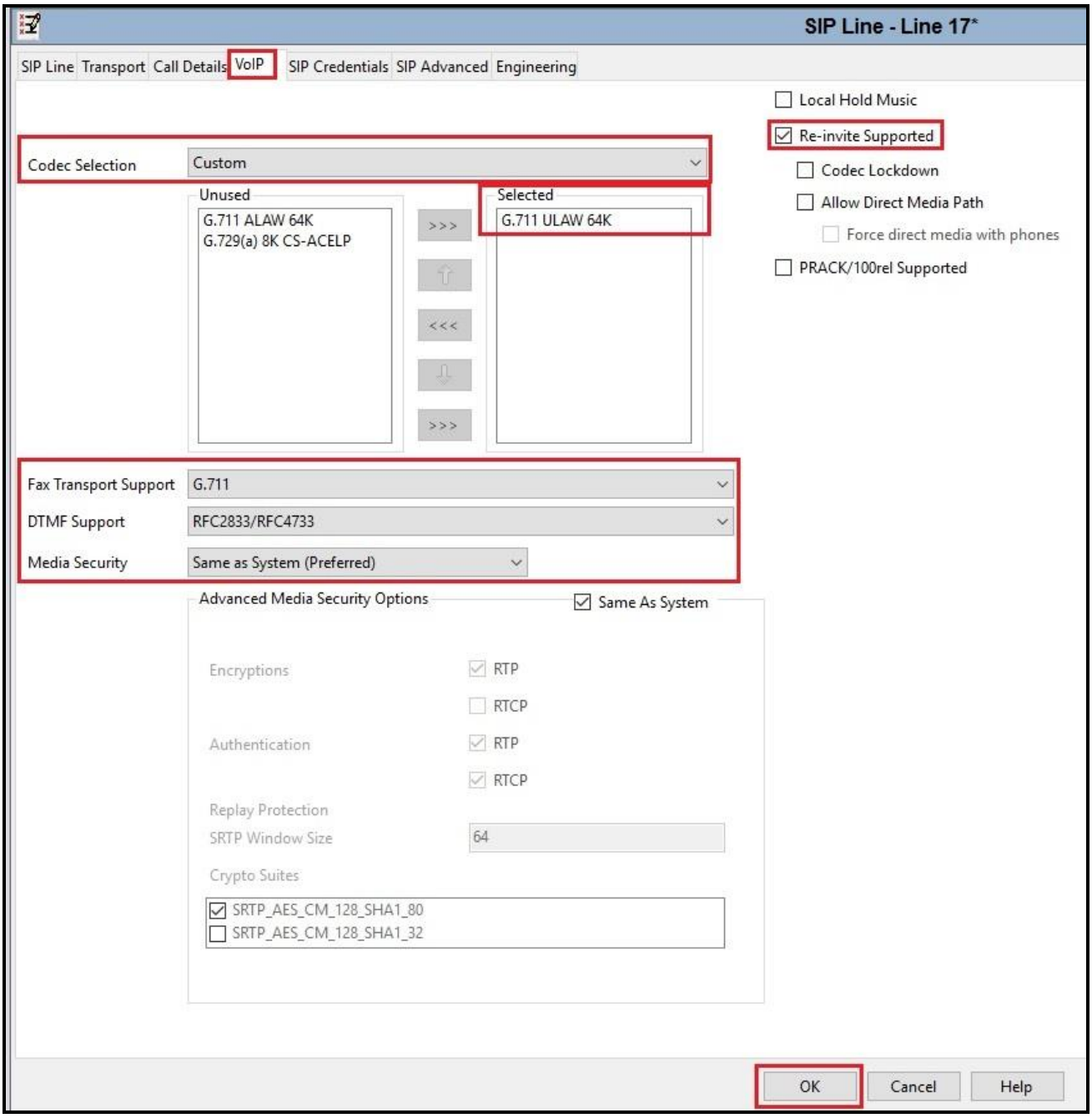


Figure 20 – SIP Line VoIP Configuration

©2021 Avaya Inc. All Rights Reserved.

Select the **Engineering** tab to enter values that apply special features to the SIP line. IP Office negotiates the use of T.38 for fax, which consist of IP Office sending a re-INVITE message with two media lines in the SDP in order, with the first media line set for audio, with the port set to 0, and the second media line set for T.38, with a valid port number. Add a SLIC to reorder media lines for T38 in the SDP so that the active one (media line set for T.38) is on the top.

- Click **Add** button to enter a SLIC
- Enter **Custom String**: **SLIC_PREFER_ACTIVE_SDP**
- Click **OK** to submit the changes

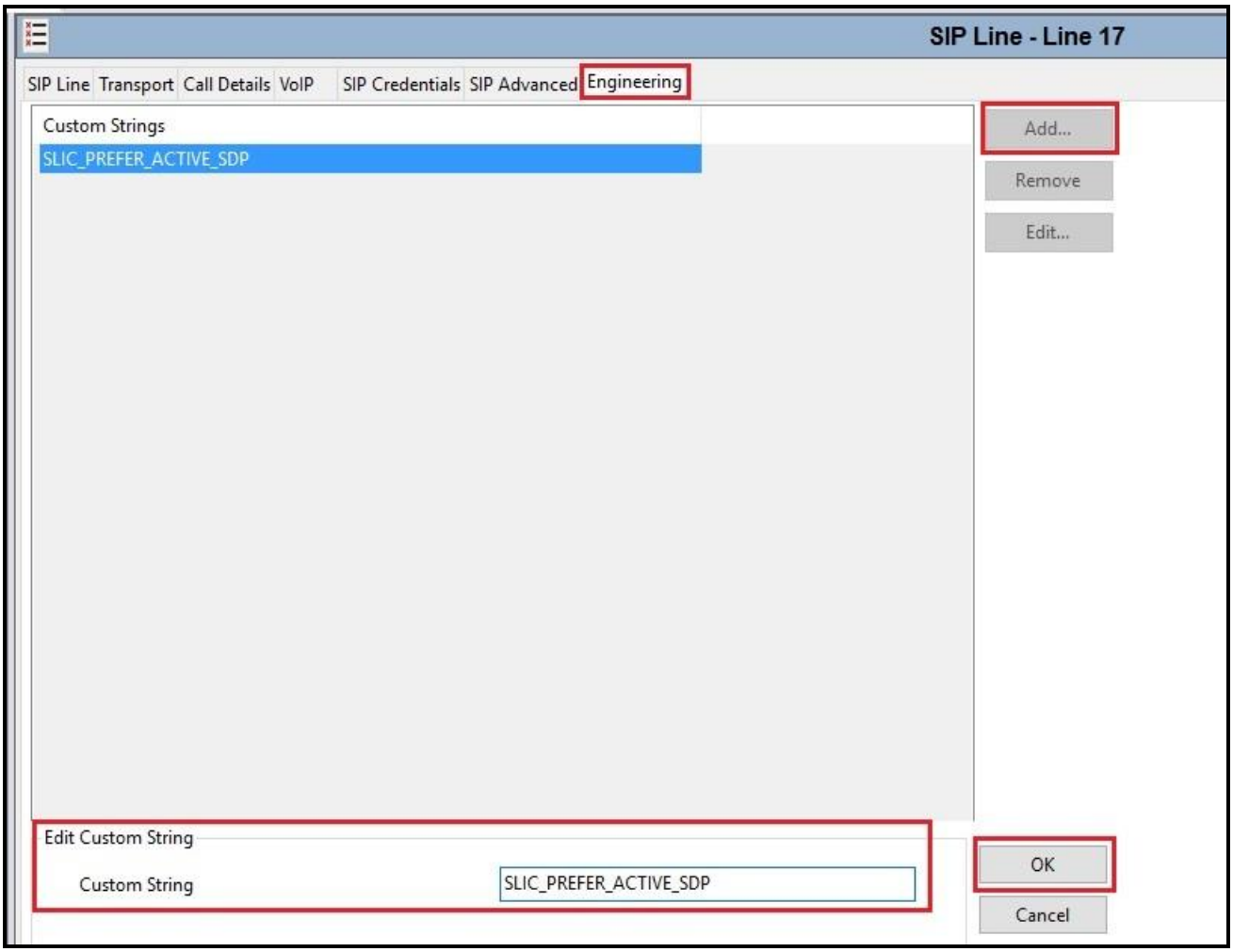


Figure 21 – SIP Line Engineering Configuration

©2021 Avaya Inc. All Rights Reserved.

5.6. IP Office Line in Primary 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.

To verify the IP Office line connecting the Primary System to the Expansion System, select **Line** on the navigation pane of Primary System and select the IP Office Line on the Group pane (line **2** on the screen below). Make note of the **Outgoing Group ID 99999** on the Details pane. The **Address** of **Gateway** is Avaya IP Office Expansion System LAN1 IP address **172.16.199.60**.

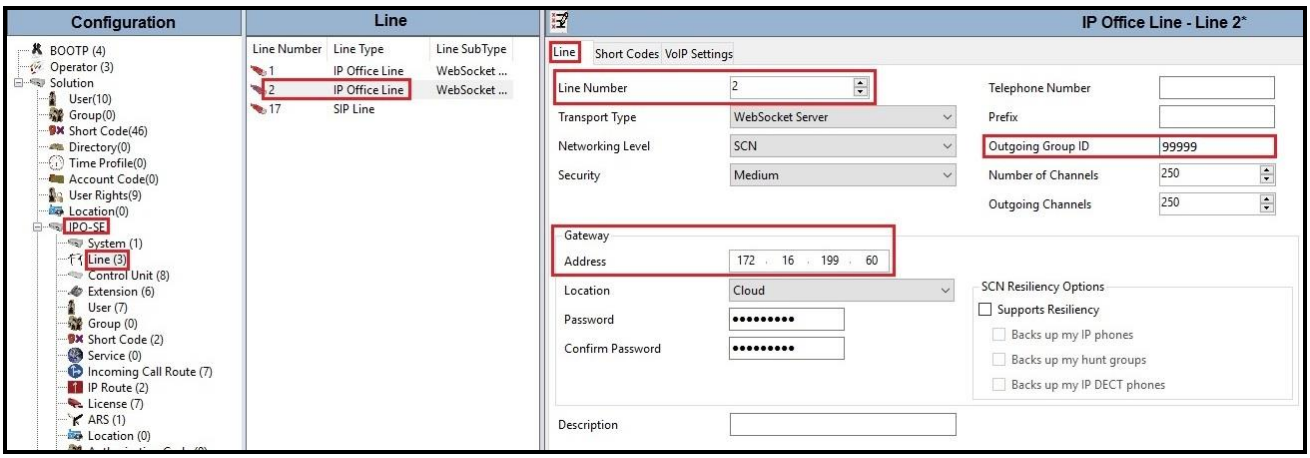


Figure 22 – IP Office Line for Primary System

©2021 Avaya Inc. All Rights Reserved.

To verify the **VoIP Settings** of the IP Office line connecting the Primary System to the Expansion System, select **VoIP Settings** tab. The selected codec is **G.711 ULAW 64K**. Select **Fax Transport Support** to **G.711** or **T38 Fallback** (This setting should be as same as the VoIP settings in SIP line of Primary System and the VoIP settings in IP Office Line of Expansion System). Under **Media Security** verify **Same as System (Preferred)** is selected (default value).

Default values may be used for all other parameters. Click **OK** to submit the changes.

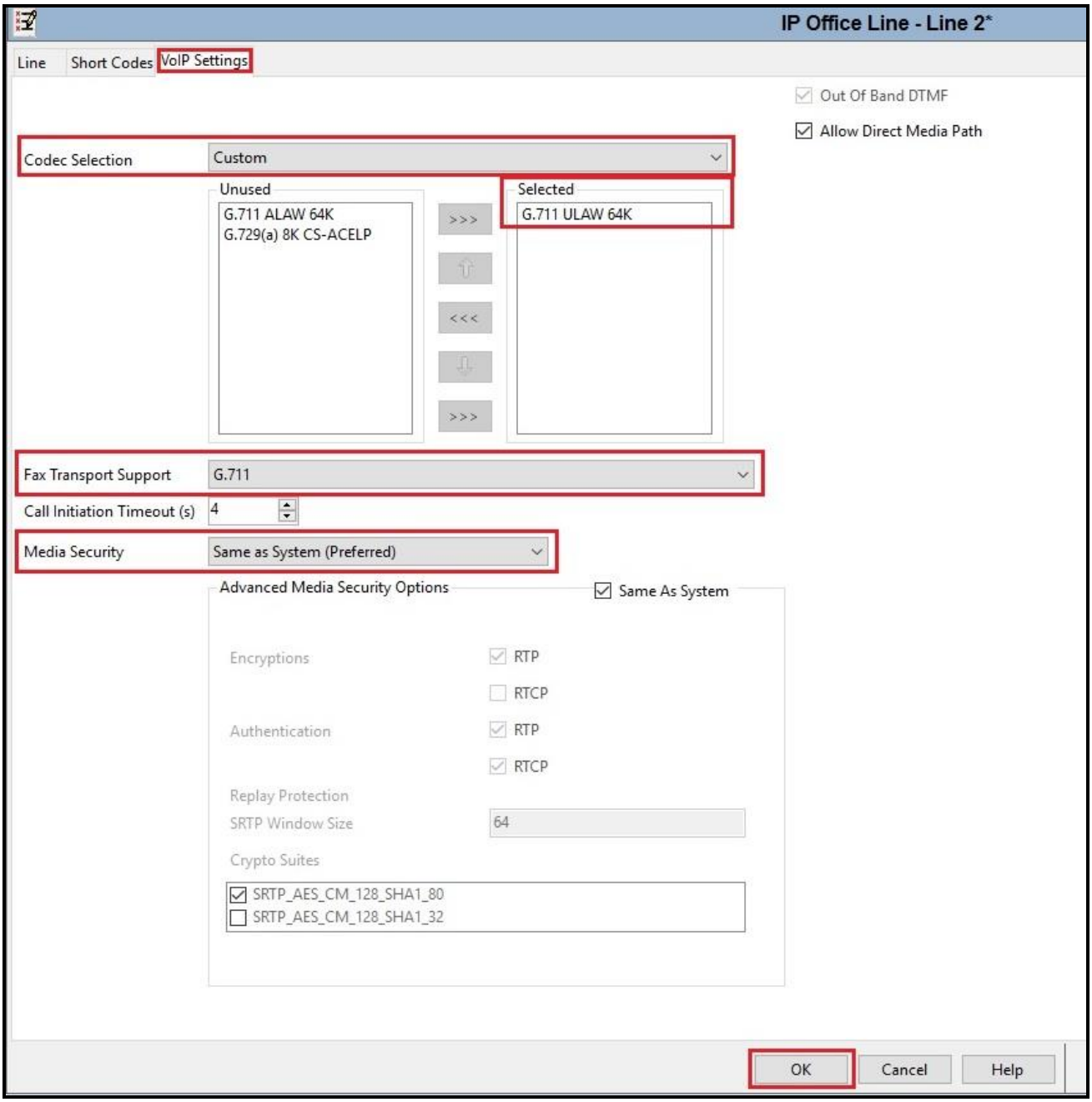


Figure 23 – IP Office Line for Primary System VoIP Settings

©2021 Avaya Inc. All Rights Reserved.

5.7. IP Office Line in Expansion System

To verify the IP Office line connecting the Expansion System to the Primary System, select Expansion Line on the navigation pane and select the IP Office Line on the Group pane (line **17** on the screen below). Make note of the **Outgoing Group ID 99999** on the Details pane. The **Address** of **Gateway** is Avaya IP Office Server Edition LAN1 IP address **10.33.10.56**.

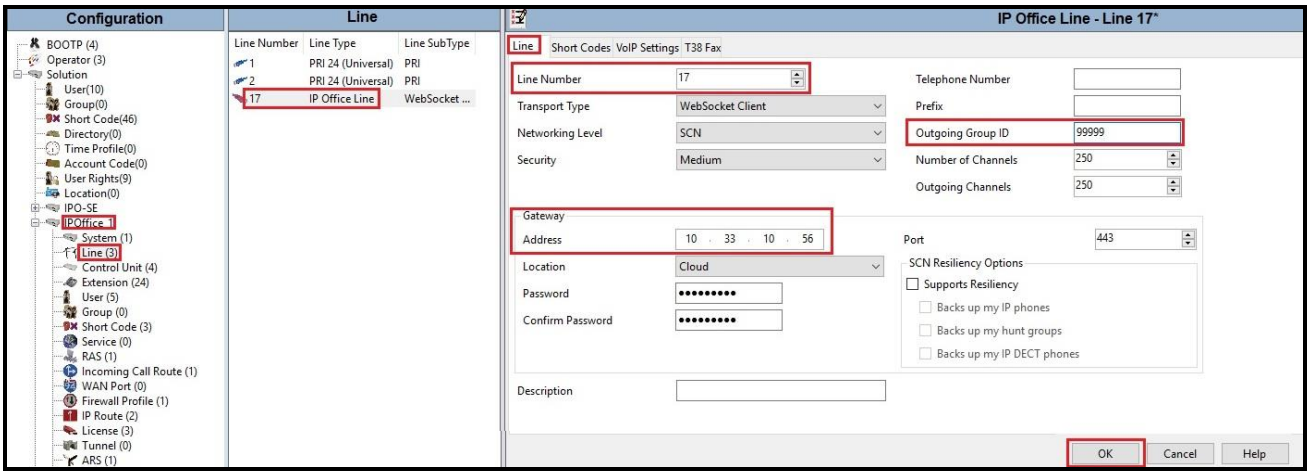


Figure 24 – IP Office Line for Expansion System

©2021 Avaya Inc. All Rights Reserved.

To verify the **VoIP Settings** of the IP Office line connecting the Expansion System to the Primary Server, select **VoIP Settings** tab. The selected codecs are **G.711 ULAW 64K**. Select **Fax Transport Support** to **G.711** or **T38 Fallback** (This setting should be as same as the VoIP settings in SIP line and IP Office Line of Primary System). Default values may be used for all other parameters. Click **OK** to submit the changes.

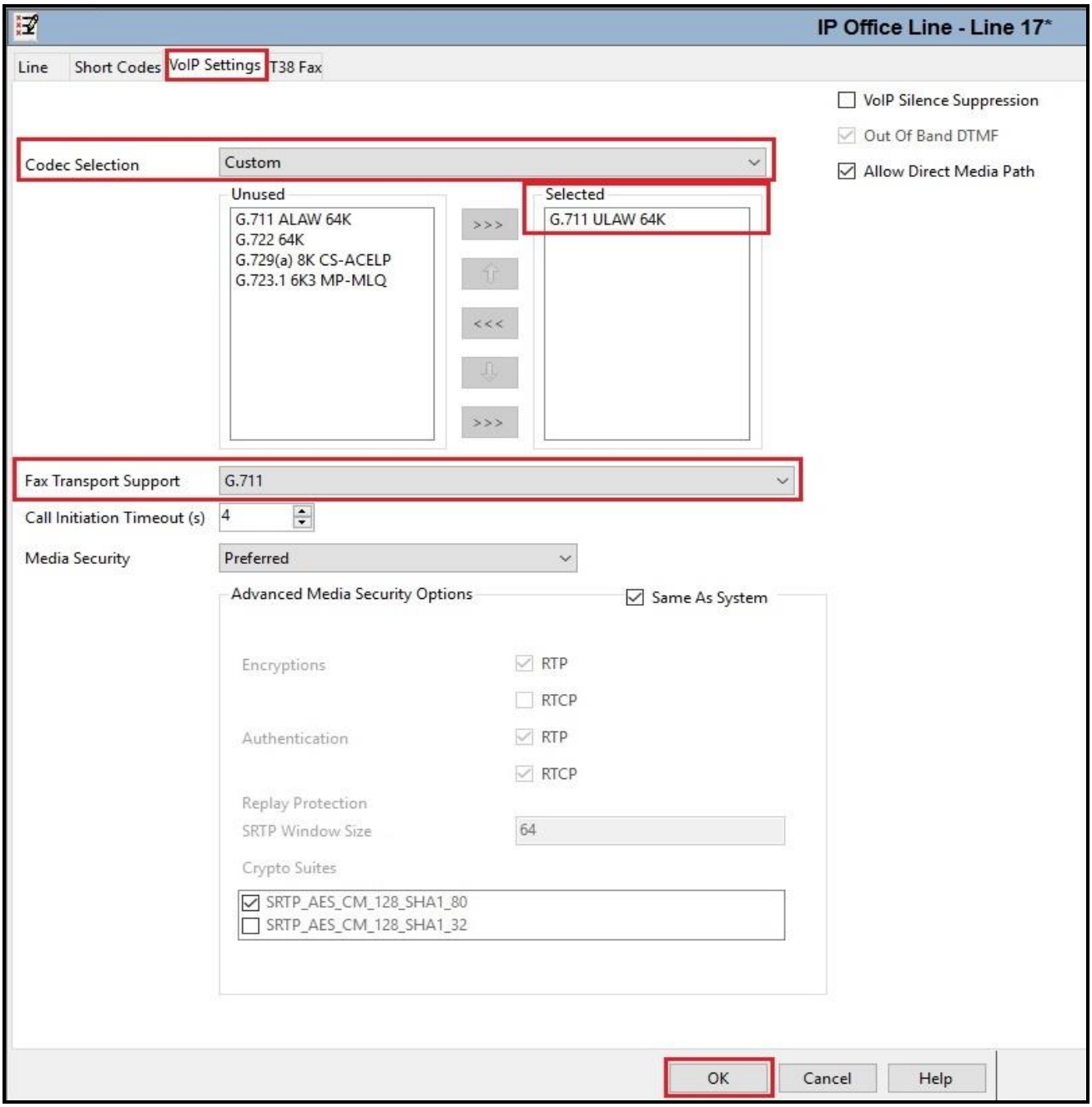


Figure 25 – IP Office Line for Expansion Server VoIP Settings

©2021 Avaya Inc. All Rights Reserved.

To verify the **T38 Fax** of the IP Office line connecting the Expansion System to the Primary Server, select **T38 Fax** tab (Note: The T38 Fax tab is only active when Fax Transport Support is selected as T38 Fallback on **VoIP Settings** tab). Uncheck the **Use Default Values** at the bottom of the screen. Set the **T.38 Fax Version** to **0**. Default values may be used for all other parameters. Click the **OK** to submit the changes.

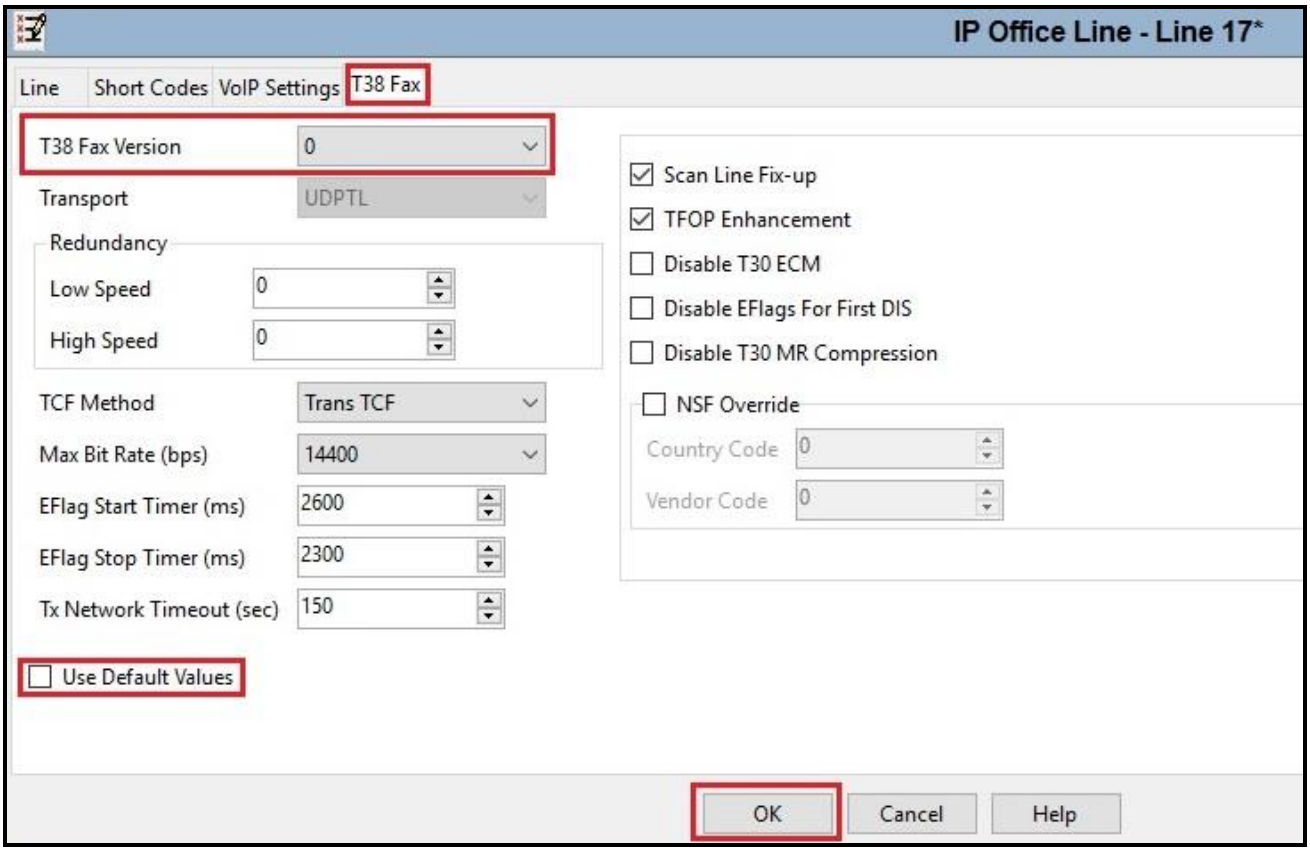


Figure 26 – IP Office Line for Expansion Server T38 Fax

5.8. Outbound Short Code

Define a short code to route outbound traffic on the SIP line to Cox Communications. 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 for Primary System used in the test configuration.
Navigate to **Solution → IPO-SE → Short Code**, right-click on **Short Code** and select **New**.

- 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

©2021 Avaya Inc. All Rights Reserved.

- 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. Note: Use the specific **W** in front of **N** for restricting all outbound calls
- Set the **Line Group ID** to the **Outgoing Group 17** defined on the **Call Details** tab on the **SIP Line** in **Section 5.5.2**. 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

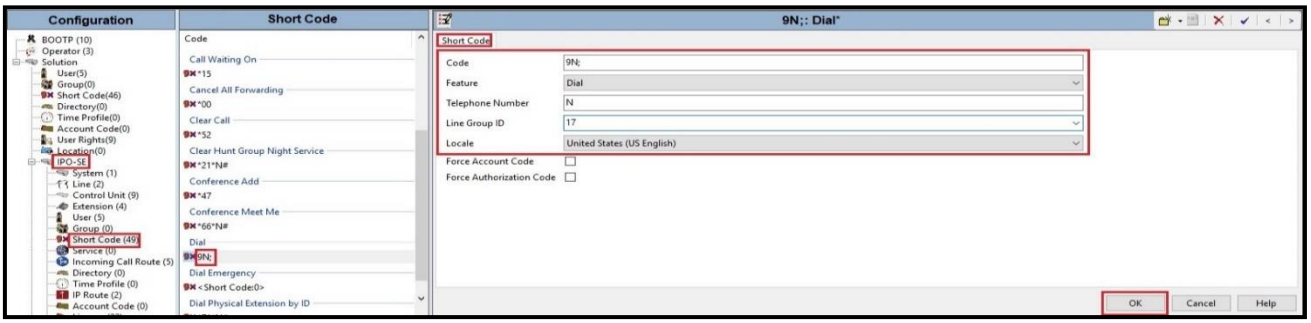
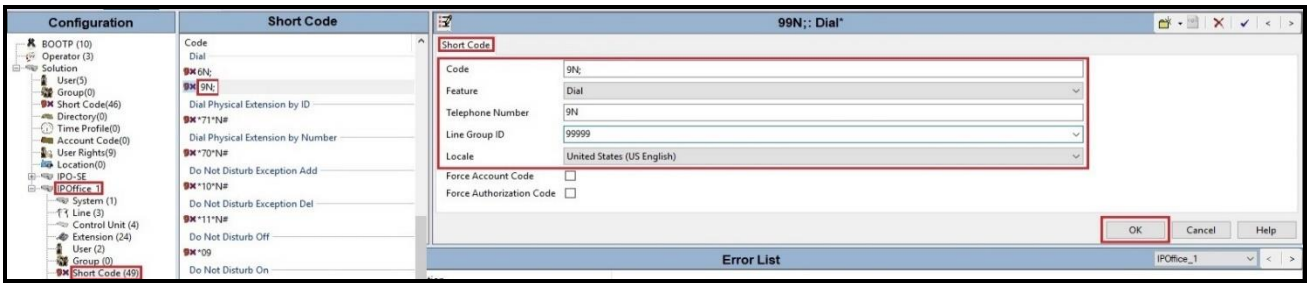


Figure 27 – Short Code 9N for Primary System

The screen below shows the details of the previously administered "**9N;**" short code for Expansion System used in the test configuration.

Navigate to **Solution → IPOffice_1 → Short Code**, right-click on **Short Code** and select **New**

- 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 (using Avaya analog or digital phones) dials 9 followed by any number
- Set **Feature** to **Dial**. This is the action that the short code will perform
- Set **Telephone Number** to **9N**
- Set the **Line Group ID** to **99999** defined on the **Outgoing Group ID** of the IP Office line connecting the Expansion System to the Primary System. This short code will use this line group when placing the outbound call via Avaya IP Office Server Edition Primary Server
- Default values may be used for all other parameters
- Click **OK** to submit the changes



©2021 Avaya Inc. All Rights Reserved.

Figure 28 – Short Code 9N for Expansion System

The feature of incoming calls from mobility extension to idle-appearance FNE (Feature Name Extension) is hosted by Avaya IP Office Server Edition. The Short Code **FNE00** was configured with the settings shown below.

Navigate to **Solution → Short Code**, right-click on **Short Code** and select **New** (Not shown)

- 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

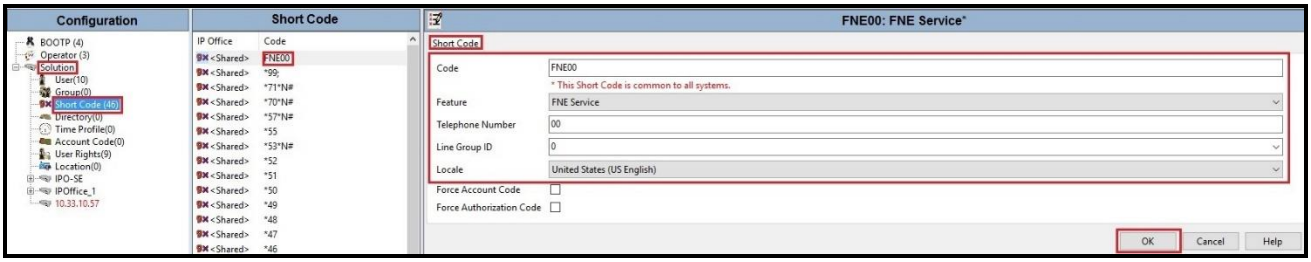


Figure 29 – Short Code FNE

©2021 Avaya Inc. All Rights Reserved.

5.9. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.5.2**. 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 **531XXX2920**. 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 header 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 **531XXX2920**. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise provided by Cox Communications. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.

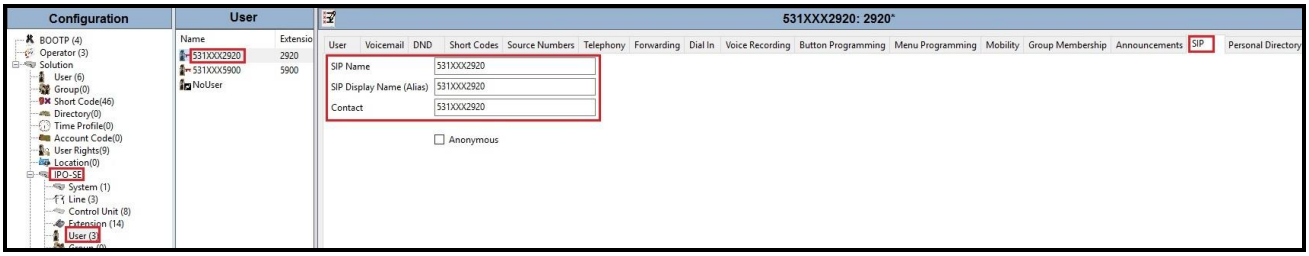


Figure 30 – User Configuration – SIP tab

©2021 Avaya Inc. All Rights Reserved.

To configure the restricted outbound call for a user by using specific W in the Short Codes, 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 **531XXX2920**. Select the **Short Codes** tab in the Details pane.

- 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 **WN**. The value **N** represents the number dialed by the user. Note: Use the specific **W** in front of **N** for restricting outbound calls for a user
- Set the **Line Group ID** to the **Outgoing Group 17** defined on the **Call Details** tab on the **SIP Line** in **Section 5.5.2**. 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

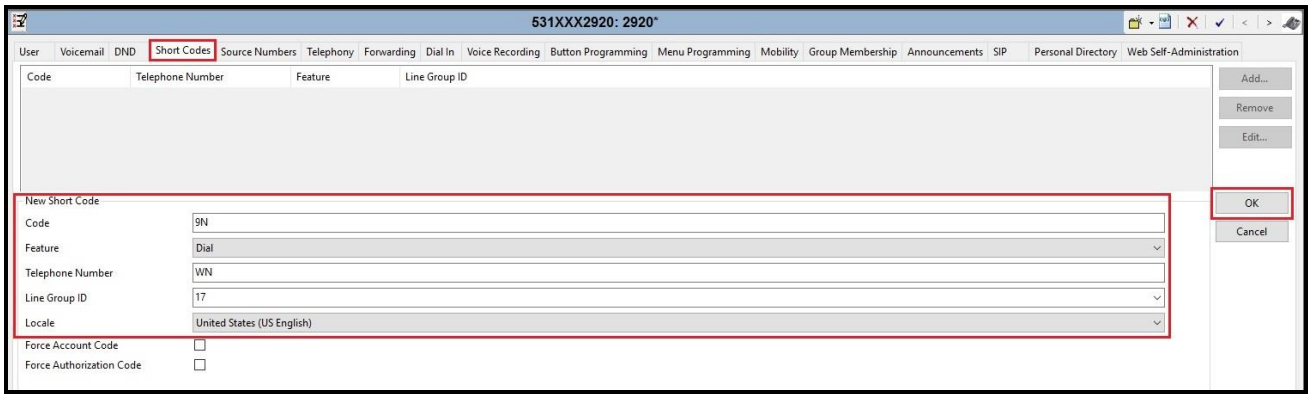


Figure 31 – User Configuration – Short Code tab

©2021 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 531XXX2920**
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 **91613XXX5096**. Check **Mobile Call Control** to allow incoming calls from mobility extension to access FNE00 (Defined in **Section 5.8**). Other options can be set according to customer requirements.

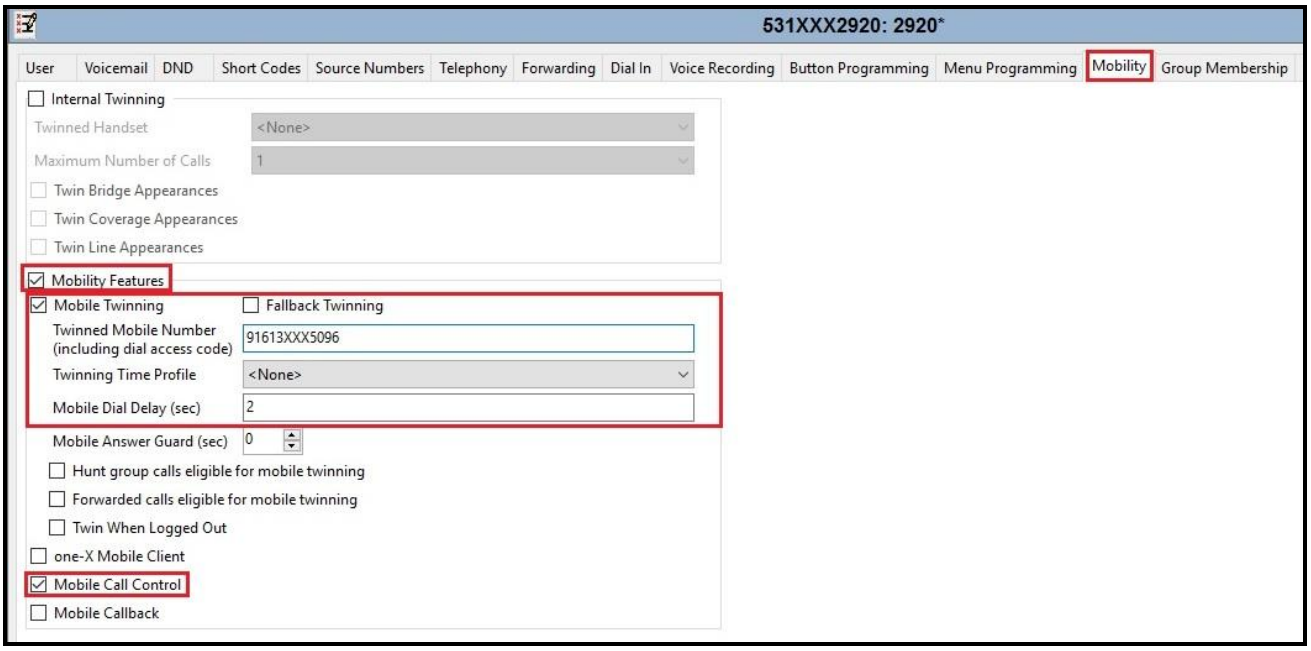


Figure 32 – Mobility Configuration for User

©2021 Avaya Inc. All Rights Reserved.

5.10. 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 **Call Details** tab on the **SIP Line** in **Section 5.5.2**
- 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 33 – 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 **531XXX2920** on line 17 are routed to **Destination 2620 531XXX2920** as below screenshot:

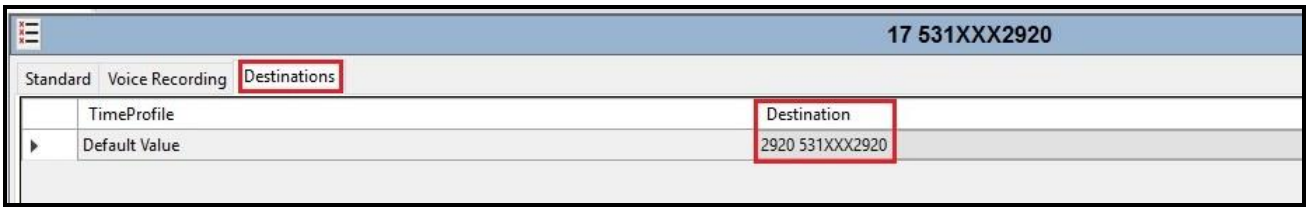


Figure 34 – Incoming Call Route for Destination 531XXX2920

©2021 Avaya Inc. All Rights Reserved.

For Feature Name Extension Service testing purpose, the incoming calls to DID number **531XXX7361** were configured to access **FNE00**. The **Destination** was appropriately defined as **FNE00** as below screenshot:

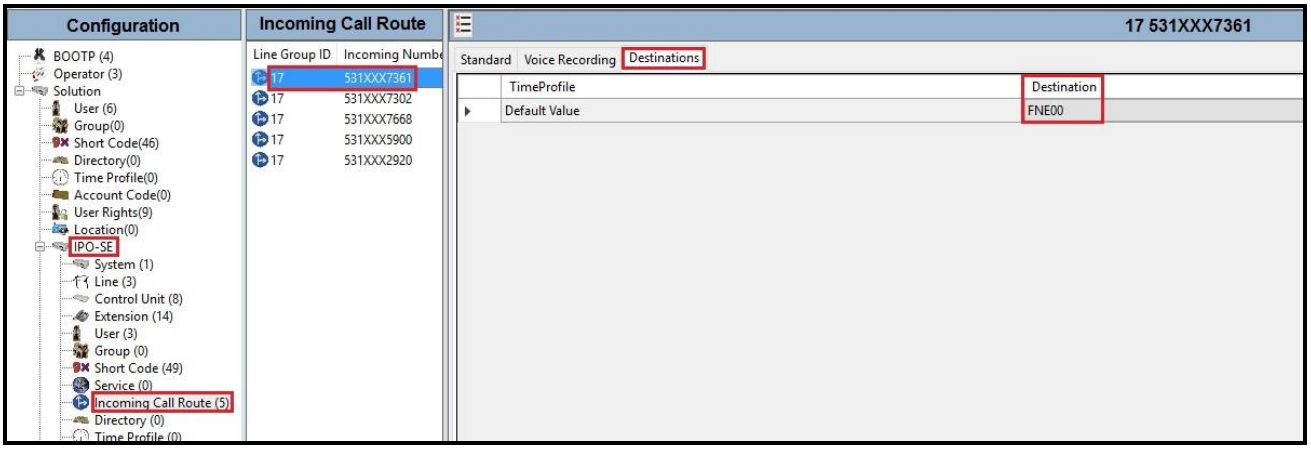


Figure 35 – Incoming Call Route for Destination FNE

For Voice Mail testing purpose, the incoming calls to DID number **531XXX7302** were configured to access **VoiceMail**. The **Destination** was appropriately defined as **VoiceMail** as below screenshot:

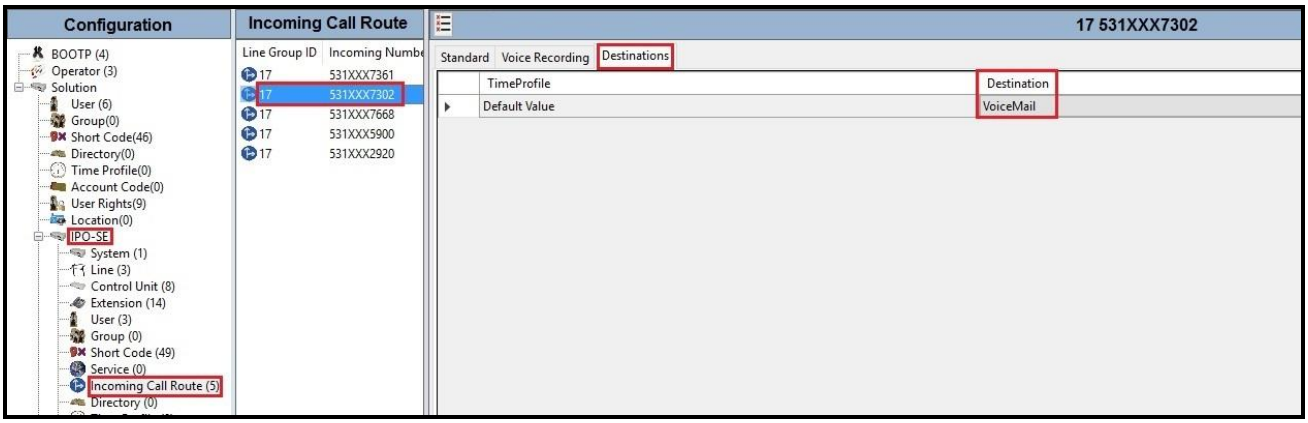


Figure 36 – Incoming Call Route for Destination VoiceMail

5.11. 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.

©2021 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 Cox Communications SIP Trunk Service.

Avaya elements reside on the Private side and the Cox Communications 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**

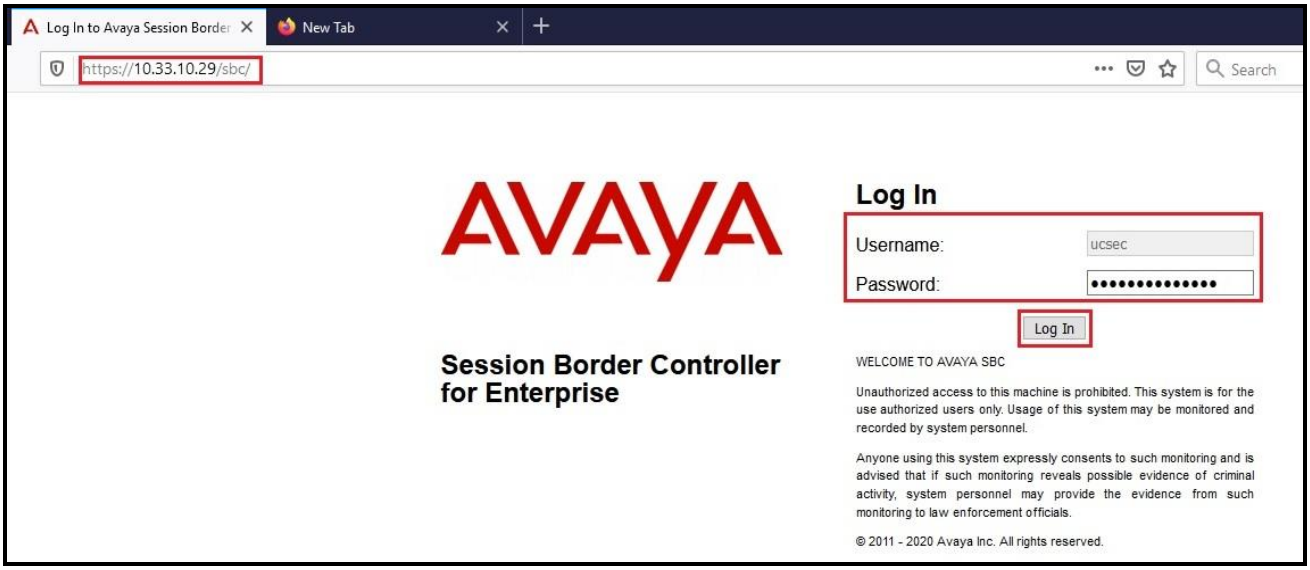


Figure 37 – Avaya SBCE Login

©2021 Avaya Inc. All Rights Reserved.

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

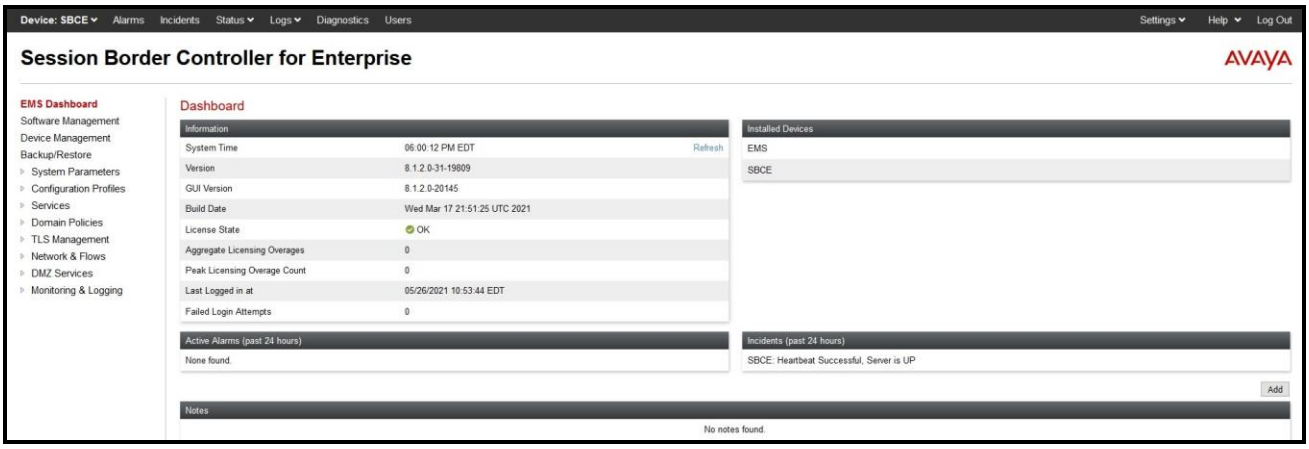


Figure 38 - Avaya SBCE Dashboard

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

Figure 39 - Avaya SBCE Device Management

©2021 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**.

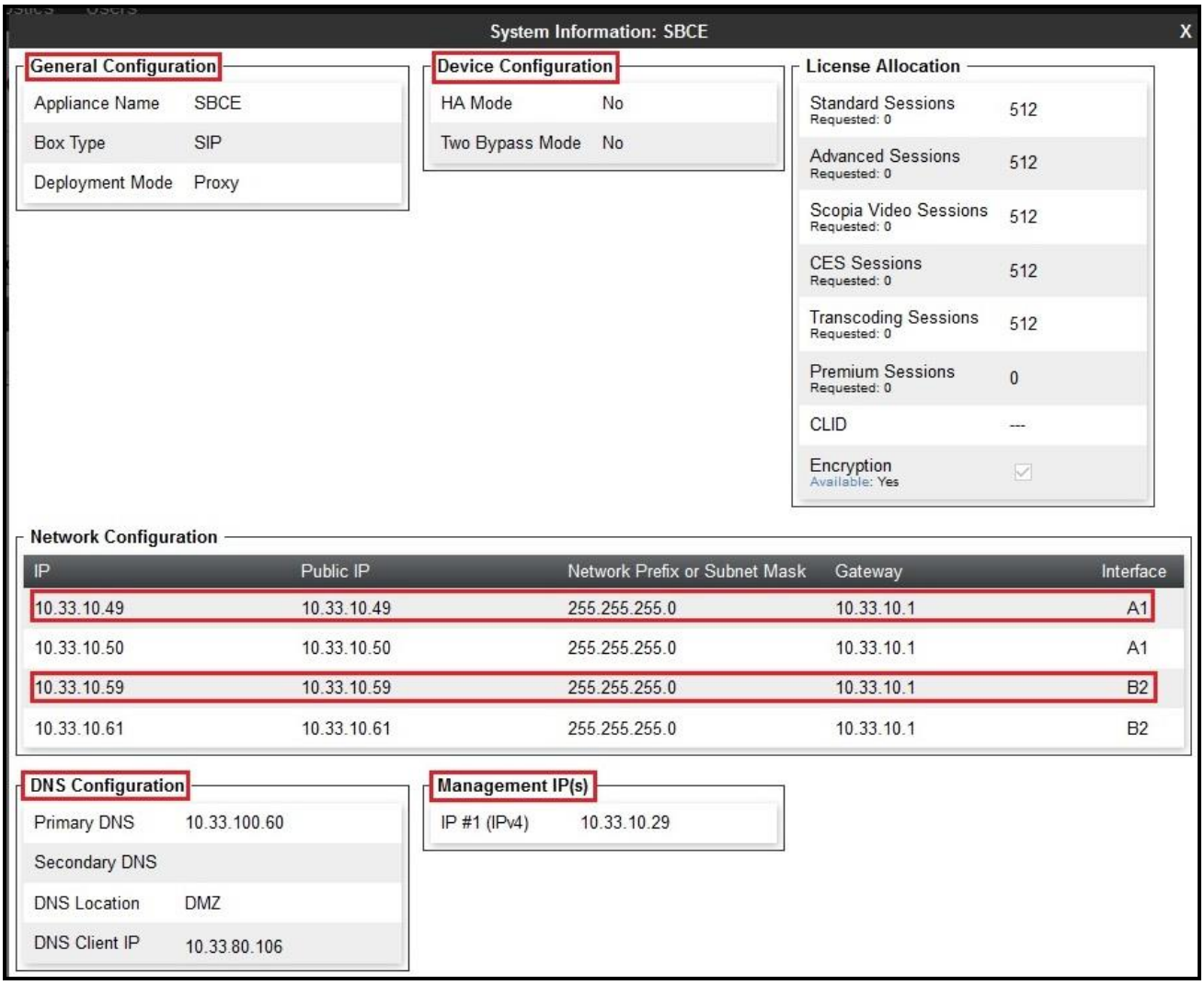


Figure 40 - Avaya SBCE System Information

©2021 Avaya Inc. All Rights Reserved.

6.2. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

6.2.1. 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 **Configuration Profiles → Server Interworking**

- Select **avaya-ru** in **Interworking Profiles**
- Click **Clone**
- Enter **Clone Name**: **IPO** and click **Finish** (not shown)
- Click **Edit** button
- Uncheck **T.38 Support** or check this option and click **Finish** (not shown). Note: Un-check this option as default for Fax G.711 pass-through mode

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

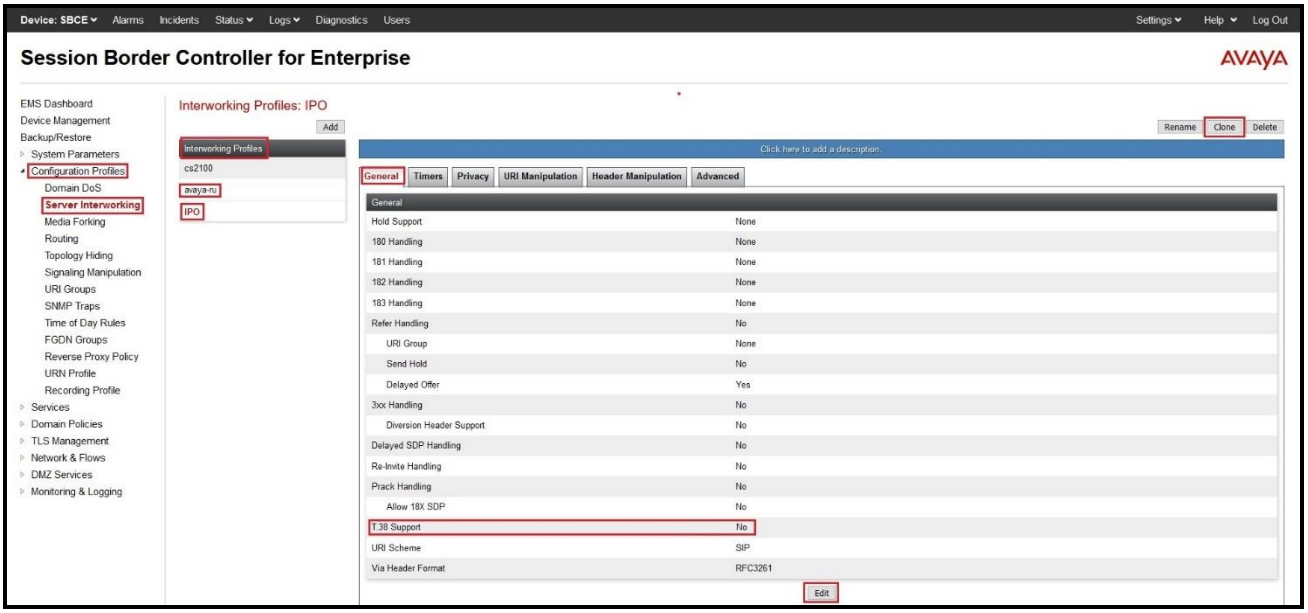


Figure 41 - Server Interworking – Avaya

©2021 Avaya Inc. All Rights Reserved.

6.2.2. Configure Server Interworking Profile – Cox Communications

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

- Enter **Profile Name**: **SP** (not shown)
- Click **Next** button to leave all options at default and click **Finish** (not shown)
- Click **Edit** button
- Uncheck **T.38 Support** or check this option and click **Finish** (not shown). Note: Un-check this option as default for Fax G.711 pass-through mode

The following screen shows that Cox Communications server interworking profile (named: **SP**) was added.

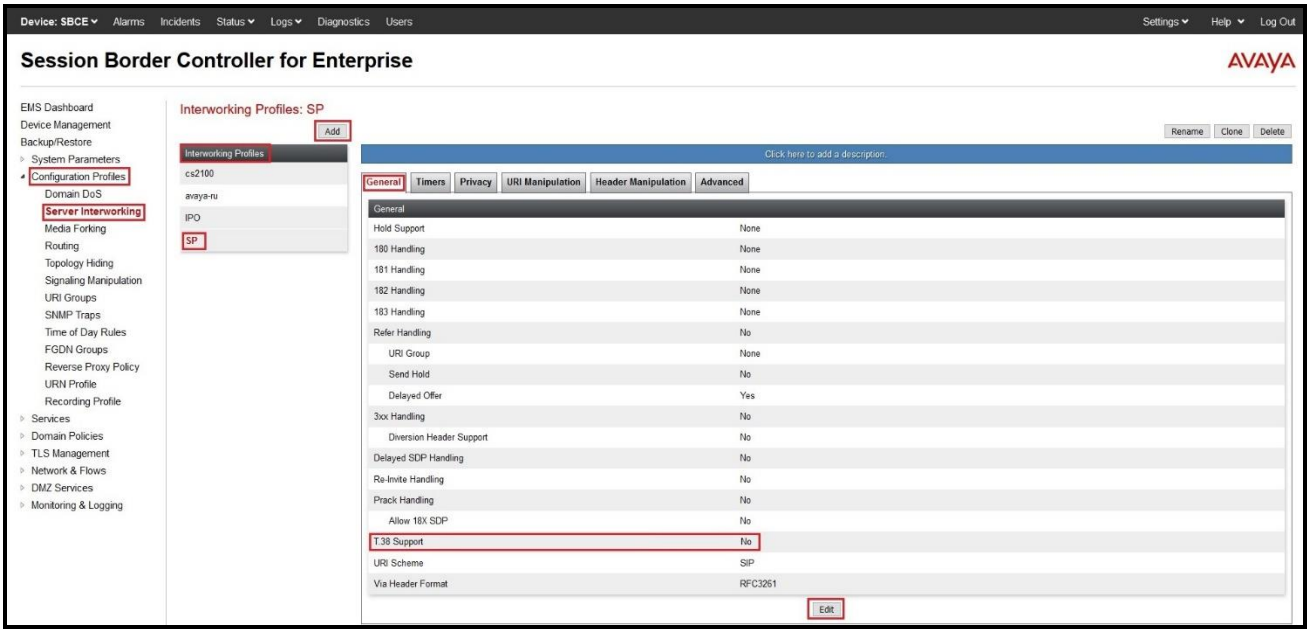


Figure 42 - Server Interworking – Cox Communications

©2021 Avaya Inc. All Rights Reserved.

6.3. Configure SIP Server

Servers are defined for each server connected to the Avaya SBCE. In this case, IP Office is connected as the Call Server and Cox managed CPE is connected as the Trunk Server

6.3.1. Configure SIP Server – Avaya Site

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

From the menu on the left-hand side, select **Services → SIP Servers → Add**.

Enter **Profile Name**: **IPO**

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

- **Server Type**: Select **Call Server**
- **TLS Client Profile**: Select **AvayaSBCClient**. Note: During the compliance test in the lab environment, demo certificates are used on Avaya Aura Session Manager, and are not recommended for production use.
- **IP Address/FQDN**: **10.33.10.56** (IP Office SE LAN1 IP address)
- **Port**: **5061**
- **Transport**: **TLS**
- Click **Finish** (not shown)

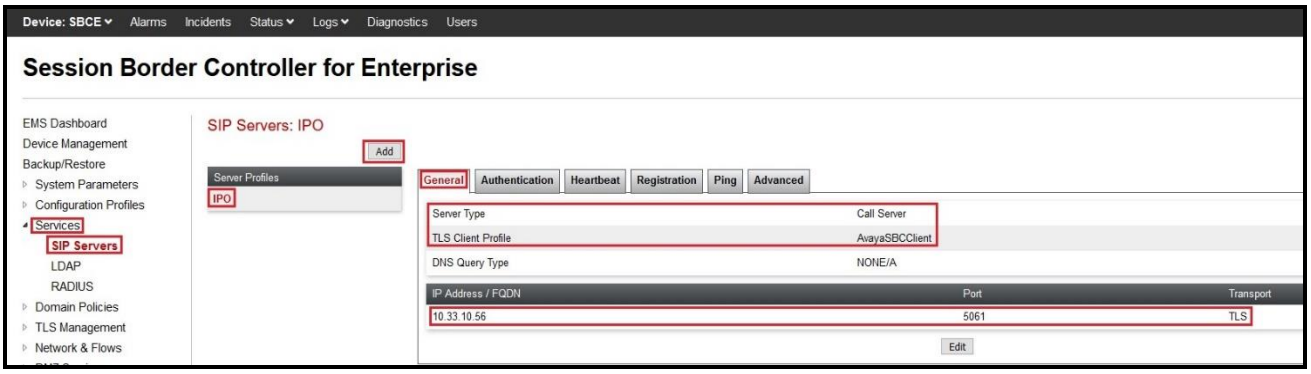


Figure 43 – Avaya Server Configuration – General

©2021 Avaya Inc. All Rights Reserved.

On the **Heartbeat** tab, click **Edit** button to enter the following:

- Check **Enable Heartbeat** option
- **Method**: **OPTIONS**
- **Frequency**: **60 seconds**
- **From URI**: **ping@10.33.10.49**
- **To URI**: **ping@10.33.10.56**
- Click **Finish** (Not shown)

Figure 44 – Avaya Server Configuration – Heartbeat

©2021 Avaya Inc. All Rights Reserved.

On the **Advanced** tab, click **Edit** button to enter the following:

- Check **Enable Grooming** box
- Select **IPO** for **Interworking Profile** (see **Section 6.2.1**)
- Click **Finish** (not shown)

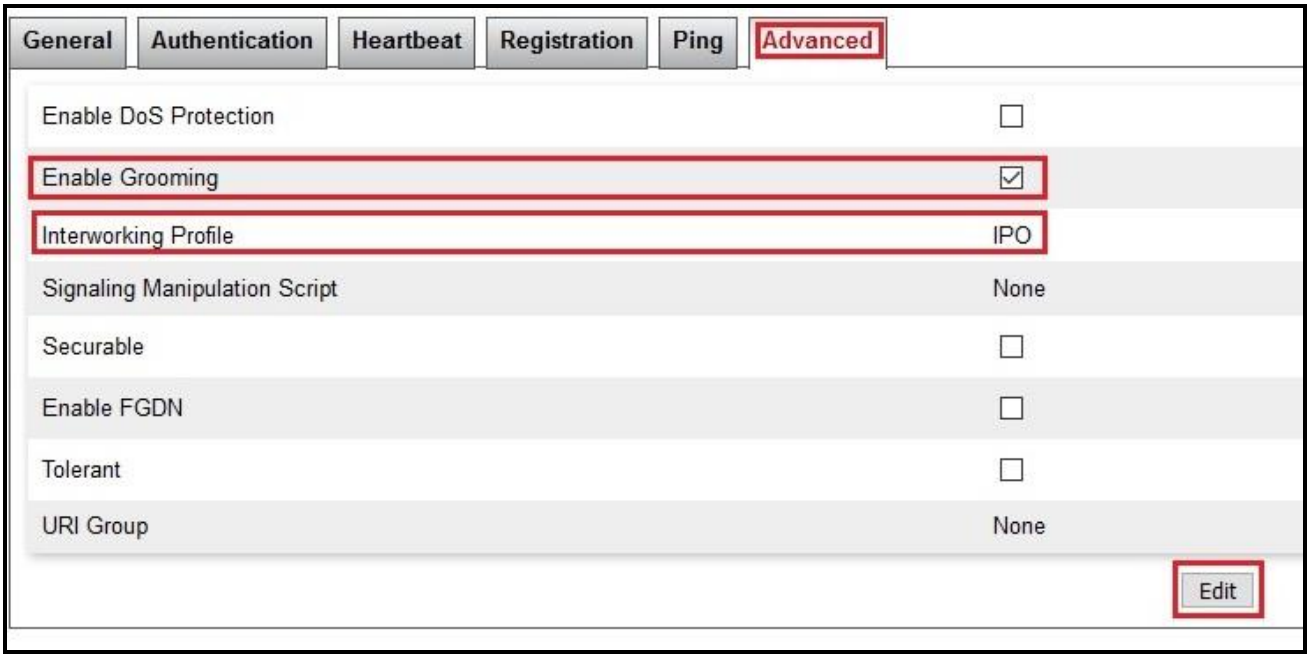


Figure 45 – Avaya Server Configuration – Advanced

©2021 Avaya Inc. All Rights Reserved.

6.3.2. Configure SIP Server – Cox Communications

From the menu on the left-hand side, select **Services → SIP Servers → Add** and enter **Profile Name**: **SP**

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

- **Server Type**: Select **Trunk Server**
- **IP Address/FQDN**: **10.33.10.60** (Cox managed CPE LAN IP address)
- **Port**: **5060**
- **Transport**: **UDP**
- Click **Finish** (not shown)

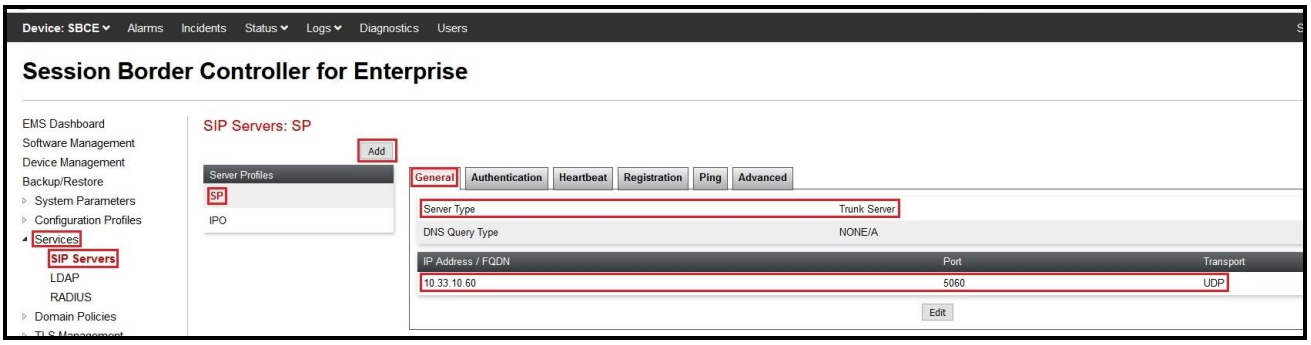


Figure 46 – Cox Communications Server Configuration – General

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

- Check **Enable Heartbeat**
- Select **Method**: **OPTIONS**
- Set **Frequency**: **60 seconds**
- Input **From URI**: **ping@10.33.10.59**
- Input **To URI**: **ping@10.33.10.60**

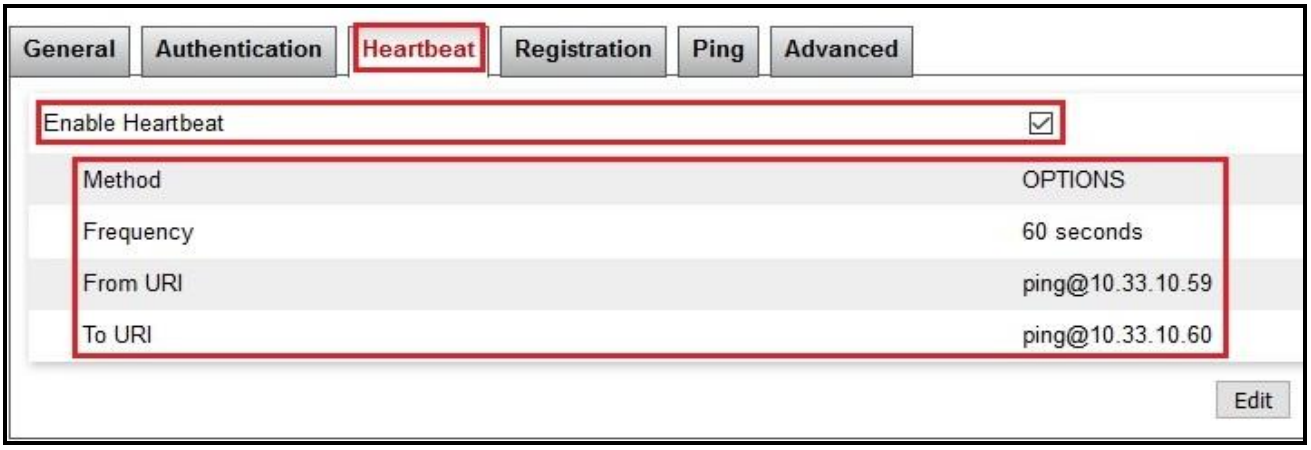


Figure 47 - Cox Communications Server Configuration – Heartbeat

©2021 Avaya Inc. All Rights Reserved.

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

- **Interworking Profile**: **SP** (see **Section 6.2.2**)
- Click **Finish** (not shown)

Figure 48 - Cox Communications Server Configuration – Advanced

©2021 Avaya Inc. All Rights Reserved.

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

- Check **Enable Authentication** option
- Input **User Name** (Cox Communications provided the user name)
- Leave **Realm** as blank
- Enter **Password** (Cox Communications provided the password)
- Enter **Confirm Password** (Cox Communications provided the password)
- Click **Finish**

Figure 49 - Cox Communications Server Configuration – Authentication

©2021 Avaya Inc. All Rights Reserved.

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

- Check **Register with All Servers** option
- Input **Refresh Interval**: **60 seconds**
- Leave **Realm** as blank
- Enter **From URI**: **531XXX0376@10.33.10.59**
- Enter **To URI**: **531XXX0376@10.33.10.60**
- Click **Finish** (Not shown)

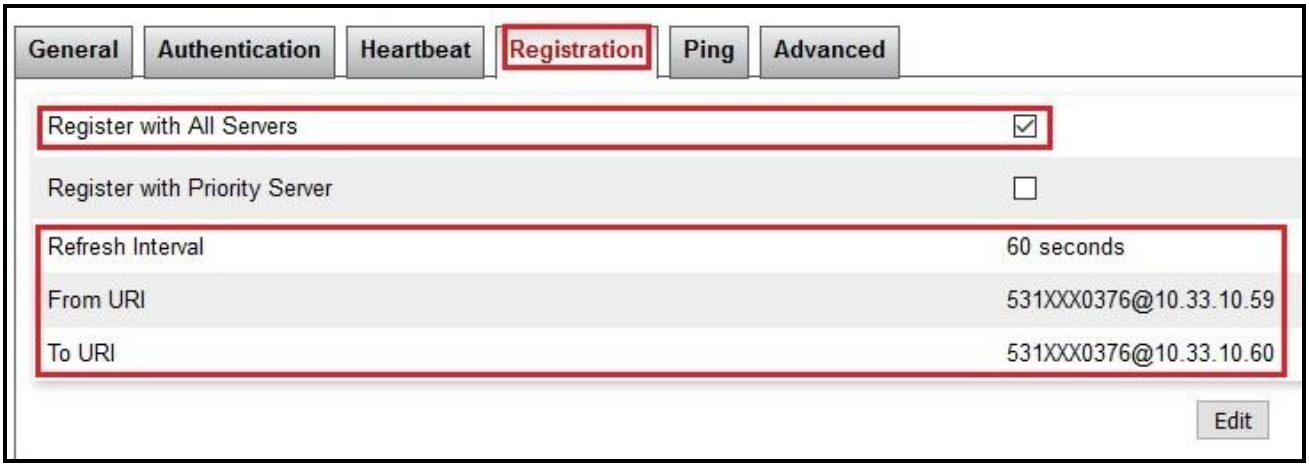


Figure 50 - Cox Communications Server Configuration – Registration

6.4. Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are routed to the service provider.

6.4.1. Configure Routing – Avaya IP Office

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

Enter **Profile Name**: **To_IPO** 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** (see **Section 6.3.1**). This selection will automatically populate the **Next Hop Address** field with **10.33.10.56:5061 (TLS)** (Avaya IP Office LAN1 port IP address)
- Click **Finish**

©2021 Avaya Inc. All Rights Reserved.

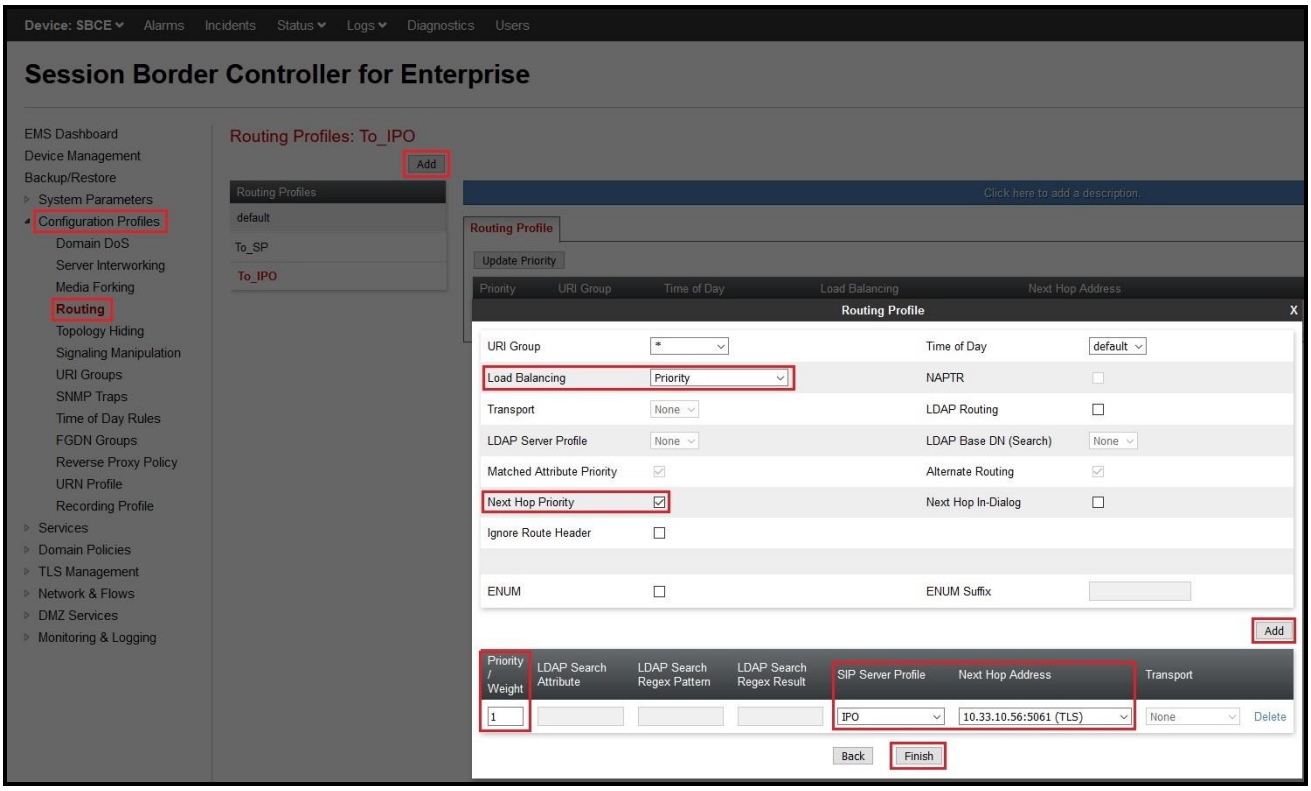


Figure 51 - Routing to Avaya IP Office

©2021 Avaya Inc. All Rights Reserved.

6.4.2. Configure Routing – Cox Communications

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

Enter **Profile Name**: **To_SP** (Not shown)

- **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**
- **Server Configuration**: **SP** (see **Section 6.3.2**). This selection will automatically populate the **Next Hop Address** field drop-down menu. Select **10.33.10.60:5060 (UDP)** (Cox managed CPE LAN IP Address)
- Click **Finish**

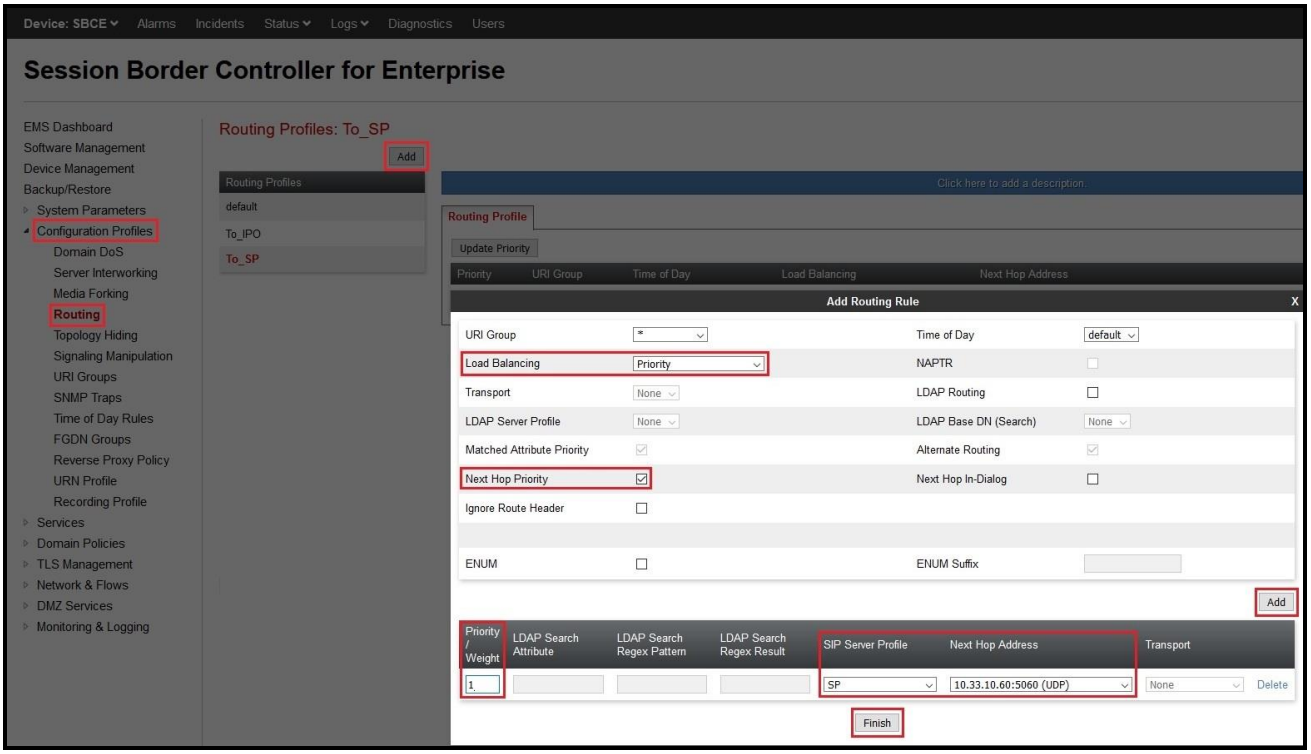


Figure 52 - Routing to Cox Communications

©2021 Avaya Inc. All Rights Reserved.

6.5. Configure Topology Hiding

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.

6.5.1. Configure Topology Hiding – Avaya Site

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

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name**: **To_IPO** and click **Finish** (not shown)
- Select **To_IPO** in **Topology Hiding Profiles** and click **Edit** button to modify as below:
  For the Header **From**,
  - In the **Criteria** column, select **IP/Domain**
  - In the **Replace Action** column, select **Overwrite**
  - In the Overwrite Value column, enter **10.33.10.49** (Avaya SBCE internal 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 **10.33.10.56** (Avaya IP Office LAN1 port IP address)

  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 **10.33.10.56** (Avaya IP Office LAN port IP address)
- Click **Finish** (not shown)

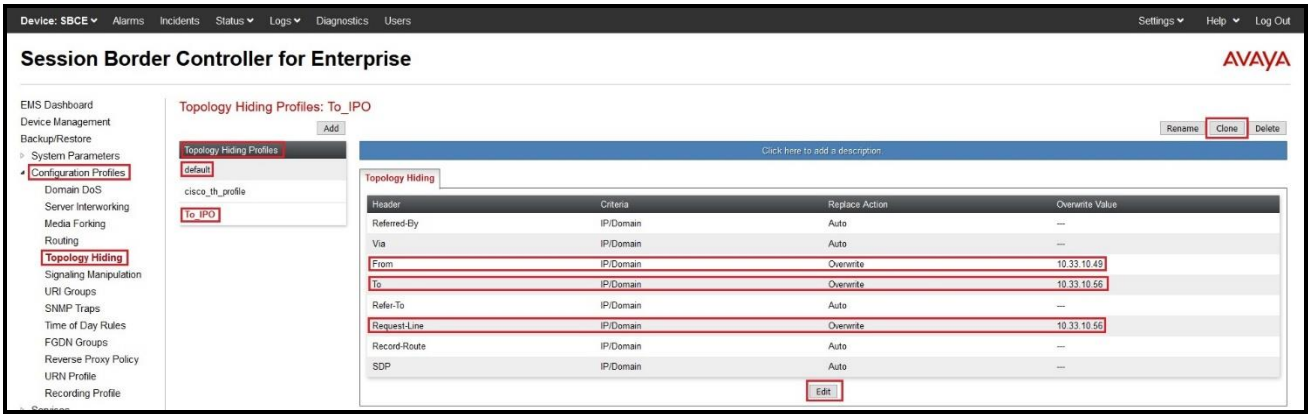


Figure 53 - Topology Hiding Avaya IP Office

©2021 Avaya Inc. All Rights Reserved.

6.5.2. Configure Topology Hiding – Cox Communications

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

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

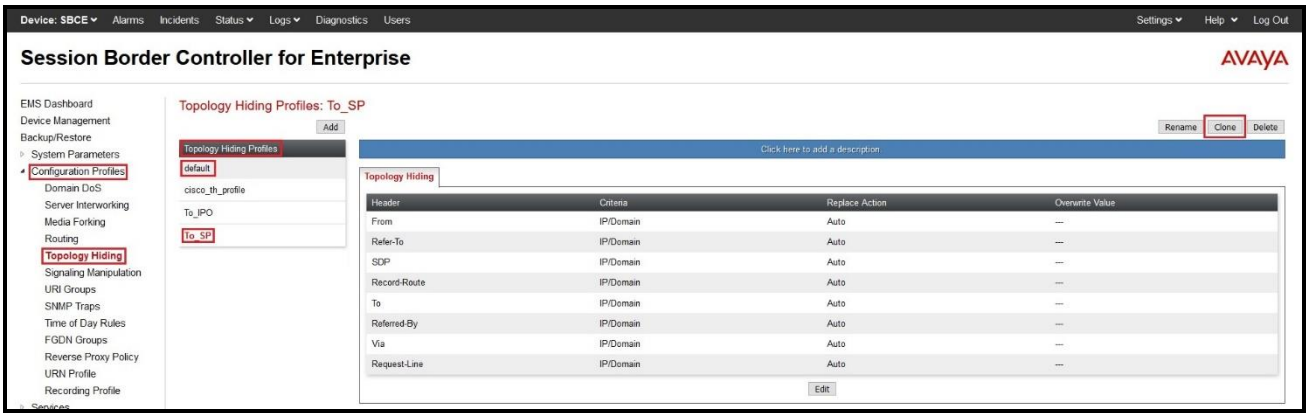


Figure 54 - Topology Hiding Cox Communications

©2021 Avaya Inc. All Rights Reserved.

6.6. 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.

6.6.1. Create Application Rules

Application rules define the type of SBC-based Unified Communication (UC) applications Avaya SBCE protects. You can also determine the maximum number of concurrent voice and video sessions that your network can process before resource exhaustion.

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**: **App-Rules** and click **Finish** button (Not shown)
- Select the **App-Rules** 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

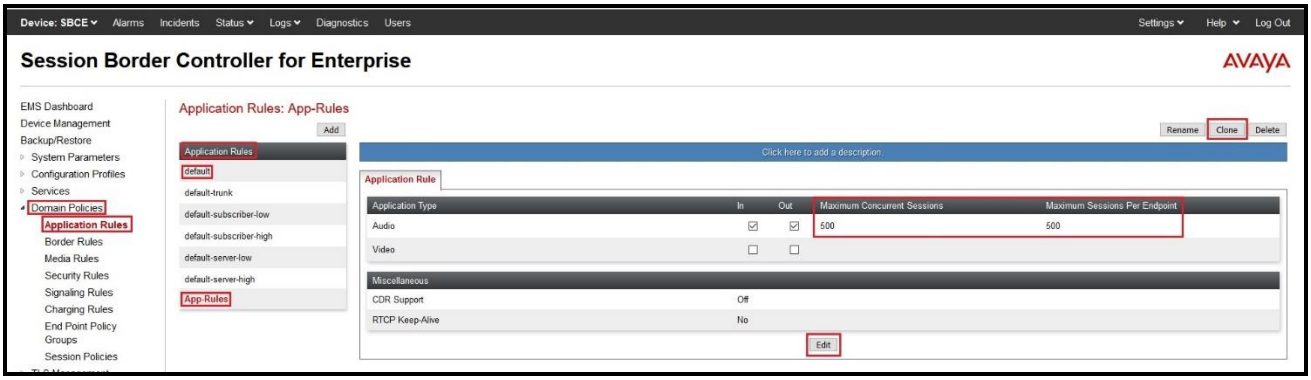


Figure 55 – Application Rule

6.6.2. Create Media Rules

Media Rules allow one to define RTP/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 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.

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

- Select the **avaya-low-med-enc** rule and click on **Clone** button

©2021 Avaya Inc. All Rights Reserved.

- Enter **Clone Name**: **IPO** and click **Finish** button (Not shown)
- Select the **IPO** rule from the list of **Media Rules** and click on **Edit** button
- Under **Audio Encryption**, select **Preferred Format #1** as **RTP** and **Preferred Format #2** as **SRTP_AES_CM_128_HMAC_SHA1_80**
- Under **Miscellaneous**, check **Capability Negotiation**
- Click **Finish** button (Not shown) to save the changes

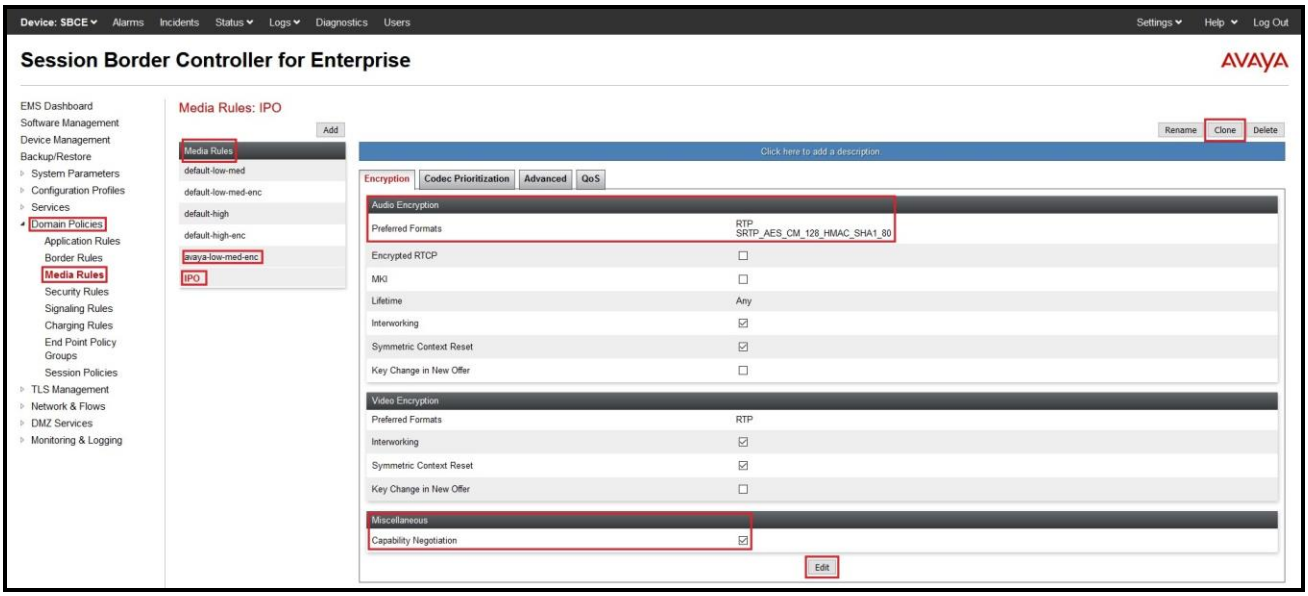


Figure 56 – Media Rule

©2021 Avaya Inc. All Rights Reserved.

6.6.3. 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.

To create an End Point Policy Group for the Enterprise, from the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**

- Select **Add**
- Enter **Group Name**: **EndPoint-Policy**
  - **Application Rule**: **App-Rules** (See **Section 6.6.1**)
  - **Border Rule**: **default**
  - **Media Rule**: **IPO** (See **Section 6.6.2**)
  - **Security Rule**: **default-low**
  - **Signaling Rule**: **default**
  - Leave other options as default
- Select **Finish** (not shown)

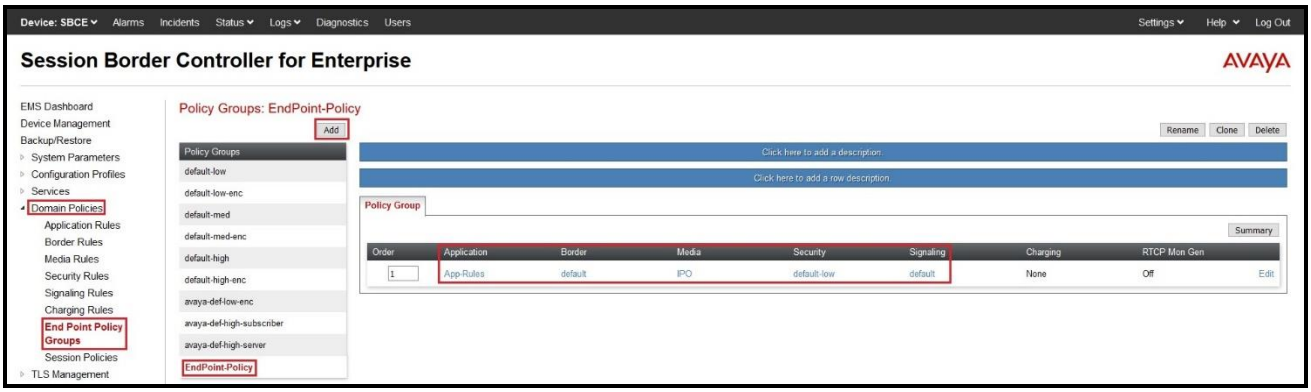


Figure 57 – End Point Policy - IPO

Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, from the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**

- Select **Add**
- Enter **Group Name**: **SP**
  - **Application Rule**: **App-Rules** (See **Section 6.6.1**)
  - **Border Rule**: **default**
  - **Media Rule**: **default-low-med**
  - **Security Rule**: **default-low**
  - **Signaling Rule**: **default**
  - Leave other options as default

©2021 Avaya Inc. All Rights Reserved.

- Select **Finish** (not shown)

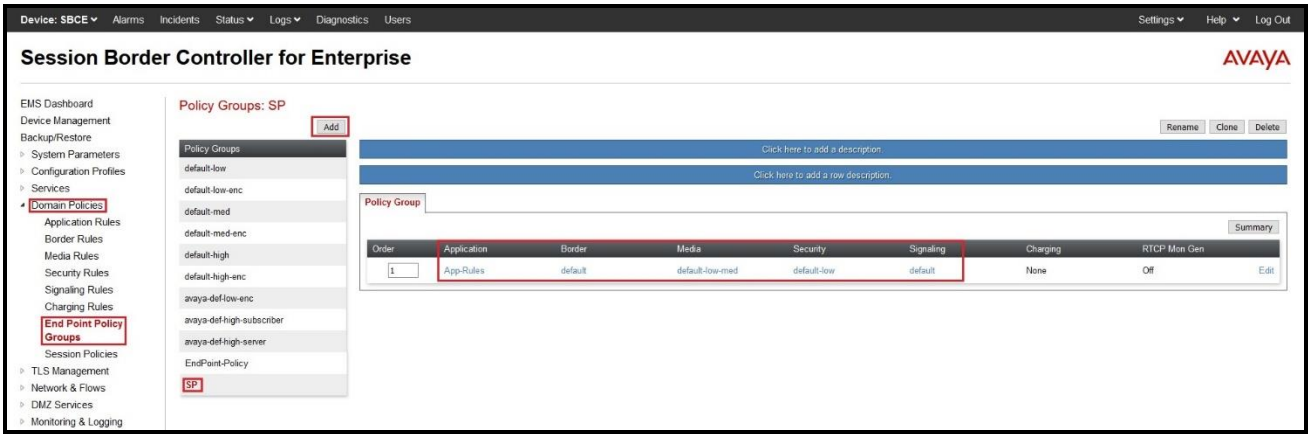


Figure 58 – End Point Policy – Cox Communications

©2021 Avaya Inc. All Rights Reserved.

6.7. Network & Flows

The Network & Flows 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.

6.7.1. Manage Network Settings

From the menu on the left-hand side, select **Network & Flows → 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**: **10.33.10.1**
  - **Subnet Mask**: **255.255.255.0**
  - **Interface**: **A1** (This is the Avaya SBCE inside interface)
  - Click the **Add** button to add the **IP Address** for inside interface: **10.33.10.49**
  - Click the **Finish** button to save the changes

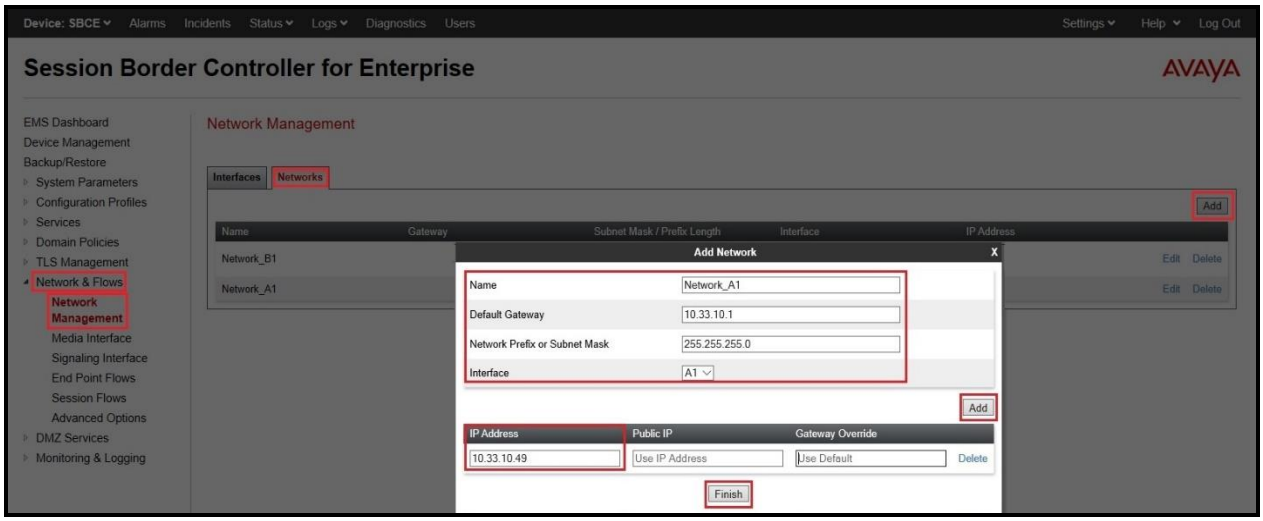


Figure 59 - Network Management – Inside Interface

©2021 Avaya Inc. All Rights Reserved.

From the menu on the left-hand side, select **Network & Flows → Network Management**.

- Select **Networks** tab and click **Add** button to add a network for the outside interface as follows:
  - **Name**: **Network_B2**
  - **Default Gateway**: **10.33.10.1**
  - **Subnet Mask**: **255.255.255.128**
  - **Interface**: **B2** (This is the Avaya SBCE outside interface)
  - Click the **Add** button to add the **IP Address** for outside interface: **10.33.10.59**
  - Click the **Finish** button to save the changes

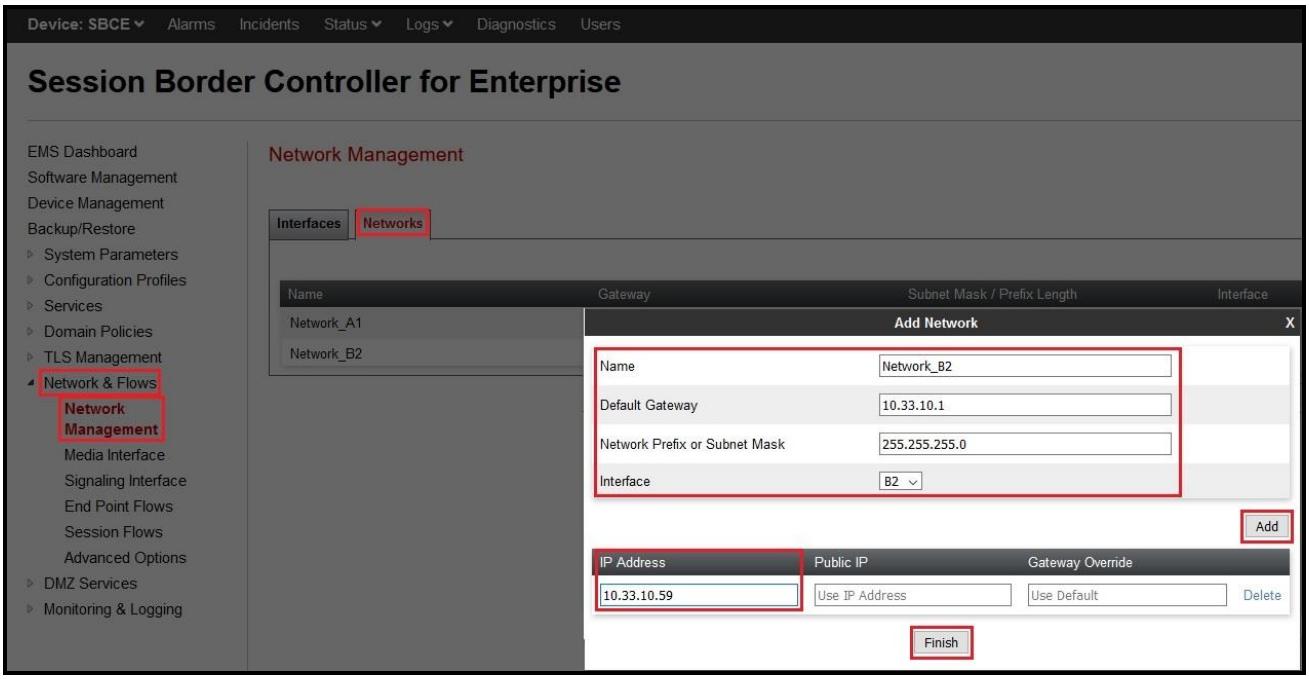


Figure 60 - Network Management – Outside Interface

©2021 Avaya Inc. All Rights Reserved.

From the menu on the left-hand side, select **Network & Flows → Network Management**

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

-

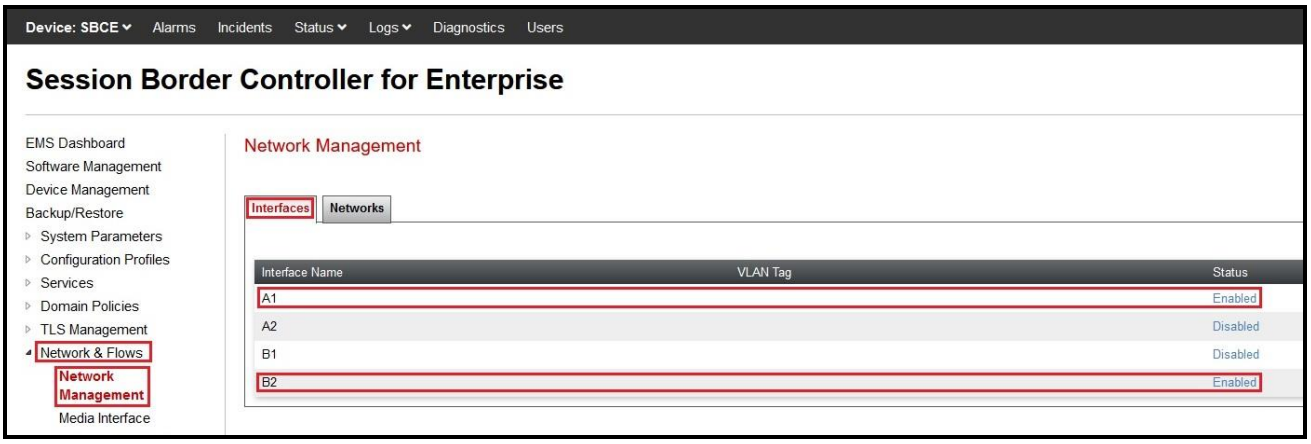


Figure 61 - Network Management – Interface Status

©2021 Avaya Inc. All Rights Reserved.

6.7.2. Create Media Interfaces

Media Interfaces define the IP Addresses and port ranges in which the Avaya SBCE will accept media streams on each interface. 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, **Network & Flows → Media Interface**

- Select the **Add** button and enter the following:
  - **Name**: **OutsideMedia**
  - **IP Address**: Select **Network_B2 (B2, VLAN 0)** and **10.33.10.59** (External IP address toward Cox managed CPE)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
  - **Name**: **InsideMedia**
  - **IP Address**: Select **Network_A1 (A1, VLAN 0)** and **10.33.10.49** (Internal IP address toward IP Office)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)

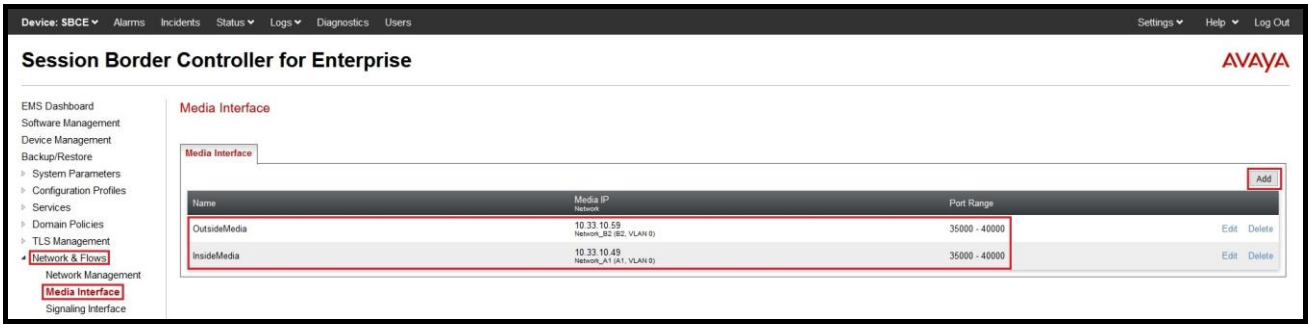


Figure 62 - Media Interface

©2021 Avaya Inc. All Rights Reserved.

6.7.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select **Network & Flows → Signaling Interface**

- Select the **Add** button and enter the following:
  - **Name**: **OutsideUDP**
  - **IP Address**: Select **Network_B2 (B2, VLAN 0)** and **10.33.10.59** (External IP address toward Cox managed CPE)
  - **UDP Port**: **5060**
  - Click **Finish** (not shown)

From the menu on the left-hand side, select **Network & Flows → Signaling Interface**

- Select the **Add** button and enter the following:
  - **Name**: **InsideTLS**
  - **IP Address**: Select **Network_A1 (A1, VLAN 0)** and **10.33.10.49** (Internal IP address toward IP Office)
  - **TLS Port**: **5061**
  - **TLS Profile**: **AvayaSBCServer**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
  - Click **Finish** (not shown)

Note: For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 the same as Cox Communications used. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061.

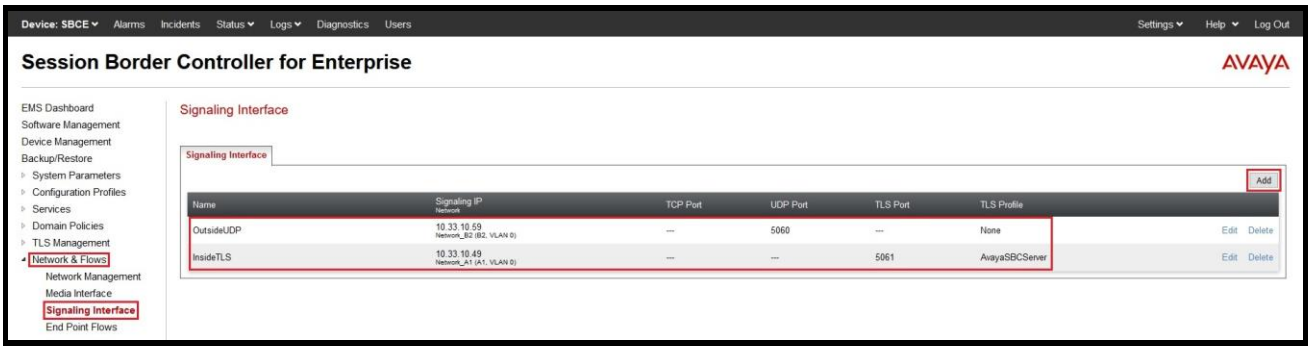


Figure 63 - Signaling Interface

©2021 Avaya Inc. All Rights Reserved.

6.7.4. Configure Server Flows

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

6.7.4.1 Create End Point Flows – Avaya IP Office

From the menu on the left-hand side, select **Network & Flows → End Point Flows**

- Select the **Server Flows** tab
- Select **Add**, enter the followings:
  - **Flow Name**: **IPO Flow**
  - **Server Configuration**: **IPO** (see **Section 6.3.1**)
  - **URI Group**: *****
  - **Transport**: *****
  - **Remote Subnet**: *****
  - **Received Interface**: **OutsideUDP** (see **Section 6.7.3**)
  - **Signaling Interface**: **InsideTLS** (see **Section 6.7.3**)
  - **Media Interface**: **InsideMedia** (see **Section 6.7.2**)
  - **Secondary Media Interface**: **None**
  - **End Point Policy Group**: **EndPoint-Policy** (see **Section 6.6.3**)
  - **Routing Profile**: **To_SP** (see **Section 6.4.2**)
  - **Topology Hiding Profile**: **To_IPO** (see **Section 6.5.1**)
  - Leave other options as default
  - Click **Finish** to save the changes

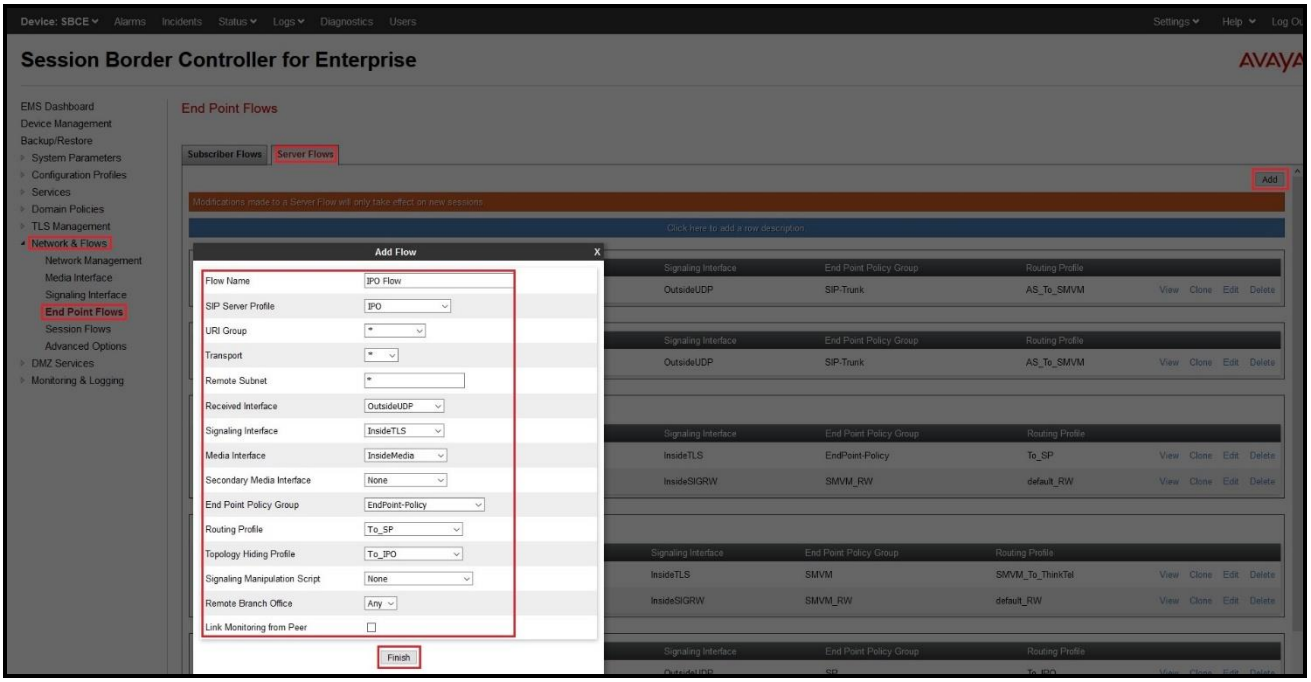


Figure 64 - End Point Flow 1

©2021 Avaya Inc. All Rights Reserved.

6.7.4.2 Create End Point Flows – Cox Communications

From the menu on the left-hand side, select **Network & Flows → End Point Flows**

- Select the **Server Flows** tab
- Select **Add**, enter the followings:
  - **Flow Name**: **SP Flow**
  - **Server Configuration**: **SP** (see **Section 6.3.2**)
  - **URI Group**: *****
  - **Transport**: *****
  - **Remote Subnet**: *****
  - **Received Interface**: **InsideTLS** (see **Section 6.7.3**)
  - **Signaling Interface**: **OutsideUDP** (see **Section 6.7.3**)
  - **Media Interface**: **OutsideMedia** (see **Section 6.7.2**)
  - **Secondary Media Interface**: **None**
  - **End Point Policy Group**: **SP** (see **Section 6.6.3**)
  - **Routing Profile**: **To_IPO** (see **Section 6.4.1**)
  - **Topology Hiding Profile**: **To_SP** (see **Section 6.5.2**)
  - Leave other options as default
  - Click **Finish** to save the changes

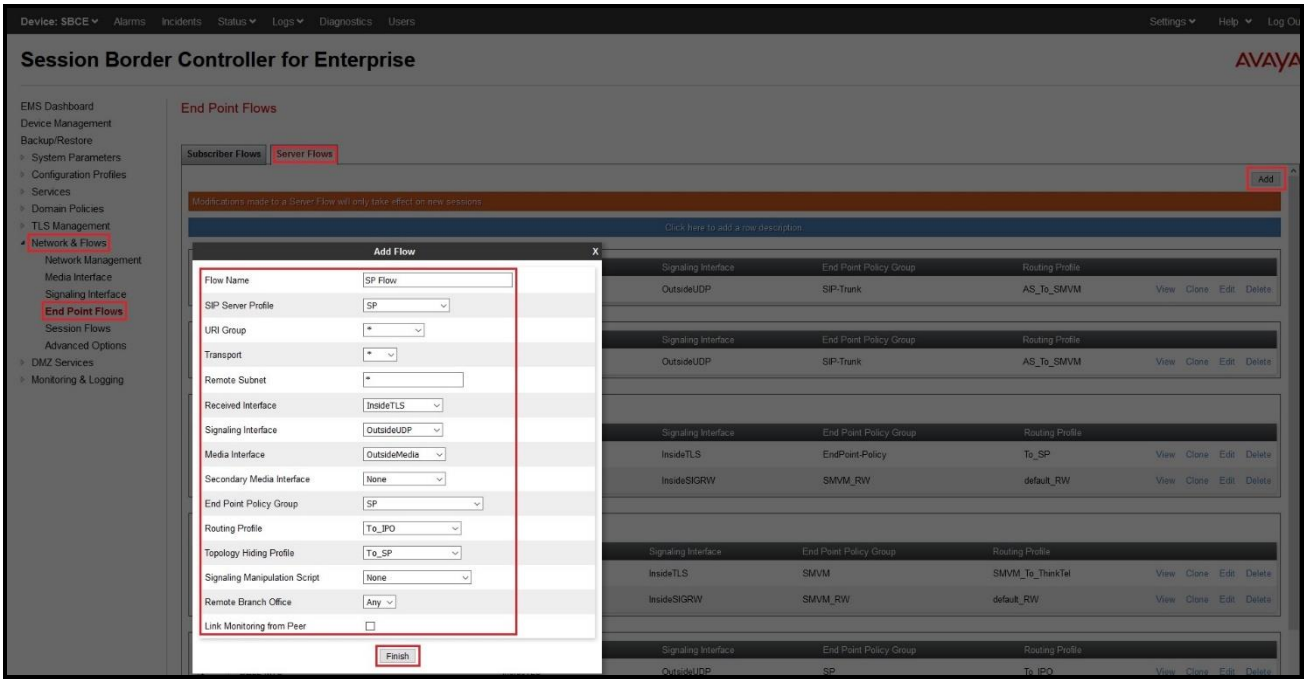


Figure 65 - End Point Flow 2

©2021 Avaya Inc. All Rights Reserved.

7. Cox Communications SIP Trunk Configuration

Cox Communications is responsible for the configuration of Cox Communications SIP Trunk Service. Cox Communications will provide the Cox managed CPE to the customer when the customer orders the Cox Communications SIP trunk service. Cox Communications will be responsible for managing the Cox managed CPE. Customer must provide the IP address used to reach the Cox managed CPE WAN port at the enterprise. Cox Communications will provide the customer necessary information to configure the SIP connection between Avaya enterprise and Cox Communications. The provided information from Cox Communications includes:

- IP address and port number used for signaling or media servers through any security devices
- DID numbers
- Authentication and Registration information
- Cox Communications SIP Trunk Specification (if applicable)

©2021 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 two active calls at the time)

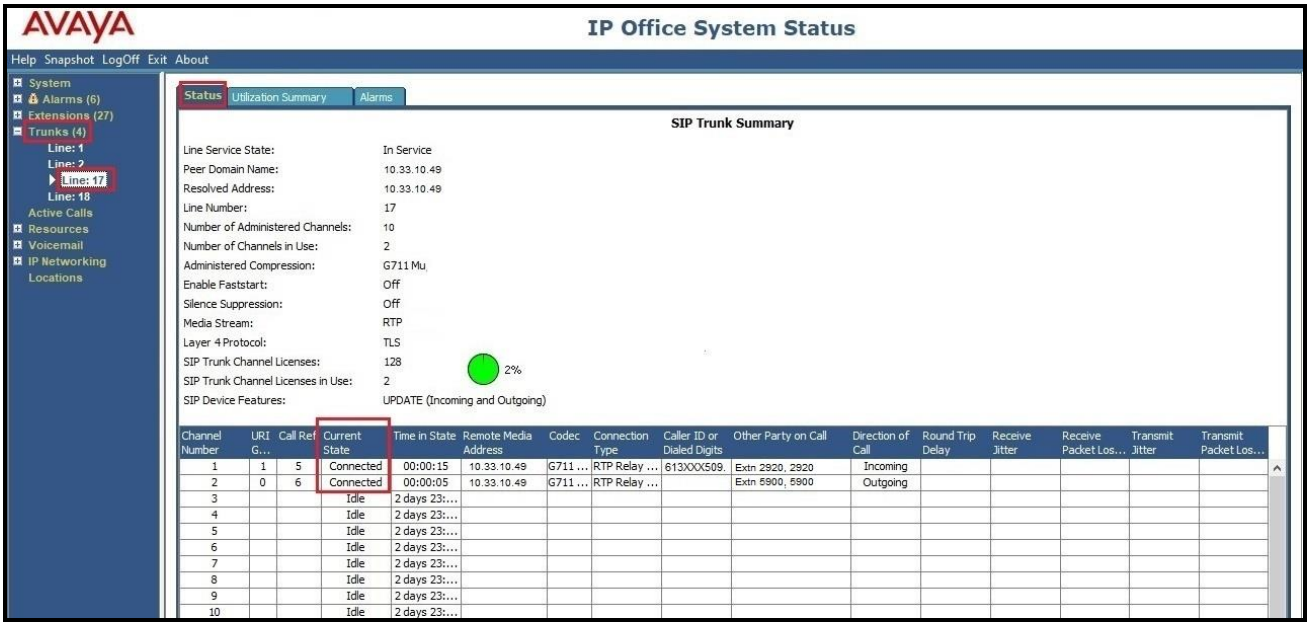


Figure 66 – SIP Trunk status

©2021 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.

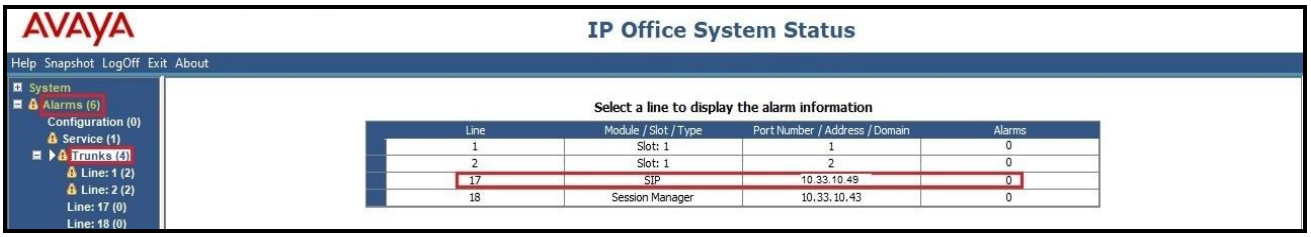


Figure 67 – SIP Trunk alarm

- 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.

©2021 Avaya Inc. All Rights Reserved.

9. Conclusion

Cox Communications passed compliance testing with the limitation listed in **Section 2.2**. These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 11.1 and the Avaya SBCE 8.1 to support Cox Communications SIP Trunking service, as shown in **Figure 1**.

10. Additional References

[1] Avaya IP Office™ Platform Release 11.1 Service Pack 1 – Release Notes / Technical Bulletin 227 General Availability, Issue 005, 11th September 2020

[2] Deploying IP Office Platform Server Edition, Release 11.1, Issue 14, April 2020

[3] IP Office Platform 11.1, Deploying Avaya IP Office Servers as Virtual Machines, August 2020

[4] IP Office Platform 11.1, Deploying an IP500 V2 IP Office Basic Edition System, Issue 36g, September 10, 2020

[5] Administering Avaya IP Office Platform with Manager, Release 11.1 SP1, July 2020.

[6] Deploying Avaya Session Border Controller on a Virtualized Environment Platform, Release 8.1, Issue 3, August 2020.

[7] Administering Avaya Session Border Controller for Enterprise, Release 8.1.x, Issue 3, August 2020.

Product documentation for Avaya products may be found at: http://support.avaya.com.

Additional IP Office documentation can be found at:
https://ipofficekb.avaya.com/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf_feed_template.html

Product documentation for Cox Communications SIP Trunking may be found at:
http://www.cox.com

©2021 Avaya Inc. All Rights Reserved.

11. Appendix A - 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 Workplace 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**.

©2021 Avaya Inc. All Rights Reserved.

11.1. Network Management on Avaya SBCE

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 internal IP address assigned to physical interface A1, and a second external IP address assigned to physical interface B2.

These are the IP addresses used in the reference configuration:

- **10.33.10.59** is the Avaya SBCE "outside" IP address previously provisioned for SIP Trunking with Cox Communications (see **Section 6.7.1**)
- **10.33.10.61** is the new Avaya SBCE "outside" IP address for Remote Worker access to Session Border Controller
- **10.33.10.49** is the Avaya SBCE "inside" IP address previously provisioned for SIP Trunking with IP Office (see **Section 6.7.1**)
- **10.33.10.50** is the new Avaya SBCE "inside" IP address for Remote Worker access to IP Office

From the menu on the left-hand side, select **Network & Flows → Network Management**

- Enter the above **IP Addresses** and **Gateway Addresses** for both the Inside and the Outside interfaces
- Select the physical interface used in the **Interface** column accordingly

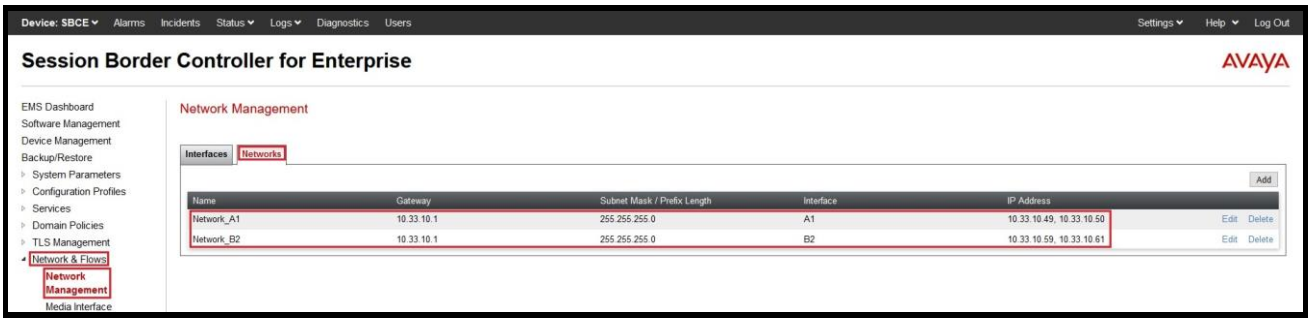


Figure 68 - Network Management

©2021 Avaya Inc. All Rights Reserved.

11.2. Media Interface on Avaya SBCE

From the menu on the left-hand side, select **Network & Flows → Media Interface**

- Select the **Add** button and enter the following:
  - **Name**: **OutsideMedRW**
  - **IP Address**: Select **Network_B2 (B2, VLAN 0)** and **10.33.10.61** (External IP address toward Remote Worker phones)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
  - **Name**: **InsideMedRW**
  - **IP Address**: Select **Network_A1 (A1, VLAN 0)** and **10.33.10.50** (Internal IP address toward IP Office)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)

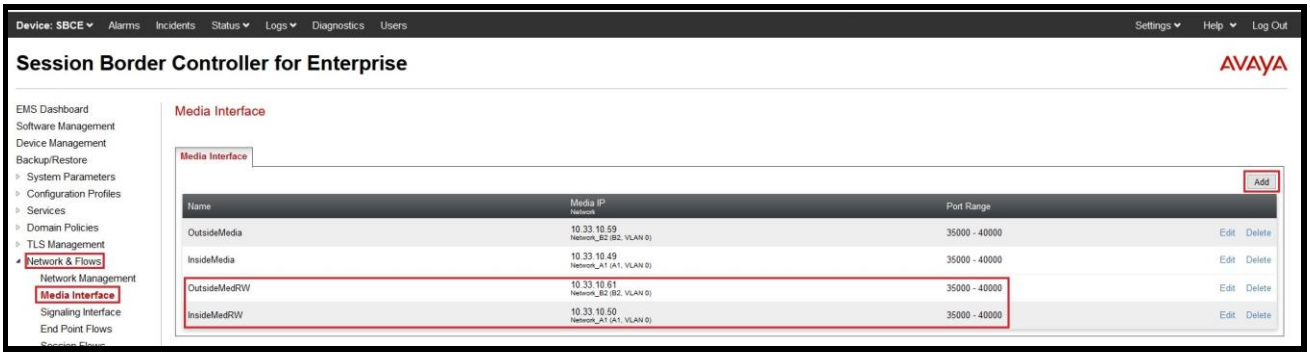


Figure 69 - Media Interface

Note: Media Interface **OutsideMedRW** is used in the Remote Worker Subscriber Flow (**Section 11.7.1**), and Media Interface **InsideMedRW** is used in the Remote Worker Server Flow (**Section 11.7.2.1**).

©2021 Avaya Inc. All Rights Reserved.

11.3. Signaling Interface on Avaya SBCE

The following screen shows the Signaling Interface settings. Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

Select the **Add** button to create Signaling Interface **OutsideSIGRW** using the parameters:

- **IP Address**: Select **Network_B2 (B2, VLAN 0)** and **10.33.10.61** (External IP address toward Remote Worker phones)
- **TLS Port**: **5061**
- **TLS Profile**: **AvayaSBCServer**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use
- Click on **Finish** (not shown)

Select the **Add** button to create Signaling Interface **InsideSIGRW** using the parameters:

- **IP Address:** Select **Network_A1 (A1, VLAN 0)** and **10.33.10.50** (Internal IP address toward IP Office)
- **TLS Port**: **5061**
- **TLS Profile**: **AvayaSBCServer**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use
- Click on **Finish** (not shown)

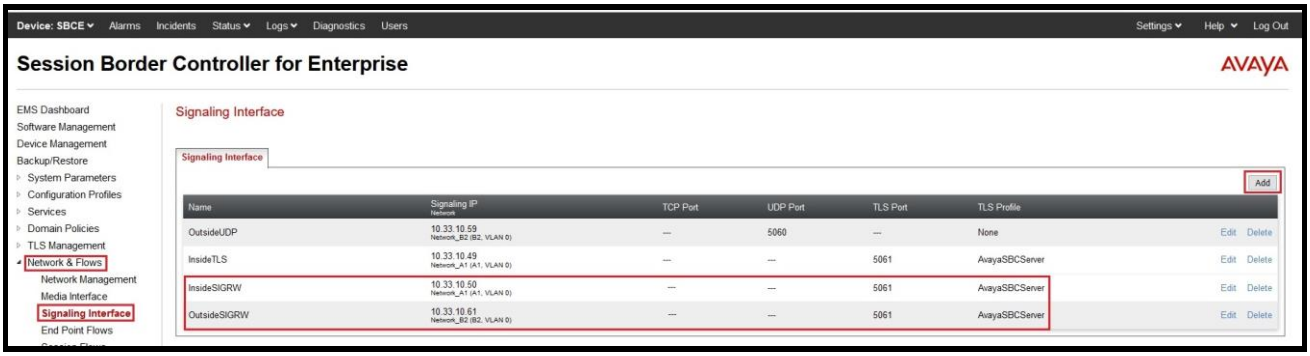


Figure 70 - Signaling Interface

Note: Signaling Interface **OutsideSIGRW** is used in the Subscriber Flows (**Section 11.7.1**), and in the Remote Worker Server Flow (**Section 11.7.2.1**). Signaling Interface **InsideSIGRW** is used in the Remote Worker Server Flow (**Section 11.7.2.1**).

©2021 Avaya Inc. All Rights Reserved.

11.4. Routing Profile on Avaya SBCE

The Routing Profile **To_IPO_RW** is created for routing the SIP traffic from Remote Worker to IP Office via Avaya SBCE.

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

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

- **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**
- **SIP Server Profile**: **IPO**
- **Next Hop Address**: **10.33.10.56:5061 (TLS)** (IP address of IP Office SE LAN1 port)
- Click **Finish** to save the changes

The Routing Profile **To_IPO_RW** is used in the Subscriber Flows (**Section 11.7.1**).

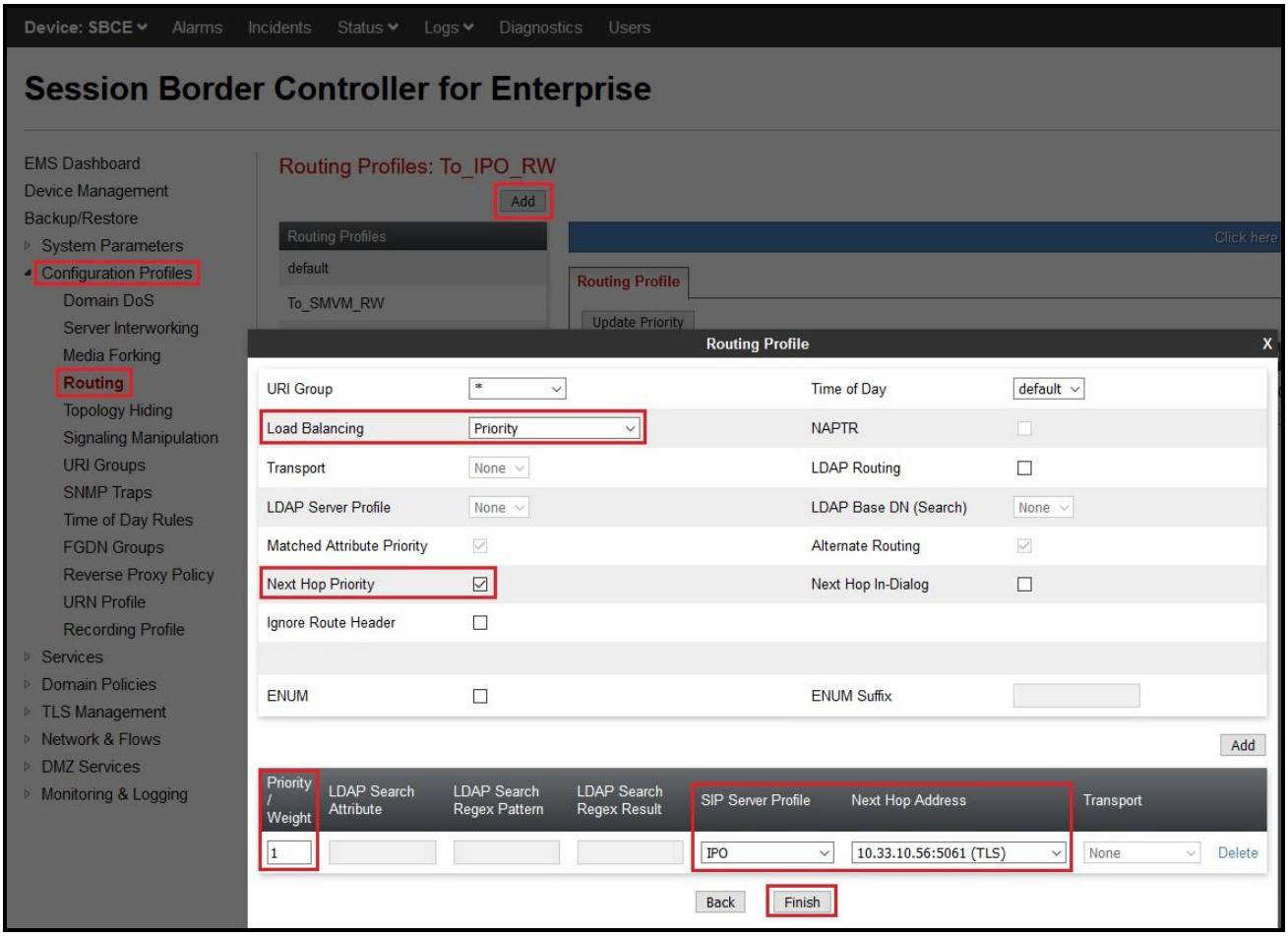


Figure 71 - Remote Worker Routing to IPO

©2021 Avaya Inc. All Rights Reserved.

The Routing Profile **default_RW** is created for routing SIP traffic from IP Office to Remote Worker via Avaya SBCE.
From the menu on the left-hand side, select **Configuration Profiles → Routing →Add**
Enter **Profile Name**: **default_RW**

- Check **Load Balancing**: **DNS/SRV**
- **NAPTR** box is checked
- Click **Finish**

The Routing Profile **default_RW** is used in the Remote Worker Server Flow in **Section 11.7.2.1**.

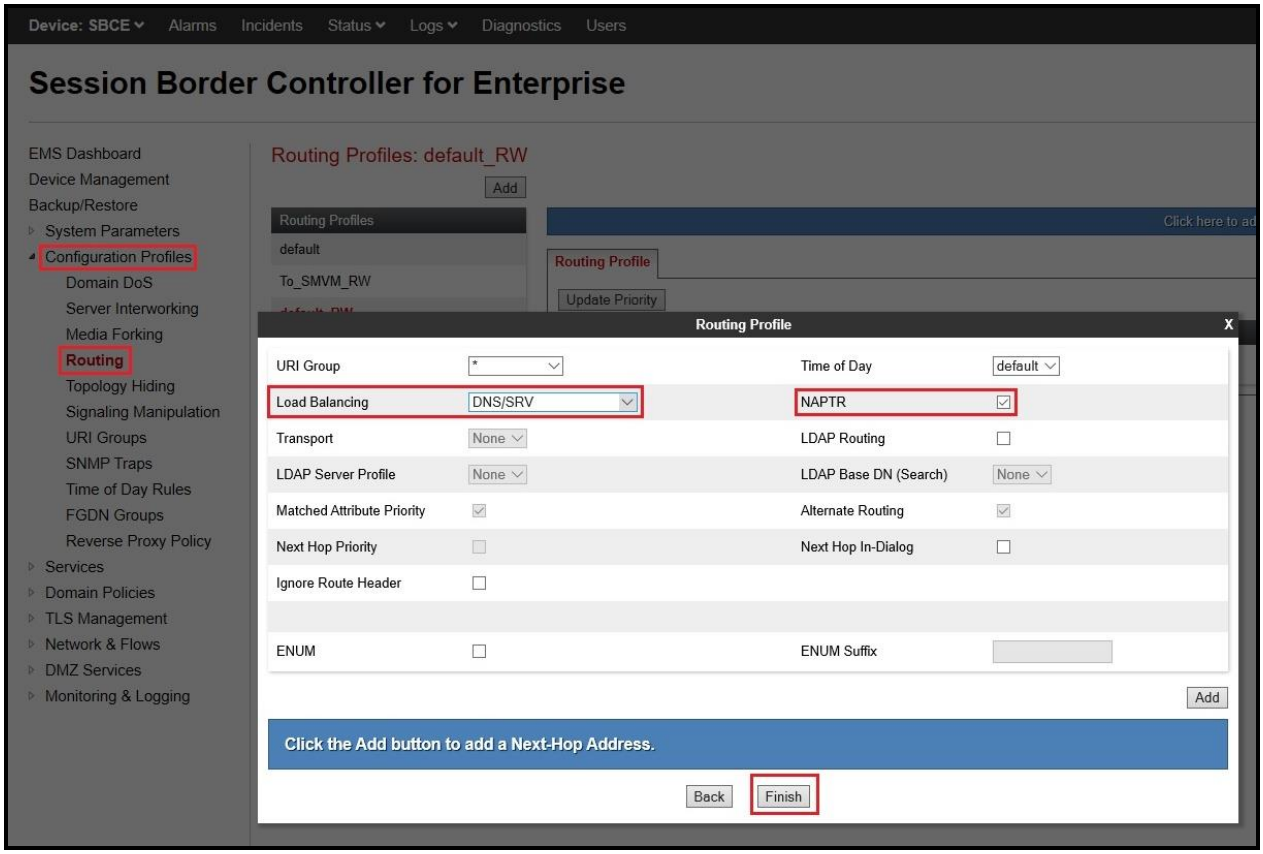


Figure 72 - Remote Worker Default Routing

©2021 Avaya Inc. All Rights Reserved.

11.5. User Agent on Avaya SBCE

User Agents are created for each type of endpoints tested. In this compliance testing, Avaya Remote Worker is used as the User Agent.

From the menu on the left-hand side, select **System Parameters → User Agents**
Click **Add** button to add the user agent:

- Enter **Name**: **Avaya Remote Worker**
- Enter **Regular Expression**: **Avaya Communicator.***
- Click on **Finish** (not shown)

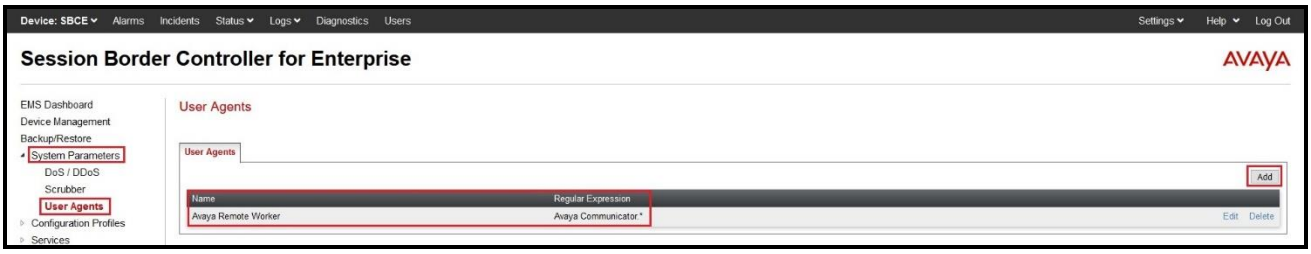


Figure 73 - User Agents for Remote Worker

©2021 Avaya Inc. All Rights Reserved.

The following abridged output of trace shows the details of an INVITE from an Avaya Workplace for Windows. The User-Agent shown in this trace will match User Agent Avaya Remote Worker shown above with a **Regular Expression** of "**Avaya Communicator.***". In this expression, "**.***" will match anything listed after the user agent name.

```
INVITE sips: 91613XXX5096@10.33.10.56 SIP/2.0
From: <sips:5900@10.33.10.56>;tag=9e53e33c-d9d1-4bc1-a164-7e5e10d3ee27
To: <sips:91613XXX5096@10.33.10.56>
CSeq: 1 INVITE
Call-ID: 832dffe4-085b-4ece-a7c3-1c9a0db6bd95
Contact: <sips:5900@172.16.199.9:49772>;+sip.instance="<urn:uuid:fddc4632-057c-4572-b12c-3e089dc51c07>"
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
Supported: eventlist,outbound,replaces
User-Agent: Avaya Communicator/3.0 (3.15.0.64.17; Avaya CSDK; Microsoft Windows NT 6.2.9200.0)
Max-Forwards: 70
Via: SIP/2.0/TLS 172.16.199.9:49772;branch=z9hG4bKfe8a4661-785e-4fef-941e-d066077a9b05
Accept-Language: en
Content-Type: application/sdp
Content-Length: 826
```

Figure 74 - Output of trace for User Agent

Note: The User Agent is defined in its associated **Subscriber Flows** in **Section 11.7.1**.

©2021 Avaya Inc. All Rights Reserved.

11.6. End Point Policy Groups on Avaya SBCE

A new End Point Policy Groups is defined for Remote Worker: **IPO_RW**.

To create the new **IPO_RW** group, click on **Add**. Enter the following:

- Enter a name (e.g., **IPO_RW**), and click on **Next** (not shown)
- The **Policy Group** window will open. Enter the following:
  - **Application Rule** = **App-Rules** (see **Section 6.6.1**)
  - **Border Rule** = **default**
  - **Media Rule** = **default-low-med**
  - **Security Rule** = **default-low**
  - **Signaling Rule** = **default**
- Click on **Finish** (not shown)

The End Point Policy Group **IPO_RW** is used in the Subscriber Flow in **Section 11.7.1** and Remote Worker Server Flow in **Section 11.7.2.1**.

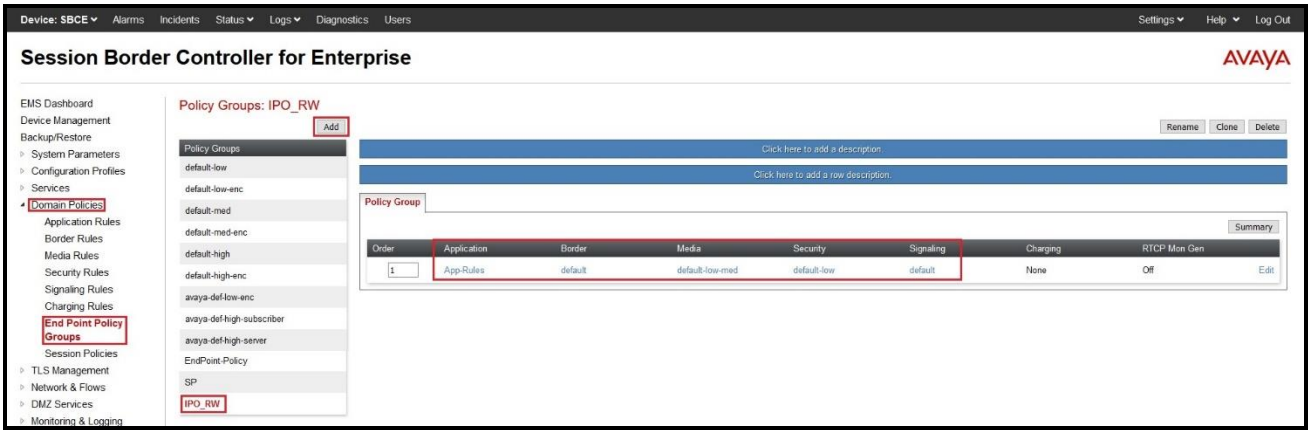


Figure 75 - Remote Worker End Point Policy

©2021 Avaya Inc. All Rights Reserved.

11.7. End Point Flows on Avaya SBCE

11.7.1. Subscriber Flow

The **Subscriber Flow** is defined for Remote Workers associated with the **User Agent Avaya Remote Worker** that was created in **Section 11.5**. The below subscriber flow is configured for Remote Worker to access IP Office via Avaya SBCE.

From the menu on the left-hand side, select **Network & Flows → End Point Flows**
On the **Subscriber Flows** tab, click on the **Add** button and enter the following:

- Enter a **Flow Name** (e.g., **Avaya Remote Worker**)
- **URI Group** = * (default)
- **User Agent** = **Avaya Remote Worker** (see **Section 11.5**)
- **Source Subnet** = ***** (default)
- **Via Host** = ***** (default)
- **Contact Host** = ***** (default)
- **Signaling Interface** = **OutsideSIGRW** (see **Section 11.3**)

Click on **Next** (not shown) and the Profile window will open (not shown). Enter the following:

- **Source** = **Subscriber**
- **Methods Allowed Before REGISTER =** Leave as default
- **Media Interface** = **OutsideMedRW** (see **Section 11.2**)
- **Received Interface** = **None**.
- **End Point Policy Group = IPO_RW** (see **Section 11.6**)
- **Routing Profile = To_IPO_RW** (see **Section 11.4**)
- **TLS Client Profile** = **None**
- **Signaling Manipulation Script** = **None**
- **Presence Server Address** = Leave as blank

Click on **Finish** (not shown).

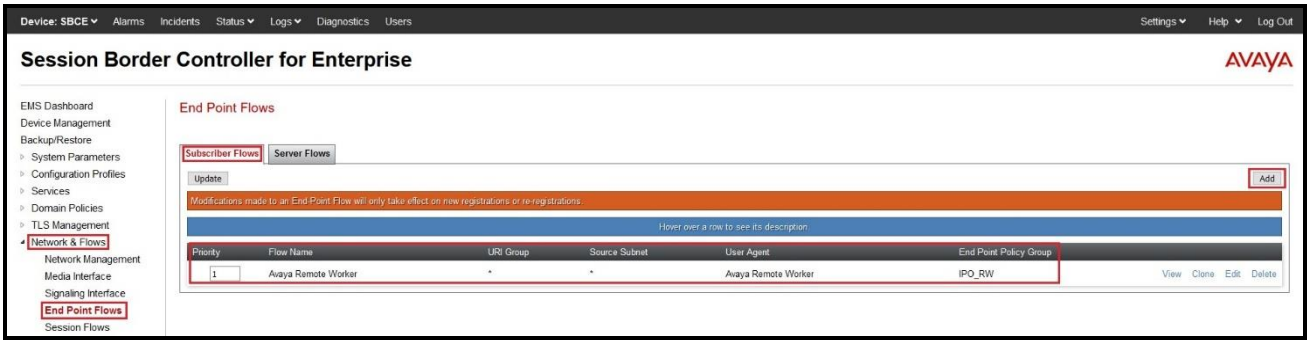
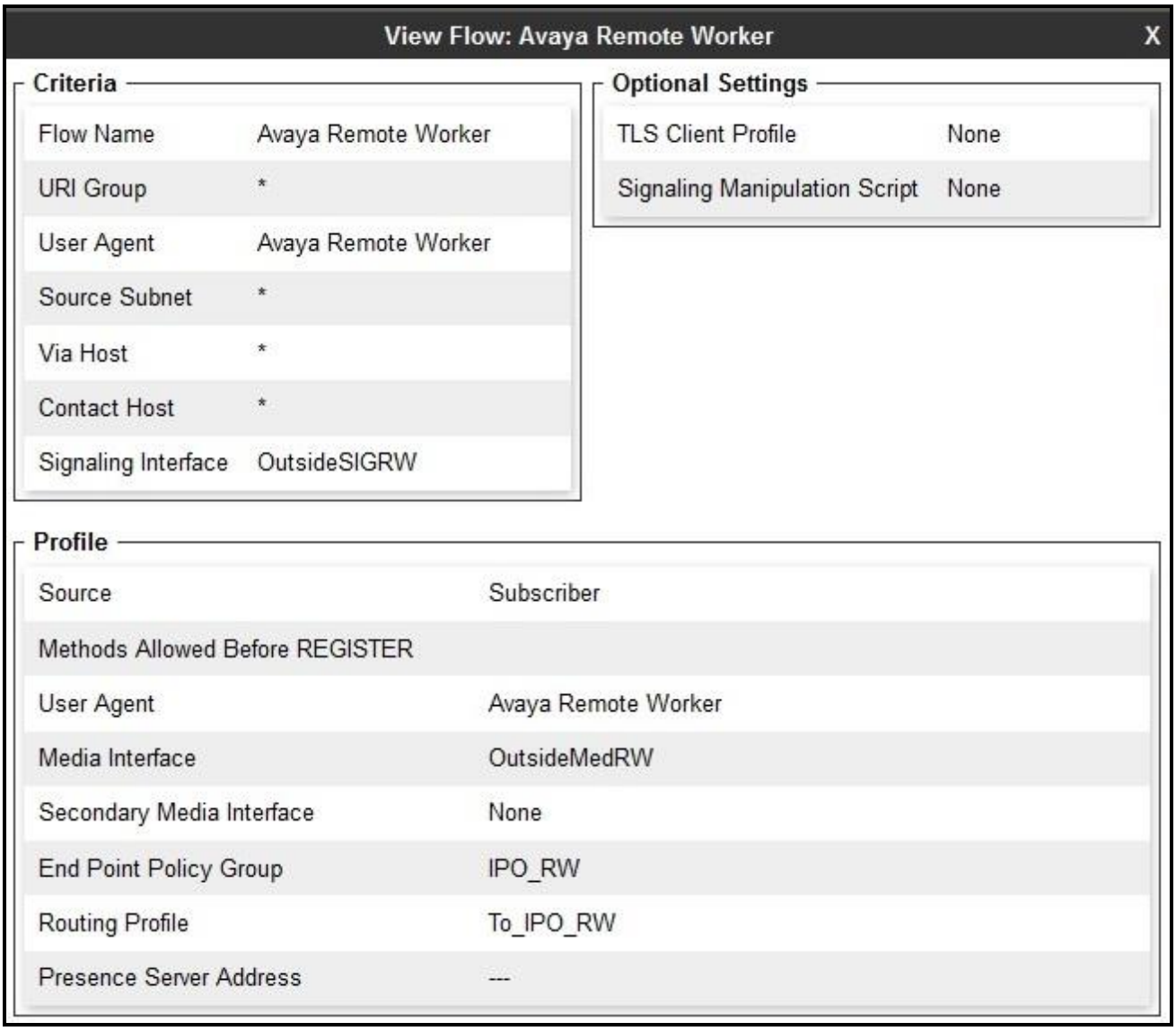


Figure 76 - Remote Worker Subscriber Flows – 1

©2021 Avaya Inc. All Rights Reserved.



View Flow: Avaya Remote Worker

Criteria

Flow Name	Avaya Remote Worker
URI Group	*
User Agent	Avaya Remote Worker
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	OutsideSIGRW

Optional Settings

TLS Client Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	Avaya Remote Worker
Media Interface	OutsideMedRW
Secondary Media Interface	None
End Point Policy Group	IPO_RW
Routing Profile	To_IPO_RW
Presence Server Address	---

Figure 77 - Remote Worker Subscriber Flows – 2

©2021 Avaya Inc. All Rights Reserved.

11.7.2. Server Flow

The new Remote Worker Server Flow (**IPO RW**) is configured for the SIP traffic flow from IP Office to Remote Worker via Avaya SBCE. Two existing Trunking Server Flows (IPO Flow in **Section 6.7.4.1** and SP Flow in **Section 6.7.4.2**) are also used for Remote Worker.

11.7.2.1 Remote Worker Server Flow

From the menu on the left-hand side, select **Network & Flows → Endpoint Flows**
Select the **Server Flows** tab and click the **Add** button (not shown) to enter the following:

- **Name = IPO RW**
- **Server Configuration** = **IPO** (see **Section 6.3.1**)
- **URI Group** = ***** (default)
- **Transport** = ***** (default)
- **Remote Subnet** = ***** (default)
- **Received Interface** = **OutsideSIGRW** (see **Section 11.3**)
- **Signaling Interface** = **InsideSIGRW** (see **Section 11.3**)
- **Media Interface** = **InsideMedRW** (see **Section 11.2**)
- **Secondary Media Interface** = **None**
- **End Point Policy Group** = **IPO_RW** (see **Section 11.6**)
- **Routing Profile** = **default_RW** (see **Section 11.4**)
- **Topology Hiding Profile** = **None** (default)
- **Signaling Manipulation Script = None** (default)
- **Remote Branch Office** = **Any** (default)
- **Link Monitoring from Peer =** uncheck (default)

Click **Finish** (not shown).

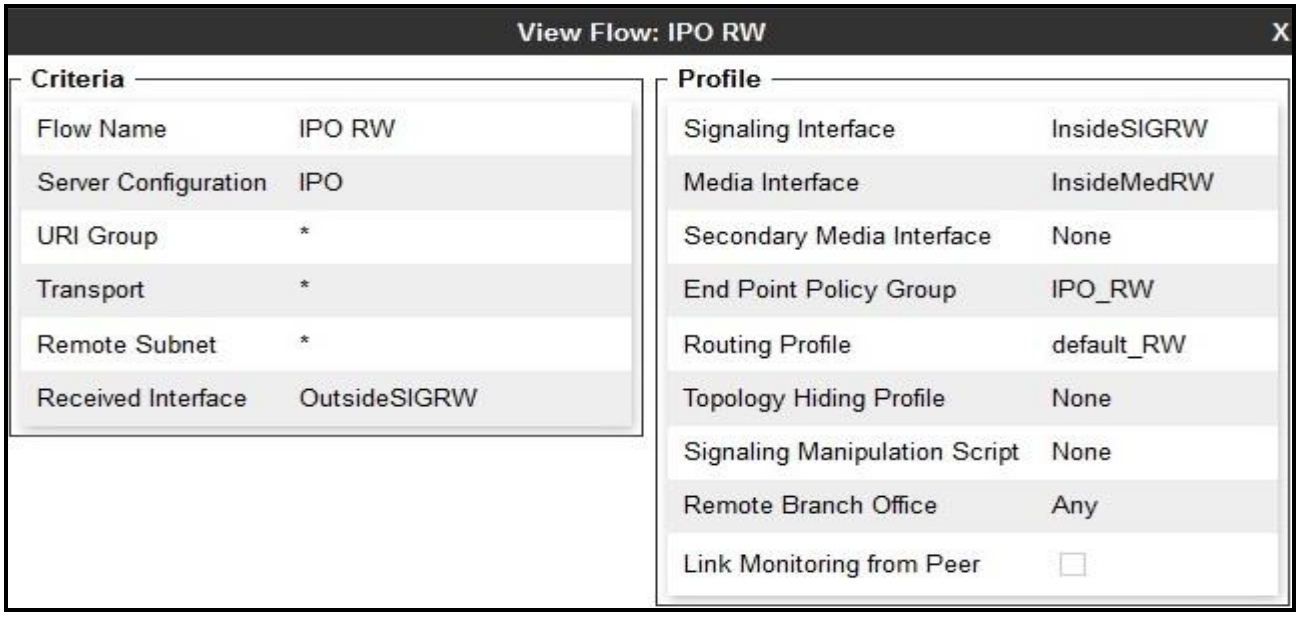


Figure 78 - Remote Worker Server Flow 1

©2021 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 6.7.4.1**), 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.

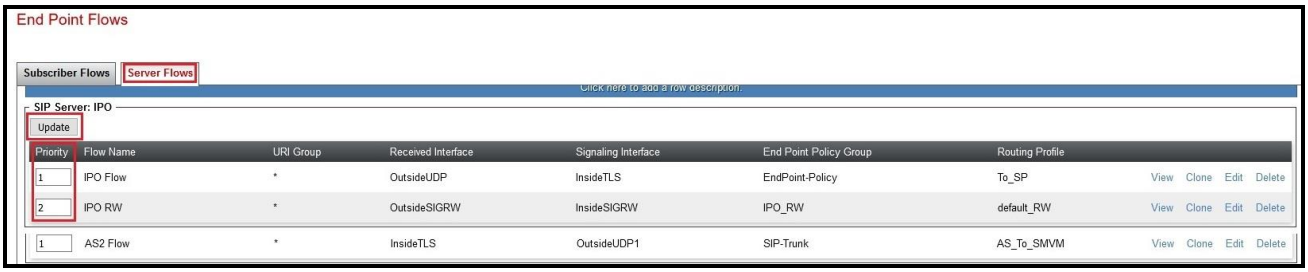


Figure 79 – Remote Worker Server Flow 2

©2021 Avaya Inc. All Rights Reserved.

11.7.2.2 Trunking Server Flow

Two existing Trunking Server Flows (IPO Flow in **Section 6.7.4.1**; SP Flow in **Section 6.7.4.2**) are also used for Remote Worker.

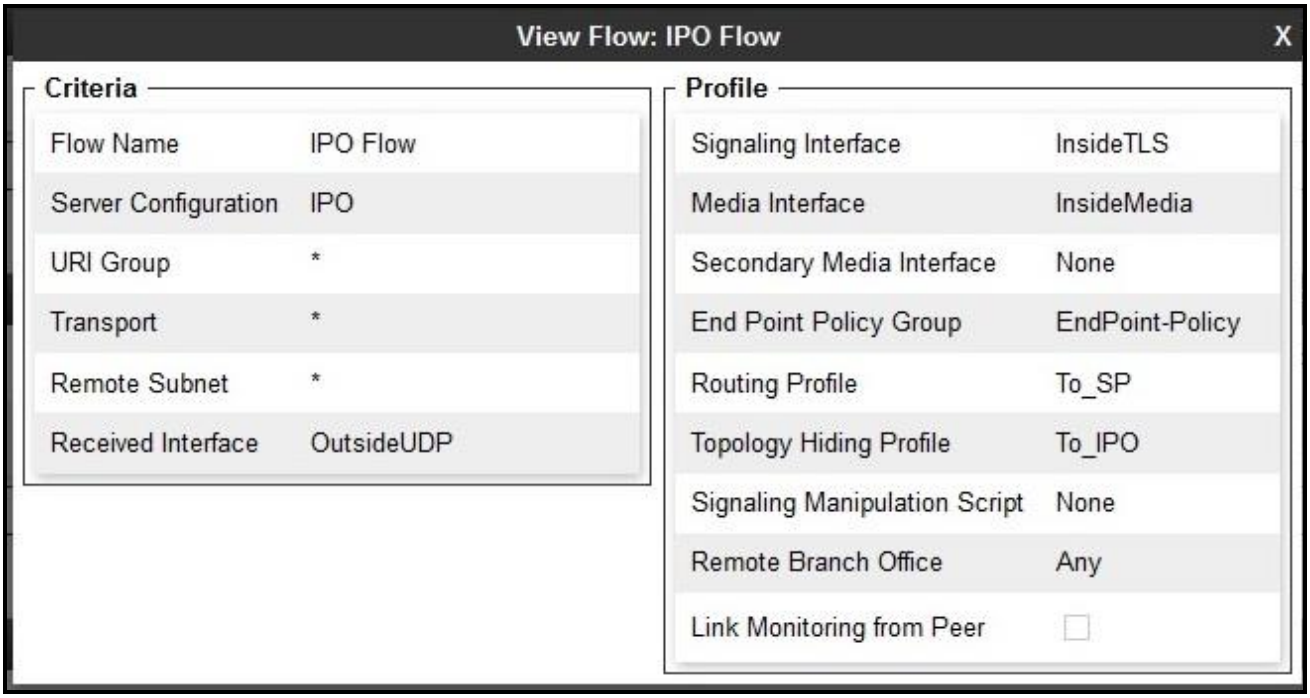


Figure 80 - Trunking Server Flow – IPO Flow

©2021 Avaya Inc. All Rights Reserved.

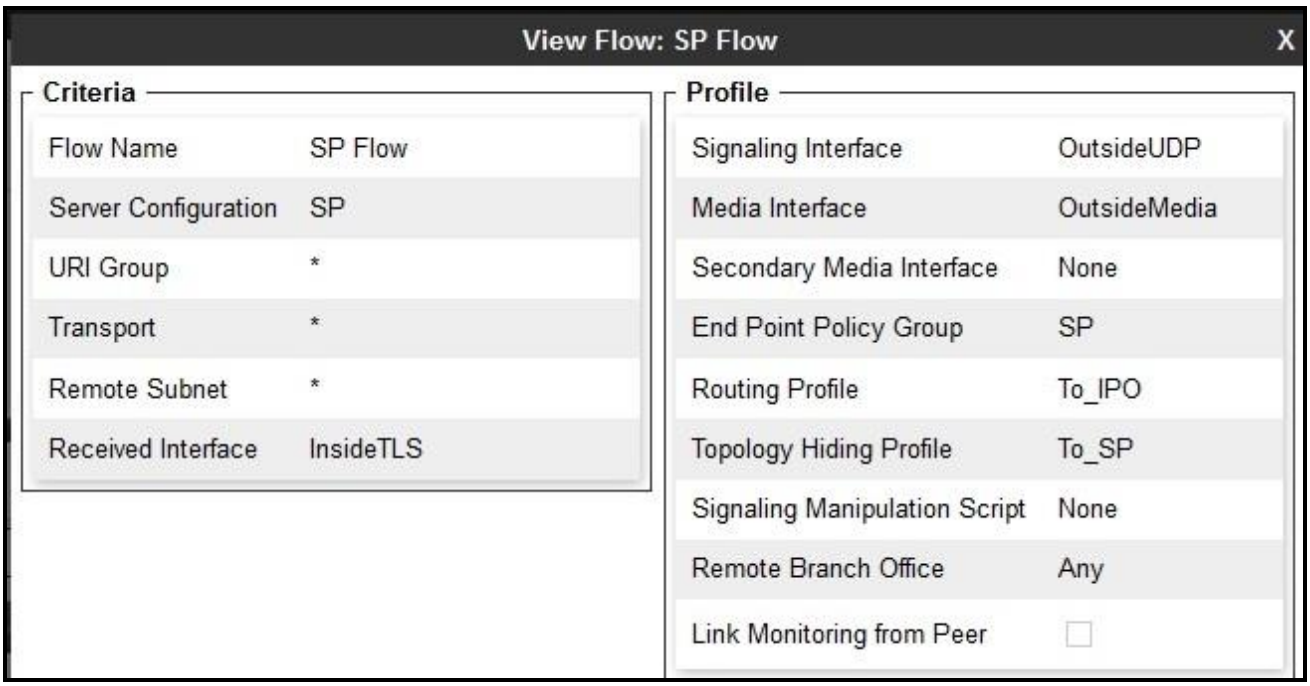


Figure 81 - Trunking Server Flow – SP Flow

©2021 Avaya Inc. All Rights Reserved.

11.8. Remote Worker Endpoint Configuration on Avaya IP Office

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

11.8.1. 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 Workplace for Windows.

The Remote Worker user provisioned is shown below. Note that since the Remote Worker endpoint used in the reference configuration is Avaya Workplace for Windows softphone, the **Enable Softphone** option is 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.

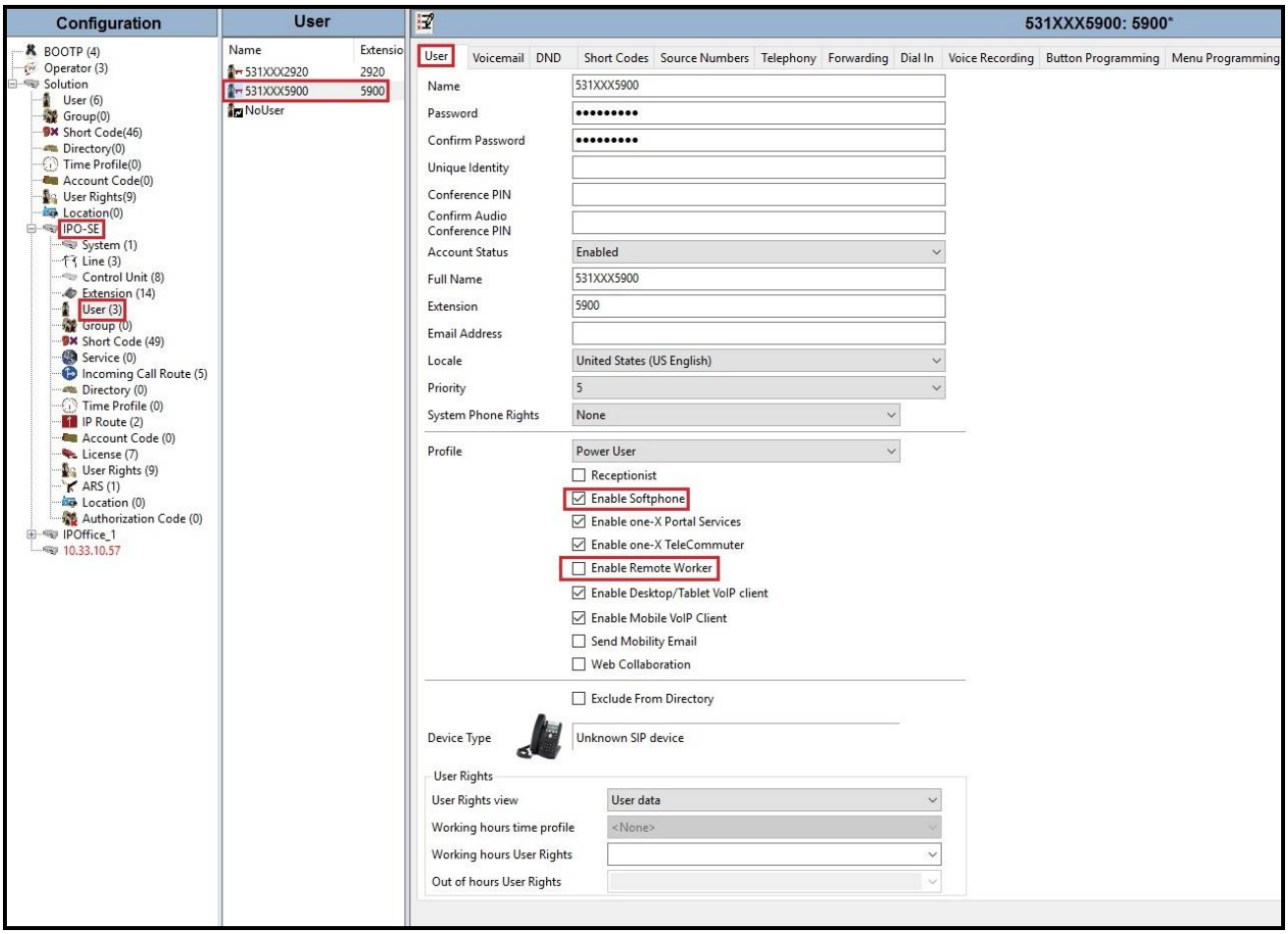


Figure 82 – Remote Worker User Configuration 1

©2021 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 5.9**).

Figure 83 – Remote Worker User Configuration 2

11.8.2. Incoming Call Route

Follow the same procedures described in **Section 5.10** for defining an Incoming Call Route to the Remote Worker.

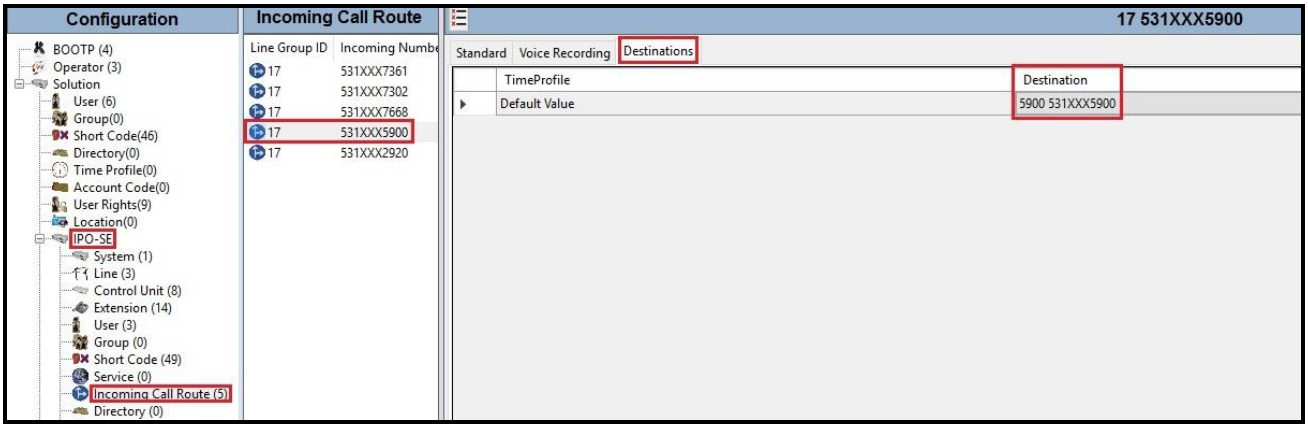


Figure 84 – Remote Worker Incoming Call Route

©2021 Avaya Inc. All Rights Reserved.

11.9. Remote Worker - Avaya Workplace for Windows Settings

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

After opening the Avaya Workplace for Windows application, select the **Options and Settings** icon

Select **Accounts** from the menu, and enter the following:

- In **Phone Service**, enter **Extension** and **Password**
- Click **DONE** the save the changes.

Select **Services → Phone Service**, and enter the following:

- **Server Address**: **10.10.80.105** (Avaya SBCE external interface IP address for remote worker)
- **Server Port**: **5061**
- **Domain**: **10.33.10.56** (Avaya IP Office SE LAN1 IP address)
- Enable **Use TLS**
- **Adhoc Conference Address**: **ConfServer@avaya.com**
- Click **DONE** the save the changes mailto:

©2021 Avaya Inc. All Rights Reserved.

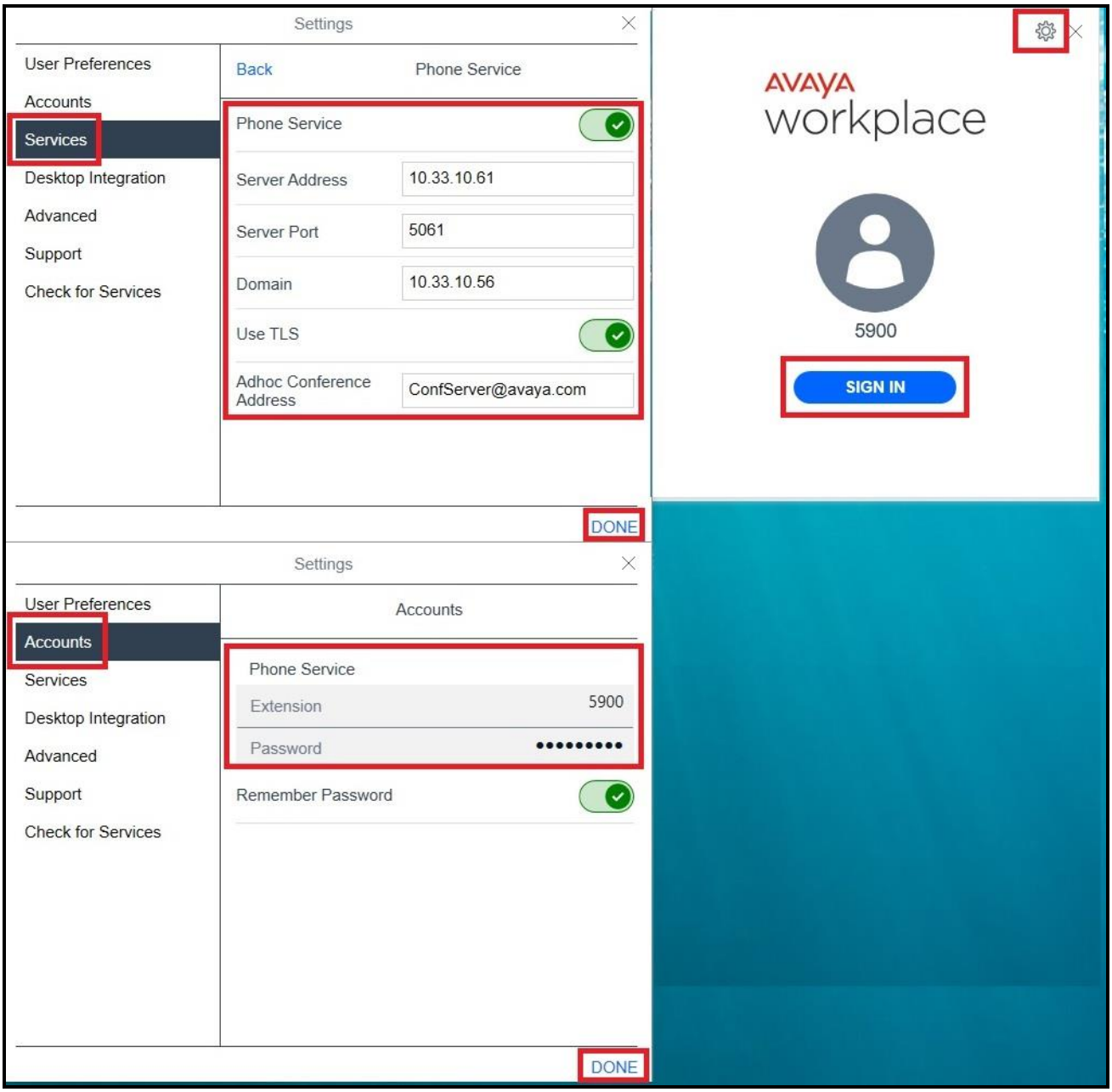


Figure 85 – Remote Worker - Avaya Workplace for Windows Settings

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

©2021 Avaya Inc. All Rights Reserved.

12. Appendix B - Cox managed CPE Configuration

The Cox managed CPE is configured to manage all SIP signaling and provides voice quality management. All data traffic also traverses the Cox managed CPE. It is part of the Cox Communications SIP trunk service and Cox Communications will provide it to the customer when the customer orders the Cox Communications SIP trunk service. Cox Communications manages it and the end-customer does not manage.

Note: Cox managed CPE is part of Cox Communications SIP trunk service offering and it is Cox Communications' responsibility for all the aspect of the Cox managed CPE (i.e. support, detail configuration, maintenance and etc). The Cox managed CPE's sample configuration included in this document is used during this compliance testing.

©2021 Avaya Inc. All Rights Reserved.

12.1. Cox managed CPE Login

The Cox managed CPE was configured with a local LAN address of 10.33.10.60 and a subnet mask of 255.255.255.0. A personal computer is configured with Ethernet IP address assigned to any address other than 10.33.10.60 in the same subnet mask, for example 10.33.10.62
Launch a web browser on personal computer and enter the following URL: http://10.33.10.60 and hit enter.

The following login window should appear:

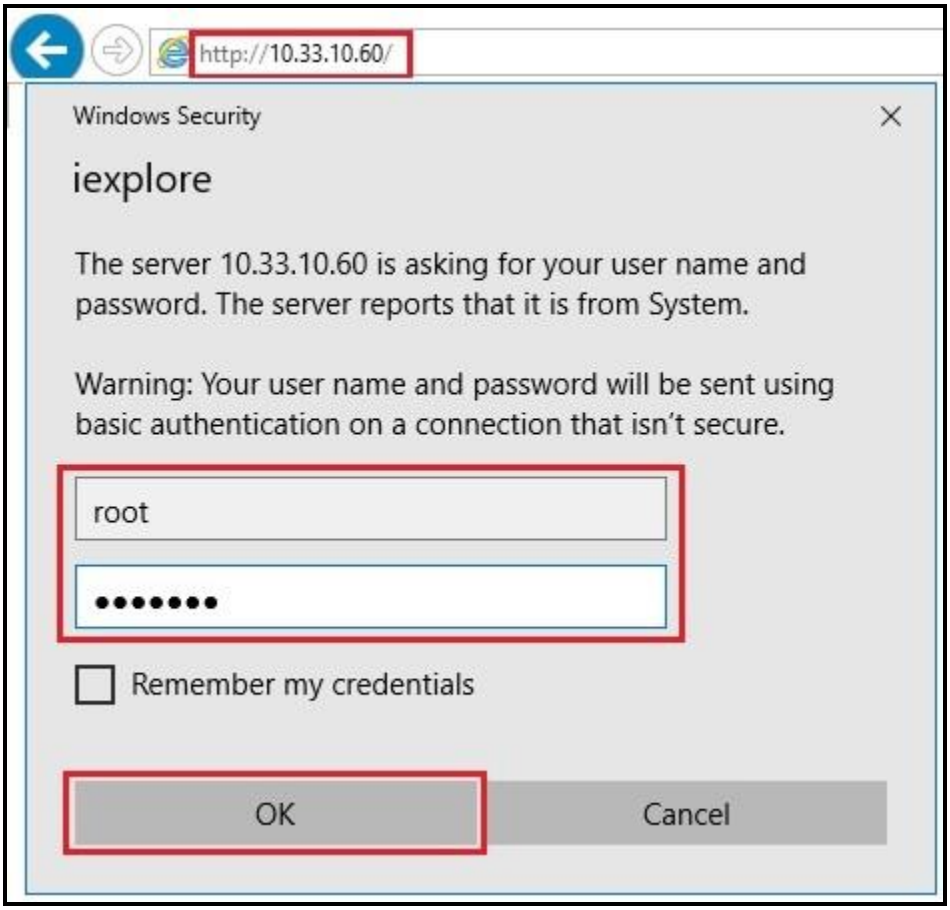


Figure 86 – Cox managed CPE Login

- Enter **user name** and **password** field
- Click **OK** and the system page should be appeared next

©2021 Avaya Inc. All Rights Reserved.

12.2. Network Configuration

From the Configuration Menu, select Network menu option.
Under Network, input the public and private networks as followings:

- LAN Interface Settings:
  - **IP Address**: **10.33.10.60**
  - **Subnet Mask**: **255.255.255.0**
  - Check **Enable VLAN Support**
  - **Default VLAN ID**: **1**
- WAN Interface IPv4 Settings:
  - Check **Static IP**
  - **IP Address**: **192.168.80.103** (Provide this IP address to service provider to set up the connectivity)
  - **Subnet Mask**: **255.255.255.128**
- Network Settings:
  - **Default Gateway**: **192.168.80.1**

Submit the changes.

©2021 Avaya Inc. All Rights Reserved.

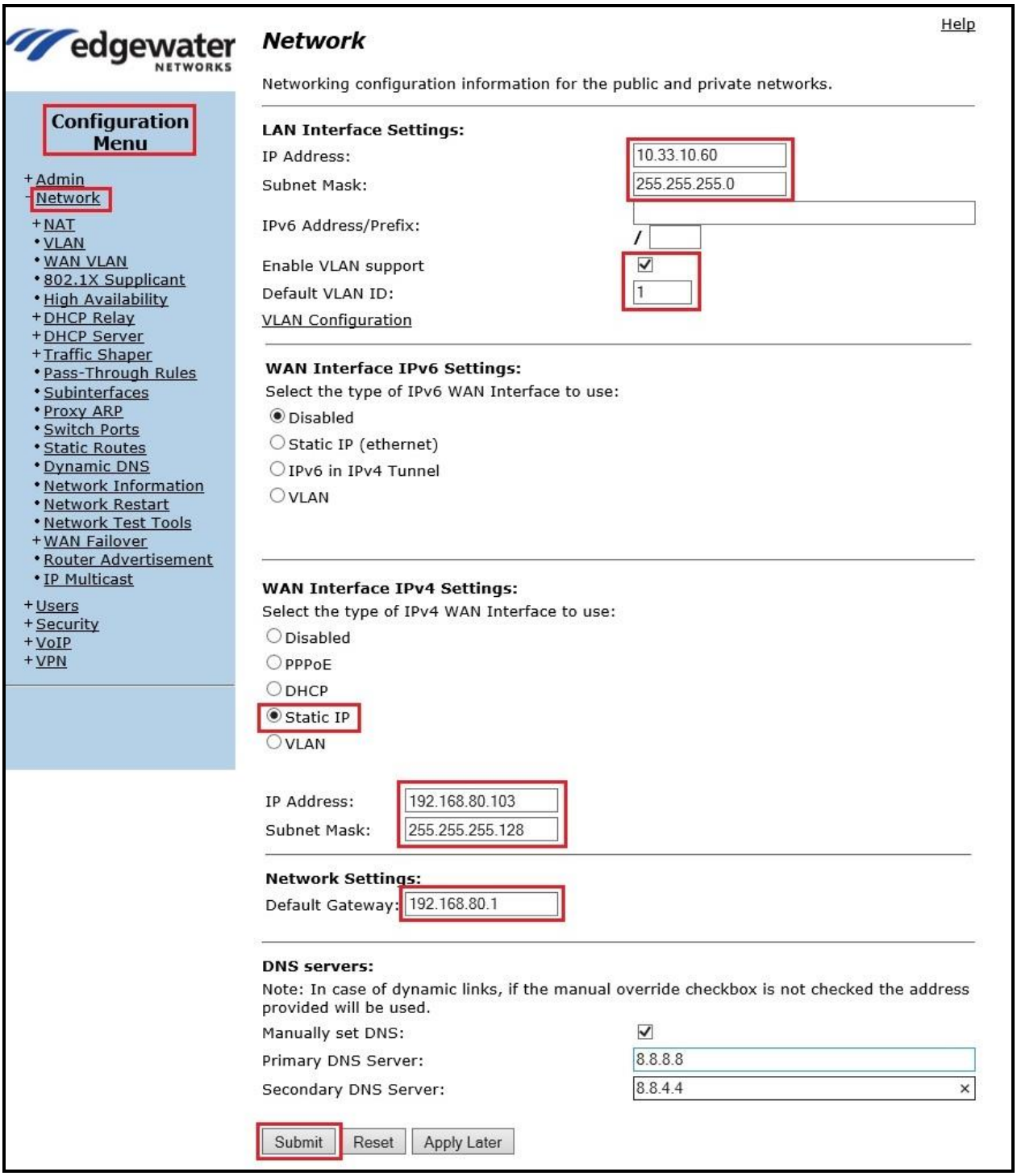


Figure 87 – Cox managed CPE Network Configuration

©2021 Avaya Inc. All Rights Reserved.

12.3. VLAN Configuration

There is a VLAN which has been created and configured as shown in capture below. Details how to create the VLAN is not shown.

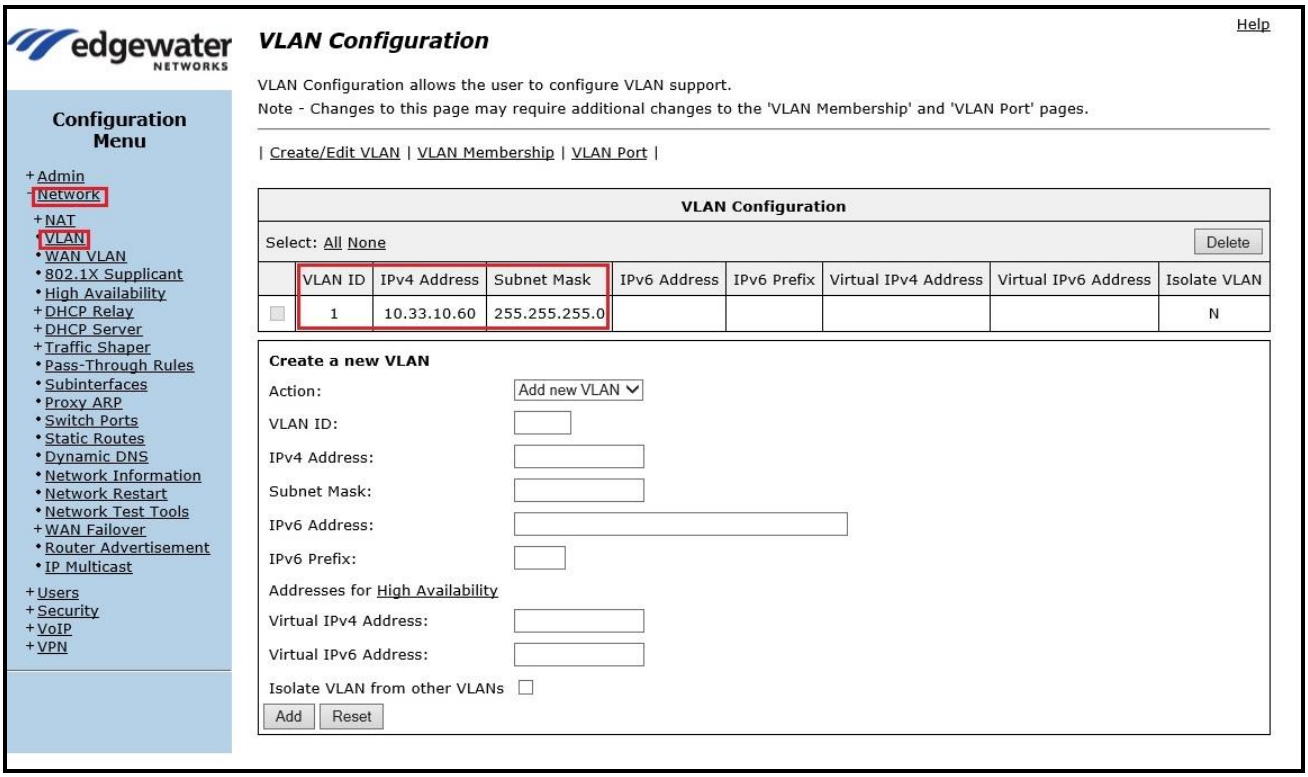


Figure 88 – Cox managed CPE VLAN Configuration

©2021 Avaya Inc. All Rights Reserved.

12.4. VoIP Settings

From the **Configuration Menu**, select **VoIP** menu option → **SIP** option.
Under **SIP Settings**, input the parameters as followings:

- **SIP Server Address**: **DUKEBWSSCM-MTC1-SA-XXXX.TC.AT.COX.NET** (Cox Communications provided this information)
- **SIP Server Port**: **5060**
- **SIP Server Transport**: **Pass Through**
- Check **Use Custom Domain**
- **SIP Server Domain**: **coxbusiness.com**

Submit the changes.

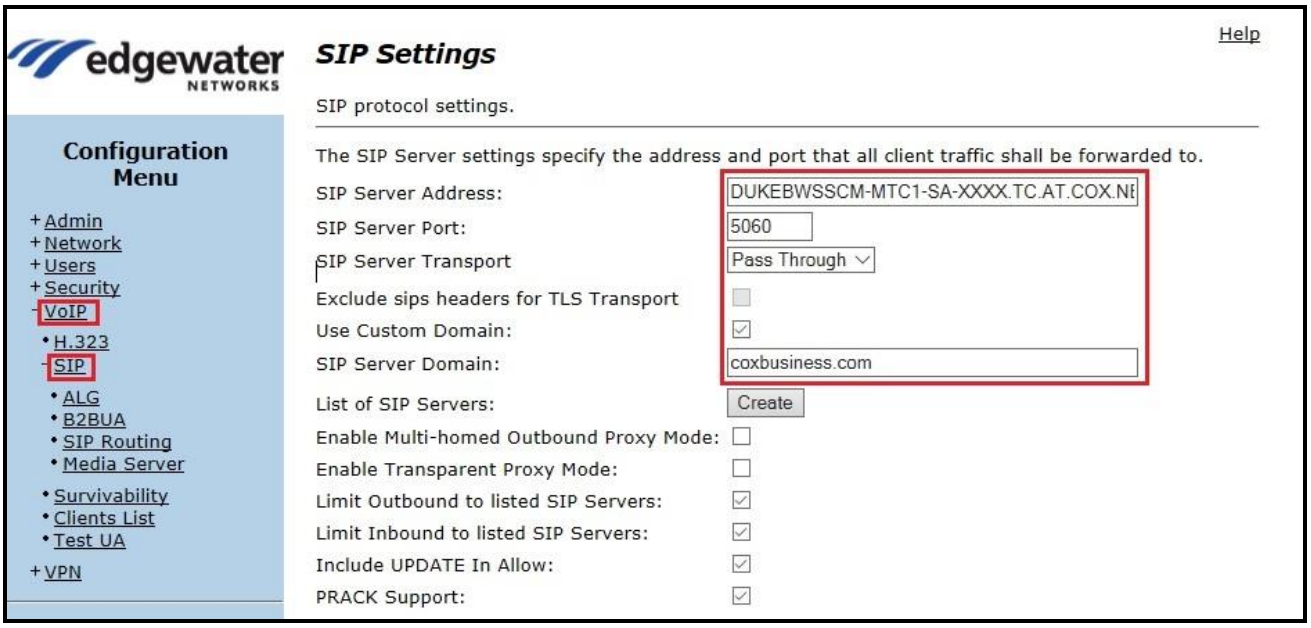


Figure 89 – Cox managed CPE SIP Settings

©2021 Avaya Inc. All Rights Reserved.

From the **Configuration Menu**, select **Survivability** to check **SIP Server Reachability** status. When the SIP Server connectivity to Cox Communications is up, the status is **Active**.

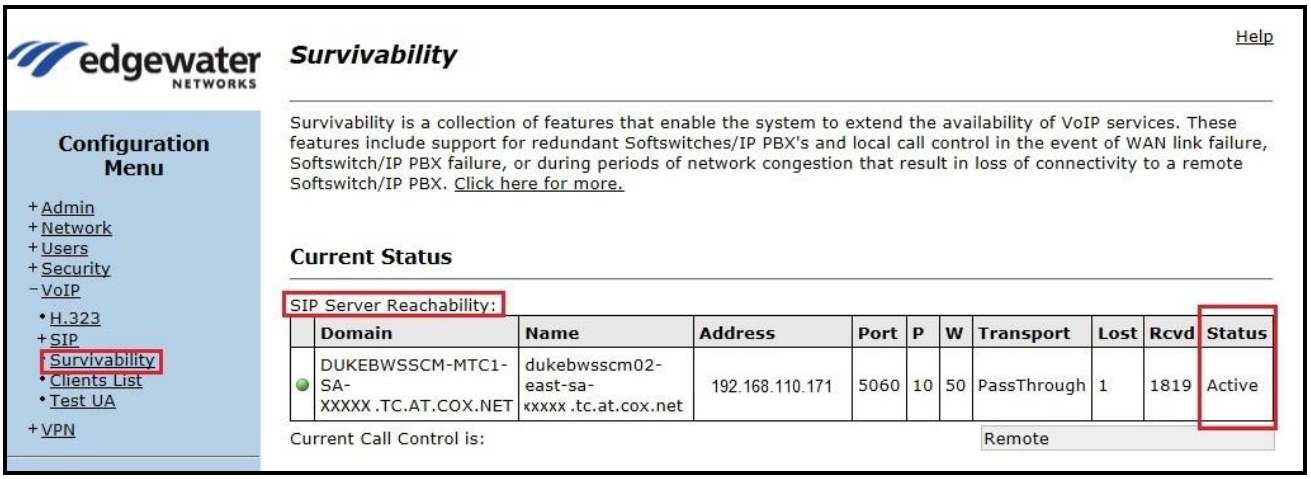


Figure 90 – Cox managed CPE SIP Server Survivability

©2021 Avaya Inc. All Rights Reserved.

12.5. ALG Trunking Configuration

From the **Configuration Menu**, select **VoIP → SIP → ALG** option.
Under **SIP Trunking Devices**, add a trunking device as followings:

- **Action**: choose **Add new trunking device**
- **Name**: **Avaya**
- **Address**: **10.33.10.59** (Avaya SBCE public interface IP address)
- **Port**: **5060**

Select **Commit** button

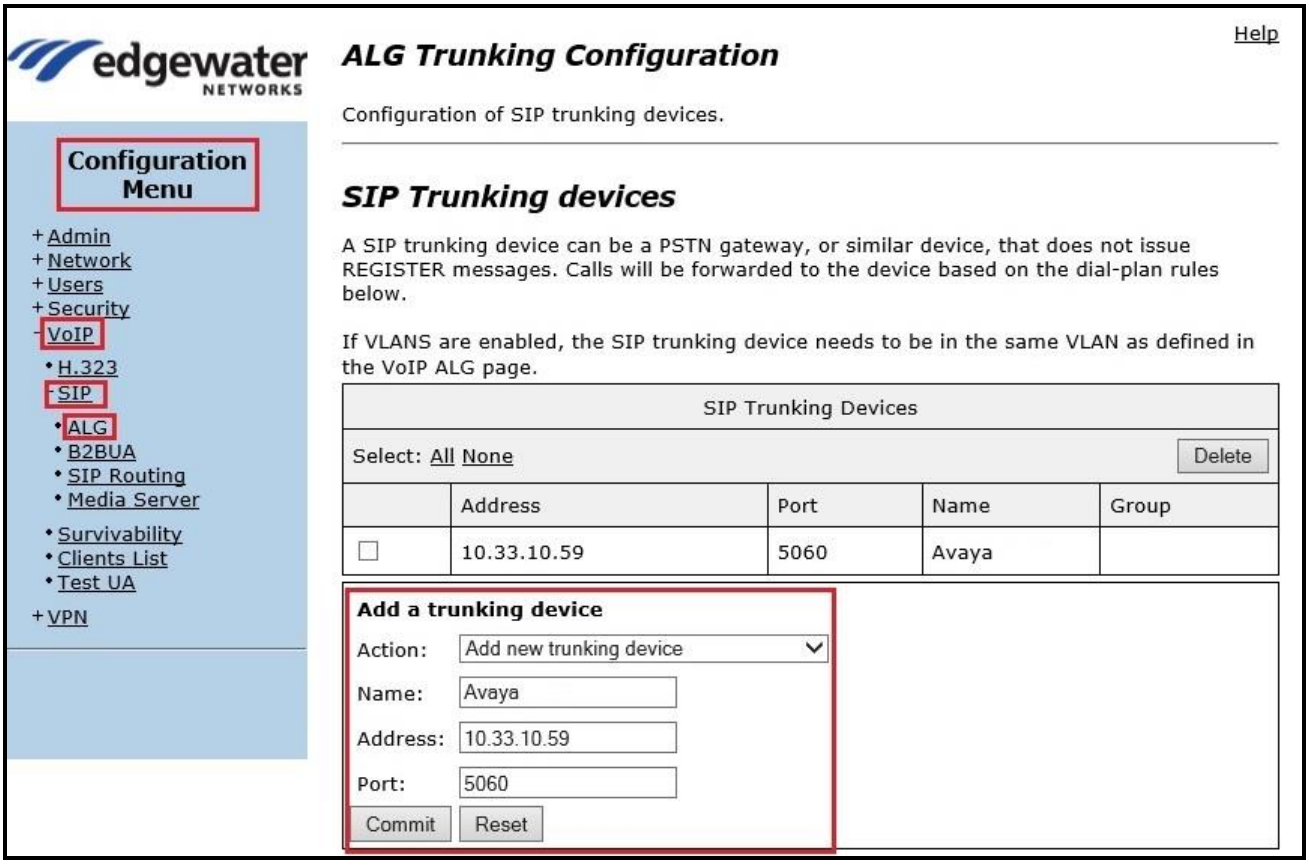
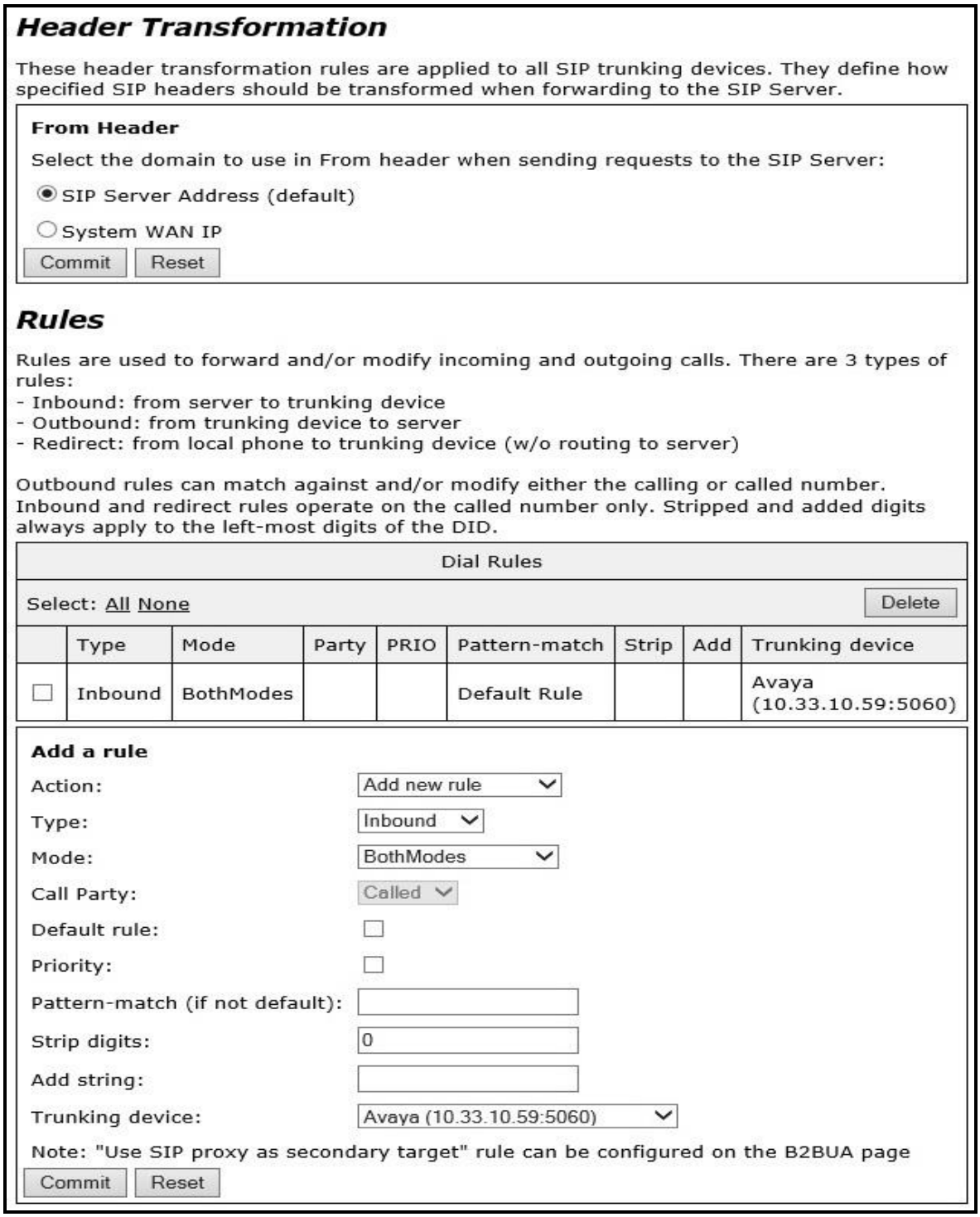


Figure 91 – Cox Managed CPE - SIP ALG Trunk Configuration

©2021 Avaya Inc. All Rights Reserved.

The following captured screens show the rest of the ALG Trunking Configuration page, continue from above screen. Detail configuration is not discussed here.



Header Transformation

These header transformation rules are applied to all SIP trunking devices. They define how specified SIP headers should be transformed when forwarding to the SIP Server.

From Header

Select the domain to use in From header when sending requests to the SIP Server:

- (●) SIP Server Address (default)
- ( ) System WAN IP

Commit | Reset

Rules

Rules are used to forward and/or modify incoming and outgoing calls. There are 3 types of rules:
- Inbound: from server to trunking device
- Outbound: from trunking device to server
- Redirect: from local phone to trunking device (w/o routing to server)

Outbound rules can match against and/or modify either the calling or called number. Inbound and redirect rules operate on the called number only. Stripped and added digits always apply to the left-most digits of the DID.

Dial Rules

Select: All None | Delete

	Type	Mode	Party	PRIO	Pattern-match	Strip	Add	Trunking device
☐	Inbound	BothModes			Default Rule			Avaya (10.33.10.59:5060)

Add a rule

Action:	Add new rule
Type:	Inbound
Mode:	BothModes
Call Party:	Called
Default rule:	☐
Priority:	☐
Pattern-match (if not default):	
Strip digits:	0
Add string:	
Trunking device:	Avaya (10.33.10.59:5060)

Note: "Use SIP proxy as secondary target" rule can be configured on the B2BUA page

Commit | Reset

Figure 92 – Cox Managed CPE - Header Transformation and Rules

©2021 Avaya Inc. All Rights Reserved.

12.6. SIP Routing Configuration

From the **Configuration Menu**, select **VoIP → SIP → SIP Routing** option. A new SIP Routing was created as below screenshot.

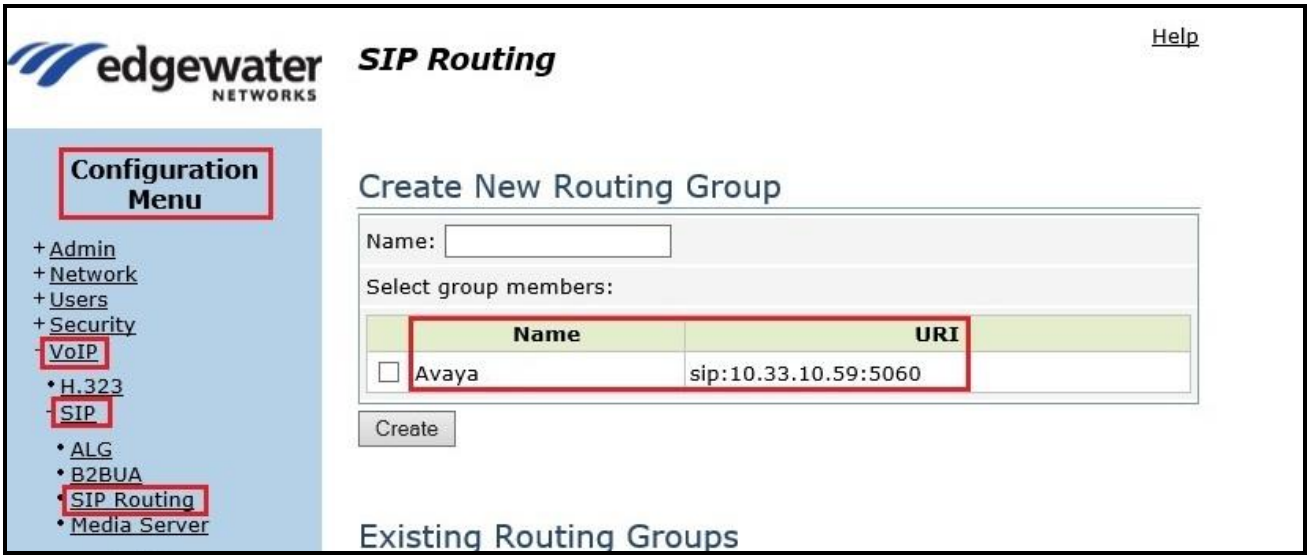


Figure 93 – Cox Managed CPE – SIP Routing Configuration

©2021 Avaya Inc. All Rights Reserved.

©2021 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.