



DevConnect Program

Application Notes for Configuring Cox Communications SIP Trunking with Avaya IP Office 12.0 and Avaya Session Border Controller 10.2 - 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 12.0 and Avaya Session Border Controller Release 10.2.

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 Avaya DevConnect Program.

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	15
5.3.1.	System – LAN1 Tab	15
5.3.2.	System – Telephony Tab	18
5.3.3.	System – VoIP Tab	19
5.4.	IP Route.....	21
5.5.	Administer SIP Line.....	23
5.5.1.	Create SIP Line from an XML Template	24
5.5.2.	Create SIP Line Manually.....	27
5.6.	IP Office Line in Primary System	32
5.7.	IP Office Line in Expansion System	34
5.8.	Outbound Short Code.....	36
5.9.	User	39
5.10.	Incoming Call Route.....	42
5.11.	Save Configuration	45
6.	Configure Avaya Session Border Controller	46
6.1.	Log in to the Avaya SBC	46
6.2.	Server Interworking.....	49
6.2.1.	Configure Server Interworking Profile – Avaya IP Office.....	49
6.2.2.	Configure Server Interworking Profile – Cox Communications	50
6.3.	Configure SIP Server	51
6.3.1.	Configure SIP Server – Avaya Site	51
6.3.2.	Configure SIP Server – Cox Communications	54
Figure 49 – Cox Communications SIP Server – Registration		57
6.4.	Routing.....	57
6.4.1.	Configure Routing – Avaya IP Office	57
6.4.2.	Configure Routing – Cox Communications	59
6.5.	Configure Topology Hiding	60
6.5.1.	Configure Topology Hiding – Avaya Site	60
6.5.2.	Configure Topology Hiding – Cox Communications.....	61
6.6.	Domain Policies	62
6.6.1.	Create Application Rules	62
6.6.2.	Create Media Rules.....	62
6.6.3.	Create Endpoint Policy Groups	63
6.7.	Network & Flows	65

6.7.1.	Manage Network Settings.....	65
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.....	74
8.	Verification Steps.....	75
9.	Conclusion.....	77
10.	Additional References.....	77
11.	Appendix - Cox Managed CPE Configuration.....	78
11.1.	Cox Managed CPE Login.....	79
11.2.	Network Configuration.....	80
11.3.	VLAN Configuration.....	82
11.4.	VoIP Settings.....	83
11.5.	B2BUA Trunking Configuration.....	85
11.6.	Trunking Group Configuration.....	90

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 12.0, Avaya IPO Voicemail Pro, Avaya Workplace for Windows (SIP mode), Avaya H.323, Avaya SIP, digital and analog deskphones. The enterprise solution connects to the Cox Communications network via the Avaya Session Border Controller (Avaya SBC). Cox Managed CPE (Edgewater EdgeMarc 2900E SIP Application-Layer Gateway) is included as part of the Service Provider service and not as part of the CPE solution (See **Section 11 Appendix** for more information).

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 SBC.

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 SBC 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.

2.1. Interoperability Compliance Testing

A simulated enterprise site with Avaya IP Office and Avaya SBC was connected to Cox Communications. 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 long hold time call stability
- Various call types including: local, long distance, international call, inbound toll-free, outbound toll-free, outbound calls to Assisted Operator, 411 Local Directory Assistance call, 911 Emergency call during the compliance testing
- SIP transport UDP/RTP and Port 5060 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 OPTIONS queries and responses
- Voicemail navigation for inbound and outbound calls
- Telephony features such as hold and resume, transfer, and conference
- T.38 fax and G.711 pass-through mode
- Off-net call forwarding
- Off-net call transfer
- Twinning to mobile phones on inbound calls
- SIP Trunk registration between Avaya SBC and Cox Managed CPE
- Remote Worker. Avaya Workplace for Windows (SIP) was used to test remote worker functionality. Note: Remote Worker was tested as part of this solution. The configuration necessary to support remote worker is beyond the scope of these Application Notes and are not included in these Application Notes. For these configuration details, see **Reference [8] in Section 10**.

Item not supported include the following:

- TLS/SRTP SIP transport
- Call redirection to the PSTN using the SIP REFER method was not tested during the compliance test, 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 method for call redirection to the PSTN was used instead.

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 equipment did not forward SIP Diversion headers (or PAI headers) to the Cox Communications network during call forward scenarios to the PSTN. This behaviour had no negative impact on the forwarded calls. It is being mentioned here simply as an observation. This issue should be fixed in a future firmware release for the Cox Communications Managed CPE equipment residing at the enterprise.

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>.

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)
- Avaya Session Border Controller
- 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 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 12.0. Avaya Voicemail Pro runs as a service on the Primary Server. The LAN1 port of Avaya IP Office is connected to Avaya SBC internal interface. The Avaya SBC external interface is connected to Cox Managed CPE LAN interface while Cox Managed CPE WAN interface 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.

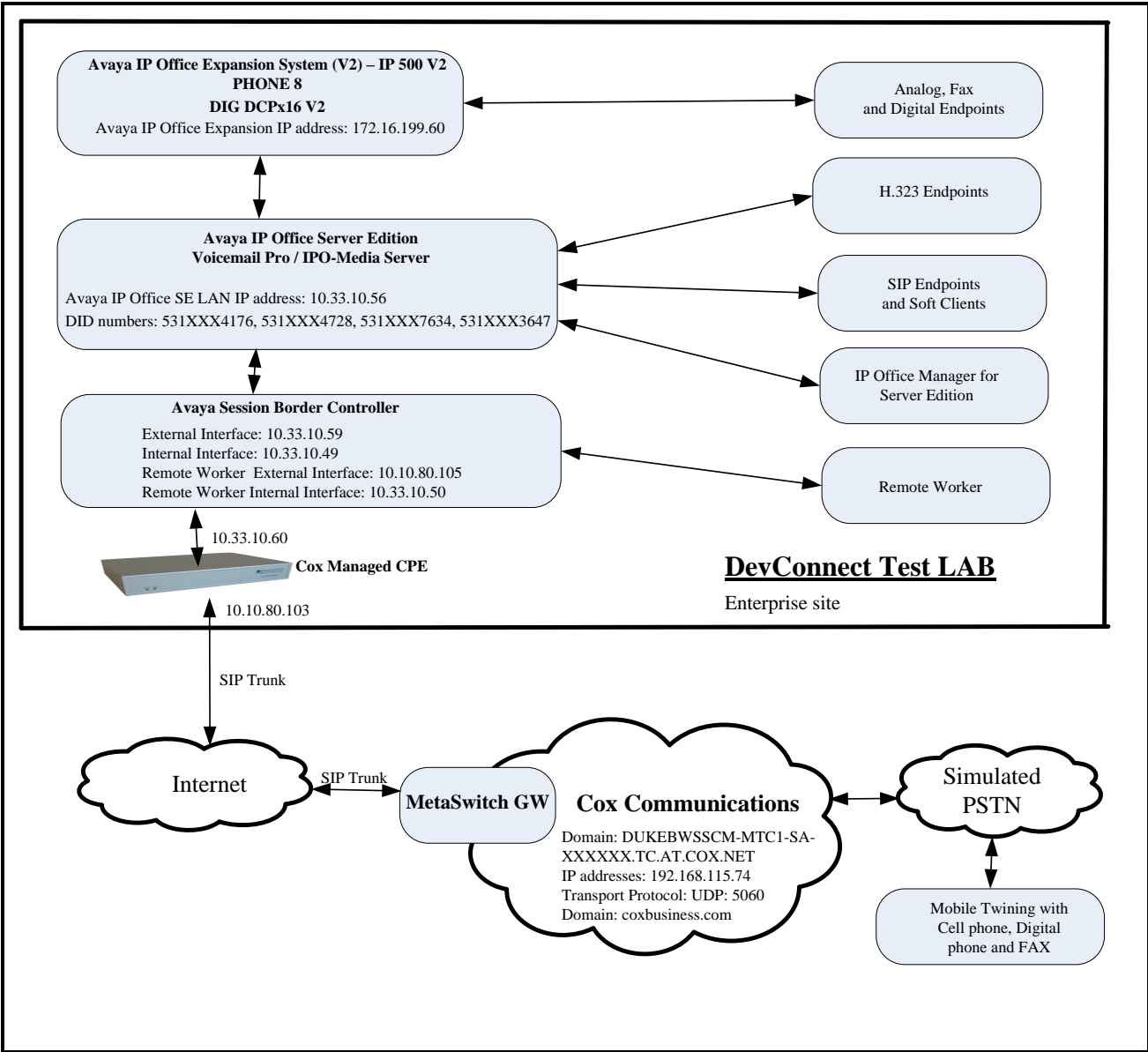


Figure 1 - Test Configuration for Avaya IP Office with Cox Communications SIP Trunk Service

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 the compliance test, outbound calls to Canadian numbers within the North American Numbering Plan (NANP) were tested. The user would dial 11 (1 + 10) digits. For these NANP calls, Avaya IP Office would send 11 digits in the Request URI and the To field of an outbound SIP INVITE message, and 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 SBC, 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 SRTP traffic between the service provider and Avaya SBC must be allowed to pass through these devices.

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 <ul style="list-style-type: none"> ▪ Primary Server Dell PowerEdge R640 – IPO-Linux-PC ▪ IPO-Media Server ▪ Voicemail Pro ▪ 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 	12.0.0.0 build 56 12.0.0.0 build 56 12.0.0.0 build 26 12.0.0.0 build 56 12.0.0.0 build 56 12.0.0.0 build 56 12.0.0.0 build 56
Avaya Session Border Controller running on VMware®-based Avaya appliance	10.2.0.0-86-24077
Avaya 1140E IP Deskphone (SIP)	04.04.33
Avaya 9641G IP Deskphone (H323)	6.8.5.5.1
Avaya 9621G IP Deskphone (H323)	6.8.5.5.1
Avaya J129 IP Deskphone (SIP)	4.0.7.1.5
Avaya Workplace Client for Windows	3.37.0.156.28
Avaya 1408D Digital Deskphone	R48
Avaya Analog Deskphone	N/A
VentaFax	7.10.258.664
Cox Communications	
Cox Managed CPE	16.4.0.1
MetaSwitch GW	4.3.40

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 via Avaya SBC. 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 SBC. 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.

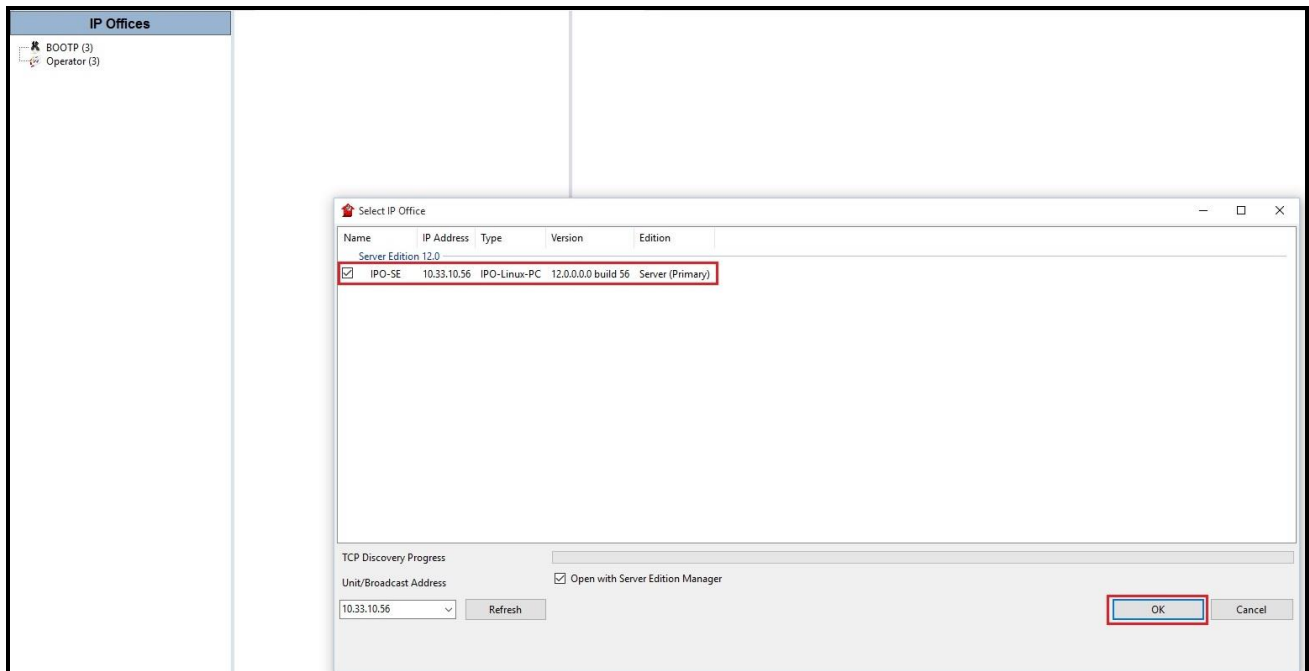


Figure 2 – Avaya IP Office Server Edition Selection

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.

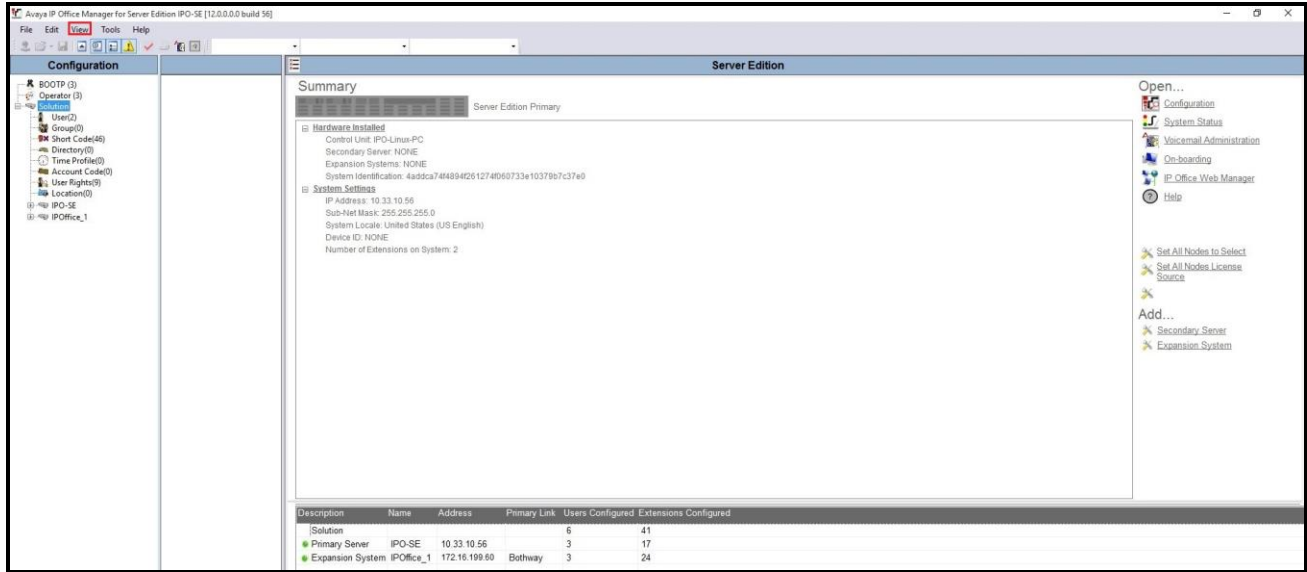


Figure 3 – Avaya IP Office Server Edition View Menu

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.

Feature	Instances	Status	Expiration Date	Source
Receptionist	4	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	1	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	4	Obsolete	Never	PLDS Nodal
VMPro TTS (Generic)	40	Obsolete	Never	PLDS Nodal
Teleworker	384	Obsolete	Never	PLDS Nodal
Mobile Worker	384	Obsolete	Never	PLDS Nodal
Office Worker	384	Valid	Never	PLDS Nodal
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	40	Obsolete	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	1	Obsolete	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal
SIP Trunk Channels	128	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal

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 SBC 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.

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

To verify the trusted certificate, locate the **Trusted Certificate Store** section, select the trusted certificate and click **View** to see the details of it.

The screenshot displays the 'Security Settings' window for 'System (1) IPO-SE'. The 'Certificates' tab is active. The 'Identity Certificate' section includes options for 'Offer Certificate' (checked), 'Offer ID Certificate Chain' (checked with a warning icon), 'Issued To' (ipo), 'Automatic Certificate Management' (unchecked), and 'Automatic Phone Provisioning' (checked). A 'View' button is highlighted. Below this, there are settings for 'Certificate Expiration Warning (days)' (60), 'Use Different Identity Certificate For SIP Telephony' (None), 'Received Certificate Checks (Management Interfaces)' (None), 'Received Certificate Checks (Telephony Endpoints)' (None), 'H.323 Security Level' (Medium), and 'SIP Security Level' (Medium). The 'Trusted Certificate Store' section shows a list of installed certificates, with 'System Manager CA' selected and its 'View' button highlighted. The 'SCEP Settings' section at the bottom includes an 'Active' checkbox, 'Request Interval (sec)' (120), 'SCEP Server IP Address/Name', 'SCEP Server Port' (443), 'SCEP URI' (/ejbca/publicweb/apply/scep/pkclient.exe), and 'SCEP Password'.

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 SBC 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 SBC connects to 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.



Figure 6 - Avaya IP Office Primary Server LAN1 Settings

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 SBC
- Check the **SIP Registrar Enable** to allow Avaya IP deskphones/softphones to register using the SIP protocol
- Input **SIP Domain Name** and **SIP Registrar 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

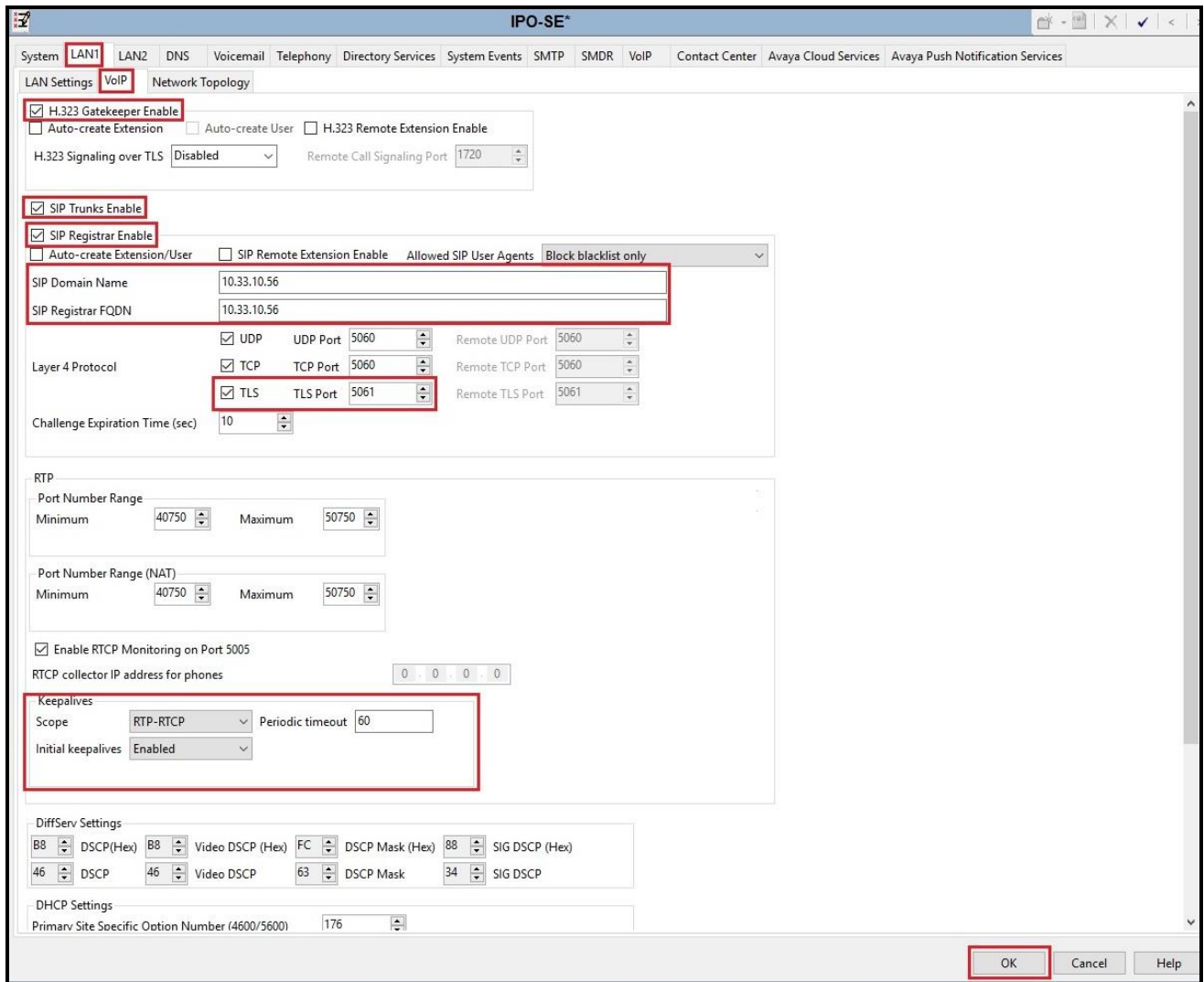


Figure 7 - Avaya IP Office Primary Server LAN1 VoIP

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.

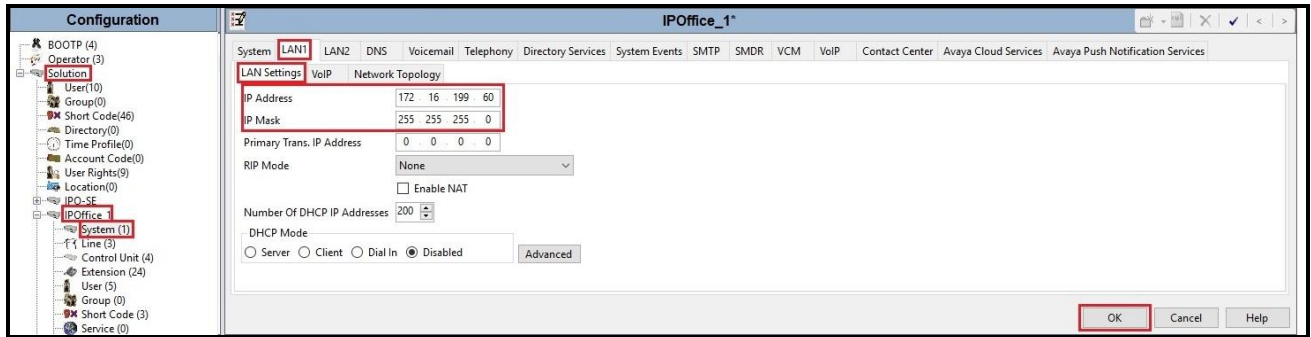


Figure 8 - Avaya IP Office Expansion Server LAN Settings

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. **U-Law** is used for Switch and Line. 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.

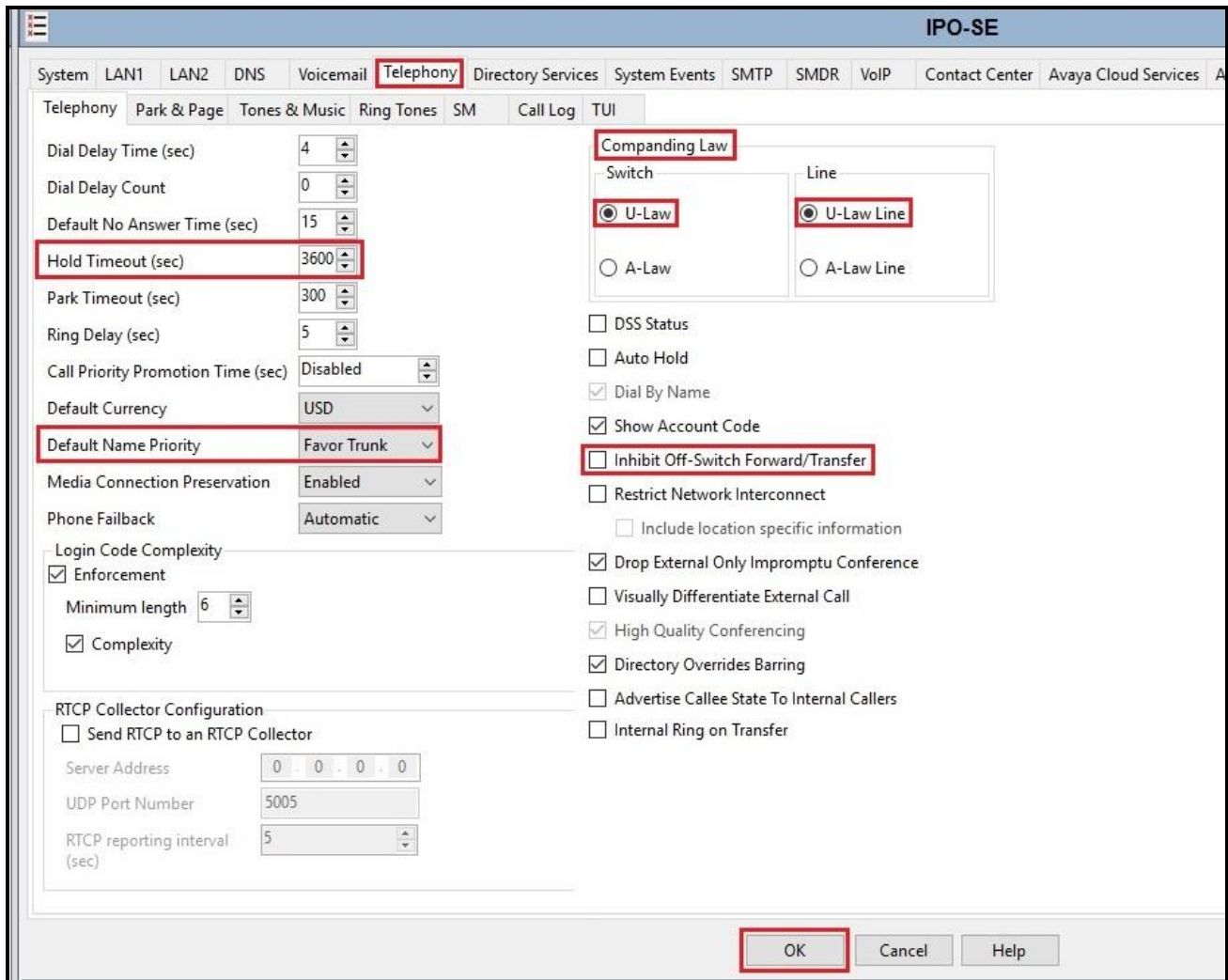


Figure 9 - Avaya IP Office Primary Server Telephony

Navigate to **Solution → IPOOffice_1 → System (1)** (not shown) and repeat the steps above to configure the **Telephony** settings for the Expansion System.

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.

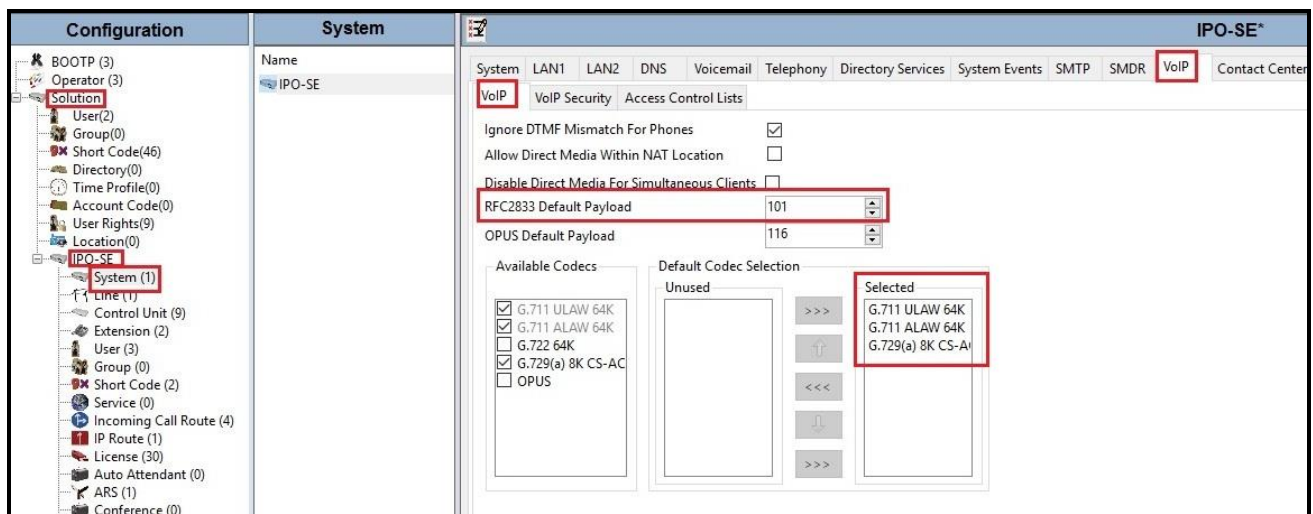


Figure 10 - Avaya IP Office Primary Server VoIP

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.

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 Security** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption.

- Verify **Strict SIPS** is not checked
- Under **Media Security Options**, select **RTP** for the **Encryptions** and **Authentication** fields
- Under **Crypto Suites**, select **SRTP_AES_CM_128_SHA1_80**
- Click **OK** to commit

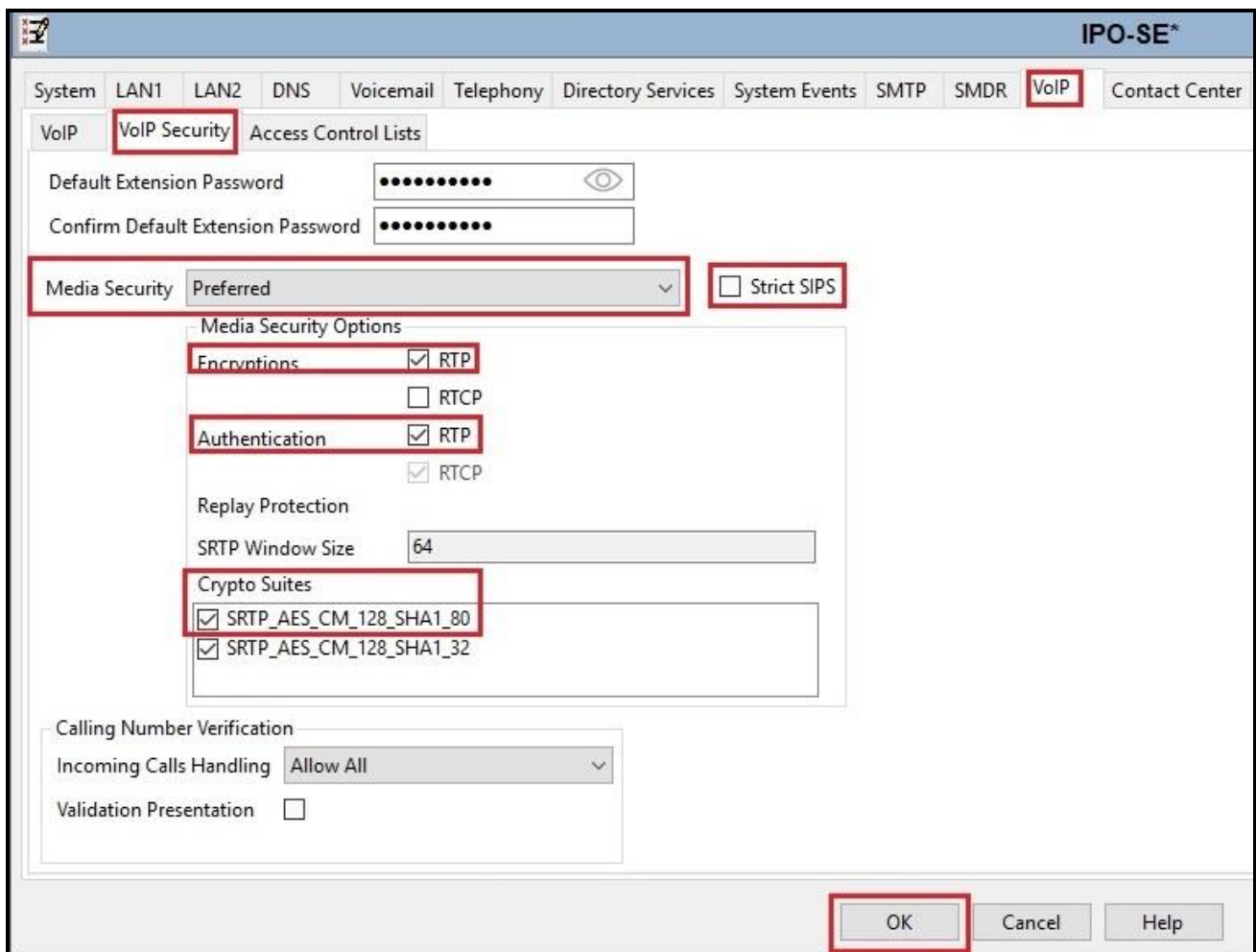


Figure 11 - Avaya IP Office Primary Server VoIP Security

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 SBC's network, e.g., **10.33.10.1**
- Set **Destination** to **LAN1** from the pull-down menu
- Click **OK** to commit

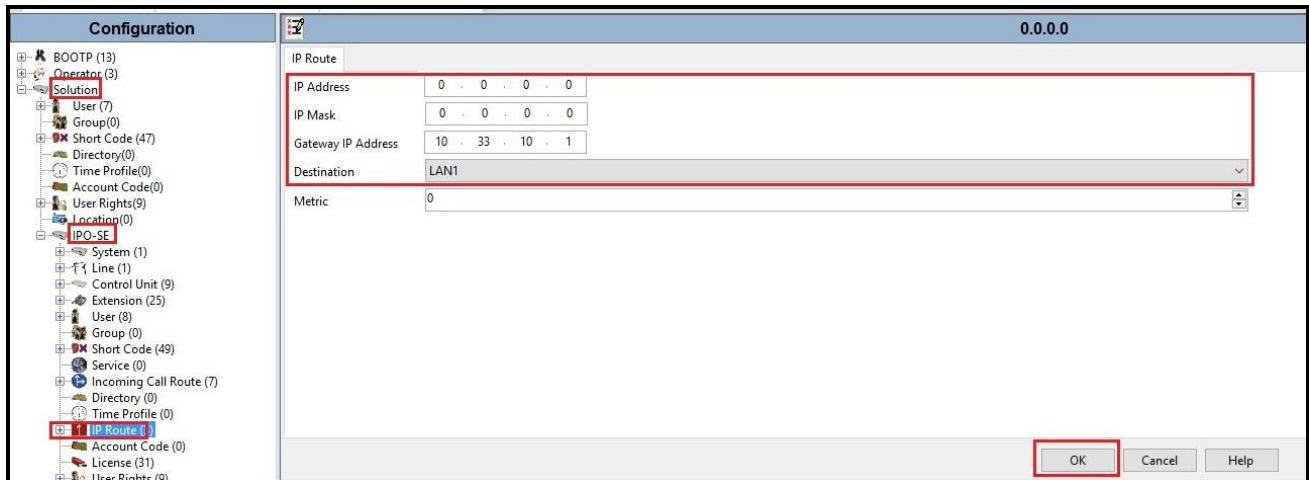


Figure 12 - Avaya IP Office Primary Server IP Route

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 the private network, e.g., **172.16.199.1**
- Set **Destination** to **LAN1** from the pull-down menu
- Click **OK** to commit

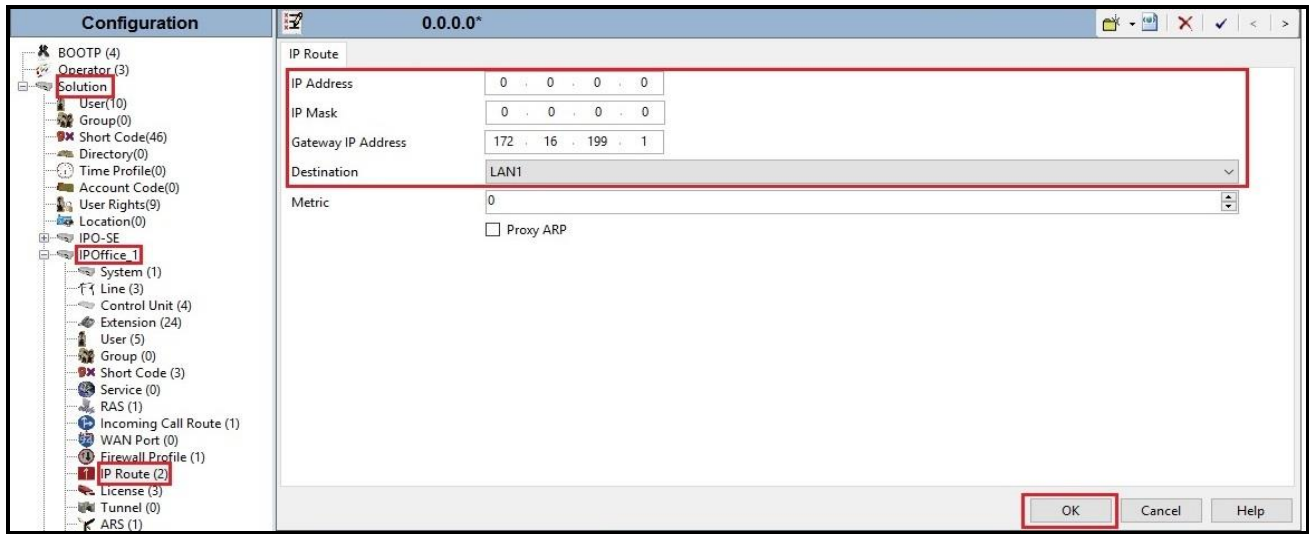


Figure 13 - Avaya IP Office Expansion Server IP Route

5.5. Administer SIP Line

A SIP Line is needed to establish the SIP connection between Avaya IP Office and Cox Communications system via Avaya SBC. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by Avaya IP Office Manager for Server Edition 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.

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 **C_IPO12SBC102.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**.

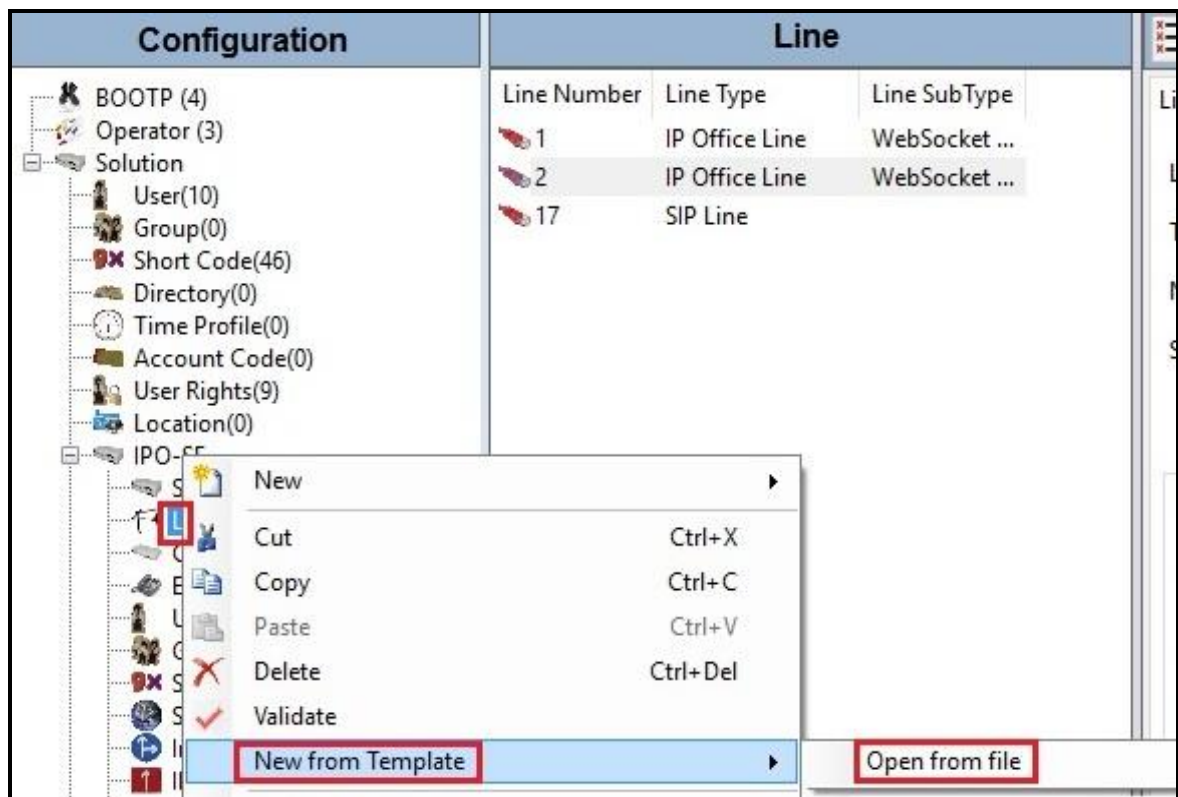


Figure 14 – Create SIP Line from Template

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.

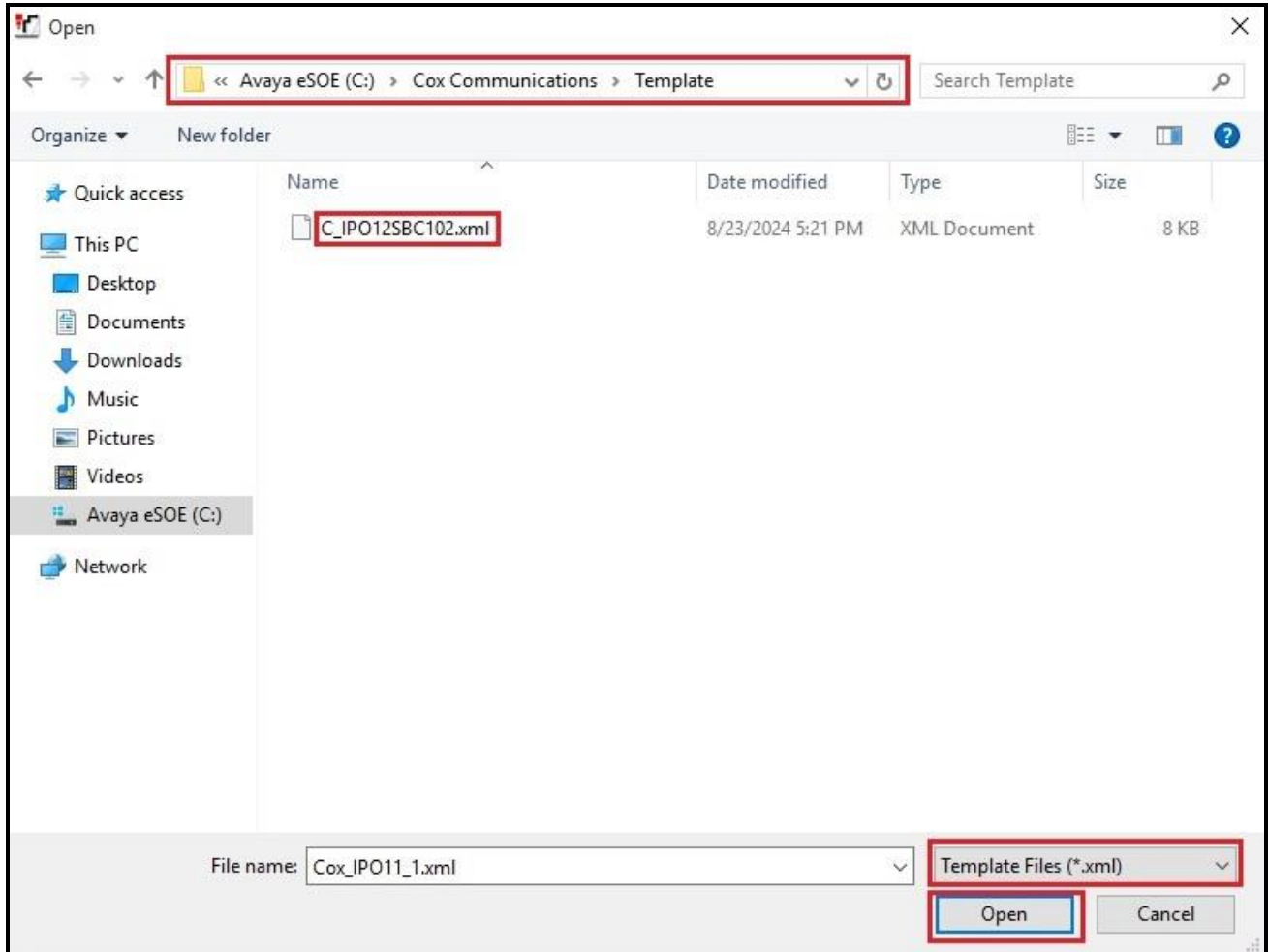


Figure 15 – Create SIP Line from directory

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**.

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 SBC 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** **Never**. Note: Cox Communications did not support SIP Refer during the compliance testing
- Default values may be used for all other parameters
- Click **OK** to commit then press **Ctrl + S** to save

The screenshot displays the 'SIP Line - Line 17' configuration window. The left pane shows a tree view with 'Line (1)' selected. The main configuration area is divided into several sections:

- Line Number:** 17
- ITSP Domain Name:** 10.33.10.49
- Local Domain Name:** 10.33.10.56
- URI Type:** SIP URI
- Location:** Cloud
- Prefix:** (empty)
- National Prefix:** (empty)
- International Prefix:** (empty)
- Country Code:** (empty)
- Name Priority:** Favor Trunk
- Description:** (empty)

Additional settings and checkboxes:

- In Service:**
- Check OOS:**
- Session Timers:**
 - Refresh Method:** Auto
 - Timer (sec):** On Demand
- Redirect and Transfer:**
 - Incoming Supervised REFER:** Never
 - Outgoing Supervised REFER:** Never
 - Send 302 Moved Temporarily:**
 - Outgoing Blind REFER:**

Buttons at the bottom: **OK**, **Cancel**, **Help**.

Figure 17 – SIP Line Configuration

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 SBC 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 Port** 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

The screenshot shows the 'SIP Line - Line 17*' configuration window. The 'Transport' tab is selected. The 'ITSP Proxy Address' field contains '10.33.10.49'. The 'Network Configuration' section includes 'Layer 4 Protocol' set to 'TLS', 'Send Port' set to '5061', and 'Use Network Topology Info' set to 'None'. The 'Listen Port' is also set to '5061'. The 'Calls Route via Registrar' checkbox is unchecked. The 'Separate Registrar' field is empty. The 'OK' button is highlighted with a red box.

Figure 18 – SIP Line Transport Configuration

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** option
- Check **Diversion Header** option
- 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** and **Diversion Header** to **Caller**
- Set all remaining fields as shown on the screenshot below
- Click **OK** to submit the changes

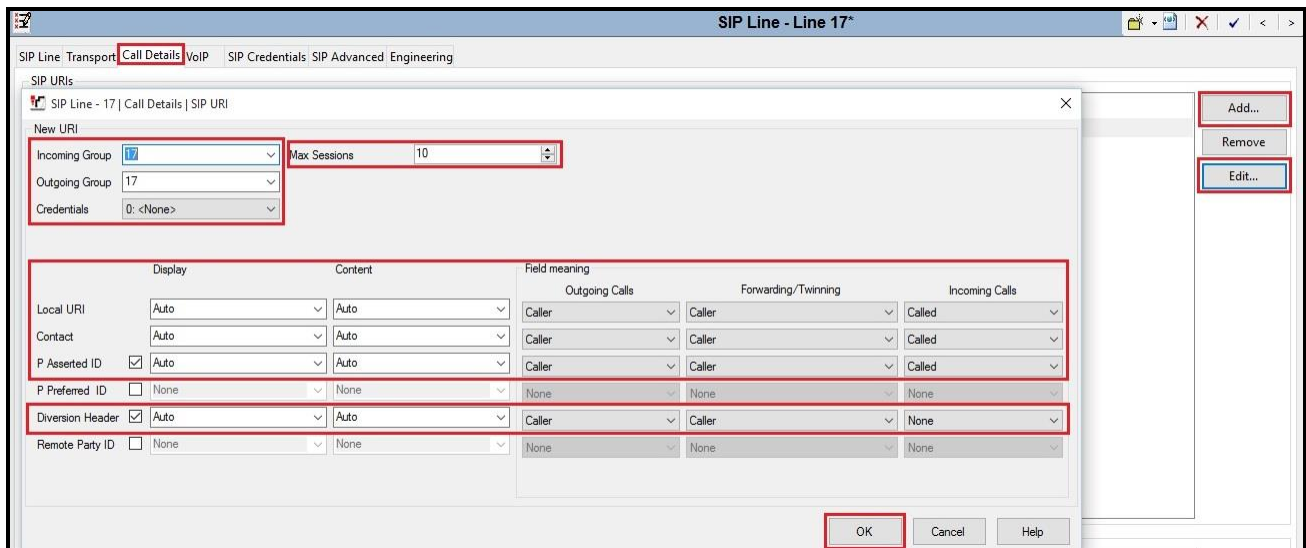


Figure 19 – SIP Line Call Details Configuration

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 **T38 Fallback** from the pull-down menu
- 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

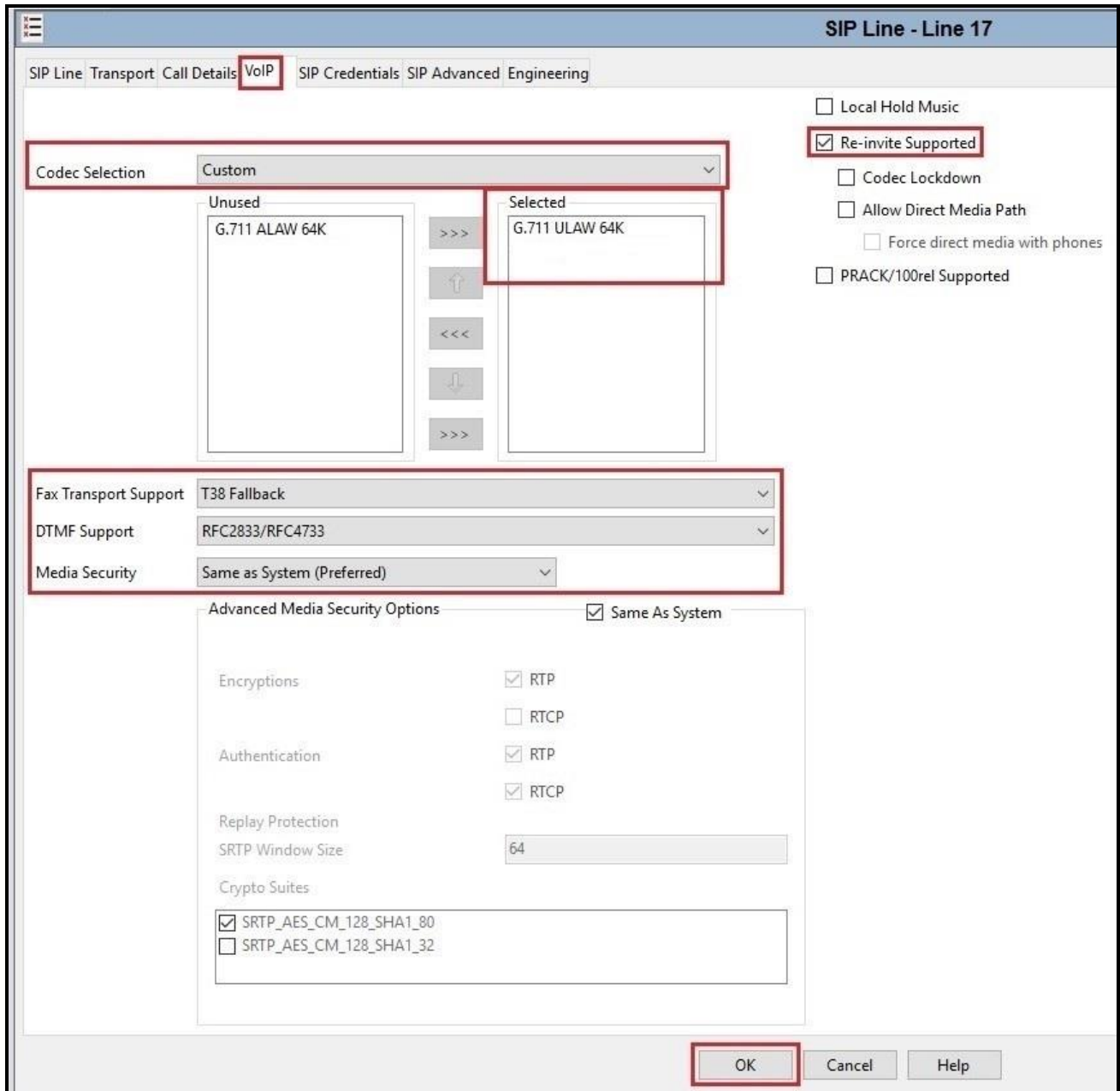


Figure 20 – SIP Line VoIP Configuration

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**.

Line Number	Line Type	Line SubType
1	IP Office Line	WebSocket ...
2	IP Office Line	WebSocket ...
17	SIP Line	

IP Office Line - Line 2

Line Number: 2

Transport Type: WebSocket Server

Networking Level: SCN

Security: Medium

Gateway Address: 172 . 16 . 199 . 60

Outgoing Group ID: 99999

Number of Channels: 250

Outgoing Channels: 250

Location: Cloud

SCN Resiliency Options:

- Supports Resiliency
- Backs up my IP phones
- Backs up my hunt groups
- Backs up my IP DECT phones

Figure 21 – IP Office Line for Primary System

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

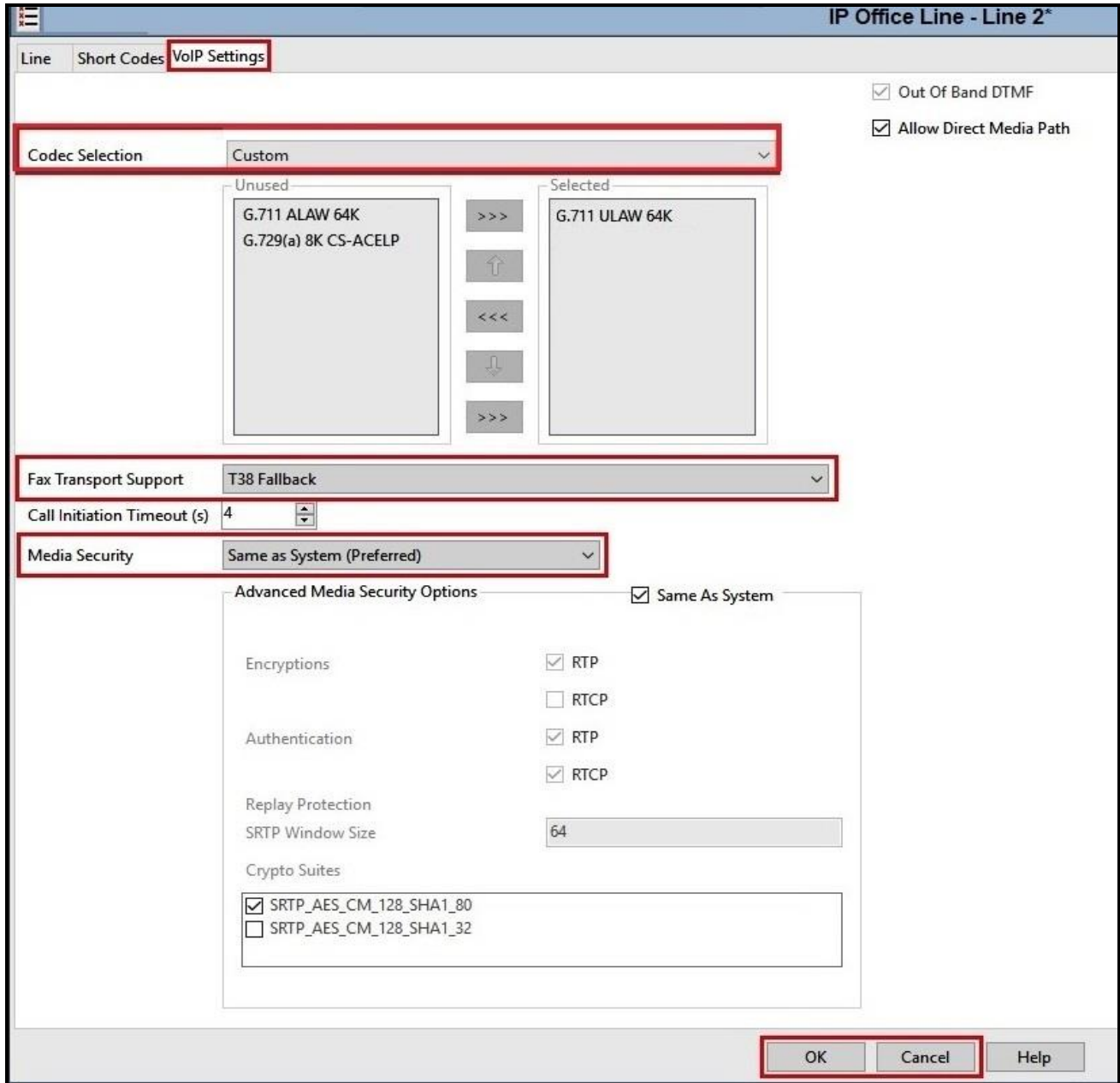


Figure 22 – IP Office Line for Primary System VoIP Settings

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**.

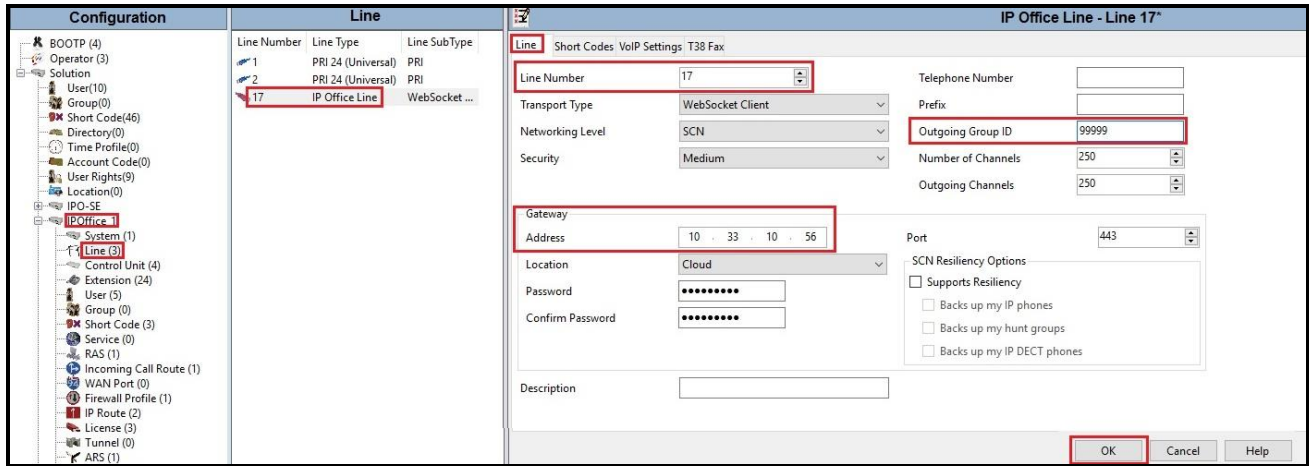


Figure 23 – IP Office Line for Expansion System

To verify the **VoIP Settings** of the IP Office line connecting the Expansion System to the Primary Server, select **VoIP Settings** tab. The selected codec is **G.711 ULAW 64K**. Select **Fax Transport Support** to **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.

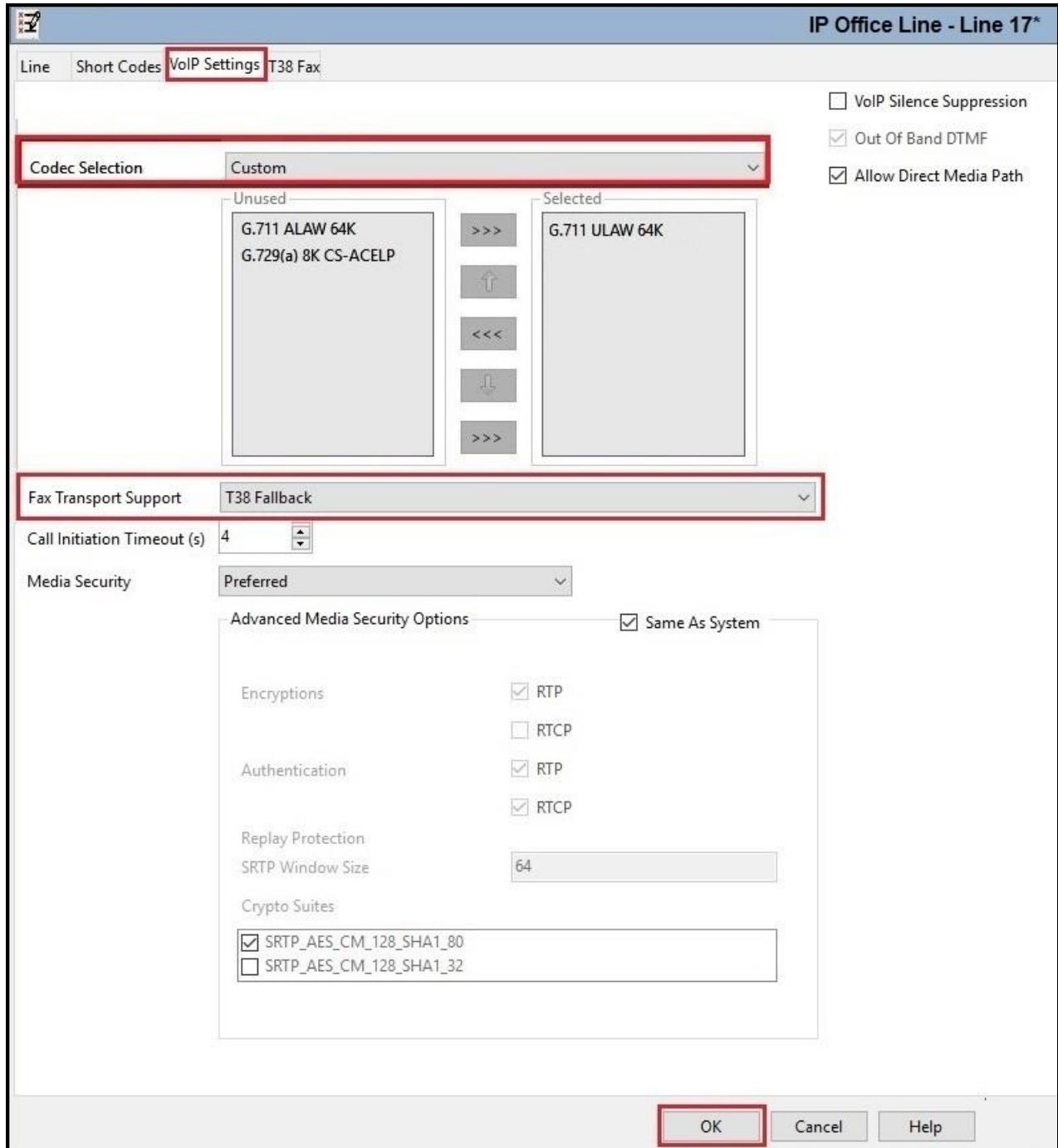


Figure 24 – IP Office Line for Expansion Server VoIP Settings

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.

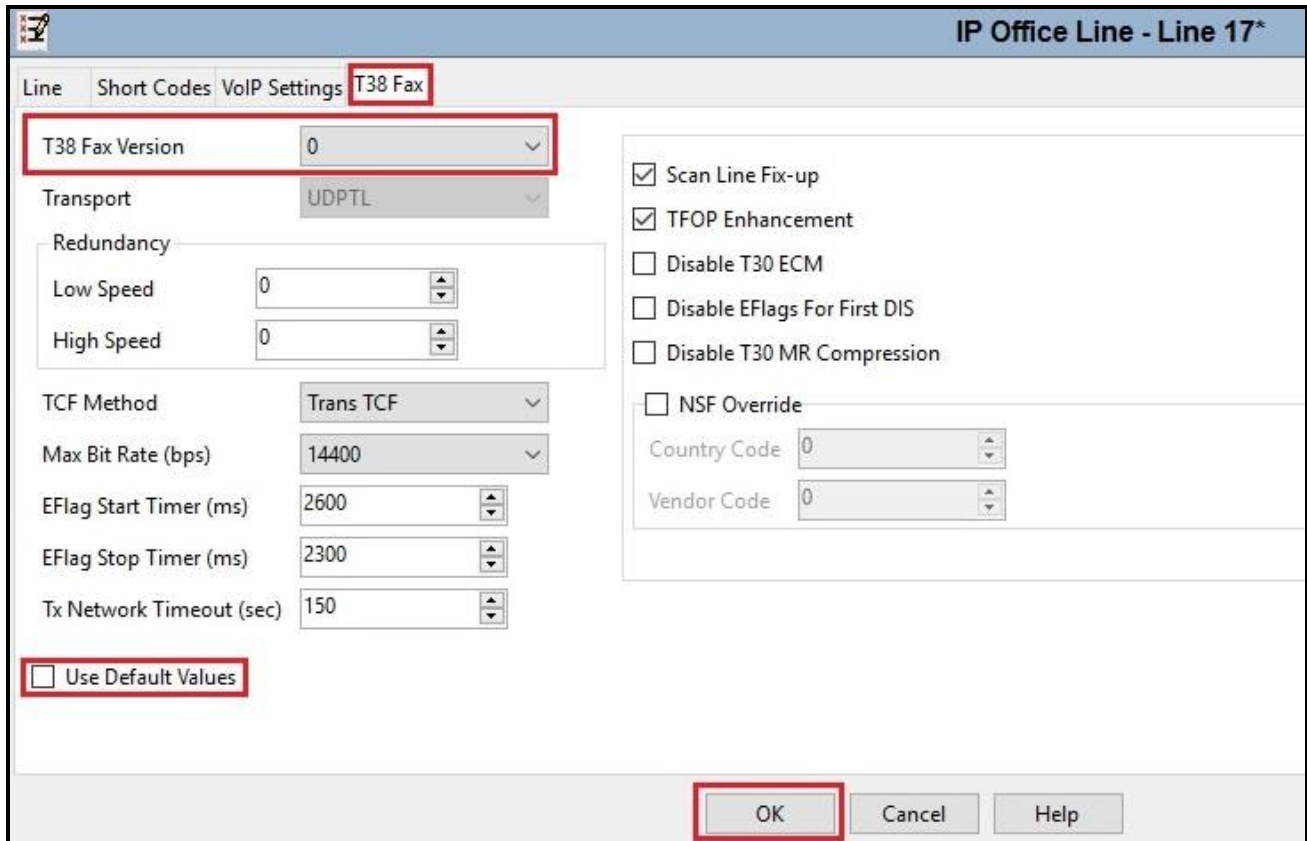


Figure 25 – IP Office Line for Expansion Server T38 Fax

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

- 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 State (US English)**
- Default values may be used for all other parameters
- Click **OK** to submit the changes

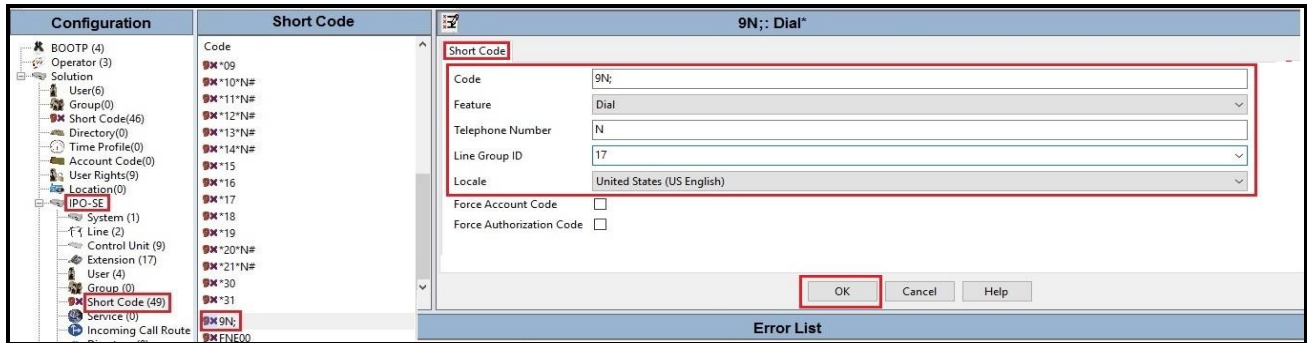


Figure 26 – Short Code 9N for Primary System

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

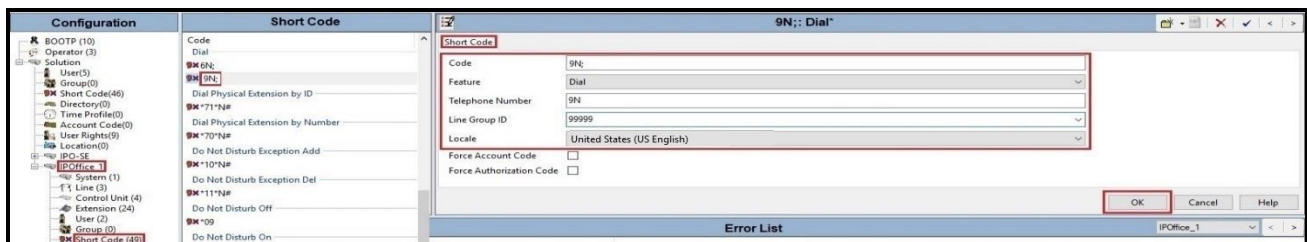


Figure 27 – Short Code 9N for Expansion System

The feature of incoming calls from mobility extension to idle-appearance FNE (Feature Name Extension) is hosted by Avaya IP Office Server Edition. The screen below shows the details of the previously administered “77700” short code for FNE Service.

Navigate to **Solution → Short Code**, right-click on **Short Code** and select **New**. 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 **77700** was configured with following parameters:

- For **Code** field, enter FNE feature code as **77700** 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

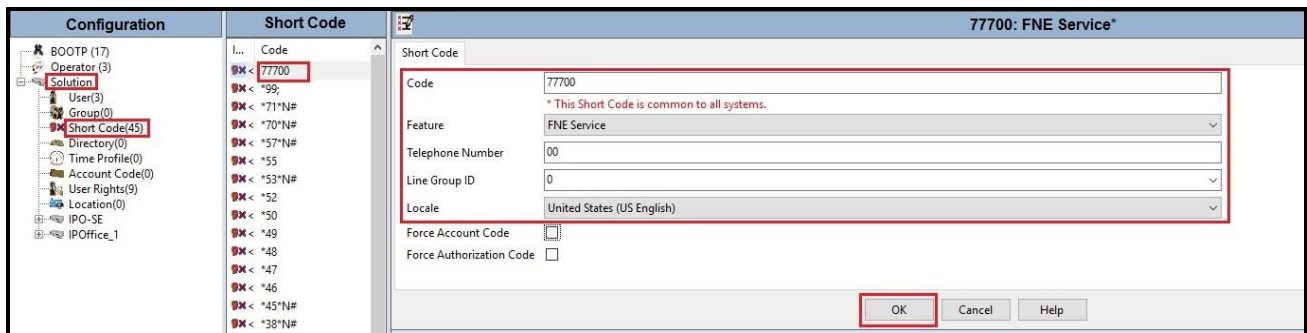


Figure 28 – Short Code FNE 77700

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 **531XXX4176**. Select the **User** tab in the Details pane.

Note: When **Auto** is selected for the **Local URI**, **Contact** and **Diversion Header** parameters (See **Section 5.5.2 - Call Detail** tab), the information in the Incoming Call Route (See **Section 5.10**) is used to populate the SIP From and Contact headers for outbound calls.

The screenshot displays the Avaya configuration interface for a user. The left navigation pane shows a tree view with 'User (3)' selected. The main configuration area is titled '531XXX4176: 4176*' and has the 'User' tab selected. The configuration fields are as follows:

Name	531XXX4176
Password	••••••••
Confirm Password	••••••••
Unique Identity	
Conference PIN	
Confirm Audio Conference PIN	
Account Status	Enabled
Full Name	531XXX4176
Extension	4176
Email Address	
Locale	United States (US English)
Priority	5
System Phone Rights	None
Profile	Power User
Receptionist	<input type="checkbox"/>
Enable Softphone	<input checked="" type="checkbox"/>
Enable one-X Portal Services	<input checked="" type="checkbox"/>
Enable one-X TeleCommuter	<input checked="" type="checkbox"/>
Enable Remote Worker	<input checked="" type="checkbox"/>
Enable Desktop/Tablet VoIP client	<input checked="" type="checkbox"/>
Enable Mobile VoIP Client	<input checked="" type="checkbox"/>
Enable MS Teams Client	<input checked="" type="checkbox"/>
Send Mobility Email	<input type="checkbox"/>
Web Collaboration	<input type="checkbox"/>

Figure 29 – User Configuration – User tab

To configure the restricted outbound call for a user by using specific W in the Short Code, 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 **531XXX4176**. 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 State (US English)**
- Default values may be used for all other parameters
- Click **OK** to submit the changes

Code	Telephone Number	Feature	Line Group ID

New Short Code	
Code	9N;
Feature	Dial
Telephone Number	WN
Line Group ID	17
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

Buttons: Add..., Remove, Edit..., OK, Cancel

Figure 30 – User Configuration – Short Code tab

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 531XXX4176**. 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 77700 (Defined in **Section 5.8**). Other options can be set according to customer requirements.

The screenshot displays the configuration interface for User 531XXX4176, specifically the Mobility tab. The interface includes several sections:

- Simultaneous:** Coverage Delay (secs) is set to 0. MS Teams URI is empty.
- Internal Twinning:** Twinned Handset is set to <None>. Maximum Number of Calls is set to 1. Options for Twin Bridge Appearances, Twin Coverage Appearances, and Twin Line Appearances are unchecked.
- Mobility Features:** This section is checked and contains:
 - Mobile Twinning
 - Fallback Twinning
 - Twinned Mobile Number (including dial access code): 91613XXX5096
 - Twinning Time Profile: <None>
 - Mobile Dial Delay (sec): 2
 - Mobile Answer Guard (sec): 0
 - Hunt group calls eligible for mobile twinning
 - Forwarded calls eligible for mobile twinning
 - Twin When Logged Out
 - one-X Mobile Client
 - Mobile Call Control
 - Mobile Callback

Figure 31 – Mobility Configuration for User

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

17 531XXX4176	
Standard	Voice Recording Destinations
Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	531XXX4176
Incoming Sub Address	
Incoming CLI	
Locale	United States (US English)
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

Figure 32 – 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 **531XXX4176** on line 17 are routed to **Destination 4176 531XXX4176** as below screenshot:

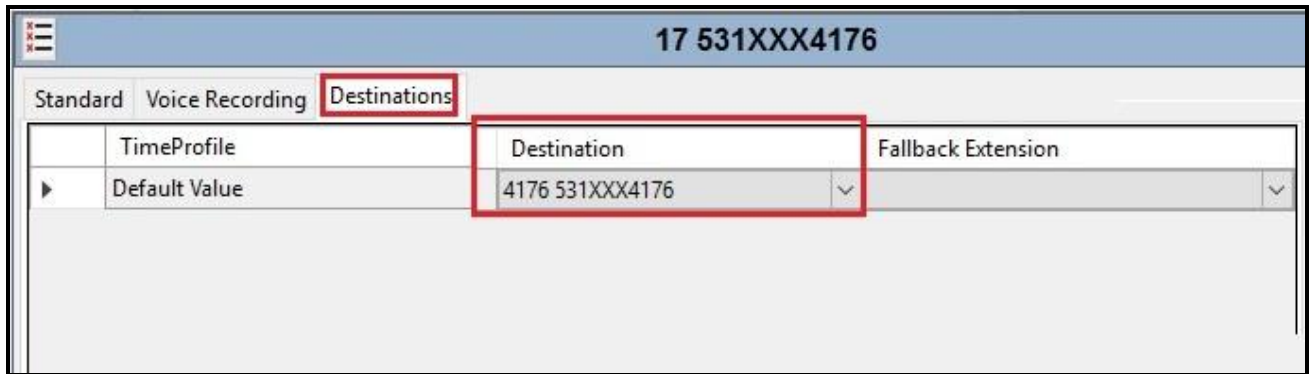


Figure 33 – Incoming Call Route for Destination 531XXX4176

For Feature Name Extension Service testing purpose, the incoming calls to DID number **531XXX7634** were configured to access to FNE Service. The **Destination** was appropriately defined as **77700** as below screenshot:

The screenshot displays the configuration for an Incoming Call Route (ICR) for the DID number 17 531XXX7634. The interface is divided into a left-hand navigation tree and a main configuration area. The navigation tree on the left shows a hierarchy of configuration objects, with 'Incoming Call Route (4)' selected and expanded to show four entries: 17 531XXX3647, 17 531XXX4176, 17 531XXX4728, and 17 531XXX7634. The main configuration area is titled '17 531XXX7634' and has three tabs: 'Standard', 'Voice Recording', and 'Destinations'. The 'Destinations' tab is active, displaying a table with the following data:

TimeProfile	Destination	Fallback Extension
Default Value	77700	

Figure 34 – Incoming Call Route for Destination FNE

For Voice Mail testing purpose, the incoming calls to DID number **531XXX3647** were configured to access **VoiceMail**. The **Destination** was appropriately defined as **VoiceMail** as below screenshot:

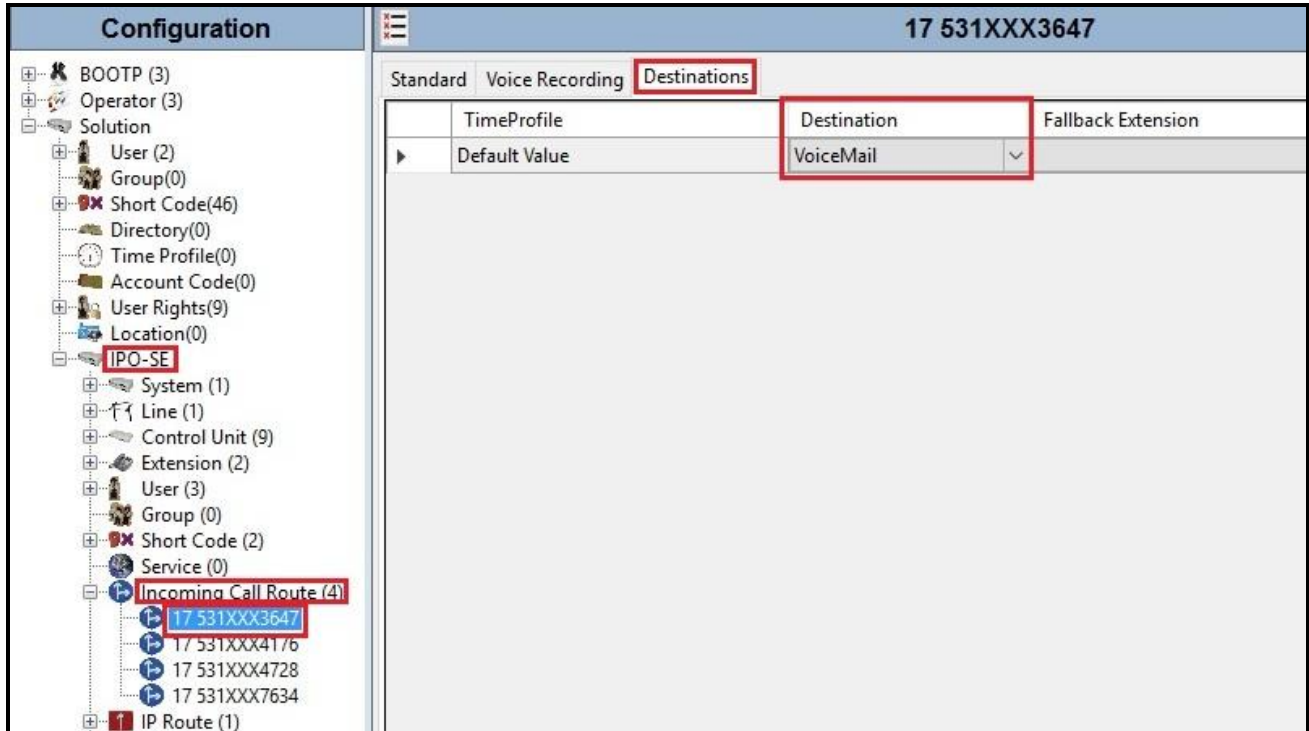


Figure 35 – Incoming Call Route for Destination VoiceMail

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.

6. Configure Avaya Session Border Controller

This section describes the configuration of Avaya SBC 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 SBC has been installed and that network connectivity exists between the systems. For more information on Avaya SBC, see relevant product documentation references in **Section 10** of these Application Notes.

6.1. Log in to the Avaya SBC

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 SBC).

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

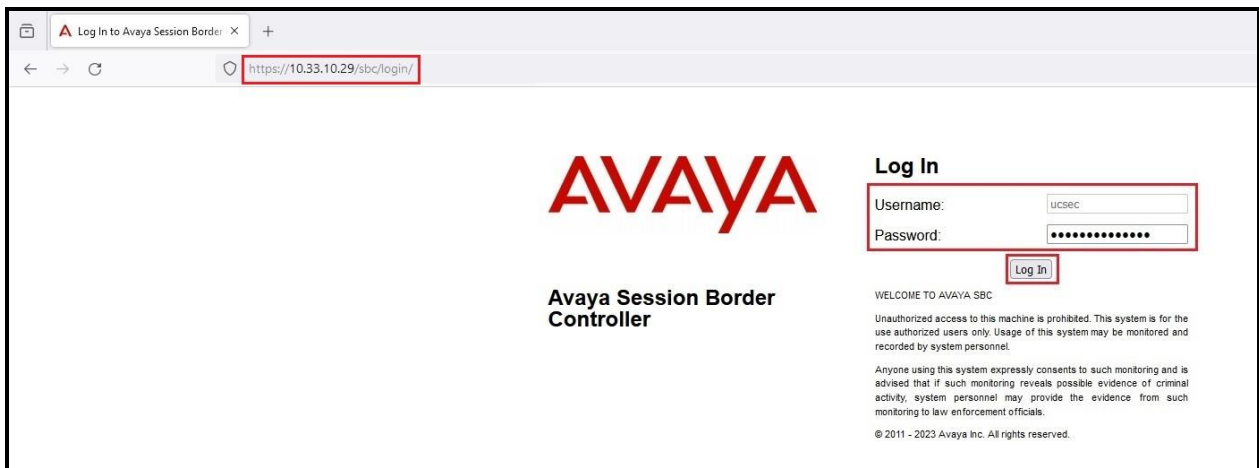


Figure 36 – Avaya SBC Login

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

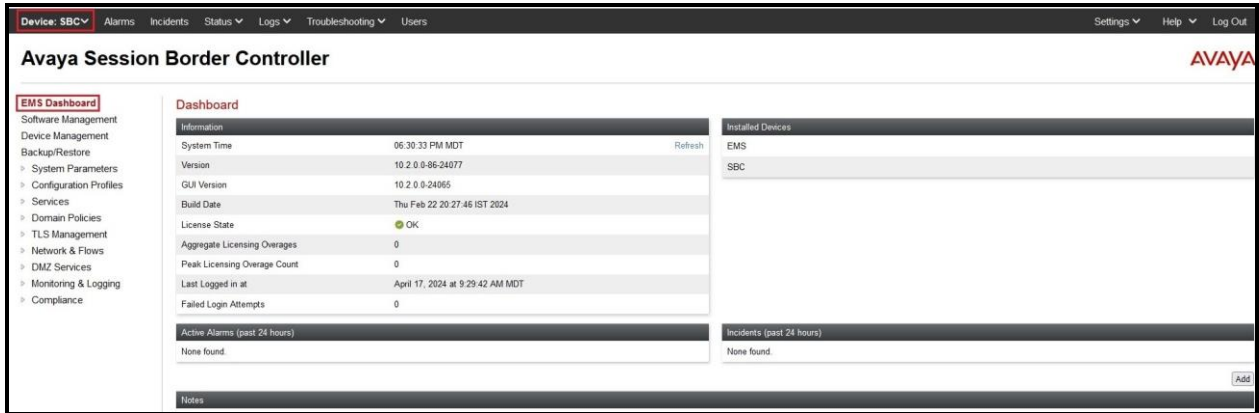


Figure 37 - Avaya SBC Dashboard

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 **SBC** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.



Figure 38 - Avaya SBC Device Management

The **System Information** screen shows **General Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**.

System Information: SBC

<p style="margin: 0;">General Configuration</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Appliance Name</td><td>SBC</td></tr> <tr><td>Box Type</td><td>SIP</td></tr> <tr><td>Deployment Mode</td><td>Proxy</td></tr> <tr><td>HA Mode</td><td>No</td></tr> </table>	Appliance Name	SBC	Box Type	SIP	Deployment Mode	Proxy	HA Mode	No	<p style="margin: 0;">Management IP(s)</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">IP #1 (IPv4)</td><td>10.33.10.29</td></tr> </table> <p style="margin: 5px 0 0 0;">DNS Configuration</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Primary DNS</td><td>10.33.100.60</td></tr> <tr><td>Secondary DNS</td><td></td></tr> <tr><td>DNS Location</td><td>DMZ</td></tr> <tr><td>DNS Client IP</td><td>10.33.10.49</td></tr> </table>	IP #1 (IPv4)	10.33.10.29	Primary DNS	10.33.100.60	Secondary DNS		DNS Location	DMZ	DNS Client IP	10.33.10.49	<p style="margin: 0;">License Allocation</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 70%;">Standard Sessions <small>Requested: 0</small></td><td style="text-align: right;">0</td></tr> <tr><td>Advanced Sessions <small>Requested: 0</small></td><td style="text-align: right;">0</td></tr> <tr><td>Scopia Video Sessions <small>Requested: 0</small></td><td style="text-align: right;">0</td></tr> <tr><td>CES Sessions <small>Requested: 0</small></td><td style="text-align: right;">0</td></tr> <tr><td>Transcoding Sessions <small>Requested: 0</small></td><td style="text-align: right;">0</td></tr> <tr><td>AMR</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>Premium Sessions <small>Requested: 0</small></td><td style="text-align: right;">0</td></tr> <tr><td>CLID</td><td style="text-align: right;">---</td></tr> <tr><td>Encryption <small>Available: Yes</small></td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> </table>	Standard Sessions <small>Requested: 0</small>	0	Advanced Sessions <small>Requested: 0</small>	0	Scopia Video Sessions <small>Requested: 0</small>	0	CES Sessions <small>Requested: 0</small>	0	Transcoding Sessions <small>Requested: 0</small>	0	AMR	<input checked="" type="checkbox"/>	Premium Sessions <small>Requested: 0</small>	0	CLID	---	Encryption <small>Available: Yes</small>	<input checked="" type="checkbox"/>
Appliance Name	SBC																																					
Box Type	SIP																																					
Deployment Mode	Proxy																																					
HA Mode	No																																					
IP #1 (IPv4)	10.33.10.29																																					
Primary DNS	10.33.100.60																																					
Secondary DNS																																						
DNS Location	DMZ																																					
DNS Client IP	10.33.10.49																																					
Standard Sessions <small>Requested: 0</small>	0																																					
Advanced Sessions <small>Requested: 0</small>	0																																					
Scopia Video Sessions <small>Requested: 0</small>	0																																					
CES Sessions <small>Requested: 0</small>	0																																					
Transcoding Sessions <small>Requested: 0</small>	0																																					
AMR	<input checked="" type="checkbox"/>																																					
Premium Sessions <small>Requested: 0</small>	0																																					
CLID	---																																					
Encryption <small>Available: Yes</small>	<input checked="" type="checkbox"/>																																					

<p style="margin: 0;">Network Configuration</p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: left;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="width: 15%;">IP</th> <th style="width: 15%;">Public IP</th> <th style="width: 20%;">Network Prefix or Subnet Mask</th> <th style="width: 20%;">Gateway</th> <th style="width: 30%;">Interface</th> </tr> </thead> <tbody> <tr><td>10.33.10.49</td><td>10.33.10.49</td><td>255.255.255.0</td><td>10.33.10.1</td><td>A1</td></tr> <tr><td>10.33.10.50</td><td>10.33.10.50</td><td>255.255.255.0</td><td>10.33.10.1</td><td>A1</td></tr> <tr><td>10.33.10.59</td><td>10.33.10.59</td><td>255.255.255.0</td><td>10.33.10.1</td><td>B1</td></tr> <tr><td>10.10.80.105</td><td>10.10.80.105</td><td>255.255.255.0</td><td>10.10.80.1</td><td>A2</td></tr> </tbody> </table>	IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface	10.33.10.49	10.33.10.49	255.255.255.0	10.33.10.1	A1	10.33.10.50	10.33.10.50	255.255.255.0	10.33.10.1	A1	10.33.10.59	10.33.10.59	255.255.255.0	10.33.10.1	B1	10.10.80.105	10.10.80.105	255.255.255.0	10.10.80.1	A2
IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface																					
10.33.10.49	10.33.10.49	255.255.255.0	10.33.10.1	A1																					
10.33.10.50	10.33.10.50	255.255.255.0	10.33.10.1	A1																					
10.33.10.59	10.33.10.59	255.255.255.0	10.33.10.1	B1																					
10.10.80.105	10.10.80.105	255.255.255.0	10.10.80.1	A2																					

Figure 39 - Avaya SBC System Information

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
- Check **T.38 Support** option and click **Finish** (not shown).

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

The screenshot displays the Avaya Session Border Controller configuration interface. On the left, a navigation menu shows 'Configuration Profiles' expanded to 'Server Interworking'. The main area shows the configuration for 'Interworking Profiles: IPO'. A table lists various SIP-related settings, with 'T.38 Support' checked. The 'Edit' button is visible at the bottom right.

Setting	Value
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	No
Mediasec	No

Figure 40 - Server Interworking – Avaya

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
- Check **T.38 Support** option and click **Finish** (not shown)

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

The screenshot displays the Avaya Session Border Controller configuration page. On the left, a navigation menu includes 'Configuration Profiles' and 'Server Interworking'. The main area shows 'Interworking Profiles: SP' with an 'Add' button. Below this, a list of profiles includes 'cs2100', 'avaya-ru', 'IPO', and 'SP'. The 'SP' profile is selected, and its configuration is shown in a table with tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, showing various settings. The 'T.38 Support' setting is highlighted with a red box and set to 'Yes'. An 'Edit' button is visible at the bottom right of the configuration table.

Setting	Value
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	No
Mediasec	No

Figure 41 - Server Interworking – Cox Communications

6.3. Configure SIP Server

Servers are defined for each server connected to the Avaya SBC. In this case, IP Office is connected as the Call Server and Cox Communications 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)

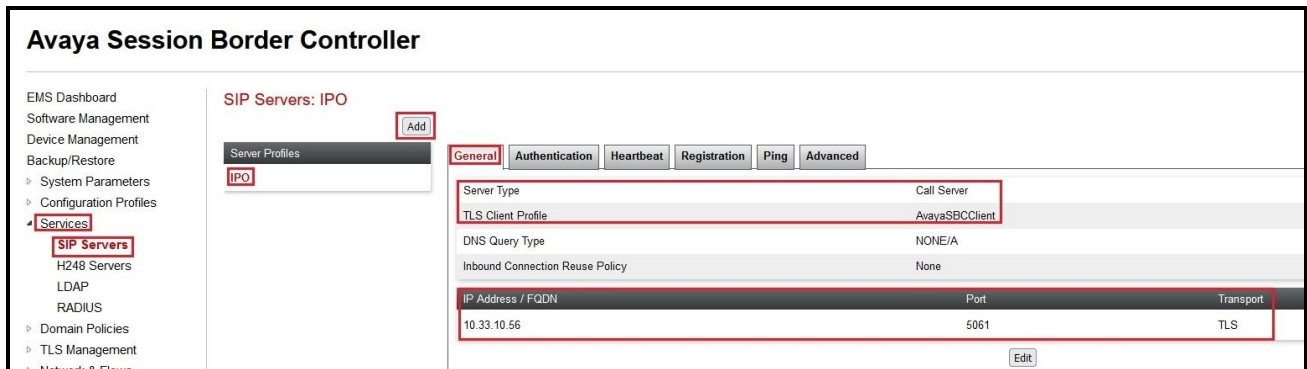


Figure 42 – Avaya SIP Server Configuration – General

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

- Check **Enable Heartbeat** option
- **Method: OPTIONS**
- Set **Retry Timeout on Connection Failure: 2 seconds**
- **Frequency: 60 seconds**
- **From URI: ping@10.33.10.49**
- **To URI: ping@10.33.10.56**
- Click **Finish** (Not shown)

Configuration Item	Value
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Retry Timeout on Connection Failure	2 seconds
Frequency	60 seconds
From URI	ping@10.33.10.49
To URI	ping@10.33.10.56

Figure 43 – Avaya SIP Server Configuration – Heartbeat

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)

General	Authentication	Heartbeat	Registration	Ping	Advanced
Enable DoS Protection					<input type="checkbox"/>
Enable Grooming					<input checked="" type="checkbox"/>
Interworking Profile					IPO
Signaling Manipulation Script					None
Securable					<input type="checkbox"/>
Enable FGDN					<input type="checkbox"/>
Tolerant					<input type="checkbox"/>
URI Group					None
NG911 Support					<input type="checkbox"/>

Figure 44 – Avaya SIP Server Configuration – Advanced

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 LAN1 IP address)
- **Port:** **5060**
- **Transport:** **UDP**
- Click **Finish** (not shown)

The screenshot shows the Avaya Session Border Controller configuration interface. The left sidebar contains a navigation menu with 'SIP Servers' selected. The main area displays the configuration for 'SIP Servers: SP' on the 'General' tab. The configuration includes:

- Server Type: Trunk Server
- DNS Query Type: NONE/A
- Inbound Connection Reuse Policy: None
- IP Address / FQDN / CIDR Range: 10.33.10.60
- Port: 5060
- Transport: UDP

Figure 45 – Cox Communications SIP Server Configuration – General

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

- Check **Enable Heartbeat**
- Select **Method: OPTIONS**
- Set **Retry Timeout on Connection Failure: 2 seconds**
- Set **Frequency: 60 seconds**
- Input **From URI: 402XXX6211@10.33.10.59** (Cox Communications provides this number)
- Input **To URI: 402XXX6211@10.33.10.60** (Cox Communications provides this number)

The screenshot shows the Avaya Session Border Controller configuration interface for the 'Heartbeat' tab. The configuration includes:

- Enable Heartbeat:
- Method: OPTIONS
- Retry Timeout on Connection Failure: 2 seconds
- Frequency: 60 seconds
- From URI: 402XXX6211@10.33.10.59
- To URI: 402XXX6211@10.33.10.60

Figure 46 - Cox Communications SIP Server – Heartbeat

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

- Uncheck **Enable Grooming** option
- **Interworking Profile: SP** (see **Section 6.2.2**)
- Click **Finish** (not shown)

General	Authentication	Heartbeat	Registration	Ping	Advanced
Enable DoS Protection					<input type="checkbox"/>
Enable Grooming					<input type="checkbox"/>
Interworking Profile					SP
Signaling Manipulation Script					None
Securable					<input type="checkbox"/>
Enable FGDN					<input type="checkbox"/>
Tolerant					<input type="checkbox"/>
URI Group					None
NG911 Support					<input type="checkbox"/>

[Edit](#)

Figure 47 – Cox Communications SIP Server – Advanced

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

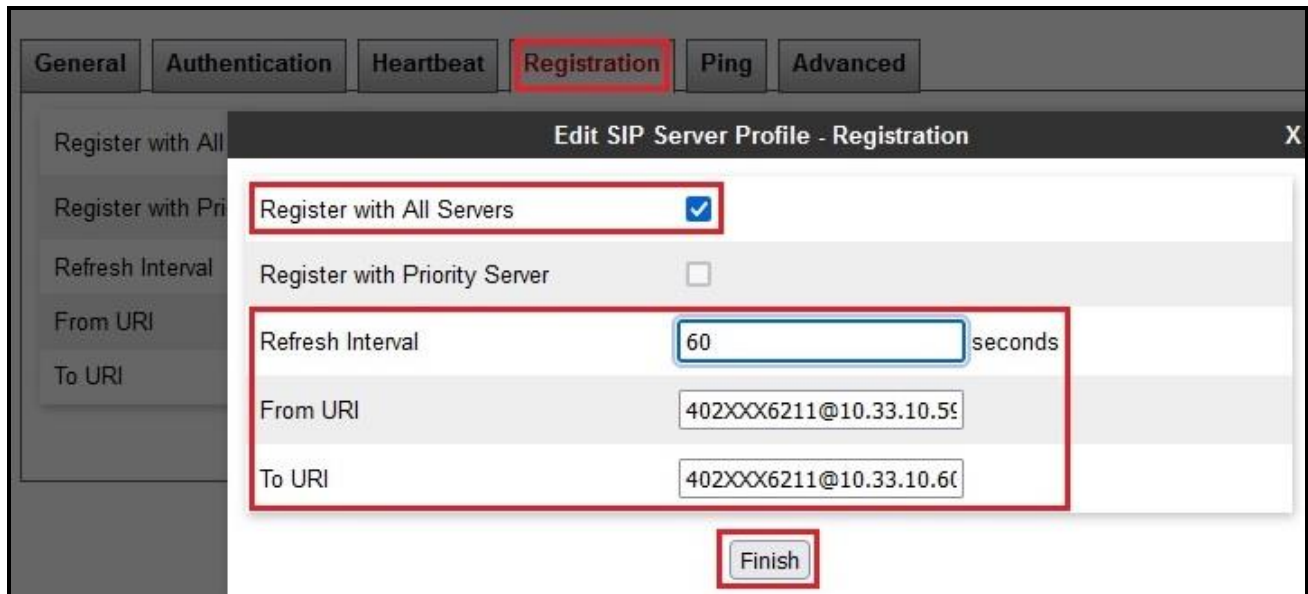
- Check **Enable Authentication** option
- Input **User Name** (Cox Communications provides the user name)
- Leave **Realm** as blank
- Enter **Password** (Cox Communications provides the password)
- Enter **Confirm Password** (Cox Communications provides the password)
- Click **Finish**

The screenshot shows a configuration window titled "Edit SIP Server Profile - Authentication". At the top, there are tabs for "General", "Authentication", "Heartbeat", "Registration", "Ping", and "Advanced". The "Authentication" tab is active. Below the tabs, there is a section for "Enable Authentication" with a checked checkbox. A red box highlights the "Enable Authentication" checkbox and the "User Name" field, which contains the text "402XXX6211". Below the "User Name" field are three more fields: "Realm" (with a note "(Leave blank to detect from server challenge)"), "Password" (with a note "(Leave blank to keep existing password)"), and "Confirm Password". All three of these fields are masked with dots. At the bottom of the window, there is a "Finish" button, also highlighted with a red box.

Figure 48 – Cox Communications SIP Server – Authentication

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

- Check **Register with All Servers** option
- Set **Refresh Interval** as **60** seconds
- Input **From URI: 402XXX6211@10.33.10.59** (Cox Communications provides this number)
- Input **To URI: 402XXX6211@10.33.10.60** (Cox Communications provides this number)
- Click **Finish**



The screenshot shows the 'Edit SIP Server Profile - Registration' window. The 'Registration' tab is selected. The 'Register with All Servers' checkbox is checked. The 'Refresh Interval' is set to 60 seconds. The 'From URI' is 402XXX6211@10.33.10.59 and the 'To URI' is 402XXX6211@10.33.10.60. A 'Finish' button is located at the bottom of the window.

Figure 49 – Cox Communications SIP Server – 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 SBC 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**

The screenshot shows the Avaya Session Border Controller configuration interface. The left sidebar contains a navigation menu with 'Configuration Profiles' and 'Routing' highlighted. The main area is titled 'Routing Profiles: To_IPO' and contains an 'Add Routing Rule' form. The form includes various settings such as 'URI Group', 'Load Balancing', 'Next Hop Priority', and 'SIP Server Profile'. A table at the bottom lists the configured routing rules.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				IPO	10.33.10.56:5061 (TLS)	None

Figure 50 - Routing to Avaya IP Office

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** and click **Next** button (not shown)

- **Load Balancing: Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight: 1**
- **SIP Server Profile: SP** (see **Section 6.3.2**). This selection will automatically populate the **Next Hop Address** field with **10.33.10.60:5060 (UDP)**
- Click **Finish**

The screenshot shows the Avaya Session Border Controller configuration interface. On the left is a navigation menu with 'Configuration Profiles' and 'Routing' highlighted. The main area shows 'Routing Profiles: To_SP' with an 'Add' button. A modal window titled 'Add Routing Rule' is open, displaying various configuration options. The 'Load Balancing' dropdown is set to 'Priority', and the 'Next Hop Priority' checkbox is checked. The 'SIP Server Profile' is set to 'SP', which has populated the 'Next Hop Address' field with '10.33.10.60:5060 (UDP)'. A table at the bottom lists the configured rule with a priority of 1. The 'Finish' button is visible at the bottom of the modal.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				SP	10.33.10.60:5060 (UDP)	None

Figure 51 - Routing to Cox Communications

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 SBC internal 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 LAN1 port IP address)
 - For the Header **To**,
 - In the **Criteria** column, select **IP/Domain**
 - In the **Replace Action** column, select **Overwrite**
 - In the **Overwrite Value** column, enter **10.33.10.56** (Avaya IP Office LAN1 port IP address)
- Click **Finish** (not shown)

The screenshot shows the Avaya Session Border Controller configuration interface. The left sidebar contains a navigation menu with 'Configuration Profiles' selected, and 'Topology Hiding' highlighted. The main area displays 'Topology Hiding Profiles: To_IPO' with a table of configurations. The table has columns for Header, Criteria, Replace Action, and Overwrite Value. The 'To_IPO' profile is selected, and its configuration is shown in the table below.

Header	Criteria	Replace Action	Overwrite Value
From	Domain	Overwrite	10.33.10.49
Request-Line	Domain	Overwrite	10.33.10.56
SDP	Domain	Auto	---
Via	Domain	Auto	---
Referred-By	Domain	Auto	---
Record-Route	Domain	Auto	---
Refer-To	Domain	Auto	---
To	Domain	Overwrite	10.33.10.56

Figure 52 - Topology Hiding Avaya IP Office

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)
- Select **To_SP** in **Topology Hiding Profiles** and click **Edit** button to enter 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: **10.33.10.59** (Avaya SBC external 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: **10.33.10.60** (Cox Managed CPE LAN 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: **10.33.10.60** (Cox Managed CPE LAN IP address)
- Click **Finish** (not shown)

The screenshot shows the Avaya Session Border Controller configuration interface. The left sidebar contains a navigation menu with 'Configuration Profiles' and 'Topology Hiding' highlighted. The main area displays 'Topology Hiding Profiles: To_SP' with a table of headers and their configurations. The table has four columns: Header, Criteria, Replace Action, and Overwrite Value. The 'From' header is configured with Criteria 'IP/Domain', Replace Action 'Overwrite', and Overwrite Value '10.33.10.59'. The 'Request-Line' header is configured with Criteria 'IP/Domain', Replace Action 'Overwrite', and Overwrite Value '10.33.10.60'. The 'To' header is configured with Criteria 'IP/Domain', Replace Action 'Overwrite', and Overwrite Value '10.33.10.60'. Other headers like 'SDP', 'Via', 'Referred-By', 'Record-Route', and 'Refer-To' are set to 'Auto' for Replace Action and have empty Overwrite Value fields. An 'Edit' button is visible at the bottom of the table.

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	10.33.10.59
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	10.33.10.60
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Overwrite	10.33.10.60

Figure 53 - Topology Hiding Cox Communications

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 SBC 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

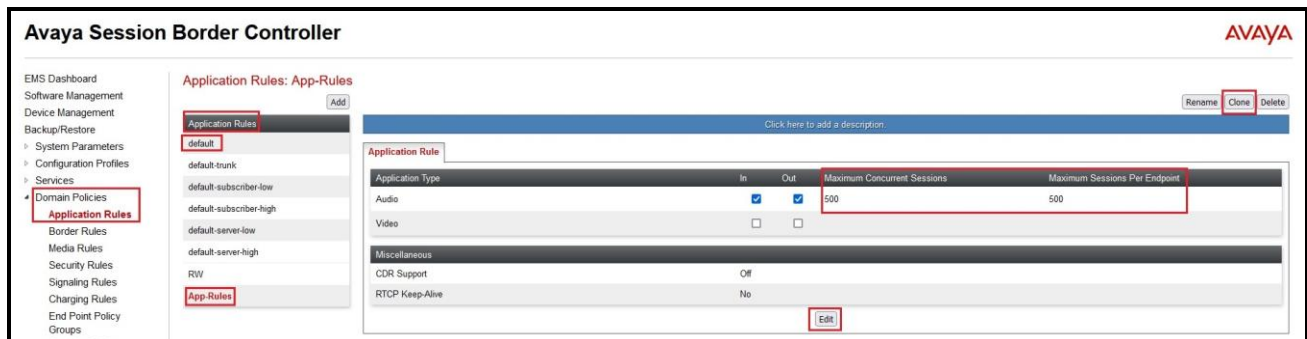


Figure 54 – Application Rule

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 SBC 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
- 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 the followings:
 - **Preferred Format #1: SRTP_AES_CM_128_HMAC_SHA1_80**
 - **Preferred Format #2: RTP**
 - Check **Interworking** option
- Under **Miscellaneous**, check **Capability Negotiation**
- Click **Finish** button (Not shown) to save the changes

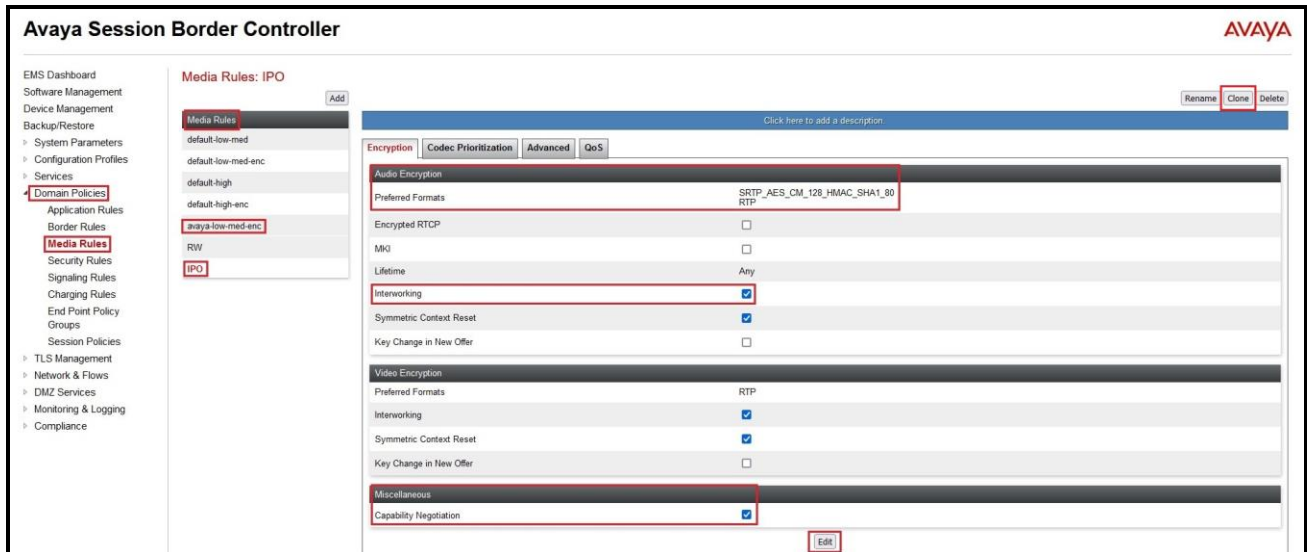


Figure 55 – Media Rule

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 SBC security features to very specific types of SIP signaling messages traversing through the enterprise.

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

- Select **Add**
- Enter **Group Name: 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)

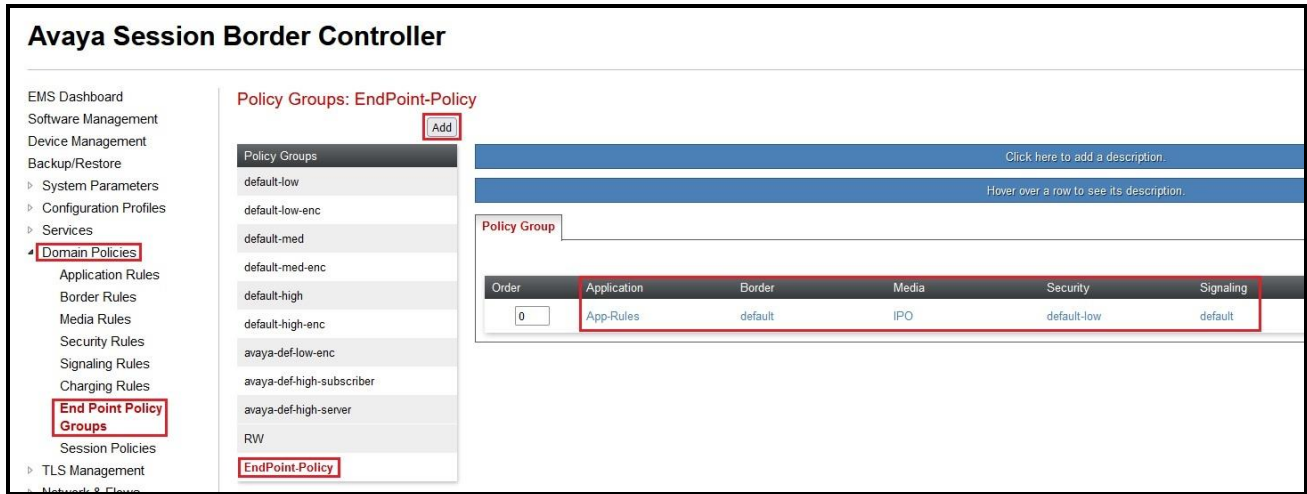


Figure 56 – End Point Policy – IPO

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
- Select **Finish** (not shown)

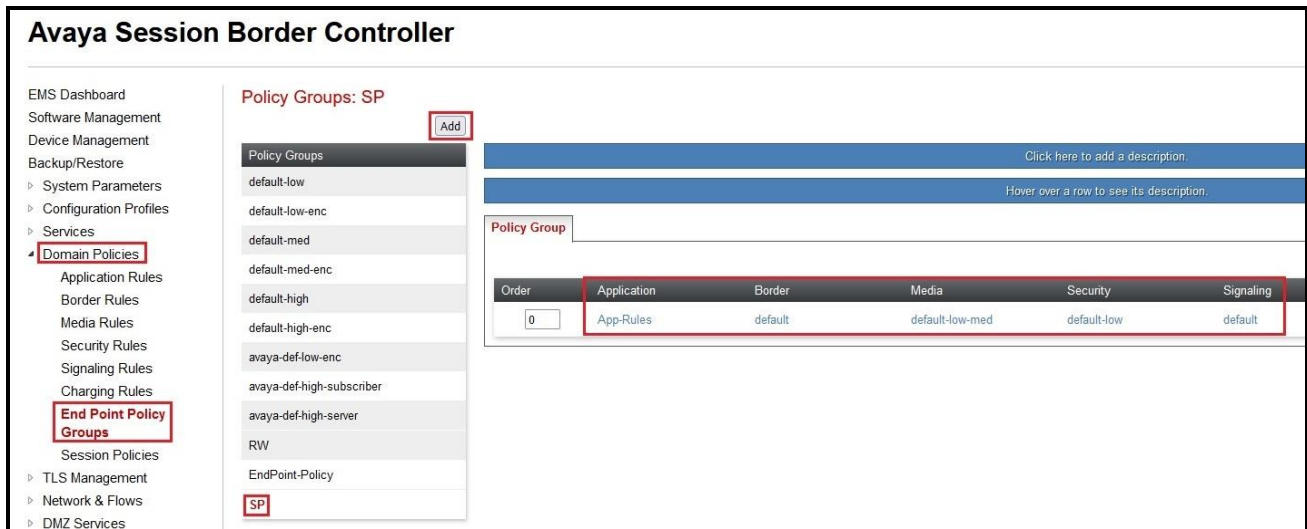


Figure 57 – End Point Policy – Cox Communications

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 SBC 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

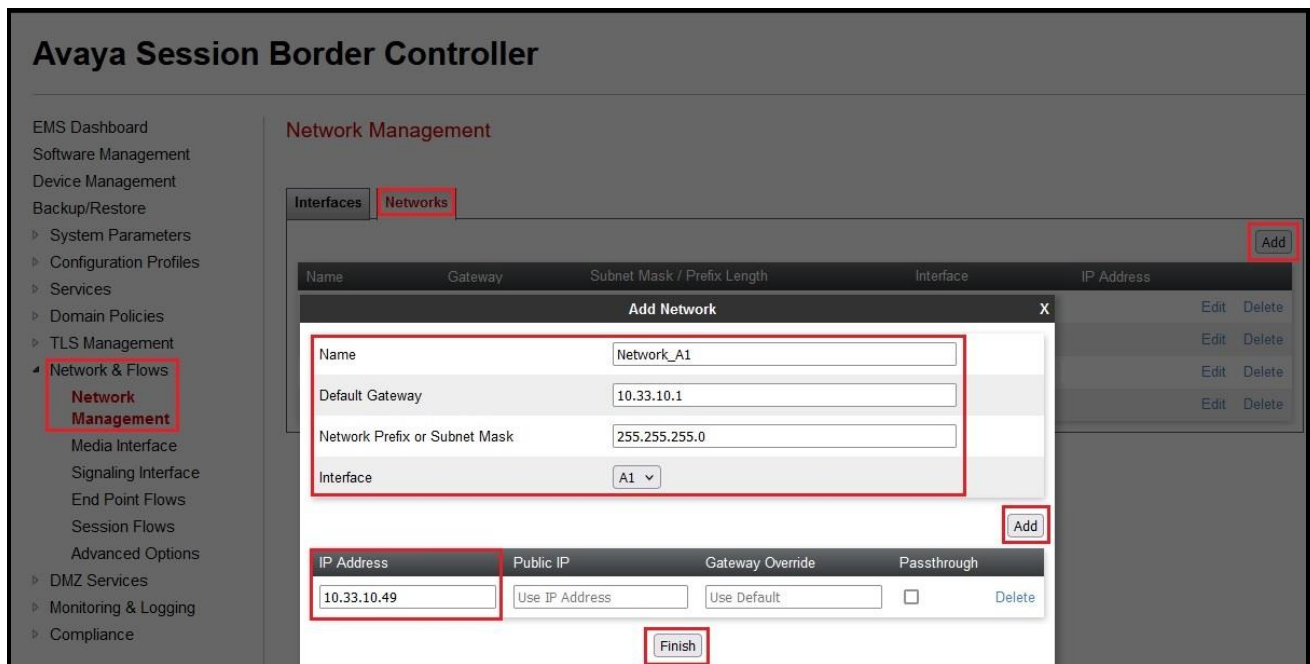


Figure 58 - Network Management – Inside Interface

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_B1**
 - **Default Gateway: 10.33.10.1**
 - **Subnet Mask: 255.255.255.0**
 - **Interface: B1** (This is the Avaya SBC 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

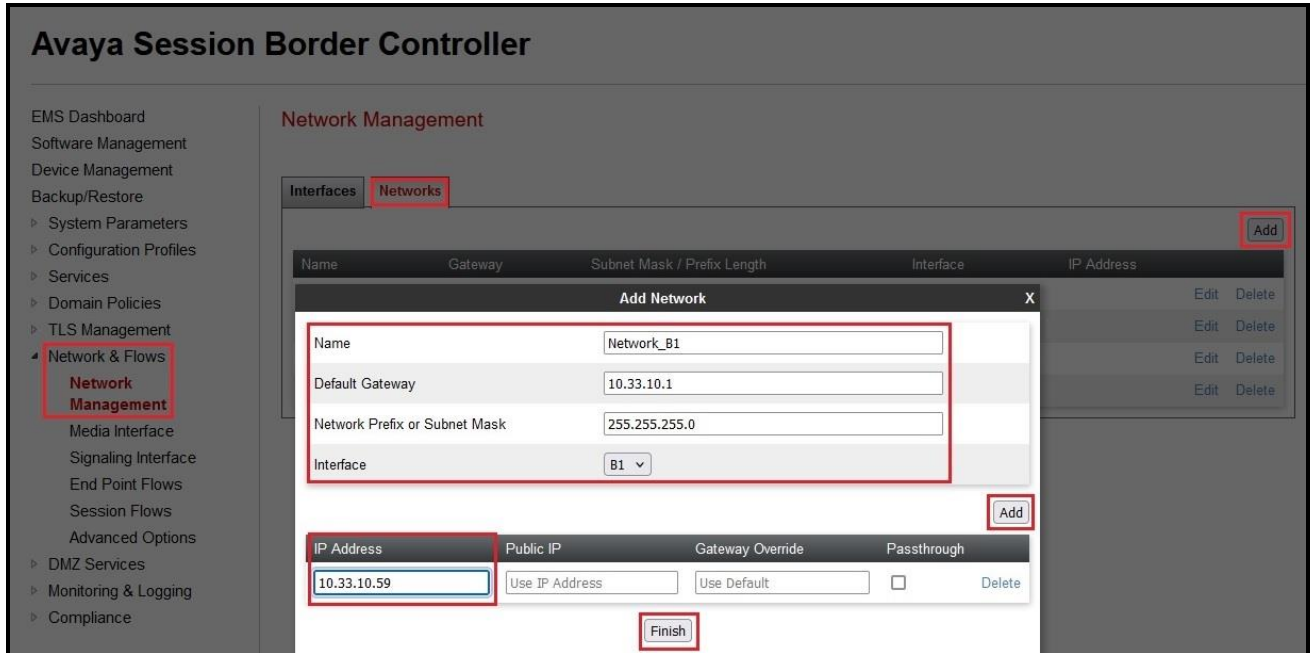
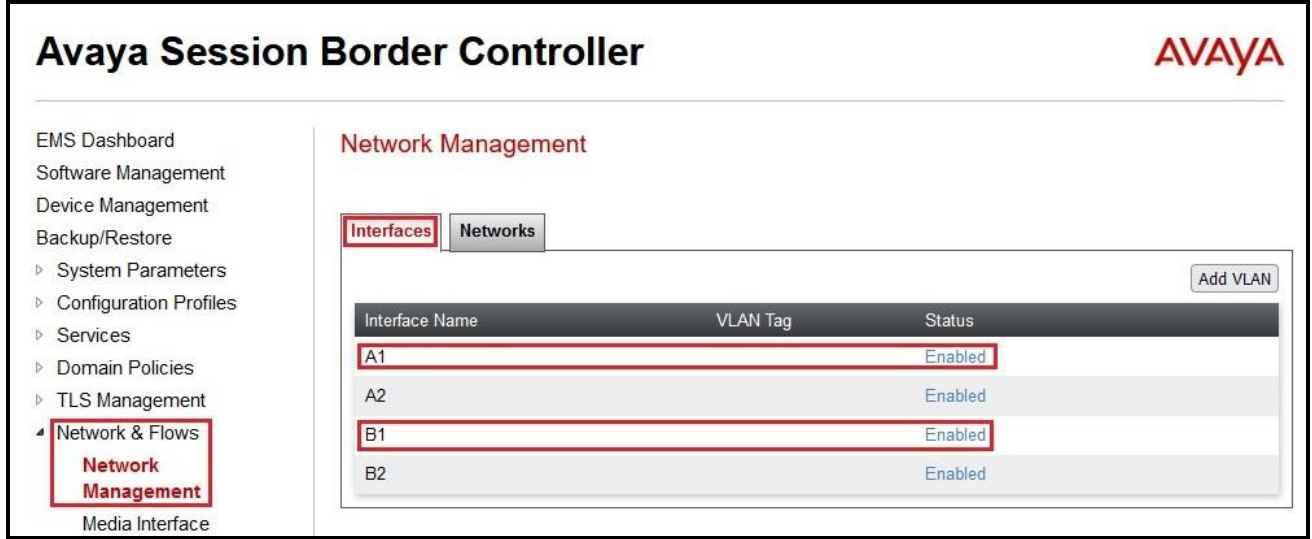


Figure 59 - Network Management – Outside Interface

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



The screenshot displays the Avaya Session Border Controller's Network Management interface. On the left is a navigation menu with 'Network & Flows' expanded to 'Network Management'. The main content area has two tabs: 'Interfaces' (selected) and 'Networks'. A table lists four interfaces: A1, A2, B1, and B2, all with 'Enabled' status. A red box highlights the 'Interfaces' tab and the 'Enabled' status for A1 and B1. An 'Add VLAN' button is in the top right of the table area.

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Enabled
B1		Enabled
B2		Enabled

Figure 60 - Network Management – Interface Status

6.7.2. Create Media Interfaces

Media Interfaces define the IP Addresses and port ranges in which the Avaya SBC will accept media streams on each interface. The default media port range on the Avaya SBC 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: 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)
- Select the **Add** button and enter the following:
 - **Name: OutsideMedia**
 - **IP Address:** Select **Network_B1 (B1, VLAN 0)** and **10.33.10.59** (External IP address toward Cox Managed CPE)
 - **Port Range: 35000 – 40000**
 - Click **Finish** (not shown)

Name	Media IP Network	Port Range	
InsideMedia	10.33.10.49 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
OutsideMedia	10.33.10.59 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit Delete

Figure 61 - Media Interface

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: OutsideSig**
 - **IP Address:** Select **Network_B1 (B1, 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: InsideSig**
 - **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 SBC was configured to listen for UDP on port 5060 the same as Cox Communications used. For the internal interface, the Avaya SBC was configured to listen for TLS on port 5061.

The screenshot shows the Avaya Session Border Controller web interface. The left-hand navigation menu is visible, with 'Network & Flows' and 'Signaling Interface' highlighted in red. The main content area is titled 'Signaling Interface' and contains a table with the following data:

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
OutsideSig	10.33.10.59 Network_B1 (B1, VLAN 0)	---	5060	---	None	Edit Delete
InsideSig	10.33.10.49 Network_A1 (A1, VLAN 0)	---	---	5061	AvayaSBCServer	Edit Delete

Figure 62 - Signaling Interface

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: OutsideSig** (see **Section 6.7.3**)
 - **Signaling Interface: InsideSig** (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

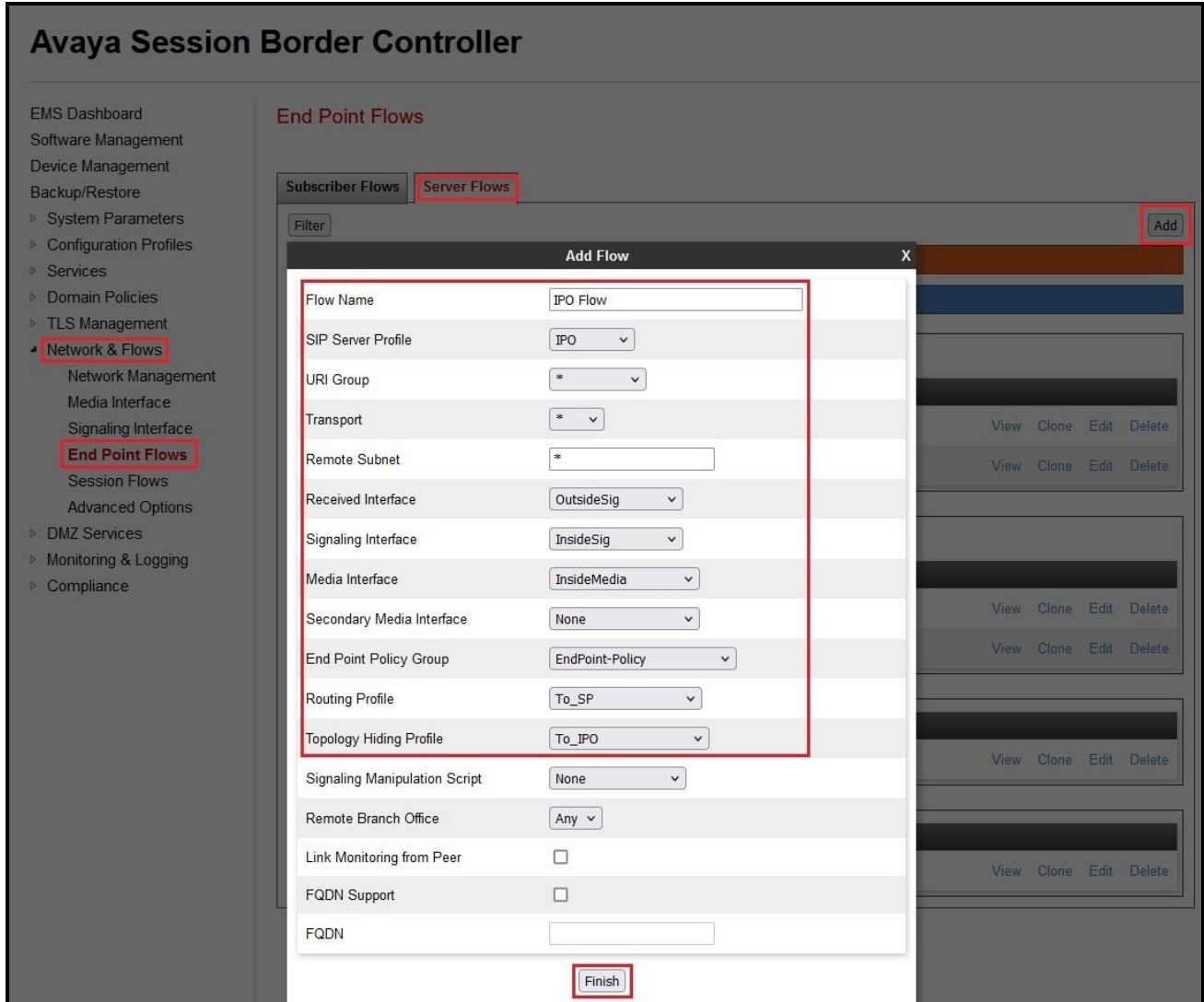


Figure 63 - End Point Flow 1

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: InsideSig** (see Section 6.7.3)
 - **Signaling Interface: OutsideSig** (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

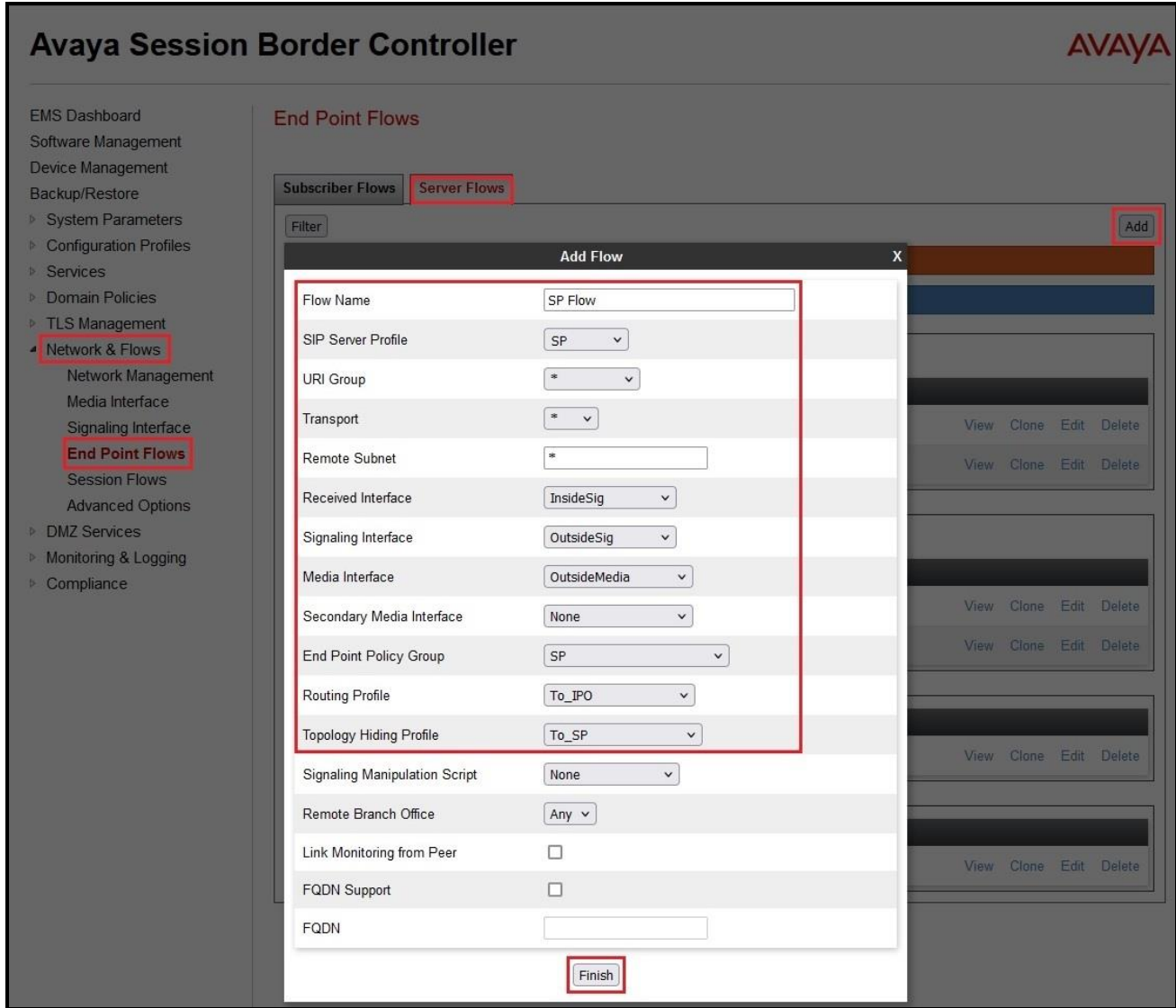


Figure 64 - End Point Flow 2

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 Avaya SBC public interface at the enterprise. Cox Communications will provide the customer necessary information to configure the SIP connection between Avaya SBC and Cox Managed CPE. Cox Communications also provides the Cox Communications SIP Specification document for reference.

The configuration between Cox Communications SIP Trunk and the enterprise is a static IP Address configuration.

8. Verification Steps

The following steps may be used to verify the configuration:

- Use the Avaya IP Office Monitor application to monitor the active SIP call traces between the enterprise and Cox Communications. Launch the application from **Start → All apps → IP Office → Monitor** on the PC where Avaya IP Office Server Edition Manager was installed. Click start/ stop buttons to capture the SIP call traces.

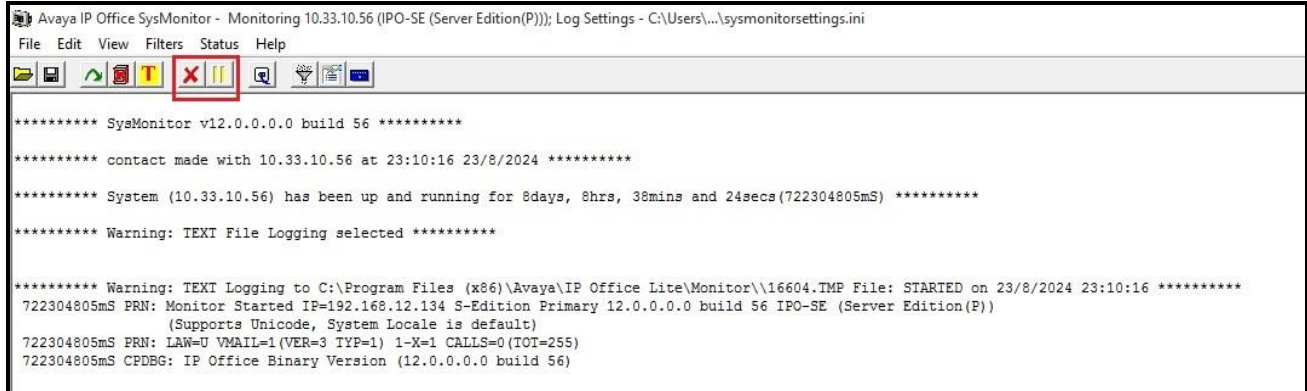


Figure 65 – SIP Trace Monitor

- 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)

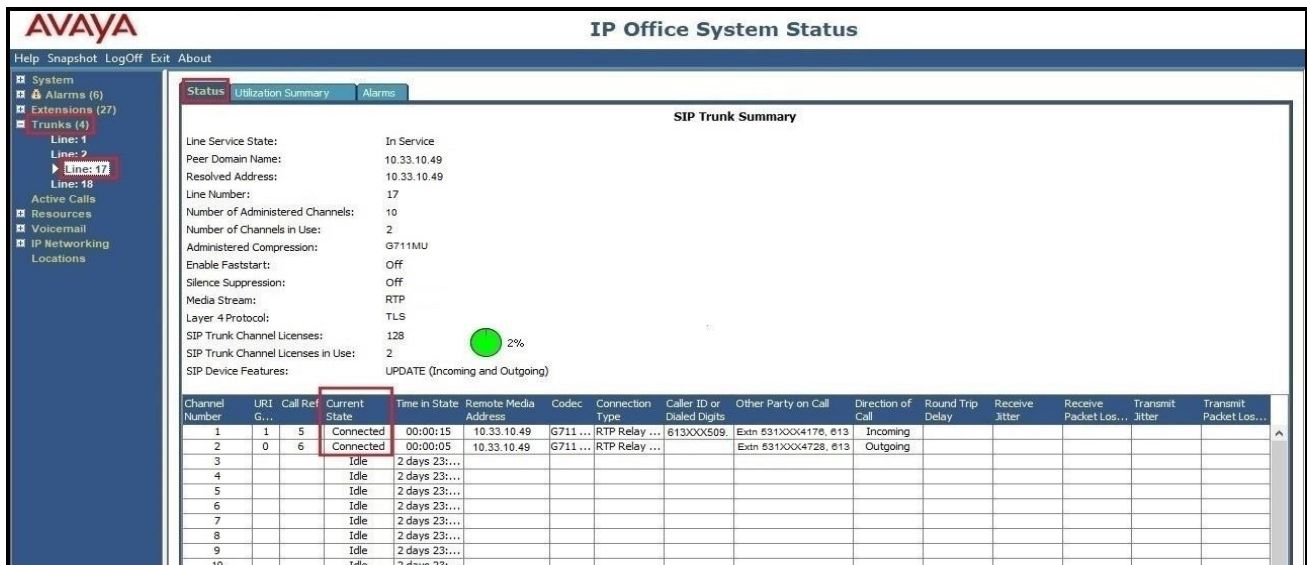


Figure 66 – SIP Trunk status

- 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.

The screenshot shows the Avaya IP Office System Status application interface. The title bar reads "AVAYA IP Office System Status". The menu bar includes "Help", "Snapshot", "LogOff", "Exit", and "About". On the left, a navigation tree shows "System", "Alarms (0)", "Configuration (0)", "Service (0)", and "Trunks (4)" with sub-items "Line: 1 (0)", "Line: 2 (0)", and "Line: 17 (0)". The main area displays a table titled "Select a line to display the alarm information".

Line	Module / Slot / Type	Port Number / Address / Domain	Alarms
1	Slot: 1	1	0
2	Slot: 1	2	0
17	SIP	10.33.10.49	0

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 SBC by executing command via the Command Line Interface (CLI): Login Avaya SBC with root user and enter the command: #traceSBC. The tool updates the database directly based on which trace mode is selected.

9. Conclusion

Cox Communications successfully passed compliance testing via the Avaya DevConnect Program. These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 12.0 and the Avaya SBC 10.2 to support Cox Communications SIP Trunking service, as shown in **Figure 1**.

10. Additional References

- [1] *Avaya IP Office™ Platform Release 12.0 Release Notes / Technical Bulletin General Availability Issue 002, June 20th, 2024*
- [2] *Deploying IP Office Server Edition and Application Servers, Release 12.0 Issue 31, April 2024*
- [3] *Deploying Avaya IP Office Servers as Virtual Machines, Release 12.1, Issue 23, August 2024*
- [4] *IP Office™ Platform 12.0, Deploying an IP Office 500 V2/V2A in IP Office Basic Edition Mode, Issue 41e, May 29th, 2024*
- [5] *Administering Avaya IP Office using Manager, Release 12.0, Issue 51.1.2, June 2024.*
- [6] *Deploying Avaya Session Border Controller on a Virtualized Environment Platform, Release 10.2.x, Issue 1, June 2024.*
- [7] *Administering Avaya Session Border Controller, Release 10.2.x, Issue 3, July 2024.*
- [8] *Application Notes for Configuring Remote Workers with Avaya Session Border Controller 8.1 on the Avaya Aura® Platform – Issue 1.0*

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/businesspartner/index.html>

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

11. Appendix - 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, etc.). The Cox Managed CPE's sample configuration included in this document is used during this compliance testing.

11.1. 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 10.33.10.49 in the same subnet mask, for example 10.33.10.60

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 68 – Cox Managed CPE Login

- Enter **User Name** and **Password** field
- Click **OK** and the system page should be appeared next

11.2. 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: 10.10.80.103** (Provide this IP Address to service provider to set up the connectivity)
 - **Subnet Mask: 255.255.255.128**
- Network Settings:
 - **Default Gateway: 10.10.80.1**

Submit the changes.



Network

[Help](#)

Networking configuration information for the public and private networks.

Configuration Menu

- + [Admin](#)
- + [Network](#)
- + [NAT](#)
- [VLAN](#)
- [WAN VLAN](#)
- [802.1X Supplicant](#)
- [High Availability](#)
- + [DHCP Relay](#)
- + [DHCP Server](#)
- + [Traffic Shaper](#)
- + [Pass-Through Rules](#)
- [Subinterfaces](#)
- [Proxy ARP](#)
- [Switch Ports](#)
- [Static Routes](#)
- [Dynamic DNS](#)
- [Network Information](#)
- [Network Restart](#)
- [Network Test Tools](#)
- + [WAN Failover](#)
- [Router Advertisement](#)
- [IP Multicast](#)
- + [Users](#)
- + [Security](#)
- [SD-WAN](#)
- + [VoIP](#)
- + [VPN](#)
- [GRE](#)

LAN Interface Settings:

IP Address:

Subnet Mask:

IPv6 Address/Prefix:

Enable VLAN support:

Default VLAN ID:

[VLAN Configuration](#)

WAN Interface IPv6 Settings:

Select the type of IPv6 WAN Interface to use:

- Disabled
- DHCP
- Static IP (ethernet)
- IPv6 in IPv4 Tunnel
- VLAN

WAN Interface IPv4 Settings:

Select the type of IPv4 WAN Interface to use:

- Disabled
- PPPoE
- DHCP
- Static IP
- VLAN

IP Address:

Subnet Mask:

Network Settings:

Default Gateway:

DNS servers:

Note: In case of dynamic links, if the manual override checkbox is not checked the address provided will be used.

Manually set DNS:

Primary DNS Server:

Secondary DNS Server:

Figure 69 – Cox Managed CPE Network Configuration

11.3. 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.

ribbon **VLAN Configuration** Help

VLAN Configuration allows the user to configure VLAN support.
 Note - Changes to this page may require additional changes to the 'VLAN Membership' and 'VLAN Port' pages.

| [Create/Edit VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN Configuration								
Select: All None Delete								
	VLAN ID	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Prefix	Virtual IPv4 Address	Virtual IPv6 Address	Isolate VLAN
<input type="checkbox"/>	1	10.33.10.60	255.255.255.0					N

Create a new VLAN

Action: [Add new VLAN](#) ▾

VLAN ID:

IPv4 Address:

Subnet Mask:

IPv6 Address:

IPv6 Prefix:

Addresses for [High Availability](#)

Virtual IPv4 Address:

Virtual IPv6 Address:

Isolate VLAN from other VLANs

[Add](#) [Reset](#)

Figure 70 – Cox Managed CPE VLAN Configuration

11.4. 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-XXXXXX.TC.AT.COX.NET**
- **SIP Server Port: 5060**
- **SIP Server Transport: Pass Through**
- Check **Use Custom Domain**
- **SIP Server Domain: coxbusiness.com**

Submit the changes.

The screenshot displays the 'SIP Settings' configuration page in the Ribbon interface. On the left, the 'Configuration Menu' is visible, with 'VoIP' and 'SIP' highlighted. The main content area is titled 'SIP Settings' and includes a 'Help' link in the top right. Below the title, there is a section for 'SIP protocol settings' and a descriptive paragraph: 'The SIP Server settings specify the address and port that all client traffic shall be forwarded to.' The configuration fields are as follows:

SIP Server Address:	DUKEBWSSCM-MTC1-SA-XXXXXX.TC.AT.COX.NET
SIP Server Port:	5060
SIP Server Transport:	Pass Through
Use Custom Domain:	<input checked="" type="checkbox"/>
SIP Server Domain:	coxbusiness.com
List of SIP Servers:	Create
Enable Multi-homed Outbound Proxy Mode:	<input type="checkbox"/>
Enable Transparent Proxy Mode:	<input type="checkbox"/>
Limit Outbound to listed SIP Servers:	<input checked="" type="checkbox"/>
Limit Inbound to listed SIP Servers:	<input checked="" type="checkbox"/>
Include UPDATE In Allow:	<input checked="" type="checkbox"/>
PRACK Support:	<input checked="" type="checkbox"/>
GEOLOCATION Support:	<input type="checkbox"/>
Call Audit Support:	<input type="checkbox"/>
Enable Sub Domain Pass Through support:	<input type="checkbox"/>

Figure 71 – Cox Managed CPE VoIP Settings

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

The screenshot shows the 'Survivability' configuration page in the Ribbon interface. On the left is a 'Configuration Menu' with 'Survivability' highlighted. The main content area includes a description of Survivability, a 'Current Status' section with a table of SIP Server Reachability, and a 'Remote' field.

Configuration Menu

- + Admin
- + Network
- + Users
- + Security
- SD-WAN
- VoIP
 - H.323
 - + SIP
 - **Survivability**
 - Clients List
 - Test UA
- + VPN
- GRE

Survivability

Survivability is a collection of features that enable the system to extend the availability of VoIP services. These features include support for redundant Softswitches/IP PBX's and local call control in the event of WAN link failure, Softswitch/IP PBX failure, or during periods of network congestion that result in loss of connectivity to a remote Softswitch/IP PBX. [Click here for more.](#)

Current Status

SIP Server Reachability:

	Domain	Name	Address	Port	P	W	Transport	Lost	Rcvd	Status
●	DUKEBWSSCM-MTC1-SA-XXXXXX.TC.AT.COX.NET	DVTCBWSSCM03-MTC1-SA-XXXXXX.TC.PH.COX.NET	192.168.115.74	5060	20	50	PassThrough	0	0	Active

SIP Server Update Received at 9:51:28 PM

Current Call Control is:

Figure 72 – Cox Managed CPE SIP Server Survivability

11.5. B2BUA Trunking Configuration

From the **Configuration Menu**, select **VoIP** menu option → **SIP** → **B2BUA**.

Under **Trunking Devices**:

- Input a recognizable **Name** for the trunking device: **Avaya**
- At **Model** pull down menu, choose **Avaya IP Office**
- Input **IP Address** of the Avaya IP Office server: **10.33.10.59**
- Input **SIP Port** of the Avaya IP Office: **5060**
- Select **Transport** as **UDP**
- Input **Username**: **402XXX6211**, which is pilot number for trunk registration to Cox Communications system
- Input **Password**: **xxxxxxxxxx**, which is provided by Cox Communications

Select **Update** button to create trunking device.

Under **Credentials and Registration**:

- Input **Username** as **402XXX6211**
- Input **Auth-User** as **402XXX6211**
- Input **Password** and **Confirm Password**: **xxxxxxxxxx**, same as Trunking Devices session above

Select **Update** button.

When the trunk is successfully registered to Cox Communications system, **Status** will be shown as **OK**.

Configuration Menu

- + Admin
- + Network
- + Users
- + Security
- **VOIP**
 - SIP
 - ALG
 - **B2BUA**
 - Trunking_Group
 - Availability
 - Media_Server
 - Survivability
 - Clients_List
 - Test_UA
- + VPN
- GRE

B2BUA Trunking Configuration Help

This page supports only IPv4 addressing.
 In order for changes to this page to be applied, you must click the "Submit" or "Apply Later" button at the bottom of the page

Trunking Devices

Name	Address	Port	Group	Username	Registration Status	Transport
✖ Avaya	10.33.10.59	5060		402XXX6211	Registered	UDP
New Entry						

Name: Model:

Address(IP/FQDN): Use DNS SRV:

Port: Transport:

Source FQDN: Ignore alias source:

Username: Password:

Authenticate Registration:

Terminate Hold Reinvite:

Credentials and Registration

AOR	Auth-User	Password	Registrar	Status	Transport
✖ 4025066211	402XXX6211	is set	default	OK	UDP
✖ default	402XXX6211	is set			
New Entry					

Credentials

Username: Auth-User:

Edit Password:

Password:

Confirm Password:

Use as default:

Figure 73 – Cox Managed CPE SIP Trunk Configuration

The following captured screens show the rest of the B2BUA Trunking Configuration page, continue from above screen. Detail configuration is not discussed here.

Actions

	Name	Send	Prio	Hunt	Request Header	Response Header	Refer-To-ReINV	Message Translation
✖	InboundAction	✓						
✖	OutboundAction	✓			✓			

New Entry

Name:

Send To: Trunking Device:

Client:

URI:

Response:

Prioritize: Refer to Re-INVITE:

Serial Hunting:

E.164 Conversion rule: Conversion mode:

Header Manipulations: Request Response

	Header	Value
Header:	<input type="text" value="Request-URI"/> <input type="button" value="v"/>	<input type="button" value="Add"/>
Value:	<input type="text"/>	

Message Translation:

Incoming Message		Outgoing Message	
Message Type	SDP Presence	Send Message	Message Type
		New Entry	
Incoming Message		Outgoing Message	
Message Type:	<input type="text" value="180 Ringing"/>	Message Type:	<input type="text" value="180 Ringing"/>
SDP Presence:	<input type="text" value="Present"/>	SDP Presence:	<input type="text" value="Present"/>
		Send Message:	<input type="text" value="Yes"/>
<input type="button" value="Add/Edit"/>			

Figure 74 – Cox Managed CPE Inbound Action Configuration

Actions							
Name	Send	Prio	Hunt	Request Header	Response Header	Refer-To-ReINV	Message Translation
<input checked="" type="checkbox"/> InboundAction	<input checked="" type="checkbox"/>						
<input checked="" type="checkbox"/> OutboundAction	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>			
New Entry							
Name:	<input type="text" value="OutboundAction"/>						
Send To:	<input checked="" type="radio"/> Trunking Device: <input type="text" value="None"/>						
	<input type="radio"/> Client: <input type="text"/>						
	<input type="radio"/> URI: <input type="text"/>						
	<input type="radio"/> Response: <input type="text"/>						
Prioritize:	<input type="checkbox"/>		Refer to Re-INVITE: <input type="checkbox"/>				
Serial Hunting:	<input type="text"/>		<input type="button" value="Add"/> <input type="text"/>				
			<input type="button" value="Delete"/>				
E.164 Conversion rule:	<input type="text" value="None"/>		Conversion mode: <input type="button" value="Add"/>				
Header Manipulations:	<input checked="" type="radio"/> Request <input type="radio"/> Response						
Header	Value						
<input checked="" type="checkbox"/>	Contact 'sip:' + \$contact.uri.user + ';tgrp=tg1320393862011;trunk-context=coxbusiness.com@' + \$env.out_intf_host + ':' + \$env.out_intf_port + ';transport=udp;user=phone'						
Header:	<input type="text" value="Request-URI"/>						<input type="button" value="Add"/>

Figure 75 – Cox Managed CPE Outbound Action Configuration

Match												
Direction	Mode	Def	Called		Calling		Privacy		Display Name		Source	Action
			Match	Pattern	Match	Pattern	Match	Pattern	Match	Pattern		
<input checked="" type="checkbox"/> Inbound	BothModes	✓									Any	InboundAction
<input checked="" type="checkbox"/> Outbound	BothModes				matches	.					Any	OutboundAction
New Entry												
Direction:	Inbound											
Mode:	BothModes											
<input checked="" type="radio"/> default												
<input type="radio"/> Pattern:												
	<input type="checkbox"/> Called Party :	matches										
	<input type="checkbox"/> Calling Party:	matches										
	<input type="checkbox"/> Privacy Hdr.:	matches										
	<input type="checkbox"/> Calling Display Name:	matches										
Source:	Any											
Action:	InboundAction											
Update												

Figure 76 – Cox Managed CPE Inbound Match Configuration

Match												
Direction	Mode	Def	Called		Calling		Privacy		Display Name		Source	Action
			Match	Pattern	Match	Pattern	Match	Pattern	Match	Pattern		
<input checked="" type="checkbox"/> Inbound	BothModes	✓									Any	InboundAction
<input checked="" type="checkbox"/> Outbound	BothModes				matches	.					Any	OutboundAction
New Entry												
Direction:	Outbound											
Mode:	BothModes											
<input type="radio"/> default												
<input checked="" type="radio"/> Pattern:												
	<input type="checkbox"/> Called Party :	matches										
	<input checked="" type="checkbox"/> Calling Party:	matches										
	<input type="checkbox"/> Privacy Hdr.:	matches										
	<input type="checkbox"/> Calling Display Name:	matches										
Source:	Any											
Action:	OutboundAction											
Update												

Figure 77 – Cox Managed CPE Outbound Match Configuration

11.6. Trunking Group Configuration

From the **Configuration Menu**, select **VoIP** menu option → **SIP** → **Trunking Group**.

Under **Create New Routing Group**

- Input a recognizable **Name** for the trunking Group: **Avaya**
- Input IP Address of **10.33.10.59**
- Click on **Create** and **Save**



The screenshot shows the 'Trunking Group Availability' page in the Ribbon configuration tool. On the left is a 'Configuration Menu' with options like Admin, Network, Users, Security, VoIP, SIP, ALG, B2BUA, Trunking Group, and Availability. The 'Trunking Group' option is selected. The main area is titled 'Create New Routing Group' and contains a form with a 'Name' field (containing 'Avaya'), a 'Select group members:' section with a table, and a 'Create' button. The table has columns for 'Name' and 'Address'.

	Name	Address
<input type="checkbox"/>	Avaya	10.33.10.59

Figure 78 – Cox Managed CPE Trunking Group

©2024 Avaya LLC All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.