



DevConnect Program

Application Notes for Configuring Avaya IP Office Release 11.1 to support Cox Communications SIP Trunking Service using UDP/RTP - Issue 1.0

Abstract

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

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

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

Cox Communications is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between Cox Communications and Avaya IP Office Release 11.1. In the sample configuration, the Avaya IP Office Server Edition solution consists of the Primary Server running the Avaya IP Office Server Edition Linux software Release 11.1, Avaya IP Office Server Edition Expansion System (IP500 V2), Avaya Voicemail Pro, WebRTC and one-X Portal services enabled, Avaya Communicator for Web, Avaya Workplace for Windows, Avaya H.323 and Avaya SIP Deskphones, digital and analog endpoints. 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 10 Appendix** for more information).

The Cox Communications Enterprise SIP Trunking Service 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 simulate an enterprise site in the DevConnect Program by connecting IP Office to Cox Communications' SIP Trunking service across the public internet. The configuration in **Figure 1** was used to exercise the features and functionality tests listed in **Section Error! Reference source not found.**

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 and Cox Communications 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 Release 11.1 was connected to Cox Communications. To verify SIP trunking interoperability, the following features and functionality were exercised during the interoperability compliance test:

- Response to SIP OPTIONS queries
- 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 Client for Windows (SIP)
- Inbound and outbound PSTN calls from/to the Avaya Communicator for Web (WebRTC) with basic telephony transfer feature
- Inbound and outbound long hold time call stability
- Various call types including: local, long distance, international call, inbound toll-free, outbound toll-free, outbound calls to Assisted Operator, 411 Local Directory Assistance call, 911 Emergency call during the compliance testing
- SIP transport UDP/RTP between Cox Communications and the simulated Avaya enterprise site
- Codec G.711MU
- Caller number/ID presentation
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls
- DTMF transmission using RFC 2833
- Voicemail navigation for inbound and outbound calls
- Telephony features such as hold and resume, transfer, and conference
- Fax T.38 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 IP Office and Cox Managed CPE.

Items not supported included 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 SIP Trunking Service 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 illustrates the test configuration. The test configuration shows an enterprise site connected to the Cox Communications network through the public internet. For confidentiality and privacy purposes, actual public IP addresses 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 includes:

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

Located at the enterprise site are Primary Server and the Cox managed CPE. The Primary Server consists of a Dell PowerEdge R640 server, running the Avaya IP Office Server Edition Linux software Release 11.1. Avaya Voicemail Pro runs as a service on the Primary Server. The LAN1 port of the Primary Server (Eth0) is connected to the enterprise LAN (Private network) and the Cox managed CPE LAN.

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 IP500V2 with the MOD DGTL STA16 expansion module which provides connections for 16 digital stations, the PHONE 8 card which provides connections for 8 analog stations, as well as a 64-channel VCM (Voice Compression Module) for supporting VoIP codecs.

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

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

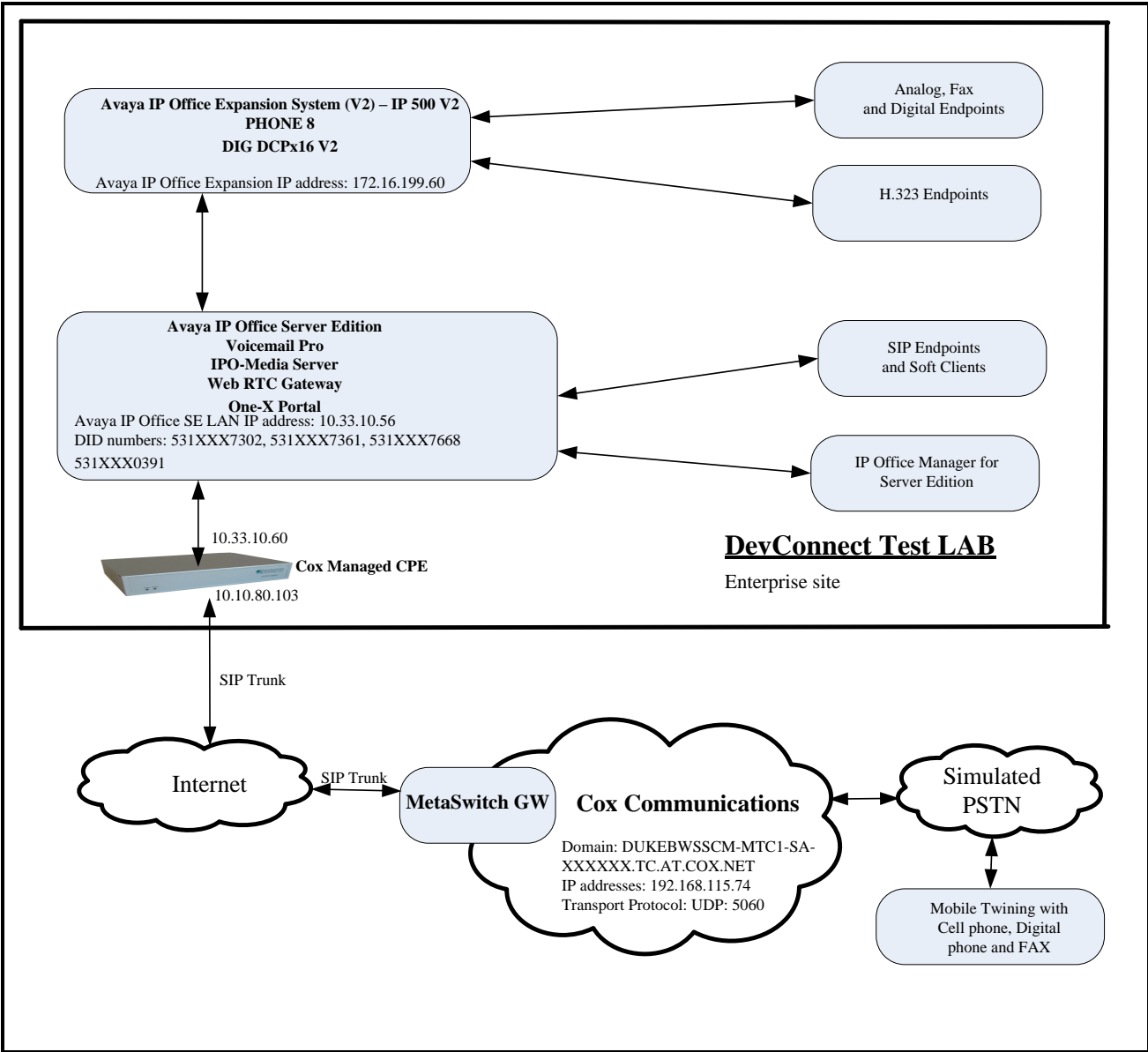


Figure 1 - Test Configuration for Avaya IP Office with Cox Communications SIP Trunk Service

Inbound calls from the service provider via the SIP trunk arrive to the Server Edition Primary Server, where Incoming Call Routes are checked to determine the call destination. In the event that the destination of the incoming call is an endpoint in the Expansion System (IP500 V2), the call is sent via the Small Community Network (SCN) H.323 trunk (IP Office Line) to the expansion IP500V2 for routing to the final endpoint. This SCN H.323 trunk is automatically created during the initial process of addition of the Expansion System to the IP Office Server Edition solution.

Similarly, outbound calls from the enterprise to the PSTN are routed via the SIP trunk to the Cox Communications. Calls originated from extensions registered to the Primary Server are routed directly to Cox Communications network, while calls originated from extensions on the Expansion System are sent to the Primary Server via SCN H.323 trunk, before being routed to Cox Communications via the SIP trunk.

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 IP Office Server Edition, 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 IP Office Server Edition 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 ▪ Web RTC Gateway ▪ one-X Portal ▪ IP Office Manager for Server Edition ▪ IP Office Expansion System (V2) – IP 500 V2 ▪ IP Office Analogue - PHONE 8 ▪ IP Office Digital - DIG DCPx16 V2 	11.1.2.4.0 build 18 11.1.2.4.0 build 18 11.1.2.4.0 build 2 11.1.2.3.0 build 2 11.1.2.4.0 build 3 11.1.2.4.0 build 18 11.1.2.4.0 build 18 11.1.2.4.0 build 18
Avaya 1140E IP Deskphone (SIP)	04.04.33
Avaya 9641G IP Deskphone (H323)	6.8.5.3.2
Avaya 9621G IP Deskphone (H323)	6.8.5.3.2
Avaya J129 IP Deskphone (SIP)	4.0.7.1.5
Avaya Communicator for Web	1.0.20.1722
Avaya Workplace Client for Windows	3.34.1.10
Avaya 1408D Digital Deskphone	R48
Avaya Analog Deskphone	N/A
VentaFax	7.10.258.664
Cox Communications	
Cox managed CPE (Edgewater EdgeMarc 2900E SIP Application-Layer Gateway)	15.8.2
MetaSwitch GW	4.3.40

Table 1: Equipment and Software Tested

Note – Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2, and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks.

5. Configure Avaya IP Office Server Edition Solution

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

This section describes the Avaya IP Office Server Edition configuration to support connectivity to Cox Communications system. 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.

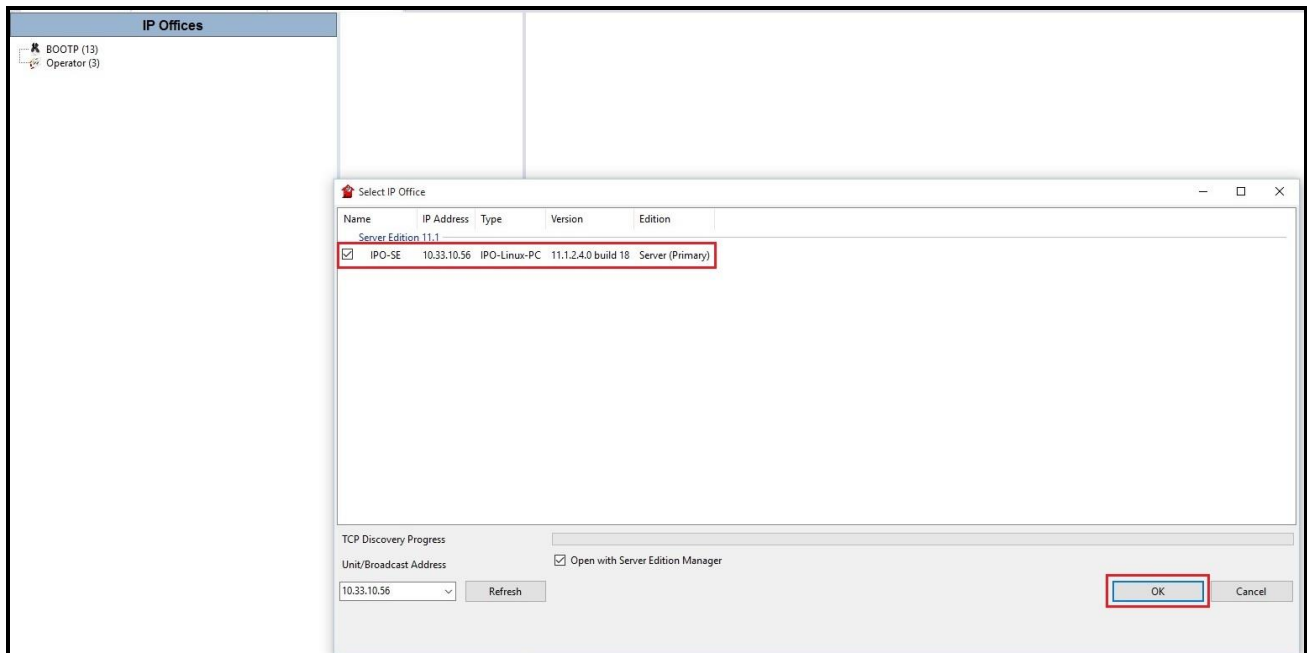


Figure 2 – Avaya IP Office Server Edition Selection

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.

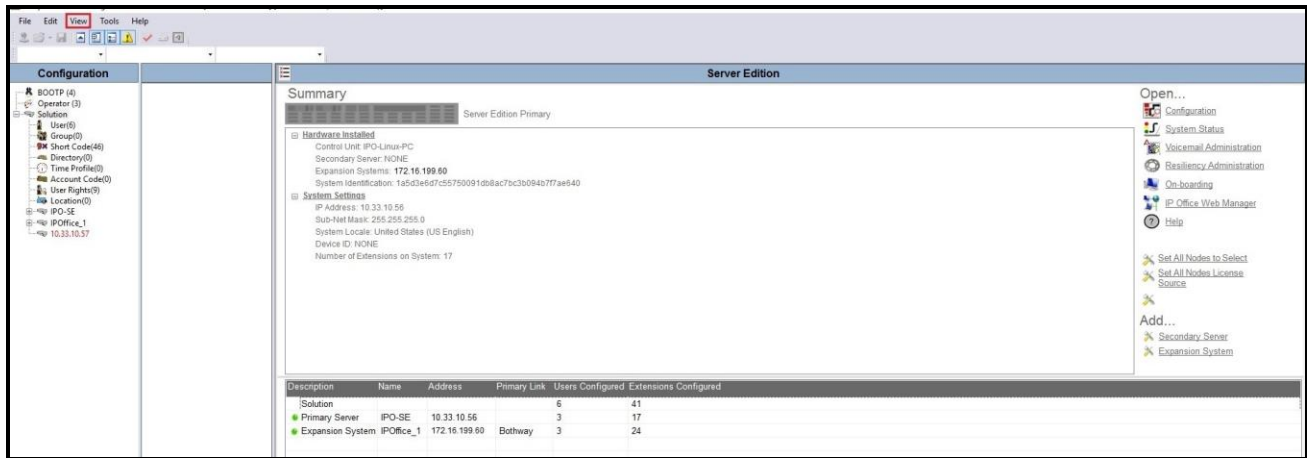
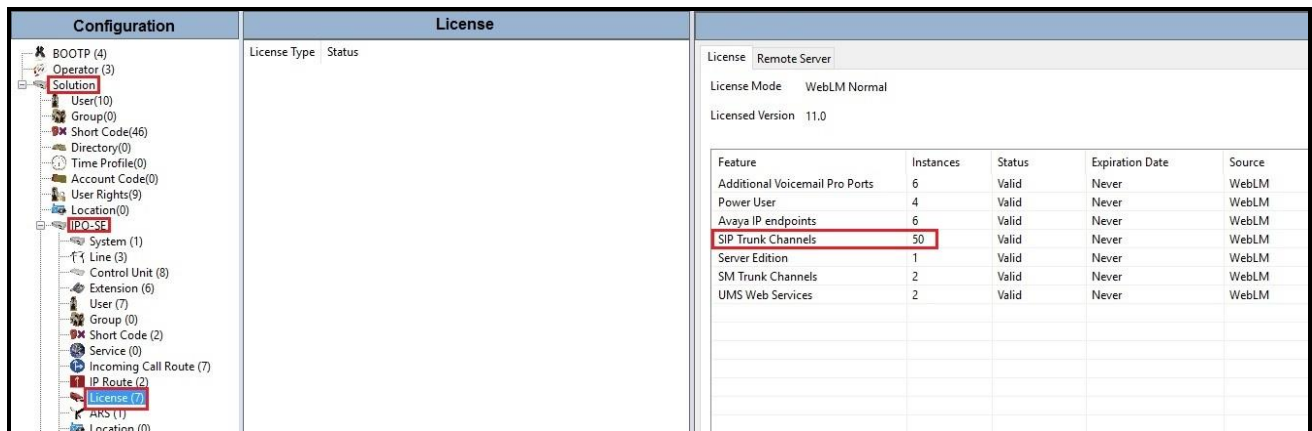


Figure 3 – Avaya IP Office Server Edition View Menu

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.



The screenshot shows the Avaya IP Office configuration interface. On the left is a navigation tree with 'Solution' expanded to 'IPO-SE' and 'License' selected. The main area is divided into 'Configuration' and 'License' panes. The 'License' pane shows a table of license details.

Feature	Instances	Status	Expiration Date	Source
Additional Voicemail Pro Ports	6	Valid	Never	WebLM
Power User	4	Valid	Never	WebLM
Avaya IP endpoints	6	Valid	Never	WebLM
SIP Trunk Channels	50	Valid	Never	WebLM
Server Edition	1	Valid	Never	WebLM
SM Trunk Channels	2	Valid	Never	WebLM
UMS Web Services	2	Valid	Never	WebLM

Figure 4 – Avaya IP Office Server Edition License

5.2. System Settings

Configure the necessary system settings.

5.2.1. System – LAN Tab

In the sample configuration, LAN1 on the Primary Server was used, and LAN1 on the Expansion System was used. Note: The LAN1 port of the Primary Server (Eth0) is connected to the enterprise LAN (Private network) and Cox managed CPE. The **IPO-SE** was used as the Primary Server name and **IPOffice_1** was used as the Expansion System name.

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.

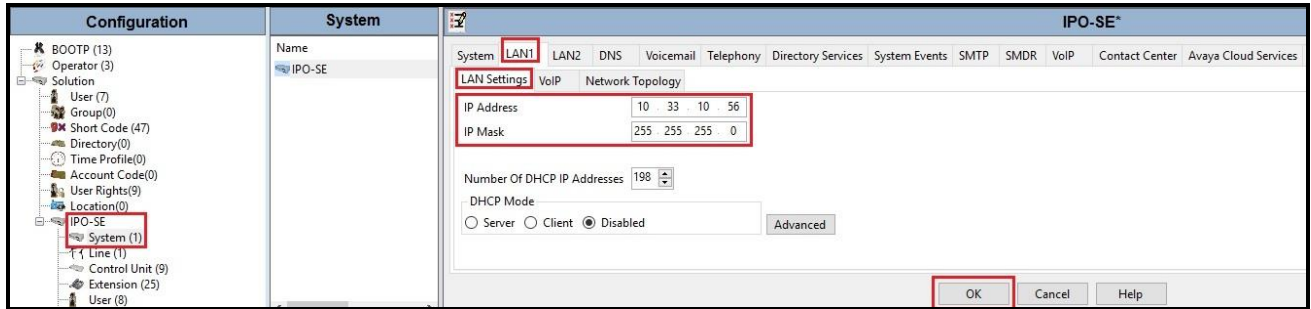


Figure 5 - Avaya IP Office Primary Server LAN1 Settings

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 Cox Communications system
- 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

The screenshot displays the configuration interface for IPO-SE*. The 'LAN1' tab is active, and the 'VoIP' sub-tab is selected. The configuration is as follows:

- H.323 Gatekeeper Enable** (checked)
- Auto-create Extension** (unchecked)
- Auto-create User** (unchecked)
- H.323 Remote Extension Enable** (checked)
- H.323 Signaling over TLS**: Disabled
- Remote Call Signaling Port**: 1720
- SIP Trunks Enable** (checked)
- SIP Registrar Enable** (checked)
- Auto-create Extension/User** (unchecked)
- SIP Remote Extension Enable** (unchecked)
- Allowed SIP User Agents**: Block blacklist only
- SIP Domain Name**: 10.33.10.56
- SIP Registrar FQDN**: 10.33.10.56
- Layer 4 Protocol**:
 - UDP** (checked): UDP Port 5060, Remote UDP Port 5060
 - TCP** (checked): TCP Port 5060, Remote TCP Port 5060
 - TLS** (checked): TLS Port 5061, Remote TLS Port 5061
- Challenge Expiration Time (sec)**: 10
- RTP**:
 - Port Number Range**: Minimum 40750, Maximum 50750
 - Port Number Range (NAT)**: Minimum 40750, Maximum 50750
 - Enable RTCP Monitoring on Port 5005** (checked)
 - RTCP collector IP address for phones**: 0.0.0.0
- Keepalives**:
 - Scope**: RTP-RTCP
 - Periodic timeout**: 60
 - Initial keepalives**: Enabled

The **OK** button is highlighted in red.

Figure 6 - 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.

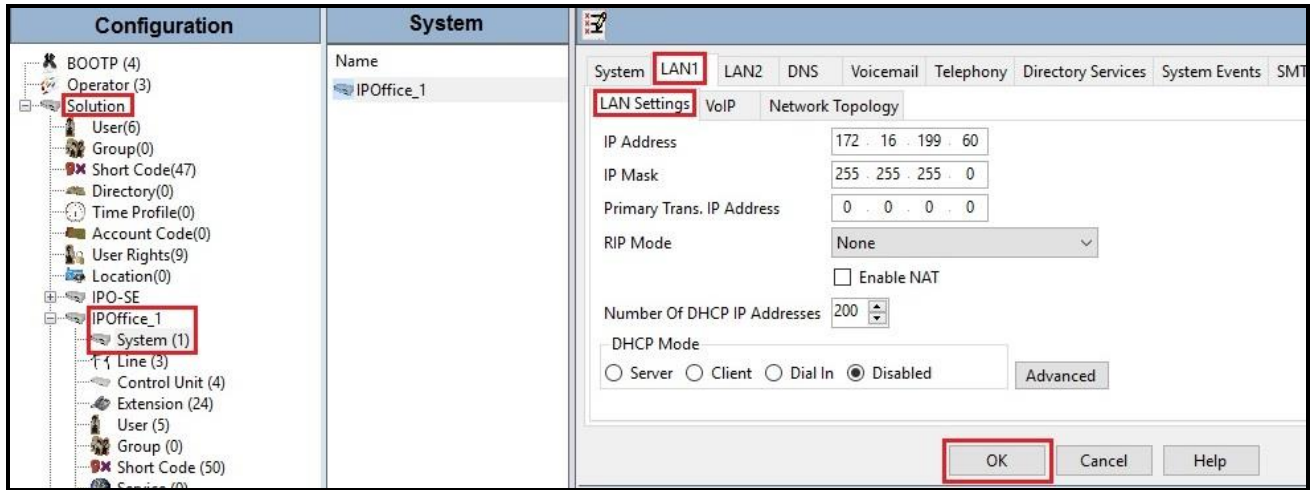


Figure 7 - Avaya IP Office Expansion Server Settings

The **VoIP** tab for LAN1 in the Expansion System (not shown) can be configured using the same values previously described for the **VoIP** tab in the Primary Server.

5.2.2. System – Telephony Tab

Navigate to **Solution → IPO-SE → System (1)** in the Navigation and Group Panes (not shown) and then navigate to the **Telephony → Telephony** tab in the Details Pane. Choose the **Companding Law** typical for the enterprise location. For North American area, **U-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the service provider across the SIP trunk. The Hold Timeout (sec) field controls how long calls remain on hold before being alerted to the user and should be set based on the customer's requirement. Set **Default Name Priority** to **Favor Trunk** to have IP Office display the name provided in the Caller ID from the SIP trunk. Defaults were used for all other settings. Click **OK** to submit the changes.

The screenshot shows the Avaya IP Office Primary Server Telephony configuration window. The window title is "IPO-SE". The "Telephony" tab is selected. The "Companding Law" section is expanded, showing "U-Law" selected under "Switch" and "U-Law Line" selected under "Line". The "Inhibit Off-Switch Forward/Transfer" checkbox is unchecked. The "Hold Timeout (sec)" field is set to 3600. The "Default Name Priority" dropdown is set to "Favor Trunk". The "OK" button is highlighted with a red box.

Figure 8 - Avaya IP Office Primary Server Telephony

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

5.2.3. System – VoIP Tab

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** (Not shown) to submit the changes.

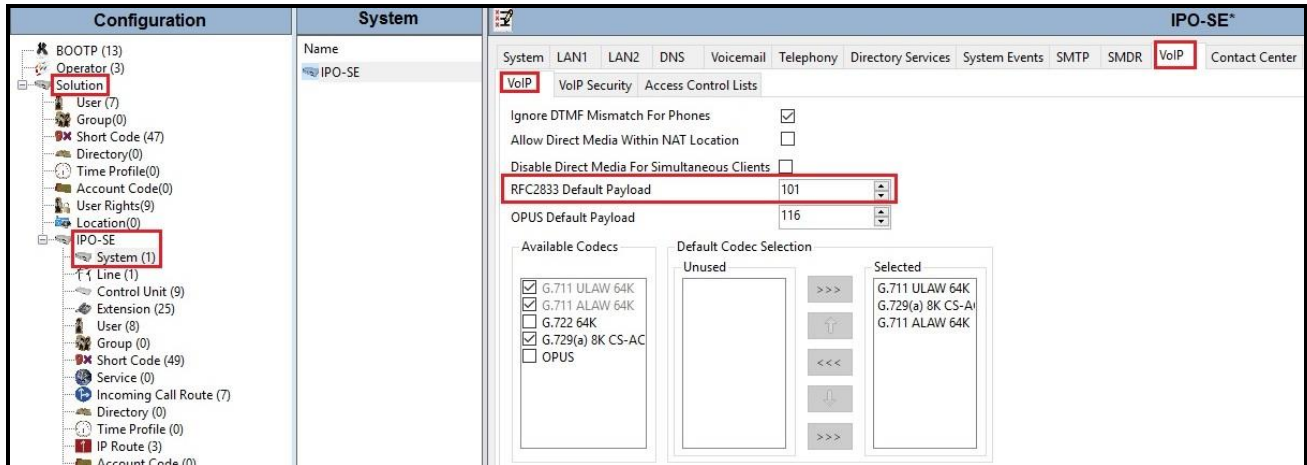


Figure 9 - Avaya IP Office Primary Server VoIP

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

5.3. IP Route

Create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to route calls to Cox Communications.

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

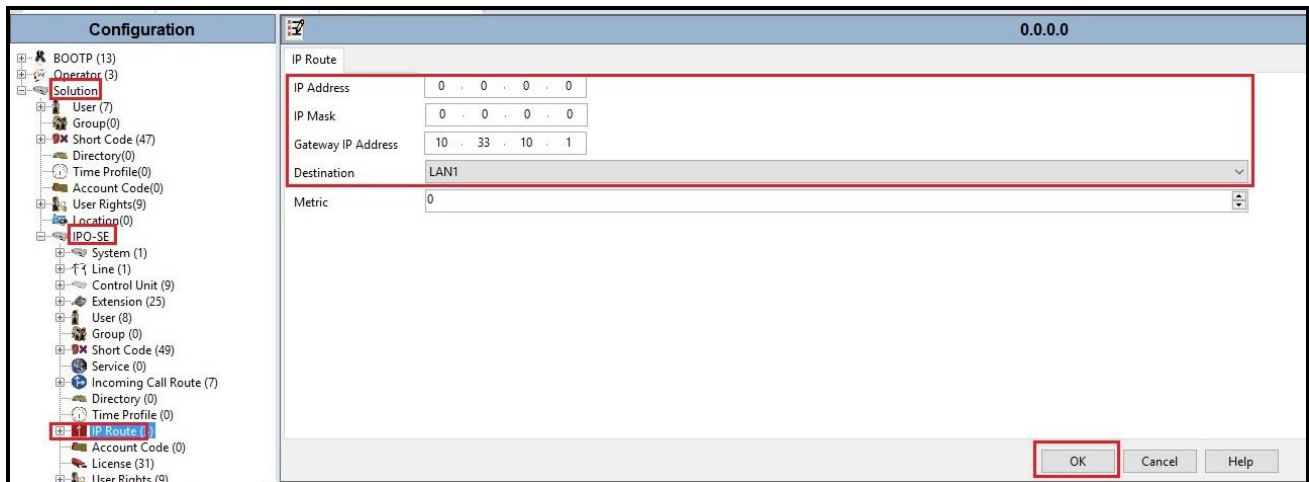


Figure 10 - Avaya IP Office Primary Server IP Route

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

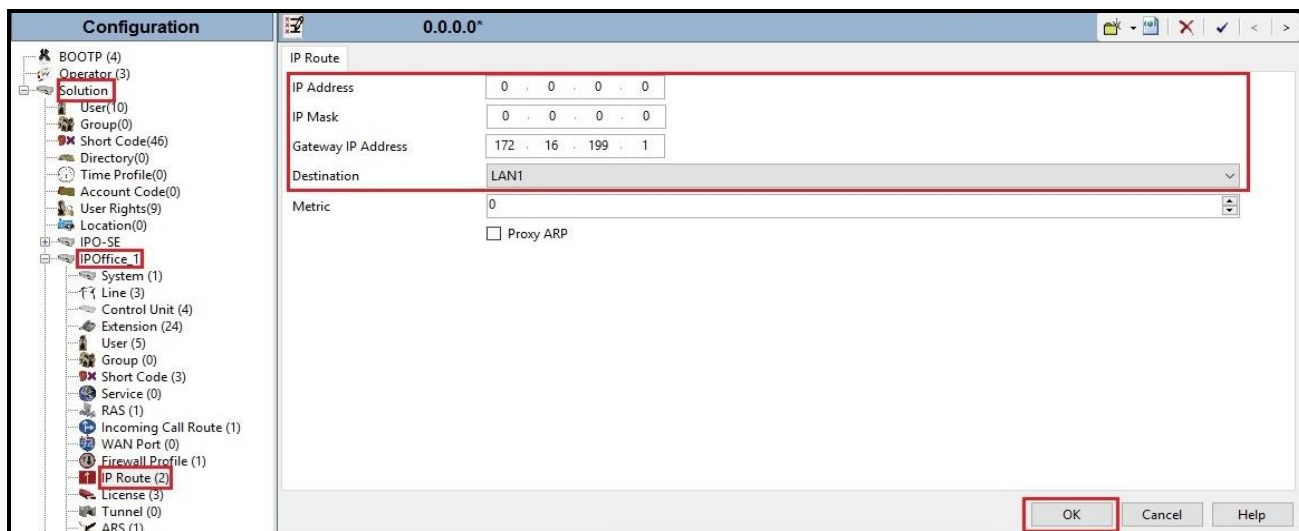


Figure 11 - Avaya IP Office Expansion Server IP Route

5.4. Administer SIP Line

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

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

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

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

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 5.4.2**.

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

5.4.1. 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 **Cox_IPO11_1.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**.

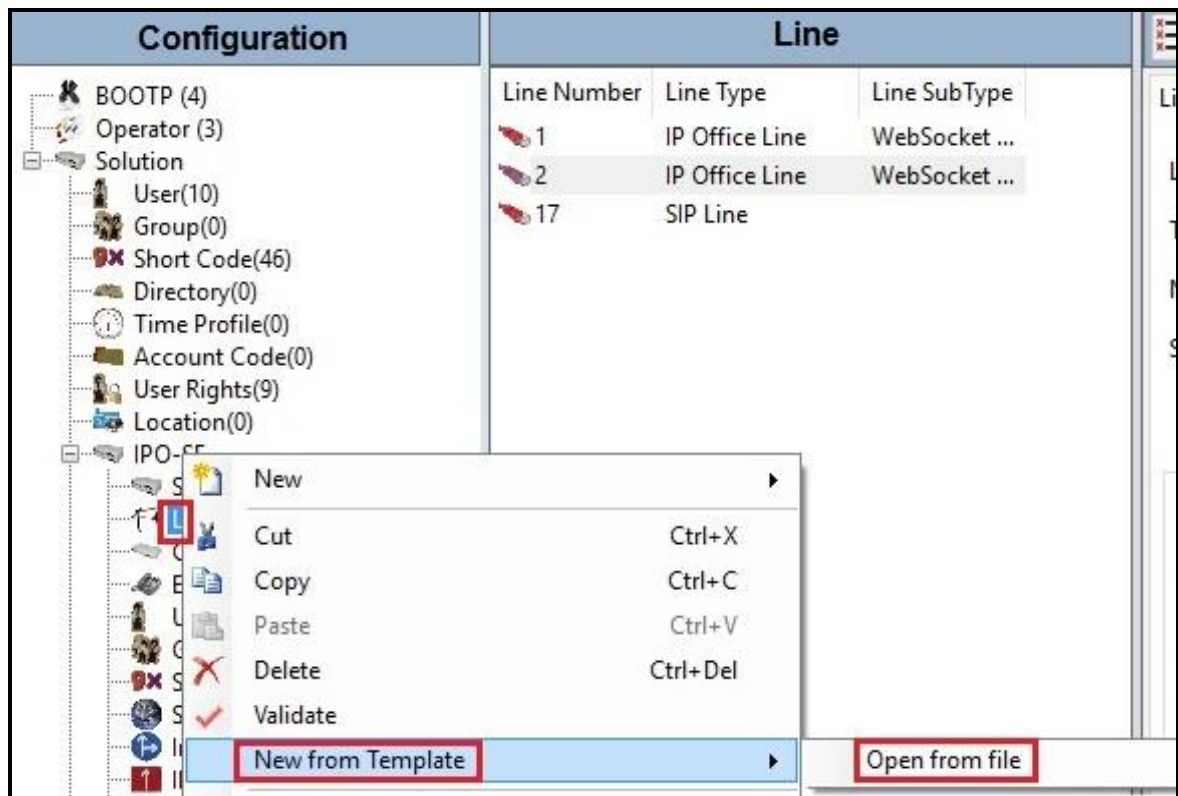


Figure 12 – Create SIP Line from an XML Template

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.

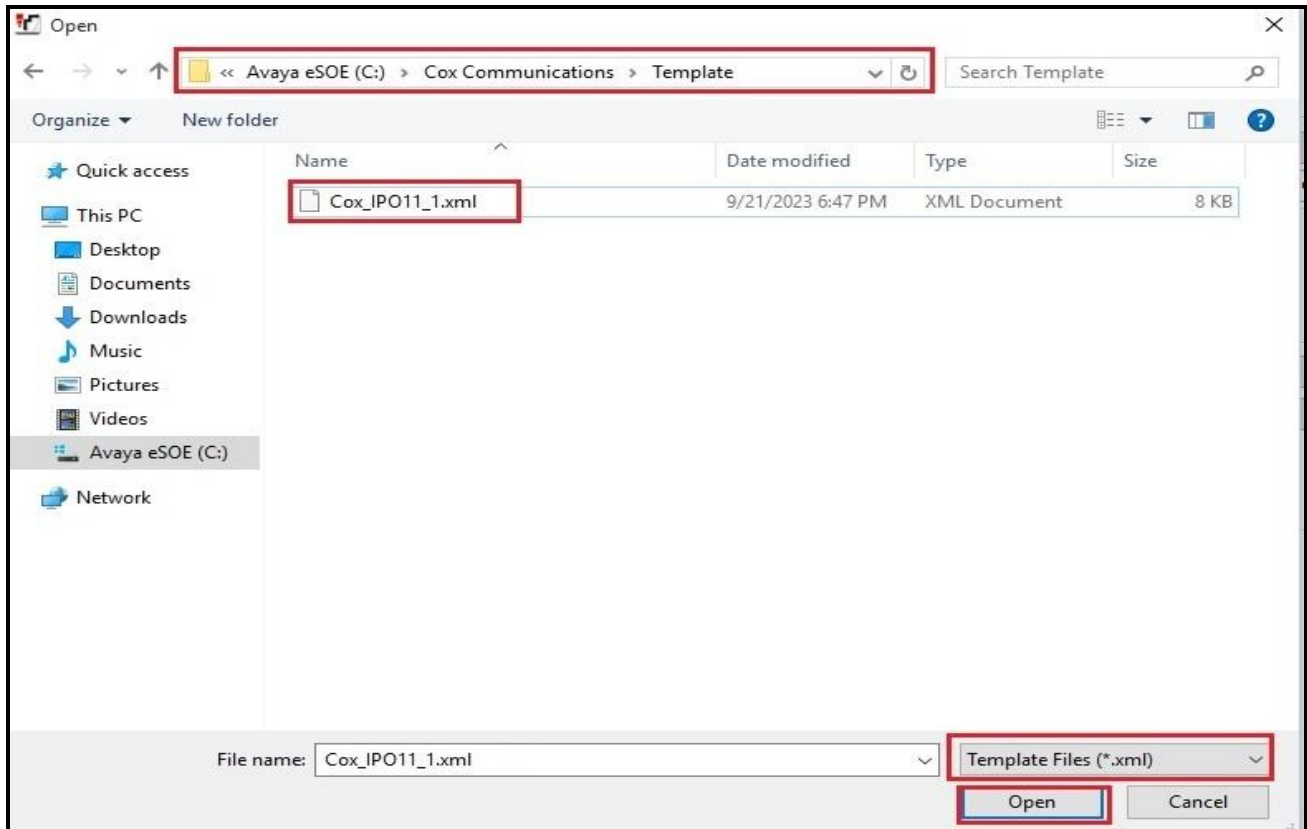


Figure 13 – Create SIP Line from directory

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



Figure 14 – 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 5.4.2**.

5.4.2. Create SIP Line Manually

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

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

- Select available **Line Number: 17**
- Set **ITSP Domain Name** to the IP address of Cox managed CPE LAN port. This field is used to specify the default host part of the SIP URI in the To and R-URI fields for outgoing calls
- Leave **Local Domain Name** to IP address of Avaya IP Office SE LAN1 port
- Check the **In Service** and **Check OOS** boxes
- 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 5.2.2**, 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

Field	Value
Line Number	17
ITSP Domain Name	10.33.10.60
Local Domain Name	10.33.10.56
URI Type	SIP URI
Location	Cloud
In Service	<input checked="" type="checkbox"/>
Check OOS	<input checked="" type="checkbox"/>
Session Timers - Refresh Method	Auto
Session Timers - Timer (sec)	On Demand
Name Priority	Favor Trunk
Redirect and Transfer - Incoming Supervised REFER	Never
Redirect and Transfer - Outgoing Supervised REFER	Never
Send 302 Moved - Temporarily	<input type="checkbox"/>
Send 302 Moved - Outgoing Blind REFER	<input type="checkbox"/>

Figure 15 – 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 Cox managed CPE LAN port: **10.33.10.60**. This is the SIP Proxy IP address used for outgoing SIP calls
- In the **Network Configuration** area, **UDP** was selected as the **Layer 4 Protocol** and the **Send Port** was set to **5060**
- The **Use Network Topology Info** parameter was set to **None**. The **Listen Port** was set to **5060**. 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
- 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 with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '10.33.10.60'. The 'Network Configuration' section shows 'Layer 4 Protocol' set to 'UDP', 'Send Port' set to '5060', and 'Use Network Topology Info' set to 'None'. The 'Listen Port' is also set to '5060'. The 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0' and '0 . 0 . 0 . 0'. The 'Calls Route via Registrar' checkbox is unchecked. The 'Separate Registrar' field is empty. The 'OK' button is highlighted with a red box.

Figure 16 – SIP Line Transport Configuration

On the **SIP Credentials** tab in the Details Pane, click **Add** button to configure the parameters as shown below:

- **User name:** Set to the value provided by Cox Communications
- **Authentication Name:** Set to the value provided by Cox Communications
- **Contact:** Set to the value provided by Cox Communications
- **Password:** Set to the value provided by Cox Communications
- **Confirm Password:** Set to the value provided by Cox Communications
- **Expiration (mins): 60**
- Check **Registration required** option
- Other parameters retain default values
- Click **OK** to commit then press Ctrl + S to save

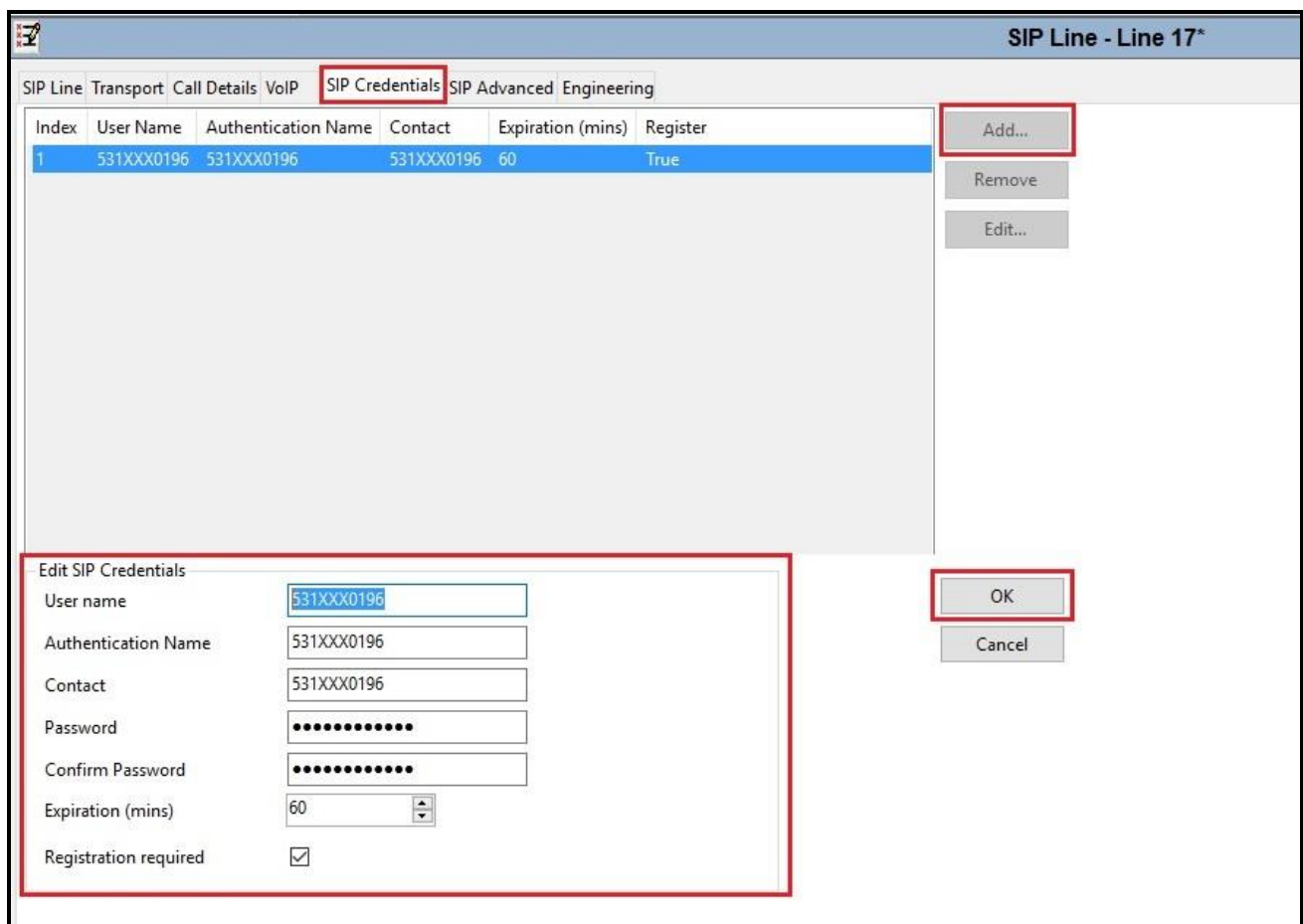


Figure 17 – SIP Line SIP Credentials Configuration

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)
- Select **Credentials** as **1:531XXX0196**
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern
- Check **P Asserted ID** and **Diversion Header** options
- Set the **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** fields to the values shown in the below screenshot
- Click **OK** to submit the changes

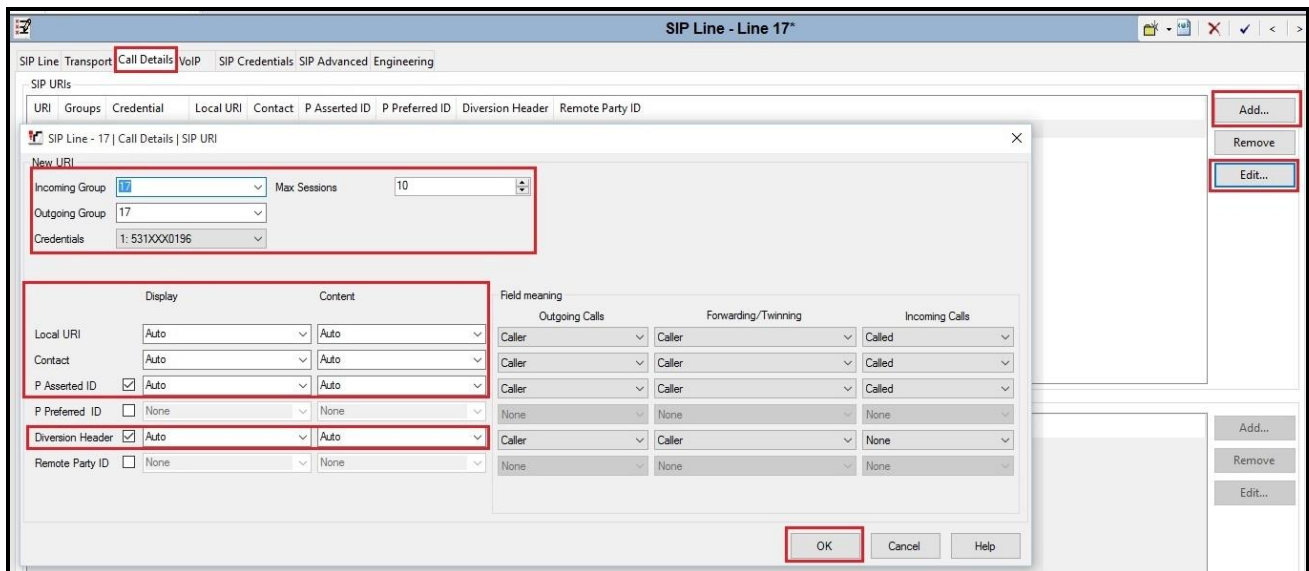


Figure 18 – SIP Line Call Details Configuration

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 supports this codec, which is sent to Cox Communications, in the Session Description Protocol (SDP) offer
- Check the **Re-invite Supported** box
- Set **Fax Transport Support** to **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
- Default values may be used for all other parameters
- Click **OK** to submit the changes

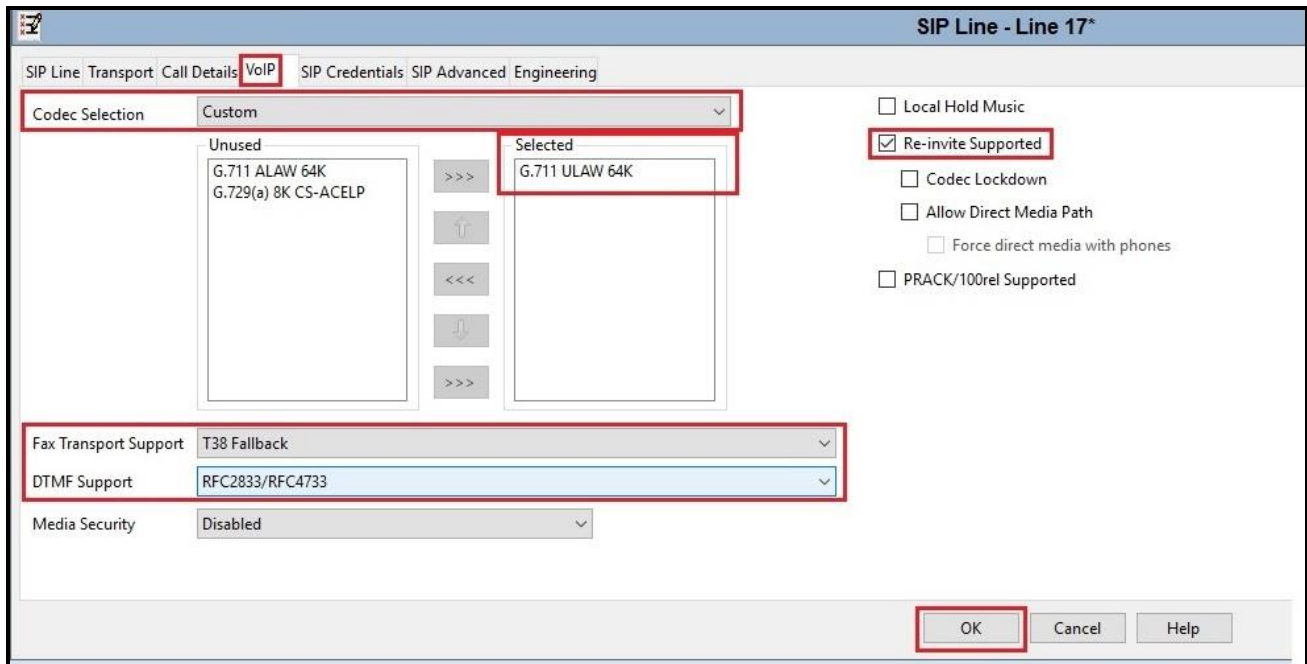


Figure 19 – SIP Line VoIP Configuration

5.5. 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**.

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'Configuration' tree with 'Line' selected under 'IP Office Line'. The middle pane shows a table of lines:

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

The right pane shows the configuration for 'IP Office Line - Line 2'. Key settings are highlighted with red boxes:

- Line Number: 2
- Transport Type: WebSocket Server
- Networking Level: SCN
- Security: Medium
- Outgoing Group ID: 99999
- Gateway Address: 172 . 16 . 199 . 60
- Location: Cloud
- SCN Resiliency Options: Supports Resiliency, Backs up my IP phones, Backs up my hunt groups, Backs up my IP DECT phones

Figure 20 – 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 codecs are **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.

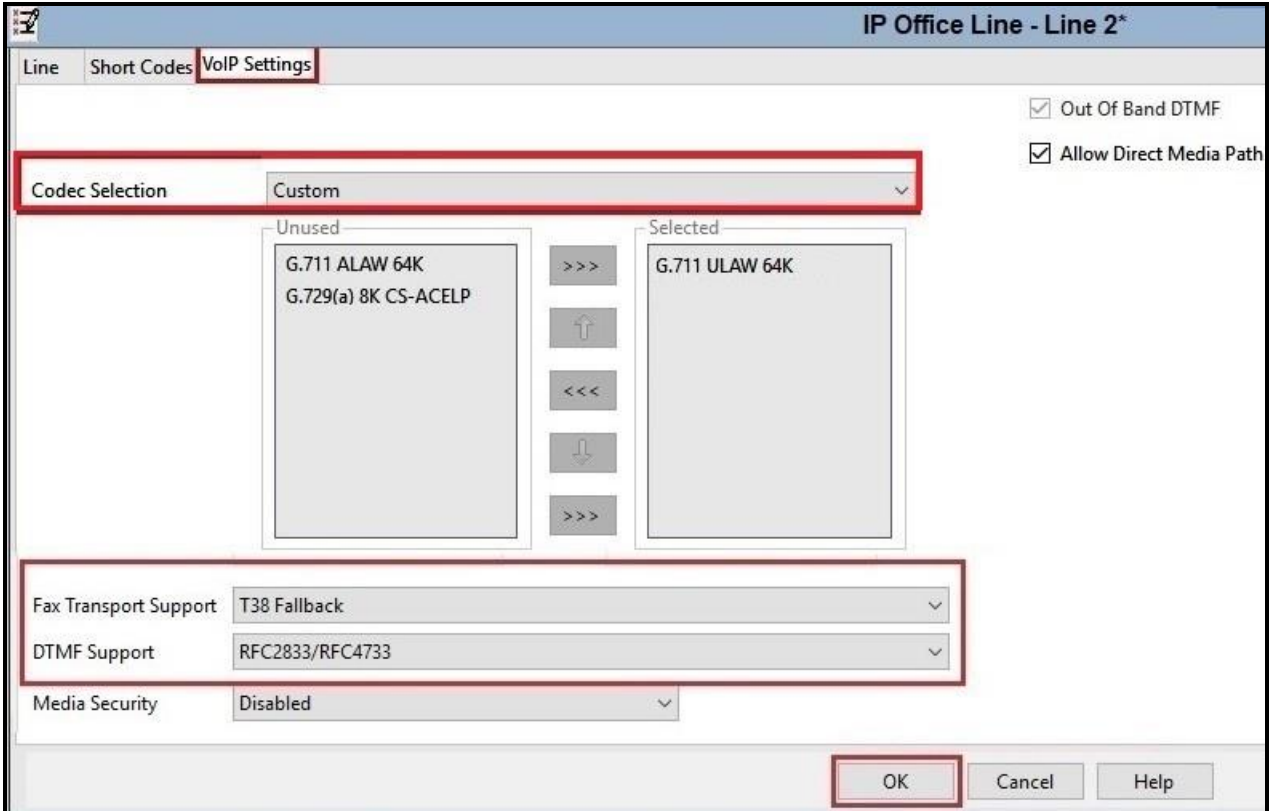


Figure 21 – IP Office Line for Primary System VoIP Settings

5.6. 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**.

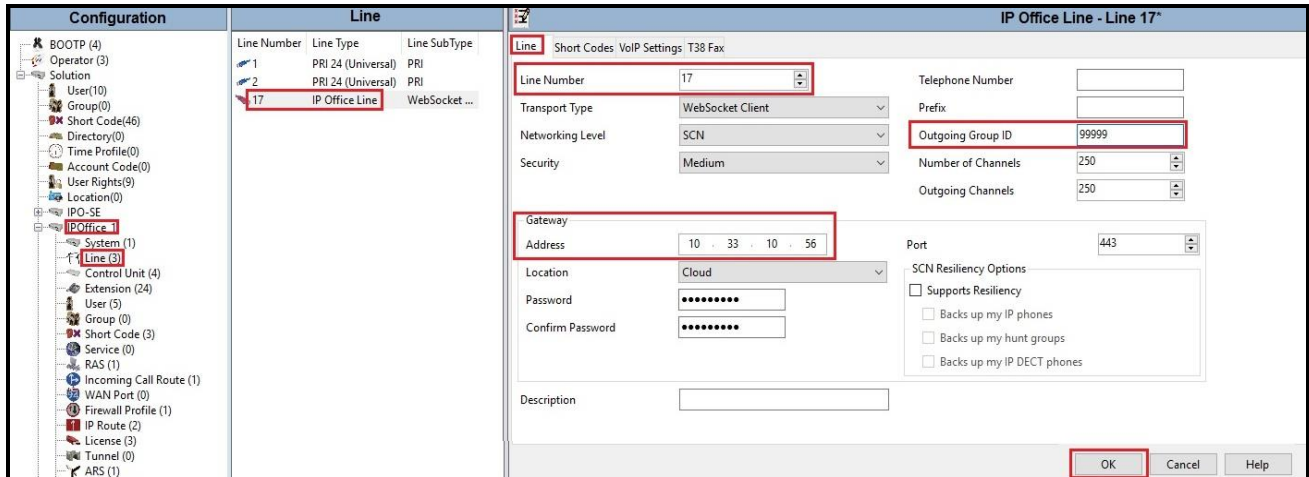


Figure 22 – IP Office Line for Expansion System

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.

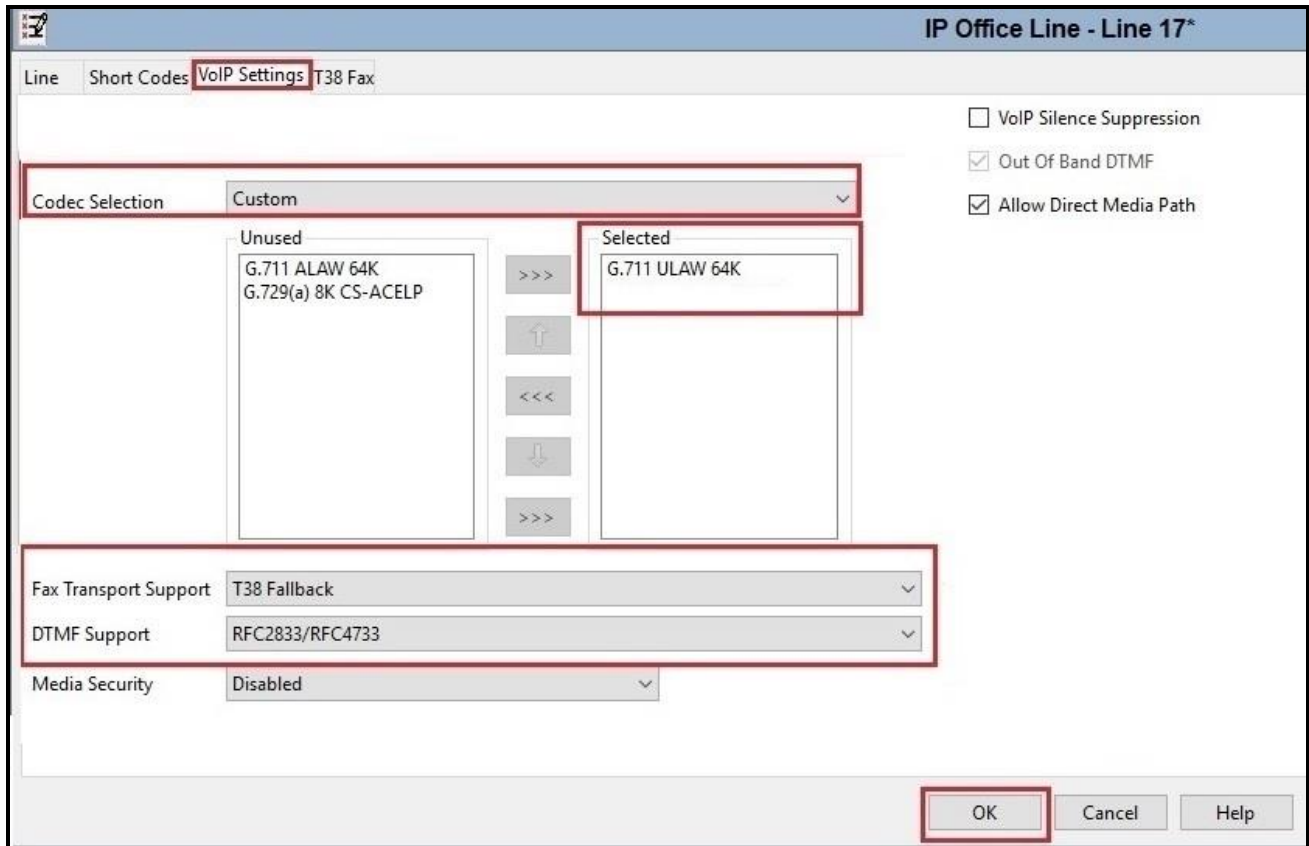


Figure 23 – IP Office Line for Expansion Server VoIP Settings

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.

The screenshot shows the configuration window for 'IP Office Line - Line 17*'. The 'T38 Fax' tab is selected. The 'T38 Fax Version' dropdown is set to '0'. The 'Transport' is set to 'UDPTL'. The 'Redundancy' section has 'Low Speed' and 'High Speed' both set to '0'. The 'TCF Method' is 'Trans TCF', 'Max Bit Rate (bps)' is '14400', 'EFlag Start Timer (ms)' is '2600', 'EFlag Stop Timer (ms)' is '2300', and 'Tx Network Timeout (sec)' is '150'. On the right, several checkboxes are checked: 'Scan Line Fix-up', 'TFOP Enhancement', and 'NSF Override'. Other checkboxes are unchecked: 'Disable T30 ECM', 'Disable EFlags For First DIS', and 'Disable T30 MR Compression'. The 'Country Code' and 'Vendor Code' are both set to '0'. At the bottom left, the 'Use Default Values' checkbox is unchecked. At the bottom right, the 'OK' button is highlighted with a red box.

Figure 24 – IP Office Line for Expansion Server T38 Fax

5.7. 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 5.4.2**. This short code will use this line group when placing the outbound call
- Set the **Locale** to **United States (US English)**
- Default values may be used for all other parameters
- Click **OK** to submit the changes



Figure 25 – Short Code 9N for Primary Server

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

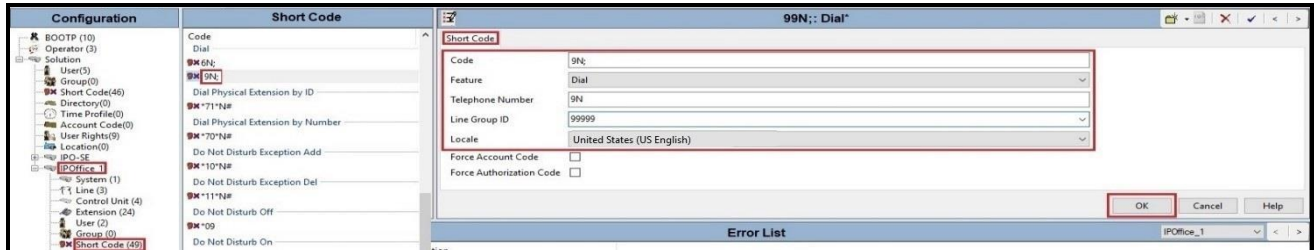


Figure 26 – Short Code 9N for Expansion System

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

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

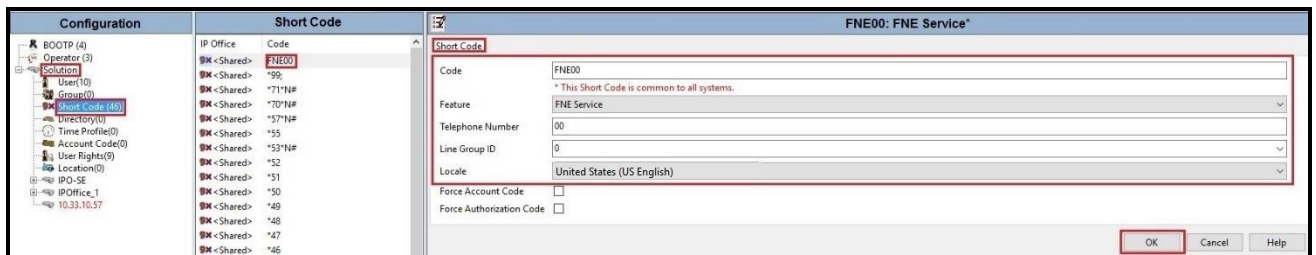


Figure 27 – Short Code FNE

5.8. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.4.2**. 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 **531XXX7302**. Select the **User** tab in the Details pane.

Note: When **Auto** is selected for the **Local URI**, **Contact** and **Diversion Header** parameters (See **Section 5.4.2 - Call Detail** tab), the information in the Incoming Call Route (See **Section 5.9**) is used to populate the SIP From and Contact headers for outbound calls.

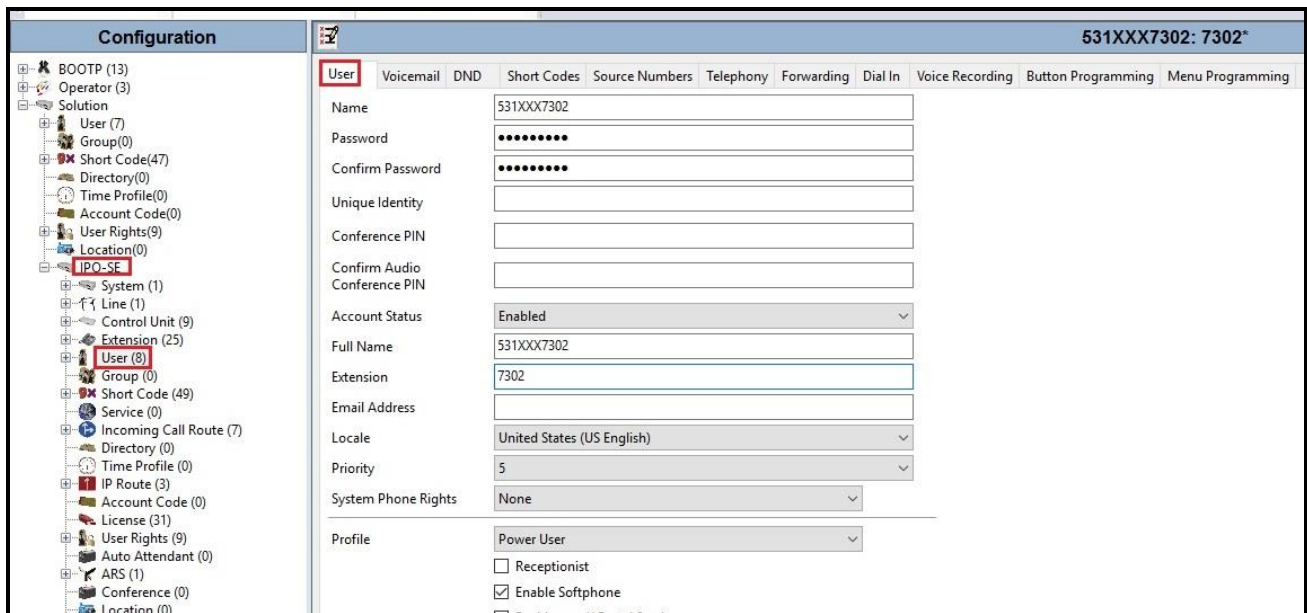


Figure 28 – User Configuration – User Tab

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 **531XXX7302**. 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 5.4.2**. This short code will use this line group when placing the outbound call
- Set the **Locale** to **United States (US English)**
- Default values may be used for all other parameters
- Click **OK** to submit the changes

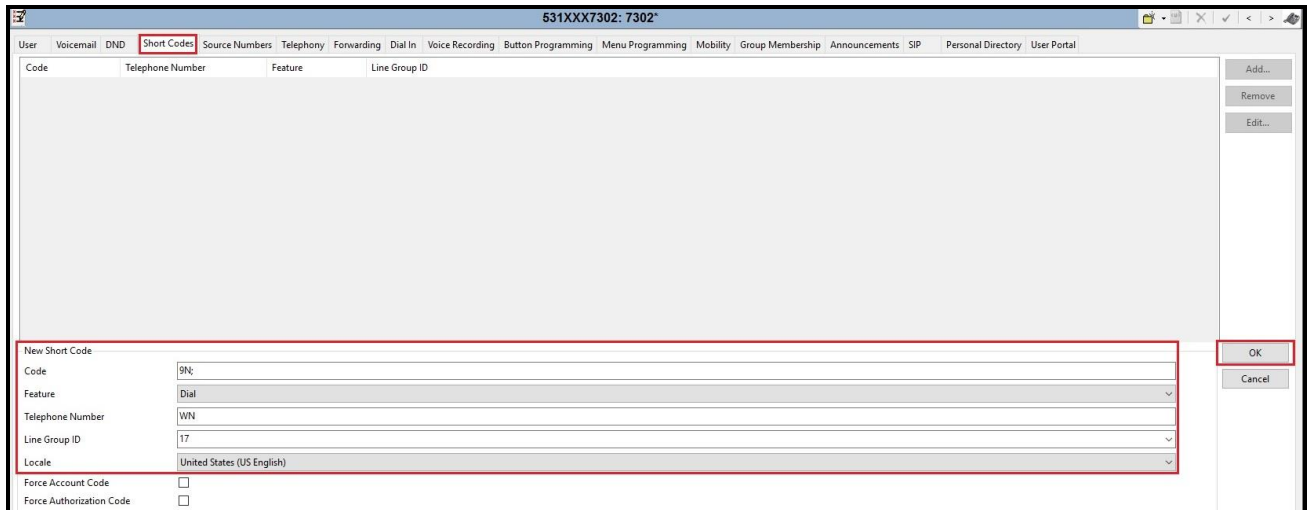


Figure 29 – User Configuration – Short Code tab

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 531XXX7302**. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone, in this case **91613XXX5096**. Check **Mobile Call Control** to allow incoming calls from mobility extension to access FNE00 (Defined in **Section 5.7**). Other options can be set according to customer requirements.

The screenshot shows the configuration page for user 531XXX7302, specifically the Mobility tab. The page title is '613XXX0771: 613XXX0771'. The 'Mobility' tab is active. The configuration is as follows:

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

Figure 30 – Mobility Configuration for User

5.9. Incoming Call Route

An Incoming Call Route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by service provider. To create an incoming call route, select **Incoming Call Route** in the left Navigation Pane, then right-click in the center Group Pane and select **New** (not shown). On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capability** to **Any Voice**
- Set the **Line Group ID** to the **Incoming Group 17** defined on the **Call Details** tab on the **SIP Line** in **Section 5.4.2**
- Set the **Incoming Number** to the incoming DID number on which this route should match
- Default values can be used for all other fields

Configuration		17 531XXX7302
Standard Voice Recording Destinations		
Bearer Capability	Any Voice	
Line Group ID	17	
Incoming Number	531XXX7302	
Incoming Sub Address		
Incoming CLI		
Locale	United States (US English)	
Priority	1 - Low	
Tag		
Hold Music Source	System Source	
Ring Tone Override	None	

Figure 31 – 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 **531XXX7302** on line 17 are routed to **Destination 7302 531XXX7302** as below screenshot:

17 531XXX7302	
Standard Voice Recording Destinations	
TimeProfile	Destination Fallback Extension
Default Value	7302 531XXX7302

Figure 32 – Incoming Call Route for Destination 531XXX7302

For Feature Name Extension Service testing purpose, the incoming calls to DID number **531XXX0391** were configured to access **FNE00**. The **Destination** was appropriately defined as **FNE00** as below screenshot:

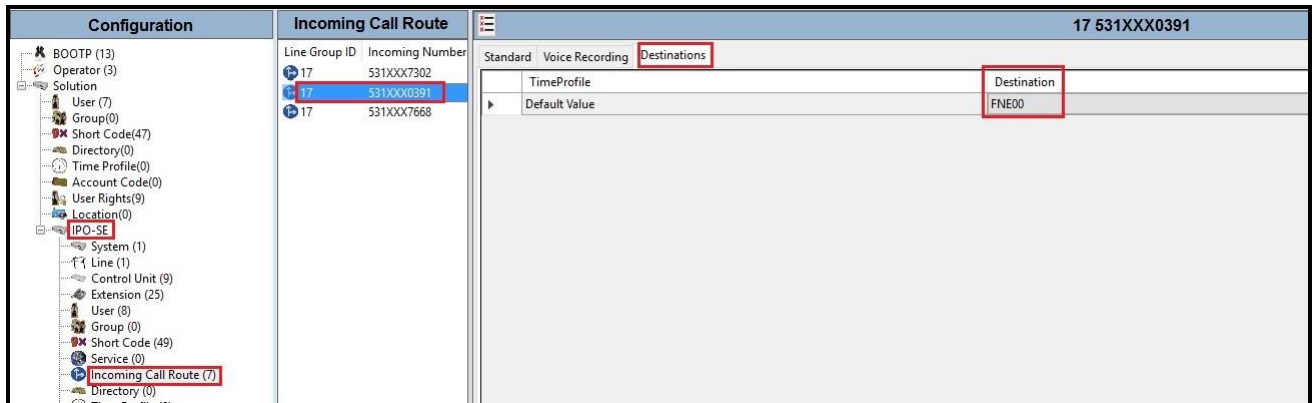


Figure 33 – Incoming Call Route for Destination FNE

For Voice Mail testing purpose, the incoming calls to DID number **531XXX7668** were configured to access **VoiceMail**. The **Destination** was appropriately defined as **VoiceMail** as below screenshot:

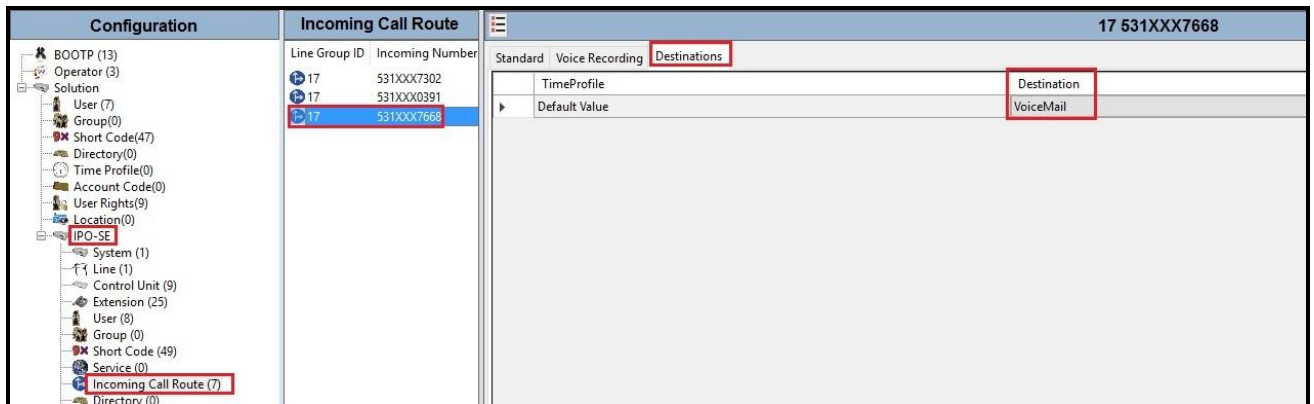


Figure 34 – Incoming Call Route for Destination VoiceMail

5.10. Save Configuration

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

6. 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 IP Office LAN port at the enterprise. Cox Communications will provide the customer necessary information to configure the SIP connection between Avaya IP Office and Cox Communications. The provided information from Cox Communications includes:

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

7. 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.

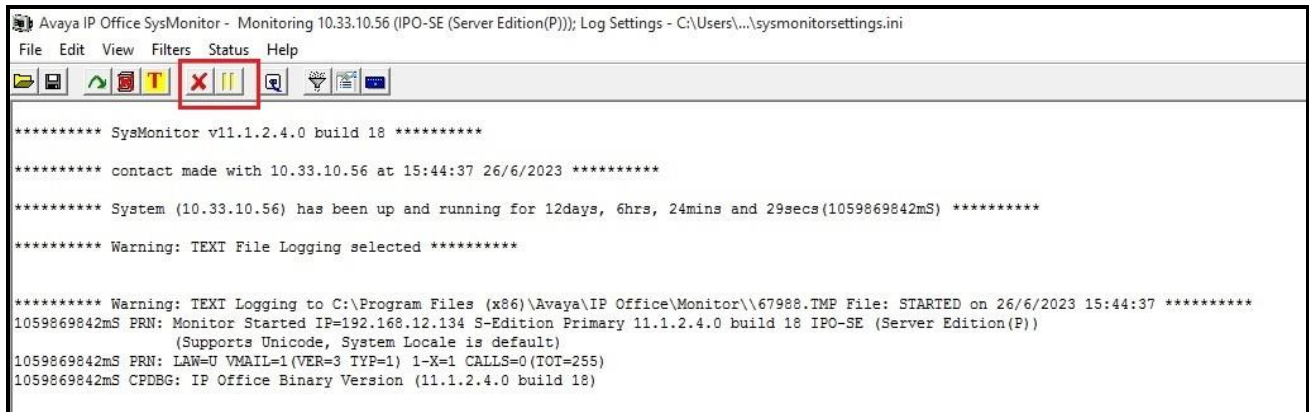


Figure 35 – SIP Trace Monitor

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

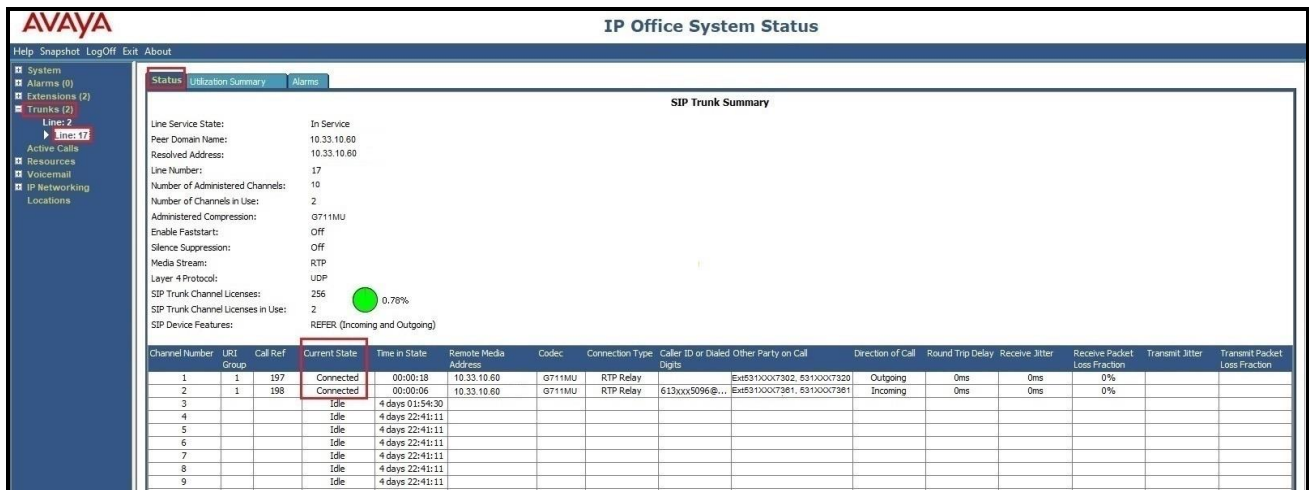


Figure 36 – SIP Trunk status

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

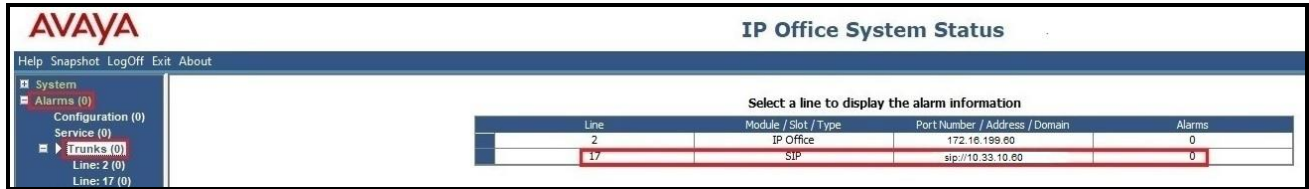


Figure 37 – SIP Trunk alarm

- Verify that a phone connected to the PSTN can successfully place a call to Avaya IP Office Server Edition with two-way audio
- Verify that a phone connected to Avaya IP Office Server Edition can successfully place a call to the PSTN with two-way audio
- Use a network sniffing tool e.g., Wireshark to monitor the SIP signaling between the enterprise and Cox Communications. The sniffer traces are captured at the LAN1 port interface of the Avaya IP Office Server Edition

8. Conclusion

Cox Communications passed compliance testing excepting the limitation in **Section 2.1** and **2.2**. These Application Notes describe the procedures required to configure the SIP connections between Avaya IP Office and the Cox Communications system as shown in **Figure 1**.

9. Additional References

- [1] *Avaya IP Office Technical Bulletin 236 / General Availability (GA)- IP Office Release 11.1.2 Service Pack 4, Issue 2, 08th February 2023*
- [2] *Deploying IP Office Server Edition and Application Servers, Release 11.1 FP2, Issue 26, January 2023*
- [3] *Deploying Avaya IP Office Servers as Virtual Machines, Release 11.1.2.4, Issue 13, January 2023*
- [4] *IP Office Platform 11.1, Deploying an IP Office 500 V2/V2A in IP Office Basic Edition Mode, Issue 38e, Monday, February 28, 2022*
- [5] *Administering Avaya IP Office using Manager, Release 11.1.2.4, Issue 43, March 2023.*
Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform, Release 10.1.x, Issue 1, December 2021

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

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

10. 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's responsibility for all the aspect of the Cox managed CPE (i.e., support, detail configuration, maintenance and etc...). The Cox managed CPE's sample configuration included in this document is used during this compliance testing.

10.1. 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:

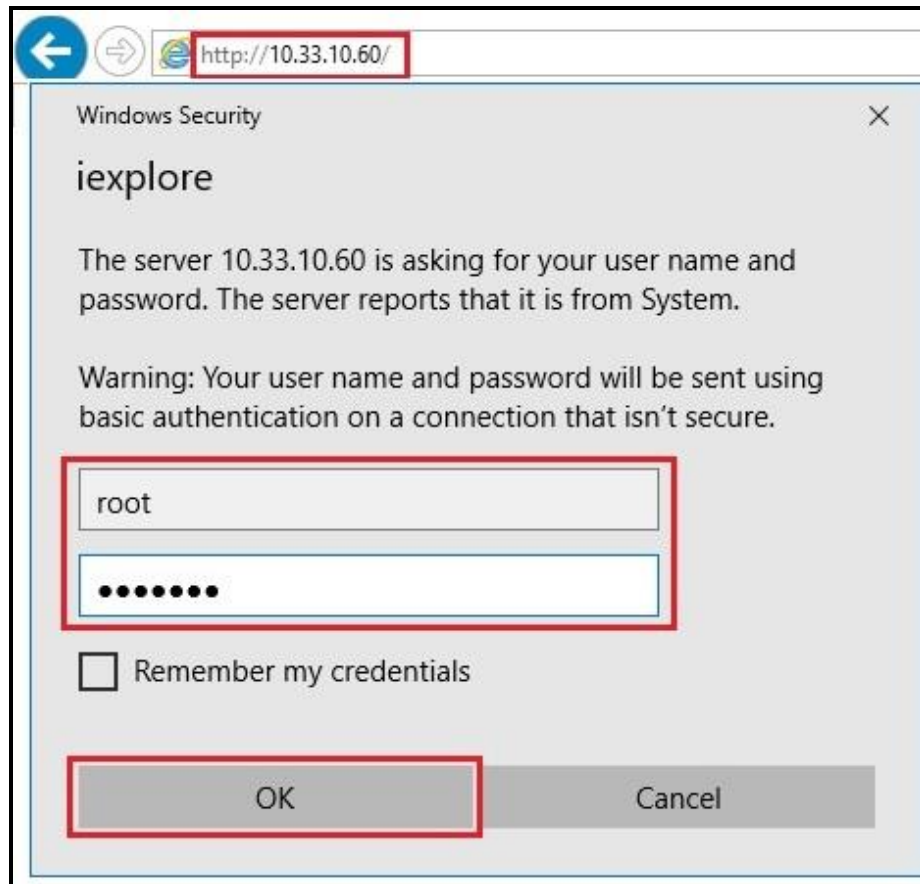


Figure 38 – Cox managed CPE Login

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

10.2. 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 39 – Cox managed CPE Network Configuration

10.3. 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 40 – Cox managed CPE VLAN Configuration

10.4. 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**
- 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 is a 'Configuration Menu' with options like Admin, Network, Users, Security, SD-WAN, VoIP, and SIP. The main content area is titled 'SIP Settings' and includes a 'Help' link. Below the title, it states 'SIP protocol settings.' and provides a description: '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

Below these fields is a 'List of SIP Servers' section with a 'Create' button. Further down are several checkboxes for advanced settings: 'Enable Multi-homed Outbound Proxy Mode', 'Enable Transparent Proxy Mode', 'Limit Outbound to listed SIP Servers', 'Limit Inbound to listed SIP Servers', 'Include UPDATE In Allow', 'PRACK Support', 'GEOLOCATION Support', 'Call Audit Support', and 'Enable Sub Domain Pass Through support'.

Figure 41 – 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.

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 42 – Cox managed CPE SIP Server Survivability

10.5. B2BUA Trunking Configuration

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

Under **Trunking Devices**:

- Input a recognizable **Name** for the trunking device: **AvayaIPOffice11**
- At **Model** pull down menu, choose **Avaya IP Office**
- Input **IP Address** of the Avaya IP Office server: **10.33.10.56**
- Input **SIP Port** of the Avaya IP Office: **5060**
- Select **Transport** as **UDP**
- Input **Username**: **531XXX0196**, 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 **531XXX0196**,
- Input **Auth-User** as **531XXX0196**
- 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
- + SD-WAN
- + VoIP
- SIP
- H.323
- ALG
- B2BUA
- Trunking_Group
- Availability
- Media Server
- Survivability
- Clients List
- Test UA
- + VPN
- GRE

Trunking Devices

Name	Address	Port	Group	Username	Registration Status	Transport
✖ AvayaIPOffice	10.33.10.56	5060		531XXX0196	Registered	UDP
New Entry						

Name: Model:

Address(IP/FQDN): Use DNS SRV:

Port: Transport:

Source FQDN:

Username: Password:

Authenticate Registration:

Credentials and Registration

AOR	Auth-User	Password	Registrar	Status	Transport
✖ 531XXX0196	531XXX0196	is set	default	OK	UDP
✖ default	531XXX0196	is set			
New Entry					

Credentials

Username: Auth-User:

Edit Password:

Password:

Confirm Password:

Use as default:

Registrar

Figure 43 – 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	Header	Refer-To-ReINV
✘	InboundAction	✓				
✘	OutboundAction	✓			✓	
<i>New Entry</i>						

Name:

Send To: Trunking Device:

Client:

URI:

Response:

Prioritize: Refer to Re-INVITE:

Serial Hunting:

E.164 Conversion rule: Conversion mode:

Header Manipulations:

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

Figure 44 – Cox managed CPE Inbound Action Configuration

Actions						
	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
✘	InboundAction	✓				
✘	OutboundAction	✓			✓	
New Entry						
Name:	OutboundAction					
Send To:	<input checked="" type="radio"/> Trunking Device:		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:	None		Conversion mode: <input type="button" value="Add"/>			
Header Manipulations:						
	Header	Value				
✘	Contact	'<sip:' + \$contact.uri.user + ';tgrp=tg1320393862017;trunk-context=coxbusiness.com@' + \$env.out_intf_host + ':' + \$env.out_intf_port + ';transport=udp;user=phone>'				
Header:	Request-URI					<input type="button" value="Add"/>

Figure 45 – Cox managed CPE Outbound Action Configuration

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

Figure 46 – Cox managed CPE Inbound Match Configuration

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

Figure 47 – Cox managed CPE Outbound Action Configuration

©2023 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.