Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Cox Communications SIP Trunking with Avaya IP Office Release 11.0 using UDP/RTP - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Cox Communications and Avaya IP Office Release 11.0.

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 at the Avaya Solution and Interoperability Test Lab.

Avaya DevConnect Confidential & Restricted. For benefit of Cox Communications only. These Application Notes may not be distributed further without written permission from DevConnect.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between Cox Communications and the Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists Avaya IP Office 500 V2 Release 11.0, Avaya embedded Voicemail, Avaya IP Office Application Server (with WebRTC and one-X Portal services enabled), Avaya Communicator for Windows (SIP mode), Avaya Communicator for Web, Avaya Equinox for Windows, Avaya H.323, Avaya SIP, digital and analog endpoints. The enterprise solution connects to the Cox Communications network.

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.

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 IP Office 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 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 Communicator for Windows (SIP)
- Inbound and outbound PSTN calls from/to the Avaya Communicator for Web (WebRTC) with basic telephony transfer feature
- Inbound and outbound PSTN calls from/to the Avaya Equinox for Windows (SIP)
- Inbound and outbound long hold time call stability
- Various call types including: local, long distance, international call, outbound calls to Assisted Operator, outbound toll-free, 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 G.711 pass-through mode
- Off-net call forwarding
- Off-net call transfer
- Twinning to mobile phones on inbound calls
- SIP Trunk registration and authentication

Items not supported or not tested including the following:

- TLS/SRTP SIP transport
- The inbound toll-free service
- Use of the SIP REFER method for network call redirection (transferring calls with the PSTN back to the PSTN)
- Fax T.38 mode

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:

1. ***The EdgeMarc did not forward Diversion header (or PAI header) to Cox Communications network in off-net call forward*** - Although the EdgeMarc did not forward Diversion header (or PAI header) to Cox Communications network in off-net call forward, the off-net call forward still worked. As far as Cox Communications are aware, there should not be anything in the default setup of the EdgeMarc to strip out Diversion header. Cox Communications would need to investigate on this issue further
2. ***Outbound Calling Party Number block (calls with privacy enabled)*** – The Calling Party Number is not blocked on calls from IP Office to the PSTN with privacy enabled at the IP Office station (Withhold Number enabled). This issue is caused by IP Office not including the privacy header (privacy = id) in the INVITE message sent to Cox Communications. This issue is under investigation by Avaya

3. ***Caller ID on calls forwarded to the PSTN and to "twinned" mobile phones*** **–** On calls originated from the PSTN to IP Office stations with either call-forward or with the mobility feature active in the IP Office station to another PSTN number, the caller ID number displays at the terminating PSTN station is always of the DID number assigned to the IP Office station, instead of the originating PSTN number. This issue is caused by IP Office sending INVITE messages to Service Provider for calls being forwarded and for twinned calls to mobile stations with the DID number assigned to the IP Office station in the "From" header instead of sending the PSTN number that originated the call. This issue is under investigation by Avaya

4. ***Conference on Avaya Equinox for Windows soft-client*** – Conference on the Avaya Equinox for Windows soft-client is not working properly. When the attempt is made to conference active calls in the Avaya Equinox for Windows soft-client by "merging" the calls together, the parties are not joined together into conference, instead a new call is made from the first active call that was held by the Equinox soft-client to the second active call held by the Equinox soft-client, with the Avaya Equinox soft-client unable to merge the active calls together into conference. This issue was only seen on the Avaya Equinox for Windows soft-client. There is no current work-around; if the conference feature is needed on an Avaya soft-client for IP Office, the Avaya Communicator for windows soft-client could be use until this issue is resolved by Avaya. This issue is under investigation by Avaya

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 IP network. 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 included:

- Avaya IP Office 500 V2
- Avaya embedded Voicemail for IP Office
- Avaya Application Server (Enabled WebRTC and one-X Portal services)
- Avaya 9600 Series IP Deskphones (H.323)
- Avaya 11x0 Series IP Deskphones (SIP)
- Avaya J129 IP Deskphone (SIP)
- Avaya 1408 Digital phone
- Avaya Analog phone
- Avaya Communicator for Windows (SIP)
- Avaya Communicator for Web (WebRTC)
- Avaya Equinox for Windows

Located at the enterprise site are Cox managed CPE (Edgewater Edgemarc 4550 SIP ALG is included as part of the Service Provider service and not as part of the CPE solution) and an Avaya IP Office 500 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. The voicemail service is embedded on Avaya IP Office. Endpoints include Avaya 9600 Series IP Telephone (with H.323 firmware), Avaya 1100 Series IP Telephone (with SIP firmware), Avaya J129 IP Telephone (with SIP firmware), Avaya 1408D Digital Telephone, Avaya Analog Telephone, Avaya Communicator for Windows/ for Web (WebRTC) and Avaya Equinox for Windows. The LAN1 port of Avaya IP Office is connected to the enterprise LAN (private network) while the LAN2 port is connected to the public network.

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

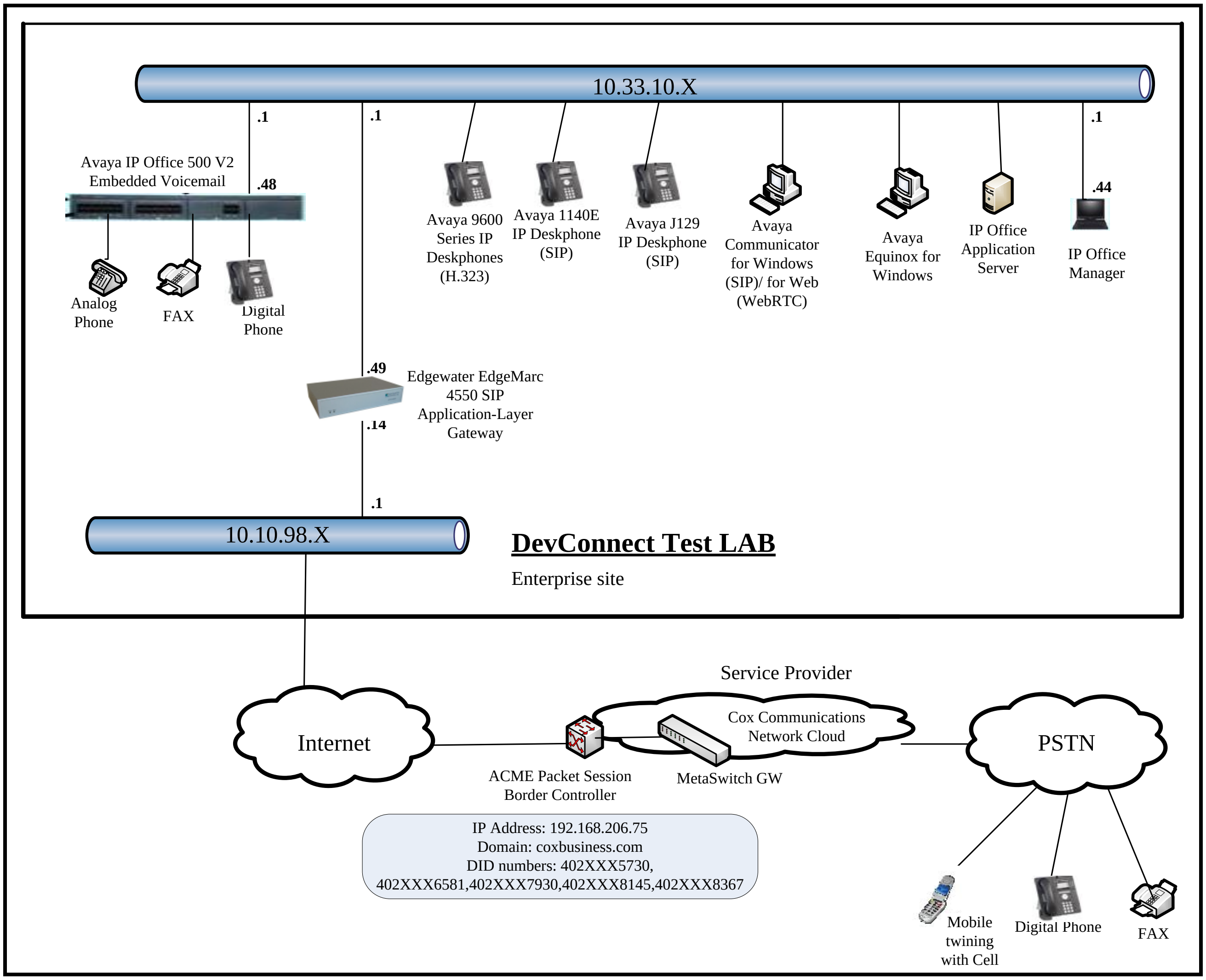

Figure 1 - Test Configuration for Avaya IP Office with Cox Communications SIP Trunk Service

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 the Cox Communications system. For calls within the North American Numbering Plan (NANP), the user would dial 11 (1 + 10) digits. Thus, for these NANP calls, Avaya IP Office would send 11 digits in the Request URI and the To field of an outbound SIP INVITE message. It was configured to send 10 digits in the From field. For inbound calls, 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 the Avaya IP Office such as a session border controller or data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that SIP and RTP traffic between the service provider and the Avaya IP Office 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:

Avaya Telephony Components	
Equipment	**Release**
Avaya IP Office solution ▪ Avaya IP Office 500V2 ▪ Embedded Voicemail ▪ Avaya Web RTC Gateway ▪ Avaya one-X Portal ▪ Avaya IP Office Manager ▪ Avaya IP Office Analogue PHONE 8 ▪ Avaya IP Office VCM64/PRID U ▪ Avaya IP Office DIG DCPx16 V2	 11.0.0.1.0 Build 8 11.0.0.1.0 Build 8 11.0.0.0.1 Build 54 11.0.0.1.0 Build 38 11.0.0.1.0 Build 8 11.0.0.1.0 Build 8 11.0.0.1.0 Build 8 11.0.0.1.0 Build 8
Avaya 1140E IP Deskphone (SIP)	04.04.23
Avaya 9641G IP Deskphone	6.6.6.04
Avaya 9621G IP Deskphone	6.6.6.04
Avaya J129 IP Deskphone	3.0.0.0.20
Avaya Communicator for Windows (SIP)	2.1.4.0 - 297
Avaya Communicator for Web	1.0.16.2220
Avaya Equinox for Windows	3.4.1.20.3 (SP1)
Avaya 1408D Digital Deskphone	R48
Avaya Analog Deskphone	N/A
HP Officejet 4500 (fax)	N/A
Cox Communications Components	
Equipment	**Release**
Edgewater EdgeMarc 4550 SIP ALG	Version 11.6.14
ACME packet SBC	SD7.1.0 MR-6 Patch 14
MetaSwitch GW	V4.1.40_SU15_P01.03

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

4.1. Configure Avaya IP Office Solution

This section describes the Avaya IP Office solution configuration necessary to support connectivity to Cox Communications. It is assumed that the initial installation and provisioning of the Avaya IP Office 500V2 has been previously completed and therefore is not covered in these Application Notes. For information on these installation tasks refer to Additional References **Section 8**.

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

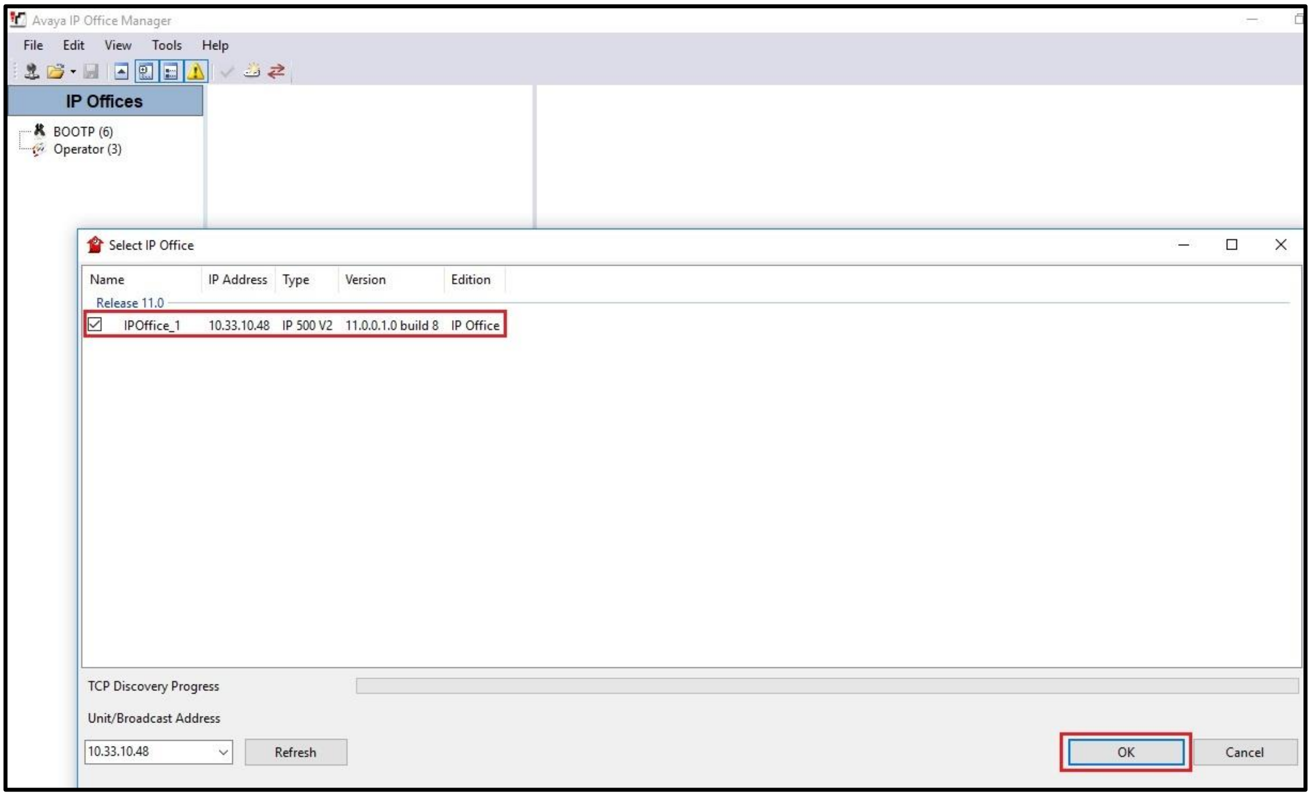

Figure 2 – Avaya IP Office Selection

4.2. Licensing

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

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

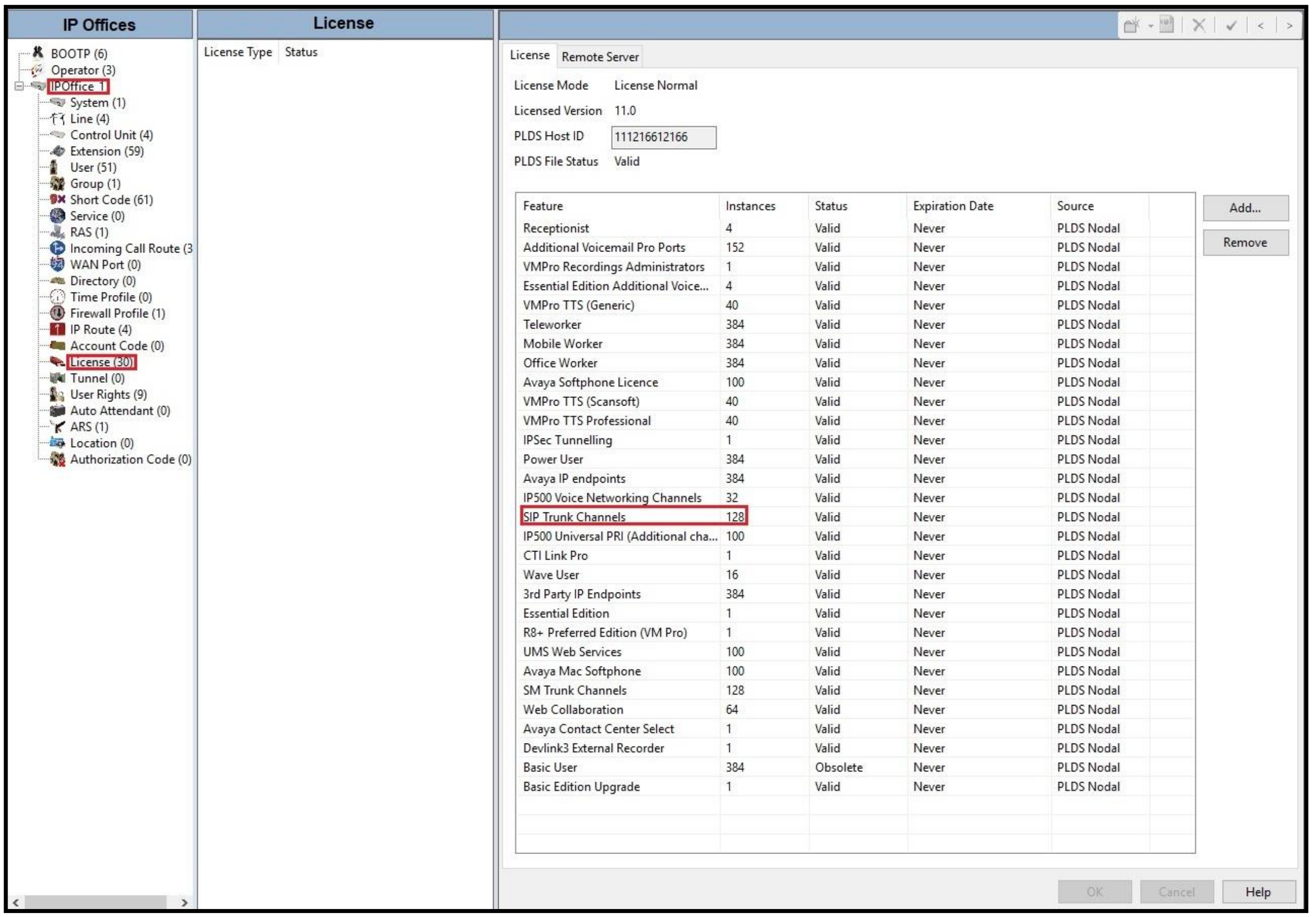

Figure 3 – Avaya IP Office License

4.3. System Tab

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

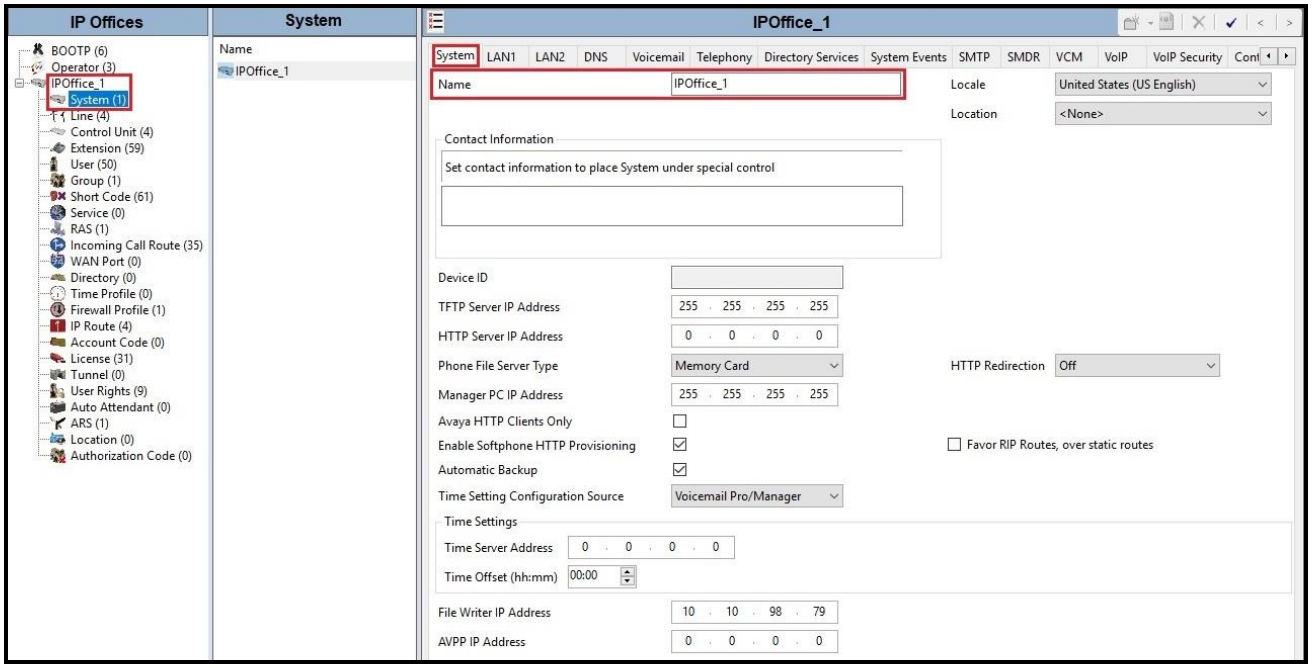

Figure 4 - Avaya IP Office System Configuration

4.4. LAN2 Settings

In the sample configuration, LAN2 is used to connect the enterprise network to Cox Communications network via Cox managed CPE.
Note: The LAN1 port of Avaya IP Office connected to the enterprise LAN (private network) is not described in this document.

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

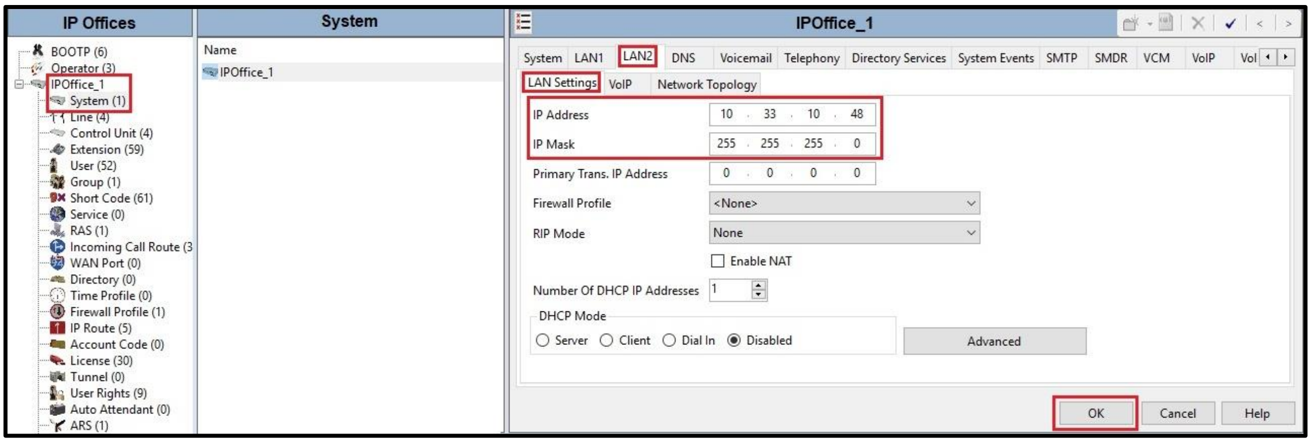

Figure 5 - Avaya IP Office LAN2 Settings

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
- Check the **SIP Registrar Enable** to allow Avaya IP deskphones/softphones to register using the SIP protocol
- Input **SIP Domain Name** as **10.33.10.48**
- The **Layer 4 Protocol** uses **UDP** with **UDP Port** as **5060**
- 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

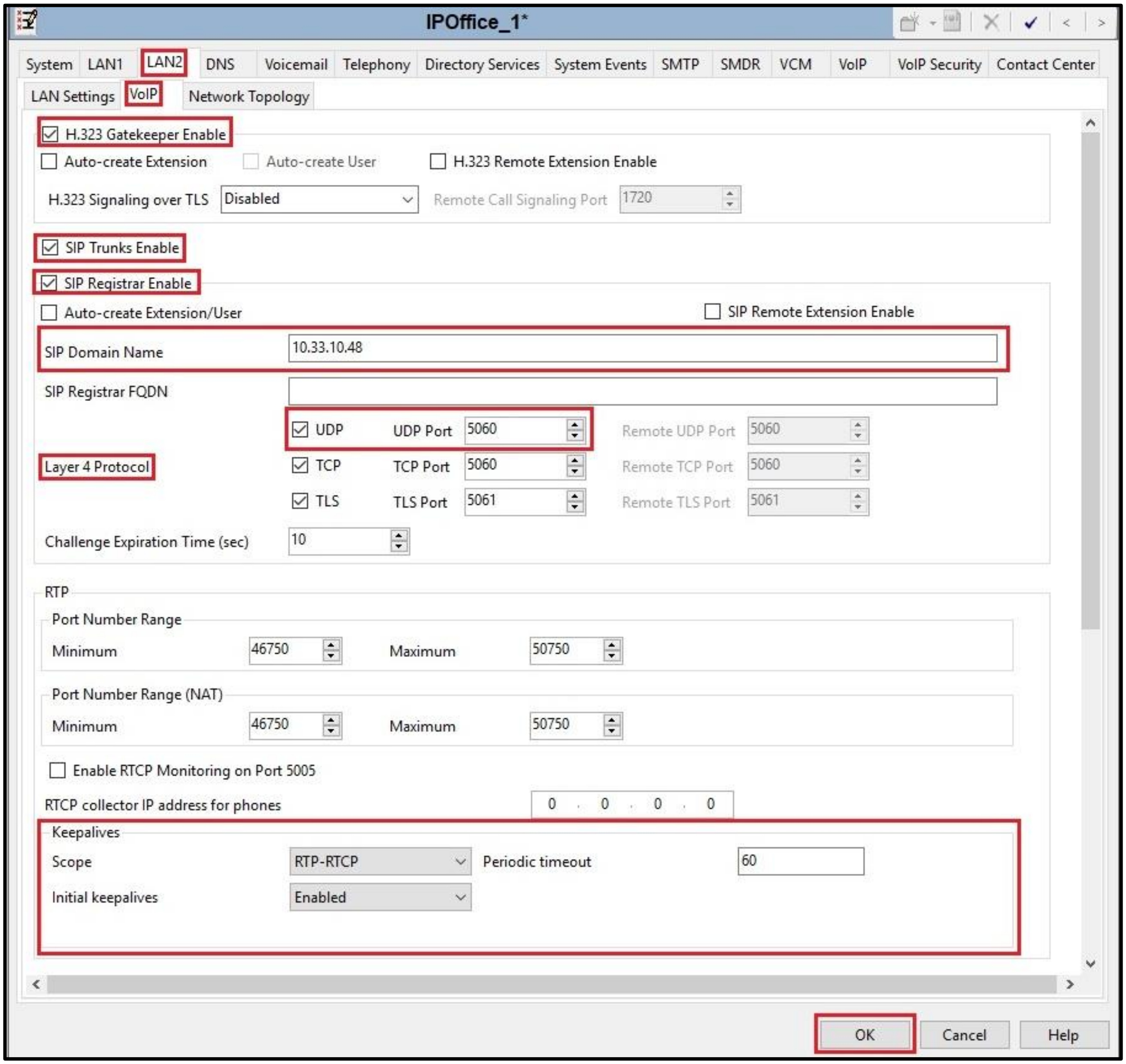

Figure 6 - Avaya IP Office LAN2 VoIP

4.5. System Telephony Settings

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

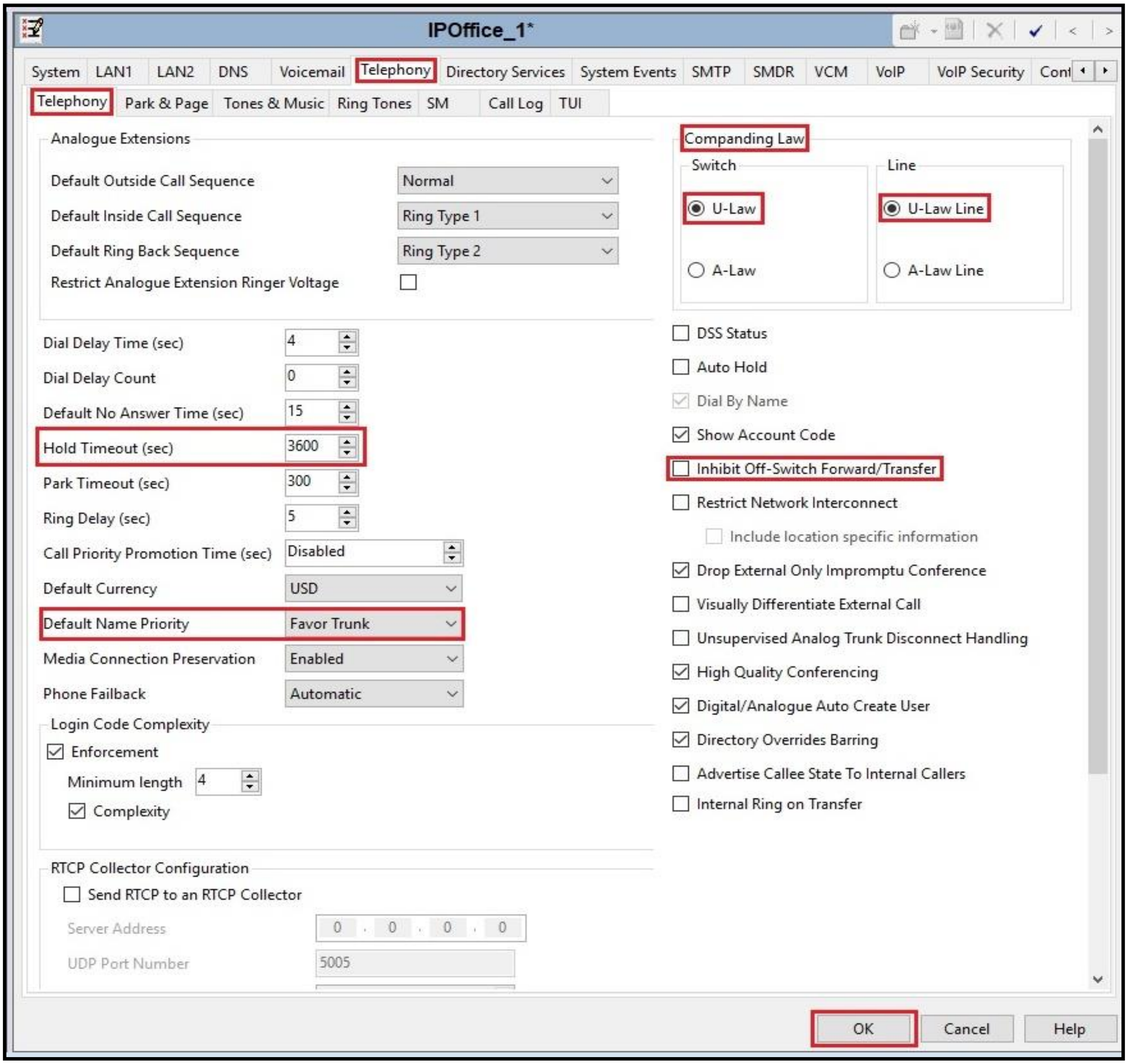

Figure 7 - Avaya IP Office Telephony

4.6. System VoIP Settings

Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes and then navigate to the **VoIP** tab in the **Details** pane. Leave the **RFC2833 Default Payload** as default of **101**. Select codec **G.711 ULAW 64K** which Cox Communications supports. Click **OK** to submit the changes.

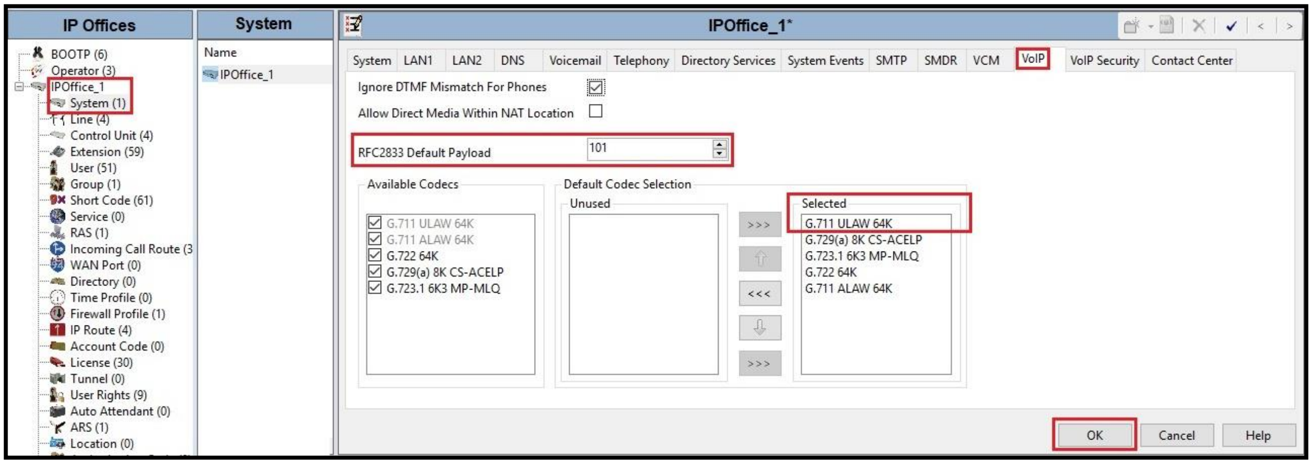

Figure 8 - Avaya IP Office VoIP

4.7. Administer SIP Line

A SIP Line is needed to establish the SIP connection between Avaya IP Office and Cox Communications system via Cox managed CPE. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by Avaya IP Office Manager to create a SIP Line. Follow the steps in **Section 4.7.1** 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 4.7.2**.

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 4.7.2**.

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

4.7.1. Create SIP Line from Template

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

1. Create a new folder in computer where Avaya IP Office Manager is installed (e.g. C:\Cox Communications\Template). Copy the template file to this folder. The template file for the compliance test is **Cox_IPO11.xml** (for SIP Line 17)
2. Import the template into Avaya IP Office Manager: From Avaya IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file from step 1 into the IP Office template directory

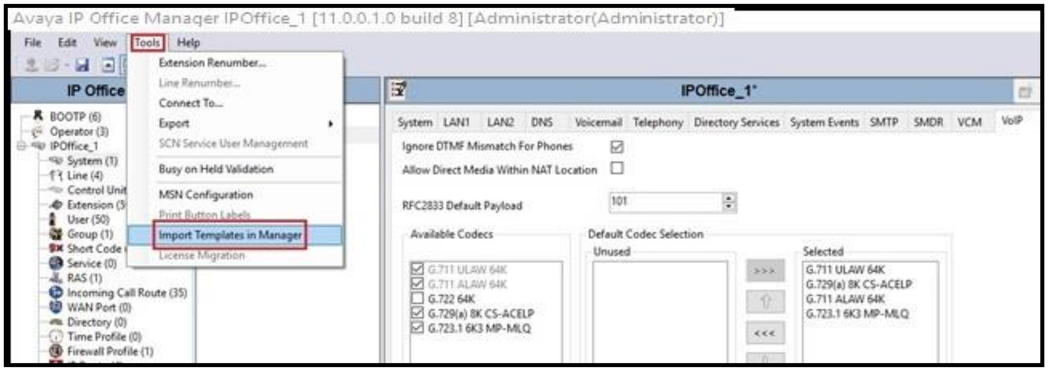

Figure 9 – Import Template for SIP Line

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

Figure 10 – Import Template for SIP Line successfully

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

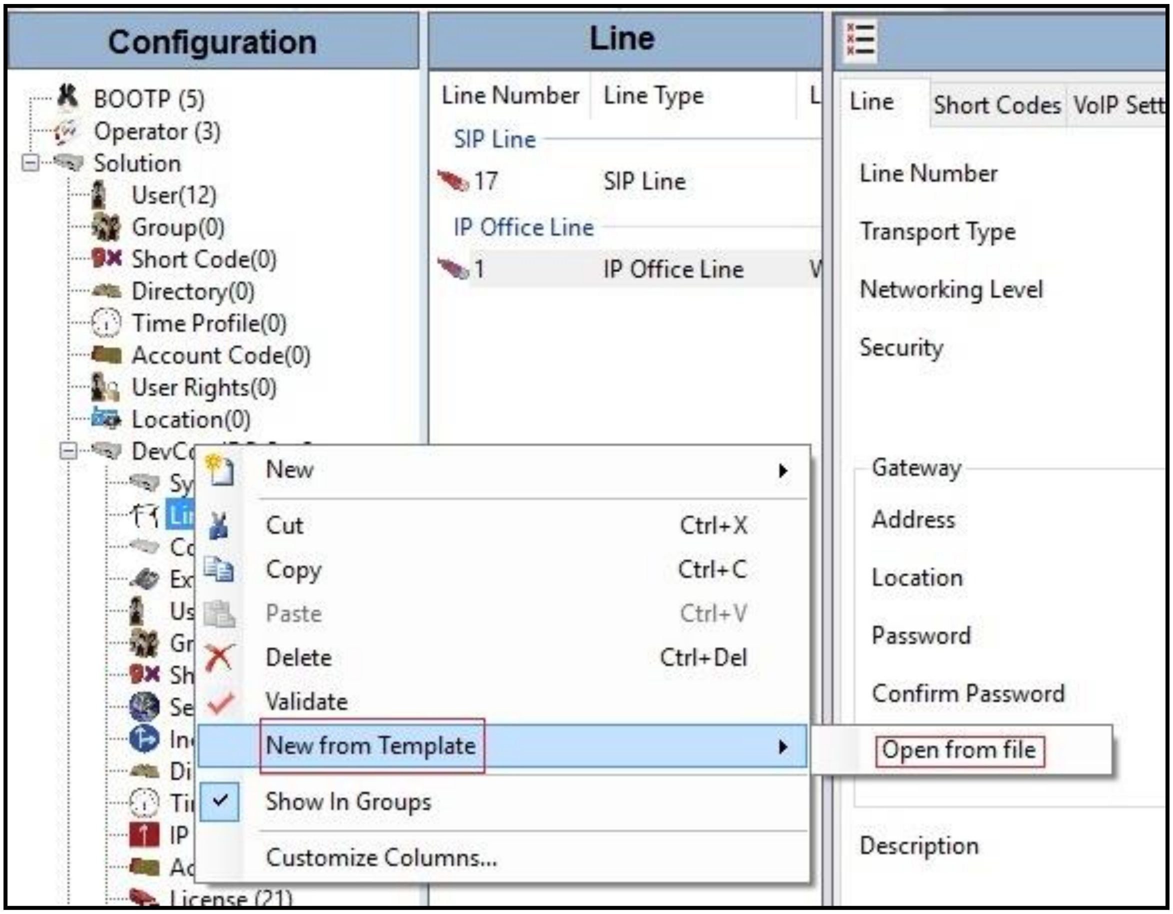

Figure 11 – Create SIP Line from Template

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

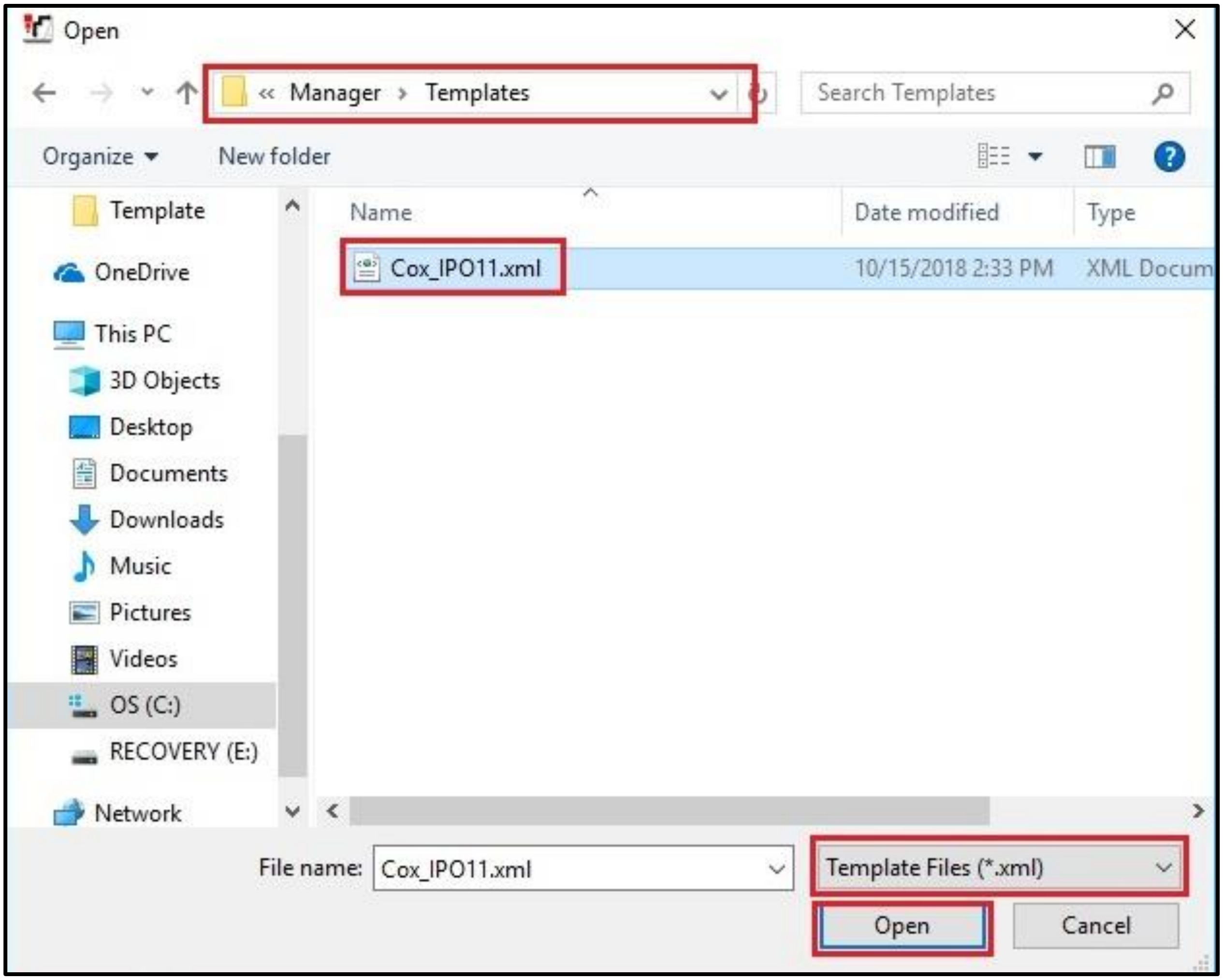

Figure 12 – Create SIP Line from IP Office Template directory

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

Figure 13 – Create SIP Line from Template successfully

5. Once the SIP Line is created, verify the configuration of the SIP Lines with the configuration shown in **Section 4.7.2**

4.7.2. 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 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
- Set **Local Domain Name** to IP address of Avaya IP Office LAN2 port. This field is used to specify the default host part of the SIP URI in the From field for outgoing calls
  Note: For the user making the call, the user part of the From SIP URI is determined by the settings of the SIP URI channel record being used to route the call (see Line → Call Details → Local URI). For the destination of the call, the user part of the To and R-URI fields are determined by dial short codes of the form 9N;/N where N is the user part of the SIP URI
- Check the **In Service** and **Check OOS** boxes
- Set **URI Type** to **SIP**
- For **Session Timers**, set **Refresh Method** to **Auto** with **Timer (sec)** to **On Demand**
- Set **Name Priority** to **Favor Trunk**. As described in **Section 4.5**, the **Default Name Priority** parameter may retain the default **Favor Trunk** setting or can be configured to **Favor Directory**. As shown below, the default **Favor Trunk** setting was used in the reference configuration
- For **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never**. Note: 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

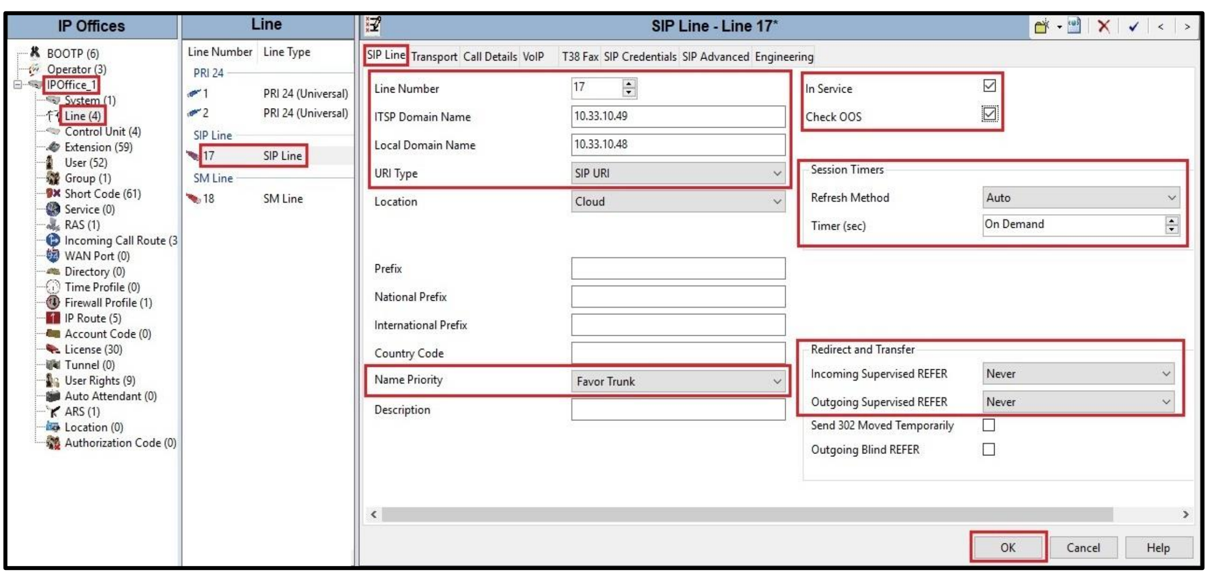

Figure 14 – SIP Line Configuration

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: **10.33.10.49**. 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 → LAN2 → Network Topology** tab for the purposes of SIP trunking. If a NAT is used between Avaya IP Office and the other end of the trunk, then the **Use Network Topology Info** field should be set to the LAN interface (**LAN2**) used by the trunk and the **System → LAN2 → Network Topology** tab needs to be configured with the details of the NAT device
- The **Calls Route via Registrar** was unchecked. In this certification testing, Cox Communications did not support the dynamic Registration on the SIP Trunk
- Other parameters retain default values
- Click **OK** to commit then press Ctrl + S to save

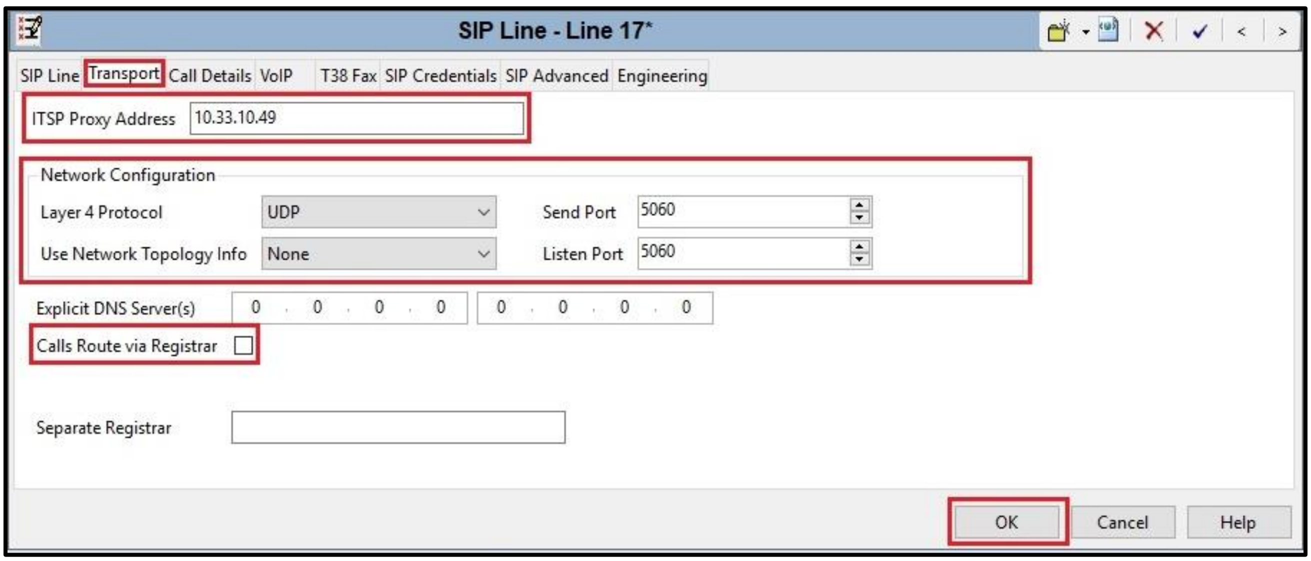

Figure 15 – SIP Line Transport Configuration

A SIP Credentials entry must be created for Digest Authentication used by Cox Communications to authenticate calls from the enterprise to the PSTN. To create a SIP Credentials entry, first select the **SIP Credentials** tab. Click the **Add** button and the **New SIP Credentials** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit…** button. In the bottom of the screen, the Edit SIP Credentials area will be opened. In the example screen below, a previously configured entry is edited. The entry was created with the parameters shown below:

- Set **User name**, **Authentication Name**, and **Contact** to the value provided by the service provider
- Set **Password** to the value provided by the service provider. **Expiration (mins)** is set to **60**
- Check the **Registration required** option. Cox Communications does require registration for Digest Authentication

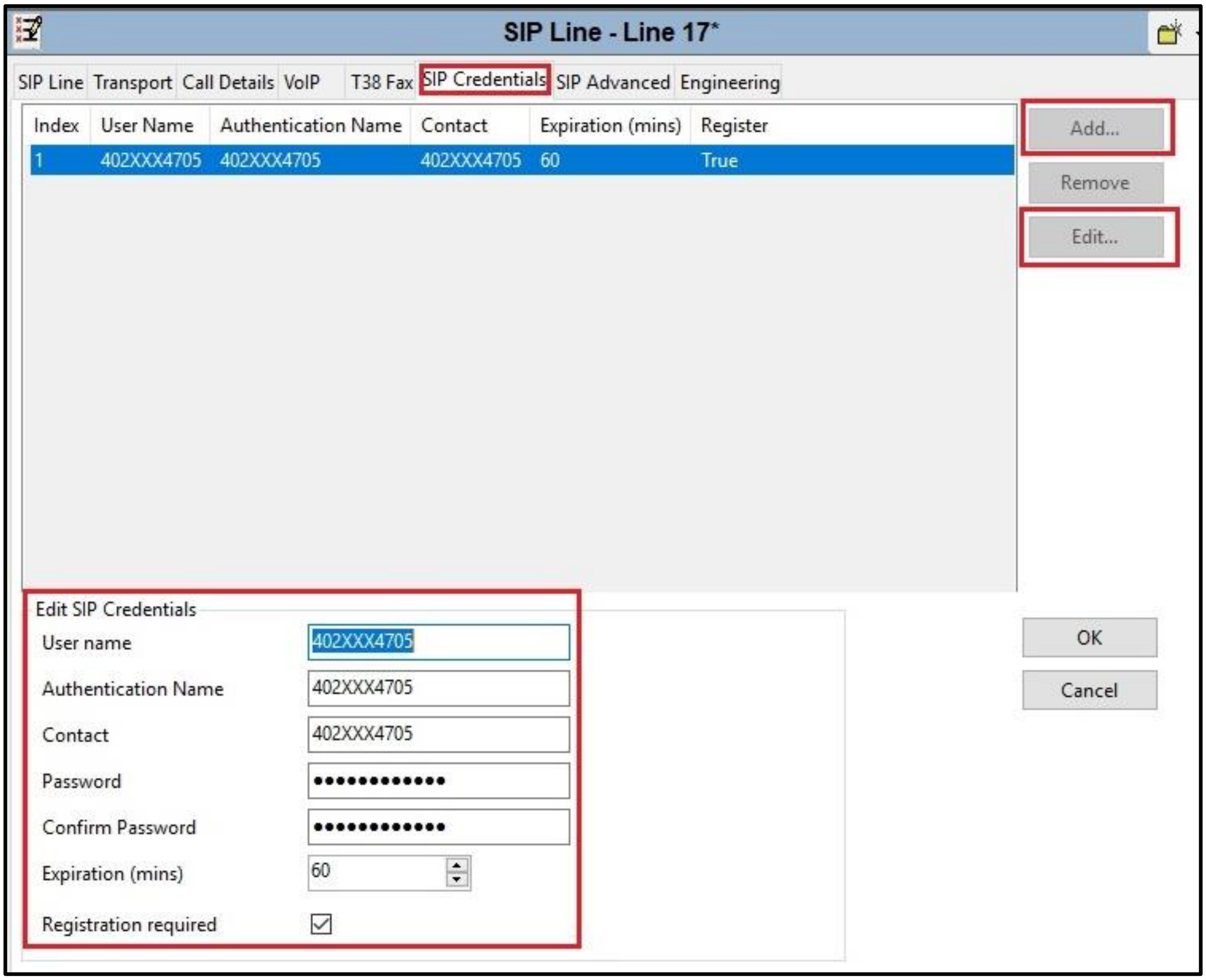

Figure 16 – SIP Line SIP Credentials Configuration

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 URI** area will appear. 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
- Set **Credentials** to **1: 402XXX4705**
- Check **P Asserted ID** and **Diversion Header** options
- Set the **Display** and **Content** of **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** to **Auto** by default. If the Auto setting is used, the SIP trunk will accept any incoming SIP call. The incoming call routing is still performed by the system Incoming Call Route (shown in **Section 4.10**) based on matching the values received with the call
- Click **OK** to submit the changes

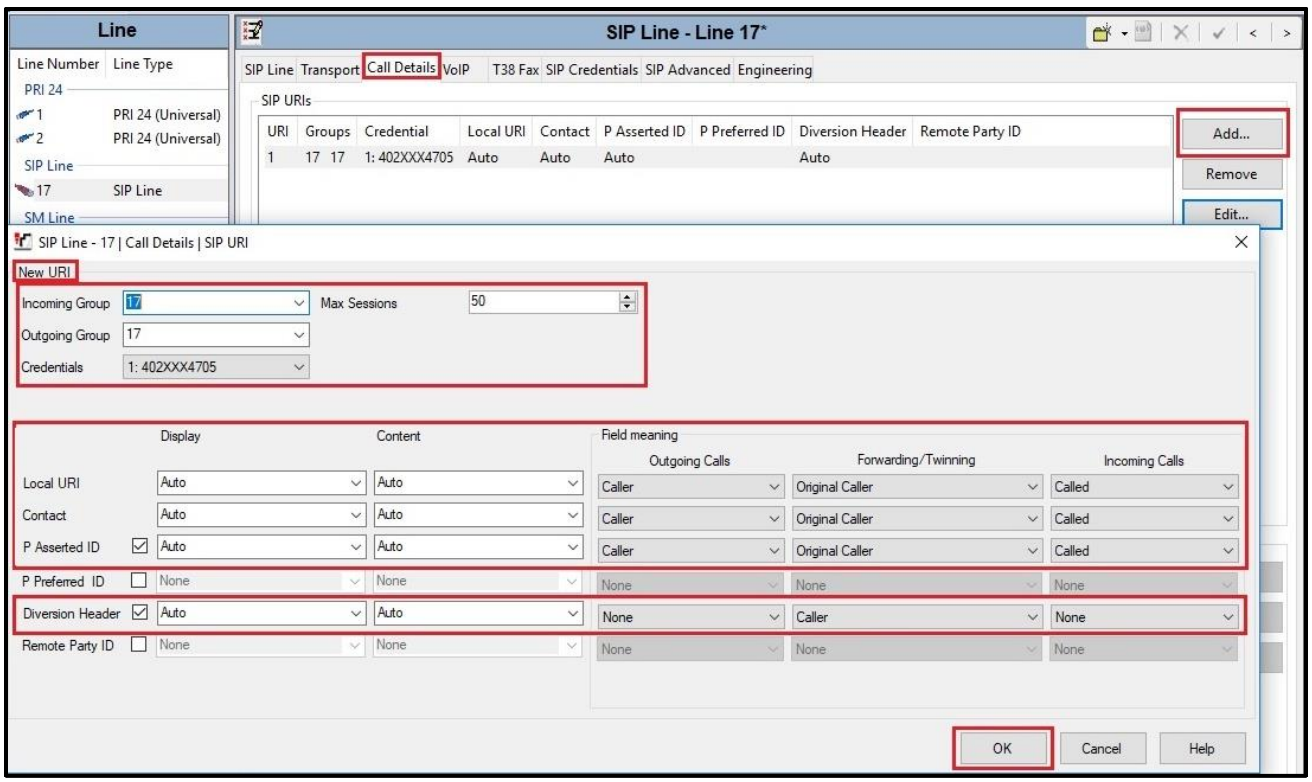

Figure 17 – SIP Line SIP Call Details Configuration

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 **G.711** from the pull-down menu. Note: Cox Communications supported only Fax G.711 pass-through mode during the compliance testing, T.38 is not supported by Cox Communications (See observation in **Section 2.1**)
- Set the **DTMF Support** to **RFC2833** from the pull-down menu. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833
- Default values may be used for all other parameters
- Click **OK** to submit the changes

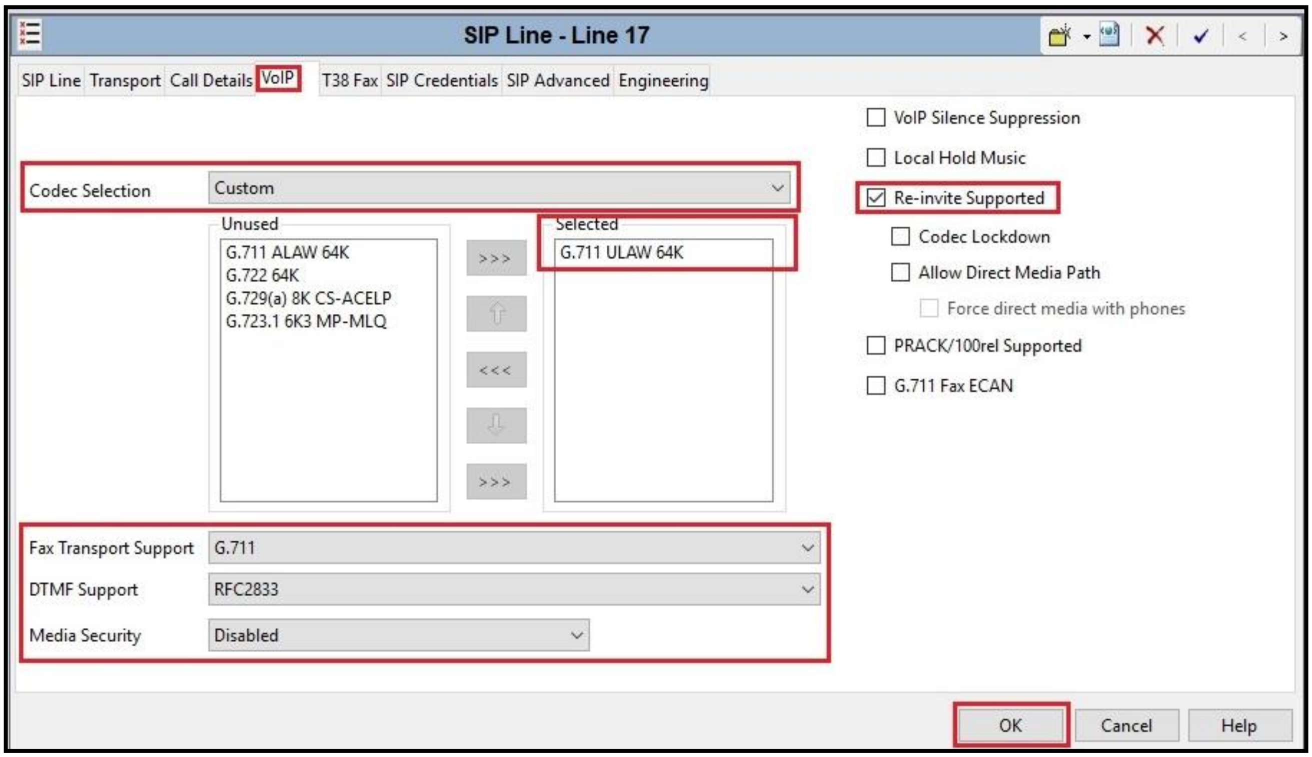

Figure 18 – SIP Line VoIP Configuration

4.8. Outgoing Call Routing

The following section describes the Short Code for outgoing traffic on the SIP line to Cox Communications via Cox managed CPE.

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

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **9N;**, this short code will be invoked when the user dials 9 followed by any number
- Set **Feature** to **Dial**. This is the action that the short code will perform
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user.
- Set the **Line Group ID** to the **Outgoing Group 17** defined on the **SIP URI** tab on the **SIP Line** in **Section 4.7.2**. This short code will use this line group when placing the outbound call
- Set the **Locale** to **United States (US English)**
- Default values may be used for all other parameters
- Click **OK** to submit the changes

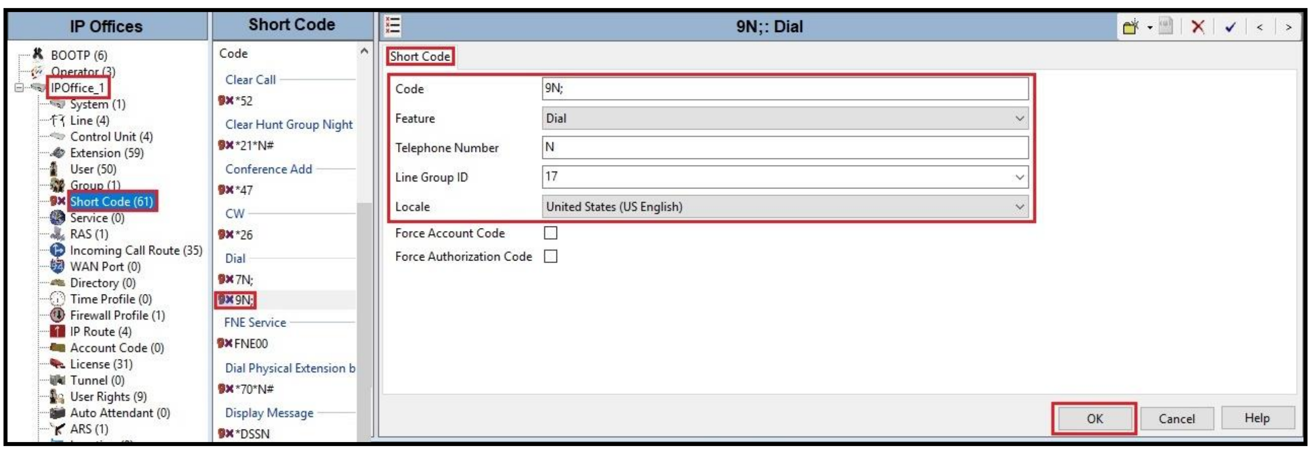

Figure 19 – Short Code 9N

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

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

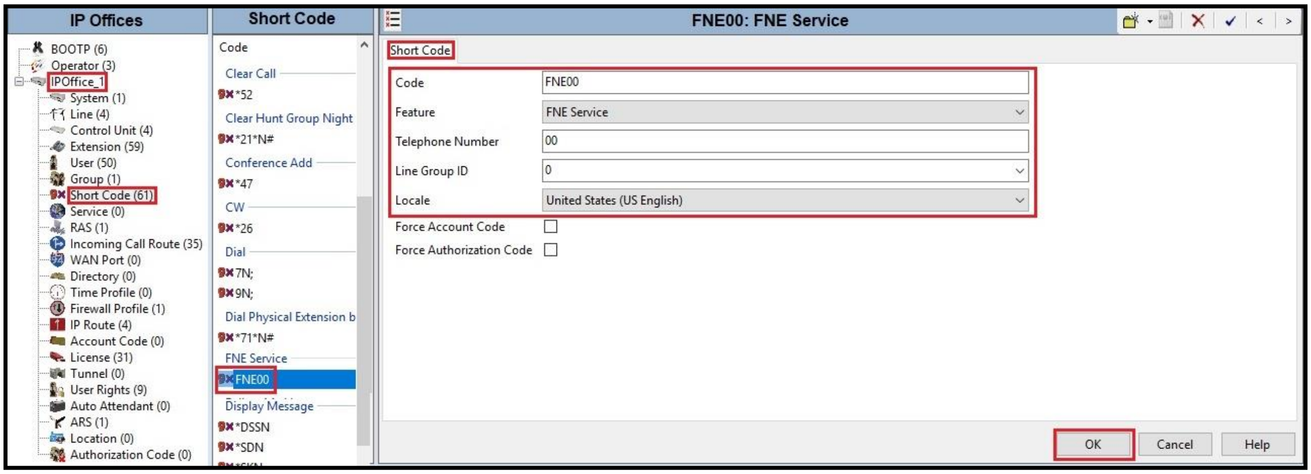

Figure 20 – Short Code FNE

4.9. User

Configure each of users that will be placing and receiving calls via the SIP Line defined in **Section 4.7**. 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, a user with **Name** as **5730** was configured.

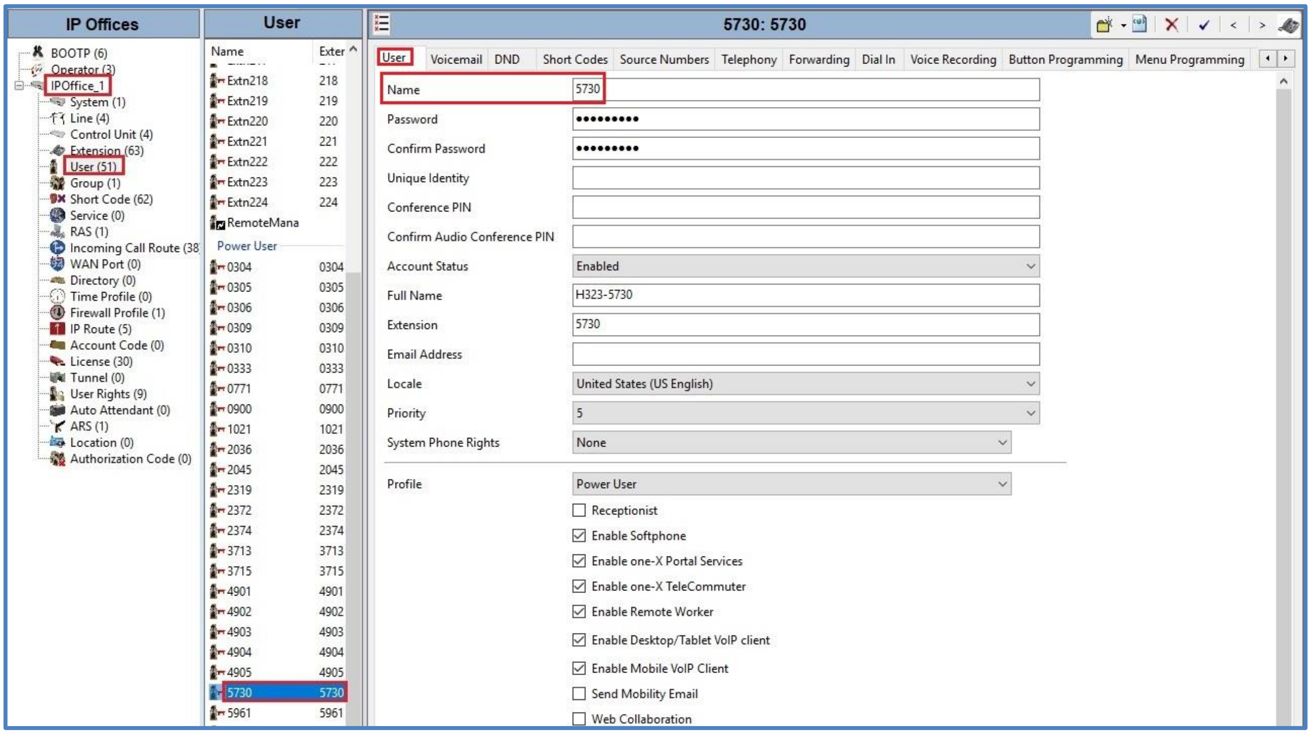

Figure 21 – User Configuration

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 5730. 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 4.8**). Other options can be set according to customer requirements.

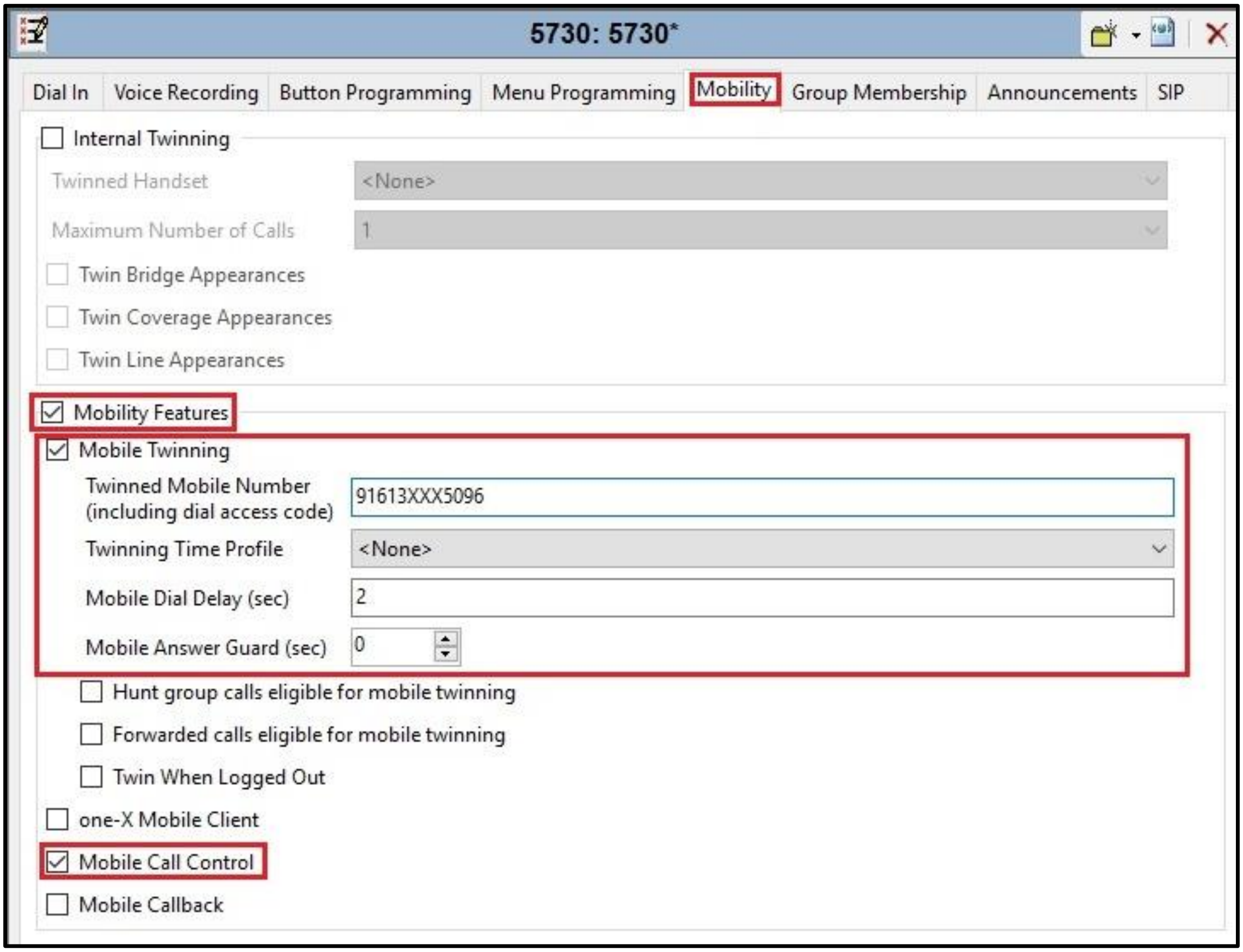

Figure 22 – Mobility Configuration for User

4.10. 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 **SIP URI** tab on the **SIP Line** in **Section 4.7.2**
- Set the **Incoming Number** to the incoming DID number on which this route should match
- Default values can be used for all other fields

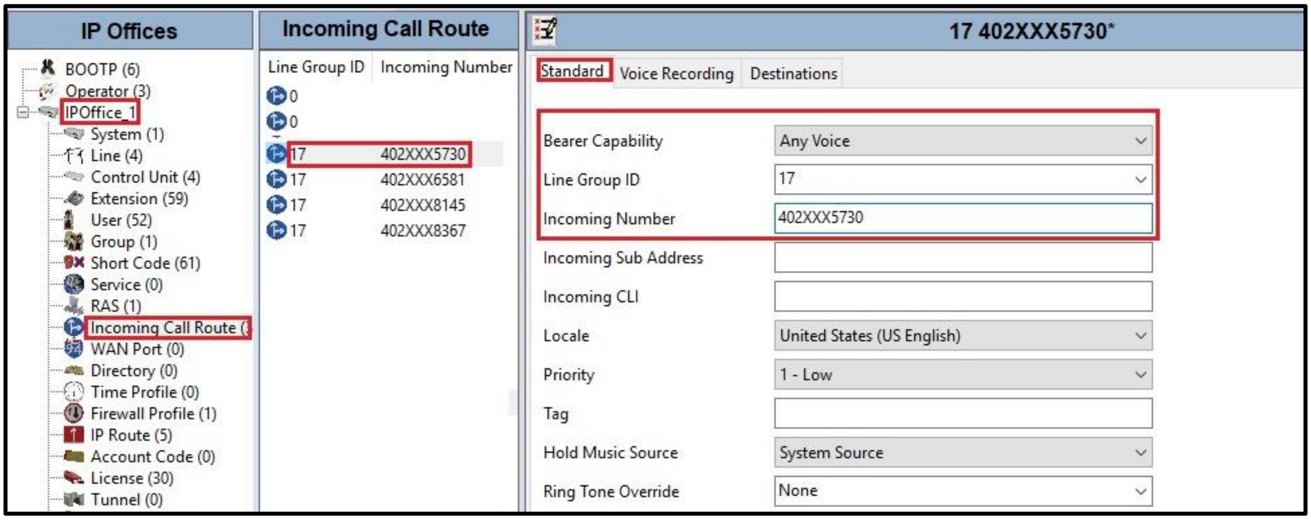

Figure 23 – Incoming Call Route Configuration

On the **Destination** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **402XXX5730** on line 17 are routed to **Destination 5730 5730** as below screenshot:

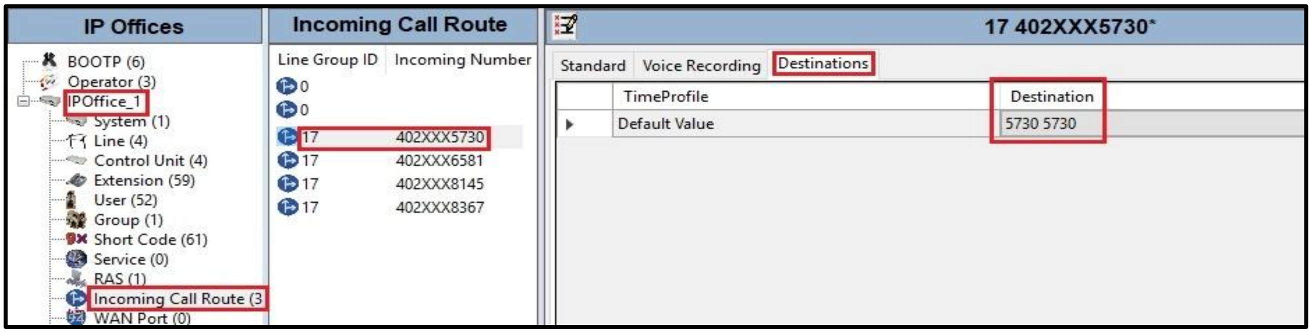

Figure 24 – Incoming Call Route for Destination 5730

For Feature Name Extension Service testing purpose, the incoming calls to DID number **402XXX8145** were configured to access **FNE00**. The **Destination** was appropriately defined as **FNE00** as below screenshot:

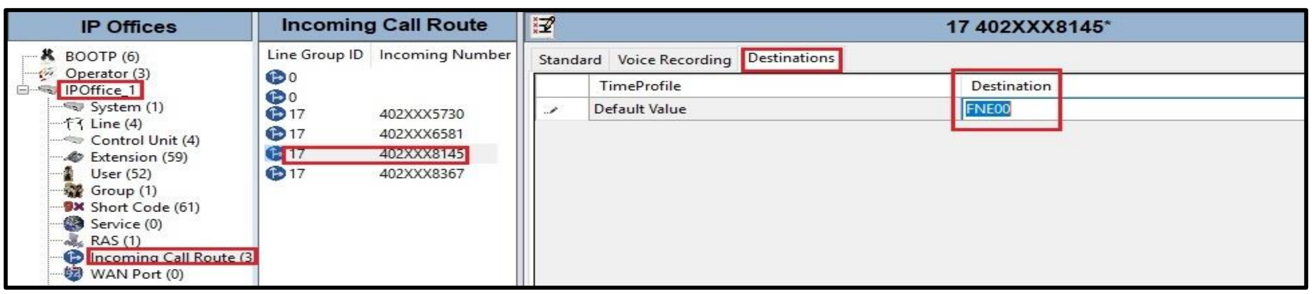

Figure 25 – Incoming Call Route for Destination FNE

For Voice Mail testing purpose, the incoming calls to DID number **402XXX8367** were configured to access **VoiceMail**. The **Destination** was appropriately defined as **VoiceMail** as below screenshot:

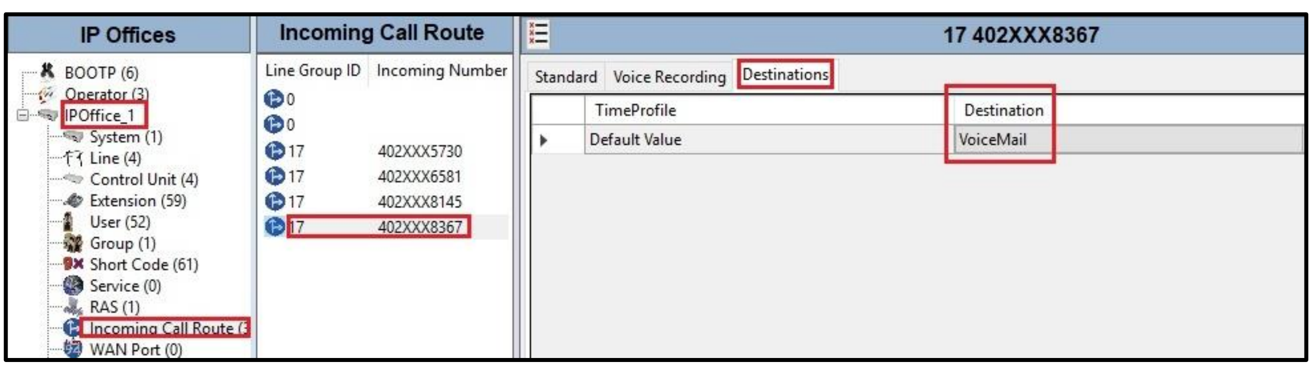

Figure 26 – Incoming Call Route for Destination VoiceMail

4.11. 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 section.

5. 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)

6. Verification Steps

The following steps may be used to verify the configuration:

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

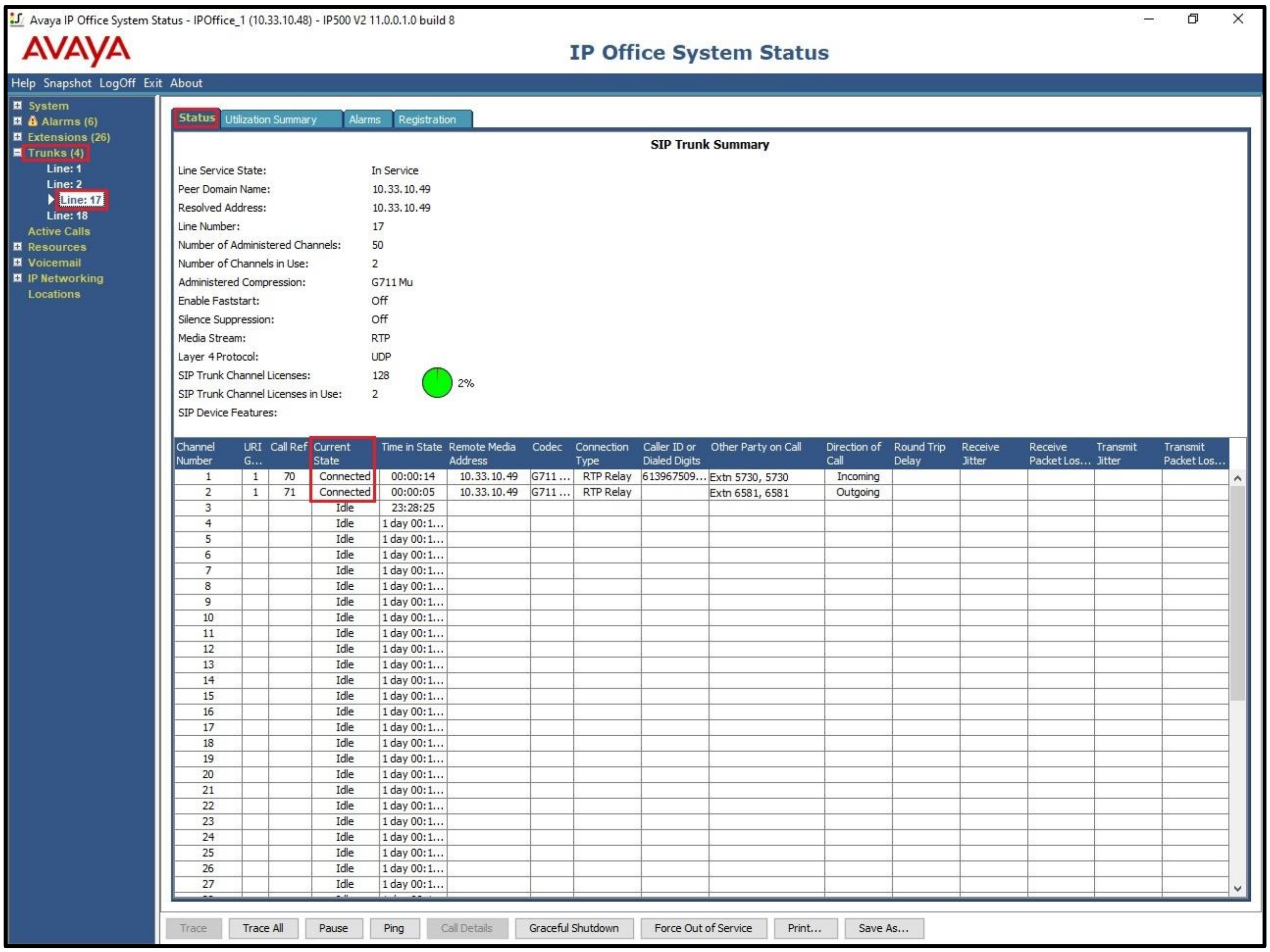

Figure 27 – SIP Trunk status

- 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

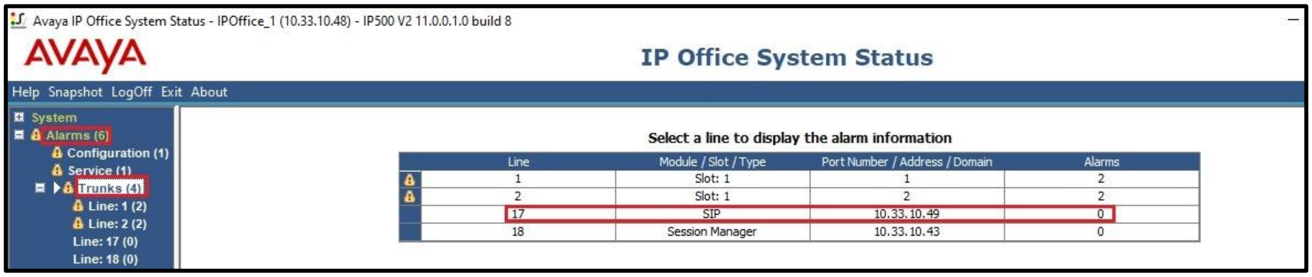

Figure 28 – SIP Trunk alarm

- 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
- 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 WAN port interface of the Cox managed CPE

7. 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**.

8. Additional References

[1] Administering Avaya IP Office Platform with Manager, Release 11.0, Issue 17a, August 2018.
[2] Deploying IP Office Essential Edition IP Office™ Platform 11.0, 15-601042 Issue 33j - (Thursday, September 13, 2018).
[3] Avaya IP Office™ Platform Release 11.0 – Release Notes / Technical Bulletin General Availability

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

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

9. 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 Comminications 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.

9.1. Cox managed CPE Login

The Cox managed CPE was configured with a local LAN address of 10.33.10.49 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 10.33.10.40
Launch a web browser on personal computer and enter the following URL: http://10.33.10.49 and hit enter.

The following login window should appear:

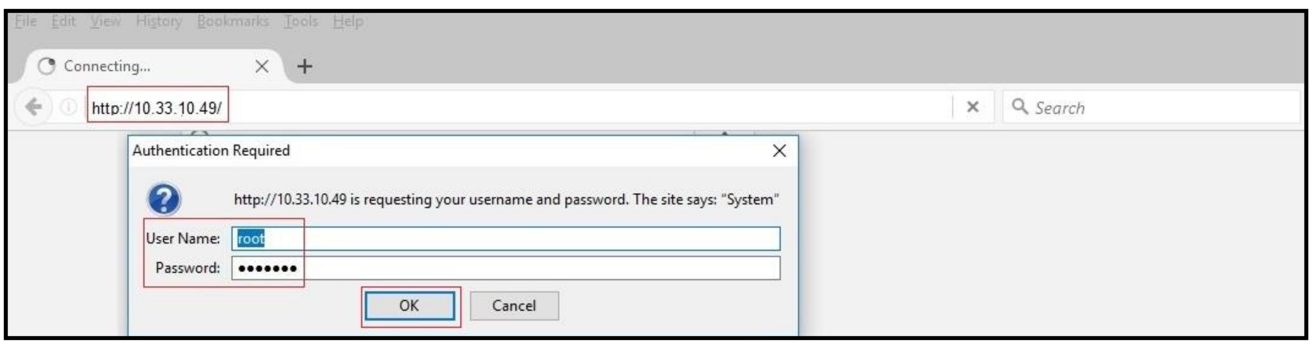

Figure 29 – Cox managed CPE Login

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

9.2. 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**: **10.33.10.49**
  - **Subnet Mask**: **255.255.255.0**
  - Check **Enable VLAN Support**
  - **Default VLAN ID**: **1**
- WAN Interface IPv4 Settings:
  - Check **Static IP**
  - **IP Address**: **10.10.98.14** (Provide this IP Address to service provider to set up the connectivity)
  - **Subnet Mask**: **255.255.255.192**
- Network Settings:
  - **Default Gateway**: **10.10.98.1**

Submit the changes.

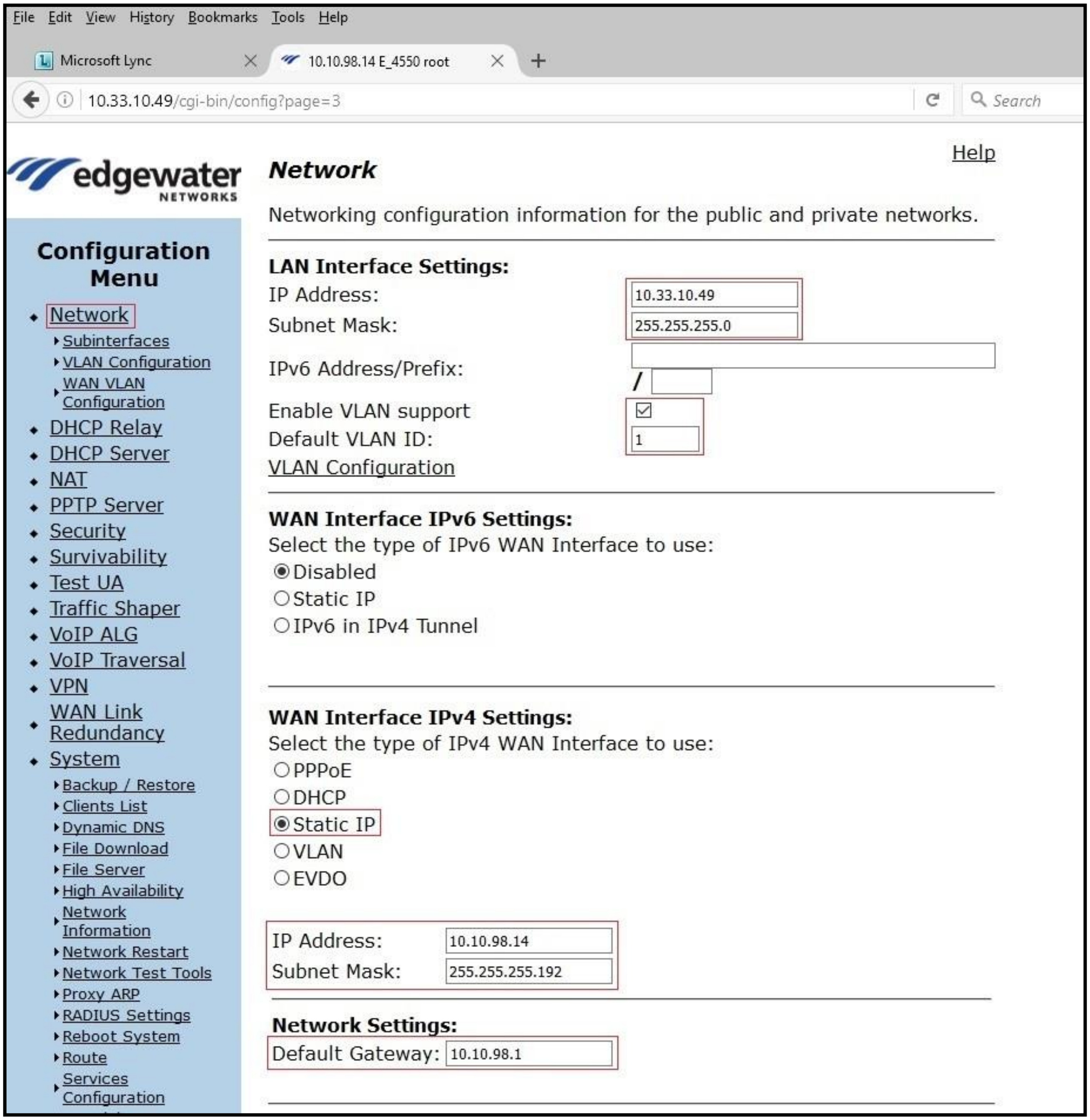

Figure 30 – Cox managed CPE Network Configuration

9.3. VLAN Configuration

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

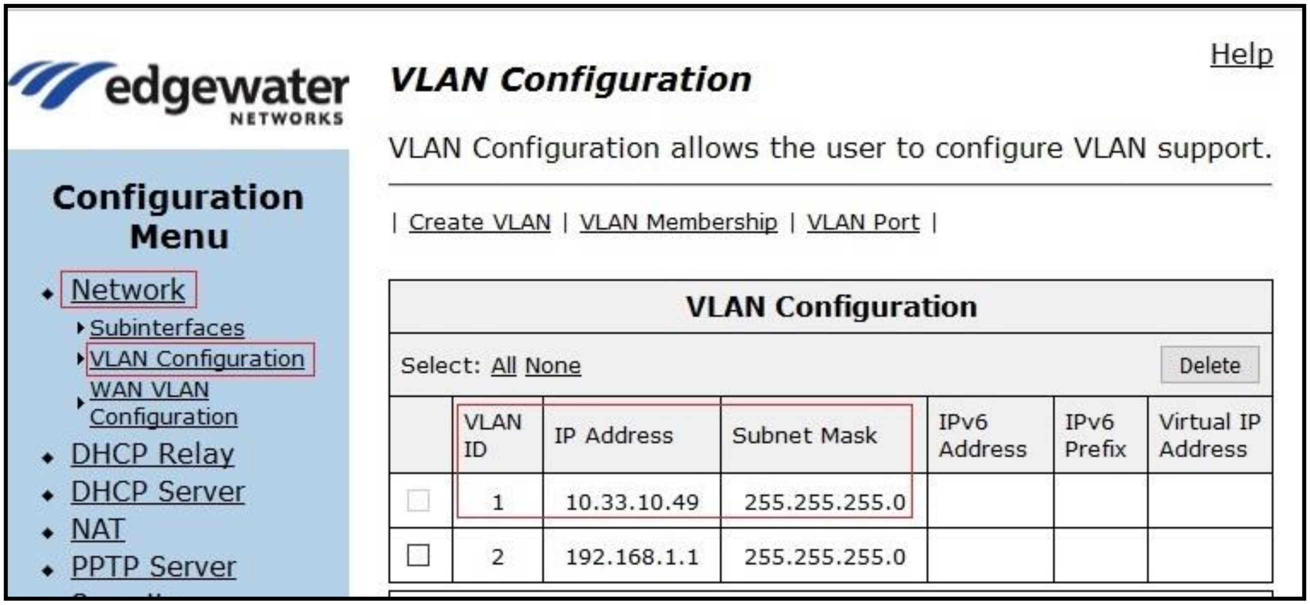

Figure 31 – Cox managed CPE VLAN Configuration

9.4. VoIP ALG Settings

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

- **SIP Server Address**: **192.168.206.75** (This is Cox Communications signaling server IP address)
- **SIP Server Port**: **5060**
- Check **Use Custom Domain**
- **SIP Server Domain**: **coxbusiness.com**

Submit the changes.

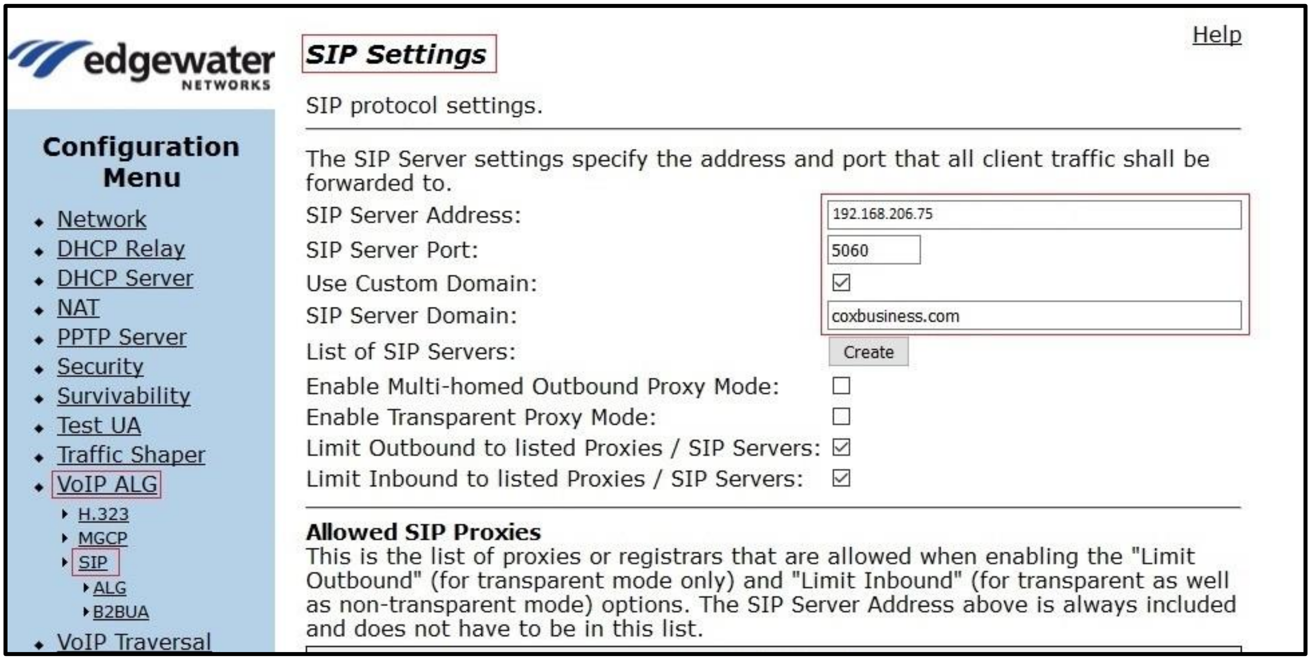

Figure 32 – Cox managed CPE VoIP ALG Settings

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

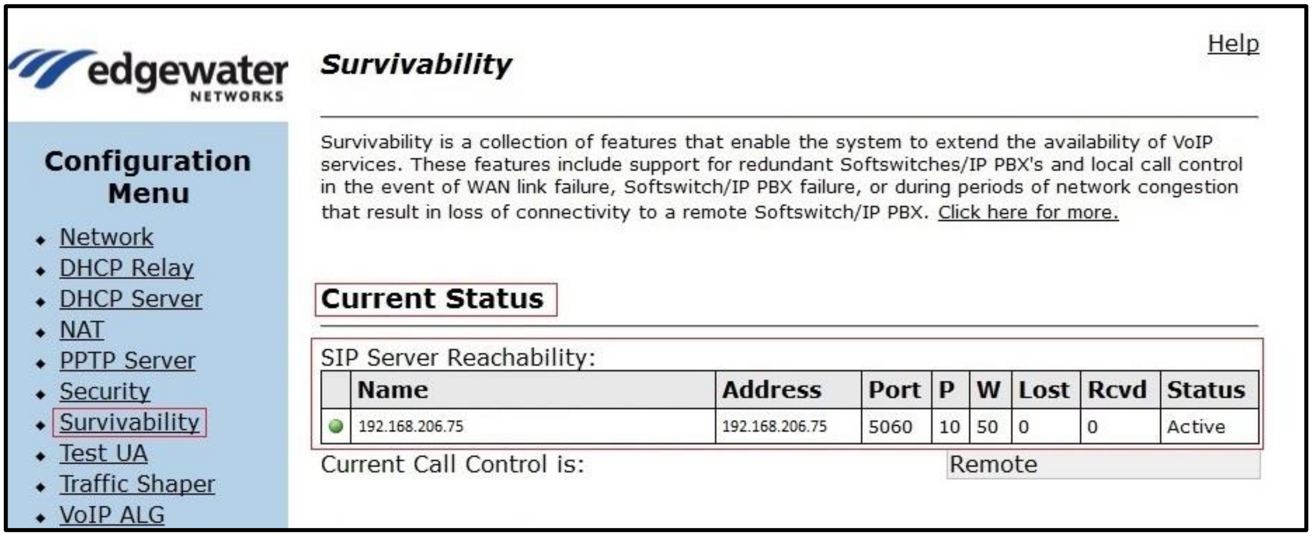

Figure 33 – Cox managed CPE SIP Server Survivability

9.5. B2BUA Trunking Configuration

From the **Configuration Menu**, select **VoIP ALG** 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: **10.33.10.48**
- Input SIP **Port** of the Avaya IP Office: **5060**
- Input **Username**: **402XXX4705**, which is pilot number for trunk registration to Cox Communications system
- Input **Password**: **xxxxxxxxxxx**, which is provided by Cox Communications

Select **Update** button to create trunking device.
Under **Trunk**:

- Input pilot number for trunk authentication, **402XXX4705**, then click **Add** button
- Check **Register Pilot**
- Input **Auth-User** as **402XXX4705**
- Input **Password**: **xxxxxxxxxxx**, same as Trunking Devices session above

Select **Submit** button (not shown).

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

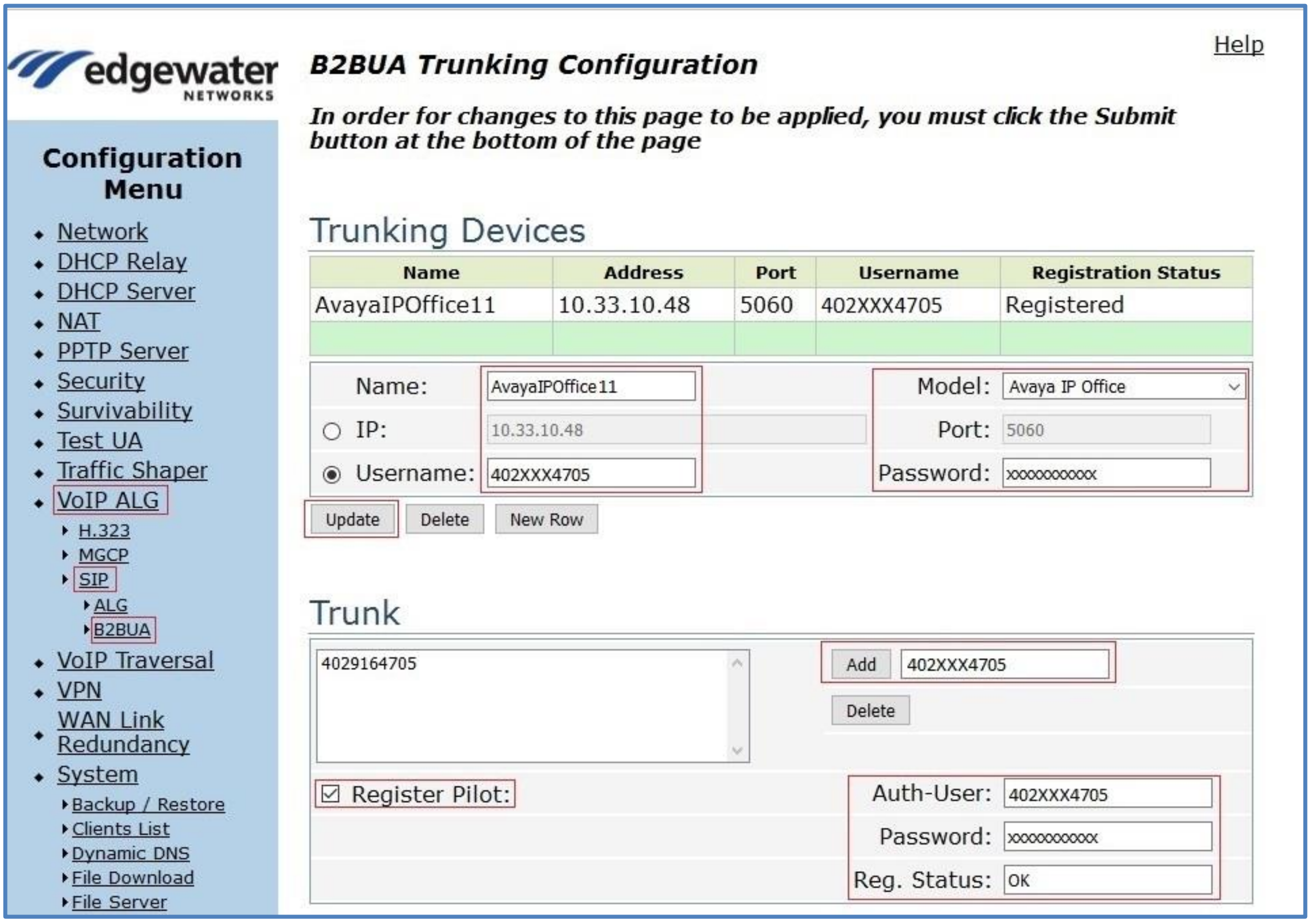

Figure 34 – Cox managed CPE SIP Trunk Configuration

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

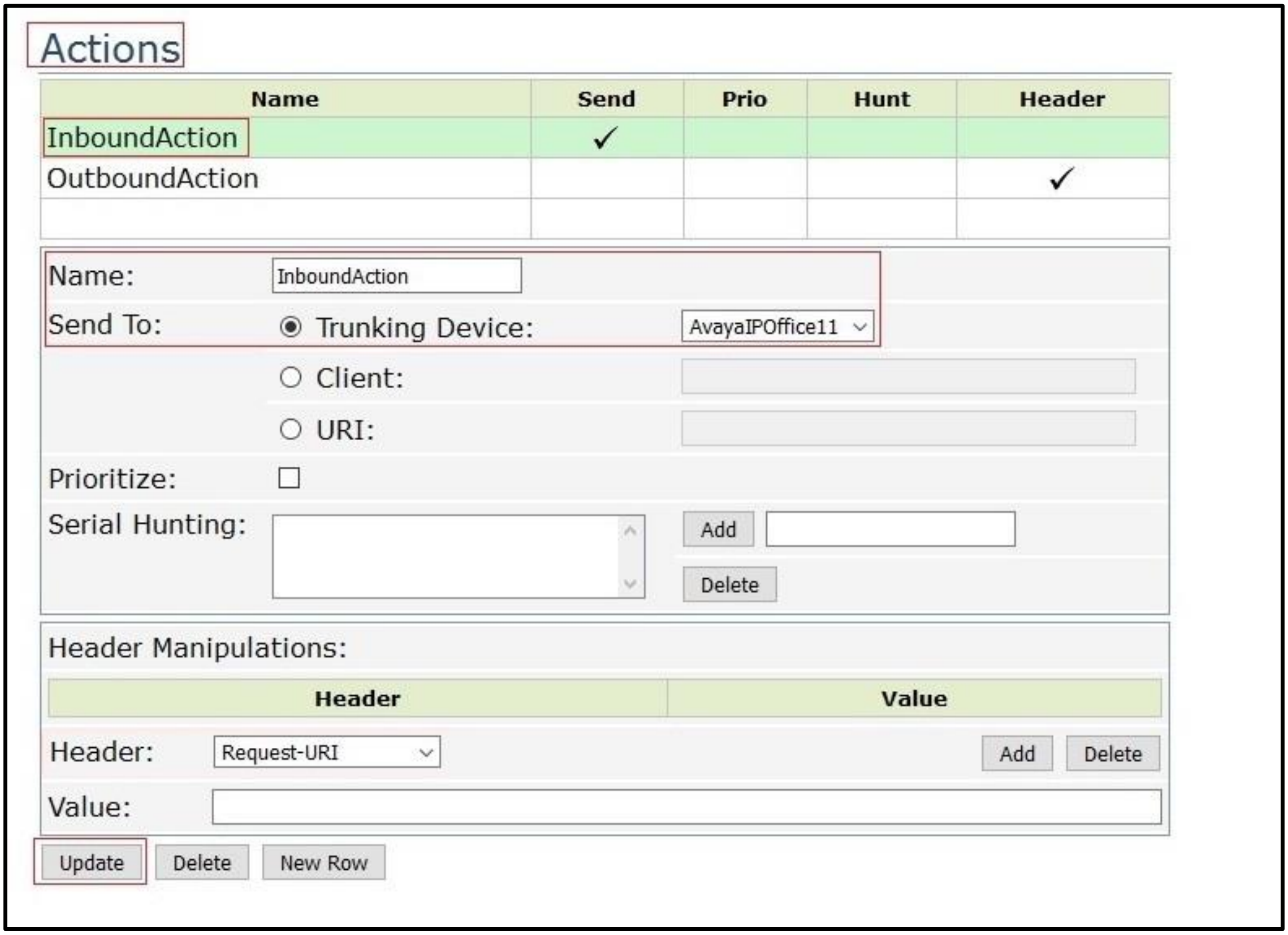

Figure 35 – Cox managed CPE Inbound Action Configuration

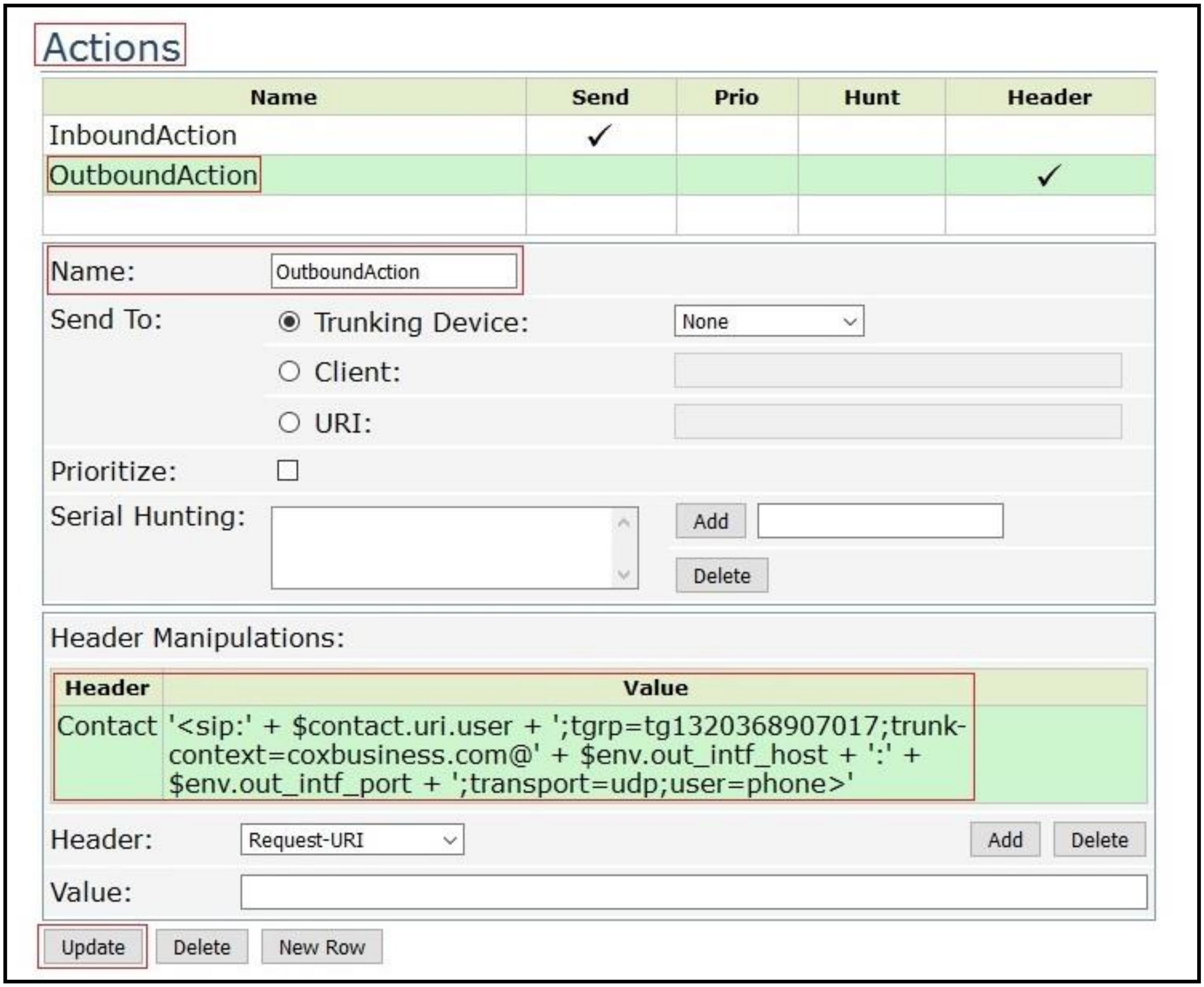

Figure 36 – Cox managed CPE Outbound Action Configuration

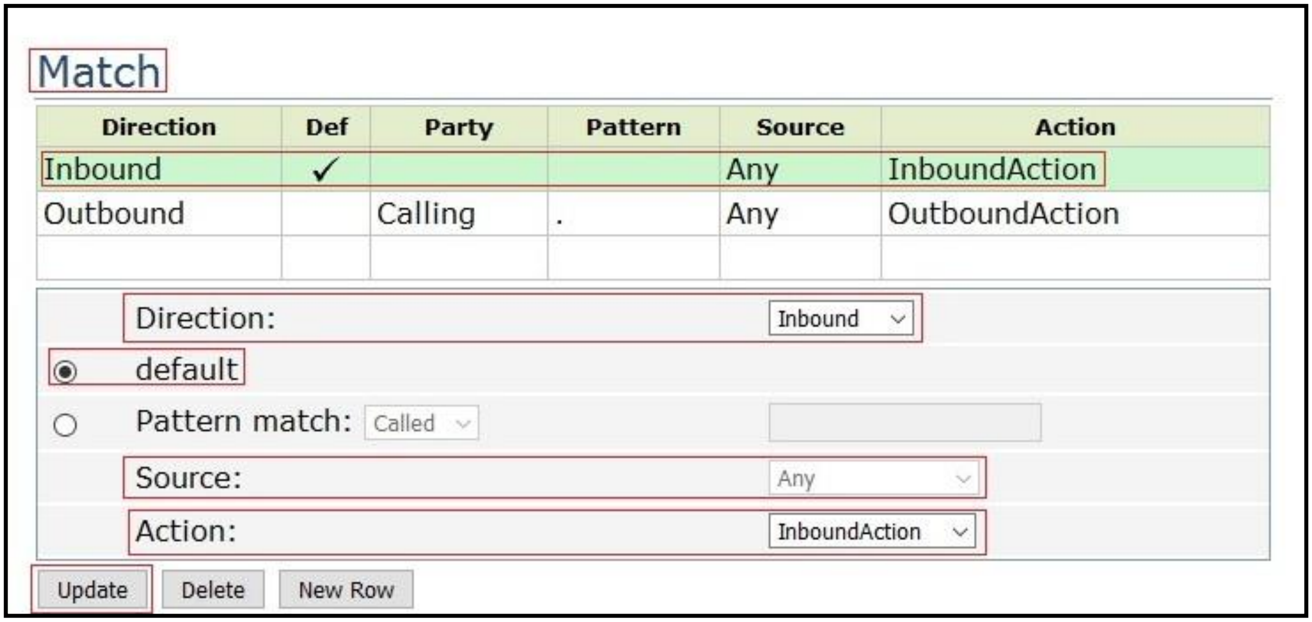

Figure 37 – Cox managed CPE Inbound Match Configuration

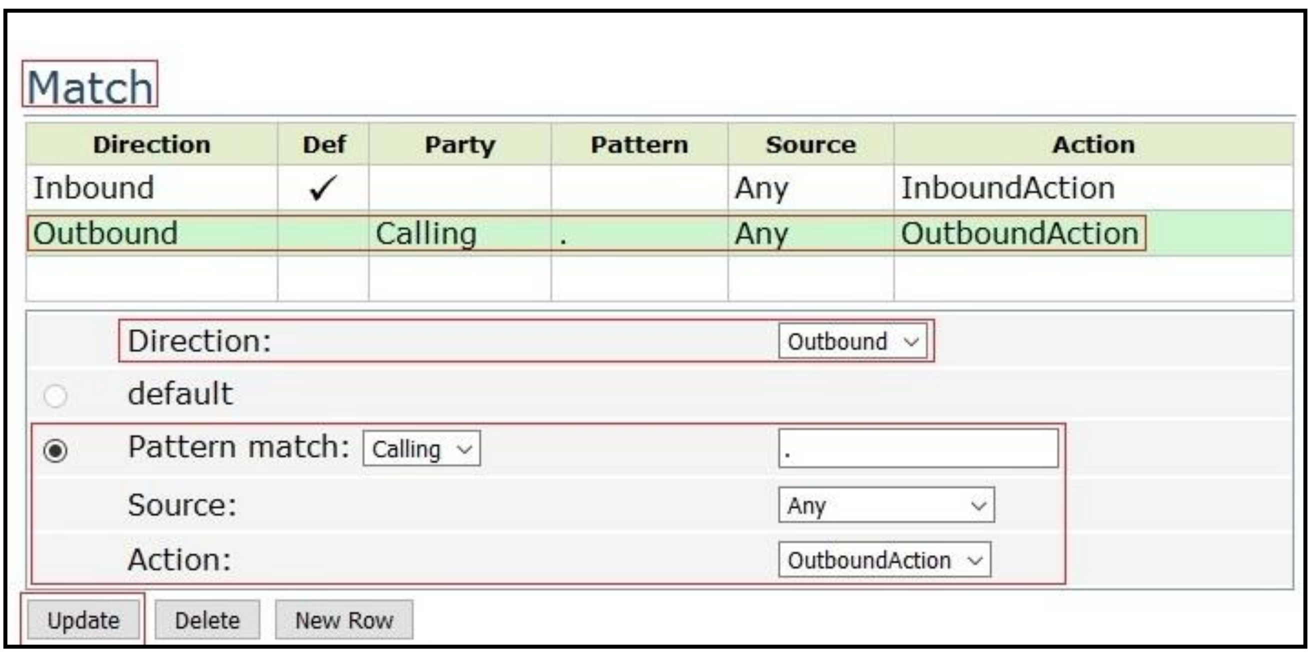

Figure 38 – Cox managed CPE Outbound Action Configuration

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.