Avaya Solution & Interoperability Test Lab

Application Notes for Posh Voice with Avaya IP Office 11.1 and Avaya Session Border Controller 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Posh Voice with Avaya IP Office release 11.1 and Avaya Session Border Controller release 10.1.

Posh Voice is a conversational AI IVR that interfaces with the Avaya solution via a SIP trunk service provider, functioning as an adjunct to the contact center. The initial call comes into Avaya IP Office and is then routed via the Avaya Session Border Controller to Posh Voice via a SIP service provider. Posh Voice interacts with callers to answer their questions and perform banking transactions using their voice in a conversational style, or DTMF using their telephone keypad. If required, Posh Voice can transfer the call back to Avaya IP Office, where it can be further processed and routed to agents or other internal or external endpoints.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

Table of Contents

1. Introduction

These Application Notes describe a reference configuration integrating an Avaya solution consisting of Avaya IP Office 11.1 and Avaya Session Border Controller 10.1 with Posh Voice.

Posh Voice is a conversational AI IVR that interfaces with the Avaya solution via a Posh Voice SIP service provider, functioning as an adjunct to the contact center. The initial call comes into Avaya IP Office and is then routed via the Avaya Session Border Controller to Posh Voice via a SIP service provider. Posh Voice interacts with callers to answer their questions and perform banking transactions using their voice in a conversational style, or DTMF using their telephone keypad. If required, Posh Voice can transfer the call back to Avaya IP Office, where it can be further processed and routed to IP Office agents, other enterprise endpoints or the PSTN.

Avaya IP Office (IP Office) is a versatile communications solution that combines the reliability and ease of a traditional telephony system with the applications and advantages of an IP telephony solution. This converged communications solution can help businesses reduce costs, increase productivity, and improve customer service.

Avaya Session Border Controller (Avaya SBC) is the point of connection between Avaya IP Office and the SIP Trunking service provider used to reach Posh Voice. Avaya SBC is used not only to secure SIP trunk connections, but also to make adjustments to the SIP signaling and media for interoperability.

Note: In these Application Notes, "Posh Voice SIP service provider" refers to a third-party SIP service provider used by Posh Voice that connects directly to Avaya SBC via a SIP trunk. Posh Voice does not provide SIP trunking services. As such, all calls between the Avaya solution and Posh Voice are routed through this SIP service provider.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on customer calls being routed via a simulated PSTN to IP Office, then to Posh Voice through the Avaya SBC and a SIP trunk service provider. Posh Voice then provided customer service via sample IVR application, which allowed customers to access information or be transferred back to an agent on IP Office. Customers interacted with Posh Voice using speech and DTMF via a telephone keypad. For example, callers made verbal requests to hear the business hours, get account balance, or to be transferred to an agent. For calls routed to an agent, Posh Voice provided customer information via UUI. Calls to Posh Voice testing and production environments were verified.

The serviceability test cases focused on simulating a network outage and also a restart on Avaya SBC. Calls to Posh Voice were verified to complete successfully after the network was restored and Avaya SBC came back in service.

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.

For the testing associated with this Application Note, the interface between Avaya SBC and the Posh Voice service provider used TLS encryption for SIP signaling, and SRTP for the media.

TLS/SRTP encryption was also used internally on the enterprise between Avaya SBC and the Avaya IP Office server and endpoints.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establish SIP trunk between Avaya SBC and the Posh Voice SIP service provider using TLS transport.
- Responses from the Posh Voice SIP service provider to SIP OPTIONS messages sent by Avaya SBC
- Inbound simulated PSTN calls routed from Avaya IP Office to Avaya SBC to Posh Voice testing and production environments.
- Posh Voice providing service to callers via a sample IVR application, and callers able to navigate the application using speech and DTMF.
- Proper call transfers from Posh Voice to an agent on the IP Office when the caller request live agent assistance.
- Inbound transferred calls from Posh Voice received on agents using Avaya SIP, H.323 and Deskphones, as well as Avaya Workplace Client for Windows softphone at the enterprise.
- Verify Posh Voice provided User-to-User (UUI) information in the Refer-To header of REFER message when transferring call to live agents.
- Proper disconnect when the call is abandoned by the caller before it is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Multiple simultaneous calls to Posh Voice.
- Telephony features, such as holding and resuming calls to Posh Voice, transferring calls to Posh Voice, joining Posh Voice in a conference, forwarding calls to Posh Voice, and calls to Posh Voice lasting more than 5 minutes.
- Proper call transfers from Posh Voice to the PSTN, via Avaya IP Office.
- DTMF transmission using RFC2833.
- SIP signaling encrypted using TLS 1.2.
- Audio encrypted using SRTP.
- Codecs G.711U and G.711A.
- Verify service is restored after a network outage.
- Verify service is restored after an Avaya SBC restart.

2.2. Test Results

Interoperability testing of Posh Voice with the Avaya solution was completed with successful results for all test cases. The following observations are noted for the sample configuration described in these Application Notes.

- **REFER Handling** − Avaya IP Office by default does not support REFER on inbound blind transfers on SIP trunks. The REFER should be handled by Avaya SBC. Enabling the Refer Handling option causes Avaya SBC to intercept and process the REFER and generate new SIP INVITE messages that are sent to the IP Office. Transfers from Posh Voice to IP Office agents and to the PSTN completed successfully after enabling this functionality on Avaya SBC.

- **User-to-User Information** – Posh Voice can provide User-to-User Information (UUI) on the Refer-To header of the REFER messages of calls that are transferred back to IP Office. The UUI data is delivered by Avaya SBC to IP Office in the User-to-User header of the new INVITE generated. At the time of the writing of these Application Notes, Avaya IP Office does not process the UUI in the User-to-User header, and the data is not passed either to other elements internally in the solution, the data is discarded.

2.3. Support

Technical support on Posh Voice can be obtained through the following:

- **Email:** support@posh.tech
- **Web:** https://www.posh.tech

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

3. Reference Configuration

Figure 1 below illustrates the test configuration with an Avaya IP Office solution connected to Posh Voice through the public internet, via the Posh Voice SIP service provider.

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

- IP Office Server Edition Primary Server
- IP Office Voicemail Pro
- IP Office Server Edition Expansion System (IP500 V2)
- Avaya Session Border Controller
- Avaya 96x1 Series IP Deskphones (H.323)
- Avaya J129 IP Deskphones (SIP)
- Avaya 9508 Digital Phones
- Avaya Workplace for Windows (SIP)

The IP Office Server Edition Primary Server runs the Server Edition Linux Release 11.1 software. Avaya Voicemail Pro runs as a service on the Primary Server. The LAN1 port of the primary server connects to the Avaya SBC internal interface. The Avaya SBC external interface is connected to the Posh Voice SIP service provider via the public network.

Note: The sample configuration used an Avaya IP Office Server Edition server on a VMware platform. Note that this solution is extensible to deployments using the standalone IP500 V2 platform as well.

The optional Expansion System (V2) is used for the support of digital, analog and additional IP stations. It consists of an Avaya IP Office 500 V2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) to provide VoIP resources.

Avaya endpoints are represented by Avaya 9608 H.323 Deskphones, Avaya J169 SIP Deskphones, Avaya 9508 Digital Deskphones, as well as Avaya Workplace for Windows (SIP) softphones.

Avaya SBC provides SIP Session Border Controller functionality, including address translation and SIP header manipulation between the SIP service provider and the CPE. In the reference configuration, Avaya SBC runs on a VMware platform. This solution is extensible to other Avaya Session Border Controller platforms as well.

In the reference configuration, Avaya SBC receives and sends traffic to the SIP service provider on port 5061, using TLS for network transport.

Inbound PSTN calls from users can arrive to Avaya IP Office via SIP, ISDN trunk, etc. In the reference configuration, a simulated PSTN SIP trunk is used to generate the inbound calls. The call is then routed by IP Office to Avaya Session Border Controller and to Posh Voice via the Posh Voice SIP service provider. Posh Voice interacts with callers to answer their questions and perform banking transactions using their voice in a conversational style, or DTMF using their telephone keypad. If the caller request live agent assistance, Posh Voice can transfer the call back to Avaya IP Office, where it can be further processed and routed to IP Office agents or other endpoints at the enterprise or the PSTN.

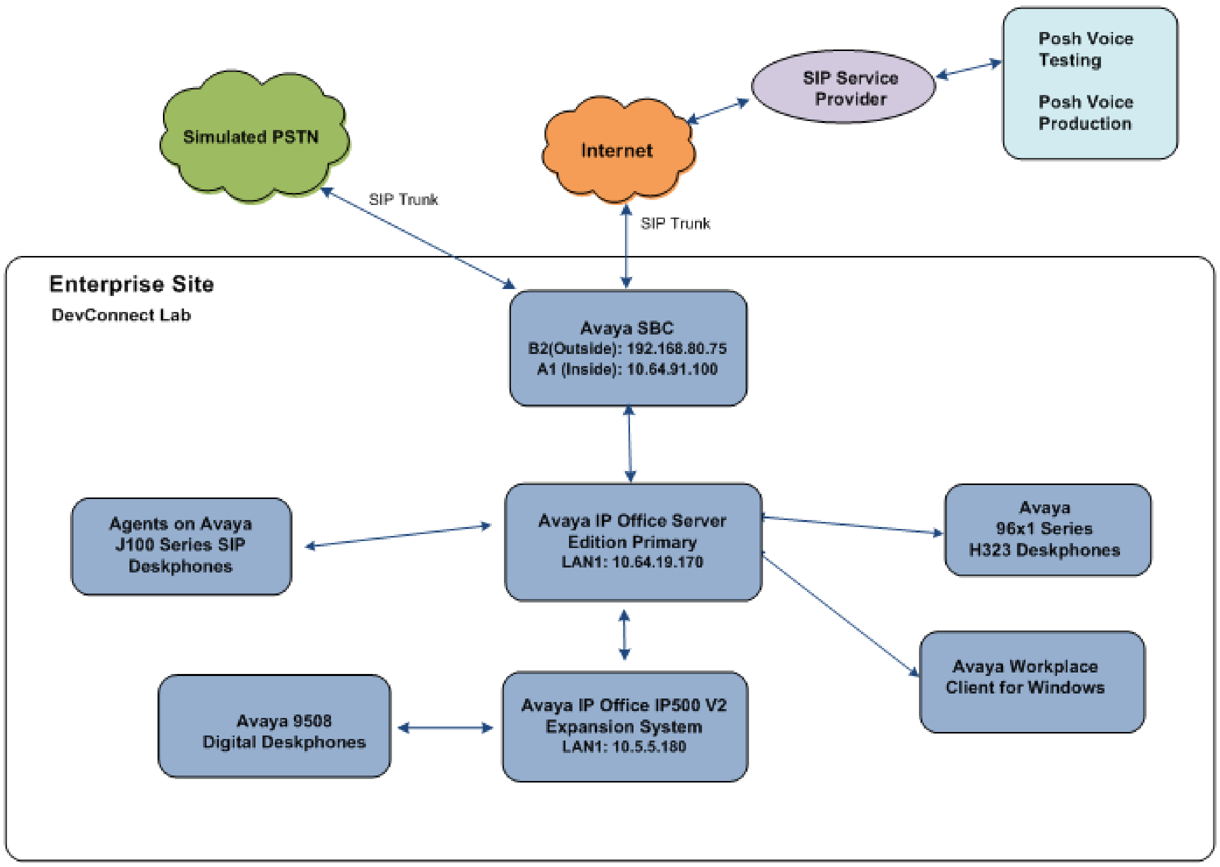


Figure 1: Avaya Interoperability Test Lab Configuration for Posh Voice

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment/Software	Release/Version
Avaya IP Office Server Edition Avaya IP Office Voicemail Pro	Release 11.1.2.4.0 Build 18 Release 11.1.2.4.0 Build 2
Avaya IP Office 500 V2 Expansion System	Release 11.1.2.4.0 Build 18
Avaya IP Office Server Edition Manager	Release 11.1.2.4.0 Build 18
Avaya Session Border Controller	10.1.2.0-64-23285
Avaya 96x1 Series IP Deskphone (H.323)	Release 6.8.5.2.3
Avaya J169 IP Deskphone (SIP)	Release 4.0.6.0.7
Avaya Workplace for Windows (SIP)	Release 3.34.0.118
Avaya 9508 Digital Deskphone	Release 0.60
Posh Voice	July 2023

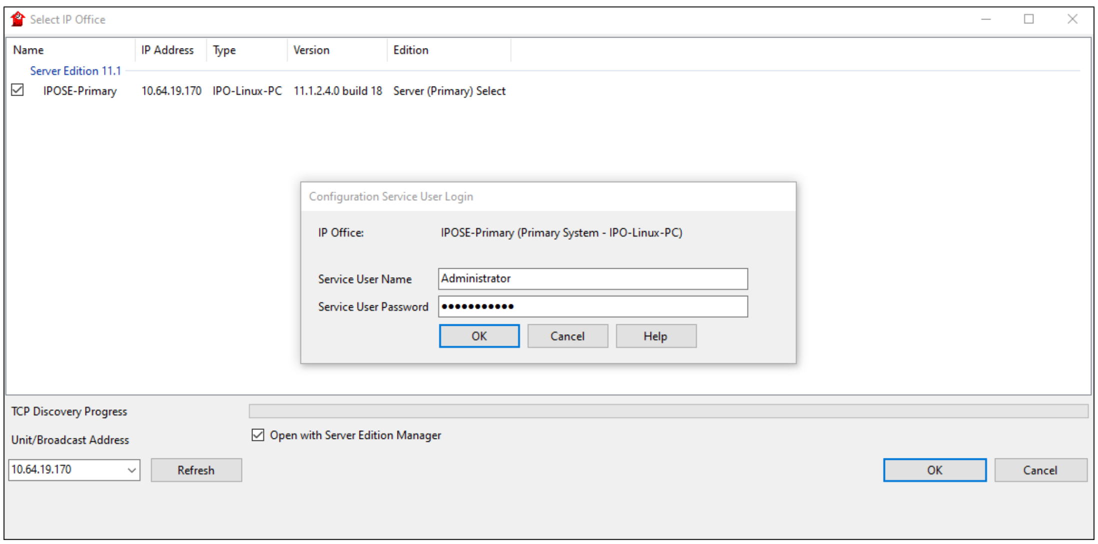
Table 1: Equipment and Software Used in the Sample Configuration

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. Note that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks.

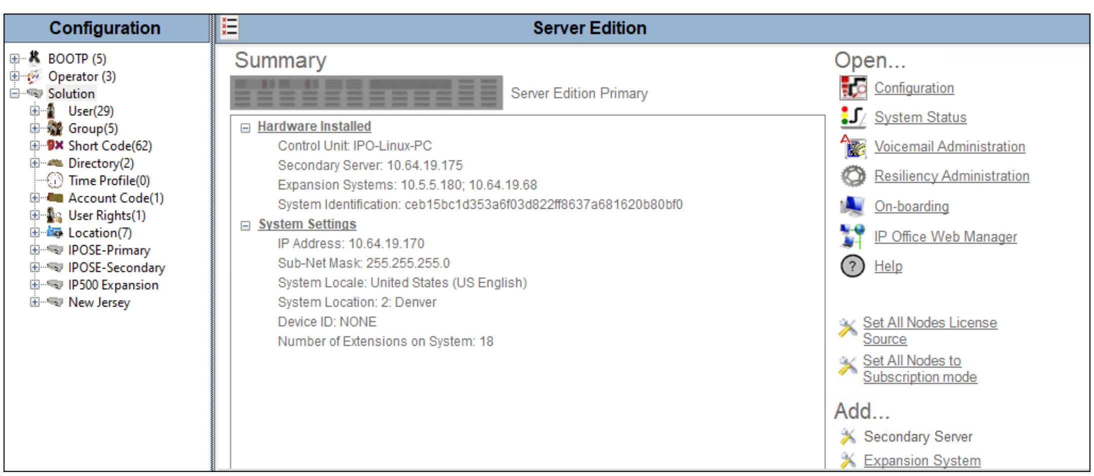
5. Avaya IP Office Configuration

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

IP Office is configured via the IP Office Manager program. For more information on IP Office Manager, consult reference [**1**]. From the IP Office Manager PC, select **Start → All Apps → IP Office → Manager** to launch the Manager application. Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials.



On Server Edition systems, the Solution View screen will appear, similar to the one shown below. 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.

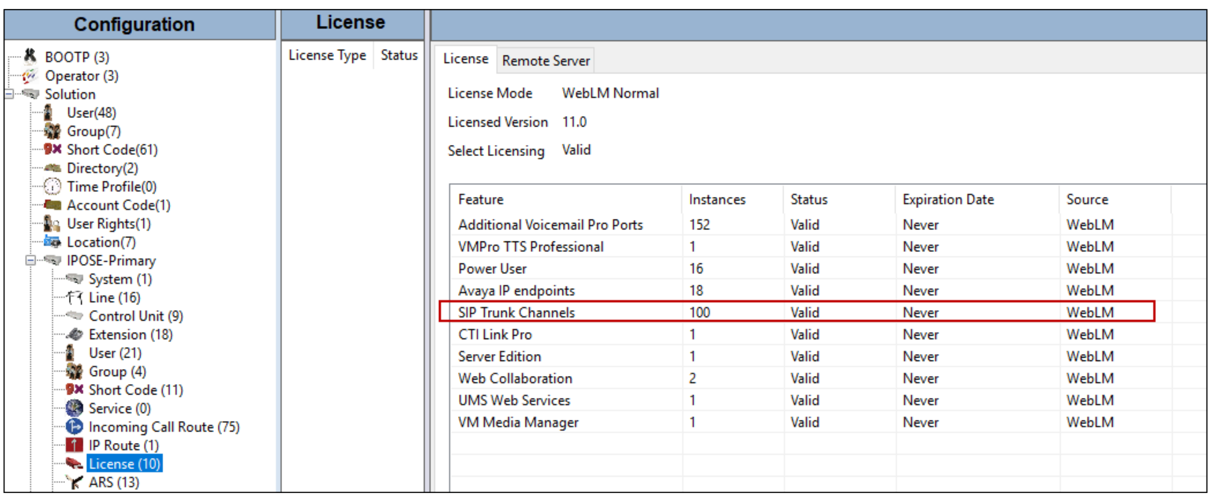


5.1. Licensing

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.

In the reference configuration, **IPOSE-Primary** was used as the system name of the Primary Server and **IP500 Expansion** was used as the system name of the Expansion System. All navigation described in the following sections (e.g., **License**) appears as submenus underneath the system name in the Navigation Pane. To verify that there is a SIP Trunk Channels license with sufficient capacity, select **Solution → IPOSE-Primary → License** on the Navigation pane and SIP Trunk Channels in the Group pane. Verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of channels provisioned for the SIP trunk.

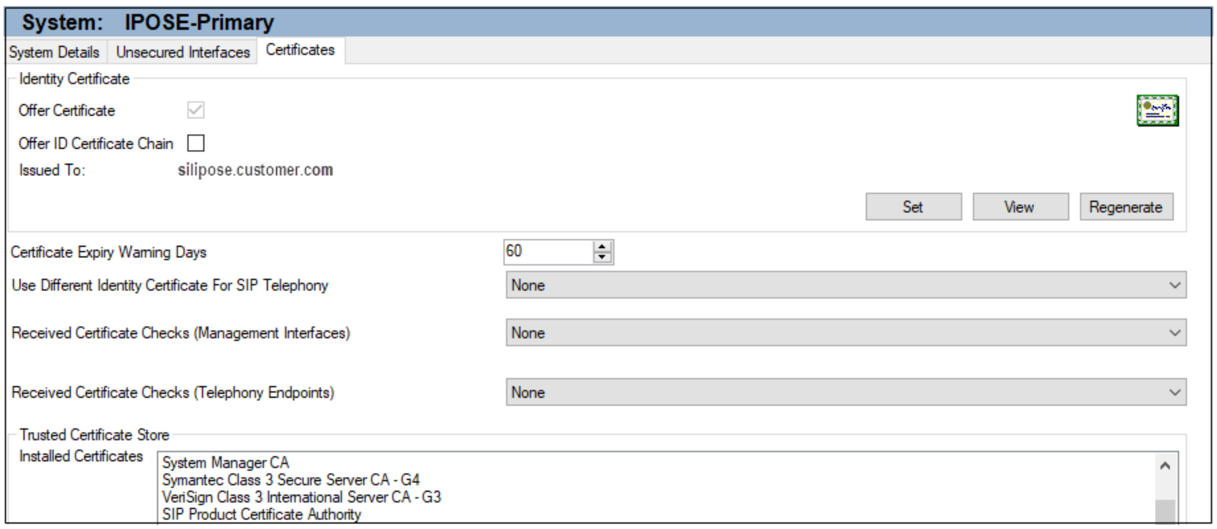


5.2. TLS Management

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

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

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

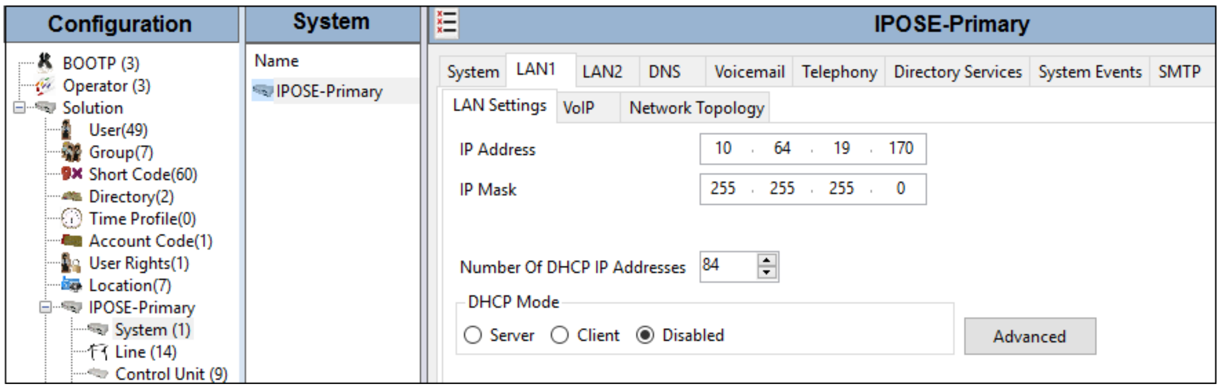


5.3. System Settings

This section illustrates the configuration of system settings. Select **System** in the Navigation pane to configure these settings. The subsection order corresponds to a left to right navigation of the tabs in the Details pane for System settings. For all of the following configuration sections, the **OK** button (not shown) must be selected in order for any changes to be saved.

5.3.1 LAN1 Settings

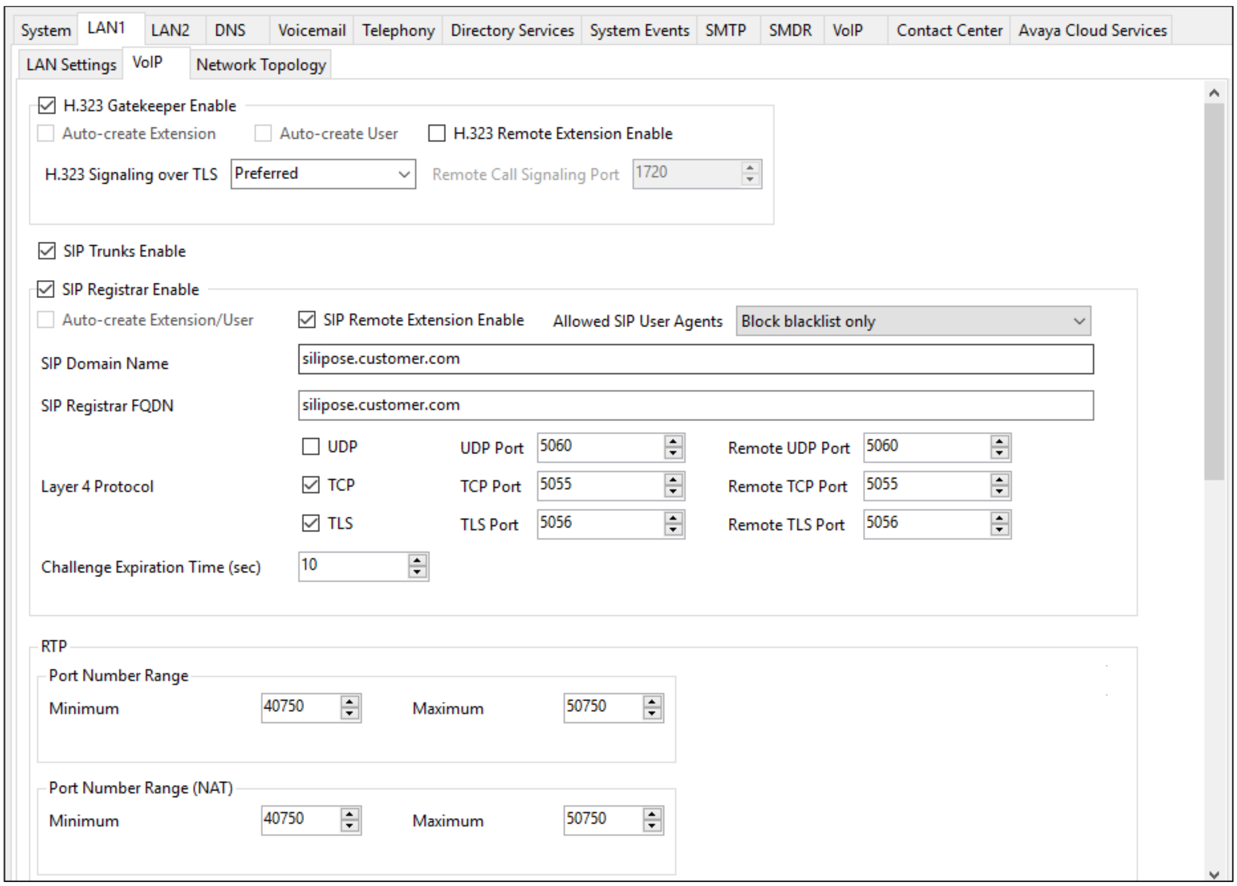
In the reference configuration, LAN1 is used to connect the Primary server to the enterprise network. To view or configure the **IP Address** of LAN1, select the **LAN1** tab followed by the **LAN Settings** tab. As shown in **Figure 1**, the IP Address of the Primary server is **10.64.19.170**. Other parameters on this screen may be set according to customer requirements.



Select the **VoIP** tab as shown in the following screen. The **H.323 Gatekeeper Enable** parameter is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the Avaya 96x1 Deskphones used in the reference configuration. The **H.323 Signaling over TLS** should be set based on customer needs. In the reference configuration it was set to **Preferred**. The **SIP Trunks Enable parameter** must be checked to enable the configuration of the SIP trunk to Avaya SBC. The **SIP Registrar Enable** parameter is checked to allow Avaya J169, and Avaya Workplace for Windows (SIP) usage.

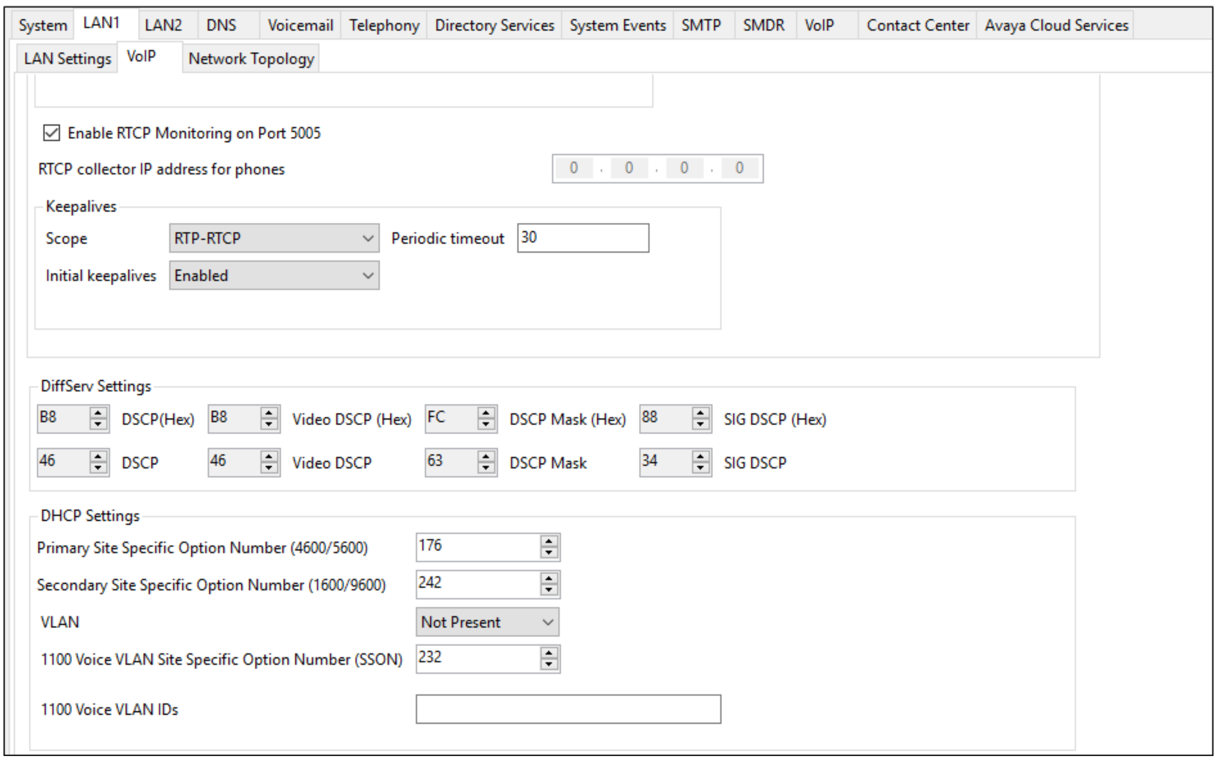
The **SIP Domain Name** and **SIP Registrar FQDN** may be set according to customer requirements. Set the **Layer 4 Protocol** section based on customer needs. In the reference configuration **TCP/5055** and **TLS/5056** were configured.

If desired, the **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media paths from Avaya SBC to the Primary server. The defaults are used here.

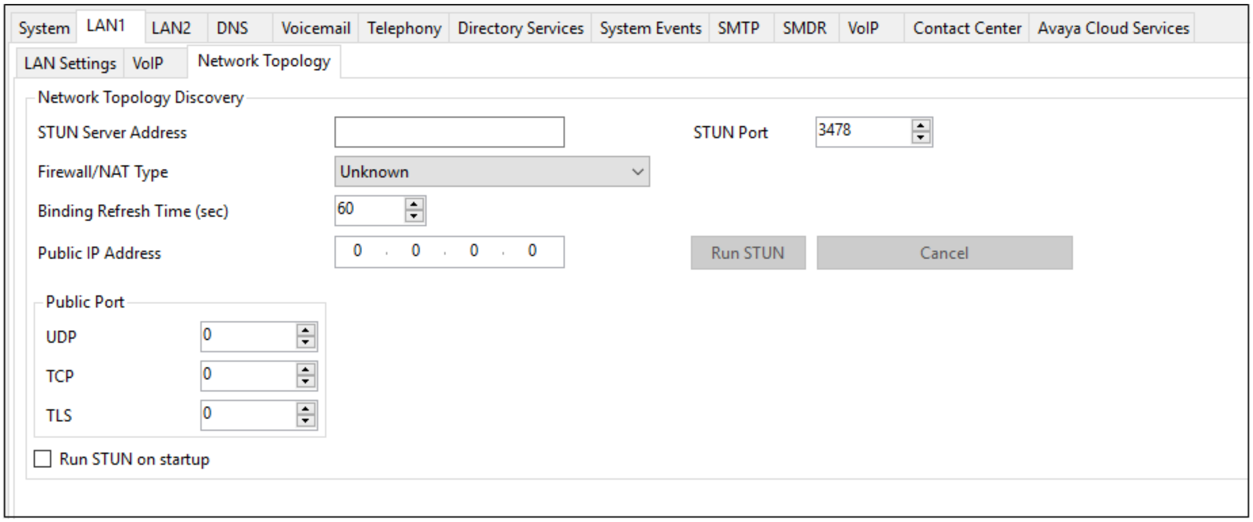


Scrolling down the page, on the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. These settings will cause the Primary server to send RTP and RTCP keepalive packets starting at the time of initial connection and every 30 seconds thereafter if no other RTP or RTCP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting to see media from the other, as well as helping to keep ports open for the duration of the call.

In the **DiffServ Settings** section, the Primary server can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services (QoS) policies for both signaling and media. The **DSCP** field is the value used for media, while the **SIG DSCP** is the value used for signaling. These settings should be set according to the customer's QoS policies in place. The default values used during the compliance test are shown.

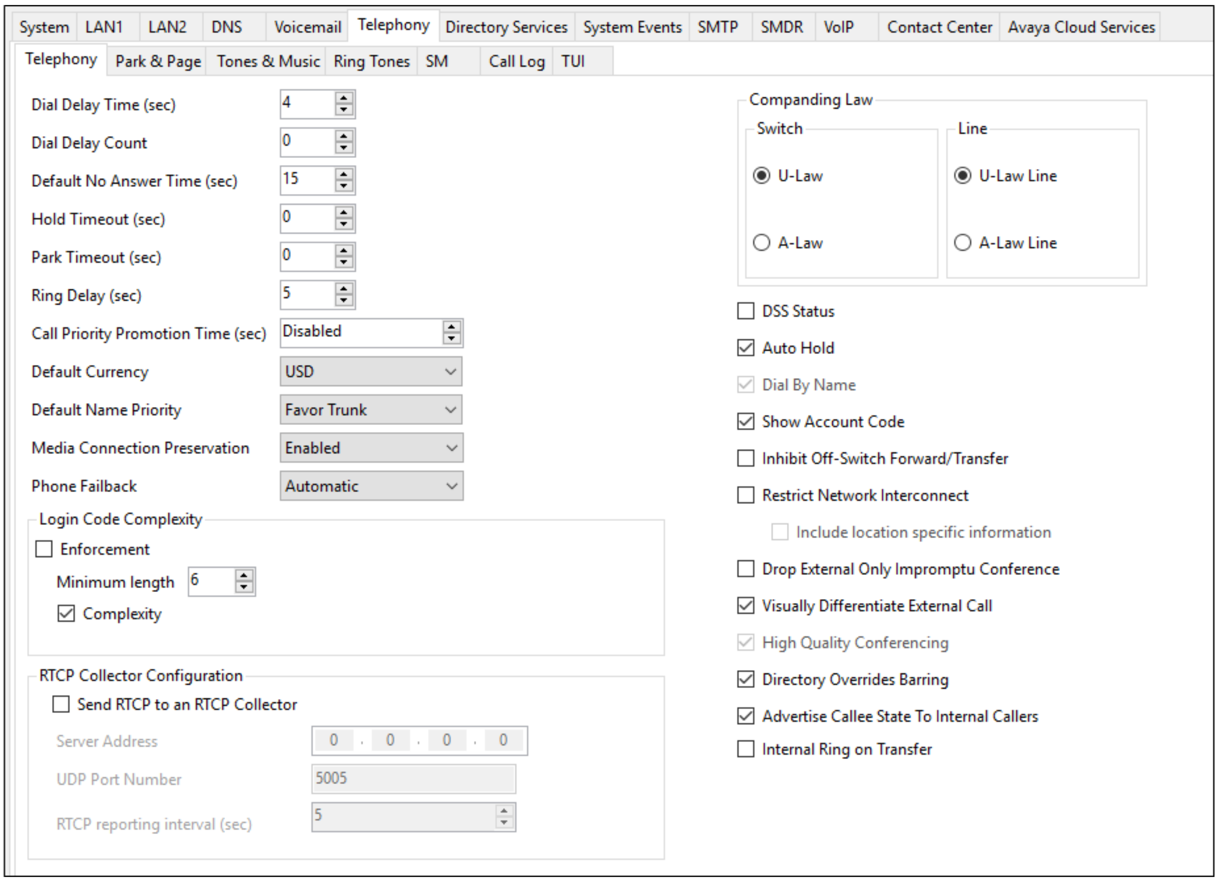


Select the **Network Topology** tab as shown in the following screen. The **Firewall/NAT Type** was set to **Unknown** in the reference configuration. **Binding Refresh Time (sec)** was set to **60** seconds. This is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages, to periodically check the status of the SIP lines configured on this interface. The **Public IP Address** and **Public Port** sections were not used in this configuration.



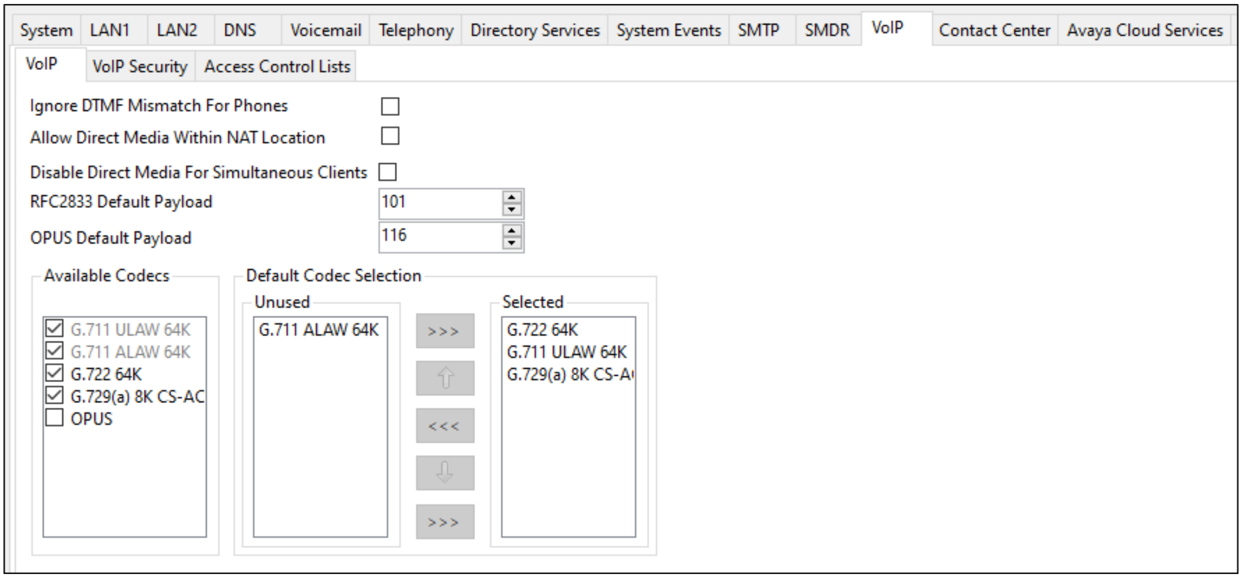
5.3.2 System Telephony Settings

To view or change telephony settings, select the **Telephony** tab and **Telephony** sub-tab as shown in the following screen. The settings presented here simply illustrate the reference configuration and are not intended to be prescriptive. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer over the SIP trunk to Posh Voice. That is, a call can arrive from the PSTN to IP Office on one trunk and be forwarded or transferred on another trunk. The **Companding Law** parameters are set to **U-Law** as is typical in North American locales. Other parameters on this screen may be set according to customer requirements.



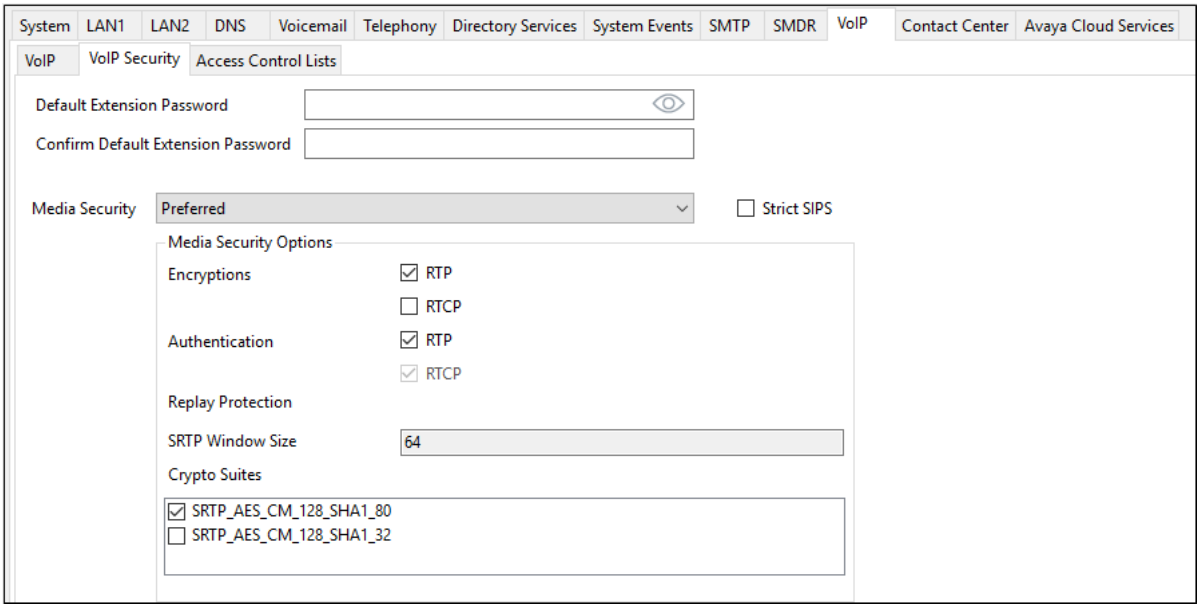
5.3.3 System VoIP Settings

To view or change system codec settings, select the **VoIP → VoIP** tab. 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.



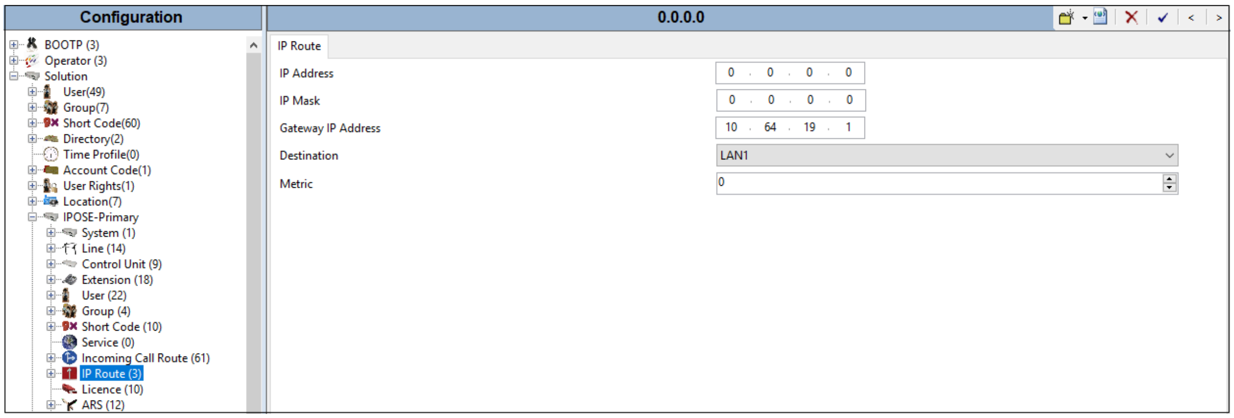
Note: The codec selections defined under this section are the codecs selected for the IP phones/ extensions. The codec selections defined under **Section 5.5.4** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

During the compliance test, SRTP was used internally on the enterprise wherever possible. To view or configure the media encryption settings, select the **VoIP → VoIP Security** tab on the Details pane. The **Media Security** drop-down menu is set to **Preferred** to have IP Office attempt to use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption. Under **Media Security Options**, **RTP** is selected for the **Encryptions** and **Authentication** fields. Under **Crypto Suites**, **SRTP_AES_CM_128_SHA1_80** is selected.



5.4. IP Route

In the reference configuration, the Primary server LAN1 port is physically connected to the local area network switch at the IP Office customer site. The default gateway for this network is 10.64.19.1. Avaya SBC resides on a different subnet and requires an IP Route to allow SIP traffic between the two devices. To add an IP Route in the Primary server, right-click **IP Route** from the Navigation pane, and select **New** (not shown). To view or edit an existing route, select **IP Route** from the Navigation pane, and select the appropriate route from the Group pane. The following screen shows the Details pane with the relevant route using **Destination LAN1**.



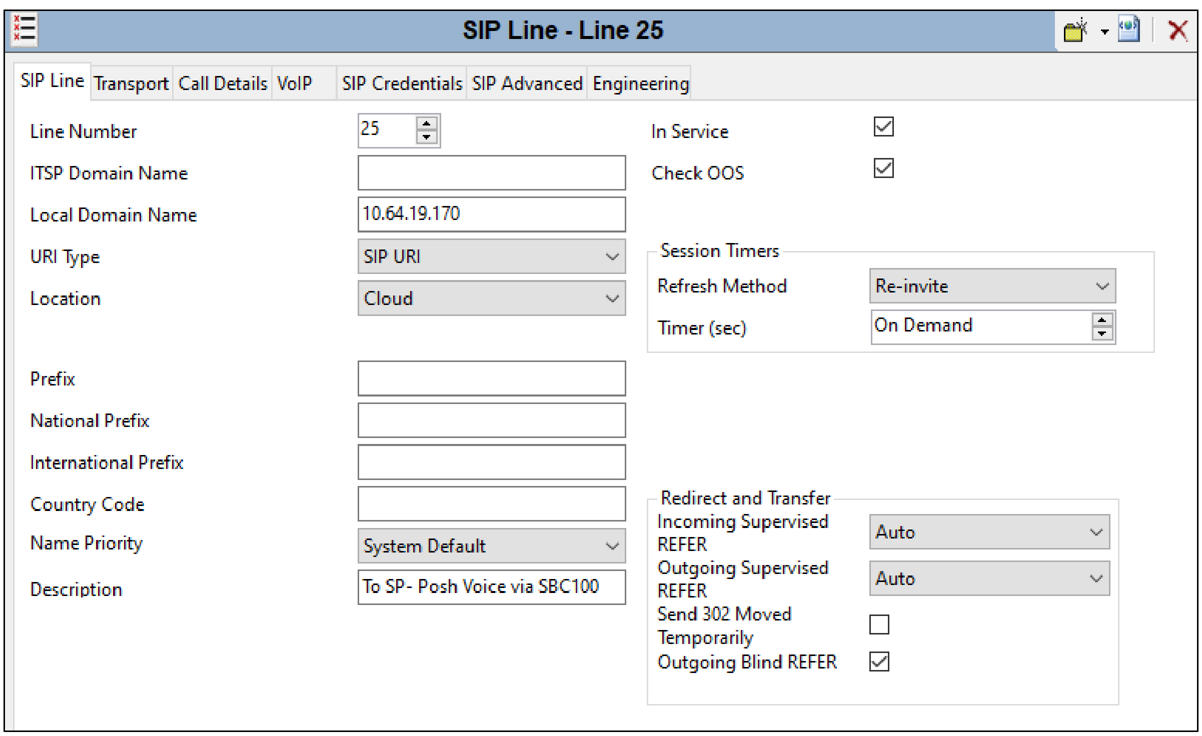
5.5. SIP Line

This section shows the configuration details for the SIP Line in IP Office Release 11.1 needed to establish the SIP connection between Avaya IP Office Server Edition and Posh Voice system via Avaya SBC.

5.5.1 SIP Line – SIP Line Tab

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:

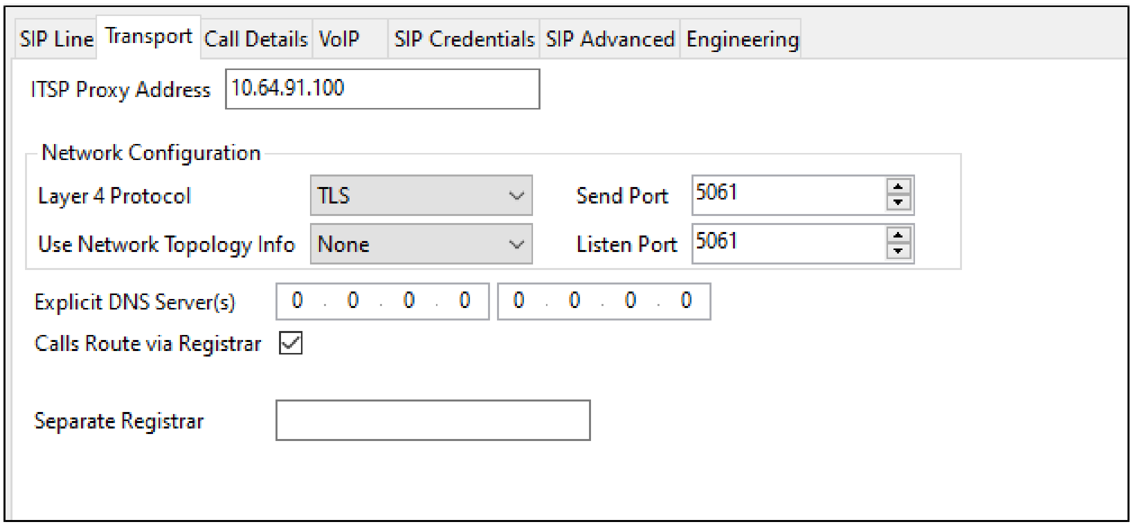
- Select an available **Line Number**: Line **25** was used.
- Check the **In Service** and **Check OOS** box.
- **ITSP Domain Name**: Leave blank.
- Input **Local Domain Name**: IP Office Primary Server LAN1 interface (e.g., **10.64.19.170**).
- Set **URI Type** to **SIP URI**
- Under **Session Timers**, set **Refresh Method** to **Re-invite** and **Timer (sec)** to **On Demand**
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Auto**.
- The **Outgoing Blind REFER** box can be optionally checked to enable use of REFER for outbound blind transfers. In the reference configuration, this parameter is checked.
- Default values may be used for all other parameters.
- Click **OK** to commit.



5.5.2 SIP Line – Transport Tab

Select the **Transport** tab. Set the following:

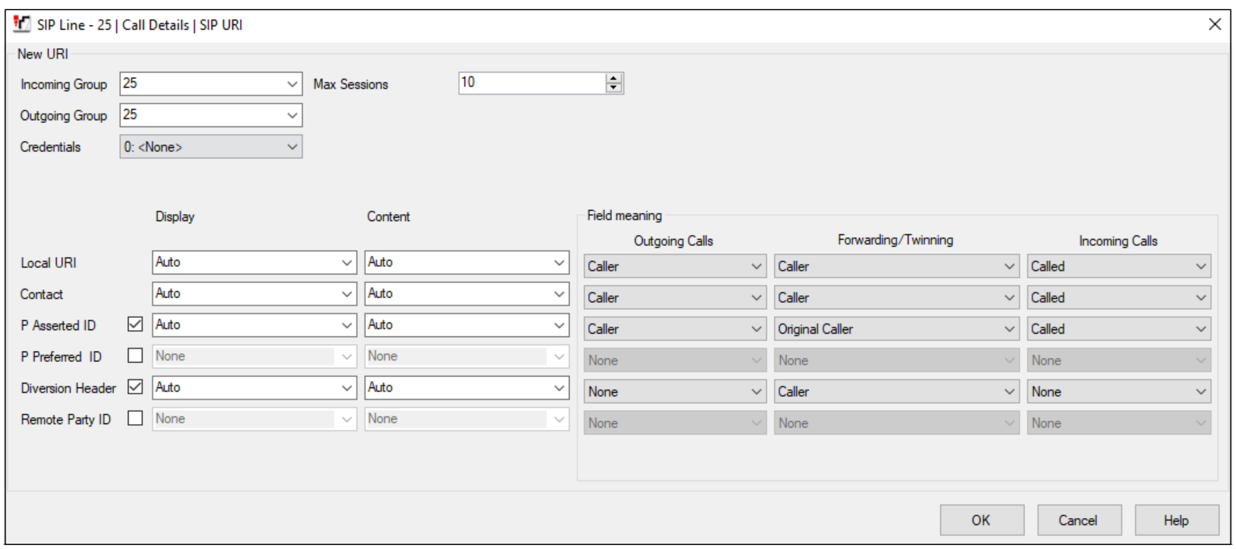
- The **ITSP Proxy Address** is set to the inside IP address of Avaya SBC as shown in **Figure 1**.
- In the **Network Configuration** area, **TLS** is selected as the **Layer 4 Protocol**. The **Send Port** and **Listen Port** can retain the default value 5061.
- The **Use Network Topology Info** parameter is set to **None**.
- Default values may be used for all other parameters.
- Click **OK** to commit.



5.5.3 SIP Line – Call Details Tab

Select the **Call Details** tab. To add a new SIP URI, click the **Add…** button. A New URI area will be opened. To edit an existing entry, click an entry in the list at the top, and click the **Edit…** button (not shown). Set the following parameters:

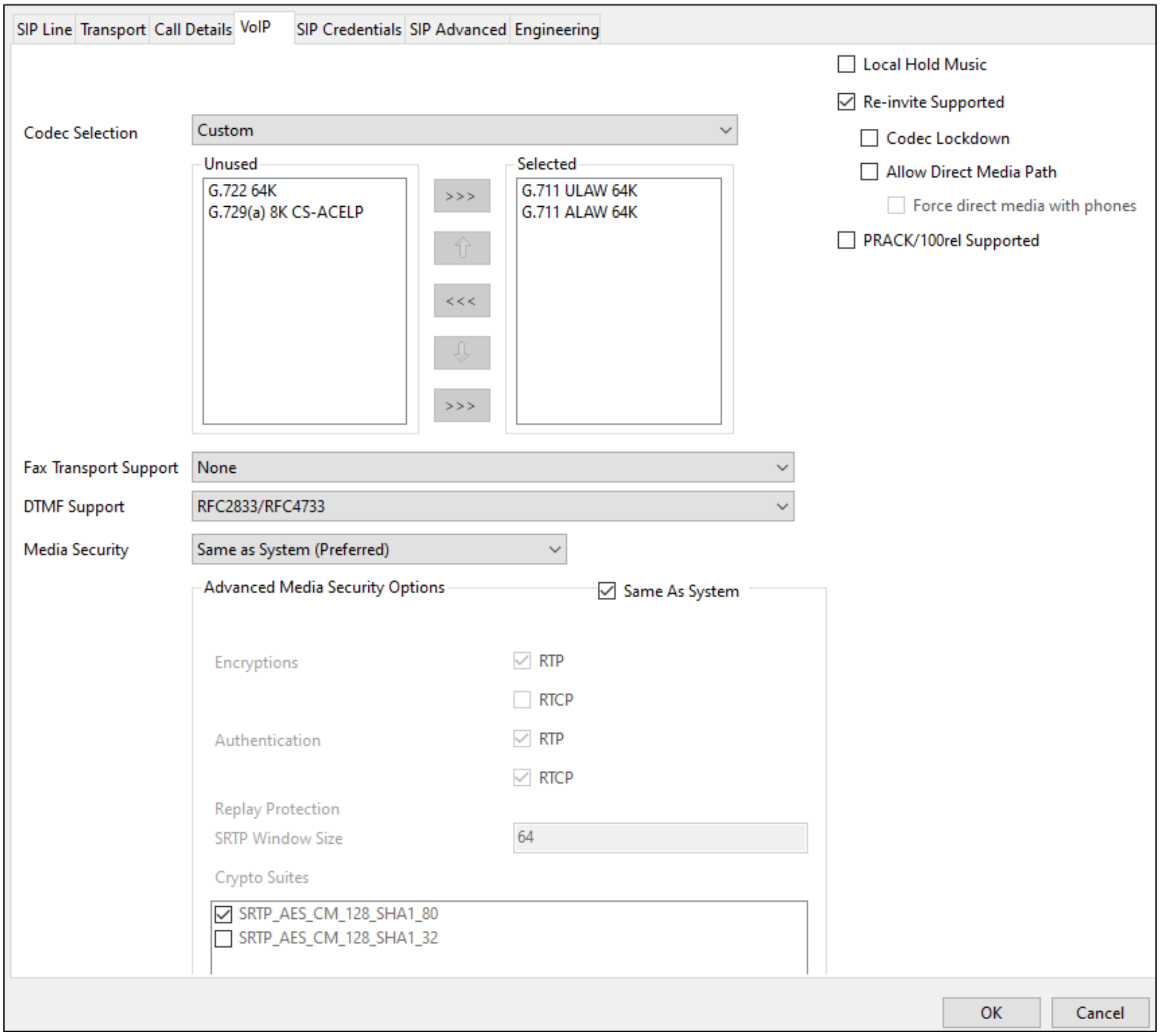
- The **Incoming Group** parameter, set here to **25**, will be referenced when configuring Incoming Call Routes to map inbound transferred calls from Posh Voice to IP Office destinations in **Section 5.8**. The **Outgoing Group** parameter, also set to **25**, will be used for routing outbound calls to Posh Voice via a Short Code (**Section 5.7**).
- The **Max Sessions** parameter was set to **10**. This value sets the maximum number of simultaneous calls that can use the URI before IP Office returns busy to any further calls.
- Select **Credentials** to **0: <None>**
- Check **P Asserted ID** option.
- Check **Diversion Header** option.
- **Auto** is selected for the **Local URI** and **Contact** parameters. With this configuration, information in the Incoming Call Route (**Section 5.8**) is used to determine what call is accepted on the SIP Line. Set the **Field meaning** section to the values shown in the screenshot below.
- Click **OK** to submit.



5.5.4 SIP Line – VoIP Tab

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

- The **Codec Selection** can be selected by choosing **Custom** from the pull-down menu, allowing an explicit ordered list of codecs to be specified. The **G.711 ULAW 64K** and **G.711 ALAW 64K** codecs are selected. This will cause IP Office to include G.711U and G.711A in the Session Description Protocol (SDP) offer, in that order.
- Check the **Re-invite Supported** box.
- The **DTMF Support** parameter remains set to the default value **RFC2833/RFC4733**.
- Set the **Media Security** field to **Same as System (Preferred)**.
- Default values may be used for all other parameters.
- Click **OK** to submit the changes.



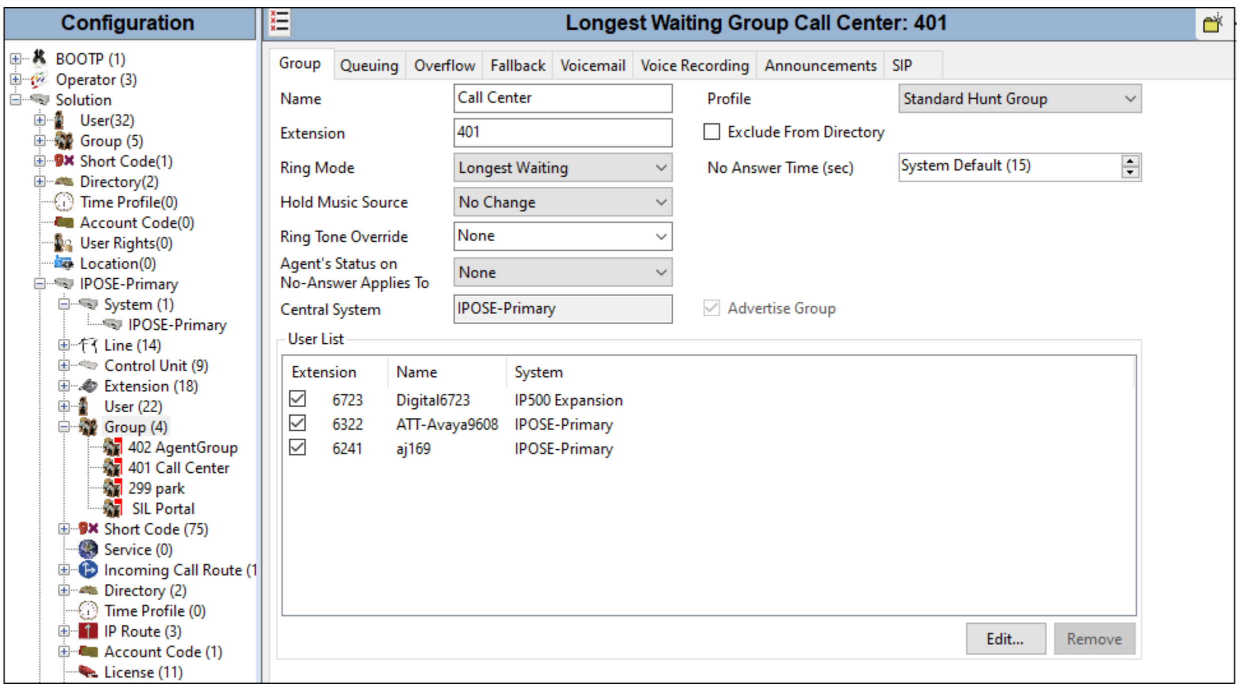
Note: no changes were made to the parameters on the **SIP Credentials**, **SIP Advanced** and **Engineering** tabs, which retained their default values.

5.6. Hunt Groups

During the verification of these Application Notes, inbound transferred calls from Posh Voice were sent to agents in IP Office hunt groups. While it is not the focus of this document, the following screens show an example configuration on one of the hunt groups used during the tests.

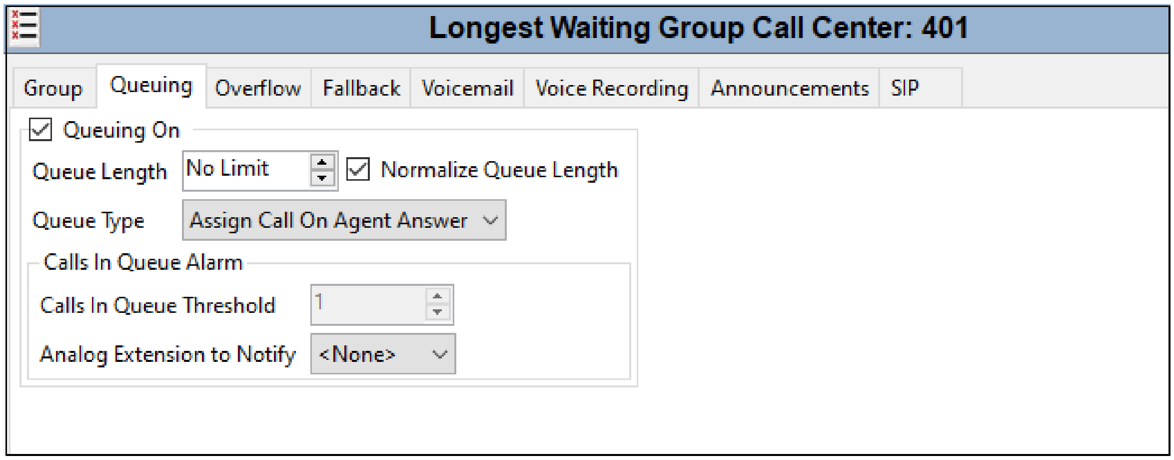
To configure a new hunt group, right-click **Group** (not shown) from the Navigation pane and select **New**. To view or edit an existing hunt group, select **Group** from the Navigation pane, and the appropriate hunt group from the Group pane.

The following screen shows the **Group** tab for a hunt group with **Extension 401** and **Name Call Center**. This hunt group was configured to contain various Avaya telephone types as shown on **Figure 1**. The **Ring Mode** was set to **Longest Waiting** (i.e., "longest waiting", most idle user receives next call). Clicking the **Edit** button allows to make changes to the **User List**.

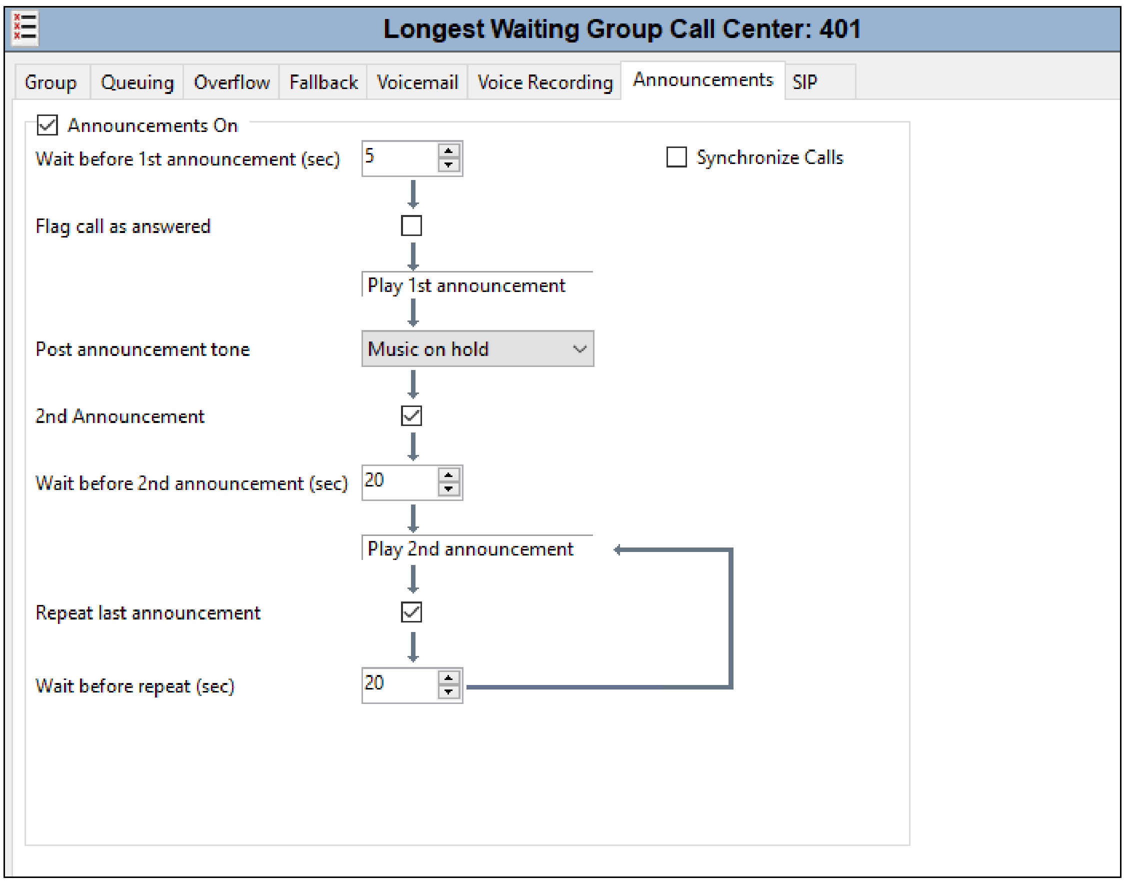


The following screen shows the **Queuing** tab for hunt group 401. In the reference configuration, the hunt group was configured to allow queuing so that incoming calls transferred from Posh Voice could be queued when all the members of the hunt group were busy on calls. The **Queue Length** was set to “No Limit”, but it can be set to specifically sized queues.

IP Office supports priority for queuing. For example, if low priority calls are waiting in queue, a higher priority call entering queue can be moved to the front of the queue and serviced before lower priority callers. For an inbound SIP trunk call, the priority can be specified on the Incoming Call Route as shown in **Section 5.8**.



The following screen shows the **Announcements** tab for hunt group 401. In this reference configuration, when a call arrives, when all members of the hunt group are busy on calls, the caller will first hear ring back tone. If a member of the hunt group does not become available after 5 seconds, the call will be answered by IP Office (i.e., 200 OK will be sent to Posh Voice), and the caller will hear a first announcement. Note that the **Flag call as answered** box is relevant for reporting applications but does not change the fact that IP Office will answer the call when the first announcement is played. If the call is still not answered after the first announcement completes, the caller will hear music, a repeating second announcement, music, and so on until the call is answered by a member of the hunt group or answered by voicemail for the hunt group (if this is configured). If a member of the hunt group becomes available while the caller is listening to ring back, music, or an announcement, the call is de-queued and delivered to the available member.



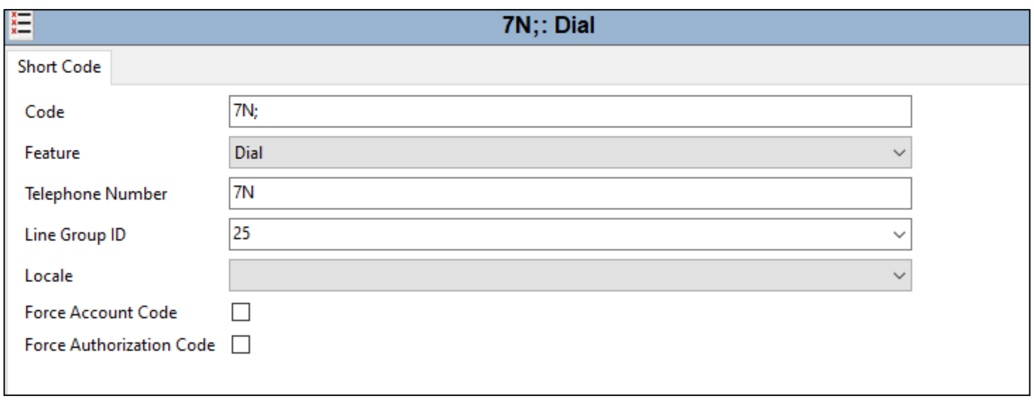
5.7. Short Codes

During the compliance test, numbers 78701 and 78702 were used to route calls to Posh Voice testing and production environments, respectively.

A short code was defined to route outbound traffic on the SIP trunk to Posh Voice. To add a short code, right click on **Short Code** (not shown) in the Navigation pane and select **New**. To edit an existing short code, click **Short Code** in the Navigation pane, and the short code to be configured in the Group pane.

The screen below shows the details of the **7N;** short code for Primary System, used in the test configuration. Navigate to **Solution → IPOSE-Primary → 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, **7N;**, this short code will be invoked when the received string is 7, followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to 7**N**.
- Set the **Line Group ID** to the **Outgoing Group 25** defined on the **Call Details** tab on the **SIP Line** in **Section 5.5.3**. This short code will use this line group when placing the outbound call.
- Default values may be used for all other parameters.
- Click **OK** to submit the changes.



Note: An existing Short Code 8N in the configuration was used to route calls via ARS to a simulated PSTN via a SIP Line (27). This will be referenced in later sections. The configuration of the elements related to this simulated PSTN trunk is not the focus of these Application Notes and it is not included in this document.

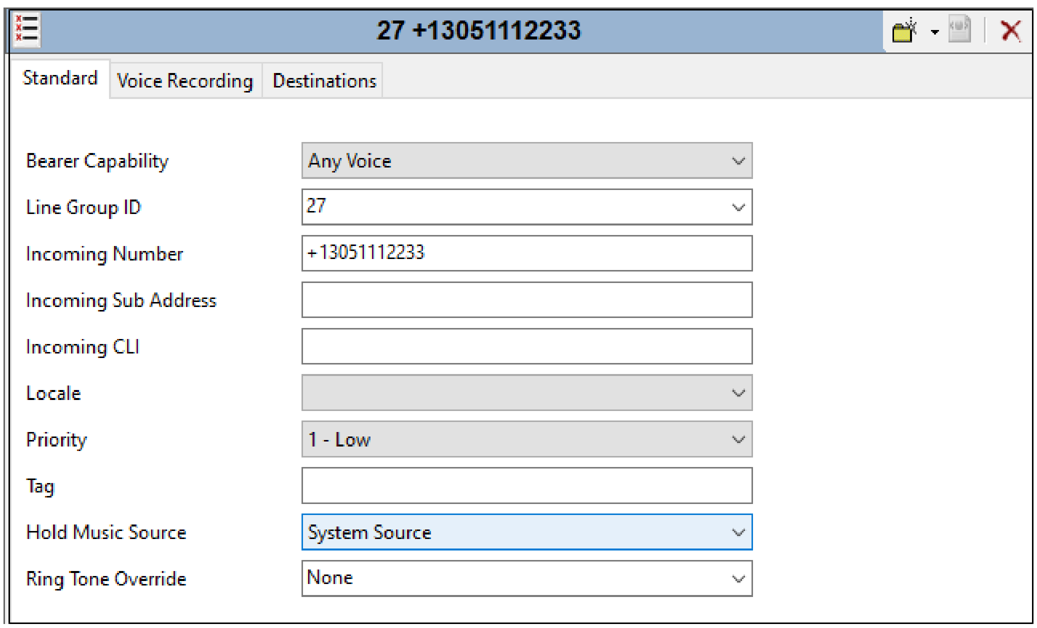
5.8. Incoming Call Routes

Incoming Call Routes map inbound numbers to a destination user, group, or function in the IP Office. To add an incoming call route, right click on **Incoming Call Route** (not shown) in the Navigation pane and select **New**. To edit an existing incoming call route, select **Incoming Call Route** in the Navigation pane, and the appropriate incoming call route to be configured in the Group pane.

5.8.1 Incoming Call Routes – Inbound PSTN Calls

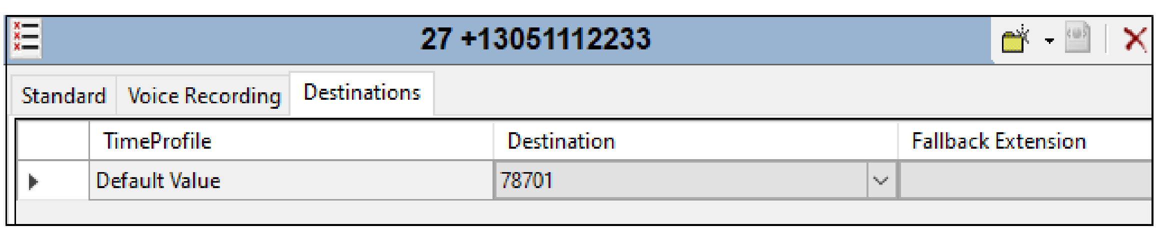
The screen below shows the incoming call route for one of the test numbers used to simulate inbound PSTN calls in the lab to the Posh Test environment.

- The **Line Group Id** is **27**, which is the SIP Line used for the simulated PSTN. See Note on **Section 5.7**.
- **Incoming Number** is set to **+13051112233** in the example.



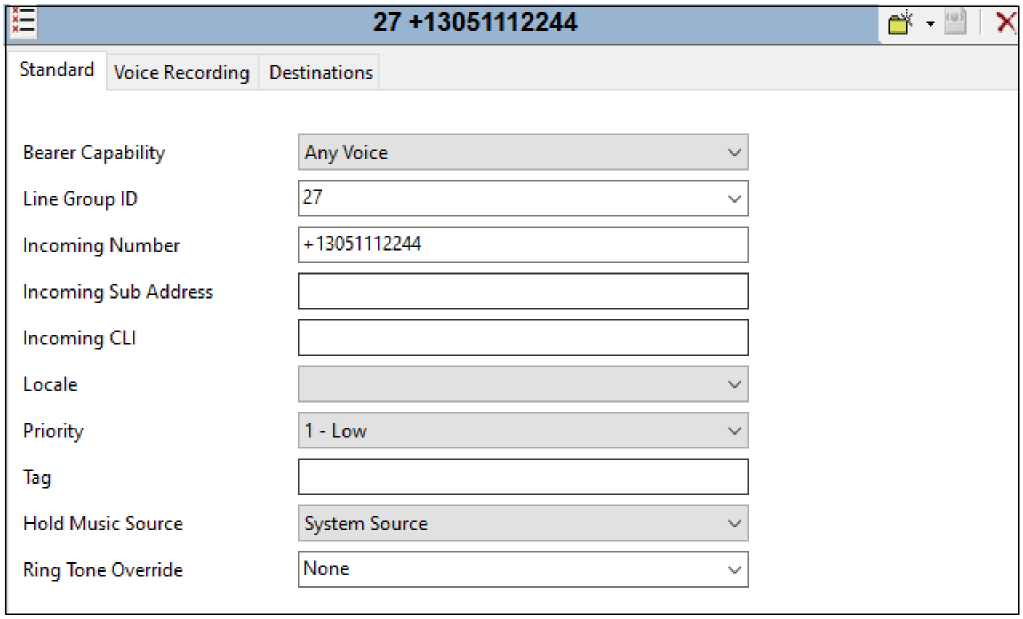
Select the **Destinations** tab.

- The **Destination** field is set to **78701**. This number will be used to route the calls to the Posh Test environment via SIP Line 25 (**Section 5.5**). This is done using the Short Code shown on **Section 5.7**.



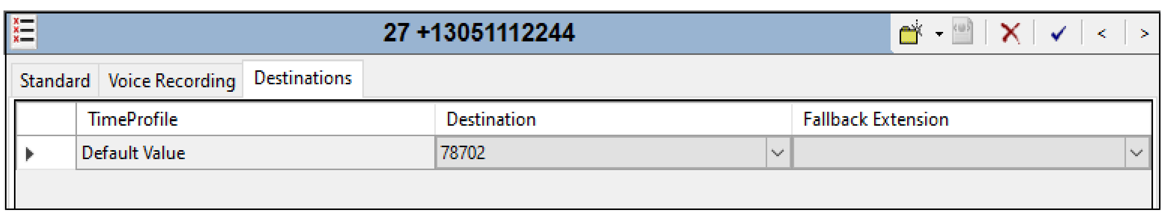
A second Incoming Call Route was created to route another simulated PSTN number to the Posh Voice production environment.

- The **Line Group Id** is **27**, which is the SIP Line used for the simulated PSTN.
- **Incoming Number** is set to **+13051112244** in the example.



Select the **Destinations** tab.

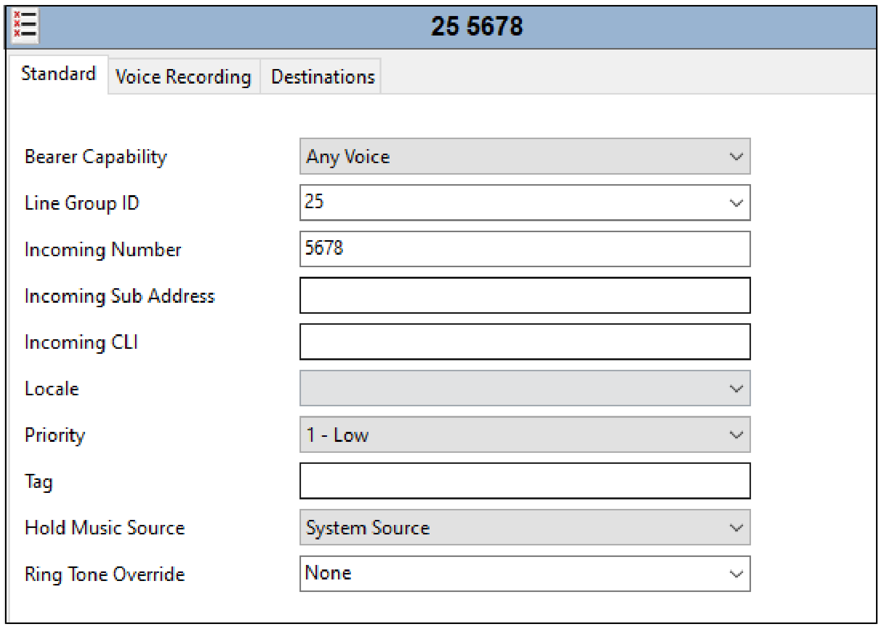
- The **Destination** field is set to **78702**. This number will be used to route the calls to the Posh Production environment via SIP Line 25 (**Section 5.5**). This is done using the Short Code shown on **Section 5.7**.



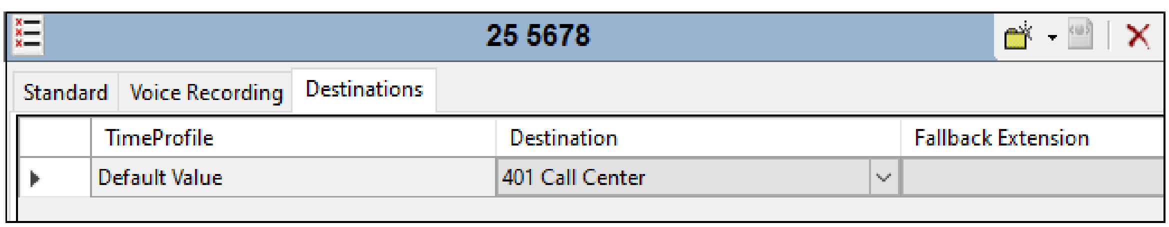
5.8.2 Incoming Call Routes – Posh Voice Transferred Calls to Hunt Group

The screen shown below, an incoming call route for **Incoming Number 5678** as illustrated. This number was sent as the SIP URI user in the Refer-To header on the REFER sent from Posh Voice, for calls that are to be transferred to an agent on a hunt group in the IP Office

- **Line Group Id** is **25**
- The **Incoming Number** is set to **5678** in the example.



Select the **Destinations** tab. From the **Destination** drop-down, select the destination to receive the call when the caller request to speak to an agent. This will be associated with IP Office hunt group extension 401, the "Call Center" hunt group.

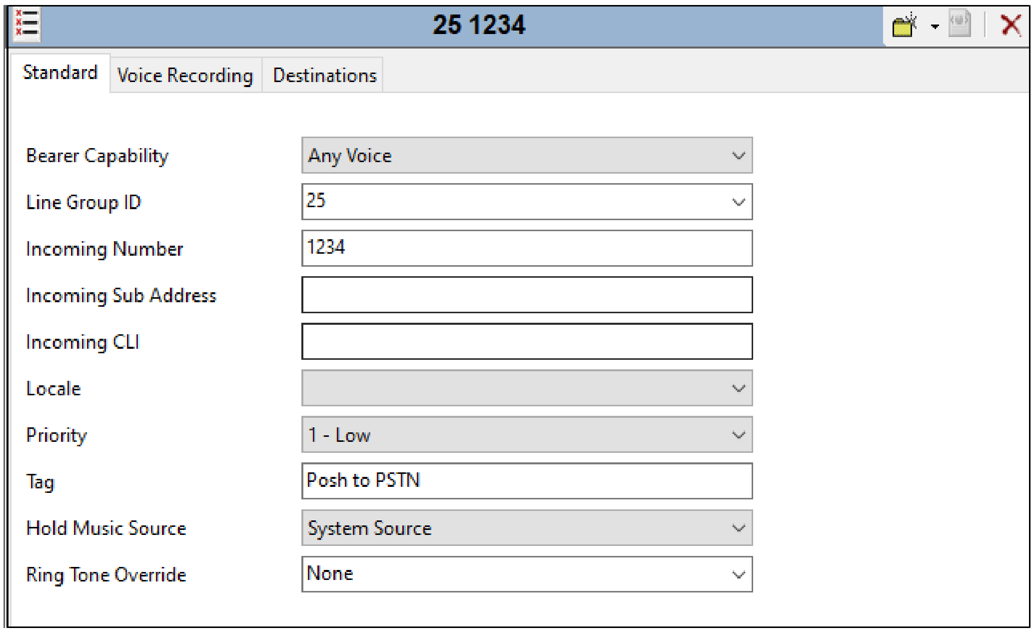


Incoming Call Routes for other IP Office groups or endpoints are not presented here, but can be configured in the same fashion.

5.8.3 Incoming Call Routes – Posh Voice Transferred Calls to the PSTN

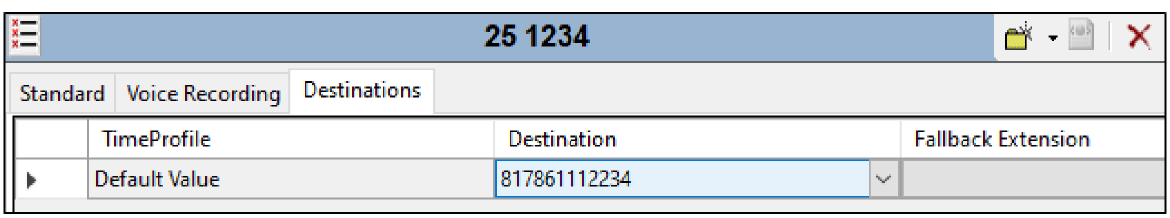
The screen shown below, an incoming call route for **Incoming Number 1234** as illustrated. This number was sent as the SIP URI user in the Refer-To header on the REFER sent from Posh Voice, for calls that are to be transferred to an outside endpoint on the PSTN.

- **Line Group Id** is **25**
- The **Incoming Number** is set to **1234** in this example.



Select the **Destinations** tab.

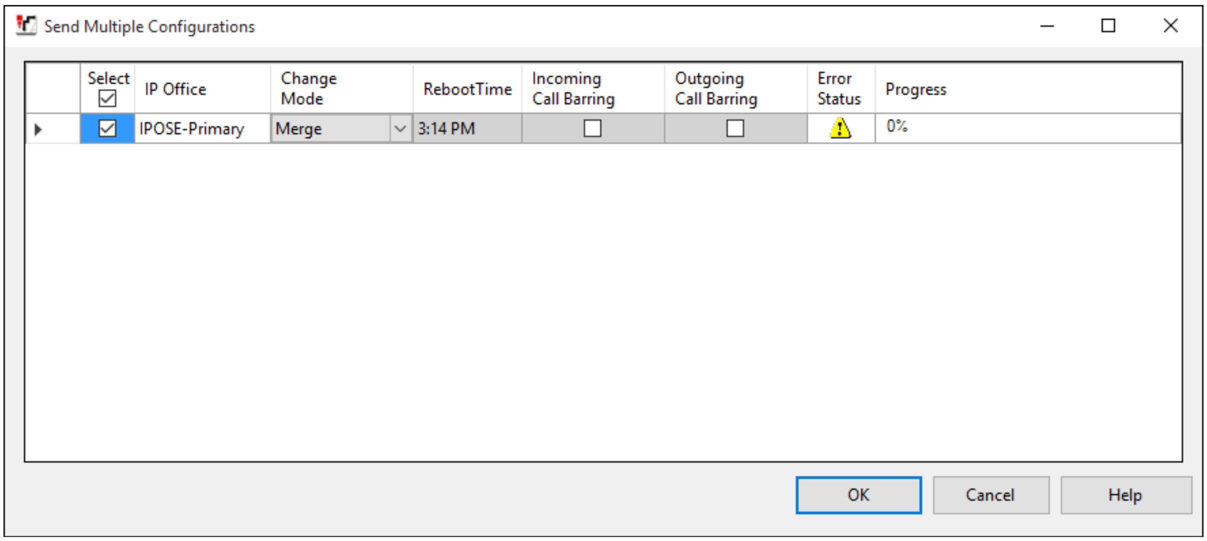
- The **Destination** field is set to the desired PSTN number, including any IP Office Short Code used to route calls to the PSTN. In the test configuration this code was 8N, and the simulated PSTN endpoint to receive the call was 17861112234, so the Destination was set to **817861112234**. This number will be used to route the calls to the simulated PSTN via a separate trunk, SIP Line 27. See Note on **Section 5.7**.



5.9. 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.

The following will appear, with either **Merge** or **Reboot** selected for the **Change Mode**, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** if desired.



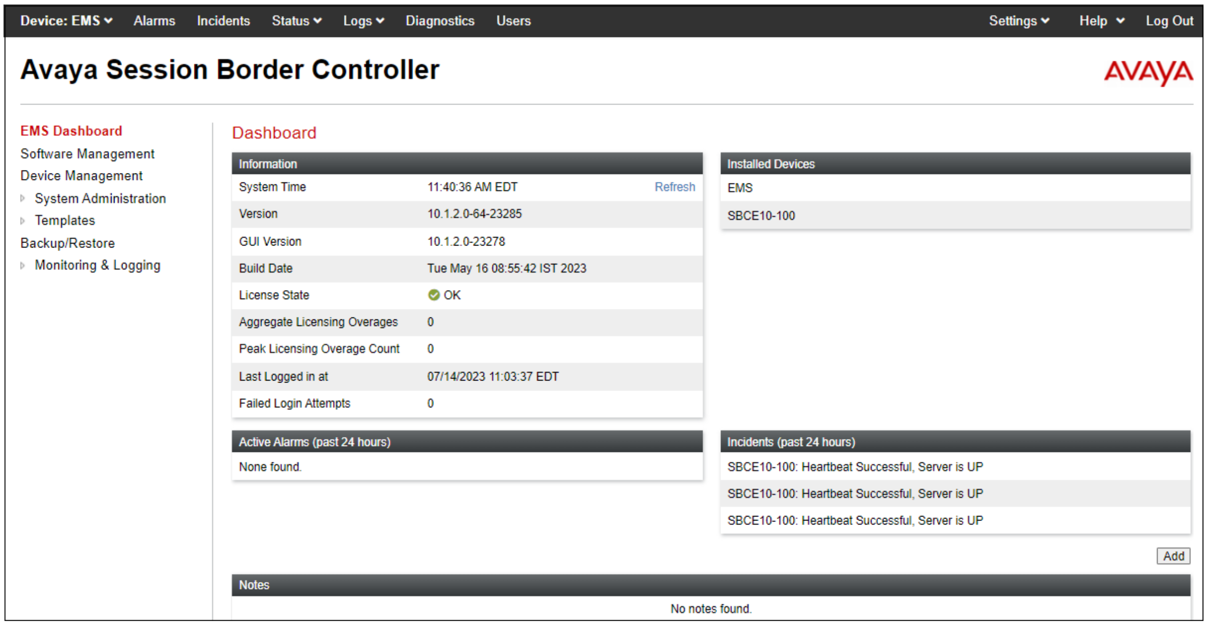
6. Avaya Session Border Controller Configuration

This section covers the configuration of Avaya SBC. It is assumed that the initial provisioning of Avaya SBC, including the assignment of the management interface IP Address and license installation, have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBC consult the Avaya SBC documentation in the **Additional References** section.

Use a WEB browser to access the Element Management Server (EMS) web interface, and enter https://*ipaddress*/sbc in the address field of the web browser, where *ipaddress* is the management LAN IP address of Avaya SBC. Log in using the appropriate credentials.

The EMS Dashboard page of Avaya SBC will appear. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBC will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

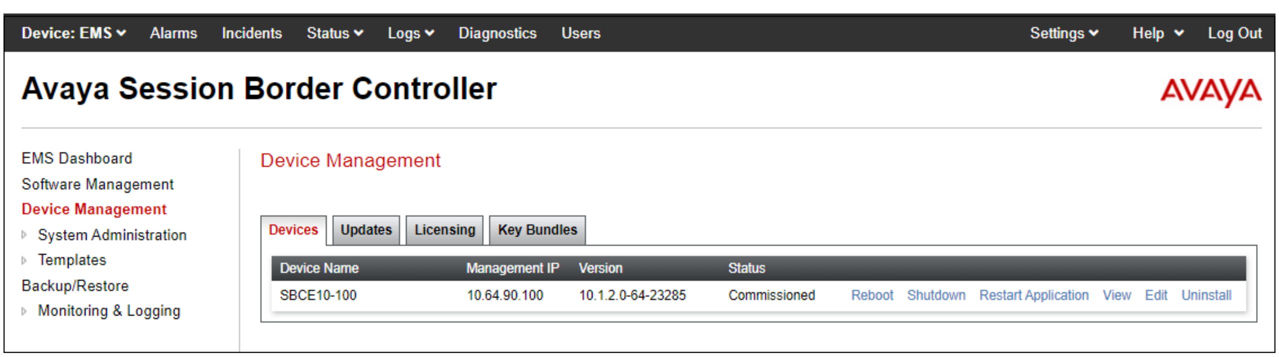
Note – The provisioning described in the following sections use the menu options listed in the left-hand column shown below.



6.1. Device Management – Status

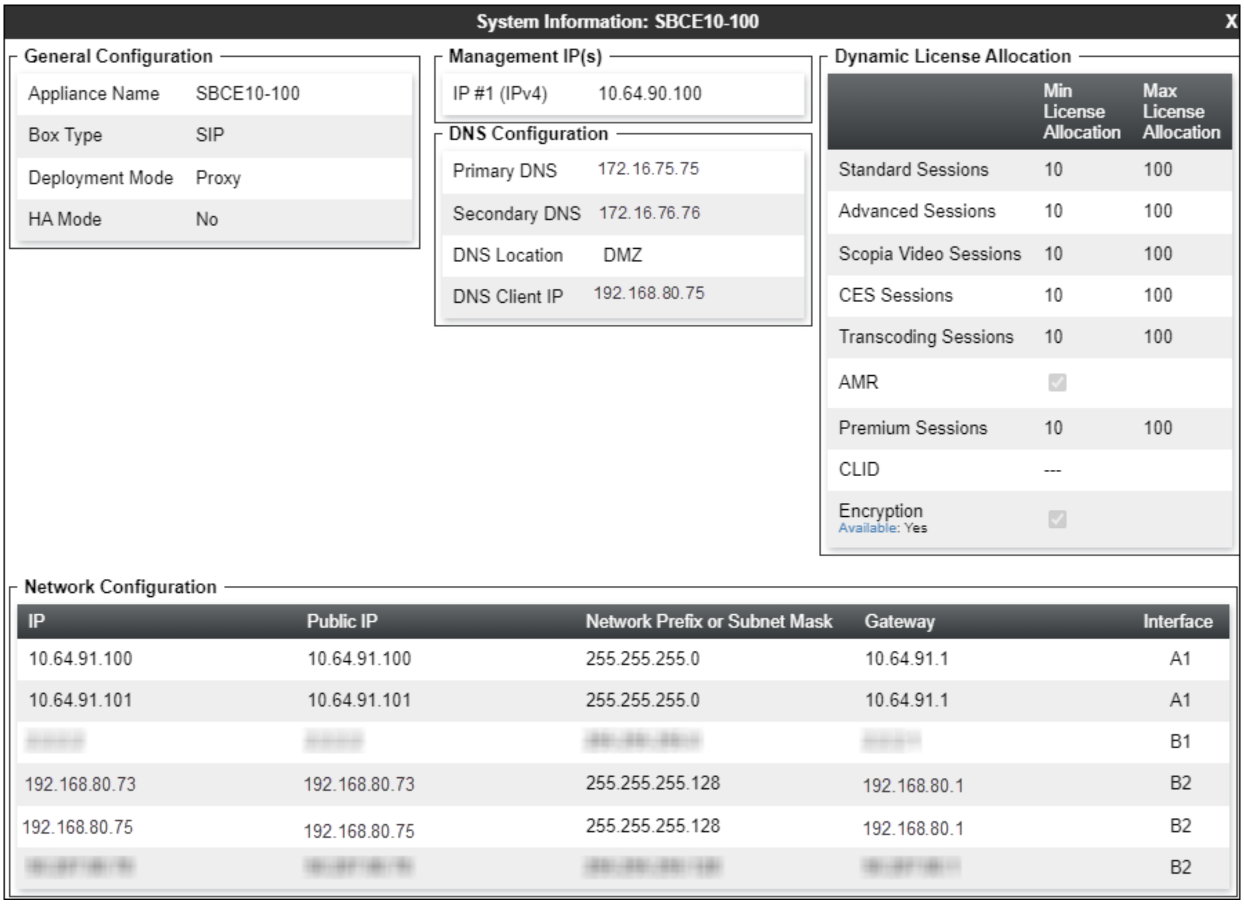
Select **Device Management** on the left-hand menu. A list of installed devices is shown on the **Devices** tab on the right pane. In the case of the sample configuration, a single device named **SBCE10-100** is shown. Verify that the **Status** column shows **Commissioned**. If not, contact your Avaya representative. To view the configuration of this device, click **View** on the screen below.

Note – Certain Avaya SBC configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.



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

Note: Public IP addresses and FQDNs used in the reference configuration on the Avaya SBC B1 and B2 interfaces, DNS servers, etc. have been masked and changed to private IP addresses in this document for security reasons.



6.2. TLS Management

Note –Avaya SBC in the test configuration used identities certificates signed by Avaya System Manager for the TLS internal connections to Avaya IP Office and other Avaya systems. The procedure to create and obtain these certificates, and the creation of TLS Client and Server Profiles for these internal connections is outside the scope of these Application Notes.

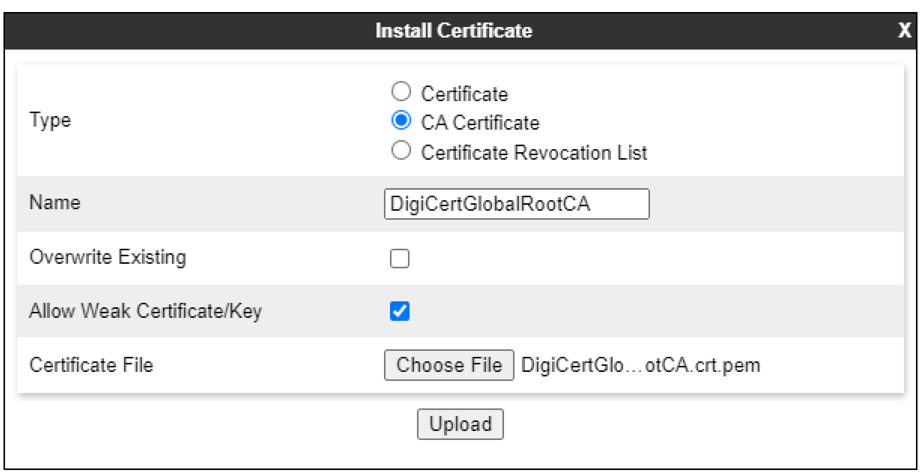
In the reference configuration, TLS encryption is used for the communication between Avaya SBC and the Posh Voice SIP service provider. The following procedures show the steps needed to support this TLS connection.

The TLS connection from Avaya SBC to the Posh Voice service provider uses a server authentication scheme. In this method of connection, the client (Avaya SBC) initiates a request to the server (service provider) for a secure session. The server then sends its identity certificate to the client. The client checks the received server identity certificate against the trusted Certification Authority (CA) certificates that are saved in its trust store, to verify that the server identity certificate is signed by a CA that the client trusts. DigiCert was used as the trusted CA by the service provider, so the DigiCert Global Root CA and DigiCert Global Root G2 certificates needed to be downloaded and imported into Avaya SBC trust store.

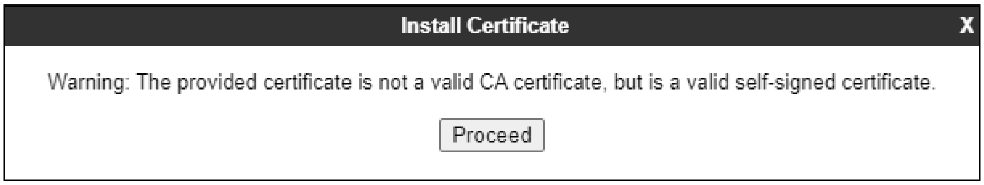
6.2.1 Install CA Certificates

Navigate to **TLS Management → Certificates** and select **Install**.

- Type: select **CA Certificate**.
- Enter a **Name** for the certificate, i.e., **DigiCertGlobalRootCA** was used in the reference configuration, matching the filename of the DigiCert Global Root CA certificate that was downloaded. This is not a requirement, as the name of the certificate could be made something different, but it was done in this way for clarity.
- Check the **Allow Weak Certificate/Key** box.
- **Certificate File**: browse and select the file previously downloaded.
- Click **Upload**.



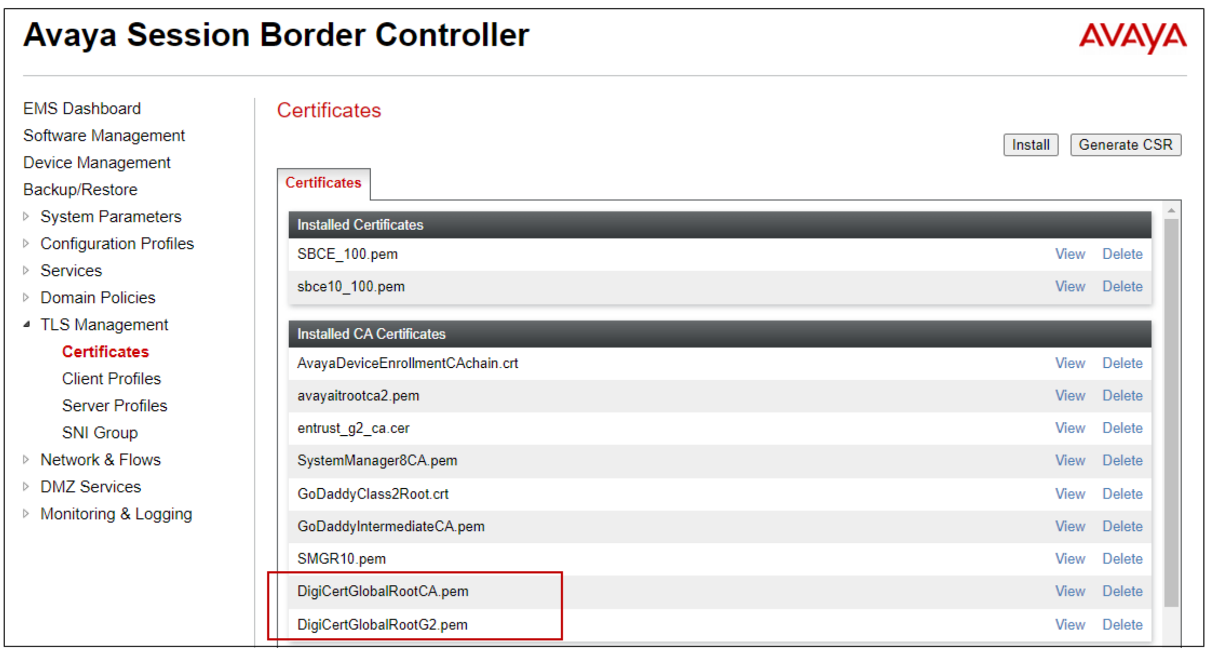
The **Install Certificate** window displays this message:



- Click the **Proceed** button.
- A window displays the certificate details. Click the **Install** button (not shown).
- An Install Certificate window displays this message: “CA Certificate installation successful.”
- Click the **Finish** button.

Repeat the previous steps for the **DigiCert Global Root G2** certificate.

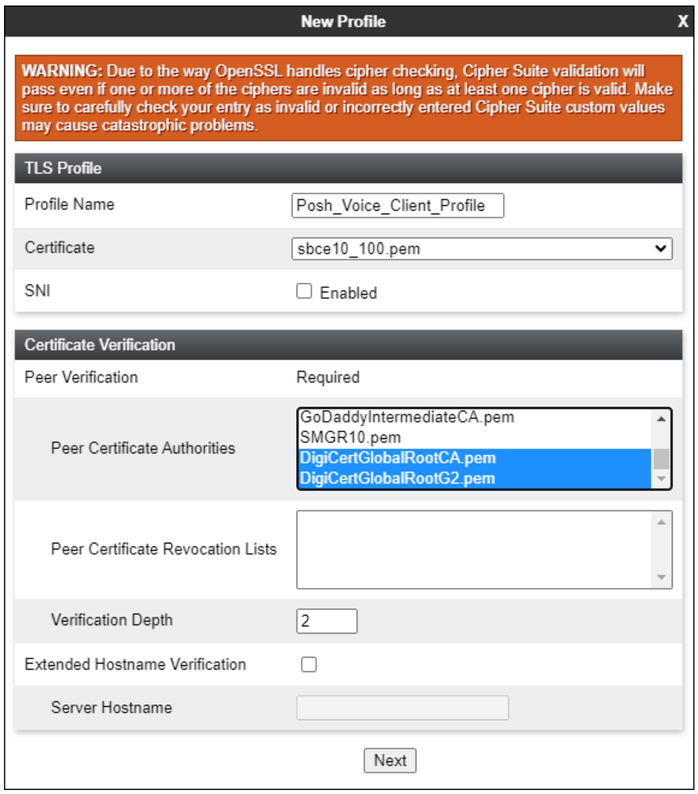
The screen below shows the installed certificates:



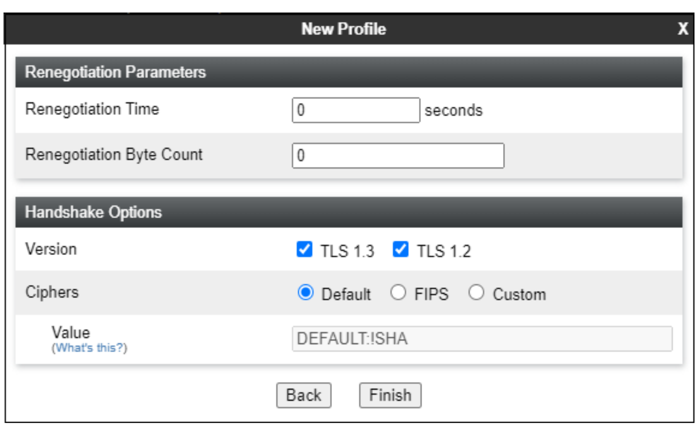
6.2.2 Client Profile for Posh Voice

Select **TLS Management → Client Profiles** and click on **Add**. Enter the following:

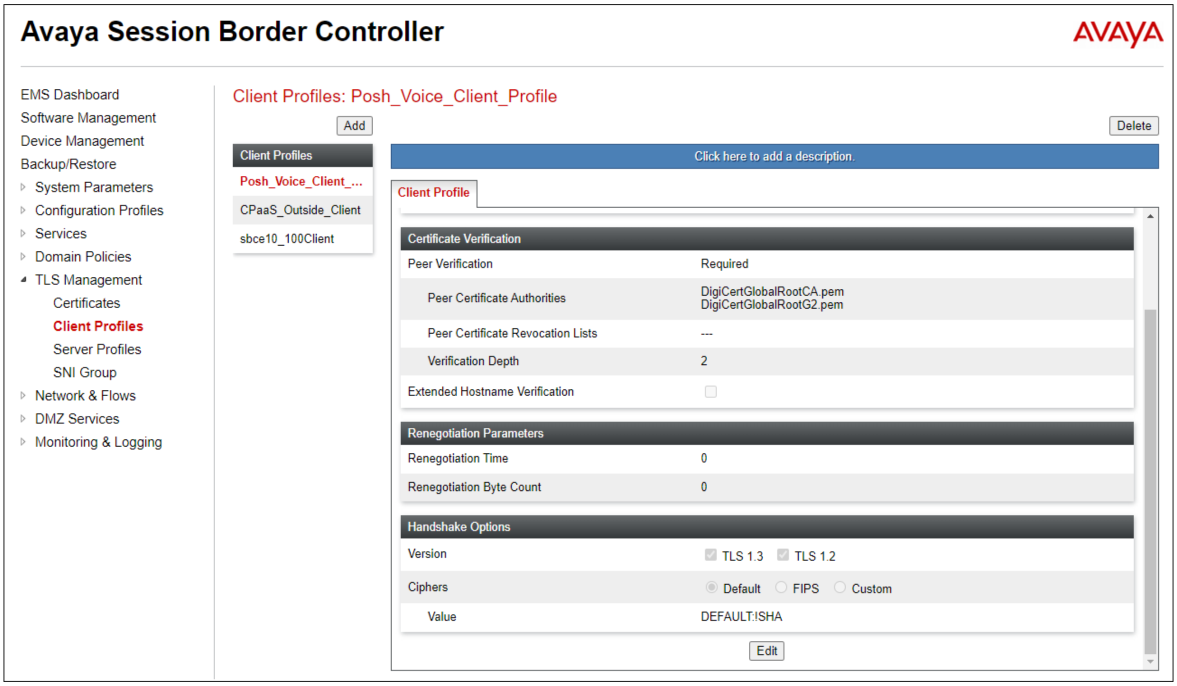
- **Profile Name:** enter descriptive name.
- **Certificate:** select the existing SBC identity certificate from the pull-down menu.
- **Peer Verification** = **Required**.
- **Peer Certificate Authorities:** Select both the **DigiCertGlobalRootCA.pem and DigiCertGlobalRootG2.pem** certificates.
- **Verification Depth:** enter **2**.
- Click **Next**.



Accept default values for the next screen and click **Finish**.

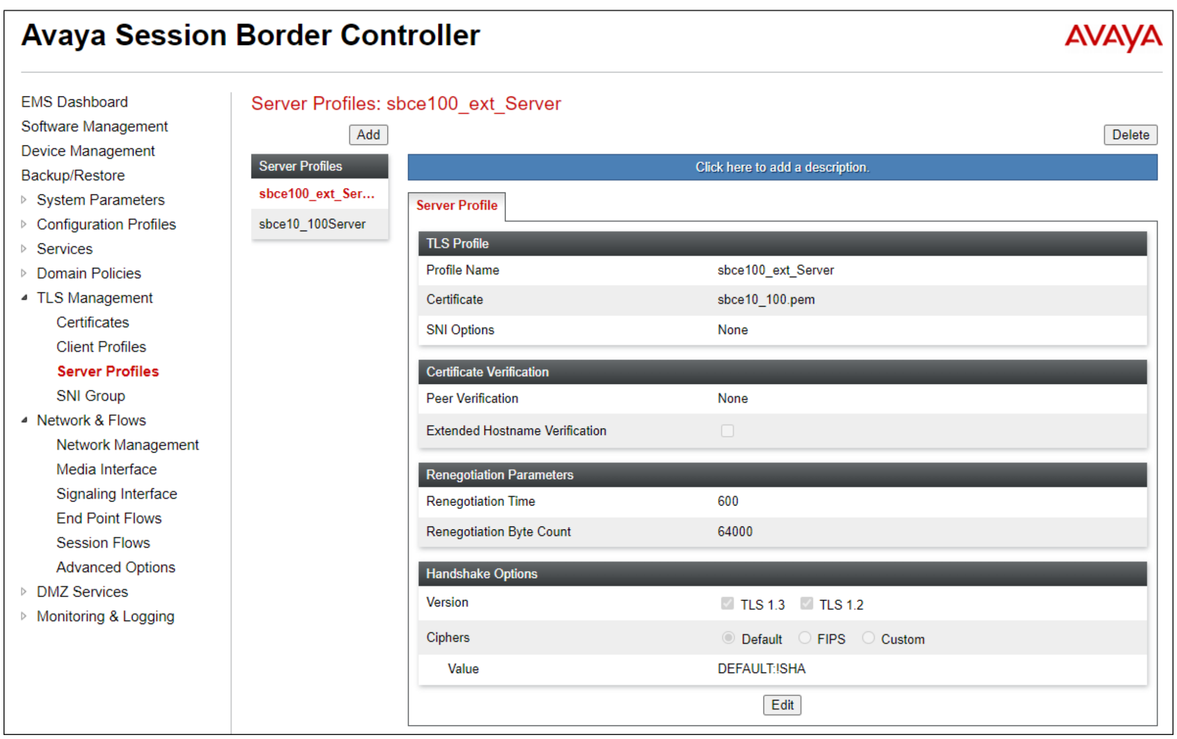


The following screen shows the completed TLS **Client Profile** form:



6.2.3 Server Profile for Posh Voice

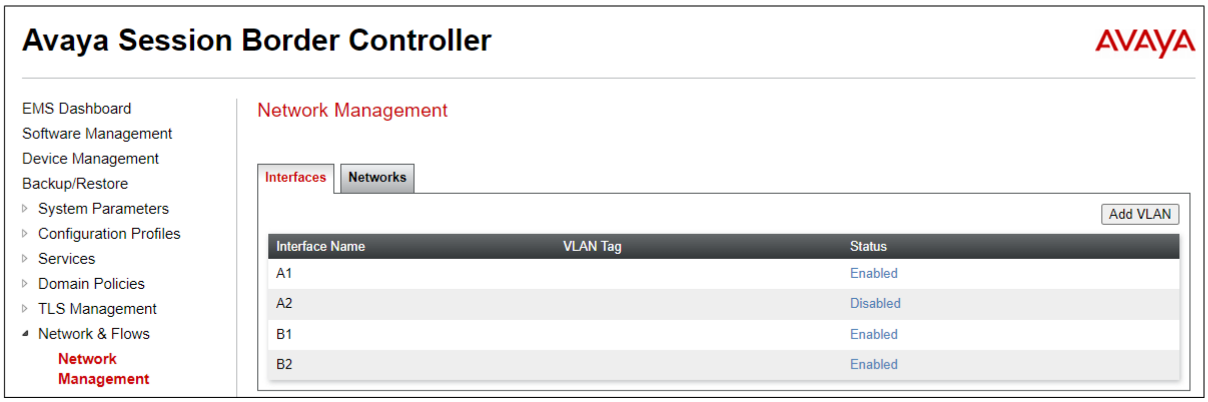
The following screen shows the existing TLS **Server Profile** used in the reference configuration. This profile was previously configured on the SBC, and reused for the connection to Posh Voice.



6.3. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBC, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

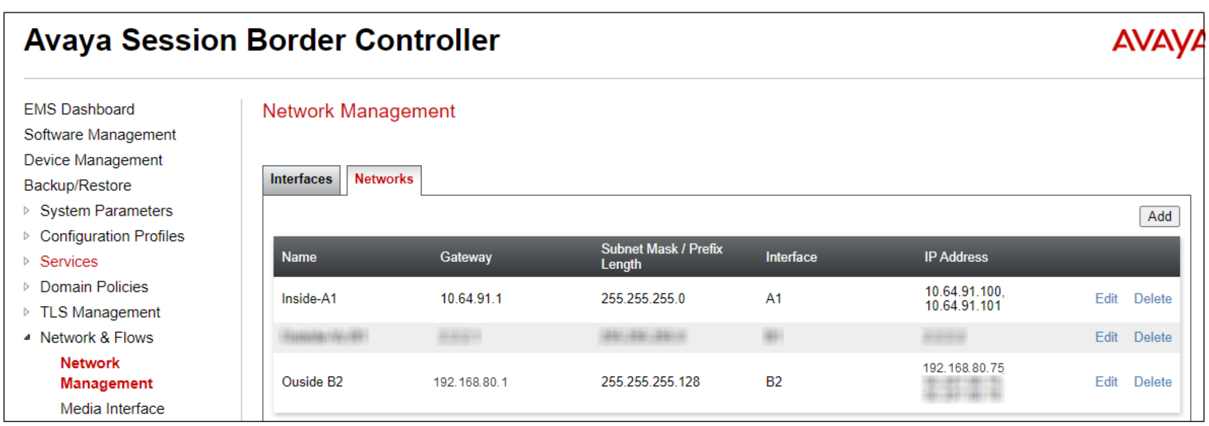
Select **Networks & Flows → Network Management** from the menu on the left-hand side. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 and B2 are used.



Select the **Networks** tab to display the IP provisioning for the A1 and B2 interfaces. Some of these values are specified during installation. Addresses can be added, modified or deleted by selecting **Edit** on each interface.

The following IP addresses were assigned to be used of Posh Voice traffic:

- **A1**: **10.64.91.100** – "Inside" IP address, toward IP Office.
- **B2: 192.168.80.75** – "Outside" IP address toward the SIP trunk to Posh Voice.

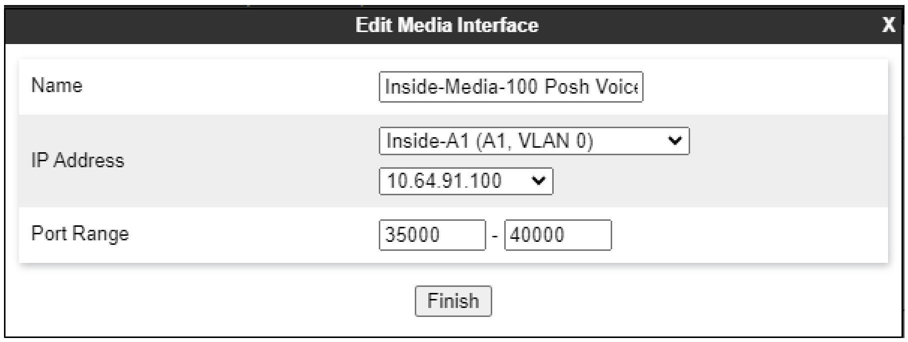


Note: Public IP addresses and FQDNs used in the reference configuration have been masked and changed to private IP addresses for security reasons.

6.4. Media Interfaces

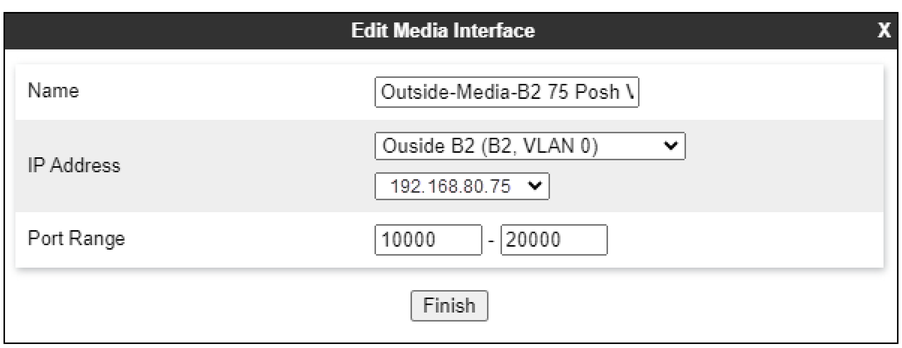
To add to the Posh Voice internal media interface select **Network & Flows → Media Interface** from the menu on the left-hand side. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name**: Enter an appropriate name (e.g., **Inside-Med-100 Posh Voice**).
- **IP Address**: Select **Inside-A1 (A1,VLAN0)** and the IP address used for Posh Voice traffic towards Avaya IP Office (e.g., **10.64.91.100**) from the drop-down menus.
- **Port Range**: **35000 – 40000**.
- Click **Finish**.



Select **Add** (not shown) to add to the Posh Voice external media interface. Enter the following:

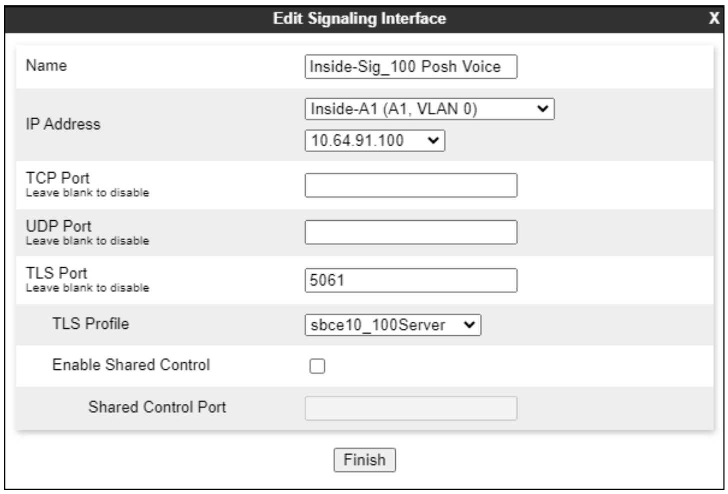
- **Name**: Enter an appropriate name (e.g., **Outside-Media-B2 75 Posh Voice**).
- **IP Address**: Select **Outside B2 (B2, VLAN0)** and the IP address used for the SIP trunk to Posh Voice (e.g., **192.168.80.75**) from the drop-down menus.
- **Port Range**: In the reference configuration, the port range was set to match the values used by the SIP service provider, **10000** – **20000**. This is not strictly necessary, as the defaults values could be used here too.
- Click **Finish**.



6.5. Signaling Interfaces

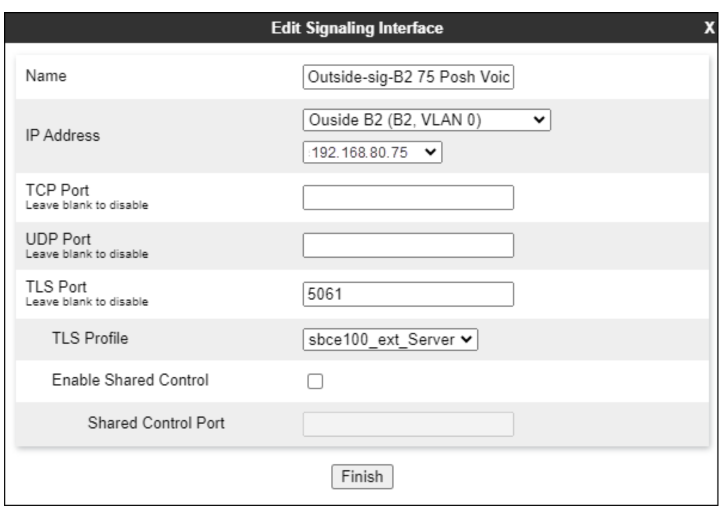
Select **Network & Flows → Signaling Interface** from the menu on the left-hand side.
Select **Add** (not shown) to add to the internal signaling interface used for Posh Voice. Enter the following:

- **Name**: Enter an appropriate name (e.g., **Inside-Sig_100 Posh Voice**).
- **IP Address**: Select **Inside A1 (A1, VLAN0)** and **10.64.91.100**.
- **TLS Port**: **5061**.
- **TLS Profile**: Select the existing TLS server profile on the enterprise (e.g., **sbce10_100Server**). See **Note** on **Section 6.2**.
- Click **Finish**.



Select **Add** (not shown), to add to the external signaling interface used for Posh Voice.

- **Name**: Enter an appropriate name (e.g., **Outside-sig-B2 75 Posh Voice**).
- **IP Address**: Select **Outside B2 (B2, VLAN0)** and **192.168.80.75.**
- **TLS Port**: **5061.**
- **TLS Profile**: Select the existing TLS server profile on the enterprise (e.g., **sbce100_ext_Server**, **Section 6.2.3**).



6.6. Server Interworking Profiles

A Server Interworking profile defines a set of parameters that aid in interworking between the SBC and a connected server. A Server Interworking profile was added for Avaya IP Office, while no Server Interworking profile was used for the Posh Voice IP service provider.

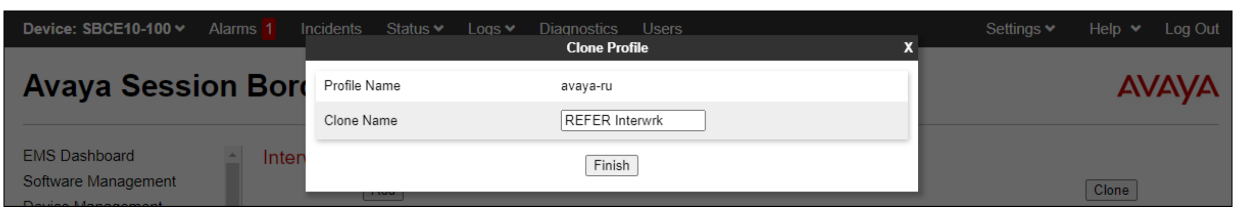
One of the Avaya SBC capabilities important in the IP Office environment is the Avaya SBC Refer Handling option. As described in **Section 3**, Posh Voice inbound call processing may include call redirection to Avaya IP Office agents, or other destinations back at the CPE. This redirection is accomplished by Posh Voice sending a SIP REFER message to Avaya SBC. Enabling the Refer Handling option in the Server Interworking profile causes Avaya SBC to intercept and process the REFER, and generate new SIP INVITE messages back to IP Office and the PSTN. This is necessary since inbound blind call transfers with REFER are not supported by Avaya IP Office by default.

Additionally, the inbound REFER message from Posh Voice may include UUI data in its Refer-To header. Avaya SBC will include this UUI data in the User-to-User header of the inbound INVITE to IP Office.

Note: At the time of the writing of these application notes, Avaya IP Office does not process the UUI in the User-to-User header, and the data is not passed either to other elements internally in the solution.

In the sample configuration, a new Server Interworking profile was cloned from the default **avaya-ru** profile and then modified.

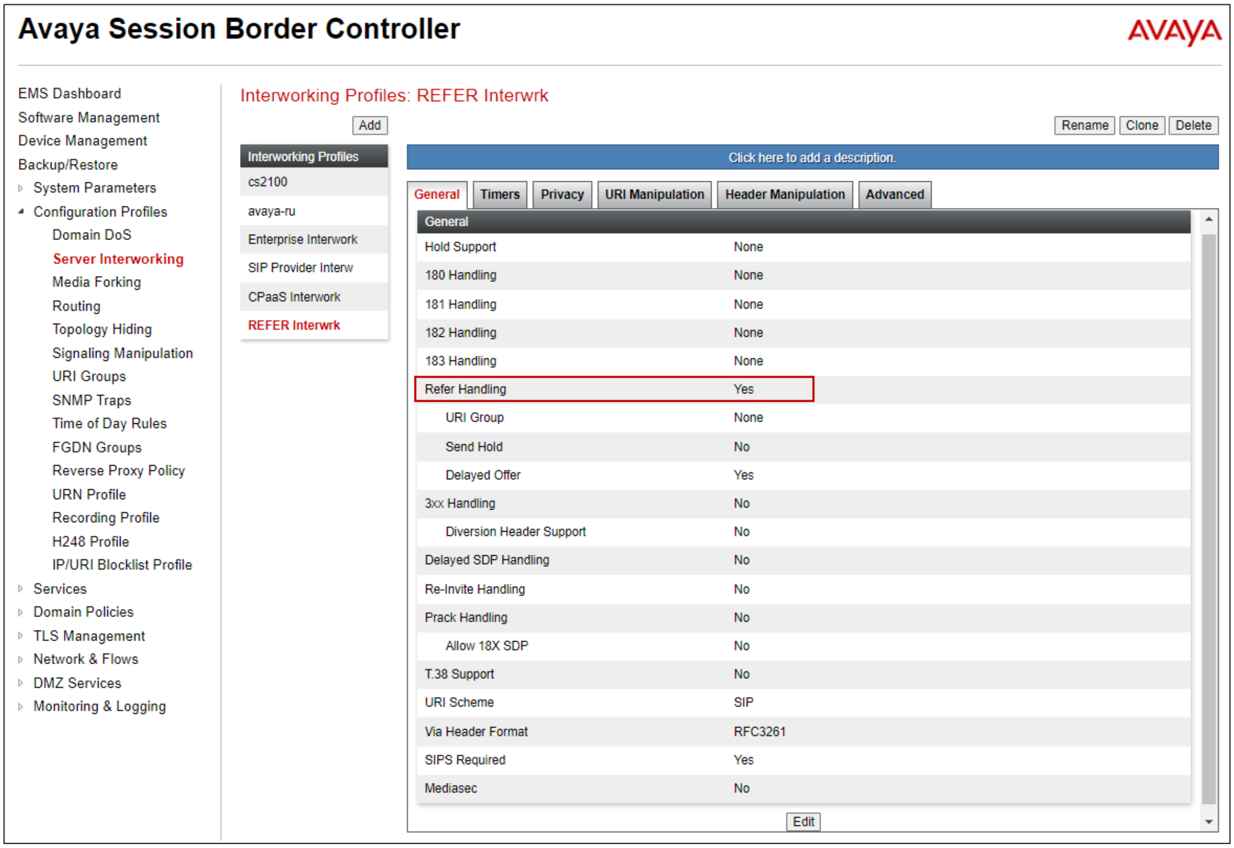
- Select **Configuration Profiles → Server Interworking** from the left-hand menu.
- Select the pre-defined **avaya-ru** profile and click the **Clone** button.
- Enter profile name: (e.g., **REFER Interwk**), and click **Finish** to continue.



The new **REFER Interwrk** profile will be listed. Select it, scroll to the bottom of the Profile screen, and click on **Edit**.

The **General** screen will open.

- Check **the Refer Handling** box.
- All other options can be left with default values.
- Click **Finish** (not shown).



This Server Interworking profile will later be applied to the SIP Server profile corresponding to IP Office.

6.7. SIP Server Profiles

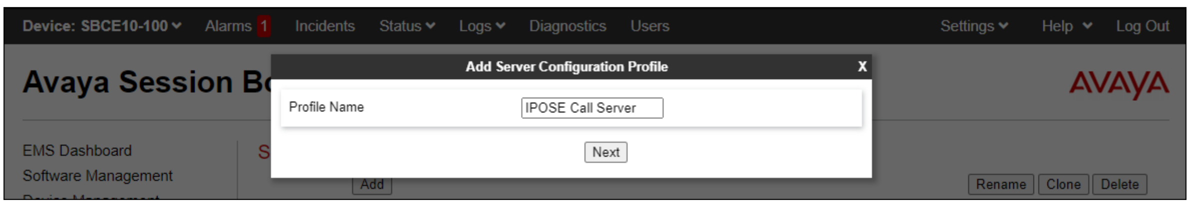
SIP Server Profiles are required for each server connected to Avaya SBC. Two profiles were configured for Posh Voice, one for Posh Voice staging and one for Posh Voice production. A SIP Server Profile for IP Office also needs to be created, or if one already exists it can be modified as shown in the next section. TLS transport was used for the SIP trunks to IP Office and the Posh Voice SIP service provider.

Note –Avaya SBC in the test configuration used identities certificates signed by Avaya System Manager for the TLS internal connections to Avaya IP Office. The procedure to create and obtain these certificates and the creation of TLS client and server profiles for these connections is outside the scope of these Application Notes.

6.7.1 SIP Server Profile – Avaya IP Office

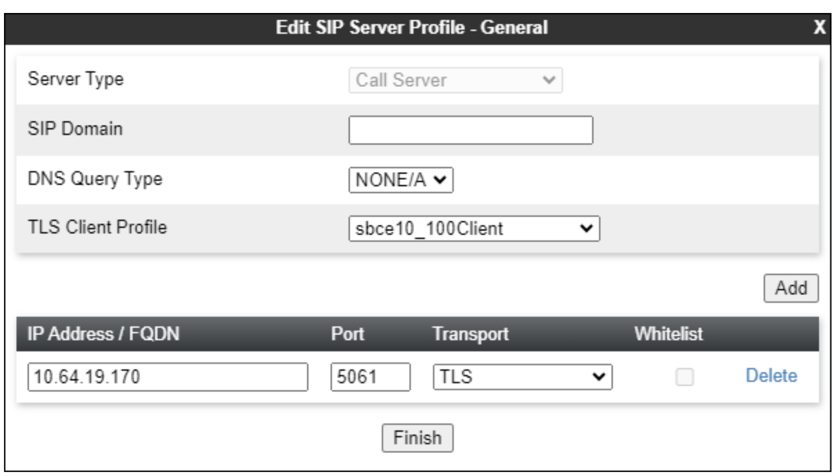
This section defines the SIP Server Profile for the Avaya SBC connection to Avaya IP Office.

- Select **Services → SIP Servers** from the left-hand menu.
- Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **IPOSE Call Server**) and click **Next**.



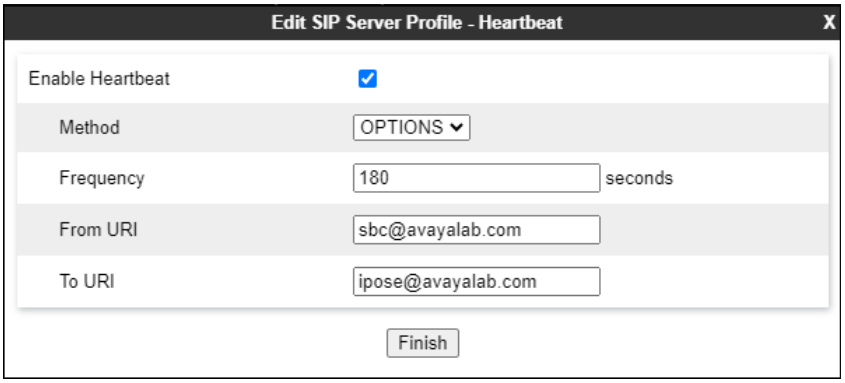
The **Add Server Configuration Profile** window will open.

- Select **Server Type**: **Call Server**.
- **TLS Client Profile**: Select the existing TLS client profile on the enterprise (e.g., **sbce10_100Client**).
- **IP Address**: **10.64.19.170** (IP Office LAN1 IP address).
- Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



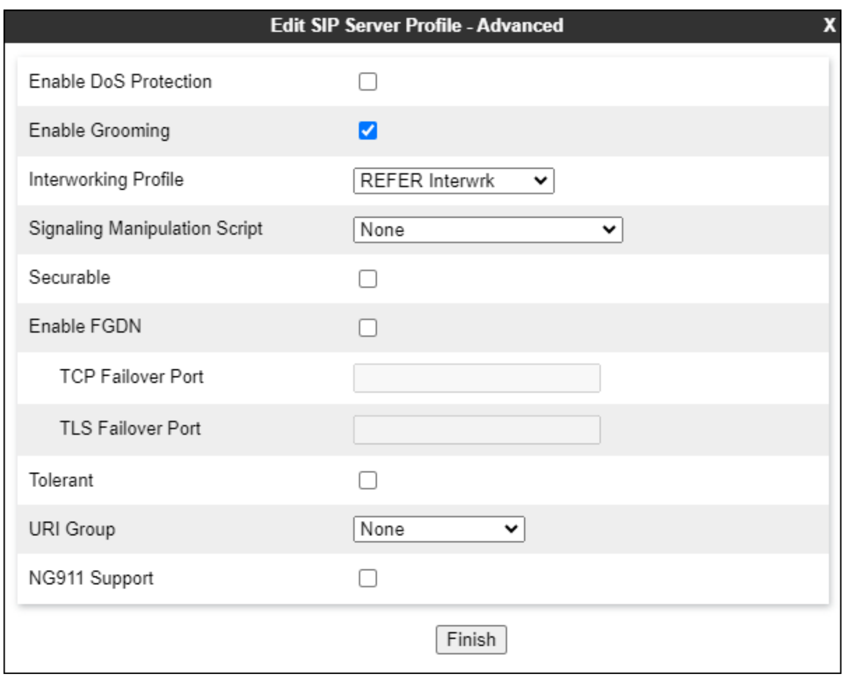
Default values can be used on the **Authentication** tab. On the **Heartbeat** tab, check the **Enable Heartbeat** box to have Avaya SBC source "heartbeats" toward IP Office.

- Select **OPTIONS** from the **Method** drop-down menu.
- Select the desired frequency that the SBC will source OPTIONS toward IP Office.
- Make logical entries in the **From URI** and **To URI** fields that will be used in the OPTIONS headers.



Default values are used on the **Registration** and **Ping** tabs. On the **Advanced** tab:

- Select the **REFER Interwk** (created in **Section 6.6**), for **Interworking Profile**.
- Since TLS transport is specified, then the **Enable Grooming** option should be enabled.
- Select **Finish**.

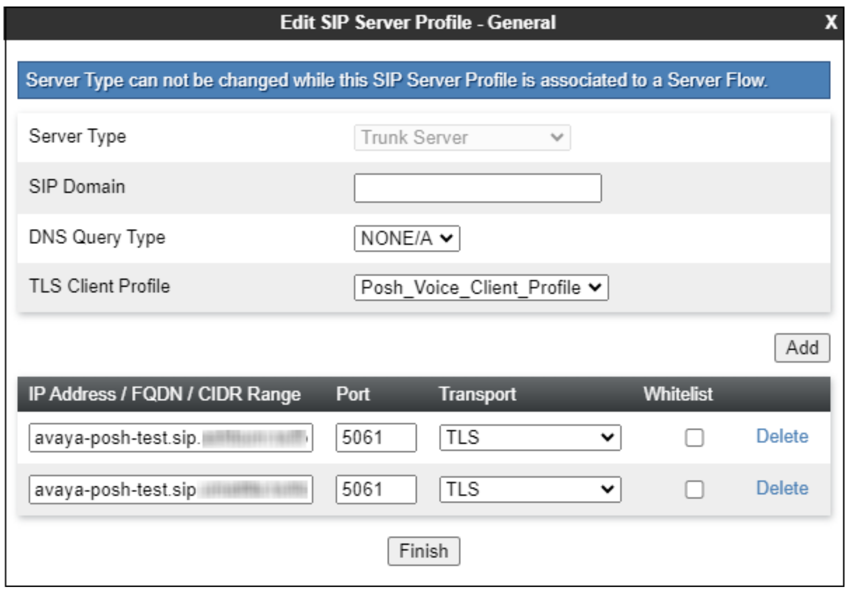


6.7.2 SIP Server Profile – Posh Voice Test

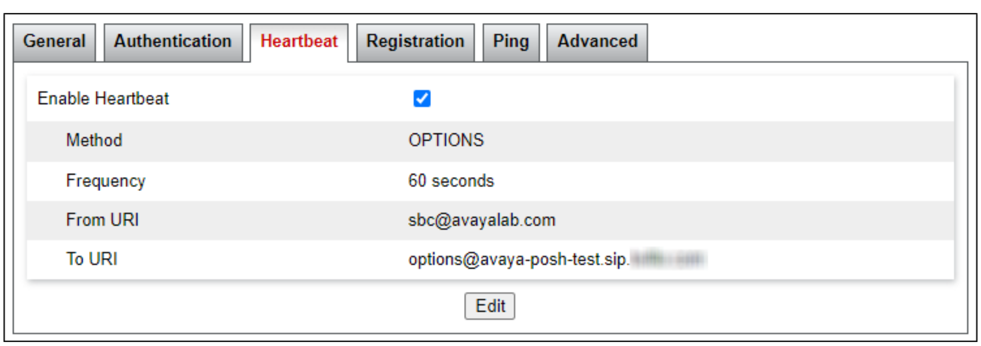
Repeat the steps in **Section 6.7.1**, with the following changes, to create a SIP Server Profile for the Avaya SBC connection to the Posh Voice Test service.

Select **Add** and enter a Profile Name (e.g., **Posh Voice Test**) and select **Next** (not shown).
On the **General** window, enter the following:

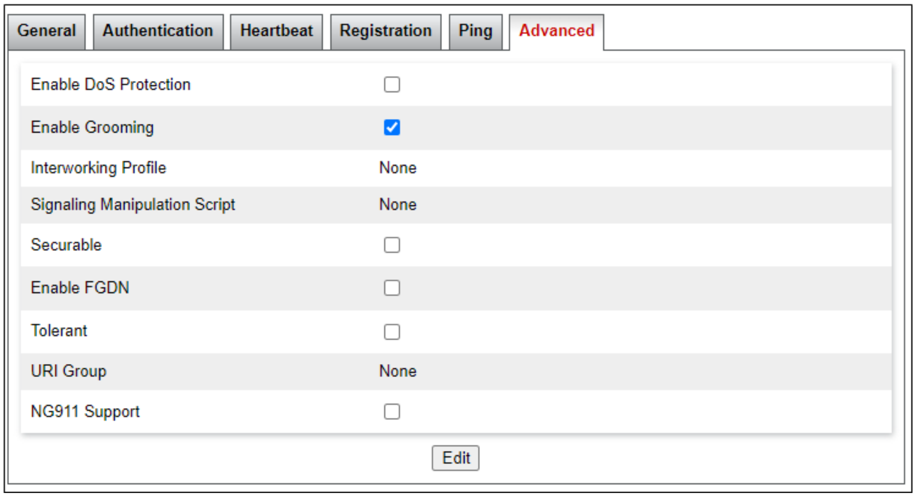
- **Server Type: Trunk Server**.
- **TLS Client Profile**: Select the client profile created for Posh Voice in **Section 6.2.2**.
- Select **Add** and enter the FQDNs for the Posh Voice Test SIP server provided by Posh Voice. The service consists of a primary and a secondary site, hence the two FQDNs.
- Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed to next tab.



Default values are used on the **Authentication** tab. On the **Heartbeat** tab, check the **Enable Heartbeat** box to optionally have the Avaya SBC source "heartbeats" toward the **Posh Voice Test** SIP server. The screen below shows the values used in the reference configuration.



Default values are used on the **Registration** and **Ping** tabs. On the **Advanced** window, **Enable Grooming** is selected. All other parameters retain their default values.

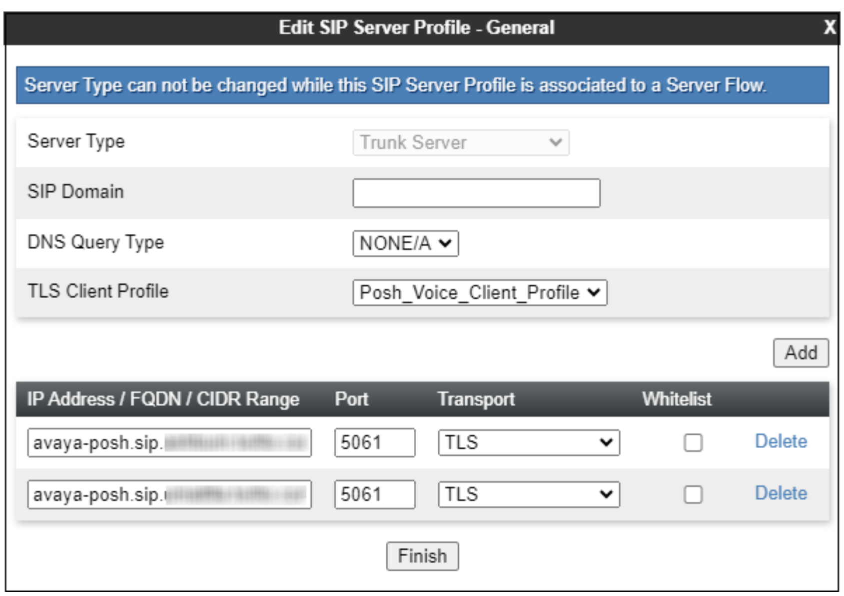


6.7.3 SIP Server Profile – Posh Voice Production

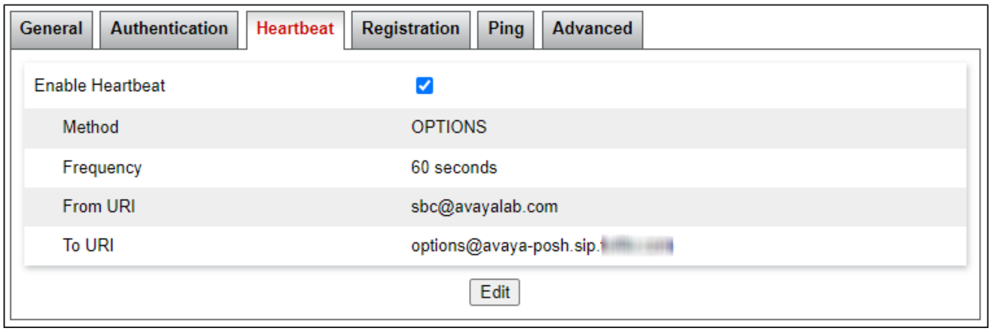
Repeat the steps in **Section 6.7.2**, with the following changes, to create a SIP Server Profile for the Avaya SBC connection to Posh Voice Production.

Select **Add** and enter a Profile Name (e.g., **Posh Voice Prod**) and select **Next** (not shown).
On the **General** window, enter the following:

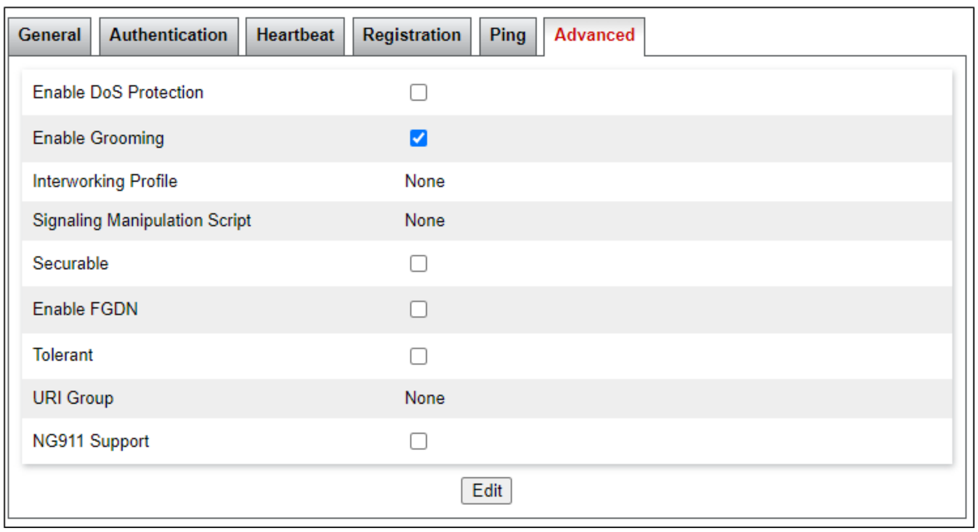
- **Server Type: Trunk Server**.
- **TLS Client Profile**: Select the client profile created for Posh Voice in **Section 6.2.2**.
- Select **Add** and enter the FQDNs for the Posh Voice Production SIP server provided by Posh Voice. The service consists of a primary and a secondary site, hence the two FQDNs.
- Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed to next tab.



Default values are used on the **Authentication** tab. On the **Heartbeat** tab, check the **Enable Heartbeat** box to optionally have the Avaya SBC source "heartbeats" toward the **Posh Voice Production** SIP server. The screen below shows the values used in the reference configuration.



Default values are used on the **Registration** and **Ping** tabs. On the **Advanced** window, **Enable Grooming** is selected. All other parameters retain their default values.



6.8. URI Groups

URI Groups were used to assist in routing calls to the Posh Voice test and production environments, as well as the routing of transferred calls from Posh Voice to IP Office agents. The following URI Groups were created:

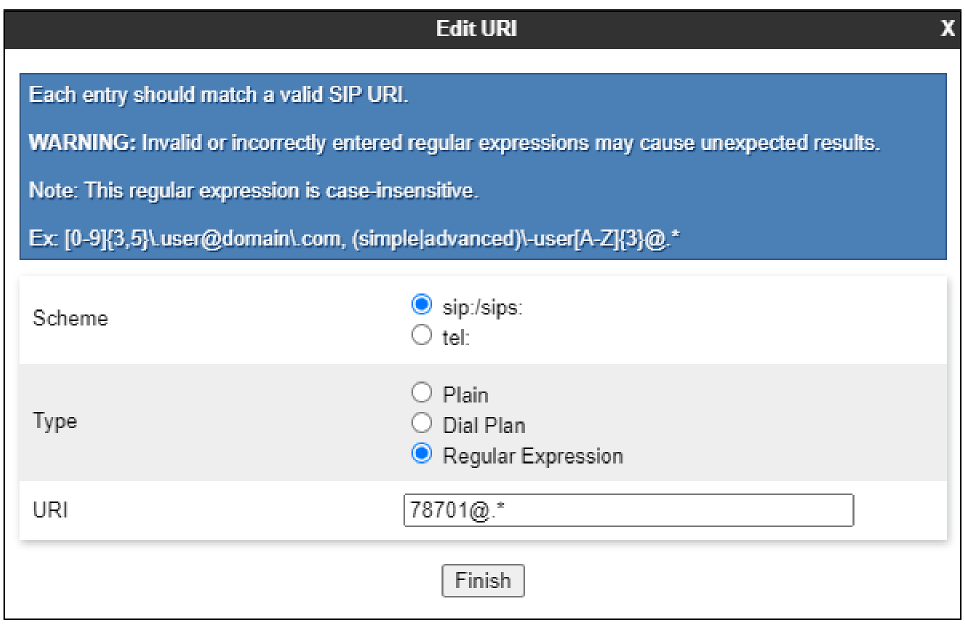
- Posh Voice Test
- Posh Voice Prod
- IP Office

6.8.1 URI Group – Posh Voice Test

Create a URI Group for the number intended to reach the Posh Voice Test service. In the reference configuration, this number was 78701, as assigned by Posh Voice and configured in the IP Office incoming call routes in **Section 5.8.1**.

Select **Configuration Profiles → URI Groups** from the left-hand menu. Select **Add** and enter a descriptive **Group Name**, e.g., **Posh Voice Test**, and select **Next** (not shown).
Enter the following:

- **Scheme**: **sip:/sips:**
- **Type: Regular Expression**
- **URI: 78701@.***
- Select **Finish**.

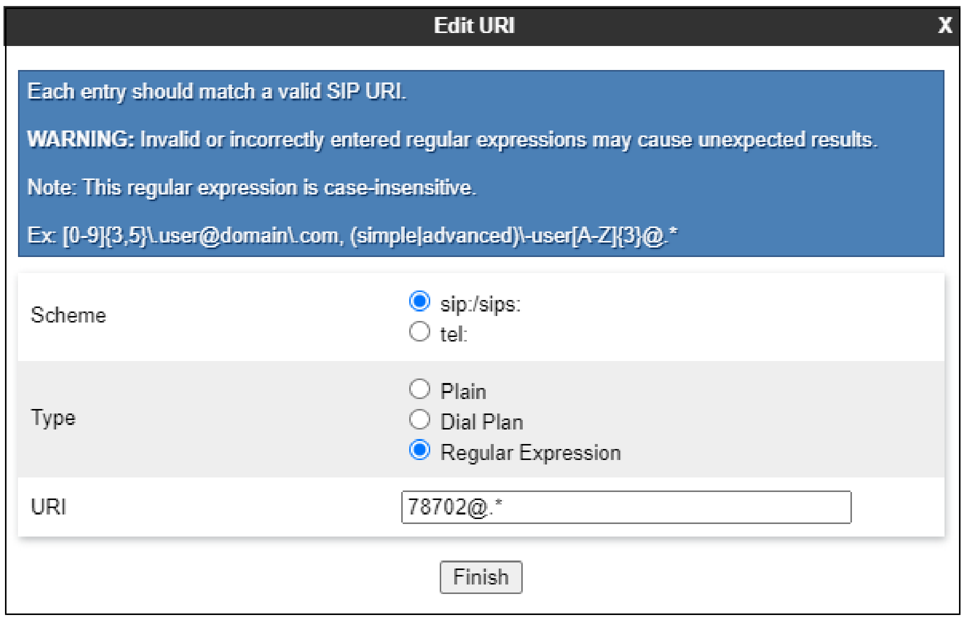


6.8.2 URI Group – Posh Voice Production

Create a URI Group for the number intended to reach the Posh Voice Production service. In the reference configuration, this number was 78702, as assigned by Posh Voice and configured in the IP Office incoming call routes in **Section 5.8.1**.

Select **Configuration Profiles → URI Groups** from the left-hand menu. Select **Add** and enter a descriptive **Group Name**, e.g., **Posh Voice Prod**, and select **Next** (not shown).
Enter the following:

- **Scheme**: **sip:/sips:**
- **Type: Regular Expression**
- **URI: 78702@.***
- Select **Finish**.



6.8.3 URI Group – IP Office

Create a URI Group for the numbers or range of numbers used for calls that are redirected from Posh Voice back to IP Office. These calls can have different destinations in the IP Office, like extensions, hunt groups, short codes, etc. In the reference configuration, these numbers were assigned by Posh Voice and they were in the 1xxx range and 5xxx range.

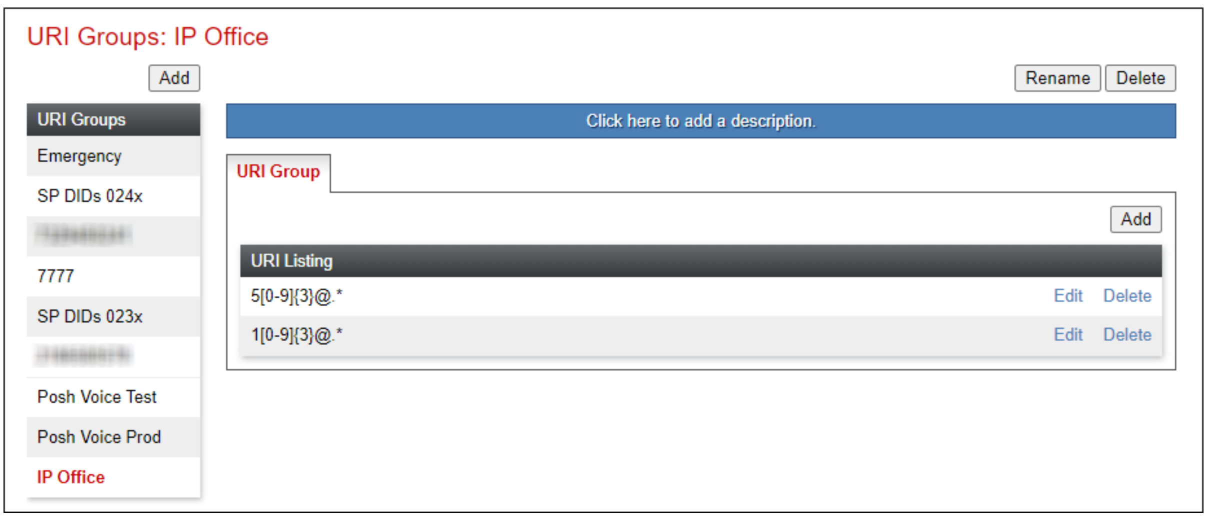
Select **Configuration Profiles → URI Groups** from the left-hand menu. Select **Add** and enter a descriptive **Group Name**, e.g., **IP Office**, and select **Next** (not shown).
Enter the following:

- **Scheme**: **sip:/sips:**
- **Type: Regular Expression**.
- **URI**: **1[0-9]{3}@.*** This will match 4-digit extensions starting with 1, e.g., 1234.
- Select **Finish**.

Select the **IP Office** URI Group just created and click **Add** on the right side of the screen to enter a second entry. Repeat the previous steps with the following difference:

- **URI**: **5[0-9]{3}@.*** This will match 4-digit extensions starting with 5, e.g., 5678
- Select **Finish**.

The screen below shows the completed URI Group:



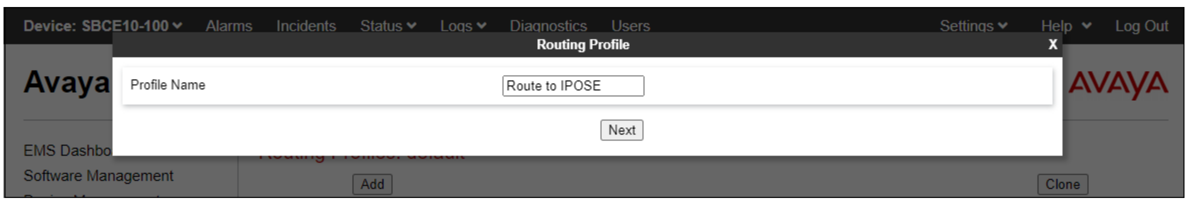
6.9. Routing Profiles

Routing Profiles are used to specify the next-hop for a SIP message. A routing profile is applied after the traffic has matched an End Point Flow defined in **Section 6.11**. The IP addresses and ports defined here will be used as destination addresses for signaling. Separate Routing Profiles were created in the reference configuration for the IP office and Posh Voice.

6.9.1 Routing Profile – IP Office

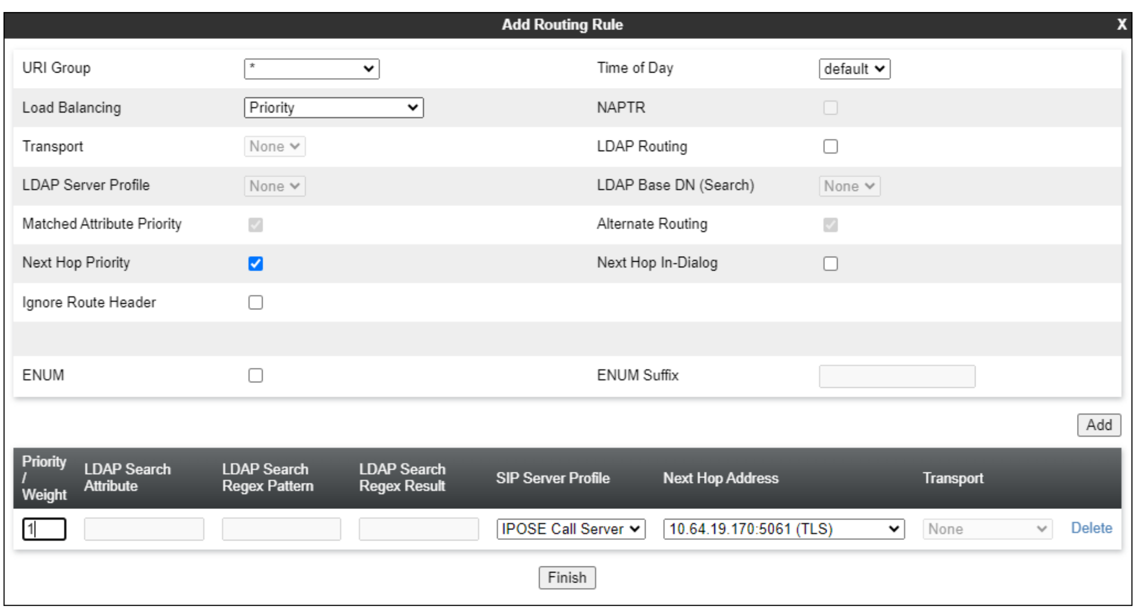
A routing profile to IP Office was already in place, and it was reused in the configuration for Posh Voice. Follow the steps below to create a routing profile to the IP Office if one doesn't already exist.

To add a Routing Profile for the IP Office, navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** (e.g., **Route to IPOSE**) and click **Next** to continue.



The Routing Rule window will open. The parameters in the top portion of the profile are left at their default settings. Click the **Add** button. The Next-Hop Address section will open at the bottom of the profile. Populate the following fields:

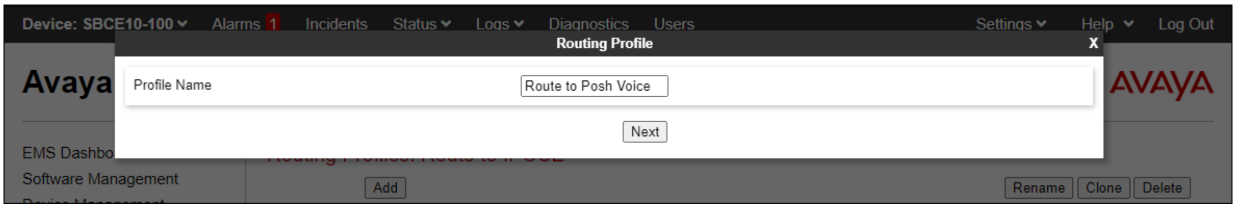
- **Priority/Weight**: **1**
- **SIP Server Profile**: **IPOSE Call Server** (from **Section 6.7.1**).
- **Next Hop Address:** Verify that the **10.64.19.170:5061 (TLS)** entry from the drop-down menu is selected (IP Office IP address). Also note that the **Transport** field is grayed out.
- Click **Finish**.



6.9.2 Routing Profile – Posh Voice

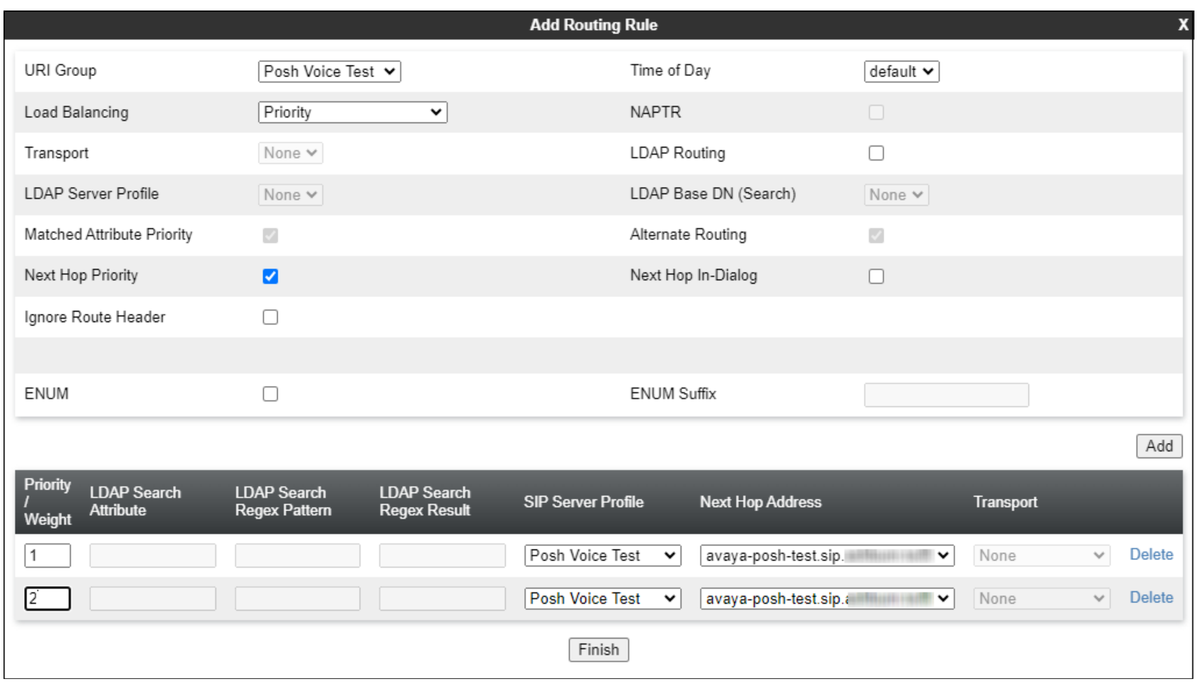
Repeat the steps in **Section 6.9.1**, with the following changes, to add a Routing Profile for the Avaya SBC connection to Posh Voice.

Navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** (e.g., **Route to Posh Voice**) and click **Next** to continue.



On the Routing Rule window, under **URI Group** select the **Posh Voice Test** URI Group created in **Section 6.8.1**. Click the **Add** button. The Next-Hop Address section will open at the bottom of the profile. Populate the following fields:

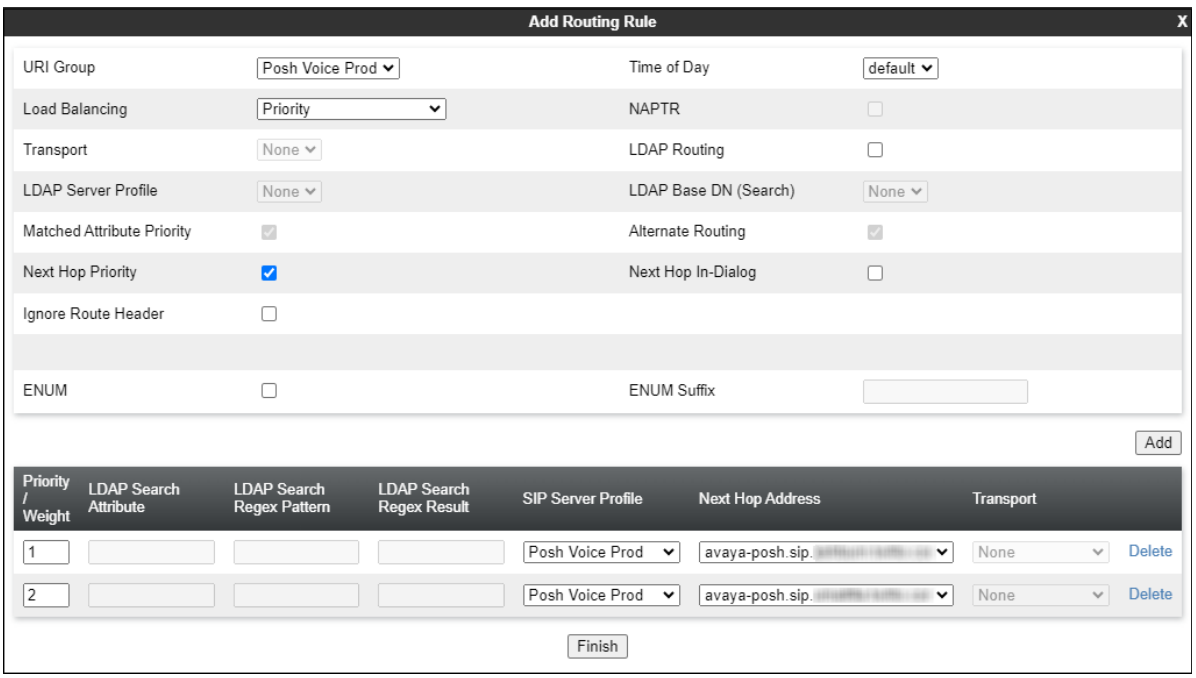
- **Priority/Weight**: **1**
- **SIP Server Profile:** Select **Posh Voice Test** (from **Section 6.7.2**).
- **Next Hop Address:** Select the FQDN of the by Posh Voice Test primary site.
- Click the **Add** button to add a second Next-Hop Address.
- **Priority/Weight**: **2**
- **SIP Server Profile:** Select **Posh Voice Test** (from **Section 6.7.2**).
- **Next Hop Address:** Select the FQDN of the by Posh Voice Test secondary site.
- Click **Finish**.



Back at the Routing Profiles screen, with the **Route to Posh Voice** profile selected, click the **Add** button on the right side of the screen to add a second routing rule to the profile.

On the Routing Profile window, under **URI Group** select the **Posh Voice prod** URI Group created in **Section 6.8.2**. Click the **Add** button. The Next-Hop Address section will open at the bottom of the profile. Populate the following fields:

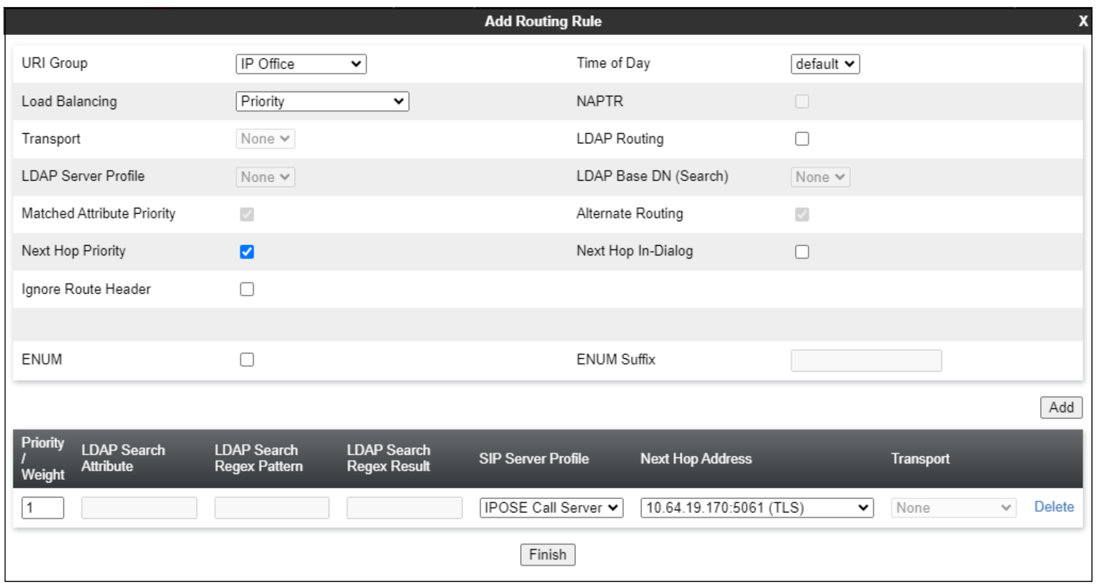
- **Priority/Weight**: **1**
- **SIP Server Profile:** Select **Posh Voice Prod** (from **Section 6.7.3**).
- **Next Hop Address:** Select the FQDN of the by Posh Voice Production primary site.
- Click the **Add** button to add a second Next-Hop Address.
- **Priority/Weight**: **2**
- **SIP Server Profile:** Select **Posh Voice Prod** (from **Section 6.7.3**).
- **Next Hop Address:** Select the FQDN of the by Posh Voice Production secondary site.
- Click **Finish**.



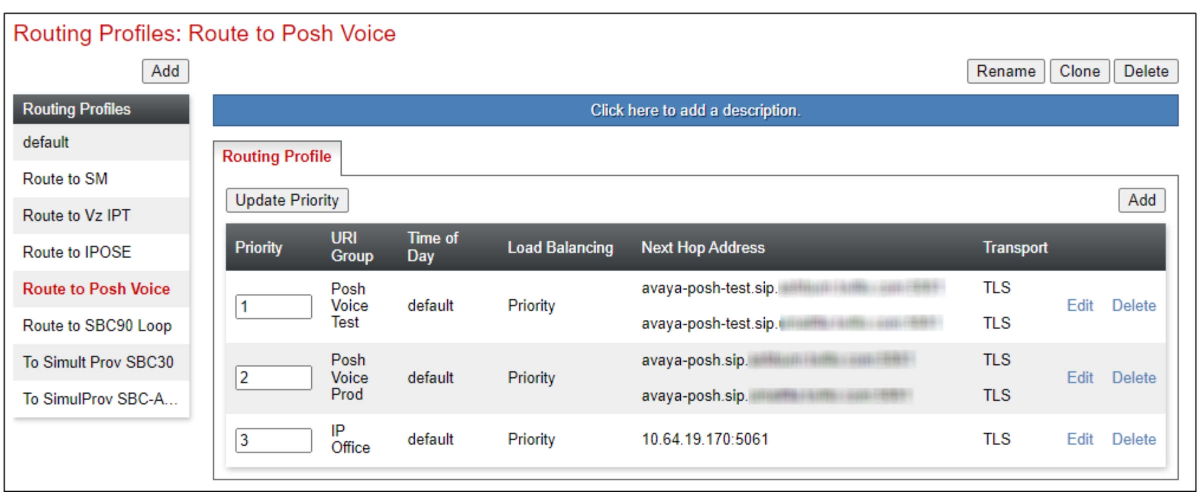
Back at the Routing Profiles screen, with the **Route to Posh Voice** profile selected, click the **Add** button on the right side of the screen to add a third routing rule to the profile. This rule is needed to provide Avaya SBC the logic to determine the proper direction of the INVITE it generates, based on the Refer-To header in REFER messages arriving from Posh Voice.

On the Routing Profile window, under **URI Group** select the **IP Office** URI Group created in **Section 6.8.3**. Click the **Add** button. The Next-Hop Address section will open at the bottom of the profile. Populate the following fields:

- **Priority/Weight**: **1**
- **SIP Server Profile:** Select **IPOSE Call Server** (from **Section 6.7.1**).
- **Next Hop Address:** Verify that the **10.64.19.170:5061 (TLS)** entry from the drop-down menu is selected.
- Click **Finish**.



The screen below shows the completed Routing Profile:

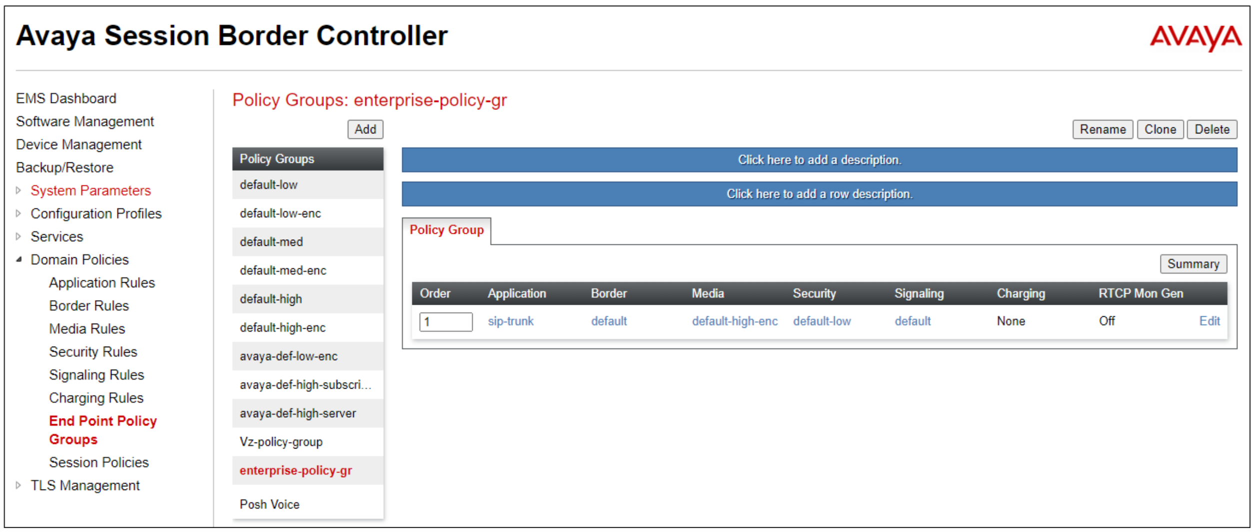


6.10. Endpoint Policy Groups

Endpoint policy groups are set of Domain Policies that will be applied to traffic between Avaya SBC and a connected server. The Endpoint Policy Group is applied to the traffic as part of the Server Flows defined later in **Section 6.11**. A new Endpoint Policy Group was defined for Posh Voice, while a Policy Group for the enterprise (IP Office) was already existing, and re-used in this configuration.

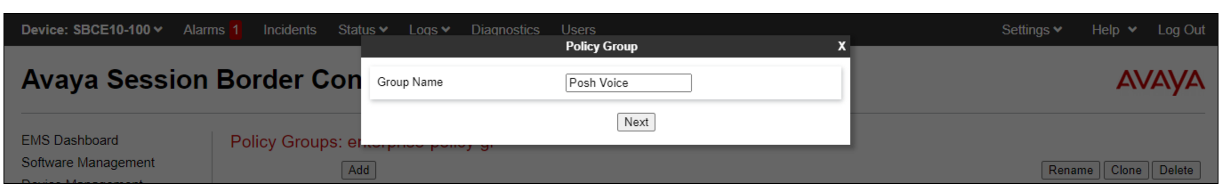
6.10.1 Endpoint Policy Group – IP Office

The following Policy Group named **enterprise-policy-gr** was already defined in Avaya SBC for the IP Office, using the values shown on the screen below. The Policy Group was reused in the configuration for Posh Voice without making any changes, but it is shown here for completeness.



6.10.2 Endpoint Policy Group – Posh Voice

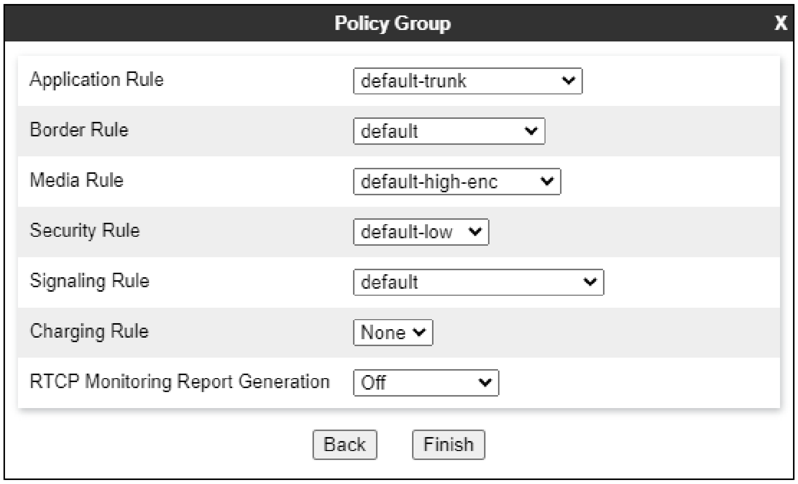
To create a new Endpoint Policy Group for Posh Voice, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the right pane, select **Add**. Enter a **Group Name** (e.g., **Posh Voice**) and click **Next** to continue.



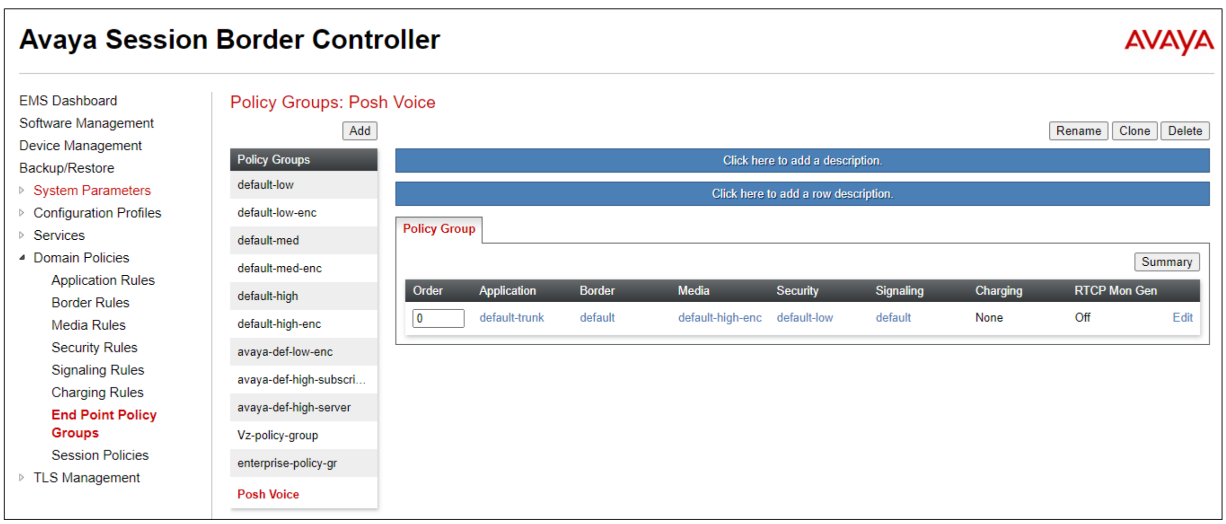
On the **Policy Group** window select the following predefined default set of rules on the SBC:

- **Application Rule**: **default-trunk**.
- **Border Rule**: **default**.
- **Media Rule**: **default-high-enc**. Note that since SRTP is used for the media to Posh Voice, this media rule is required.
- **Security Rule**: **default-low**.
- **Signaling Rule**: **default**.

- **Charging Rule**: **None**.
- **RTCP Monitoring Report Generation**: **Off**.
- Select **Finish**.



The completed Policy Group **Posh Voice** is shown on the screen below.



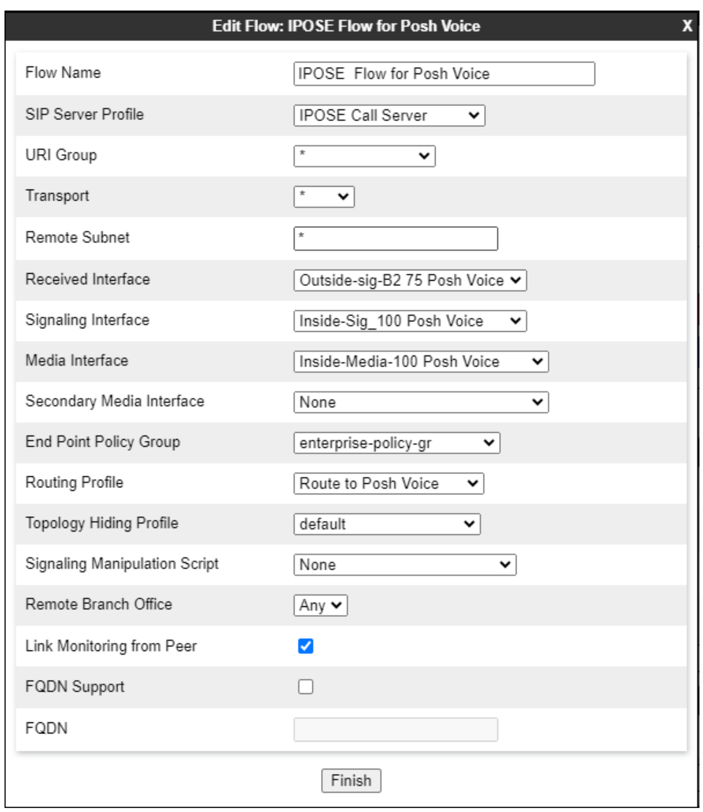
6.11. Endpoint Flows – Server Flows

Server Flows combine the interfaces, polices, and profiles defined in the previous sections into inbound and outbound flows. When a packet is received by Avaya SBC, the content of the packet (IP addresses, SIP URIs, etc.) is used to determine which flow it matches, so that the appropriate policies can be applied. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. Separate Server Flows are created for IP Office and Posh Voice.

6.11.1 Server Flows – IP Office

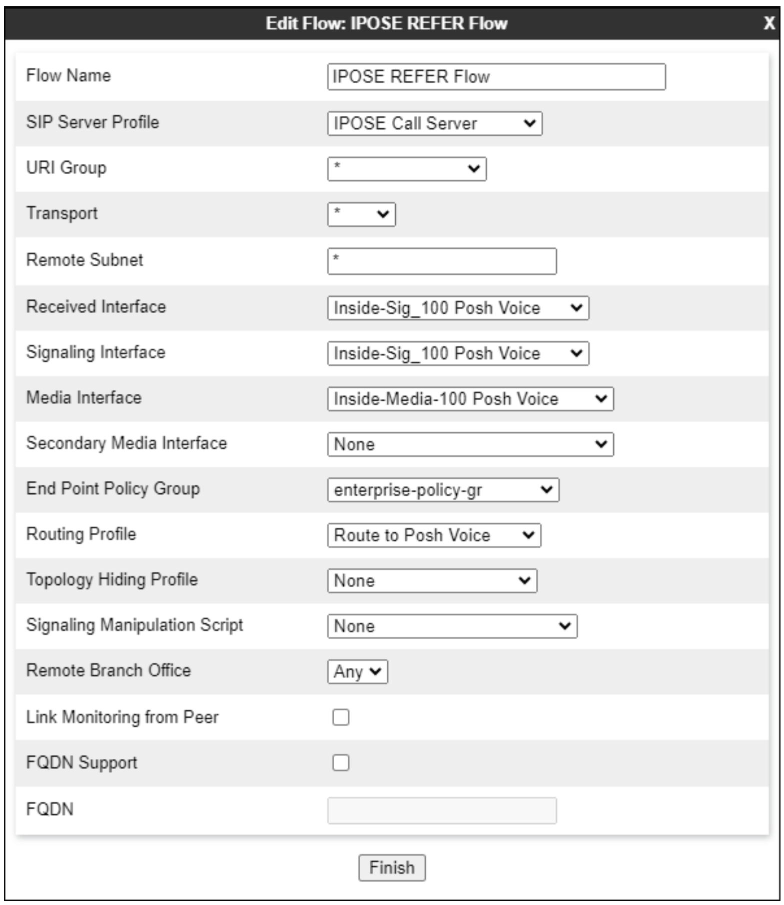
Select **Network and Flows → Endpoint Flows** from the menu on the left-hand side, and select the **Server Flows** tab and click **Add** (not shown). Enter the following parameters:

- **Flow Name**: **IPOSE Flow to Posh Voice**.
- **SIP Server Profile**: **IPOSE Call Server** (**Section 6.7.1**).
- **URI Group**, **Transport**, **Remote Subnet**: *
- **Received Interface**: **Outside-sig-B2 75 Posh Voice** (**Section 6.5**).
- **Signaling Interface**: **Inside-Sig_100 Posh Voice** (**Section 6.5**).
- **Media Interface**: **Inside-Media-100 Posh Voice** (**Section 6.4**).
- **End Point Policy Group**: **enterpr-policy-policy** (**Section 6.10.1**).
- **Routing Profile**: **Route to Posh Voice** (**Section 6.9.2**).
- **Topology Hiding Profile**: **default**.
- Check the **Link Monitoring from Peer** box.
- Let other fields at the default values. Click **Finish**.



The screen below shows the Server Flow named **IPOSE REFER Flow** created in the reference configuration, with the following parameters. This "self-flow" was needed for the Refer Handling feature operation on the Avaya SBC.

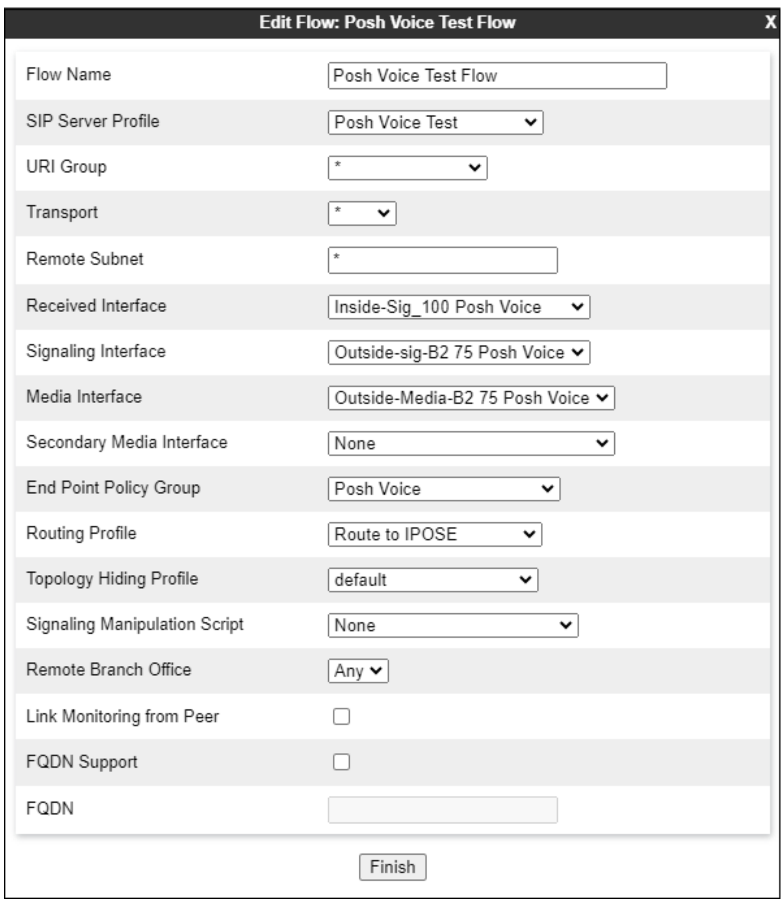
- **SIP Server Profile**: **IPOSE Call Server** (**Section 6.7.1**).
- **URI Group**, **Transport**, **Remote Subnet**: *
- **Received Interface**: **Inside-Sig_100 Posh Voice** (**Section 6.5**).
- **Signaling Interface**: **Inside-Sig_100 Posh Voice** (**Section 6.5**).
- **Media Interface**: **Inside-Media-100 Posh Voice** (**Section 6.4**).
- **End Point Policy Group**: **enterpr-policy-policy** (**Section 6.10.1**).
- **Routing Profile**: **Route to Posh Voice** (**Section 6.9.2**).
- Let other fields at the default values.
- Click **Finish**.



6.11.2 Server Flow – Posh Voice Test

The screen below shows the Server Flow for Posh Voice Test created in the reference configuration, with the following parameters:

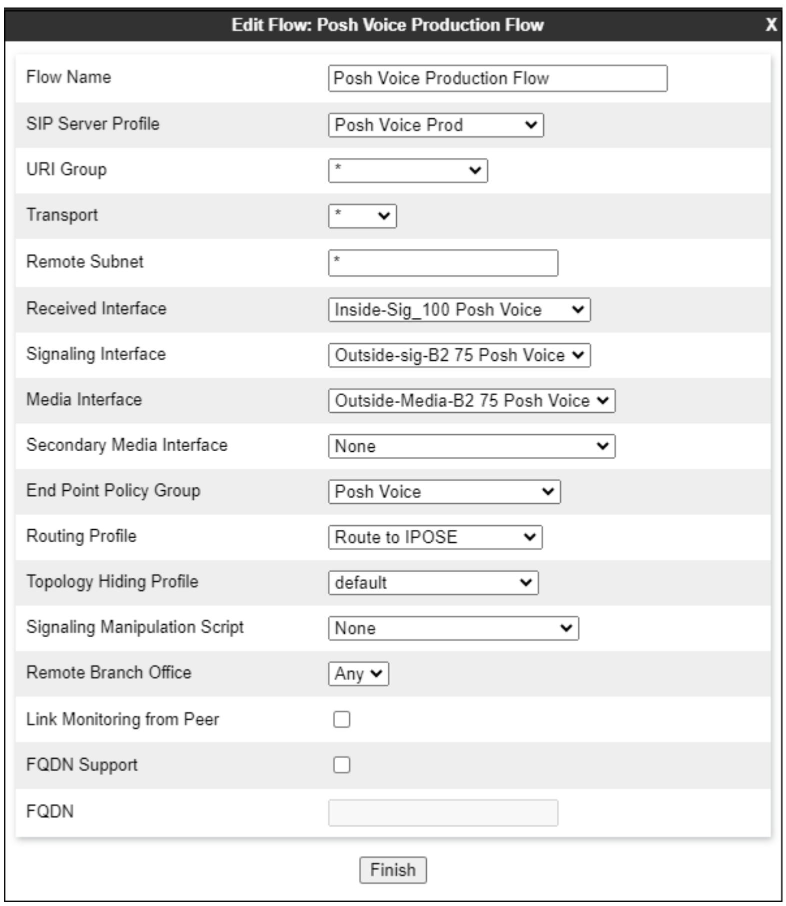
- **Flow Name**: **Posh Voice Test Flow**.
- **SIP Server Profile**: **Posh Voice Test** (**Section 6.7.2**).
- **URI Group**, **Transport**, **Remote Subnet**: *****
- **Received Interface**: **Inside-Sig_100 Posh Voice** (**Section 6.5**).
- **Signaling Interface**: **Outside-sig-B2 75 Posh Voice (Section 6.5**).
- **Media Interface**: **Outside-Media-B2 75 Posh Voice** (**Section 6.4**).
- **End Point Policy Group**: **Posh Voice** (**Section 6.10.2**).
- **Routing Profile**: **Route to IPOSE** (**Section 6.9.1**).
- **Topology Hiding Profile**: **default**.
- Let other fields at the default values.
- Click **Finish**.



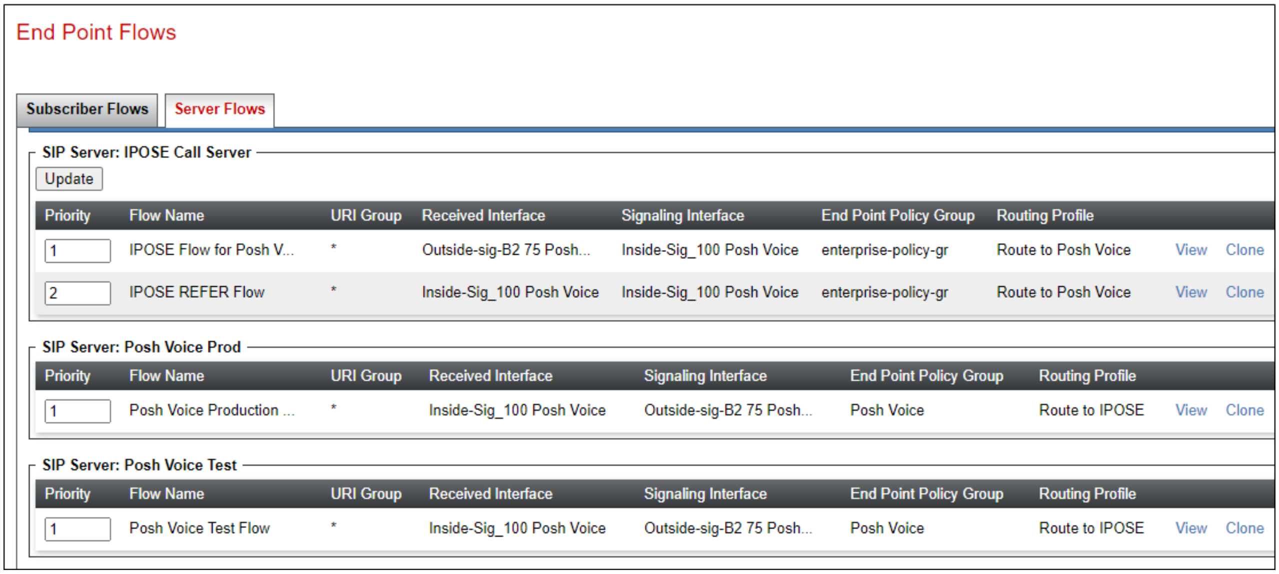
6.11.3 Server Flow – Posh Voice Production

The screen below shows the Server Flow for Posh Voice Prod created in the reference configuration, with the following parameters:

- **Flow Name**: **Posh Voice Production Flow**.
- **SIP Server Profile**: **Posh Voice Prod** (**Section 6.7.3**).
- **URI Group**, **Transport**, **Remote Subnet**: *
- **Received Interface**: **Inside-Sig_100 Posh Voice** (**Section 6.5**).
- **Signaling Interface**: **Outside-sig-B2 75 Posh Voice (Section 6.5**).
- **Media Interface**: **Outside-Media-B2 75 Posh Voice** (**Section 6.4**).
- **End Point Policy Group**: **Posh Voice** (**Section 6.10.2**).
- **Routing Profile**: **Route to IPOSE** (**Section 6.9.1**).
- **Topology Hiding Profile**: **default**.
- Let other fields at the default values.
- Click **Finish**.



The screen below shows the **Server Flows** tab once the configuration is completed.



7. Posh Voice Configuration

The configuration of Posh Voice is performed by Posh technical personnel. For provisioning, Posh will require the following information:

- Avaya SBC public IP address.
- Extension numbers (hunt groups, short codes, etc.) where Posh Voice will transfer calls to agents at Avaya IP Office.

8. Verification Steps

Complete the following general steps to verify correct functionality of the Avaya configuration with Posh Voice.

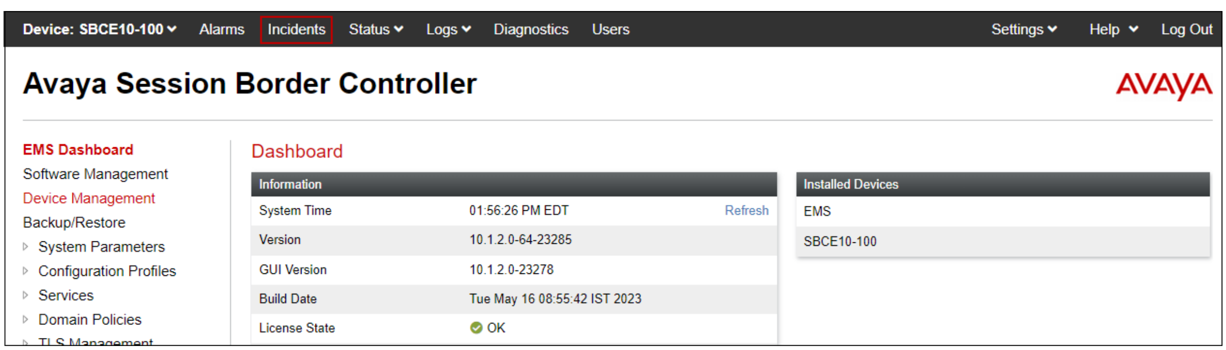
- Place a call to Posh Voice and verify the application answers and the appropriate greeting is heard.
- Caller navigates through the application using speech and DTMF. Verify Posh Voice provides the requested information.
- Posh Voice transfers call to an agent or PSTN. Verify the transferred call is established with two-way audio.
- Caller terminates the call successfully.

8.1. Avaya SBC

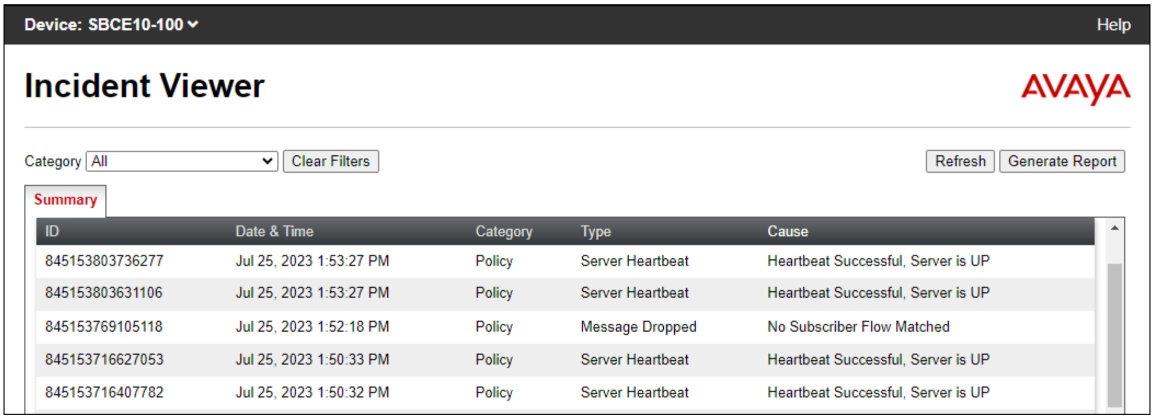
This section provides verification steps that may be performed on the Avaya SBC.

8.1.1 Incidents

The Incident Viewer can be accessed from the Avaya SBC top navigation menu as highlighted in the screen shot below.



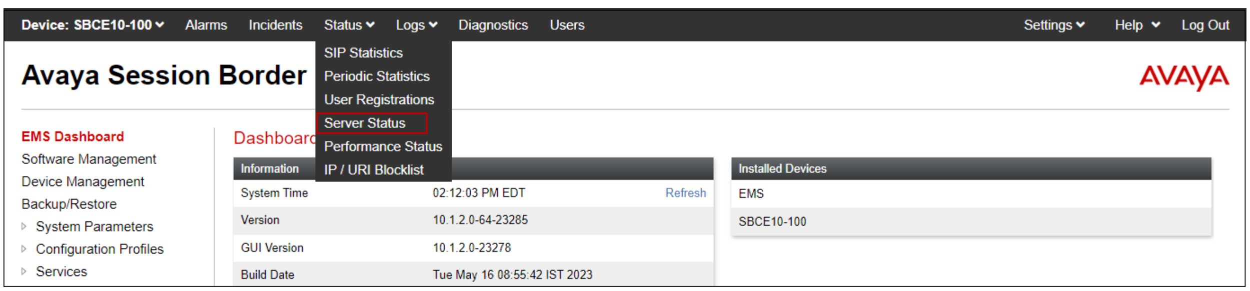
Use the Incident Viewer to verify server heartbeats and to troubleshoot routing and other failures.



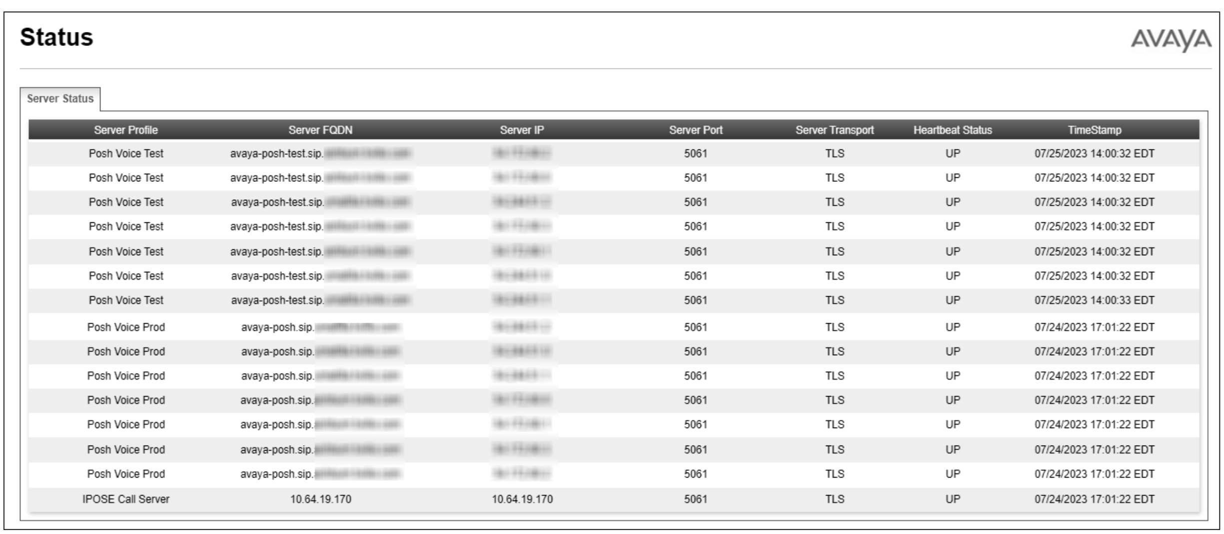
ID	Date & Time	Category	Type	Cause
845153803736277	Jul 25, 2023 1:53:27 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
845153803631106	Jul 25, 2023 1:53:27 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
845153769105118	Jul 25, 2023 1:52:18 PM	Policy	Message Dropped	No Subscriber Flow Matched
845153716627053	Jul 25, 2023 1:50:33 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
845153716407782	Jul 25, 2023 1:50:32 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP

8.1.2 Server Status

The **Server Status** can be access from the Avaya SBC top navigation menu by selecting the **Status** menu, and then **Server Status**.



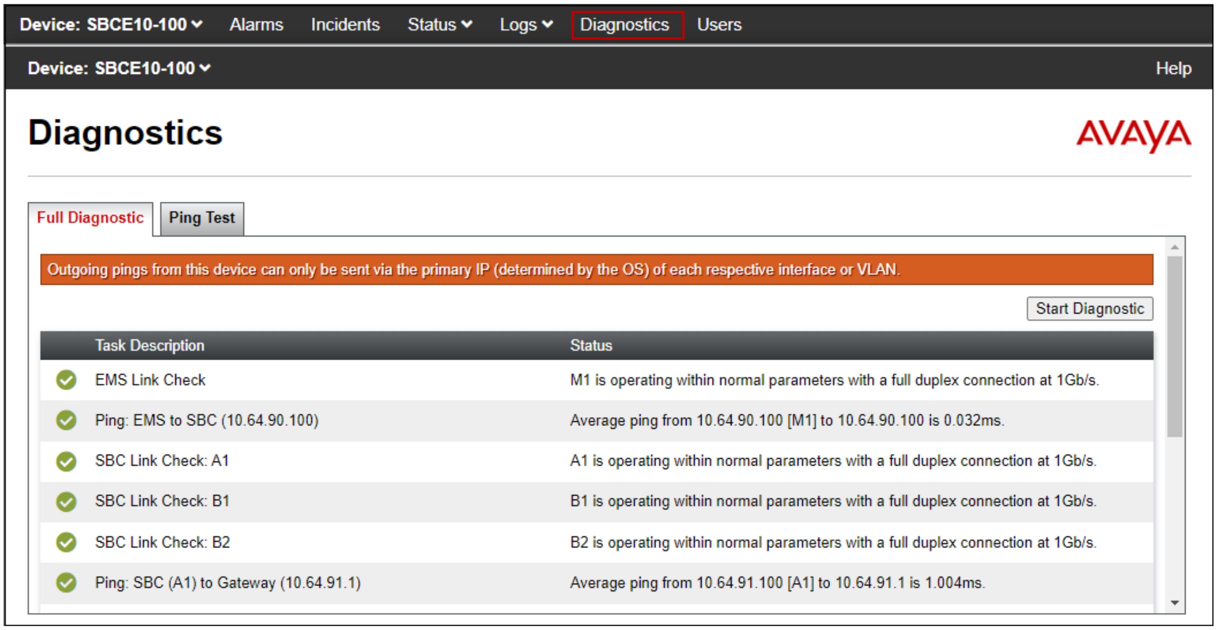
The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Configuration profiles, as configured in **Section 6.7**.



Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	TimeStamp
Posh Voice Test	avaya-posh-test.sip.[illegible]	[illegible]	5061	TLS	UP	07/25/2023 14:00:32 EDT
Posh Voice Test	avaya-posh-test.sip.[illegible]	[illegible]	5061	TLS	UP	07/25/2023 14:00:32 EDT
Posh Voice Test	avaya-posh-test.sip.[illegible]	[illegible]	5061	TLS	UP	07/25/2023 14:00:32 EDT
Posh Voice Test	avaya-posh-test.sip.[illegible]	[illegible]	5061	TLS	UP	07/25/2023 14:00:32 EDT
Posh Voice Test	avaya-posh-test.sip.[illegible]	[illegible]	5061	TLS	UP	07/25/2023 14:00:32 EDT
Posh Voice Test	avaya-posh-test.sip.[illegible]	[illegible]	5061	TLS	UP	07/25/2023 14:00:32 EDT
Posh Voice Test	avaya-posh-test.sip.[illegible]	[illegible]	5061	TLS	UP	07/25/2023 14:00:33 EDT
Posh Voice Prod	avaya-posh.sip.[illegible]	[illegible]	5061	TLS	UP	07/24/2023 17:01:22 EDT
Posh Voice Prod	avaya-posh.sip.[illegible]	[illegible]	5061	TLS	UP	07/24/2023 17:01:22 EDT
Posh Voice Prod	avaya-posh.sip.[illegible]	[illegible]	5061	TLS	UP	07/24/2023 17:01:22 EDT
Posh Voice Prod	avaya-posh.sip.[illegible]	[illegible]	5061	TLS	UP	07/24/2023 17:01:22 EDT
Posh Voice Prod	avaya-posh.sip.[illegible]	[illegible]	5061	TLS	UP	07/24/2023 17:01:22 EDT
Posh Voice Prod	avaya-posh.sip.[illegible]	[illegible]	5061	TLS	UP	07/24/2023 17:01:22 EDT
Posh Voice Prod	avaya-posh.sip.[illegible]	[illegible]	5061	TLS	UP	07/24/2023 17:01:22 EDT
IPOSE Call Server	10.64.19.170	10.64.19.170	5061	TLS	UP	07/24/2023 17:01:22 EDT

8.1.3 Diagnostics

This screen provides a **Full Diagnostics** tool to verify the link of each interface and ping the configured next-hop gateways and DNS servers. The **Ping Test** tool can be used to ping specific devices from any Avaya SBC interface.



8.1.4 Tracing

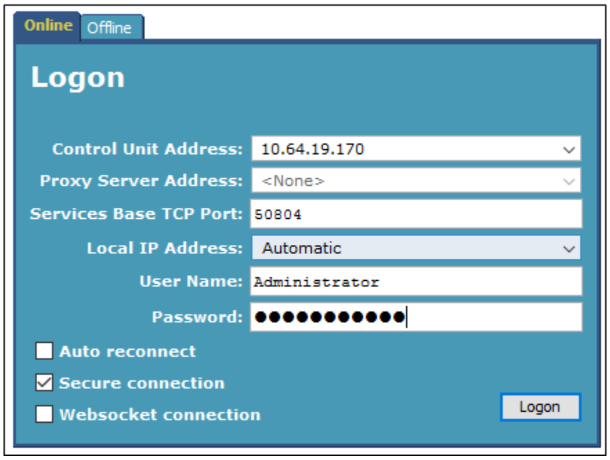
tracesbc is an Avaya Session Border Controller command line tool for traffic analysis. Log into the Avaya SBC command line management interface to run this command. In Avaya SBC version 10.1.2, root credentials are required to run this command.

8.2. Avaya IP Office

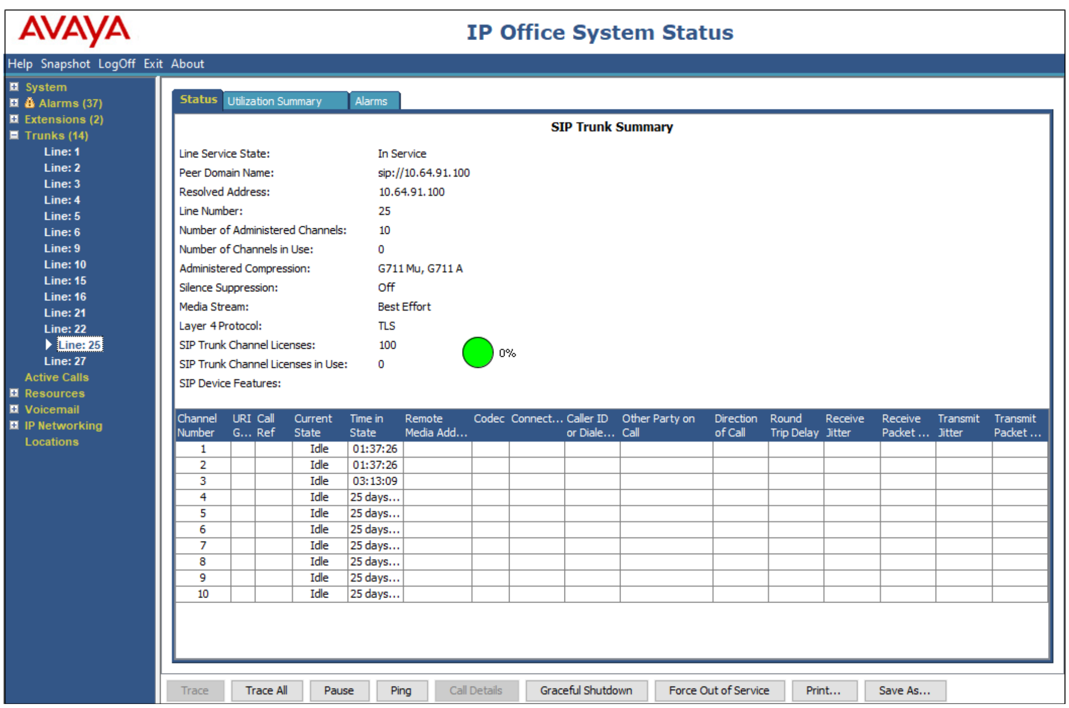
This section provides verification steps that may be performed with the IP Office.

8.2.1 System Status Application

The Avaya IP Office System Status application can be used to verify the service state of the SIP line. From the IP Office Manager application, select **File → Advanced → System Status**. Under **Control Unit IP Address** select the IP address of the IP Office system under verification. Log in using the appropriate credentials.



On the left pane, select the SIP line used to connect IP Office to Posh Voice via Avaya SBC (**Line 25** in the reference configuration). On the **Status** tab in the right pane, verify that the **Current State** is ***Idle*** for each channel (assuming no active calls at present time).



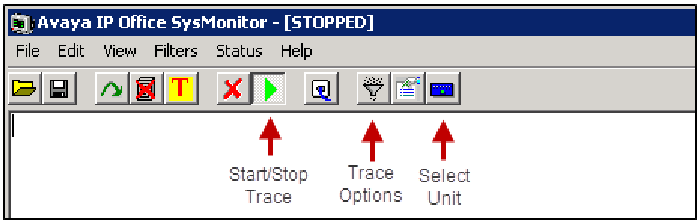
Channel Number	URI G...	Call Ref	Current State	Time in State	Remote Media Add...	Codec	Connect...	Caller ID or Diale...	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet ...	Transmit Jitter	Transmit Packet ...
1			Idle	01:37:26											
2			Idle	01:37:26											
3			Idle	03:13:09											
4			Idle	25 days...											
5			Idle	25 days...											
6			Idle	25 days...											
7			Idle	25 days...											
8			Idle	25 days...											
9			Idle	25 days...											
10			Idle	25 days...											

In the lower part of the screen, the **Trace All** button may be pressed to display real time tracing information as calls are made using this SIP Line. The **Ping** button can be used to ping the other end of the SIP trunk (e.g., Avaya SBC).

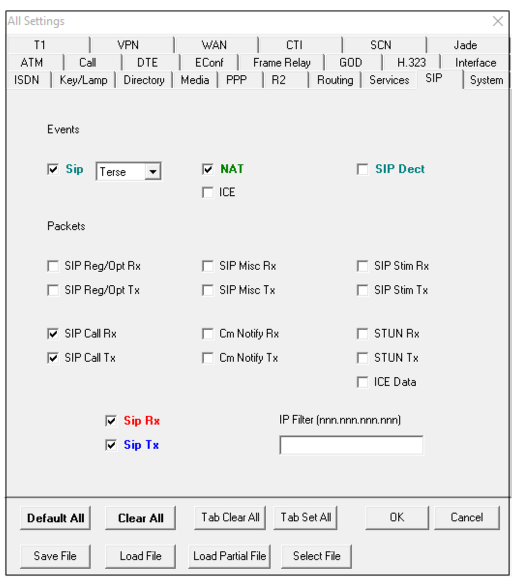
Select the **Alarms** tab and verify that no alarms are active on the SIP line (not shown).

8.2.2 System Monitor

The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the IP Office system under verification.



Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting to the desired color.



9. Conclusion

These Application Notes have described the configuration steps required to integrate Posh Voice with an Avaya solution consisting of Avaya IP Office release 11.1 and Avaya Session Border Controller release 10.1. Posh Voice connected to the Avaya solution via a SIP service provider. Callers were able to interact with Posh Voice using speech and DTMF to retrieve and provide information. Posh Voice was able to transfer the call to IP Office agents when requested by the caller, and also to endpoints on the PSTN.

All test cases completed successfully, with the observation noted in **Section 2.2**.

10. Additional References

This section references documentation relevant to these Application Notes. In general, Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya IP Office™ Platform with Manager*, Release 11.1, Issue 2, May 2020.
[2] *Administering Avaya Session Border Controller* Release 10.1.x, Issue 6, May 2023.
[3] *RFC 3261 SIP: Session Initiation Protocol*. https://www.ietf.org/rfc/rfc3261.txt

Additional IP Office documentation can be found at:
https://ipofficekb.avaya.com/

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.