Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunking Using Verizon Business IP Contact Center VoIP Inbound with Avaya IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 8.0.1 – Issue 1.0

Abstract

These Application Notes describe a reference configuration using Session Initiation Protocol (SIP) trunking between the Verizon Business IP Contact Center VoIP Inbound SIP Trunk Service and an Avaya IP Office solution. In the reference configuration, the Avaya IP Office solution consists of Avaya IP Office Server Edition Release 11.1, Avaya Session Border Controller for Enterprise Release 8.1 and Avaya SIP, H.323, digital, and analog endpoints.

These Application Notes complement previously published Application Notes by illustrating the configuration screens and Avaya testing of IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 8.1.

The Verizon Business IP Contact Center VoIP Inbound offer referenced within these Application Notes enables a business to receive inbound toll-free calls via standards-based SIP trunks, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

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.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted in the Avaya Solution & Interoperability Test Lab, utilizing a Verizon Business Private IP (PIP) circuit connection to the Verizon Business IP Contact Center service.

Table of Contents

1. Introduction

These Application Notes describe a reference configuration using Session Initiation Protocol (SIP) trunking between the Verizon Business IP Contact Center VoIP Inbound Service (Verizon Business IPCC) and an Avaya IP Office solution. In the reference configuration, the Avaya IP Office solution consists of Avaya IP Office Server Edition Primary Server Release 11.1, an IP500 V2 Expansion System Release 11.1, Avaya Session Border Controller for Enterprise Release 8.1 and Avaya SIP, H.323, digital, and analog endpoints.

Customers using Avaya IP Office with the Verizon Business IPCC service are able to receive inbound toll-free calls from the PSTN via the SIP protocol. The converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI. This service provides toll free inbound calling via standards-based SIP trunks as well as re-routing of inbound toll-free calls to alternate destinations based upon SIP messages (i.e., REFER) generated by the Avaya IP Office.

In the reference configuration, an Avaya Session Border Controller for Enterprise (Avaya SBCE) is used as an edge device between the Avaya IP Office and Verizon business. The Avaya SBCE performs SIP header manipulation and provides topology hiding, as well as a variety of other functions providing security and the presentation of a standardized SIP interface.

Verizon Business IPCC service can be delivered to the customer premise via either a Private IP (PIP) or Internet Dedicated Access (IDA) IP network terminations. Although the configuration documented in these Application Notes used Verizon's IPCC service terminated via a PIP network connection, the solution validated in this document applies also to IP Contact Center services delivered via IDA service terminations.

For more information on the Verizon Business IPCC service, visit https://enterprise.verizon.com/products/customer-experience-services/transport-and-intelligent-routing/ip-contact-center/

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Verizon Business IPCC service, as depicted in **Figure 1**. The Avaya SBCE and IP Office were configured to use the commercially available SIP Trunking solution provided by the Verizon Business IPCC service. This allowed Avaya IP Office to receive inbound toll-free calls from the PSTN via the SIP protocol.

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 systems and Verizon Business IPCC Services did not include use of any specific encryption features as requested by Verizon.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products wherever possible.

2.1. Interoperability Compliance Testing

The testing included executing the test cases detailed in **Section 11**, reference [VZ-Test-Plan], which contains the Verizon Business IPCC Interoperability Lab Test Plan. To summarize, the testing included the following successful SIP trunk interoperability compliance testing:

- SIP OPTIONS monitoring of the health of the SIP trunk was verified. Verizon Business, Avaya SBCE, and IP Office can all monitor health using SIP OPTIONS.
- Proper recovery from induced failure conditions such as IP Office reboots, and IP network outages between Verizon and IP Office, of short and long durations.
- Incoming calls from the PSTN were routed to the toll-free numbers assigned by Verizon Business to the Avaya IP Office location. These incoming calls arrived via the SIP Line configured in **Section 5.5** and were answered by Avaya H.323 telephones, Avaya SIP telephones, Avaya IX™ Workplace for Windows (SIP) softphones, Avaya digital and analog telephones, as well as Avaya IP Office Voicemail Pro.
- Proper disconnect when either party hangs up an active call.
- Proper disconnect when the PSTN caller abandons (i.e., hangs up) a toll-free call before the IP Office party has answered.
- Proper SIP 486 response and busy tone heard by the caller when a PSTN user calls a toll-free number directed to a busy IP Office user, an IP Office user with Do-not-disturb active, or an IP Office user that is logged out (i.e., assuming no redirection is configured for these conditions). Similarly, busy tone is heard when a PSTN user calls a toll-free number directed to a hunt group whose queue is "full" (i.e. if no redirection is configured for hunt group busy conditions, see **Section 5.7.2**).
- Proper termination of an inbound IP Toll Free call left in a ringing state for a relatively long duration.
- The display of caller ID on display-equipped Avaya IP Office telephones was verified. The IP Office capability to use the caller ID received from Verizon to look up and display a name from a configurable directory was also exercised successfully.
- Privacy requests for inbound toll-free calls from the PSTN were verified. That is, when privacy is requested by a PSTN caller (e.g., dialing *67 from a mobile phone), the inbound toll-free call can be successfully completed to an IP Office telephone user while

presenting a “WITHHELD” or anonymous display to an IP Office user (i.e., rather than the caller’s telephone number).

- Inbound toll-free long holding time call stability.
- Inbound fax calls using T.38 and G.711.
- Telephony features such as hold and resume, transfer of toll-free calls to other IP Office users, and conference of toll-free calls.
- Incoming voice calls using the G.729(a) and G.711 ULAW codecs, and proper protocol procedures related to media.
- DTMF transmission using RFC 2833. Successful IP Office Voicemail Pro menu navigation for incoming toll-free calls.
- Incoming toll-free calls directed to the Hunt Groups configured in **Section 5.7.2** were verified. Incoming calls could be queued, queued with priority, and be answered by members of the hunt group as members become available.
- Outgoing calls from the Avaya IP Office location to the PSTN were routed via a SIP Line to the Verizon Business IP Trunk service described in reference [IPT-IPO111SBC81]. As detailed in reference [IPT-IPO111SBC81], these outgoing PSTN calls can be originated from Avaya H.323 telephones, Avaya SIP telephones, Avaya digital telephones, and analog endpoints. The display of caller ID on display-equipped PSTN telephones was verified. In the context of inbound toll-free calls using Verizon Business IPCC, inbound toll-free calls arriving via the SIP Line configured in **Section 5.5** could be forwarded or twinned out the Verizon Business IP Trunk service SIP Line. Inbound toll-free calls from the Verizon Business IPCC SIP Line could also trigger mobile callback calls that use the Verizon Business IP Trunk service SIP Line.
- Call Forwarding of Verizon toll-free calls to PSTN destinations via the Verizon Business IP Trunk service documented in reference [IPT-IPO111SBC81], presenting true calling party information to the mobile phone.
- Mobile twinning of Verizon toll-free calls to a mobile phone via the Verizon Business IP Trunk service documented in reference [IPT-IPO111SBC81], presenting true calling party information to the mobile phone.
- Proper DiffServ markings for Avaya SBCE SIP signaling and RTP media.
- Avaya Remote Worker configuration via the Avaya SBCE.

2.2. Test Results

Interoperability testing of the reference configuration was completed with successful results. The following observations were noted.

- During the compliance test, some inbound toll-free calls are transferred back to the Verizon Business IPCC service to be routed to alternate destinations. Since the Verizon Business IPCC in the reference configuration is an inbound only service, the call transfer is achieved by IP Office sending a SIP REFER message, with a Refer-To without a Replaces header, back to Verizon. This functionality is limited to Voicemail Pro modules and certain SIP endpoints using blind transfer (e.g., Avaya 1140E, and Avaya IX™ Workplace for Windows). Other endpoints like J100 series IP telephones, H.323, digital, or analog endpoints do not support this type of transfer.
- On inbound toll-free calls that are transferred back out to the Verizon Business IPCC service using SIP REFER, Verizon sends a NOTIFY message after the "referred" call has been released from the IP Office. Since IP Office cannot associate this NOTIFY with any active call, it sends a "481 Call/Transaction Does Not Exist" to Verizon in response. No user perceived problem occurs because of this anomaly.
- When transferring an inbound Verizon Business IPCC toll-free call back out the Verizon Business IPCC service using SIP REFER to a third party that is busy, Verizon disconnects the call and no error message or busy tone is heard by the originating caller.
- The Verizon Business IPCC Services suite does not support the SIP 302 Redirect method.

2.3. Support

For technical support on Verizon Business IPCC Services offer, visit online support at http://www.verizonenterprise.com/support/

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates an example Avaya IP Office solution connected to the Verizon Business IP Contact Center SIP Trunk service. The Avaya equipment is located on a private IP subnet. An enterprise edge router provides access to the Verizon Business network via a Verizon Business T1 circuit. This circuit is provisioned for the Verizon Business Private IP (PIP) service.

In the reference configuration, the Avaya SBCE receives traffic from the Verizon Business IPCC service on port 5060 and sends traffic to port 5072, using UDP for network transport, as required by the Verizon Business IPCC service. Verizon provided five toll-free numbers associated with the IP Contact Center service. These toll-free numbers were mapped to IP Office destinations via Incoming Call Routes as shown in **Section 5.9**. The Avaya CPE environment domain known to Verizon was *adevc.avaya.globalipcom.com*.

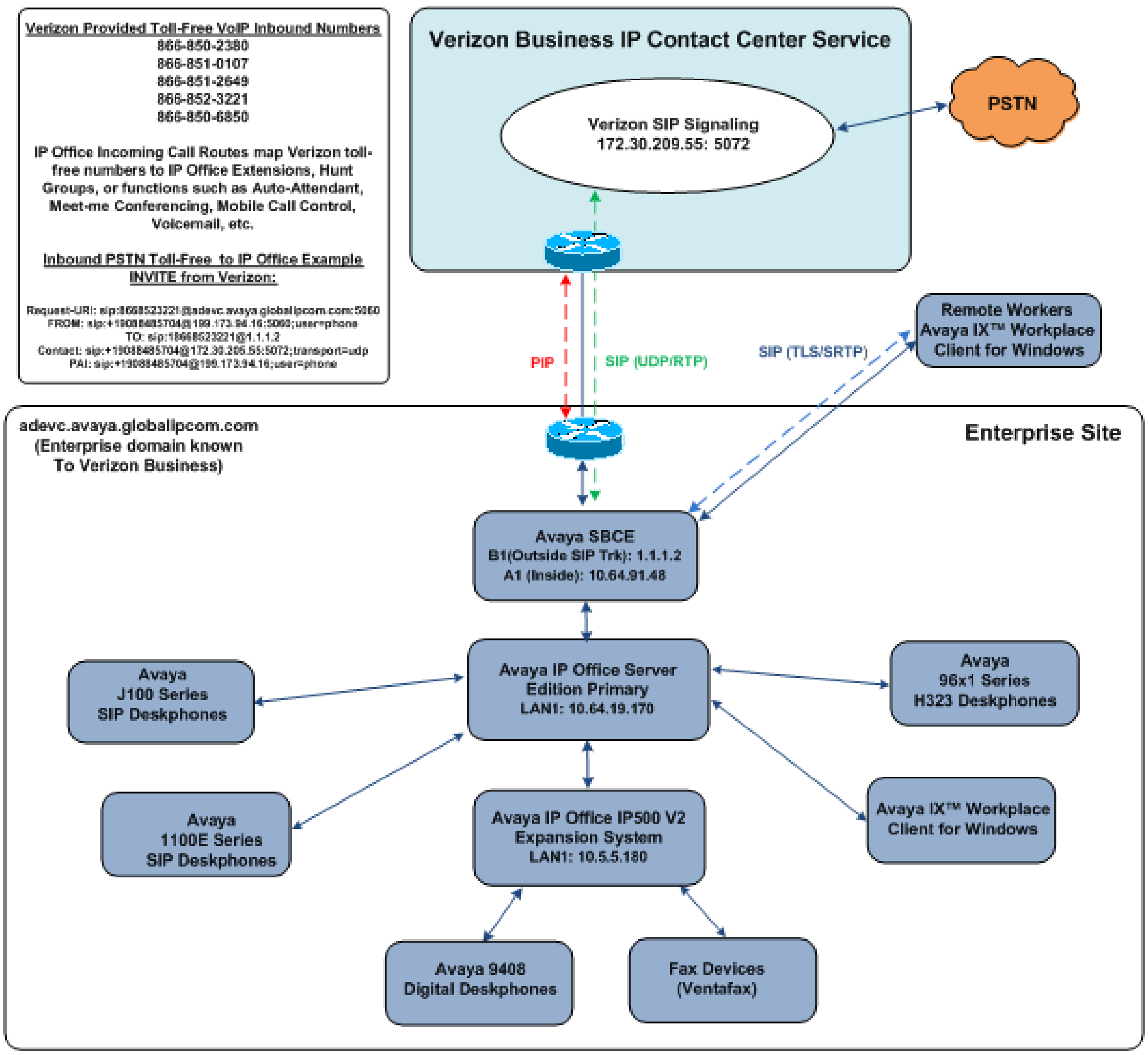


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon Business IP Trunk service used for outgoing calls, as described in **Section 2.1**, required different SIP line configuration parameters than what were needed for the Verizon Business IPCC service. A new SIP line was created in IP Office towards Avaya SBCE to support the Verizon Business IPCC service. This SIP line is separate from the SIP line previously created towards Avaya SBCE for Verizon Business IP Trunk service as described in reference [IPT-IPO111SBC81]. Having separate SIP lines for each Verizon service will allow for unique parameters to be set on IP Office to accommodate the differences between the two services. In order to support two SIP lines going towards the same Avaya SBCE, the Avaya SBCE was configured with two internal IP addresses designated for SIP trunk traffic.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to IP Office via the Avaya SBCE. Remote workers feature the same functionality as any other endpoint within the enterprise. This functionality was successfully tested during the compliance test.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. For more information on configuring the Avaya SBCE for IP Office remote workers, consult Error! Reference source not found. in the Additional References section.

4. Equipment and Software Validated

Table 1 shows the equipment and software used in the reference configuration.

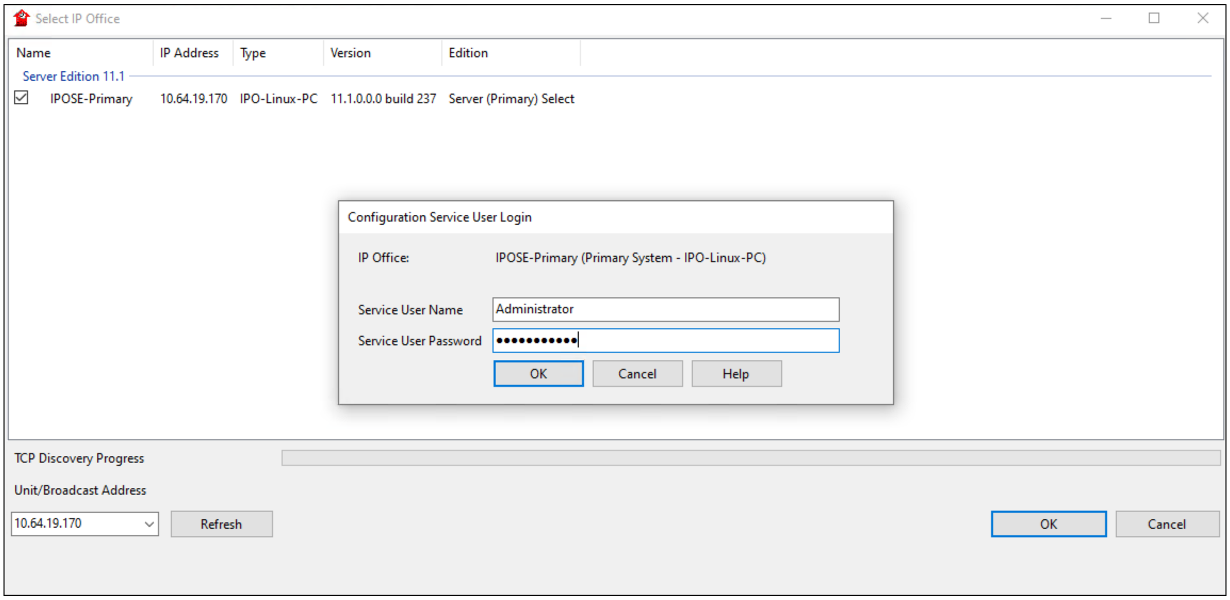
Avaya IP Telephony Solution Components	
Equipment	**Software**
Avaya IP Office Server Edition - Avaya IP Office Voicemail Pro	Release 11.1.0.0.0 Build 237 Release 11.1.0.0.0 Build 234
Avaya IP Office 500 V2 Expansion System	Release 11.1.0.0.0 Build 237
Avaya IP Office Manager	Release 11.1.0.0.0 Build 237
Avaya Session Border Controller for Enterprise	8.1.0.0.14-18490
Avaya 96x1 Series IP Deskphone (H.323)	Release 6.8304
Avaya 1140E IP Deskphone (SIP)	Release 04.04.23.00
Avaya J169 IP Deskphone (SIP)	Release 4.0.5.0.10
Avaya IX™ Workplace for Windows (SIP)	Release 3.8.5.41.23
Avaya 9508 Digital Deskphone	Release 0.60

Table 1: Equipment and Software Tested

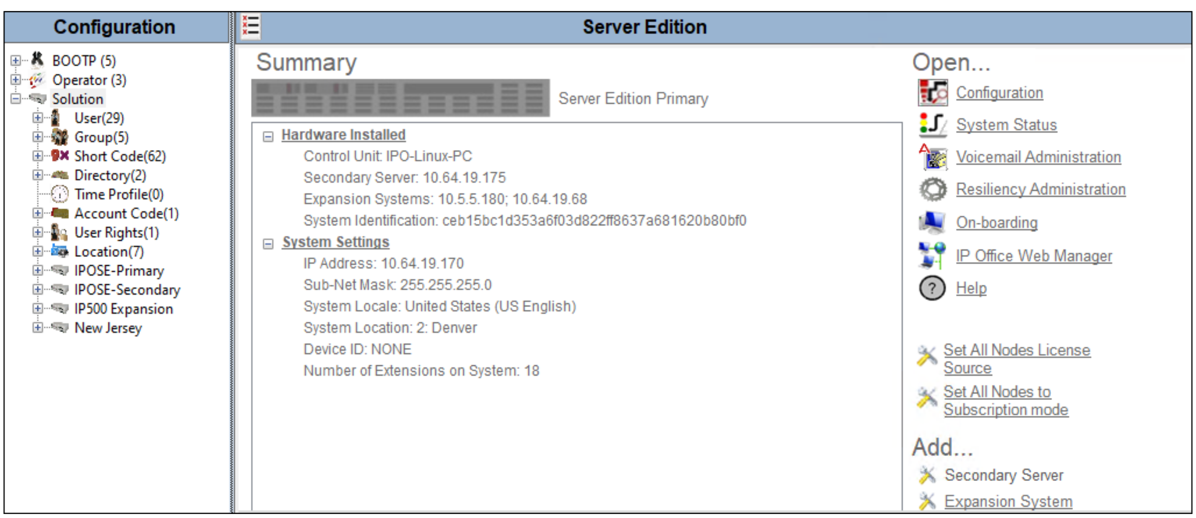
Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2, and also when deployed with all configurations of IP Office Server Edition. Note that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks.

5. Avaya IP Office Primary Server Configuration

IP Office is configured via the IP Office Manager program. For more information on IP Office Manager, consult reference **Error! Reference source not found.**. 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. All the Avaya IP Office configurable components are shown in the left pane, known as the Navigation Pane. Clicking the “plus” sign next to the Primary server system name, e.g., **IPOSE-Primary**, on the navigation pane will expand the menu on this server.

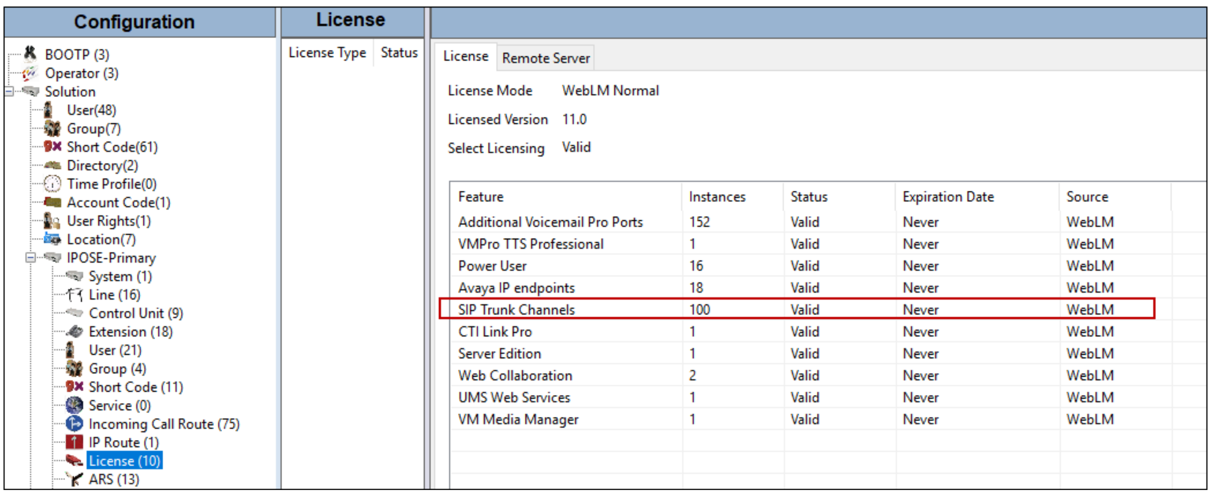


5.1. Licensing

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.

The configuration and features described in these Application Notes require the 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.

Navigate to **License** in the Navigation Pane. In the Details 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.

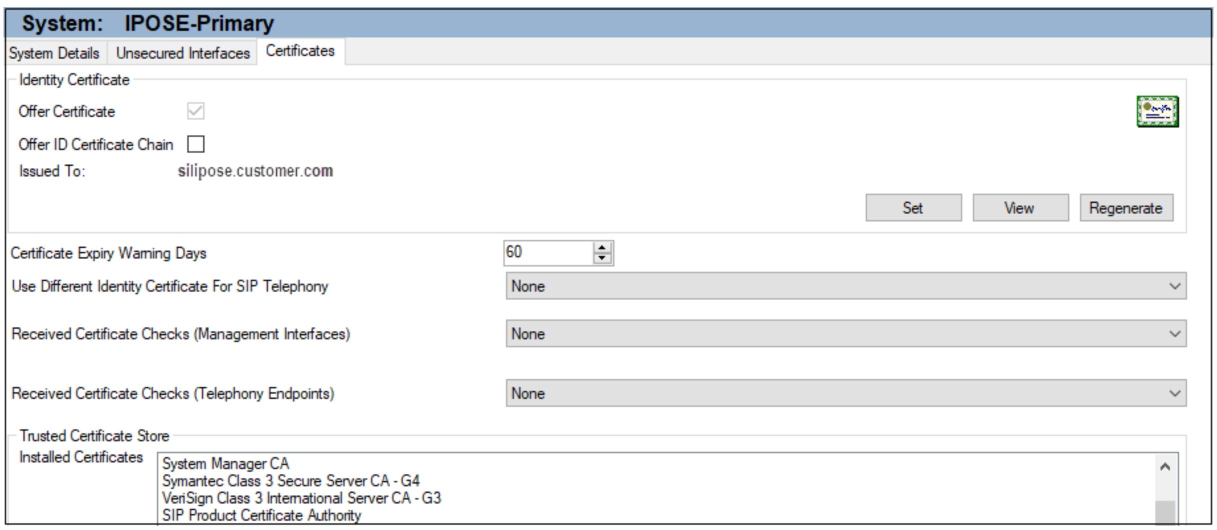


5.2. TLS Management

For the compliance test, the signaling on the SIP trunk between IP Office and the Avaya SBCE was secured using TLS. Testing was done using identity certificates signed by a local certificate authority **SystemManager CA**. 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.

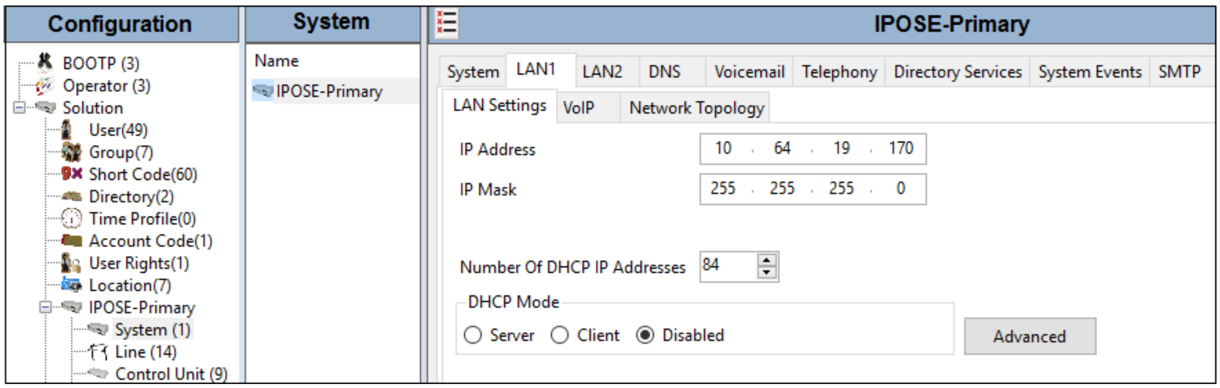


5.3. System Settings

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

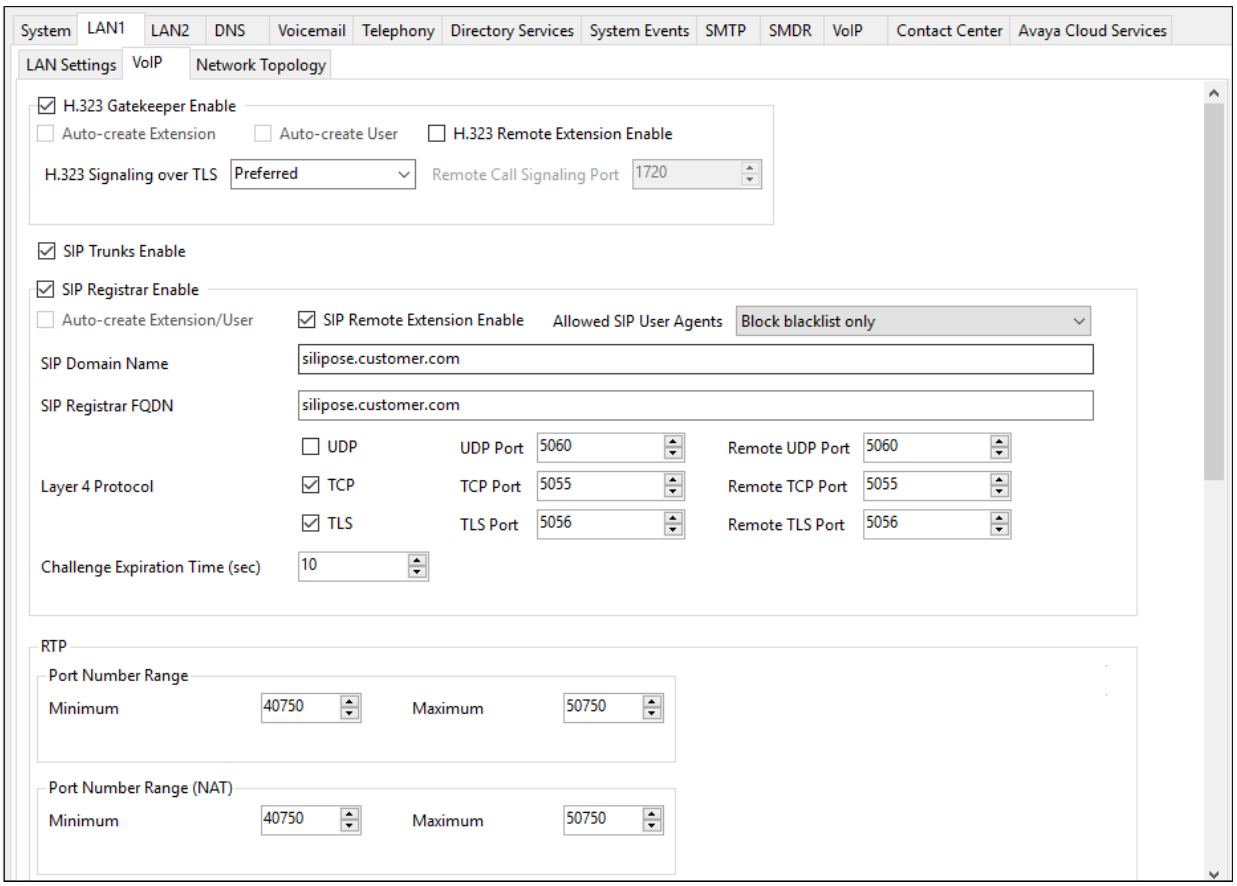
In the reference configuration, LAN1 is used to connect the Primary server to the enterprise network. To view or configure the **IP Address** of LAN1, select the **LAN1** tab followed by the **LAN Settings** tab. As shown in **Figure 1**, the IP Address of the Primary server is **10.64.19.170**. Other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



Select the **VoIP** tab as shown in the following screen. The **H323 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 SIP trunks to Verizon Business. The **SIP Registrar Enable** parameter is checked to allow Avaya J169, Avaya 1140E, and Avaya IX™ Workplace for Windows (SIP) usage.

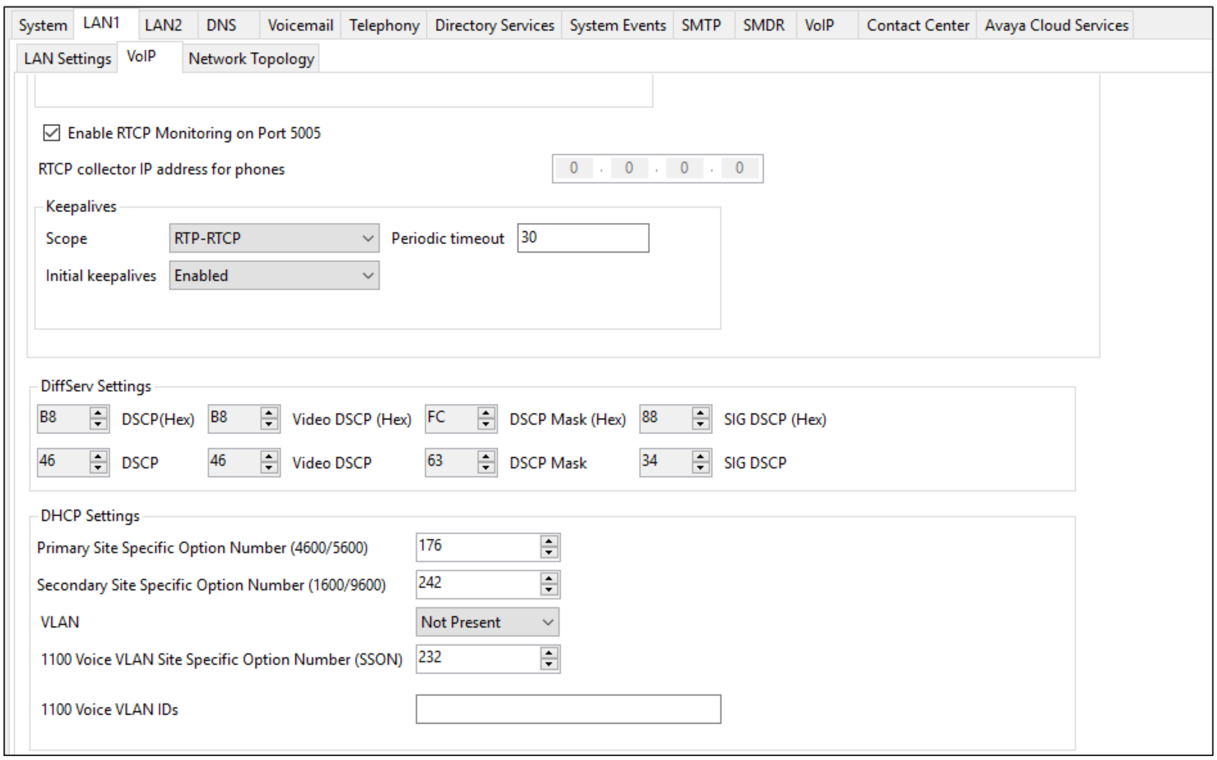
The **SIP Domain Name** and **SIP Registrar FQDN** may be set according to customer requirements. Set the **Layer 4 Protocol** section based on customer needs. In the reference configuration **TCP/5055** and **TLS/5056** were configured.

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

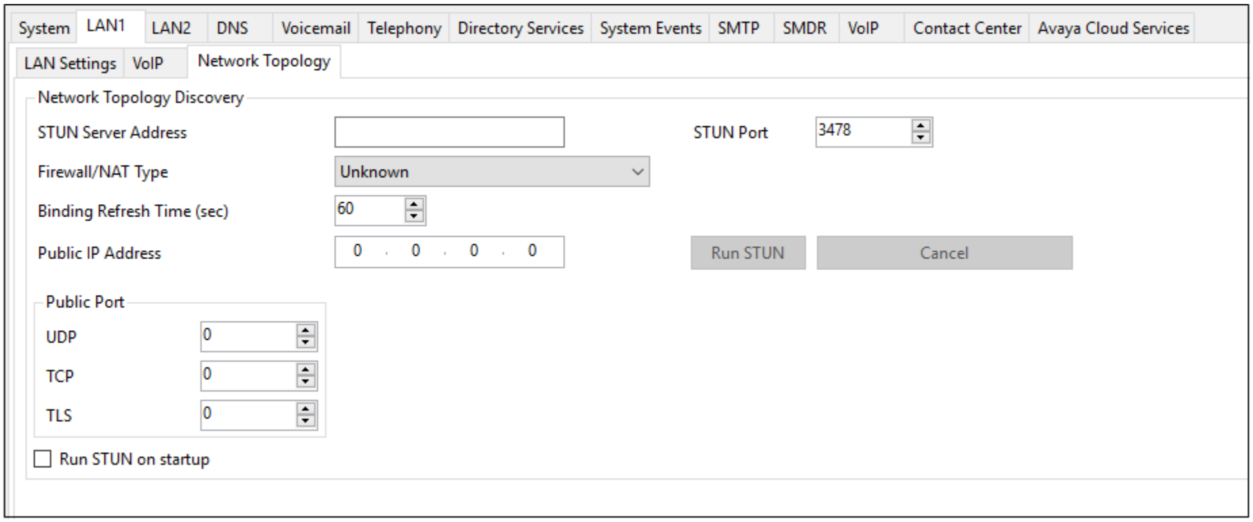


Scrolling down the page, on the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. These settings will cause the Primary server to send RTP and RTCP keepalive packets starting at the time of initial 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.

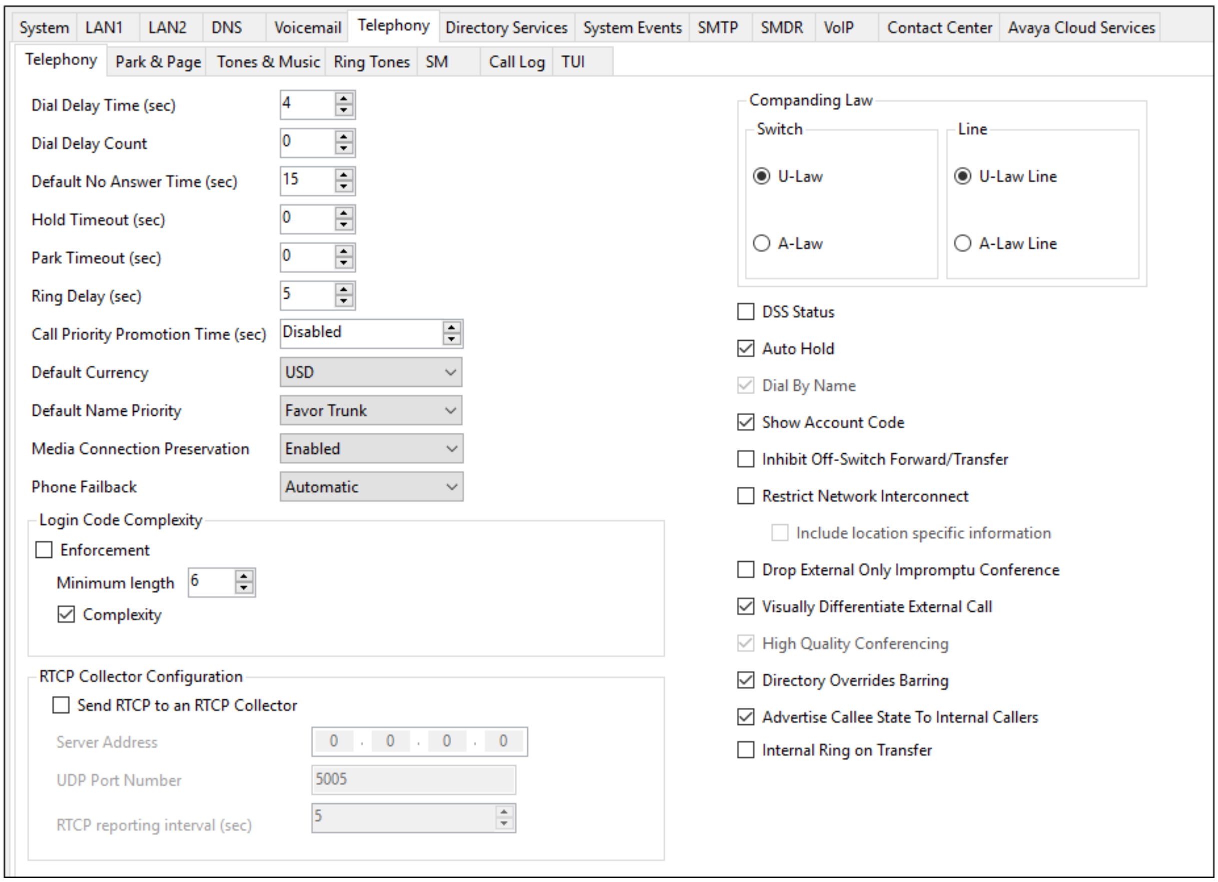


Select the **Network Topology** tab as shown in the following screen. The **Firewall/NAT Type** was set to **Unknown** in the reference configuration. **Binding Refresh Time (sec)** was set to **60** seconds. This is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages,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



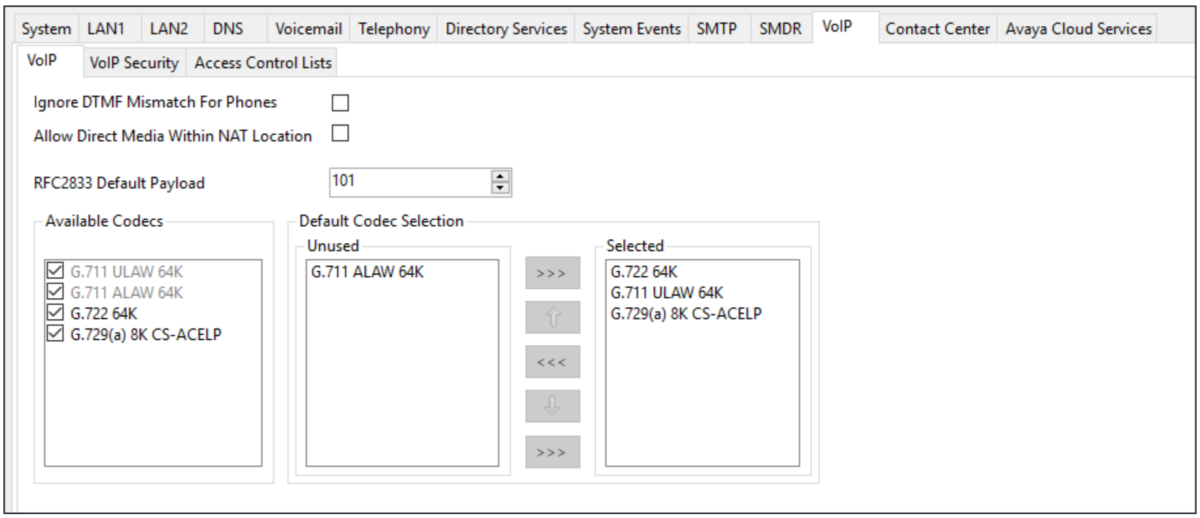
5.3.2. System Telephony Settings

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. In the reference configuration, the **Inhibit Off-Switch Forward/Transfer** box is unchecked so that call forwarding and call transfer to PSTN destinations via the Verizon Business IP Trunk service can be tested. That is, a call can arrive to IP Office via the Verizon IP Contact Center service and be forwarded or transferred back to the PSTN with the outbound leg of the call using the Verizon IP Trunk service. 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.

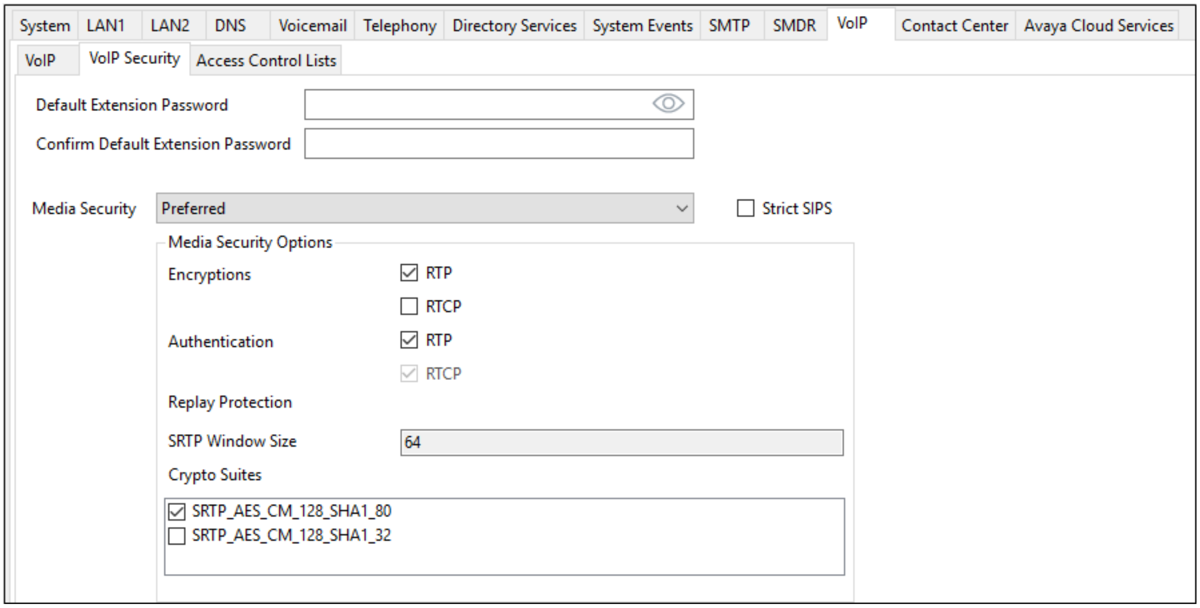


5.3.3. System VoIP Settings

To view or change system codec settings, select the **VoIP → VoIP** tab. The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. During the compliance test, this was set to **101**, the value preferred by Verizon Business. For codec selection, on the left, observe the list of **Available Codecs**. In the example screen below, which is not intended to be prescriptive, the parameter next to each codec is checked, making all the codecs available in other screens where codec configuration may be performed (such as the SIP Line in **Section 5.5.5**). The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis, using the up, down, left, and right arrows. By default, all IP (SIP and H.323) lines and extensions will assume the system default codec selection, unless configured otherwise for the specific line or extension.

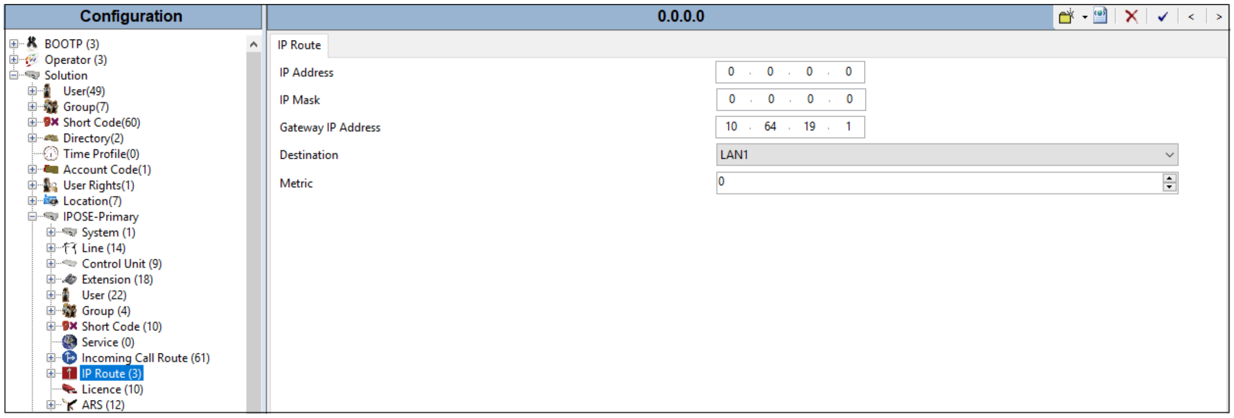


During the compliance test, SRTP was used internal to the enterprise wherever possible. To view or configure the media encryption settings, select the **VoIP → VoIP Security** tab on the Details pane. The **Media Security** drop-down menu is set to **Preferred** to have IP Office attempt use encrypted 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. The Avaya SBCE 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 screens for the SIP Line in IP Office Release 11.1. 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 IP Office Manager to create a SIP Line. Follow the steps in **Section 5.5.1** to create the SIP Line from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.5.2 – 5.5.6**.

In addition, the following SIP Line settings are not supported on Basic Edition:

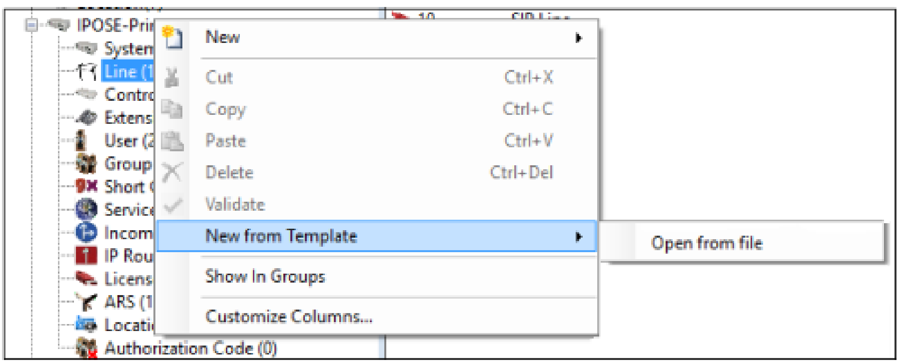
- SIP Line – Originator number for forwarded and twinning calls.
- Transport – Second Explicit DNS Server.
- SIP Credentials – Registration Requirement.
- SIP Advanced Engineering.

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 **Sections 5.5.2 – 5.5.6**.

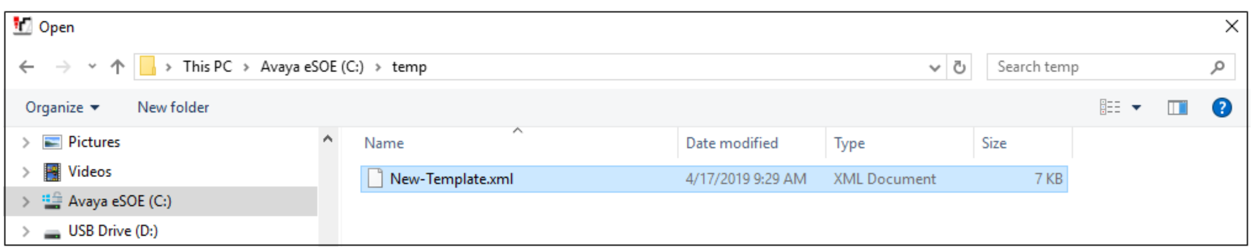
5.5.1. Importing a SIP Line Template

Note – DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500v2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

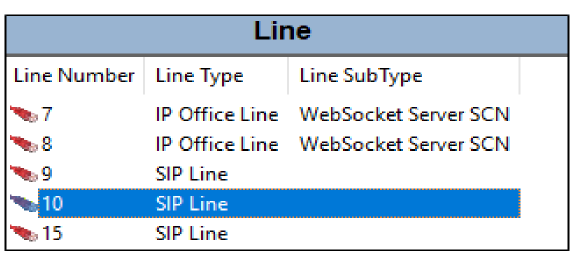
Copy a previously created template file to the computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New →New from Template**. Select **Open from file.**



Navigate to the directory where the template was copied on the local computer (e.g., *\temp*) and select it. Click **Open** (not shown).



The new SIP Line is created, and it will appear on the **Navigation** pane (e.g., SIP Line **10**). The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.5.2** to **5.5.6**.



Line

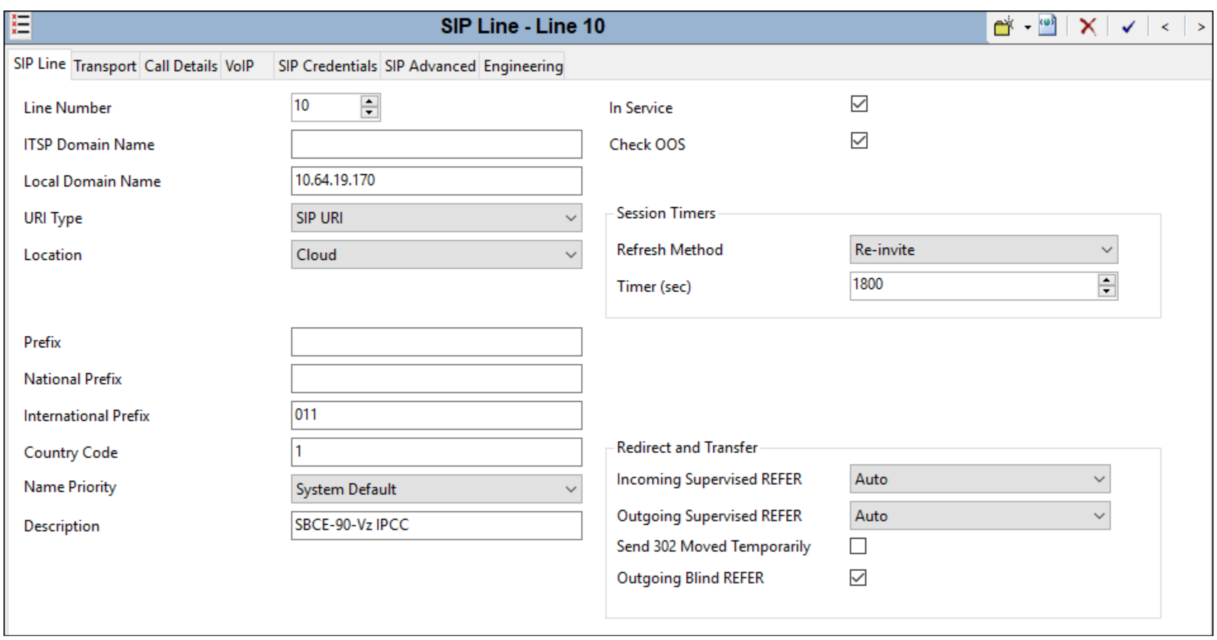
Line Number	Line Type	Line SubType
7	IP Office Line	WebSocket Server SCN
8	IP Office Line	WebSocket Server SCN
9	SIP Line	
10	SIP Line	
15	SIP Line	

5.5.2. SIP Line – SIP Line Tab

The **SIP Line** tab in the Details pane is shown below for Line Number 10, used for Avaya SBCE to the Verizon Business IPCC service. The **ITSP Domain Name** is left blank. Local Domain Name is set to the IP address of the Avaya IP Office LAN1 interface (e.g., **10.64.19.170**). By default, the **In Service** and **Check OOS** boxes are checked. With these settings, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.

In the reference configuration, the IP Office **Country Code** is set to **1**. The From and PAI headers received from Verizon for calls from U.S. PSTN numbers contain "+1" before the calling PSTN number. By configuring the IP Office **Country Code** to 1, the caller ID display presented to IP Office users will be the PSTN number without any codes or prefixes. For example, a call from 3035387006 would display 3035387006. If the **Country Code** does not match the value following the "+" from Verizon, the IP Office user display would show the contents of the **International Prefix** field, followed by the value following the "+", followed by the PSTN number. For example, if the Country Code parameter were left blank, the IP Office user would see a display such as "01113035387006". Aside from display implications, if the **Country Code** is not configured, other patterns may also fail to match as expected, such as a match on the **Incoming CLI** field of the Incoming Call Route. See **Section 5.9.3** for configuration of incoming call routing based on the calling number.

Under **Session Timers**, the **Refresh Method** is set to **Re-invite** and the **Timer (seconds)** is set to **1800**. With this configuration, IP Office will send re-INVITEs every 15 minutes (half of the set value) to keep the active session alive.

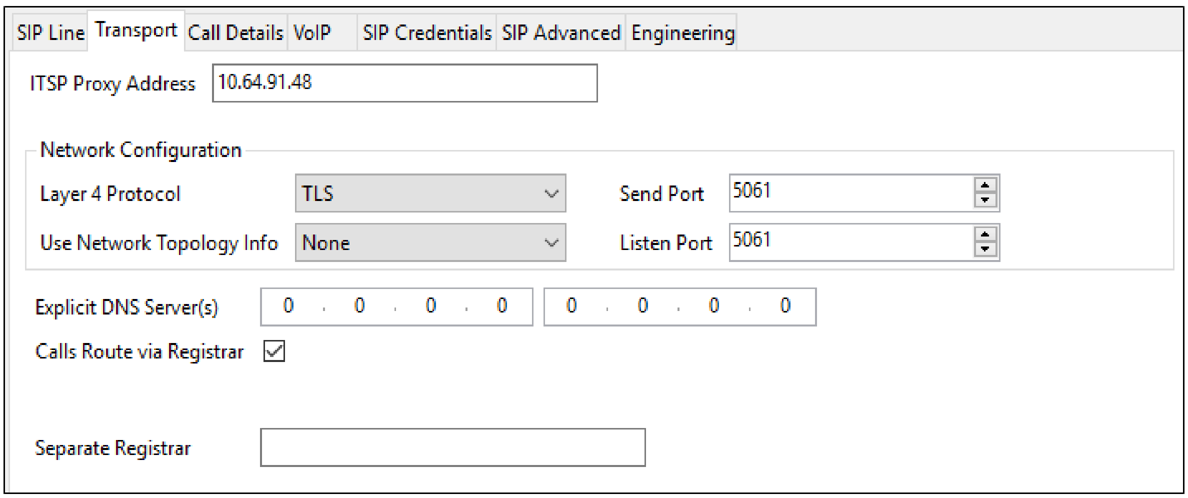


Under **Redirect and Transfer**, the default automatic determination of **Incoming Supervised REFER** and **Outgoing Supervised REFER** is **Auto**. A supervised transfer occurs when a consultation call is made and the REFER contains a Replaces header. The Verizon Business

IPCC service does not support supervised REFER, and with this setting, IP Office will not use REFER for supervised transfers. The **Send 302 Moved Temporarily** setting is unchecked, as Verizon does not support receiving a 302 Moved Temporarily message. The **Outgoing Blind REFER** box can be optionally checked to enable use of REFER for blind transfers. In the reference configuration, this parameter is checked. See **Section 2.2** for limitations.

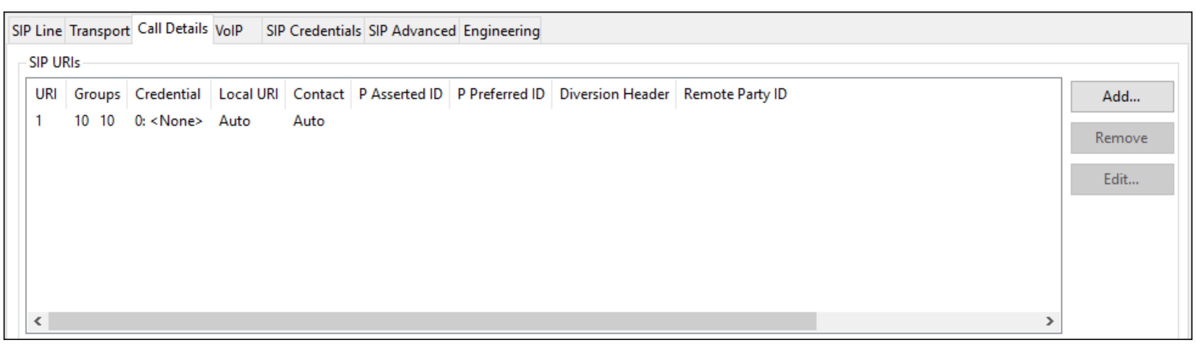
5.5.3. SIP Line – Transport Tab

Select the **Transport** tab. The **ITSP Proxy Address** is set to the inside IP address of the Avaya SBCE 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**.



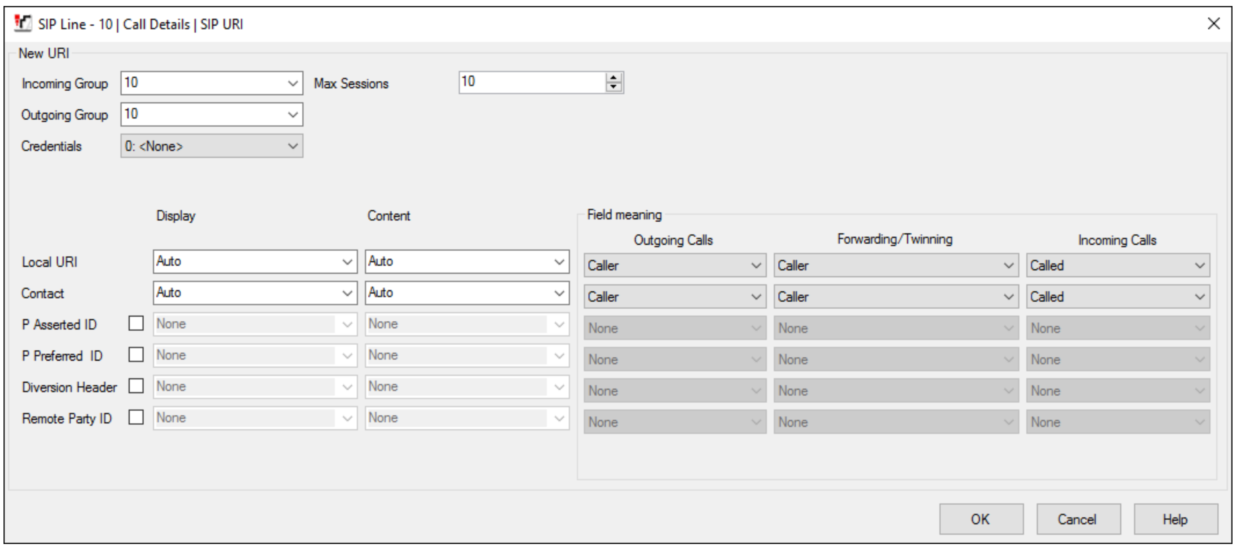
5.5.4. SIP Line – Call Details Tab

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.



In the example screen below, a previously configured entry is edited. The **Incoming Group** parameter, set here to **10**, will be referenced when configuring Incoming Call Routes to map inbound SIP trunk calls to IP Office destinations in **Section 5.9**. The **Outgoing Group** parameter, also set to **10**, is relevant when using the SIP REFER method to transfer an inbound toll-free call back out the Verizon Business IPCC service. 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.

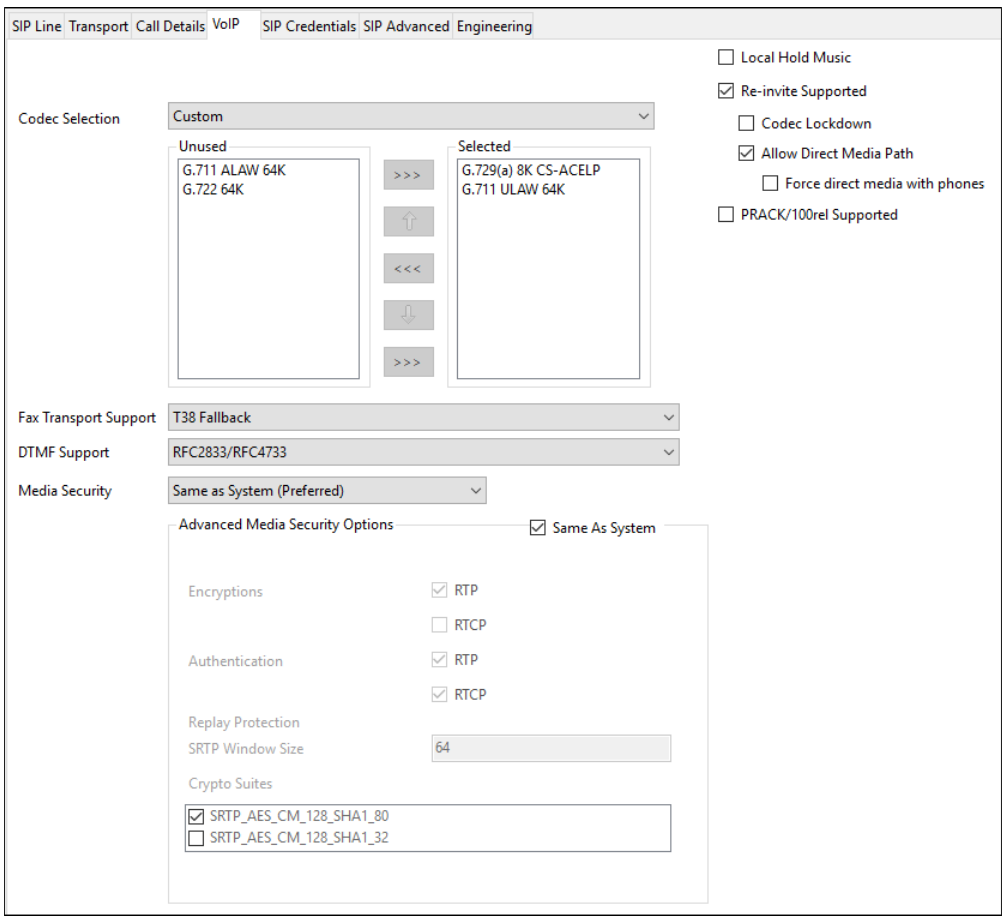
Auto is selected for the **Local URI** and **Contact** parameters. With this configuration, information in the Incoming Call Route (**Section 5.9**) is used to determine what call is accepted on the SIP Line. Set the **Field meaning** section to the values shown in the screenshot below.



5.5.5. SIP Line – VoIP Tab

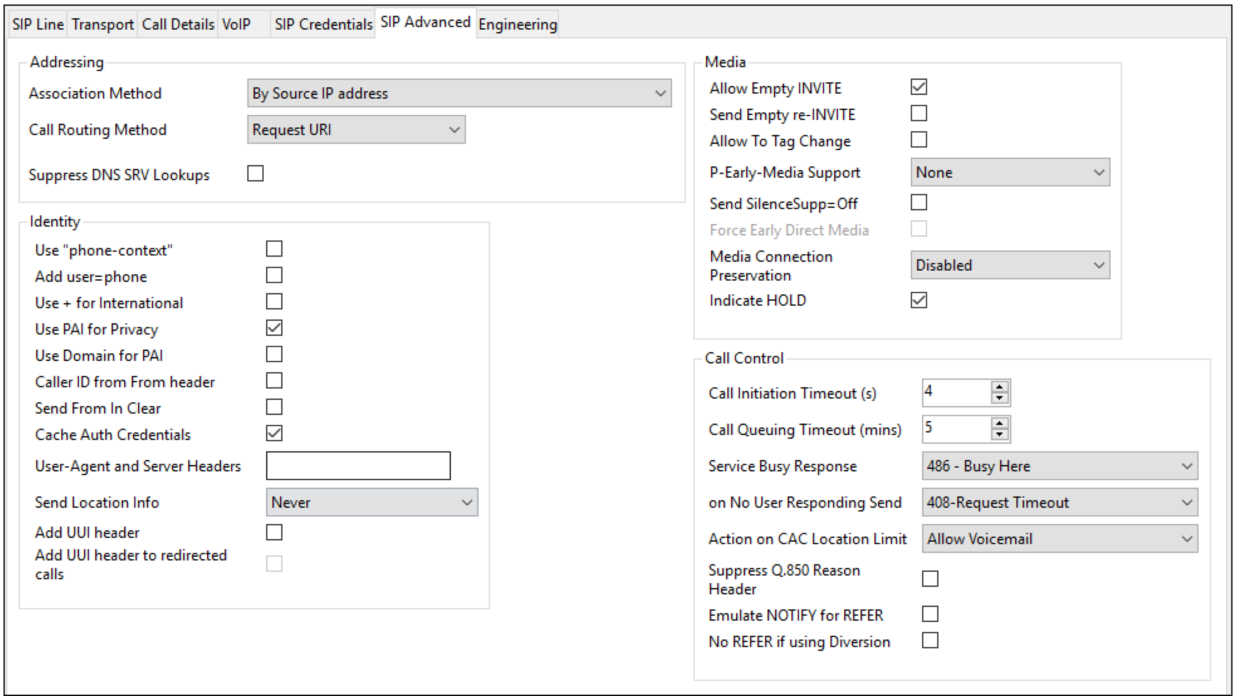
Select the **VoIP** tab. The **Codec Selection** drop-down parameter **System Default** (default) will match the codecs set in the system wide Default Selection list (**System → Codecs**). In the reference configuration, **Custom** is selected and the codecs **G729(a) 8K CS-ACELP** and **G.711 ULAW 64K** preferred by Verizon are specified. This will cause IP Office to include G.729a and G.711MU in the Session Description Protocol (SDP) offer, in that order. The **Fax Transport Support** drop-down is set to **T38 Fallback**. This enables T.38 to be used if supported, and fall back to G.711 if not. The **DTMF Support** parameter can remain set to the default value **RFC2833/RFC4733**. The **Media Security** drop-down menu is set to **Same as System (Preferred)** to have IP Office use the system setting for media security set in **Section 5.3.3** to encrypted RTP toward Avaya SBCE. The **Re-invite Supported** parameter is checked to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk. The **Allow Direct Media Path** parameter can be checked to allow for direct media between IP endpoints and the internal interface of the Avaya SBCE, if possible within the network infrastructure, freeing up DSP resources on the Primary server.

For PSTN originations, Verizon preferred the G.729a codec in the SDP, while also allowing the G.711MU codec. During testing, the IP Office configuration was varied such that G.711MU was the preferred or only codec listed, and G.711MU calls were also successfully verified.



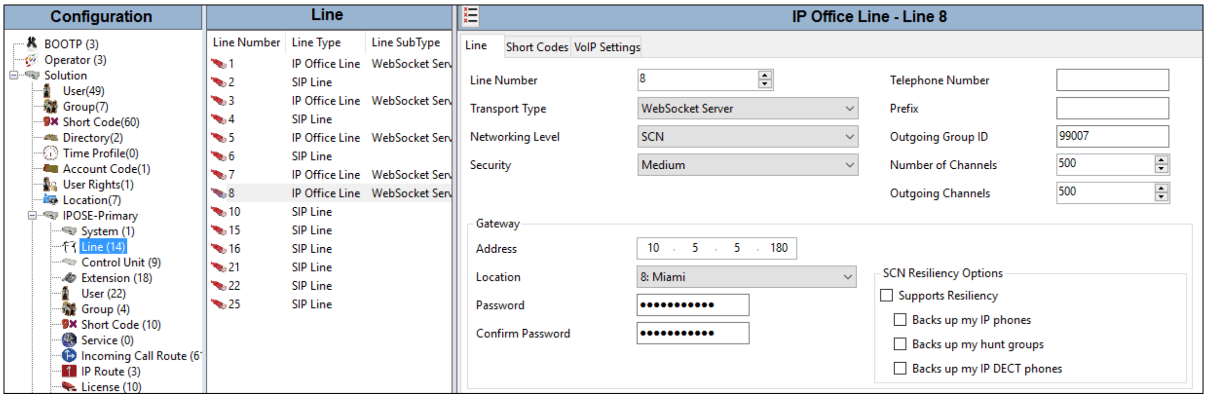
5.5.6. SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab. In the **Media** area, the **Allow Empty INVITE** box is checked to allow IP Office to be the recipient of a Verizon Business IPCC enhanced transfer where the initial INVITE may not have SDP information. The **Indicate HOLD** box is checked to have IP Office signal to Verizon when a call is placed on/off hold. Other parameters may be left at default values.

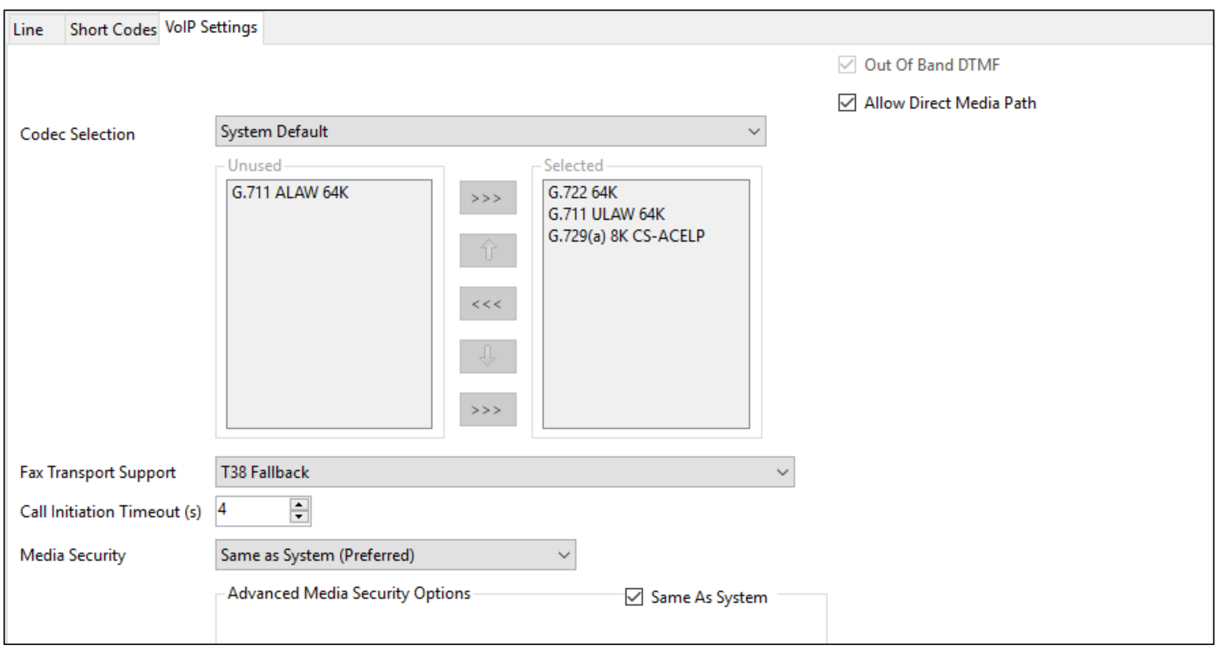


5.6. IP Office Line

In IP Office Server Edition systems, IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate line to be configured in the Group pane. The screen below shows the IP Office Line to the IP500 V2 Expansion System.



The screen below shows the IP Office Line, **VoIP Settings** tab. In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. **Fax Transport Support** is set to **T.38 Fallback**. The **Media Security** is set to **Same as System (Preferred)** to have IP Office use the system setting for media security set in **Section 5.3.3** to encrypted RTP. Default values were used for all other parameters.

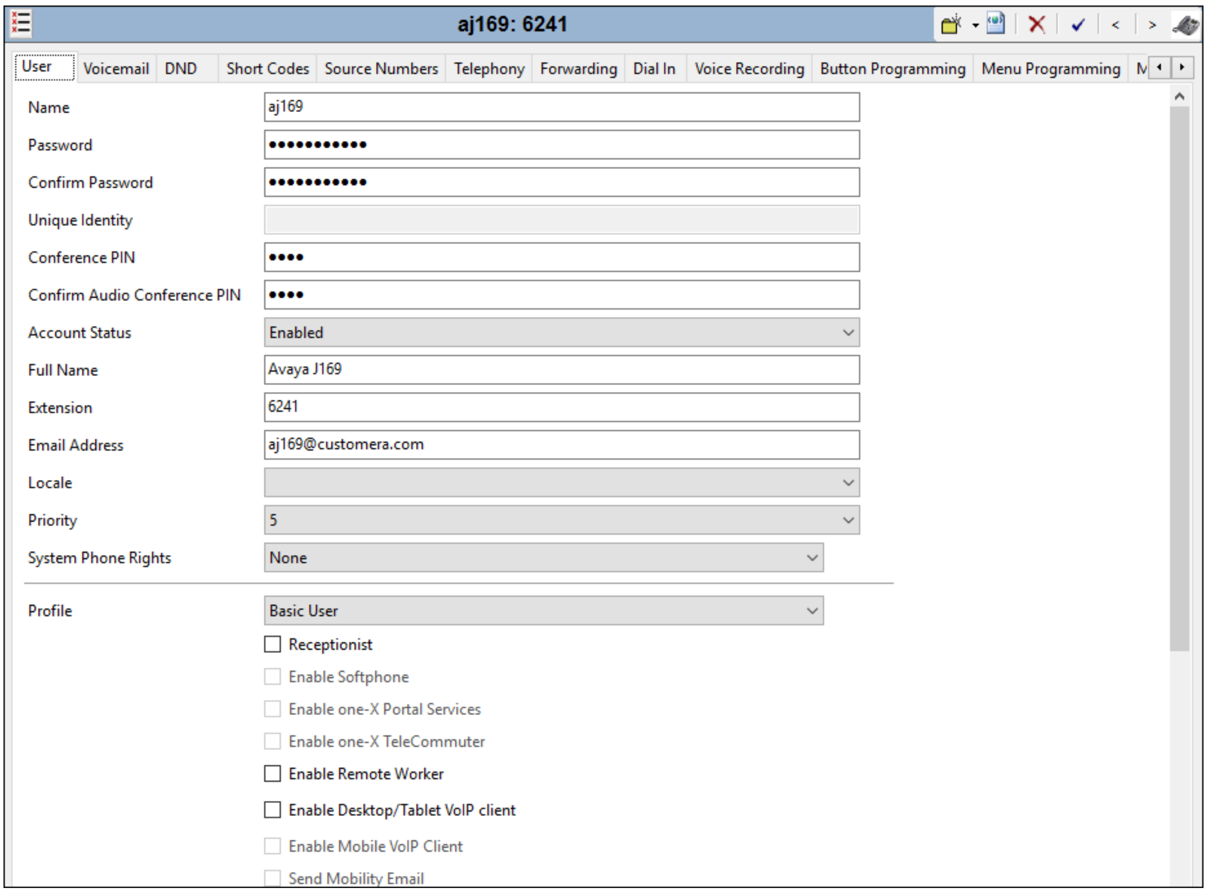


5.7. Users, Extensions, and Hunt Groups

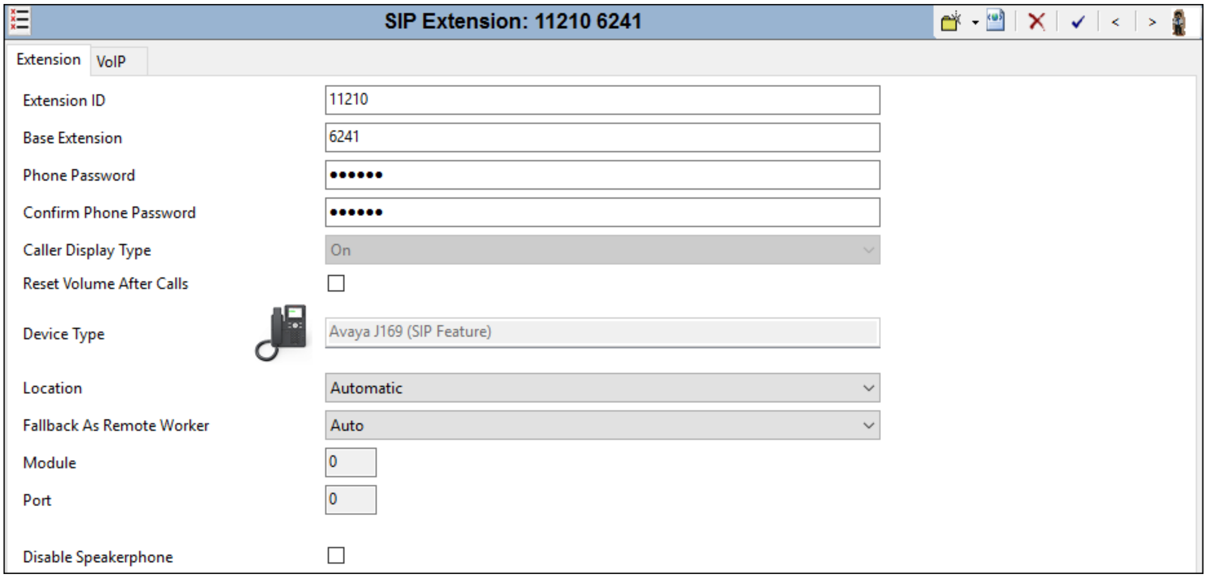
In this section, examples of IP Office Users, Extensions, and Hunt Groups will be illustrated. In the interests of brevity, not all users and extensions shown in **Figure 1** will be presented, since the configuration can be easily extrapolated to other users. To add a User, right click on **User** in the Navigation pane, and select **New**. To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured in the Group pane.

5.7.1. SIP User 6241

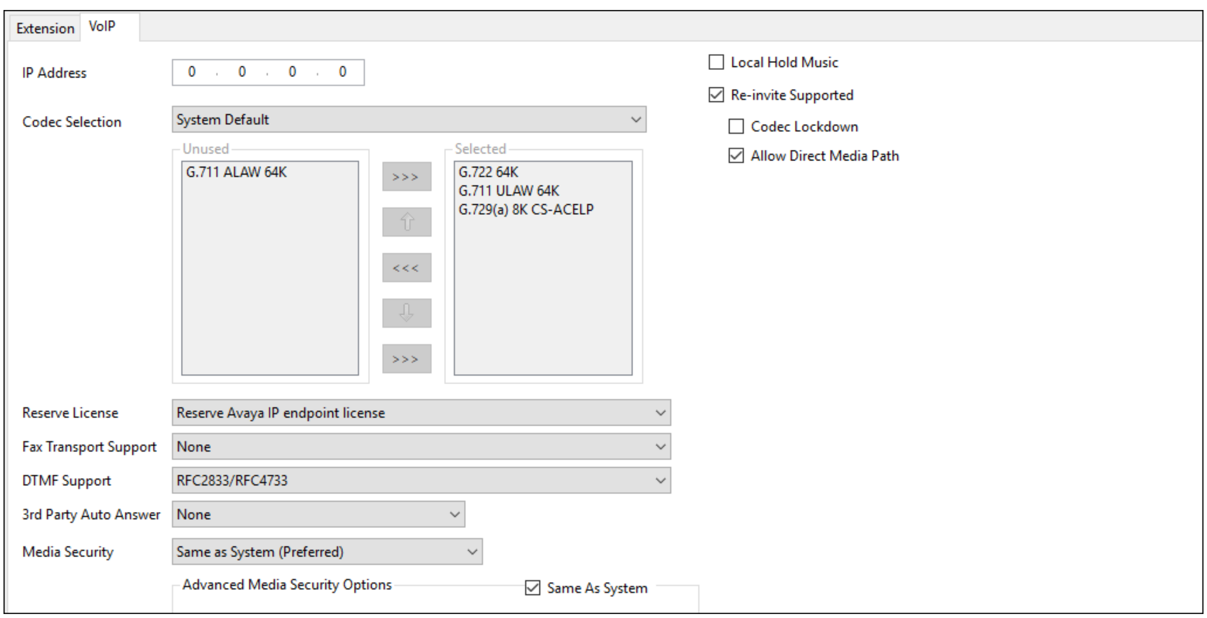
The following screen shows the **User** tab for user 6241. This user corresponds to an Avaya J169 SIP endpoint.



The following screen shows the Extension information for this user. To view, select **Extension** from the Navigation pane, and the appropriate extension from the Group pane.



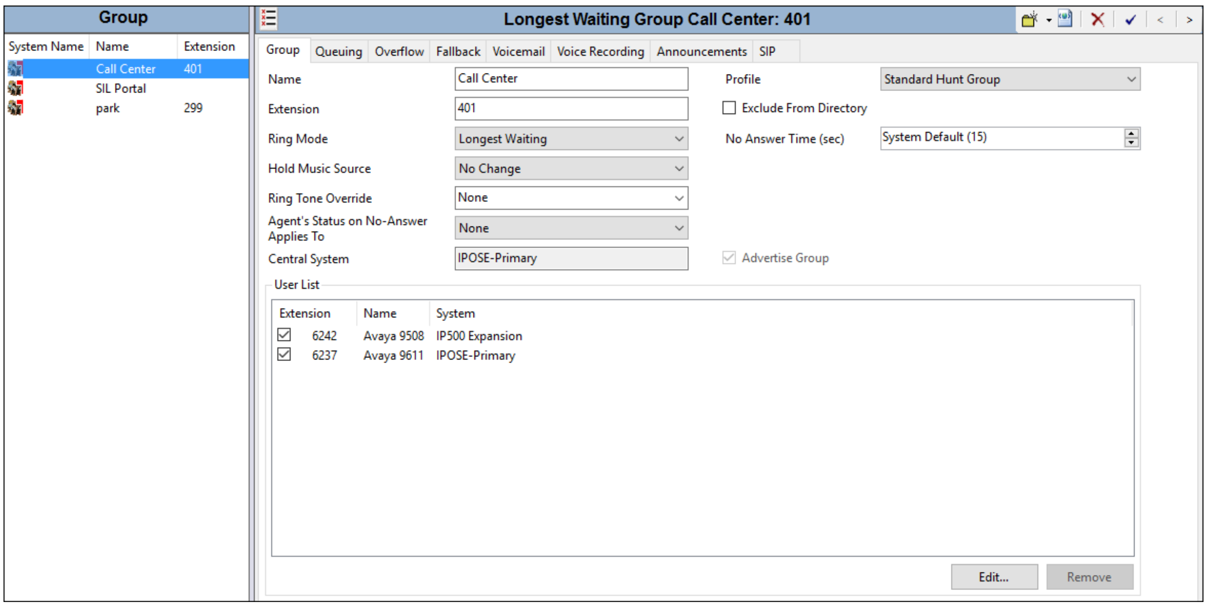
The following screen shows the **VoIP** tab for the extension. The **IP Address** field may be left blank. Check the **Reserve Avaya IP endpoint license** box. The **Codec Selection** parameter may retain the default setting **System Default** to follow the system configuration shown in **Section 5.3.3**. The Media Security parameter may also retain the default setting **Same as System (Preferred)** to follow the system configuring shown in **Section 5.3.3**.



5.7.2. Hunt Groups

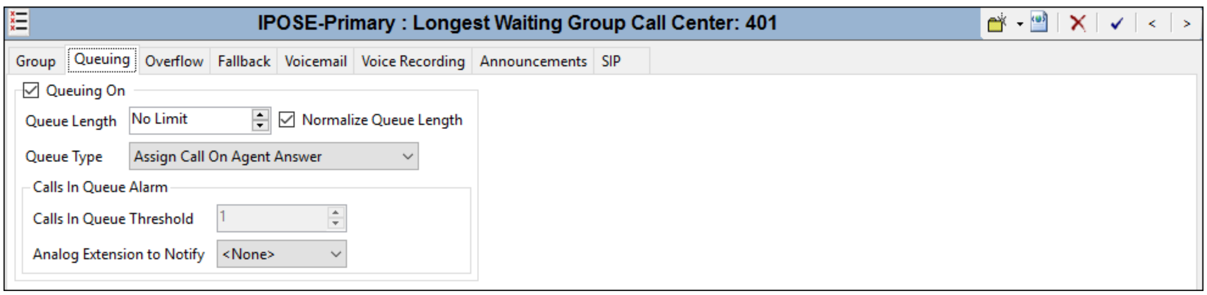
During the verification of these Application Notes, users could also receive incoming calls as members of a hunt group. To configure a new hunt group, right-click **Group** (not shown) from the Navigation pane and select **New**. To view or edit an existing hunt group, select **Group** from the Navigation 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 telephones from **Figure 1**. The **Ring Mode** was set to **Longest Waiting** (i.e., "longest waiting", most idle user receives next call). Click the **Edit** button to change the **User List**.

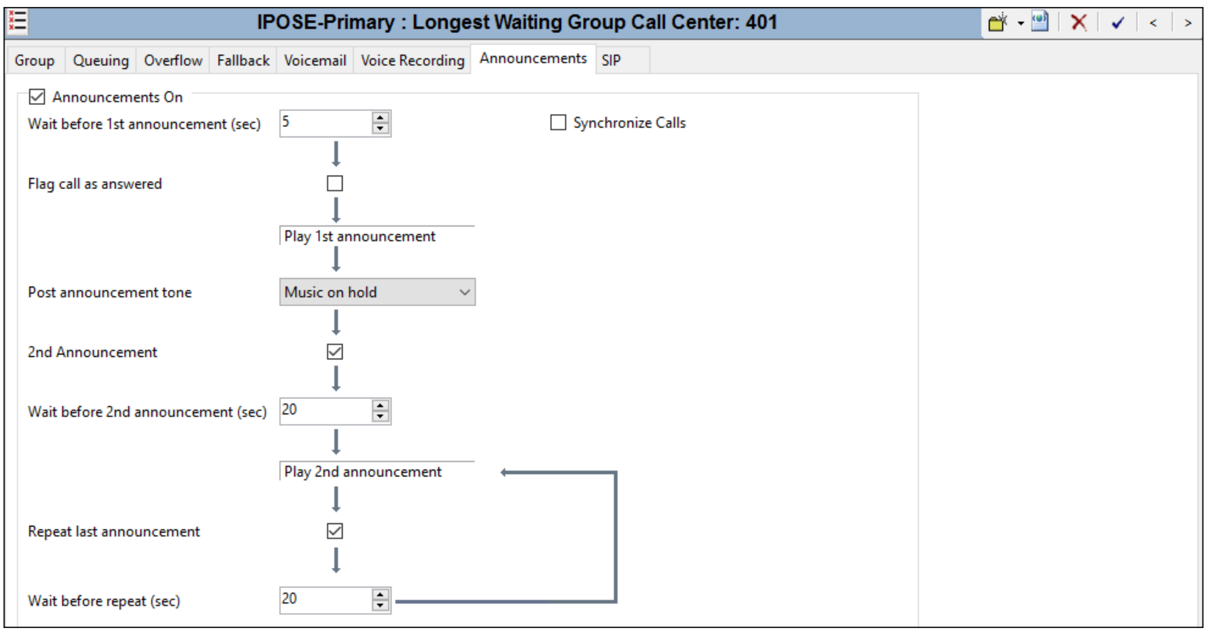


The following screen shows the **Queuing** tab for hunt group 401. In the reference configuration, the hunt group was configured to allow queuing so that incoming Verizon toll-free calls could be queued when all the members of the hunt group were busy on calls. In the testing associated with these Application Notes, the **Queue Length** was varied using both "No Limit" and specifically sized queues. For example, if the **Queue Length** is configured to 2, and if two calls are already in queue, a third call to the Verizon toll-free number corresponding to this hunt group will get busy tone because IP Office will send a 486 Busy Here (i.e., if there is no Voicemail for the hunt group). As another example, if the **Queue Length** has a fixed limit of 2, and if two calls are already in queue, a third call to the Verizon toll-free number destined for this hunt group from a priority caller (see **Section 5.9.3**) will be queued ahead of non-priority callers, temporarily expanding the queue.

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 5.9.3**.



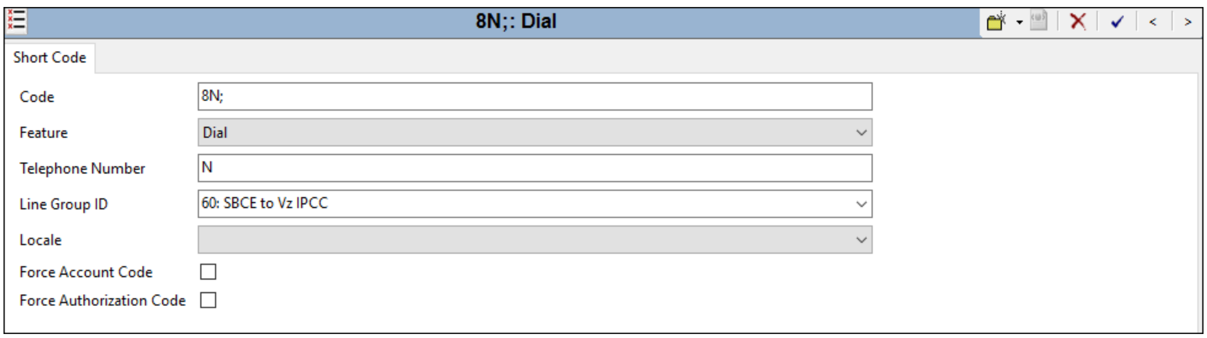
The following screen shows the **Announcements** tab for hunt group 401. In the reference configuration, when a call arrives, when all members of the hunt group are busy on calls, the caller will first hear ring back tone. If a member of the hunt group does not become available after 10 seconds, the call will be answered by IP Office (i.e., 200 OK will be sent to Verizon), and the toll-free 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 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.



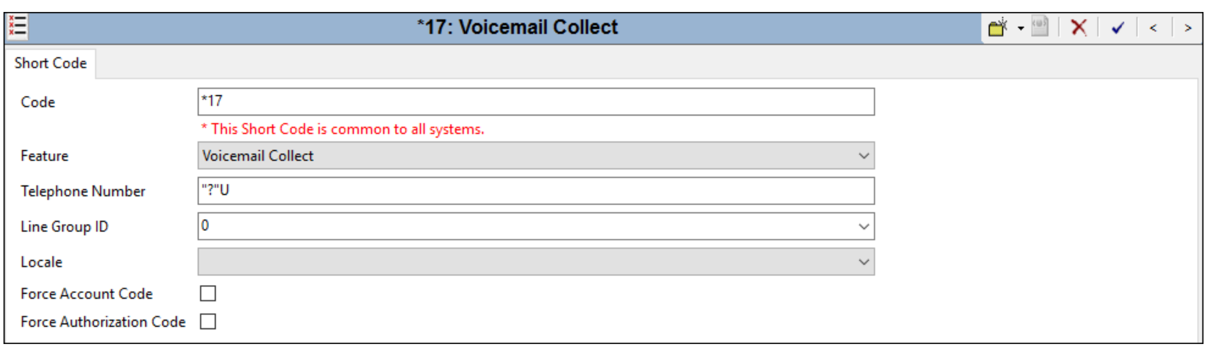
5.8. Short Codes

In this section, various examples of IP Office short codes will be illustrated. 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.

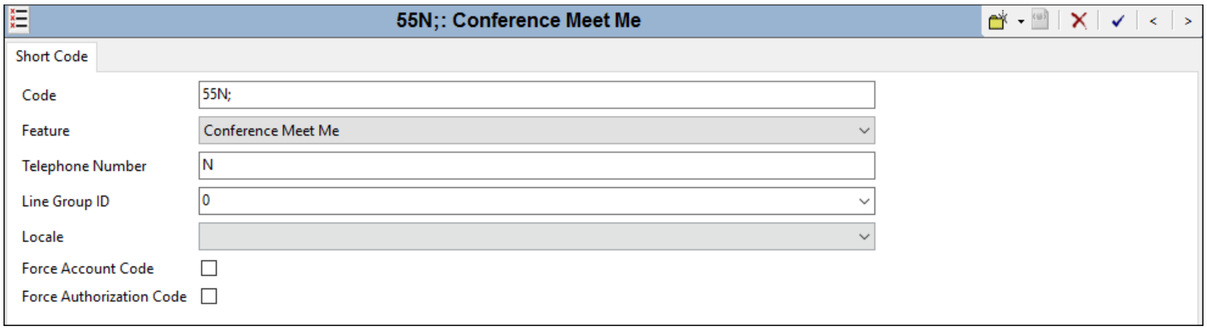
Verizon Business IPCC service allows for blind transfers out their service using the SIP REFER Method. In the screen shown below, the short code **8N** is illustrated. The **Code** parameter is set to **8N**. The **Feature** parameter is set to **Dial**. The **Telephone Number** parameter is set to **N**. The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message. The **Line Group ID** parameter is set to **60: SBCE to Vz IPCC**, configurable via ARS. See **Section 5.11** for example ARS route configuration for "60: SBCE to Vz IPCC".



The following screen illustrates a short code that acts like a feature access code rather than a means to access a SIP Line. In this case, the **Code** "***17**" is defined for **Feature** "**Voicemail Collect**". This short code will be used as one means to allow a Verizon toll-free number to be programmed to route directly to voice messaging, via inclusion of this short code as the destination of an Incoming Call Route. See **Section 5.9** for configuration of Incoming Call Routes.



The following screen illustrates another short code. In this case, the **Code** "**55N;**" is defined for **Feature** "**Conference Meet Me**". The **Telephone Number** parameter is set to **N**. In the verification of these Application Notes, this short code was used in conjunction with a Voicemail Pro module named "MeetMeConf". Although the Voicemail Pro configuration is beyond the scope of these Application Notes, the module enabled a PSTN caller to dial a Verizon toll-free number, be prompted to enter a conference ID and PIN by Voicemail Pro, and then be transferred to the appropriate meet-me conference based on the ID entered by the caller. Local IP Office callers could also dial 556xxx to join the corresponding conference ID.

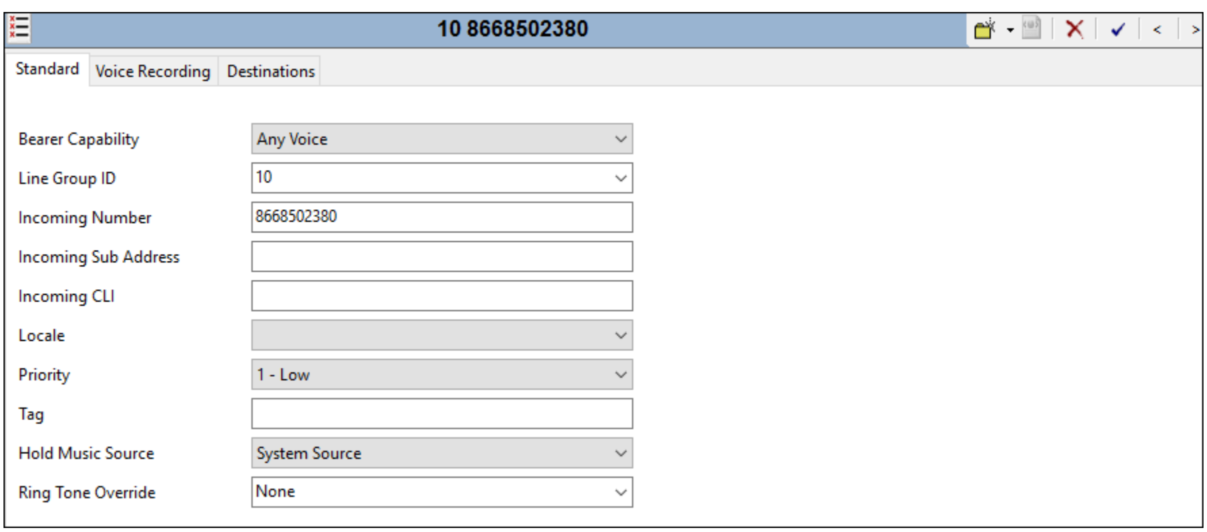


5.9. Incoming Call Routes

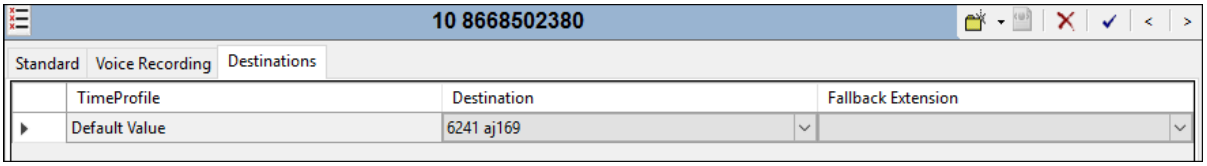
In this section, IP Office Incoming Call Routes are illustrated. Each Incoming Call Route will map a Verizon Business toll-free number to a destination user, group, or function on IP Office. In some cases, the destination will be chosen based on the combination of the toll-free number and the caller id of the caller. 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.

5.9.1. Incoming Call Route to a Specific Telephone Extension

In the screen shown below, the incoming call route for **Incoming Number 8668502380** is illustrated. The **Line Group Id** is **10**, matching the **Incoming Group** field configured in the **Call Details** tab for the SIP Line to the Verizon Business IPCC service, in **Section 5.5.4**.



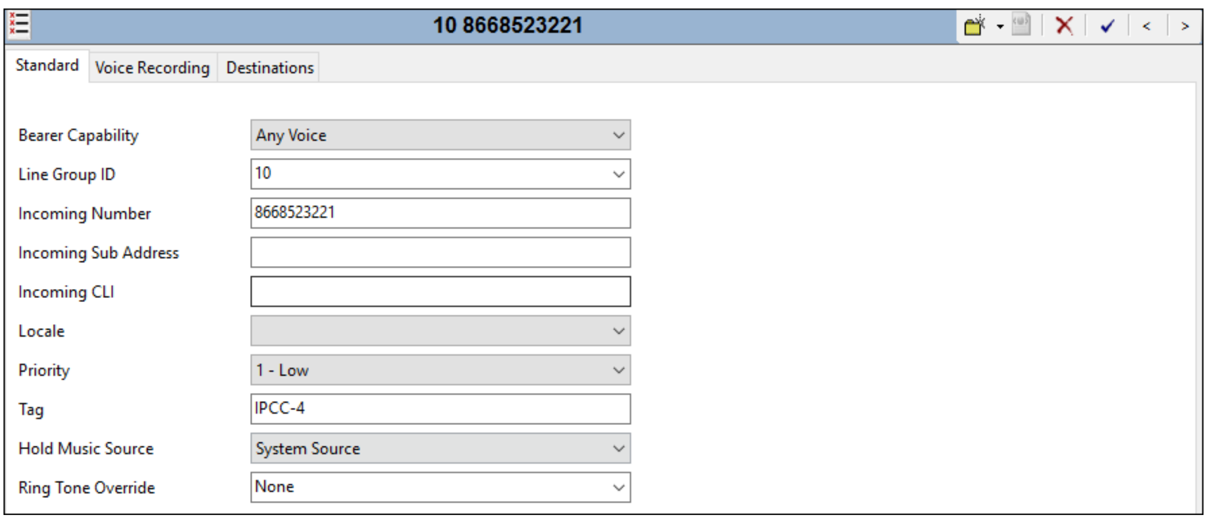
Select the **Destinations** tab. From the **Destination** drop-down, select an extension to receive the call when a PSTN user dials 8668502380. This number is associated with IP Office user extension 6241. (The **Destination** was changed in the course of testing to associate different destinations with the toll-free numbers.)



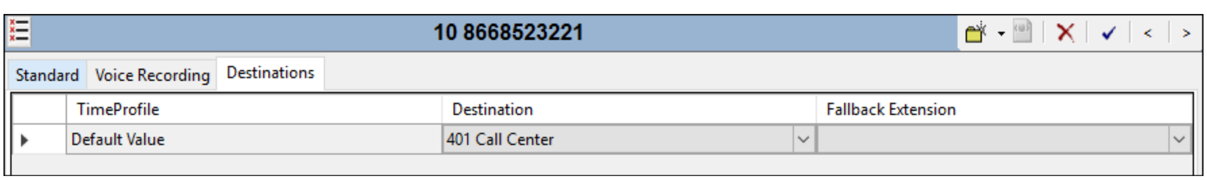
Incoming Call Routes for other direct mappings of toll-free numbers to IP Office users are not presented here but are configured in the same fashion.

5.9.2. Incoming Call Routes to a Hunt Group by Dialed Toll-Free Number

In the screen shown below, an incoming call route for **Incoming Number 8668523221** is illustrated. The **Line Group Id** is **10**, matching the Incoming Group field configured in the Call Details tab for the SIP Line to Verizon Business in **Section 5.5.4** Optionally, the **Tag** parameter can be populated with a descriptive name that will associate the call with this incoming call route.



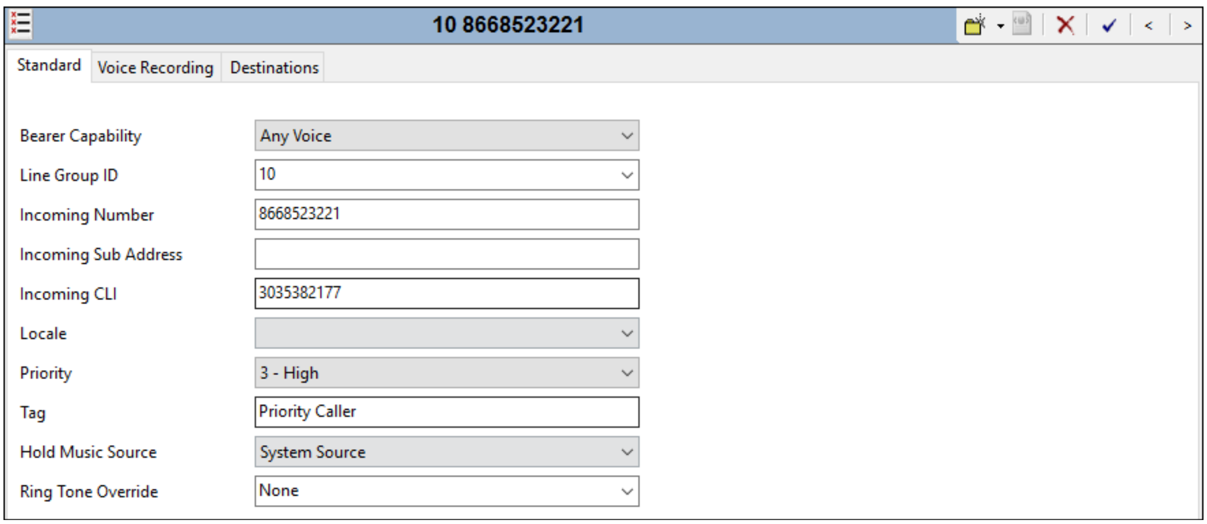
Select the **Destinations** tab. From the **Destination** drop-down, select the destination to receive the call when an arbitrary PSTN user dials 8668523221. This toll-free number is associated with IP Office hunt group extension 401, the "Call Center" hunt group.



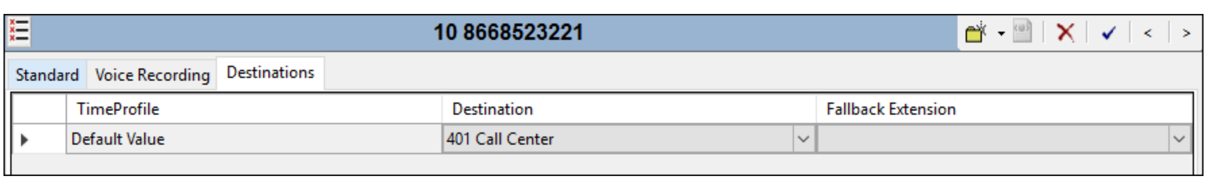
5.9.3. Incoming Call Routes Based on Calling Party Number

This section presents a simple example showing that IP Office can use the calling party number to distinguish call priority or call destination, for calls to the same toll-free number. Although the matching shown here is based on the full calling number, partial matching is also possible (e.g., to match a calling area code for a targeted geographic treatment).

In the screen shown below, the incoming call route for **Incoming Number 8668523221** and **Incoming CLI 3035382177** is illustrated. The **Line Group Id** is **10**, matching the Incoming Group field configured in the Call Details tab for the SIP Line to Verizon Business in **Section 5.5.4**. Note that the **Incoming Number** is the same as the toll-free number configured in the previous section. This route will be used for calls to the toll-free number specifically from a caller with caller ID "3035382177". In this case, to allow this caller to be treated with priority when calling in, the **Priority** field is set to **3 - High**. Optionally, the **Tag** parameter can be populated with a descriptive name that will associate the call with this incoming call route.

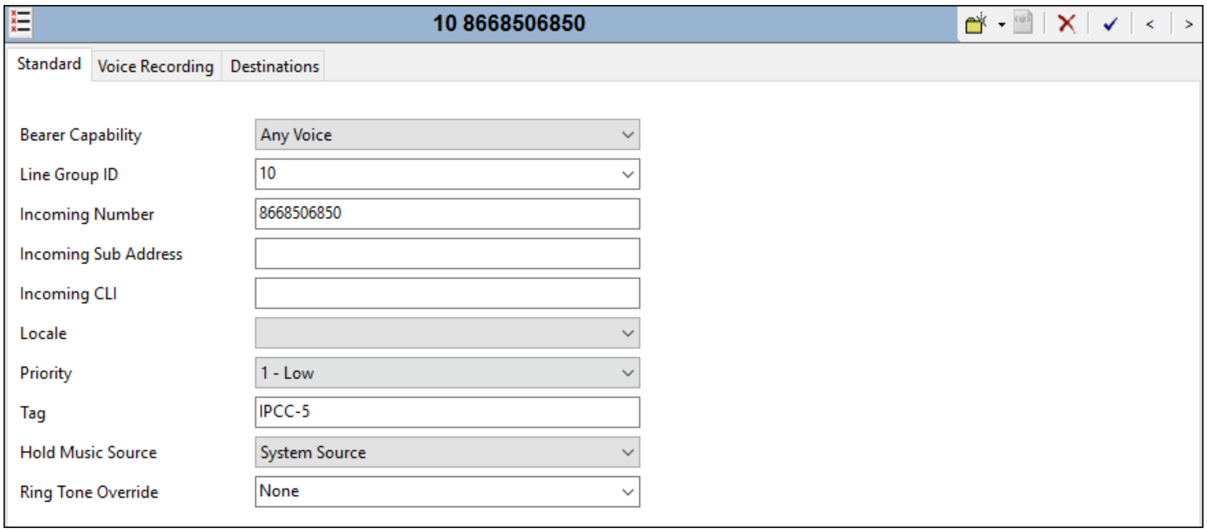


Select the **Destinations** tab. From the **Destination** drop-down, select the extension to receive the call when PSTN user 3035382177 dials 8668523221. In this case, the **Destination** is also the hunt group **401 Call Center**, but since high priority has been configured via the **Standard** tab, incoming calls from this caller will move to the front of the queue and be serviced before calls waiting in queue from other non-priority callers.



5.9.4. Incoming Call Routes to Various IP Office Features

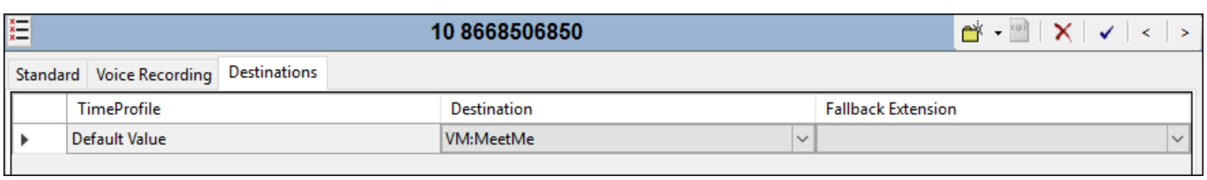
In the reference configuration, the incoming call route for **Incoming Number 8668506850** was varied to test different destination features, such as Voice Mail, Mobile Call Control, Refer Call Redirection, and Conference Bridge. The screen showing the **Standard** tab for this toll-free number is shown below.



When configuring an Incoming Call Route, the **Destination** field can be manually configured with a number such as a short code, or certain keywords available from the drop-down list. At different times during testing, the **Destinations** tab for 8668506850 was configured to contain the following destinations:

- ***17** (short code "Voicemail Collect", as shown in **Section 5.8**). With this destination, an incoming call to 8668506850 will be delivered directly to voice mail, allowing the caller to log-in to voice mail and access messages.
- **VM:MeetMe**. With this destination, an incoming call to 8668506850 will be delivered directly to the Voicemail Pro module "MeetMe" created for use as a conference bridge.
- **VM:Refer**. With this destination, an incoming call to 8668506850 will be delivered directly to the Voicemail Pro module "Refer" created for use as a Refer Call Redirection example. See **Section 5.10** for an illustration of this Voicemail Pro module.

An example screen showing the short code configured for a Voicemail Pro module is shown below.

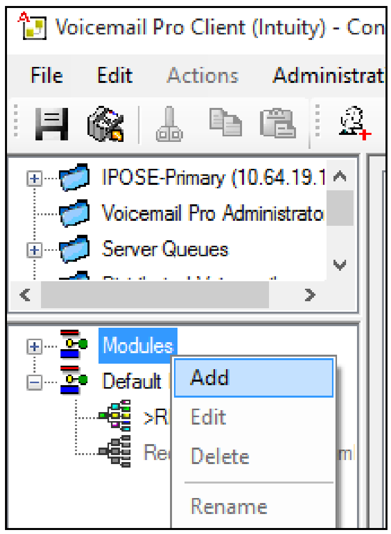


5.10. Voicemail Pro Refer Module

Note - While Avaya Voicemail Pro provisioning and programming is beyond the scope of this document, a sample module is described below.

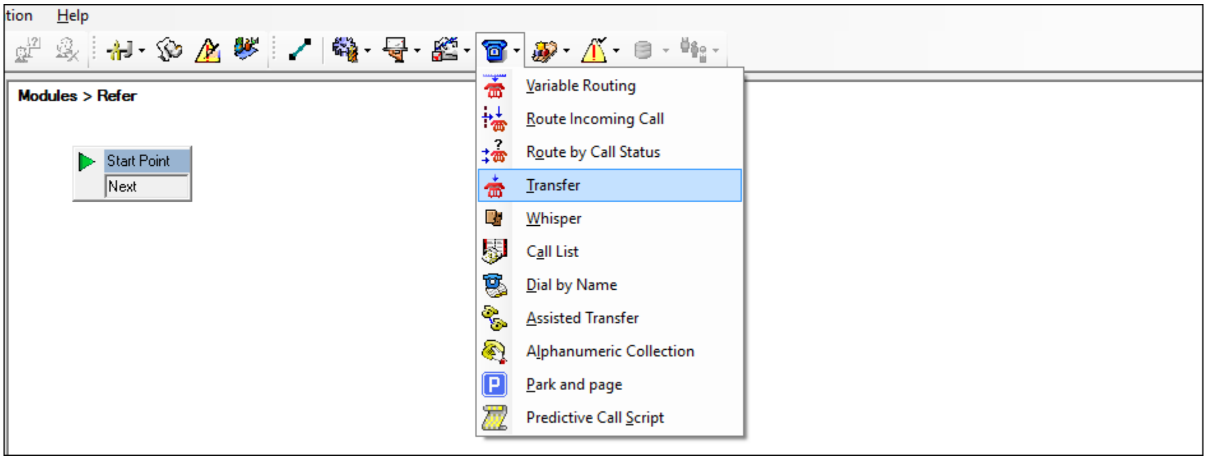
The Refer module is provisioned to play an announcement to the caller, and then generate a Refer (without Replaces) back to the Verizon Business IPCC service. This is accomplished via the Voicemail Pro Client interface.

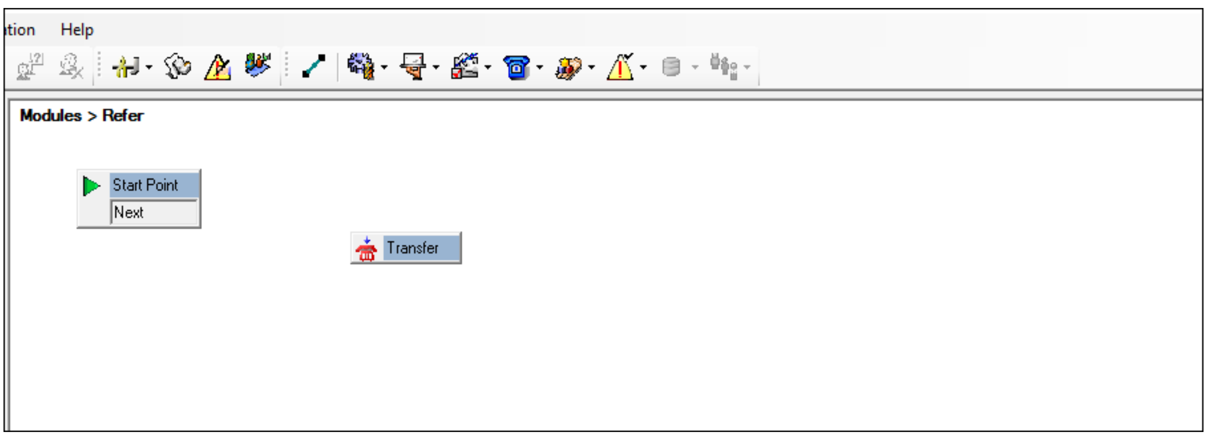
From the IP Office Manager PC, select **Start → All Apps → IP Office → Voicemail Pro Client** to launch the Voicemail Pro Client interface. Navigate to **File → Login**, select the proper Voicemail Pro system, and log in using the appropriate credentials (not shown). Create a **Start Point** by right clicking on **Modules** and selecting **Add**.



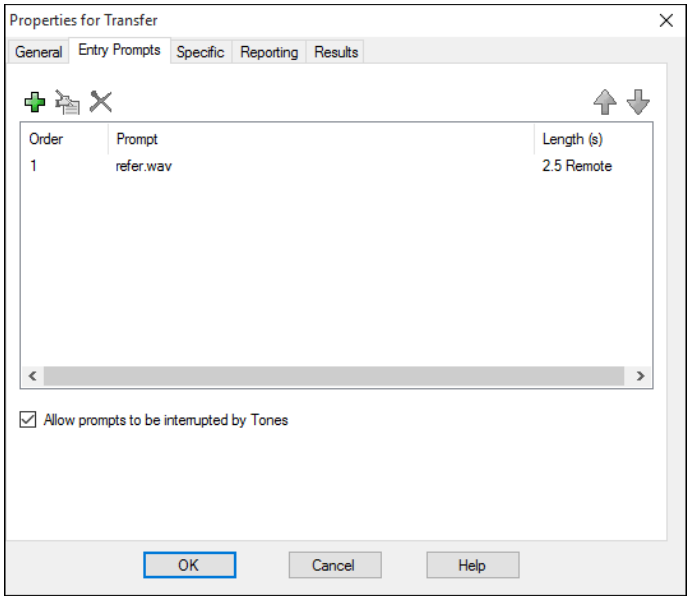
Enter a name (e.g., **Refer**) and click on **OK** (not shown). The new module "Refer" will appear, and a **Start Point** icon will appear in the work area.

Click on the **Telephony Actions** icon , select the **Transfer** icon , and click on the work area to place the **Transfer** icon in the work area.

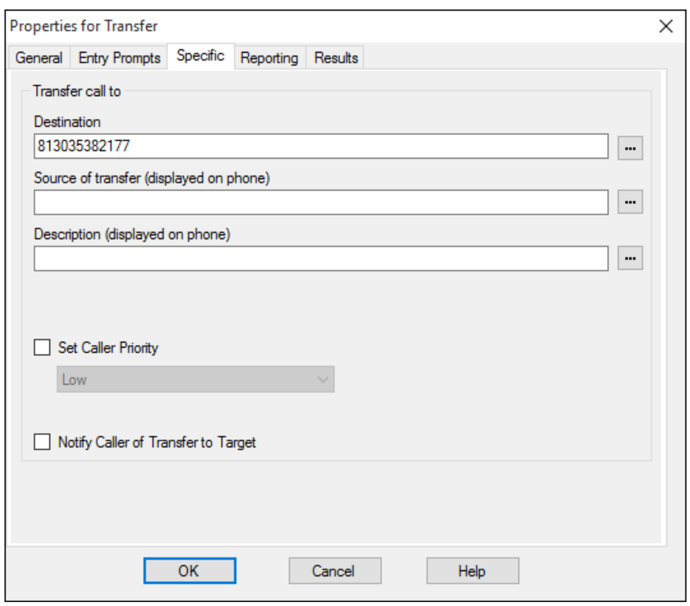




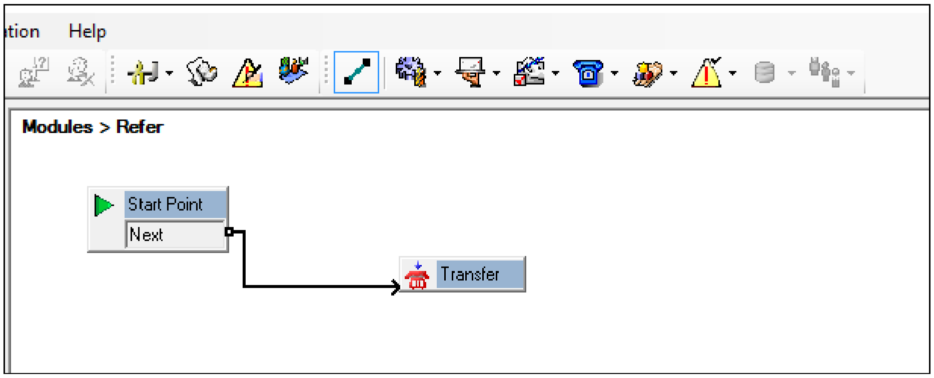
Double click on the **Transfer** icon, select the **Entry Prompts** tab and select or create an announcement to be played to the caller prior to the Refer (e.g., **refer.wav**). To modify an existing recording, double click on the .wav file and rerecord. If no .wav files exist, click on the  icon to open the .wav file editor.



On the **Specific** tab enter the destination, including the outbound Short Code (e.g., **813035382177**). Click on **OK**.



From the options bar, select the **Connector** icon and drag a connecting flow line from the **Start Point** box to the **Transfer** box.



From the top menu select **File → Save & Make Live** or select the icon.

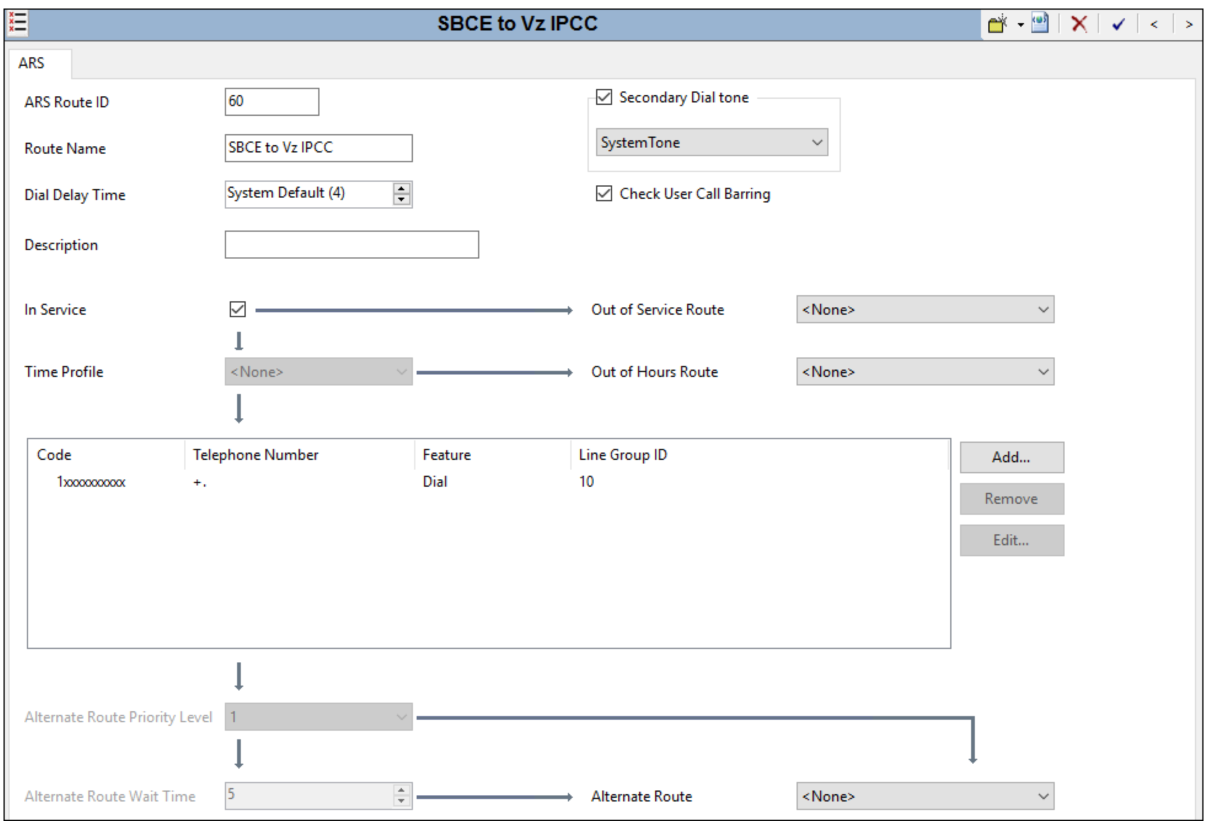
When the associated Verizon Business Toll-Free number is received, IP Office will send the call to Voicemail Pro (see **Section 5.9.4**). The caller will hear the announcement (e.g., **refer.wav**), and Voicemail Pro/Avaya IP Office will send a REFER back to the Verizon Business IPCC service, specifying "13035382177" in the Refer-To header. The Verizon Business IPCC service will then send a new Invite to the 1-303-538-2177 destination.

5.11. Alternate Route Selection (ARS)

Alternate Route Selection (ARS) is used to route outbound traffic to the SIP line. To define a new ARS route, right-click **ARS** in the Navigation pane and select **New**. In the Details pane that appears, a collection of matching patterns (similar to short codes) can be entered to route calls as shown below.

To add a new ARS route, right-click **ARS** in the Navigation pane, and select **New**. To view or edit an existing ARS route, select **ARS** in the Navigation pane, and select the appropriate route name in the Group pane.

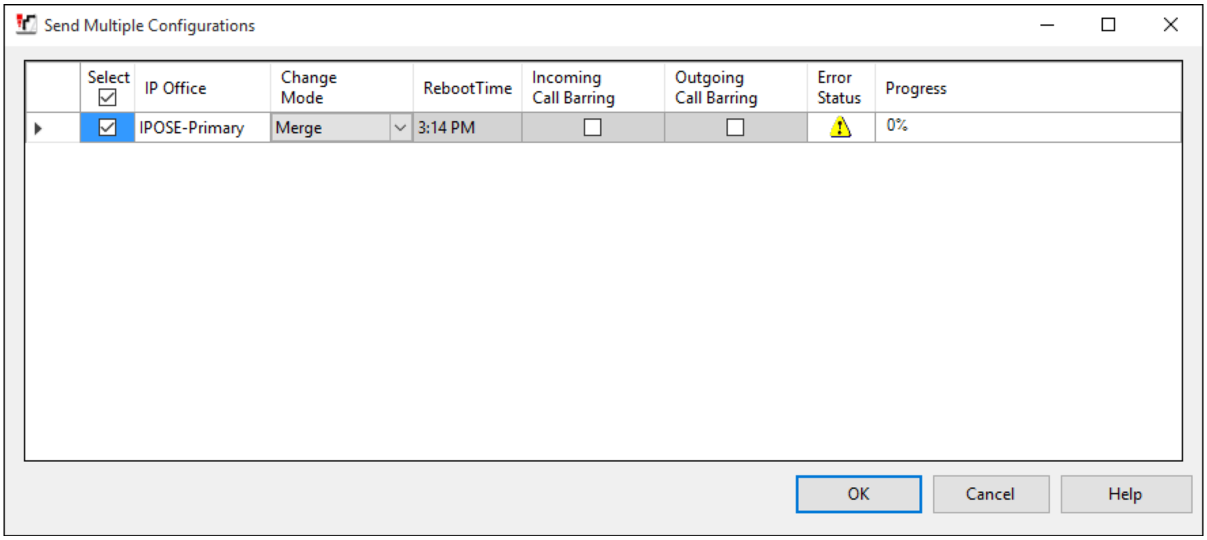
The following screen shows an example ARS configuration for the route named **SBCE to Vz IPCC**. Verizon Business IPCC service allows for blind transfers using the SIP REFER Method. The sequence of **X**s used in the **Code** column of the entries to specify the exact number of digits to be expected following the access code. The entry below shows that for calls to area codes in the North American Numbering Plan, the user dials 8, followed by 11 digits. The **Telephone Number** is set to "**+.**". This prepends a plus sign (+) to the beginning of the number dialed, denoting a global E.164 number. This is the format preferred by Verizon Business IPCC service for the destination number specified in the Refer-To header. The **Line Group ID** is set to **10** matching the number of the **Outgoing Group** configured on the **Call Details** tab of SIP Line 10 to Verizon Business (**Section 5.5.4**).



5.12. Save Configuration

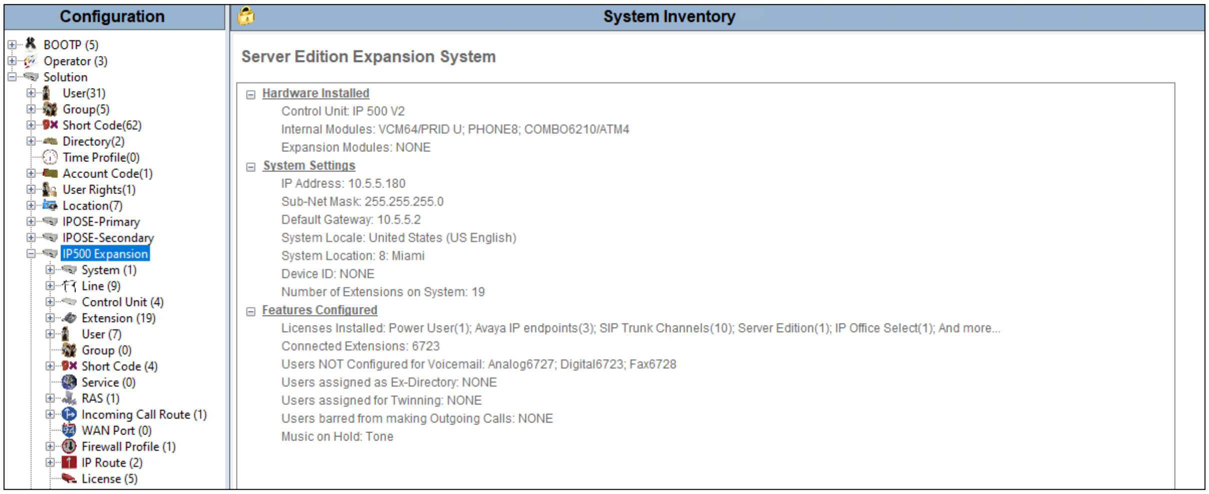
Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections.

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.



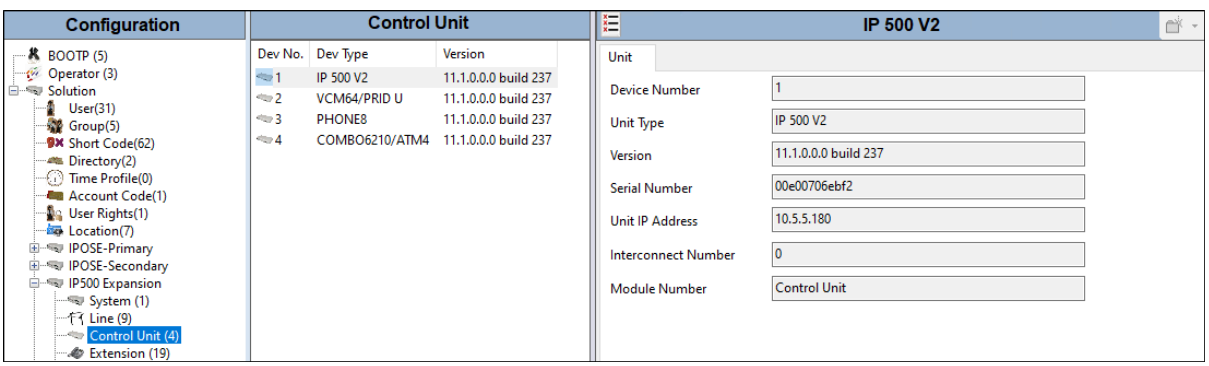
6. Avaya IP Office Expansion Configuration

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. Clicking the "plus" sign next to **IP500 Expansion** on the left navigation pane will expand the menu on this server.



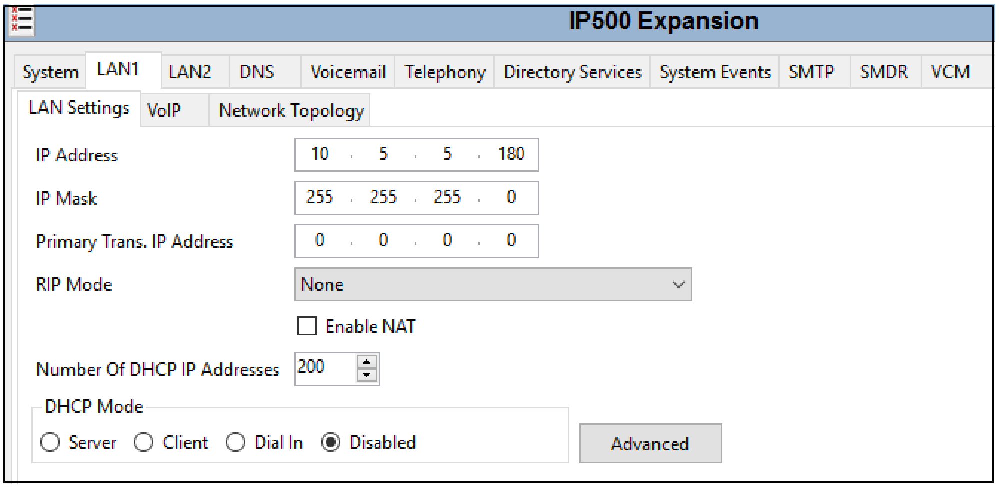
6.1. Expansion System - Physical Hardware

In the sample configuration, the IP500 V2 Expansion System contained a PHONE8 analog card and a COMBO6210 card, for the support of analog and digital stations. Also included is a VCM64 (Voice Compression Module). Both the VCM64 and the COMBO6210 cards provide voice compression channels to the control unit. Voice compression channels are needed to support VoIP calls, including IP extensions and or IP trunks.



6.2. Expansion System - LAN Settings

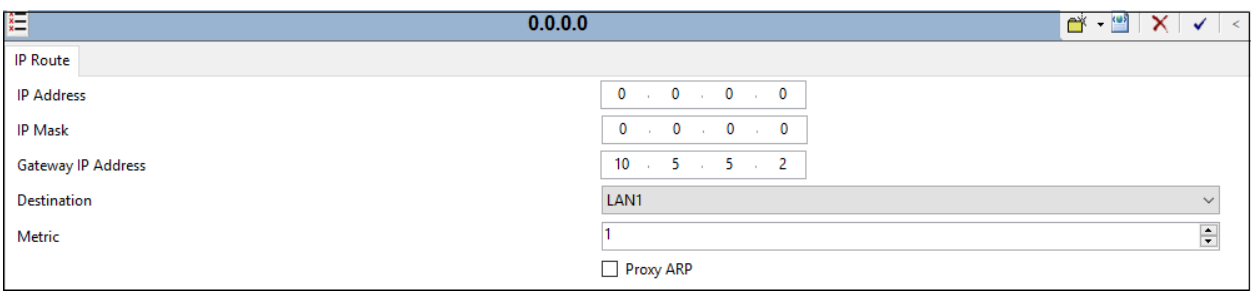
In the sample configuration, LAN1 is used to connect the Expansion System to the enterprise network. To view or configure the LAN1 IP address, select **System** on the Navigation pane. Select the **LAN1 → LAN Settings** tab on the Details pane. As shown in **Figure 1**, the IP Address of the Expansion System is **10.5.5.180**. Other parameters on this screen may be set according to customer requirements.



Defaults were used on the **VoIP** and **Network Topology** tabs (not shown).

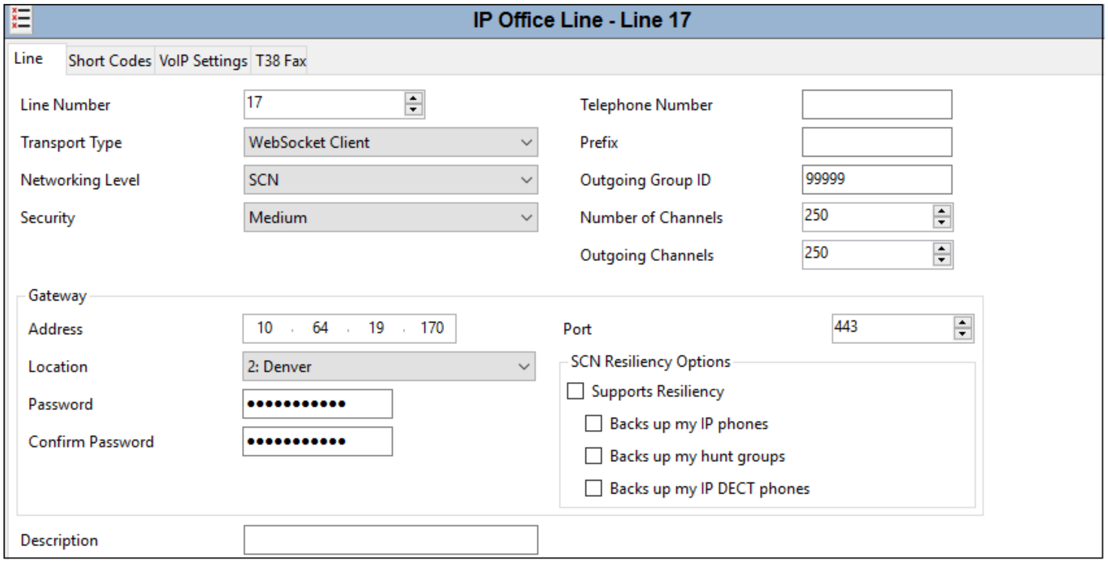
6.3. Expansion System - IP Route

To create an IP route for the Expansion System, right-click on **IP Route** on the left Navigation pane. Select **New** (not shown). The configuration is similar to the one on the Primary server (**Section 5.4**), with the difference that in the reference configuration, the default gateway for the Expansion System is **10.5.5.2**.

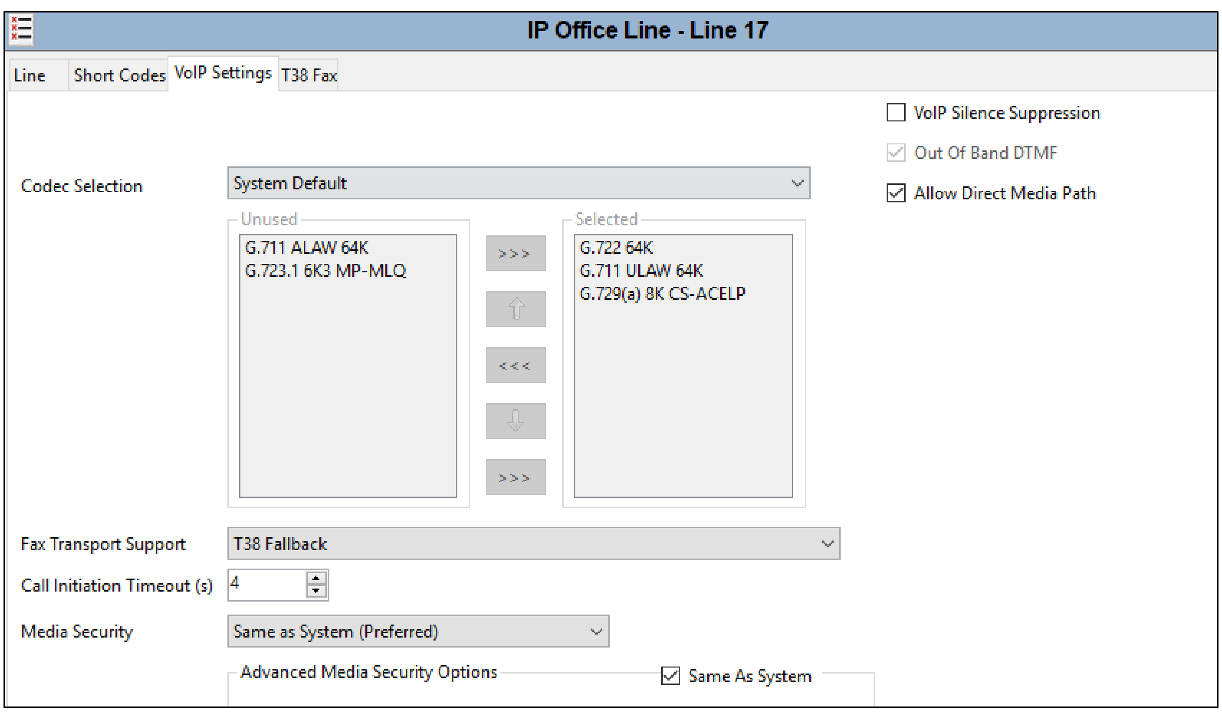


6.4. Expansion System - IP Office Line

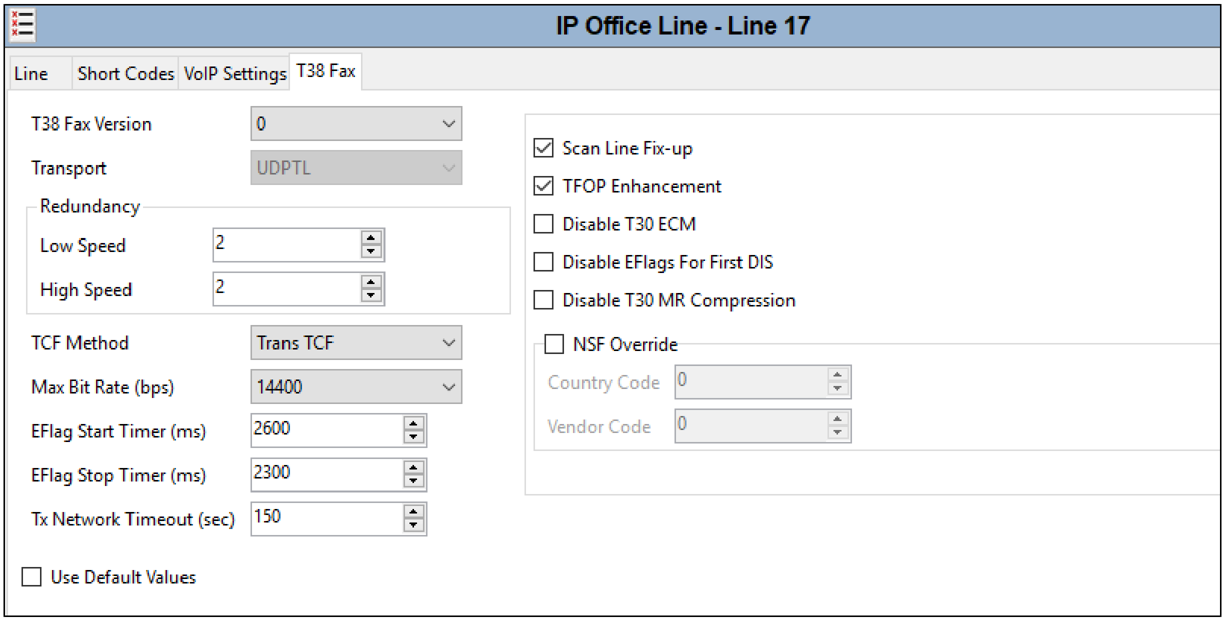
The IP Office Lines are automatically created on each server when the Expansion System is added to the solution. Below is the IP Office Line (**Line Number 17**) to the Primary server.



In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. To accommodate T.38 fax, select the **VoIP Settings** tab and set **Fax Transport Support** to **T38 Fallback.** The **Media Security** drop-down menu is set to "**Same as System (Preferred)**" to have IP Office use the system setting for media security set in **Section 5.3.3** to encrypted RTP.

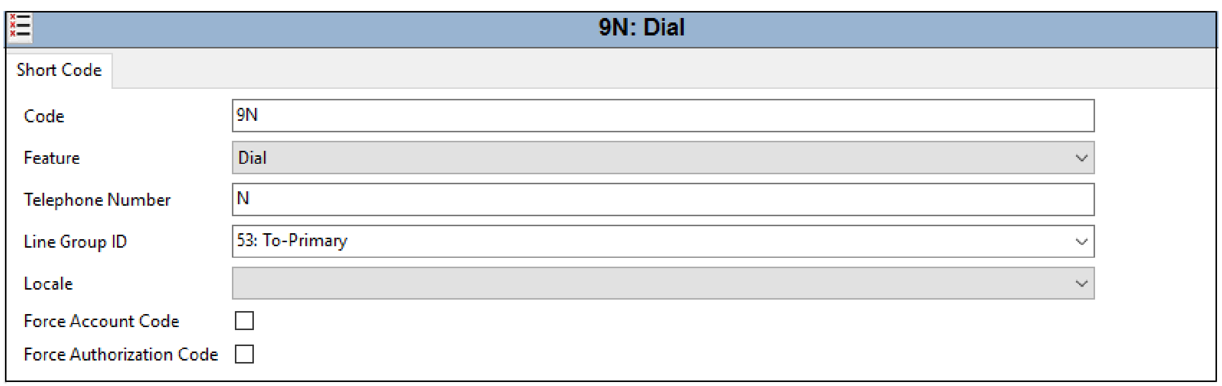


Select the **T38 Fax** tab. The **Use Default Values** box is unchecked, and the **T38 Fax Version** is set to **0**. In the **Redundancy** area, the **Low Speed** and **High Speed** parameters are set to **2**. All other values are left at default.



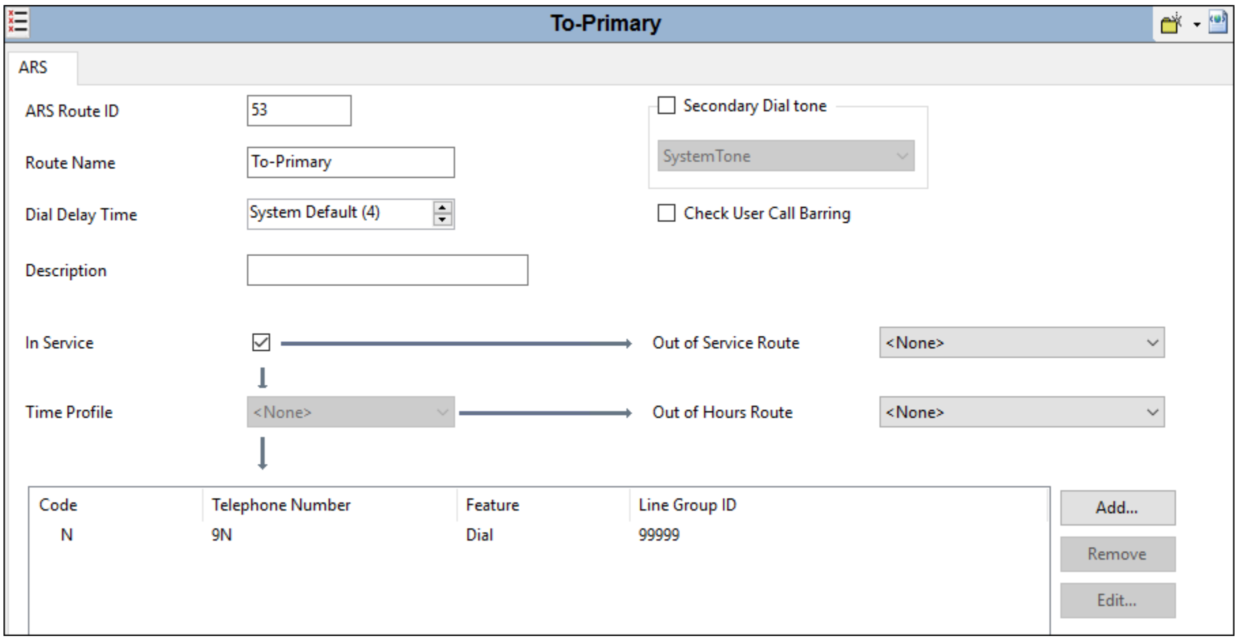
6.5. Expansion System - Short Codes

Similar to the configuration of the Primary server in **Section 5.8**, a Short Code is created to access ARS. In the reference configuration, the **Line Group ID** is set to an ARS route illustrated in the next section.



6.6. Expansion System - Automatic Route Selection – ARS

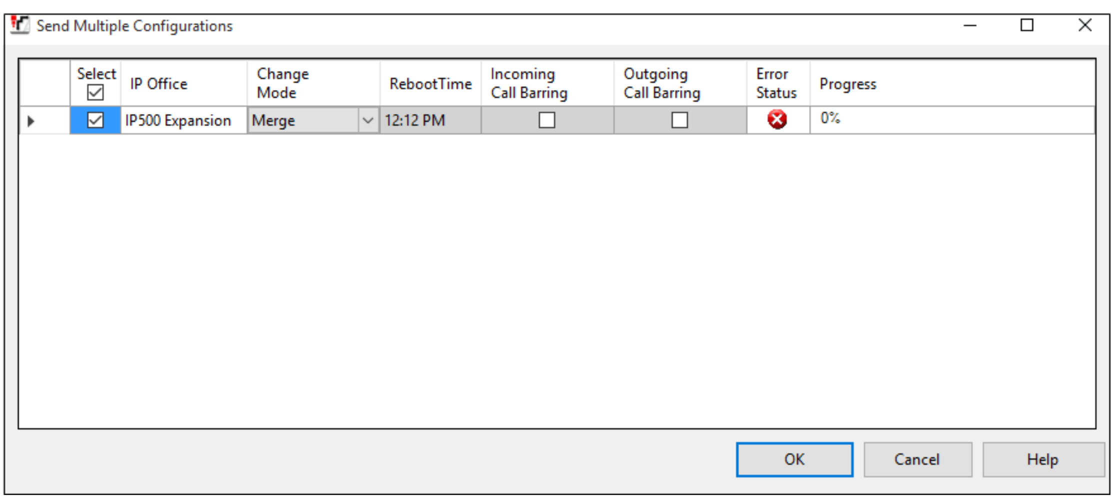
The following screen shows an example ARS configuration for the route named **To-Primary** on the Expansion System. The **Telephone Number** is set to **9N**. The **Line Group ID** is set to **99999** matching the number of the **Outgoing Group ID** configured on the IP Office Line 17 to the Primary server (**Section 6.4**).



6.7. Save IP Office Expansion System 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, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to proceed.



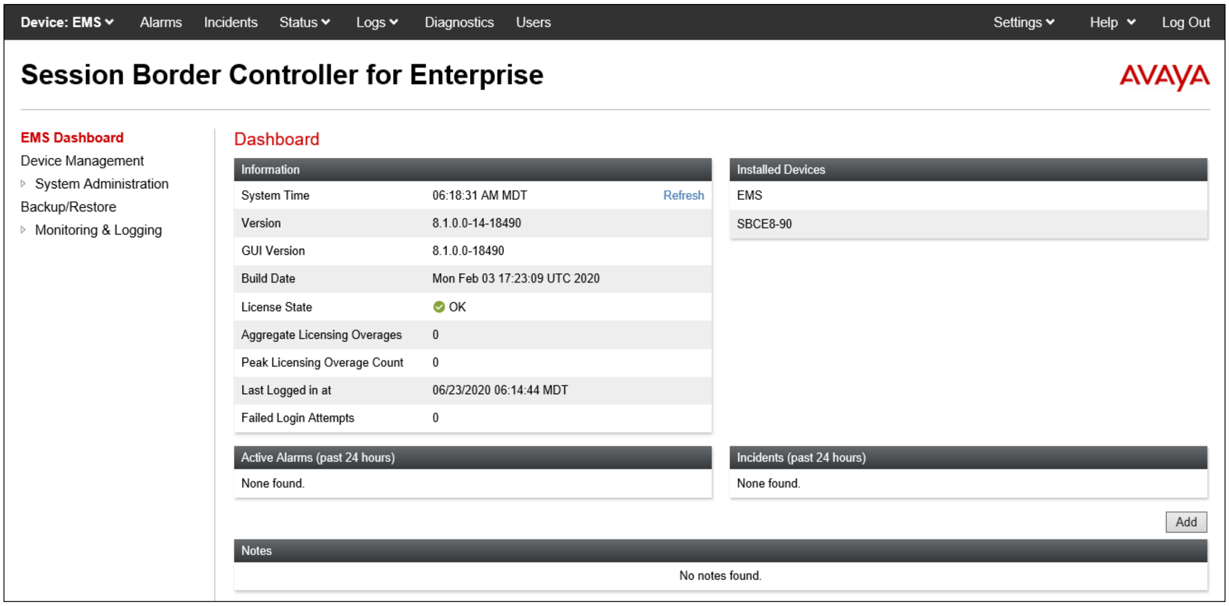
7. Configure Avaya Session Border Controller for Enterprise

In the reference configuration, Avaya SBCE is used as an edge device between the CPE and Verizon Business.

This section covers the configuration of the Avaya SBCE. It is assumed that the initial provisioning of the Avaya SBCE, 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 SBCE consult the Avaya SBCE 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 the Avaya SBCE. Log in using the appropriate credentials.

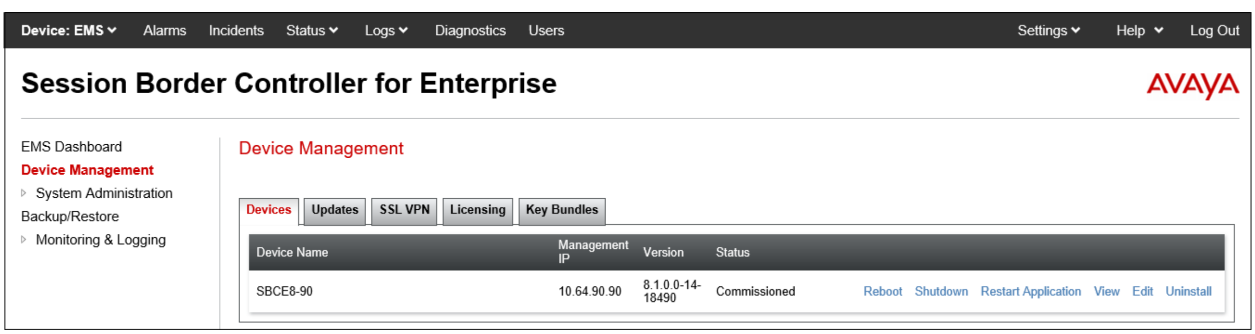
The EMS Dashboard page of the Avaya SBCE will appear. Note that the installed software version is displayed. Verify that the **License State** is **“OK”**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.



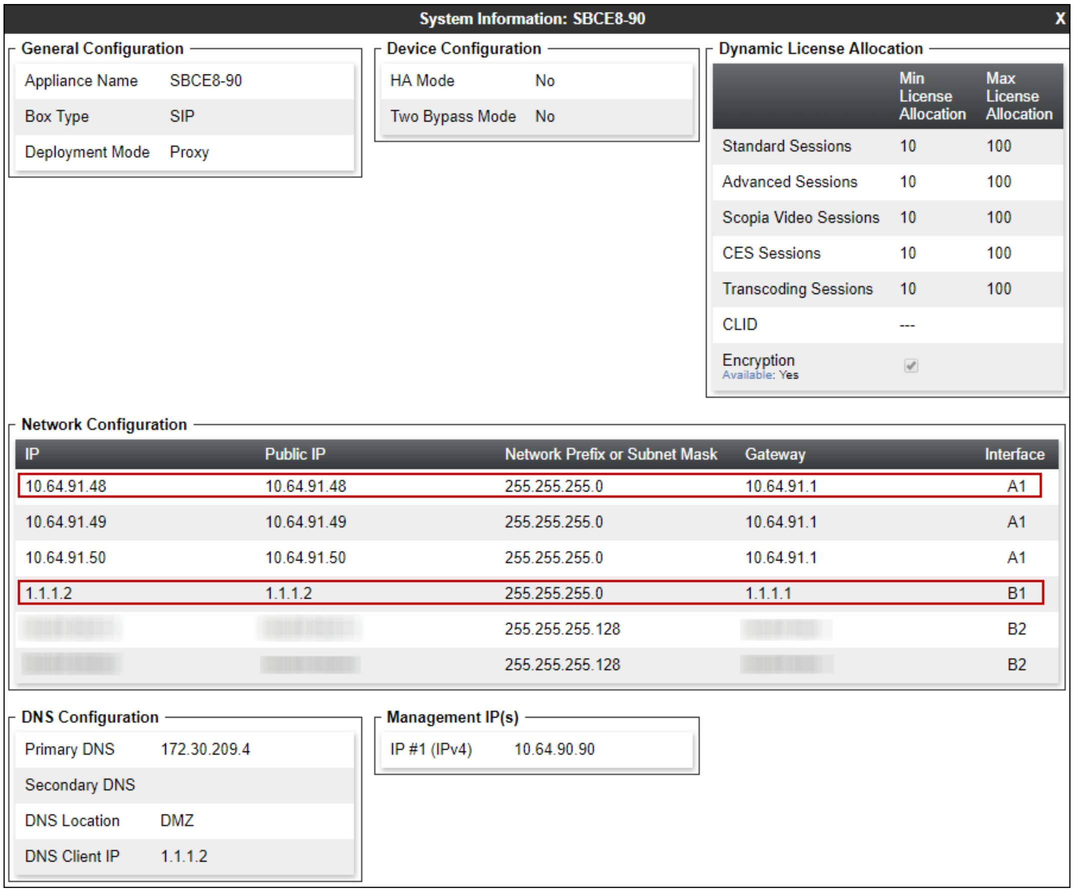
7.1. Device Management – Status

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 **SBCE8-90** 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 SBCE 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**. In the shared test environment, the highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to Verizon. Other IP addresses assigned to interfaces **A1** and **B2** on the screen below are used to support remote workers and are not the focus of these Application Notes. Note that the **Management IP** must be on a separate subnet from the IP interfaces designated for SIP traffic.



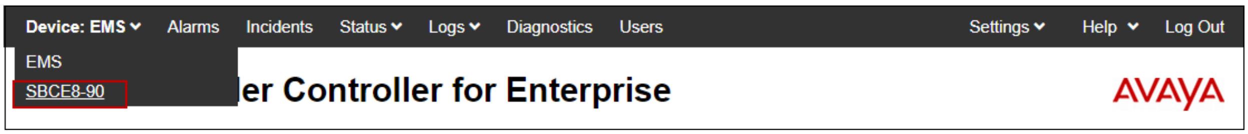
7.2. TLS Management

Note – Testing was done using identity certificates signed by a local certificate authority. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

In the reference configuration, TLS transport is used for the communication between IP Office and Avaya SBCE. The following procedures show how to view the certificates and configure the profiles to support the TLS connection.

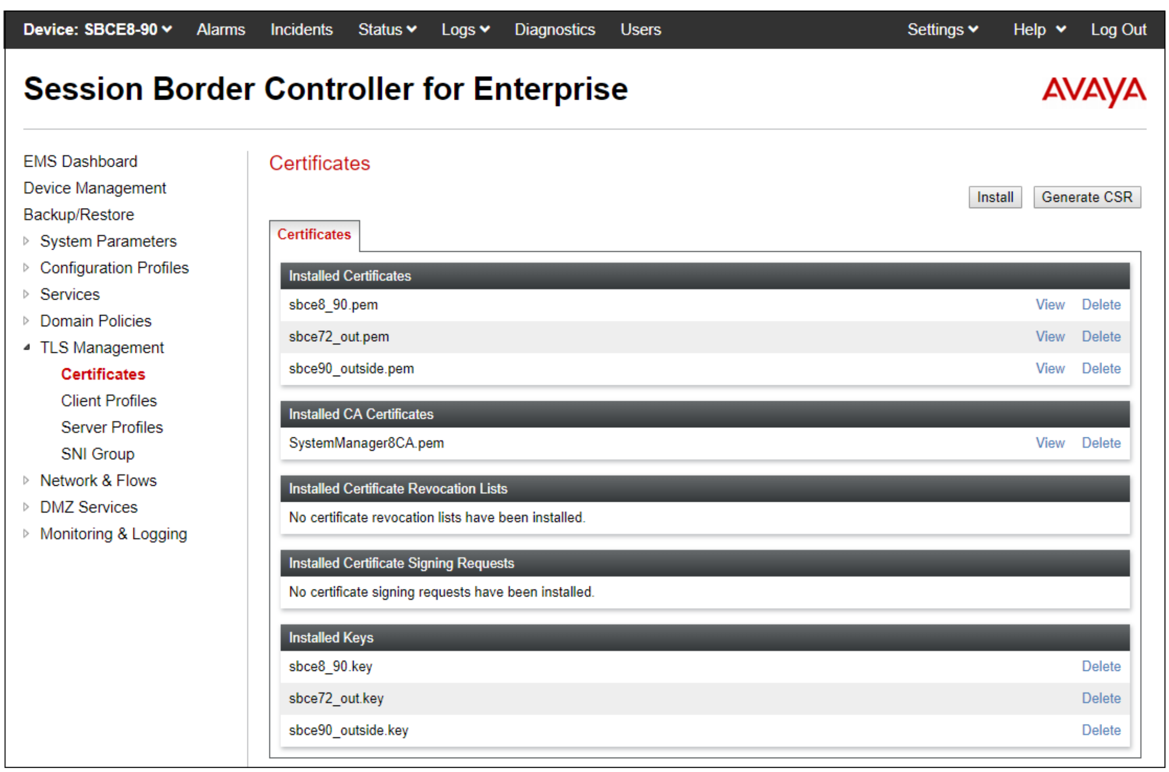
7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

To access the SBCE configuration menus, select the SBCE device from the top navigation menu.



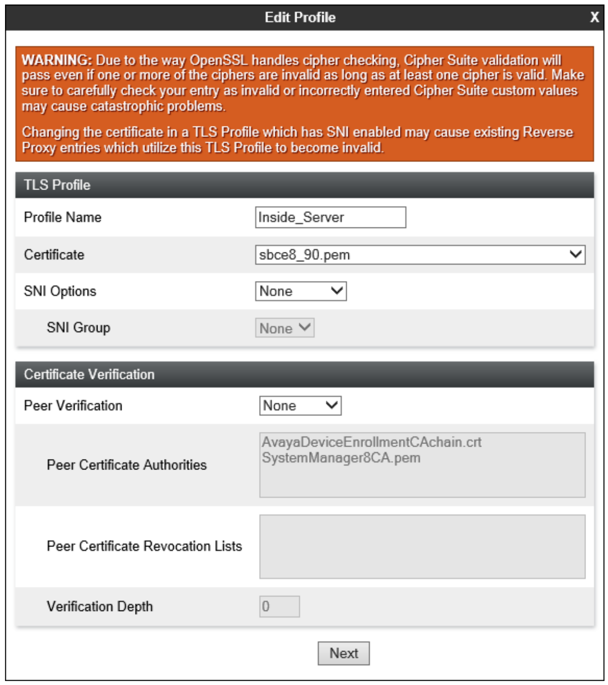
Note – The provisioning described in the following sections use the menu options listed in the left-hand column shown below.

Select **TLS Management → Certificates** from the left-hand menu. Verify the root CA certificate is present in the **Installed CA Certificates** area. The signed identity certificate is present in the **Installed Certificates** area. The private key associated with the identity certificate is present in the **Installed Keys** area.

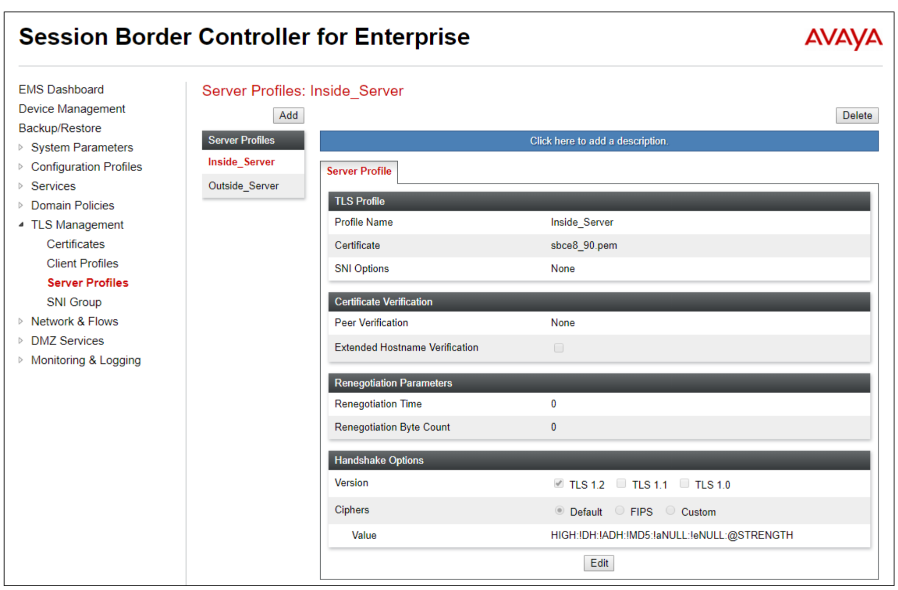


7.2.2. Server Profiles

Navigate to **TLS Management → Server Profiles** and click the **Add** button to add a new profile or select an existing profile. Enter a descriptive **Profile Name** such as **Inside_Server** show below. Select the Avaya SBCE identity certificate for the inside interface from the **Certificate** drop-down menu. In the reference configuration this is **sbce8_90.pem**. Select **None** from the **Peer Verification** drop-down menu. Click **Next** and accept default values for the next screen, then click **Finish** (not shown).

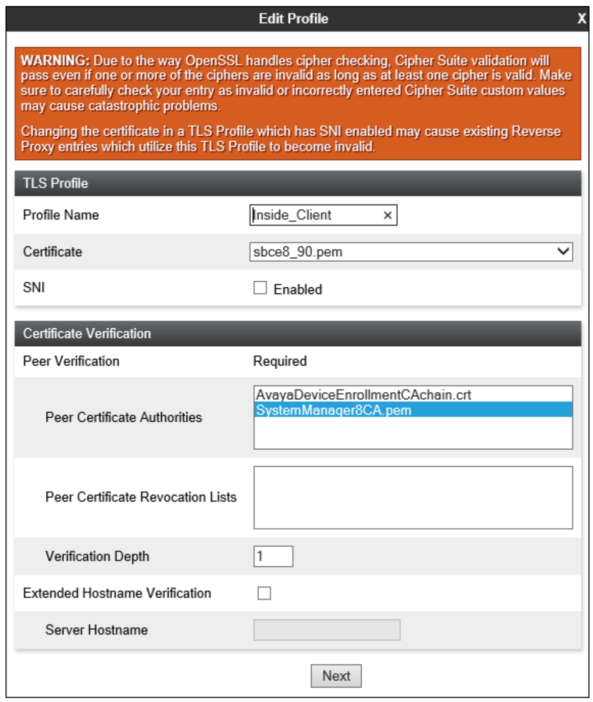


The following screen shows the completed TLS **Server Profile** form:

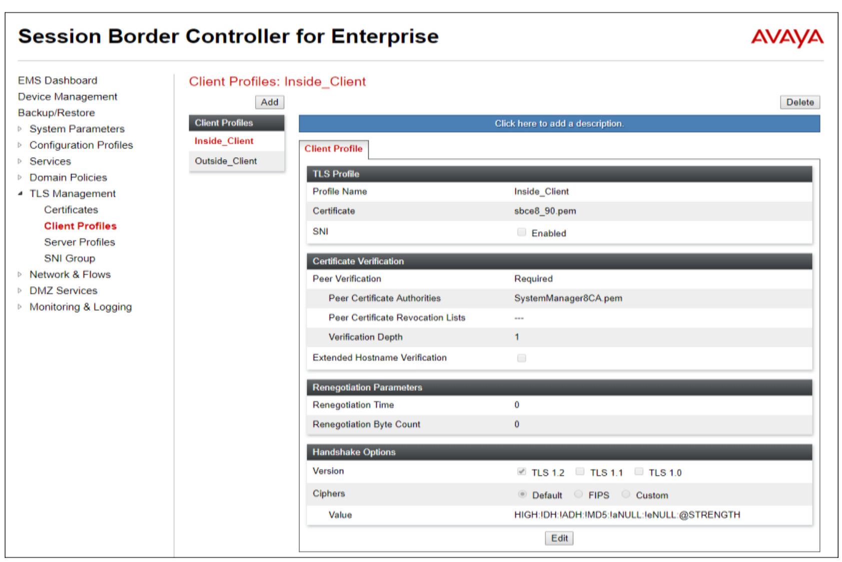


7.2.3. Client Profiles

Navigate to **TLS Management → Client Profiles** and click the **Add** button to add a new profile or select an existing profile. Enter a descriptive **Profile Name**, such as **Inside_Client** show below. Select the identity certificate from the **Certificate** drop-down menu. In the reference configuration this is **sbce8_90.pem**. The **Peer Certificate Authorities** field is set to the root certificate used to verify the IP Office certificate, e.g., **SystemManager8CA.pem**. The **Verification Depth** field is set to **1**. Click **Next** and accept default values for the next screen and click **Finish** (not shown).

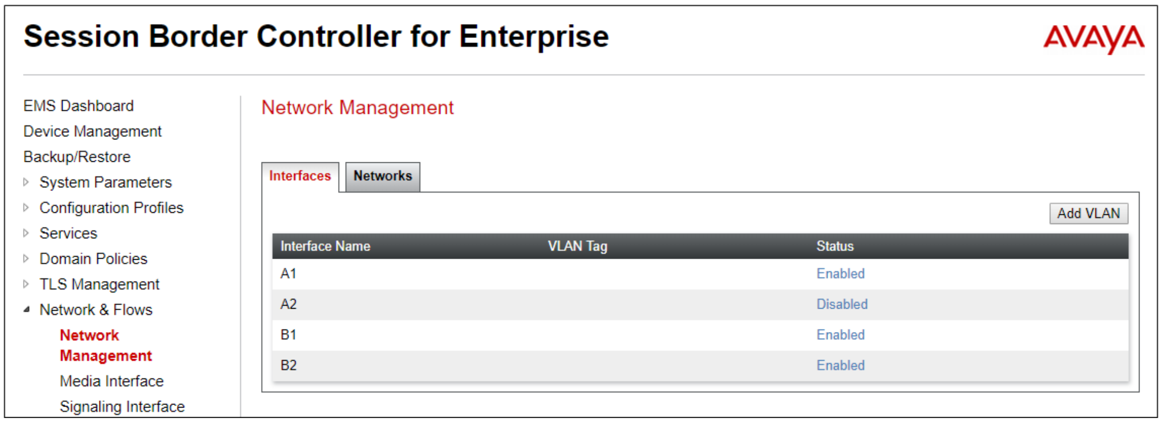


The following screen shows the completed TLS **Client Profile** form:



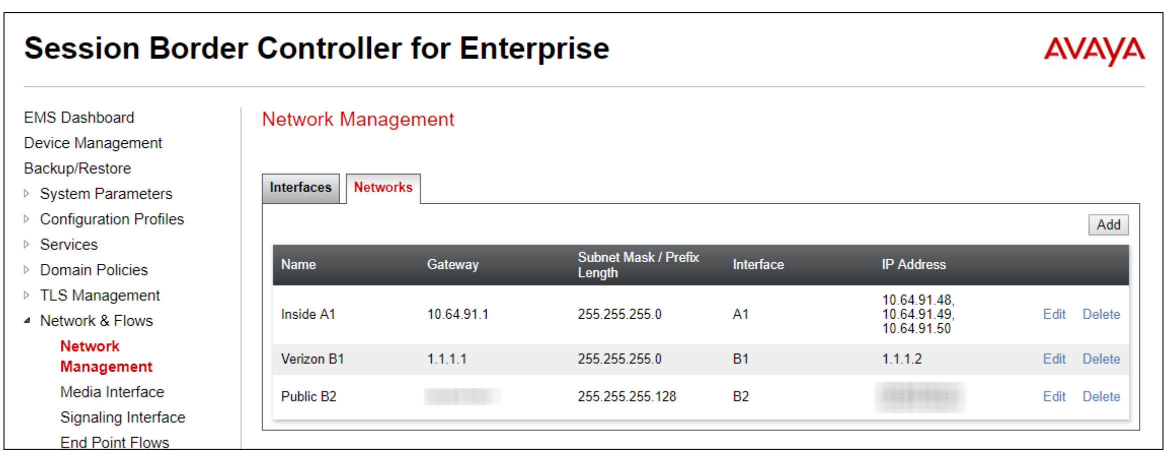
7.3. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, 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. Navigate to **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 B1 are used.



Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however, some of these values may not be changed if associated provisioning is in use.

- **A1**: **10.64.91.48** – "Inside" IP address, configured for Verizon Business IPCC VoIP Inbound Service to IP Office.
- **A1**: **10.64.91.50** – "Inside" IP address configured for Verizon Business IP Trunk SIP Trunk Service to IP Office. This address is used to connect IP Office to the Verizon Business IP Trunk service as illustrated in reference [IPT-IPO111SBC81].
- **B1: 1.1.1.2** – "Outside" IP address toward the Verizon SIP trunk. This address is known to Verizon and is associated with the FQDN *adevc.avaya.globalipcom.com*.

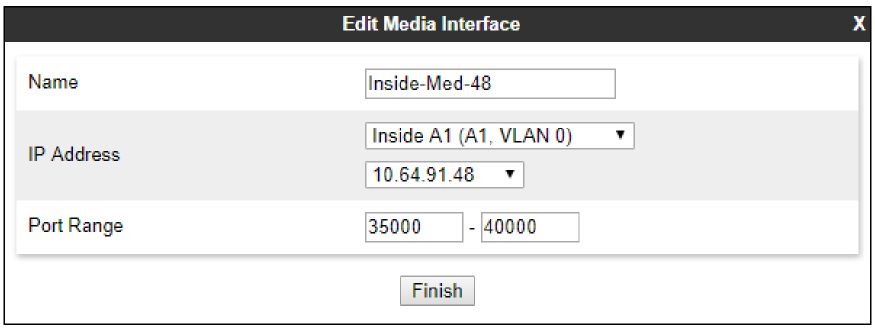


7.4. Media Interfaces

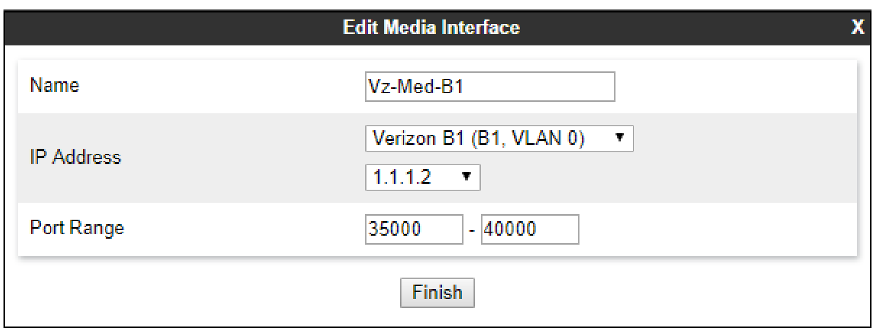
Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBCE will accept media from the connected server. Create a SIP Media Interface for both the inside and outside IP interfaces.

To create a new Media Interface, navigate to Select **Network & Flows → Media Interface** from the menu on the left-hand side and select **Add** (not shown).

The screen below shows the **Inside-Med-48** Media Interface created toward the IP Office. On the **IP Address** drop-down menus, **Inside-A1 (A1,VLAN0)** and **10.64.91.48** are selected. Default **Port Range** values are used.



The screen below shows the **Vz-Med-B1** Media Interface created toward Verizon. On the **IP Address** drop-down menus, **Verizon-B1 (B1,VLAN0)** and **1.1.1.2** are selected. Default **Port Range** values are used.

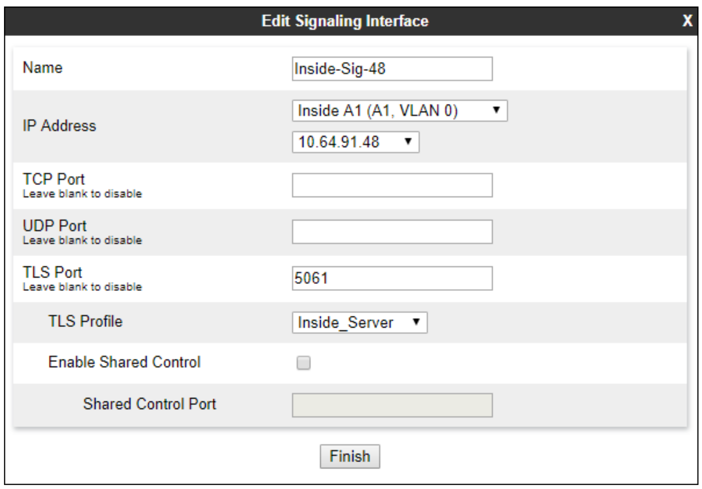


7.5. Signaling Interfaces

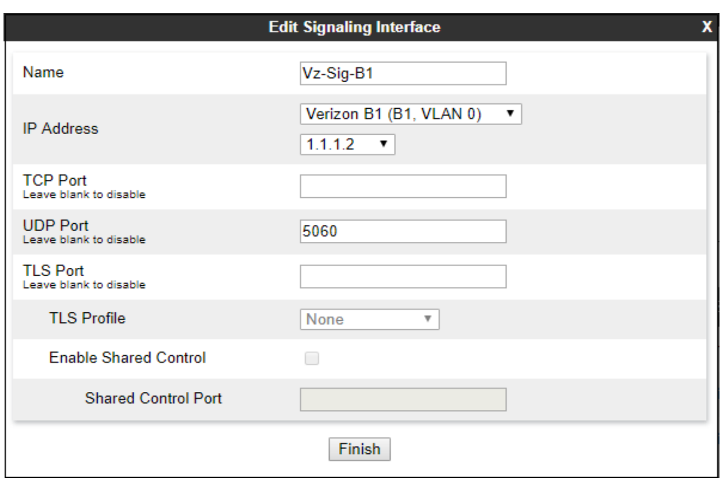
The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to Select **Network & Flows → Media Interface** from the menu on the left-hand side and select **Add** (not shown).

The screen below shows the **Inside-Sig-48** Signaling Interface created toward the IP Office. On the **IP Address** drop-down menus, **Inside-A1 (A1,VLAN0)** and **10.64.91.48** are selected. **TLS Port 5061** is used. The TLS server profile created in **Section 7.2.2** (e.g., **Inside_Server**) is selected on the TLS Profile drop-down menu.



The screen below shows the **Vz-Sig-B1** Signaling Interface created toward Verizon. On the **IP Address** drop-down menus, **Verizon-B1 (B1,VLAN0)** and **1.1.1.2** are selected. **UDP Port 5060** is used.



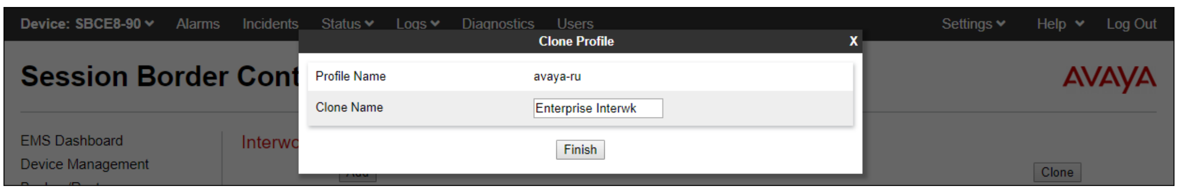
7.6. Server Interworking Profile

The Server Internetworking profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

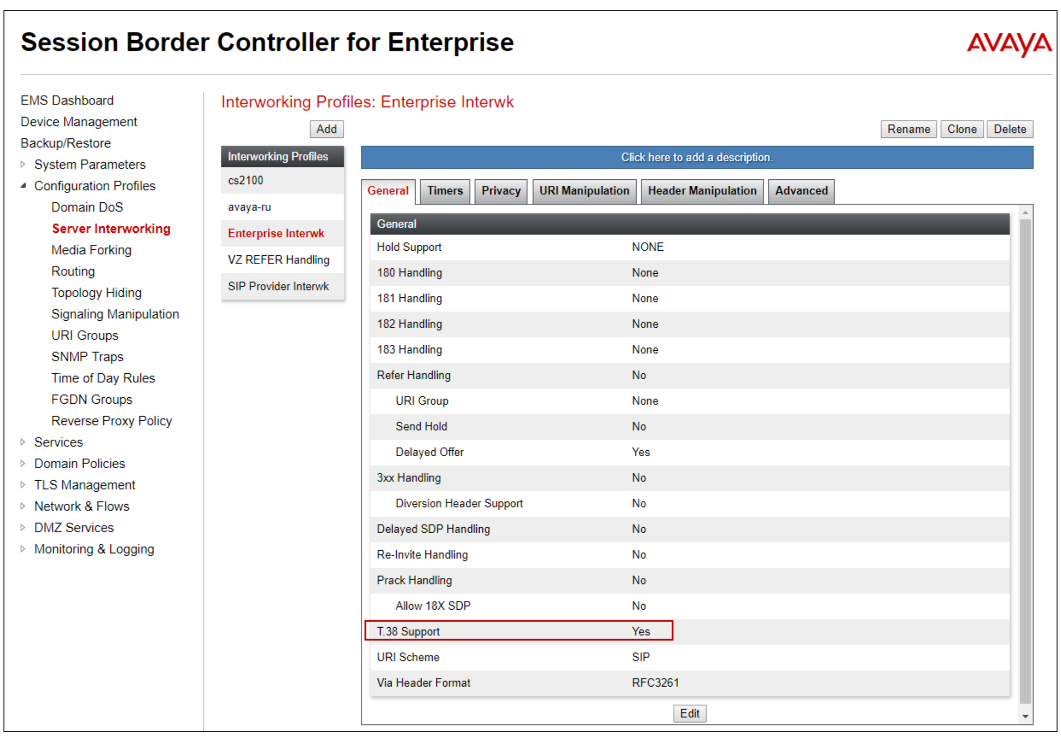
In the reference configuration, separate Server Interworking Profiles were created for IP Office and Verizon Business IPCC service.

7.6.1. Server Interworking Profile – IP Office

In the reference configuration, the IP Office Server Interworking profile was cloned from the default **avaya-ru** profile. To clone a Server Interworking Profile for IP Office, navigate to **Configuration Profiles → Server Interworking**, select the **avaya-ru** profile and click the **Clone** button. Enter a **Clone Name** and click **Finish** to continue.

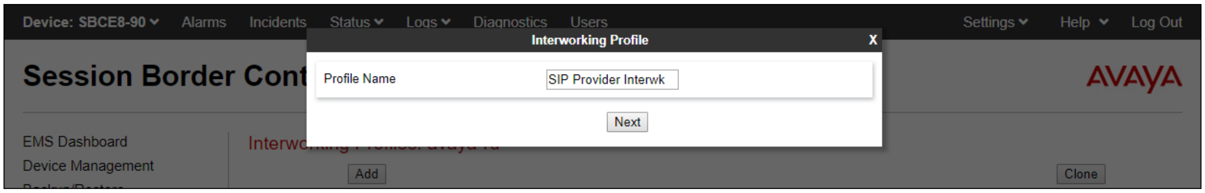


The following screen shows the **Enterprise Interwk** profile used in the reference configuration, with **T.38 Support** set to **Yes**. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish** (not shown). Default values can be used for all other fields.

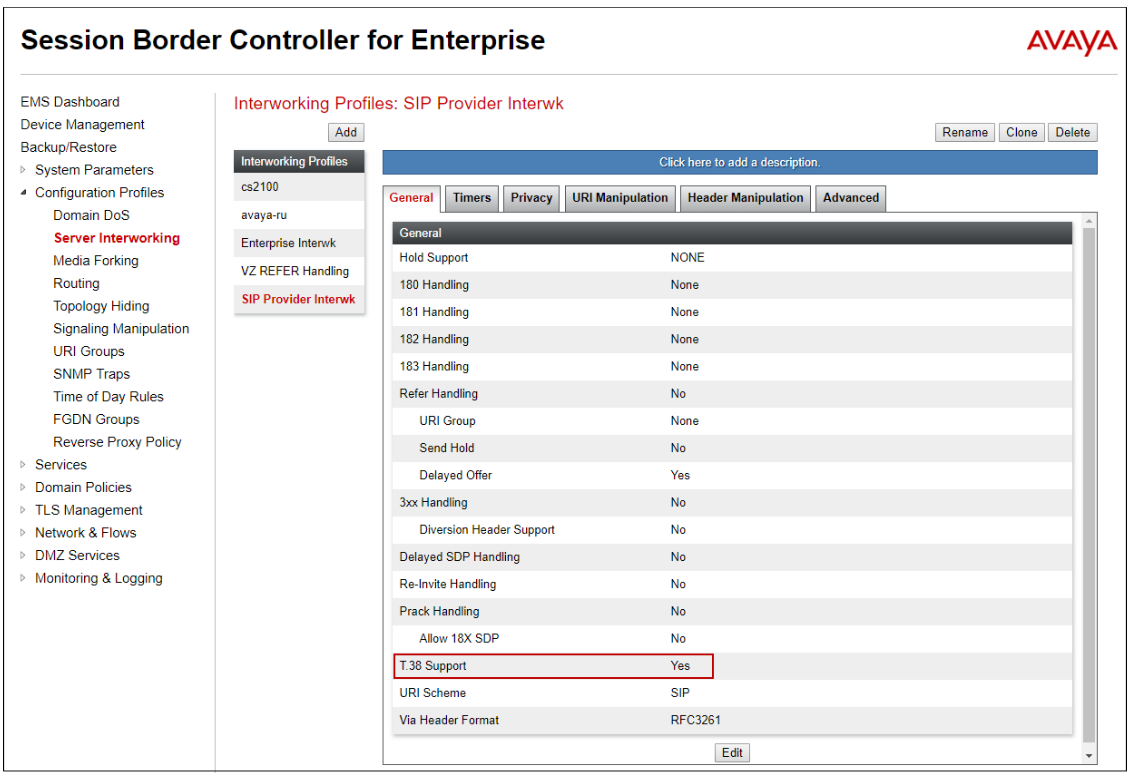


7.6.2. Server Interworking Profile – Verizon

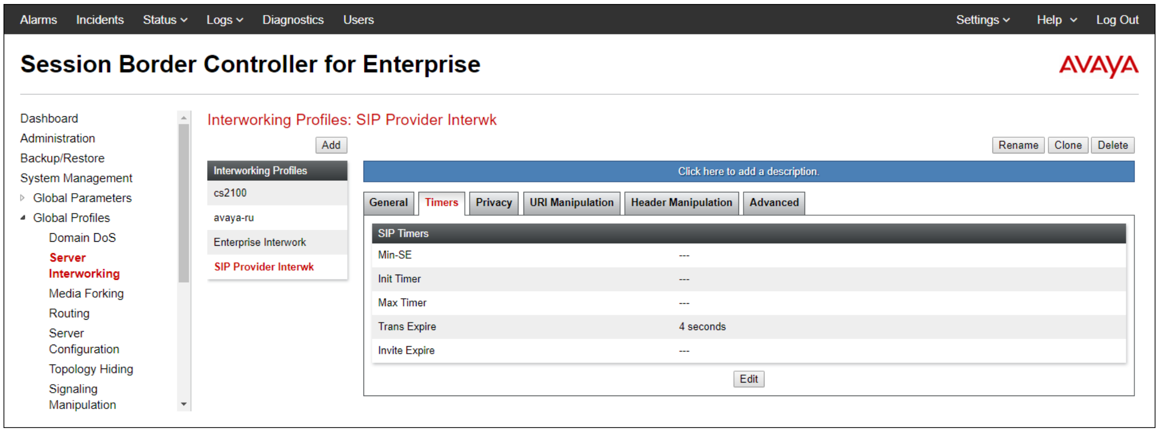
To create a new Server Interworking Profile for Verizon, navigate to **Configuration Profiles → Server Interworking** and click **Add** as shown below. Enter a **Profile Name** and click **Next**.



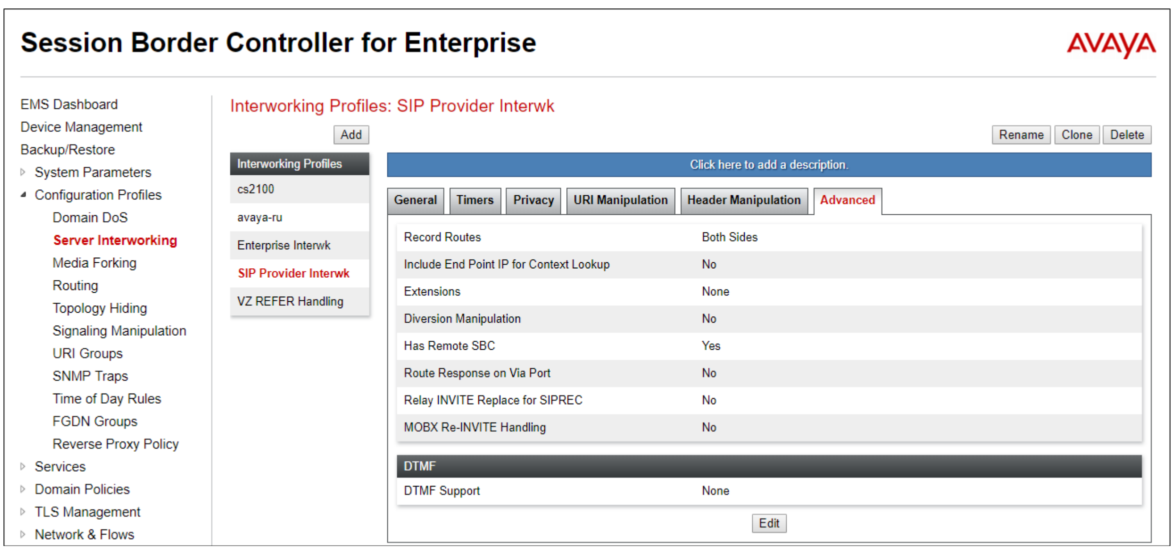
The following screens show the **SIP Provider Interwk** profile used in the reference configuration. On the **General** tab, default values are used with the exception of **T.38 Support** set to **Yes**.



The **Timers** tab shows the values used for compliance testing for the **Trans Expire** field. The **Trans Expire** timer sets the allotted time the Avaya SBCE will try the first primary server before trying the secondary server, if one exists.



Default parameters were used for the **Privacy**, **URI Manipulation**, and **Header Manipulation** tabs (not shown). On the **Advanced** tab, **Record Routes** is set to **Both Sides**. Default values can be used for all other fields.

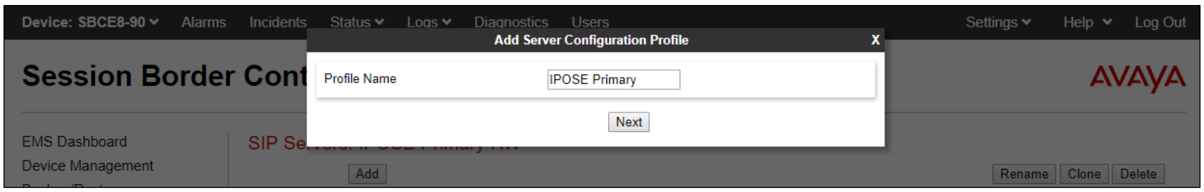


7.7. SIP Servers Profiles

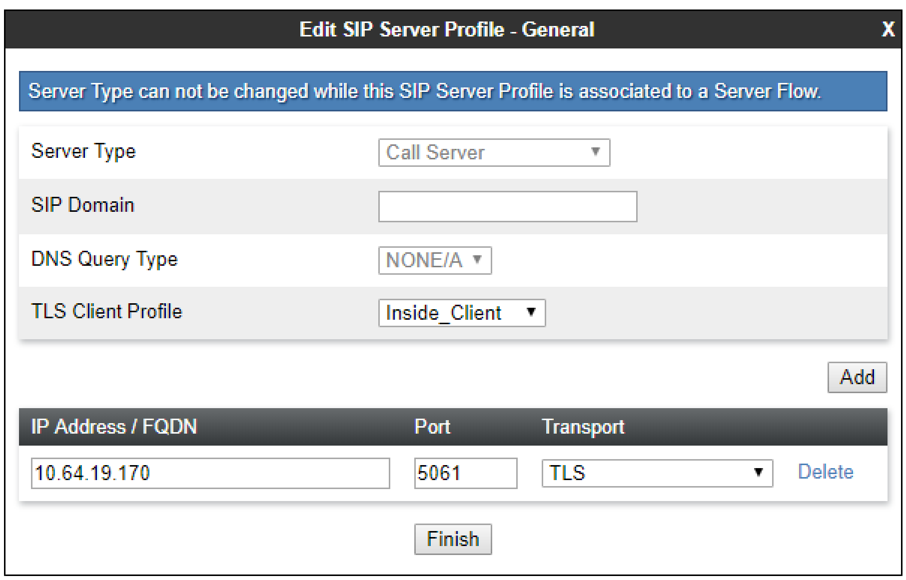
The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

7.7.1. SIP Server Profile – IP Office

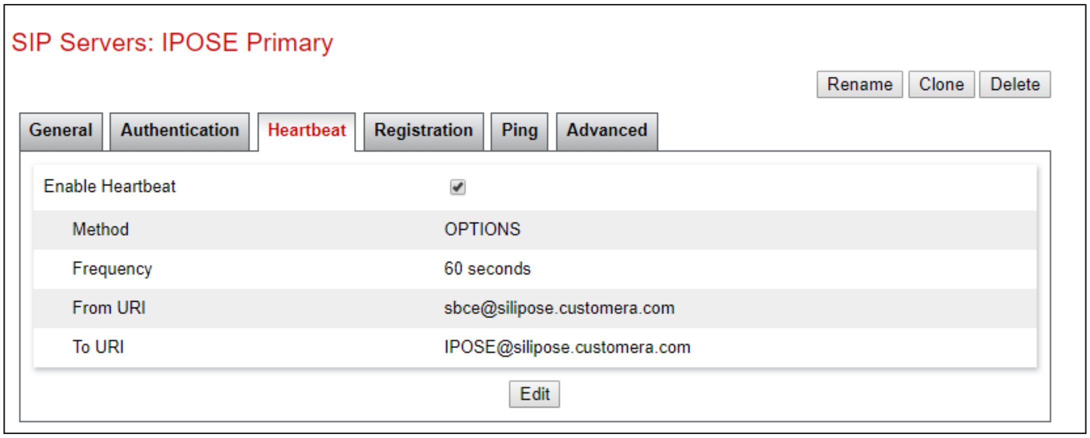
To add a SIP Server Profile for IP Office, navigate to **Services → SIP Servers** on the left-hand menu and click **Add**. Enter a descriptive name for the new profile and click **Next**.



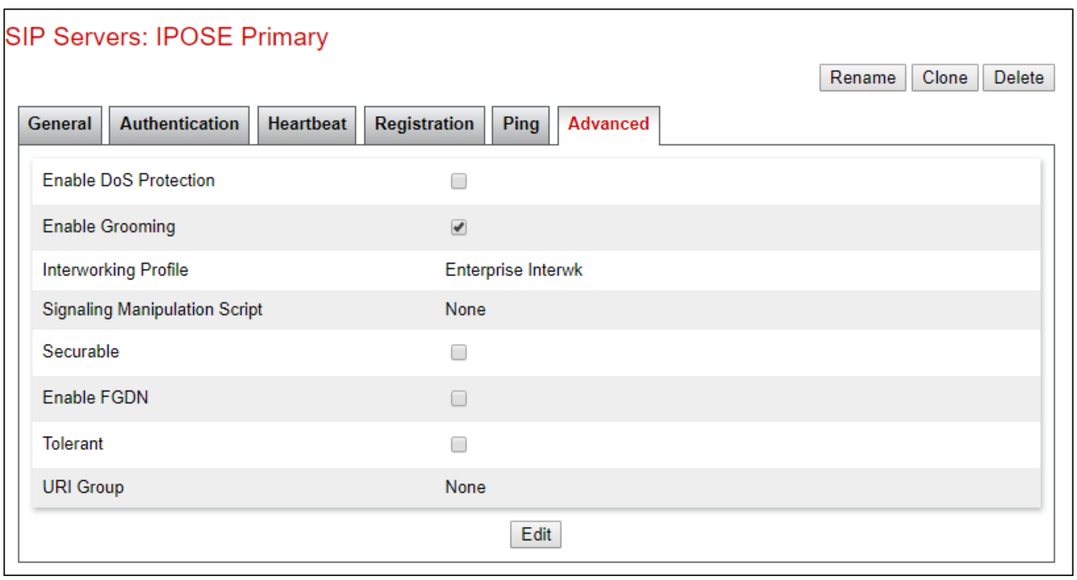
The following screen illustrate the SIP Server Profile named **IPOSE Primary**. In the **General** parameters, the **Server Type** is set to **Call Server**. In the **IP Address / FQDN** field, the IP Address of IP Office LAN 1 interface in the sample configuration is entered. This IP address is **10.64.19.170**. Under **Port**, **5061** is entered, and the **Transport** parameter is set to **TLS**. The TLS profile **Inside_Client** created in **Section 7.2.3** is selected for **TLS Client Profile**. 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, click **Next** (not shown) to proceed to the **Heartbeats** tab. The Avaya SBCE can be configured to source "heartbeats" in the form of PINGs or SIP OPTIONS towards IP Office. Check the **Enable Heartbeat** box and select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE.

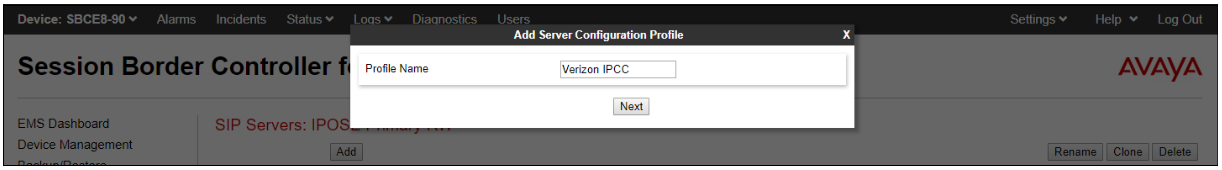


On the **Advanced** tab, select the **Enable Grooming** checkbox. The **Interworking Profile** is set to the **Enterprise Interwk** profile created in **Section 7.6.1** for IP Office.

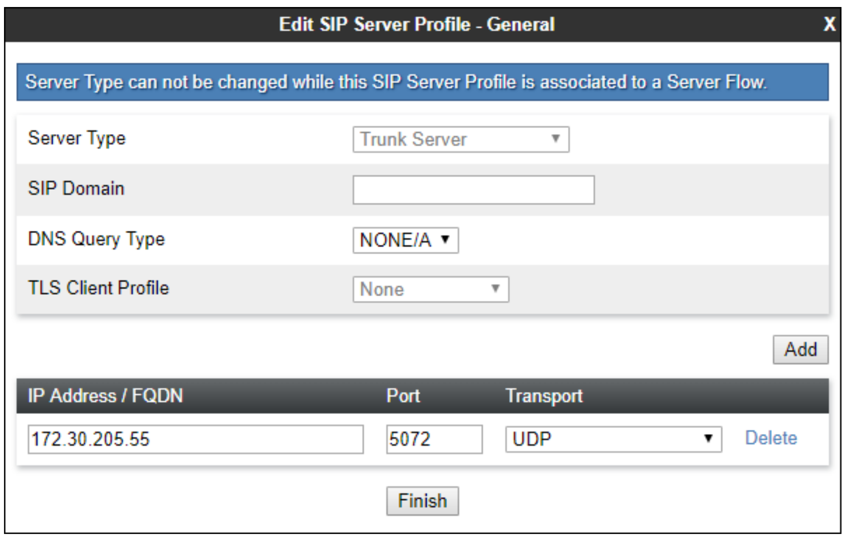


7.7.2. SIP Server Profile - Verizon

To add a SIP Server Profile for Verizon, navigate to **Services → SIP Servers** and click **Add**. Enter a descriptive name for the new profile and click **Next**.

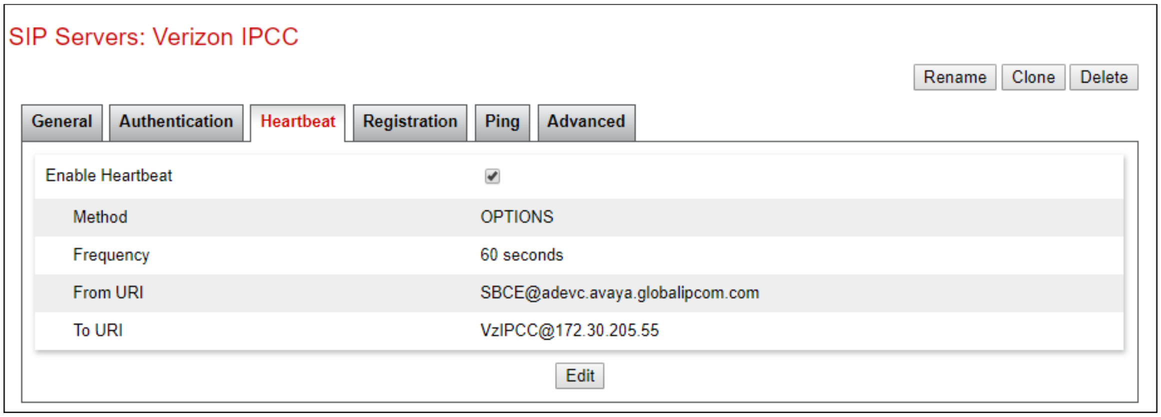


The following screens illustrate the SIP Server Profile named **Verizon IPCC**. In the **General** parameters, the **Server Type** is set to **Trunk Server**. The **DNS Query Type** is set to **NONE/A**. In the **IP Address / FQDN** field, the Verizon-provided IP address is entered. This is **172.30.205.55**. Under **Port**, **5072** is entered, and the **Transport** parameter is set to **UDP**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

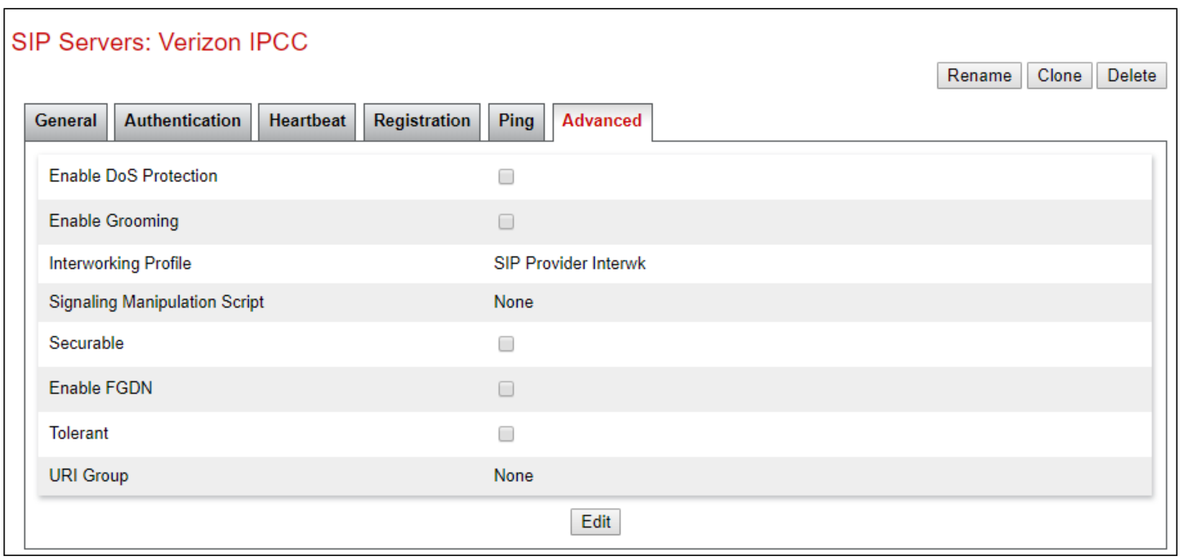


Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeats** tab. The Avaya SBCE can be configured to source "heartbeats" in the form of SIP OPTIONS towards Verizon. This configuration is optional. Independent of whether the Avaya SBCE is configured to source SIP OPTIONS towards Verizon, Verizon will receive OPTIONS from the IP Office site as a result of the **Check OOS** parameter being enabled on IP Office (see **Section 5.5.2**). When IP Office sends SIP OPTIONS to the inside IP Address of the Avaya SBCE, the Avaya SBCE will send SIP OPTIONS to Verizon Business. When Verizon Business responds, the Avaya SBCE will pass the response to IP Office.

Check the **Enable Heartbeat** box and select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE.



On the **Advanced** tab, **Enable Grooming** is not used for UDP connections and left unchecked. The **Interworking Profile** is set to **SIP Provider Interwk** created in **Section 7.6.2** for Verizon.

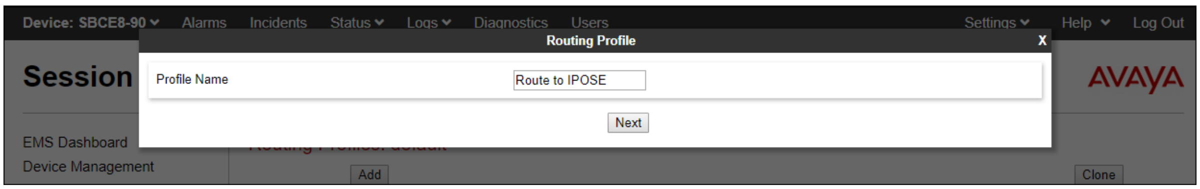


7.8. Routing Profiles

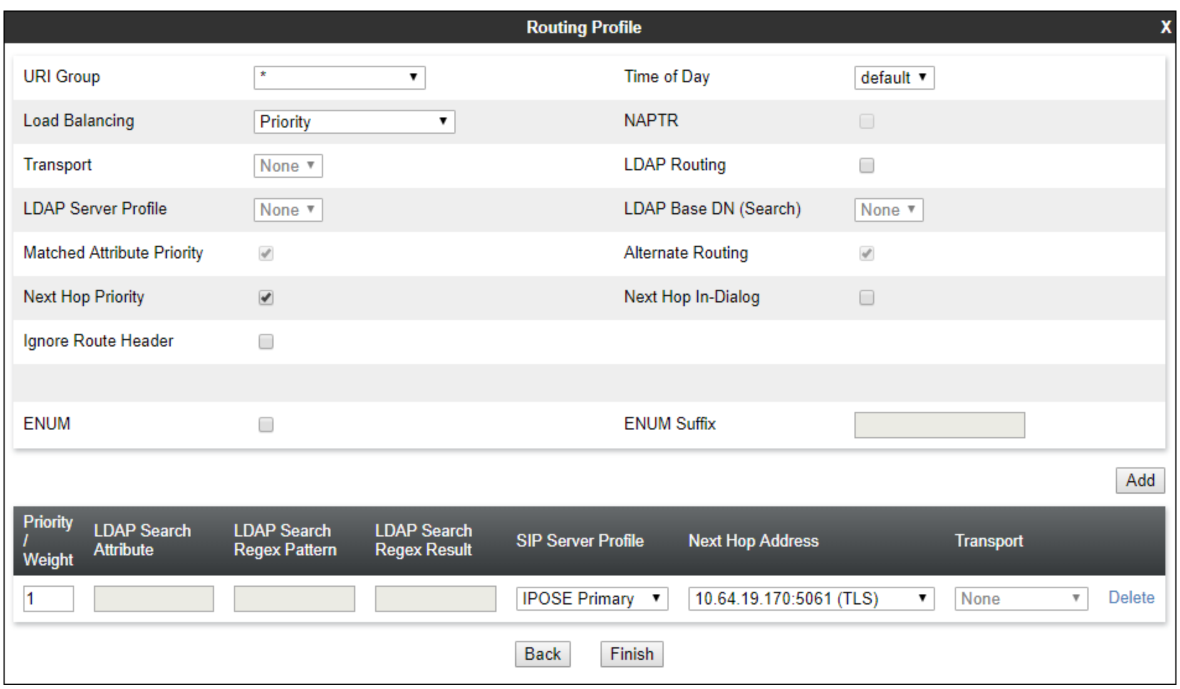
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types. Separate Routing Profiles were created in the reference configuration for IP Office and the Verizon Business IPCC service.

7.8.1. Routing Profile – IP Office

To add a routing profile for the IP Office, navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.

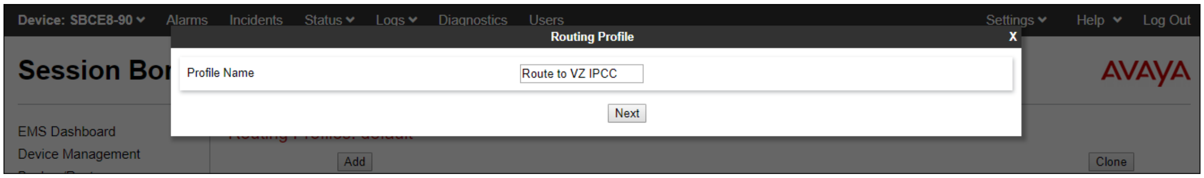


The following screen shows the Routing Profile **Route to IPOSE** created in the reference configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to **1**, and the IP Office **SIP Server Profile**, created in **Section 7.7.1**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the SIP Server Profile, and **Transport** becomes greyed out. Click **Finish**.

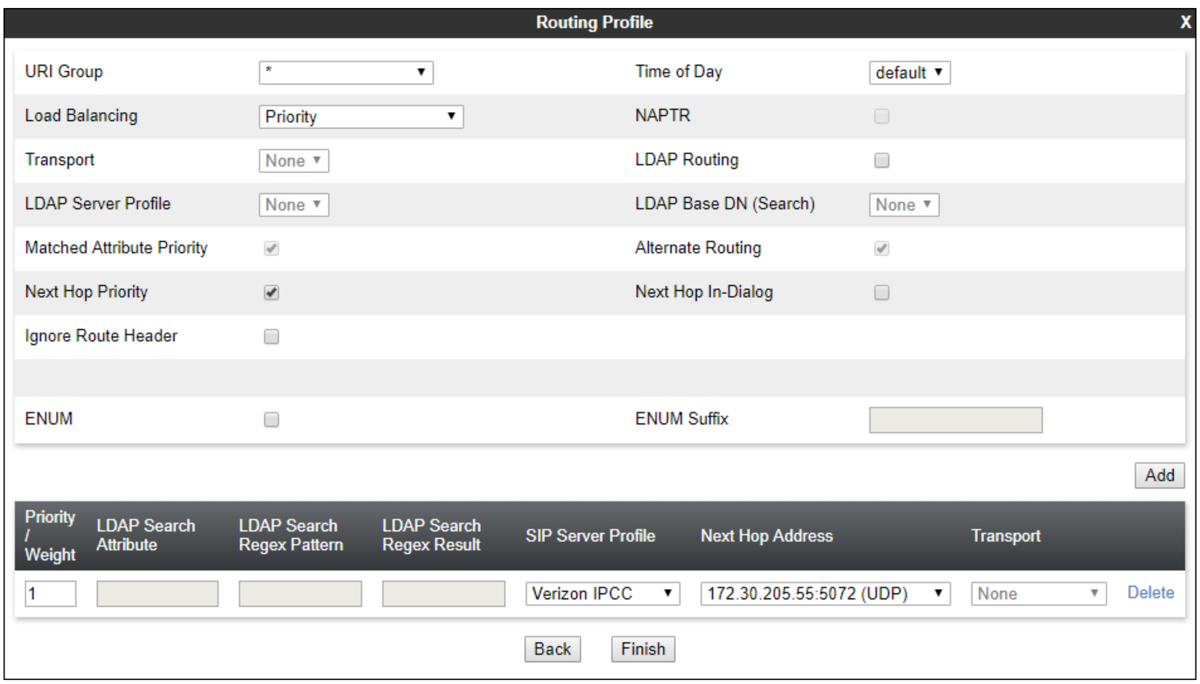


7.8.2. Routing Profile – Verizon

Similarly add a Routing Profile to the Verizon Business IPCC service.



The following screen shows the Routing Profile **Route to VZ IPCC** created in the reference configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to **1**, and the Verizon **Server Configuration**, created in **Section 7.7.2**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the Server Configuration, and the Transport becomes greyed out. Click **Finish**.



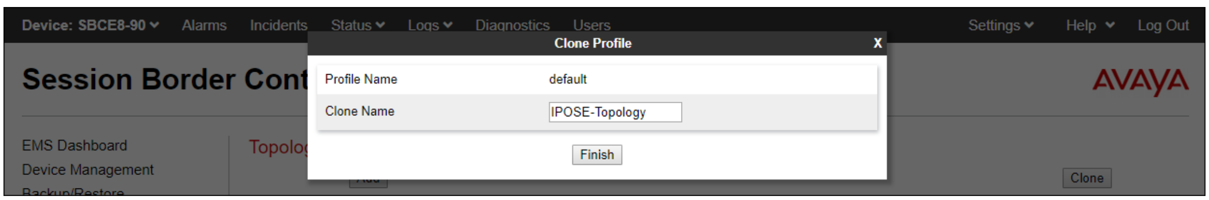
7.9. Topology Hiding Profiles

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

Topology Hiding can also be used as an interoperability tool to adapt the host portion of the SIP headers, to the IP addresses or domains expected on the service provider and the enterprise networks.

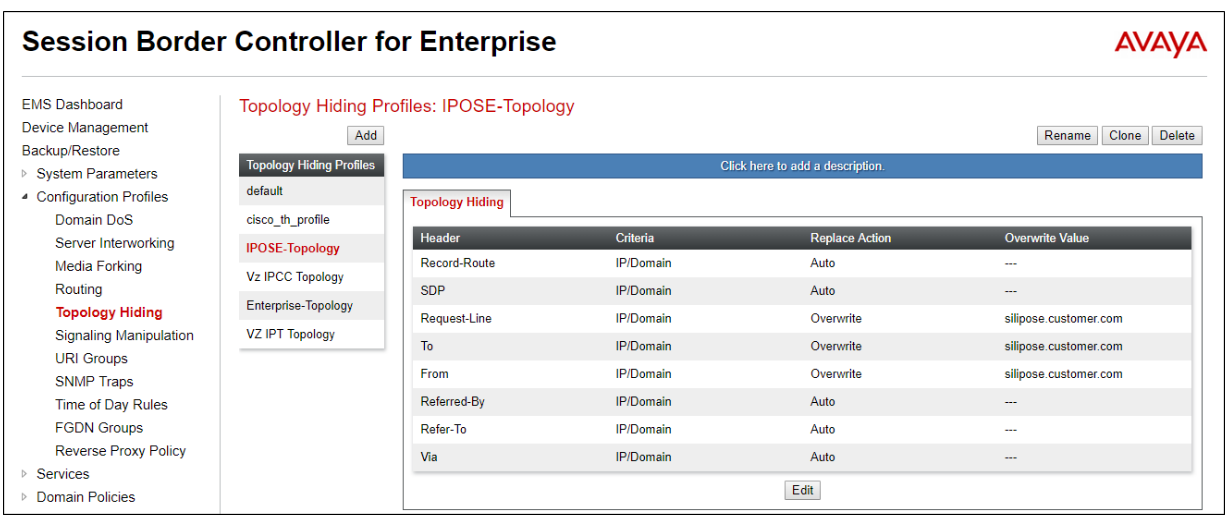
7.9.1. Topology Hiding – IP Office

In the sample configuration, the IP Office Topology Hiding profile was cloned from the **default** profile and then modified. Select **Configuration Profiles → Topology Hiding** from the left-hand menu. Select the pre-defined **default** profile and click the **Clone** button. Enter profile name (e.g., **IPOSE-Topology**) and click **Finish** to continue.



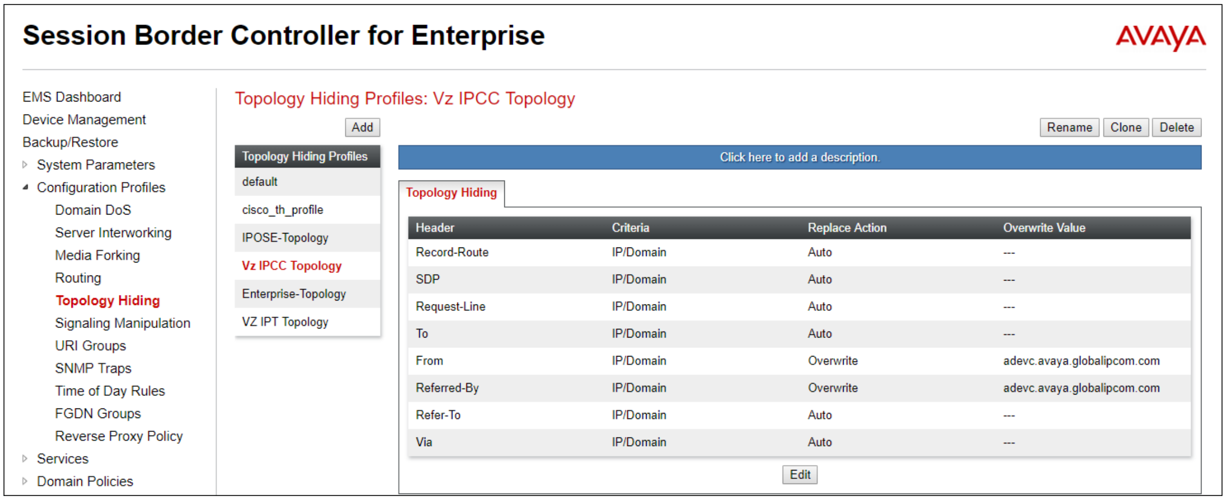
On the newly created profile, in the **Replace Action** column, an action of **Auto** will replace the header field with the IP address of the Avaya SBCE interface, while **Overwrite** will use the value in the **Overwrite Value**.

The screen below shows the **IPOSE-Topology** used in the reference configuration. For the **Request-Line**, **To** and **From** headers, **Overwrite** is selected under the **Replace Action** column. The domain of the enterprise (e.g., **silipose.customer.com**) is entered on the **Overwrite Value** field.



7.9.2. Topology Hiding – Verizon

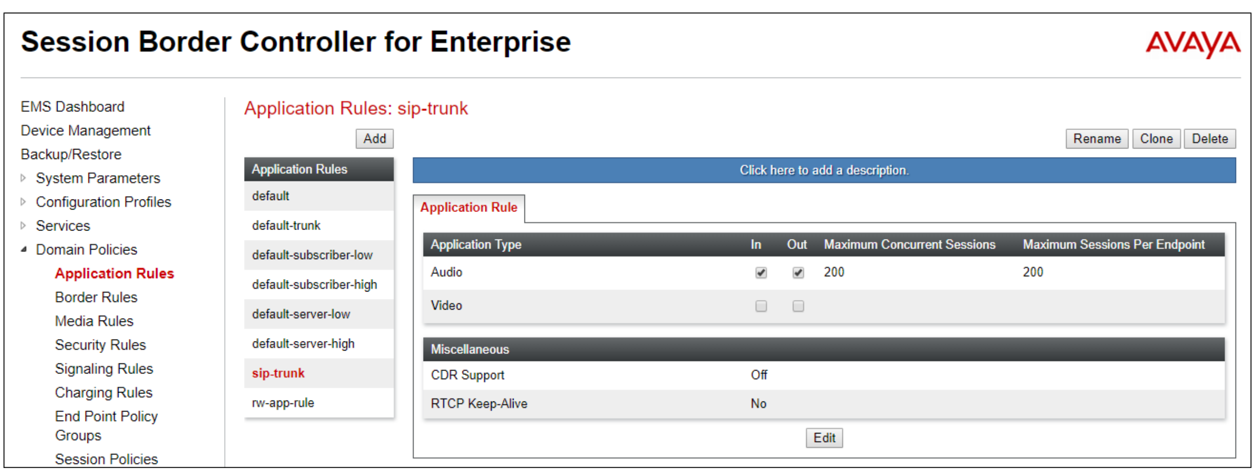
Similarly create a Topology Hiding profile for the Avaya SBCE connection to Verizon. Enter a Profile Name (e.g., **VZ IPCC Topology**). Overwrite the **From** and **Referred-By** headers with the FQDNs known by Verizon, as shown on the screen below.



7.10. Application Rule

Application Rules define which types of SIP-based Unified Communications applications the Avaya SBCE security device will protect. In addition, the maximum number of concurrent voice and video sessions the network will process are set, in order to prevent resource exhaustion.

Select **Domain Policies → Application Rules** from the left-side menu as shown below. Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the reference configuration, the **sip-trunk** profile was created for IP Office and Verizon Business. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** application to a value slightly larger than the licensed sessions. For example, if licensed for 150 sessions set the values to **200**. The **Maximum Session Per Endpoint** should match the **Maximum Concurrent Sessions**.

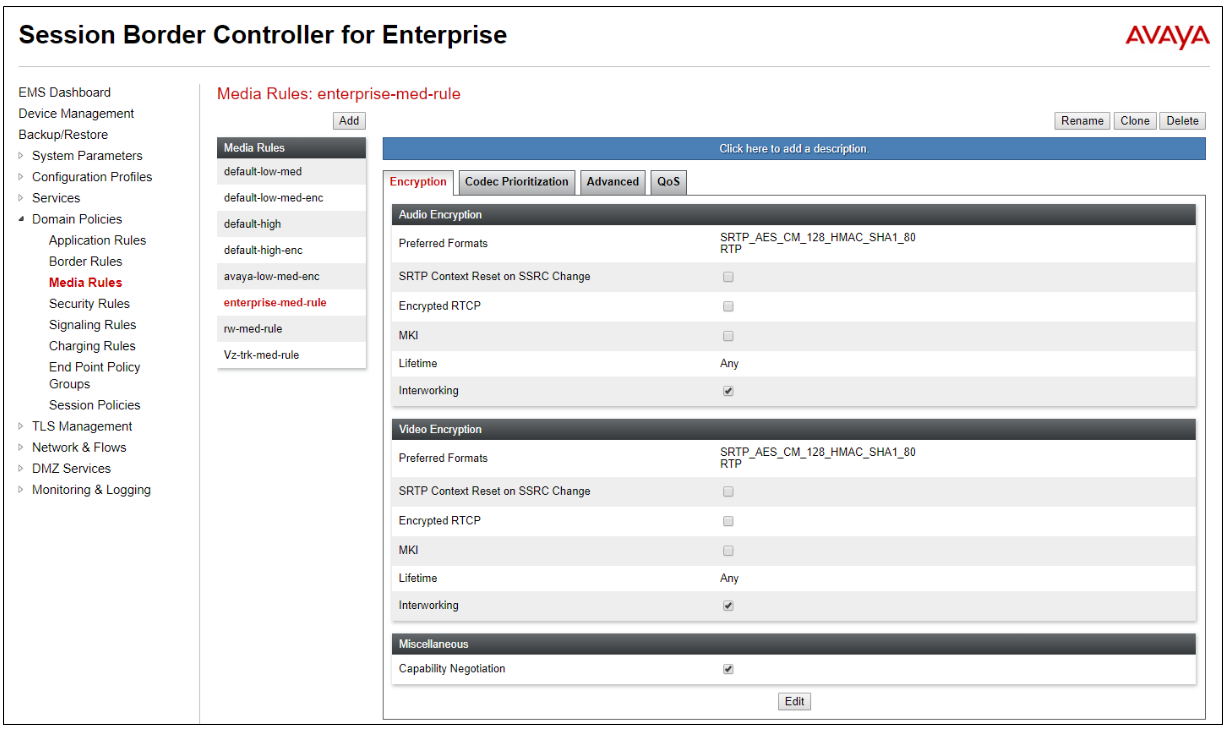


7.11. Media Rules

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

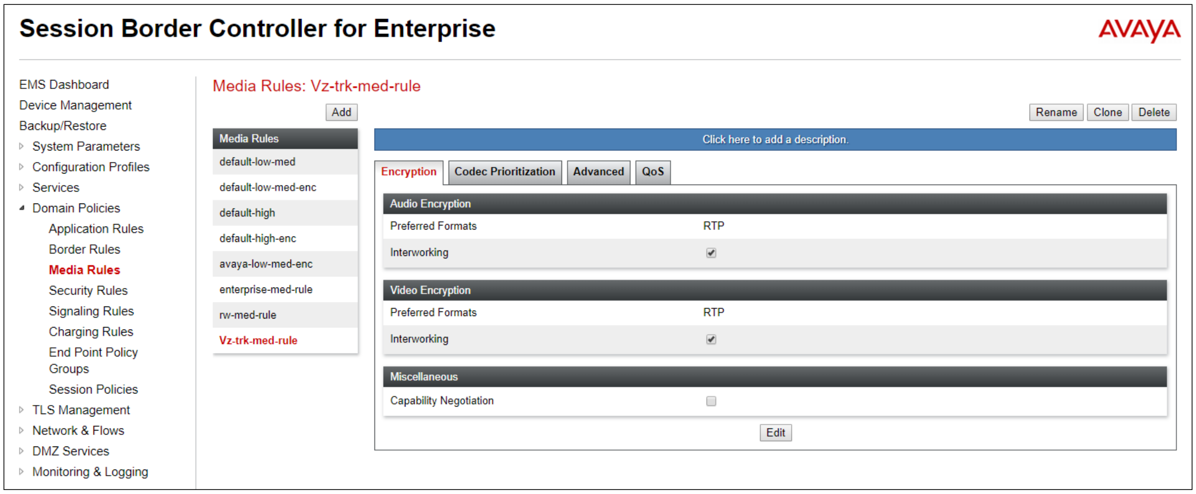
To create a Media Rule for the IP Office, select **Domain Policies → Media Rules** from the left-side menu. In the sample configuration, the default **avaya-low-med-enc** rule was cloned for IP Office, and then modified as shown on the screen below. With the **avaya-low-med-enc** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

The Media Rule **enterprise-med-rule** created for the IP Office is shown below. The **Preferred Formats** are changed to include **SRTP_AES_CM_128_HMAC_SHA1_80** as the first choice and **RTP** as second. In the **Miscellaneous** section, **Capability Negotiation** is checked. All other fields retained their default cloned value.

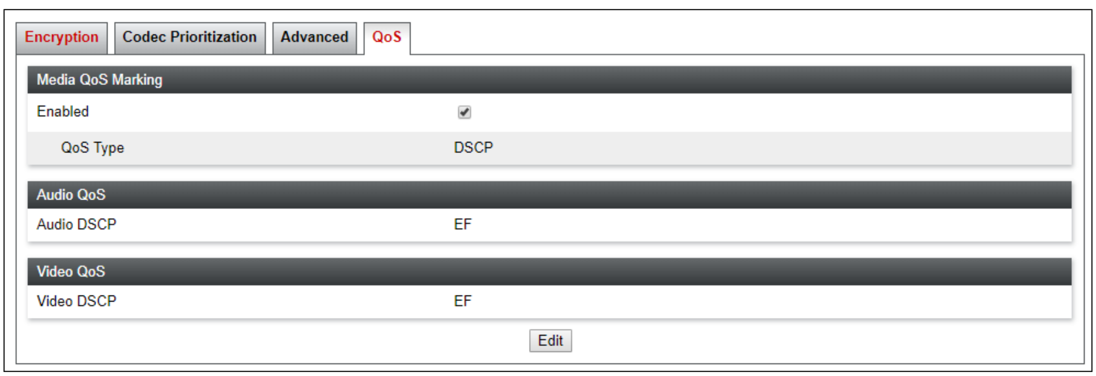


Similarly, a Media Rule is created for Verizon. In this case, the **default-low-med** profile was cloned. With the **default-low-med** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

The Media Rule named **Vz-trk-med-rule**, used for Verizon in the sample configuration is shown below.



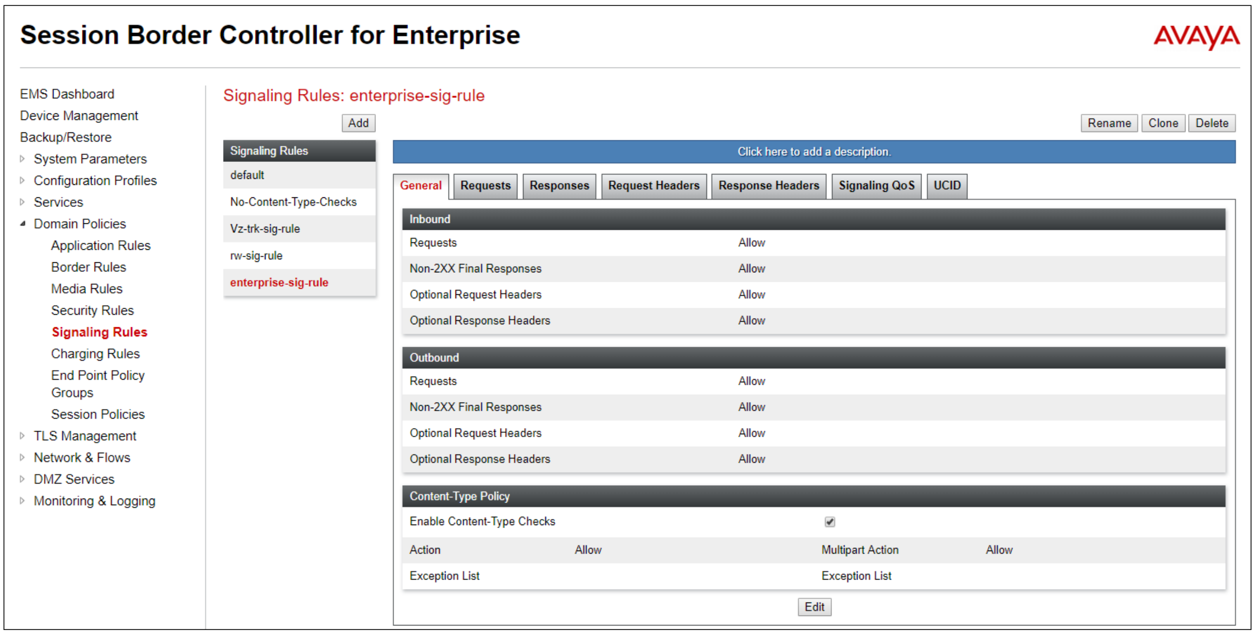
Note the DSCP values **EF** for expedited forwarding (default value) used for Media **QoS,** as specified by Verizon.



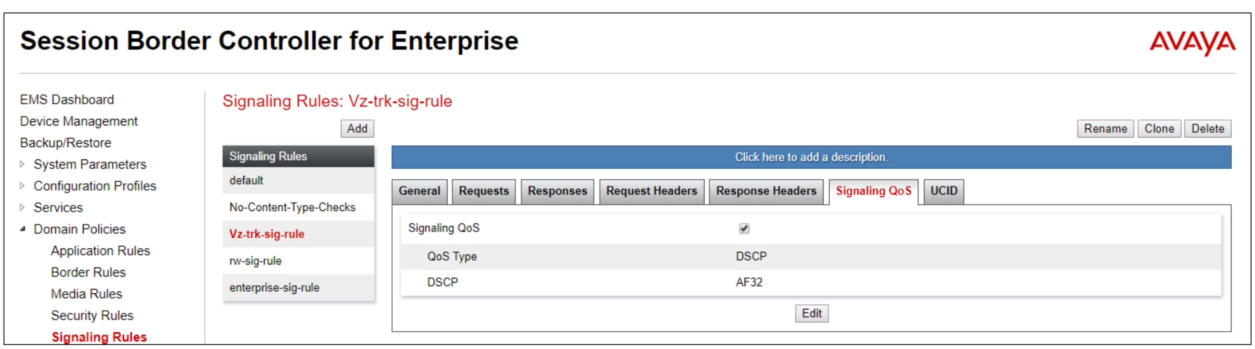
7.12. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. Signaling Rules are also used to define QoS parameters for the SIP signaling packets.

Clone and modify the **default** signaling rule as needed, to add the proper quality of service to the SIP signaling. To clone a signaling rule, navigate to **Domain Policies → Signaling Rules**. With the **default** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown). In the reference configuration, signaling rule **enterprise-sig-rule** is unchanged from the default rule.



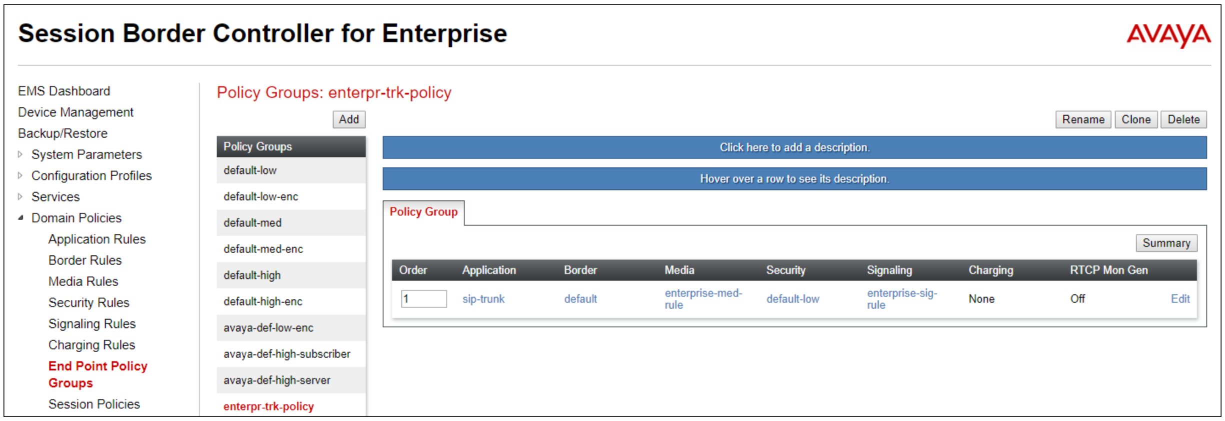
Signaling rule **Vz-trk-sig-rule** was also cloned from the default rule and used for Verizon. The settings for **Signaling QoS** are changed from the default values to **DSCP** value **AF32** for assured forwarding, as specified by Verizon, shown below.



7.13. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 7.14**.

To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add** as shown below. The following screen shows the **enterpr-trk-policy** created for IP Office. The details of the non-default rules chosen are shown in previous sections.



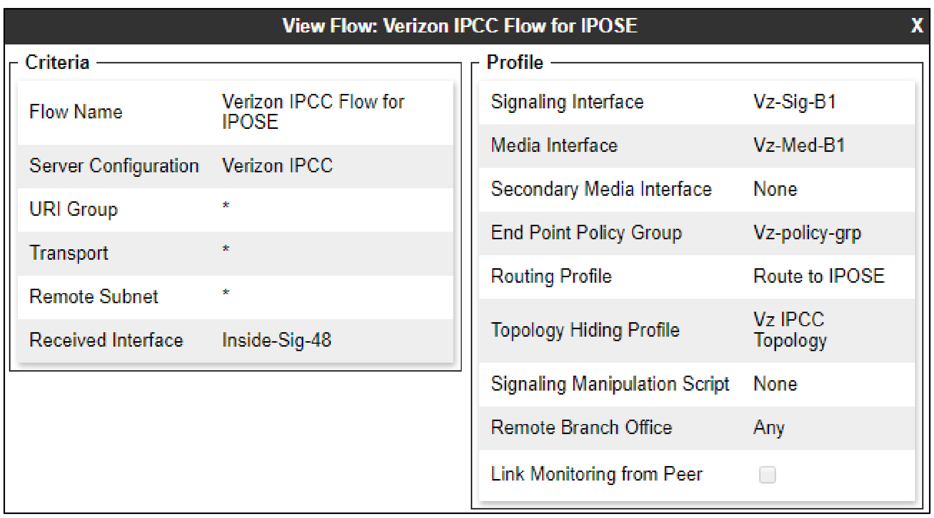
The following screen shows the **Vz-policy-grp** created for Verizon Business IP Trunking service. The details of the non-default rules chosen are shown in previous sections.

7.14. End Point 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 SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow.

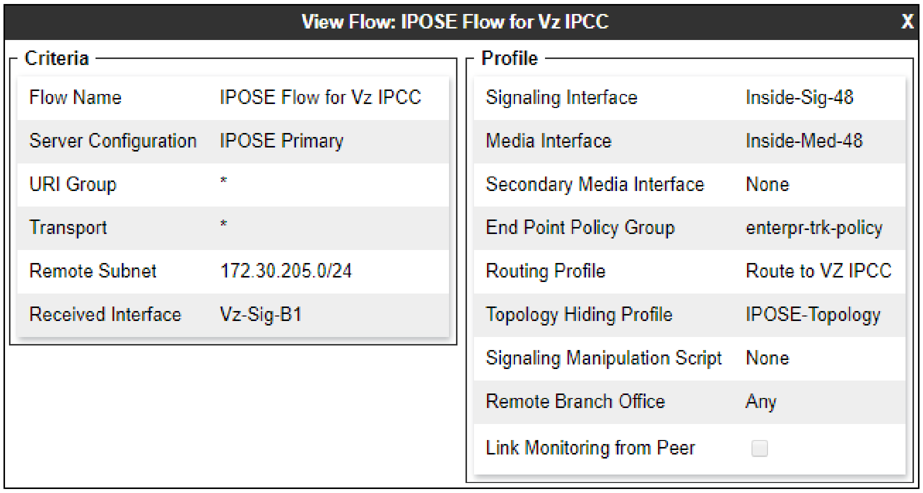
Create a Server Flow for IP Office and Verizon Business IPCC service. To create a Server Flow, navigate to **Networks & Flows → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown).

The following screen shows the flow named **Verizon IPCC Flow for IPOSE** viewed from the reference configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.



Once again, select the **Server Flows** tab and click **Add** (not shown). The following screen shows the flow named **IPOSE Flow for Vz IPCC** viewed from the reference configuration.

This flow uses the interfaces, polices, and profiles defined in previous sections. In addition, the **Remote Subnet** is configured with the Verizon-provided IP address/mask of the subnet for the IPCC service, i.e., **172.30.205.0/24**.



View Flow: IPOSE Flow for Vz IPCC

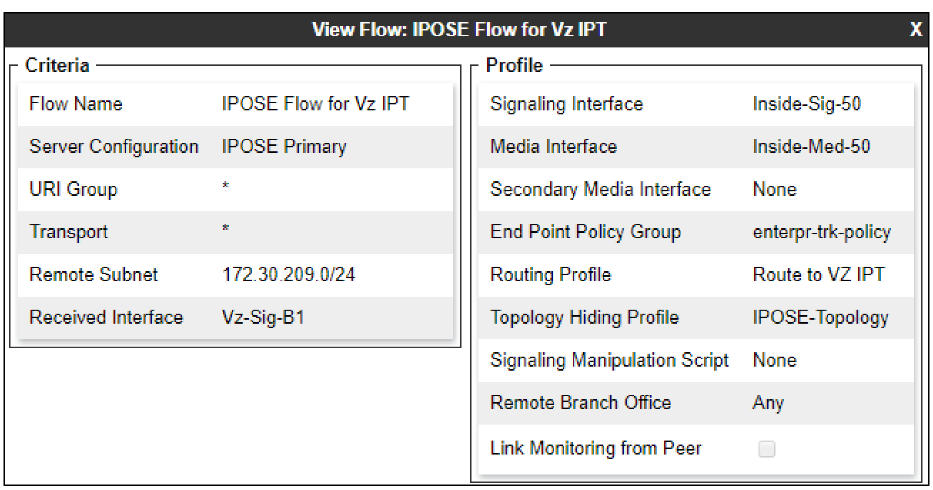
Criteria

Flow Name	IPOSE Flow for Vz IPCC
Server Configuration	IPOSE Primary
URI Group	*
Transport	*
Remote Subnet	172.30.205.0/24
Received Interface	Vz-Sig-B1

Profile

Signaling Interface	Inside-Sig-48
Media Interface	Inside-Med-48
Secondary Media Interface	None
End Point Policy Group	enterpr-trk-policy
Routing Profile	Route to VZ IPCC
Topology Hiding Profile	IPOSE-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	

For illustration, the following screen shows the flow named **IPOSE Flow for Vz IPT** viewed from the reference configuration. This flow was originally created for use with Verizon Business IP Trunk service as shown in [IPT-IPO111SBC81]. Similar to the **IPOSE Flow for Vz IPCC** flow shown above, the **Remote Subnet** is also configured. However, it is configured with the Verizon-provided IP address/mask of the subnet for IP Trunk service, rather than the IPCC service. This is shown here to illustrate how the Avaya SBCE can send SIP traffic out on different internal signaling and media interfaces based on the **Criteria** specified in the flow. In the reference configuration provided, a Verizon Business IP Trunk SIP call from IP address 172.30.209.21 will use internal IP address 10.64.91.50 towards IP Office, while a Verizon Business IPCC SIP call from IP address 172.30.205.55 will use internal IP address 10.64.91.48. This will allow IP Office to have separate unique SIP Line configurations to the Avaya SBCE for each Verizon service.



View Flow: IPOSE Flow for Vz IPT

Criteria

Flow Name	IPOSE Flow for Vz IPT
Server Configuration	IPOSE Primary
URI Group	*
Transport	*
Remote Subnet	172.30.209.0/24
Received Interface	Vz-Sig-B1

Profile

Signaling Interface	Inside-Sig-50
Media Interface	Inside-Med-50
Secondary Media Interface	None
End Point Policy Group	enterpr-trk-policy
Routing Profile	Route to VZ IPT
Topology Hiding Profile	IPOSE-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	

8. Verizon Business Configuration

Information regarding Verizon Business IP Contact Center service offer can be found by contacting a Verizon Business sales representative, or by visiting https://enterprise.verizon.com/products/customer-experience-services/transport-and-intelligent-routing/ip-contact-center/.

The configuration described in these Application Notes was located in the Avaya Solutions and Interoperability Lab. The Verizon Business IP Contact Center service was accessed via a Verizon Private IP (PIP) T1 connection as described in Section 1. Verizon Business provided the necessary service provisioning, which included the domain *adevc.avaya.globalipcom.com* for the Avaya IP Office location.

For service provisioning, Verizon will require the customer IP address of the Avaya Session Border Controller for Enterprise. For the compliance testing, Verizon provided the IP address and port used by the Verizon SBC, as well as the toll-free numbers. This information was used to complete the configuration of the Avaya IP Office and the Avaya Session Border Controller for Enterprise shown in the previous sections.

9. Verification Steps

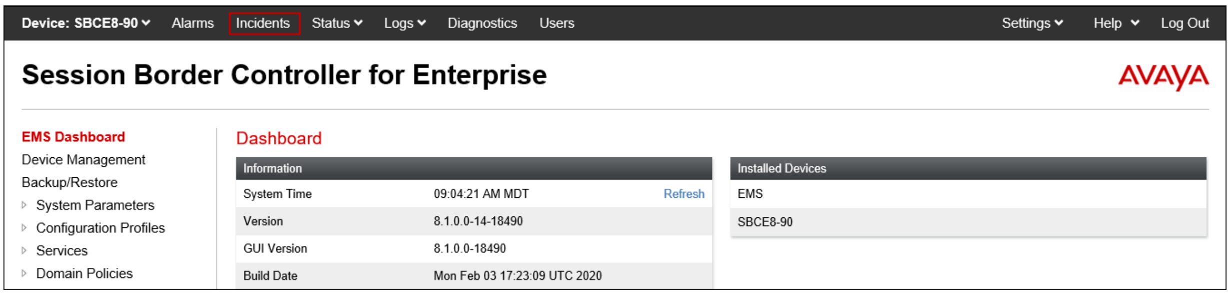
This section provides example verifications of the Avaya configuration with Verizon Business Private IP (PIP) Trunk service.

9.1. Avaya SBCE

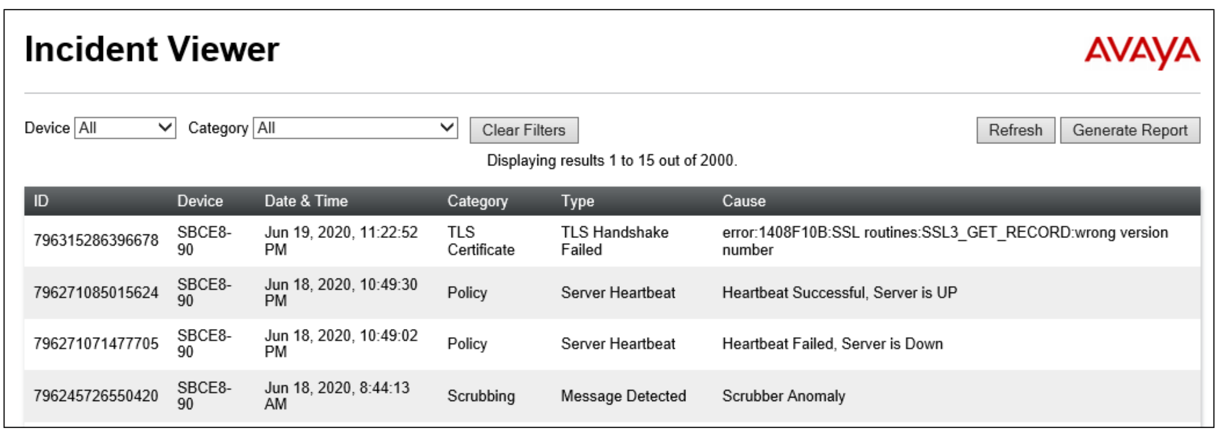
This section provides verification steps that may be performed with the Avaya SBCE.

9.1.1. Incidents

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



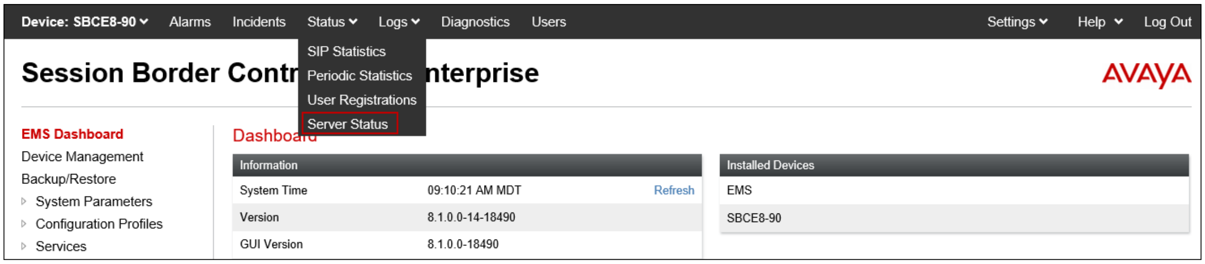
Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures.



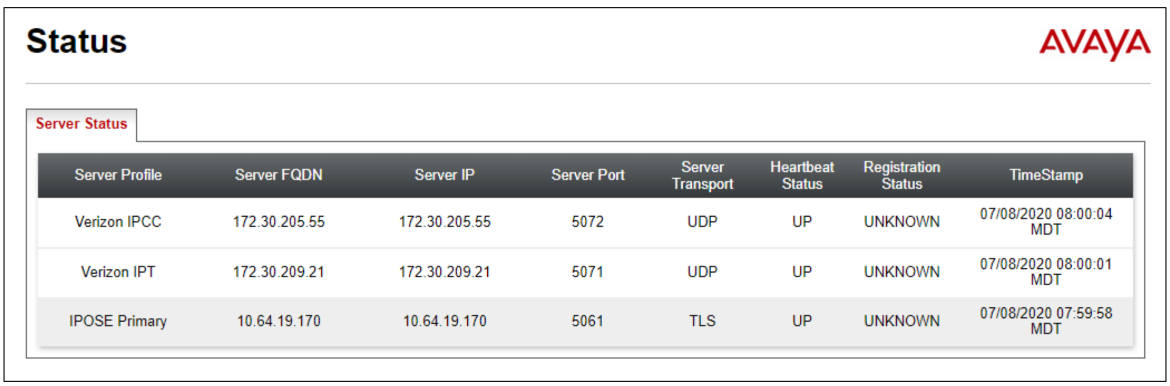
ID	Device	Date & Time	Category	Type	Cause
796315286396678	SBCE8-90	Jun 19, 2020, 11:22:52 PM	TLS Certificate	TLS Handshake Failed	error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number
796271085015624	SBCE8-90	Jun 18, 2020, 10:49:30 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
796271071477705	SBCE8-90	Jun 18, 2020, 10:49:02 PM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
796245726550420	SBCE8-90	Jun 18, 2020, 8:44:13 AM	Scrubbing	Message Detected	Scrubber Anomaly

9.1.2. Server Status

The **Server Status** screen can be accessed from the Avaya SBCE top navigation menu by selecting the **Status** menu, and then **Server Status**.

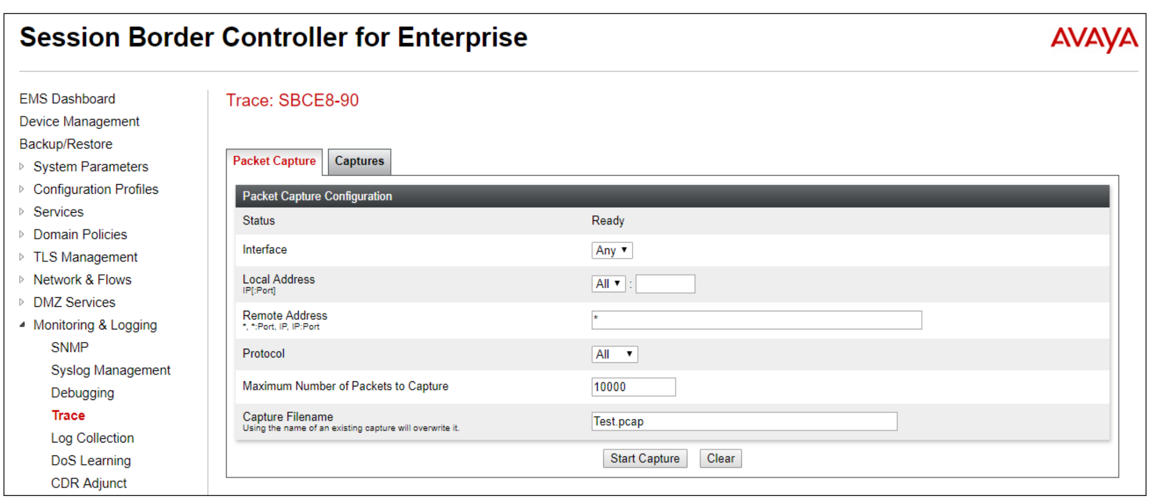


The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Configuration profiles, as configured in **Section 7.7**.

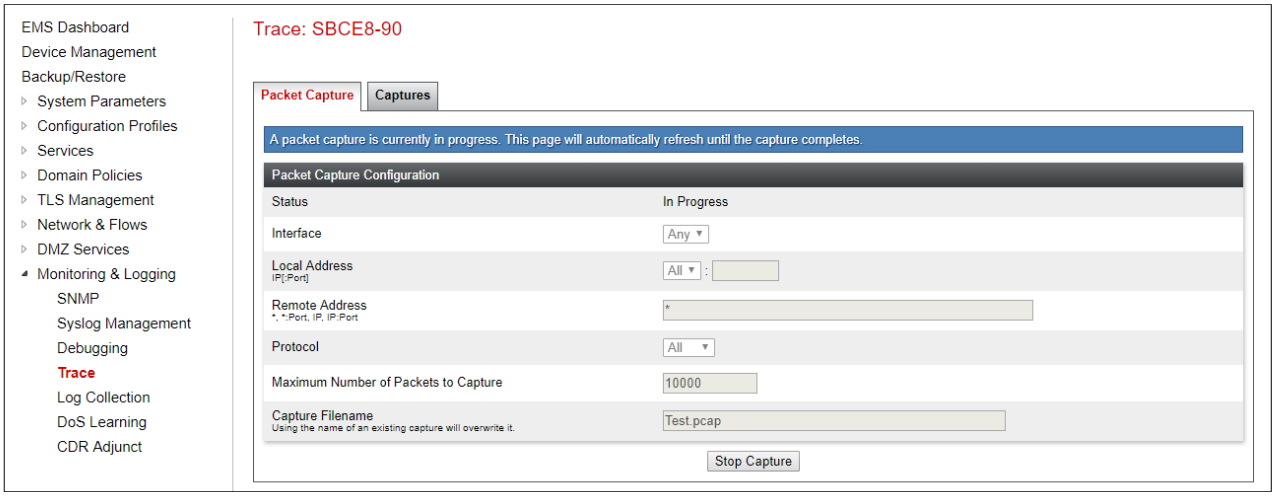


9.1.3. Tracing

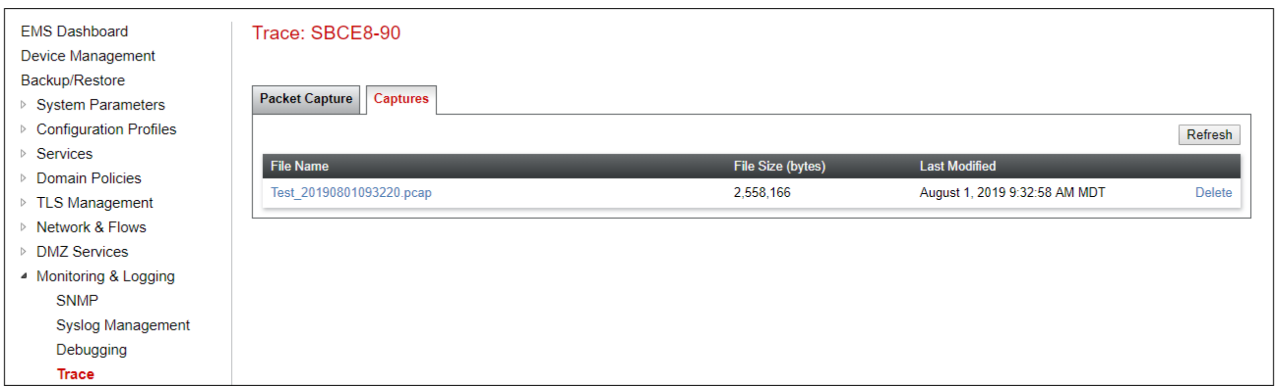
To take a call trace, navigate to **Monitoring & Logging → Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.



When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, click the **Stop Capture** button at the bottom.



Select the **Captures** tab at the top and the capture will be listed; select the **File Name** and choose to open it with an application like Wireshark.

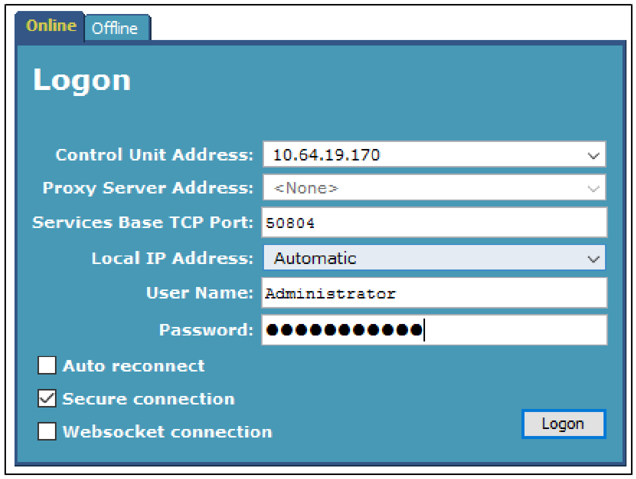


9.2. Avaya IP Office

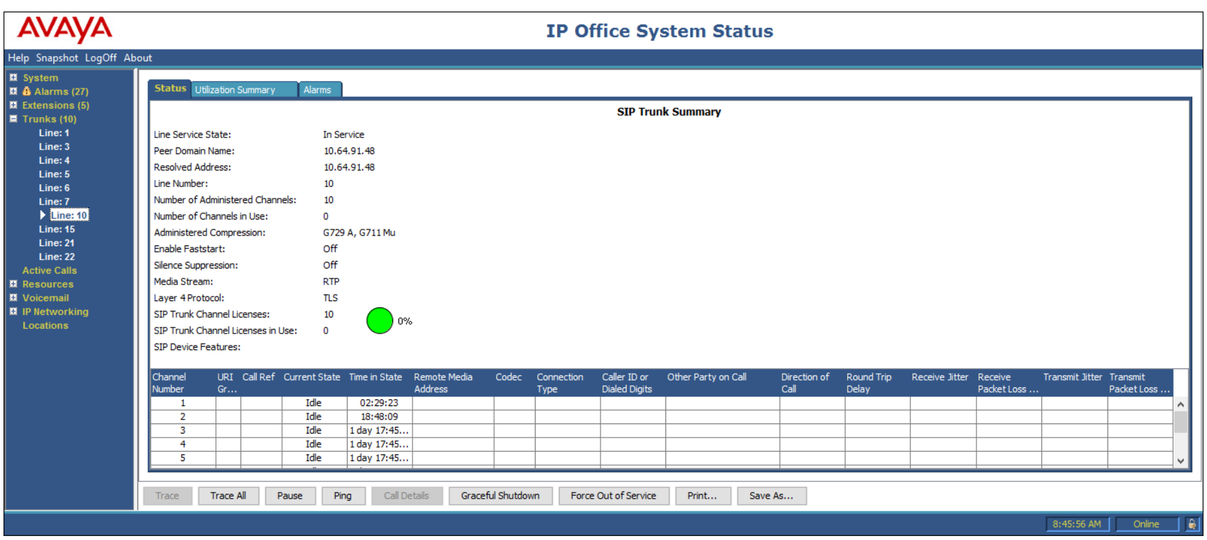
This section provides verification steps that may be performed with the IP Office.

9.2.1. 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.

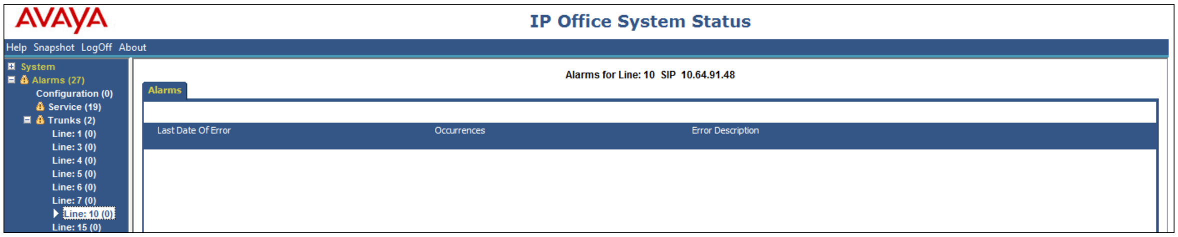


Select the SIP line from the left pane (**Line 10** in the reference configuration). On the **Status** tab in the right pane, verify that the **Current State** is ***Idle*** for each channel (assuming no active calls at present time).



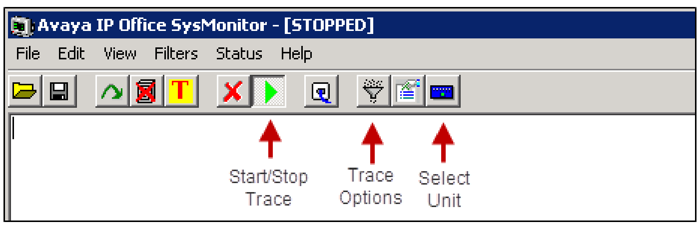
In the lower part of the screen, the **Trace All** button may be pressed to display real time tracing information as calls are made using this SIP Line. The **Ping** button can be used to ping the other end of the SIP trunk (e.g., Avaya SBCE).

Select the **Alarms** tab and verify that no alarms are active on the SIP line.

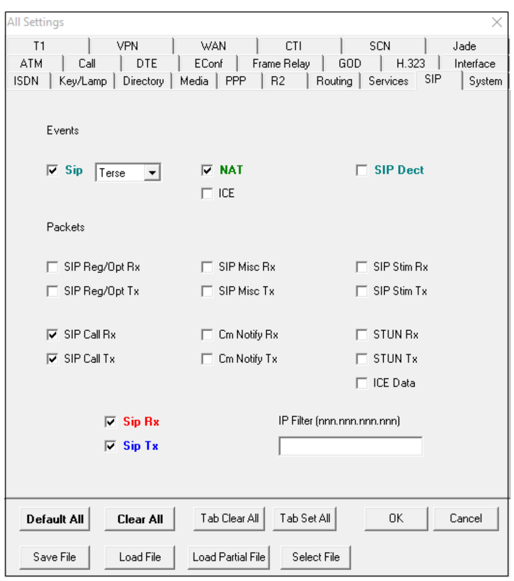


9.2.2. System Monitor

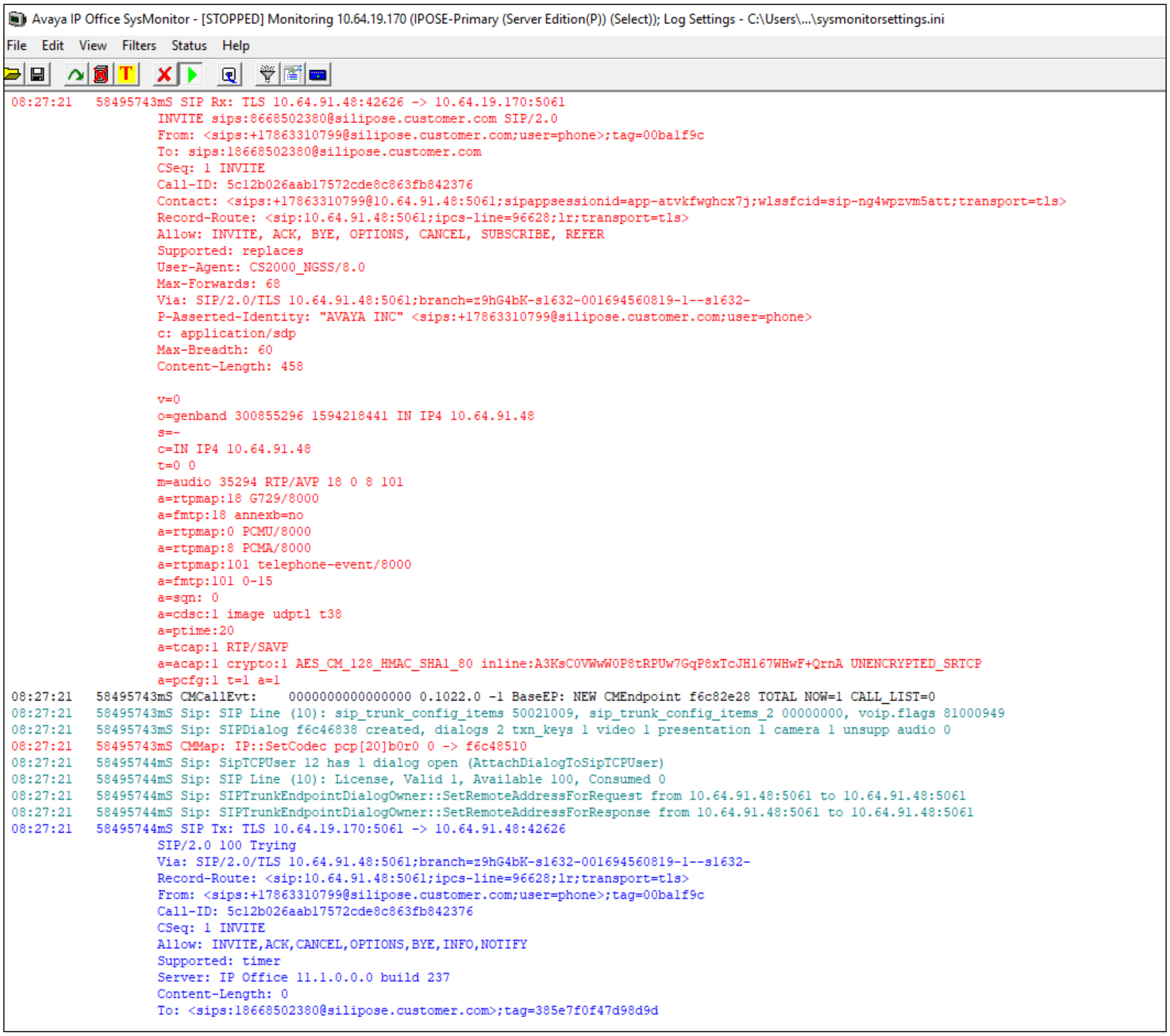
The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP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



As an example, the following shows a portion of the monitoring window for an inbound call to Verizon IP Toll Free number 1-866-850-2380. Details of the SIP INVITE message sent by Verizon are shown below. This information matches the configuration in these Application Notes and is not intended to be prescriptive. The intent is to illustrate the INVITE sent by Verizon in the reference configuration, along with the means to retrieve this type of trace information from IP Office.


Avaya IP Office SysMonitor - [STOPPED] Monitoring 10.64.19.170 (IPOSE-Primary (Server Edition(P)) (Select)); Log Settings - C:\Users\...\sysmonitorsettings.ini

File Edit View Filters Status Help

```
08:27:21   58495743mS SIP Rx: TLS 10.64.91.48:42626 -> 10.64.19.170:5061
                INVITE sips:8668502380@silipose.customer.com SIP/2.0
                From: <sips:+17863310799@silipose.customer.com;user=phone>;tag=00ba1f9c
                To: sips:18668502380@silipose.customer.com
                CSeq: 1 INVITE
                Call-ID: 5c12b026aab17572cde8c863fb842376
                Contact: <sips:+17863310799@10.64.91.48:5061;sipappsessionid=app-atvkfwghcx7j;wlssfcid=sip-ng4wpzvm5att;transport=tls>
                Record-Route: <sip:10.64.91.48:5061;ipcs-line=96628;lr;transport=tls>
                Allow: INVITE, ACK, BYE, OPTIONS, CANCEL, SUBSCRIBE, REFER
                Supported: replaces
                User-Agent: CS2000_NGSS/8.0
                Max-Forwards: 68
                Via: SIP/2.0/TLS 10.64.91.48:5061;branch=z9hG4bK-s1632-001694560819-1--s1632-
                P-Asserted-Identity: "AVAYA INC" <sips:+17863310799@silipose.customer.com;user=phone>
                c: application/sdp
                Max-Breadth: 60
                Content-Length: 458

                v=0
                o=genband 300855296 1594218441 IN IP4 10.64.91.48
                s=-
                c=IN IP4 10.64.91.48
                t=0 0
                m=audio 35294 RTP/AVP 18 0 8 101
                a=rtpmap:18 G729/8000
                a=fmtp:18 annexb=no
                a=rtpmap:0 PCMU/8000
                a=rtpmap:8 PCMA/8000
                a=rtpmap:101 telephone-event/8000
                a=fmtp:101 0-15
                a=sqn: 0
                a=cdsc:1 image udptl t38
                a=ptime:20
                a=tcap:1 RTP/SAVP
                a=acap:1 crypto:1 AES_CM_128_HMAC_SHA1_80 inline:A3KsC0VWwW0P8tRPUw7GqP8xTcJH167WHwF+QrnA UNENCRYPTED_SRTCP
                a=pcfg:1 t=1 a=1
08:27:21   58495743mS CMCallEvt:    0000000000000000 0.1022.0 -1 BaseEP: NEW CMEndpoint f6c82e28 TOTAL NOW=1 CALL_LIST=0
08:27:21   58495743mS Sip: SIP Line (10): sip_trunk_config_items 50021009, sip_trunk_config_items_2 00000000, voip.flags 81000949
08:27:21   58495743mS Sip: SIPDialog f6c46838 created, dialogs 2 txn_keys 1 video 1 presentation 1 camera 1 unsupp audio 0
08:27:21   58495743mS CMMap: IP::SetCodec pcp[20]b0r0 0 -> f6c48510
08:27:21   58495744mS Sip: SipTCPUser 12 has 1 dialog open (AttachDialogToSipTCPUser)
08:27:21   58495744mS Sip: SIP Line (10): License, Valid 1, Available 100, Consumed 0
08:27:21   58495744mS Sip: SIPTrunkEndpointDialogOwner::SetRemoteAddressForRequest from 10.64.91.48:5061 to 10.64.91.48:5061
08:27:21   58495744mS Sip: SIPTrunkEndpointDialogOwner::SetRemoteAddressForResponse from 10.64.91.48:5061 to 10.64.91.48:5061
08:27:21   58495744mS SIP Tx: TLS 10.64.19.170:5061 -> 10.64.91.48:42626
                SIP/2.0 100 Trying
                Via: SIP/2.0/TLS 10.64.91.48:5061;branch=z9hG4bK-s1632-001694560819-1--s1632-
                Record-Route: <sip:10.64.91.48:5061;ipcs-line=96628;lr;transport=tls>
                From: <sips:+17863310799@silipose.customer.com;user=phone>;tag=00ba1f9c
                Call-ID: 5c12b026aab17572cde8c863fb842376
                CSeq: 1 INVITE
                Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY
                Supported: timer
                Server: IP Office 11.1.0.0.0 build 237
                Content-Length: 0
                To: <sips:18668502380@silipose.customer.com>;tag=385e7f0f47d98d9d
```

10. Conclusion

IP Office is a highly modular IP telephone system designed to meet the needs of home offices, standalone businesses, and networked offices for small and medium enterprises.

These Application Notes demonstrated how IP Office Release 11.1 with Avaya Session Border Controller for Enterprise Release 8.1 can be successfully combined with a Verizon Business IP Contact Center VoIP Inbound Service connection to enable a business to receive toll-free calls. Utilizing this solution, IP Office customers can leverage the operational efficiencies and cost savings associated with SIP trunking while gaining the advanced technical features provided through the marriage of best of breed technologies from Avaya and Verizon.

11. Additional References

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

[1] *IP Office, Deploying IP Office Server Edition*, Release 11.1, Issue 14, April 2020.
[2] *IP Office™ Platform 11.0, Deploying Avaya IP Office Servers as Virtual Machines*, June 2020.
[3] *IP Office™ Platform 11.1, Deploying an IP500 V2 IP Office Essential Edition,* June 2020.
[4] *Administering Avaya IP Office™ Platform with Manager,* Release 11.1, Issue 2, May 2020.
[5] *Administering Avaya IP Office™ Platform with Web Manager*, Release 11.1, Issue 2, May 2020.
[6] *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac and Windows*, Release 3.8, Issue 1, March 2020.
[7] *Using Avaya IX™ Workplace Client for Android, iOS, Mac and Windows*, Release 3.8, Issue 1, March 2020.
[8] *IP Office Platform 11.1, IP Office SIP Phones with ASBCE, Issue 04c*, April 2020.
[9] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 8.1, April 2020.
[10] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1, Issue 2, April 2020.
[11] *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/

The Application Notes referenced below correspond to the formal compliance testing by Avaya and Verizon Business for IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 8.1 with Verizon IP Trunk Service Suite:

[IPT-IPO111SBC81] Application Notes for SIP Trunking Using Verizon Business IP Trunk SIP Trunk Service with Avaya IP Office Release 11.0 and Avaya Session Border Controller for Enterprise Release 8.0.1, Issue 1.0

Information in the following Verizon documents was also used for these Application Notes. Contact a Verizon Business Account Representative for additional information.

- [VZ-Test-Plan] Test Suite for CPE IP Trunking Interoperability v1.6
- [VZ-Spec] Verizon Business IPCC Trunk Interface Network Interface Specification, Document Version 2.2.1.9

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.