Avaya Solution & Interoperability Test Lab

Application Notes for Avaya IP Office Release 11.1 and Avaya Session Border Controller for Enterprise 8.1 with AT&T IP Flexible Reach - Enhanced Features - Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya IP Office 11.1 and Avaya Session Border Controller for Enterprise 8.1 with the AT&T IP Flexible Reach - Enhanced Features service using AVPN or ADI/PNT transport connections.

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 AT&T IP Flexible Reach - Enhanced Features service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long-distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

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

AT&T is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

©2020 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction ... 4
2. General Test Approach and Test Results ... 5
   2.1. Interoperability Compliance Testing ... 6
   2.2. Test Results ... 7
   2.3. Support ... 8
3. Reference Configuration ... 9
   3.1. Illustrative Configuration Information ... 11
   3.2. Call Flows ... 12
      3.2.1. Inbound ... 12
      3.2.2. Outbound ... 13
      3.2.3. Call Forward ... 14
      3.2.4. Coverage to Voicemail ... 15
4. Equipment and Software Validated ... 16
5. Avaya IP Office Primary Server Configuration ... 17
   5.1. Licensing ... 19
   5.2. TLS Management ... 20
   5.3. System Settings ... 21
      5.3.1. LAN1 Tab ... 21
      5.3.2. Voicemail Tab ... 24
      5.3.3. Telephony Tab ... 25
      5.3.4. VoIP Tab ... 26
   5.4. IP Route ... 28
   5.5. SIP Line ... 29
      5.5.1. Creating a SIP Line from an XML Template ... 30
      5.5.2. SIP Line – SIP Line tab ... 31
      5.5.3. SIP Line - Transport Tab ... 32
      5.5.4. SIP Line – Call Details tab ... 33
      5.5.5. SIP Line - VoIP tab ... 34
      5.5.6. SIP Line – SIP Advanced Tab ... 35
   5.6. IP Office Line ... 36
   5.7. Incoming Call Route ... 37
   5.8. Short Codes ... 38
   5.9. Automatic Route Selection (ARS) ... 39
   5.10. Outbound Calling Party Information ... 41
      5.10.1. Short Code- User ... 41
      5.10.2. Short Code - ARS ... 42
   5.11. Save IP Office Primary Server Configuration ... 43
6. Avaya IP Office Expansion System Configuration ... 44
   6.1. Expansion System - Physical Hardware ... 44
   6.2. Expansion System - LAN Settings ... 45
   6.3. Expansion System - IP Route ... 45
   6.4. Expansion System - IP Office Line ... 46
   6.5. Expansion System - Short Codes ... 47

©2020 Avaya Inc. All Rights Reserved.

6.6. Expansion System - Automatic Route Selection – ARS 48
6.7. Save IP Office Expansion System Configuration 48
7. Configure Avaya Session Border Controller for Enterprise 49
7.1. Device Management – Status 50
7.2. TLS Management 52
7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise 52
7.2.2. Server Profiles 53
7.2.3. Client Profiles 55
7.3. Network Management 57
7.4. Media Interfaces 58
7.5. Signaling Interfaces 59
7.6. Server Interworking Profiles 60
7.6.1. Server Interworking Profile – IP Office 60
7.6.2. Server Interworking Profile – AT&T 61
7.7. SIP Servers Profiles 63
7.7.1. SIP Server Profile – IP Office 63
7.7.2. SIP Server Profile – AT&T 65
7.8. Routing Profiles 68
7.8.1. Routing Profile – IP Office 68
7.8.2. Routing Profile – AT&T 69
7.9. Topology Hiding Profiles 70
7.10. Application Rules 71
7.11. Media Rules 72
7.12. Signaling Rules 74
7.13. Endpoint Policy Groups 75
7.14. Advanced Options 76
7.15. End Point Flows - Server Flow 77
8. AT&T IP Flexible Reach – Enhanced Features Configuration 79
9. Verification Steps 79
9.1. Avaya SBCE 79
9.1.1. Incidents 79
9.1.2. Server Status 80
9.1.3. Tracing 80
9.2. Avaya IP Office 82
9.2.1. System Status 82
9.2.2. System Monitor 83
10. Conclusion 84
11. Additional References 84

©2020 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps for configuring Avaya IP Office release 11.1 (Avaya IP Office) and the Avaya Session Border Controller for Enterprise release 8.1 (Avaya SBCE) with the AT&T IP Flexible Reach - Enhanced Features service using AT&T Virtual Private Network (AVPN) or AT&T Dedicated Internet Service (ADI/PNT) transport connections.

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

The Avaya Session Border Controller for Enterprise is the point of connection between Avaya IP Office and the AT&T IP Flexible Reach - Enhanced Features service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling and media for interoperability.

The AT&T IP Flexible Reach - Enhanced Features service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach - Enhanced Features service allows enterprises in the U.S.A. to place outbound local and long-distance calls receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites. The AT&T IP Flexible Reach - Enhanced Features service utilizes AVPN[1] or ADI/PNT[2] transport service.

Note – The AT&T IP Flexible Reach - Enhanced Features service will be referred to as AT&T IPFR-EF in the remainder of this document.

[1] AVPN uses compressed RTP (cRTP).
[2].ADI/PNT does not support cRTP.

©2020 Avaya Inc. All Rights Reserved.

2. General Test Approach and Test Results

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.

The interoperability compliance testing focused on verifying inbound and outbound call flows between IPFR-EF and the Customer Premises Equipment (CPE) containing the Avaya SBCE, and Avaya IP Office (see **Section 3.2** for call flow examples).

The test environment described in these Application Notes consisted of:

- A simulated enterprise with the Avaya SBCE, Avaya IP Office, Avaya SIP, H.323, digital and analog endpoints, as well as fax machine emulators (Ventafax).
- An IPFR-EF production circuit, to which the simulated enterprise was connected via AVPN transport.

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 the AT&T Flexible Reach service did not include use of any specific encryption features as requested by AT&T.

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

©2020 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the IPFR-EF network. Calls were made to/from the PSTN across the IPFR-EF network, to/from the CPE.

The following SIP trunking VoIP features were tested with the IPFR-EF service:

- Incoming and outgoing voice calls between PSTN, the IPFR-EF service, the Avaya SBCE, and Avaya IP Office, utilizing Avaya SIP, H.323, digital, and analog endpoints.
- Additional PSTN numbering plans (e.g., operator assist, toll-free and International).
- Requests for privacy (i.e., caller anonymity) for Avaya IP Office outbound calls to the PSTN, as well as privacy requests for inbound calls from the PSTN to Avaya IP Office users.
- SIP OPTIONS messages used to monitor the health of the SIP trunk from both Avaya IP Office and AT&T.
- Incoming and outgoing calls using the G.729A and G.711 ULAW codecs.
- Call redirection with Diversion Header.
- Long duration calls.
- DTMF transmission (RFC 2833) for successful PSTN and Avaya IP Office menu navigation.
- Telephony features such as hold, transfer, and conference.
- Avaya IP Office Mobile twinning to a mobile phone when the associated Avaya IP Office extension is called, as well as Mobility features such as Mobile Callback and Mobile Call Control.
- Avaya Remote Worker configuration (Avaya Workplace Client for Windows) via Avaya SBCE.
- Inbound/Outbound fax calls using T.38 or G.711.
- Failover test between primary and secondary AT&T Border Elements.
- AT&T IPFR-EF service features such as:
    - Simultaneous Ring
    - Sequential Ring
    - Call Forward – Always
    - Call Forward – Busy
    - Call Forward – Ring No Answer
- Blind and Attended transfers utilizing SIP REFER messaging.

©2020 Avaya Inc. All Rights Reserved.

2.2. Test Results

The test objectives stated in **Section 2.1**, with limitations as noted below, were verified.

1. **Avaya IP Office only supports a packet size (ptime) of 20 msecs –** AT&T recommends that for maximum customer bandwidth utilization, a ptime value of 30 should be specified. Avaya IP Office only supports a ptime value of 20 msecs, which was the value negotiated on inbound and outbound calls to AT&T. No issues were observed during testing as a result.

2. **Fax Support**
   - Inbound T.38 fax calls fail when the CPE fax machine is a Super G3 (SG3) fax device. Avaya IP Office may not send a re-INVITE to renegotiate to T.38 for inbound fax calls in cases where both the PSTN and CPE fax devices support Super Group 3 (SG3) speeds. If the SG3 connection is fully established at the beginning of the call, the CPE fax device may not negotiate down to G3 speeds and IP Office will not detect the G3 tones necessary for T.38.
   - Outbound G.711 fax calls failed during the compliance test. After the initial voice setup at G.729A, the Avaya SBCE failed to forward the G.711 re-INVITE arriving from AT&T to the private side. This issue is currently under investigation by the Avaya SBCE development team.
   - T.38 should be the preferred method for fax. If the CPE fax device supports SG3 speeds (33600 bps), a good practice is to disable SG3 on the CPE fax device, if possible.

3. **SIP OPTIONS** – AT&T IPFR service is configured to send SIP OPTIONS messages with Max-Forwards header equal to 0. This is done by design by AT&T. Avaya SBCE responded correctly with "483 Too Many Hops". On SIP OPTIONS sent from the Avaya SBCE to the network, AT&T responded with "405 Method Not Allowed". In both cases, AT&T considers these as acceptable responses to keep the trunk in service.

4. **Emergency 911/E911 Services Limitations and Restrictions** – Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) documented in these Application Notes will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer's responsibility to ensure proper operation with the equipment/software vendor.

   While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when the E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at http://new.serviceguide.att.com. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please

©2020 Avaya Inc. All Rights Reserved.

review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

2.3. Support

For more information on the AT&T IP Flexible Reach service visit: https://www.business.att.com/products/sip-trunking.html. AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

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.

©2020 Avaya Inc. All Rights Reserved.

3. Reference Configuration

The reference configuration used in these Application Notes is shown in **Figure 1** below and consists of the following components:

- Avaya IP Office provides the voice communications services for the enterprise. In the reference configuration, Avaya IP Office runs on the Avaya IP Office Server Edition platform. Note that this solution is extensible to deployments using the standalone IP500 V2 platform as well.
- In the sample configuration, the Primary server runs the Avaya IP Office Server Edition Linux software. Avaya Voicemail Pro runs as a service on the Primary Server. The LAN1 port of the Primary Server is connected to the enterprise LAN. The LAN2 port was not used.
- The Expansion System (V2) is used for the support of digital, analog and additional IP stations. It consists of an Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module). The LAN1 port of the Avaya IP Office IP500V2 is connected to the enterprise LAN, while the LAN2 port was not used.
- Avaya endpoints are represented with an Avaya 9608 H.323 Deskphone, Avaya J129 and J169 SIP Deskphones, an Avaya 1140E SIP Deskphone, an Avaya 9508 Digital Deskphone, as well as Avaya Equinox for Windows (SIP) sofphone. Fax endpoints are represented by PCs running Ventafax emulation software connected by modem to an Avaya IP Office analog port.
- Voicemail Pro (running on the Primary server) provided the voice messaging capabilities in the reference configuration. This solution is extensible to the Avaya IP Office embedded voice mail as well.
- In the reference configuration, Avaya IP Office interface “LAN 1” is connected to the private CPE network. The “LAN 2” interface was not used.
- Avaya Session Border Controller for Enterprise (Avaya SBCE) running on VMware platform. This solution is extensible to other Avaya Session Border Controller for Enterprise platforms as well.
- TLS/5061 is the recommended transport protocol/port to use on the Avaya IP Office LAN1 connection to the Avaya SBCE A1 interface. However, TCP/5060 may be used for this connection if desired.
- The AT&T IPFR-EF service requires the following SIP trunk network settings between the Avaya SBCE B2 (SIP Trunk) interface and the IPFR-EF Border Element:
    - UDP transport using port 5060
    - RTP port ranges 16384-32767
- AT&T provided the inbound and outbound access numbers (DID and DNIS) used in the reference configuration. Note that the IPFR-EF service may deliver 10 or 7 digits in the SIP Invite R-URI depending on the circuit order provisioning. In the reference configuration the IPFR-EF service delivered 10 digits.
- The Avaya IP Office and the Avaya SBCE used in the reference configuration were deployed using the following configuration.
    - IP Office LAN1 interface connected to the CPE private network.
    - Avaya SBCE A1 interface connected to the CPE private network.
    - Avaya SBCE B2 interface connected to the AT&T IPFR-EF network router.

©2020 Avaya Inc. All Rights Reserved.

- An Avaya Remote Worker endpoint (Avaya Workplace Client for Windows) was used in the reference configuration. The Remote Worker endpoint resides on the public side of an Avaya SBCE (via a TLS connection), and registers/communicates with IP Office as though it was an endpoint residing in the private CPE space.

Note – The configuration of the Remote Worker environment is beyond the scope of this document. Refer to [**7**] on the **Additional References** section for information on Remote Worker deployments.

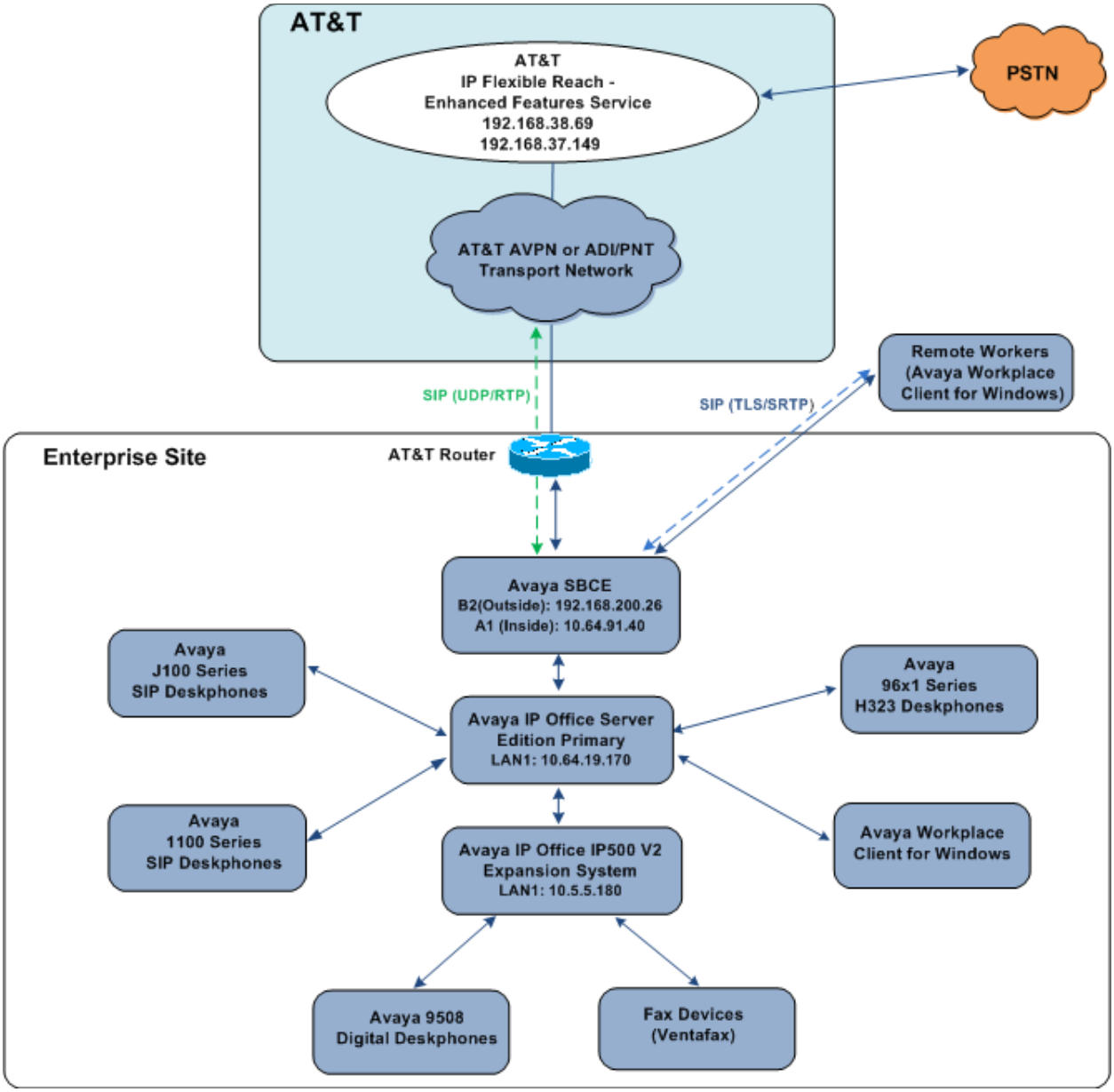


Figure 1: Test Configuration

©2020 Avaya Inc. All Rights Reserved.

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes and are for illustrative purposes only. Customers must obtain and use the values based on their own specific configurations.

Note – For security reasons, public IP addresses used in the reference configuration for the Avaya SBCE and the AT&T Border Elements (BEs), located in the AT&T IPFR-EF network, are not included in this document. However, as placeholders in the following configuration sections, the IP addresses **192.168.200.26** (Avaya SBCE "Outside" interface B2), and **192.168.38.69 /192.168.37.149** (AT&T BE IP addresses), are specified. In addition, AT&T DID/DNIS numbers shown in this document are examples as well. AT&T Customer Care will provide the actual Border Element IP addresses and DID/DNIS numbers as part of the IPFR-EF provisioning process.

Component	Illustrative Value in these Application Notes
Avaya IP Office	
Primary Server, LAN1 interface	10.64.19.170
Expansion System, LAN1 Interface	10.5.5.180
Avaya SBCE	
"Inside Interface", A1	10.64.91.40
"Outside" Interface, B2	192.168.200.26
AT&T IPFR-EF Service	
Border Element IP Address	192.168.38.69 & 192.168.37.149

Table 1: Illustrative Values Used in these Application Notes

©2020 Avaya Inc. All Rights Reserved.

3.2. Call Flows

To understand how inbound and outbound AT&T IPFR-EF service calls are handled by Avaya IP Office, four basic call flows are described in this section.

3.2.1. Inbound

The first call scenario illustrated in the figure below is an inbound AT&T IPFR-EF service call that arrives on Avaya IP Office, which in turn routes the call to a hunt group, phone or a fax endpoint.

1. A PSTN phone originates a call to an IPFR-EF service number.
2. The PSTN routes the call to the AT&T IPFR-EF service network.
3. The AT&T IPFR-EF service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any specified SIP header modifications, and routes the call to Avaya IP Office.
5. Avaya IP Office applies any necessary digit manipulations based upon the DID and routes the call to a hunt group, phone or a fax endpoint.

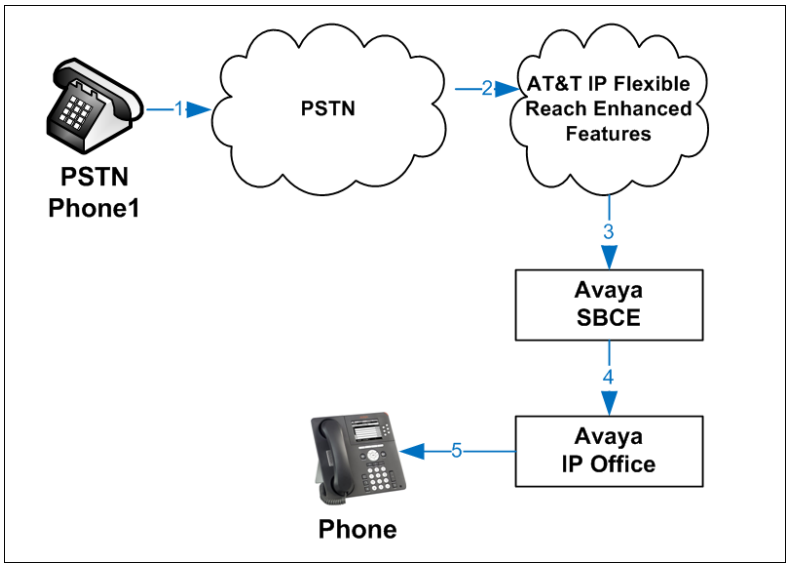


Figure 2: Inbound AT&T IPFR-EF Call

©2020 Avaya Inc. All Rights Reserved.

3.2.2. Outbound

The second call scenario illustrated in the figure below is an outbound call initiated on Avaya IP Office for delivery to AT&T IPFR-EF service.

1. An Avaya IP Office phone or fax endpoint originates a call to an AT&T IPFR-EF service number for delivery to PSTN.
2. Avaya IP Office applies any necessary origination treatment (verifying permissions, determining the proper route, selecting the outgoing trunk, etc.) and sends the call to the Avaya SBCE.
3. The Avaya SBCE performs SIP Network Address Translation (NAT) and any specified SIP header modifications, and routes the call to the AT&T IPFR-EF service.
4. The AT&T IPFR-EF service delivers the call to PSTN.
5. PSTN delivers the call to a phone or fax endpoint.

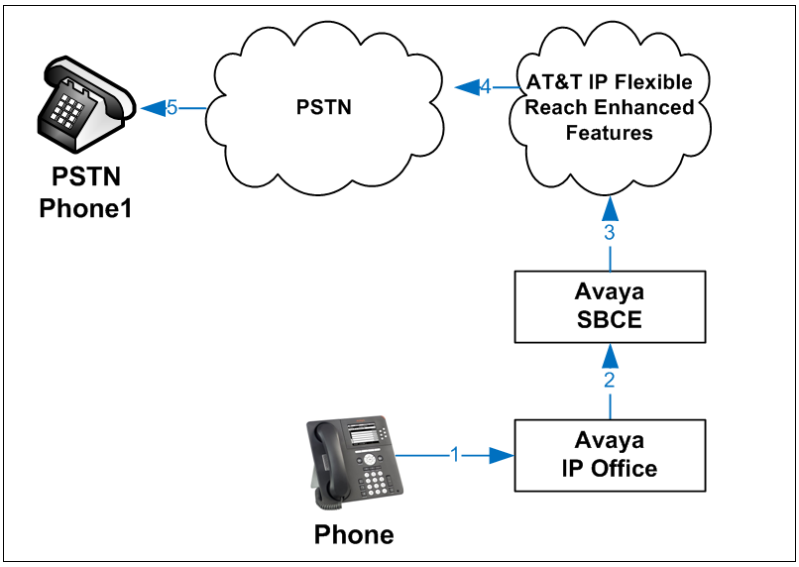


Figure 3: Outbound Call to AT&T IPFR-EF

©2020 Avaya Inc. All Rights Reserved.

3.2.3. Call Forward

The third call scenario illustrated in the figure below is an inbound AT&T IPFR-EF service call destined for an Avaya IP Office station that has set Call Forwarding to an alternate destination. Without answering the call, Avaya IP Office redirects the call back to the AT&T IPFR-EF service for routing to the alternate destination.

Note – AT&T requires the Diversion header be used when a call is redirected to AT&T IPFR-EF service (See **Section 5.5.4**).

1. Same as the first call scenario in **Section 3.2.1**.
2. Because the Avaya IP Office phone has set Call Forward to another AT&T IPFR-EF service number, Avaya IP Office initiates a new call back out to the AT&T IPFR-EF service network. This new SIP INVITE will contain a Diversion Header.
3. The AT&T IPFR-EF service places a call to the alternate destination and upon answer, Avaya IP Office connects the calling party (PSTN Phone) to the target party (Target Phone).

Note – The IPFR-EF service offers similar Call Forwarding features that allow users to predefine alternate call destinations based on Ring-No-Answer, Busy, Not Reachable, or Unconditional criteria.

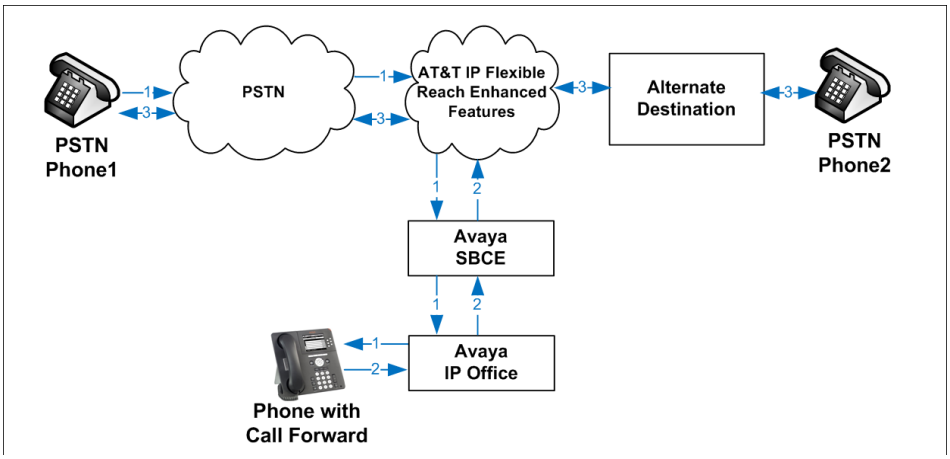


Figure 4: Call Forward

©2020 Avaya Inc. All Rights Reserved.

3.2.4. Coverage to Voicemail

The call scenario illustrated in the figure below is an inbound call that is covered to Voicemail. In the reference configuration, the Voicemail system used is Voicemail Pro.

1. Same as the first call scenario in **Section 3.2.1**.
2. The Avaya IP Office phone does not answer the call, and the call covers to Voicemail Pro.

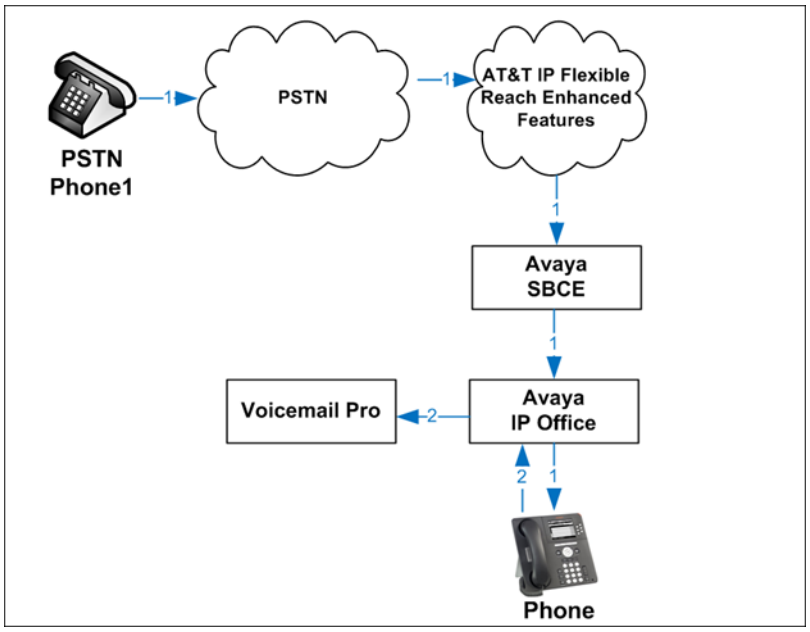


Figure 5: Coverage to Avaya IP Office Voicemail

©2020 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition - Avaya IP Office Voicemail Pro	Release 11.1.0.1.0 Build 95 Release 11.1.0.1.0 Build 14
Avaya IP Office 500 V2 Expansion System	Release 11.1.0.1.0 Build 95
Avaya IP Office Manager	Release 11.1.0.1.0 Build 95
Avaya Session Border Controller for Enterprise	Release 8.1.1.0-19214
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 4.0.6.0.7
Avaya 9508 Digital Deskphone	Release 0.60
Avaya Workplace Client for Windows	Release 3.9.1.46.29
Fax Device	Ventafax 7.10

Table 1: Equipment and Software Versions

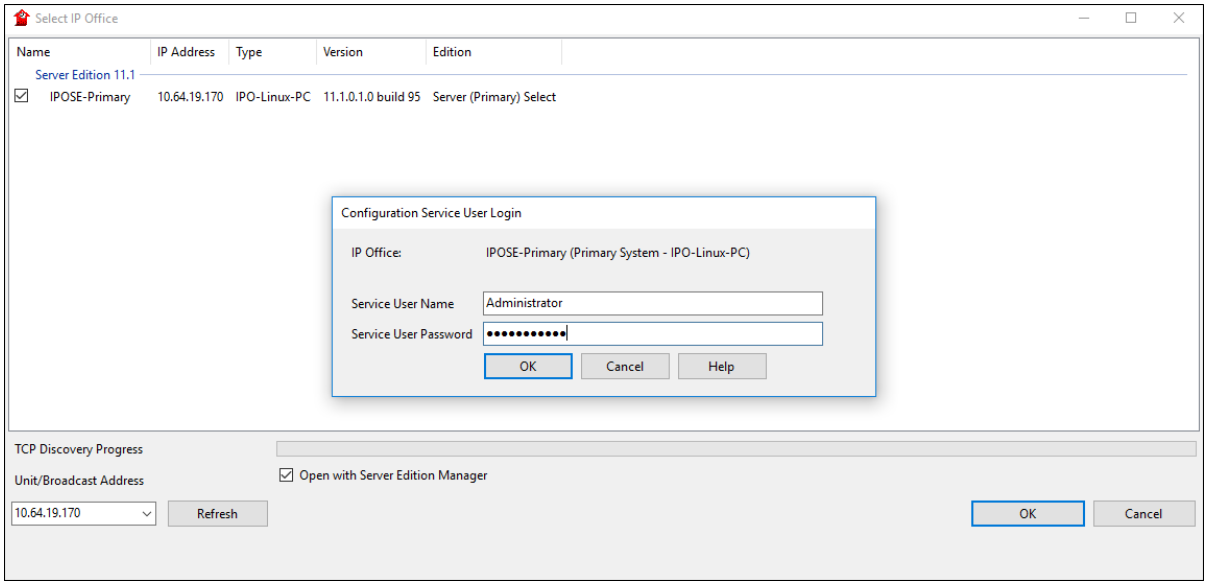
Note – Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2, and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks.

©2020 Avaya Inc. All Rights Reserved.

5. Avaya IP Office Primary Server Configuration

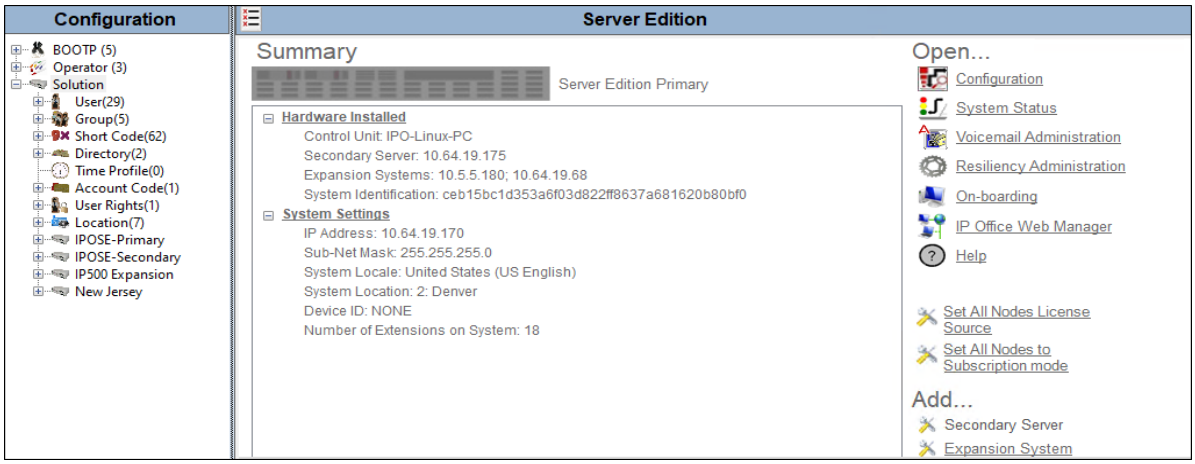
Note – This section describes attributes of the reference configuration but is not meant to be prescriptive. In the following sections, only the parameters that are highlighted in **bold** text are applicable to the reference configuration. Other parameter values may or may not match based on local configurations. Many forms contain multiple tabs. Only those tabs with provisioning related to the reference configuration are discussed. Any other tab/form should be considered default values. Additionally, the screen shots referenced in these sections may not be the complete form.

Avaya IP Office is configured through the Avaya IP Office Manager application. From the PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the Manager application. Log in using the appropriate credentials.



©2020 Avaya Inc. All Rights Reserved.

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.



In the screens presented in the following sections, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center and the Details pane on the right side. These panes will be referenced throughout the rest of this document.

Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

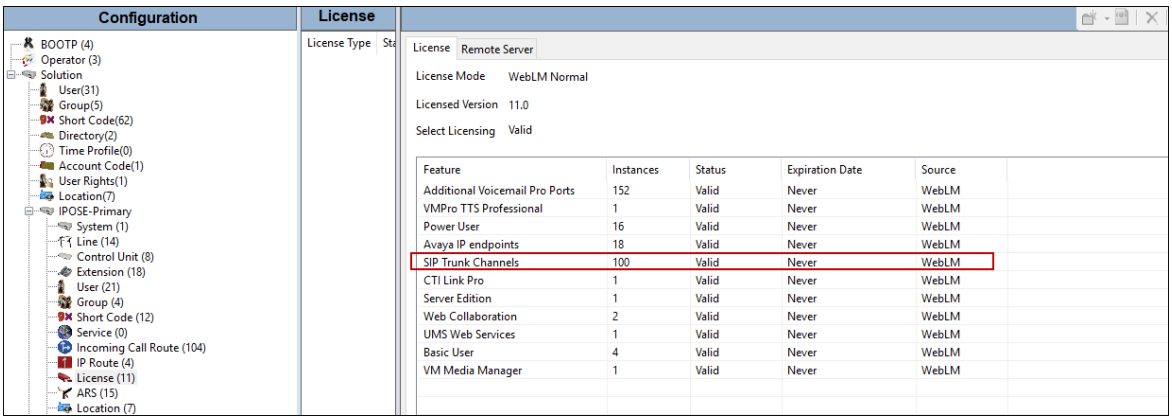
©2020 Avaya Inc. All Rights Reserved.

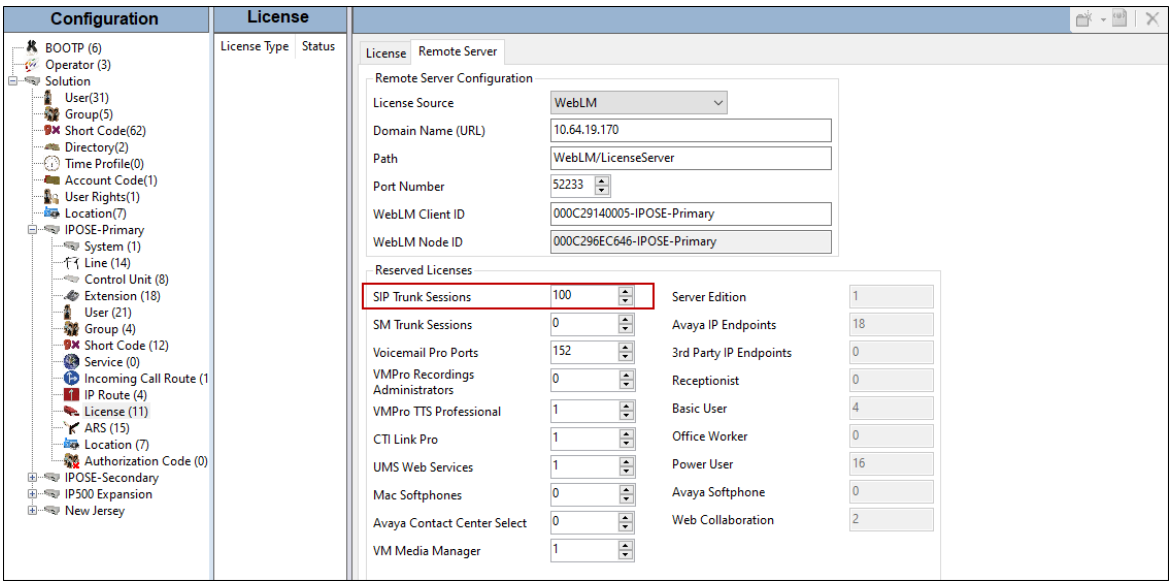
5.1. Licensing

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.

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.

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.





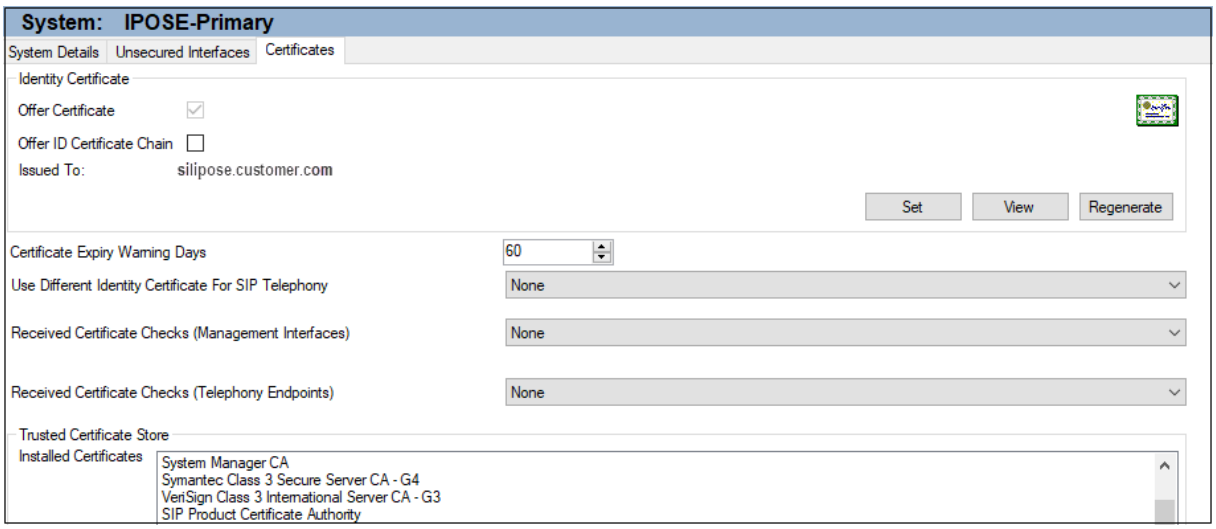
©2020 Avaya Inc. All Rights Reserved.

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.



©2020 Avaya Inc. All Rights Reserved.

5.3. System Settings

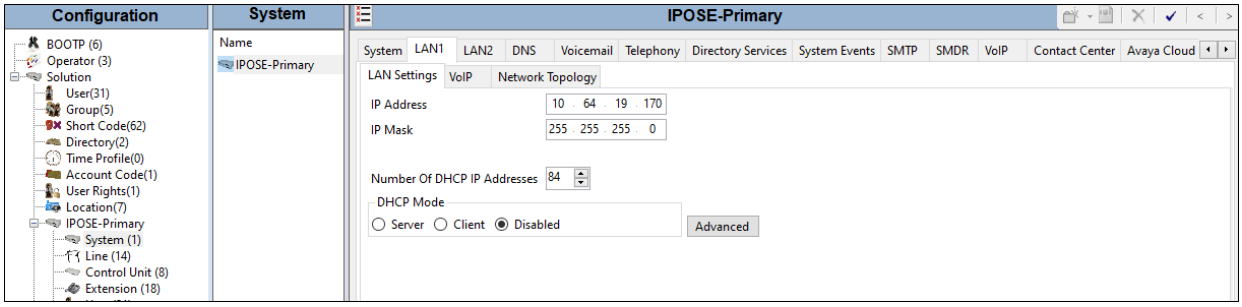
This section illustrates the configuration of system settings. Select **System** on the Navigation pane to configure these settings. The subsection order corresponds to a left to right navigation of the tabs in the Details pane for System settings. For all the following configuration sections, the **OK**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

5.3.1. LAN1 Tab

In the sample configuration, LAN1 is used to connect the Primary Server to the enterprise private network.

To view or configure the LAN 1 IP address and subnet mask, select the **LAN1 → LAN Settings** tab and enter the information as needed, according to customer specific requirements:

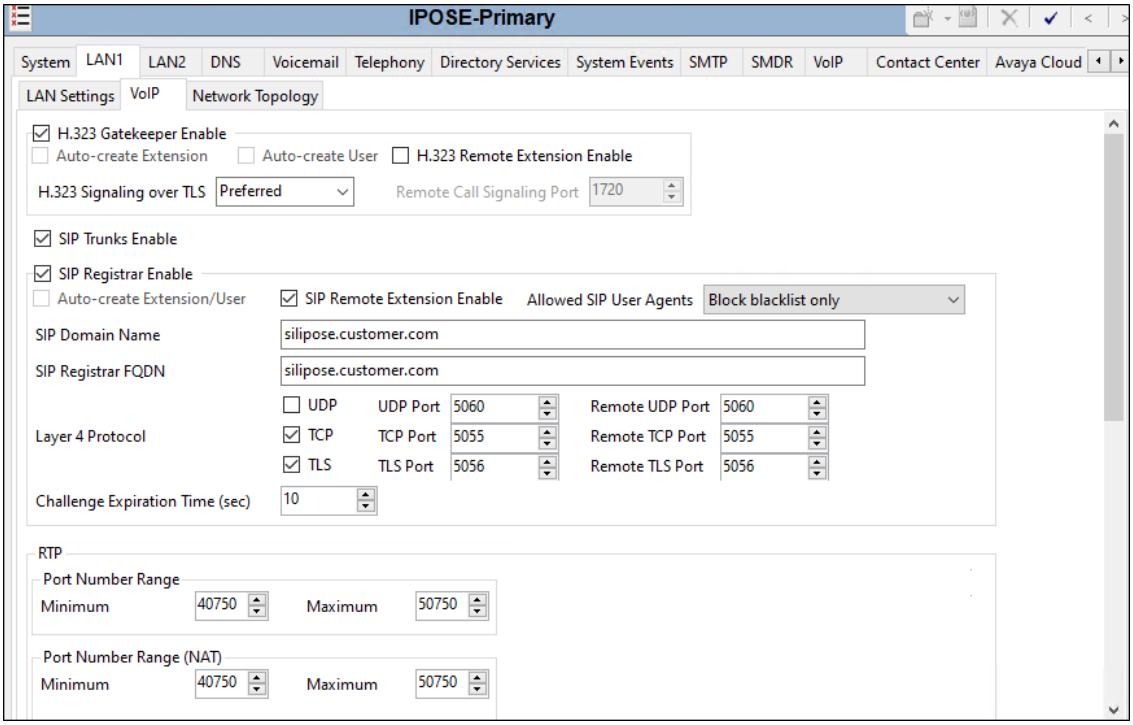
- **IP Address**: **10.64.19.170** was used in the reference configuration.
- **IP Mask**: **255.255.255.0** was used in the reference configuration.
- Click the **OK** button (not shown).



©2020 Avaya Inc. All Rights Reserved.

Select the **LAN1 → VoIP** tab as shown in the following screen. The following settings were used in the reference configuration:

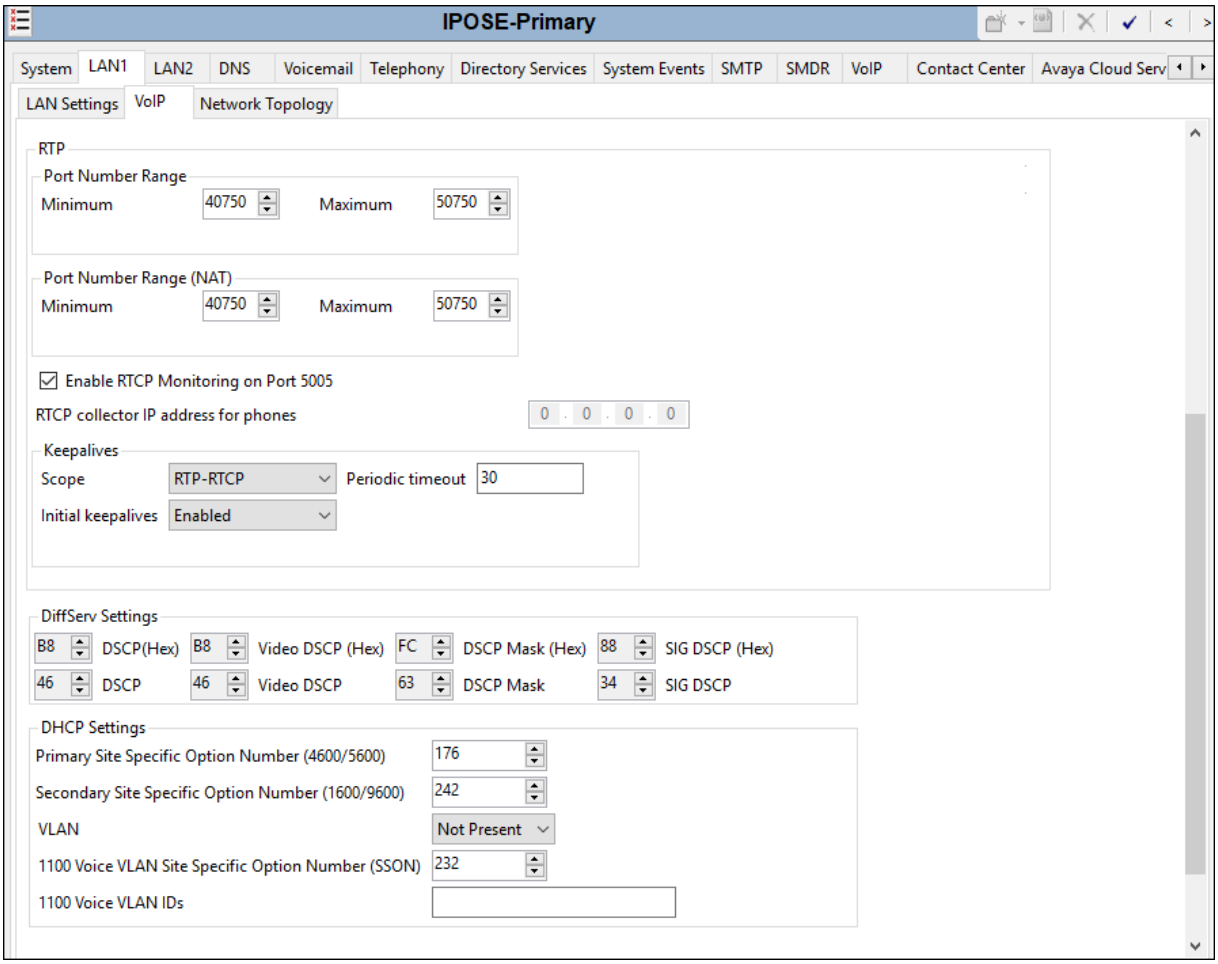
- The **H.323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the Avaya 96x1-Series Deskphones used in the reference configuration.
- The H.323 Signaling over TLS should be set based on customer needs. In the reference configuration it was set to **Preferred**.
- The **SIP Trunks Enable** parameter must be checked to enable the configuration of SIP trunks to AT&T.
- The **SIP Registrar Enable** box was checked to allow Avaya J100-Series Deskphones, Avaya 1100-Series Deskphones and Avaya Equinox usage.
- The **Domain Name** and **SIP Registrar FQDN** may be set according to customer requirements. The values used in the reference configuration are shown.
- Set the **Layer 4 Protocol** section based on customer needs. In the reference configuration **TCP/5055** and **TLS/5056** were configured.



©2020 Avaya Inc. All Rights Reserved.

Scroll down the page:

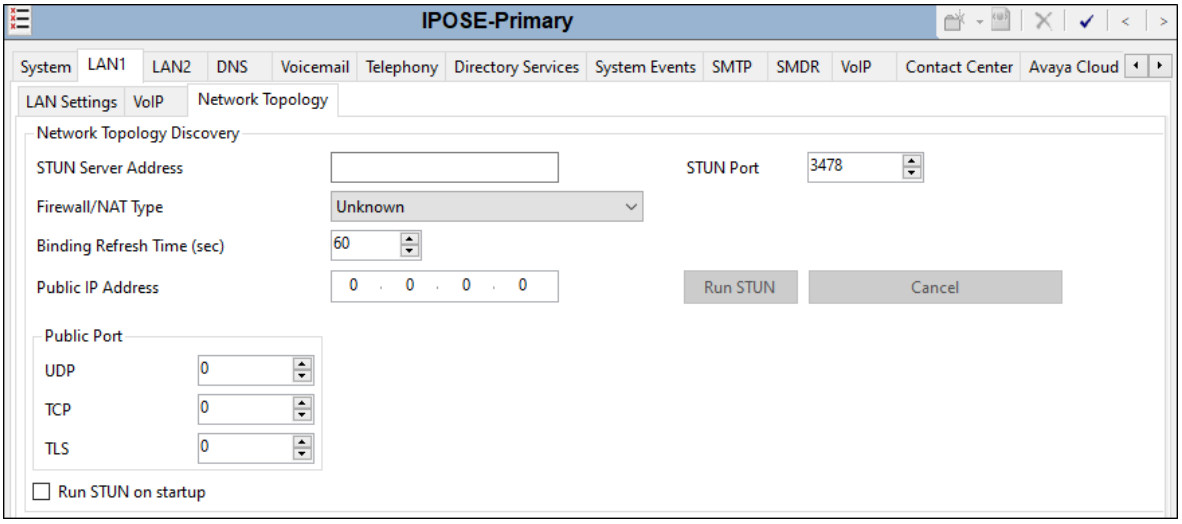
- Verify the **RTP Port Number Range**. Based on this setting, Avaya IP Office will request RTP media to be sent to a UDP port in the configurable range for calls using LAN1. The **Minimum** and **Maximum** port numbers were kept at their default values in the reference configuration.
- In the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. This is done to prevent possible issues with network firewalls closing idle RTP channels.
- In the **DiffServ Settings** section, IP Office 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.
- Click **OK** to commit (not shown).



©2020 Avaya Inc. All Rights Reserved.

Select the **LAN1 → Network Topology** tab as shown in the following screen, and enter the following:

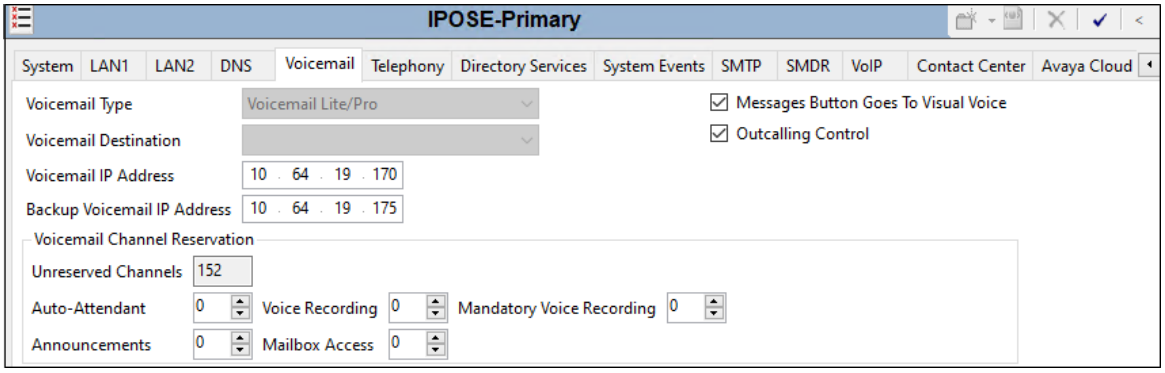
- **Firewall/NAT Type** was set to **Unknown** in the reference configuration.
- The **Public IP Address** and **Public Port** sections are not used for the AT&T IPFR-EF SIP trunk service connection.
- Click the OK button (not shown).



5.3.2. Voicemail Tab

As described in **Section 3**, Voicemail Pro was used in the reference configuration.

- Set **Voicemail Type** to **Voicemail Lite/Pro**.
- Set **Voicemail IP Address** to the IP address of the server hosting voicemail. In the reference configuration, this is the Primary server, **10.64.19.170**.
- Other parameters on this screen are default. Click the **OK** button (not shown).

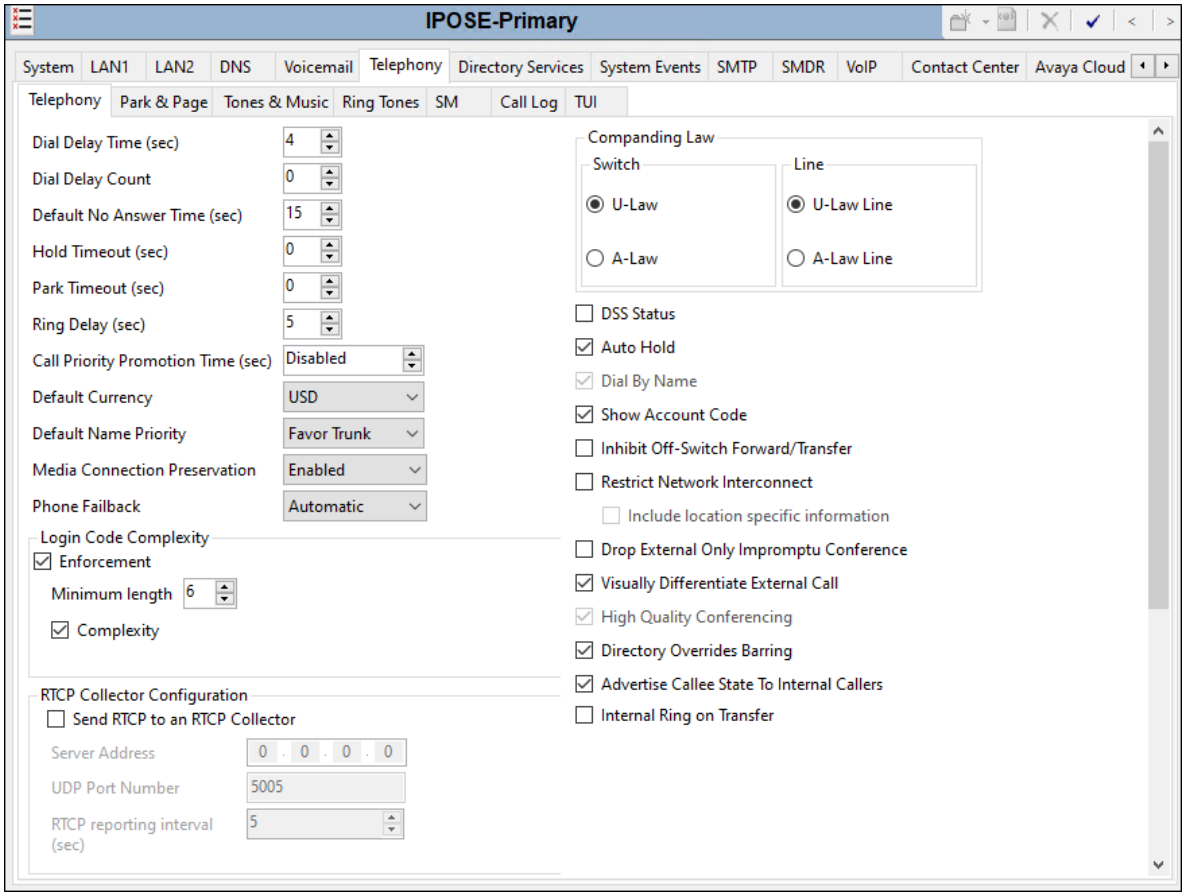


©2020 Avaya Inc. All Rights Reserved.

5.3.3. Telephony Tab

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 values used in the reference configuration and are not intended to be prescriptive.

- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave this setting checked.
- Set the **Companding Law** parameters to **U-Law** as is typical in North America.
- Default values are used in the other fields.
- Click the **OK** button (not shown).



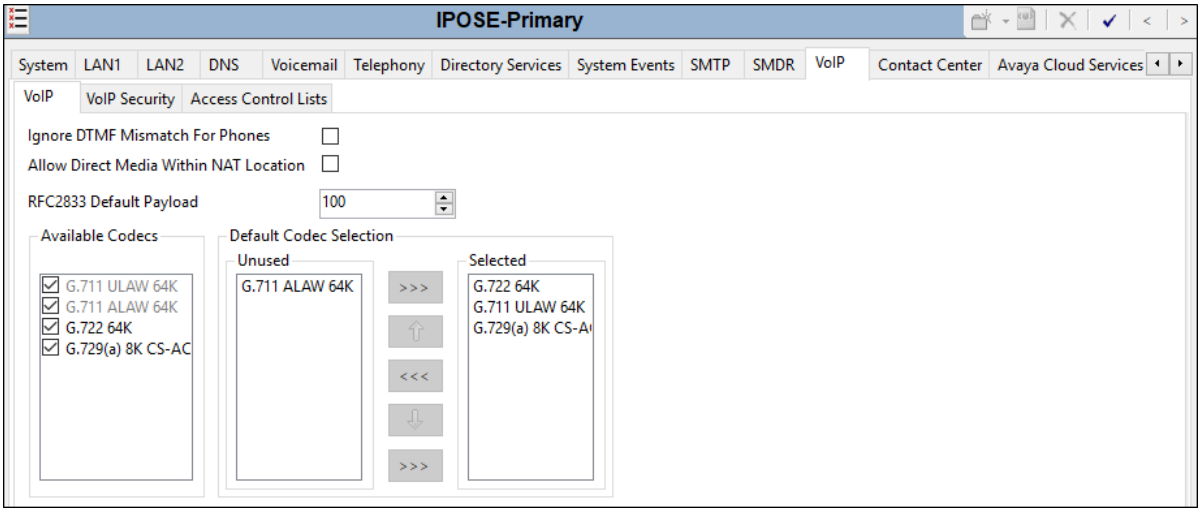
©2020 Avaya Inc. All Rights Reserved.

5.3.4. VoIP Tab

Navigate to the **VoIP** tab in the Details pane to view or change the system codecs and VoIP security settings.

Select the **VoIP → VoIP** tab. Configure the following parameters:

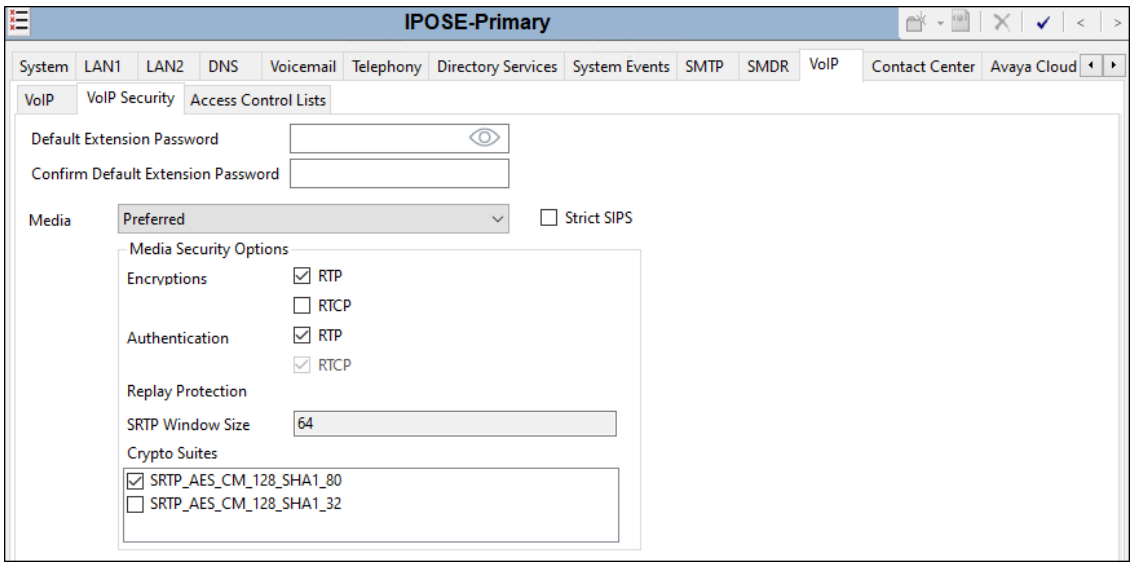
- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. During the compliance test, this was set to **100**, the value preferred by AT&T.
- For codec selection, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order were used.
- Click **OK** to commit (not shown).



©2020 Avaya Inc. All Rights Reserved.

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.

- Set the **Media Security** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption.
- Under **Media Security Options**, select **RTP** for the **Encryptions** and **Authentication** fields.
- Under **Crypto Suites**, select **SRTP_AES_CM_128_SHA1_80**.
- Click **OK** to commit (not shown).



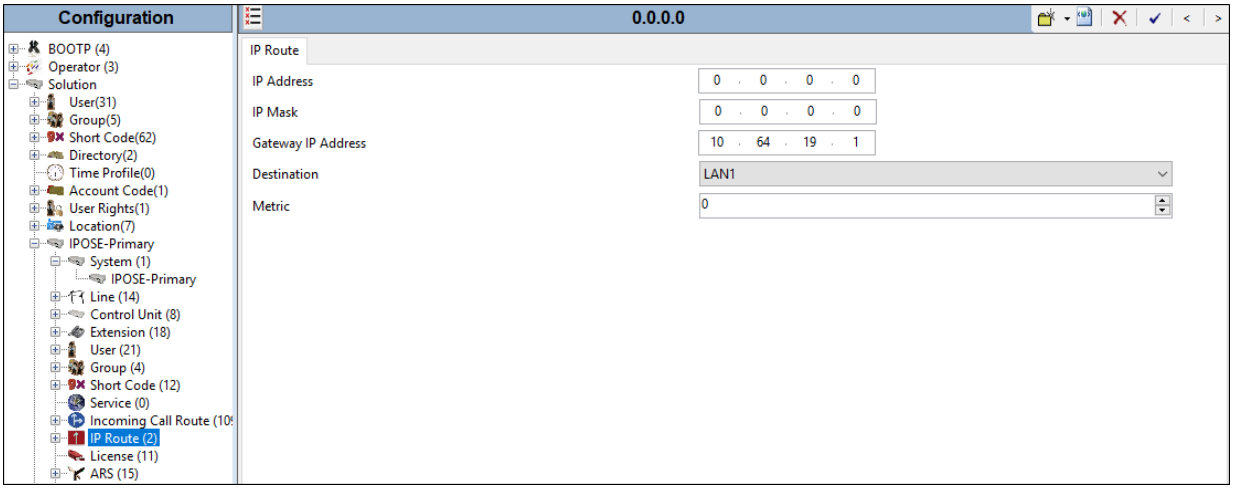
©2020 Avaya Inc. All Rights Reserved.

5.4. IP Route

In the sample configuration, the IP Office LAN1 port is physically connected to the local area network switch at the IP Office customer site. The Avaya SBCE resides on a different subnet and requires an IP route to allow SIP traffic between the two devices.

To create a new IP route, right-click on **IP Route** on the left navigation pane. Select **New** (not shown).

- Set the **IP Address** and **IP Mask** of the subnet of the private side of the Avaya SBCE, or enter **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP Address of the router in the IP Office subnet. The default gateway for this network is **10.64.19.1**.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).



©2020 Avaya Inc. All Rights Reserved.

5.5. SIP Line

The following sections describe the configuration of a SIP Line. The SIP Line terminates the CPE end of the SIP trunk to the AT&T IPFR-EF service.

The recommended method for creating/configuring a SIP Line is to use the template associated with the provisioning described in these Application Notes. The template is an .xml file that can be used by Avaya IP Office Manager to create a new SIP Line for SIP trunking with the AT&T IPFR-EF service. Follow the steps in **Section 5.5.1** to create a SIP Trunk 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 trunk registration 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** to **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.

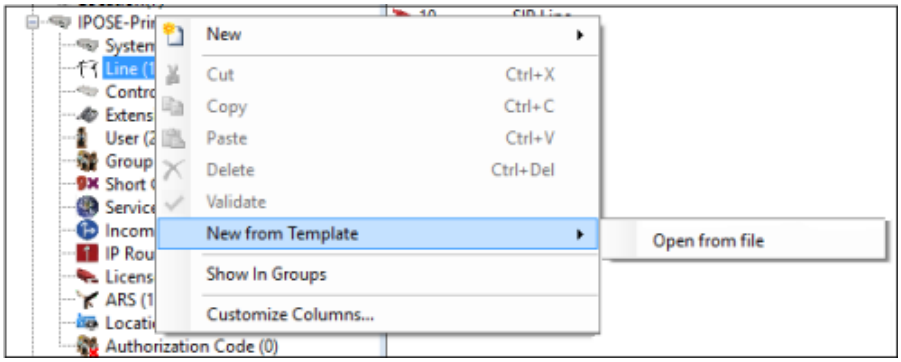
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.5.2** to **5.5.6**.

©2020 Avaya Inc. All Rights Reserved.

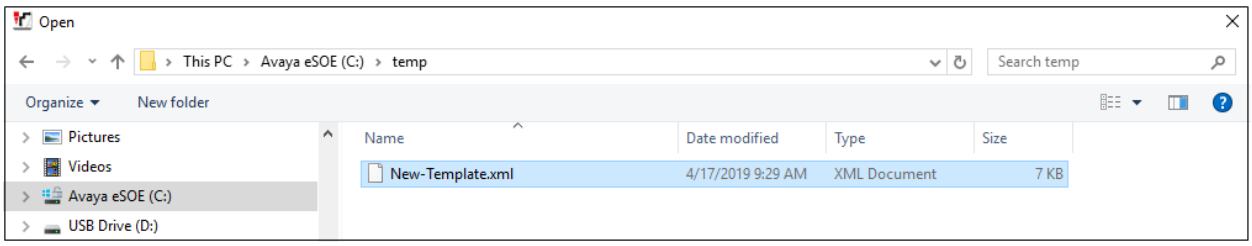
5.5.1. Creating a SIP Line from an XML Template

> **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 (IP500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

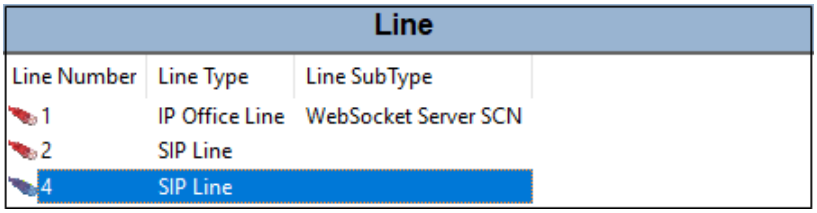
Copy a previously created template file to the computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New →New from Template**. Select **Open from file**.



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 **4**). The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.5.2 to 5.5.6**.



Line

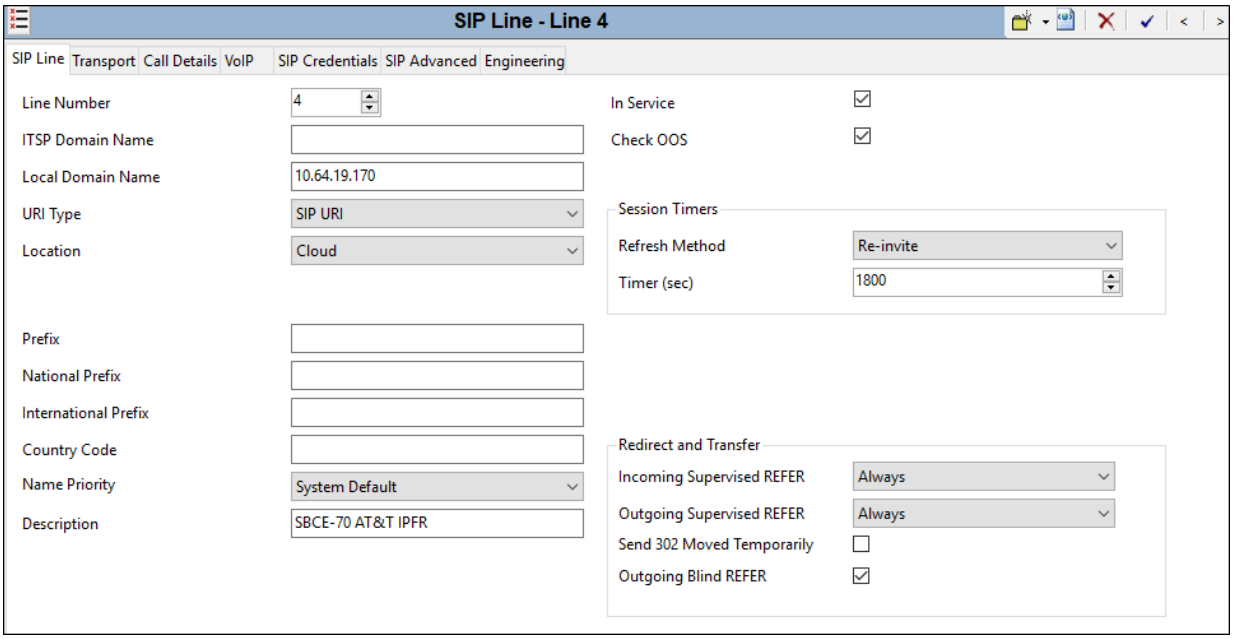
Line Number	Line Type	Line SubType
1	IP Office Line	WebSocket Server SCN
2	SIP Line	
4	SIP Line	

©2020 Avaya Inc. All Rights Reserved.

5.5.2. SIP Line – SIP Line tab

On the **SIP Line** tab in the **Details** pane, configure or verify the parameters as shown below:

- **ITSP Domain Name**: leave as the default (blank) to have IP Office send the **ITSP Proxy Address** as the domain name. See **Section 5.5.3**.
- **Local Domain Name:** Set to the public IP address of the Avaya IP Office LAN1 interface (e.g., **10.64.19.170**).
- Verify that **In Service** box is checked, the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- **Refresh Method:** Set to **Re-Invite**, as AT&T does not support UPDATE
- Set **Timer (seconds)** to **1800**. This field specifies the session expiry time. With this value, a session refresh message is sent every 15 minutes, at the half way point of the expiry time.
- **Incoming Supervised Refer**: Set this field to **Always** to enable Avaya IP Office to accept REFER sent by the network during a transfer scenario.
- **Outgoing Supervised Refer**: Set this field to **Always** to enable Avaya IP Office to use REFER (with Replaces) for station-initiated call transfer scenarios back to PSTN.
- **Outgoing Blind Refer**: Optional. Enable this option to support Refer (without Replaces) for "Blind" (unattended) transfers (e.g., transfer-to party is still ringing when the transfer operation is completed). If this feature is not enabled, then Refer (with Replaces) will be used. **Note – This feature is only supported with certain SIP telephones and Voicemail call flows**.
- Use the default values for the other fields.
- Click **OK** (not shown).

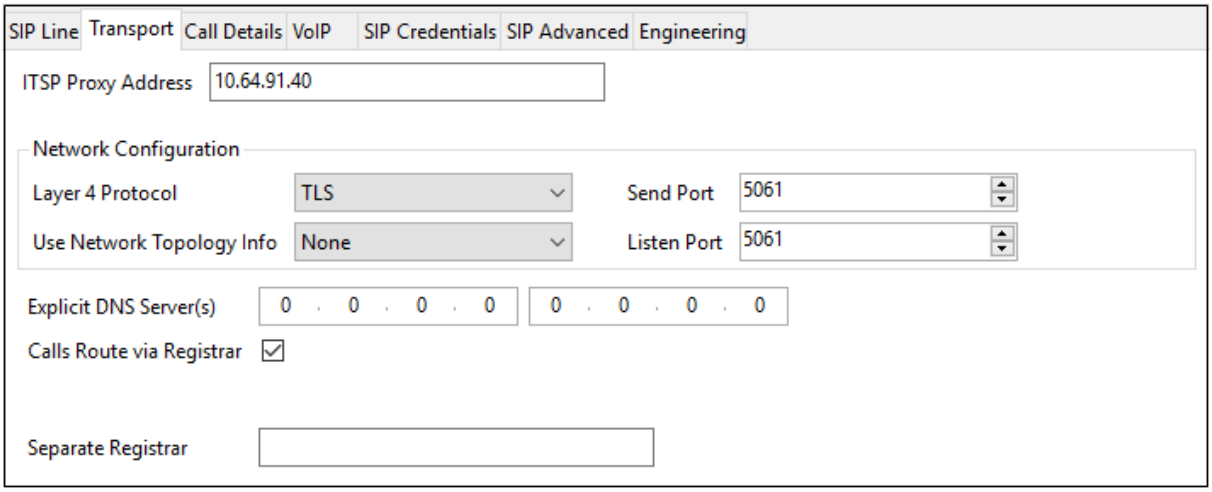


©2020 Avaya Inc. All Rights Reserved.

5.5.3. SIP Line - Transport Tab

Select the **SIP Line → Transport** tab and configure the following:

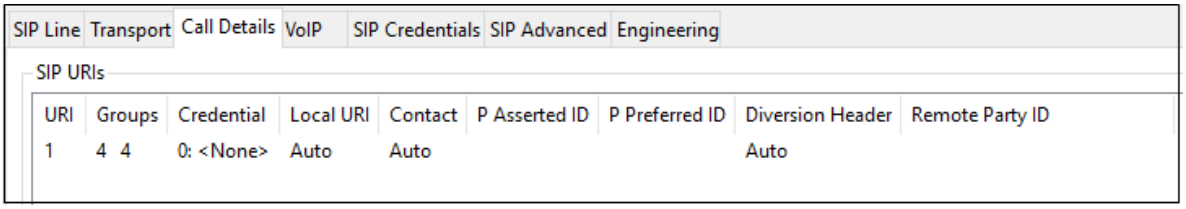
- **ITSP Proxy Address:** Set to the Avaya SBCE A1 IP address (e.g., **10.64.91.40**).
- **Network Configuration → Layer 4 Protocol**: Set to **TLS**.
- **Network Configuration → Send Port**: Set to **5061**.
- **Network Configuration → Use Network Topology Info**: Set to **None**.
- **Network Configuration → Listen Port**: Set to **5061**.
- Verify **Calls Route via Registrar:** Enabled (default)
- **Click OK** (not shown).



©2020 Avaya Inc. All Rights Reserved.

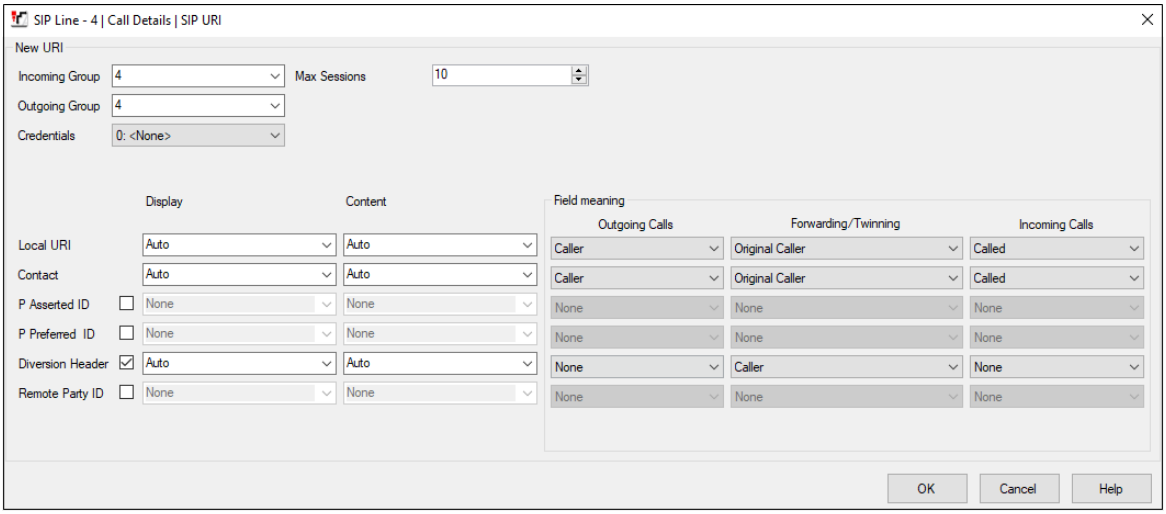
5.5.4. SIP Line – Call Details tab

Select the **Call Details** tab. To add a new SIP URI, click the **Add…** button. To review an existing SIP URI, select it and click the **Edit** button.



The **SIP URI** window will open. Configure the following:

- **Incoming Group:** Set to **4** (SIP Line 4). This value references the **Line Group ID** set on the **Incoming Call Routes** in **Section 5.7**.
- **Max Sessions:** In the reference configuration this was set to **10**. This sets the maximum number of simultaneous calls that can use the URI before Avaya IP Office returns busy to any further calls.
- **Outgoing Group:** Set to **4** (SIP Line 4). This will be used for routing outbound calls to AT&T via the **ARS** configuration (**Section 5.9**).
- Verify the **Diversion Header** is checked.
- For the **Local URI**, **Contact** and **Diversion Header** leave the selections under the **Display** and **Content** columns to the default **Auto**. With this setting, IP Office will use the information on the **Incoming Call Routes** (**Section 5.7**) to populate the From and Contact headers on outbound calls, and also to determine which inbound calls will be allowed on the SIP line.
- On the **Field meaning** section, set the values under the **Outgoing Calls**, **Forwarding/ Twinning** and **Incoming Calls** columns as shown on the screenshot below.
- Click **OK**.



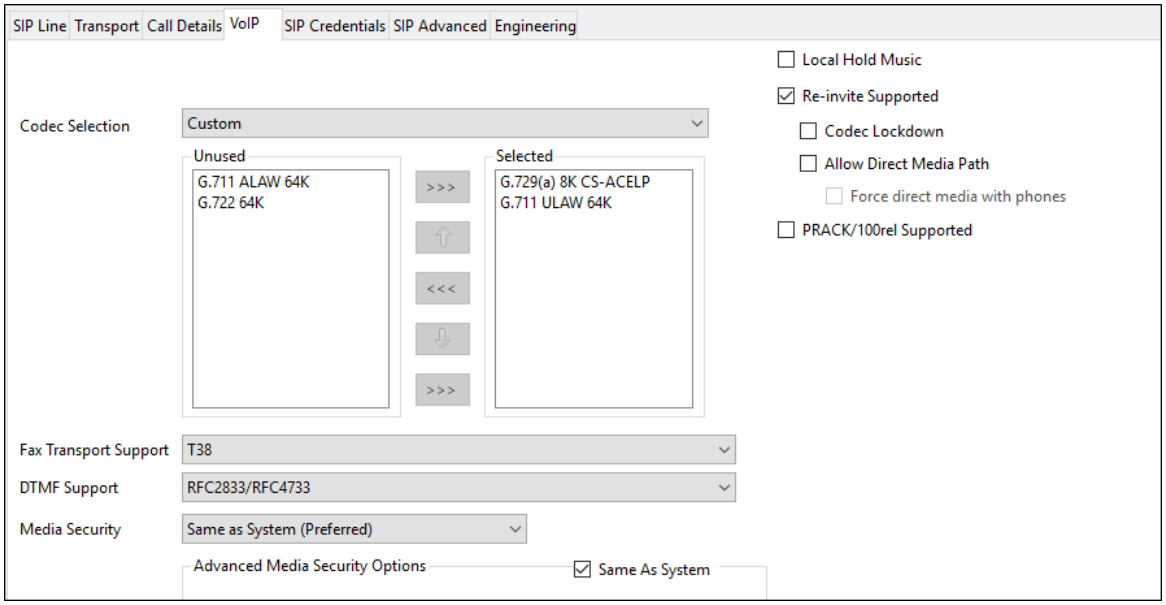
©2020 Avaya Inc. All Rights Reserved.

In the reference configuration, the single SIP URI shown was sufficient to allow incoming calls for AT&T DID numbers destined for specific IP Office users, hunt groups or short codes.

5.5.5. SIP Line - VoIP tab

Select the **SIP Line → VoIP** tab. Set the parameters as shown below:

- The **Codec Selection** drop-down box → **System Default** will list all available codecs. In the reference configuration, **Custom** was selected with **G729(a) 8K CS-ACELP** and **G.711 ULAW 64K** specified. This causes Avaya IP Office to include these codecs in the Session Description Protocol (SDP) offer, and in the order specified. Note that in the reference configuration G.729A is set as the preferred codec on the SIP trunk to the AT&T IPFR-EF network.
- Set the **Fax Transport Support** drop-down menu to **T.38**. Note that Error Correction Mode (ECM) is enabled by default on the **T.38 Fax** tab (**Section 6.4**). ECM is supported by the AT&T IPFR-EF service. G.711 fax was also tested in the reference configuration (T.38 option disabled); however, there were problems. T.38 is the preferred method for fax. See **Section 2.2** for limitations.
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set the **Media Security** drop-down menu to **Same as System (Preferred)** to have IP Office use the system setting for media security set in **Section 5.3.4** to encrypted RTP toward Avaya SBCE.
- The **Re-invite Supported** parameter can be 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.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).

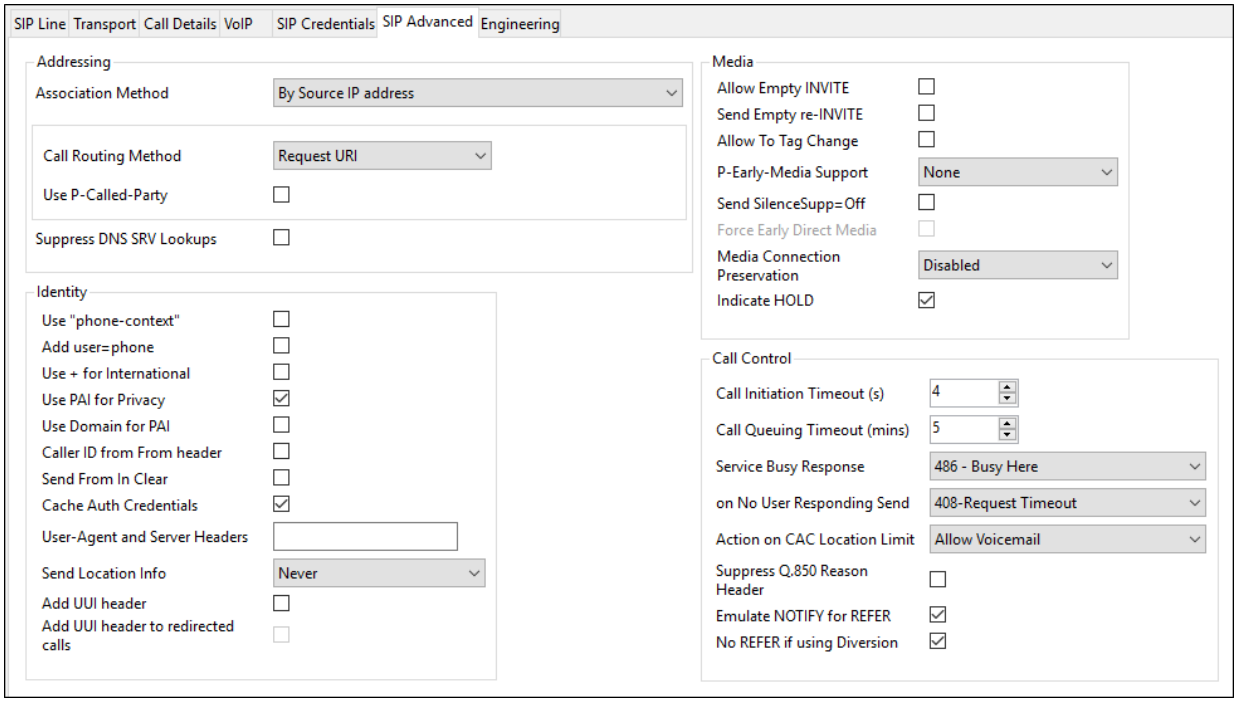


©2020 Avaya Inc. All Rights Reserved.

5.5.6. SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab. Set the parameters as shown below:

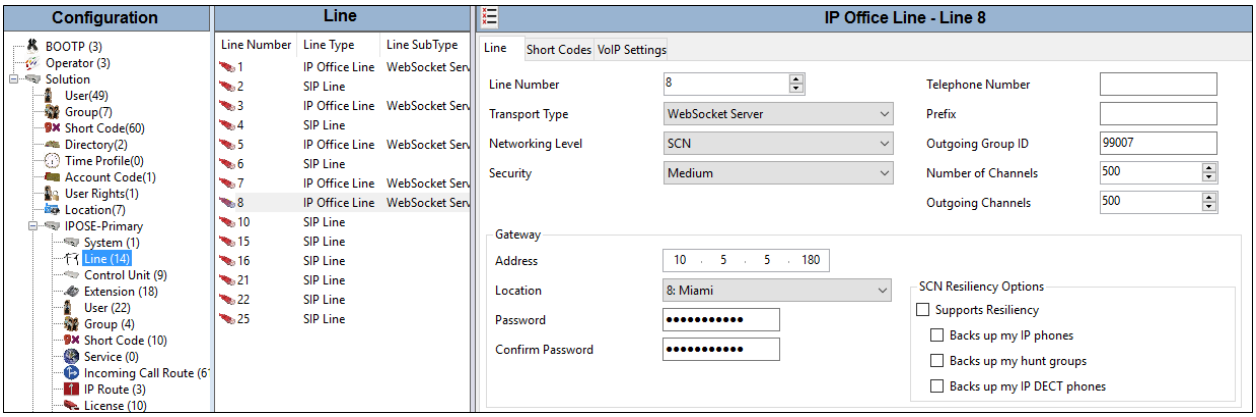
- Check the box for **Use PAI for Privacy**. By default, Avaya IP Office will use the PPI (P-Preferred-Identity) header for signaling user information when privacy is invoked. However, AT&T utilizes the PAI (P-Asserted-Identity) header for privacy. Therefore, Avaya IP Office is configured to use the PAI header to pass the calling party information for authentication and billing when privacy is used.
- Select **Indicate HOLD**. IP Office can be configured to signal when a call is placed on hold by sending an INVITE with media attribute "sendonly". AT&T in turn will respond with media attribute "recvonly" and will stop sending RTP media for the duration the call is on hold. When the call is taken off of hold, IP Office will send another INVITE with media attribute "sendrecv" indicating to AT&T to start sending RTP again.
- Select **Emulate NOTIFY for Refer**. The AT&T IPFR-EF service does not support NOTIFY. Some Avaya endpoints (e.g., Avaya 1140E Deskphone) require receipt of a NOTIFY when Refer based call transfers are performed. This option will send a NOTIFY to these endpoints.
- By default, Avaya IP Office sends Refer in addition to Diversion header for call forward scenarios. However, AT&T only requires Diversion header. Therefore, in the reference configuration the **No Refer if using Diversion** was selected.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



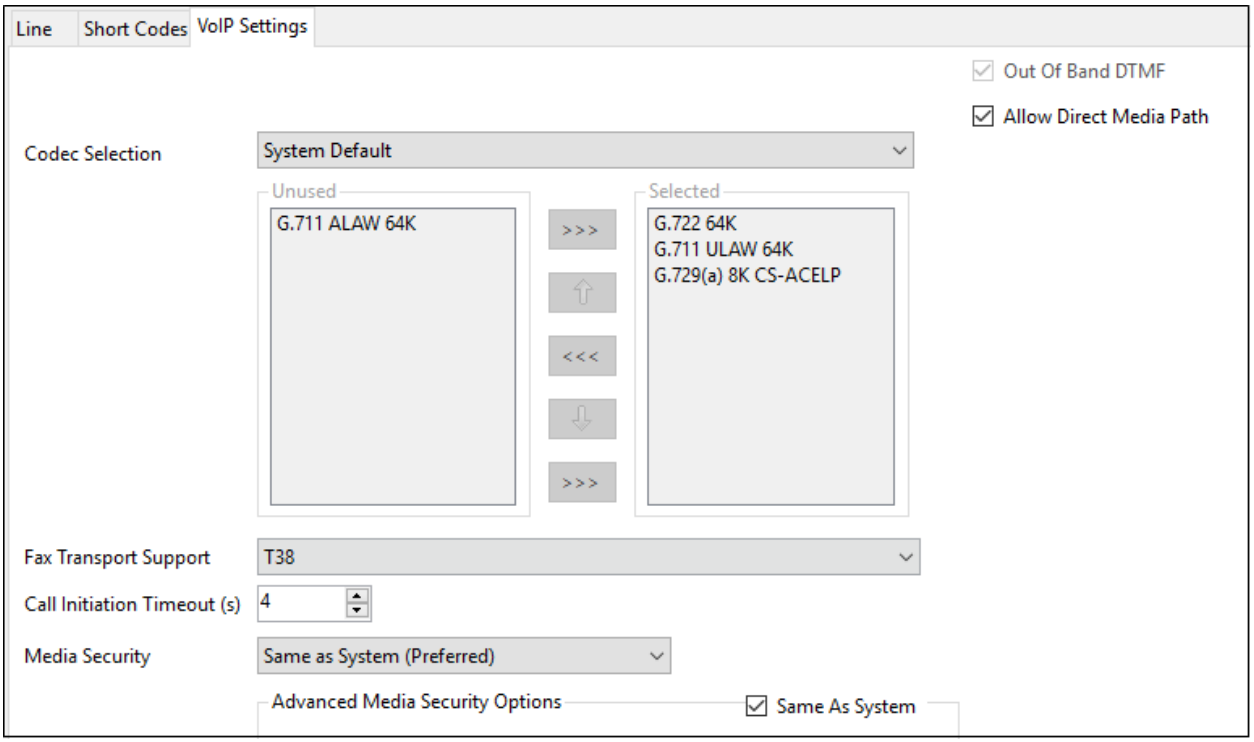
©2020 Avaya Inc. All Rights Reserved.

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**. Default values were used for all other parameters.



©2020 Avaya Inc. All Rights Reserved.

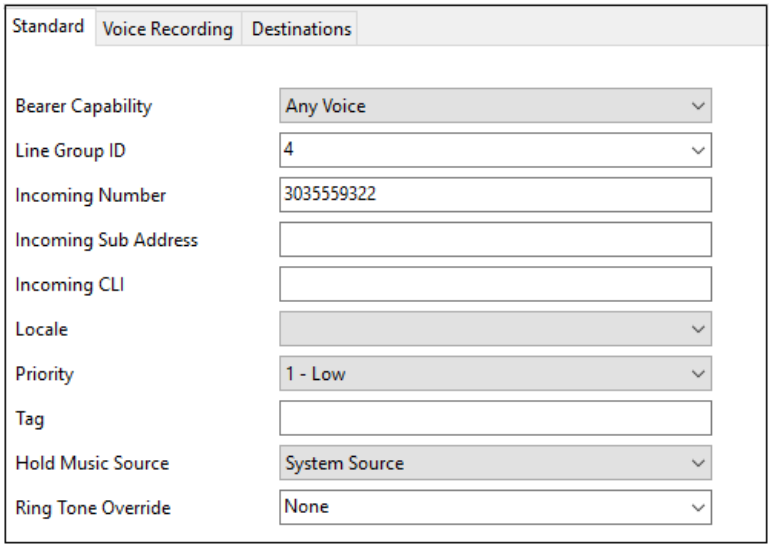
5.7. Incoming Call Route

Incoming call routes map inbound AT&T DNIS numbers to internal extensions, hunt groups, short codes, etc., within the IP Office system. To add an incoming call route, right click on **Incoming Call Route** in the **Navigation** pane and select **New** (not shown). On the Details Pane, under the **Standard** tab, set the parameters as show below:

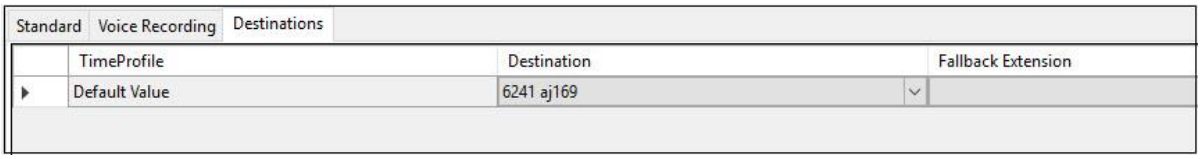
- Set **Bearer Capacity** to **Any Voice**.
- The **Line Group ID** is set to **4**. This matches the **Incoming Group** field configured in the **Call Details** tab for the SIP Line on **Section 5.5.4**.
- On the **Incoming Number**, enter the DID number for this route.

Note - When the destination is a user's extension, the **Incoming Number** can be used to construct the From and Contact headers to be used in place of the extension number in the outgoing SIP INVITE for that user.

- Default values may be used for all other parameters.



Select the **Destinations** tab. From the **Destination** drop-down menu, select the endpoint associated with this DID number. In the reference configuration, AT&T DNIS number **3035559322** was associated with the Avaya IP Office user at extension **6241**.



Repeat this process to route the rest of the AT&T DNIS numbers to additional users, as well as other Avaya IP Office destinations (Hunt Group, Voicemail, Short Codes, etc.).

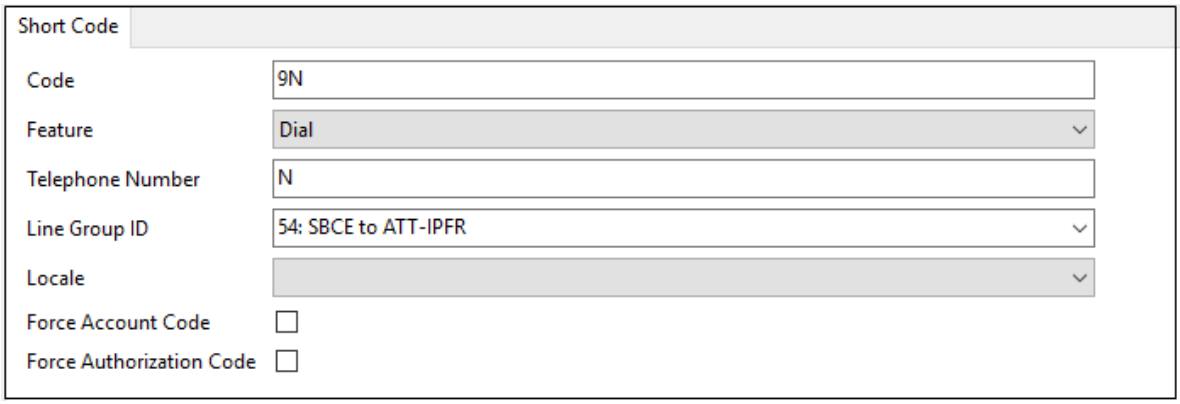
©2020 Avaya Inc. All Rights Reserved.

5.8. Short Codes

Avaya IP Office uses Automatic Route Selection (ARS) to route outbound traffic to the SIP line. A short code is needed to send the outbound traffic to the ARS route. To create the short code used for ARS, right-click on **Short Code** in the Navigation Pane and select **New** (not shown). The screen below shows the creation of the short code **9N** used in the reference configuration. When the Avaya IP Office users dialed 9 plus any number N, calls were directed to **Line Group 54**, configurable via ARS and defined next in **Section 5.9**.

On the **Short Code** tab in the Details Pane, configure the parameters as shown below.

- In the **Code** field, enter the dial string which will trigger this short code, in this case **9N**. This short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix.
- Set the **Line Group ID** to the ARS route to be used. In the example shown, the call is directed to **Line Group 54: SBCE to ATT-IPFR**.



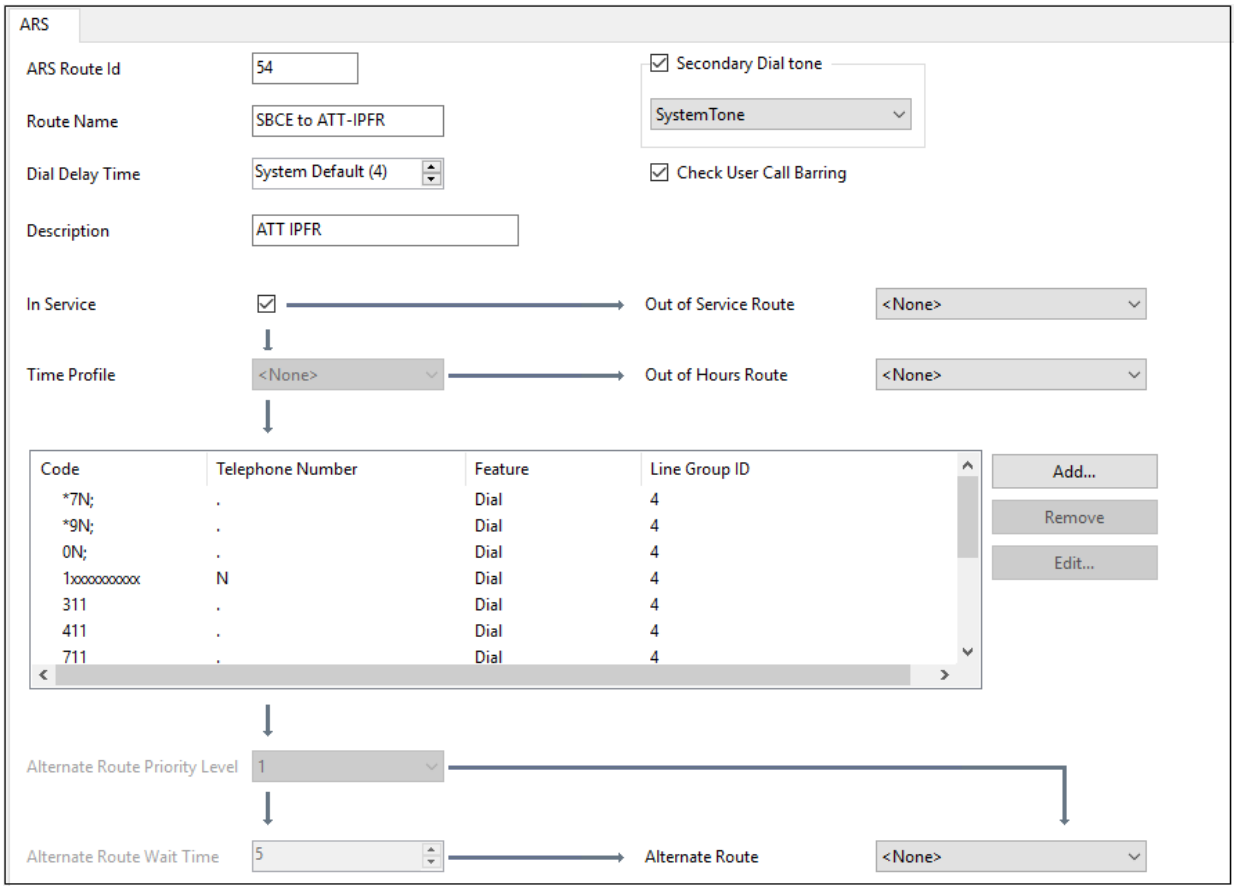
©2020 Avaya Inc. All Rights Reserved.

5.9. Automatic Route Selection (ARS)

While detailed coverage of ARS is beyond the scope of these Application Notes, this section includes some basic screen illustrations of the ARS settings used during the compliance test.

As described in **Section 5.8**, Short Code **9N** was defined for ARS access. Therefore, outbound calls via ARS are dialed as 9 plus the number. ARS will strip off the 9, and it will process the call based on the remaining digits.

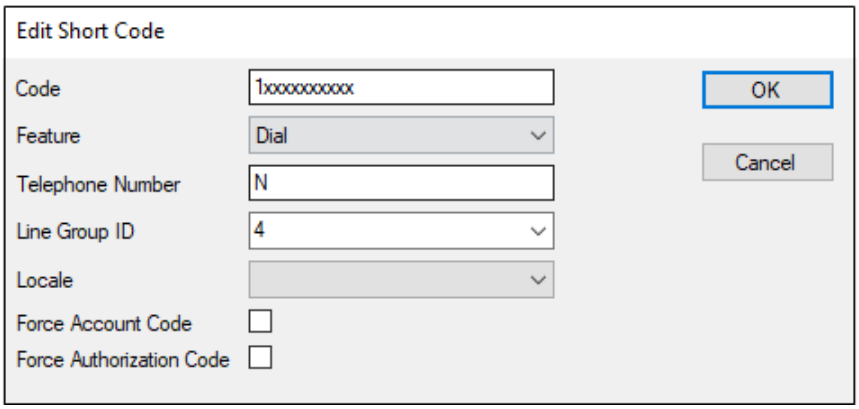
To add a new ARS route, right-click **ARS** in the **Navigation** pane, and select **New** (not shown). The following screen shows the **ARS Route ID 54**, created in the sample configuration.



©2020 Avaya Inc. All Rights Reserved.

To add a new ARS table entry, click on the **Add** button. To change an existing entry, select the entry and click on the **Edit** button.

The example below shows the entry for 11 (1+10) digit calls.



- Set **Code** to **1xxxxxxxxxx**
  This means any dialed string starting with a 1, and 11 digits in total will be routed to the specified Line Group.
- **Feature** = **Dial**.
- **Telephone Number** = **N**.
  With this setting the leading 1 will be excluded, and only the remaining 10 digits will be sent to AT&T.
- **Line Group ID = 4** (SIP Line 4).

©2020 Avaya Inc. All Rights Reserved.

5.10. Outbound Calling Party Information

According to the SIP URI configuration on **Section 5.5.4**, Avaya IP Office will use the information on the Incoming Number field on the Incoming Call Routes (**Section 5.7**) to populate the From and Contact headers on outbound calls from the IP Office users. These headers are used by the service provider to deliver Caller ID information to the receiving end of the call.

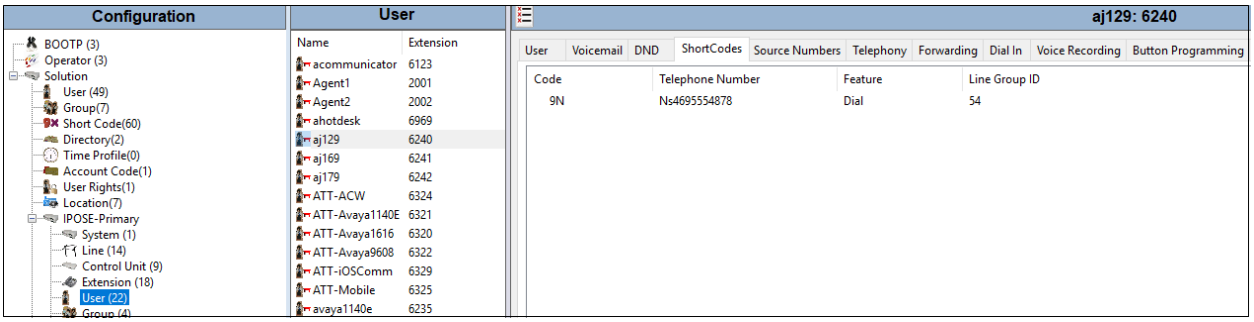
There are cases where the IP Office user may not be associated with an Incoming Call Route. In other situations, it may be desired to send the same outbound caller ID for all the users in the enterprise. Short Codes can be created to construct the From and Contact headers in the outgoing SIP INVITE message.

5.10.1. Short Code- User

In cases where a user does not have an associated Incoming Call Route with a 10-digit number assigned to it, a Short Code can be created for that user to set the outbound caller ID.

To set a Short Code for an existing user, select **User** in the Navigation pane, and select the appropriate user to be configured in the Group pane. Select the **Short Code** tab on the Details pane and click **Add** (not shown).

The following screen shows the **Short Codes** tab for user 6240. This user does not have an associated Incoming Call Route.



- Set **Code** to **9N**.
- In the example, the **Telephone Number** is set to "**Ns4695554878**". The number after the "s" will be sent on the From and Contact headers in the outgoing SIP INVITE on calls from this user.
- **Feature** = **Dial**.
- **Line Group ID = 54**, the ARS route to be used for AT&T.

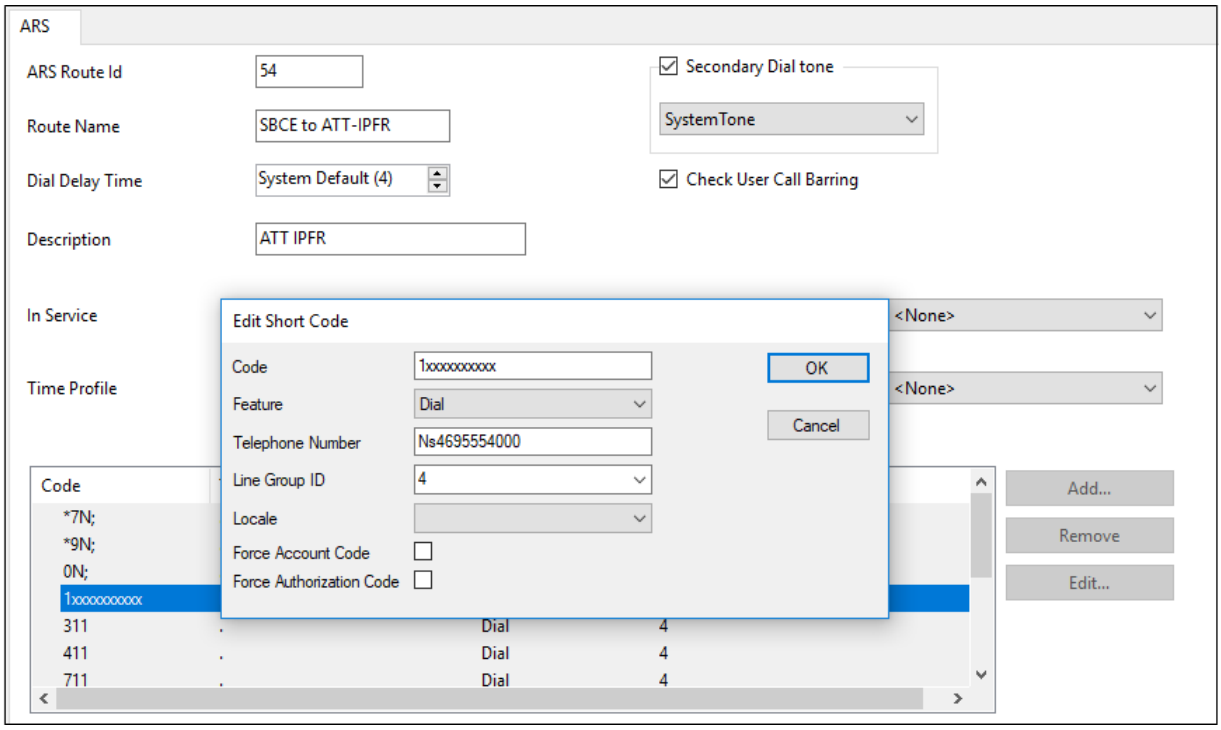
©2020 Avaya Inc. All Rights Reserved.

5.10.2. Short Code - ARS

There may be other specific cases when it is preferred to send the same caller ID on outbound calls for all the users in the enterprise, for example, the published main number for the location.

Short Code entries on the ARS table (**Section 5.9**) can be created or edited, to modify the From and Contact headers in the outgoing SIP INVITE messages for all outbound calls.

On the screen below, an existing ARS Short Code entry was modified. The **Telephone Number** is set to "**Ns4695554000**". The number after the "s" will be sent on the From and Contact headers in the outgoing SIP INVITE on calls from all users in the Avaya IP Office using this ARS route.



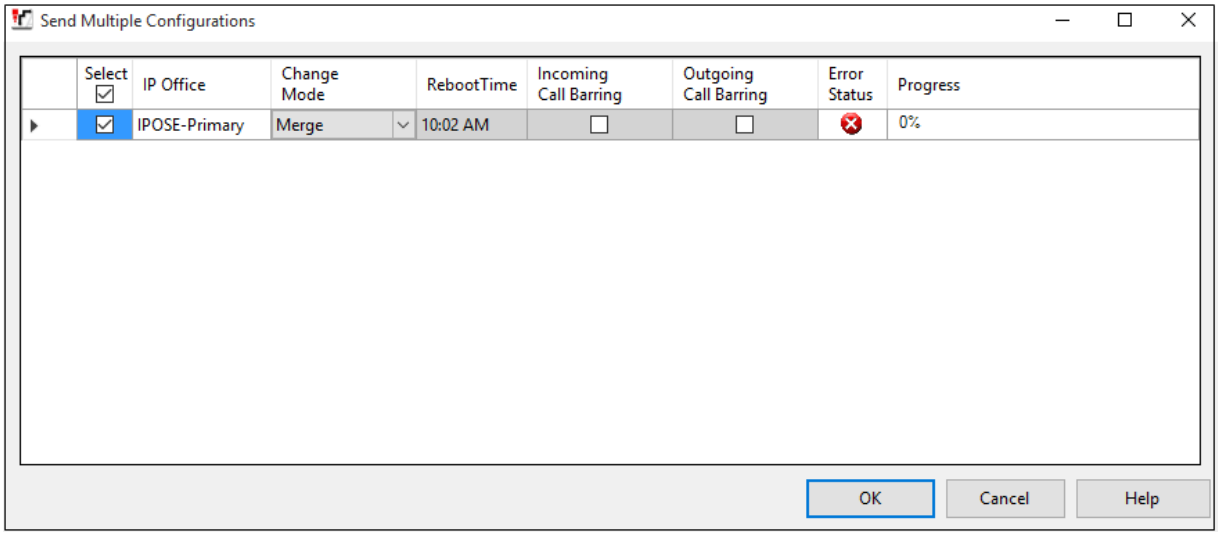
©2020 Avaya Inc. All Rights Reserved.

5.11. Save IP Office Primary Server Configuration

The provisioning changes made in Avaya IP Office Manager must be applied to the Avaya IP Office server in order for the changes to take effect. At the top of the Avaya IP Office Manager page, click **File → Save Configuration** (if that option is grayed out, no changes are pending).

A screen similar to the one below will appear, with either **Merge** or **Immediate** automatically selected, based on the nature of the configuration changes. The **Merge** option will save the configuration change with no impact to the current system operation. The **Immediate** option will save the configuration and cause the Avaya IP Office server to reboot.

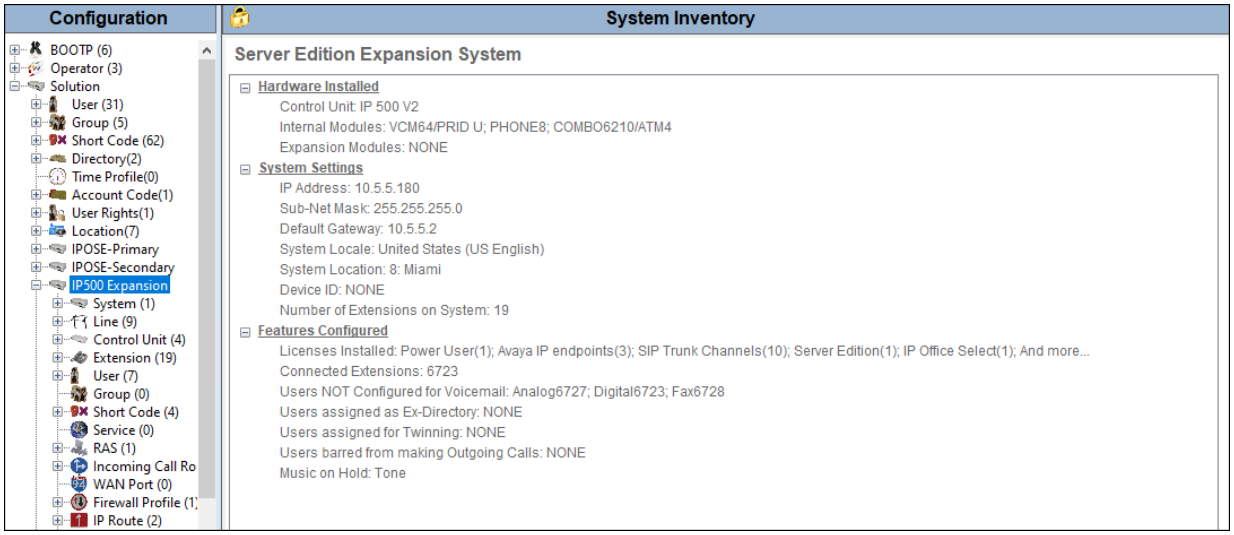
Click **OK** to execute the save.



©2020 Avaya Inc. All Rights Reserved.

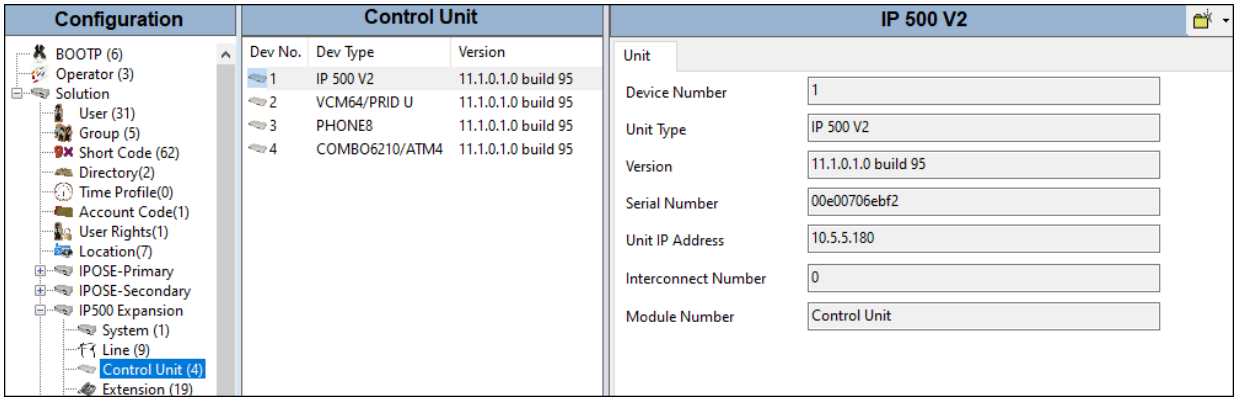
6. Avaya IP Office Expansion System Configuration

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.

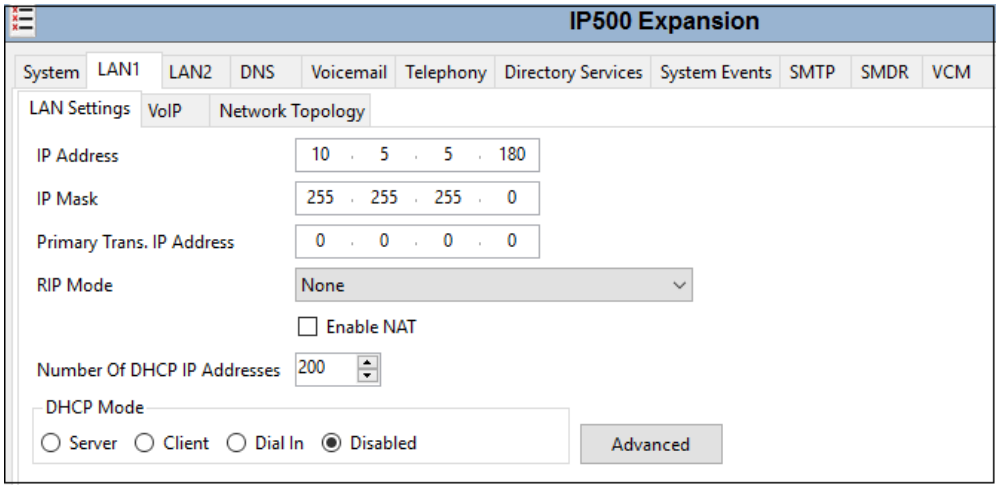


©2020 Avaya Inc. All Rights Reserved.

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, and enter the following:

- **IP Address: 10.5.5.180** was used in the reference configuration.
- **IP Mask: 255.255.255.0** was used in the reference configuration
- Click the **OK** button (not shown).

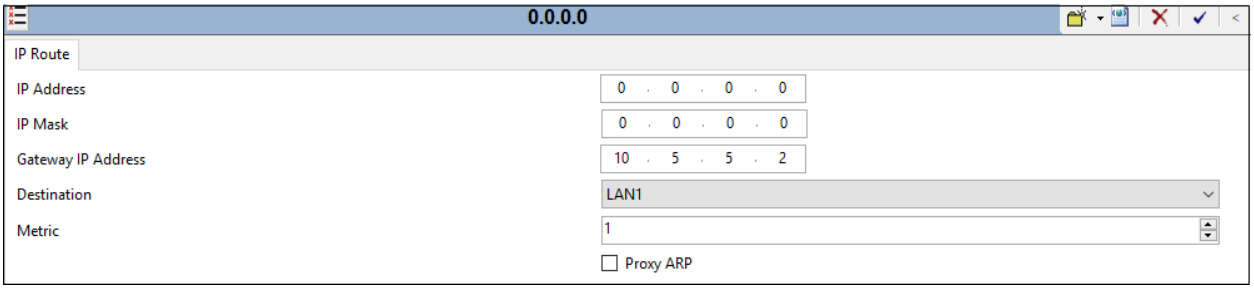


Defaults were used on the **VoIP** and **Network Topology** tabs (not shown).

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).

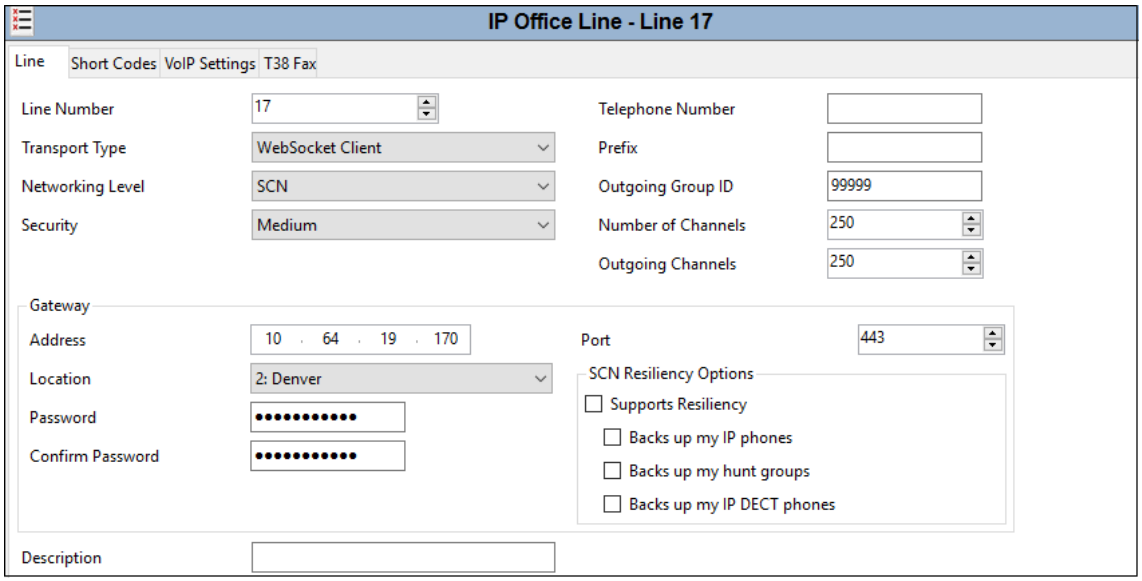
- Enter **0.0.0.0** on the **IP Address** and **IP Mask** fields to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet. The default gateway in the reference configuration was **10.5.5.2**
- Set **Destination** to **LAN1** from the pull-down menu.



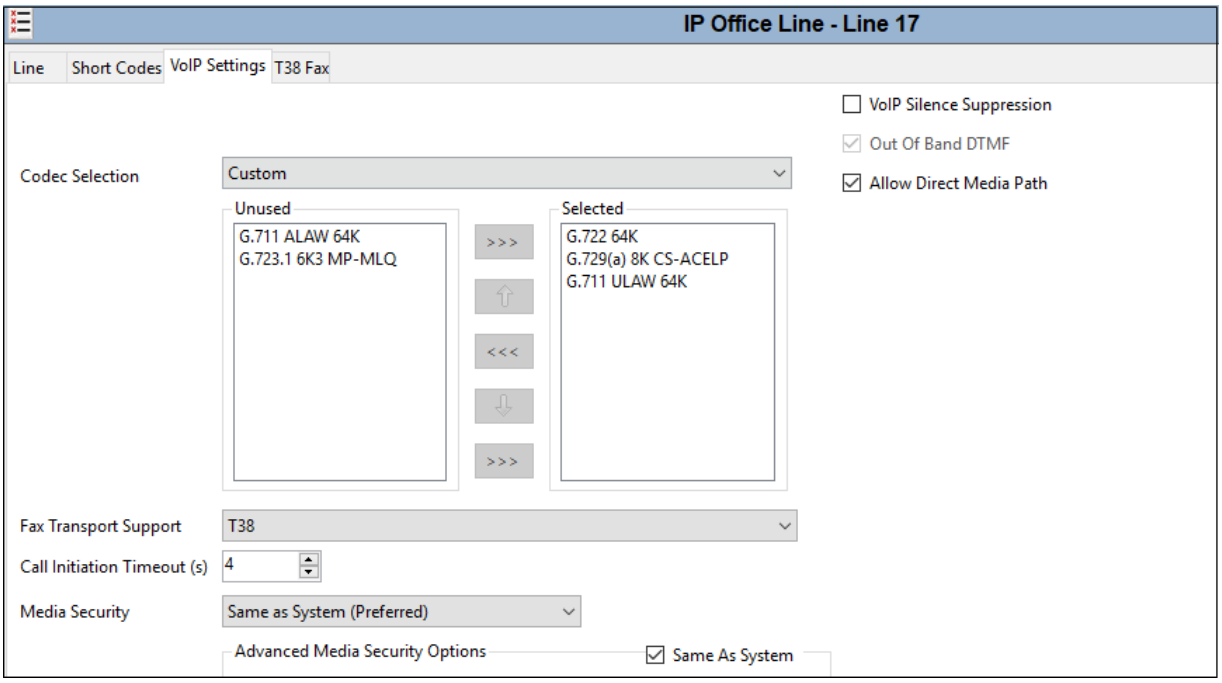
©2020 Avaya Inc. All Rights Reserved.

6.4. Expansion System - IP Office Line

The IP Office Line was automatically created on each server when the Expansion System is added to the solution. Below is the IP Office Line to the Primary server.

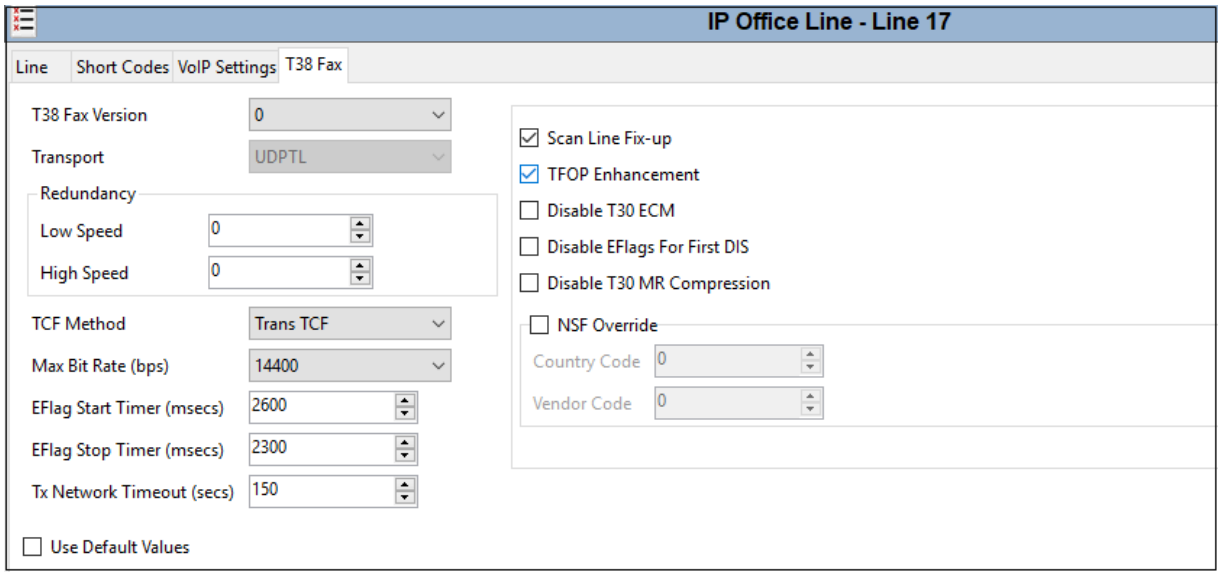


In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. To accommodate T.38 fax, select the **VoIP Settings** tab and set **Fax Transport Support** to **T38.**



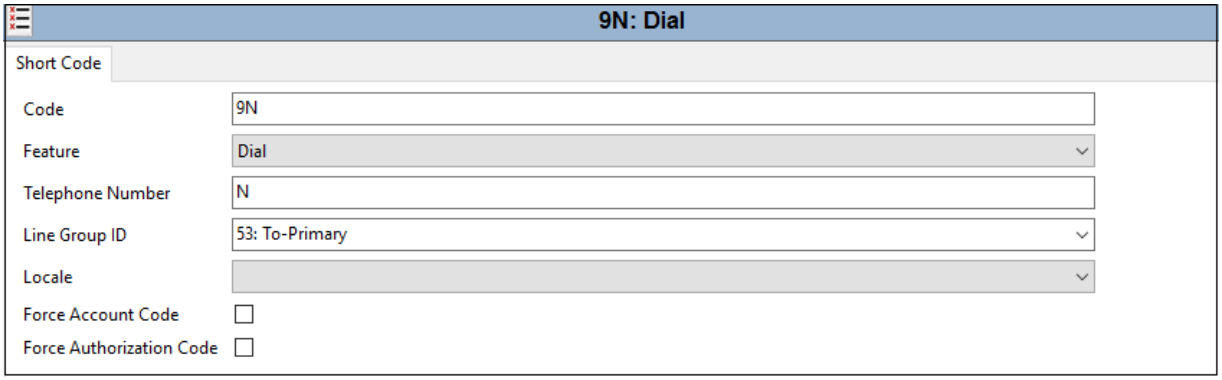
©2020 Avaya Inc. All Rights Reserved.

Select the **T38 Fax** tab. The **Use Default Values** box is unchecked, and the **T38 Fax Version** is set to "**0**". All other values are left at default.



6.5. Expansion System - Short Codes

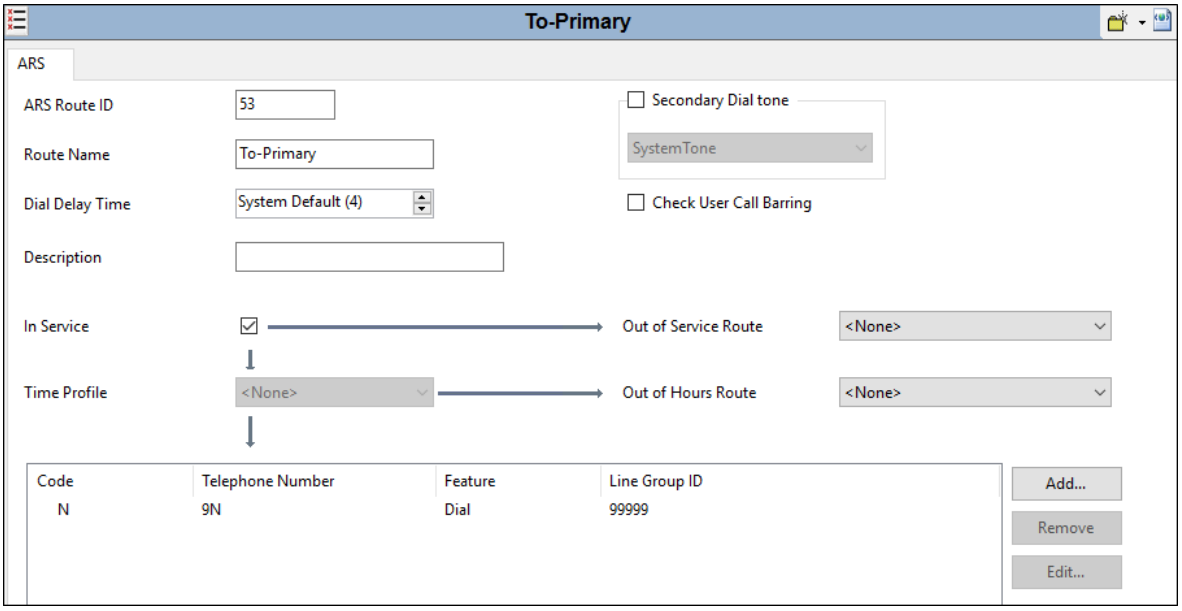
Similar to the configuration of the Primary server in **Section 5.8**, create a Short Code to access ARS. In the reference configuration, the **Line Group ID** is set to the ARS route illustrated in the next section.



©2020 Avaya Inc. All Rights Reserved.

6.6. Expansion System - Automatic Route Selection – ARS

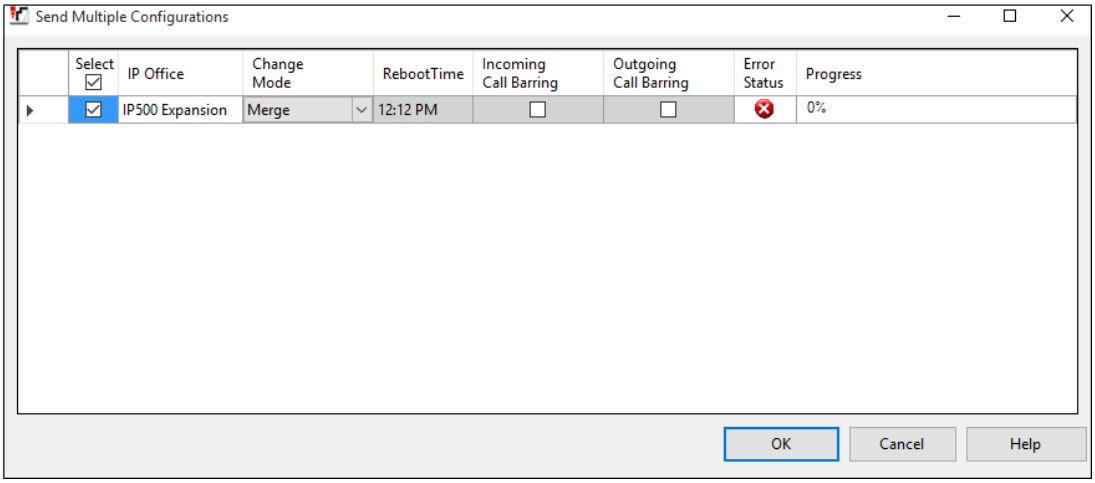
The following screen shows an example ARS configuration for the route named "**To-Primary**" on the Expansion System. The **Telephone Number** is set to **9N**. The **Line Group ID** is set to "**99999**" matching the number of the **Outgoing Group** configured on the IP Office Line 17 to the Primary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



©2020 Avaya Inc. All Rights Reserved.

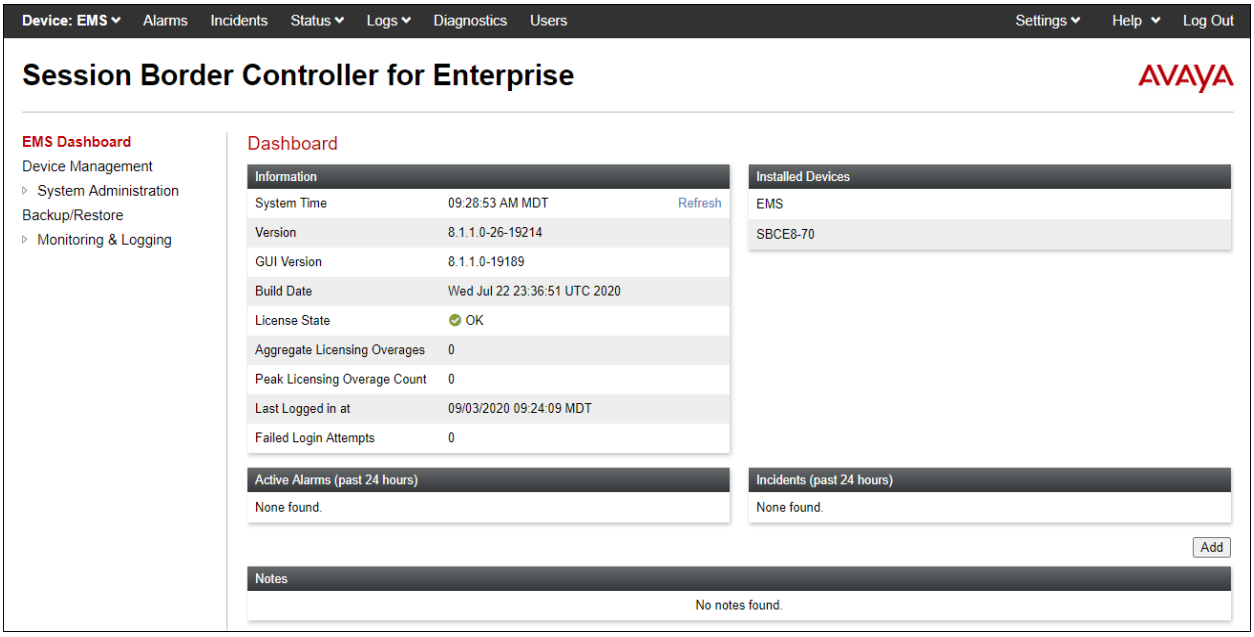
7. Configure Avaya Session Border Controller for Enterprise

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.

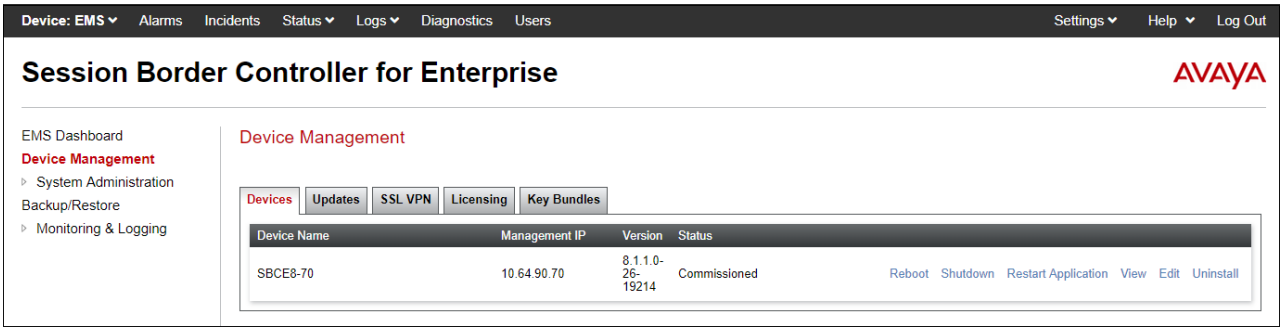
The EMS Dashboard page of the Avaya SBCE will appear. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.



7.1. Device Management – Status

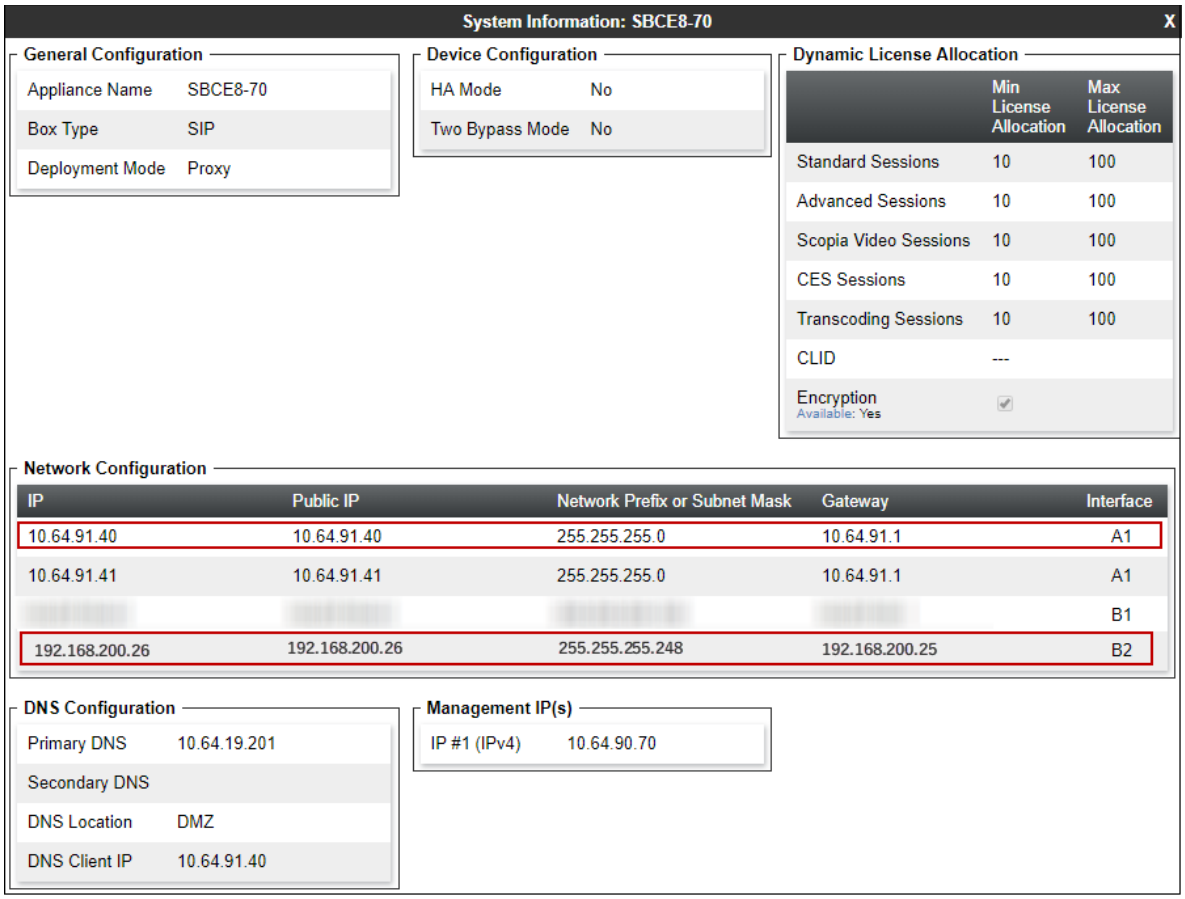
Select **Device Management** on the left-hand menu. A list of installed devices is shown on the **Devices** tab on the right pane. In the case of the sample configuration, a single device named **SBCE8-70** is shown. Verify that the **Status** column shows **Commissioned**. If not, contact your Avaya 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.



©2020 Avaya Inc. All Rights Reserved.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. In the shared test environment, the highlighted **A1** and **B2** IP addresses are the ones relevant to the configuration of the SIP trunk to AT&T.



System Information: SBCE8-70

General Configuration

Appliance Name	SBCE8-70
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	10	100
Advanced Sessions	10	100
Scopia Video Sessions	10	100
CES Sessions	10	100
Transcoding Sessions	10	100
CLID	---	
Encryption Available: Yes	✓	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.91.40	10.64.91.40	255.255.255.0	10.64.91.1	A1
10.64.91.41	10.64.91.41	255.255.255.0	10.64.91.1	A1
[illegible]	[illegible]	[illegible]	[illegible]	B1
192.168.200.26	192.168.200.26	255.255.255.248	192.168.200.25	B2

DNS Configuration

Primary DNS	10.64.19.201
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.64.91.40

Management IP(s)

IP #1 (IPv4)	10.64.90.70

©2020 Avaya Inc. All Rights Reserved.

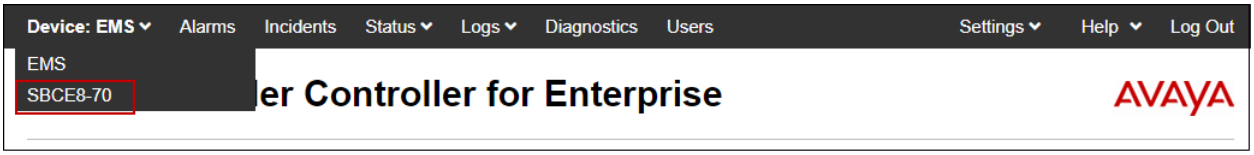
7.2. TLS Management

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.

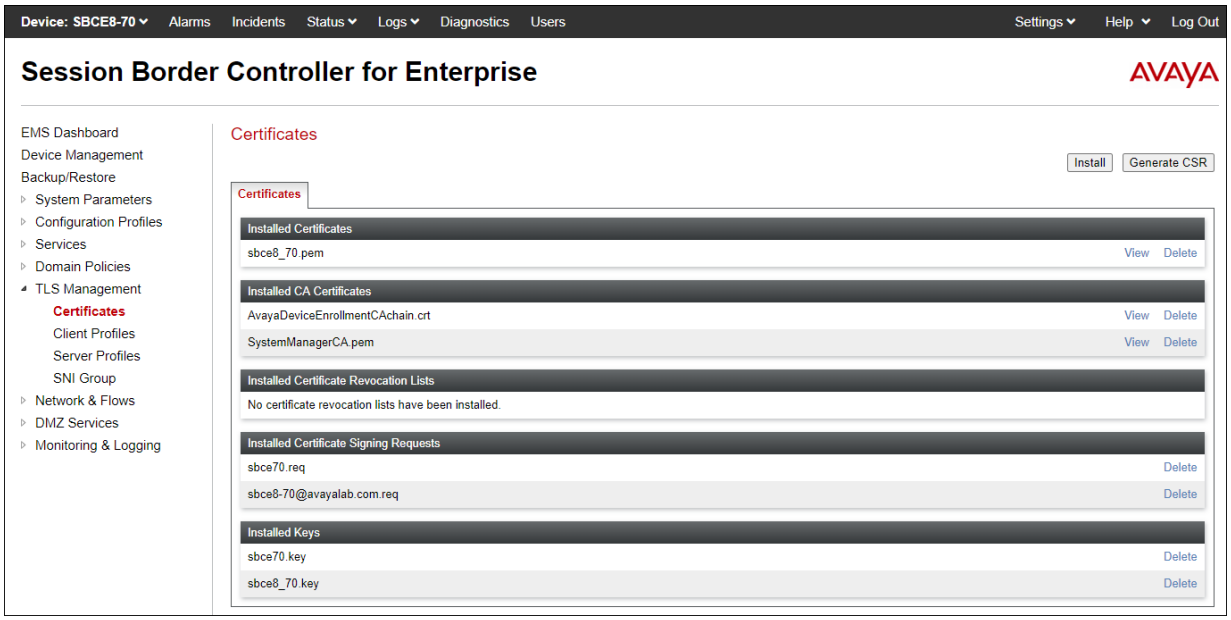
7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

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



Select **TLS Management → Certificates** from the left-hand menu. Verify the following:

- 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.



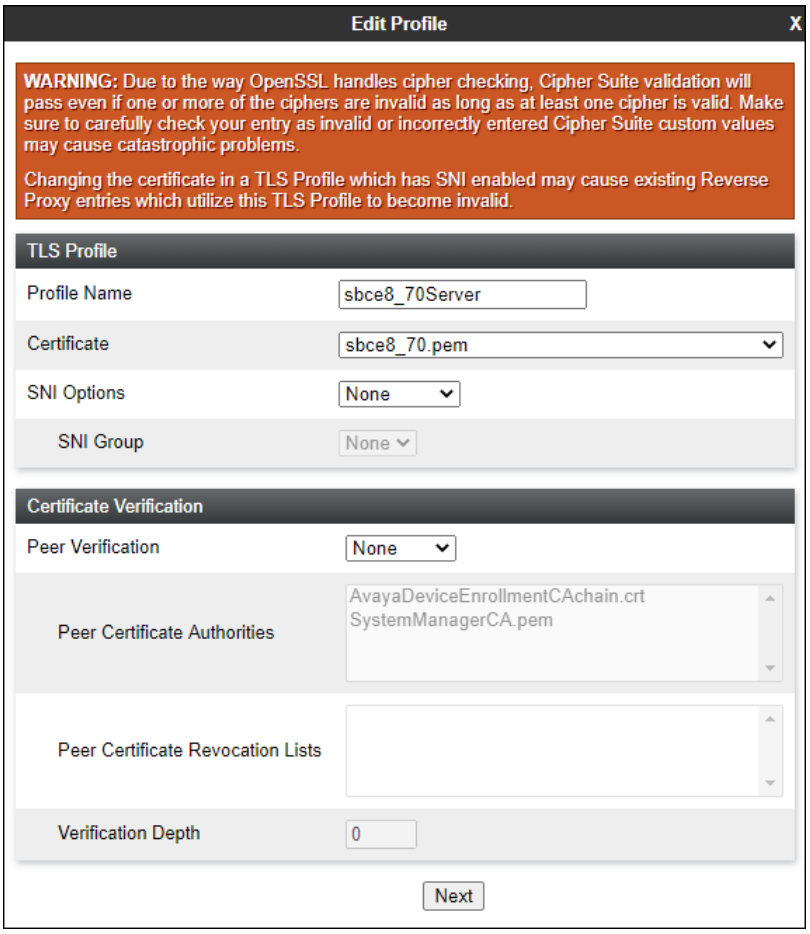
©2020 Avaya Inc. All Rights Reserved.

7.2.2. Server Profiles

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

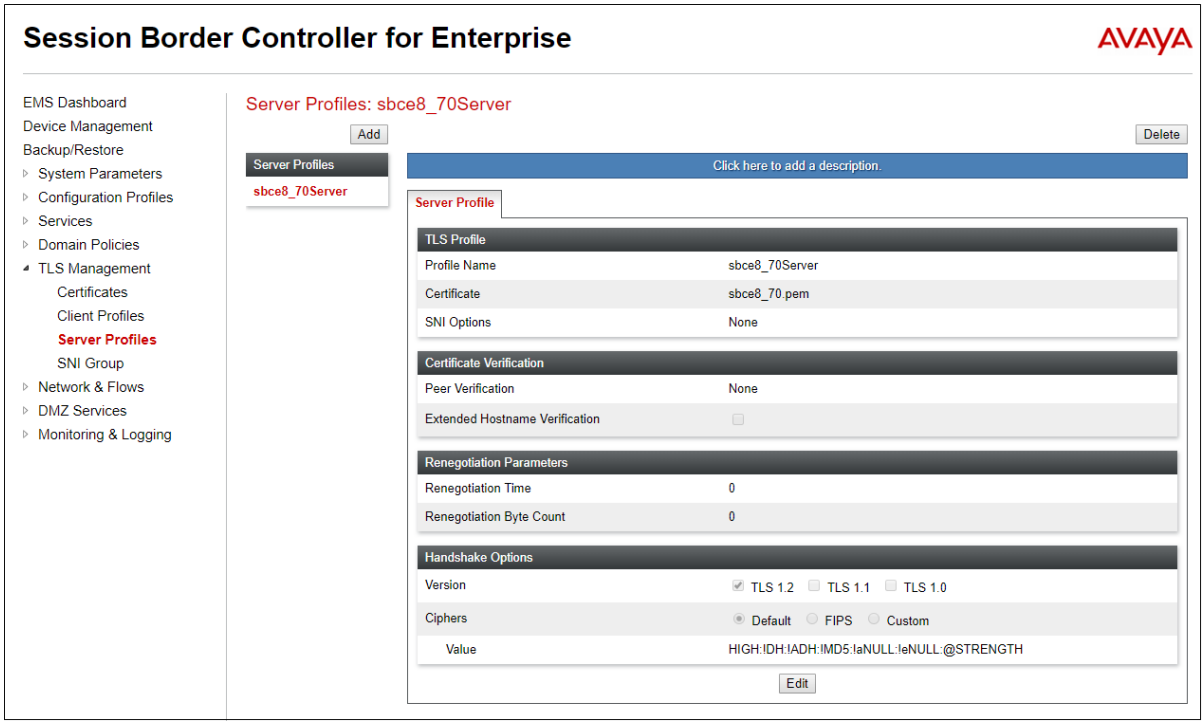
- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbce8_70.pem**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

Accept default values for the next screen (not shown) and click **Finish**.



©2020 Avaya Inc. All Rights Reserved.

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



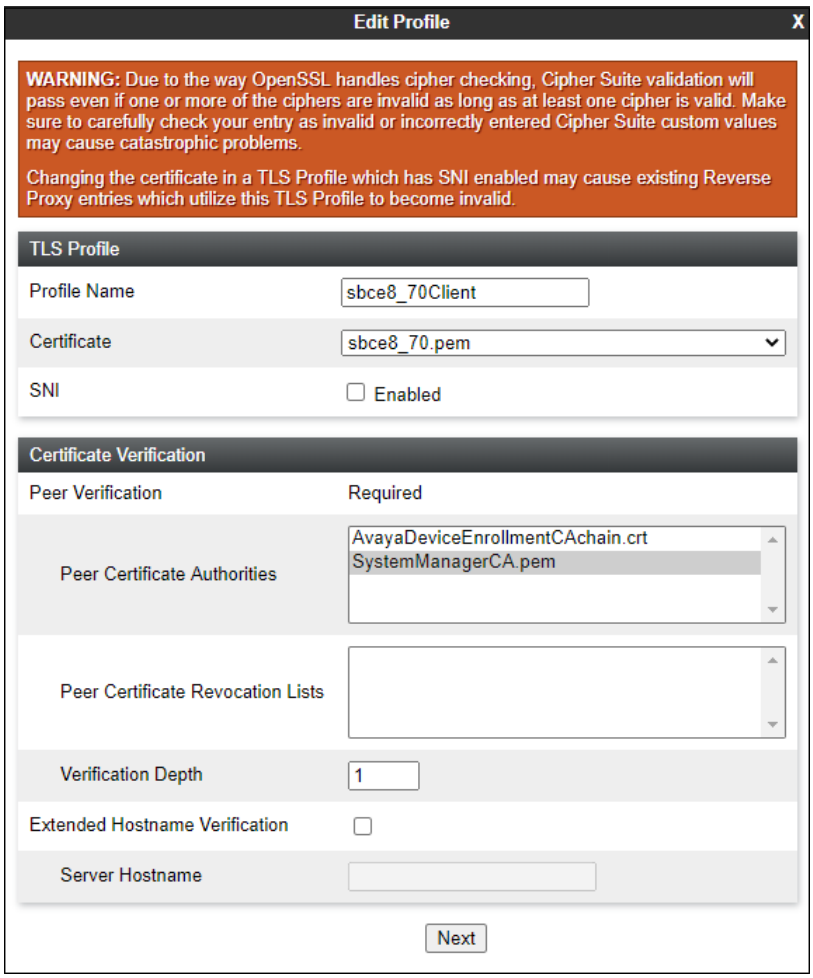
©2020 Avaya Inc. All Rights Reserved.

7.2.3. Client Profiles

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

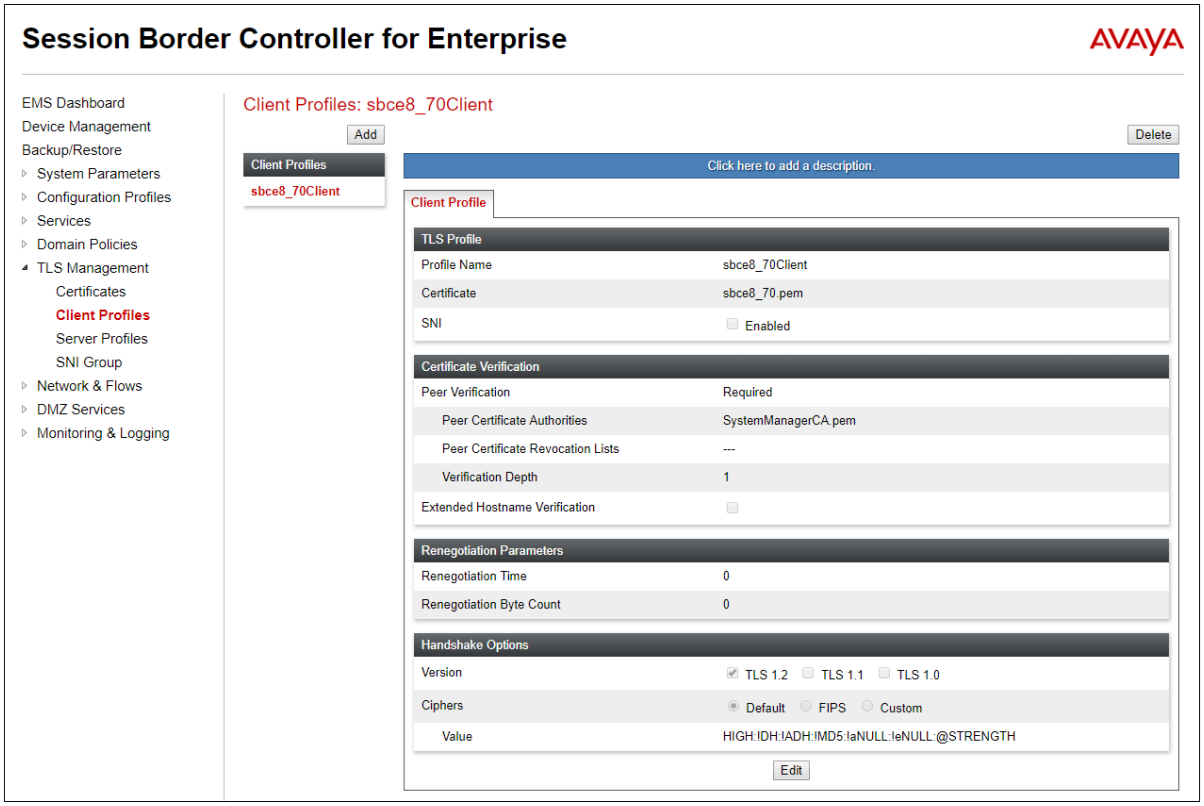
- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbce8_70.pem**, from pull down menu.
- **Peer Verification** = **Required**.
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **SystemManagerCA.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

Accept default values for the next screen (not shown) and click **Finish**.



©2020 Avaya Inc. All Rights Reserved.

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



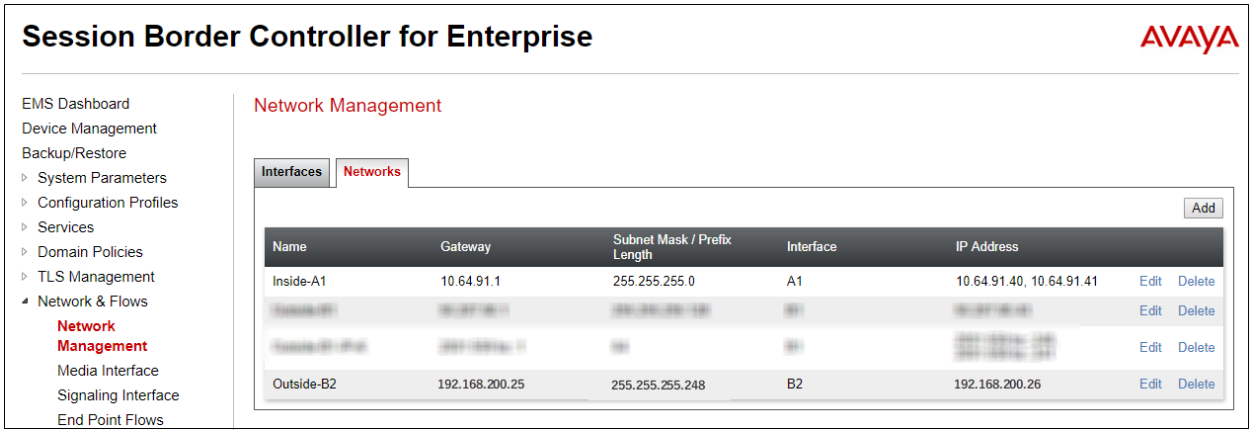
©2020 Avaya Inc. All Rights Reserved.

7.3. Network Management

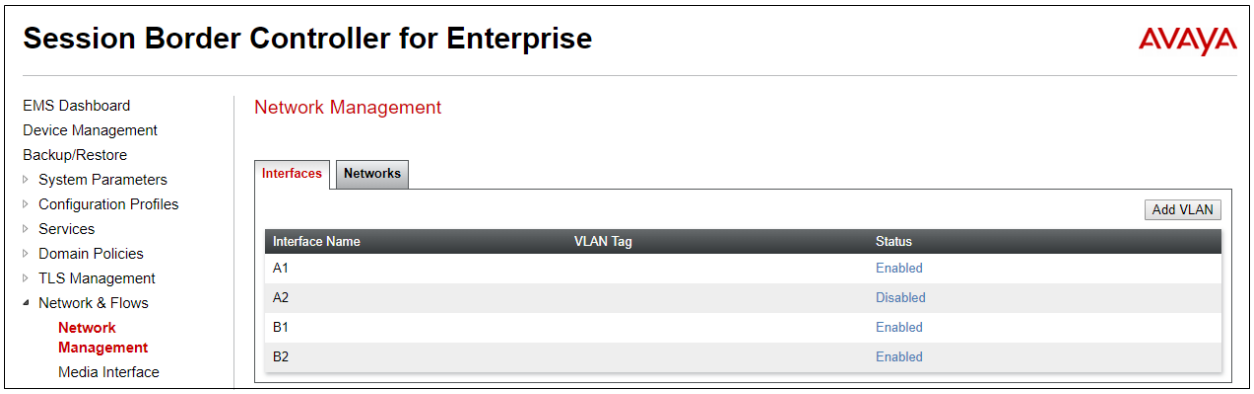
The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the 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**. On the **Networks** tab, verify the IP addresses assigned to the interfaces. The following screen shows the enterprise interface is assigned to **A1** and the interface towards AT&T is assigned to **B2**.

The following Avaya SBCE IP addresses and associated interfaces were used in the sample configuration:

- **B2: 192.168.200.26** – IP address configured for the AT&T IPFR-EF service. This address is known to AT&T. See **Section 3**.
- **A1**: **10.64.91.40** – IP address configured for AT&T IPFR-EF service to IP Office.



Verify that the interfaces are enabled on the **Interfaces** tab. The following screen shows interfaces **A1** and **B2** with status **Enabled**. To enable an interface, click the corresponding **Disabled** link under the Status column to change it to **Enabled**.



©2020 Avaya Inc. All Rights Reserved.

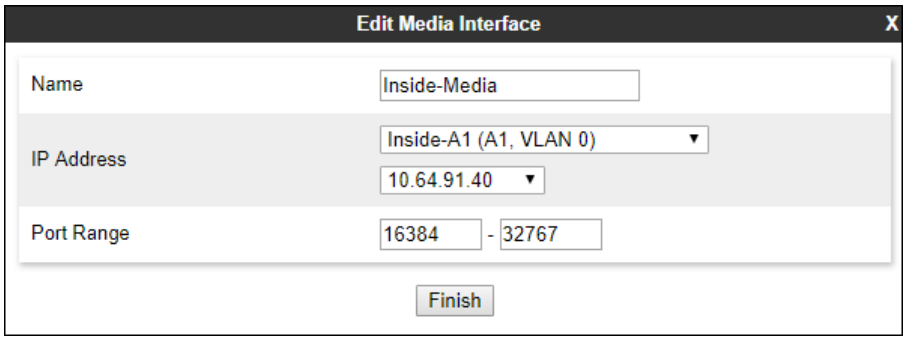
7.4. Media Interfaces

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.

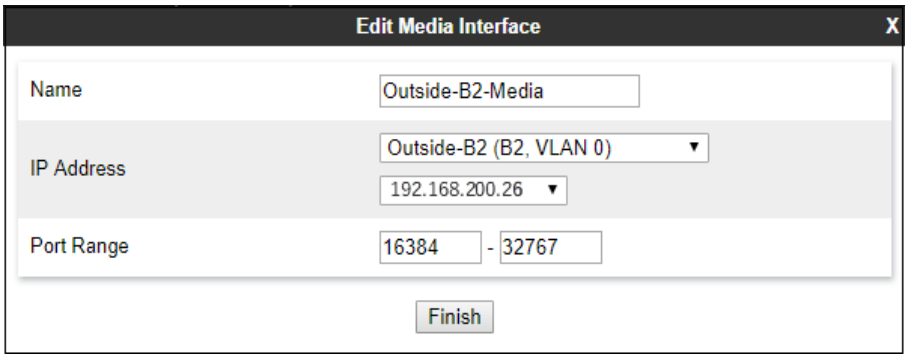
To create a new Media Interface in the enterprise direction, navigate to **Network & Flows → Media Interface** on the left-hand side menu, and click **Add** (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Select the Avaya SBCE private IP Address from the **IP Address** drop-down menu. Note that the **Port Range** was configured with the values required by AT&T (**16384** – **32767**). Click **Finish**.

Some ports in the range required by AT&T were already allocated by the Avaya SBCE for internal use, by default. See **Section 7.14** for the steps required to reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T could be accommodated.

The screen below shows the **Inside-Media** media interface created in the reference configuration.



A second Media Interface towards the AT&T network was similarly created with the name **Outside-B2-Media**, as shown below. The outside IP Address of the Avaya SBCE on the B2 interface was selected from the drop-down menu. The **Port Range** was configured with the values required by AT&T (**16384** – **32767**).

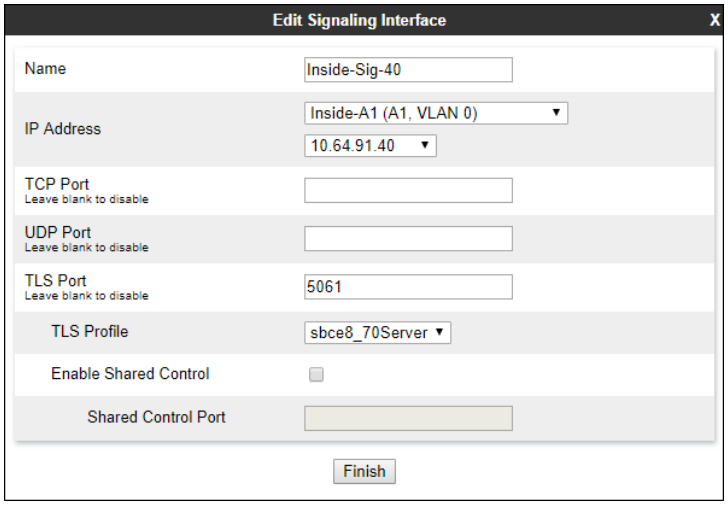


©2020 Avaya Inc. All Rights Reserved.

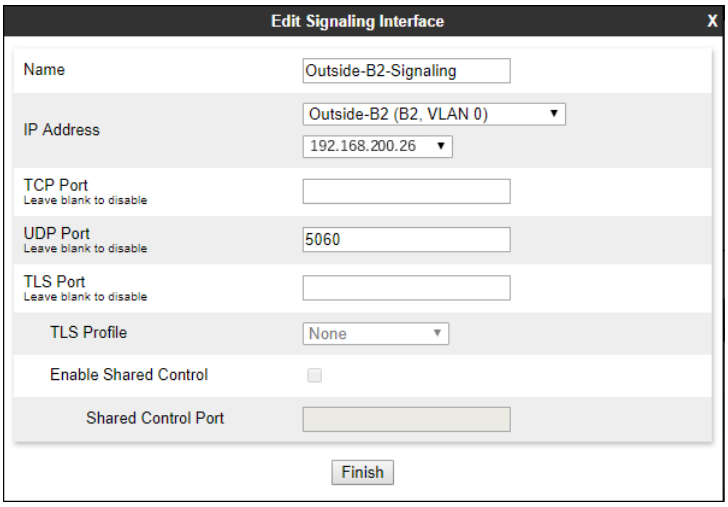
7.5. Signaling Interfaces

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 the inside and outside IP interfaces.

To create a new Signaling Interface on the enterprise direction, navigate to **Network & Flows → Signaling Interface** and click **Add**. On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. Since TLS is used in the sample configuration to listen for signaling traffic from the IP Office, **5061** is entered under **TLS Port**. The TLS Profile is set to the TLS server profile **sbce8_70Server** shown on **Section 7.2.2**. Click **Finish**.



A second Signaling Interface with the name **Outside-B2-Signaling** was similarly created in the network direction. The B2 interface IP Address of the Avaya SBCE was selected from the drop-down menu. Under **UDP Port,** enter **5060** as specified by AT&T. Click **Finish**.



©2020 Avaya Inc. All Rights Reserved.

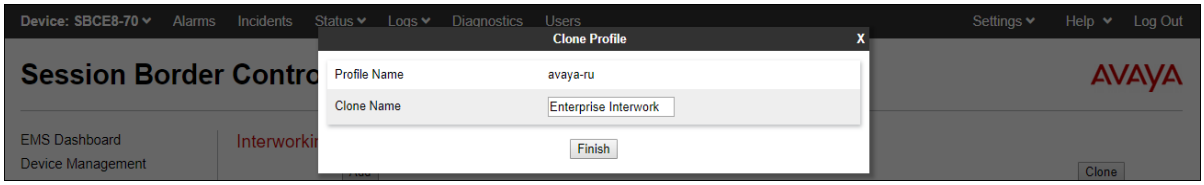
7.6. Server Interworking Profiles

The Server Internetworking profiles include 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.

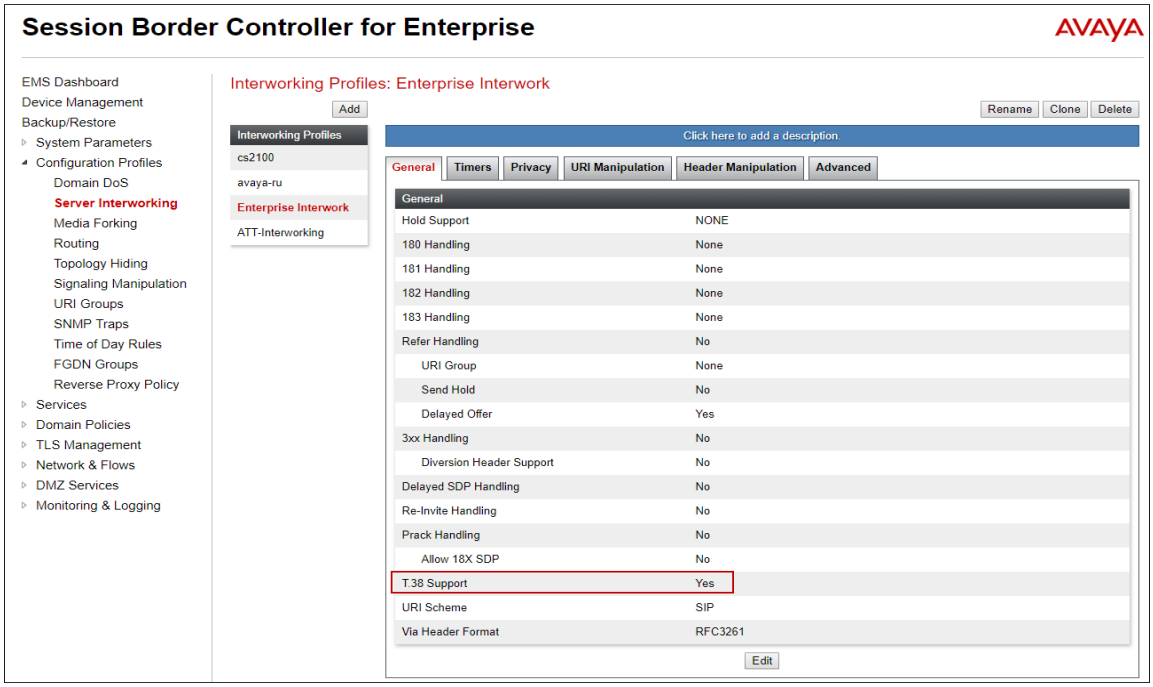
In the sample configuration, separate Server Interworking Profiles were created for IP Office and AT&T IPFR-EF service.

7.6.1. Server Interworking Profile – IP Office

In the sample 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 **avayu-ru** profile and click the **Clone** button. Enter a **Clone Name** and click **Finish** to continue.



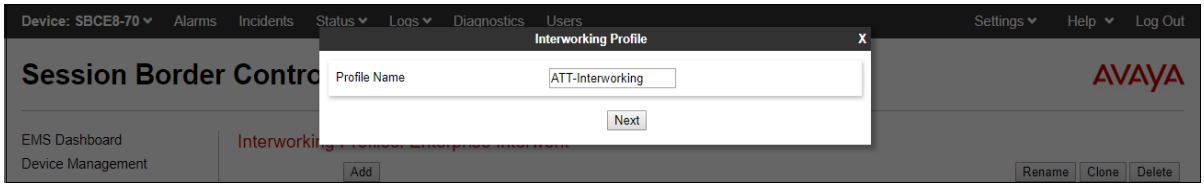
The following screen shows the **Enterprise Interwork** profile used in the sample configuration, with **T.38 Support** set to **Yes**. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish**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



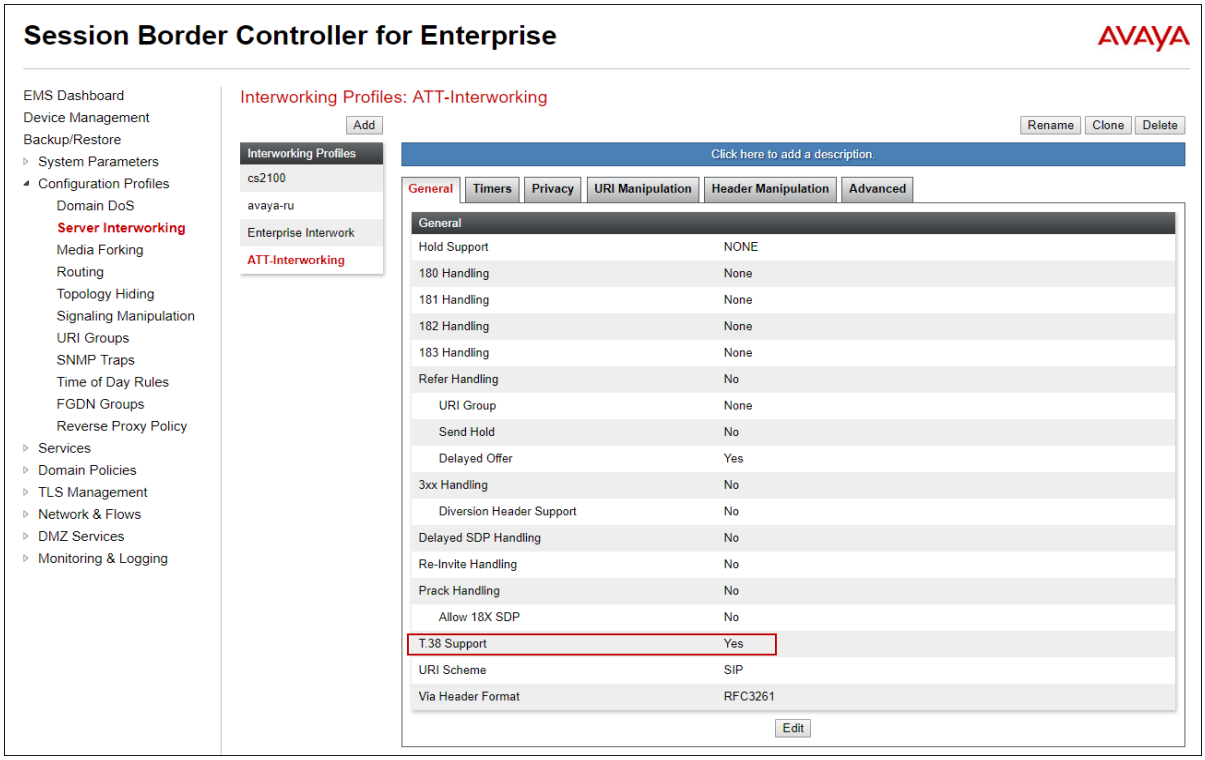
©2020 Avaya Inc. All Rights Reserved.

7.6.2. Server Interworking Profile – AT&T

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

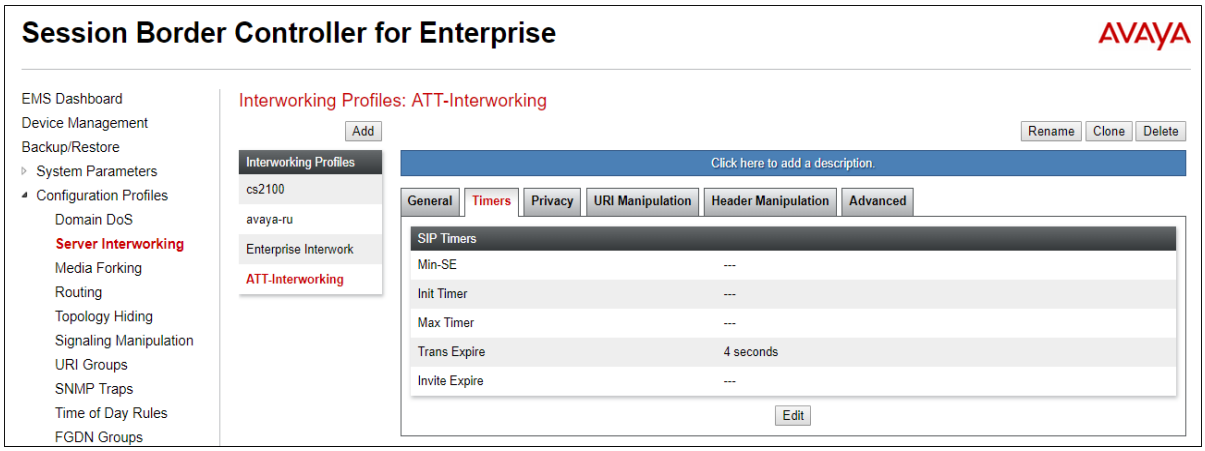


The following screens show the **ATT-Interworking** profile used in the sample configuration. On the **General** tab, default values are used with the exception of **T.38 Support** set to **Yes**.

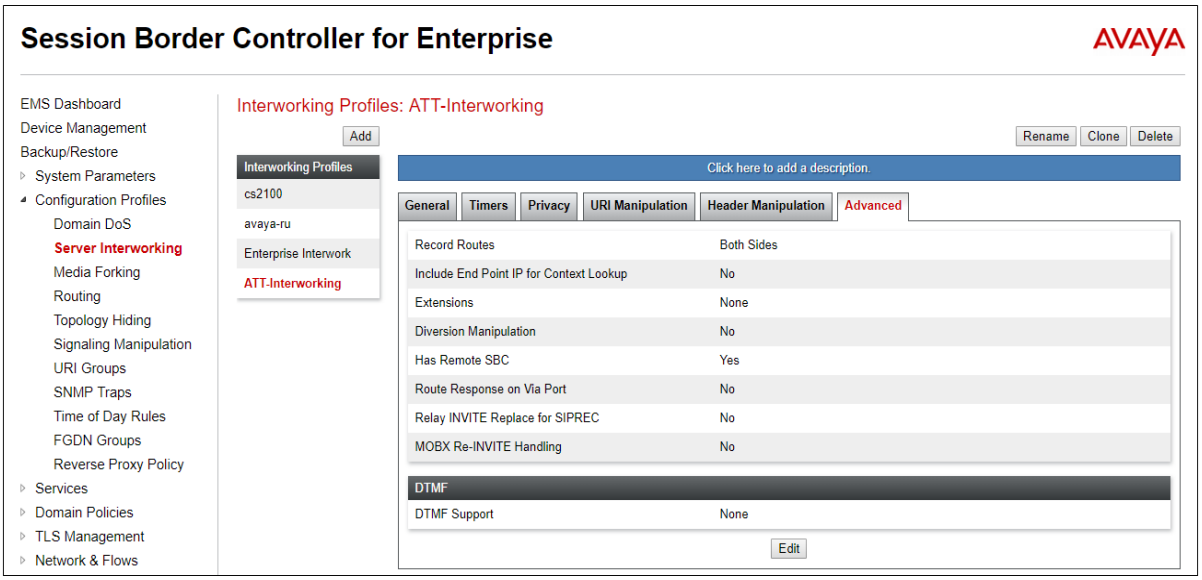


©2020 Avaya Inc. All Rights Reserved.

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 it exists (see **Sections 7.7.2** and **7.8.2** for multiple AT&T border elements configuration).



Click **Next** to accept default parameters for the **Privacy**, **URI Manipulation**, and **Header Manipulation** tabs (not shown) and advance to the **Advanced** area. **Record Routes** is set to **Both Sides**. Default values can be used for all other fields.



©2020 Avaya Inc. All Rights Reserved.

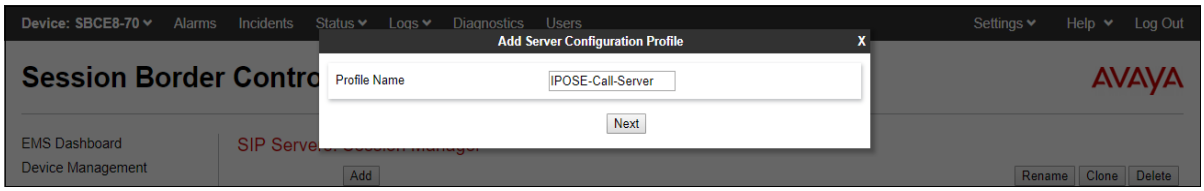
7.7. SIP Servers Profiles

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.

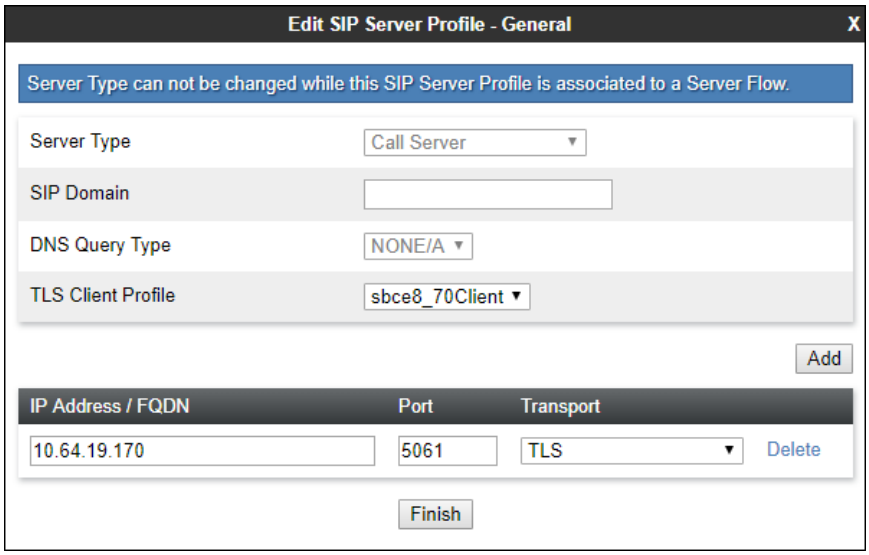
In the sample configuration, separate SIP Servers Profiles were created for the IP Office and the AT&T IPFR-EF service.

7.7.1. SIP Server Profile – IP Office

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

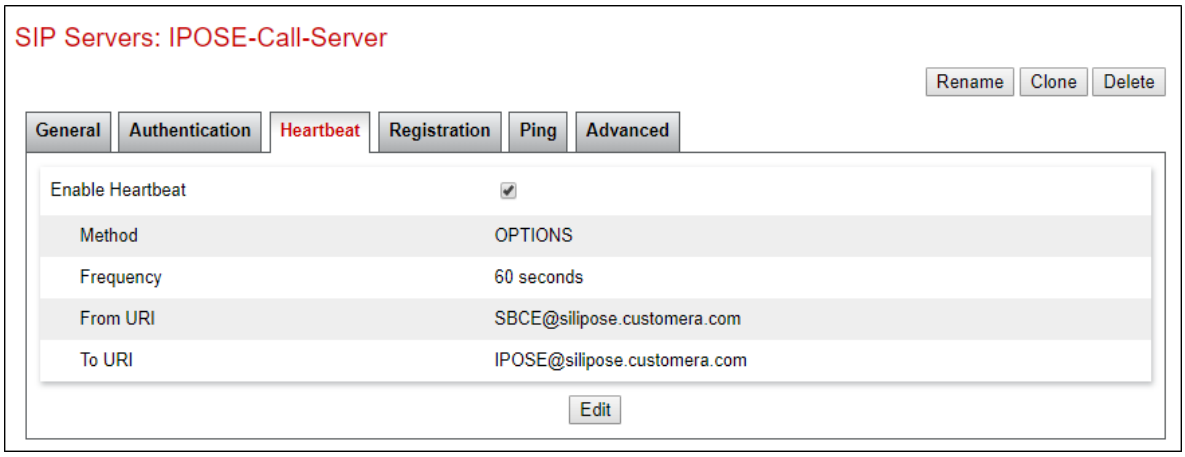


The following screens illustrate the SIP Server Profile named **IPOSE-Call-Server**. In the **General** parameters, the **Server Type** is set to **Call Server**. In the **IP Address / FQDN** field, the IP Address of IP Office LAN 1 interface in the sample configuration is entered. This IP address is **10.64.19.170**. Under **Port**, **5061** is entered, and the **Transport** parameter is set to **TLS**. The TLS profile **sbce8_70Client** 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**.

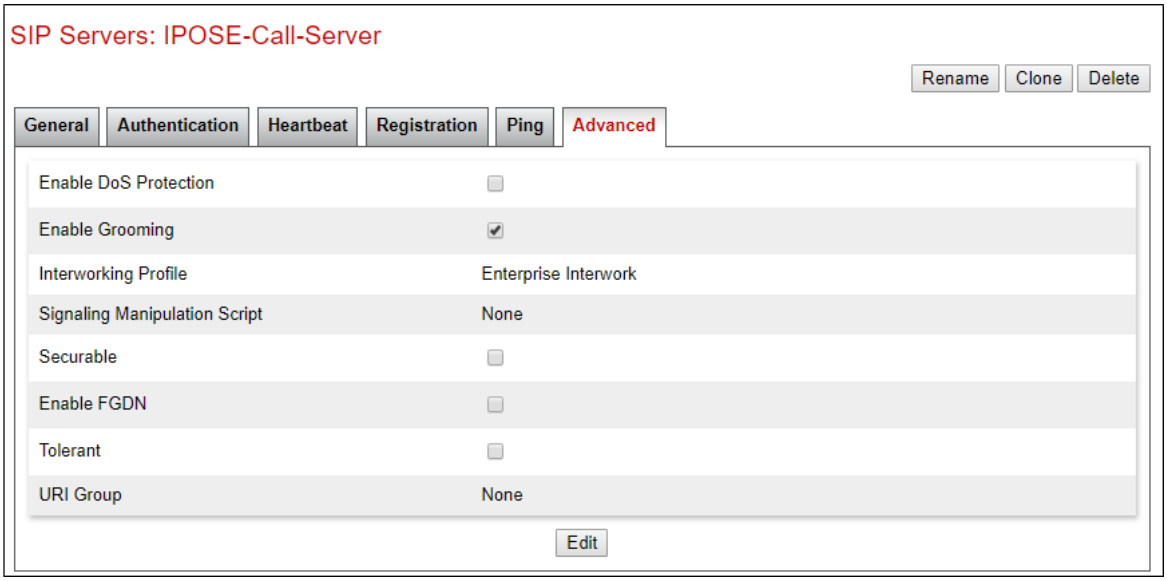


©2020 Avaya Inc. All Rights Reserved.

Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeat** tab. The Avaya SBCE can be optionally 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 towards IP Office.



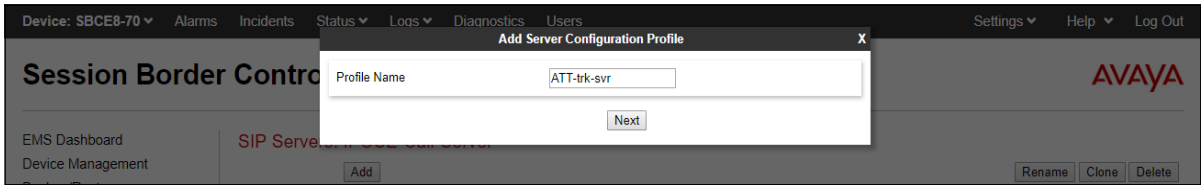
On the **Advanced** tab, **Enable Grooming** is check and the **Interworking Profile** is set to **Enterprise Interwork** created in **Section 7.6.1** for IP Office.



©2020 Avaya Inc. All Rights Reserved.

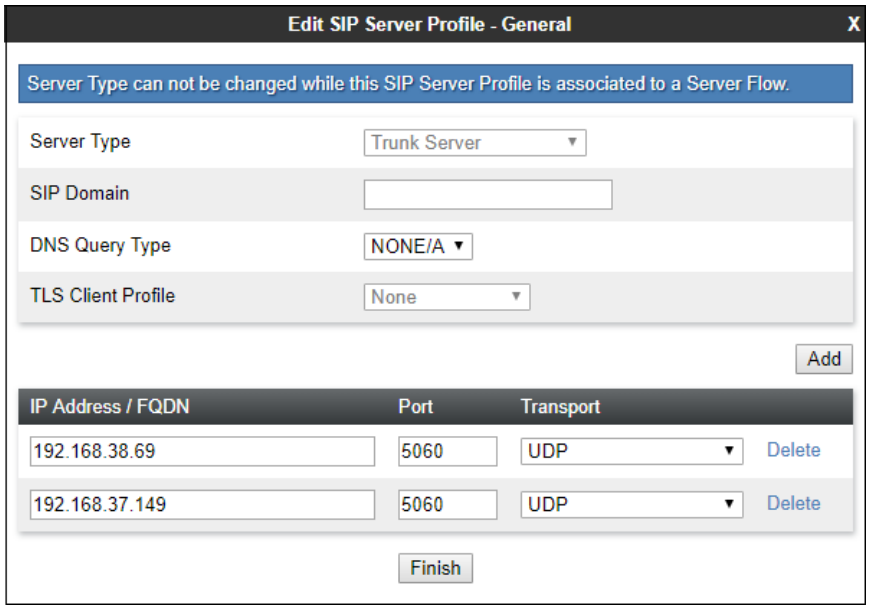
7.7.2. SIP Server Profile – AT&T

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



In the reference configuration, AT&T provided two network border elements, **192.168.38.69** (Primary) and **192.168.37.149** (Secondary), for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration.

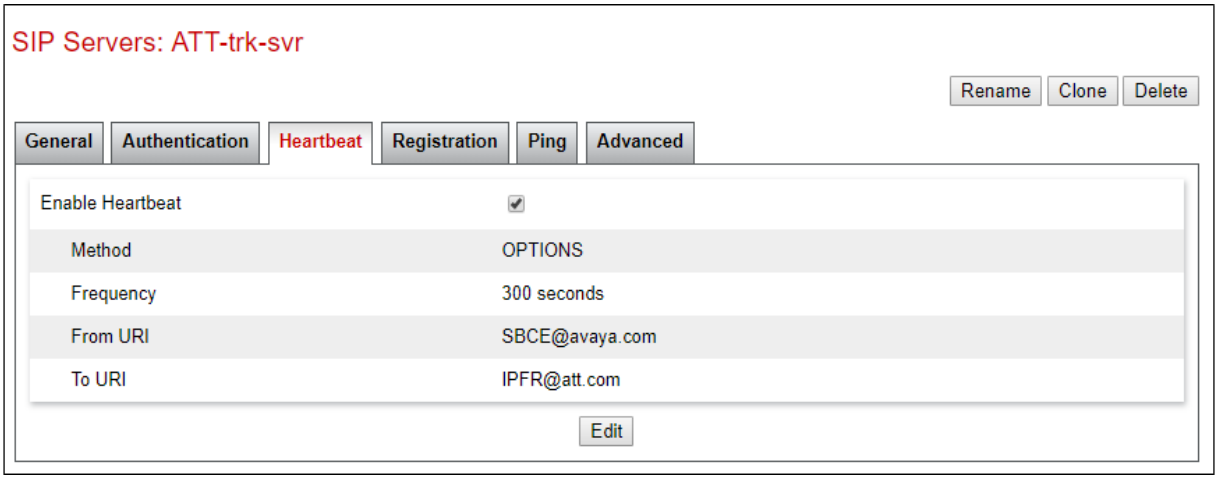
The following screens illustrate the SIP Server Profile **ATT-trk-svr**. In the **General** parameters, the **Server Type** is set to **Trunk Server**. In the **IP Address / FQDN** fields, the AT&T-provided network border elements IP addresses are entered. This is **192.168.38.69** (Primary) and **192.168.37.149** (Secondary). Under **Port**, **5060** 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**.



©2020 Avaya Inc. All Rights Reserved.

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 AT&T. This configuration is optional. Independent of whether the Avaya SBCE is configured to source SIP OPTIONS towards AT&T, AT&T 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 private IP Address of the Avaya SBCE, the SBCE will send SIP OPTIONS to AT&T. When AT&T responds, the SBCE will pass the response to IP Office.

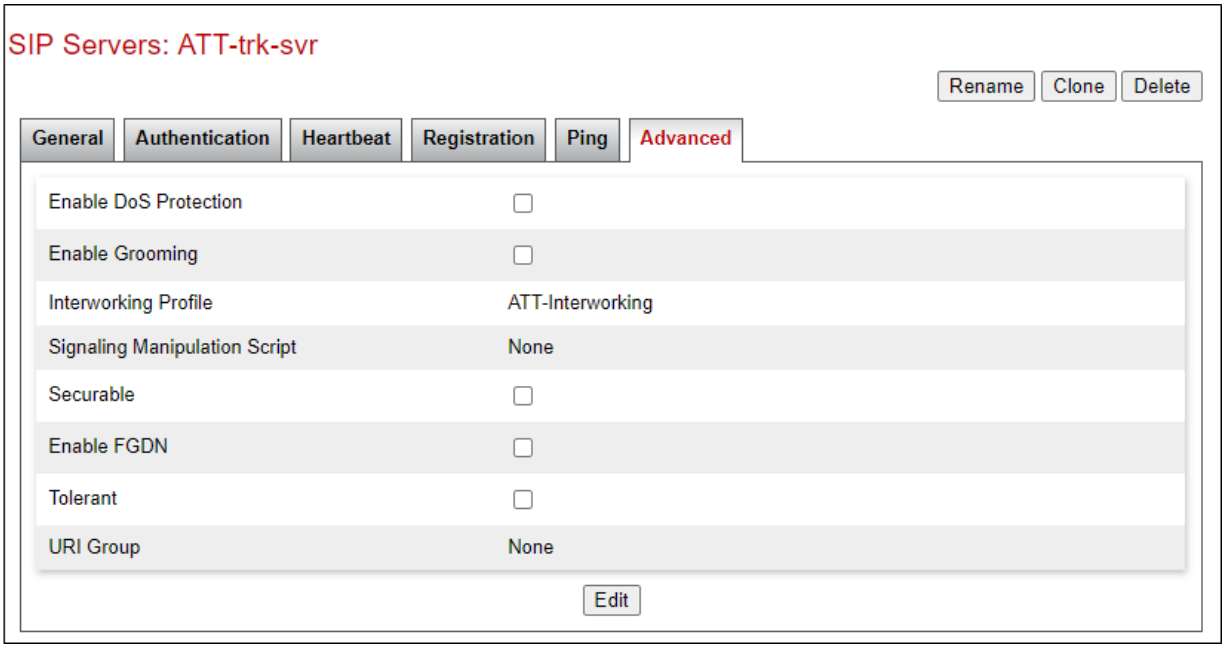
Select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE. If adding a new profile, click **Next** to continuing to the **Advanced** settings.



Note - Avaya SBCE will issue OPTIONS messages to the primary (192.168.38.69) and secondary (192.168.37.149) border elements. If the SBCE fails to get a response to the OPTIONS sent to 192.168.38.69, the SBCE will redirect outbound calls to 192.168.37.149.

©2020 Avaya Inc. All Rights Reserved.

On the **Advanced** tab, **Enable Grooming** is not used for UDP connections and is left unchecked. The **Interworking Profile** is set to **ATT-Interworking** created in **Section 7.6.2** for AT&T.



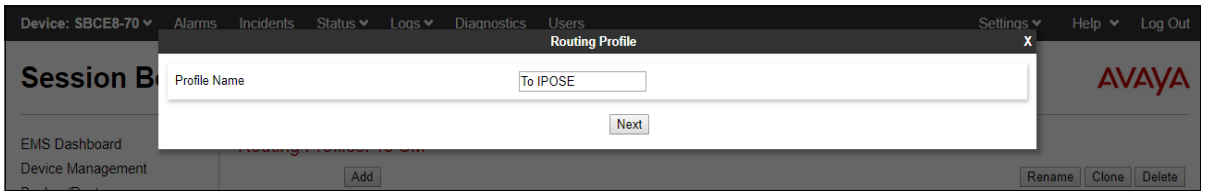
©2020 Avaya Inc. All Rights Reserved.

7.8. Routing Profiles

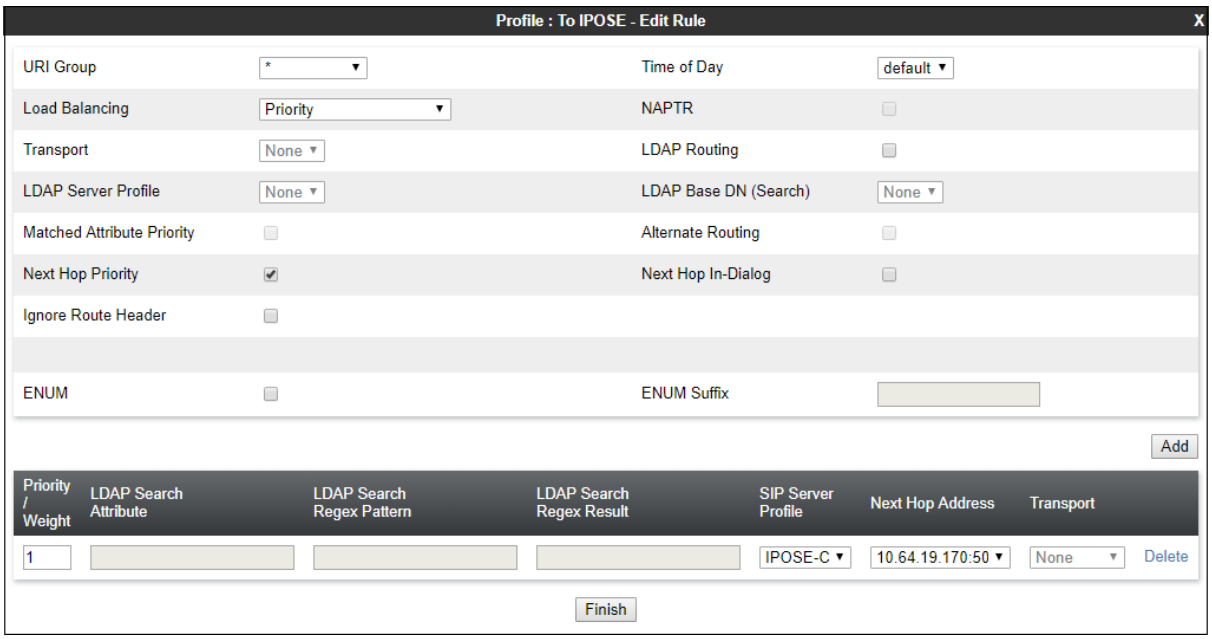
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport 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 AT&T IPFR-EF service.

7.8.1. Routing Profile – IP Office

To add the 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 **To IPOSE** created in the sample configuration. The parameters in the top portion of the profile are left at their default settings. Clicking the **Add** button on this screen allows to enter the routing rule at the bottom of the profile. 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** (IP address, port and transport) is automatically selected with the values from the IP Office SIP Server Profile, and **Transport** becomes grayed out. Click **Finish**.



©2020 Avaya Inc. All Rights Reserved.

7.8.2. Routing Profile – AT&T

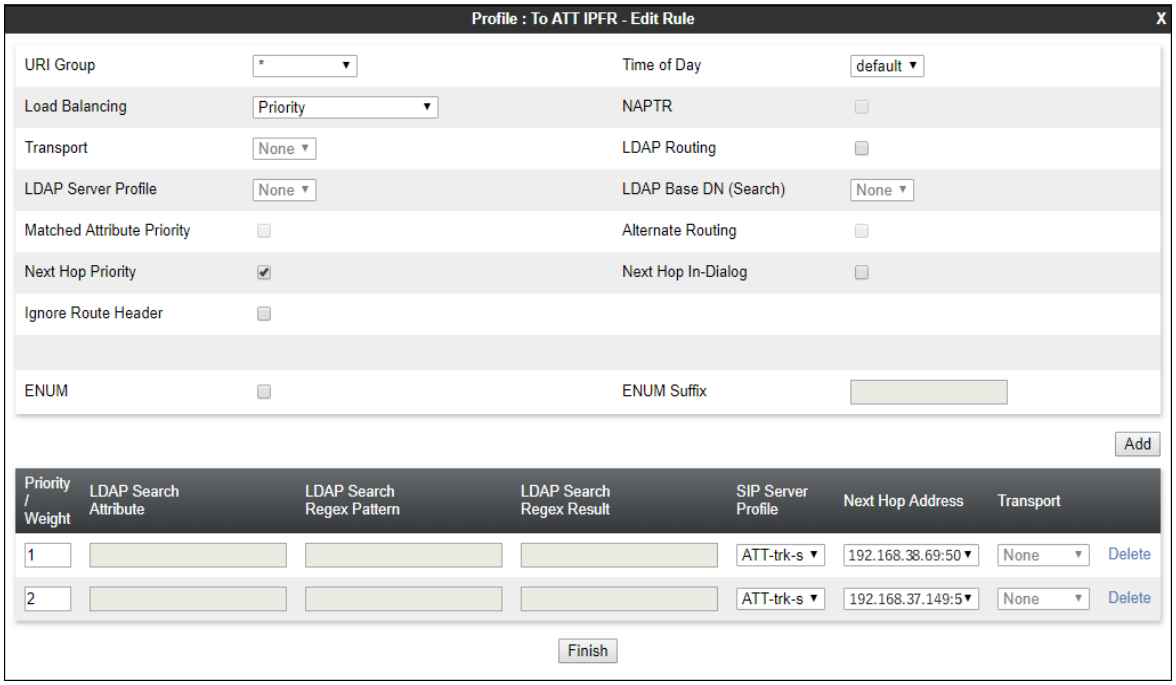
Similarly, add a Routing Profile to AT&T. The following screen shows the Routing Profile **To ATT IPFR** created in the sample configuration. The parameters in the top portion of the profile are left at their default settings.

For the first routing rule (AT&T Primary Border Element), set the following:

- Set **Priority / Weight** to **1**
- **SIP Server Profile**: select the AT&T profile created in **Section 7.7.2** from the drop-down menu.
- On the **Next Hop Address** select **192.168.38.69:5060 (UDP)** from the drop-down menu.

For the second routing rule (AT&T Secondary Border Element):

- Set **Priority / Weight** to **2**
- **SIP Server Profile**: select the AT&T profile created in **Section 7.7.2** from the drop-down menu.
- On the **Next Hop Address** select **192.168.37.149:5060 (UDP)** from the drop-down menu.
- Click **Finish**.



Note – If desired, the **Load Balancing** parameter may be used to modify how the two defined AT&T Border Elements are accessed. **Priority** was used in the Reference Configuration.

©2020 Avaya Inc. All Rights Reserved.

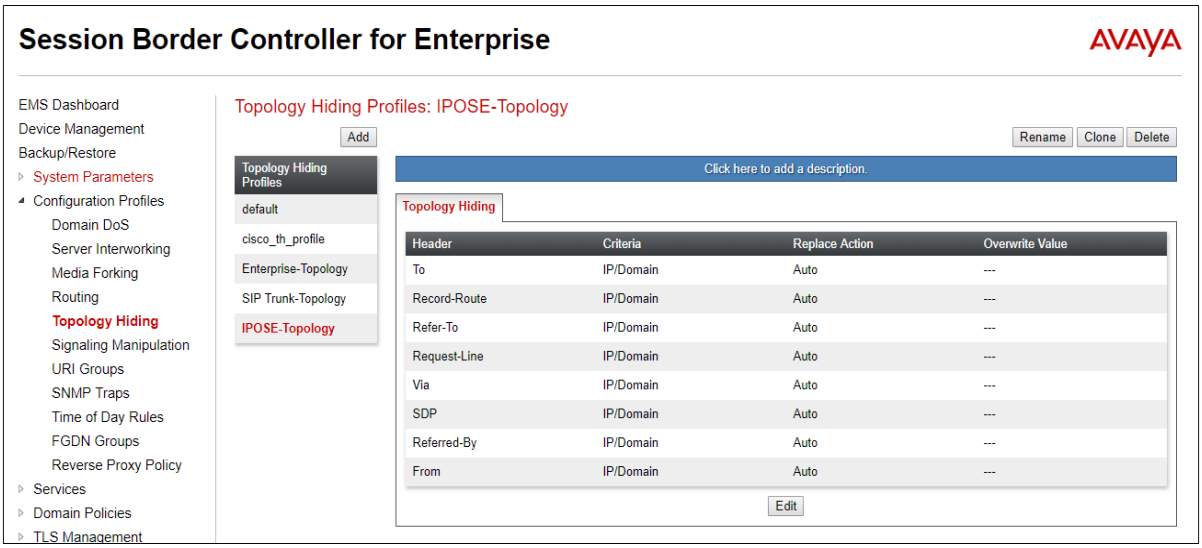
7.9. Topology Hiding Profiles

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.

To create the Topology Hiding profiles for IP Office and AT&T, navigate to **Configuration Profiles → Topology** Hiding. Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the sample configuration, the **default** profile was cloned for both IP Office and AT&T. They will later be applied to the Server Flows in **Section 7.15**.

In the **Replace Action** column an action of **Auto** will replace the header field with the IP address of the Avaya SBCE interface and the **Overwrite** will use the value in the **Overwrite Value**.

In the example shown, **IPOSE-Topology** was cloned from the default. A second profile, **SIP-Trunk-Topology** (not shown) was similarly cloned from the default.

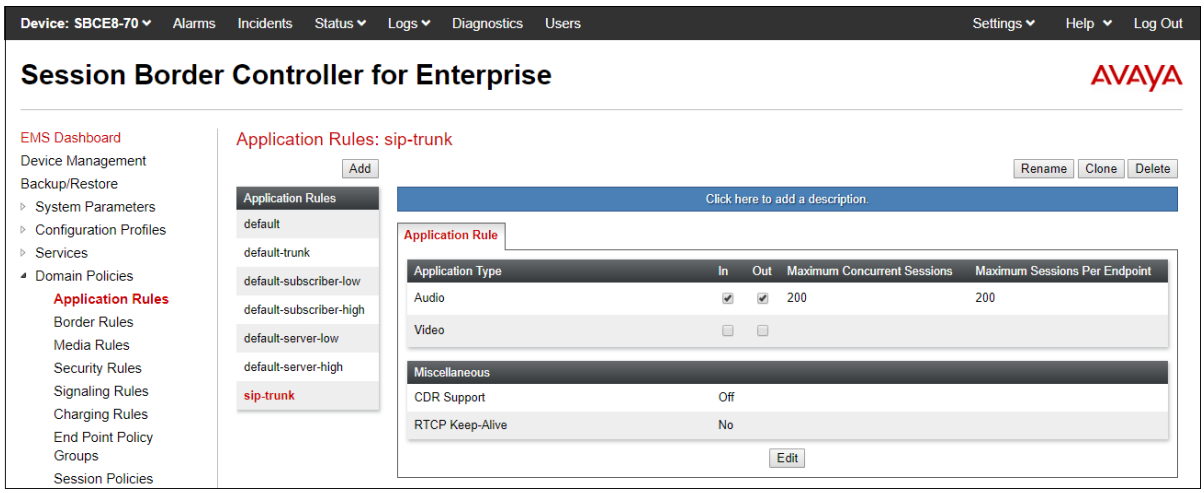


©2020 Avaya Inc. All Rights Reserved.

7.10. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, you can determine the maximum number of concurrent voice and video sessions the network will process 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 application rule to edit. In the sample configuration, the **sip-trunk** rule was created for IP Office and AT&T. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** and **Video** applications to a value slightly larger than the licensed sessions. For example, if licensed for 150 session set the values to **200**. The **Maximum Session Per Endpoint** should match the **Maximum Concurrent Sessions**.



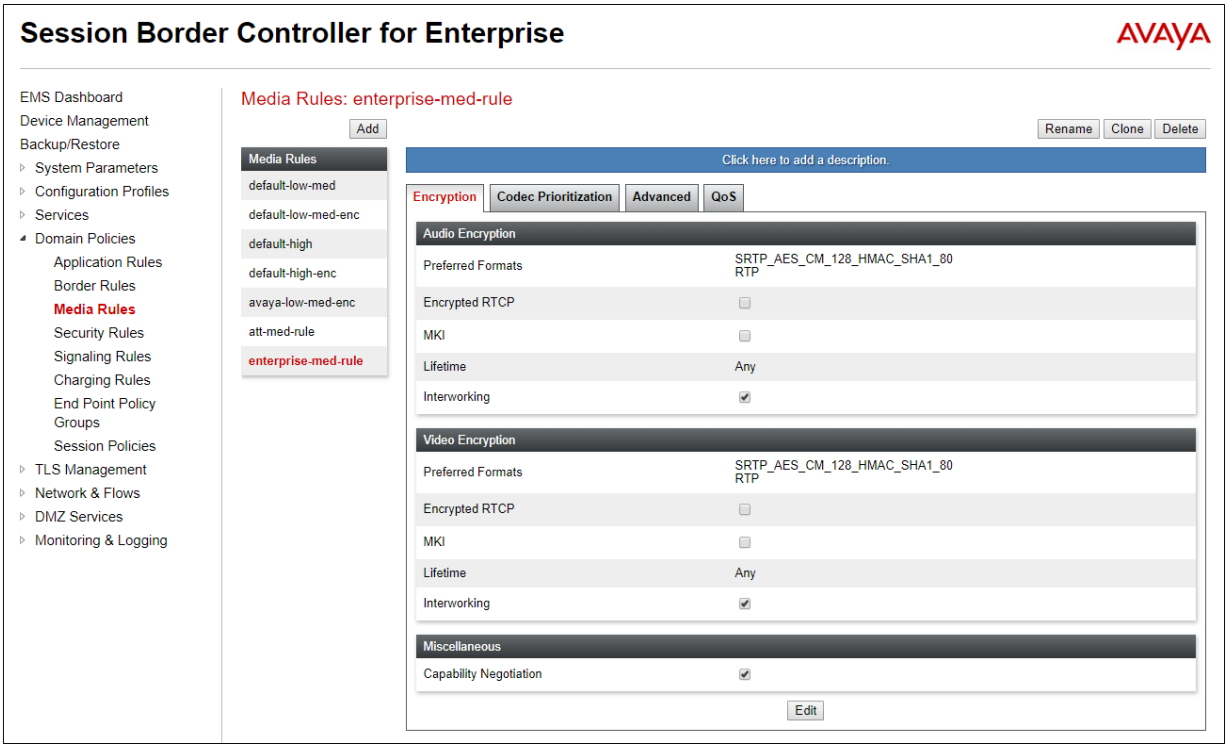
©2020 Avaya Inc. All Rights Reserved.

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).

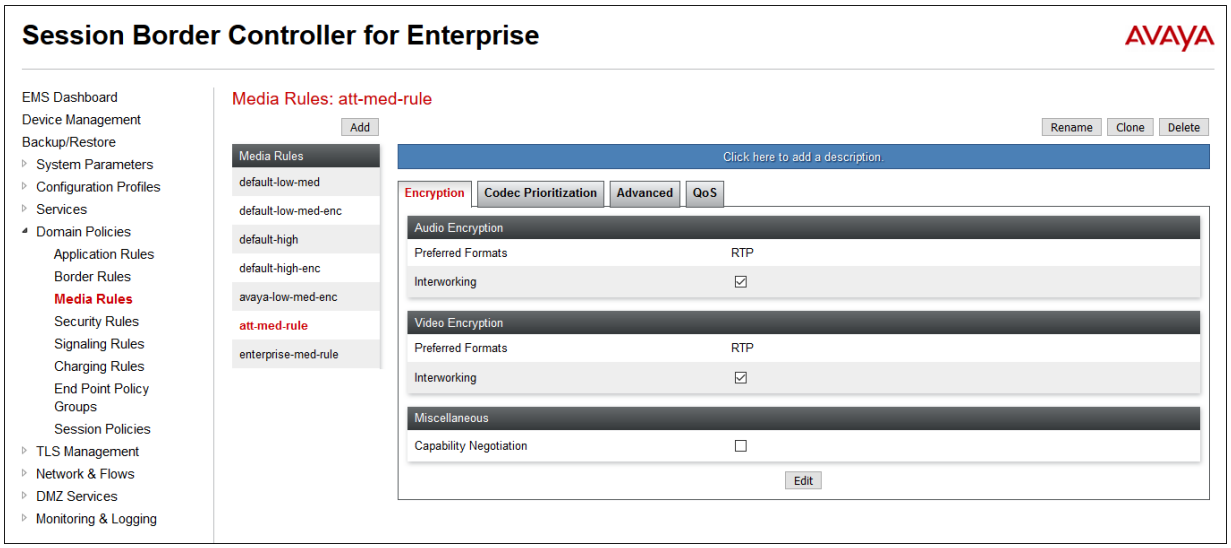
The Media Rule **enterprise-med-rule** created for the IP Office is shown below.



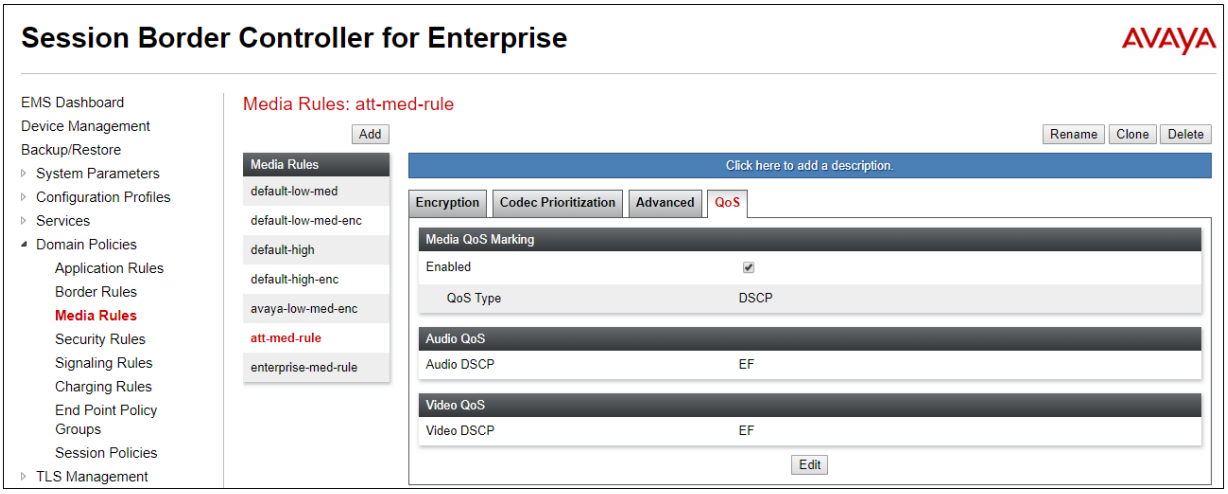
©2020 Avaya Inc. All Rights Reserved.

Similarly, the default **default-low-med** rule was cloned to create the Media Rule for AT&T IPFR-EF.

The Media Rule named **att-med-rule** used in the sample configuration for AT&T is shown below:



Note the DSCP values **EF** for expedited forwarding (default value) used for **Media QoS**.

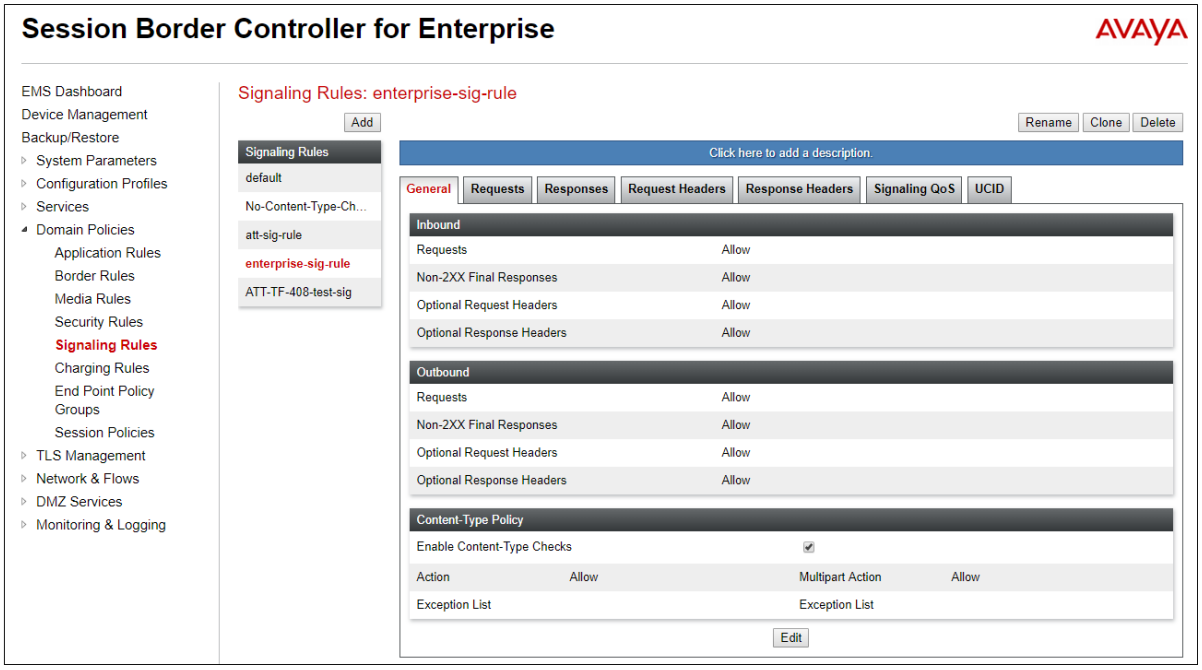


©2020 Avaya Inc. All Rights Reserved.

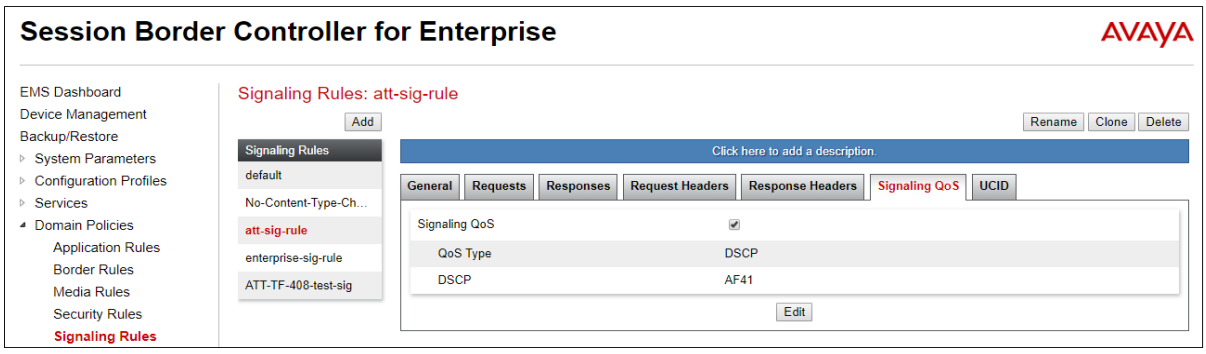
7.12. Signaling Rules

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. When SIP signaling packets are received by Avaya SBCE, they are parsed and "pattern-matched" against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Clone and modify the **default** signaling rule 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 sample configuration, Signaling Rule **enterprise-sig-rule** was left unchanged from the default rule.



Signaling Rule **att-sig-rule** was also cloned from the **default** rule and used for AT&T. The DSCP value **AF41** for assured forwarding (default value) was set for **Signaling QoS**.

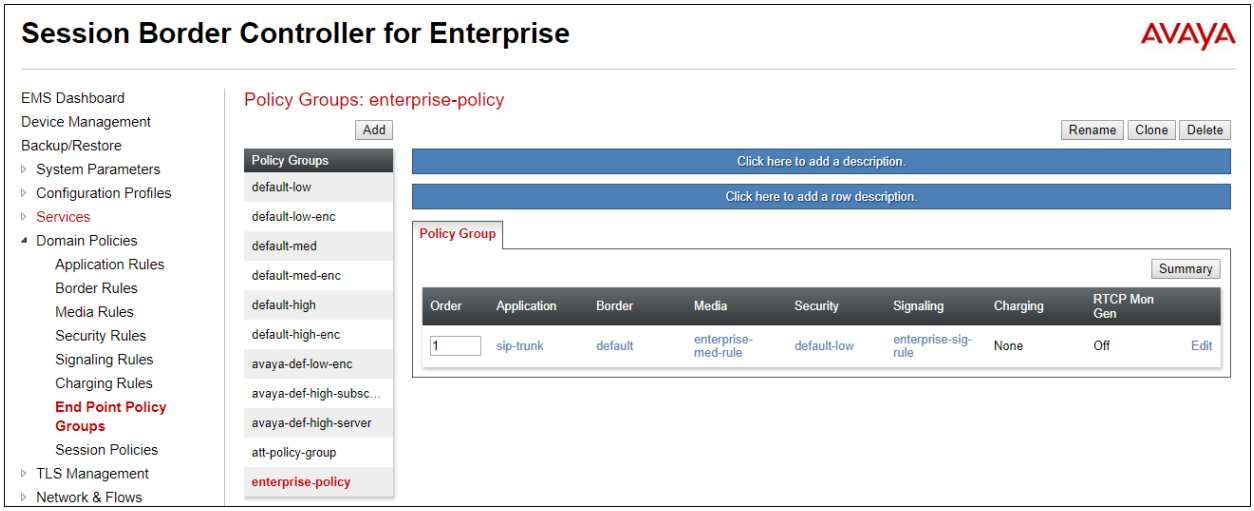


©2020 Avaya Inc. All Rights Reserved.

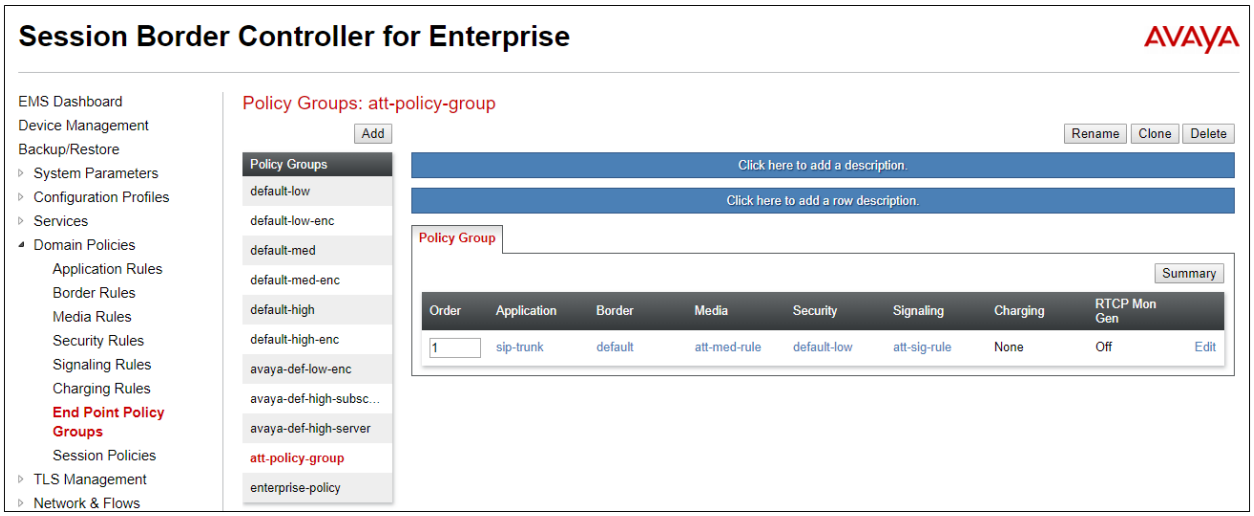
7.13. Endpoint Policy Groups

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 7.15**.

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 **enterprise-policy** created for IP Office. The details of the non-default rules chosen are shown in previous sections.



The following screen shows the **att-policy-group** created for AT&T. The details of the non-default rules chosen are shown in previous sections.

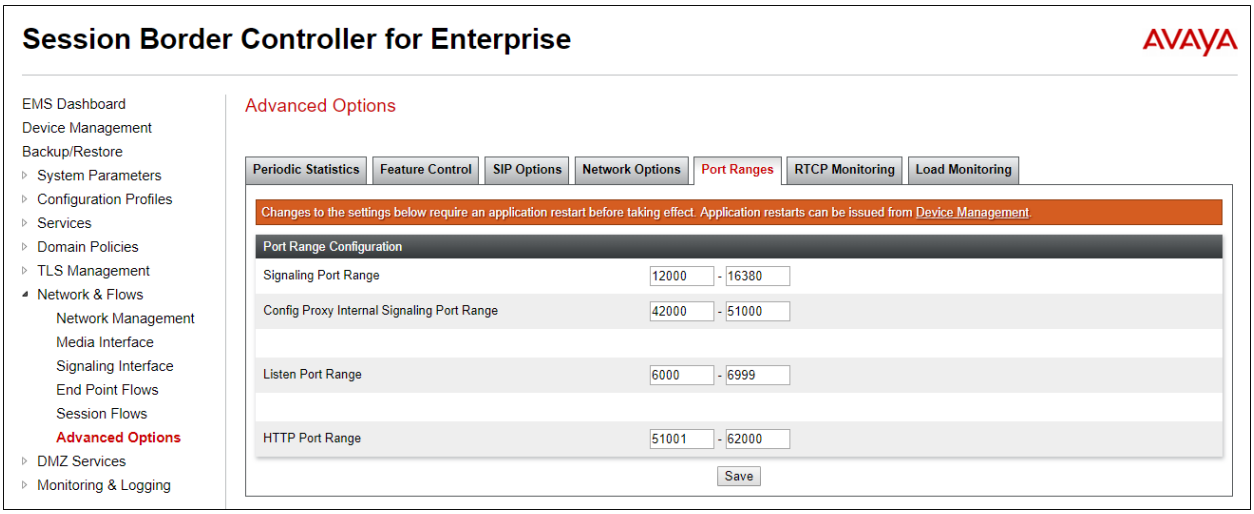


©2020 Avaya Inc. All Rights Reserved.

7.14. Advanced Options

In **Section 7.4**, the media UDP port ranges required by AT&T are configured (**16384** – **32767**). However, by default ranges 12000 to 21000 and 22000 to 31000 are already allocated by the Avaya SBCE for internal use. The following steps reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T can be defined in **Section 7.4**.

Step 1 - Select **Network & Flows → Advanced Options** from the menu on the left-hand side.
Step 2 - Select the **Port Ranges** tab.
Step 3 - In the **Signaling Port Range** row, change the range to **12000** – **16380**
Step 4 - In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000** – **51000**.
Step 5 – In the **Listen Port Range** row, change the range to **6000** – **6999**.
Step 6 – In the **HTTP Port Range** row, change the range to **51001** – **62000**.
Step 7 - Select **Save**. Note that changes to these values require an application restart (see **Section 7.1**).



©2020 Avaya Inc. All Rights Reserved.

7.15. End Point Flows - Server Flow

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 AT&T IPFR-EF service. To create a Server Flow, navigate to **Network & Flows → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown).

The following screen shows the flow named **IPO Flow production** viewed from the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.

View Flow: IPO Flow Production X

Criteria

Flow Name	IPO Flow Production
Server Configuration	IPOSE-Call-Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Outside-B2-Signaling

Profile

Signaling Interface	Inside-Sig-40
Media Interface	Inside-Media
Secondary Media Interface	None
End Point Policy Group	enterprise-policy
Routing Profile	To ATT IPFR
Topology Hiding Profile	IPOSE-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	

©2020 Avaya Inc. All Rights Reserved.

Once again, select the **Server Flows** tab and click **Add**. The following screen shows the flow named **IPFR flow** viewed from the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.

View Flow: IPFR Flow X

Criteria

Flow Name	IPFR Flow
Server Configuration	ATT-trk-svr
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside-Sig-40

Profile

Signaling Interface	Outside-B2-Signaling
Media Interface	Outside-B2-Media
Secondary Media Interface	None
End Point Policy Group	att-policy-group
Routing Profile	To IPOSE
Topology Hiding Profile	SIP Trunk-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	

©2020 Avaya Inc. All Rights Reserved.

8. AT&T IP Flexible Reach – Enhanced Features Configuration

AT&T provides the IPFR-EF service border element IP address, the access DID numbers, and the associated DNIS digits used in the reference configuration. In addition, the AT&T IPFR-EF features, and their associated access numbers, are also assigned by AT&T.

9. Verification Steps

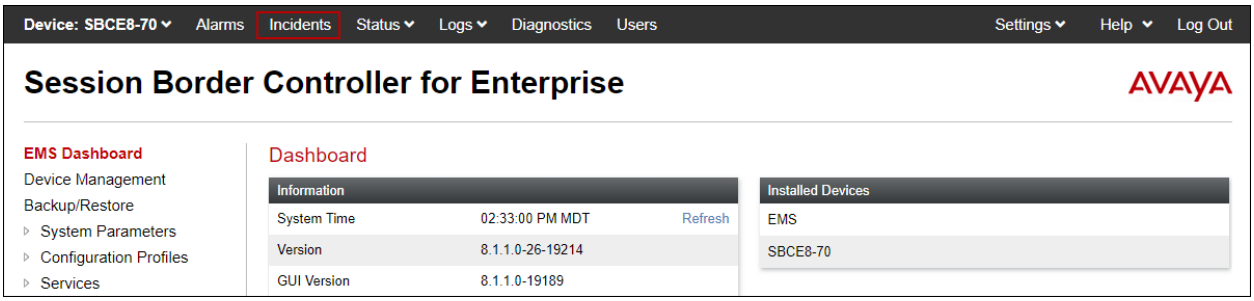
This section provides example verifications of the Avaya configuration with AT&T IPFR-EF service.

9.1. Avaya SBCE

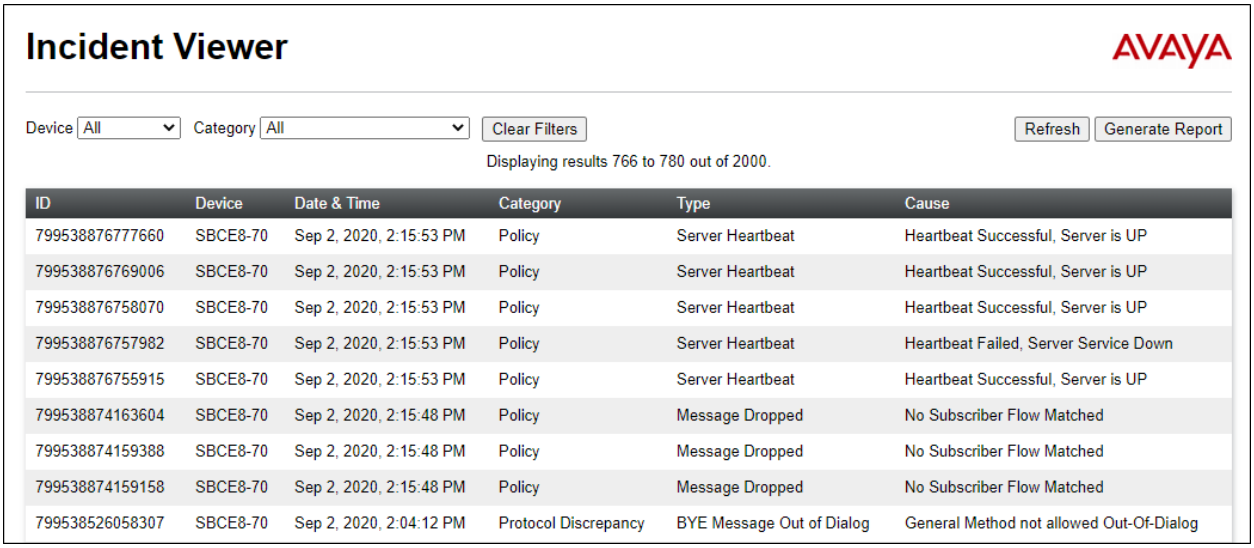
This section provides verification steps that may be performed with the Avaya SBCE.

9.1.1. Incidents

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



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

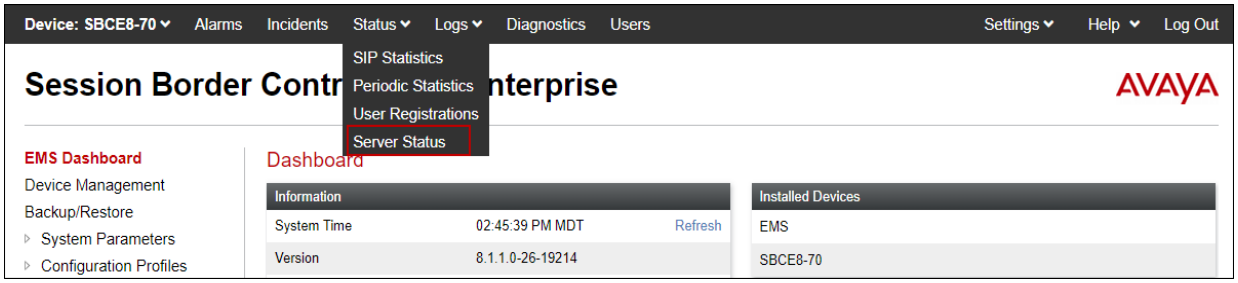


ID	Device	Date & Time	Category	Type	Cause
799538876777660	SBCE8-70	Sep 2, 2020, 2:15:53 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
799538876769006	SBCE8-70	Sep 2, 2020, 2:15:53 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
799538876758070	SBCE8-70	Sep 2, 2020, 2:15:53 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
799538876757982	SBCE8-70	Sep 2, 2020, 2:15:53 PM	Policy	Server Heartbeat	Heartbeat Failed, Server Service Down
799538876755915	SBCE8-70	Sep 2, 2020, 2:15:53 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
799538874163604	SBCE8-70	Sep 2, 2020, 2:15:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
799538874159388	SBCE8-70	Sep 2, 2020, 2:15:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
799538874159158	SBCE8-70	Sep 2, 2020, 2:15:48 PM	Policy	Message Dropped	No Subscriber Flow Matched
799538526058307	SBCE8-70	Sep 2, 2020, 2:04:12 PM	Protocol Discrepancy	BYE Message Out of Dialog	General Method not allowed Out-Of-Dialog

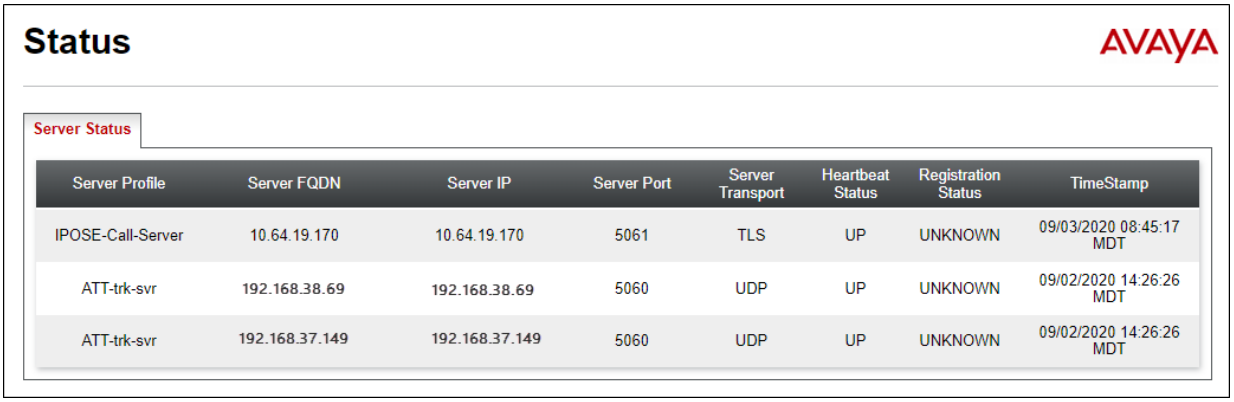
©2020 Avaya Inc. All Rights Reserved.

9.1.2. Server Status

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



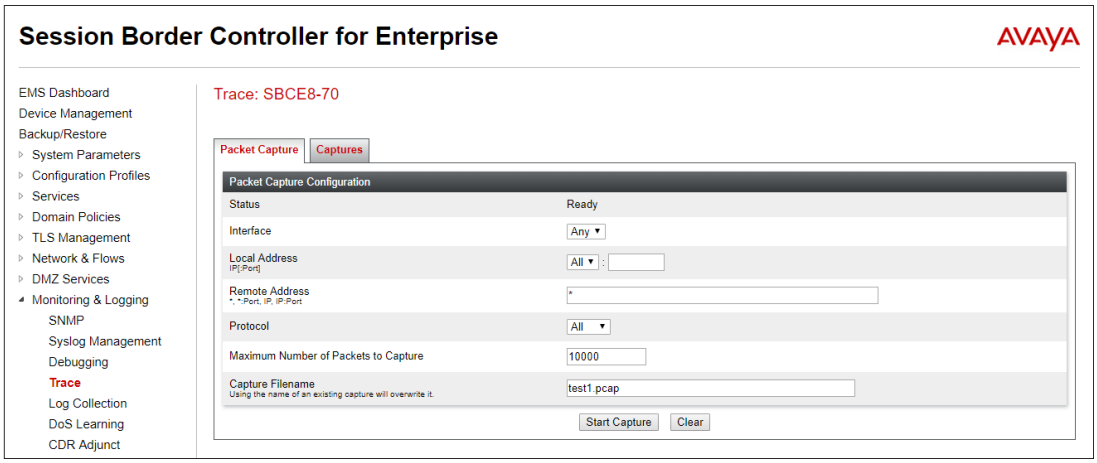
The Server Status screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Configuration profiles, as configured in **Section 7.7**.



Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
IPOSE-Call-Server	10.64.19.170	10.64.19.170	5061	TLS	UP	UNKNOWN	09/03/2020 08:45:17 MDT
ATT-trk-svr	192.168.38.69	192.168.38.69	5060	UDP	UP	UNKNOWN	09/02/2020 14:26:26 MDT
ATT-trk-svr	192.168.37.149	192.168.37.149	5060	UDP	UP	UNKNOWN	09/02/2020 14:26:26 MDT

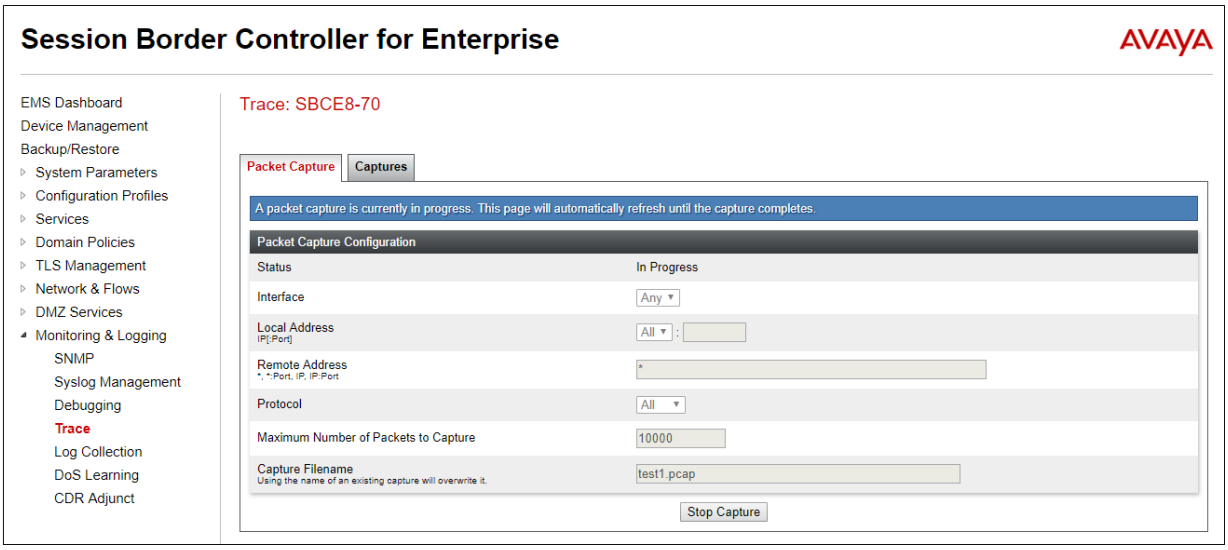
9.1.3. Tracing

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

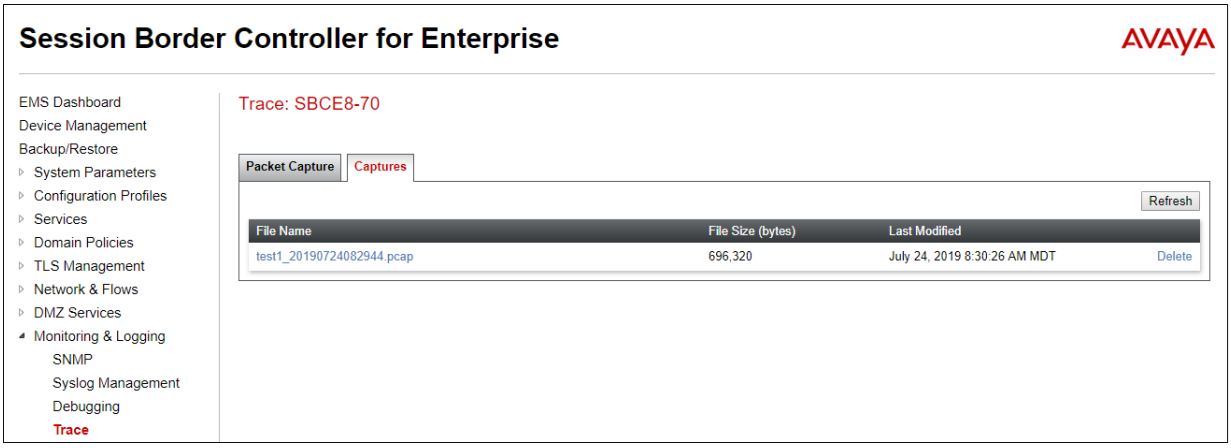


©2020 Avaya Inc. All Rights Reserved.

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



Select the **Captures** tab to view the files created during the packet capture.



The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like WireShark.

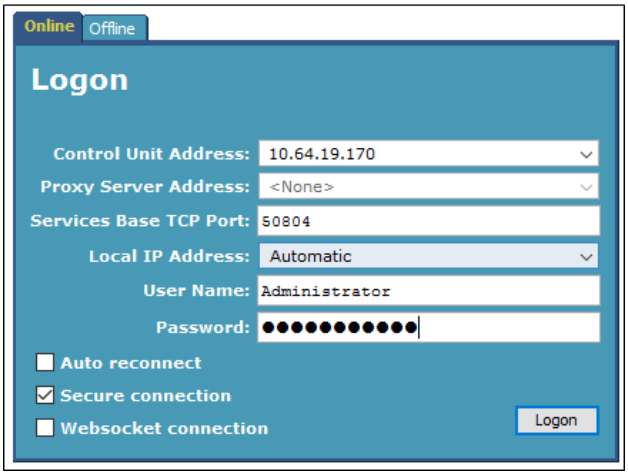
©2020 Avaya Inc. All Rights Reserved.

9.2. Avaya IP Office

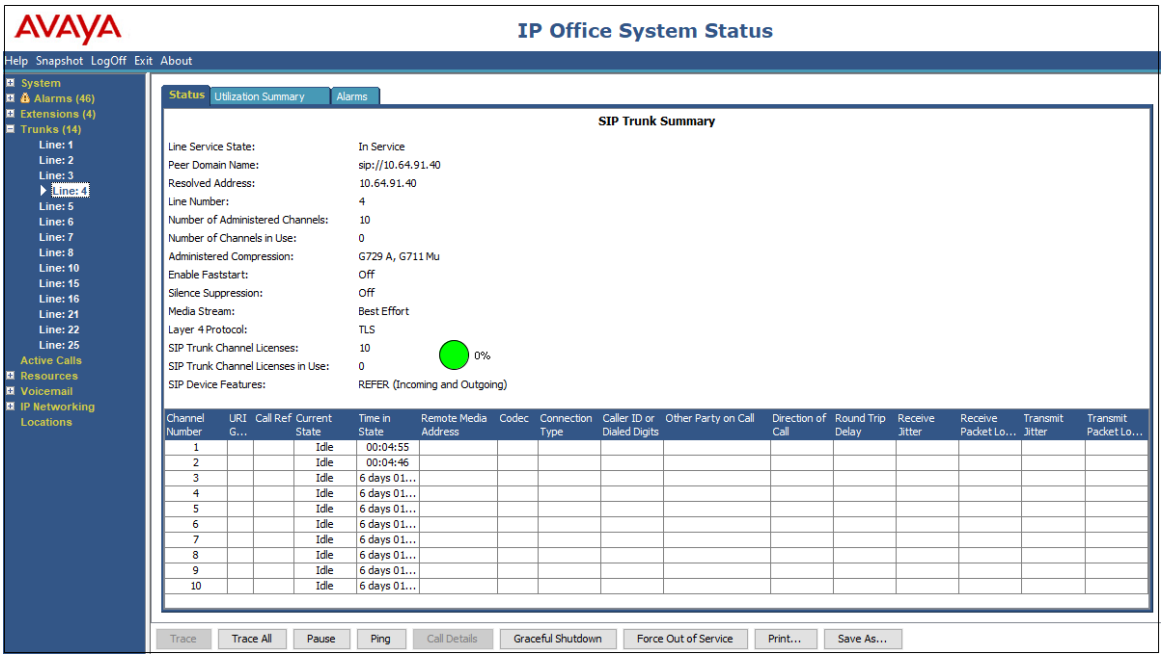
This section provides verification steps that may be performed with the IP Office.

9.2.1. System Status

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.



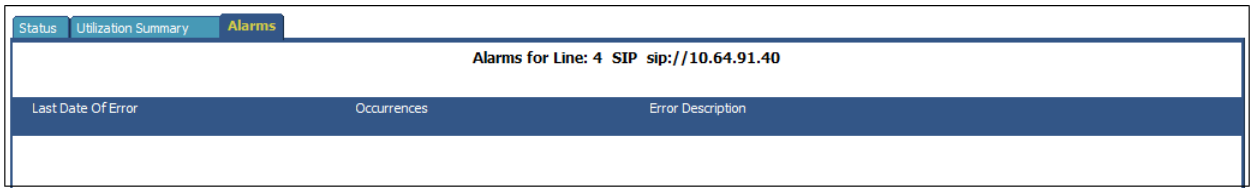
Select the SIP line from the left pane (**Line 4** in the reference configuration). On the **Status** tab in the right pane, verify that the **Current State** is ***Idle*** for each channel (assuming no active calls at present time).



©2020 Avaya Inc. All Rights Reserved.

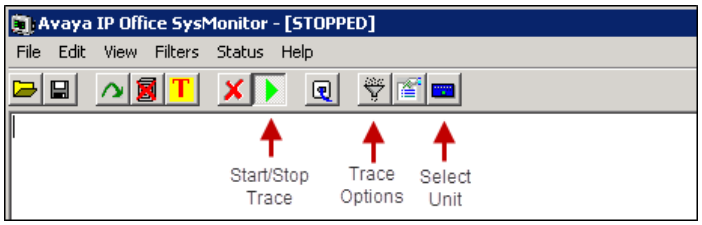
In the lower part of the screen, the **Trace All** button may be pressed to display real time tracing information as calls are made using this SIP Line. The **Ping** button can be used to ping the other end of the SIP trunk (e.g., Avaya SBCE).

S**elec**t the **Alarms** tab and verify that no alarms are active on the SIP line.

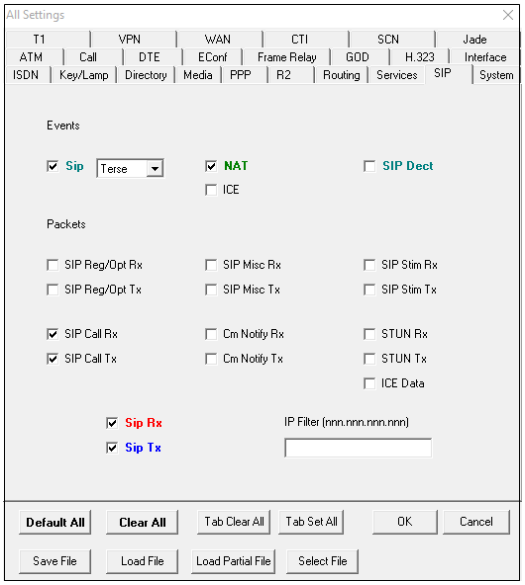


9.2.2. System Monitor

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.



©2020 Avaya Inc. All Rights Reserved.

10. Conclusion

As illustrated in these Application Notes, Avaya IP Office Release 11.1 and the Avaya Session Border Controller for Enterprise 8.1 can be configured to interoperate successfully with the AT&T IP Flexible Reach - Enhanced Features service using **AVPN** or **ADI/PNT** transport connections, within the limitations described in **Section 2.2**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

11. Additional References

This section references the documentation relevant to these Application Notes. Product documentation for Avaya IP Office, including the following, 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 11.1, Deploying Avaya IP Office Servers as Virtual Machines,* August 2020
[3] *IP Office Platform 11.1, Deploying an IP500 V2 IP Office Essential Edition System*, August 2020.
[4] *Administering Avaya IP Office™ Platform with Manager,* Release 11.1 SP1, July 2020.
[5] *Administering Avaya IP Office™ Platform with Web Manager,* Release 11.1 SP1, July 2020.
[6] *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac and Windows,* August 2020
[7] *IP Office Platform 11.1, IP Office SIP Phones with ASBCE, Issue 04c*, July 2020
[8] *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform, Release 8.1.x,* August 2020.
[9] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, August 2020.
[10] *RFC 3261 SIP: Session Initiation Protocol*. https://www.ietf.org/rfc/rfc3261.txt

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

AT&T IPFR-EF Service

Information on the AT&T IP Flexible Reach service can be found here:
https://www.business.att.com/products/sip-trunking.html

©2020 Avaya Inc. All Rights Reserved.

©2020 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.