Avaya Solution & Interoperability Test Lab

Application Notes for Avaya IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 8.1 with AT&T IP Toll Free Service - 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 Toll Free service using AVPN or ADI/PNT transport connections.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution providing toll-free services over SIP trunks for business customers.

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.

Table of Contents

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 (Avaya SBCE) release 8.1 with the AT&T IP Toll Free 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 Toll Free 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 Toll Free service is a managed Voice over IP (VoIP) communications solution providing toll-free services over SIP trunks for business customers. The AT&T Toll Free service utilizes AVPN[1] or ADI/PNT[2] transport services.

Note – The AT&T IP Toll Free service will be referred to as IPTF in the remainder of this document.

[1] AVPN uses compressed RTP (cRTP).

[2] ADI/PNT does not support cRTP.

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 IPTF 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 Avaya IP Office 11.1, Avaya SBCE 8.1, Avaya SIP, H.323, Digital and Analog telephones, as well as fax machine emulators (Ventafax).
- Laboratory versions of the IPTF service, 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 Toll Free 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.

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 IPTF network. Calls were made from the PSTN across the IPTF test network, to the CPE.

The interoperability compliance testing focused on verifying inbound call flows (see **Section 3.2**) between Avaya IP Office, Avaya SBCE and the IPTF service.

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 AT&T network.

The following SIP trunking VoIP features were tested with the IPTF service:

- Incoming calls from PSTN, routed by the IPTF service, to the Avaya SBCE and the Avaya IP Office. These calls are via the Avaya IP Office SIP Line and may be generated/answered by Avaya SIP telephones/Softphones, H.323 telephones, Analog telephones, Digital telephones, Analog fax machines or via Hunt Groups. Coverage to Voicemail Pro, and Voicemail Pro auto-attendant applications, were also used.
- Inbound fax using T.38 or G.711, and G3 or SG3 endpoints.
- Proper disconnect when the caller abandons a call before answer, and when the Avaya IP Office party or the PSTN party terminates an active call.
- Proper busy tone heard when an Avaya IP Office user calls a busy PSTN user, or a PSTN user calls a busy Avaya IP Office user (i.e., if no redirection was configured for user busy conditions).
- SIP OPTIONS monitoring of the health of the SIP trunk. In the reference configuration Avaya IP Office sent OPTIONS to the IPTF service Border Element and AT&T responded with *405 Method Not Allowed* (which is the expected response). That response is sufficient for Avaya IP Office to consider the connection up.
- Incoming calls using the G.729A and G.711 ULAW codecs.
- Long duration calls.
- DTMF transmission (RFC 2833) for successful voice mail navigation, including navigation of a simple auto-attendant application configured on Voicemail Pro, as well as IPTF DTMF generated features.
- Telephony features such as call waiting, hold, transfer, and conference.
- Avaya Remote Worker configuration (Avaya Workplace Client for Windows SIP softphone) via Avaya SBCE.
- Verify reception of IPTF SIP Multipart/NSS headers, including SDP and XML content.
- AT&T IP Toll Free features such as Legacy Transfer Connect and Alternate Destination Routing.

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** – Although no issues were found during testing, AT&T recommends that for maximum customer bandwidth utilization, a ptime value of 30 should be specified.

2. **IP Toll Free ADR Call Redirection feature based on SIP error code response** – Upon receiving an error response, IPTF service can be configured to invoke ADR Call Redirection. The following error codes were producible by the reference configuration and tested successfully; 408 Request Timeout, 480 Temporarily Unavailable, 486 Busy Here, and 503 Service Unavailable. The following error codes are also supported by IPTF service, but were not producible by the reference configuration, and thus not tested; 500 Server Internal Error, 504 Server Timeout, and 600 Busy Everywhere.

3. **Enhanced CID – NSS feature**. The inbound calls to Avaya IP Office are not exercising the Enhanced CID feature. Although Avaya IP Office is accepting SIP Multipart/NSS headers, it is neither passing nor acting upon it. It is simply being ignored.

4. **IP Office determines the codec priority** – IP Office will follow the codec priority based on the Codec Selection on the SIP Line VoIP tab, see **Section 5.5.5**. It will not follow the codec priority set by the IPTF service.

5. **Codec G.729B is not supported on IP Office Server Edition server** – Specific test cases on the AT&T Test Plan requiring the use of codec G.729B at the CPE could not be executed. Codec G729B is not supported on SIP trunks terminating on the Avaya IP Office Server Edition Linux server platform, as deployed on the test configuration. Codec G.729B is supported when the SIP trunk is terminated on an IP Office IP500 V2 standalone or expansion system.

6. **Inbound User-to-User Information is not supported with IP Office** – User-to-User Information (UUI) is not supported on inbound SIP trunk calls. IP Office is able to successfully receive an inbound call from AT&T containing UUI, but the UUI data is simply ignored.

7. **Inbound T.38 or G.711 fax calls fail when the sender and receiver are both Super G3 (SG3) fax devices** – During testing it was found that when the sender and receiver both used SG3 fax devices, and an inbound fax call was placed to Avaya IP Office using either T.38 or G.711, the fax calls failed to connect. SG3 speeds (33600 bps), should be disabled on the CPE fax devices if possible.

2.3. Support

AT&T customers may obtain support for the AT&T IP Toll Free service by calling (800) 325-5555.

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. Customers may also use specific numbers (provided on http://support.avaya.com) to directly access specific support and consultation services based upon their Avaya support agreements.

3. Reference Configuration

Note – Documents used to provision the test environment are listed in **Section 11**. References to these documents are indicated by the notation **[x]**, where *x* is the document reference number.

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

- Avaya IP Office provides the voice communications services for a particular enterprise site. 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, running as a service on the Primary Server, provided the voice messaging capabilities in the reference configuration.
- The Expansion System (V2) is used for the support of digital, analog and additional IP stations. It consists of an Avaya IP Office 500 V2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module).
- Avaya endpoints are represented with an Avaya 9608 H.323 Deskphone, Avaya J169 SIP Deskphones, an Avaya 1140E SIP Deskphone, an Avaya 9508 Digital Deskphone, as well as Avaya Workplace Client for Windows (SIP) softphone. Fax endpoints are represented by PCs running Ventafax emulation software connected by modem to an Avaya IP Office analog port.
- The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPTF service and the CPE. In the reference configuration, the Avaya SBCE runs on a VMware platform. This solution is extensible to other Avaya Session Border Controller for Enterprise platforms as well.

- 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 B1 interface connected to the AT&T network.
- 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.
- UDP transport via port 5060 was used between the Avaya SBCE and AT&T.
- The AT&T IPTF service requires 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 IPTF service may deliver various digit lengths in the SIP Invite Request-URI depending on the circuit order provisioning. In the reference configuration, the IPTF service delivered 10 digits.
- 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 the 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 [**8**] on the **Additional References** section for information on Remote Worker deployments.

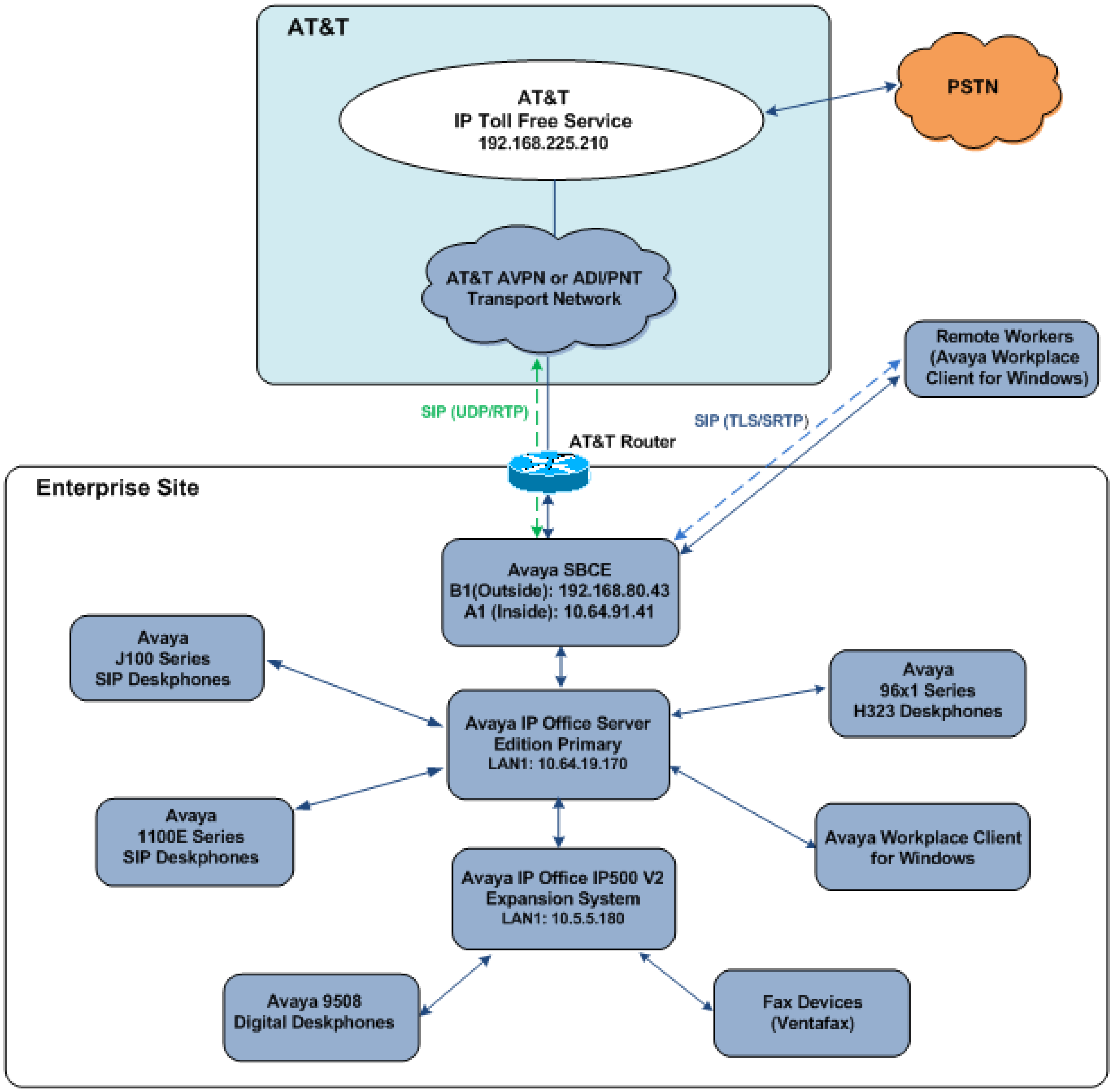


Figure 1: Test Configuration

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 – The Avaya SBCE "B1" interface communicates with AT&T Border Elements (BEs) located in the AT&T IPTF network. For security reasons, the IP addresses of the AT&T BEs are not included in this document. However, as placeholders in the following configuration sections, the IP addresses **192.168.80.43** (Avaya SBCE "B1"), and **192.168.225.210** (AT&T BE address), 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 IPTF 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	10.64.91.41
"Outside" Interface, B1	192.168.80.43
AT&T IPTF Service	
Border Element IP Address	192.168.225.210

Table 1: Illustrative Values Used in these Application Notes

3.2. Call Flows

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

3.2.1. Basic Inbound

The first call scenario illustrated in the figure below is an inbound AT&T IPTF 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 IPTF service number.
2. The PSTN routes the call to the AT&T IPTF service network.
3. The AT&T IPTF 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.

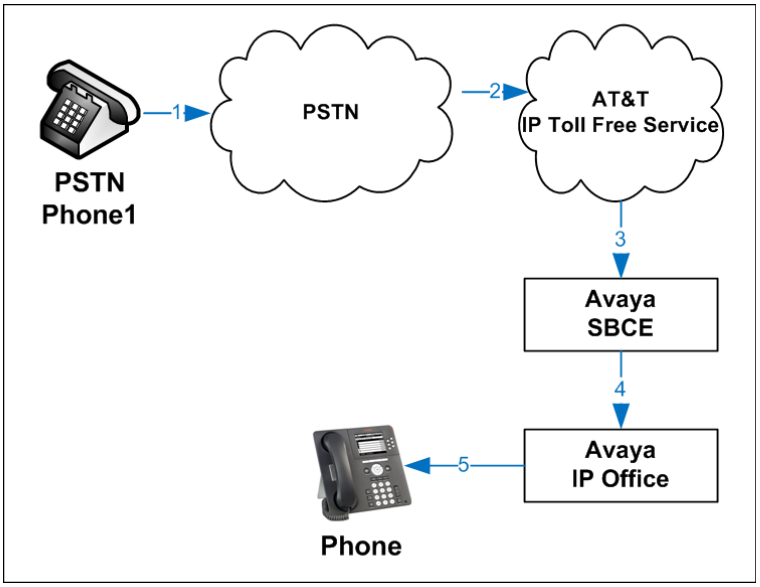


Figure 2: Inbound AT&T IPTF Call

3.2.2. 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, running on the Application Server.

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 the external application Avaya IP Office Voicemail Pro.

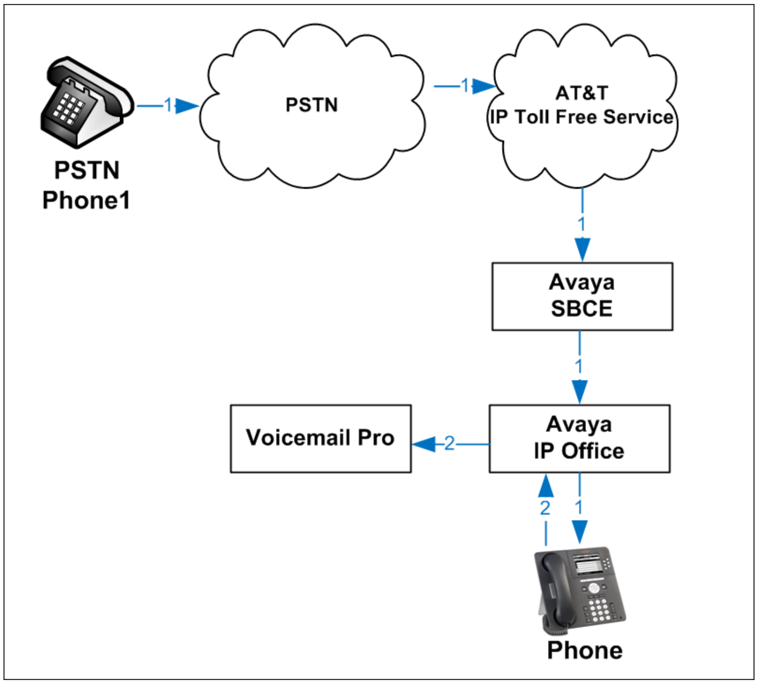


Figure 3: Coverage to Voicemail (Voicemail Pro)

3.2.3. Inbound to Voicemail Pro Auto Attendant

The call scenario illustrated in the figure below summarizes an inbound call that is routed by Avaya IP Office to a predefined Auto Attendant Module in Voicemail Pro. Based on the caller interaction, the call is then routed to a hunt group or extension.

1. Same as the first call scenario in **Section 3.2.1**.
2. Avaya IP Office applies any necessary digit manipulations based upon the DID and routes the call to an Auto Attendant module in Avaya IP Office Voicemail Pro.
3. After listening to the Auto Attendant prompts, the caller selects one of the options. Voicemail Pro redirects the call back to the IP Office, to be routed to the intended destination.
4. Avaya IP Office sends the call to the proper hunt group or extension.

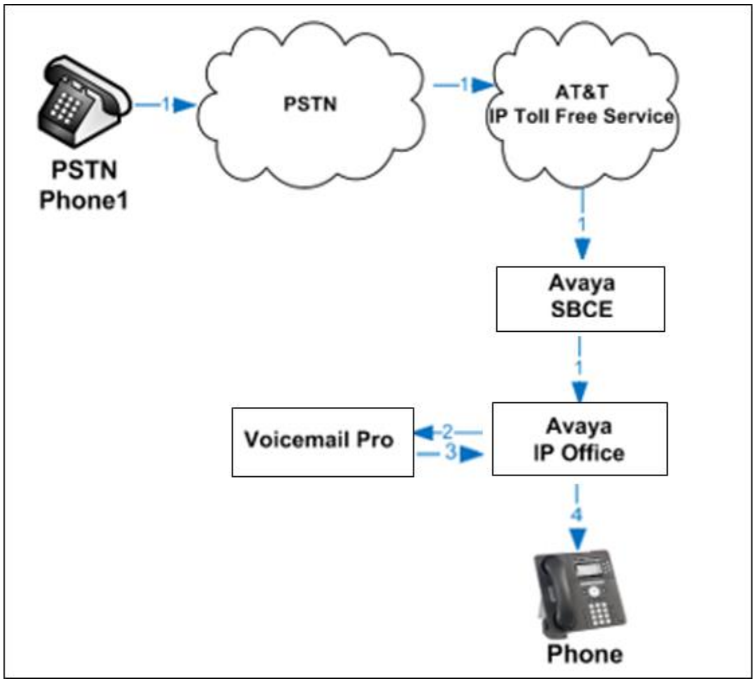


Figure 4: Inbound to Auto Attendant (Voicemail Pro)

4. Equipment and Software Validated

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

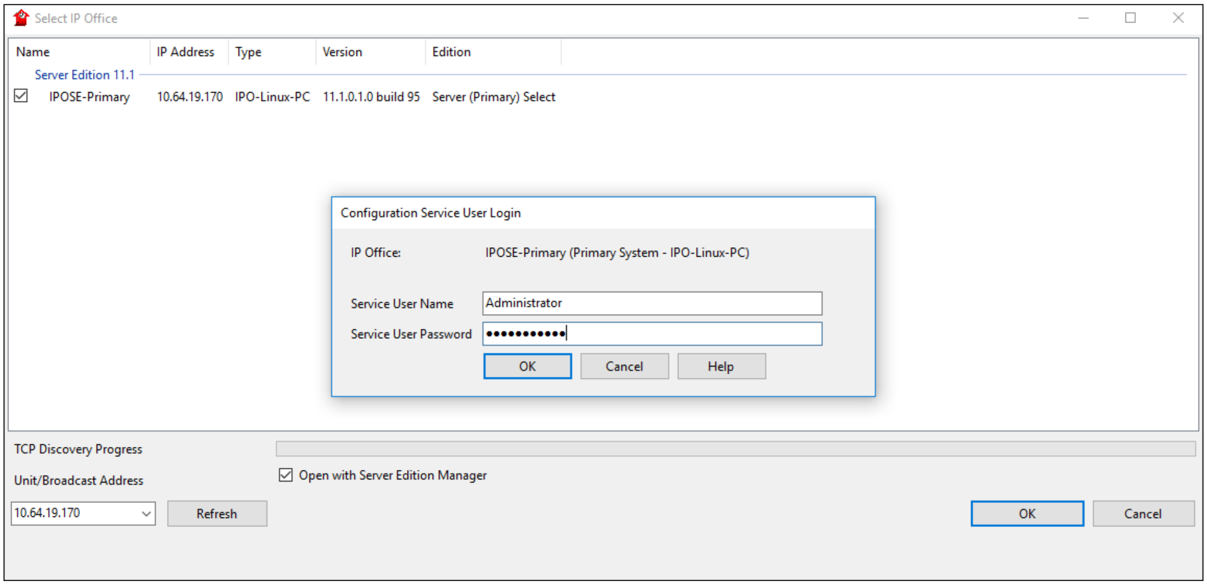
Equipment/Software	**Release/Version**
Avaya	
Avaya IP Office Server Edition - Avaya IP Office Voicemail Pro	Release 11.1.0.1.0 Build 95 Release 11.1.0.1.0 Build 14
Avaya IP Office 500 V2 Expansion System	Release 11.1.0.1.0 Build 95
Avaya IP Office Manager	Release 11.1.0.1.0 Build 95
Avaya Session Border Controller for Enterprise	Release 8.1.1.0-26-19214 Patch 19242
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 Workplace Client for Windows (SIP)	Release 3.11.0.44.25
Avaya 9508 Digital Deskphone	Release 0.60
Avaya 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.

5. Avaya IP Office Primary Server Configuration

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.



Select IP Office

Name	IP Address	Type	Version	Edition
Server Edition 11.1				
☑ IPOSE-Primary	10.64.19.170	IPO-Linux-PC	11.1.0.1.0 build 95	Server (Primary) Select

Configuration Service User Login

IP Office: IPOSE-Primary (Primary System - IPO-Linux-PC)

Service User Name: Administrator

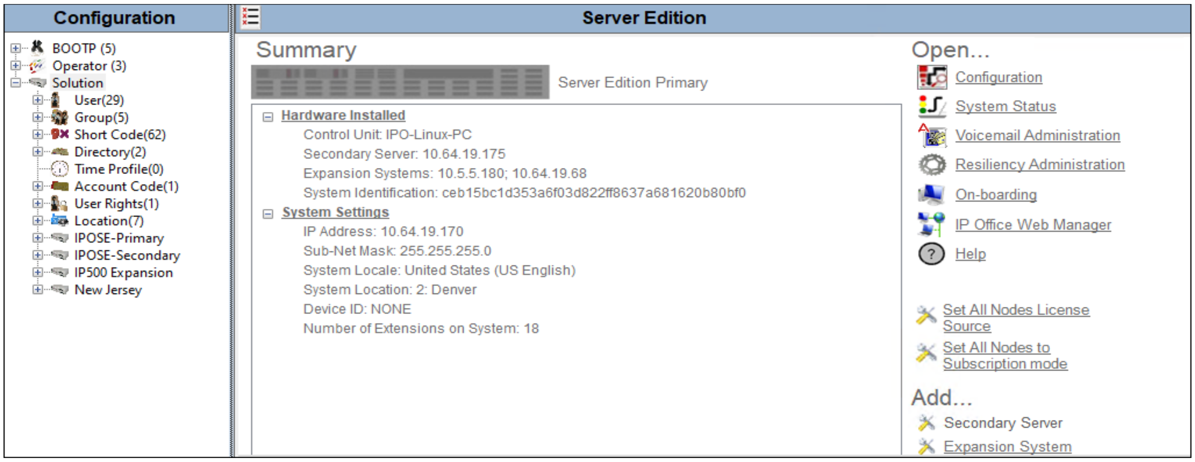
Service User Password: ●●●●●●●●●●●

TCP Discovery Progress

Unit/Broadcast Address: 10.64.19.170

☑ Open with Server Edition Manager

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.



Summary

Server Edition Primary

Hardware Installed

Control Unit: IPO-Linux-PC
Secondary Server: 10.64.19.175
Expansion Systems: 10.5.5.180; 10.64.19.68
System Identification: ceb15bc1d353a6f03d822ff8637a681620b80bf0

System Settings

IP Address: 10.64.19.170
Sub-Net Mask: 255.255.255.0
System Locale: United States (US English)
System Location: 2: Denver
Device ID: NONE
Number of Extensions on System: 18

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.

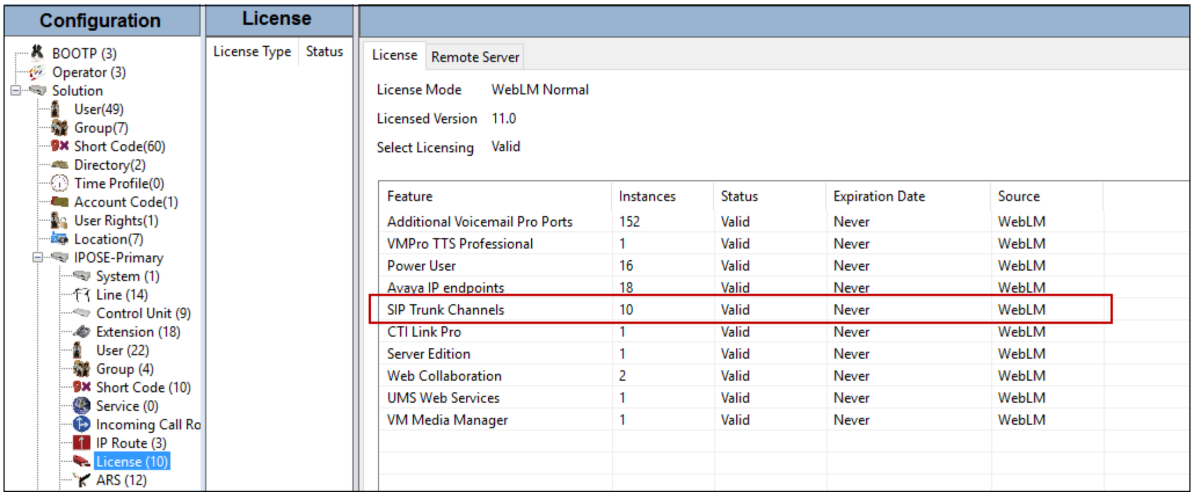
Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

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.



License Mode WebLM Normal

Licensed Version 11.0

Select Licensing Valid

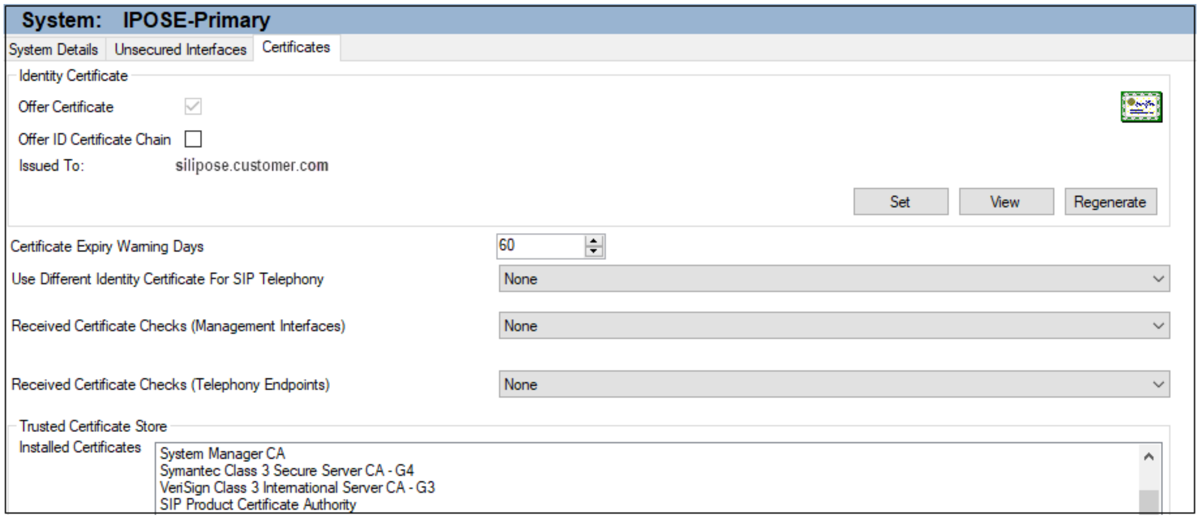
Feature	Instances	Status	Expiration Date	Source
Additional Voicemail Pro Ports	152	Valid	Never	WebLM
VMPro TTS Professional	1	Valid	Never	WebLM
Power User	16	Valid	Never	WebLM
Avaya IP endpoints	18	Valid	Never	WebLM
SIP Trunk Channels	10	Valid	Never	WebLM
CTI Link Pro	1	Valid	Never	WebLM
Server Edition	1	Valid	Never	WebLM
Web Collaboration	2	Valid	Never	WebLM
UMS Web Services	1	Valid	Never	WebLM
VM Media Manager	1	Valid	Never	WebLM

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.



System: IPOSE-Primary

Identity Certificate

Offer Certificate ☑

Offer ID Certificate Chain □

Issued To: silipose.customer.com

Certificate Expiry Warning Days: 60

Use Different Identity Certificate For SIP Telephony: None

Received Certificate Checks (Management Interfaces): None

Received Certificate Checks (Telephony Endpoints): None

Trusted Certificate Store

Installed Certificates:
System Manager CA
Symantec Class 3 Secure Server CA - G4
VeriSign Class 3 International Server CA - G3
SIP Product Certificate Authority

5.3. System Settings

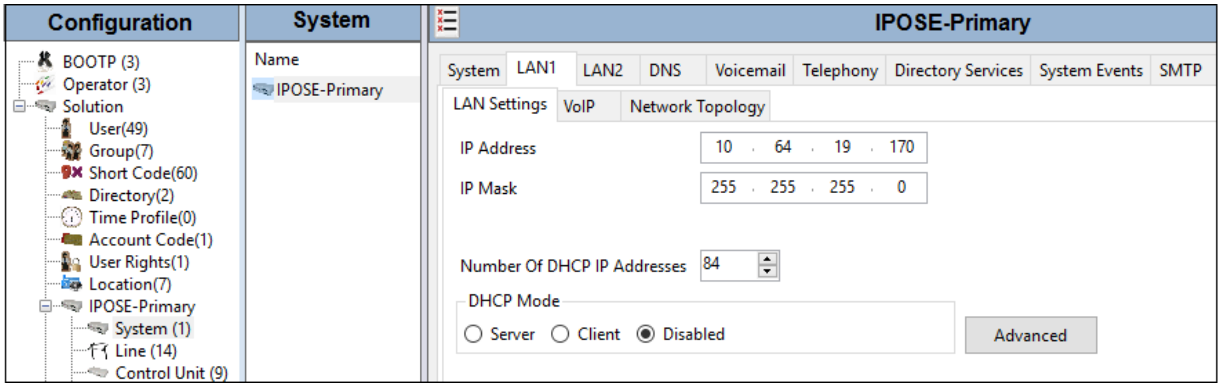
This section illustrates the configuration of system settings. Select **System** on the Navigation pane to configure these settings. The subsection order corresponds to a left to right navigation of the tabs in the Details pane for System settings. For all the following configuration sections, the **OK** 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).



IP Address: 10 . 64 . 19 . 170

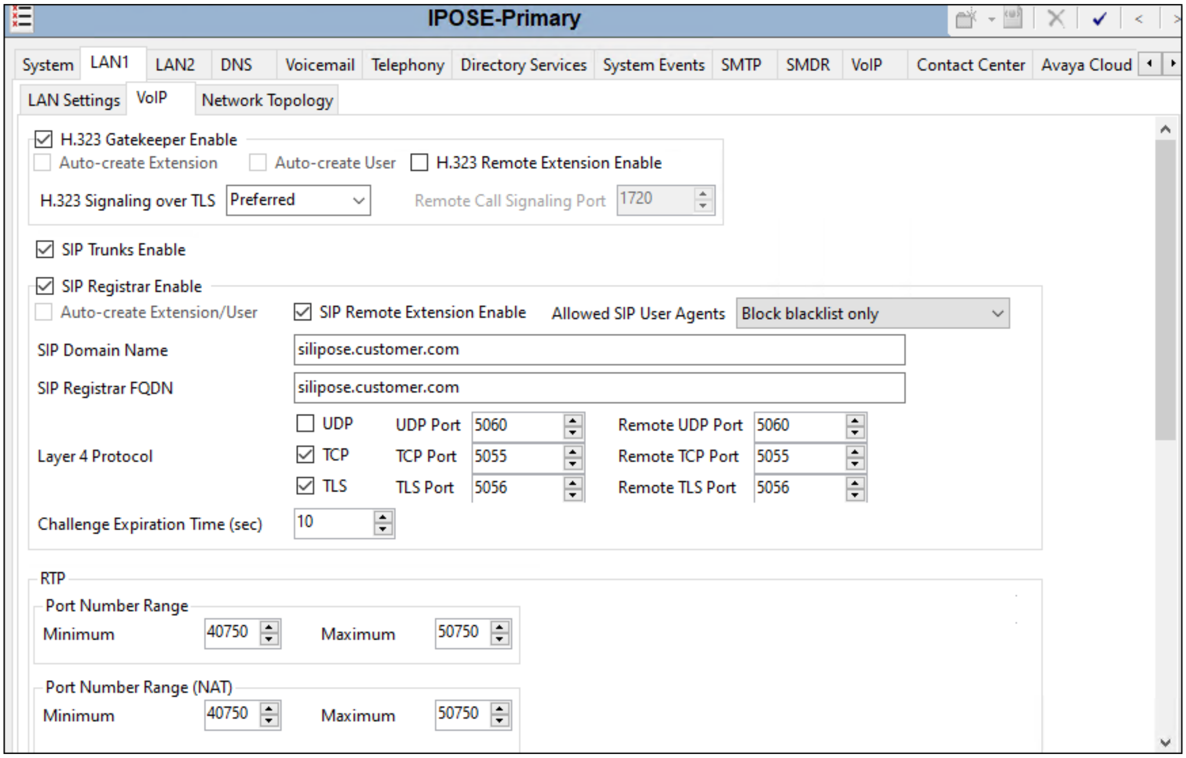
IP Mask: 255 . 255 . 255 . 0

Number Of DHCP IP Addresses: 84

DHCP Mode: ○ Server ○ Client ● Disabled

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

- The **H323 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 Workplace Client for Windows 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.



☑ H.323 Gatekeeper Enable

□ Auto-create Extension □ Auto-create User □ H.323 Remote Extension Enable

H.323 Signaling over TLS: Preferred Remote Call Signaling Port: 1720

☑ SIP Trunks Enable

☑ SIP Registrar Enable

□ Auto-create Extension/User ☑ SIP Remote Extension Enable Allowed SIP User Agents: Block blacklist only

SIP Domain Name: silipose.customer.com

SIP Registrar FQDN: silipose.customer.com

Layer 4 Protocol:

□ UDP	UDP Port	5060	Remote UDP Port	5060
☑ TCP	TCP Port	5055	Remote TCP Port	5055
☑ TLS	TLS Port	5056	Remote TLS Port	5056

Challenge Expiration Time (sec): 10

RTP

Port Number Range

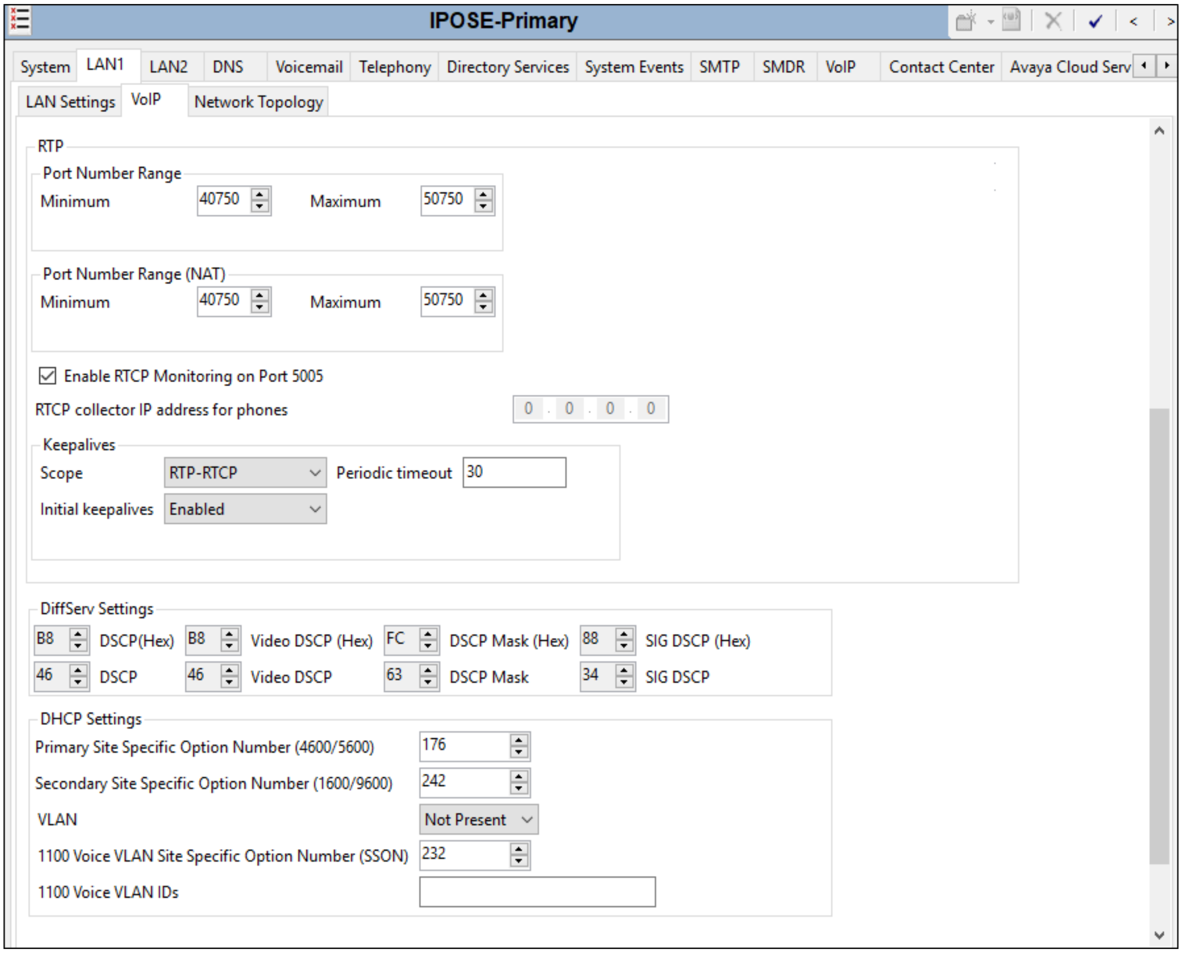
Minimum: 40750 Maximum: 50750

Port Number Range (NAT)

Minimum: 40750 Maximum: 50750

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).



RTP

Port Number Range

Minimum 40750 Maximum 50750

Port Number Range (NAT)

Minimum 40750 Maximum 50750

☑ Enable RTCP Monitoring on Port 5005

RTCP collector IP address for phones 0 . 0 . 0 . 0

Keepalives

Scope RTP-RTCP Periodic timeout 30

Initial keepalives Enabled

DiffServ Settings

B8 DSCP(Hex) B8 Video DSCP (Hex) FC DSCP Mask (Hex) 88 SIG DSCP (Hex)

46 DSCP 46 Video DSCP 63 DSCP Mask 34 SIG DSCP

DHCP Settings

Primary Site Specific Option Number (4600/5600) 176

Secondary Site Specific Option Number (1600/9600) 242

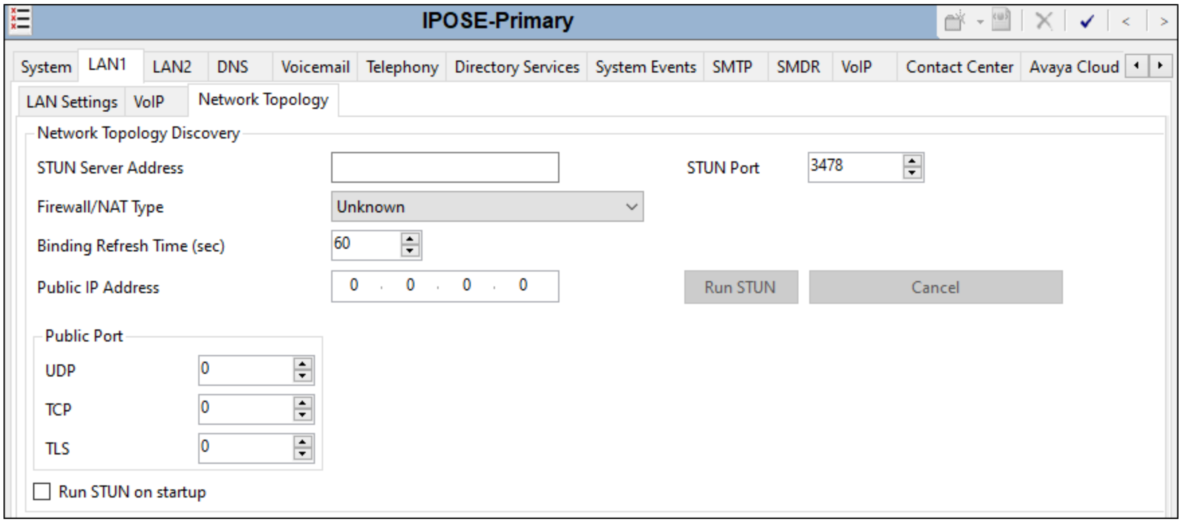
VLAN Not Present

1100 Voice VLAN Site Specific Option Number (SSON) 232

1100 Voice VLAN IDs

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 IPTF SIP trunk service connection.
- Click the **OK** button (not shown).



Network Topology Discovery

STUN Server Address		STUN Port	3478
Firewall/NAT Type	Unknown		
Binding Refresh Time (sec)	60		
Public IP Address	0 . 0 . 0 . 0		

Public Port

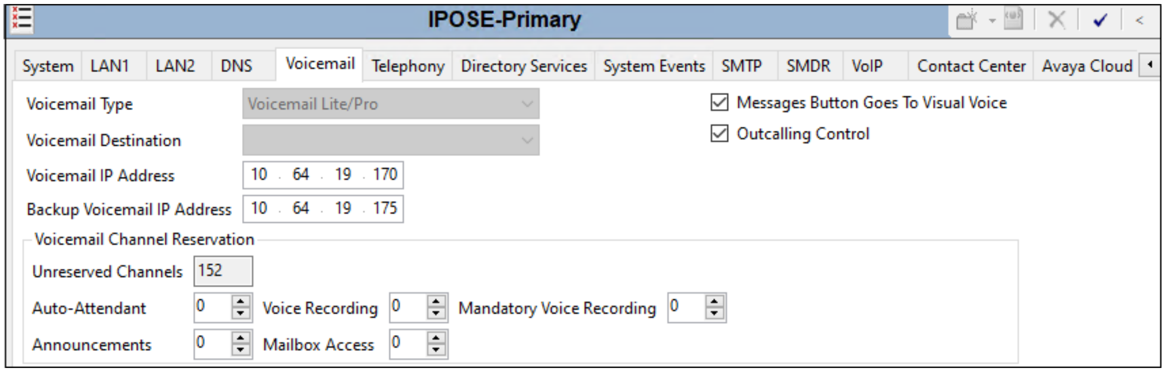
UDP	0
TCP	0
TLS	0

□ Run STUN on startup

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).



Voicemail Type	Voicemail Lite/Pro
Voicemail Destination	
Voicemail IP Address	10 . 64 . 19 . 170
Backup Voicemail IP Address	10 . 64 . 19 . 175

☑ Messages Button Goes To Visual Voice

☑ Outcalling Control

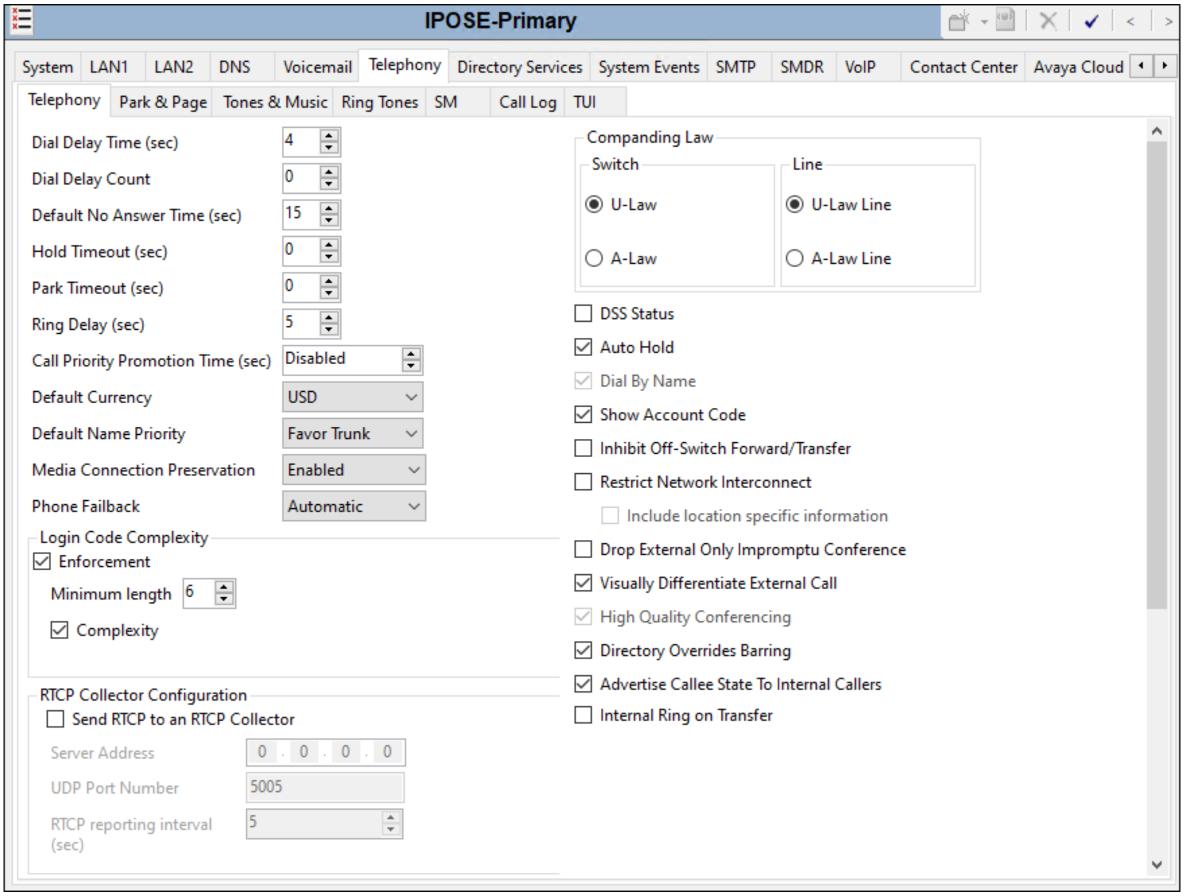
Voicemail Channel Reservation

Unreserved Channels	152				
Auto-Attendant	0	Voice Recording	0	Mandatory Voice Recording	0
Announcements	0	Mailbox Access	0		

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).



Dial Delay Time (sec): 4
Dial Delay Count: 0
Default No Answer Time (sec): 15
Hold Timeout (sec): 0
Park Timeout (sec): 0
Ring Delay (sec): 5
Call Priority Promotion Time (sec): Disabled
Default Currency: USD
Default Name Priority: Favor Trunk
Media Connection Preservation: Enabled
Phone Failback: Automatic

Login Code Complexity
☑ Enforcement
Minimum length: 6
☑ Complexity

RTCP Collector Configuration
□ Send RTCP to an RTCP Collector
Server Address: 0 . 0 . 0 . 0
UDP Port Number: 5005
RTCP reporting interval (sec): 5

Companding Law
Switch: ● U-Law ○ A-Law
Line: ● U-Law Line ○ A-Law Line

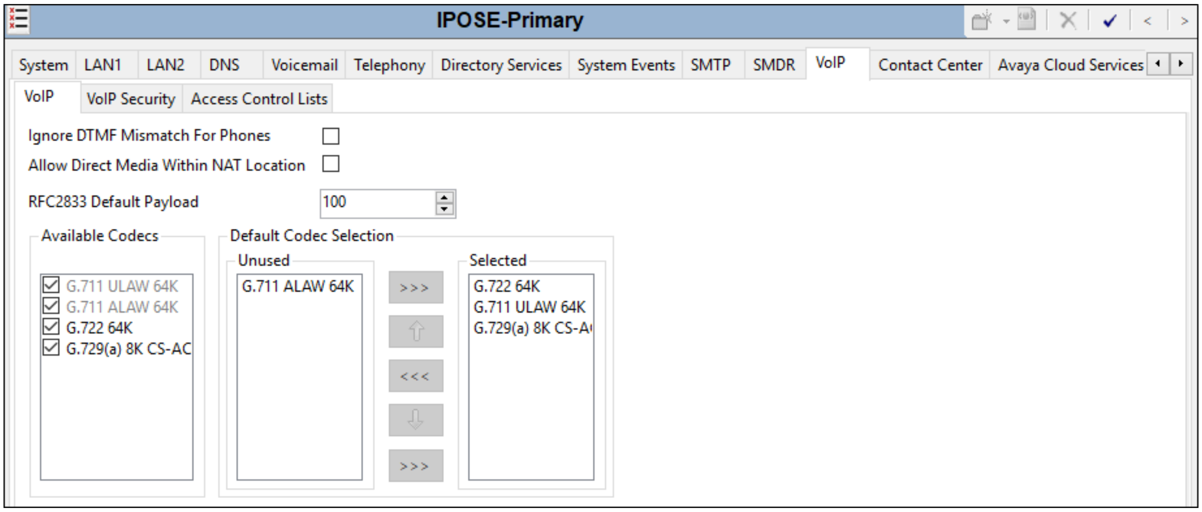
□ DSS Status
☑ Auto Hold
☑ Dial By Name
☑ Show Account Code
□ Inhibit Off-Switch Forward/Transfer
□ Restrict Network Interconnect
□ Include location specific information
□ Drop External Only Impromptu Conference
☑ Visually Differentiate External Call
☑ High Quality Conferencing
☑ Directory Overrides Barring
☑ Advertise Callee State To Internal Callers
□ Internal Ring on Transfer

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).



Ignore DTMF Mismatch For Phones □

Allow Direct Media Within NAT Location □

RFC2833 Default Payload 100

Available Codecs

☑ G.711 ULAW 64K
☑ G.711 ALAW 64K
☑ G.722 64K
☑ G.729(a) 8K CS-AC

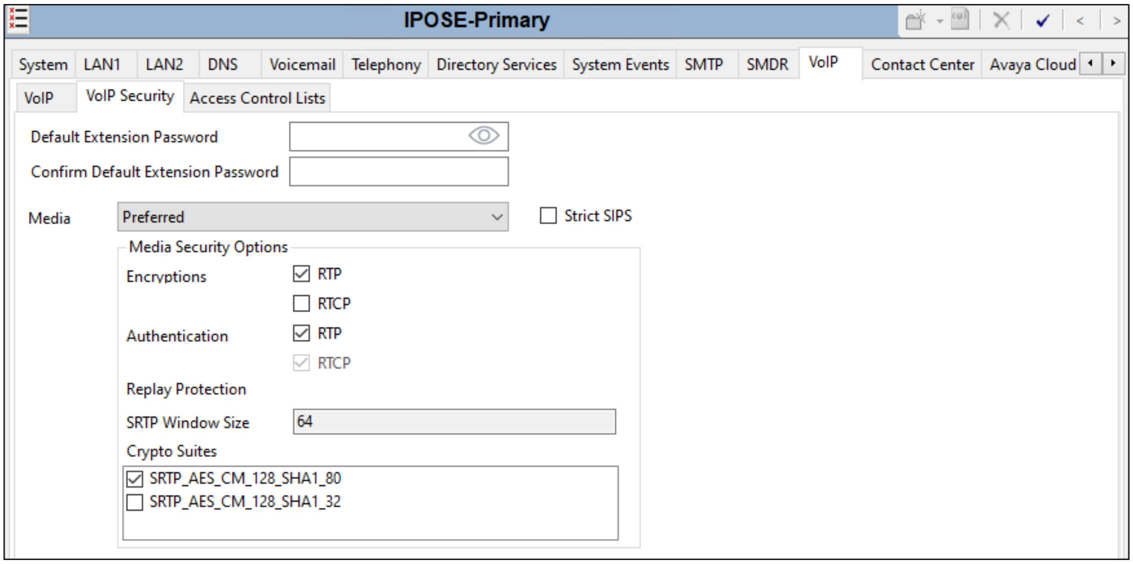
Default Codec Selection

Unused: G.711 ALAW 64K

Selected:
G.722 64K
G.711 ULAW 64K
G.729(a) 8K CS-A

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).



Default Extension Password
Confirm Default Extension Password

Media: Preferred

□ Strict SIPS

Media Security Options

Encryptions: ☑ RTP □ RTCP

Authentication: ☑ RTP ☑ RTCP

Replay Protection

SRTP Window Size: 64

Crypto Suites

☑ SRTP_AES_CM_128_SHA1_80

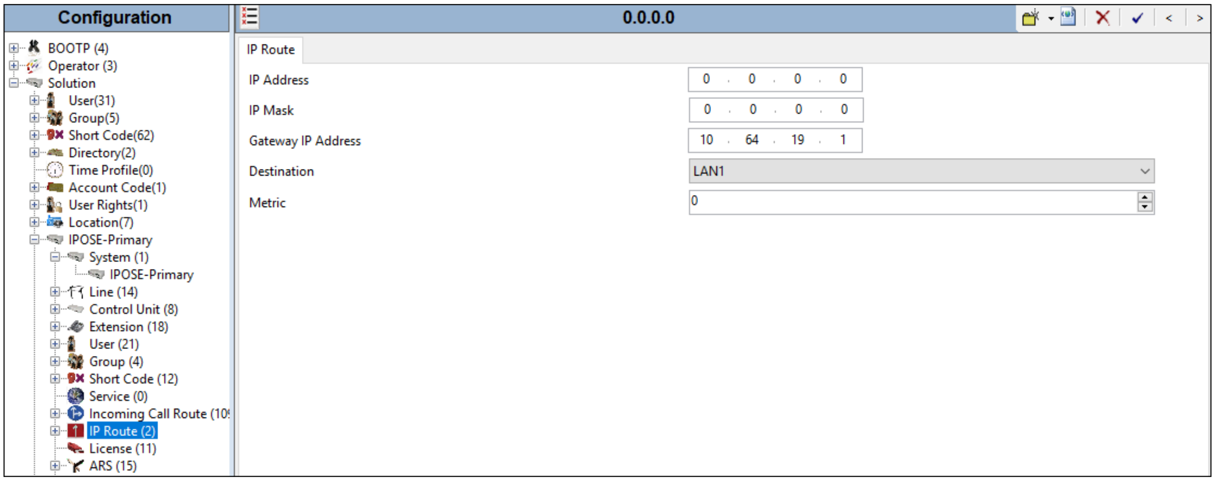
□ SRTP_AES_CM_128_SHA1_32

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).



IP Address: 0 . 0 . 0 . 0
IP Mask: 0 . 0 . 0 . 0
Gateway IP Address: 10 . 64 . 19 . 1
Destination: LAN1
Metric: 0

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 IPTF 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 IPTF 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:

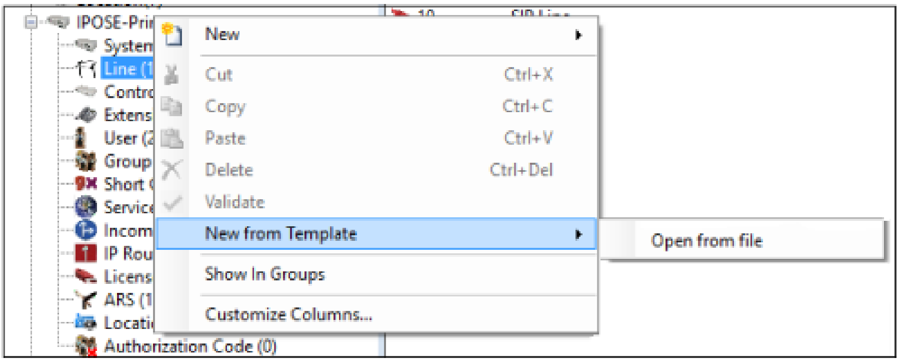
- SIP Line – Originator number for forwarded and twinning calls.
- Transport – Second Explicit DNS Server.
- SIP Credentials – Registration Requirement.
- SIP Advanced Engineering.

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**.

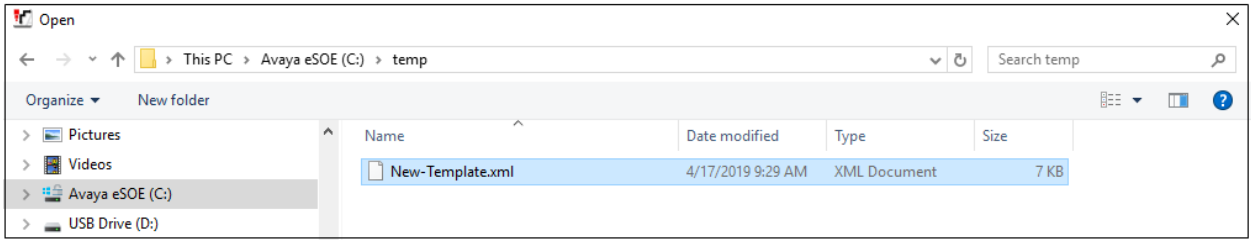
5.5.1. Creating a SIP Line from an XML Template

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.**

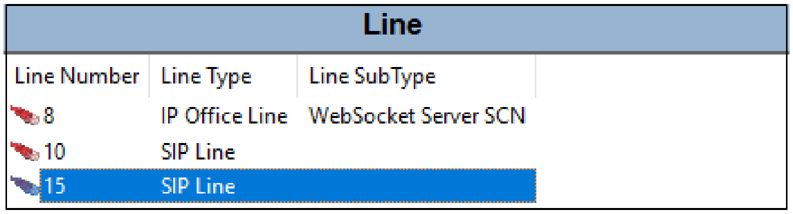


Navigate to the directory where the template was copied on the local computer (e.g., *temp*) and select it. Click **Open** (not shown).



Name	Date modified	Type	Size
New-Template.xml	4/17/2019 9:29 AM	XML Document	7 KB

The new SIP Line is created, and it will appear on the **Navigation** pane (e.g., SIP Line **15**). The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.5.2** to **5.5.6**.



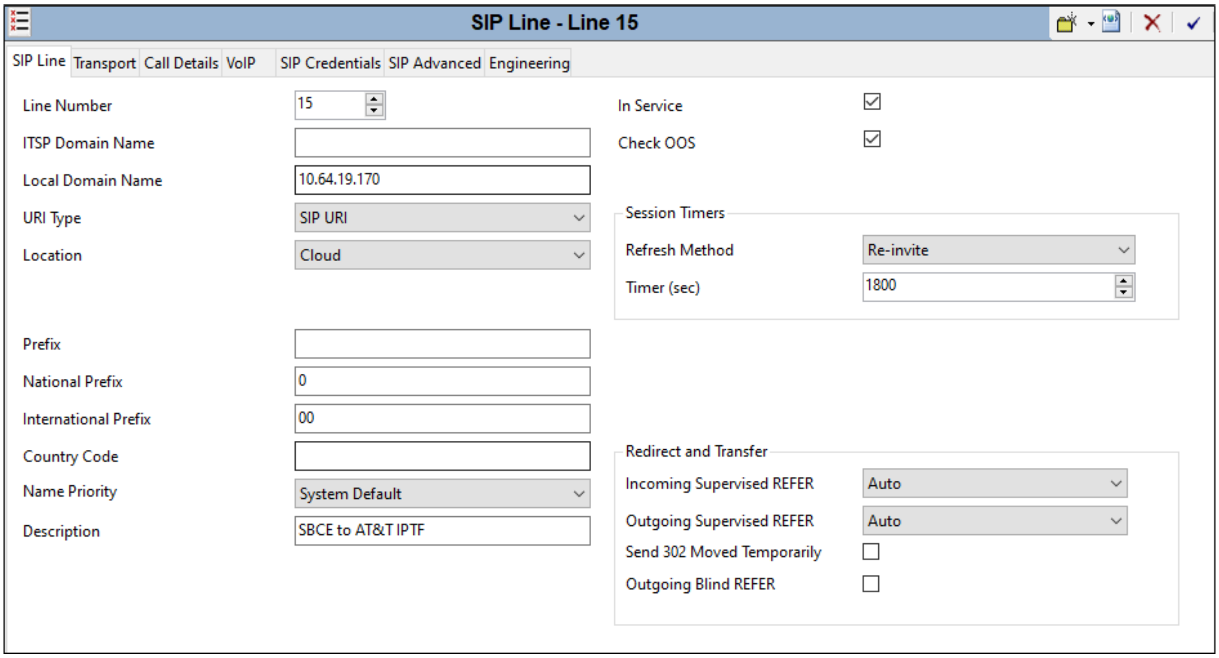
Line

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

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 **Auto** (default).
- **Outgoing Supervised Refer**: Set this field to **Auto** (default).
- **Send 302 Moved Temporarily**: Verify this is unchecked (default).
- **Outgoing Blind Refer**: Verify this is unchecked (default).
- Use the default values for the other fields.
- Click **OK** (not shown).



SIP Line - Line 15

Line Number: 15
ITSP Domain Name:
Local Domain Name: 10.64.19.170
URI Type: SIP URI
Location: Cloud
Prefix:
National Prefix: 0
International Prefix: 00
Country Code:
Name Priority: System Default
Description: SBCE to AT&T IPTF

In Service ☑
Check OOS ☑

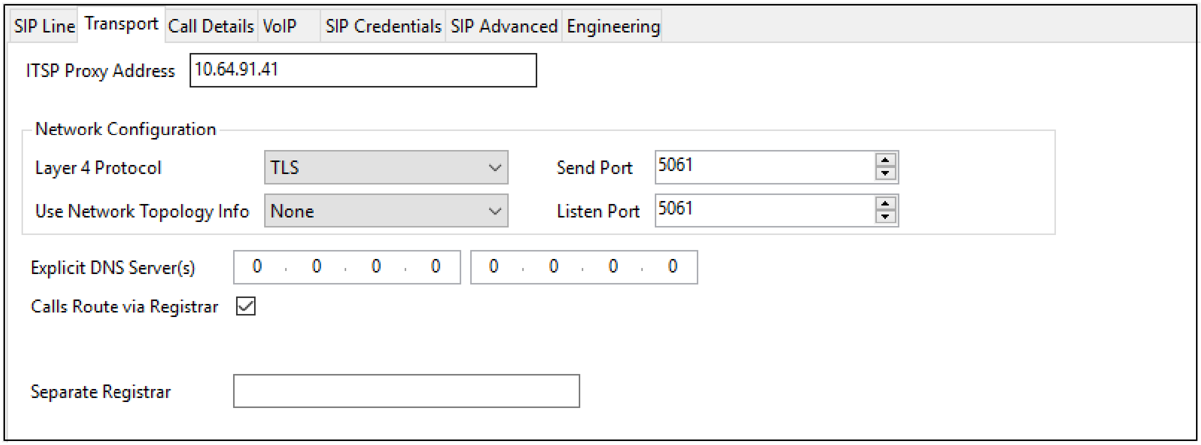
Session Timers
Refresh Method: Re-invite
Timer (sec): 1800

Redirect and Transfer
Incoming Supervised REFER: Auto
Outgoing Supervised REFER: Auto
Send 302 Moved Temporarily ☐
Outgoing Blind REFER ☐

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., **10.64.91.41**).
- **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).



ITSP Proxy Address: 10.64.91.41

Network Configuration

Layer 4 Protocol: TLS

Send Port: 5061

Use Network Topology Info: None

Listen Port: 5061

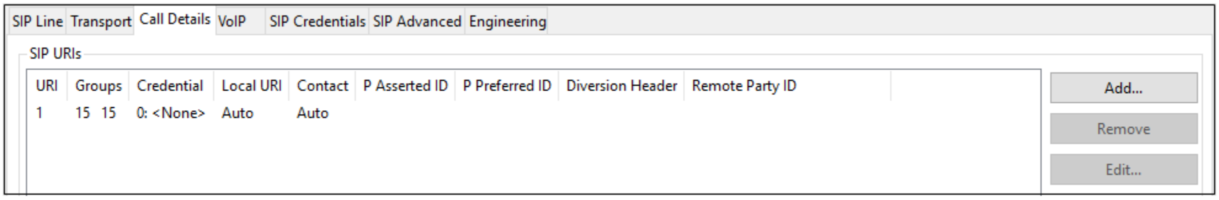
Explicit DNS Server(s): 0 . 0 . 0 . 0 | 0 . 0 . 0 . 0

Calls Route via Registrar ☑

Separate Registrar

5.5.4. SIP Line – Call Details tab

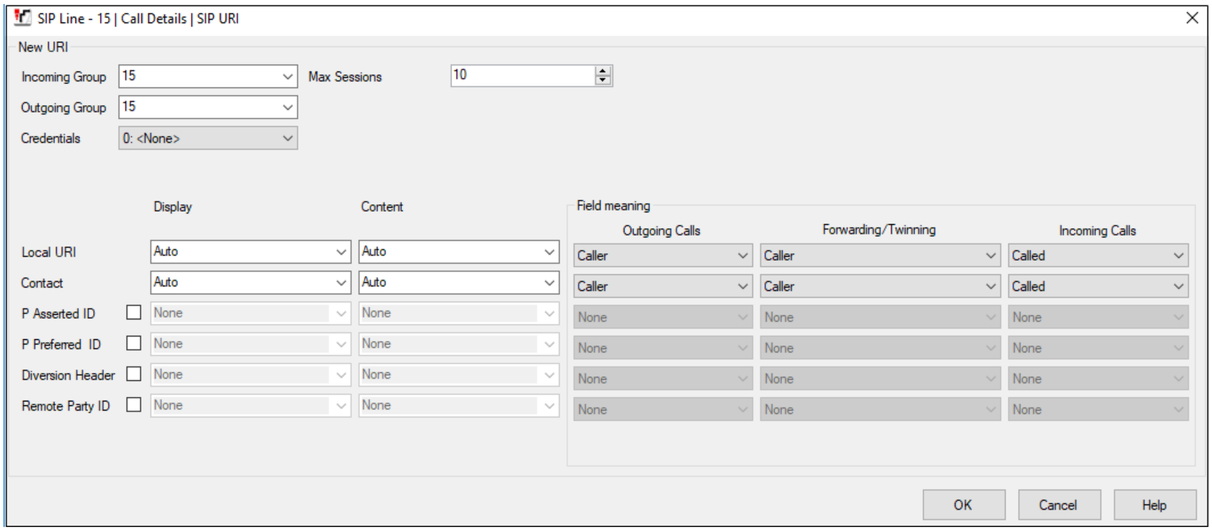
Select the **Call Details** tab. To add a new SIP URI, click the **Add…** button. To review an existing SIP URI, select it and click the **Edit** button.



URI	Groups	Credential	Local URI	Contact	P Asserted ID	P Preferred ID	Diversion Header	Remote Party ID
1	15 15	0: <None>	Auto	Auto				

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

- **Incoming Group:** Set to an unused group number, e.g., **15**. This value references the **Line Group ID** set on the **Incoming Call Routes** in **Section 5.8**.
- **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 an unused group number, e.g., **15**.
- For the **Local URI**, and **Contact** fields, leave the selections under the **Display** and **Content** columns to the default **Auto**.
- On the **Field meaning** section, set the values as shown on the screenshot below.
- Click **OK**.



Incoming Group: 15 Max Sessions: 10

Outgoing Group: 15

Credentials: 0: <None>

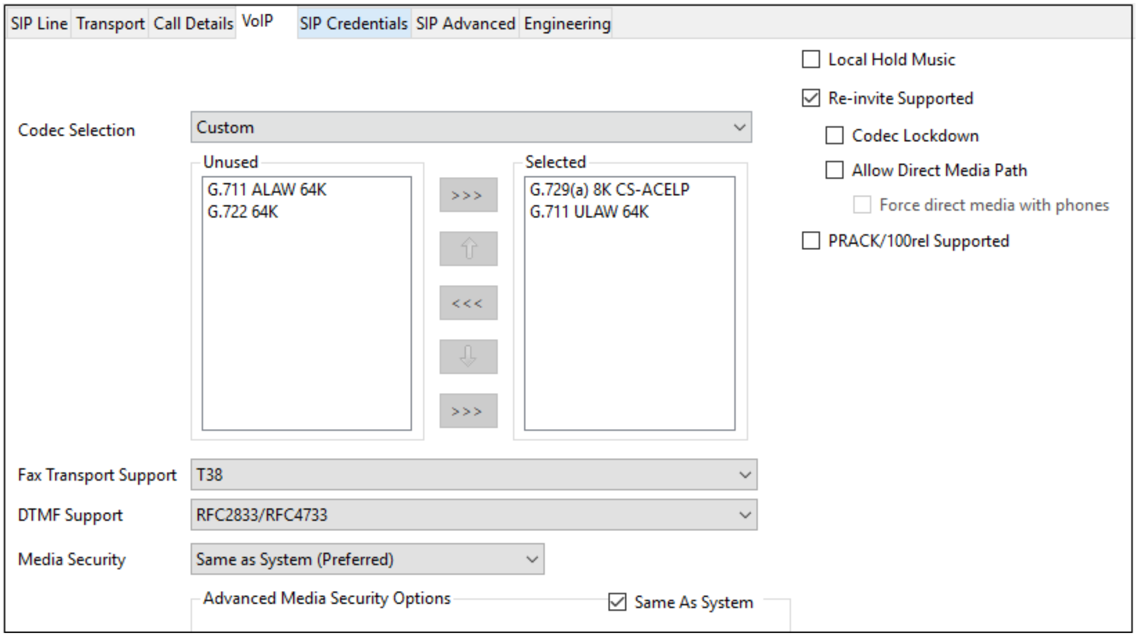
		Display	Content	Outgoing Calls	Forwarding/Twinning	Incoming Calls
Local URI		Auto	Auto	Caller	Caller	Called
Contact		Auto	Auto	Caller	Caller	Called
P Asserted ID	☐	None	None	None	None	None
P Preferred ID	☐	None	None	None	None	None
Diversion Header	☐	None	None	None	None	None
Remote Party ID	☐	None	None	None	None	None

- To edit an existing entry, click an entry in the list and click the **Edit** button.
- When all SIP URI entries have been added or edited, click **OK** at the bottom of the screen (not shown).

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 IPTF network.
- T.38 fax is the preferred method for fax. Set the **Fax Transport Support** to **T.38** from drop-down menu. G.711 fax was additionally tested in the reference configuration (T.38 option disabled). See **Section 2.2** for limitations in the use of SG3 fax machines at the CPE.
- 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)**. Verify that the **Same as System** parameter is checked. This setting will use the same media security level for the trunk as is defined for the system in **Section 5.3.4**. The system level media security is set to **Preferred,** specifying that SRTP is preferred over RTP.
- 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).



Codec Selection: Custom

Unused: G.711 ALAW 64K, G.722 64K

Selected: G.729(a) 8K CS-ACELP, G.711 ULAW 64K

Fax Transport Support: T38

DTMF Support: RFC2833/RFC4733

Media Security: Same as System (Preferred)

Advanced Media Security Options

☑ Same As System

□ Local Hold Music

☑ Re-invite Supported

□ Codec Lockdown

□ Allow Direct Media Path

□ Force direct media with phones

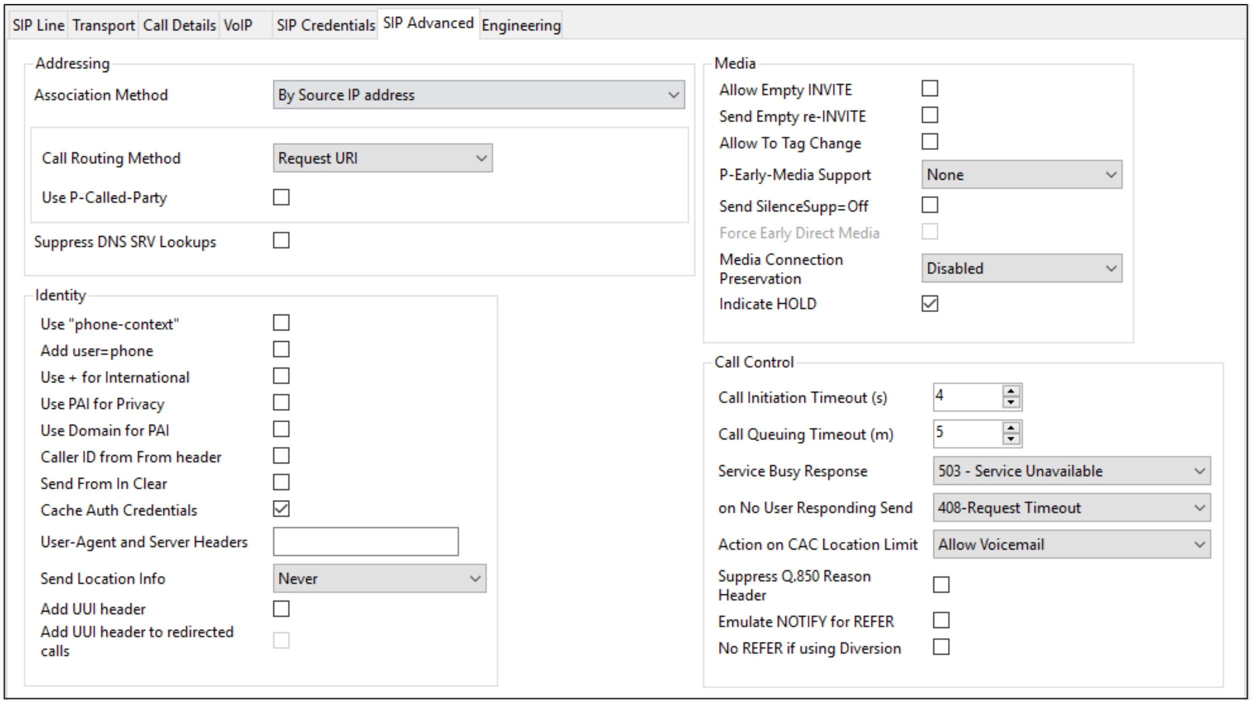
□ PRACK/100rel Supported

5.5.6. SIP Line – SIP Advanced Tab

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.

To have Avaya IP Office signal to AT&T when a call is placed on/off hold, select the **SIP Line → SIP Advanced** tab and enter the following:

- Select **Indicate HOLD** in the **Media** section.
- Click **OK** to commit (not shown).



Addressing

Association Method: By Source IP address

Call Routing Method: Request URI

Use P-Called-Party ☐

Suppress DNS SRV Lookups ☐

Identity

Use "phone-context" ☐

Add user=phone ☐

Use + for International ☐

Use PAI for Privacy ☐

Use Domain for PAI ☐

Caller ID from From header ☐

Send From In Clear ☐

Cache Auth Credentials ☑

User-Agent and Server Headers:

Send Location Info: Never

Add UUI header ☐

Add UUI header to redirected calls ☐

Media

Allow Empty INVITE ☐

Send Empty re-INVITE ☐

Allow To Tag Change ☐

P-Early-Media Support: None

Send SilenceSupp=Off ☐

Force Early Direct Media ☐

Media Connection Preservation: Disabled

Indicate HOLD ☑

Call Control

Call Initiation Timeout (s): 4

Call Queuing Timeout (m): 5

Service Busy Response: 503 - Service Unavailable

on No User Responding Send: 408-Request Timeout

Action on CAC Location Limit: Allow Voicemail

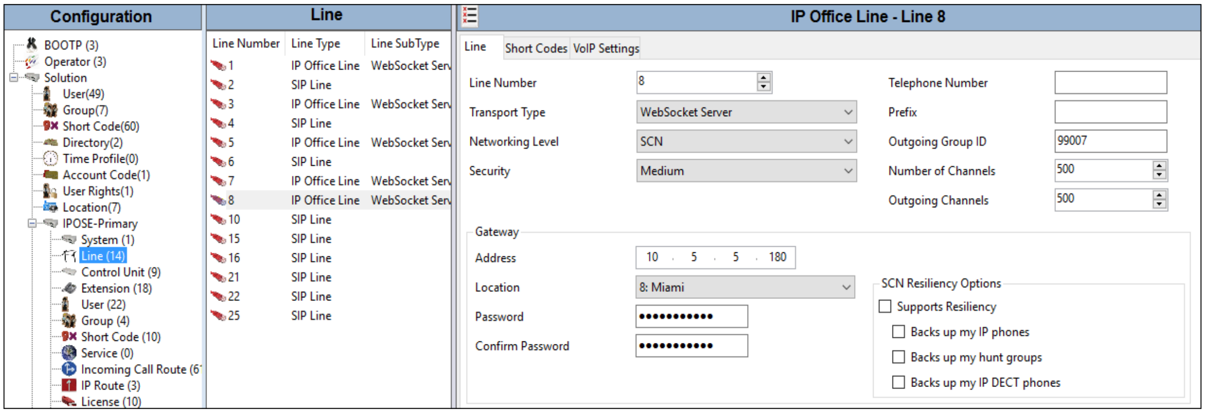
Suppress Q.850 Reason Header ☐

Emulate NOTIFY for REFER ☐

No REFER if using Diversion ☐

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.



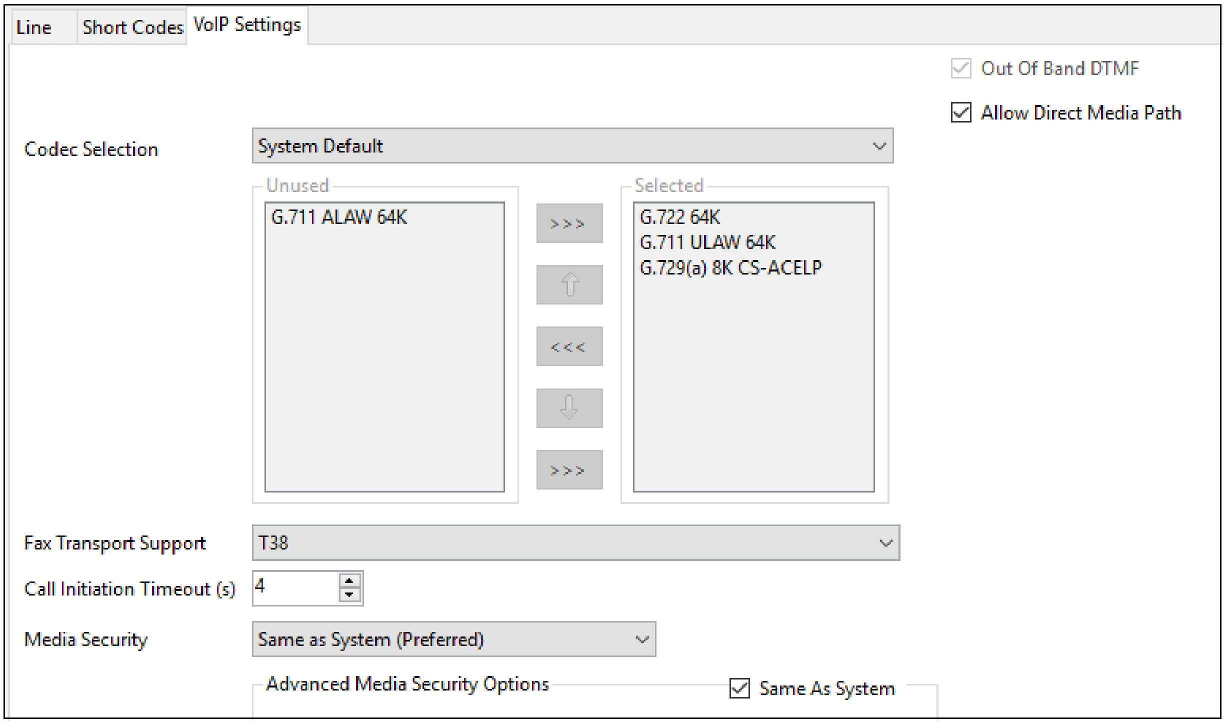
Line Number	Line Type	Line SubType
1	IP Office Line	WebSocket Serv
2	SIP Line	
3	IP Office Line	WebSocket Serv
4	SIP Line	
5	IP Office Line	WebSocket Serv
6	SIP Line	
7	IP Office Line	WebSocket Serv
8	IP Office Line	WebSocket Serv
10	SIP Line	
15	SIP Line	
16	SIP Line	
21	SIP Line	
22	SIP Line	
25	SIP Line	

Line Number: 8
Transport Type: WebSocket Server
Networking Level: SCN
Security: Medium
Telephone Number:
Prefix:
Outgoing Group ID: 99007
Number of Channels: 500
Outgoing Channels: 500

Gateway
Address: 10 . 5 . 5 . 180
Location: 8: Miami
Password: ●●●●●●●●●●●
Confirm Password: ●●●●●●●●●●●

SCN Resiliency Options
□ Supports Resiliency
□ Backs up my IP phones
□ Backs up my hunt groups
□ Backs up my IP DECT phones

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.



☑ Out Of Band DTMF
☑ Allow Direct Media Path

Codec Selection: System Default

Unused
G.711 ALAW 64K

Selected
G.722 64K
G.711 ULAW 64K
G.729(a) 8K CS-ACELP

Fax Transport Support: T38
Call Initiation Timeout (s): 4
Media Security: Same as System (Preferred)

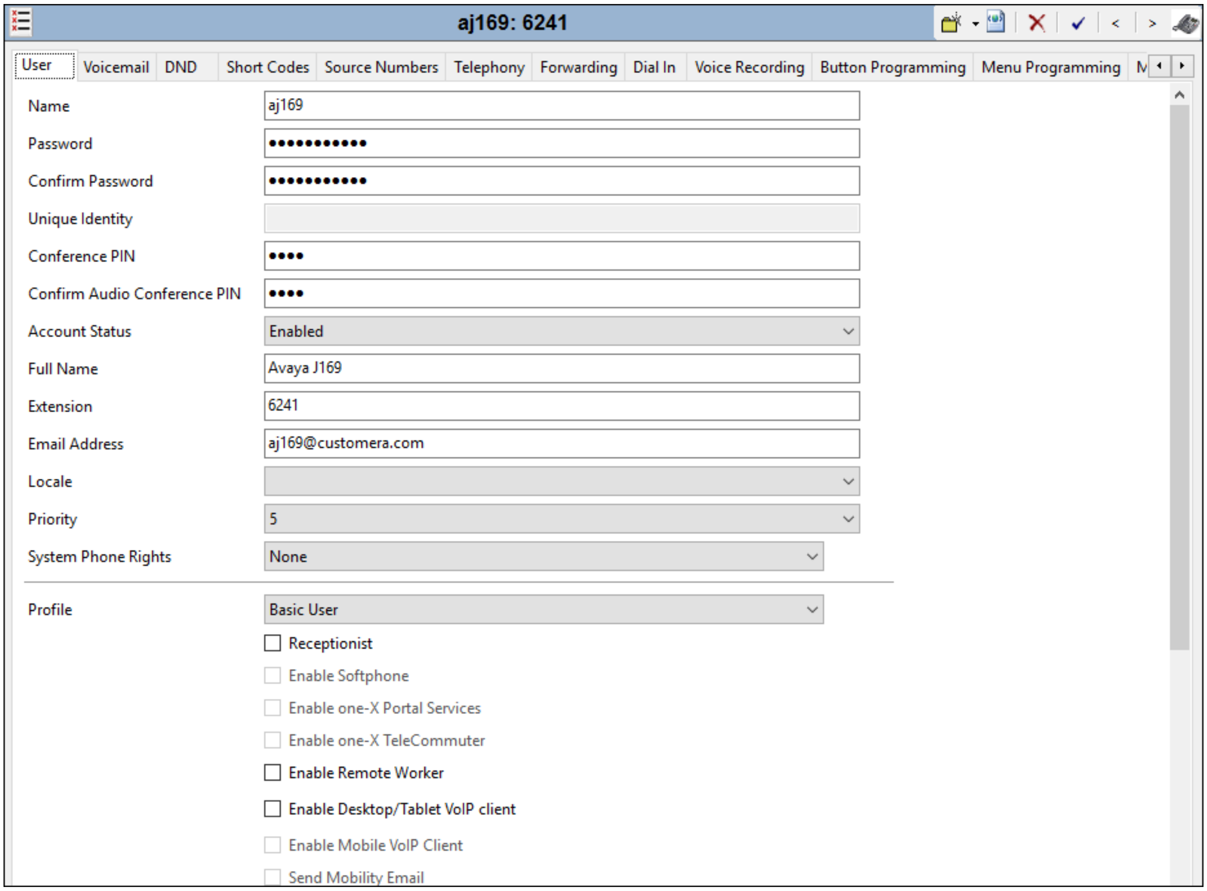
Advanced Media Security Options
☑ Same As System

5.7. Users, Extensions, and Hunt Groups

In this section, examples of IP Office Users, Extensions, and Groups will be illustrated. In the interests of brevity, only one of the users and extensions shown in **Figure 1** will be presented, since the configuration can be easily extrapolated to other users. To add a User, right click on **User** in the **Navigation** pane, and select **New**. To edit an existing User, select **User** in the **Navigation** pane, and select the appropriate user to be configured in the **Group** pane.

5.7.1. User

The following screen shows the **User** tab for user 6241. As shown in **Figure 1**, this user corresponds to the Avaya J169 SIP endpoint.



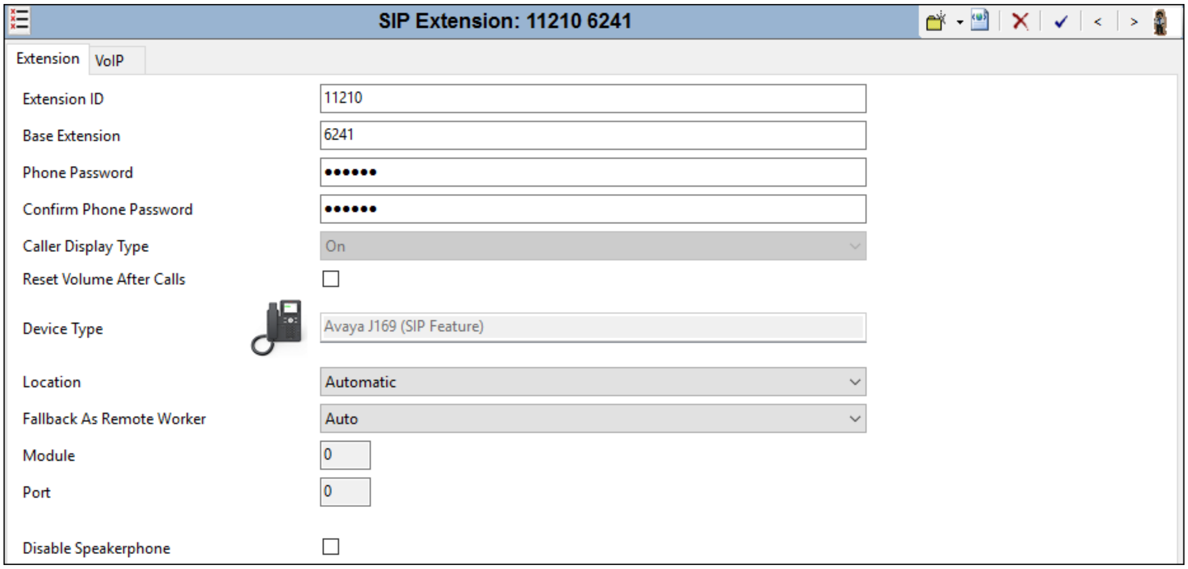
aj169: 6241

Name	aj169
Password	●●●●●●●●●●●
Confirm Password	●●●●●●●●●●●
Unique Identity	
Conference PIN	●●●●
Confirm Audio Conference PIN	●●●●
Account Status	Enabled
Full Name	Avaya J169
Extension	6241
Email Address	aj169@customera.com
Locale	
Priority	5
System Phone Rights	None
Profile	Basic User

□ Receptionist
□ Enable Softphone
□ Enable one-X Portal Services
□ Enable one-X TeleCommuter
□ Enable Remote Worker
□ Enable Desktop/Tablet VoIP client
□ Enable Mobile VoIP Client
□ Send Mobility Email

5.7.2. Extension

The following screen shows the Extension information for user 6241 (Avaya J169 SIP). To view, select **Extension** from the Navigation pane, and the appropriate extension from the Group pane.

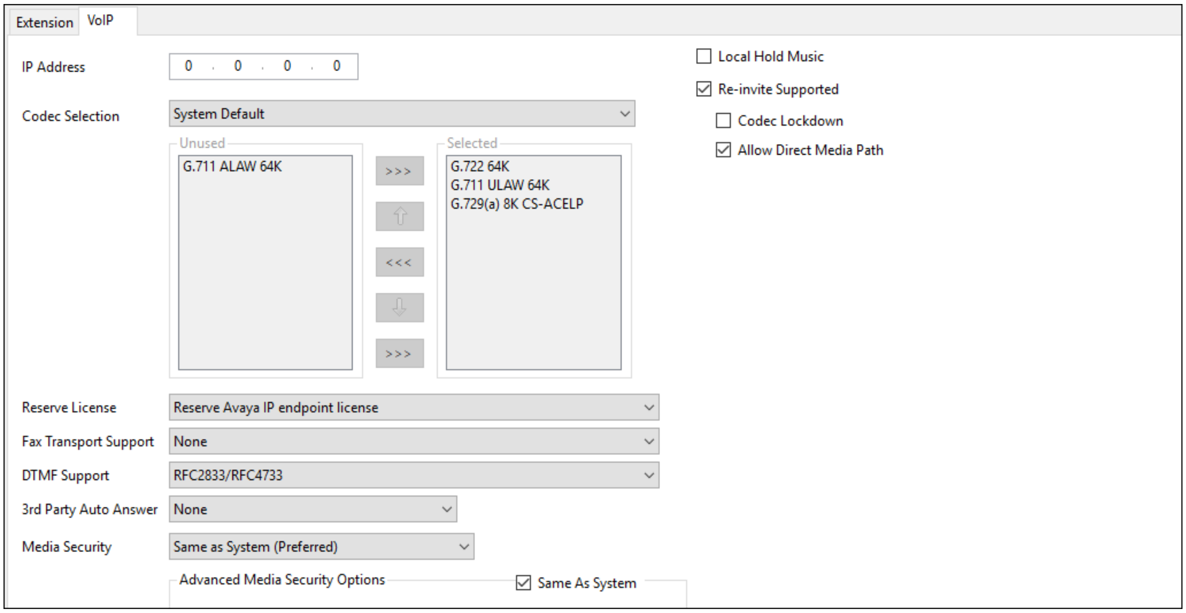


SIP Extension: 11210 6241

Extension | VoIP

Extension ID	11210
Base Extension	6241
Phone Password	••••••
Confirm Phone Password	••••••
Caller Display Type	On
Reset Volume After Calls	□
Device Type	Avaya J169 (SIP Feature)
Location	Automatic
Fallback As Remote Worker	Auto
Module	0
Port	0
Disable Speakerphone	□

The following screen shows the **VoIP** tab for the extension. The **IP Address** field may be left blank. Check the **Reserve Avaya IP endpoint license** box. The **Codec Selection** parameter may retain the default setting "**System Default**" to follow the system configuration shown in **Section 5.3.4**. The Media Security parameter may also retain the default setting "**Same as System (Preferred)**" to follow the system configuring shown in **Section 5.3.4**.



Extension | VoIP

IP Address	0 . 0 . 0 . 0
Codec Selection	System Default
Unused	G.711 ALAW 64K
Selected	G.722 64K G.711 ULAW 64K G.729(a) 8K CS-ACELP
Reserve License	Reserve Avaya IP endpoint license
Fax Transport Support	None
DTMF Support	RFC2833/RFC4733
3rd Party Auto Answer	None
Media Security	Same as System (Preferred)

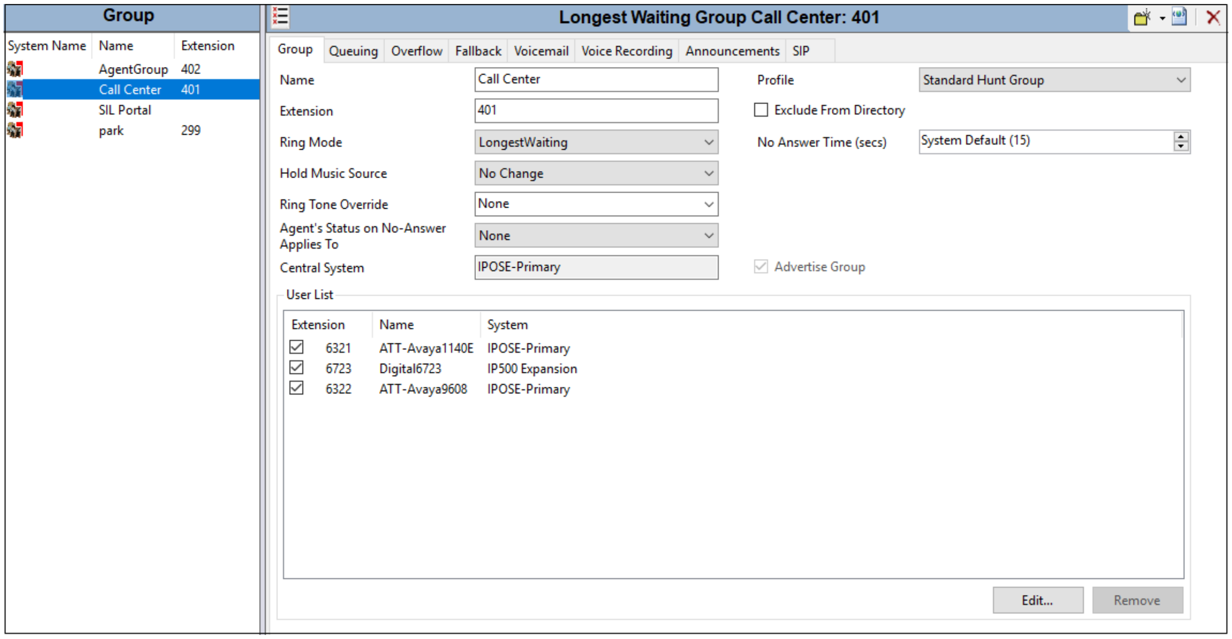
Advanced Media Security Options ☑ Same As System

□ Local Hold Music
☑ Re-invite Supported
□ Codec Lockdown
☑ Allow Direct Media Path

5.7.3. Hunt Groups

During the verification of these Application Notes, users could also receive incoming calls as members of a hunt group. To configure a new hunt group, right-click **Group** from the Navigation pane, and select **New**. To view or edit an existing hunt group, select **Group** from the Navigation pane, and the appropriate hunt group from the Group pane.

The following screen shows the **Group** tab for hunt group 401. The telephone extensions in the **User List** are rung based the extension that has been unused for the longest period, due to the **Ring Mode** setting "**Longest Waiting**" (i.e., "longest waiting", most idle user receives next call). Click the **Edit** button to change the **User List**.



Group

System Name	Name	Extension
	AgentGroup	402
	Call Center	401
	SIL Portal	
	park	299

Longest Waiting Group Call Center: 401

Name: Call Center
Extension: 401
Ring Mode: LongestWaiting
Hold Music Source: No Change
Ring Tone Override: None
Agent's Status on No-Answer Applies To: None
Central System: IPOSE-Primary
Profile: Standard Hunt Group
□ Exclude From Directory
No Answer Time (secs): System Default (15)
☑ Advertise Group

User List

	Extension	Name	System
☑	6321	ATT-Avaya1140E	IPOSE-Primary
☑	6723	Digital6723	IP500 Expansion
☑	6322	ATT-Avaya9608	IPOSE-Primary

In the reference configuration, these steps were used to create the additional Hunt Group "AgentGroup" (402).

5.8. Incoming Call Route

Note – The digits defined and matched in the Incoming Call Route table, are the DNIS digits specified in the AT&T Request-URI, not the DID digits dialed by the caller.

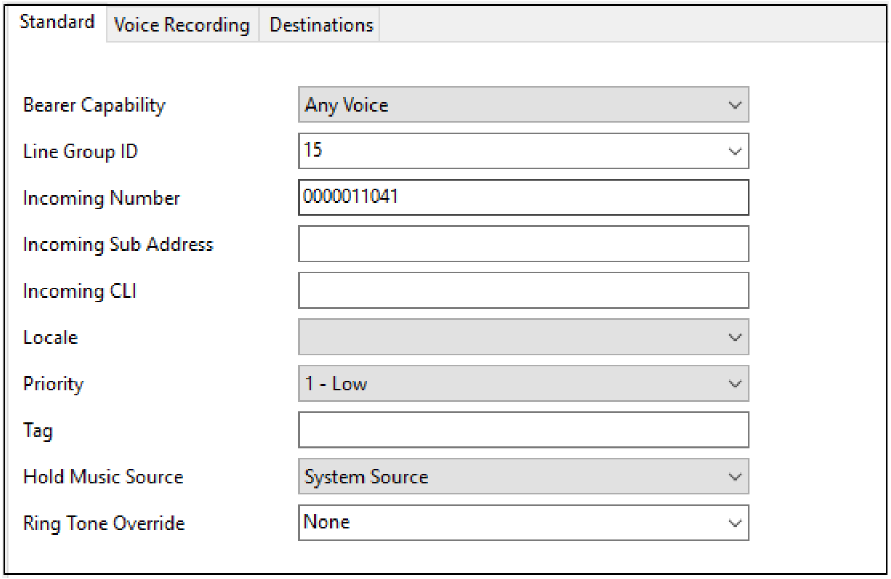
The Incoming Call Route table will map specific AT&T DNIS numbers to an IP Office User, or Hunt Group, as well as to Voicemail Pro scripts.

To add an incoming call route, right click on **Incoming Call Route** in the Navigation pane and select **New** (not shown). To edit an existing incoming call route, select an **Incoming Call Route** in the Navigation pane, and the associated call route information is displayed in the Group pane.

5.8.1. Calls to IP Office Stations and Hunt Groups

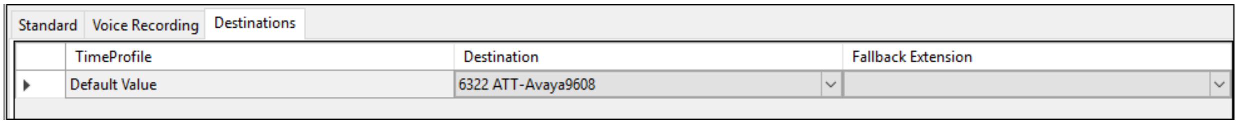
In the example below, the incoming number **0000011041** is directed to H.323 phone 6322.
On the **Standard** tab enter the following:

- **Line Group ID**: Enter the SIP Line defined in **Section 5.5** (e.g., **15**).
- **Incoming Number**: Enter the associated DNIS digits sent by AT&T (e.g., **0000011041**).
- Use default values for the remaining fields and click **OK** (not shown).



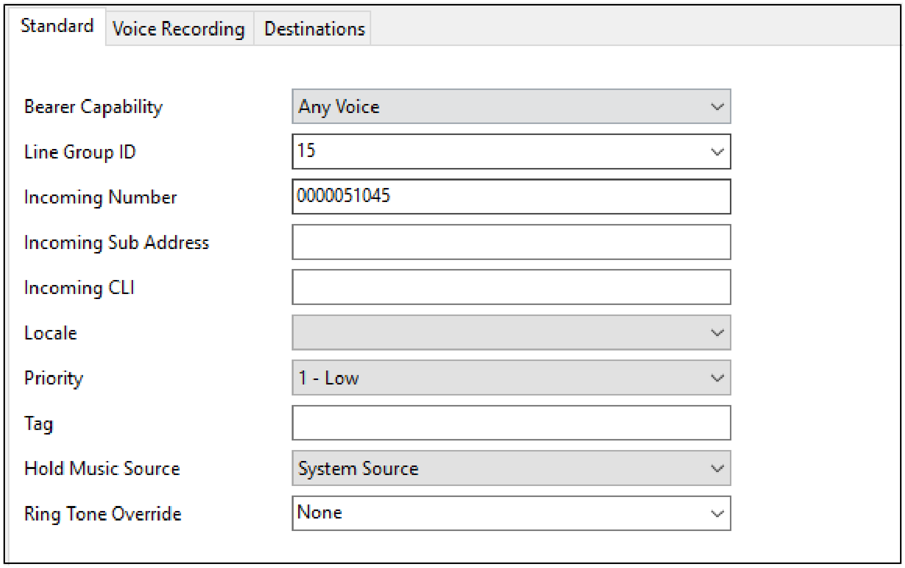
Bearer Capability	Any Voice
Line Group ID	15
Incoming Number	0000011041
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

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 **0000011041** was associated with the Avaya IP Office user at extension **6322**.

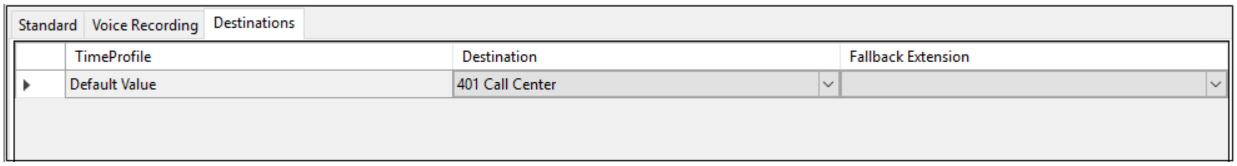


TimeProfile	Destination	Fallback Extension
Default Value	6322 ATT-Avaya9608	

Below is an example of a call for AT&T DNIS **0000051045** being directed to Hunt Group **401** (Call Center).



Bearer Capability	Any Voice
Line Group ID	15
Incoming Number	0000051045
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None



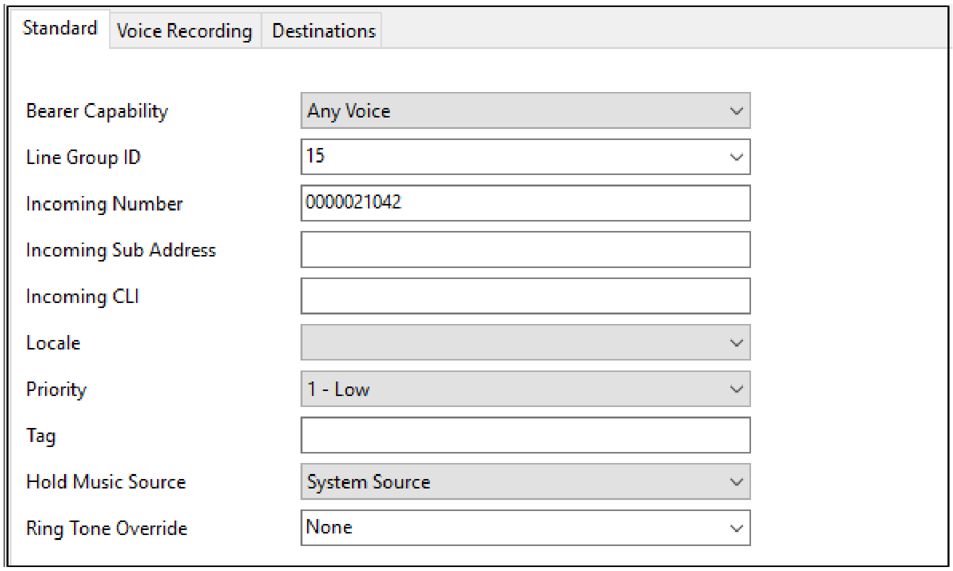
TimeProfile	Destination	Fallback Extension
Default Value	401 Call Center	

5.8.2. Calls to Voicemail Pro Scripts

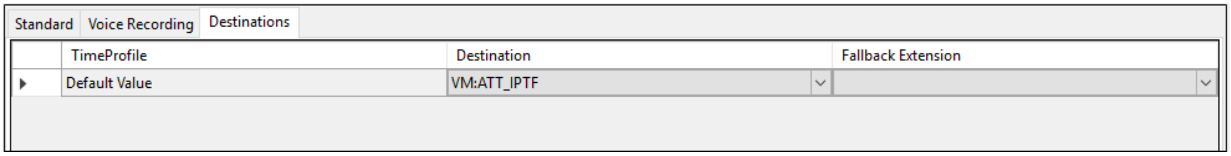
As described next in **Section 5.9**, Voicemail Pro scripts are defined with specific names. These script names are specified as destinations in the Incoming Call Route table.

In the example below, incoming number **0000021042** is directed to the Voicemail Pro Auto-Attendant script **ATT_IPTF**.

1. On the **Standard** tab repeat the steps in **Section 5.8.1**, with the following changes:
   - **Incoming Number**: Enter the associated DNIS digits sent by AT&T (e.g., **0000021042**).
2. On the **Destinations** tab enter the following:
   - In the **Destinations** column, enter the string **VM:ATT_IPTF** from the drop down menu (note if the voicemail module does not appear in the list, enter the value manually).
   - Use default values for the remaining fields and click **OK** (not shown).



Bearer Capability	Any Voice
Line Group ID	15
Incoming Number	0000021042
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None



TimeProfile	Destination	Fallback Extension
Default Value	VM:ATT_IPTF	

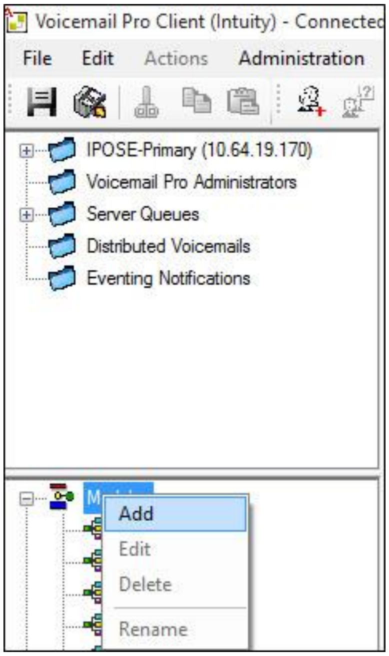
5.9. Call Center Provisioning in Voicemail Pro

Note – While Voicemail Pro provisioning and programming is beyond the scope of this document, a sample Auto-Attendant script is described below.

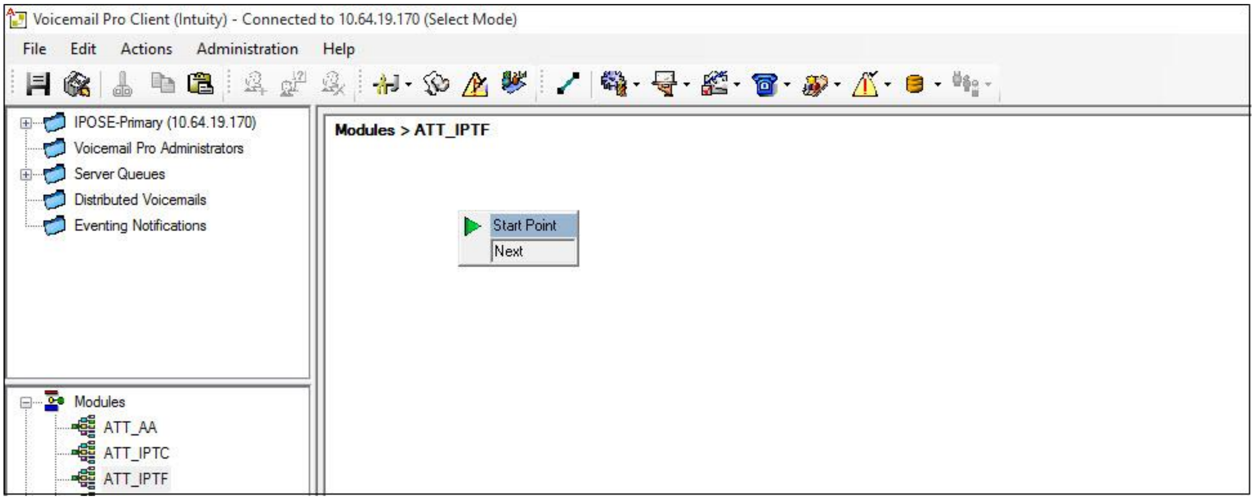
In the reference configuration, Voicemail Pro is used for Voicemail processing as well as for simulating basic Call Center functionality.

The Auto-Attendant function was provisioned to prompt callers to select a numeric option (1, 2, or 3), that would transfer the call to an associated Avaya IP Office Hunt Group (Call Center, AgentGroup), or to a specific extension. This is accomplished via the following steps:

1. Hunt Groups **Call Center** and **AgentGroup** are created in IP Office (**Section 5.7.3**).
2. User 6241 is created in IP Office (**Section 5.7.1**)
3. Incoming Call Route for DNIS digits **0000021042** is defined for access to the Auto-Attendant script (**Section 5.8.2**).
4. Via the Voicemail Pro GUI interface:
    - Open the **Voicemail Pro Client** application and log in to the Voicemail Pro server (not shown).
    - Create a **Start Point** by right clicking on **Modules** and selecting **Add**.

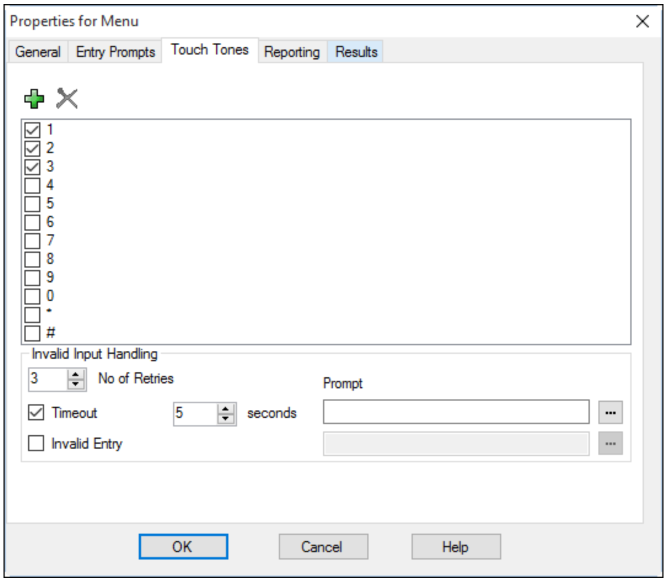


- Enter a name (e.g., **ATT_IPTF**) and click on **OK** (not shown). The new script “ATT_IPTF” will appear under Modules and a Start Point icon will appear in the work area.



- Click on the **Start Point** icon to activate the script options at the top of the screen. From the options, select the **Basic Actions** icon, select the **Menu** icon, and click on the work area to place the **Menu** icon.
  i. Double click the **Start Point** icon.
    1. On the **General** tab → **Token Name**, enter **Start Point** and click **OK** (not shown).

  ii. Double click the **Menu** icon.
    1. On the **General** tab → **Token Name**, enter **Menu** (not shown).
    2. On the **Entry Prompts** tab (not shown), select or create an **Entry Prompt** that will tell the caller what digits to press (e.g., **mainmenu.wav**). To modify an existing recording, double click on the .wav file and rerecord. If no .wav files exist, double click on the icon to open the .wav editor.
    3. On the **Touch Tone** tab:
       a. Select **1, 2,** and **3** as the possible entry digits.
       b. Select **3** for **No of Retries**.
    4. Click on **OK**.



Properties for Menu

General | Entry Prompts | Touch Tones | Reporting | Results

☑ 1
☑ 2
☑ 3
☐ 4
☐ 5
☐ 6
☐ 7
☐ 8
☐ 9
☐ 0
☐ *
☐ #

Invalid Input Handling

3 No of Retries

Prompt

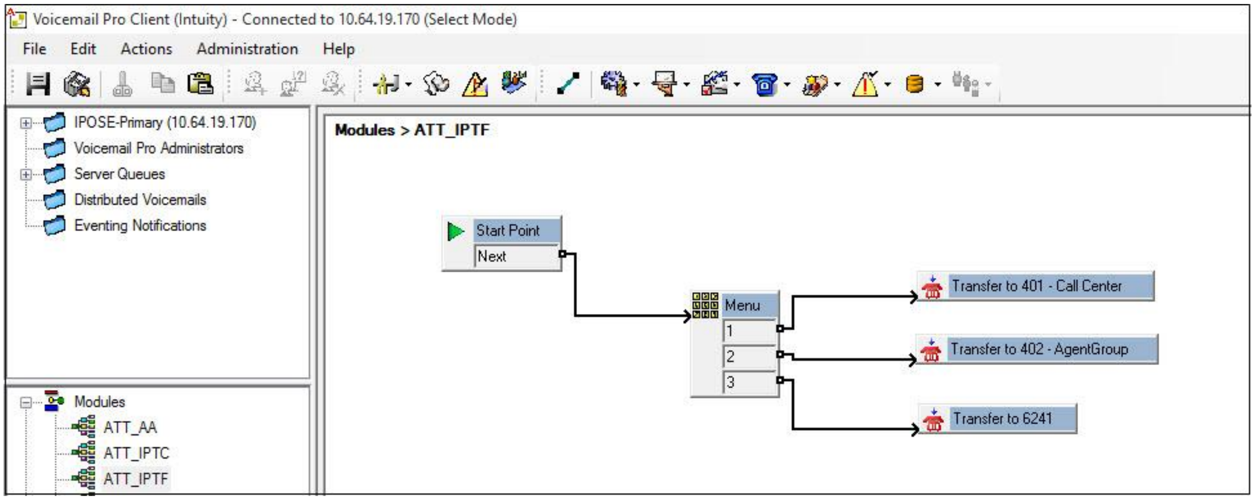
☑ Timeout 5 seconds

☐ Invalid Entry

OK | Cancel | Help

- Click on the Telephony Actions icon ☎, select the Transfer icon ☎, and click on the work area to place the **Transfer** icon in the work area. This will be used for “Call Center”. Select and place two more Transfer Icons (these will be used for “AgentGroup” and “User 6241”).
    - i. Double click on the first **Transfer** icon.
        1. On the **General** tab → **Token Name** = **Transfer to 401 - Call Center** (not shown).
        2. On the **Specific** tab → **Destination = 401** (not shown).
    - ii. Double click on the second **Transfer** icon.
        1. On the **General** tab → **Token Name** = **Transfer to 402 - AgentGroup** (not shown).
        2. On the **Specific** tab → **Destination** = **402** (not shown).
    - iii. Double Click on the third **Transfer** icon.
        1. On the **General** tab, **Token Name** = **Transfer to 6241** (not shown).
        2. On the **Specific** tab, **Destination = 6241** (not shown).

- From the options bar, select the Connector icon and:
    - i. Drag a connecting flow line from the **Start Point** box to the **Menu** box (see screen shot below).
    - ii. Drag connecting flow lines from each of the **Menu** options to their associated **Transfer** boxes (see screenshot below).


Voicemail Pro Client (Intuity) - Connected to 10.64.19.170 (Select Mode)
File
Edit
Actions
Administration
Help
IPOSE-Primary (10.64.19.170)
Voicemail Pro Administrators
Server Queues
Distributed Voicemails
Eventing Notifications
Modules
ATT_AA
ATT_IPTC
ATT_IPTF
Modules > ATT_IPTF
Start Point
Next
Menu
1
2
3
Transfer to 401 - Call Center
Transfer to 402 - AgentGroup
Transfer to 6241

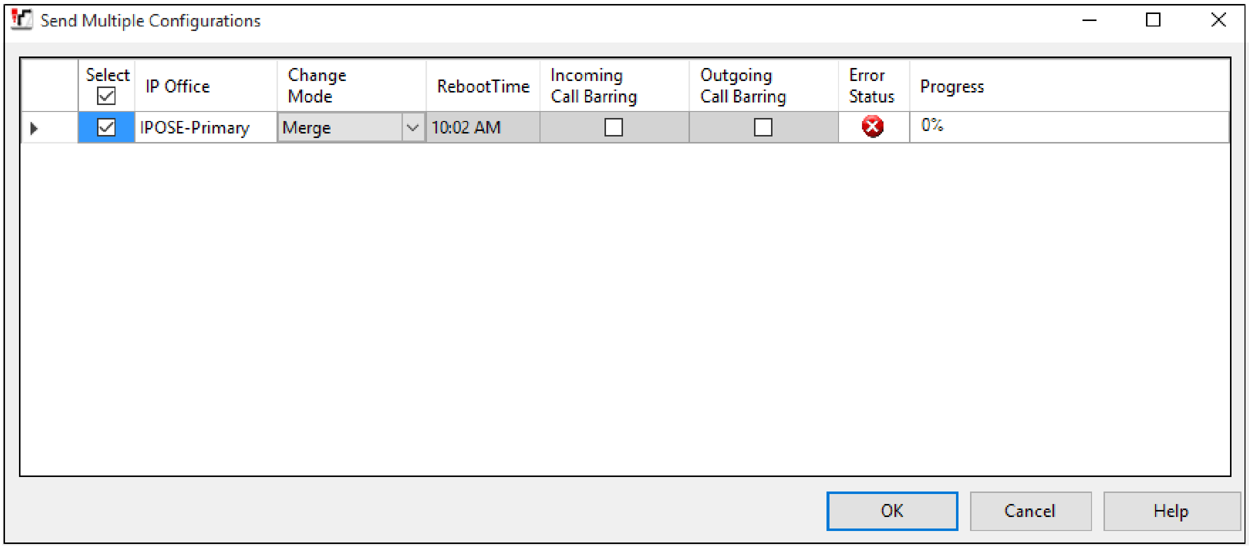
5. From the top menu select **File → Save & Make Live** or select the icon.

When the associated AT&T DNIS number is received (e.g., **0000021042**), IP Office will send the call to Voicemail Pro. The caller will be prompted to enter 1, 2, or 3 to access Call Center, AgentGroup, or user 6241. The associated Avaya IP Office extension (e.g., 401, 402, or 6241) will then ring.

5.10. 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).

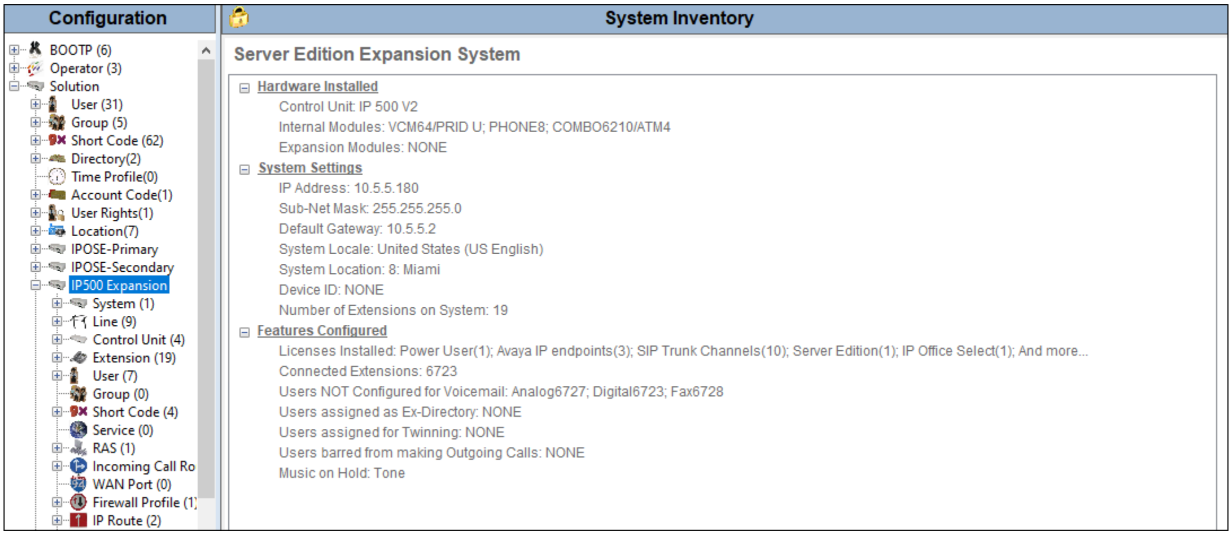
A screen similar to the one below will appear, with either **Merge** or **Reboot** automatically selected, based on the nature of the configuration changes. Note that clicking **OK** may cause a service disruption. Click **OK** to proceed.



	Select ☑	IP Office	Change Mode	RebootTime	Incoming Call Barring	Outgoing Call Barring	Error Status	Progress
▸	☑	IPOSE-Primary	Merge	10:02 AM	□	□	☒	0%

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.



Server Edition Expansion System

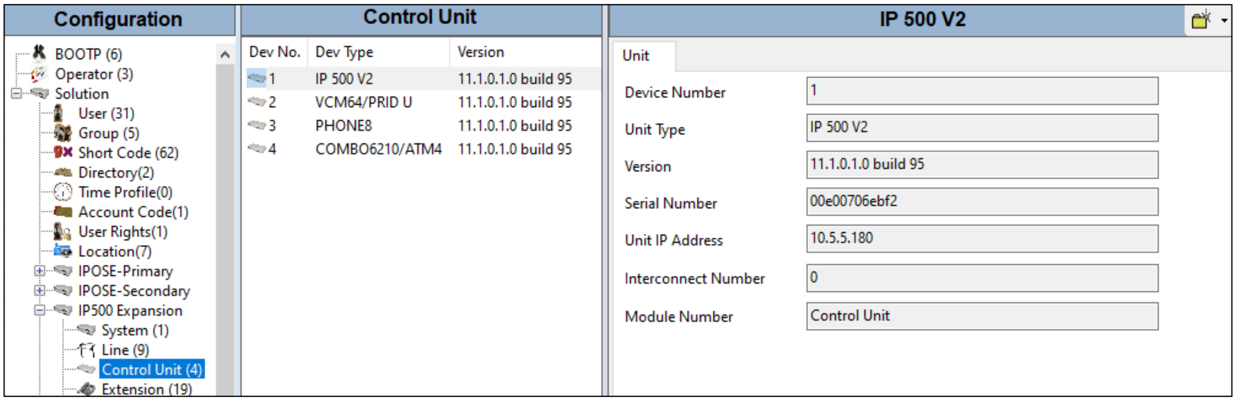
Hardware Installed
- Control Unit: IP 500 V2
- Internal Modules: VCM64/PRID U; PHONE8; COMBO6210/ATM4
- Expansion Modules: NONE

System Settings
- IP Address: 10.5.5.180
- Sub-Net Mask: 255.255.255.0
- Default Gateway: 10.5.5.2
- System Locale: United States (US English)
- System Location: 8: Miami
- Device ID: NONE
- Number of Extensions on System: 19

Features Configured
- Licenses Installed: Power User(1); Avaya IP endpoints(3); SIP Trunk Channels(10); Server Edition(1); IP Office Select(1); And more...
- Connected Extensions: 6723
- Users NOT Configured for Voicemail: Analog6727; Digital6723; Fax6728
- Users assigned as Ex-Directory: NONE
- Users assigned for Twinning: NONE
- Users barred from making Outgoing Calls: NONE
- Music on Hold: Tone

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.



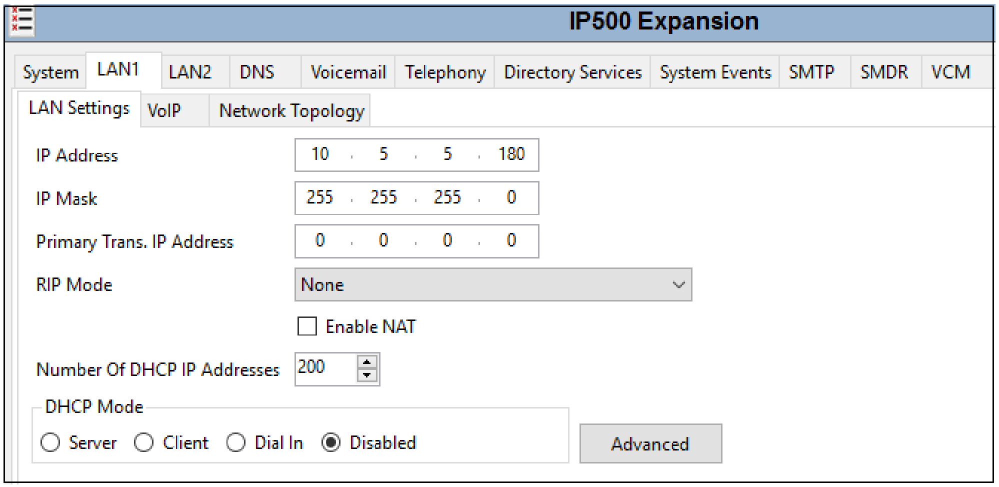
Dev No.	Dev Type	Version
1	IP 500 V2	11.1.0.1.0 build 95
2	VCM64/PRID U	11.1.0.1.0 build 95
3	PHONE8	11.1.0.1.0 build 95
4	COMBO6210/ATM4	11.1.0.1.0 build 95

Device Number	1
Unit Type	IP 500 V2
Version	11.1.0.1.0 build 95
Serial Number	00e00706ebf2
Unit IP Address	10.5.5.180
Interconnect Number	0
Module Number	Control Unit

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).



IP500 Expansion

IP Address	10 . 5 . 5 . 180
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	0 . 0 . 0 . 0
RIP Mode	None
	□ Enable NAT
Number Of DHCP IP Addresses	200

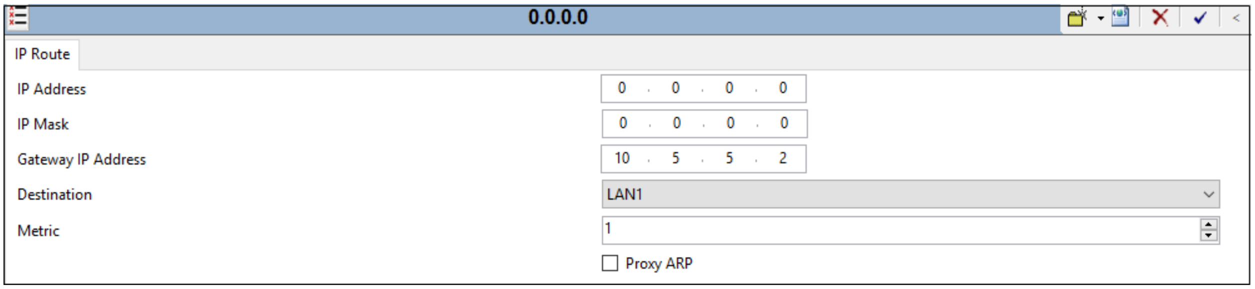
DHCP Mode: ○ Server ○ Client ○ Dial In ● Disabled

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.

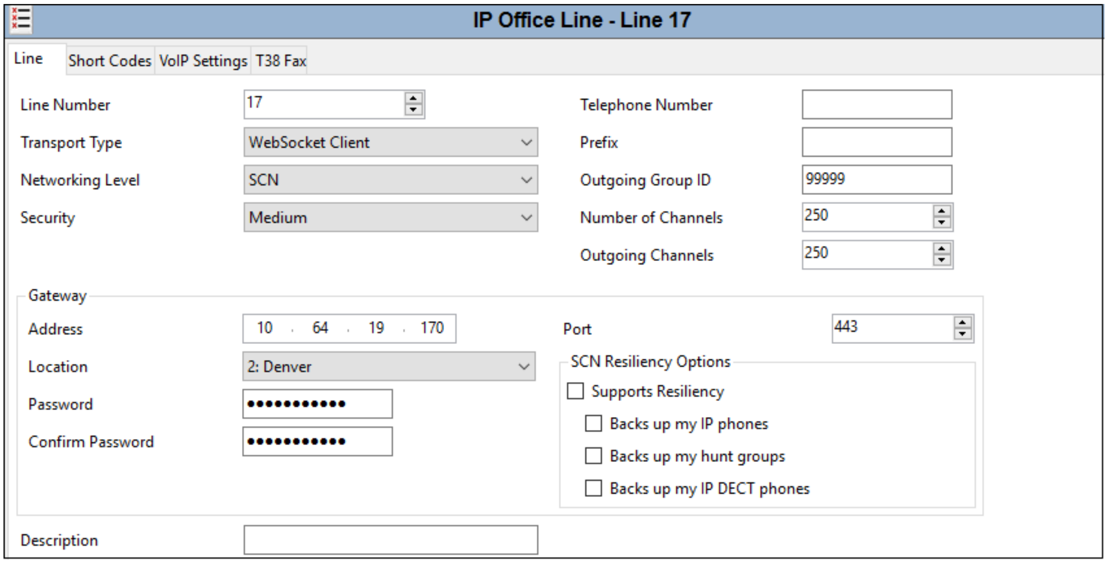


0.0.0.0

IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	10 . 5 . 5 . 2
Destination	LAN1
Metric	1
	□ Proxy ARP

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.



IP Office Line - Line 17

Line Number	17	Telephone Number	
Transport Type	WebSocket Client	Prefix	
Networking Level	SCN	Outgoing Group ID	99999
Security	Medium	Number of Channels	250
		Outgoing Channels	250

Gateway

Address	10 . 64 . 19 . 170	Port	443
Location	2: Denver		
Password	•••••••••••		
Confirm Password	•••••••••••		

SCN Resiliency Options

☐ Supports Resiliency

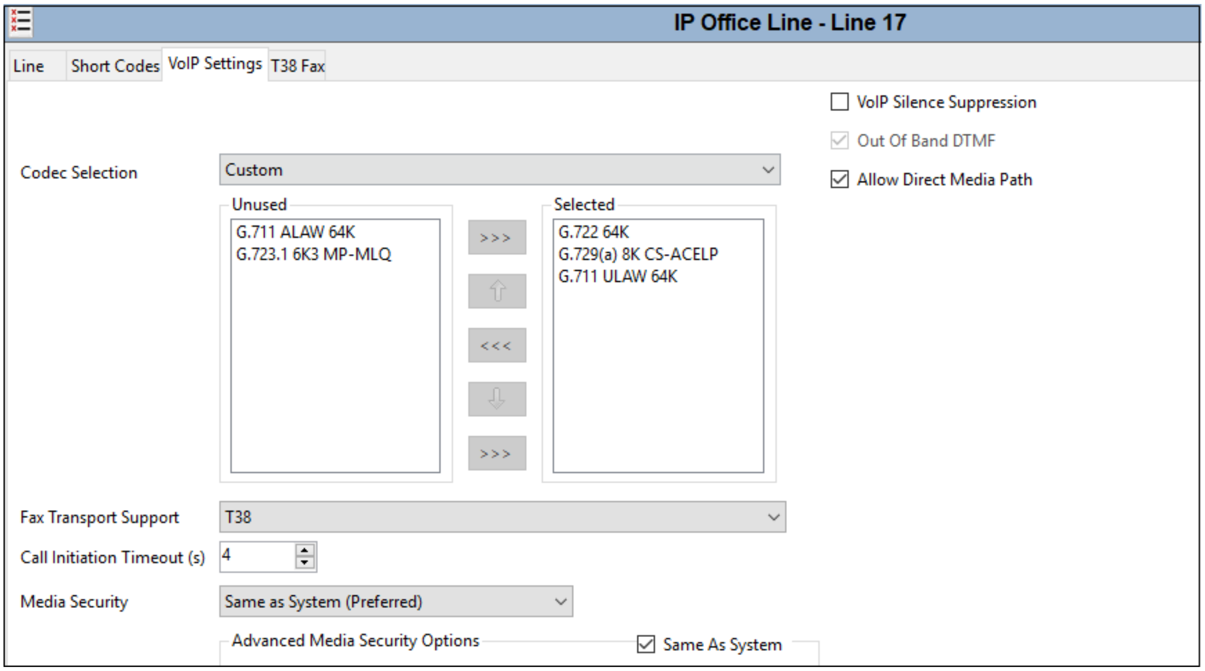
☐ Backs up my IP phones

☐ Backs up my hunt groups

☐ Backs up my IP DECT phones

Description

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.**



IP Office Line - Line 17

☐ VoIP Silence Suppression

☑ Out Of Band DTMF

☑ Allow Direct Media Path

Codec Selection: Custom

Unused	Selected
G.711 ALAW 64K	G.722 64K
G.723.1 6K3 MP-MLQ	G.729(a) 8K CS-ACELP
	G.711 ULAW 64K

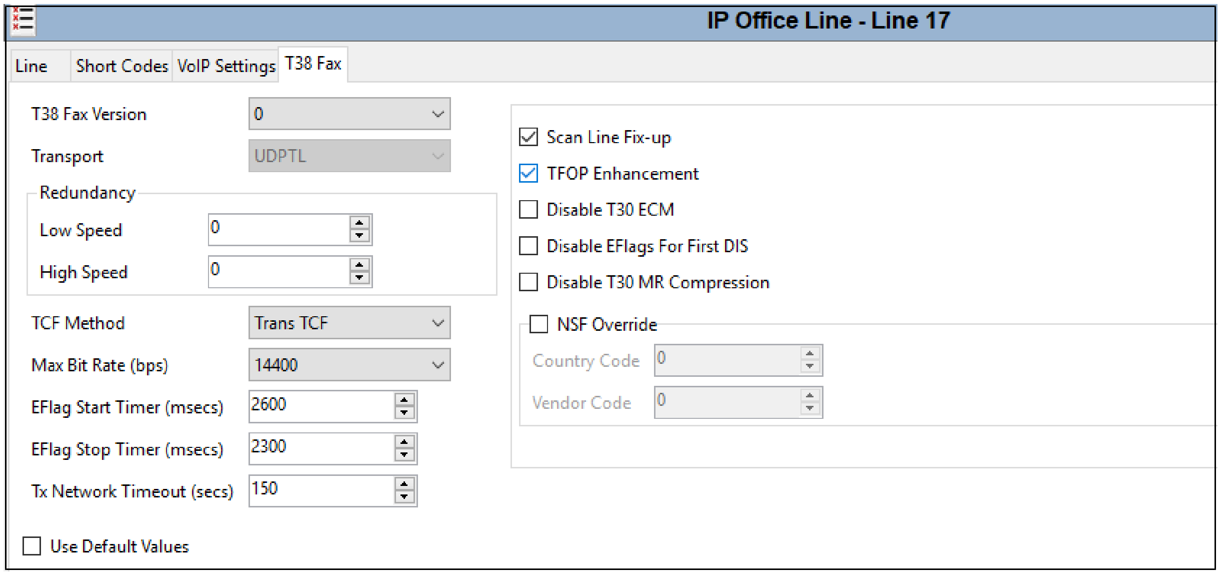
Fax Transport Support: T38

Call Initiation Timeout (s): 4

Media Security: Same as System (Preferred)

Advanced Media Security Options ☑ Same As System

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.



IP Office Line - Line 17

Line | Short Codes | VoIP Settings | T38 Fax

T38 Fax Version: 0

Transport: UDPTL

Redundancy

Low Speed: 0

High Speed: 0

TCF Method: Trans TCF

Max Bit Rate (bps): 14400

EFlag Start Timer (msecs): 2600

EFlag Stop Timer (msecs): 2300

Tx Network Timeout (secs): 150

□ Use Default Values

☑ Scan Line Fix-up

☑ TFOP Enhancement

□ Disable T30 ECM

□ Disable EFlags For First DIS

□ Disable T30 MR Compression

□ NSF Override

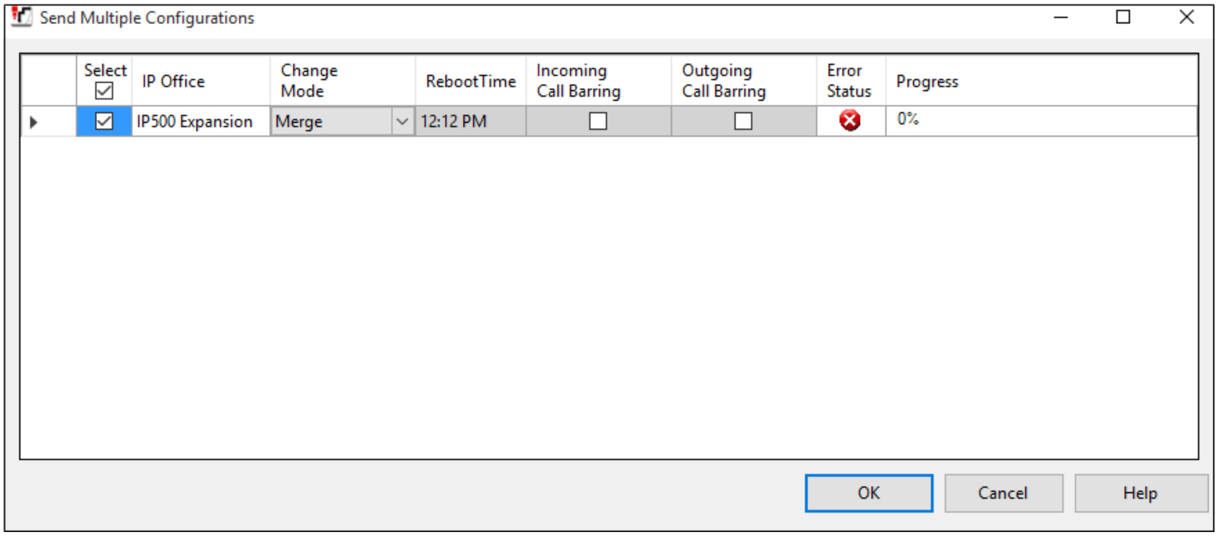
Country Code: 0

Vendor Code: 0

6.5. Save IP Office Expansion System Configuration

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

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



Send Multiple Configurations

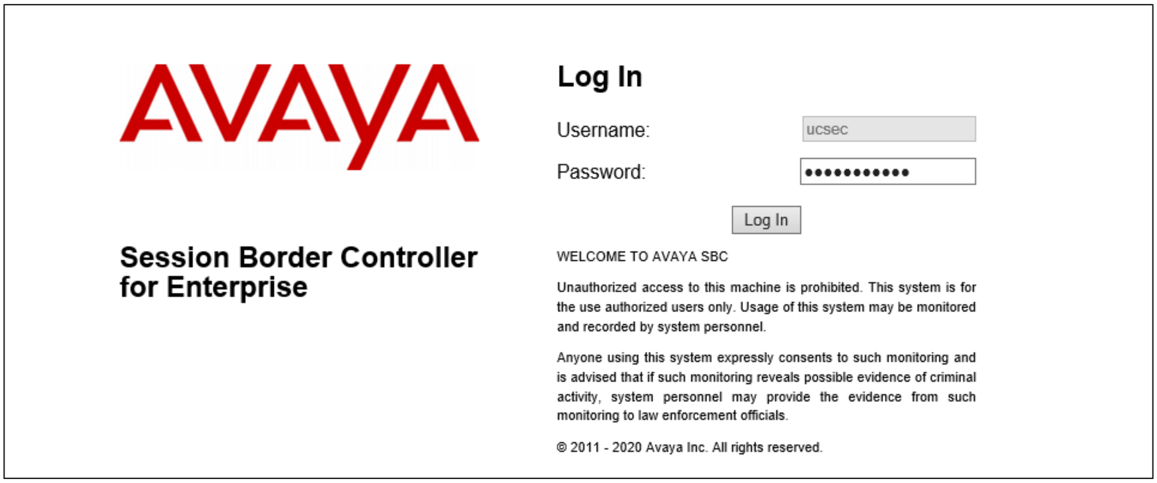
Select ☑	IP Office	Change Mode	RebootTime	Incoming Call Barring	Outgoing Call Barring	Error Status	Progress
☑	IP500 Expansion	Merge	12:12 PM	□	□	☒	0%

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.



Log In

Username: ucsec

Password: ●●●●●●●●●●●

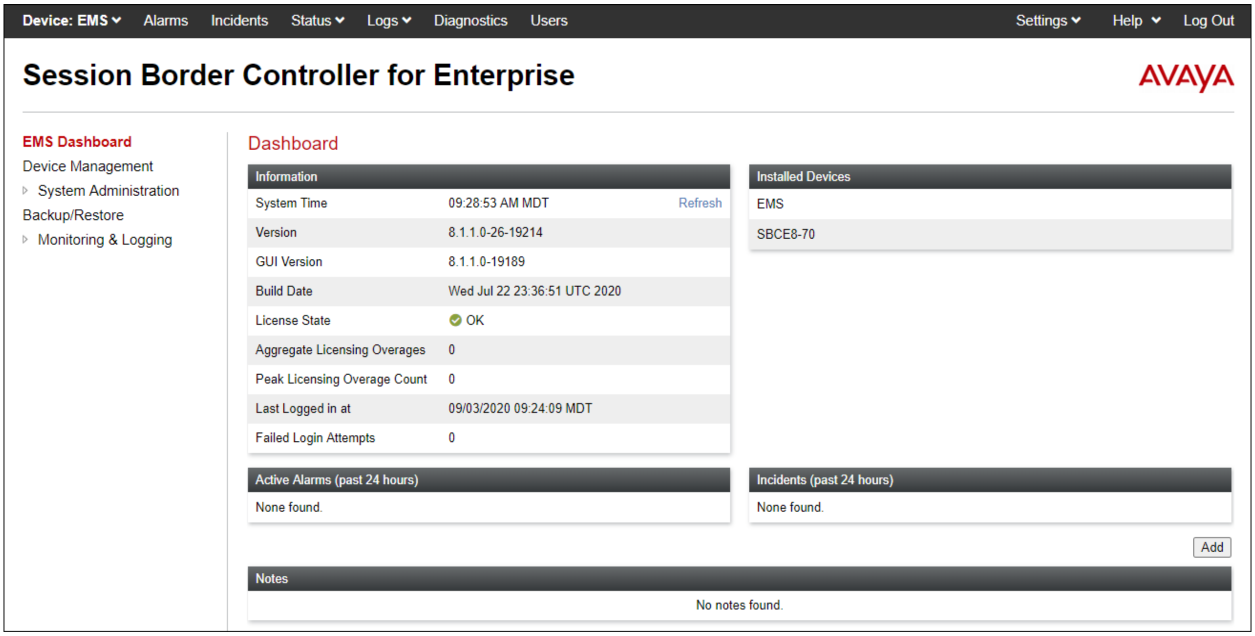
WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

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.



Session Border Controller for Enterprise

Dashboard

Information	
System Time	09:28:53 AM MDT
Version	8.1.1.0-26-19214
GUI Version	8.1.1.0-19189
Build Date	Wed Jul 22 23:36:51 UTC 2020
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	09/03/2020 09:24:09 MDT
Failed Login Attempts	0

Installed Devices
EMS
SBCE8-70

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

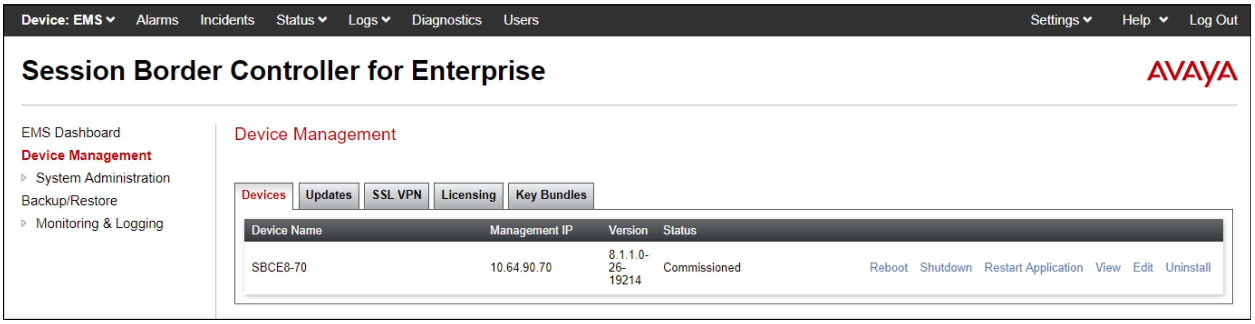
Notes

No notes found.

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.

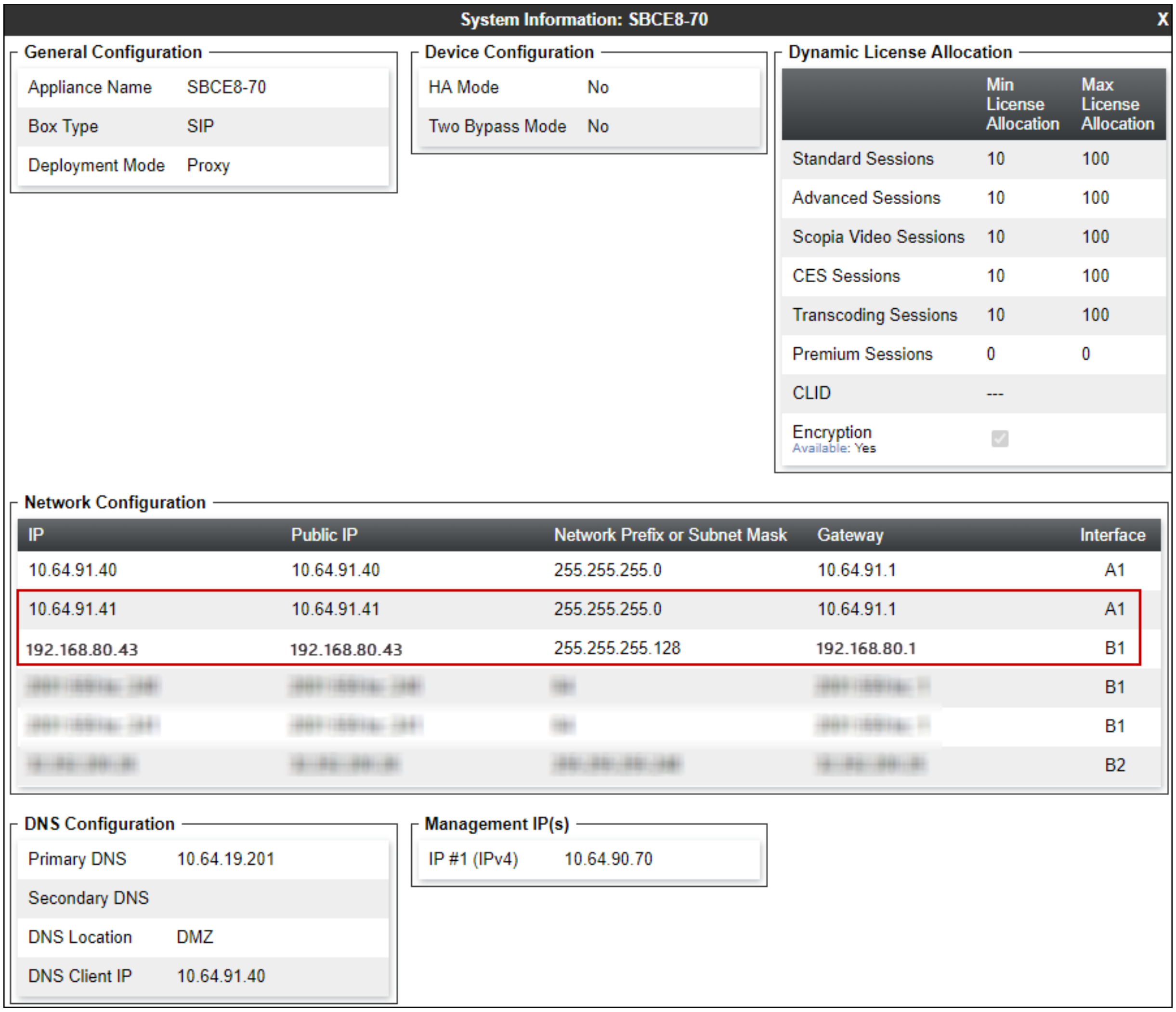


Session Border Controller for Enterprise

Device Management

Device Name	Management IP	Version	Status	
SBCE8-70	10.64.90.70	8.1.1.0-26-19214	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

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 **B1** 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
Premium Sessions	0	0
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
192.168.80.43	192.168.80.43	255.255.255.128	192.168.80.1	B1
[redacted]	[redacted]	[redacted]	[redacted]	B1
[redacted]	[redacted]	[redacted]	[redacted]	B1
[redacted]	[redacted]	[redacted]	[redacted]	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

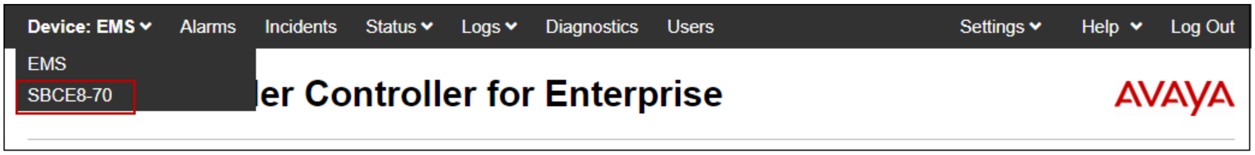
7.2. TLS Management

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.

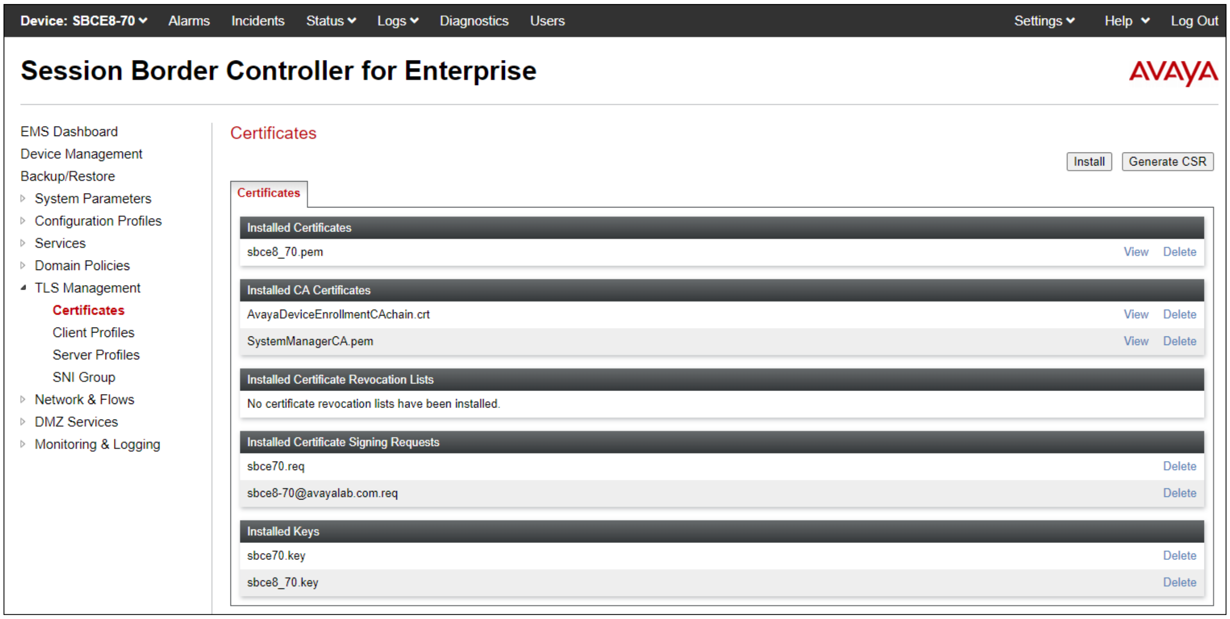
7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

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.



Installed Certificates
sbce8_70.pem View Delete

Installed CA Certificates
AvayaDeviceEnrollmentCAchain.crt View Delete
SystemManagerCA.pem View Delete

Installed Certificate Revocation Lists
No certificate revocation lists have been installed.

Installed Certificate Signing Requests
sbce70.req Delete
sbce8-70@avayalab.com.req Delete

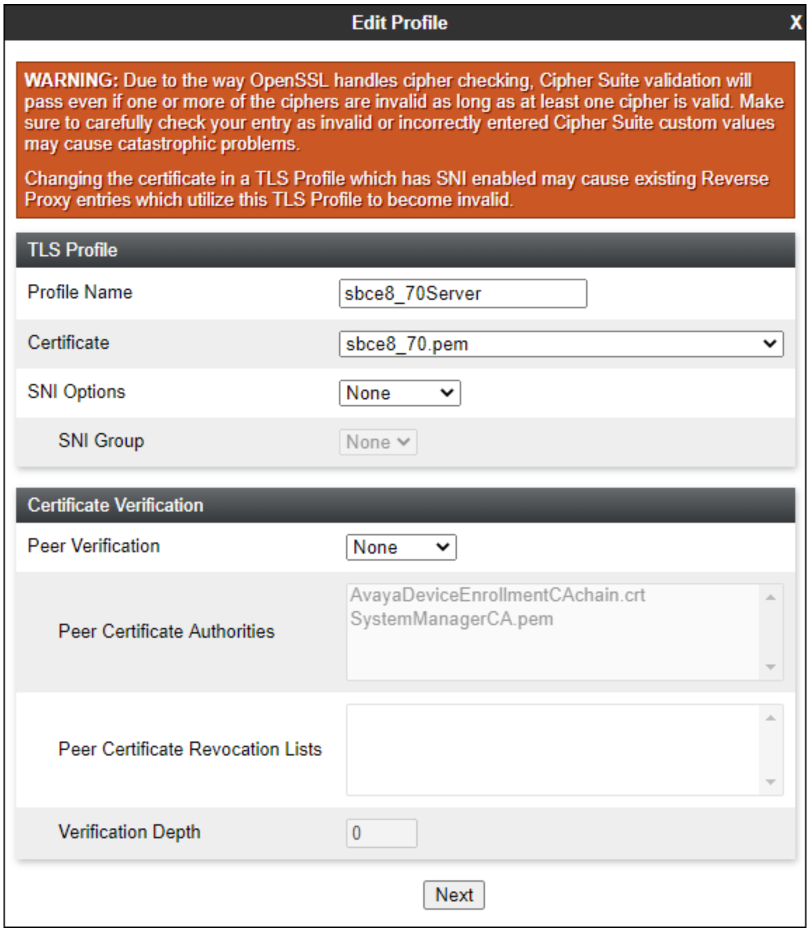
Installed Keys
sbce70.key Delete
sbce8_70.key Delete

7.2.2. Server Profiles

Step 1 - 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**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.



Edit Profile

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

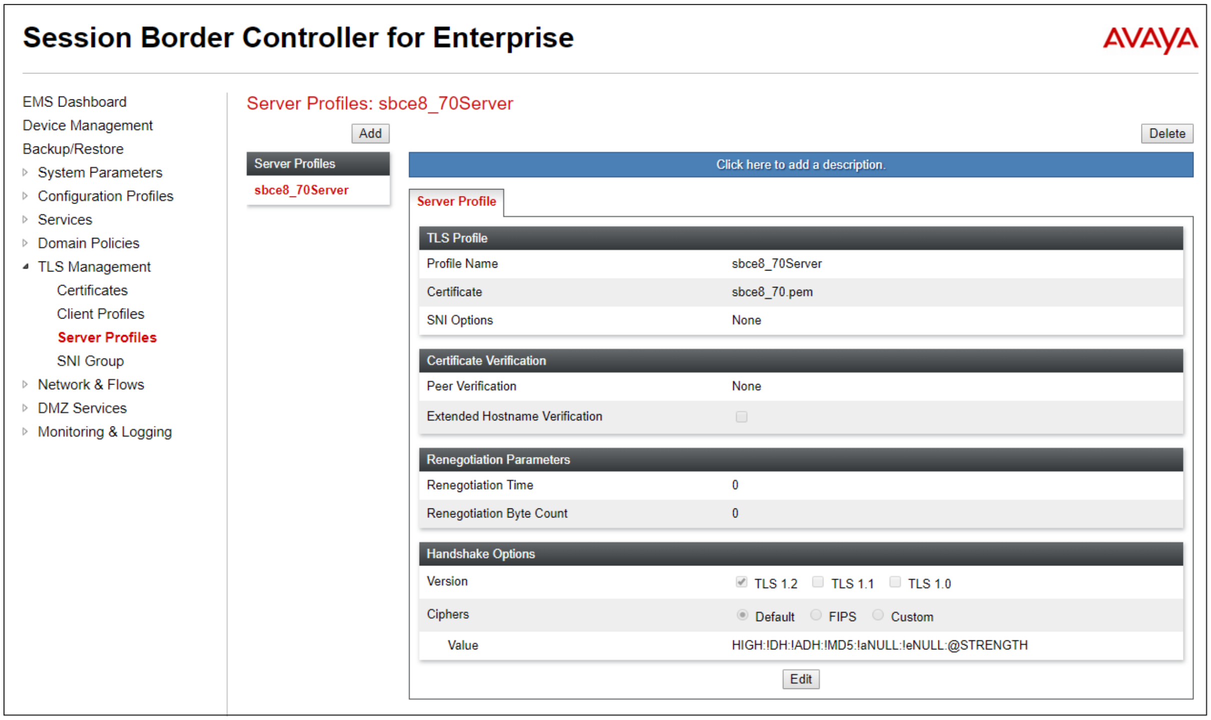
TLS Profile

Profile Name	sbce8_70Server
Certificate	sbce8_70.pem
SNI Options	None
SNI Group	None

Certificate Verification

Peer Verification	None
Peer Certificate Authorities	AvayaDeviceEnrollmentCAchain.crt SystemManagerCA.pem
Peer Certificate Revocation Lists	
Verification Depth	0

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



Server Profiles: sbce8_70Server

TLS Profile	
Profile Name	sbce8_70Server
Certificate	sbce8_70.pem
SNI Options	None

Certificate Verification	
Peer Verification	None
Extended Hostname Verification	□

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

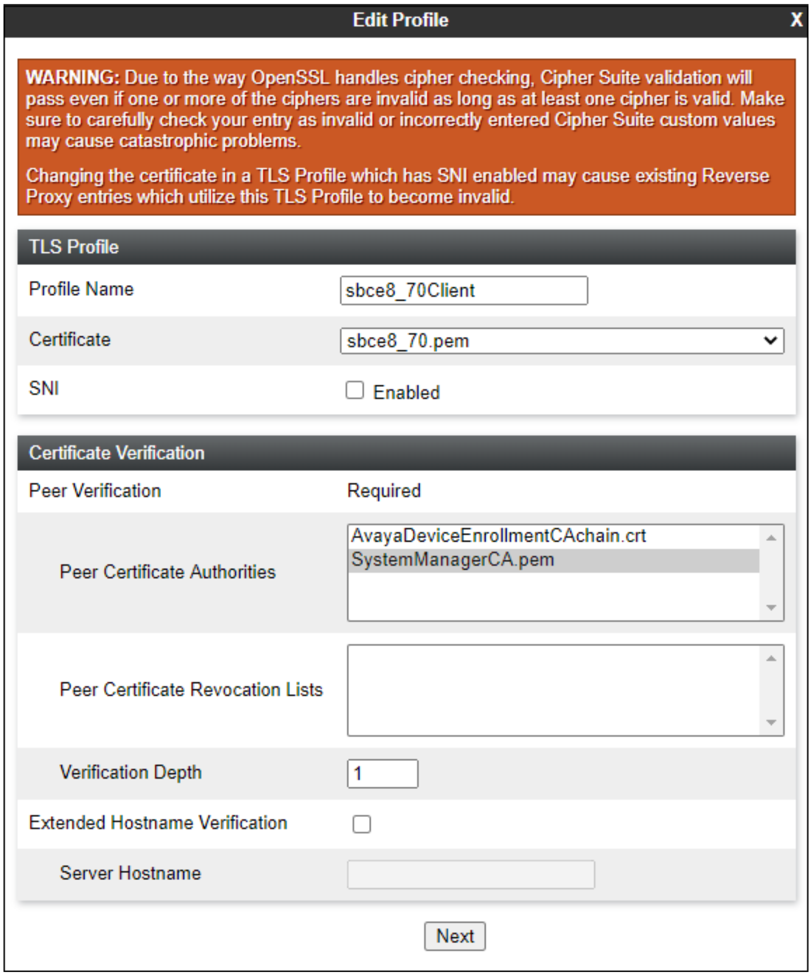
Handshake Options	
Version	☑ TLS 1.2 □ TLS 1.1 □ TLS 1.0
Ciphers	● Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

7.2.3. Client Profiles

Step 1 - 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**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.



WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

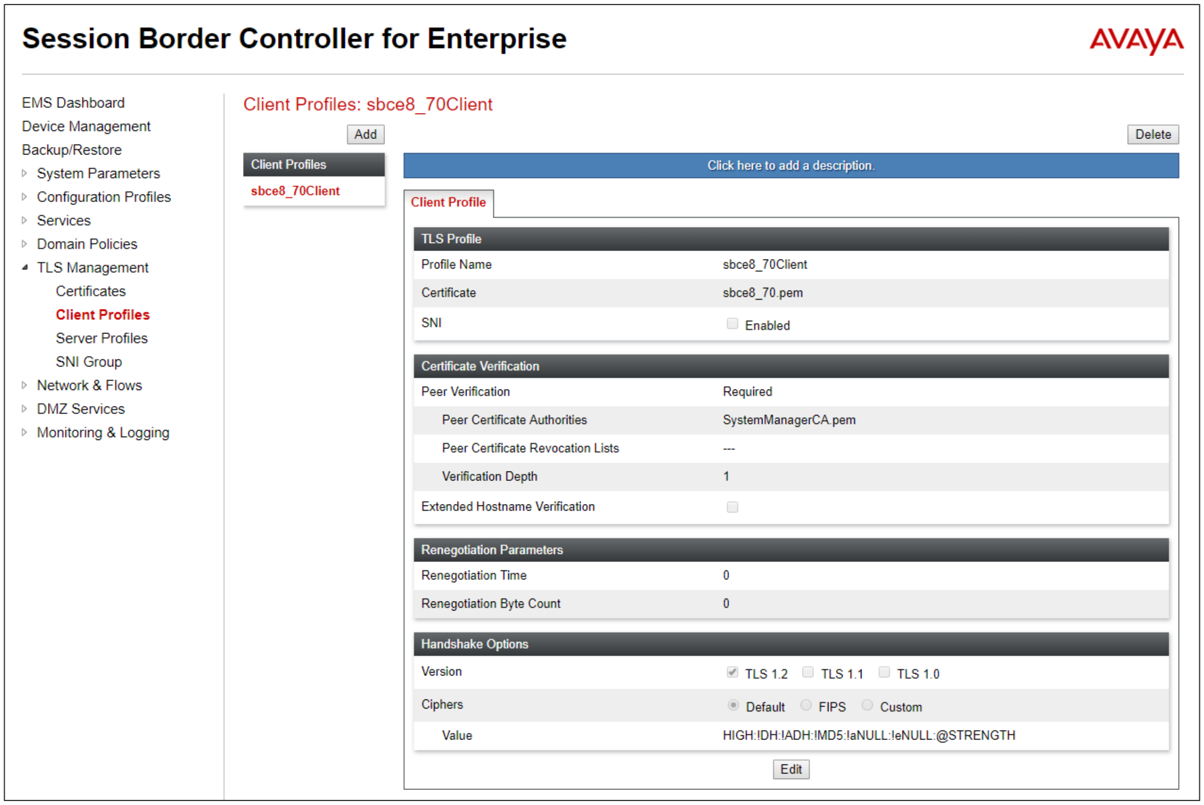
TLS Profile

Profile Name	sbce8_70Client
Certificate	sbce8_70.pem
SNI	□ Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	AvayaDeviceEnrollmentCAchain.crt SystemManagerCA.pem
Peer Certificate Revocation Lists	
Verification Depth	1
Extended Hostname Verification	□
Server Hostname	

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



Client Profiles: sbce8_70Client

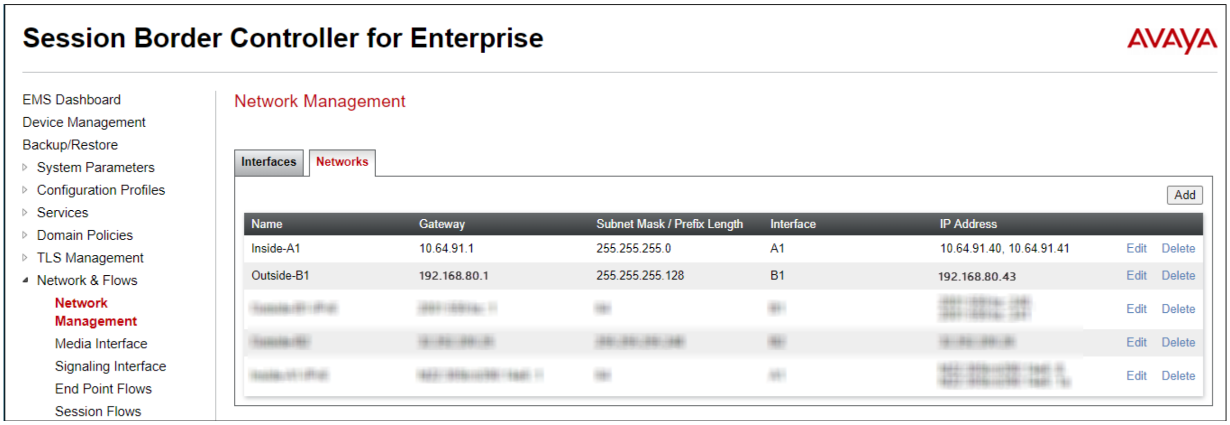
TLS Profile	
Profile Name	sbce8_70Client
Certificate	sbce8_70.pem
SNI	□ Enabled
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	□
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	☑ TLS 1.2 □ TLS 1.1 □ TLS 1.0
Ciphers	● Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

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 **B1**.

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

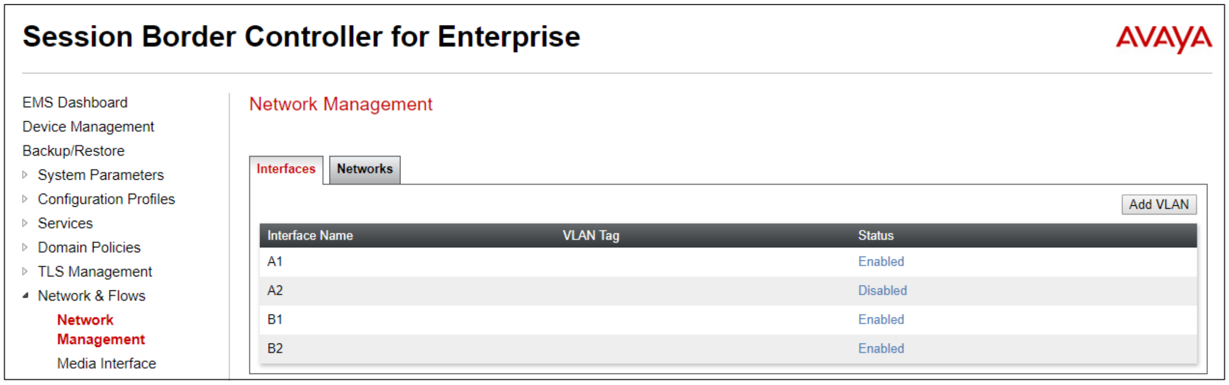
- **A1**: **10.64.91.41** – IP address configured for AT&T IPTF to IP Office.
- **B1: 192.168.80.43** – IP address configured for the AT&T IPTF service. This address is known to AT&T. See **Section 3**.



Network Management

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Inside-A1	10.64.91.1	255.255.255.0	A1	10.64.91.40, 10.64.91.41	Edit	Delete
Outside-B1	192.168.80.1	255.255.255.128	B1	192.168.80.43	Edit	Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Edit	Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Edit	Delete
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Edit	Delete

Verify that the interfaces are enabled on the **Interfaces** tab. The following screen shows interfaces **A1** and **B1** with status **Enabled**. To enable an interface, click the corresponding **Disabled** link under the Status column to change it to **Enabled**.



Network Management

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Enabled

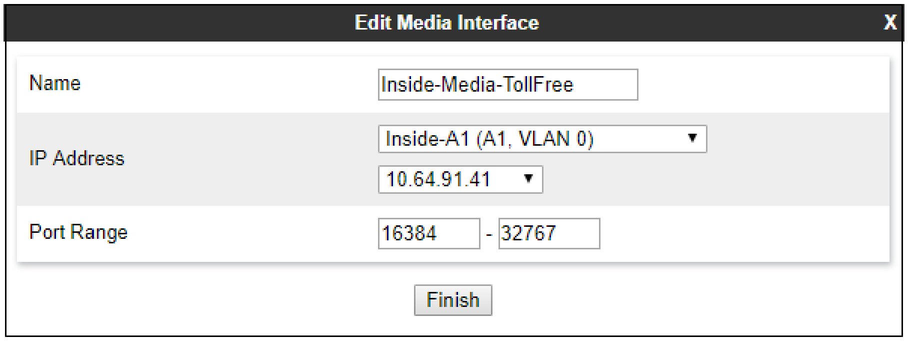
7.4. Media Interfaces

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**.

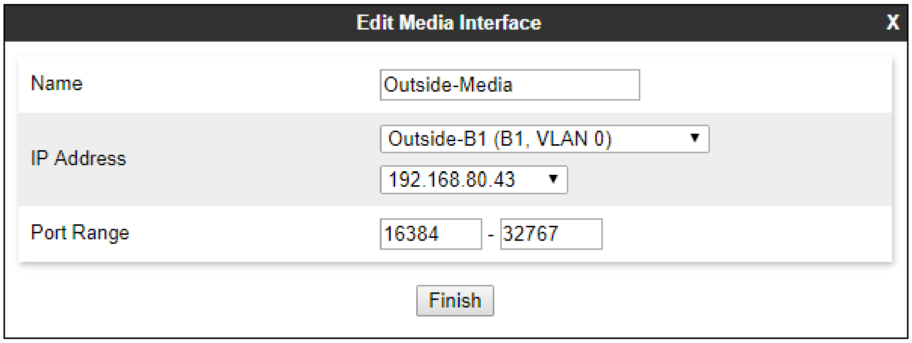
Some ports in the range required by AT&T were already allocated by the Avaya SBCE for internal use, by default. See **Section 7.14** for the steps required to reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T could be accommodated.

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



Name: Inside-Media-TollFree
IP Address: Inside-A1 (A1, VLAN 0) ▼
10.64.91.41 ▼
Port Range: 16384 - 32767

A second Media Interface towards the AT&T network was similarly created with the name **Outside-Media**, as shown below. The outside IP Address of the Avaya SBCE on the B1 interface was selected from the drop-down menu. The **Port Range** was configured with the values required by AT&T (**16384** – **32767**).

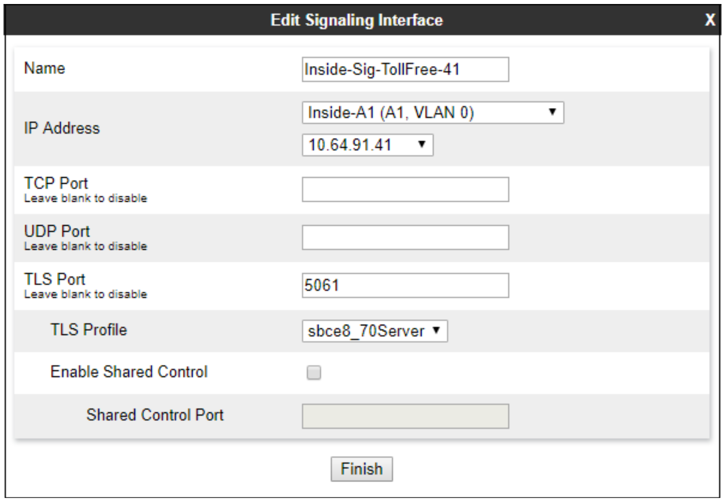


Name: Outside-Media
IP Address: Outside-B1 (B1, VLAN 0) ▼
192.168.80.43 ▼
Port Range: 16384 - 32767

7.5. Signaling Interfaces

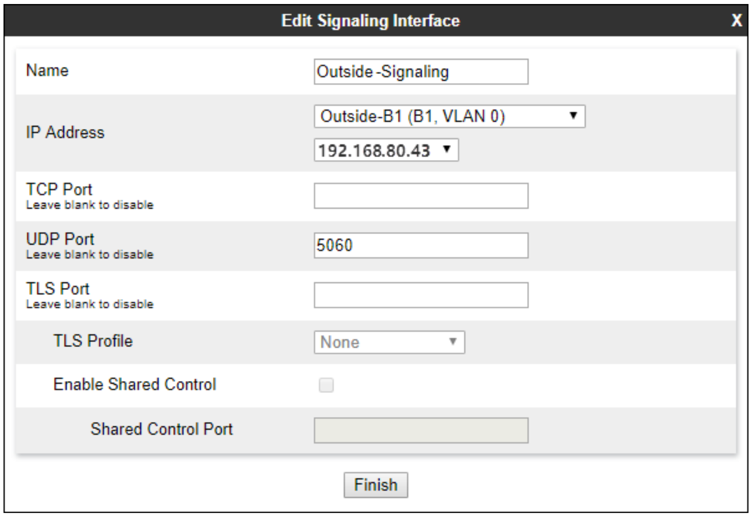
The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a signaling interface for the inside and outside IP interfaces.

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**.



Name	Inside-Sig-TollFree-41
IP Address	Inside-A1 (A1, VLAN 0) 10.64.91.41
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	5061
TLS Profile	sbce8_70Server
Enable Shared Control	☐
Shared Control Port	

A second Signaling Interface with the name **Outside-Signaling** was similarly created in the network direction. The B1 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**.



Name	Outside -Signaling
IP Address	Outside-B1 (B1, VLAN 0) 192.168.80.43
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	
TLS Profile	None
Enable Shared Control	☐
Shared Control Port	

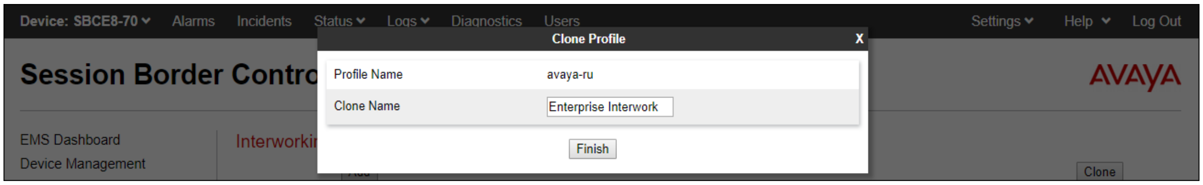
7.6. Server Interworking Profile

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

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

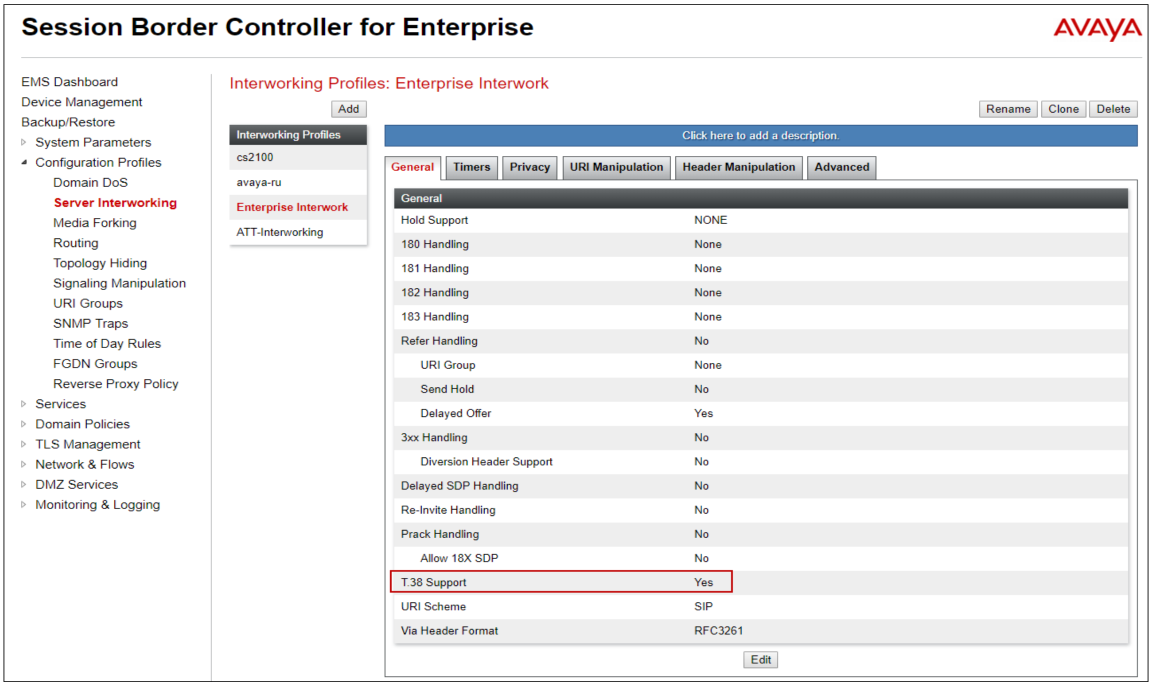
7.6.1. Server Interworking Profile – IP Office

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.



Profile Name	avaya-ru
Clone Name	Enterprise Interwork

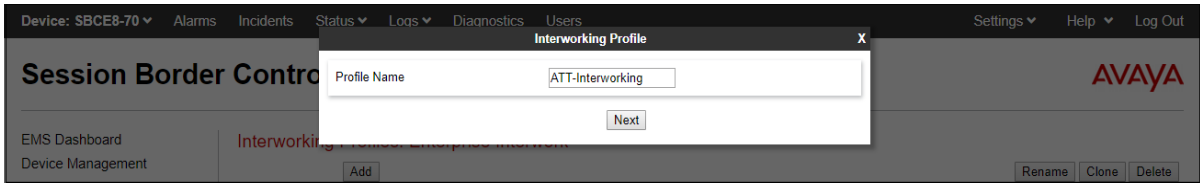
The following screen shows the **Enterprise Interwork** profile used in the sample configuration, with **T.38 Support** set to **Yes**. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish**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



General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

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**.

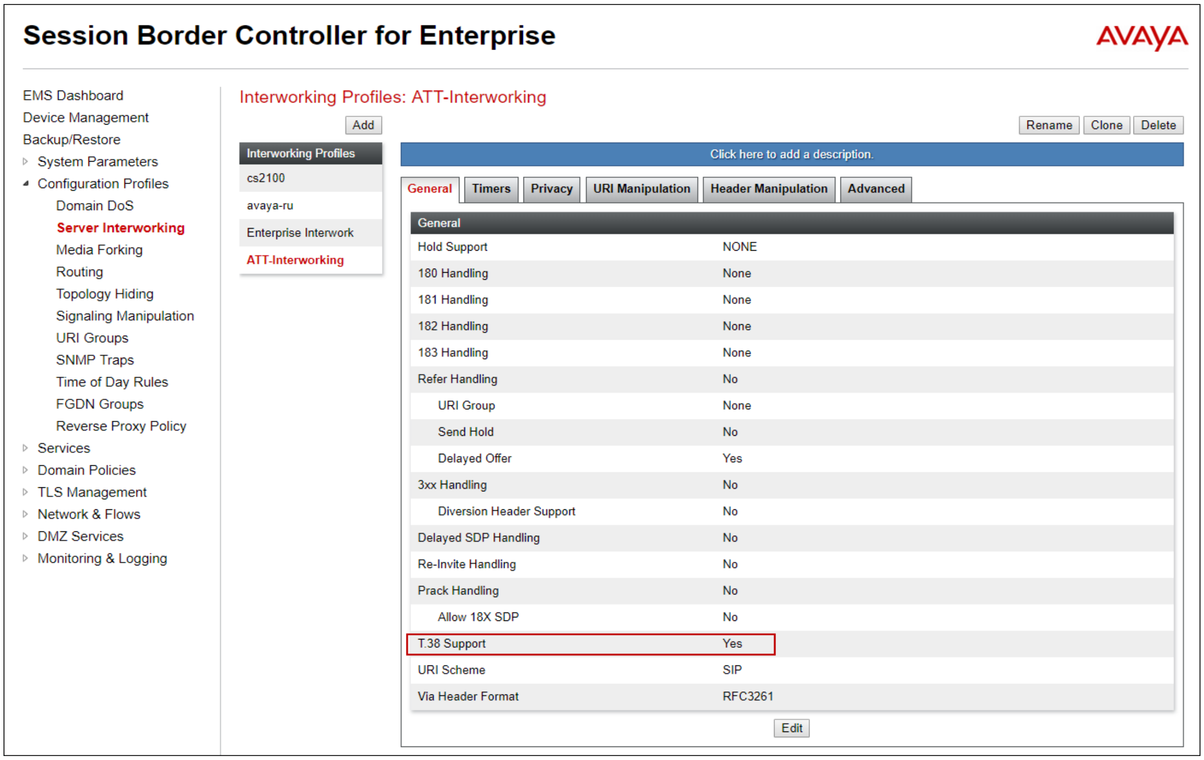


Interworking Profile

Profile Name	ATT-Interworking

Next

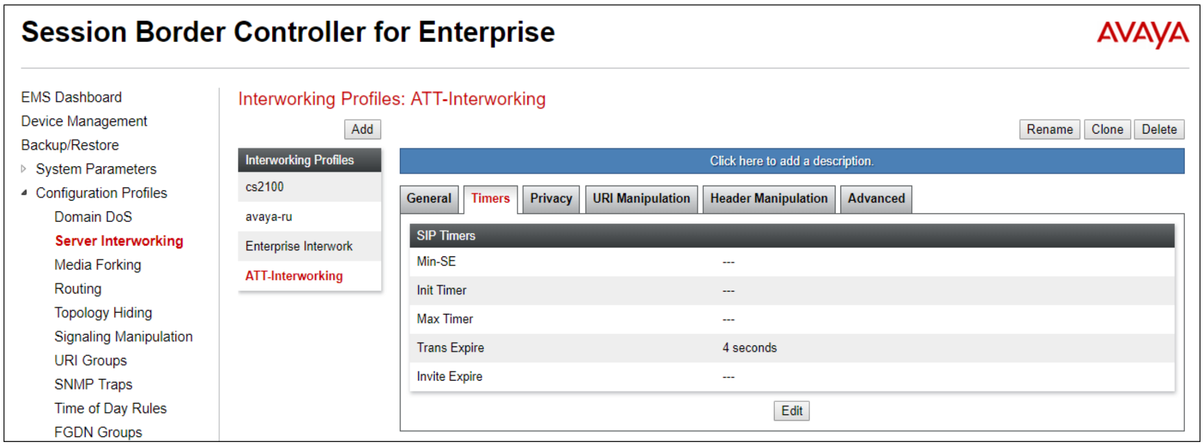
The following screens show the **ATT-Interworking** profile used in the sample configuration. On the **General** tab, default values are used with the exception of **T.38 Support** set to **Yes**.



Interworking Profiles: ATT-Interworking

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

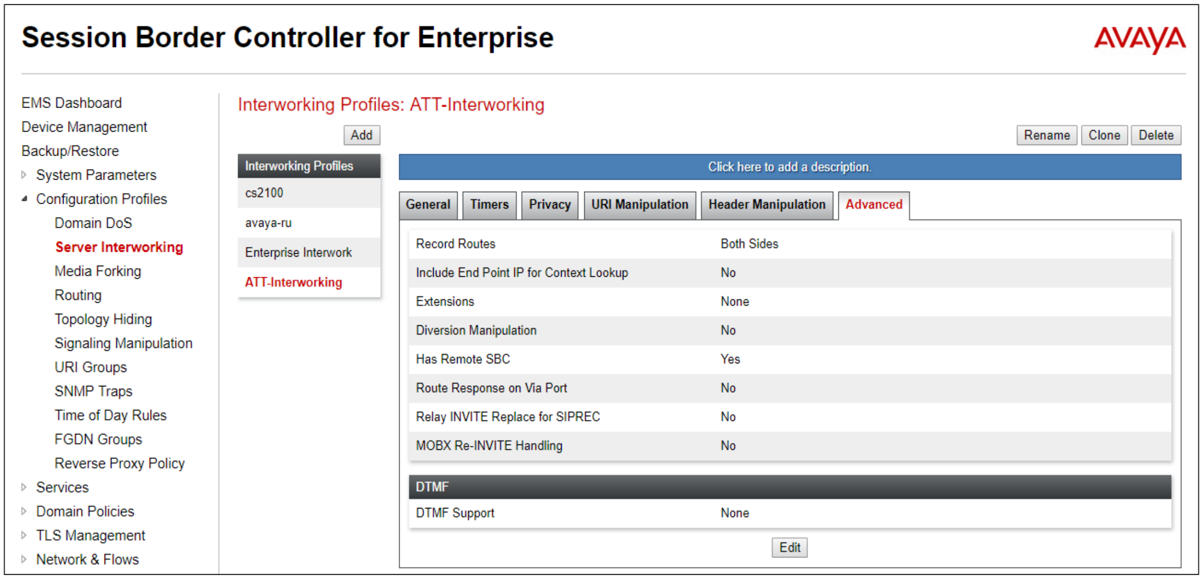
The **Timers** tab shows the values used for compliance testing for the **Trans Expire** field. The **Trans Expire** timer sets the allotted time the Avaya SBCE will try the first primary server before trying the secondary server, if one exists.



Interworking Profiles: ATT-Interworking

SIP Timers	
Min-SE	---
Init Timer	---
Max Timer	---
Trans Expire	4 seconds
Invite Expire	---

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.



Interworking Profiles: ATT-Interworking

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No

DTMF	
DTMF Support	None

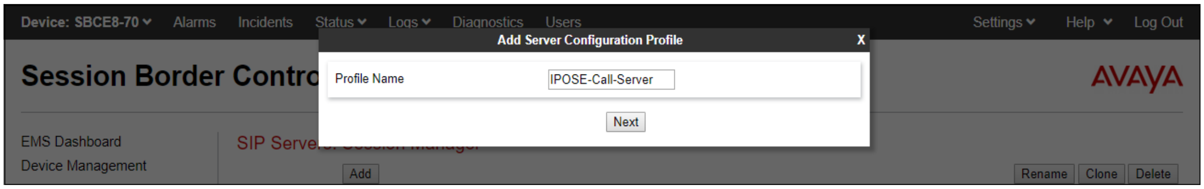
7.7. SIP Servers Profiles

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 Server Configurations profiles were created for the IP Office and the AT&T IPTF 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**.

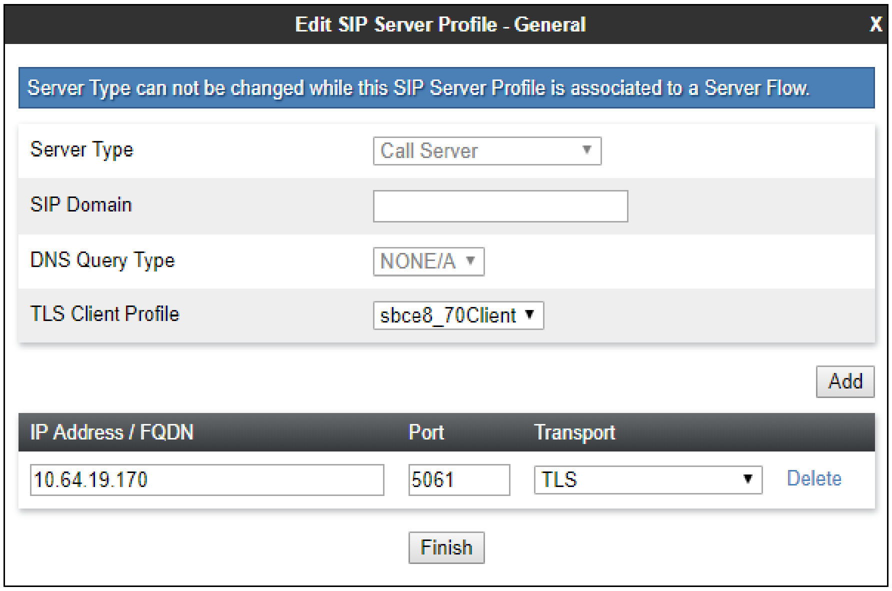


Add Server Configuration Profile

Profile Name	IPOSE-Call-Server

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**.



Edit SIP Server Profile - General

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

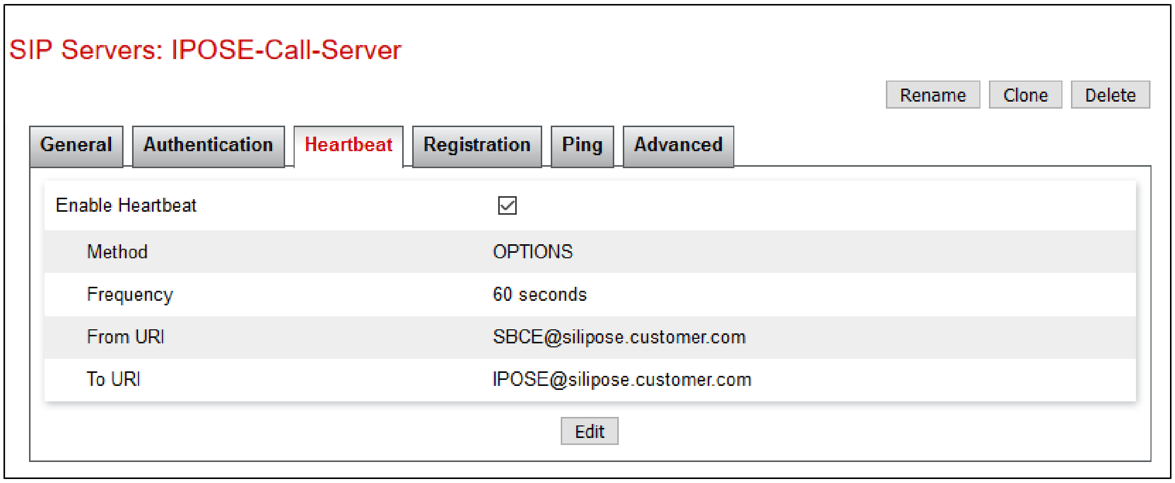
Server Type	Call Server
SIP Domain	
DNS Query Type	NONE/A
TLS Client Profile	sbce8_70Client

Add

IP Address / FQDN	Port	Transport	
10.64.19.170	5061	TLS	Delete

Finish

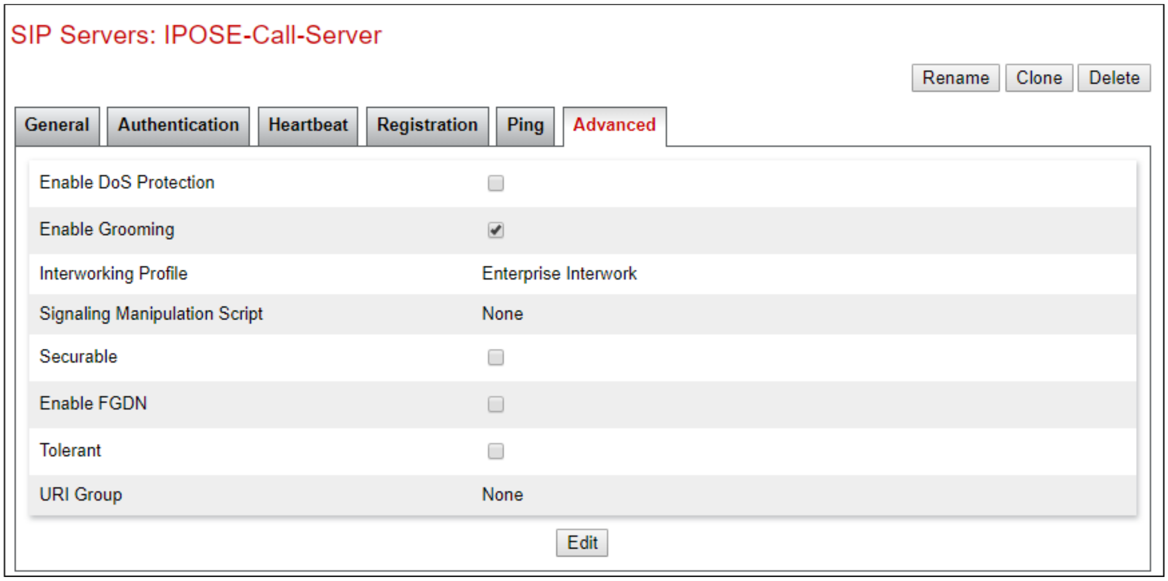
Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeat** tab. The Avaya SBCE can be optionally configured to source “heartbeats” in the form of PINGs or SIP OPTIONS towards IP Office. Check the **Enable Heartbeat** box and select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS towards IP Office.



SIP Servers: IPOSE-Call-Server

Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	SBCE@silipose.customer.com
To URI	IPOSE@silipose.customer.com

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.

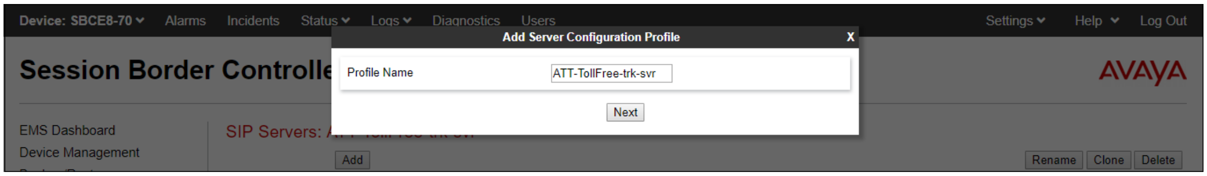


SIP Servers: IPOSE-Call-Server

Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	Enterprise Interwork
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
Tolerant	□
URI Group	None

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**.

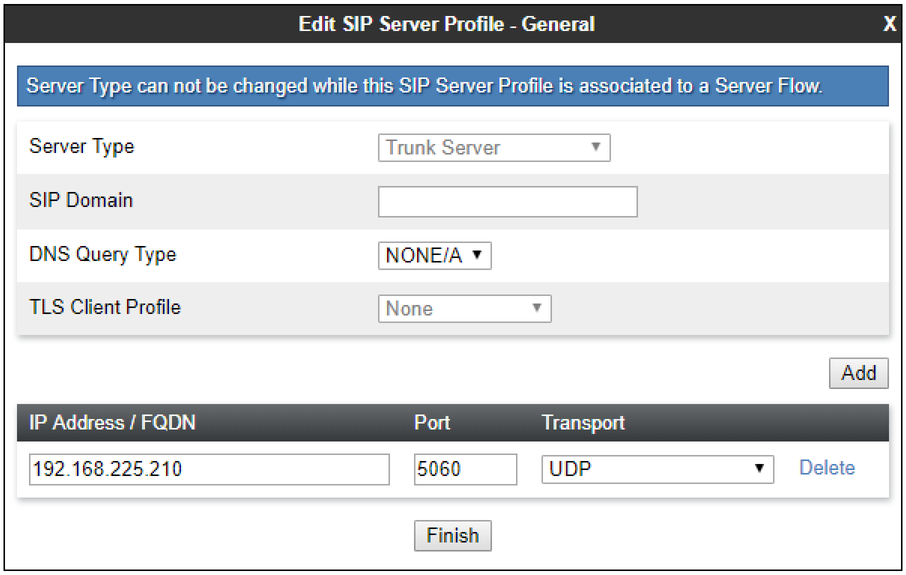


Add Server Configuration Profile

Profile Name: ATT-TollFree-trk-svr

Next

The following screens illustrate the SIP Server Profile **ATT-TollFree-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 element IP address is entered. This is **192.168.225.210**. 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**.



Edit SIP Server Profile - General

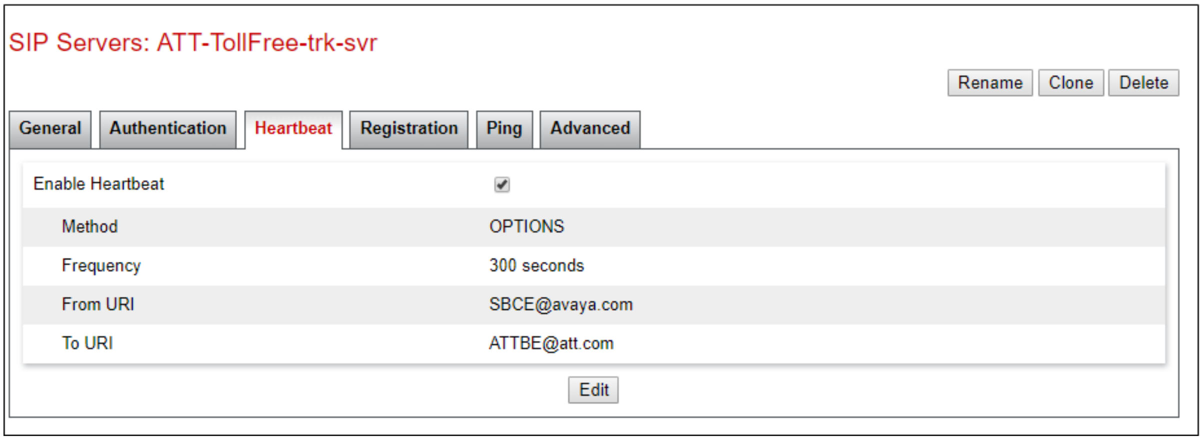
Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type	Trunk Server
SIP Domain	
DNS Query Type	NONE/A
TLS Client Profile	None

IP Address / FQDN	Port	Transport	
192.168.225.210	5060	UDP	Delete

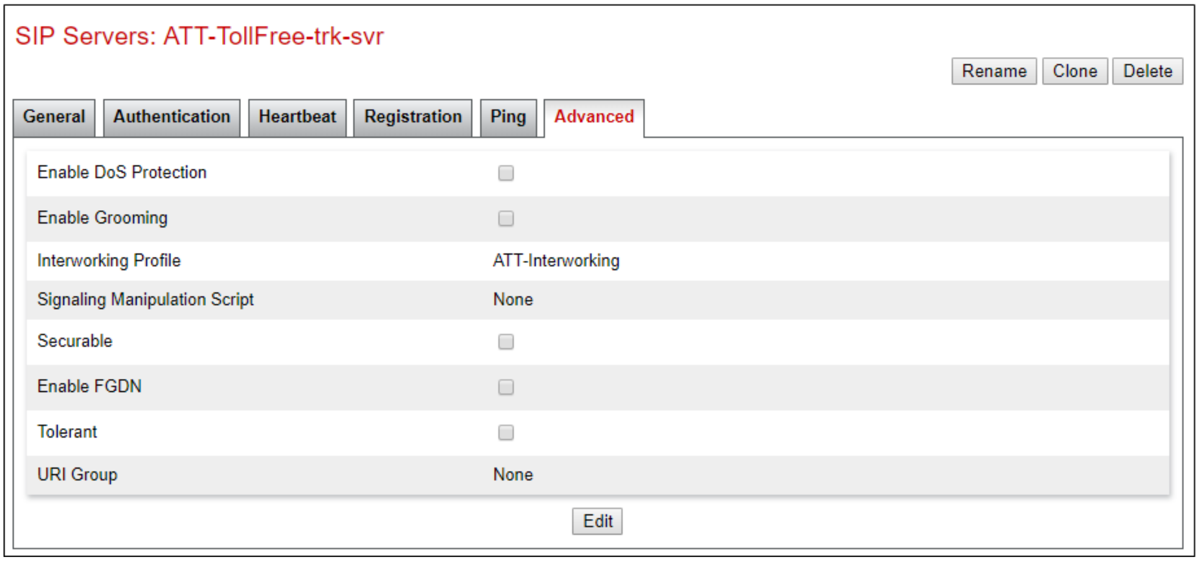
Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeats** tab. The Avaya SBCE can be configured to source "heartbeats" in the form of SIP OPTIONS towards AT&T. This configuration is optional. Independent of whether the Avaya SBCE is configured 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 Avaya SBCE will send SIP OPTIONS to AT&T. When AT&T responds, the Avaya 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.


SIP Servers: ATT-TollFree-trk-svr

Enable Heartbeat	☑
Method	OPTIONS
Frequency	300 seconds
From URI	SBCE@avaya.com
To URI	ATTBE@att.com

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.


SIP Servers: ATT-TollFree-trk-svr

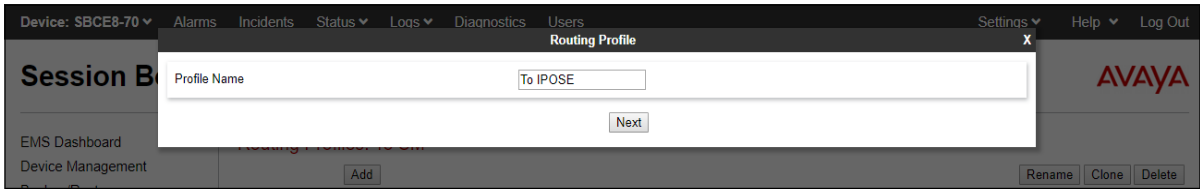
Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	ATT-Interworking
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
Tolerant	□
URI Group	None

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 IPTF 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.

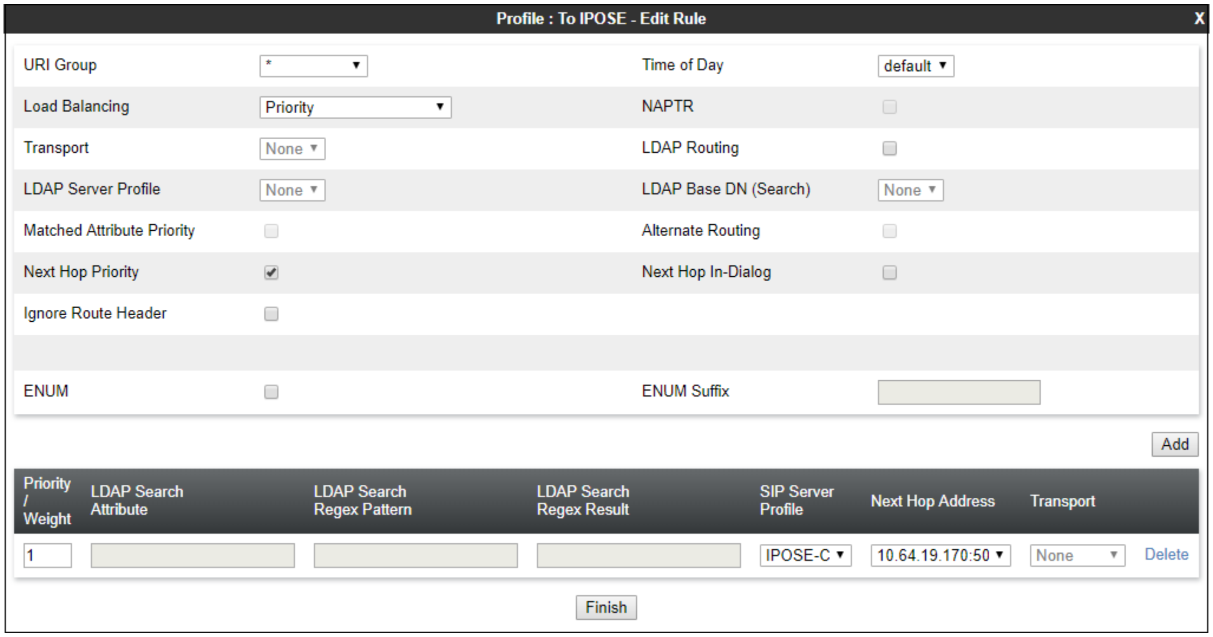


Routing Profile

Profile Name	To IPOSE

Next

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**.



Profile : To IPOSE - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	

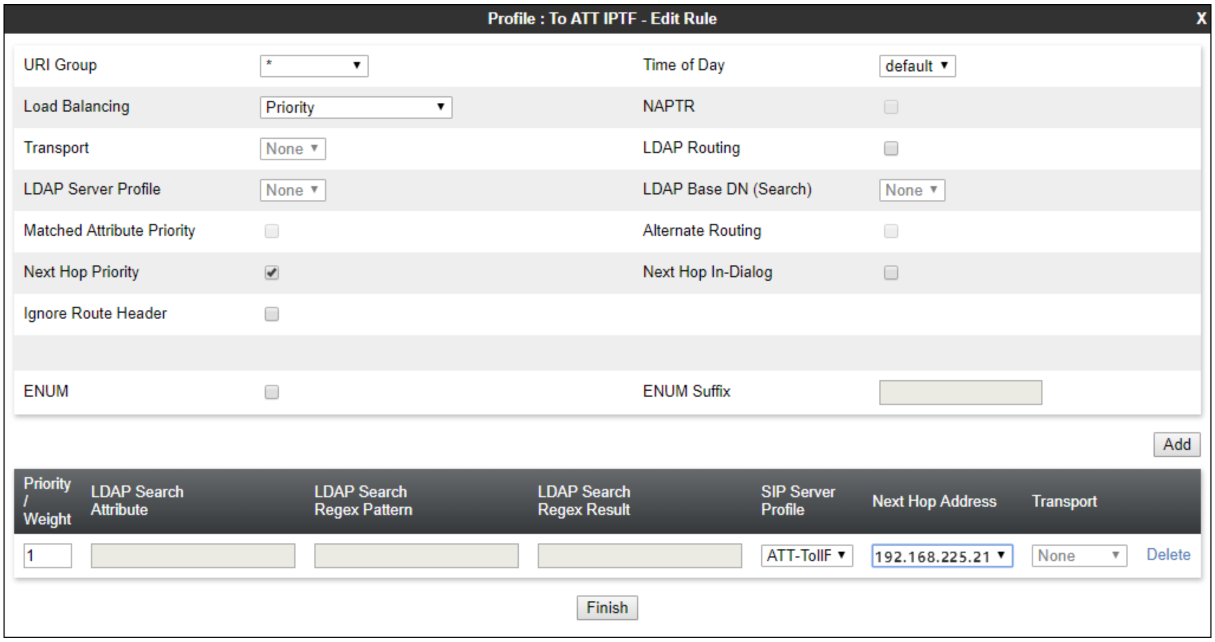
Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				IPOSE-C	10.64.19.170:50	None	Delete

Finish

7.8.2. Routing Profile – AT&T

Similarly, add a Routing Profile to AT&T. The following screen shows the Routing Profile **To ATT IPTF** created in the sample configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to **1**, and the AT&T **SIP Server Profile**, created in **Section 7.7.2**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the AT&T SIP Server Profile, and **Transport** becomes greyed out. Click **Finish**.



Profile : To ATT IPTF - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				ATT-TollF	192.168.225.21	None	Delete

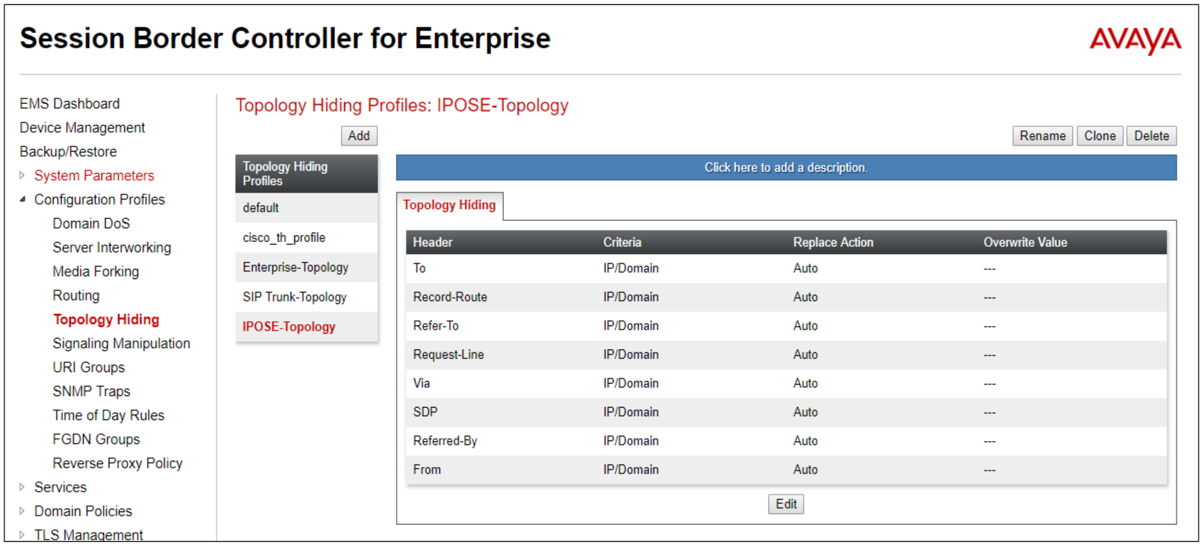
7.9. Topology Hiding Profile

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.

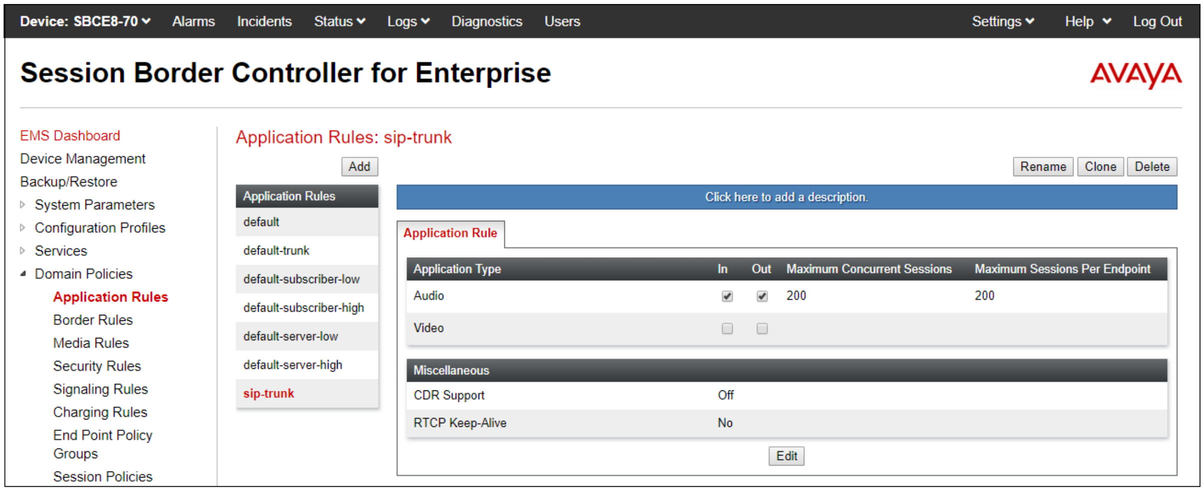


Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
From	IP/Domain	Auto	---

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**.



Application Rules: sip-trunk

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	200	200
Video	□	□		

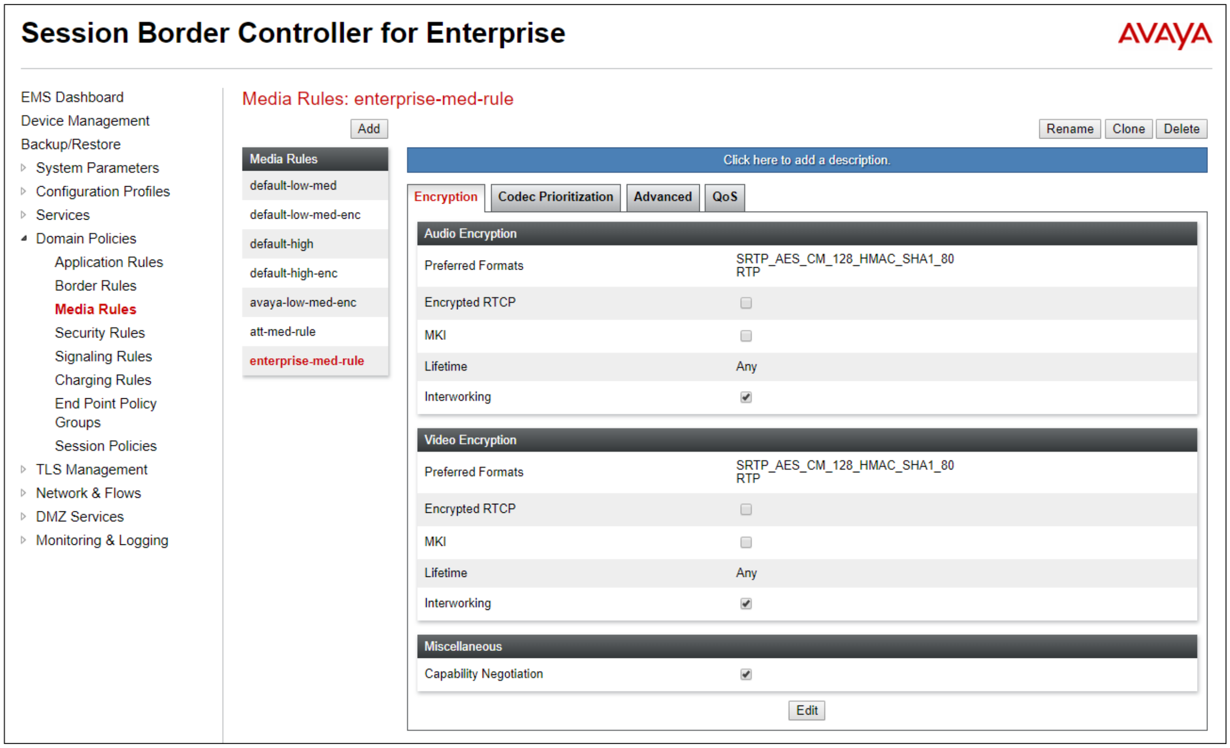
Miscellaneous	
CDR Support	Off
RTCP Keep-Alive	No

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.



Media Rules: enterprise-med-rule

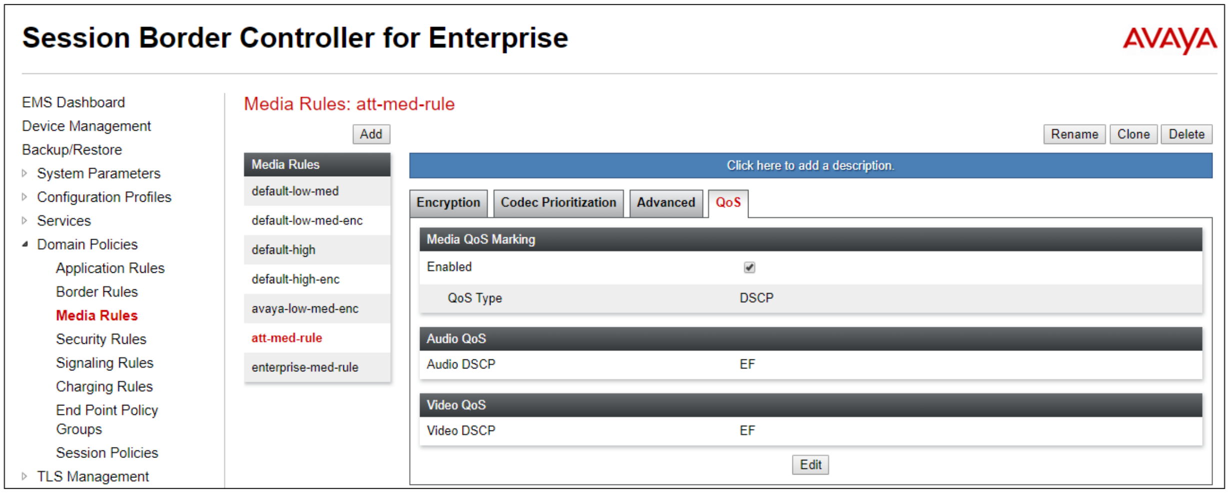
Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
Encrypted RTCP	☐
MKI	☐
Lifetime	Any
Interworking	☑

Video Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
Encrypted RTCP	☐
MKI	☐
Lifetime	Any
Interworking	☑

Miscellaneous	
Capability Negotiation	☑

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

The Media Rule named **att-med-rule** used in the sample configuration for AT&T IPTF is shown below, with the DSCP values **EF** for expedited forwarding (default value) for **Media QoS**.



Media Rules: att-med-rule

Media QoS Marking	
Enabled	☑
QoS Type	DSCP

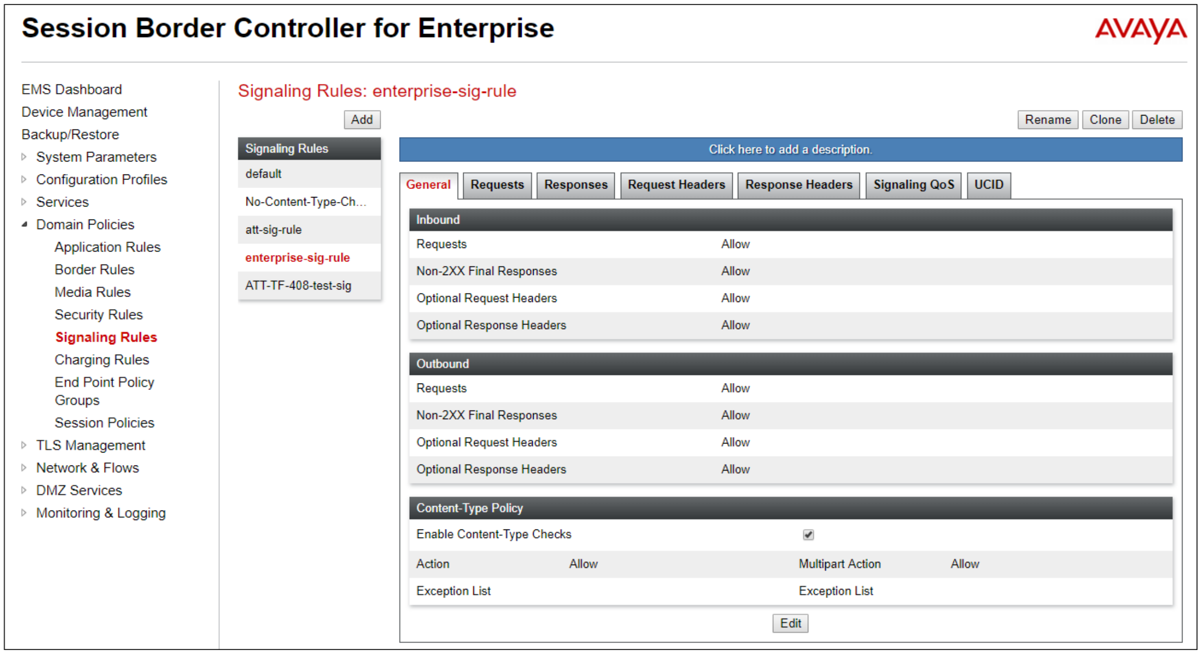
Audio QoS	
Audio DSCP	EF

Video QoS	
Video DSCP	EF

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** is unchanged from the default rule.



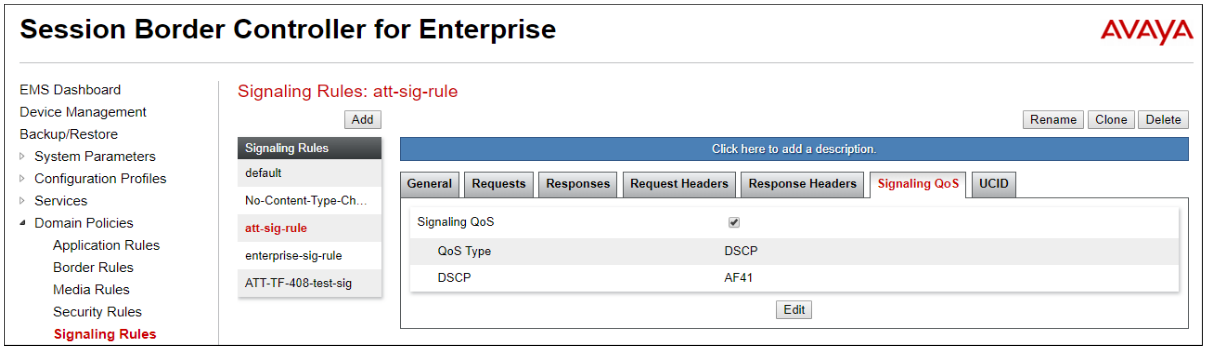
Signaling Rules: enterprise-sig-rule

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks	☑		
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

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**.



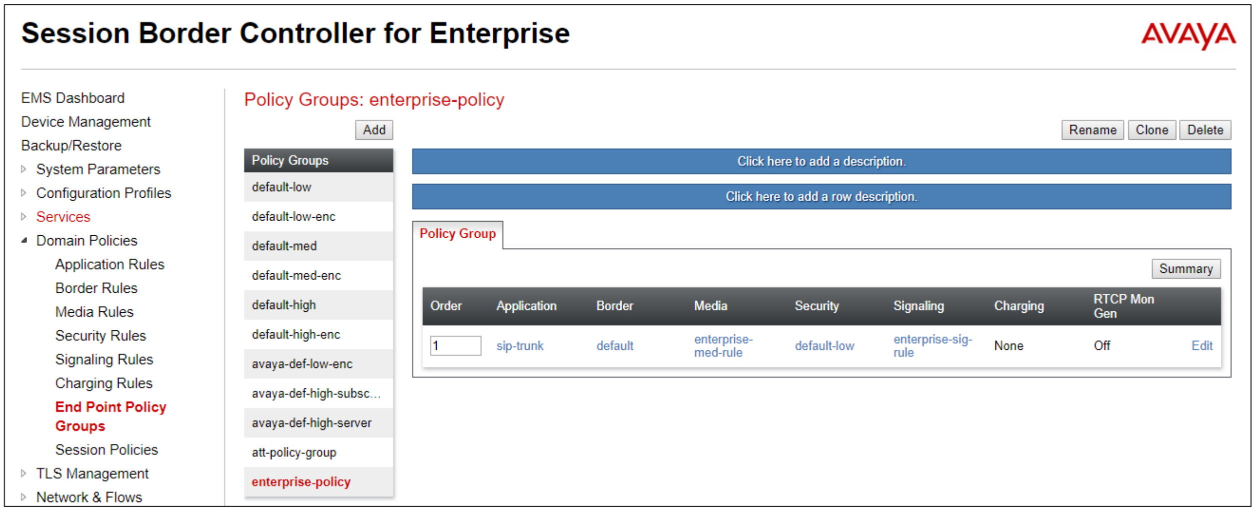
Signaling Rules: att-sig-rule

Signaling QoS	☑
QoS Type	DSCP
DSCP	AF41

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**.

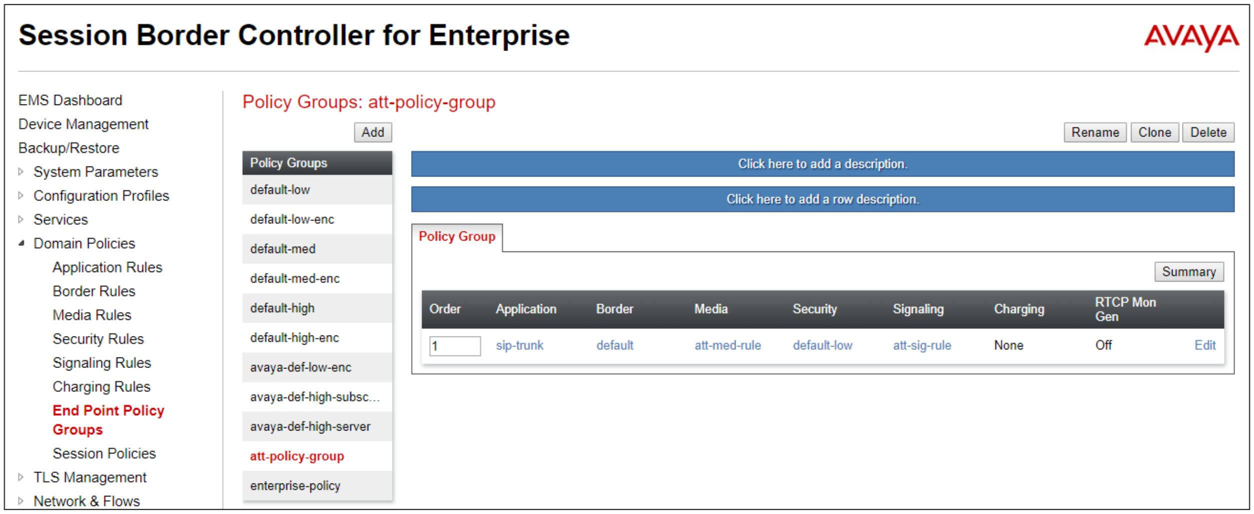
To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add** as shown below. The following screen shows the **enterprise policy** created for IP Office. The details of the non-default rules chosen are shown in previous sections.



Policy Groups: enterprise-policy

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	sip-trunk	default	enterprise-med-rule	default-low	enterprise-sig-rule	None	Off	Edit

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.



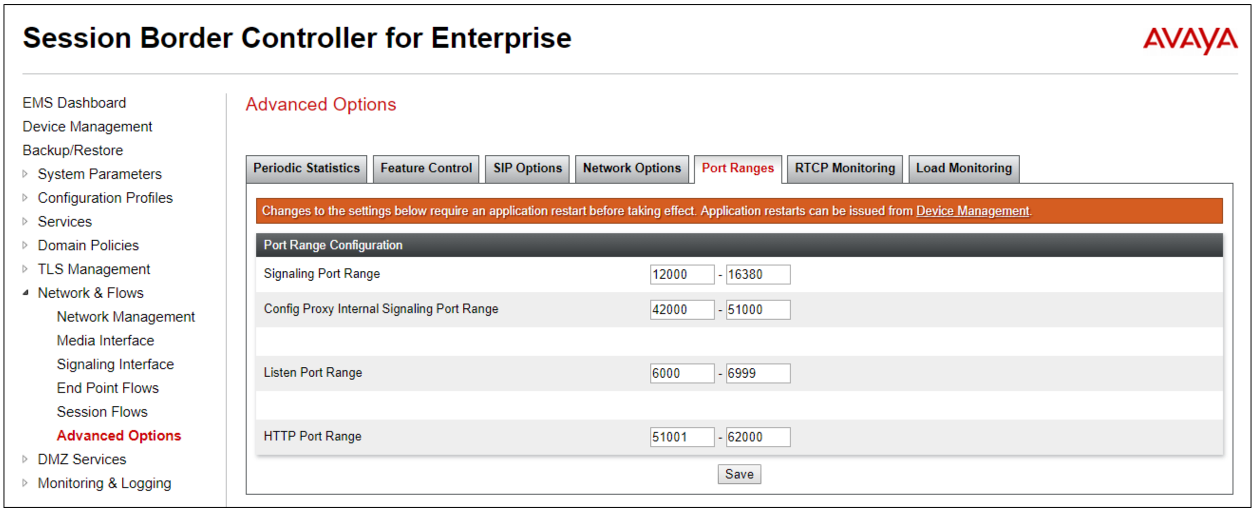
Policy Groups: att-policy-group

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	sip-trunk	default	att-med-rule	default-low	att-sig-rule	None	Off	Edit

7.14. Advanced Options

In **Section 7.4**, the media UDP port ranges required by AT&T are configured (**16384** – **32767**). However, by default part of this range is already allocated by the Avaya SBCE for internal use (22000 - 31000). The following steps reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T can be defined as shown 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**).



Changes to the settings below require an application restart before taking effect. Application restarts can be issued from Device Management.

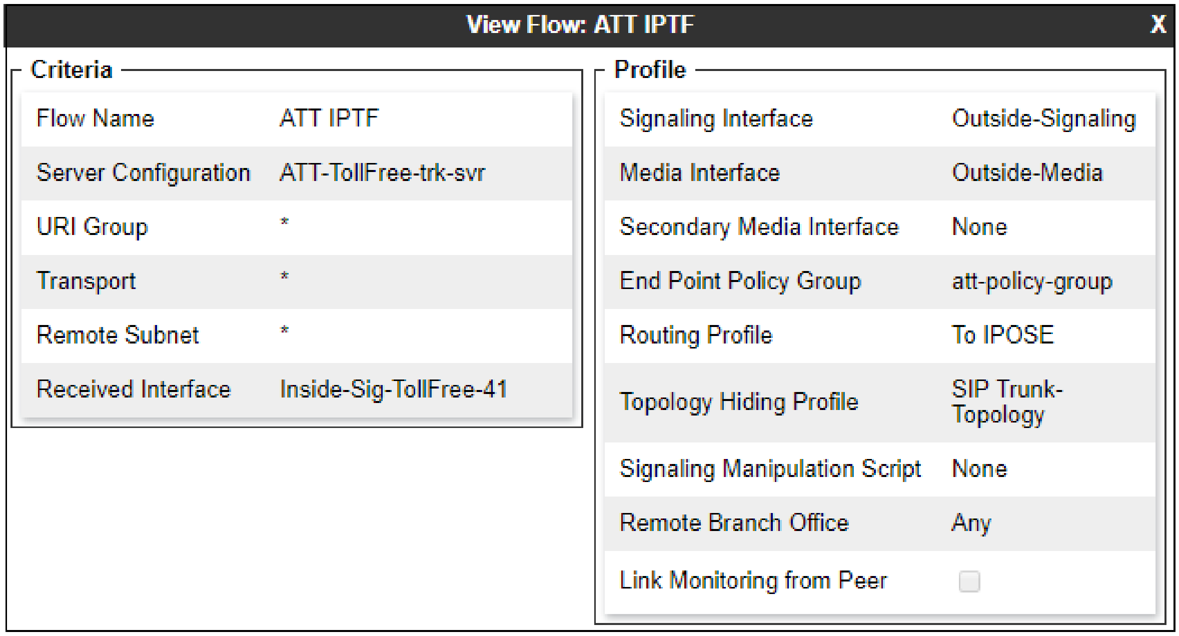
Port Range Configuration		
Signaling Port Range	12000	16380
Config Proxy Internal Signaling Port Range	42000	51000
Listen Port Range	6000	6999
HTTP Port Range	51001	62000

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 IPTF service. To create a Server Flow, navigate to **Networks & Flows → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown).

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



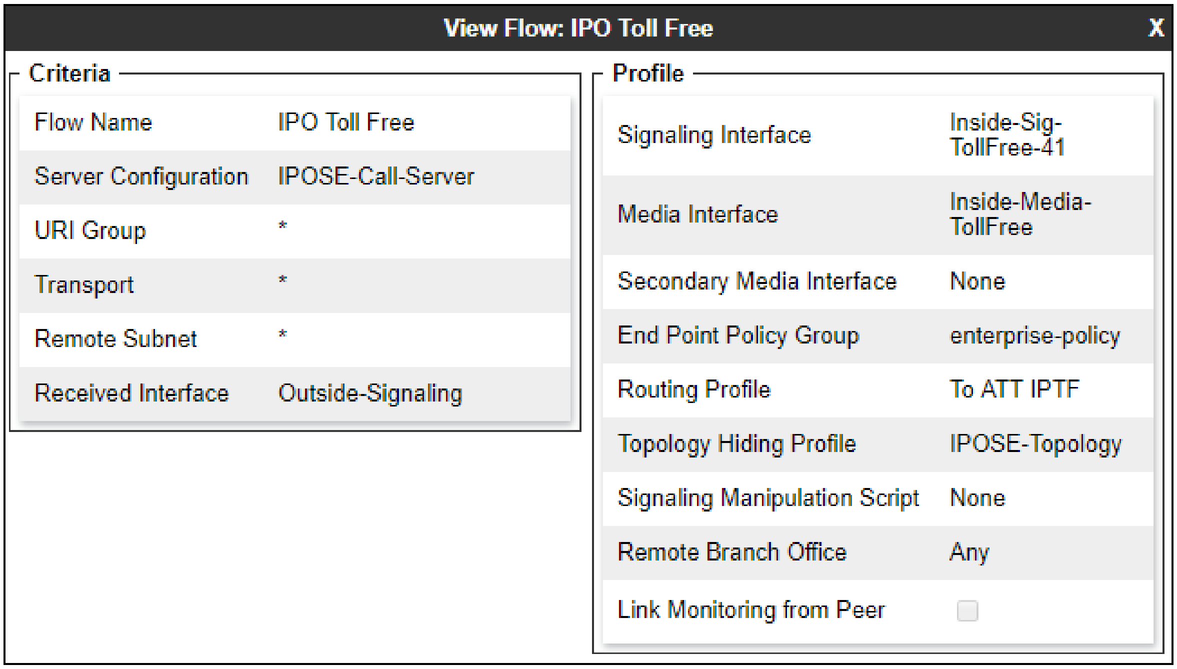
Criteria

Flow Name	ATT IPTF
Server Configuration	ATT-TollFree-trk-svr
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside-Sig-TollFree-41

Profile

Signaling Interface	Outside-Signaling
Media Interface	Outside-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	□

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



View Flow: IPO Toll Free

Criteria

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

Profile

Signaling Interface	Inside-Sig-TollFree-41
Media Interface	Inside-Media-TollFree
Secondary Media Interface	None
End Point Policy Group	enterprise-policy
Routing Profile	To ATT IPTF
Topology Hiding Profile	IPOSE-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□

8. AT&T IP Toll Free Service Configuration

AT&T provides the IPTF service border element IP address, the access DID numbers, and the associated DNIS digits used in the reference configuration. In addition, the AT&T IPTF features, and their associated access numbers, are also assigned by AT&T. AT&T requires that the Avaya SBCE public (B1) IP address be provided to the IPTF service, as part of the provisioning process. For more information, consult reference **[12]**.

9. Verification Steps

The following procedures may be used to verify the Avaya IP Office Release 11.1 and Avaya SBCE Release 8.1 with the AT&T IPTF service configuration.

9.1. AT&T IP Toll Free Service

The following scenarios may be executed to verify functionality with the AT&T IPTF service:

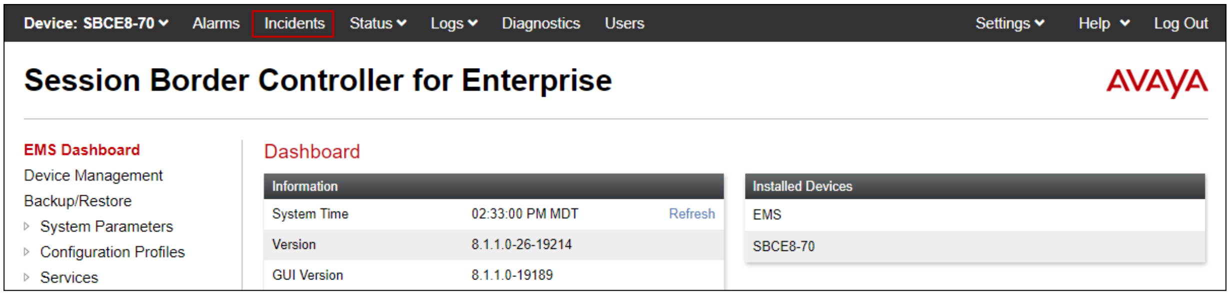
- Place inbound calls, answer the calls, and verify that two-way talk path exists. Verify that the calls remain stable for several minutes and disconnects properly.
- Incoming calls using the G.729A and G.711 ULAW codecs.
- Verify basic call functions such as hold, transfer, and conference.
- Place an inbound call to a telephone, but do not answer the call. Verify that the call covers to voicemail (e.g., Voicemail Pro). Retrieve the message either locally or from PSTN.
- Using the appropriate IPTF access numbers and codes, verify the "Legacy Transfer Connect" DTMF initiated features.
- Inbound fax using T.38 or G.711. See **Section 2.2** for limitations.
- SIP OPTIONS monitoring of the health of the SIP trunk.

9.2. Avaya SBCE

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

9.2.1. Incidents

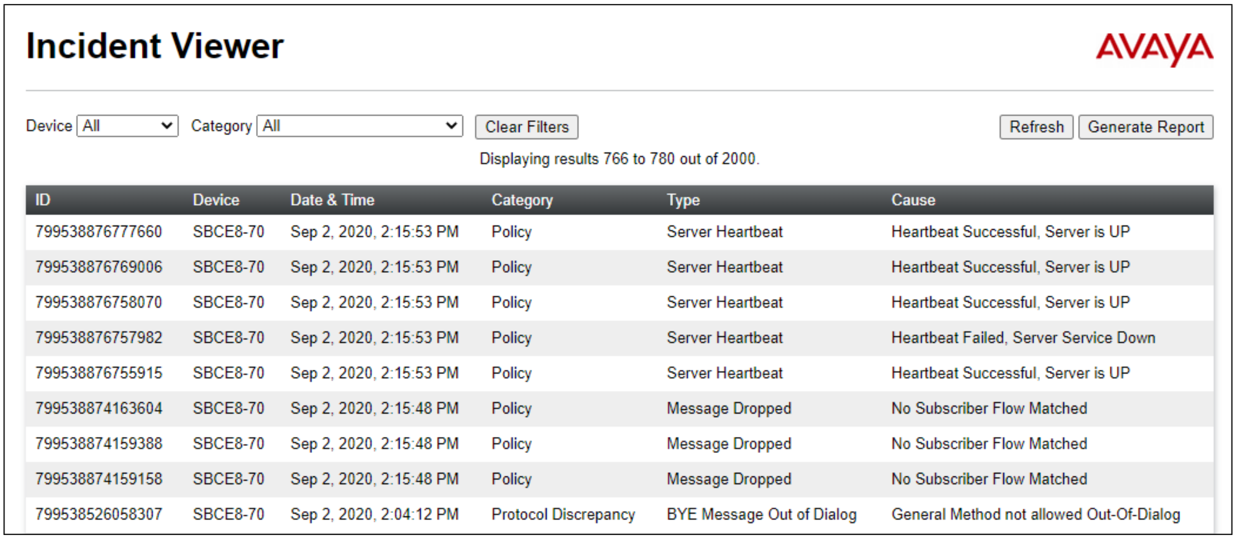
The Incident Viewer can be accessed from the Avaya SBCE top navigation menu as highlighted in the screenshot below.



Information	
System Time	02:33:00 PM MDT
Version	8.1.1.0-26-19214
GUI Version	8.1.1.0-19189

Installed Devices
EMS
SBCE8-70

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

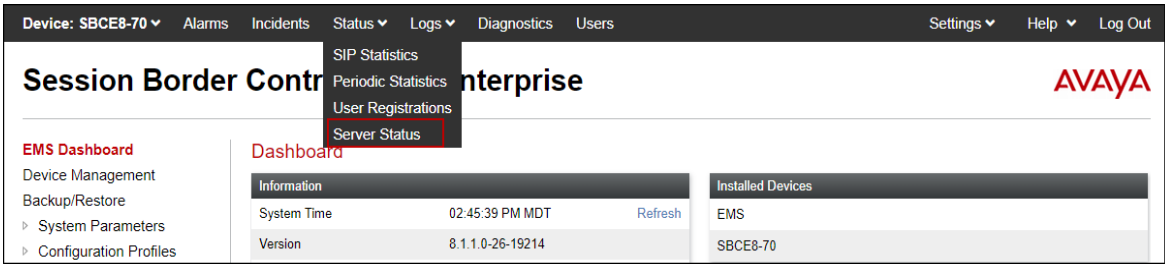


Displaying results 766 to 780 out of 2000.

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

9.2.2. Server Status

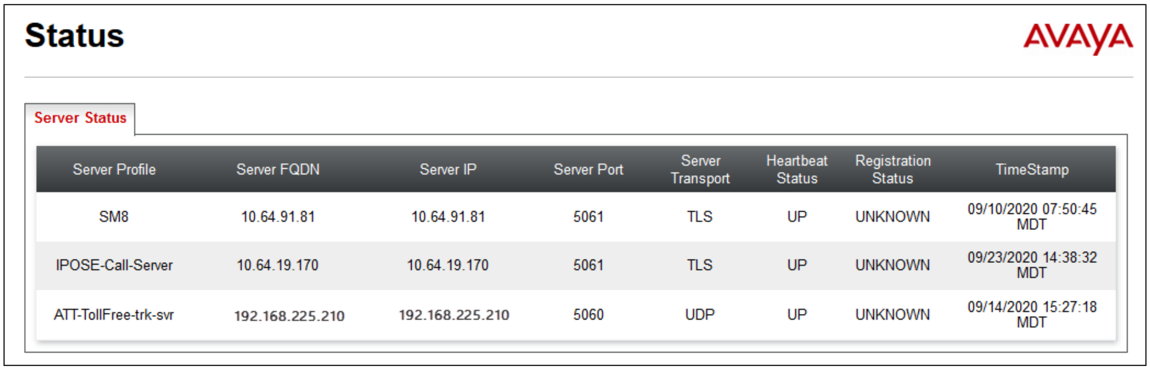
The Server Status screen can be accessed from the Avaya SBCE top navigation menu by selecting the Status menu, and then Server Status.



Information		
System Time	02:45:39 PM MDT	Refresh
Version	8.1.1.0-26-19214	

Installed Devices
EMS
SBCE8-70

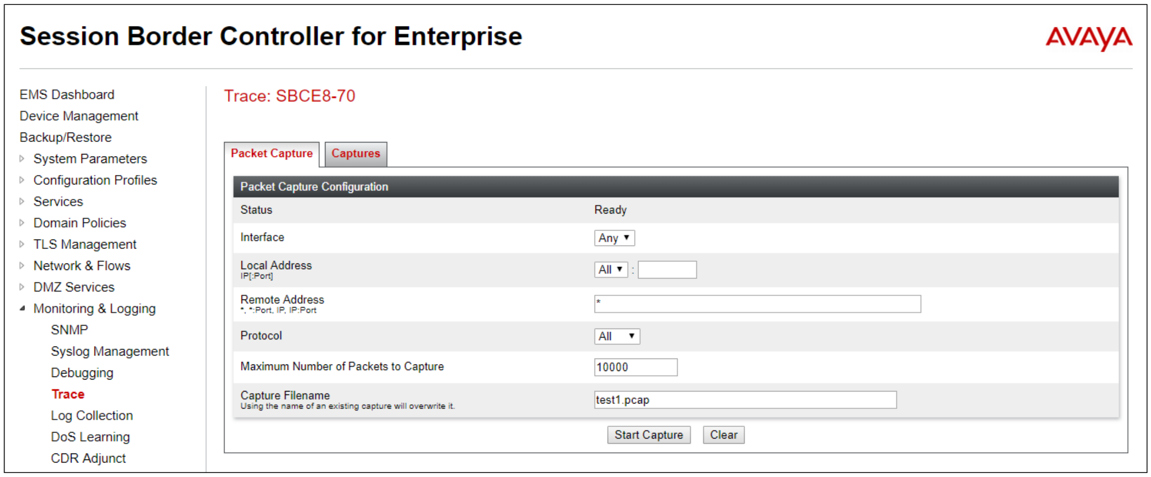
Server Status provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Configuration profile, as configured in **Section 7.7**.



Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
SM8	10.64.91.81	10.64.91.81	5061	TLS	UP	UNKNOWN	09/10/2020 07:50:45 MDT
IPOSE-Call-Server	10.64.19.170	10.64.19.170	5061	TLS	UP	UNKNOWN	09/23/2020 14:38:32 MDT
ATT-TollFree-trk-svr	192.168.225.210	192.168.225.210	5060	UDP	UP	UNKNOWN	09/14/2020 15:27:18 MDT

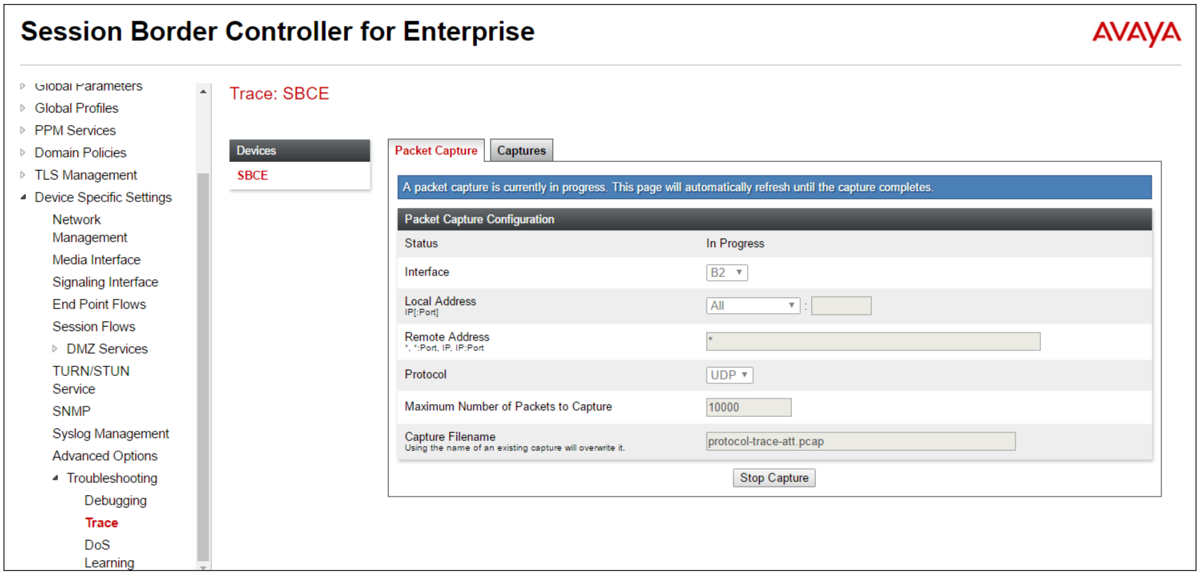
9.2.3. Tracing

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



Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename Using the name of an existing capture will overwrite it.	test1.pcap

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

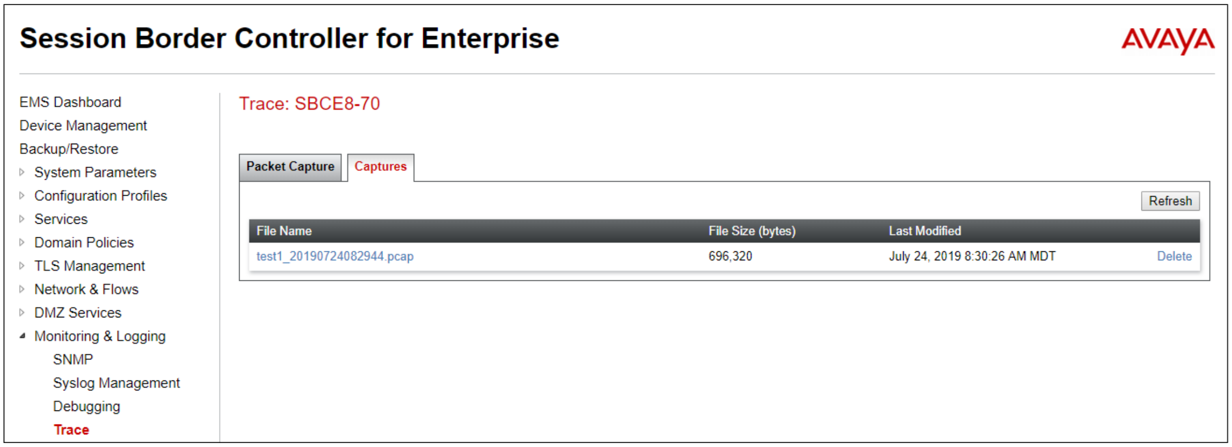


Trace: SBCE

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration	
Status	In Progress
Interface	B2
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	UDP
Maximum Number of Packets to Capture	10000
Capture Filename Using the name of an existing capture will overwrite it.	protocol-trace-att.pcap

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



Trace: SBCE8-70

File Name	File Size (bytes)	Last Modified	
test1_20190724082944.pcap	696,320	July 24, 2019 8:30:26 AM MDT	Delete

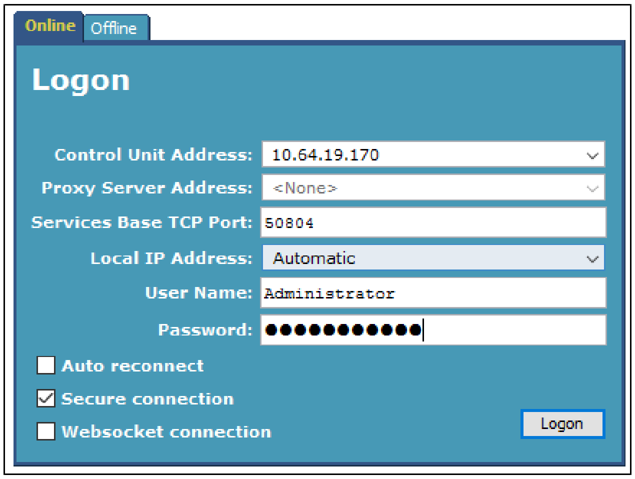
The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like Wireshark.

9.3. Avaya IP Office

The following items may be used to analyze/troubleshoot Avaya IP Office operations.

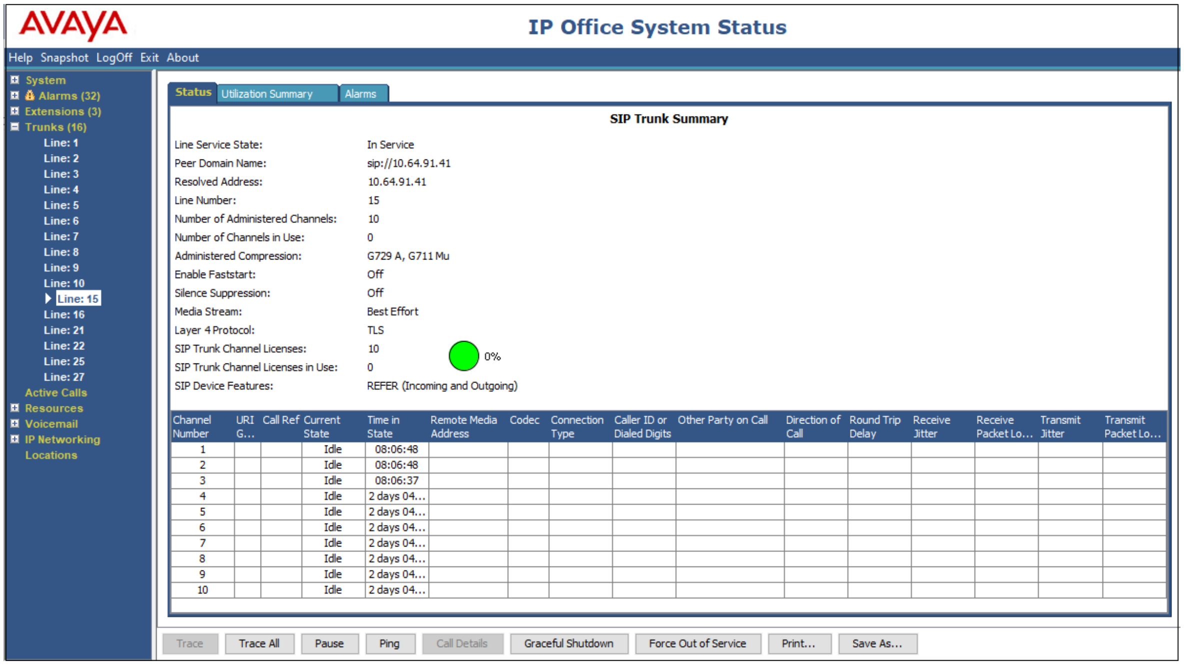
9.3.1. System Status Application

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



Control Unit Address: 10.64.19.170
Proxy Server Address: <None>
Services Base TCP Port: 50804
Local IP Address: Automatic
User Name: Administrator
Password: ●●●●●●●●●●●
□ Auto reconnect
☑ Secure connection
□ Websocket connection

Select the SIP line from the left pane (**Line 15** 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).



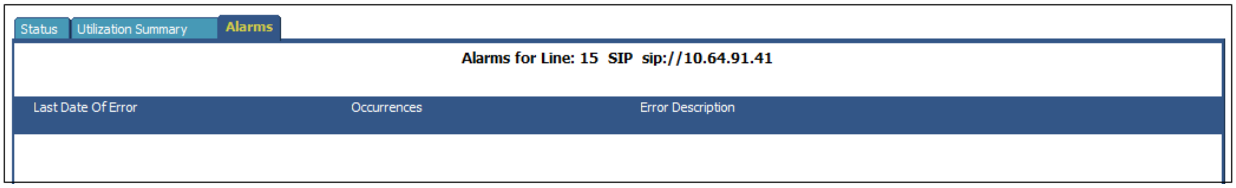
SIP Trunk Summary

Line Service State: In Service
Peer Domain Name: sip://10.64.91.41
Resolved Address: 10.64.91.41
Line Number: 15
Number of Administered Channels: 10
Number of Channels in Use: 0
Administered Compression: G729 A, G711 Mu
Enable Faststart: Off
Silence Suppression: Off
Media Stream: Best Effort
Layer 4 Protocol: TLS
SIP Trunk Channel Licenses: 10 ● 0%
SIP Trunk Channel Licenses in Use: 0
SIP Device Features: REFER (Incoming and Outgoing)

Channel Number	URI G...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Lo...	Transmit Jitter	Transmit Packet Lo...
1			Idle	08:06:48											
2			Idle	08:06:48											
3			Idle	08:06:37											
4			Idle	2 days 04...											
5			Idle	2 days 04...											
6			Idle	2 days 04...											
7			Idle	2 days 04...											
8			Idle	2 days 04...											
9			Idle	2 days 04...											
10			Idle	2 days 04...											

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

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

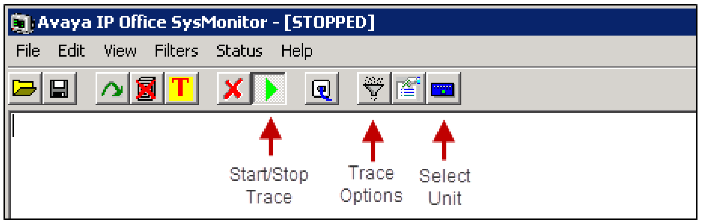


Alarms for Line: 15 SIP sip://10.64.91.41

Last Date Of Error	Occurrences	Error Description

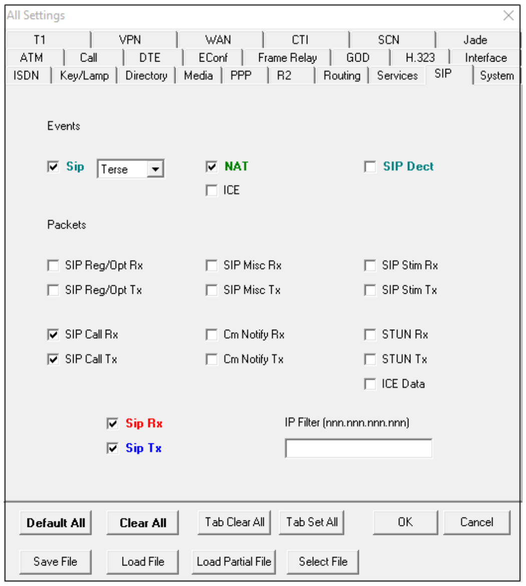
9.3.2. System Monitor Application

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.



Start/Stop Trace
Trace Options
Select Unit

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.



Events

☑ Sip Terse
☑ NAT
□ ICE
□ SIP Dect

Packets

□ SIP Reg/Opt Rx
□ SIP Reg/Opt Tx
☑ SIP Call Rx
☑ SIP Call Tx
□ SIP Misc Rx
□ SIP Misc Tx
□ Cm Notify Rx
□ Cm Notify Tx
□ SIP Stim Rx
□ SIP Stim Tx
□ STUN Rx
□ STUN Tx
□ ICE Data

☑ Sip Rx
☑ Sip Tx

IP Filter (nnn.nnn.nnn.nnn)

10. Conclusion

As illustrated in these Application Notes, Avaya IP Office Release 11.1 and the Avaya Session Border Controller for Enterprise Release 8.1 can be configured to interoperate successfully with the AT&T IP Toll Free service using **AVPN** or **ADI/PNT** transport connections, utilizing service features listed in **Section 2.1**, and 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

Avaya:

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 11.0, 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*, September 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] *IP Office™ Platform 11.1, Administering Avaya IP Office Platform Voicemail Pro*, September 2020.
[7] *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac and Windows*, August 2020
[8] *IP Office™ Platform 11.1, IP Office SIP Phones with ASBCE, Issue 04c*, July 2020
[9] *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform, Release 8.1.x*, August 2020.
[10] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, August 2020.
[11] *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 IPTF Service:

[12] AT&T IP Toll Free Service description -
https://www.business.att.com/products/ip-toll-free.html

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.