Avaya Solution & Interoperability Test Lab

Application Notes for Avaya IP Office and Avaya Session Border Controller for Enterprise in High Availability Configuration to support BT Wholesale Hosted SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 11.1 and Avaya Session Border Controller for Enterprise Release 8.1 in a High Availability configuration, to support BT Wholesale Hosted SIP Trunking Service.

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

The test was performed to verify SIP trunk registration and functionality during different failover scenarios of the Avaya Session Border Controller for Enterprise. Calls were placed to and from the public switched telephone network (PSTN) with various Avaya endpoints.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

©2022 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction ... 4
2. General Test Approach and Test Results ... 5
   2.1. Interoperability Compliance Testing ... 6
   2.2. Test Results ... 7
   2.3. Support ... 7
3. Reference Configuration ... 8
4. Equipment and Software Validated ... 11
5. Avaya IP Office Primary Server Configuration ... 12
   5.1. Licensing ... 13
   5.2. TLS Management ... 14
   5.3. System Settings ... 15
      5.3.1. LAN1 Settings ... 15
      5.3.2. Voicemail Settings ... 18
      5.3.3. System Telephony Settings ... 19
      5.3.4. System VoIP Settings ... 20
   5.4. IP Route ... 22
   5.5. SIP Line ... 23
      5.5.1. Creating a SIP Trunk from an XML Template ... 24
      5.5.2. SIP Line – SIP Line Tab ... 25
      5.5.3. SIP Line - Transport Tab ... 26
      5.5.4. SIP Line – Call Details Tab ... 26
      5.5.5. SIP Line - VoIP Tab ... 28
      5.5.6. SIP Line – SIP Advanced Tab ... 29
   5.6. IP Office Line ... 30
   5.7. Incoming Call Routes ... 31
   5.8. Outbound Call Routing ... 32
      5.8.1. Short Codes ... 32
      5.8.2. ARS Route ... 33
   5.9. Users ... 34
   5.10. Save Configuration ... 35
6. Avaya IP Office Expansion Configuration ... 36
   6.1. Expansion System - Physical Hardware ... 36
   6.2. Expansion System - LAN Settings ... 37
   6.3. Expansion System - IP Route ... 37
   6.4. Expansion System - IP Office Line ... 38
   6.5. Expansion System - Short Codes ... 39
   6.6. Expansion System - Automatic Route Selection – ARS ... 39
   6.7. Save IP Office Expansion System Configuration ... 40
7. Configure Avaya Session Border Controller for Enterprise ... 41
   8.1. Add Avaya SBCE devices to EMS ... 42
   8.2. Install Avaya SBCE ... 43
   8.3. TLS Management ... 46
      8.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise ... 46
      8.3.2. Server Profiles ... 47

©2022 Avaya Inc. All Rights Reserved.

8.3.3. Client Profiles 48
8.4. Network Management 49
8.5. Media Interfaces 50
8.6. Signaling Interfaces 51
8.7. Server Interworking Profile 52
8.7.1. Server Interworking Profile – IP Office 52
8.7.2. Server Interworking Profile – Service Provider 53
8.8. SIP Server Profiles 55
8.8.1. SIP Server Profile – IP Office 55
8.8.2. SIP Server Profile – Service Provider 57
8.9. Routing Profiles 60
8.9.1. Routing Profile – IP Office 60
8.9.2. Routing Profile – Service Provider 61
8.10. Topology Hiding Profile 62
8.10.1. Topology Hiding – IP Office 62
8.10.2. Topology Hiding – Service Provider 63
8.11. Application Rules 63
8.12. Media Rules 64
8.13. Signaling Rules 66
8.14. Endpoint Policy Groups 67
8.15. End Point Flows - Server Flows 68
9. BT Wholesale Hosted SIP Trunking Service Configuration 70
10. Verification Steps 71
10.1. Avaya SBCE 71
10.1.1. Device Management 71
10.1.2. Alarms 71
10.1.3. Incidents 72
10.1.4. Server Status 73
10.1.5. Tracing 74
10.2. Avaya IP Office 75
10.2.1. System Status Application 75
10.2.2. System Monitor 77
11. Conclusion 78
12. Additional References 78

©2022 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe a reference configuration using Session Initiation Protocol (SIP) trunking between the BT Wholesale Hosted SIP Trunking service offer and an Avaya IP Office solution. In the reference configuration, the Avaya IP Office solution consists of an Avaya IP Office Server Edition Primary Server (Primary server), an IP500 V2 Expansion System and an Avaya Session Border Controller for Enterprise (Avaya SBCE) in a High Availability (HA) configuration.

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 SBCE is the point of connection between Avaya IP Office and the BT Wholesale Hosted SIP Trunking service. It is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling and media for interoperability.

Enterprises might deploy the Avaya SBCE in High Availability mode to ensure signaling and media preservation in the event of any hardware or software failures of the Session Border Controller server. High availability requires a minimum of two Avaya SBCE devices and one standalone Element Management System (EMS) server.

The BT Wholesale Hosted SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the IP Office solution are able to place and receive PSTN calls via a broadband wide area network (WAN) connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

The terms “service provider”, “BT”, “BT Wholesale” or “BT Wholesale Hosted” will be used interchangeably throughout these Application Notes.

©2022 Avaya Inc. All Rights Reserved.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to BT's network via the public Internet, as depicted in **Figure 1**, and exercise the features and functionalities listed in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). 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.

©2022 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability the following features and functionalities were exercised during the interoperability compliance test:

- Public DNS "SRV" record queries to establish SIP trunk connections to BT SIP servers.
- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, Digital and Analog telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider's network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323, Digital and Analog telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider's network.
- Incoming and outgoing PSTN calls to/from Avaya Workplace Client for Windows (SIP).
- Caller ID presentation.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two-way speech-path. Testing was performed with codecs: G.722 64K, G.711A, G.729(a) and G.711U, BT's preferred codec order.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- SIP Trunk Registration after SBCE HA failover.
- Call preservation of existing calls after SBCE HA failover.
- Processing of new inbound and outbound calls after SBCE HA failover.
- Avaya Remote Worker functionality, using Avaya IX™ Workplace for Windows softphones, registered to the IP Office via a separate Avaya SBCE.

Note: Remote Workers were used as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

©2022 Avaya Inc. All Rights Reserved.

2.2. Test Results

Interoperability testing of BT Wholesale Hosted SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **SIP OPTIONS Messages** – During the compliance test BT did not send SIP OPTIONS messages to IP Office. IP Office did send SIP OPTIONS messages to BT via the Avaya SBCE. This was sufficient to keep the SIP trunk in service.
- **Outbound calls processing after failover**: During testing it was found that on new outbound calls attempted immediately after an Avaya SBCE HA failover, there was a delay of about 6 seconds before the new active SBCE started processing calls again. The delay seemed to be introduced by the DNS SRV query that is performed on the new active Avaya SBCE before it can re-register the SIP trunk to BT. This delay affected new outbound calls only. Existing calls were preserved, and new inbound calls were processed without any noticeable delay after the Avaya SBCE switchover. This issue is under investigation by Avaya.

2.3. Support

For support on BT Wholesale Hosted SIP Trunking Service visit the corporate Web page at: https://www.btwholesale.com/pages/static/home.htm

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

©2022 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the test configuration used for the DevConnect compliance testing. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the BT Wholesale Hosted SIP Trunking Service through the public Internet.

Avaya IP Office provides the voice communications services for the enterprise. In the reference configuration, Avaya IP Office runs on the Avaya IP Office Server Edition platform. Note that this solution is extensible to deployments using the standalone IP500 V2 platform as well.

In the sample configuration, the Primary server runs the Avaya IP Office Server Edition Linux software. Avaya Voicemail Pro runs as a service on the Primary Server. The LAN1 port of the Primary Server is connected to the enterprise LAN. The LAN2 port was not used.

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

The Avaya SBCE is located at the edge of the enterprise. It has two physical interfaces, interface B1 is used to connect to the public network, while interface A1 is used to connect to the private network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. The Avaya SBCE provides network address translation at both the IP and SIP layers.

In the reference configuration, the Avaya SBCE is deployed in High Availability mode, where the HA pair is deployed within the enterprise in a parallel mode configuration. High availability requires a minimum of two Avaya SBCE devices and one standalone Element Management System (EMS) server. The Avaya SBCE HA can be deployed as a pair either in the enterprise DMZ or core, or geographically dispersed where each Avaya SBCE resides in a separate, physical facility, over a network with minimum or no latency. In the reference configuration, the Avaya SBCEs run on a VMware platform. This solution is extensible to other Avaya Session Border Controller for Enterprise platforms as well.

In the SBCE HA configuration, the active SBCE is the primary server through which all signaling packets are routed. The interface ports on the standby SBCE do not process any traffic. When a failure is detected on the primary SBCE by the Avaya Element Management System (EMS), the network interface ports of the original primary SBCE are automatically disabled and the network interface ports of the standby are enabled, thus becoming the new active server.

High availability requires Gratuitous Address Resolution Protocol (GARP) support on the connected network elements. When the primary Avaya SBCE fails over, the secondary Avaya SBCE broadcasts a GARP message to announce that the secondary Avaya SBCE is now receiving requests. The GARP message announces that a new MAC address is associated with the Avaya SBCE IP address. Devices that do not support GARP must be on a different subnet with a GARP-aware router or L3 switch to avoid direct communication with the SBCE.

©2022 Avaya Inc. All Rights Reserved.

Note: Devices that do not support GARP that are directly connected to the SBCE interfaces will fail in a HA environment, as they will continue sending packets to the original primary Avaya SBCE after a failover.

All IP addresses configured on the Network Configuration screen are shared between both HA devices in HA deployment mode. The HA devices are also configured with private, default IP addresses on the M2 interface that are used to replicate signaling and media data between each other over the HA link. The configured interfaces are inoperative on the standby or secondary device until the device becomes active or primary. When the devices failover, the active device sends a GARP message to update the ARP tables of the neighboring HA device to begin receiving traffic.

IP endpoints at the enterprise included Avaya 96x1 Series IP Deskphones (with H.323 firmware), Avaya J100 Series IP Deskphones (with SIP firmware), Avaya Workplace Client for Windows (SIP), and Avaya Digital and Analog Deskphones. IP endpoints were registered to the Primary IP Office Server; non-IP endpoints (analog and digital) were registered to the Expansion System.

The transport protocol between the Avaya SBCE and BT, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network, is SIP over TLS.

For inbound calls, the calls flowed from BT's network to the Avaya SBCE, then to IP Office.

Outbound calls to the PSTN were first processed by IP Office. Once IP Office selected the proper SIP trunk, the call was routed to the Avaya SBCE for egress to BT's network.

For the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to BT's network. The short code 9 was stripped off by Avaya IP Office, but the remaining N digits were sent unaltered to BT's network.

In an actual customer configuration, the enterprise site may include additional network components between the service provider and the IP Office system, such as a session border controller or data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that all SIP and RTP traffic between the service provider and the IP Office system must be allowed to pass through these devices.

For confidentiality and privacy purposes, public IP addresses, domain names, and routable DID numbers used during the compliance testing have been masked.

©2022 Avaya Inc. All Rights Reserved.

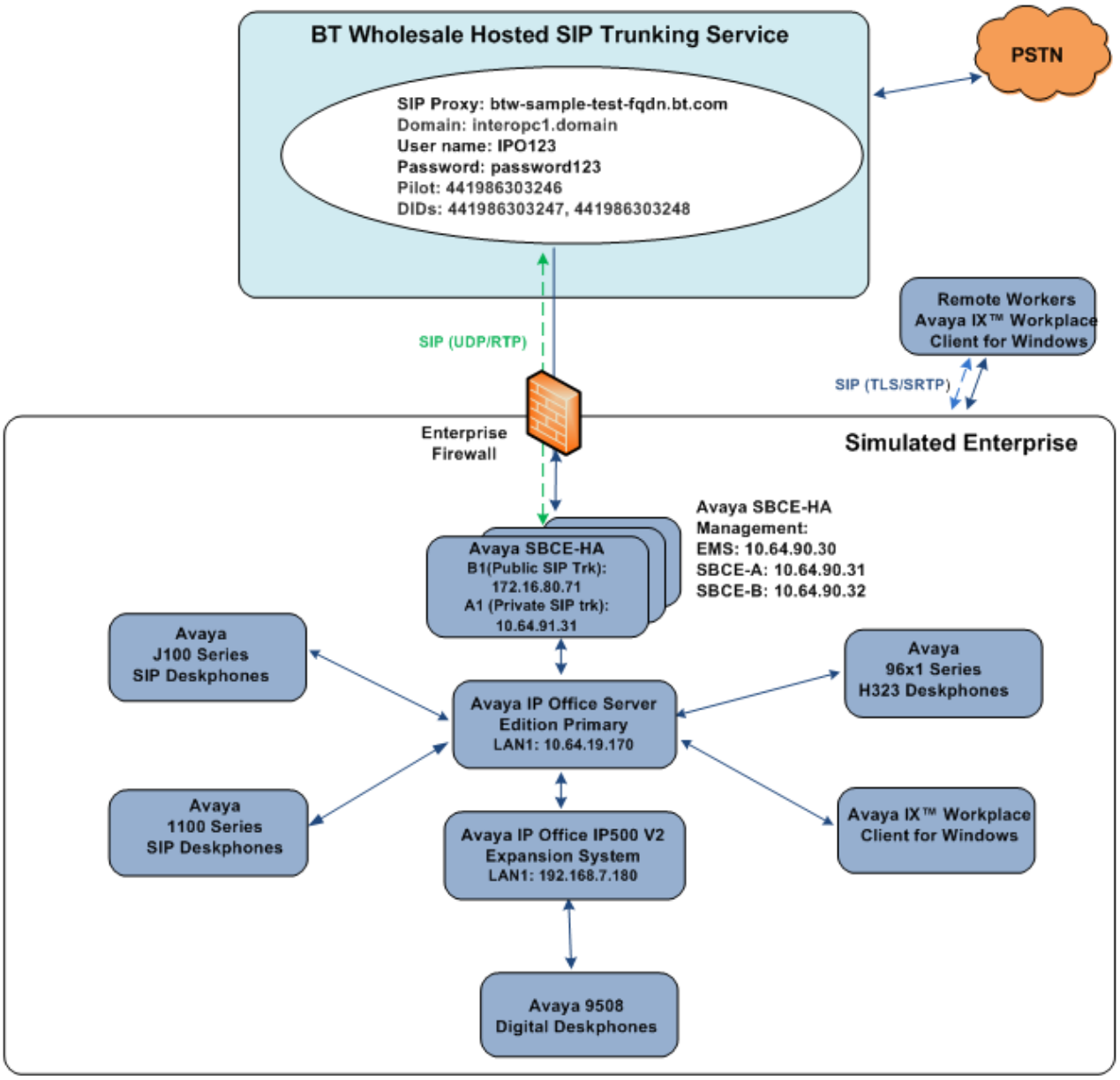


Figure 1: Avaya Interoperability Test Lab Configuration

©2022 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

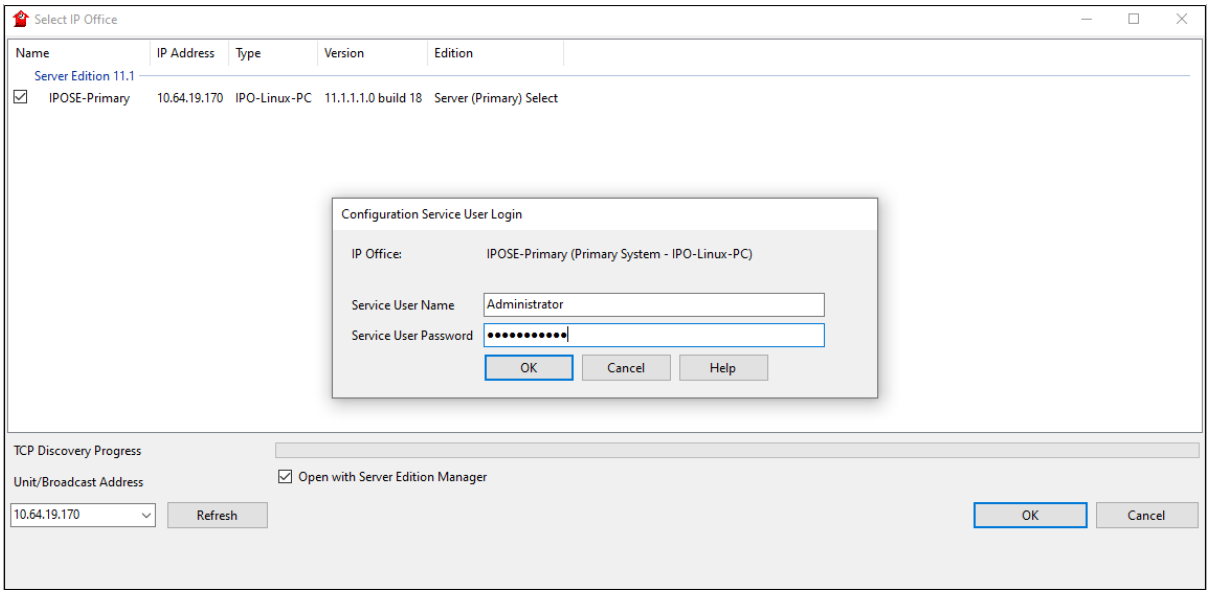
Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server) • Avaya IP Office Voicemail Pro	11.1.1.1.0 Build 18 11.1.1.1.0 Build 6
Avaya IP Office IP500 V2 (Expansion Systems)	11.1.1.1.0 Build 18
Avaya IP Office Manager	11.1.1.1.0 Build 18
Avaya Session Border Controller for Enterprise (EMS)	8.1.3.0-31-21052
Avaya Session Border Controller for Enterprise (SBCE pair)	8.1.3.0-31-21052
Avaya 96x1 Series IP Deskphones (H.323)	6.8304
Avaya J169 IP Deskphones (SIP)	4.0.6.0.7
Avaya 1140E IP Deskphone (SIP)	04.04.23.00
Avaya 9508 Digital Telephone	0.60
Avaya Workplace Client for Windows (SIP).	3.23.0.64
BT Wholesale Hosted SIP Trunking Service	
Acme Packet 6350	SCZ8.4p7k
BroadWorks	R22

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.

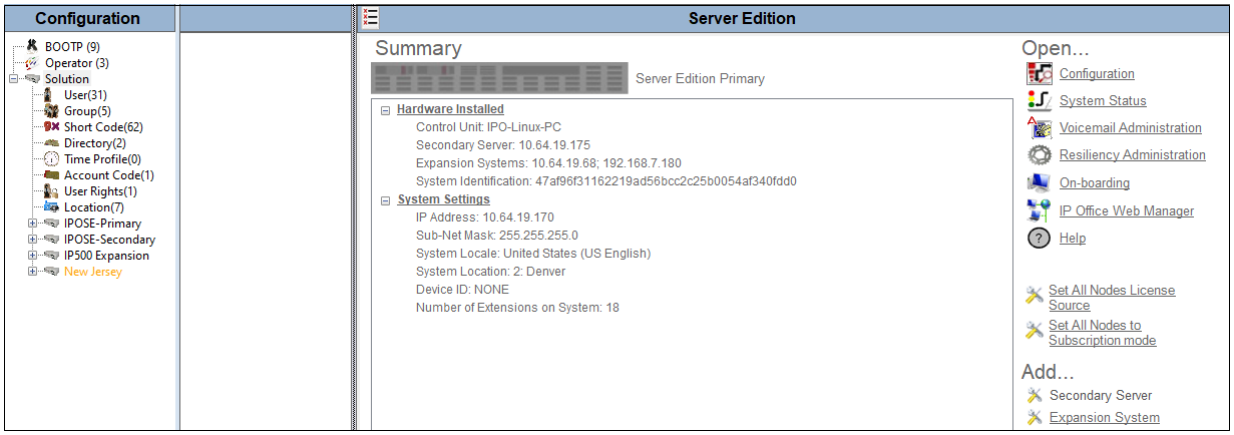
©2022 Avaya Inc. All Rights Reserved.

5. Avaya IP Office Primary Server Configuration

IP Office is configured via the IP Office Manager program. For more information on IP Office Manager, consult reference **[4]**. From the IP Office Manager PC, select **Start → Programs → IP Office → Manager** to launch the Manager application. Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials.



On Server Edition systems, the Solution View screen will appear, similar to the one shown below. All the Avaya IP Office configurable components are shown in the left pane, known as the Navigation Pane. Clicking the "plus" sign next to the Primary server system name, e.g., **IPOSE-Primary**, on the navigation pane will expand the menu on this server.



©2022 Avaya Inc. All Rights Reserved.

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

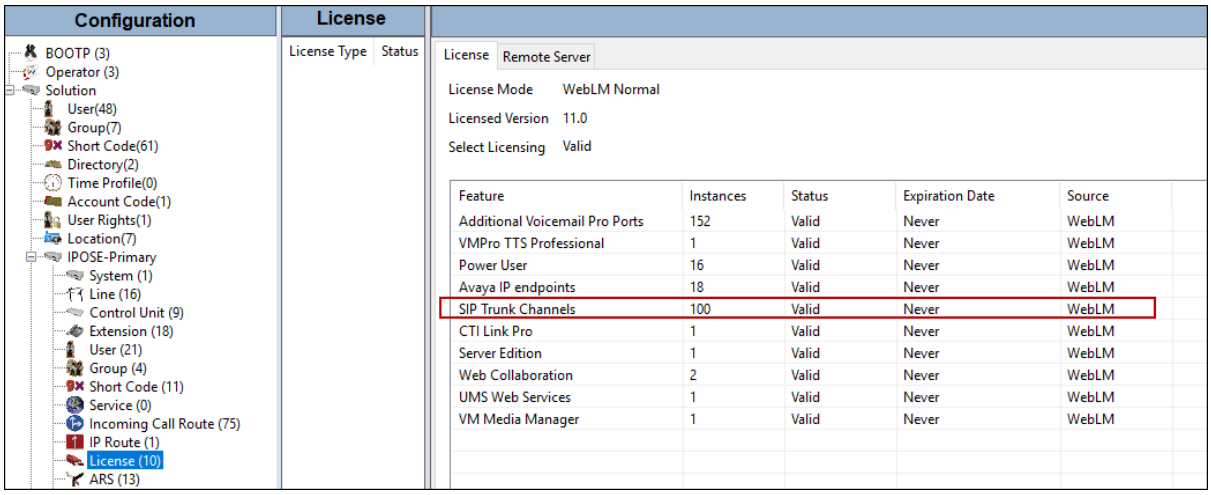
Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

5.1. Licensing

In the reference configuration, **IPOSE-Primary** was used as the system name of the Primary Server and **IP500 Expansion** was used as the system name of the Expansion System. All navigation described in the following sections (e.g., **License**) appears as submenus underneath the system name in the Navigation Pane.

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

Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of channels provisioned for the SIP trunk.



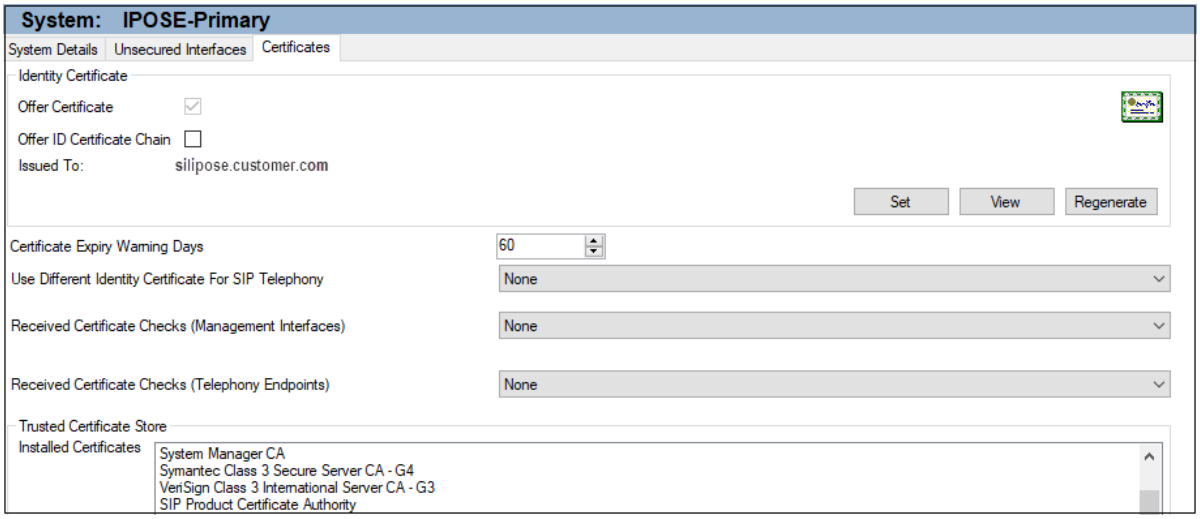
©2022 Avaya Inc. All Rights Reserved.

5.2. TLS Management

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

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

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



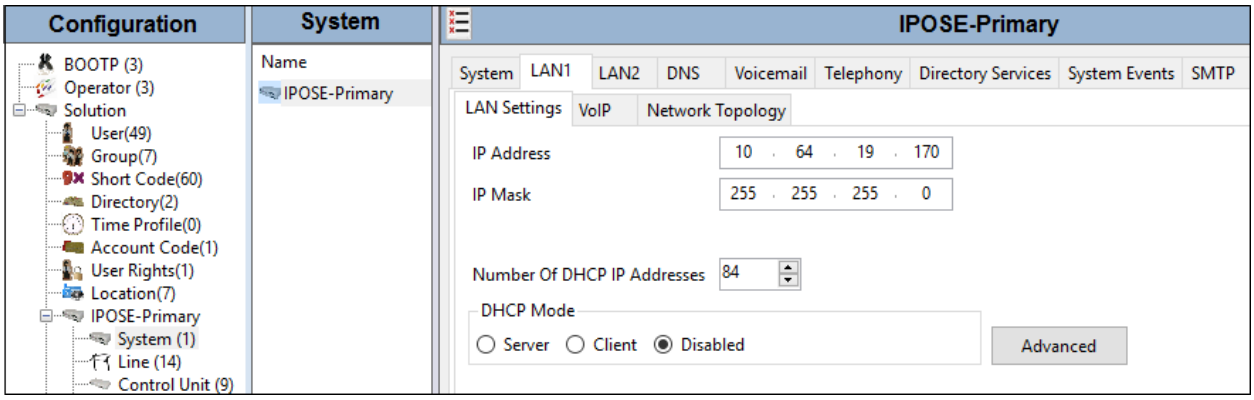
©2022 Avaya Inc. All Rights Reserved.

5.3. System Settings

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

5.3.1. LAN1 Settings

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

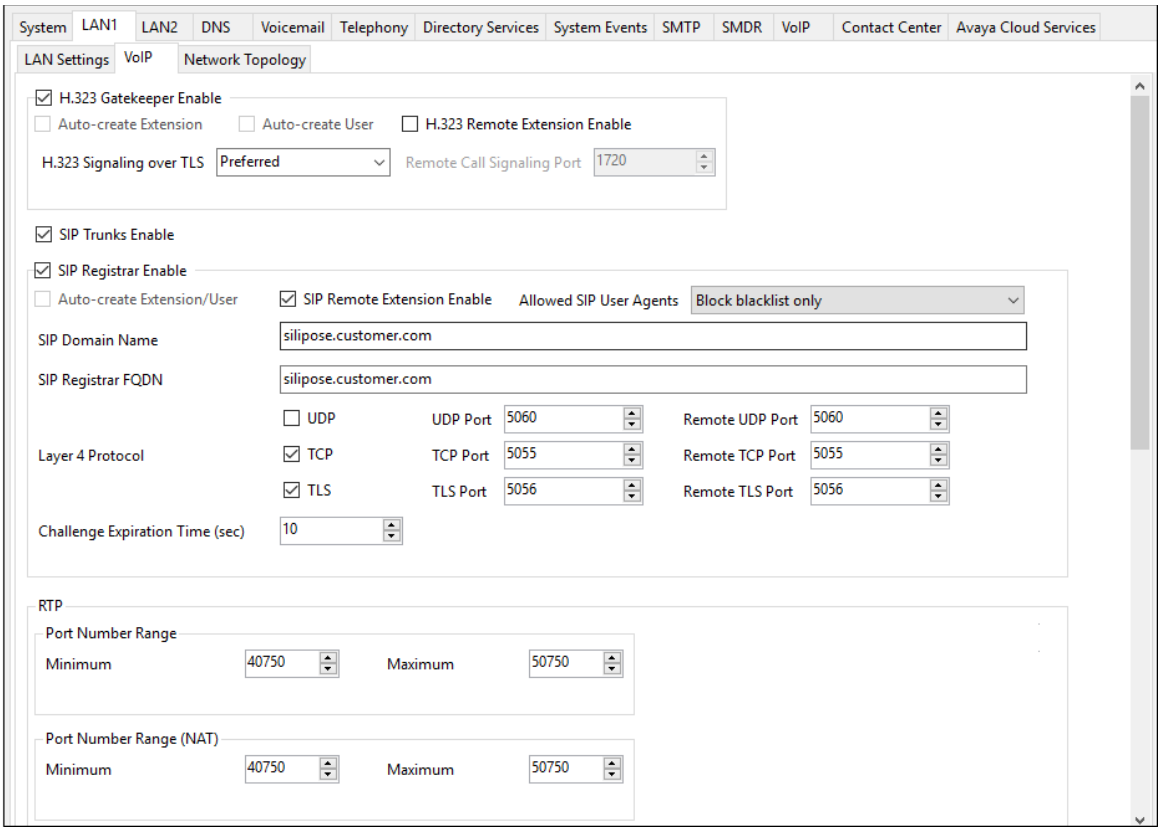


©2022 Avaya Inc. All Rights Reserved.

Select the **VoIP** tab as shown in the following screen. The **H323 Gatekeeper Enable** parameter is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the Avaya 96x1 deskphones used in the reference configuration. The **H.323 Signaling over TLS** should be set based on customer needs. In the reference configuration it was set to **Preferred**. The **SIP Trunks Enable parameter** must be checked to enable the configuration of SIP trunks to BT. The **SIP Registrar Enable** parameter is checked to allow Avaya J169, Avaya 1140E, and Avaya Equinox usage.

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

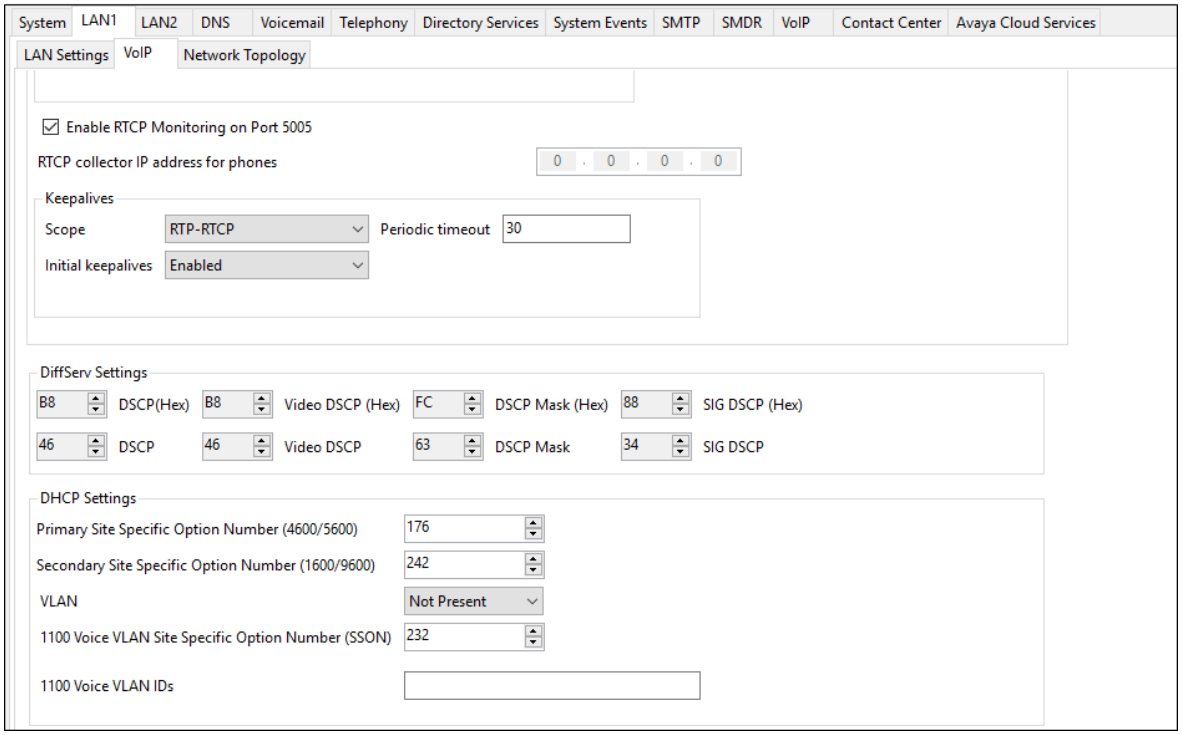
If desired, the **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media paths from Avaya SBCE to the Primary server. The defaults are used here.



©2022 Avaya Inc. All Rights Reserved.

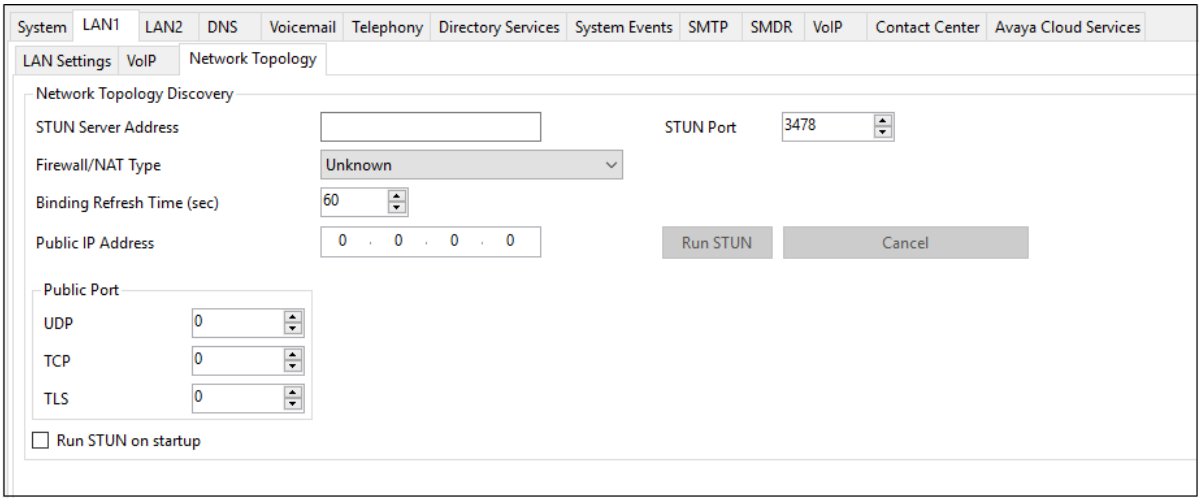
Scrolling down the page, on the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. These settings will cause the Primary server to send RTP and RTCP keepalive packets starting at the time of initial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

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



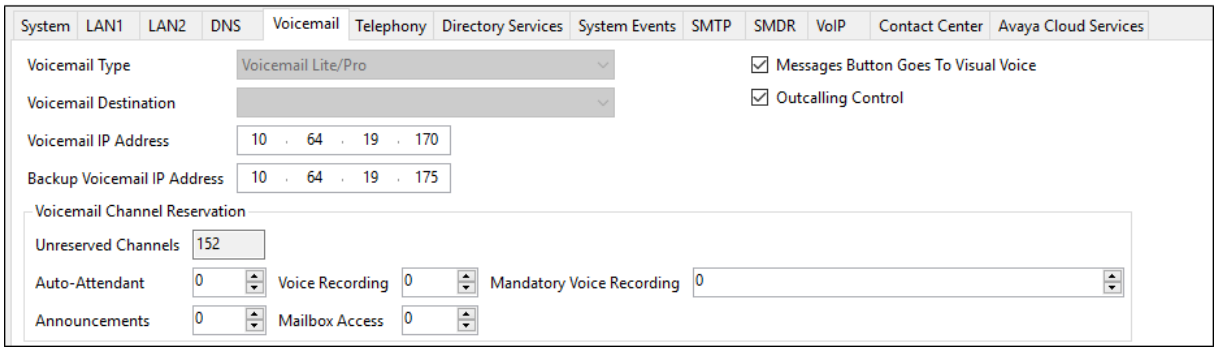
©2022 Avaya Inc. All Rights Reserved.

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



5.3.2. Voicemail Settings

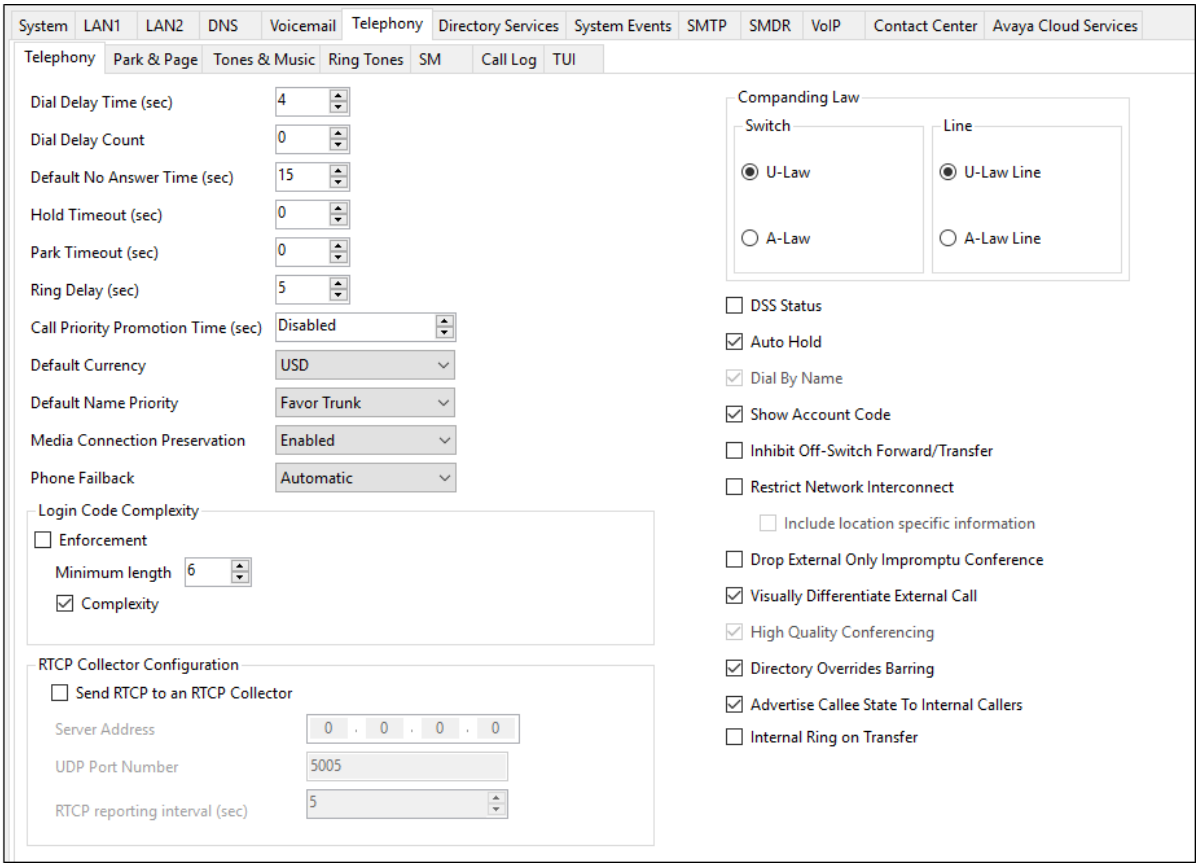
To view or change voicemail settings, select the **Voicemail** tab as shown in the following screen. The settings presented here simply illustrate the reference configuration and are not intended to be prescriptive. The **Voicemail Type** in the reference configuration is **Voicemail Lite/Pro**. The **Voicemail IP Address** in the reference configuration is **10.64.19.170**, the IP address of the Primary server running the Voicemail Pro software.



©2022 Avaya Inc. All Rights Reserved.

5.3.3. System Telephony Settings

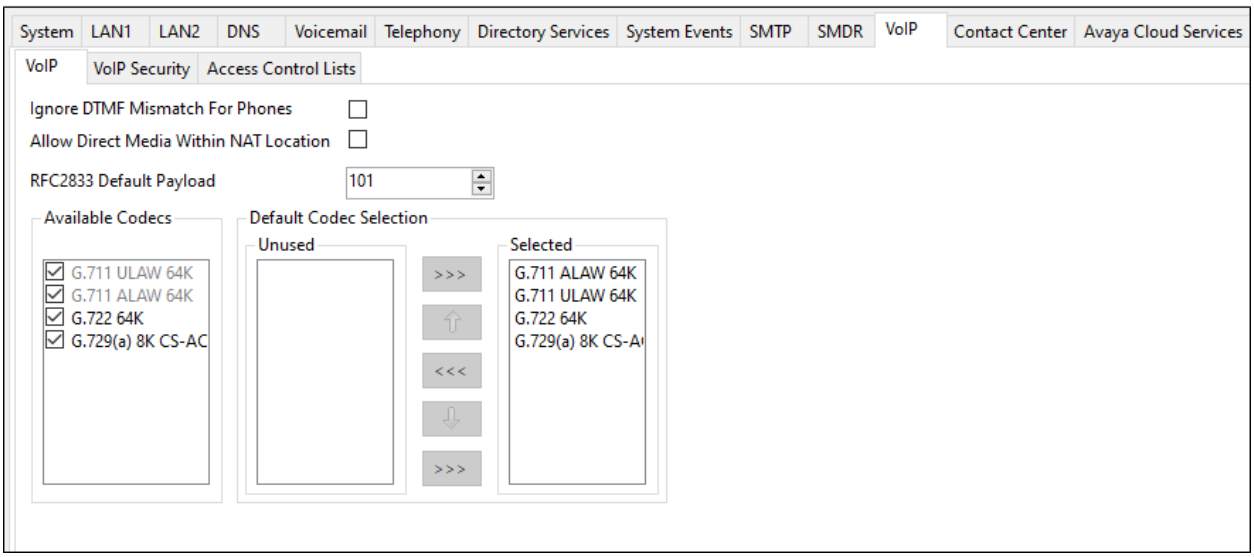
To view or change telephony settings, select the **Telephony** tab and **Telephony** sub-tab as shown in the following screen. The settings presented here simply illustrate the reference configuration and are not intended to be prescriptive. In the reference configuration, the **Inhibit Off-Switch Forward/Transfer parameter** is unchecked so that call forwarding and call transfer to PSTN destinations via the BT SIP Trunk can be tested. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave this setting checked. Other parameters on this screen may be set according to customer requirements.



©2022 Avaya Inc. All Rights Reserved.

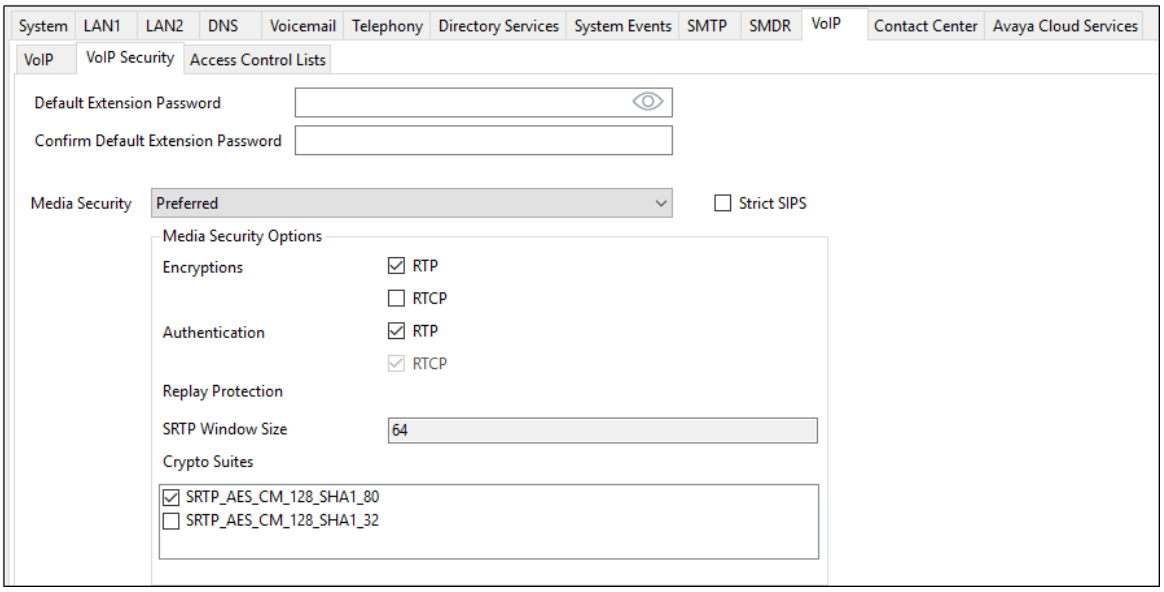
5.3.4. System VoIP Settings

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



©2022 Avaya Inc. All Rights Reserved.

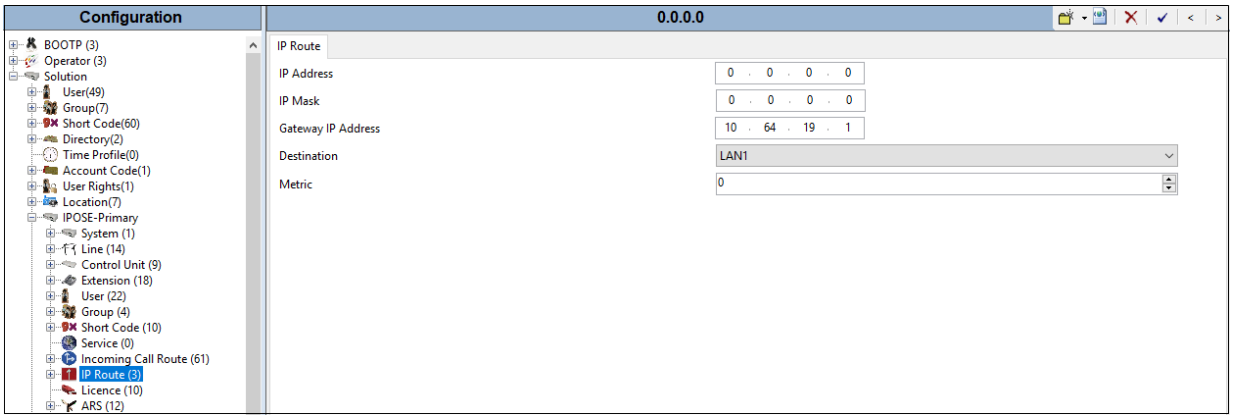
During the compliance test, SRTP was used internal to the enterprise wherever possible. To view or configure the media encryption settings, select the **VoIP → VoIP Security** tab on the Details pane. The **Media Security** drop-down menu is set to **Preferred** to have IP Office attempt use encrypted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



©2022 Avaya Inc. All Rights Reserved.

5.4. IP Route

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



©2022 Avaya Inc. All Rights Reserved.

5.5. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and BT. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.5.1** to create the SIP Line from the template.

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

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries

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

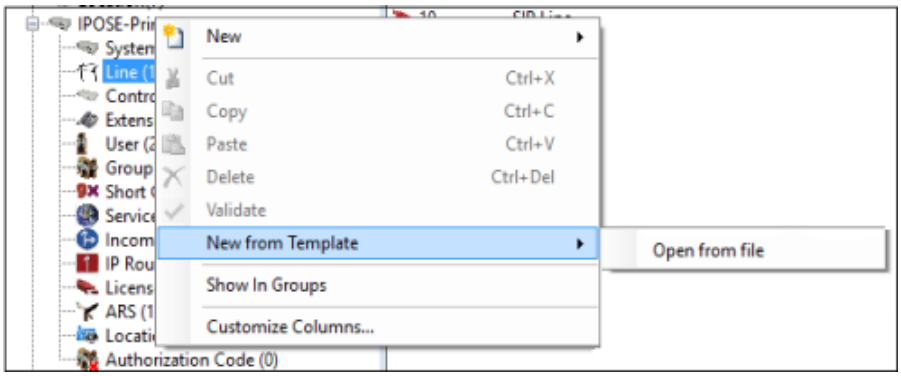
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.5.2** to **5.5.6**.

©2022 Avaya Inc. All Rights Reserved.

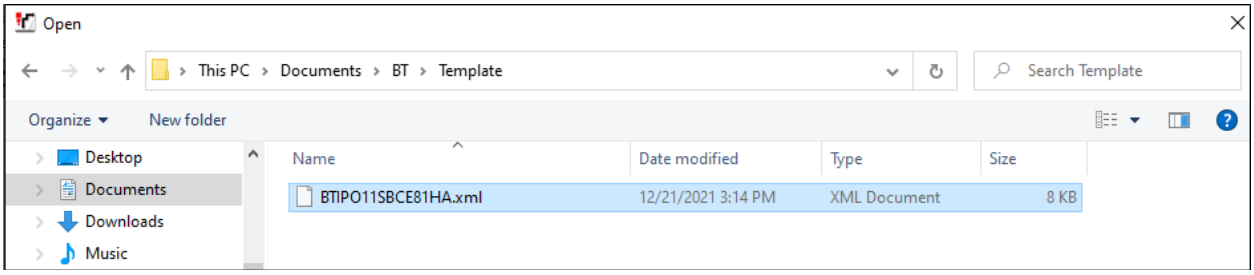
5.5.1. Creating a SIP Trunk from an XML Template

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 (500 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 and select it. Click **Open** (not shown).



The new SIP Line is created, and it will appear on the **Navigation** pane (e.g., SIP Line **30**). The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.5.2** to **5.5.6**.

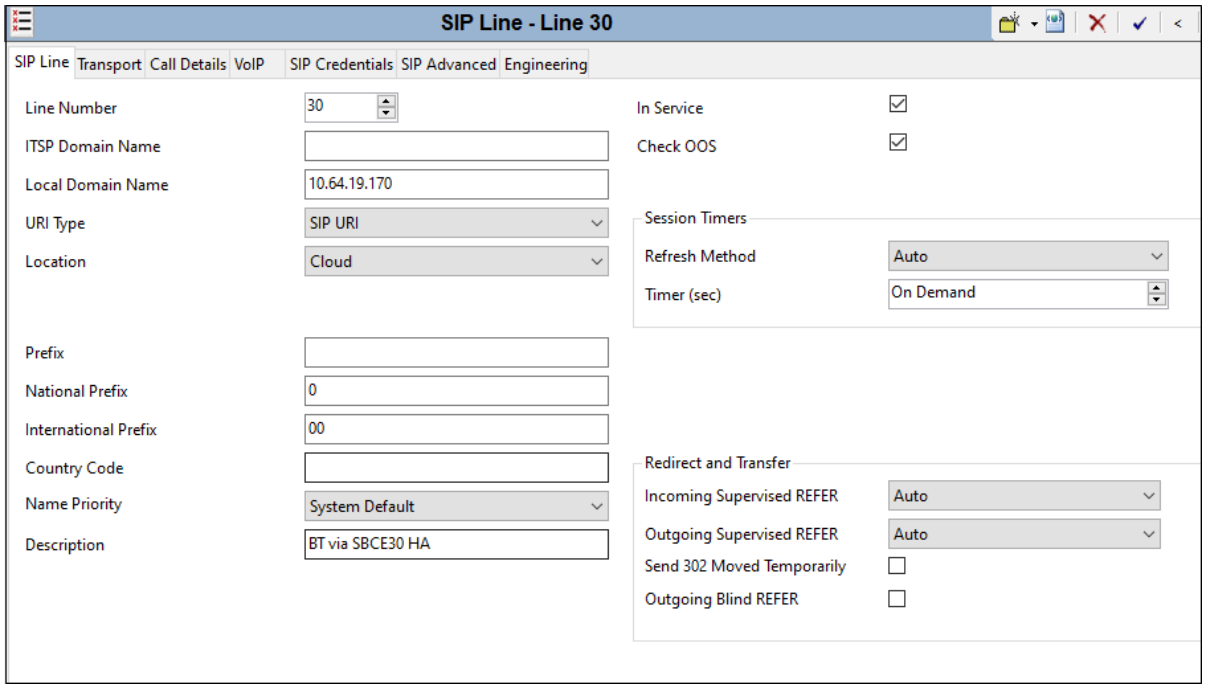
©2022 Avaya Inc. All Rights Reserved.

5.5.2. SIP Line – SIP Line Tab

The **SIP Line** tab in the Details pane is shown below for Line Number **30**, used to connect to the Avaya SBCE and the BT SIP Trunking service. The **ITSP Domain Name** is left blank, to have IP Office send the **ITSP Proxy Address** as the domain name (see **Section 5.5.3**). **Local Domain Name** is set to the IP address of the Avaya IP Office LAN1 interface (e.g., **10.64.19.170**). By default, the **In Service** and **Check OOS** boxes are checked. In the reference configuration, IP Office will use the SIP OPTIONS method to periodically check the SIP Line. The time between SIP OPTIONS sent by IP Office will use the **Binding Refresh Time** for LAN1, as shown in **Section 5.3.1**.

Under **Session Timers**, the **Refresh Method** is set to "**Auto**" and the **Timer (seconds)** is set to **On Demand**, the default values.

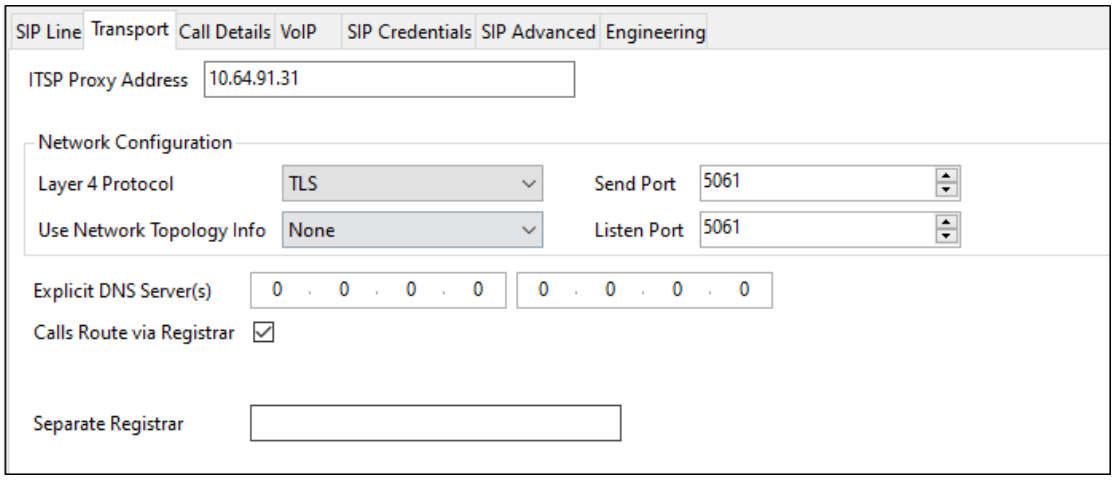
Under **Redirect and Transfer**, the default setting **Auto** for the automatic determination of **Incoming Supervised REFER** and **Outgoing Supervised REFER** is used. Alternatively, the default can be overridden with "**Never**" to explicitly disable use of supervised REFER.



©2022 Avaya Inc. All Rights Reserved.

5.5.3. SIP Line - Transport Tab

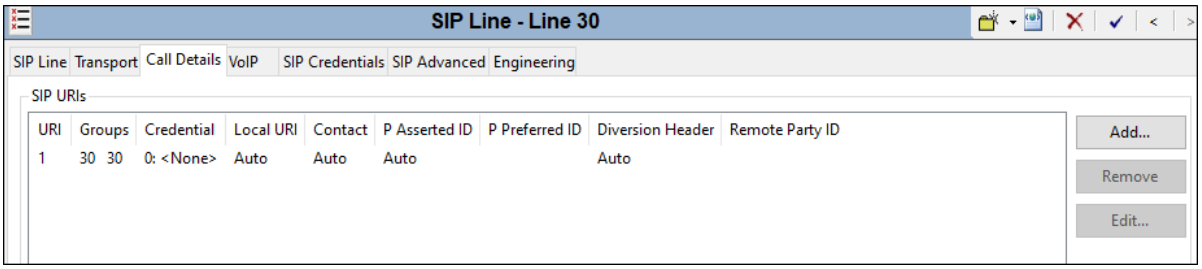
Select the **Transport** tab. The **ITSP Proxy Address** is set to the inside IP address of the Avaya SBCE as shown in **Figure 1**. In the **Network Configuration** area, **TLS** is selected as the **Layer 4 Protocol**. The **Send Port** and **Listen Port** can retain the default value 5061. The **Use Network Topology Info** parameter is set to **None**.



Note: In the reference configuration, for increased security, the TLS protocol is used in the connection between the IP Office and the Avaya SBCE. If TLS is not required, TCP could also be used if desired.

5.5.4. SIP Line – Call Details Tab

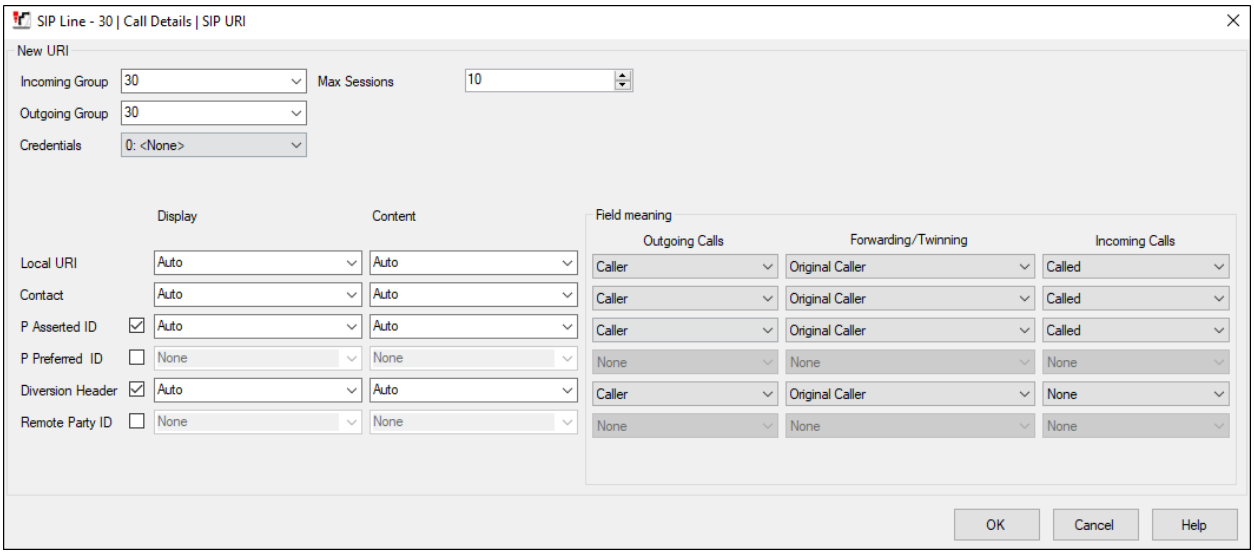
Select the **Call Details** tab. To add a new SIP URI, click the **Add…** button. A New URI area will be opened. To edit an existing entry, click an entry in the list at the top, and click the **Edit…** button.



©2022 Avaya Inc. All Rights Reserved.

In the example screen below, a previously configured entry is edited. The **Incoming Group** parameter, set here to **30**, will be referenced when configuring Incoming Call Routes to map inbound SIP trunk calls to IP Office destinations in **Section 5.7**. The **Outgoing Group** parameter, also set to **30**, will be used for routing outbound calls to BT via ARS (**Section 5.8**). The **Max Sessions** parameter was set to "**10**". This value sets the maximum number of simultaneous calls that can use the URI before IP Office returns busy to any further calls.

Auto is selected for the **Local URI**, **Contact**, **P-Asserted ID** and **Diversion Header** parameters. With this configuration, information in the Incoming Call Route (**Section 5.7**) is used determine what call is accepted on the SIP Line. The Incoming Call Route for individual users will also be used to populate the SIP From, Contact and P-Asserted-Identity headers for outbound calls. Set the **Field meaning** section to the values shown in the screenshot below.

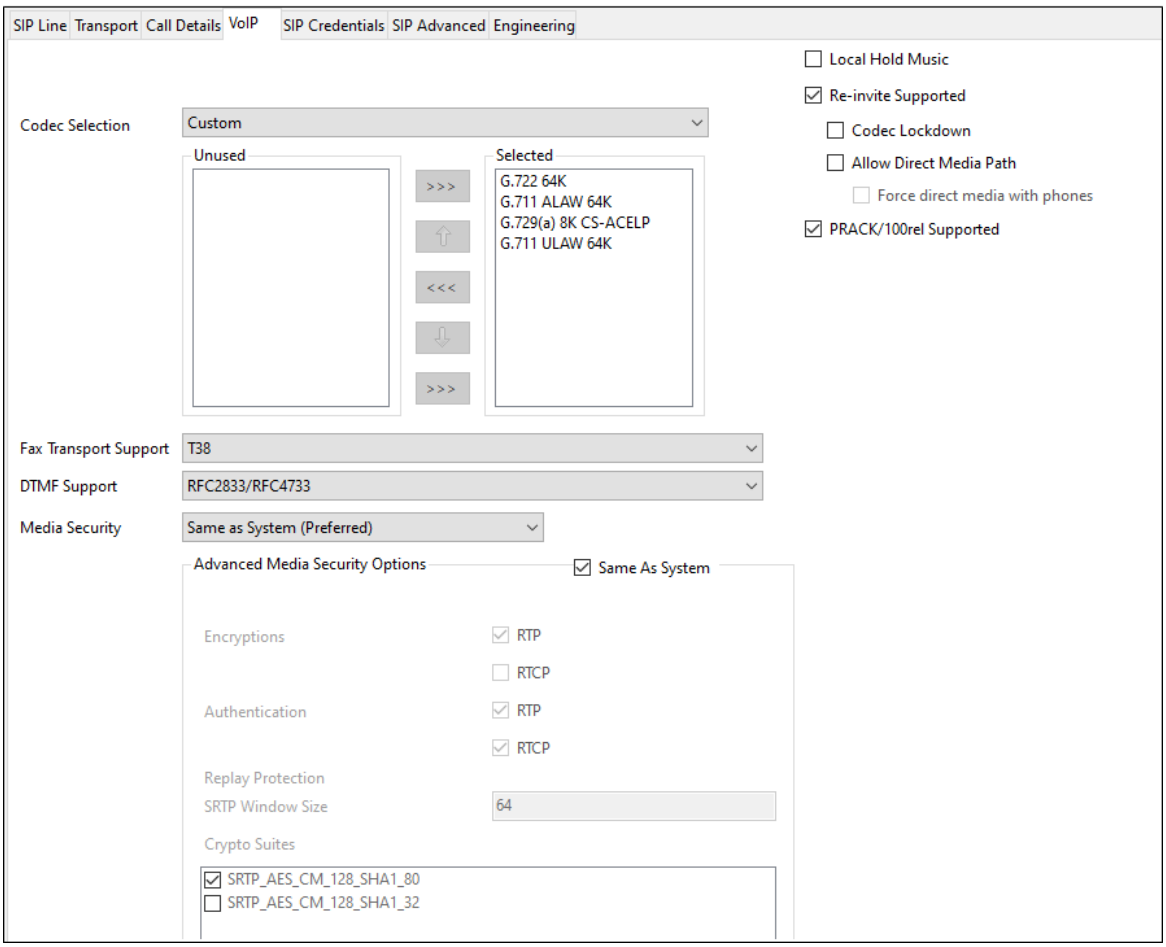


In the reference configuration, the single SIP URI shown above was sufficient to allow incoming calls for BT DID numbers destined for specific IP Office users, hunt groups or short codes.

©2022 Avaya Inc. All Rights Reserved.

5.5.5. SIP Line - VoIP Tab

Select the **VoIP** tab. The **Codec Selection** drop-down parameter **System Default** (default) will match the codecs set in the system wide Default Selection list (**System → VoIP**). In the reference configuration, **Custom** is selected and the codecs **G.722 64K**, **G.711ALAW, G.729(a)** and **G.711ULAW** preferred by BT are specified. This will cause IP Office to include these codecs in the Session Description Protocol (SDP) offer, in that order. The **Fax Transport Support** drop-down is set to **T38**. The **DTMF Support** parameter can remain set to the default value **RFC2833/RFC4733**. The **Media Security** drop-down menu is set to **Same as System (Preferred)** to have IP Office use the system setting for media security set in **Section 5.3.4** to encrypted RTP toward Avaya SBCE. The **Re-invite Supported** parameter is checked to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk. The **PRACK/100rel Supported** box is checked, to advertise the support of provisional responses on the SIP trunk.

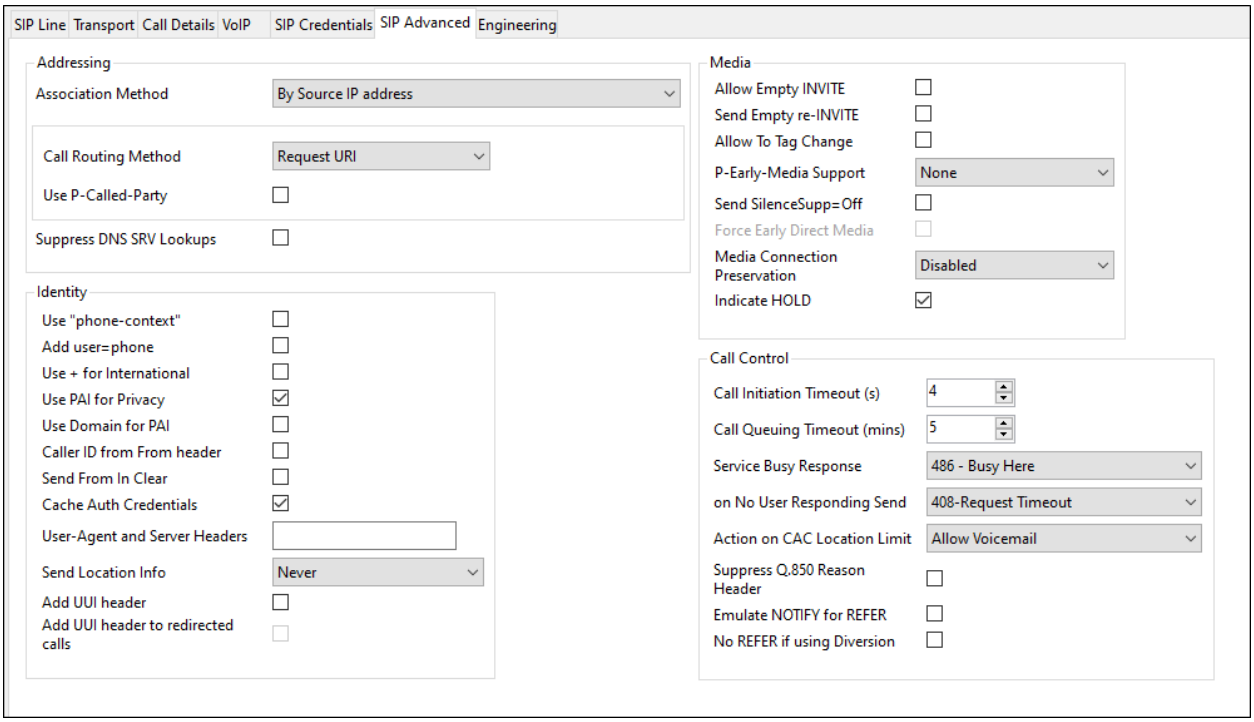


©2022 Avaya Inc. All Rights Reserved.

5.5.6. SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab. In the **Addressing** area, select **Request URI** for **Call Routing Method**. In the **Identity** area, the **Use PAI for Privacy** parameter is checked to include the caller's DID number in the P-Asserted-Identity (PAI) SIP header for a privacy requested call. This PAI SIP header is required by BT to admit an otherwise anonymous caller to the network. In the **Media** area, the **Indicate HOLD** parameter is checked to have IP Office send an INVITE with media attribute "sendonly", indicating the call was placed on hold.

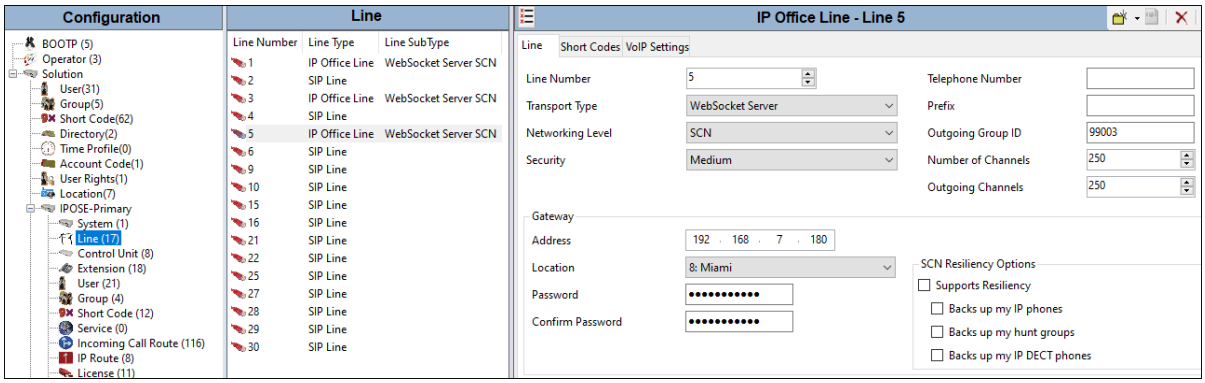
Default values may be used for all other parameters.



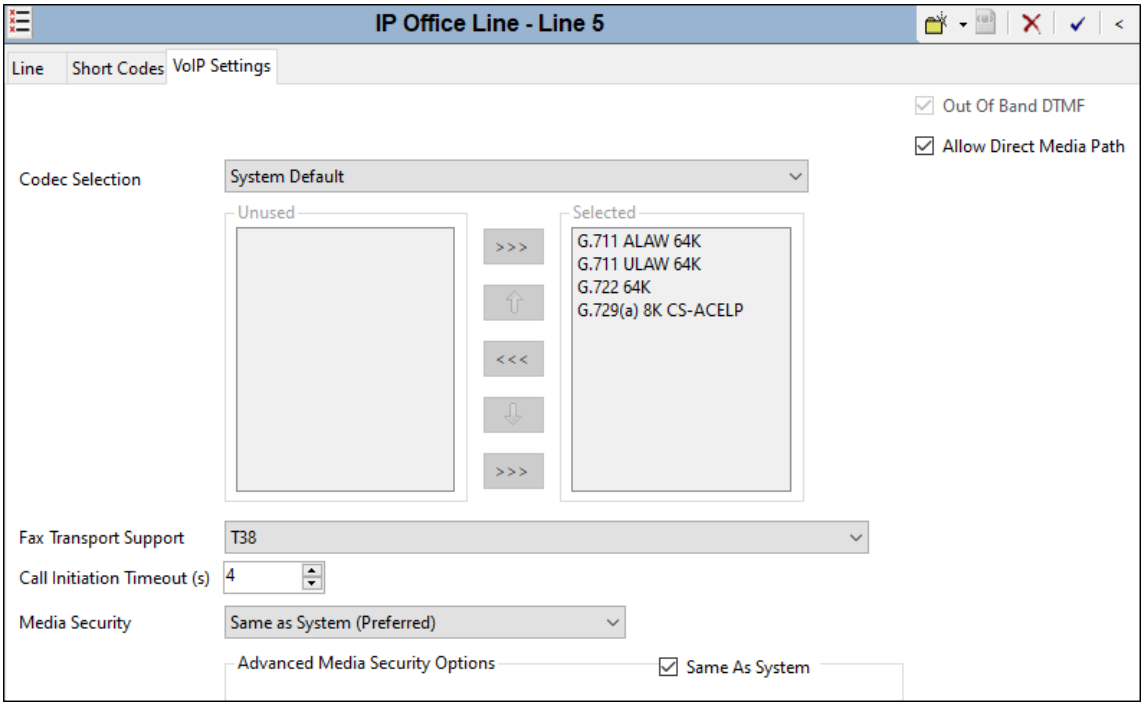
©2022 Avaya Inc. All Rights Reserved.

5.6. IP Office Line

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



The screen below shows the IP Office Line, **VoIP Settings** tab. In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. **Fax Transport Support** is set to **T.38**. The **Media Security** is set to **Same as System (Preferred)** to have IP Office use the system setting for media security set in **Section 5.3.4** to encrypted RTP. Default values were used for all other parameters.



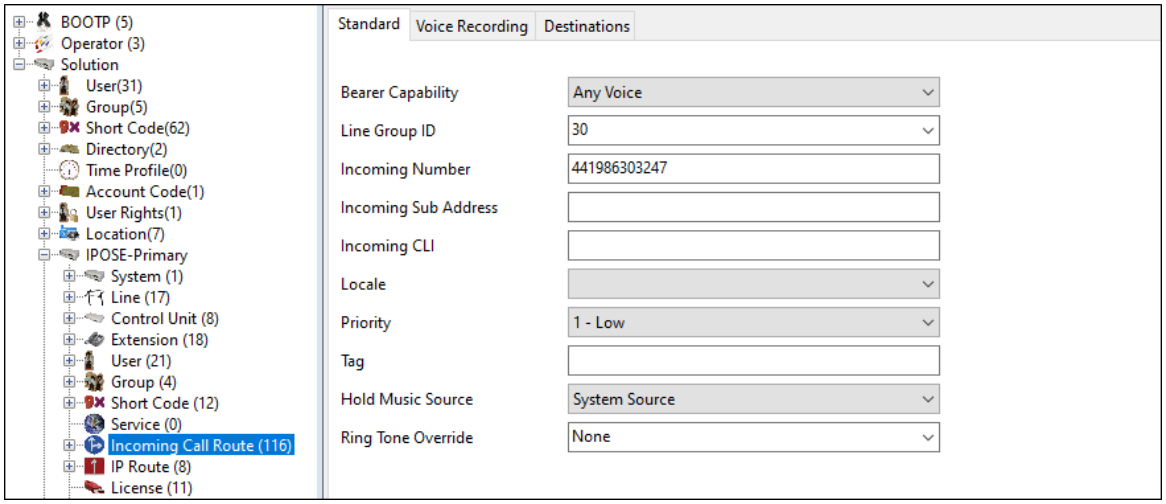
©2022 Avaya Inc. All Rights Reserved.

5.7. Incoming Call Routes

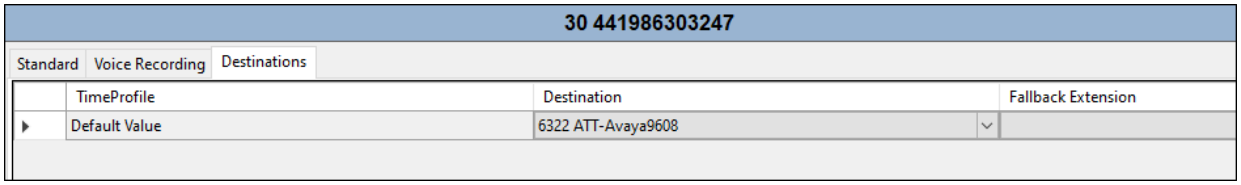
In this section, IP Office Incoming Call Routes are illustrated. To add an incoming call route, right click on **Incoming Call Route** in the Navigation pane and select **New**. To edit an existing incoming call route, select **Incoming Call Route** in the Navigation pane, and the appropriate incoming call route to be configured in the Group pane.

In the screen shown below, a simple incoming call route is illustrated. The **Line Group Id** is **30**, matching the **Incoming Group** field configured in the **SIP URI** tab for the SIP Line in **Section 5.5.4**. The **Incoming Number** field is set to the incoming number on which this route should match. Matching is right to left.

Note: When the destination is a user's extension, the **Incoming Number** can be used to construct the From, Contact and P-Asserted-Identity headers in place of the extension number in the outgoing SIP INVITE message for the user, for caller ID purposes.



On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. Click the **OK** button (not shown). In this example, incoming calls to 441986303247 on line 30 are routed to extension 6322.



Repeat this process as needed to assign incoming call routes to additional IP Office users, as well as for other Avaya IP Office destinations (Hunt Group, Voicemail, Short Codes, etc.).

©2022 Avaya Inc. All Rights Reserved.

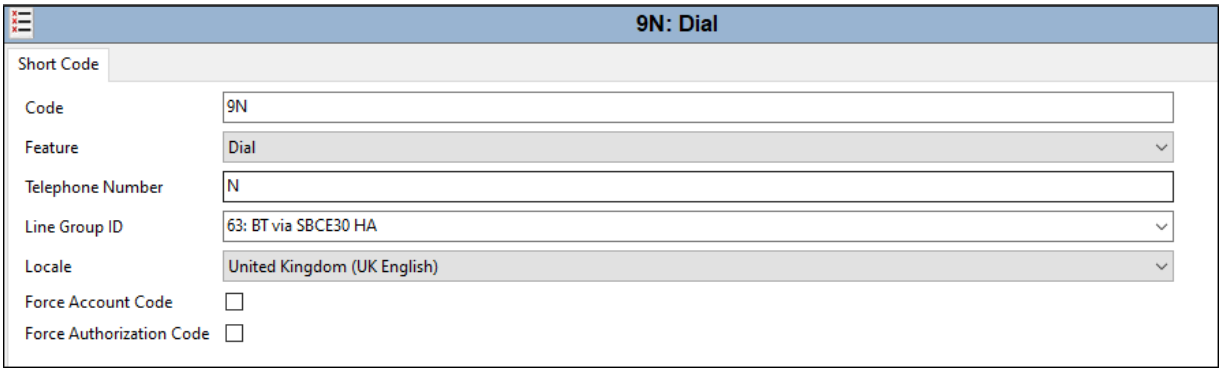
5.8. Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. While detailed coverage of ARS is beyond the scope of these Application Notes, and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance testing.

5.8.1. Short Codes

To add a short code for outbound dialing, right click on **Short Code** in the Navigation pane, and select **New**. To edit an existing short code, click **Short Code** in the Navigation pane, and the short code to be configured in the Group pane.

In the screen shown below, the short code **9N** is illustrated. The **Code** parameter is set to **9N**. The **Feature** parameter is set to **Dial**. The **Telephone Number** parameter is set to **N**. The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message. The **Line Group ID** parameter is set to **63: BT via SBCE30 HA**, configurable via ARS.



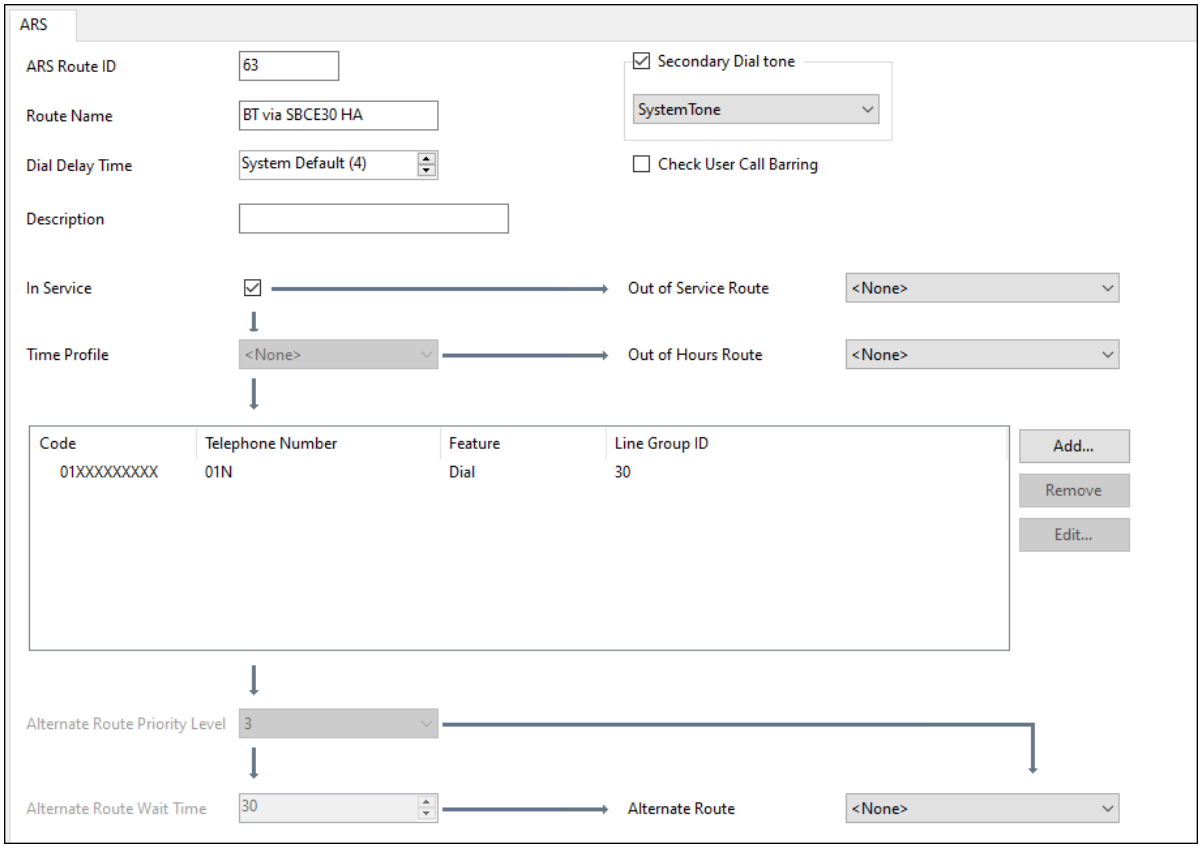
©2022 Avaya Inc. All Rights Reserved.

5.8.2. ARS Route

As described in **Section 5.8.1**, Short Code **9N** was defined for ARS access. Therefore, outbound calls via ARS are dialed as 9 plus the number. ARS will strip off the 9, and it will process the call based on the remaining digits.

To add a new ARS route, right-click **ARS** in the **Navigation** pane, and select **New** (not shown). The following screen shows the **ARS Route ID 63**, created in the sample configuration. During the compliance tests, after dialing 9 the user dialed prefix **01** followed by 9 digits (represented by the **Code** with string **01** and **9 Xs)**. The **Telephone Number** is set to **01N**. The value N represents the additional number of digits dialed by the user after dialing 01. The **Feature** is set to **Dial,** and the **Line Group ID** is set to **30,** matching the number of the **Outgoing Group** configured on the **SIP URI** tab of SIP Line 30 to BT (**Section 5.5.4**).

Other dialing codes should be created as needed.

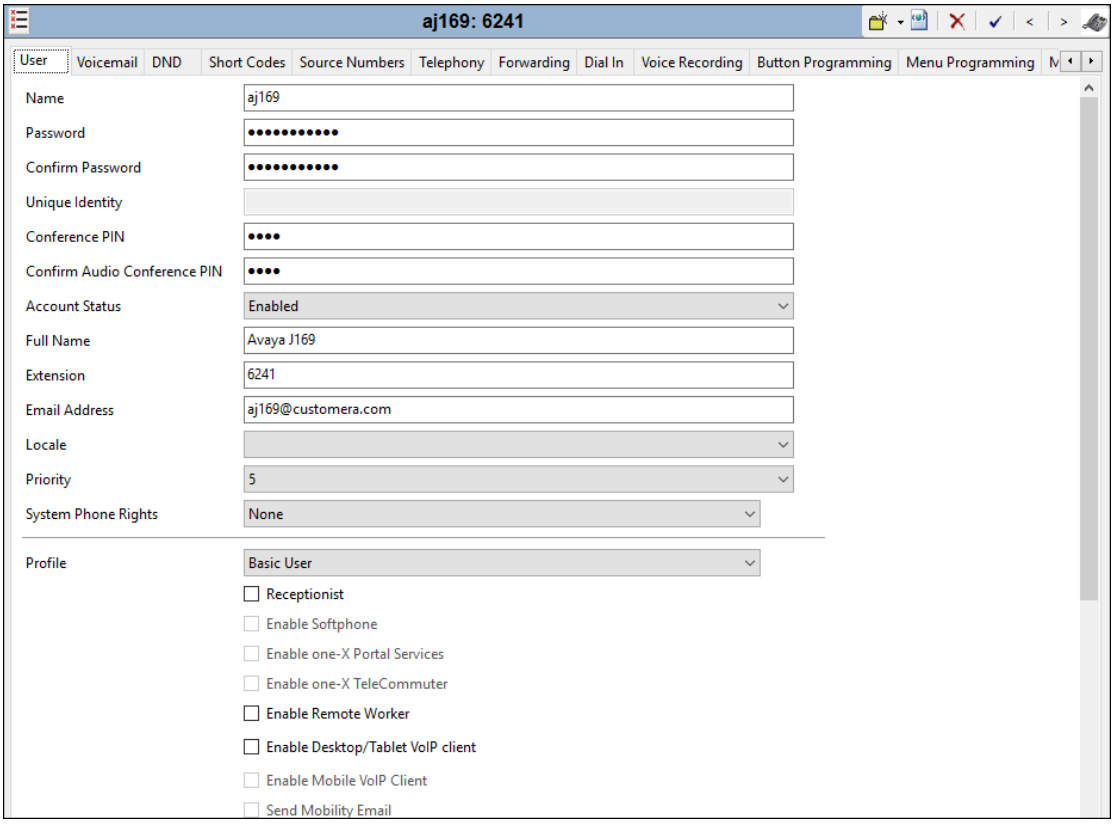


©2022 Avaya Inc. All Rights Reserved.

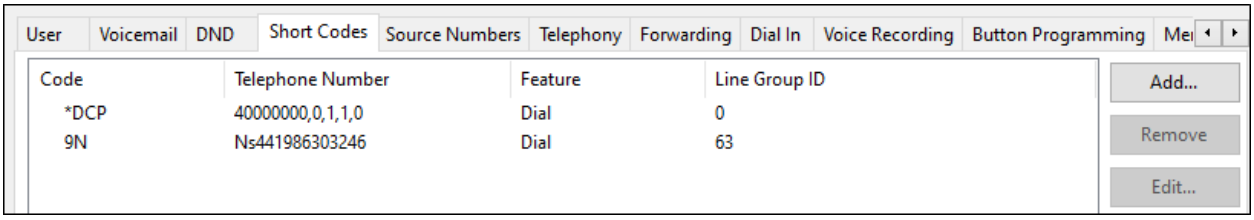
5.9. Users

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

The following screen shows the **User** tab for user 6241, corresponding to the Avaya J169 SIP endpoint.



Optionally, if the user does not have a telephone number assigned to it in the incoming call route (**Section 5.7**), a user Short Code can be created to set the outbound caller ID. The following screen shows the **Short Codes** tab for user 6241. This user is not associated with an incoming call route. The **Telephone Number** is set to **Ns441986303246**. The number after "s" is used to construct the From, Contact and PAI headers in the outgoing SIP INVITE message.

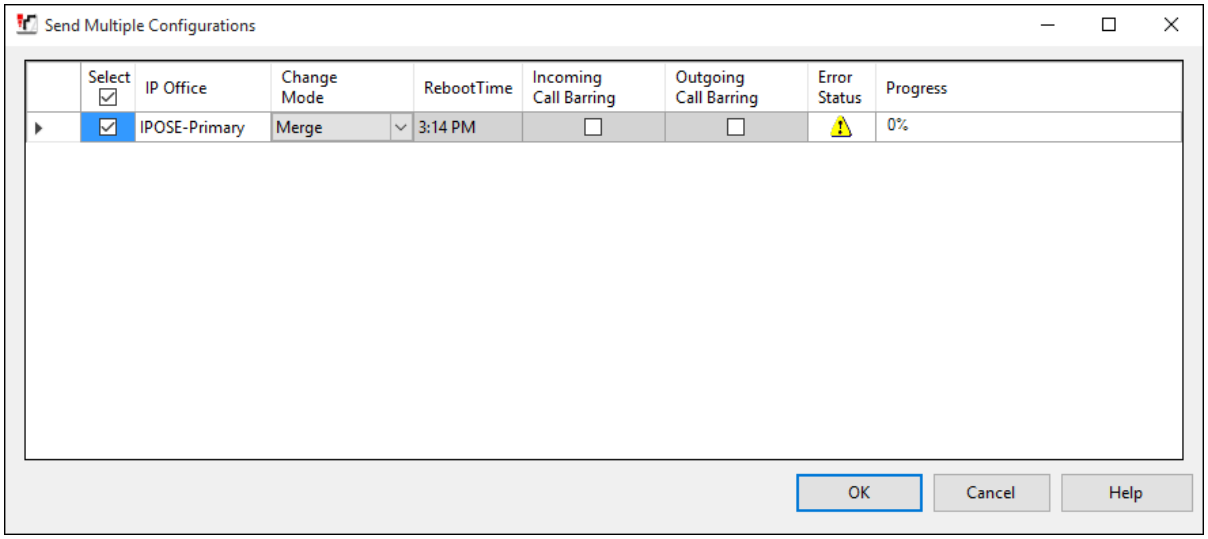


©2022 Avaya Inc. All Rights Reserved.

5.10. Save Configuration

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

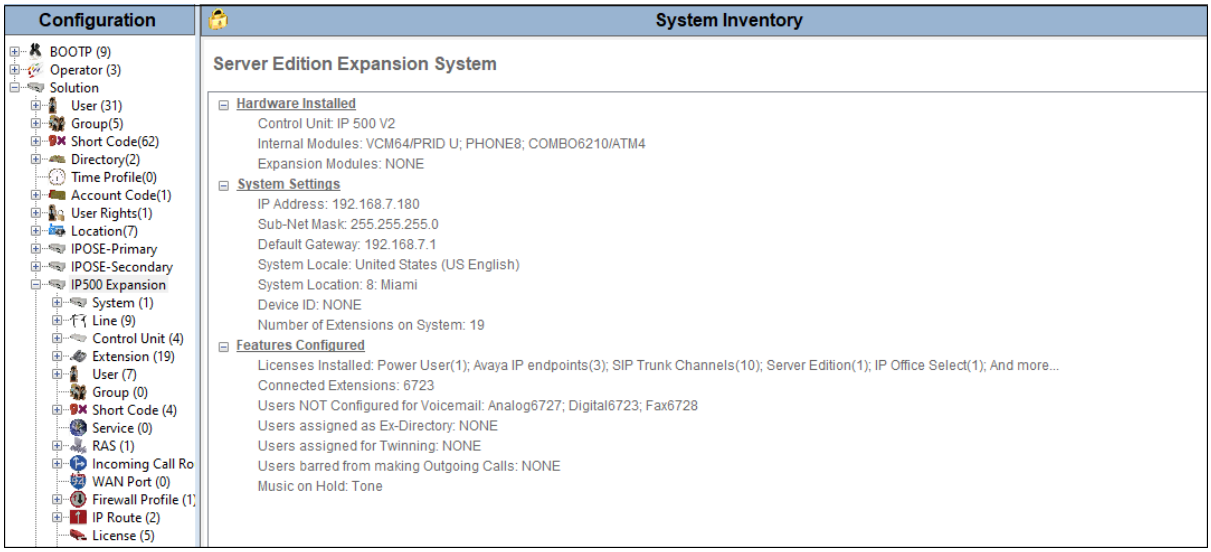
The following will appear, with either **Merge** or **Reboot** selected for the **Change Mode**, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** if desired.



©2022 Avaya Inc. All Rights Reserved.

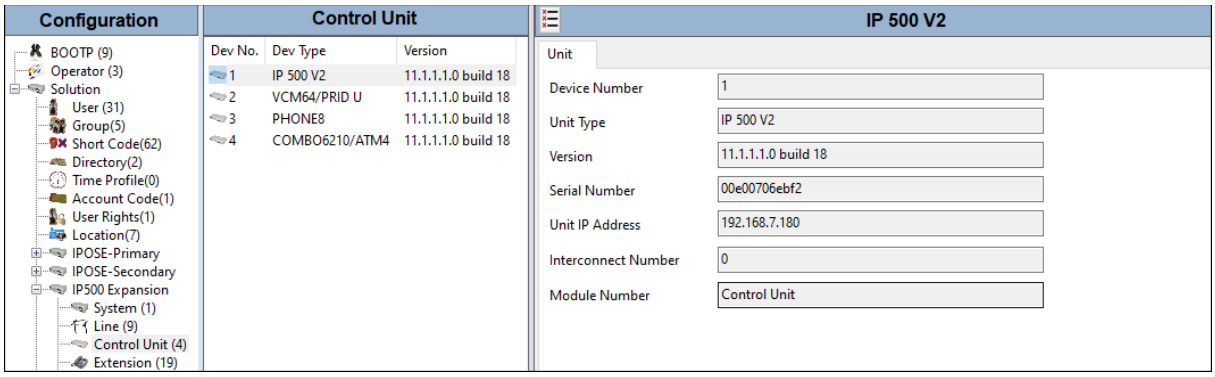
6. Avaya IP Office Expansion Configuration

Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials. Clicking the "plus" sign next to **IP500 Expansion** on the left navigation pane will expand the menu on this server.



6.1. Expansion System - Physical Hardware

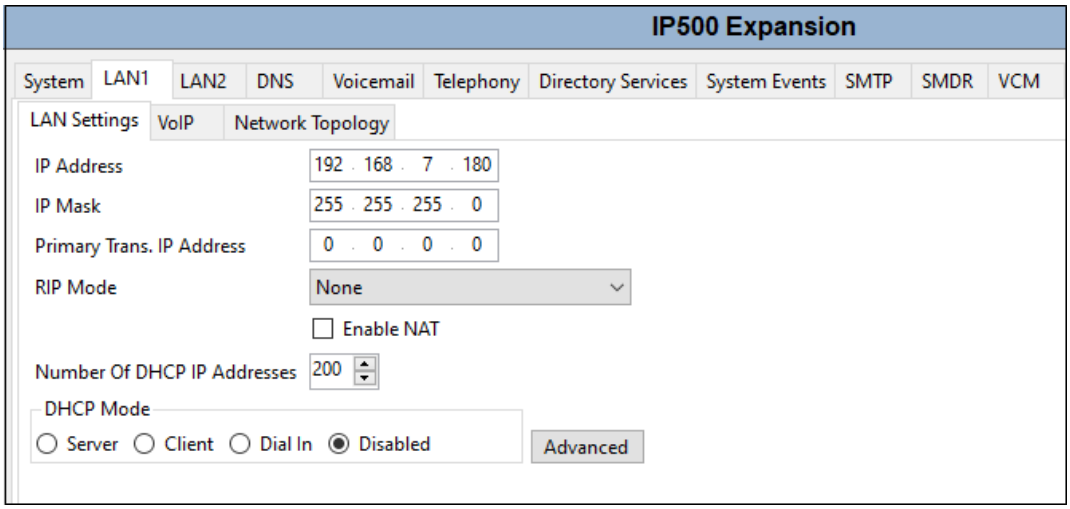
In the sample configuration, the IP500 V2 Expansion System contained a PHONE8 analog card and a COMBO6210 card, for the support of analog and digital stations. Also included is a VCM64 (Voice Compression Module). Both the VCM64 and the COMBO6210 cards provide voice compression channels to the control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



©2022 Avaya Inc. All Rights Reserved.

6.2. Expansion System - LAN Settings

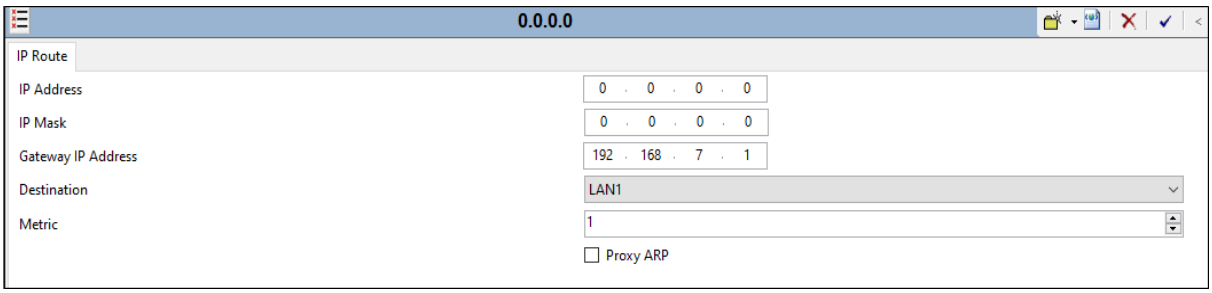
In the sample configuration, LAN1 is used to connect the Expansion System to the enterprise network. To view or configure the LAN1 IP address, select **System** on the Navigation pane. Select the **LAN1 → LAN Settings** tab on the Details pane. As shown in **Figure 1**, the IP Address of the Expansion System is **192.168.7.180**. Other parameters on this screen may be set according to customer requirements



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

6.3. Expansion System - IP Route

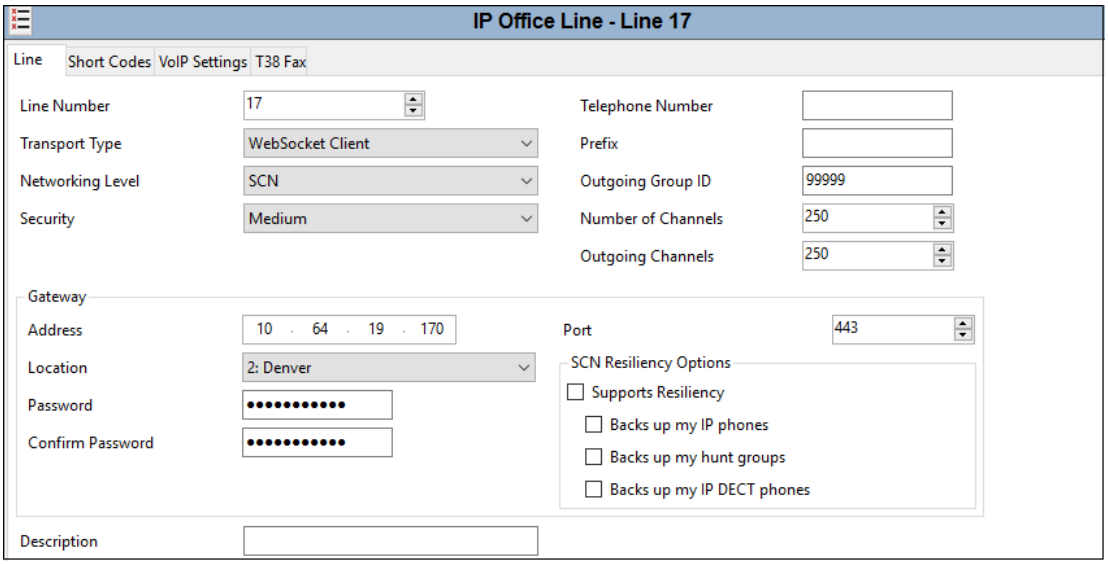
To create an IP route for the Expansion System, right-click on **IP Route** on the left Navigation pane. Select **New** (not shown). The configuration is similar to the one on the Primary server (**Section 5.4**), with the difference that in the reference configuration, the default gateway for the Expansion System is **192.168.7.1**.



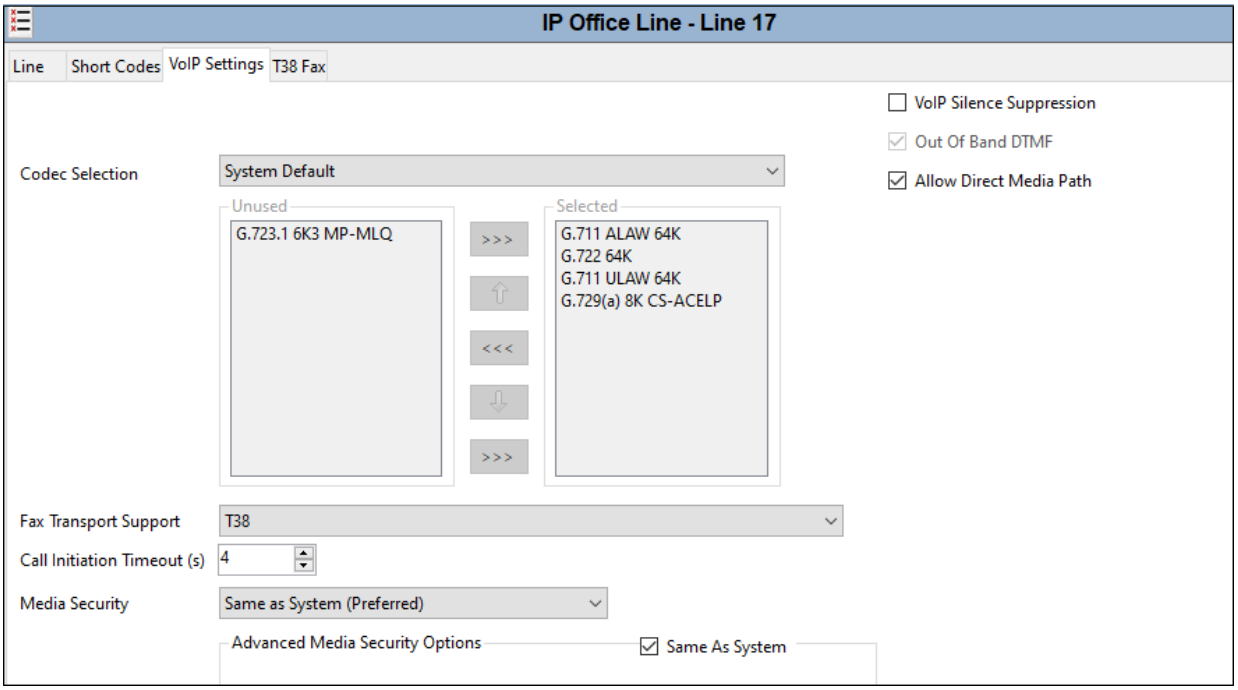
©2022 Avaya Inc. All Rights Reserved.

6.4. Expansion System - IP Office Line

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



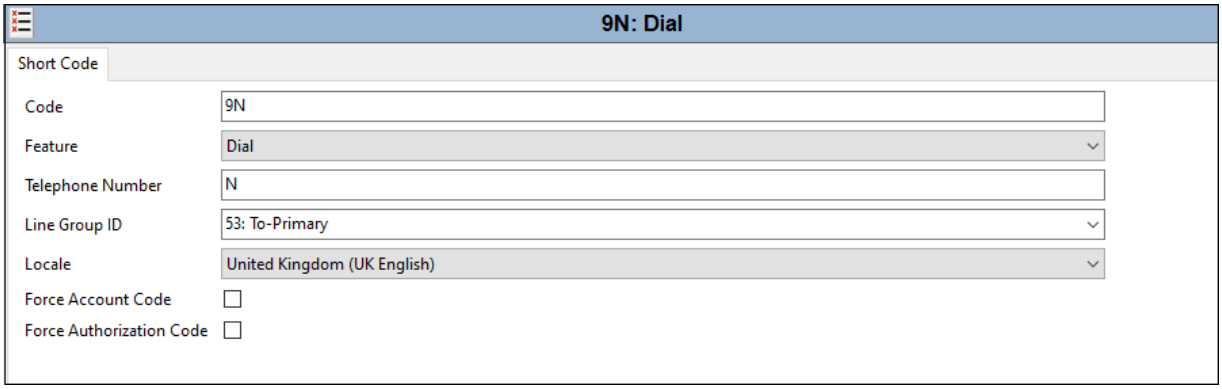
In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. To accommodate T.38 fax, select the **VoIP Settings** tab and set **Fax Transport Support** to **T38**. The **Media Security** drop-down menu is set to "**Same as System (Preferred)**" to have IP Office use the system setting for media security set in **Section 5.3.4**.



©2022 Avaya Inc. All Rights Reserved.

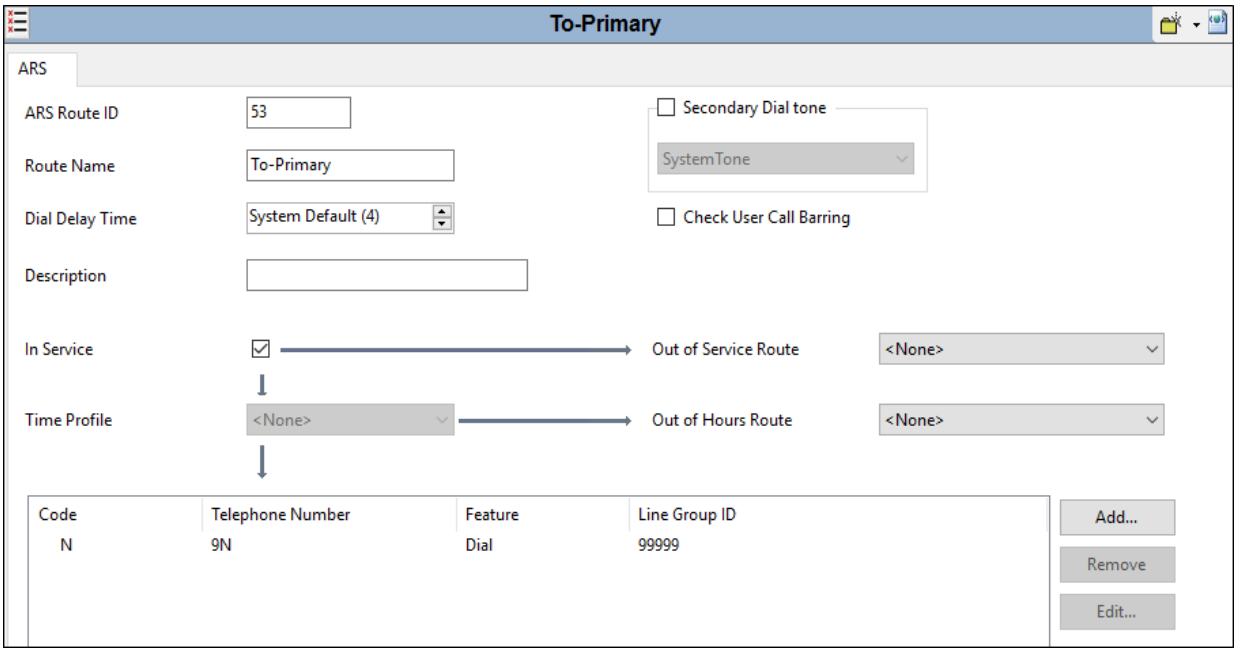
6.5. Expansion System - Short Codes

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



6.6. Expansion System - Automatic Route Selection – ARS

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

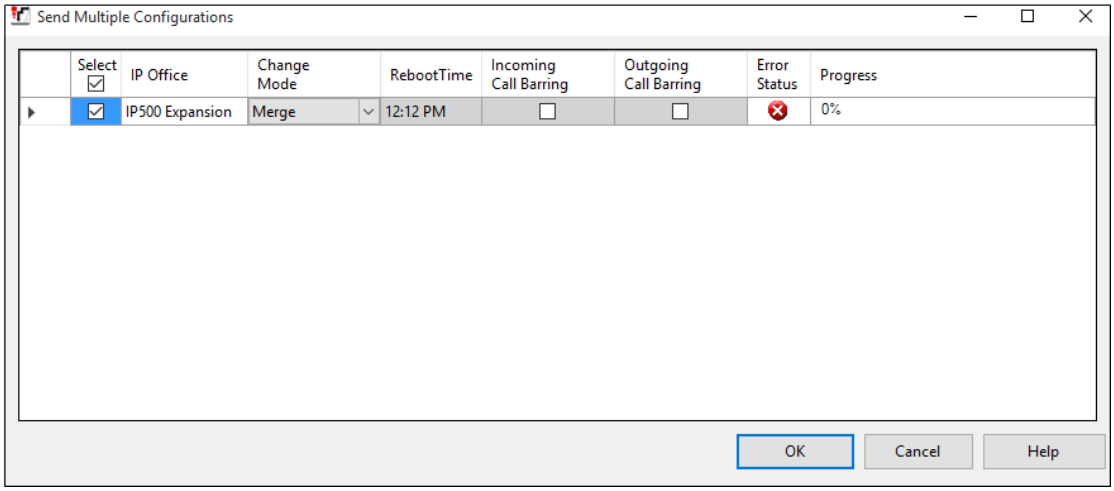


©2022 Avaya Inc. All Rights Reserved.

6.7. Save IP Office Expansion System Configuration

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

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



©2022 Avaya Inc. All Rights Reserved.

7. Configure Avaya Session Border Controller for Enterprise

In the reference configuration, Avaya SBCE in High Availability mode is deployed as the edge device between the CPE and the BT Wholesale Hosted SIP Trunking Service..

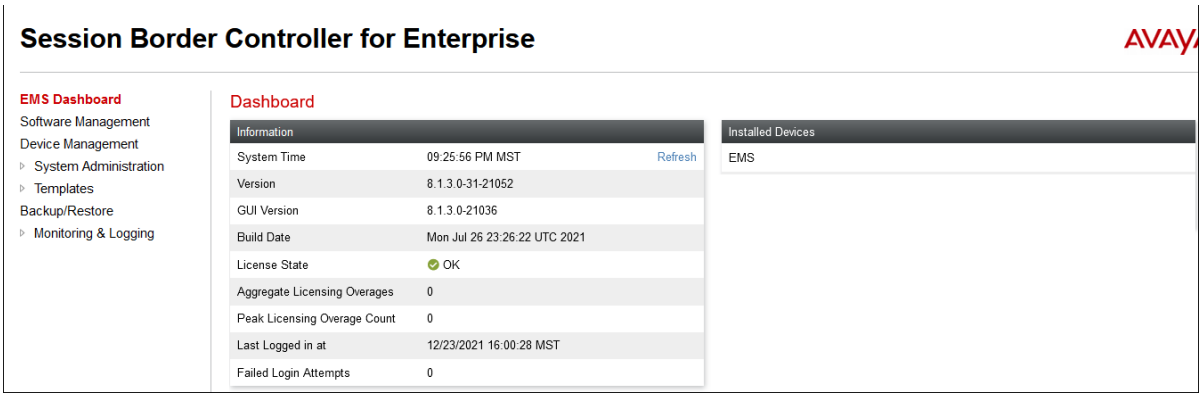
Avaya SBCE HA pairs can be deployed in an enterprise in a parallel mode configuration. In the parallel configuration the signaling packets are routed only to the Active (primary) Avaya SBCE which performs all data processing: the interface ports on the stand-by Avaya SBCE do not process any traffic. The Management interfaces on the Avaya SBCE appliances have different IP addresses, but the signaling/media interfaces have the same IP address.

Note: The SBCE can only be deployed in HA mode if the HA feature is enabled on the license file. If the required feature is not enabled, contact an authorized Avaya sales representative.

This section covers the addition of the Avaya SBCE HA pair to the EMS, and the SBCE configuration via the EMS GUI. It is assumed that the software installation and initial provisioning of the Avaya EMS and SBCE pair of servers, including the assignment of the management interfaces IP Addresses and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

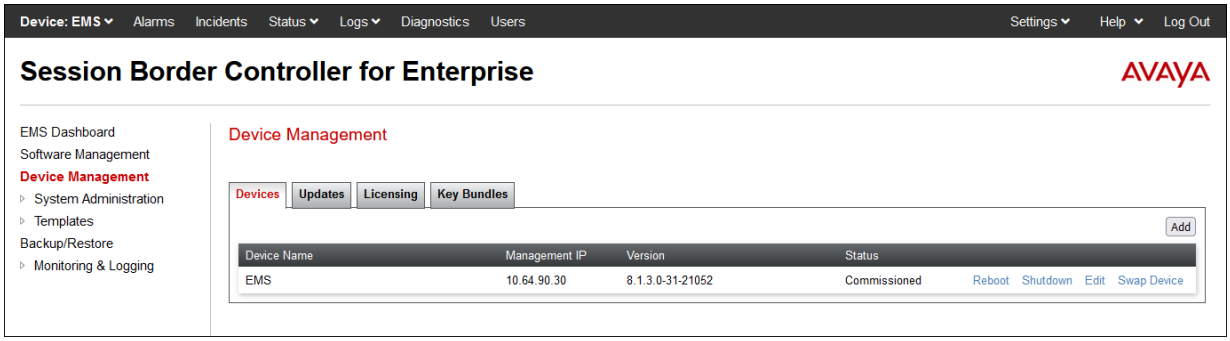
Use a web browser to access the Element Management Server (EMS) web interface and enter https://*ipaddress*/sbc in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE. Log in using the appropriate credentials.

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

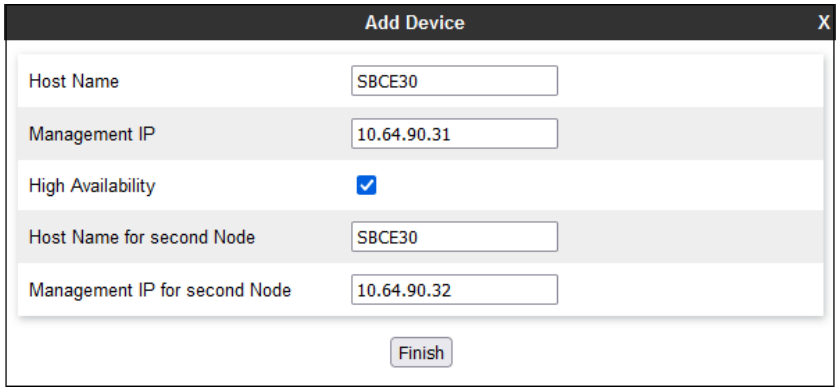


8.1. Add Avaya SBCE devices to EMS

It is assumed that the SBCEs software installation and initial configuration via CLI has already been completed. Consult [**6**] on the References section for details. Select **Device Management** on the left-hand menu, then select **Add.**

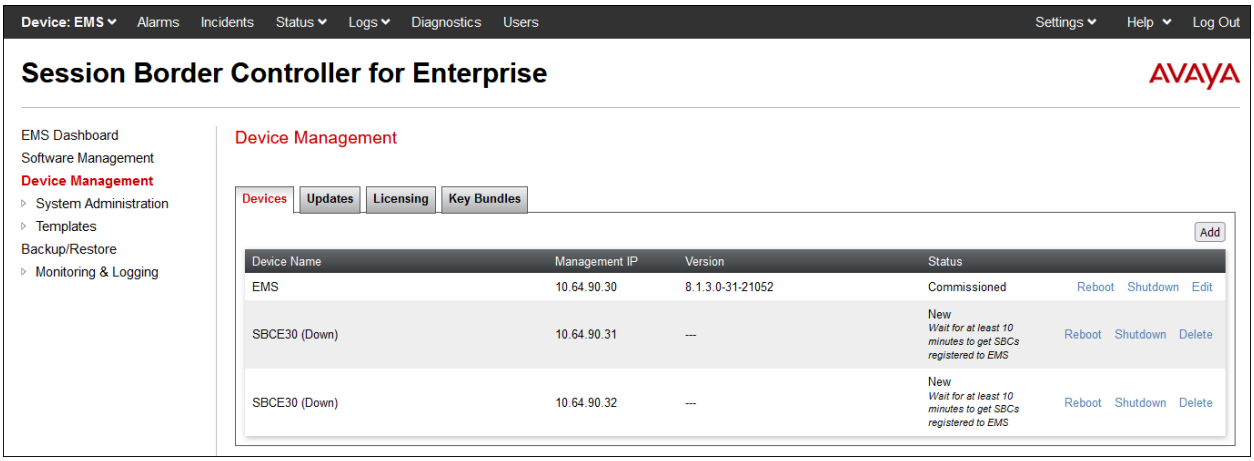


Enter the **Host Name** and **Management IP** addresses of the two Avaya SBCEs in the HA pair. Check the **High Availability** box. Click **Finish**.



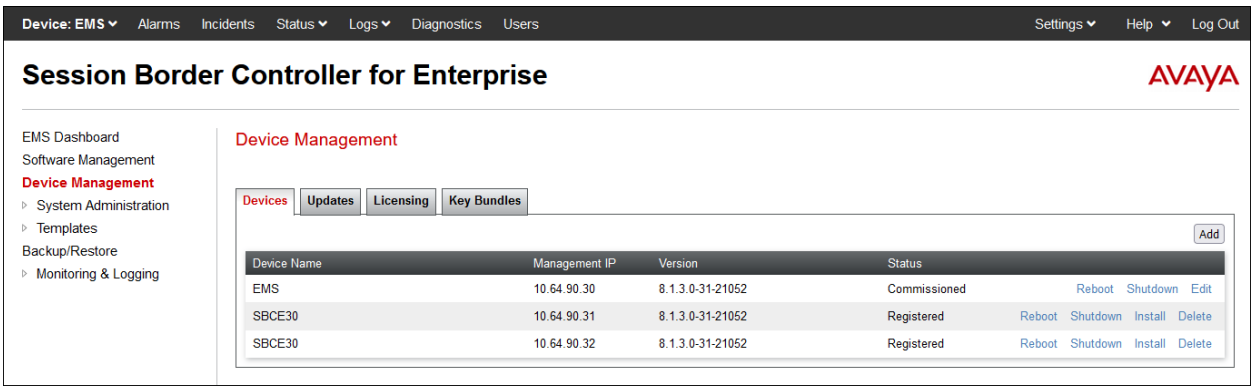
©2022 Avaya Inc. All Rights Reserved.

The newly added SBCEs will appear on the list of devices, with a message under the **Status** column with instructions to wait for the SBCEs to register to the EMS.



8.2. Install Avaya SBCE

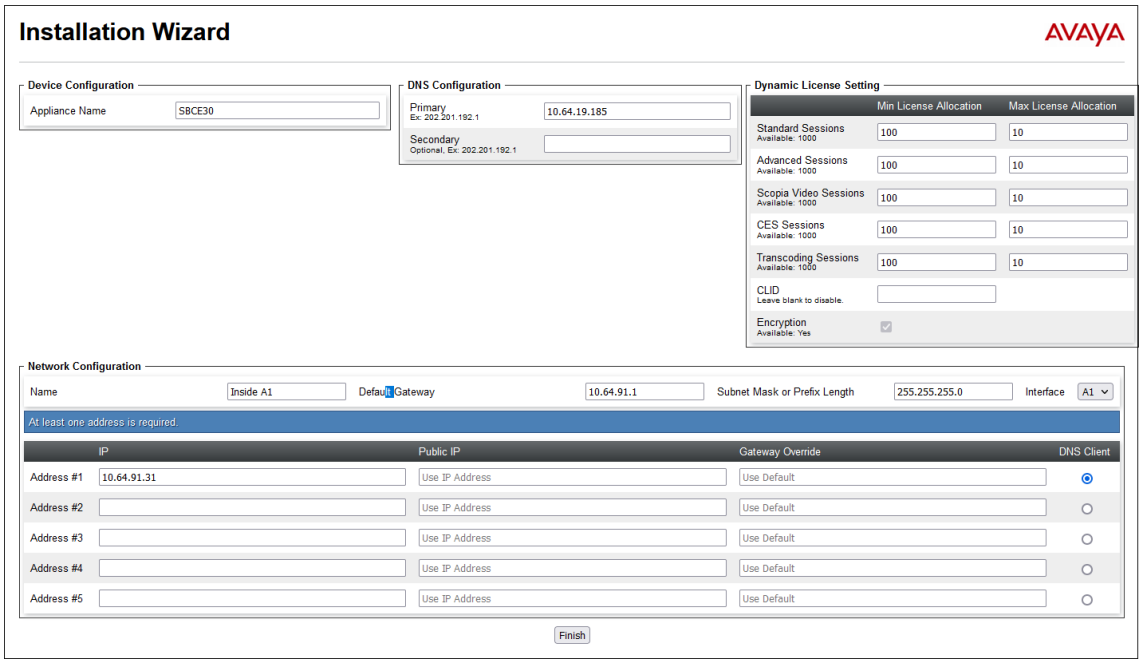
After several minutes, the **Status** column for the SBCEs on the **Device Management** screen should change to **Registered**.



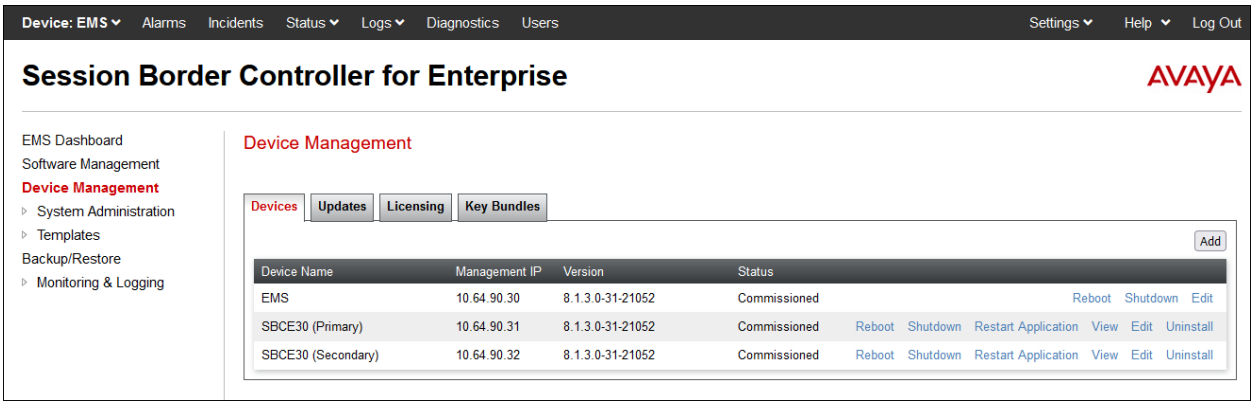
©2022 Avaya Inc. All Rights Reserved.

On the first SBCE device on the list, select **Install**. The **Installation Wizard** screen will appear. Enter the **Appliance Name**, the DNS Server under **DNS Configuration**, and the minimum and maximum licenses allocated to the SBCE under the **Dynamic License Settings**.

On the **Network Configuration** section, enter the settings for at least one of the interfaces of the SBCE. In the example below, the **Inside A1** network is configured on interface **A1**. The IP address is set to **10.64.91.31**. Click **Finish**.



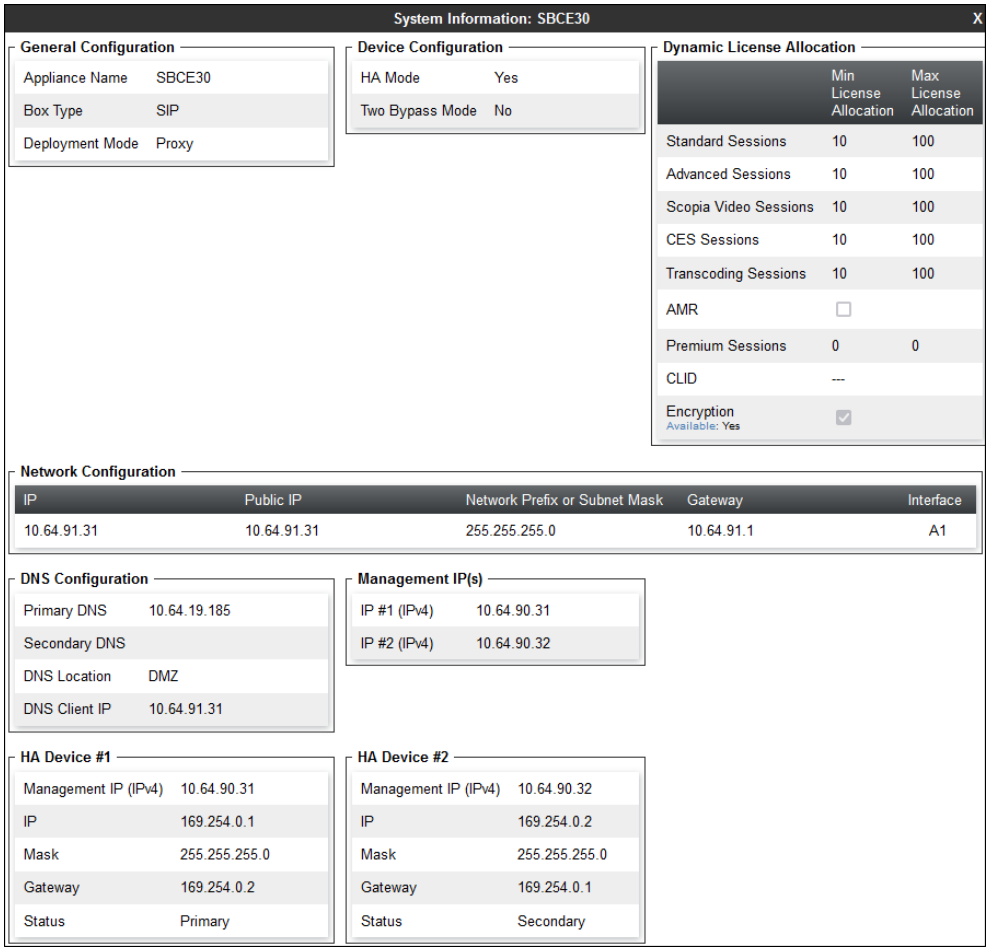
The **Status** column for the SBCE pair should change to **Commissioned**. Also, **Primary** and **Secondary** should appear next to the SBCE **Device Name**, indicating if the SBCE is currently active or standby. To view the configuration of the SBCE devices, click **View** on one of the SBCEs on the screen below.



©2022 Avaya Inc. All Rights Reserved.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information previously provided. On the **Device Configuration** area, **HA Mode** is set to **Yes**. Under **Network Configuration**, the interface **A1** is used to connect the SBCE to the internal enterprise private network. The interface **B1** used to connect to the external network and the SIP trunk to BT will be defined later on **Section 8.4**. Note that the two SBCE HA appliances will share the same IP addresses for signaling and media on interfaces **A1** and **B1**.

At the bottom of the screen, the specific IP configuration for the two HA devices and current status is show. In the example, IP addresses **10.64.90.31** and **10.64.90.32** correspond to the Management Interface **M1** on each SBCE. IP addresses **169.254.0.1** and **169.254.0.2** are automatically assigned during installation, and correspond to interface **M2** on each SBCE, used for the layer 2 HA link between the two servers.



On the **Dynamic License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

©2022 Avaya Inc. All Rights Reserved.

8.3. TLS Management

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

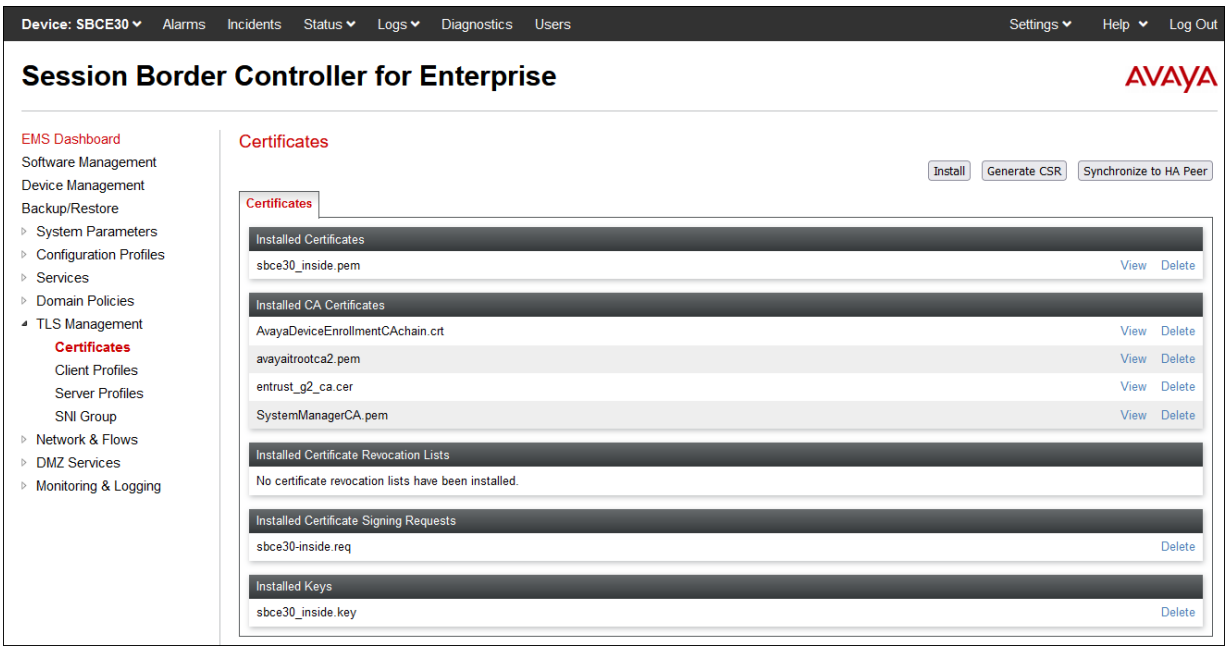
Note – Testing was done using identity certificates signed by a local certificate authority. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

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

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

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

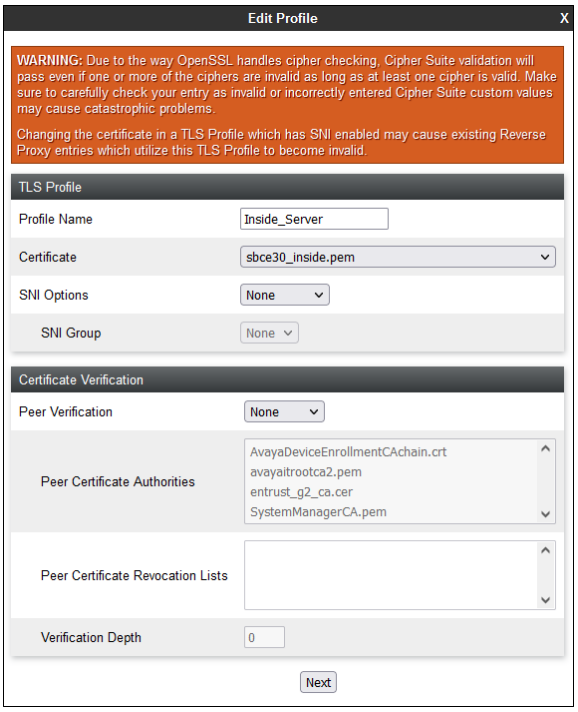
Select **TLS Management → Certificates** from the left-hand menu. Verify the root CA certificate is present in the **Installed CA Certificates** area. The signed identity certificate is present in the **Installed Certificates** area. The private key associated with the identity certificate is present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



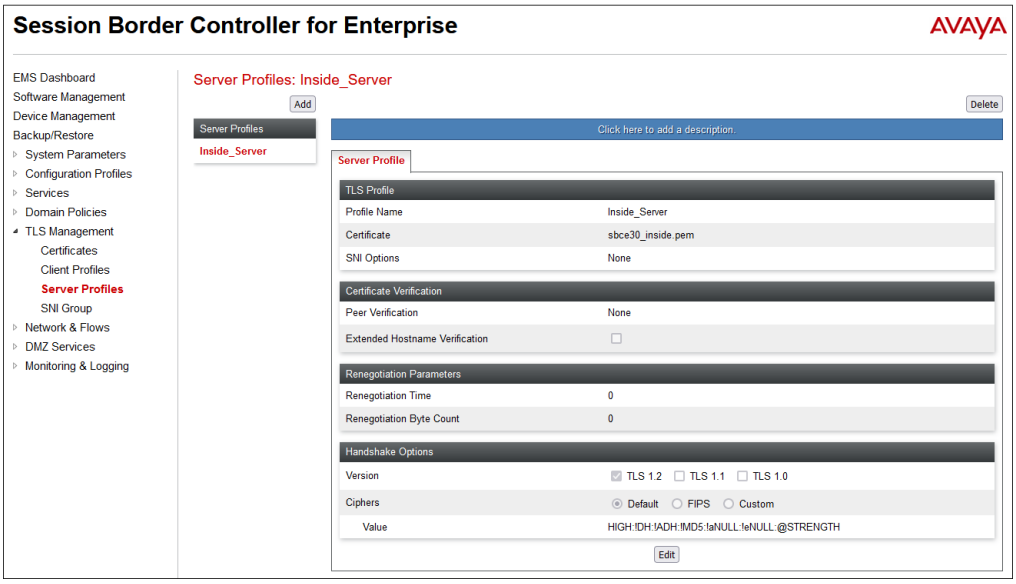
©2022 Avaya Inc. All Rights Reserved.

8.3.2. Server Profiles

Navigate to **TLS Management → Server Profiles** and click the **Add** button to add a new profile or select an existing profile. Enter a descriptive **Profile Name** such as **Inside_Server** show below. Select the Avaya SBCE identity certificate for the inside interface from the **Certificate** drop-down menu. In the reference configuration this is **sbce30_inside.pem**. Select **None** from the **Peer Verification** drop-down menu. Click **Next** and accept default values for the next screen, then click **Finish** (not shown).



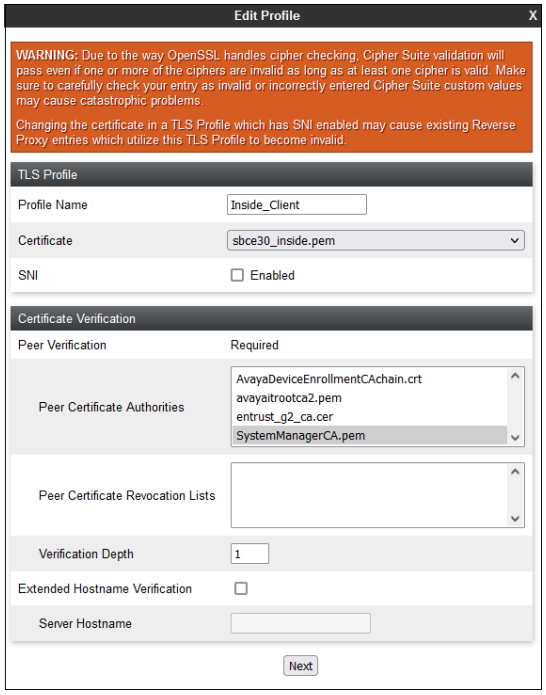
The following screen shows the completed TLS **Server Profile** form:



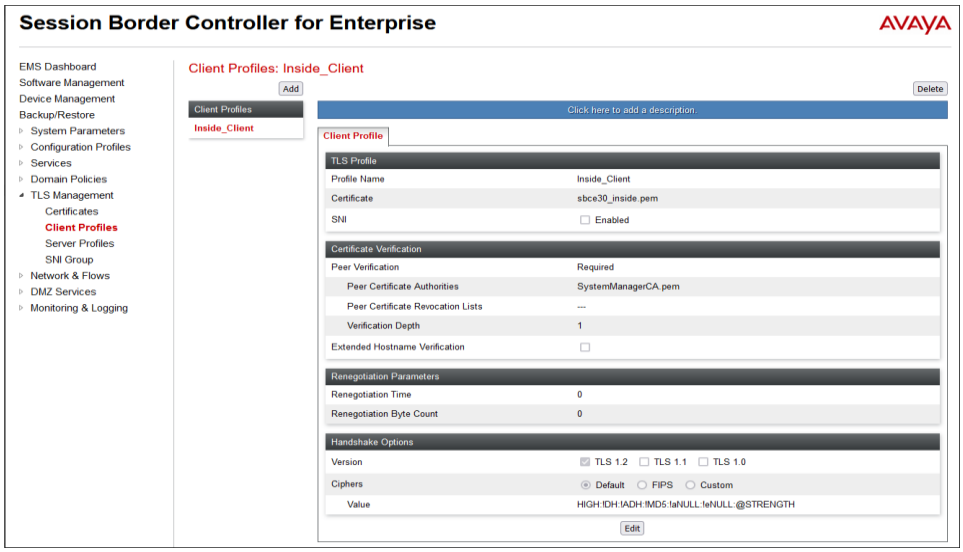
©2022 Avaya Inc. All Rights Reserved.

8.3.3. Client Profiles

Navigate to **TLS Management → Client Profiles** and click the **Add** button to add a new profile or select an existing profile. Enter a descriptive **Profile Name**, such as **Inside_Client** show below. Select the identity certificate from the **Certificate** drop-down menu. In the reference configuration this is **sbce30_inside.pem**. The **Peer Certificate Authorities** field is set to the root certificate used to verify the IP Office certificate, e.g., **SystemManagerCA.pem**. The **Verification Depth** field is set to **1**. Click **Next** and accept default values for the next screen and click **Finish** (not shown).



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

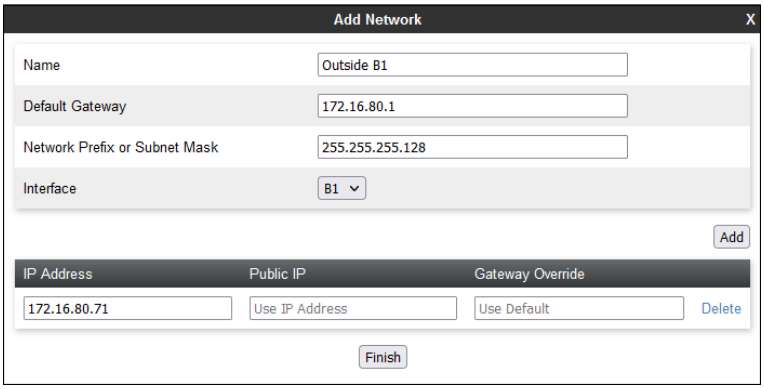


©2022 Avaya Inc. All Rights Reserved.

8.4. Network Management

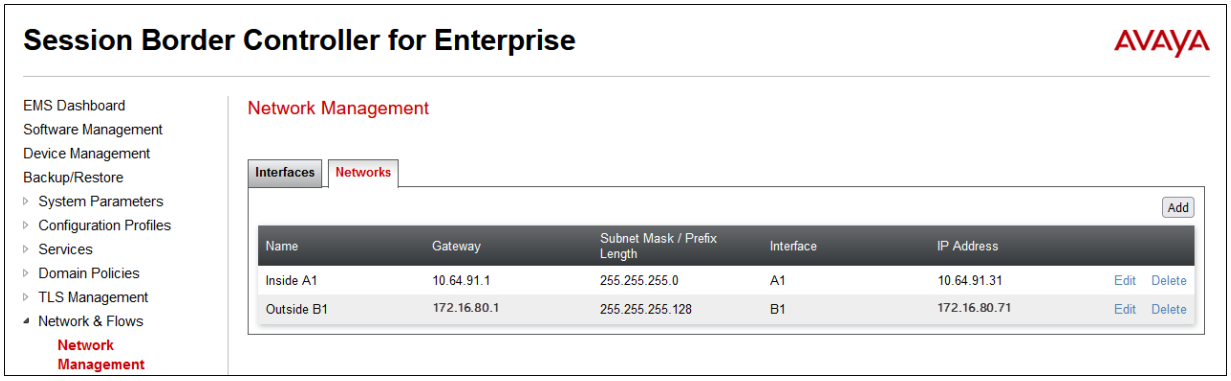
The Network Management screen is where the network interface settings are configured and enabled. Some of these values are specified during installation. Navigate to **Networks & Flows → Network Management** from the menu on the left-hand side. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 and B1 are used.

On the **Networks** tab, select **Add** to enter the settings for the B1 interface.



The screen below shows the network settings used in the reference configuration. These settings can be modified by selecting **Edit**; however, some of these values may not be changed if associated provisioning is in use.

- **A1**: **10.64.91.31** – "Inside" IP address, toward IP Office.
- **B1: 172.16.80.71** – "Outside" IP address toward the BT SIP trunk.



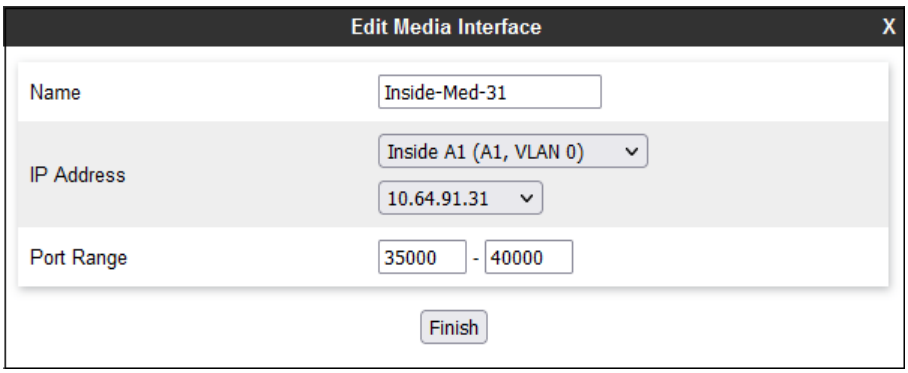
©2022 Avaya Inc. All Rights Reserved.

8.5. Media Interfaces

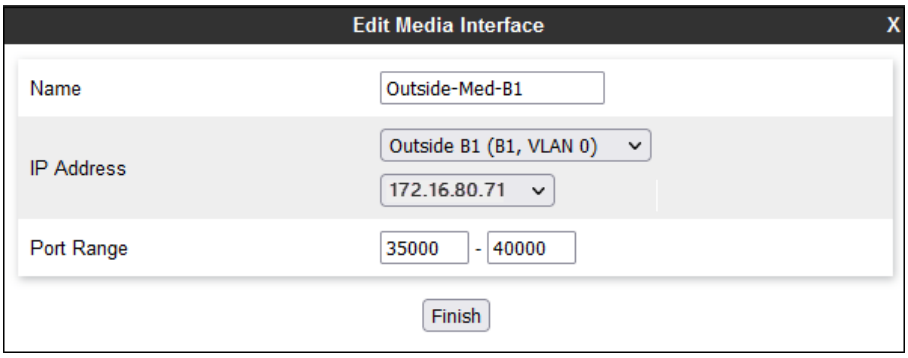
Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which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

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

The screen below shows the **Inside-Med-31** Media Interface created toward the IP Office. On the **IP Address** drop-down menus, **Inside-A1 (A1,VLAN0)** and **10.64.91.31** are selected. Default **Port Range** values are used.



The screen below shows the **Outside-Med-B1** Media Interface created toward BT. On the **IP Address** drop-down menus, **Outside-B1 (B1,VLAN0)** and **172.16.80.71** are selected. Default **Port Range** values are used.



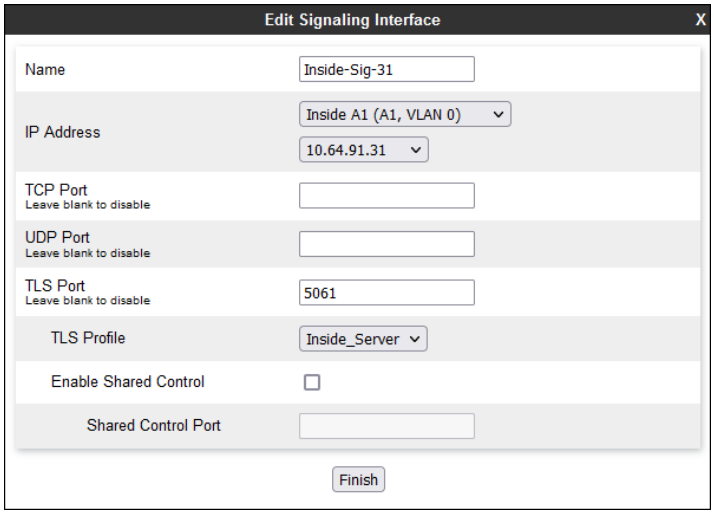
©2022 Avaya Inc. All Rights Reserved.

8.6. Signaling Interfaces

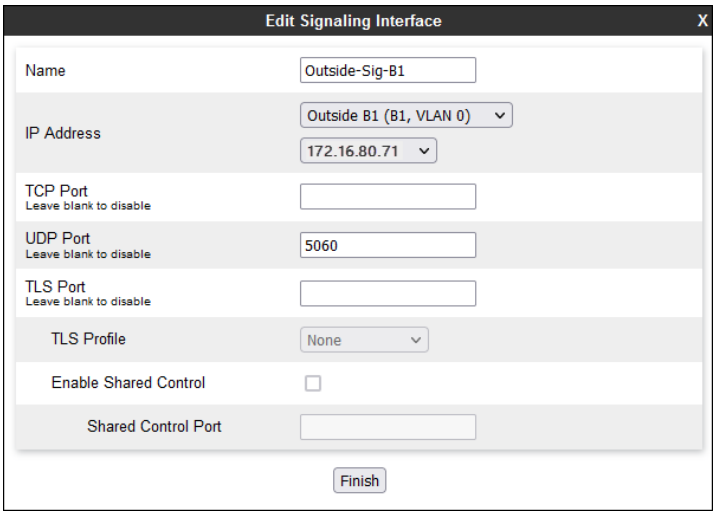
The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces.

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

The screen below shows the **Inside-Sig-31** Signaling Interface created toward the IP Office. On the **IP Address** drop-down menus, **Inside-A1 (A1,VLAN0)** and **10.64.91.31** are selected. **TLS Port 5061** is used. The TLS server profile created in **Section 8.3.2** (e.g., **Inside_Server**) is selected on the TLS Profile drop-down menu.



The screen below shows the **Outside-Sig-B1** Signaling Interface created toward BT. On the **IP Address** drop-down menus, **Outside-B1 (B1,VLAN0)** and **172.16.80.71** are selected. **UDP Port 5060** is used.



©2022 Avaya Inc. All Rights Reserved.

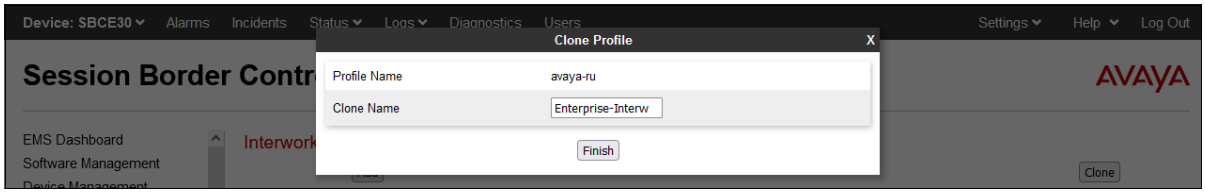
8.7. Server Interworking Profile

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

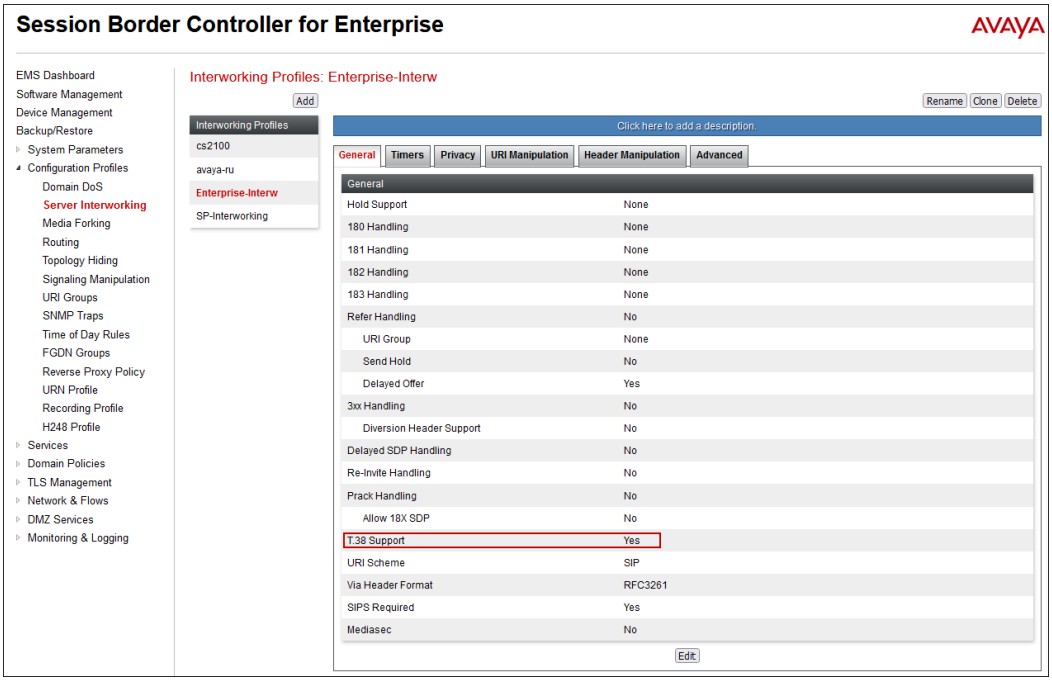
In the reference configuration, separate Server Interworking Profiles were created for IP Office and the BT Wholesale Hosted SIP Trunking service.

8.7.1. Server Interworking Profile – IP Office

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



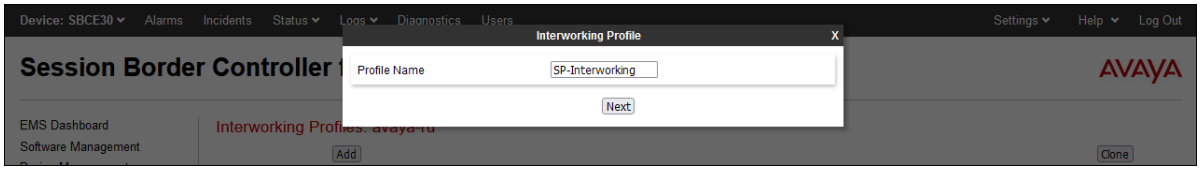
The following screen shows the **Enterprise-Interwk** profile used in the reference configuration, with **T.38 Support** set to **Yes**. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish**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



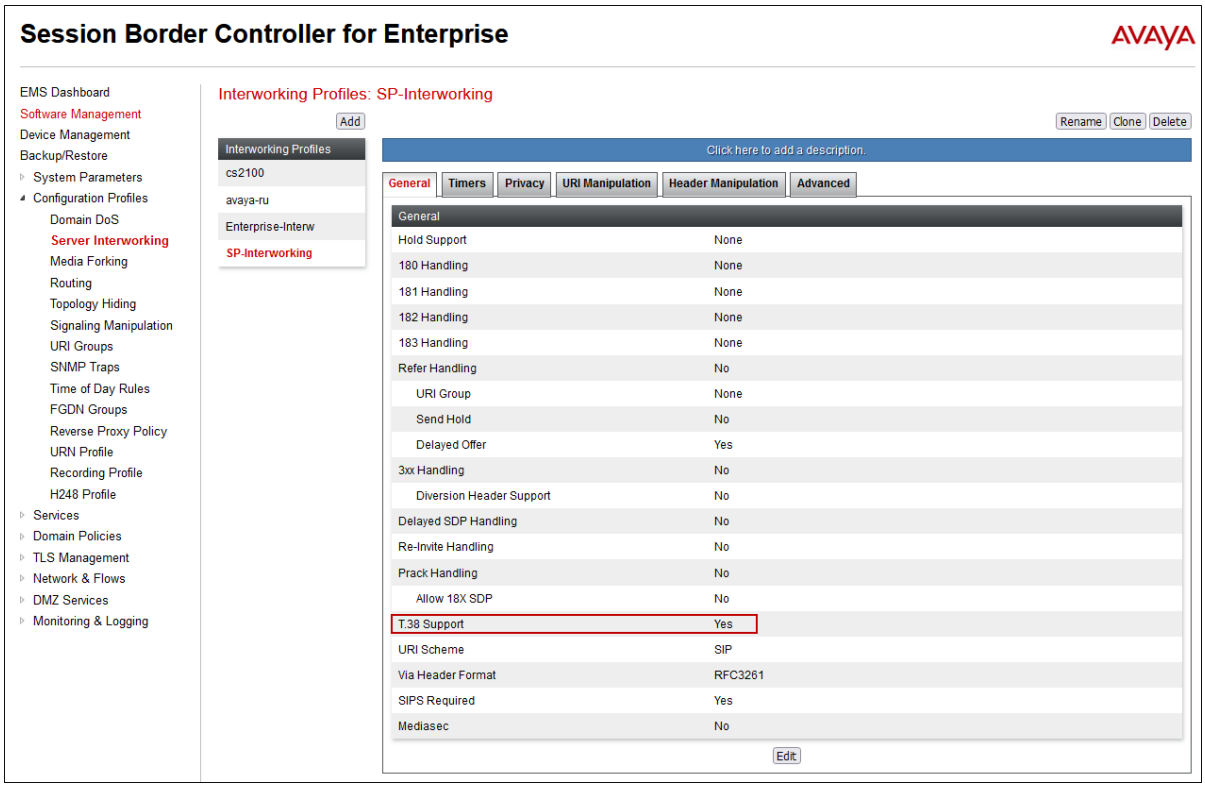
©2022 Avaya Inc. All Rights Reserved.

8.7.2. Server Interworking Profile – Service Provider

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

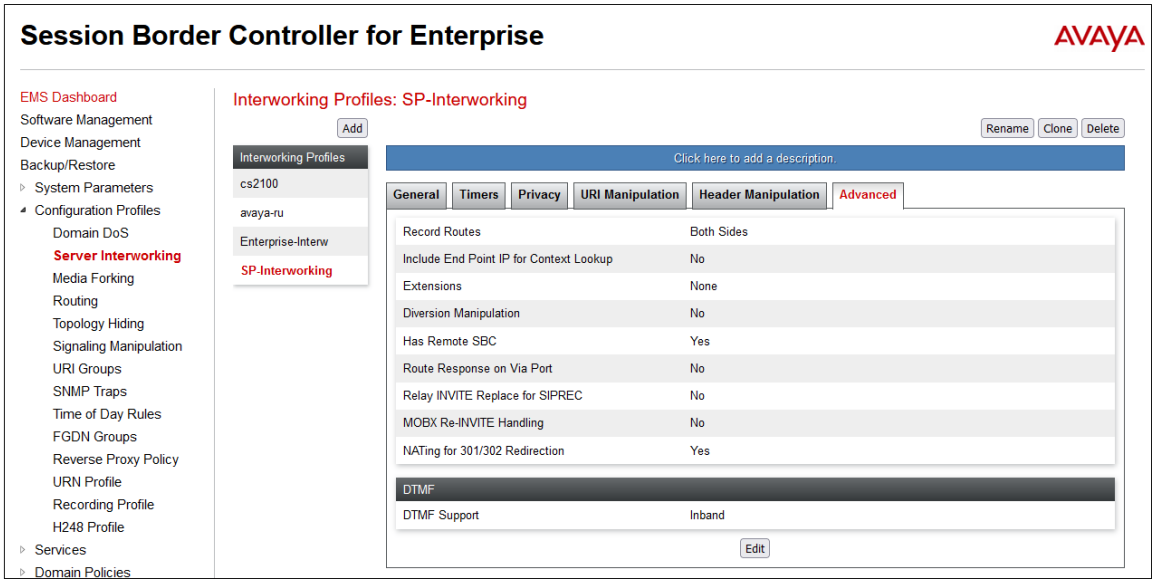


The following screens show the **SP-Interworking** profile used in the reference configuration. On the **General** tab, default values are used with the exception of **T.38 Support** which is set to **Yes**.



©2022 Avaya Inc. All Rights Reserved.

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



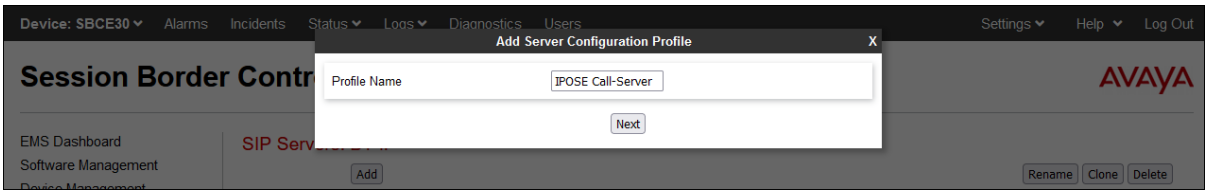
©2022 Avaya Inc. All Rights Reserved.

8.8. SIP Server Profiles

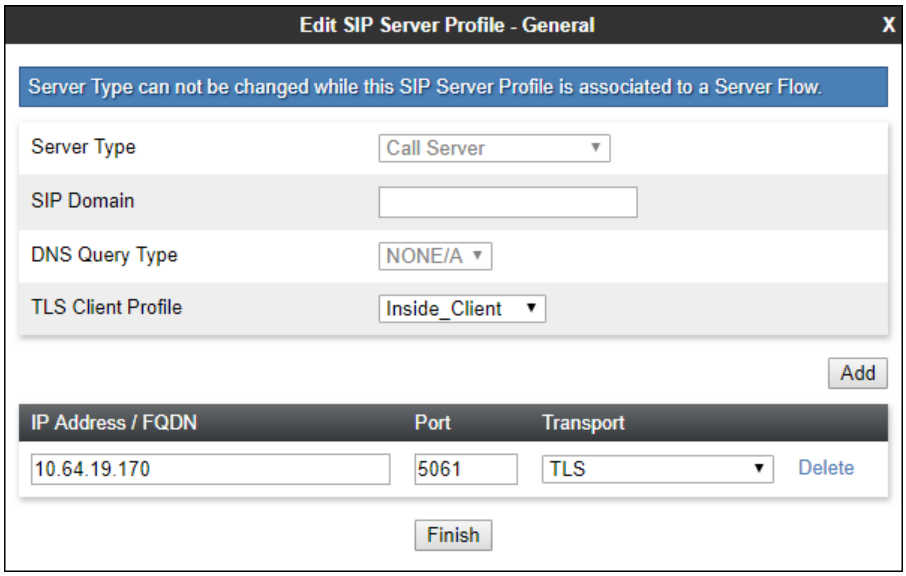
The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

8.8.1. SIP Server Profile – IP Office

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

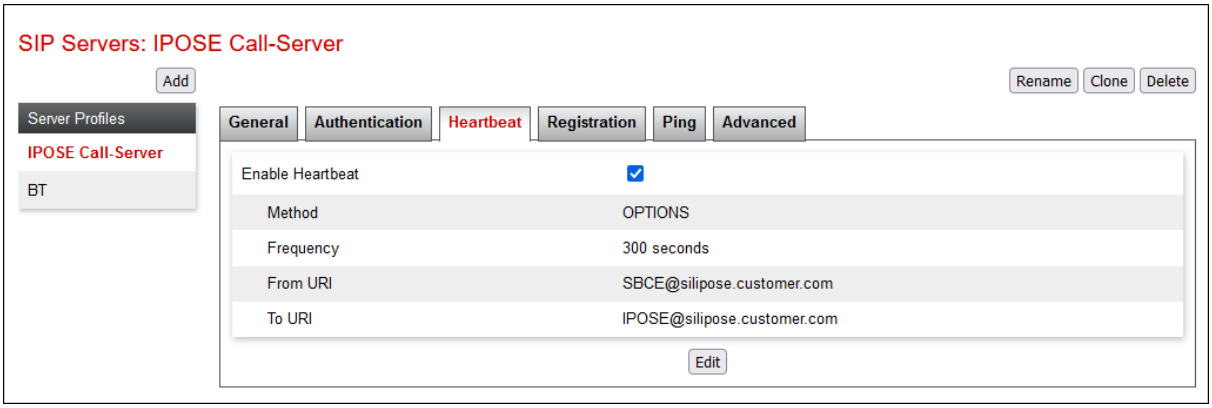


The following screen illustrate the SIP Server Profile named **IPOSE Call-Server**. In the **General** parameters, the **Server Type** is set to **Call Server**. In the **IP Address / FQDN** field, the IP Address of IP Office LAN 1 interface in the sample configuration is entered. This IP address is **10.64.19.170**. Under **Port**, **5061** is entered, and the **Transport** parameter is set to **TLS**. The TLS profile **Inside_Client** created in **Section 8.3.3** is selected for **TLS Client Profile**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

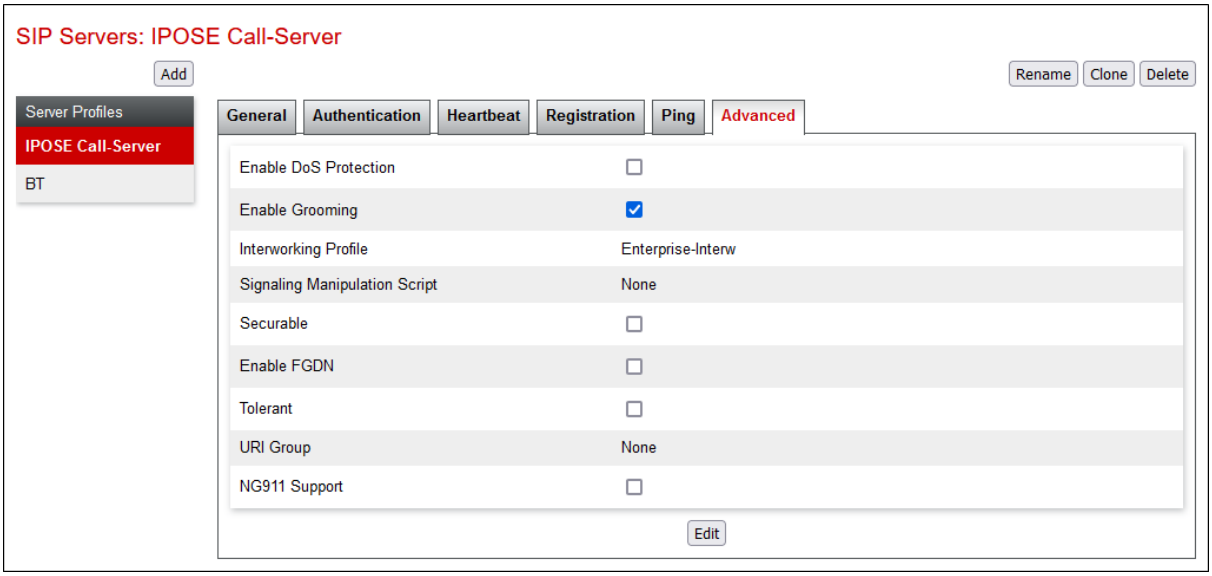


©2022 Avaya Inc. All Rights Reserved.

Default values can be used on the **Authentication** tab. Click **Next** (not shown) to proceed to the **Heartbeats** tab. The Avaya SBCE can be configured to source "heartbeats" in the form of PINGs or SIP OPTIONS towards IP Office. Check the **Enable Heartbeat** box and select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE.



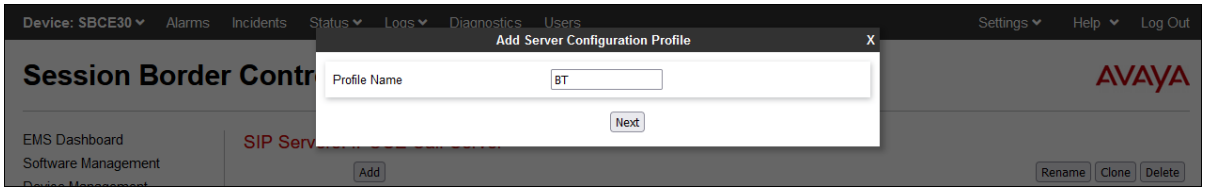
On the **Advanced** tab, select the **Enable Grooming** checkbox. The **Interworking Profile** is set to the **Enterprise-Interwk** profile created in **Section 8.7.1** for IP Office.



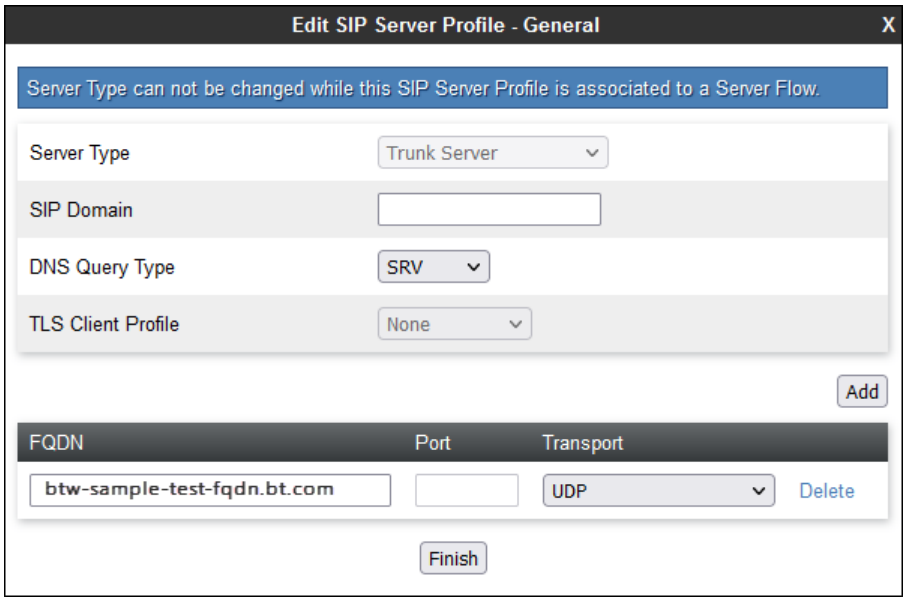
©2022 Avaya Inc. All Rights Reserved.

8.8.2. SIP Server Profile – Service Provider

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

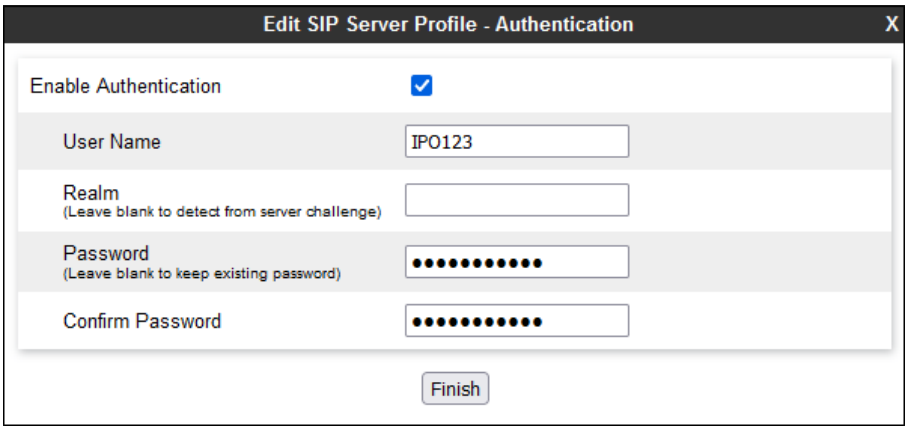


The following screens illustrate the SIP Server Profile named **BT**. In the **General** parameters, the **Server Type** is set to **Trunk Server**. The **DNS Query Type** is set to **SRV**. In the **IP Address / FQDN** field, the BT-provided SIP proxy server FQDN is entered. In the example below, this is **btw-sample-test-fqdn.bt.com**. The **Transport** parameter is set to **UDP**. Note that the **Port** field is grayed out, since the port number is discovered via the DNS SRV query. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

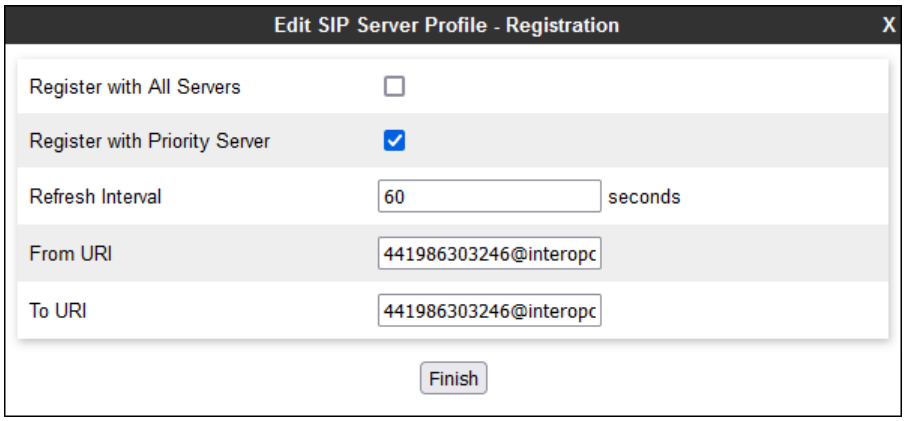


©2022 Avaya Inc. All Rights Reserved.

On the **Authentication** tab, the **Enable Authentication** box is checked. On the **User Name** and **Password** fields, **e**nter the credential information provided by BT for the SIP trunk registration. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

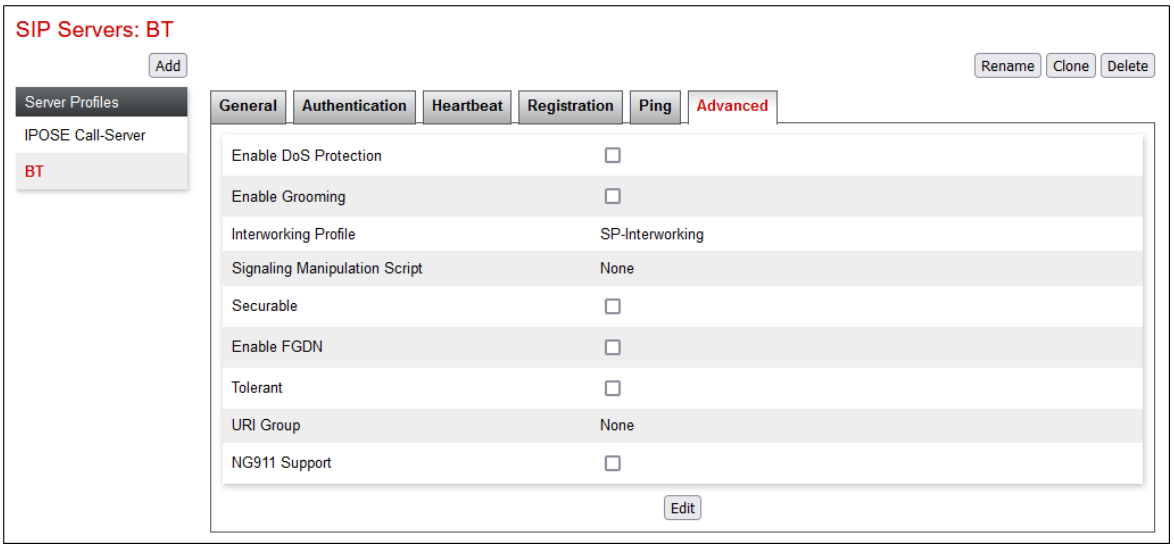


No changes are made on the **Heartbeat** tab (not shown). On the **Registration** tab, check the **Register with Priority Server** box. Under **Refresh Interval**, enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with BT. **60** seconds was the value used during the compliance test. The **From URI** and **To URI** entries for the REGISTER messages are built using the pilot number and domain name assigned by BT to the SIP trunk. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



©2022 Avaya Inc. All Rights Reserved.

On the **Advanced** tab, **Enable Grooming** is not used for UDP connections and is left unchecked. The **Interworking Profile** is set to the **SP-Interworking** profile created in **Section 8.7.2** for BT.



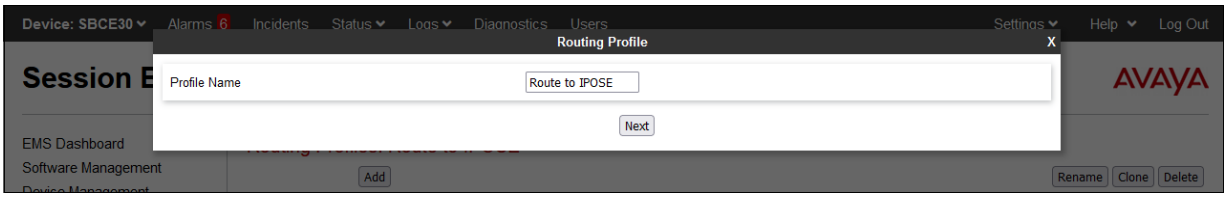
©2022 Avaya Inc. All Rights Reserved.

8.9. Routing Profiles

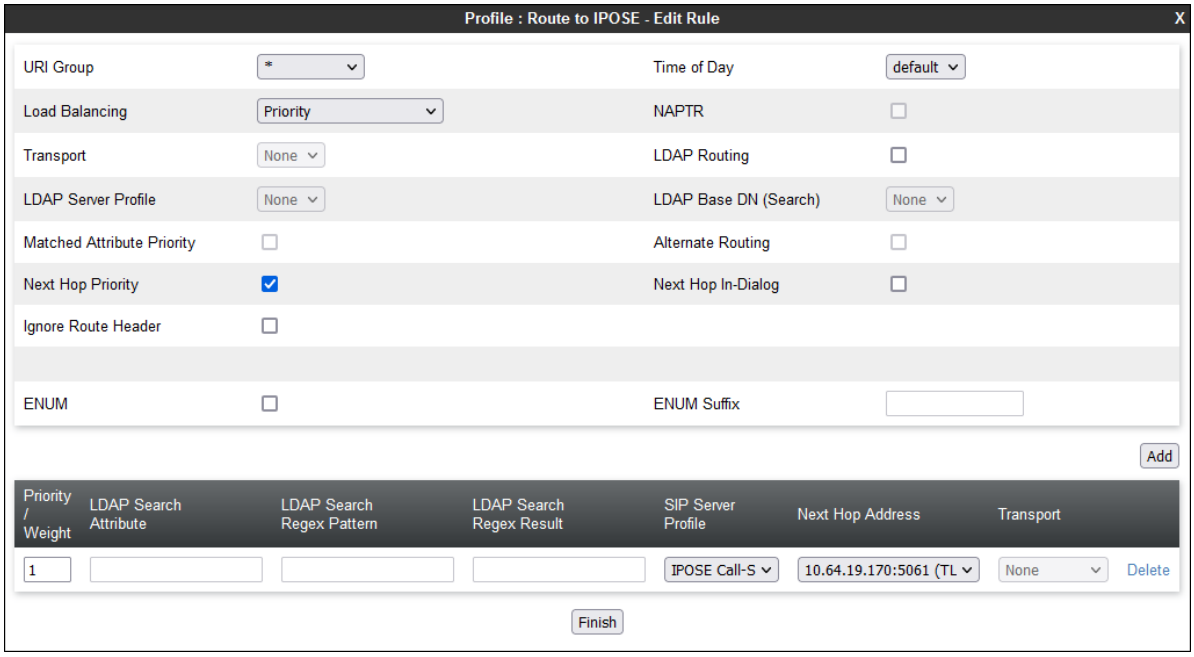
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

8.9.1. Routing Profile – IP Office

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



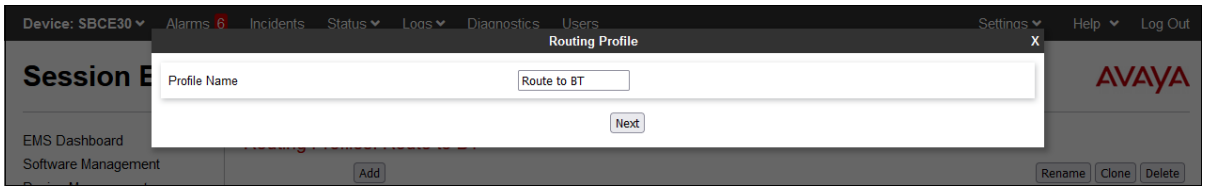
The following screen shows the Routing Profile R**oute to IPOSE** created in the reference configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to **1**, and the IP Office **SIP Server Profile**, created in **Section 8.8.1**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the SIP Server Profile, and **Transport** becomes greyed out. Click **Finish**.



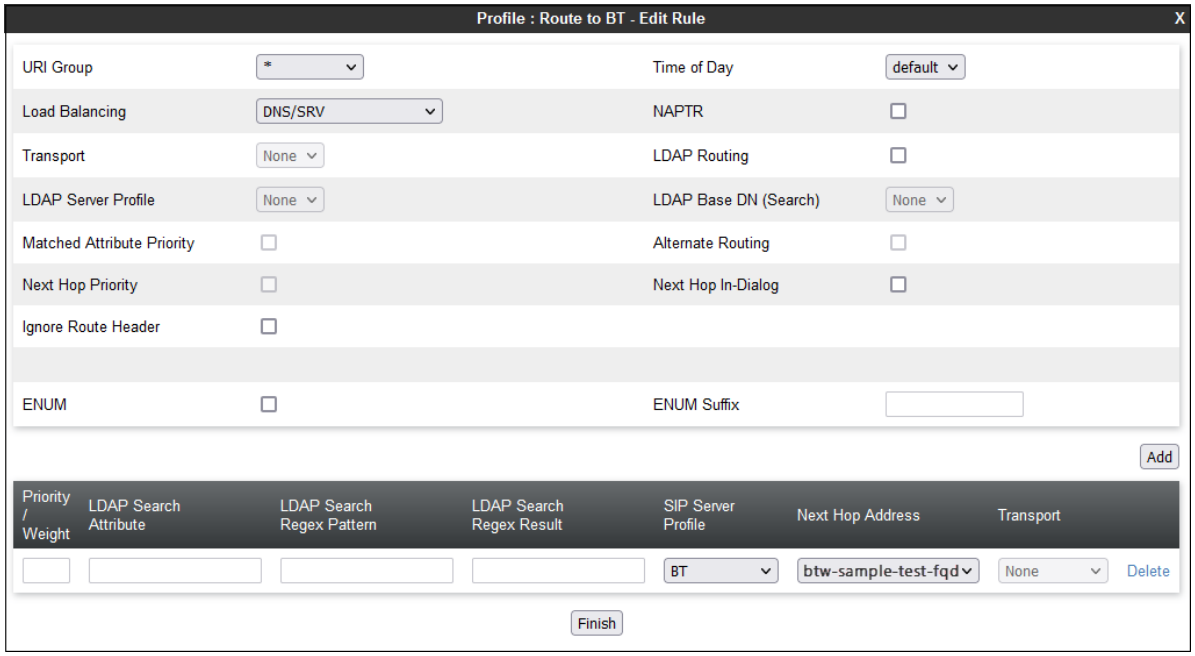
©2022 Avaya Inc. All Rights Reserved.

8.9.2. Routing Profile – Service Provider

Similarly add a Routing Profile to the BT Wholesale Hosted SIP Trunking Service.



The following screen shows the Routing Profile **Route to BT** created in the reference configuration. In the top portion of the profile, the **Load Balancing** parameter is set to **DNS/SRV**. Under **SIP Server Profile**, the **BT** profile, created in **Section 8.8.2**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the SIP Server Profile, and **Transport** becomes greyed out. Click **Finish**.



©2022 Avaya Inc. All Rights Reserved.

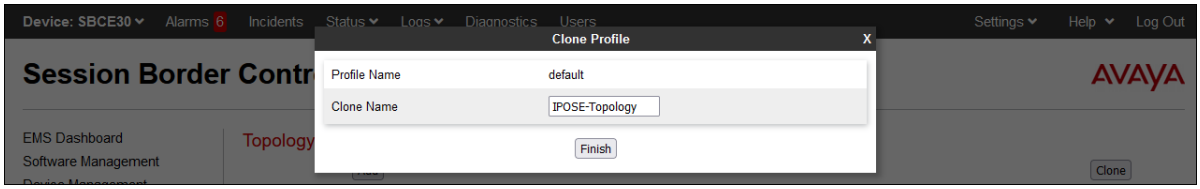
8.10. Topology Hiding Profile

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.

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

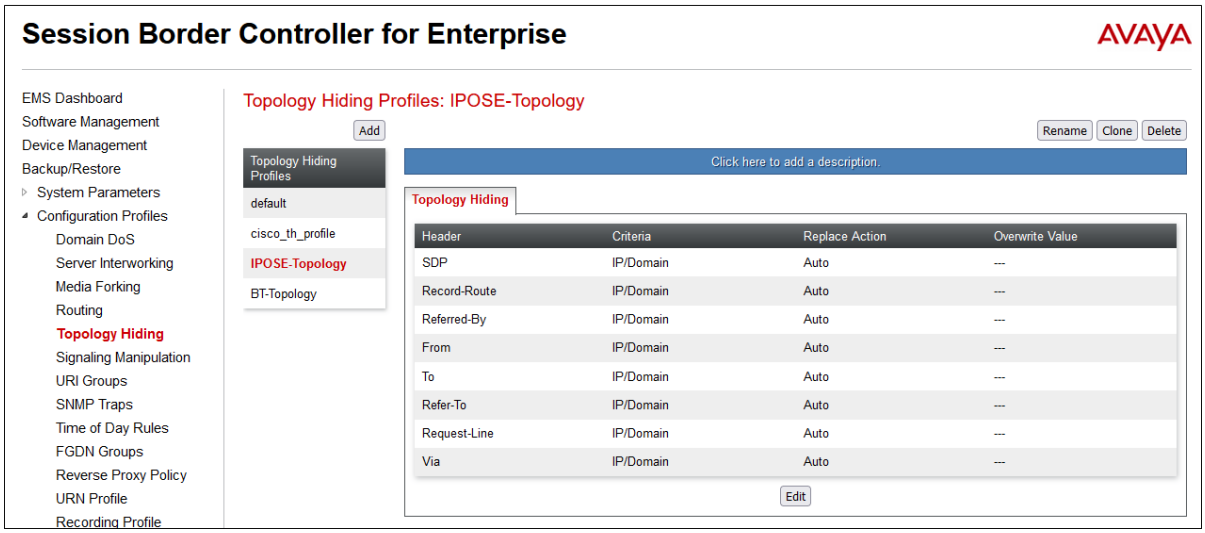
8.10.1. Topology Hiding – IP Office

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



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

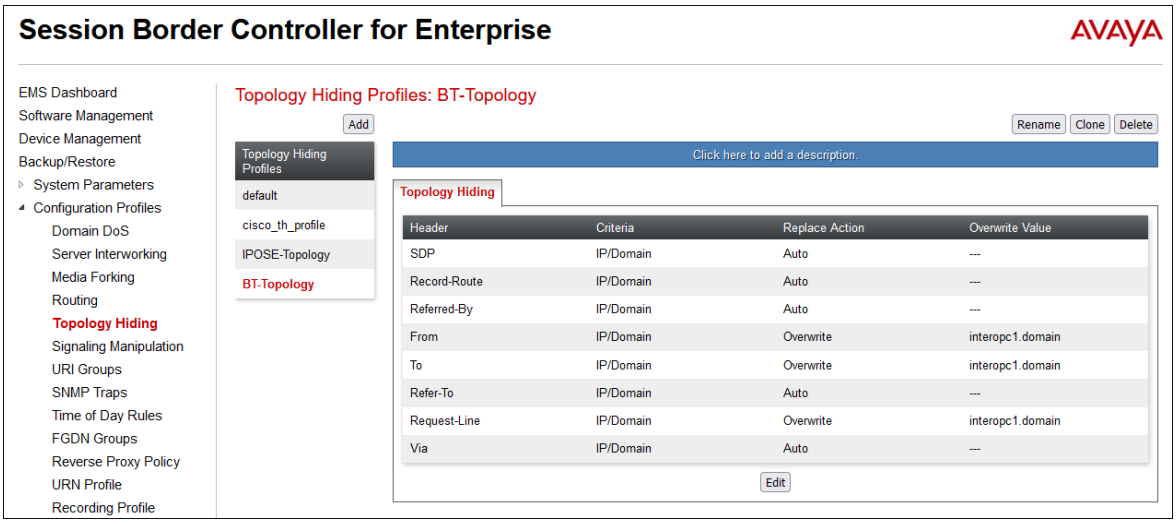
For the **IPOSE-Topology** profile, the **Replace Action** field was left at the default **Auto** for all headers.



©2022 Avaya Inc. All Rights Reserved.

8.10.2. Topology Hiding – Service Provider

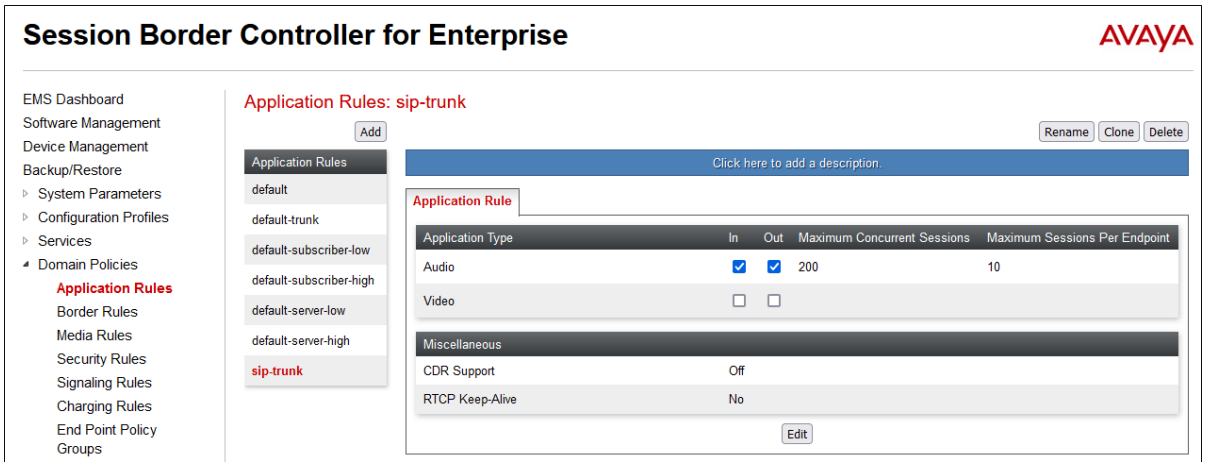
Similarly create a Topology Hiding profile for the Avaya SBCE connection to BT. Enter a Profile Name (e.g., **BT Topology**). For the **Request-Line**, **To** and **From** headers, **Overwrite** is selected under the **Replace Action** column. The domain used by the service provider on the SIP trunk (e.g., **interopc1.domain**) is entered on the **Overwrite Value** field.



8.11. Application Rules

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

Select **Domain Policies → Application Rules** from the left-side menu as shown below. Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the reference configuration, the **sip-trunk** profile was created for IP Office and BT. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** application to a value slightly larger than the licensed sessions. For example, if licensed for 150 sessions set the values to **200**. The **Maximum Session Per Endpoint** was set to **10**.



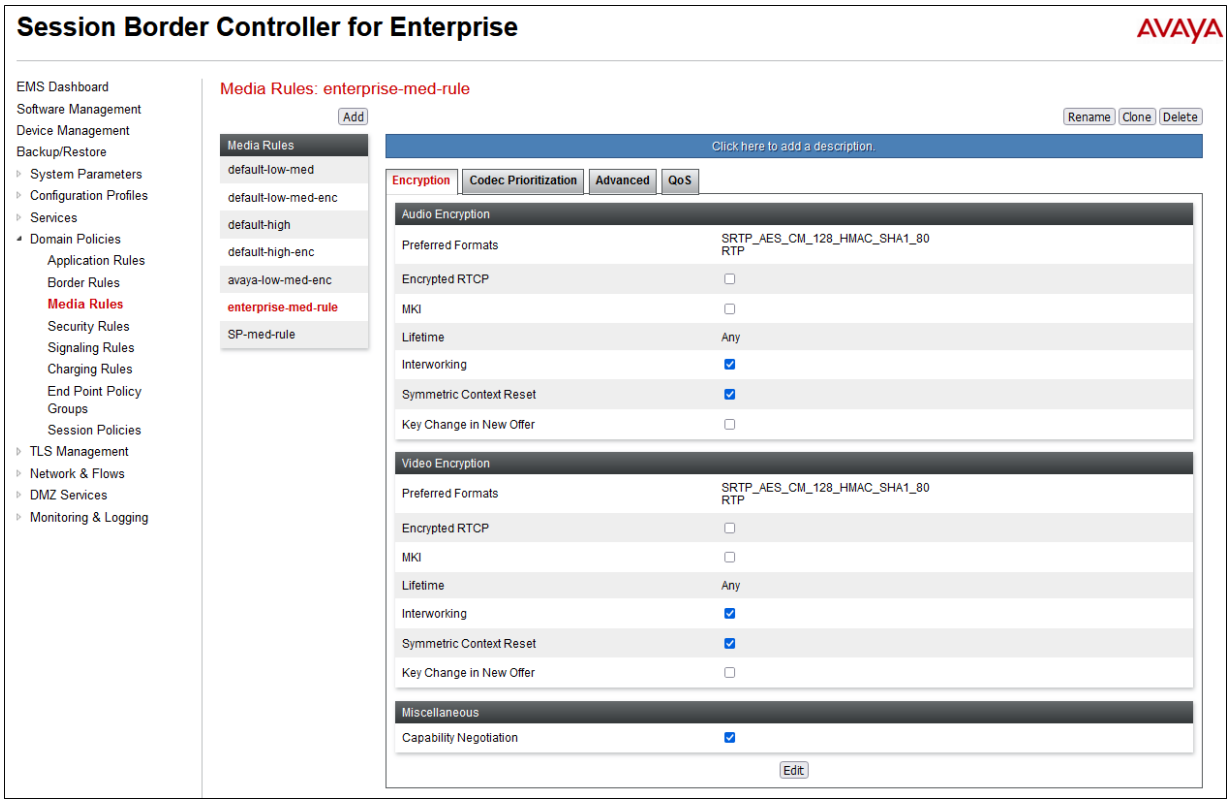
©2022 Avaya Inc. All Rights Reserved.

8.12. Media Rules

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

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

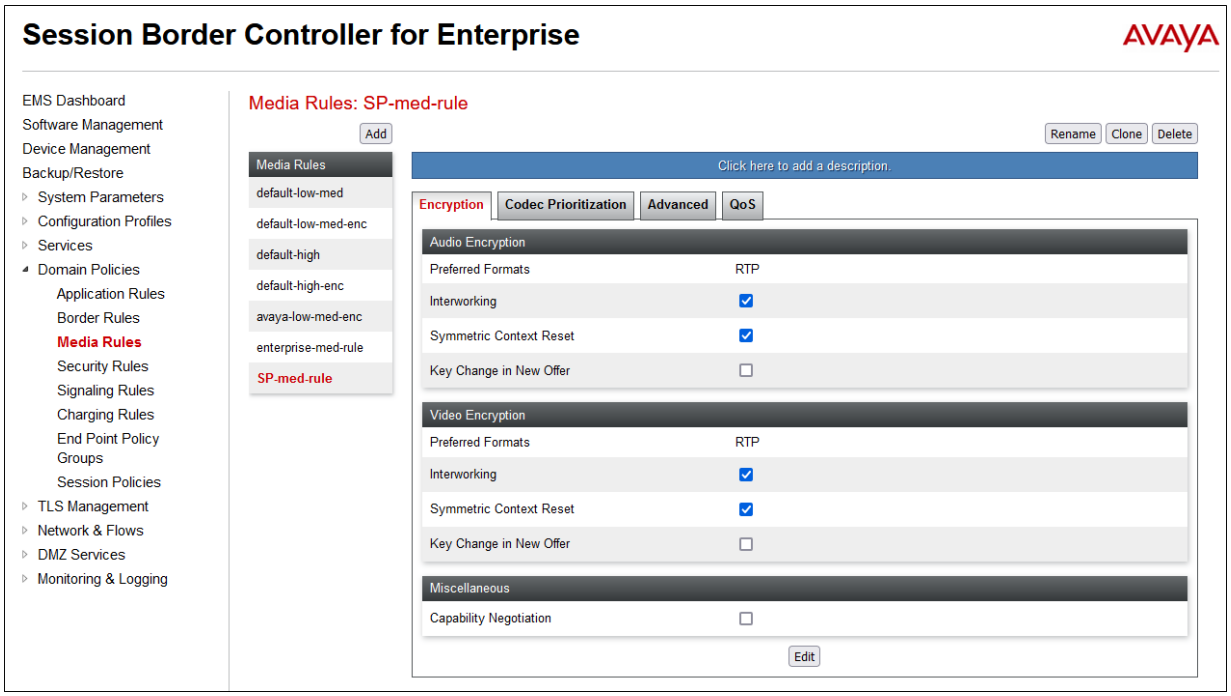
The Media Rule **enterprise-med-rule** created for the IP Office is shown below. The **Preferred Formats** are changed to include **SRTP_AES_CM_128_HMAC_SHA1_80** as the first choice and **RTP** as second. In the **Miscellaneous** section, **Capability Negotiation** is checked. All other fields retained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



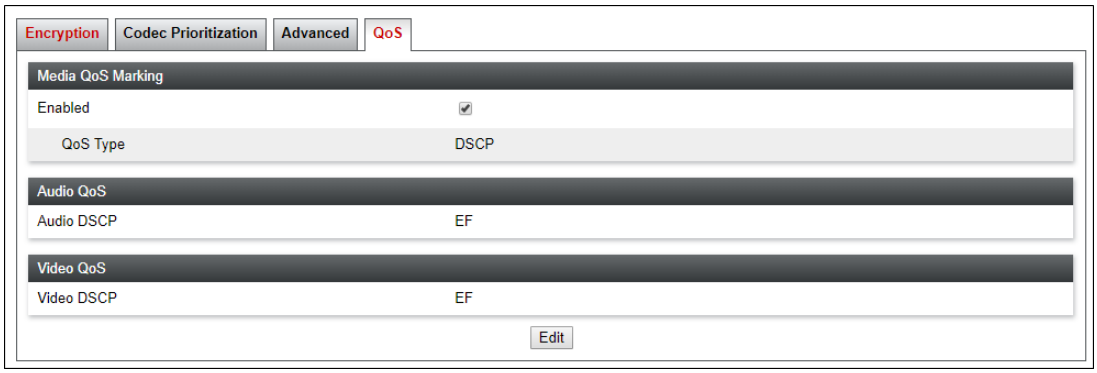
©2022 Avaya Inc. All Rights Reserved.

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

The Media Rule named **SP-med-rule**, used for BT in the sample configuration is shown below.



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

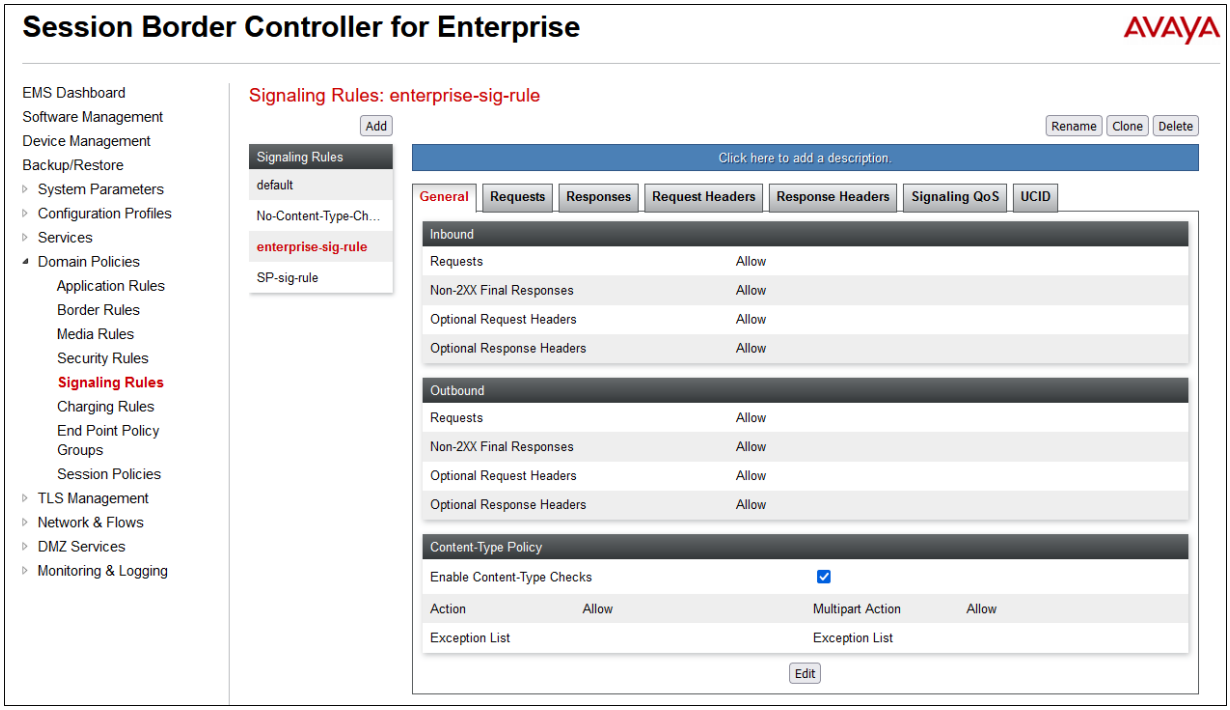


©2022 Avaya Inc. All Rights Reserved.

8.13. Signaling Rules

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

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



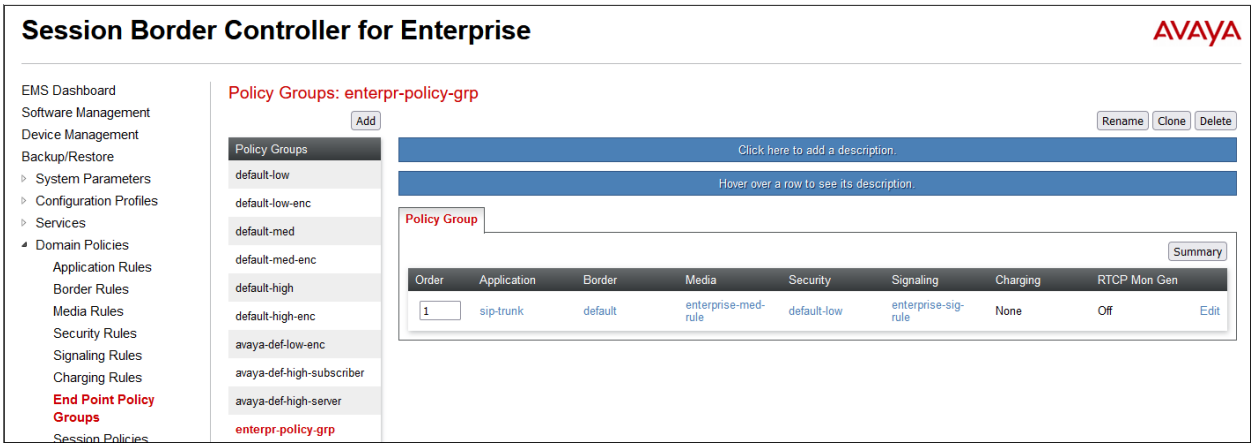
A signaling rule **SP-sig-rule** was also cloned from the default rule and used for BT, also left unchanged from the default rule. Note the DSCP value **AF41** for assured forwarding (default value) used for **Signaling QoS.**

©2022 Avaya Inc. All Rights Reserved.

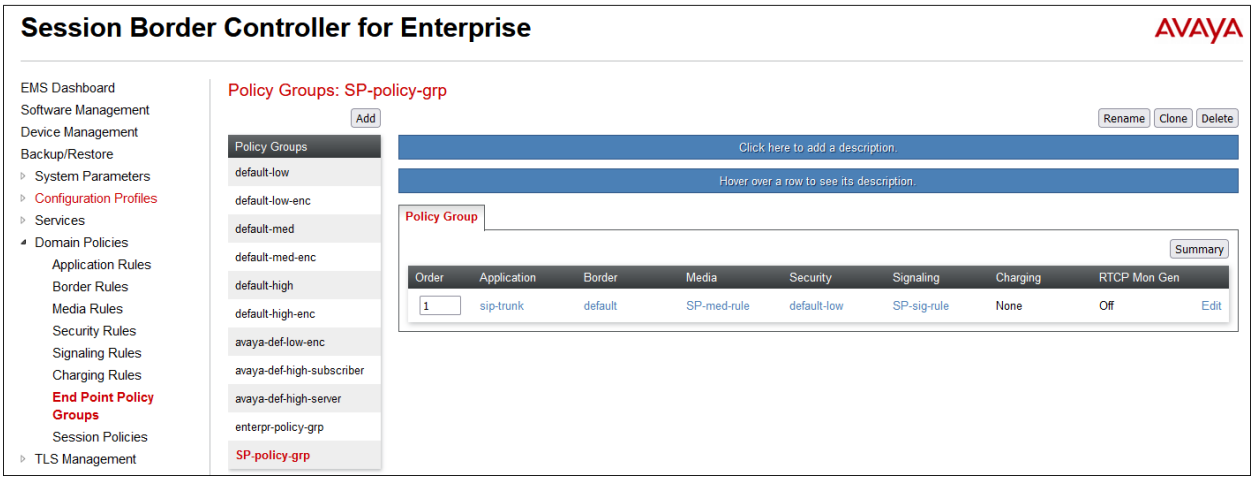
8.14. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is latter applied to a Server Flow in **Section 8.15**.

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



The following screen shows the **SP-policy-grp** created for BT. The details of the non-default rules chosen are shown in previous sections.



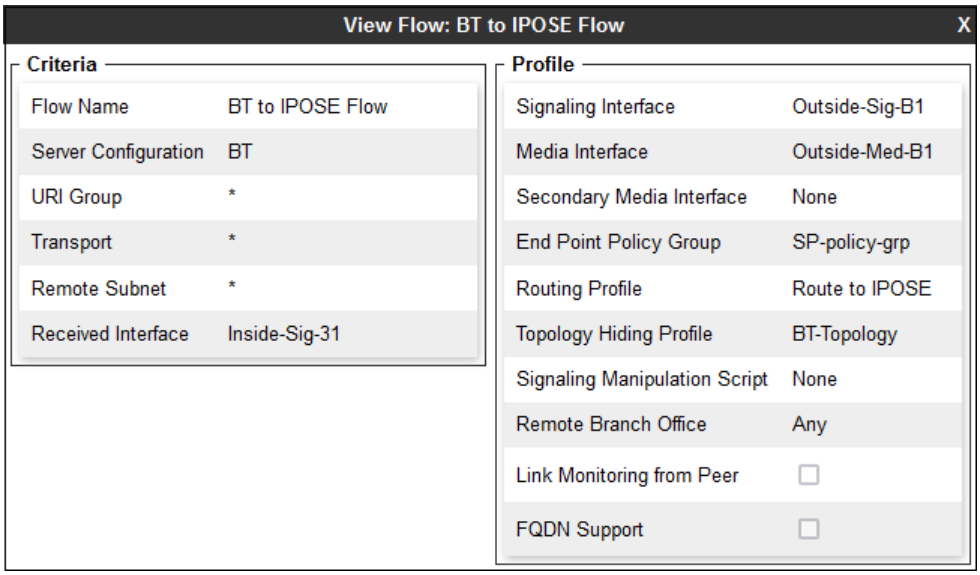
©2022 Avaya Inc. All Rights Reserved.

8.15. End Point Flows - Server Flows

Server Flows combine the interfaces, polices, and profiles defined in the previous sections into inbound and outbound flows. When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow.

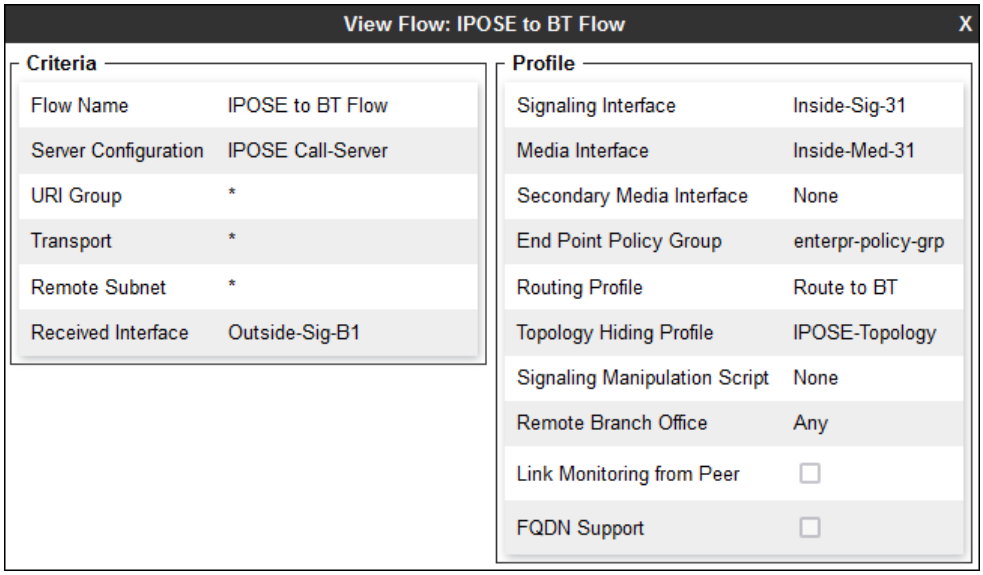
Create Server Flows for IP Office and the BT Wholesale Hosted SIP Trunking Service. To create a Server Flow, navigate to **Network and Flows → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown).

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

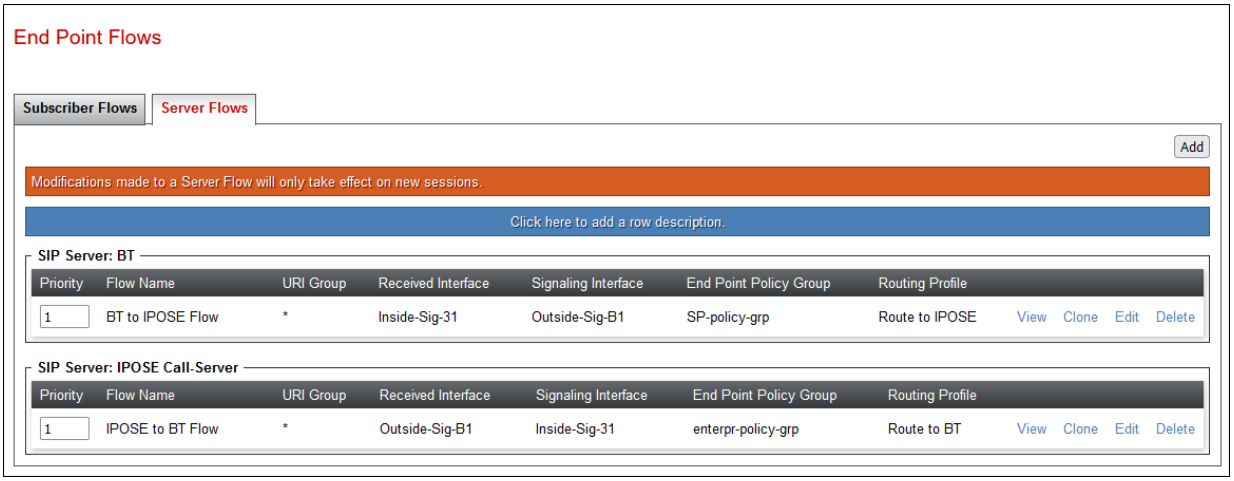


©2022 Avaya Inc. All Rights Reserved.

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



The following screen capture shows the newly created **End Point Flows**.



©2022 Avaya Inc. All Rights Reserved.

9. BT Wholesale Hosted SIP Trunking Service Configuration

To use BT Wholesale Hosted SIP Trunking Service, a customer must request the service from BT using the established sales processes. The process can be started by contacting BT via the corporate web site at: https://www.btwholesale.com/pages/static/home.htm and requesting information.

During the signup process, BT and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to BT's network.

BT is responsible for the configuration of BT Wholesale Hosted SIP Trunking Service. The customer will need to provide the public IP address used to reach the Avaya Session Border Controller for Enterprise at the enterprise, the public IP address assigned to interface B1.

BT will provide the customer the necessary information to configure Avaya IP Office and the Avaya Session Border Controller for Enterprise following the steps discussed in the previous sections, including:

BT will provide the following information:

- SIP Trunk registration credentials (User Name, Password, etc.).
- BT's Domain Name and SIP Proxy FQDN.
- DNS IP addresses.
- DID numbers, etc.

©2022 Avaya Inc. All Rights Reserved.

10. Verification Steps

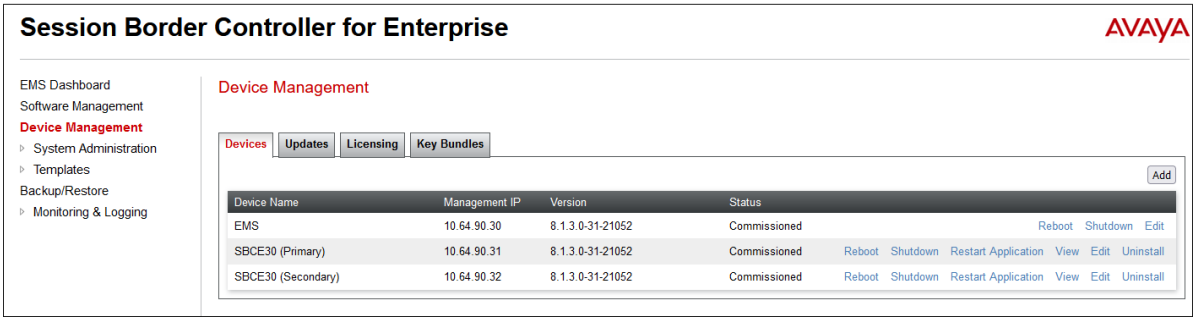
This section provides example verifications of the Avaya configuration with the BT Wholesale Hosted SIP Trunking Service.

10.1. Avaya SBCE

The following verification steps that may be performed within the Avaya SBCE.

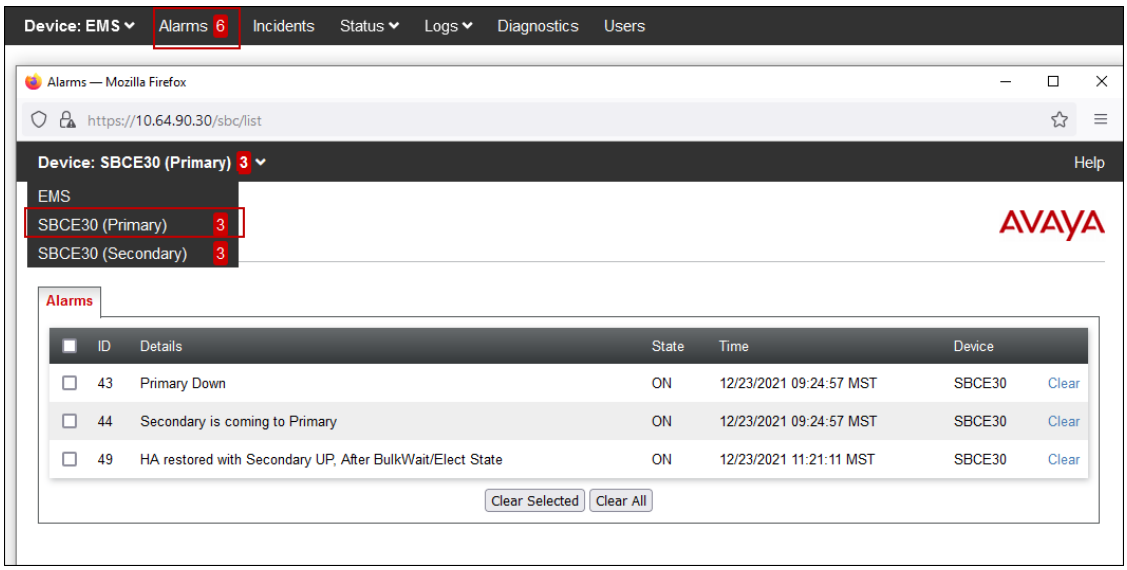
10.1.1. Device Management

The Device Management screen provides general information of the devices under control of the EMS, as well as the Primary / Secondary status of each SBCE appliance.



10.1.2. Alarms

The Alarms log is accessed from the Avaya SBCE top navigation menu as highlighted in the screen shot below, and selecting the desired device.

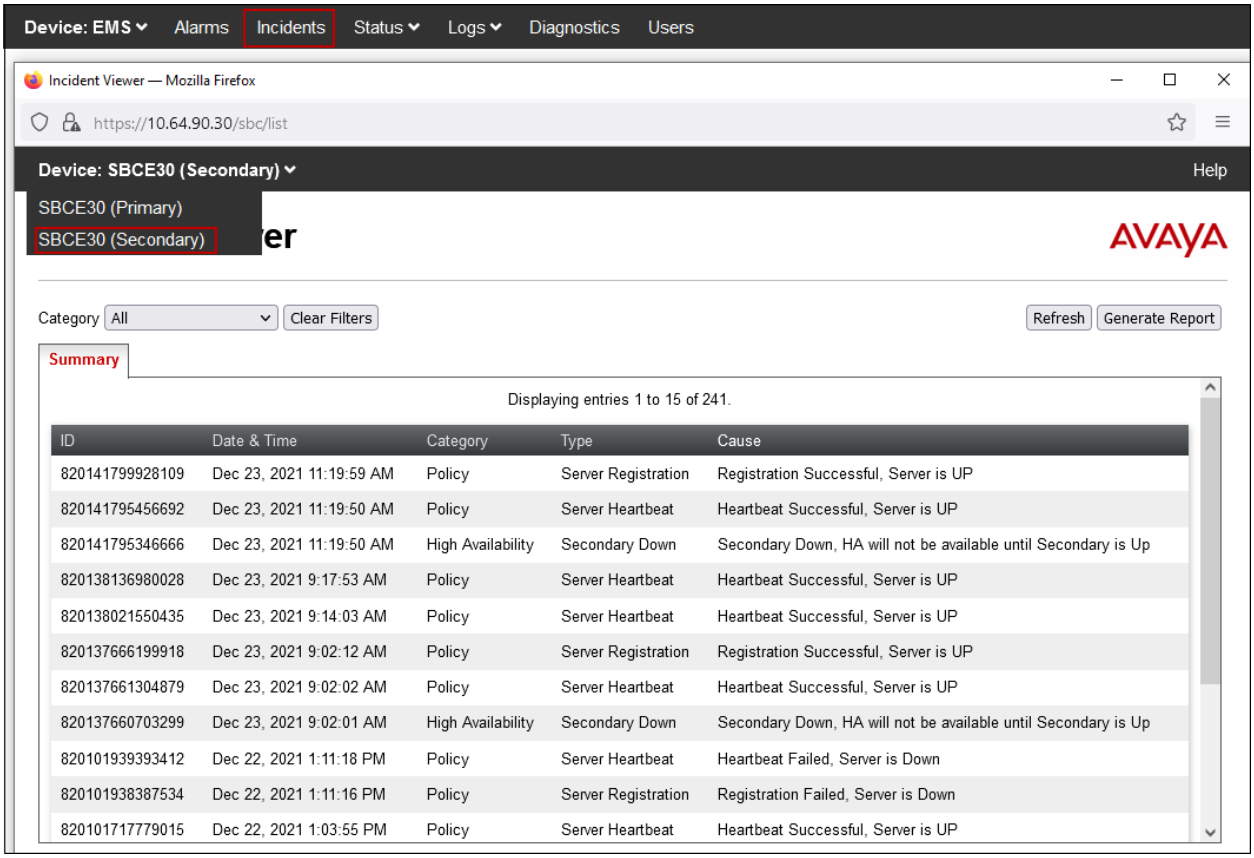


©2022 Avaya Inc. All Rights Reserved.

10.1.3. Incidents

The Incident Viewer can be accessed from the Avaya SBCE top navigation menu and selecting the desired device.

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

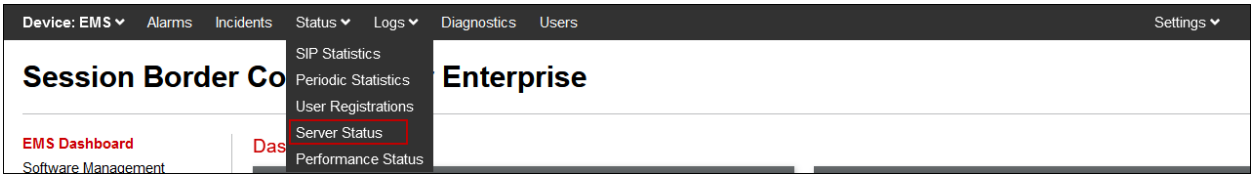


ID	Date & Time	Category	Type	Cause
820141799928109	Dec 23, 2021 11:19:59 AM	Policy	Server Registration	Registration Successful, Server is UP
820141795456692	Dec 23, 2021 11:19:50 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
820141795346666	Dec 23, 2021 11:19:50 AM	High Availability	Secondary Down	Secondary Down, HA will not be available until Secondary is Up
820138136980028	Dec 23, 2021 9:17:53 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
820138021550435	Dec 23, 2021 9:14:03 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
820137666199918	Dec 23, 2021 9:02:12 AM	Policy	Server Registration	Registration Successful, Server is UP
820137661304879	Dec 23, 2021 9:02:02 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
820137660703299	Dec 23, 2021 9:02:01 AM	High Availability	Secondary Down	Secondary Down, HA will not be available until Secondary is Up
820101939393412	Dec 22, 2021 1:11:18 PM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
820101938387534	Dec 22, 2021 1:11:16 PM	Policy	Server Registration	Registration Failed, Server is Down
820101717779015	Dec 22, 2021 1:03:55 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP

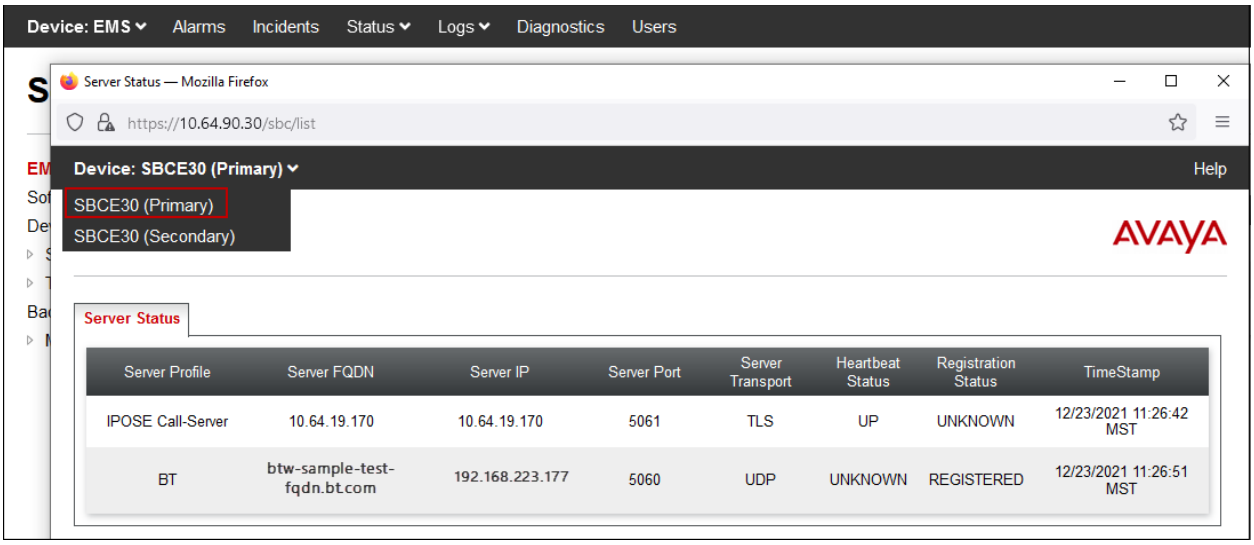
©2022 Avaya Inc. All Rights Reserved.

10.1.4. Server Status

The **Server Status** can be access from the Avaya SBCE top navigation menu by selecting the **Status** menu, **Server Status** and choosing the desired device.



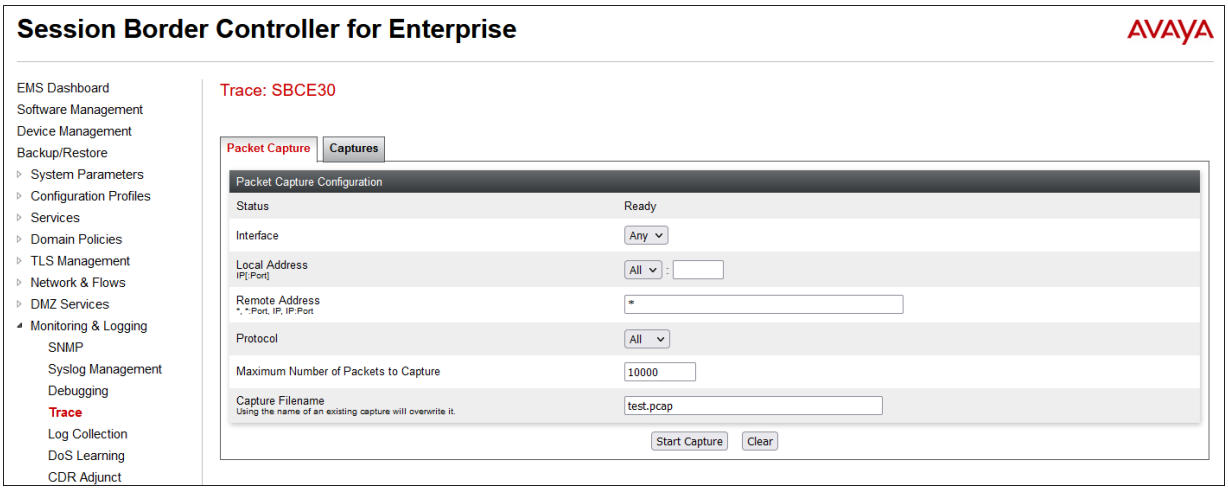
The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat or Registration to be enabled on the SIP Server Configuration profiles, as configured in **Section 8.8**.



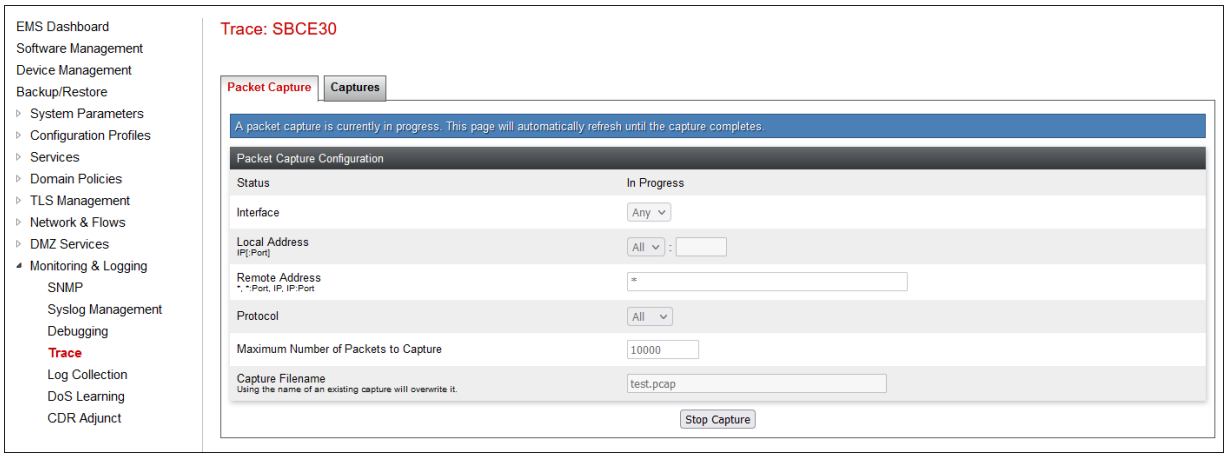
©2022 Avaya Inc. All Rights Reserved.

10.1.5. Tracing

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

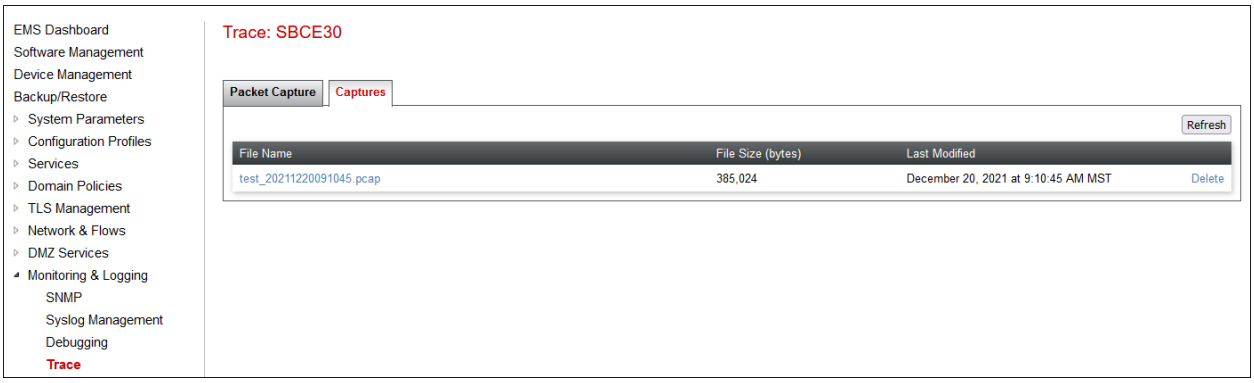


When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, click the **Stop Capture** button at the bottom.



©2022 Avaya Inc. All Rights Reserved.

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



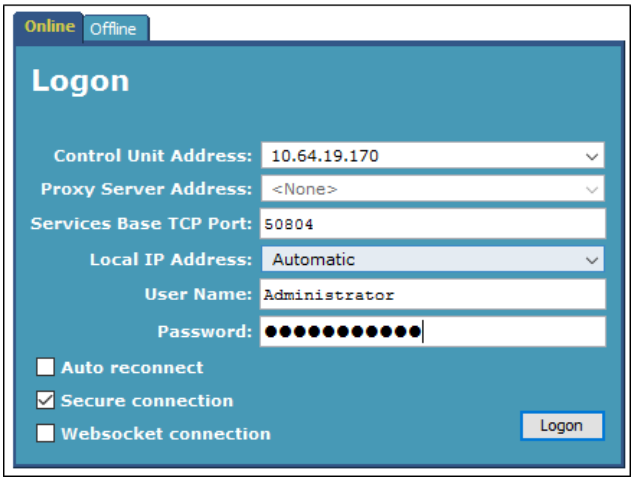
Also, the **traceSBC** tool can be used to monitor the SIP signaling messages between the Service provider and the Avaya SBCE. The tool is run from the SBCE CLI command.

10.2. Avaya IP Office

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

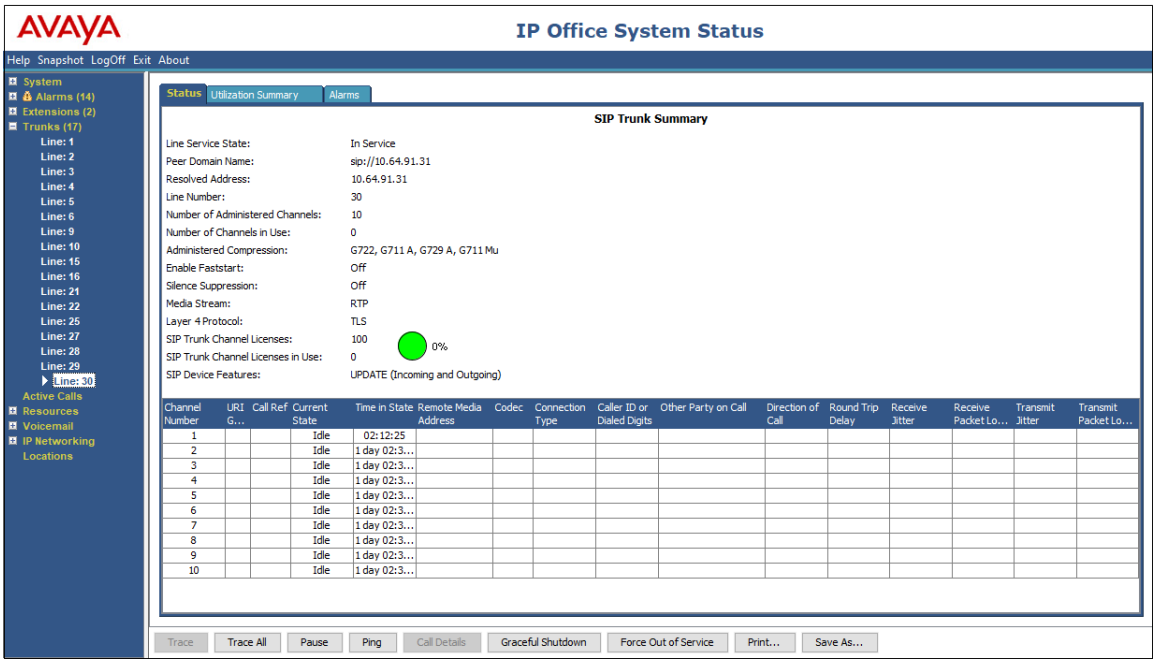
10.2.1. System Status Application

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



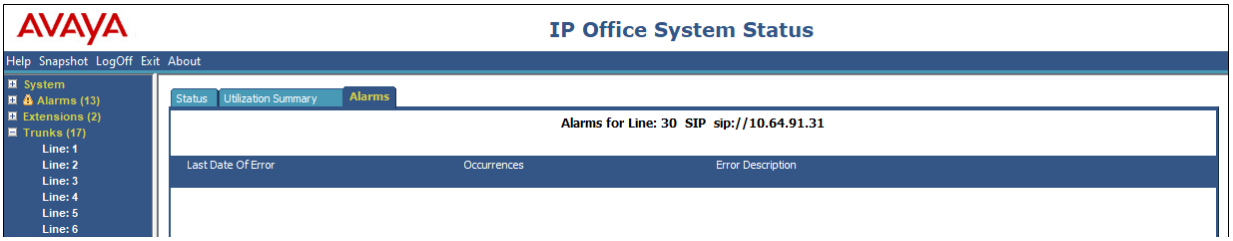
©2022 Avaya Inc. All Rights Reserved.

Select the SIP line from the left pane (**Line 30** in the reference configuration). On the **Status** tab in the right pane, verify that the **Current State** is ***Idle*** for each channel (assuming no active calls at present time).



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

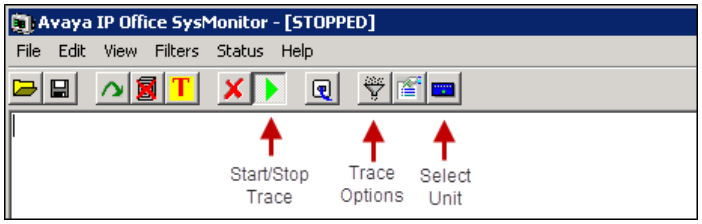
Select the **Alarms** tab and verify that no alarms are active on the SIP line.



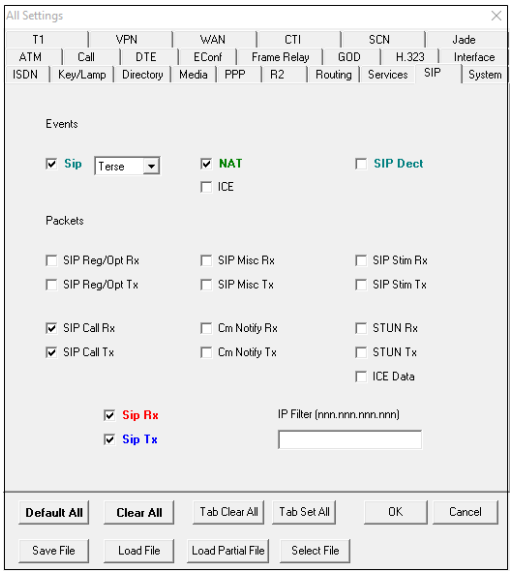
©2022 Avaya Inc. All Rights Reserved.

10.2.2. System Monitor

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



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



©2022 Avaya Inc. All Rights Reserved.

11. Conclusion

These Application Notes describe the procedures required to configure Avaya IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 8.1 in a High Availability configuration to connect to BT Wholesale Hosted SIP Trunking Service. BT Wholesale Hosted SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

12. Additional References

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

[1] *Deploying IP Office Server Edition Servers*, November 2021.
[2] *Deploying IP Office Servers as Virtual Machines*, November 2021.
[3] *IP Office™ Platform 11.1, Deploying an IP500 V2 IP Office Essential Edition System*, November 2021.
[4] *Administering IP Office with IP Office Manager*, November 2021.
[5] *Administering Avaya IP Office with Web Manager*, November 2021.
[6] *Deploying Avaya Session Border Controller on a Virtualized Environment Platform*, Release 8.1.x, August 2021.
[7] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, August 2021.
[8] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 8.1.x, August 2021.

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

©2022 Avaya Inc. All Rights Reserved.

©2022 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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