



Application Notes for Configuring BT Wholesale Hosted SIP Trunking Service with Avaya IP Office 10 and Avaya Session Border Controller for Enterprise Release 7.1 - Issue 1.1

Abstract

These Application Notes describe the procedures for configuring BT Wholesale Hosted Session Initiation Protocol (SIP) Trunking with Avaya IP Office Release 10 and Avaya Session Border Controller for Enterprise Release 7.1.

BT Wholesale Hosted SIP Trunking provides PSTN access via a SIP trunk between the enterprise and the BT Wholesale network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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.

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

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider BT Wholesale (BT) and the Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of an Avaya IP Office Server Edition Release 10, Avaya Session Border Controller for Enterprise Release 7.1 (Avaya SBCE), Avaya Voicemail Pro, Avaya Communicator for Windows, and Avaya H.323, SIP, digital, and analog endpoints.

The BT SIP Trunking service referenced within these Application Notes is designed for business customers. The service enables local long distance and international PSTN calling via standards-based SIP trunks as an alternative to legacy analog or digital trunks, without the need for additional TDM enterprise gateways and the associated maintenance costs.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office to connect to BT SIP Trunking service via the Avaya SBCE. This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests 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 these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the BT SIP Trunking service did not include use of any specific encryption features as requested by **BT**.

2.1. Interoperability Compliance Testing

A simulated enterprise site with Avaya IP Office was connected to BT SIP Trunking service via the Avaya SBCE. To verify SIP trunking interoperability, the following features and functionality were exercised during the interoperability compliance test:

- Response to SIP OPTIONS queries.

- SIP trunk registration and authentication.
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound long holding time call stability.
- Various call types including: local, long distance, international, outbound toll-free, operator service and directory assistance.
- Codec G.711A and G.729.
- Caller number/ID presentation.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.
- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- Telephony features such as hold and resume, transfer, and conference.
- Fax T.38 and G.711 pass-through modes.
- Off-net call forwarding.
- Twinning to mobile phones on inbound calls.
- Avaya Communicator for Windows.
- Avaya Communicator for Web client (WebRTC).
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

Note:

Remote Worker and Avaya Communicator for Web (WebRTC) were tested as part of this solution. The configuration necessary to support remote worker and Avaya Communicator for Web is beyond the scope of these Application Notes and are not included in these Application Notes. For these configuration details, see **Reference [8]** and **[9]**.

2.2. Test Results

BT SIP Trunking passed compliance testing.

Items supported but not tested included the following:

- Inbound toll-free, outbound toll-free, outbound international, local directory assistance, fax G.711 pass-through mode and Emergency.

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

- **OPTIONS** – BT did not configure to send SIP OPTIONS message to Avaya. However, BT responded to Avaya OPTIONS message with 403 Forbidden-Source Endpoint Lookup Failed.

- **Call Redirection Using Refer (namely Call Forward, Blind and Consultative Transfers)**
– There were number of error codes seen such as; 405, 491 or 487. However, the call transfers were completed with 2 ways audio. There was no user impacted except user may see the Avaya SIP desk-phone (11xx series) and soft-phone displaying “Transfer failed” at the end of the call transfer.
- **Fax G.711 Failed** – BT system supported both T.38 and G.711 (pass-through) modes and both were enabled. However, during the call for fax G.711, BT system sent re-INVITE to negotiate for T.38 fax. This, intern, caused Avaya system to respond 488 Not Acceptable here as IP Office was set to G.711 fax only. The recommendation is to use T.38 fax setting only on IP Office system.

2.3. Support

For technical support on the Avaya products described in these Application Notes, visit <http://support.avaya.com>.

For technical support on BT SIP Trunking, contact BT at <https://www.btwholesale.com>

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to the BT SIP Trunking service via the Avaya SBCE through the public IP network. For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

Located at the enterprise site is an Avaya IP Office Server Edition with an Avaya IP 500 V2 Expansion System which provides connections for 16 digital stations and the extension PHONE 8 card which provides connections for 8 analog stations to the PSTN as well as 64-channel VCM (Voice Compression Module) for supporting VoIP codecs. The LAN1 port of Avaya IP Office is connected to the enterprise LAN while the LAN2 port is connected to the public IP network via Avaya SBCE. Endpoints include an Avaya 9600 Series IP Telephone (with H.323 firmware), Avaya 11x0 Series IP Telephone (with SIP firmware), an Avaya 9508 Digital Telephone, an Avaya Symphony 2000 Analog Telephone, an Avaya Communicator for Web and an Avaya Communicator for Windows. A separate Windows PC runs Avaya IP Office Manager to configure and administer the Avaya IP Office.

Mobility Twinning is configured for some of the Avaya IP Office users so that calls to these user phones will also ring and can be answered at the configured mobile phones.

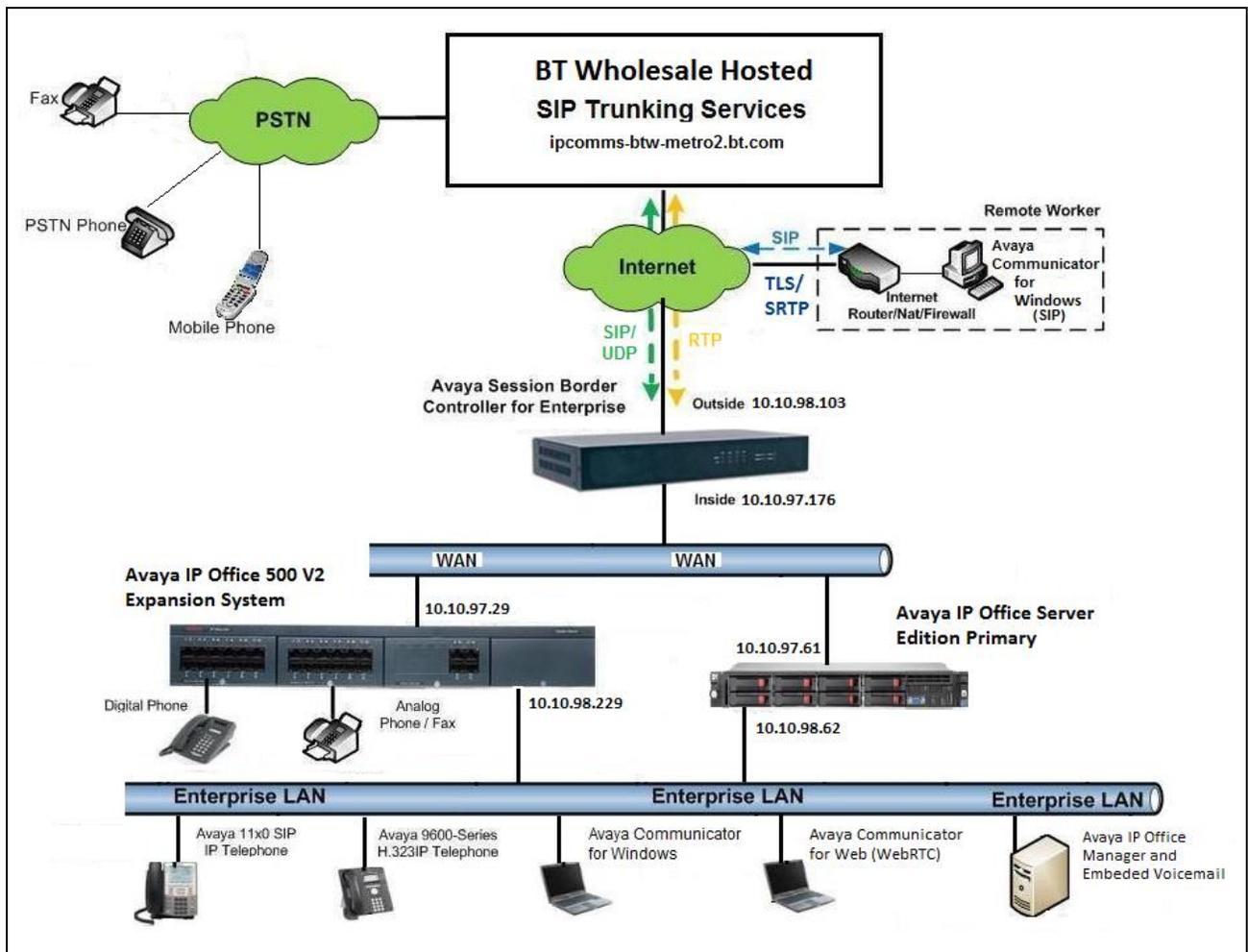


Figure 1: Test Configuration for Avaya IP Office with BT SIP Trunking Service

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment	Release
Avaya IP Office Server Edition	10.0.0.3.0.5
Avaya IP Office 500v2 (Expansion)	10.0.0.3.0.5
Avaya IP Office Manager	10.0.0.3.0.5
Avaya IP Office Embedded Voicemail	10.0.0.3.0.5
Avaya WebRTC Gateway	10.0.0.3.0 build 10
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.1.0.2-01-13249
Avaya 11x0 IP Telephone (SIP)	SIP11x0e04.04.23.00
Avaya 9621G IP Telephone (H.323)	6.6.401
Avaya Communicator for Windows	2.1.3
Avaya Communicator for Web (WebRTC)	1.0.16.2220
Avaya Digital Telephone (9508)	0.45
Avaya Symphony 2000 Analog Telephone	N/A
Fax	N/A
BT Wholesale Hosted SIP Trunking Service Components	
Component	Release
ASBC Genband	Q20 9.1.13
BroadWorks	R20 SP1

Note: The test results documented in these Application Notes apply to standalone IP Office 500 V2 deployments as well as all configurations of IP Office Server Edition.

5. Configure Avaya IP Office

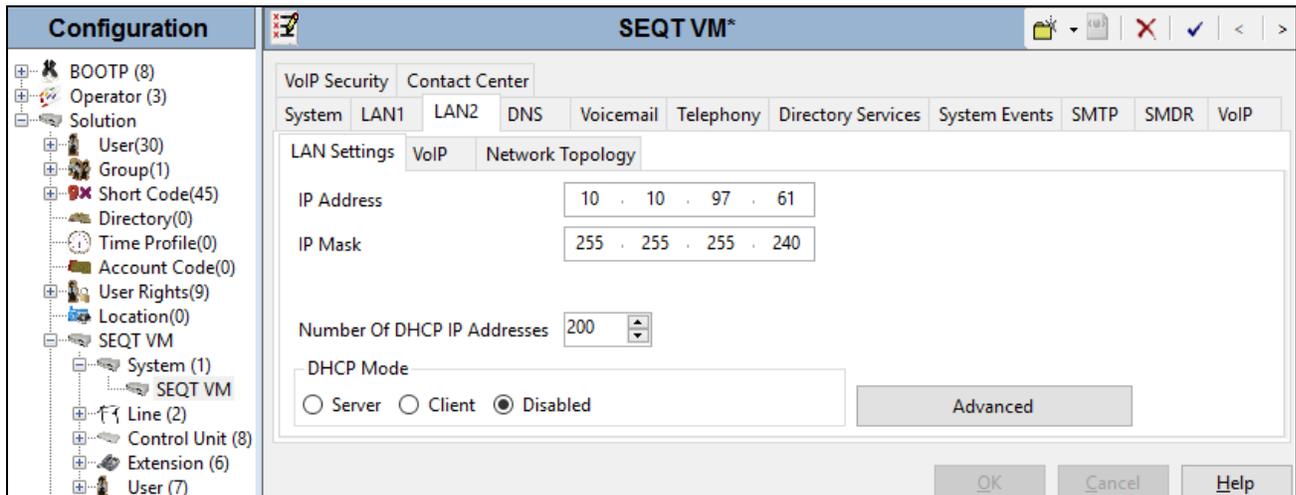
This section describes the Avaya IP Office configuration to support connectivity to BT SIP Trunking service through Avaya SBCE. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start** → **Programs** → **IP Office** → **Manager** to launch the application. Navigate to **File** → **Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials. A management window will appear similar to the one shown in the next section. The appearance of the IP Office Manager can also be customized using the **View** menu. In some screens presented in this section, the **View** menu was configured to show the **Navigation** pane on the left side, the **Group** pane in the center, and the **Details** pane on the right side. Some of these panes will be referenced in Avaya IP Office configuration. Proper licensing as well as standard feature configurations that are not directly related to the interface with the service provider (such as LAN interface to the enterprise site) is assumed to be already in place.

5.1. LAN Settings

In the sample configuration, the **SEQT VM** was used as the system name and the WAN port was used to connect the Avaya IP Office to the public network. The LAN2 settings correspond to the WAN port on the Avaya IP Office.

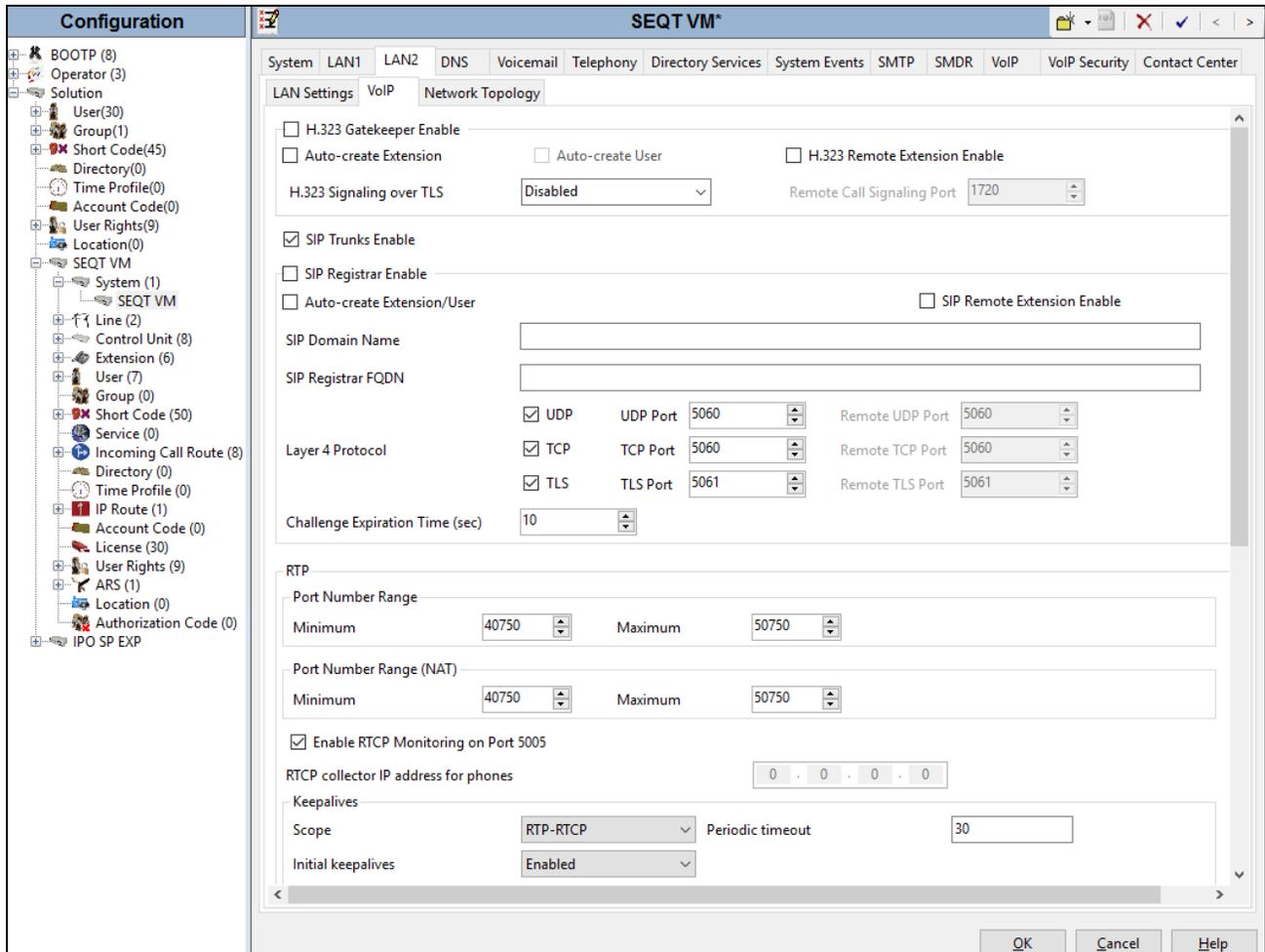
To access the LAN settings, first navigate to **System (1)** → **SEQT VM** in the **Navigation** pane and then navigate to the **LAN2** → **LAN Settings** tab in the **Details** pane.

- Set the **IP Address** field to the IP address assigned to the IP Office WAN port.
- Set the **IP Mask** field to the mask used on the public network.
- All other parameters should be set according to customer requirements.
- Click **OK**.



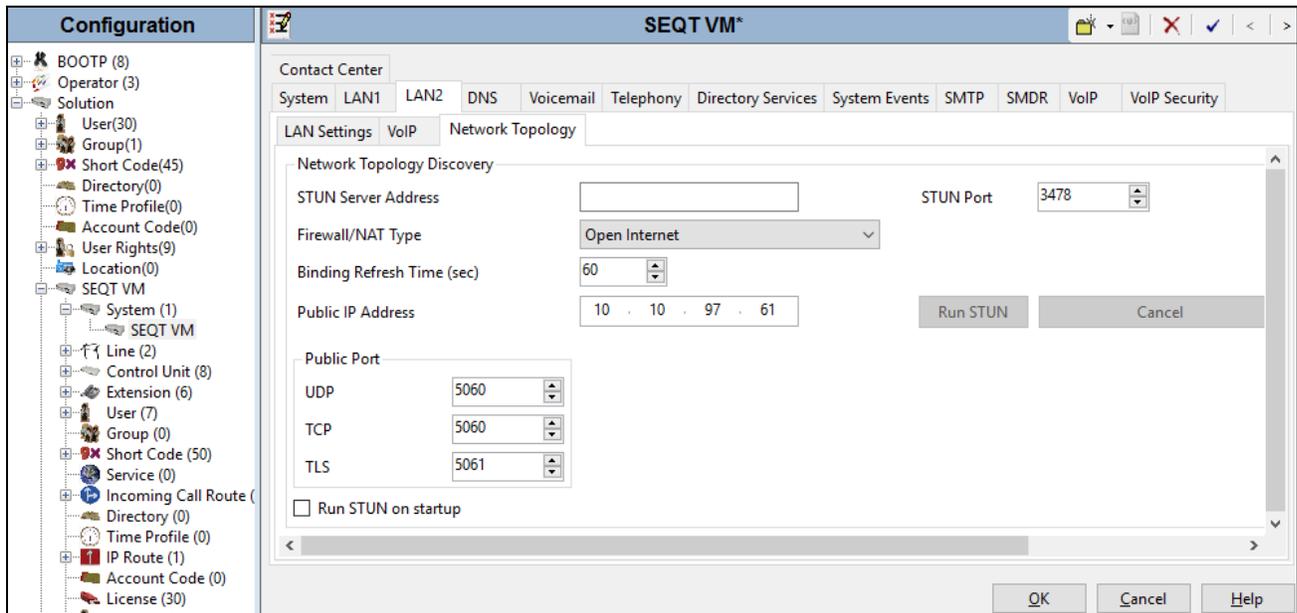
Select the **VoIP** tab as shown in the following screen.

- Ensure **H323 Gatekeeper Enable** box is unchecked.
- The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks to BT.
- The **Layer 4 Protocol**, check the **UDP**, **TCP** and **TLS** boxes. Then set **UDP** and **TCP Ports** to **5060**, and **TLS port** to **5061**.
- **Enable RTCP Monitoring on Port 5005** and **Keepalives** should be set as shown in capture below.
- All other parameters should be set according to customer requirements.
- Click **OK**.



On the **Network Topology** tab in the **Details** pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. No firewall or network address translation (NAT) device was used in the compliance test as shown in **Figure 1**, so the parameter was set to **Open Internet**. With this configuration, **STUN** will not be used.
- Set **Binding Refresh Time (seconds)** to **60**. This value is used as one input to determine the frequency at which IP Office will send SIP OPTIONS messages to the service provider.
- Set **Public IP Address** to the IP address of IP Office WAN port. **Public Port** is set to **5060** for **UDP** and **TCP**, and **5061** for **TLS**.
- All other parameters should be set according to customer requirements.
- Click **OK**.



In the compliance test, the LAN1 interface was used to connect IP Office to the enterprise site IP network. The LAN1 interface configuration is not directly relevant to the interface with BT SIP Trunking service, and therefore is not described in these Application Notes.

5.2. System Telephony Settings

Navigate to the **Telephony** → **Telephony** Tab in the **Details** pane.

- Choose the **Companding Law** typical for the enterprise location. **A-LAW** is used as member is in Europe.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the service provider across the SIP trunk.
- Other parameters are left at default.
- Click **OK**.

The screenshot displays the configuration interface for SEQT VM, specifically the **Telephony** tab. The left sidebar shows a tree view of the configuration hierarchy, with **SEQT VM** selected. The main panel is divided into several sections:

- Telephony Parameters:** Includes fields for Dial Delay Time (4), Dial Delay Count (0), Default No Answer Time (15), Hold Timeout (720), Park Timeout (300), Ring Delay (5), Call Priority Promotion Time (Disabled), Default Currency (USD), Default Name Priority (Favor Trunk), Media Connection Preservation (Enabled), and Phone Failback (Automatic).
- Login Code Complexity:** Includes an **Enforcement** checkbox, a **Minimum length** field (4), and a **Complexity** checkbox.
- RTCP Collector Configuration:** Includes a **Send RTCP to an RTCP Collector** checkbox, a **Server Address** field (0.0.0.0), a **UDP Port Number** field (5005), and an **RTCP expiration interval (sec)** field (5).
- Companding Law:** This section is expanded to show two sub-sections: **Switch** and **Line**. In both, the **A-Law** radio button is selected, with **A-Law Line** selected in the **Line** sub-section.
- Additional Options:** Includes checkboxes for **DSS Status**, **Auto Hold**, **Dial By Name** (checked), **Show Account Code** (checked), **Inhibit Off-Switch Forward/Transfer** (unchecked), **Restrict Network Interconnect** (unchecked), **Include location specific information** (unchecked), **Drop External Only Impromptu Conference** (unchecked), **Visually Differentiate External Call** (unchecked), **High Quality Conferencing** (checked), **Directory Overrides Barring** (checked), and **Advertise Callee State To Internal Callers** (unchecked).

At the bottom right, there are **OK**, **Cancel**, and **Help** buttons.

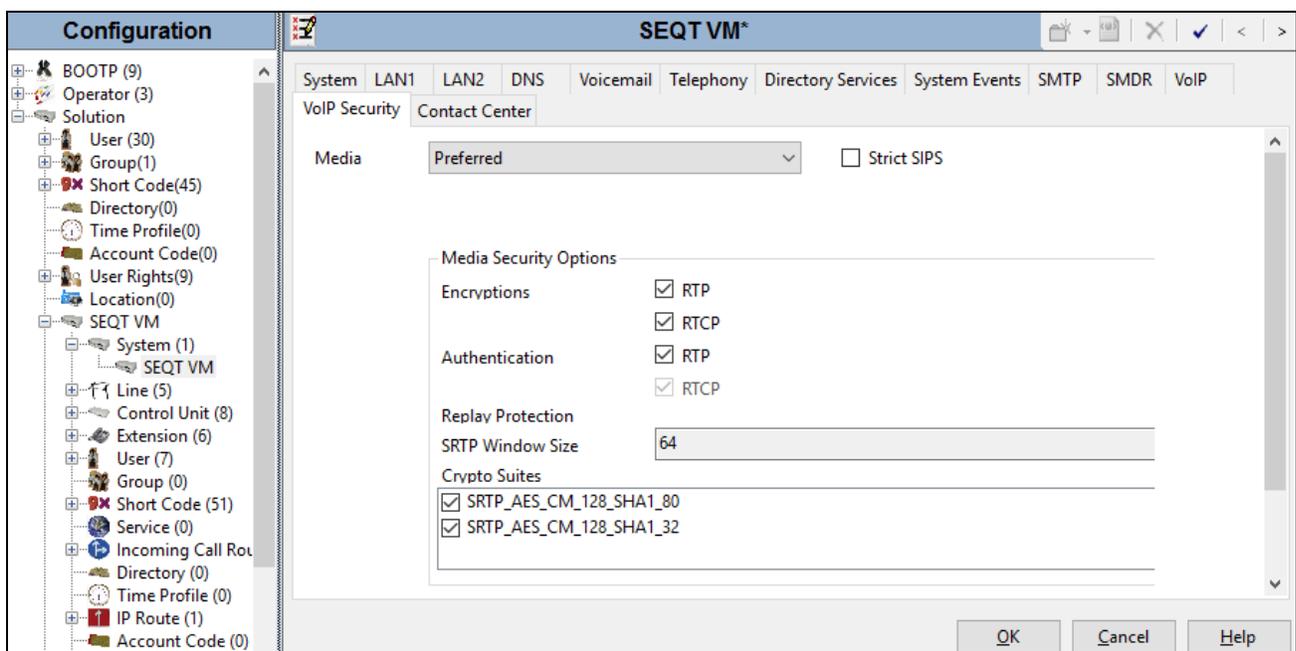
5.3. VoIP Security Settings

When enabling SRTP on the system, the recommended setting for **Media** is *Preferred*. In this scenario, IP Office uses SRTP if supported by the other end, and otherwise uses RTP. If the *Enforced* setting is used, and SRTP is not supported by the other end, the call is not established.

Individual SIP lines and extensions have media security settings that can override system level settings. This can be used for special cases where the trunk or extension setting must be different from the system settings.

In the compliance testing, *Preferred* is set at system, trunk and extension level to allow the system to fall back to non-secure media in case there is issue with SRTP. This would help to avoid blackout situation within the enterprise network. In some specific deployments, if supported, *Enforced* is set at the trunk level to ensure the secured communication over the public internet using both signaling (TLS) and media (SRTP). Navigate to **System → VoIP Security** tab and configure as follows:

- Select *Preferred* for **Media Security**. The system attempts to use secure media first and if unsuccessful, falls back to non-secure media within the IP Office system.
- Check **RTCP** check-box.
- Other parameters are left as default.
- Click **OK**.



5.4. Administer a SIP Line

A SIP line is needed to establish the SIP connection between IP Office and BT SIP Trunking service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.4.1** to create the SIP Line from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.4.2**.

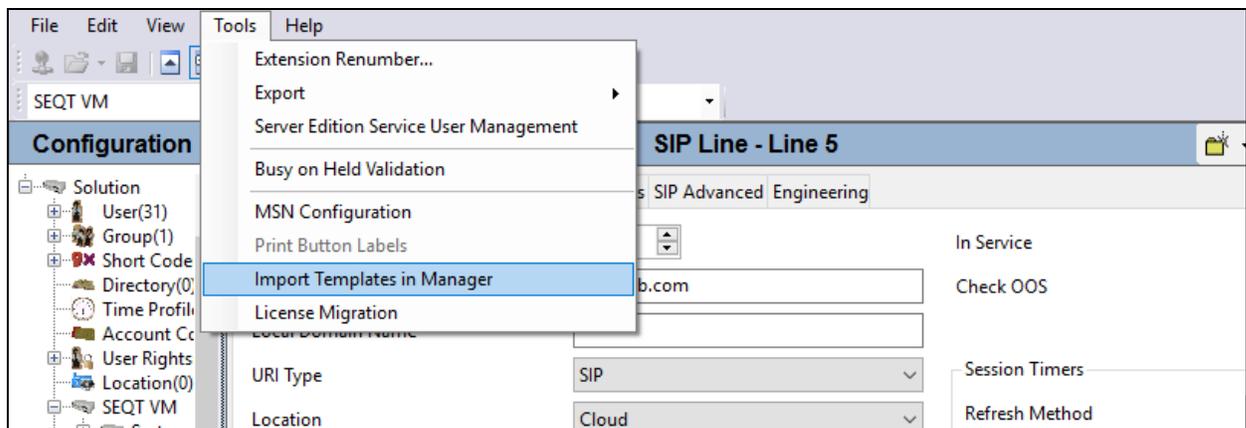
Also, the following SIP Line settings are not supported on Basic Edition:

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

Alternatively, a SIP Line can be created manually. To do so right-click **Line** in the Navigation Pane and select **New** → **SIP Line**, then follow the steps outlined in **Sections 5.4.2**.

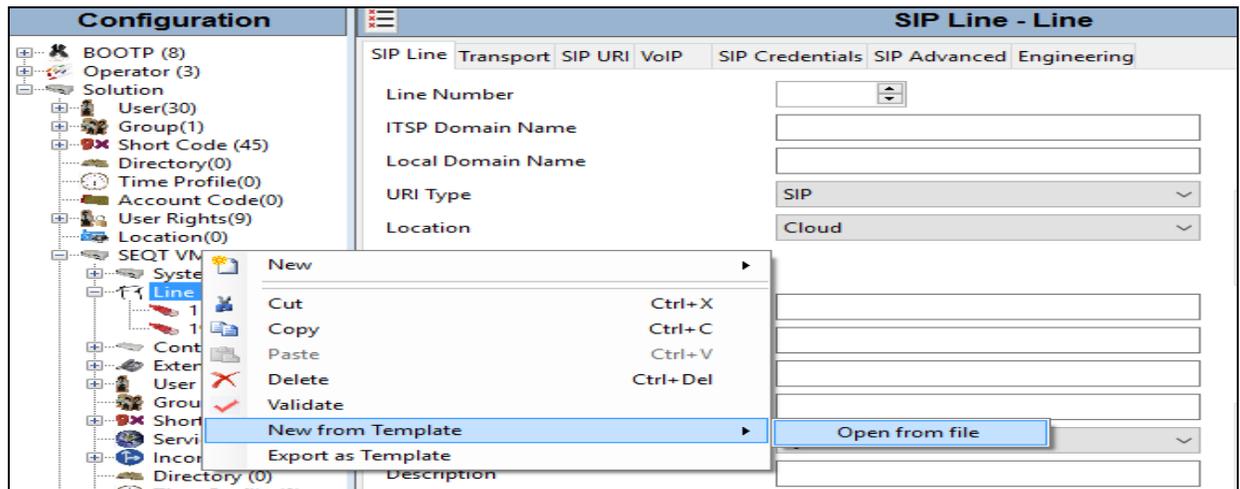
5.4.1. Create SIP Line from Template

1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **BTWSIPO10SBCE71.xml**. The file name is important in locating the proper template file in **Step 4**.
2. Import the template into IP Office Manager.
From IP Office Manager, select **Tools** → **Import Templates in Manager**. This action will copy the template file into the IP Office template directory. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.

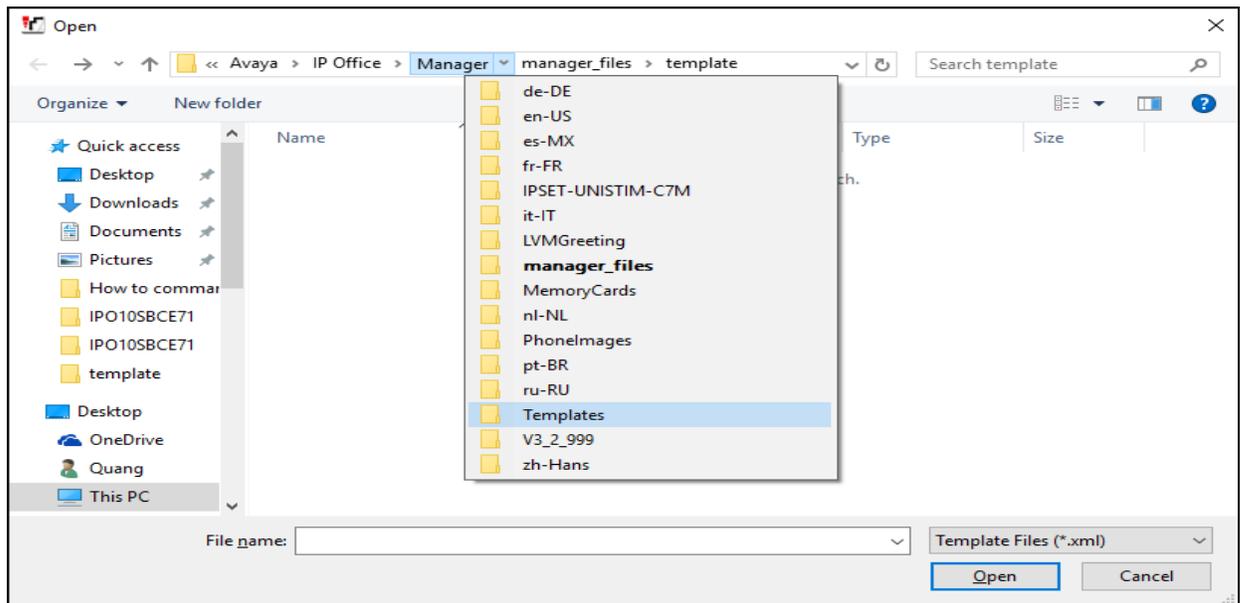


In the resulting pop-up window that appears (not shown), select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window will appear (not shown) stating success or failure. Next click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

- To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New** → **New from Template** → **Open from file**.



- On the “Open” pop-up window, navigate to **Manager** → **Templates** and make sure **Template File (.xml)** is the file type selected. Then select the file “**BTWSIPO10SBCE71.xml**”. Click **Open** and **OK** (not shown).



- Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Section 5.4.2**.

5.4.2. Create SIP Line Manually

To create a SIP line, begin by navigating to **Line** in the left **Navigation** pane and then right click to select **New** → **SIP Line**. On the **SIP Line** tab in the **Details** pane, configure the parameters as shown below:

- Set **ITSP Domain Name** to the enterprise domain so that IP Office uses this domain as the host portion of SIP URI in SIP headers such as the From header.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- **Incoming Supervised REFER** is set to **Auto** to allow IP Office to support call transfer using re-INVITE and REFER methods.
- **Outgoing Supervised REFER** is set to **Auto** to allow IP Office to support call transfer using re-INVITE and REFER methods.
- Other parameters are set as default values.
- Click **OK**.

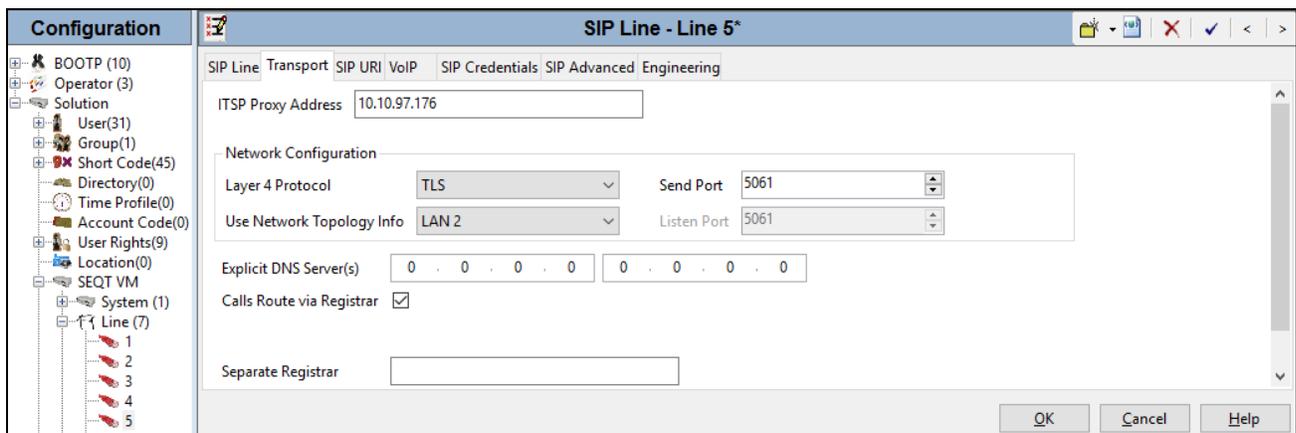
The screenshot displays the 'SIP Line - Line 5' configuration window. The left pane shows a tree view with 'Line (7)' selected. The main pane is divided into several sections:

- Line Number:** 5
- ITSP Domain Name:** avayalab.com
- Local Domain Name:** (empty)
- URI Type:** SIP
- Location:** Cloud
- Prefix:** (empty)
- National Prefix:** (empty)
- International Prefix:** (empty)
- Country Code:** (empty)
- Name Priority:** System Default
- Description:** (empty)
- In Service:**
- Check OOS:**
- Session Timers:**
 - Refresh Method:** Auto
 - Timer (sec):** On Demand
- Redirect and Transfer:**
 - Incoming Supervised REFER:** Auto
 - Outgoing Supervised REFER:** Auto
 - Send 302 Moved Temporarily:**
 - Outgoing Blind REFER:**

Buttons for OK, Cancel, and Help are visible at the bottom right.

Select the **Transport** tab and enter the following information.

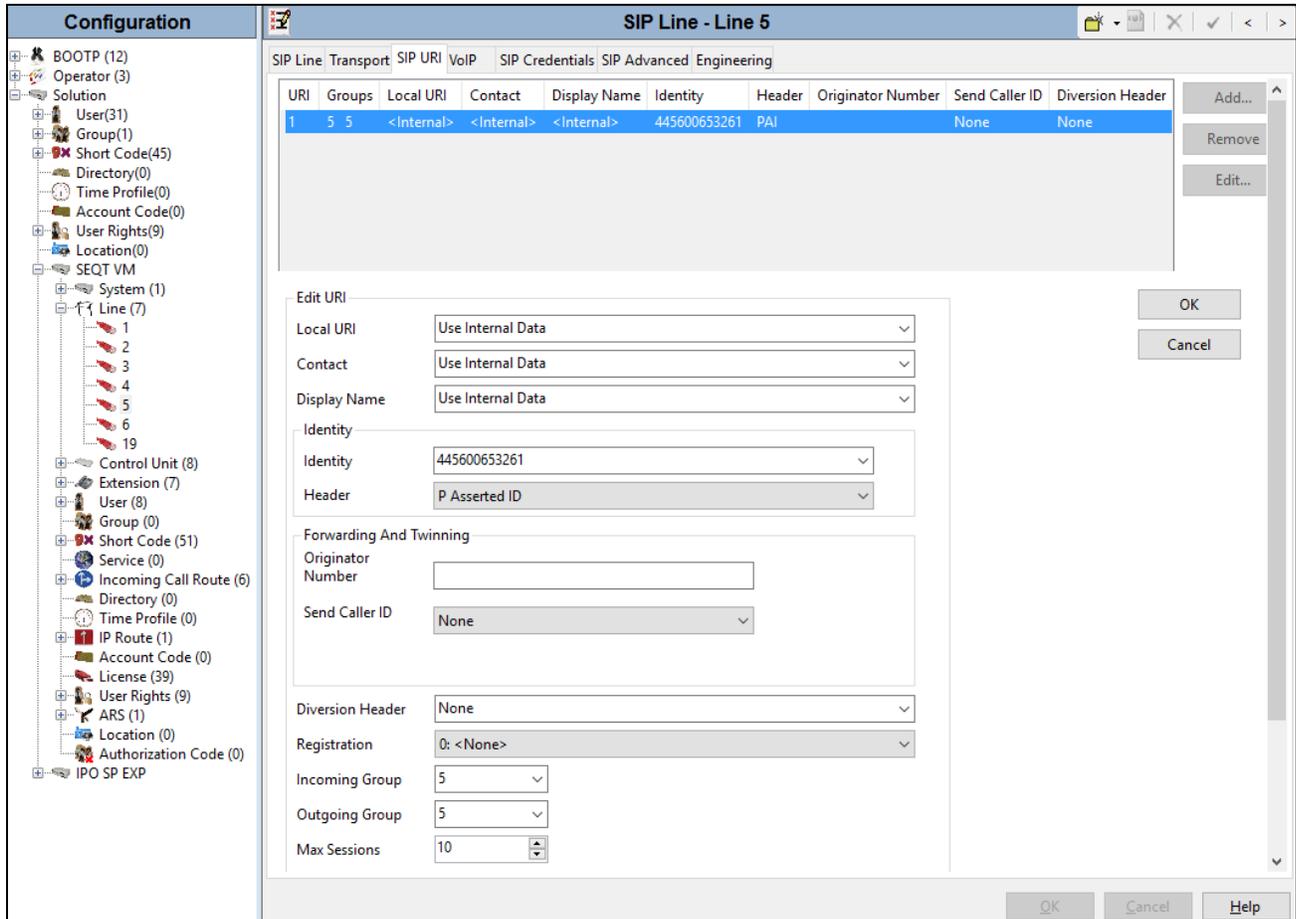
- The **ITSP Proxy Address** is set to the internal interface of Avaya SBCE.
- **Layer 4 Protocol** is set to **TLS**.
- **Send Port** is set to the port number of IP Office, **5061**.
- **Use Network Topology Info** parameter is set to **LAN 2**. This associates the SIP Line with the parameters in the **System** → **LAN2** → **Network Topology** tab.
- Other parameters retain default values in the screen below.
- Click **OK**.



A **SIP URI** entry **URI 1** is created to match incoming numbers that IP Office will accept on this line. Select the **SIP URI** tab, click **Add** button and then **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button. In the example screen below, a previously configured entry is edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an IP Office user. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**. This setting allows calls on this line which SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.7**.
- Set **Identity** to **pilot number** and **Header** to **P Asserted ID** for **Identity**.
- Set **Send Caller ID** to **None** for **Forward** and **Twinning**.
- Set **Diversion Header** to **None**.
- Associate this line with an incoming line group in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. For the compliance test, a new incoming and outgoing group **5** was defined that only contains this line (line 5).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Other parameters retain default values and or set according customer requirements.
- Click **OK**.

SIP Entry **URI 1** is shown below.



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

- The **Codec Selection** can be selected by choosing *Custom* from the pull-down menu, allowing an explicit ordered list of codecs to be specified.
- Selecting *G.711 ALAW64K, G.711ULAW 64K, G.722 64K and G.729(a) 8K CS-ACELP* codec supported by the BT SIP Trunking service, in the Session Description Protocol (SDP) offer.
- Set **Fax Transport Support** to *T38* from the pull-down.
- Set the **DTMF Support** field to *RFC2833/RFC4733* from the pull-down menu. This directs IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- **Media Security** is set to *Same as System (Preferred)* and check the **Same As System** checkbox.
- Default values may be used for all other parameters.
- Click **OK**.

Configuration

SIP Line - Line 5

SIP Line Transport SIP URI VoIP SIP Credentials SIP Advanced Engineering

Codec Selection: Custom

Unused: [Empty Box]

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

Local Hold Music:

Re-invite Supported:

Codec Lockdown:

Allow Direct Media Path:

Force direct media with phones:

PRACK/100rel Supported:

Fax Transport Support: T38

DTMF Support: RFC2833/RFC4733

Media Security: Same as System (Preferred)

Advanced Media Security Options: Same As System

Encryptions: RTP, RTCP

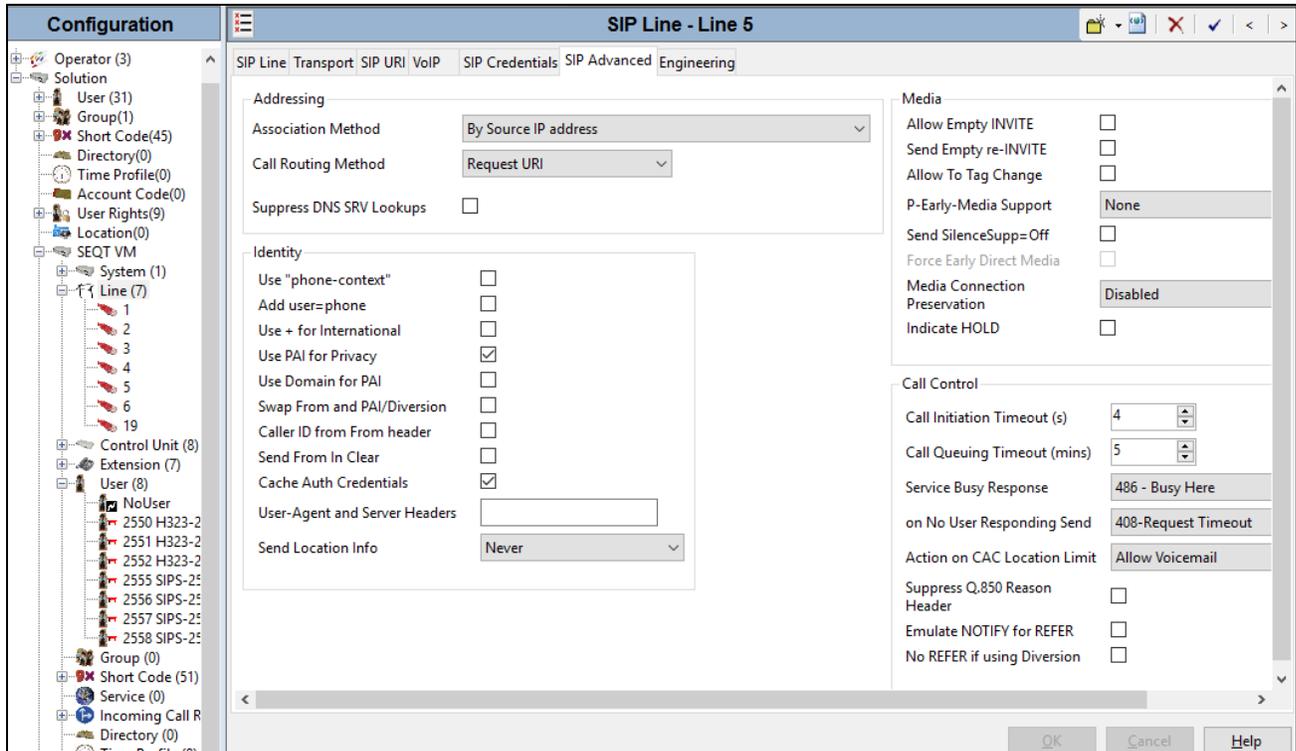
Authentication: RTP, RTCP

Replay Protection: SRTP Window Size: 64

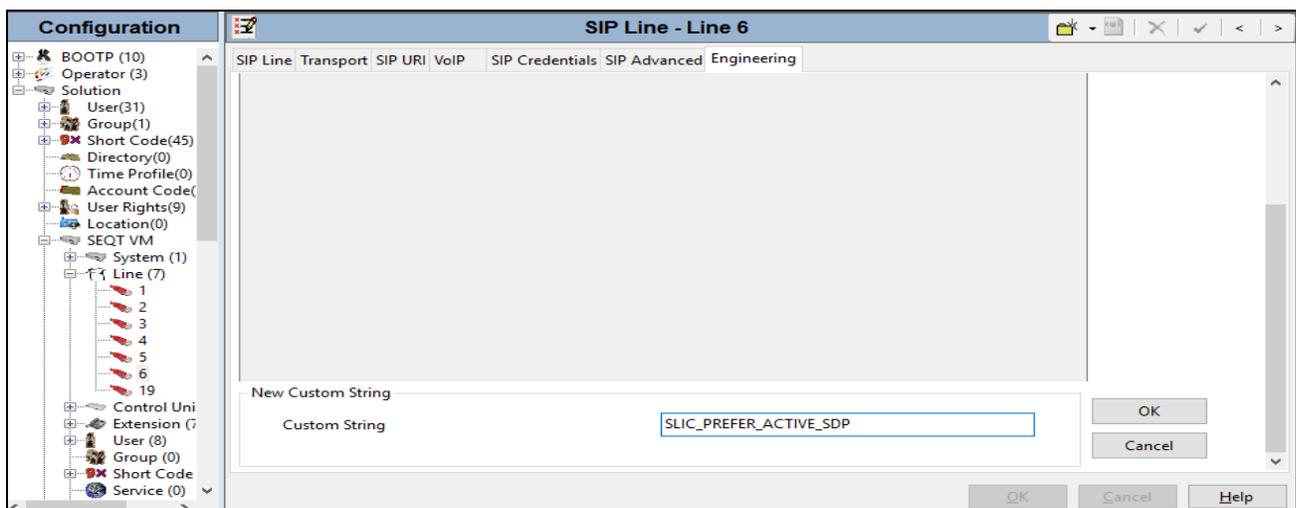
Crypto Suites: SRTP_AES_CM_128_SHA1_80, SRTP_AES_CM_128_SHA1_32

OK Cancel Help

Select the **Advanced** tab, enable **Use PAI for Privacy** parameter. Click **OK**.

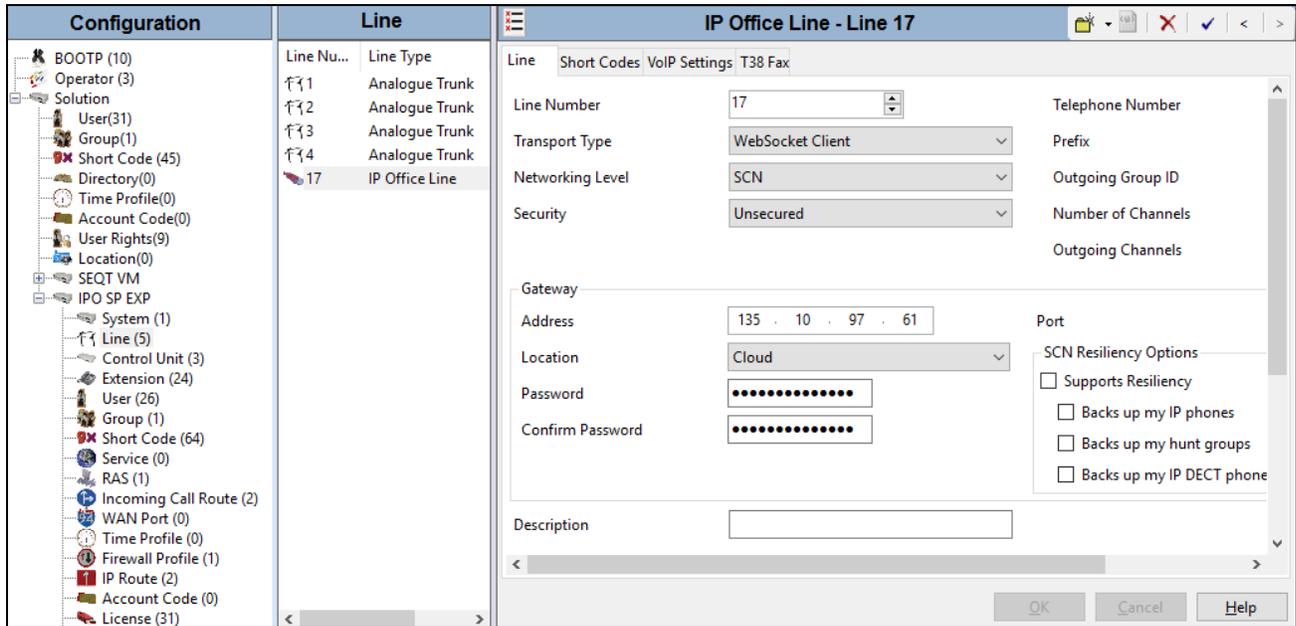


Avaya IP Office sent re-INVITE to negotiate fax T.38 with Session Description Protocol containing the media description for audio port number 0, following the media description for fax “image port# udptl t38”. Even though it was RFC compliant, Service Provider system could not handle it properly. Therefore, a costumed string “**SLIC_PREFER_ACTIVE_SDP**” was added to the SIP line configuration to swap the order of the media description of “image port# udptl t38” on top. To set this costumed string, select the **Engineering** tab, click **Add** button and then enter the **Custom String** as shown. Click **OK**.



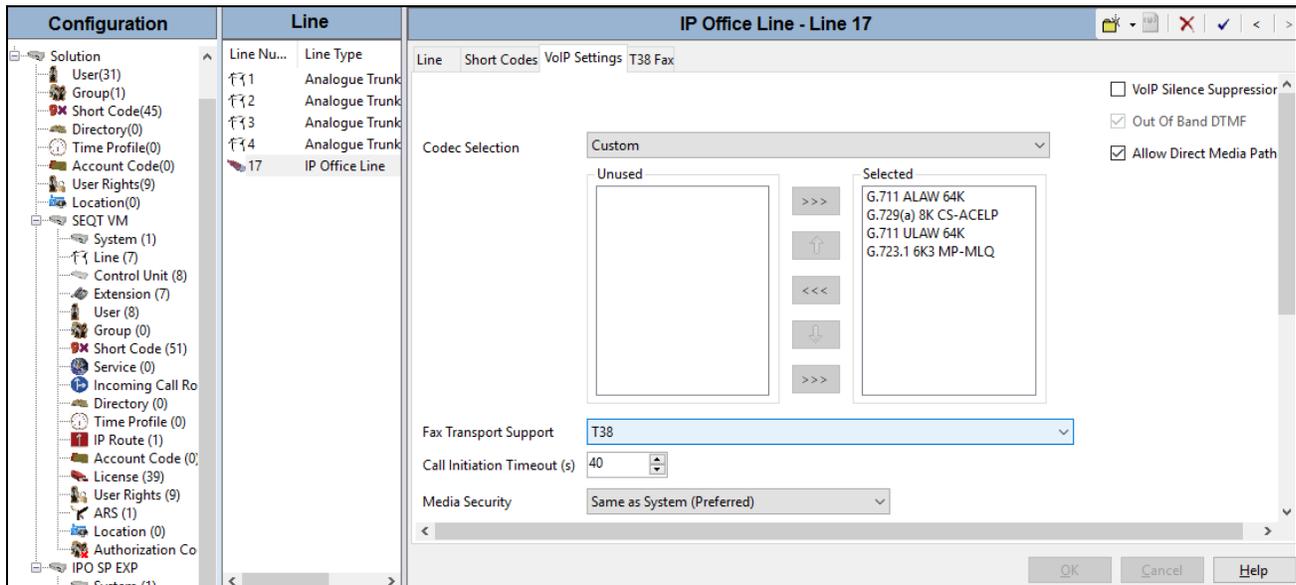
5.5. IP Office Line

The IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. Below is the IP Office Line to the Primary server.



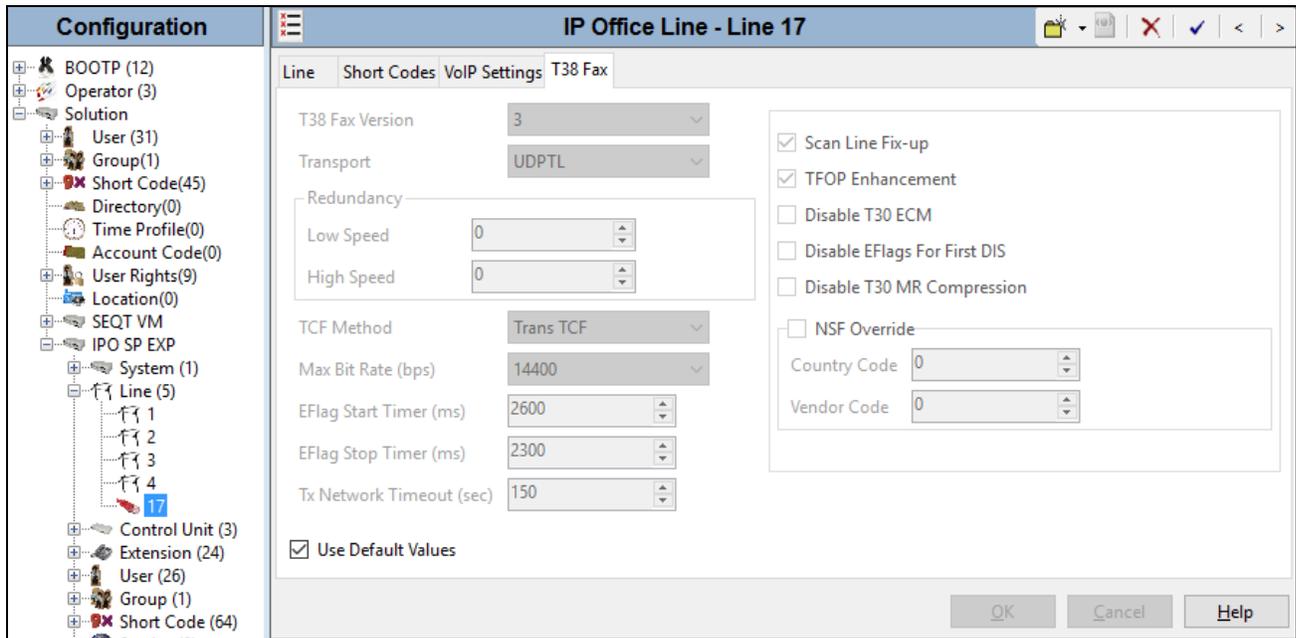
In this testing configuration, a fax machine is connected to one of the analog ports on the Expansion System. To accommodate T.38 fax, select the **VoIP Settings** tab and configure the following:

- Select **T38** for **Fax Transport Support**.



Select the **T38 Fax** tab and enter the following:

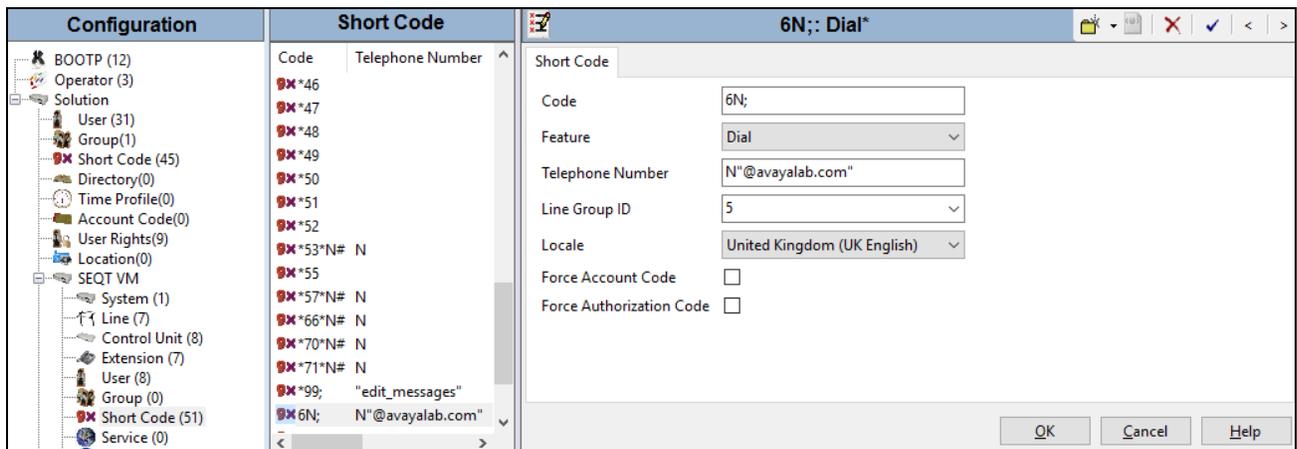
- Ensure the **Use Default Value** is enabled. This will allow the Avaya IP Office to match whatever version of T.38 fax supported by service provider.
- Click **OK**.



5.6. Short Code

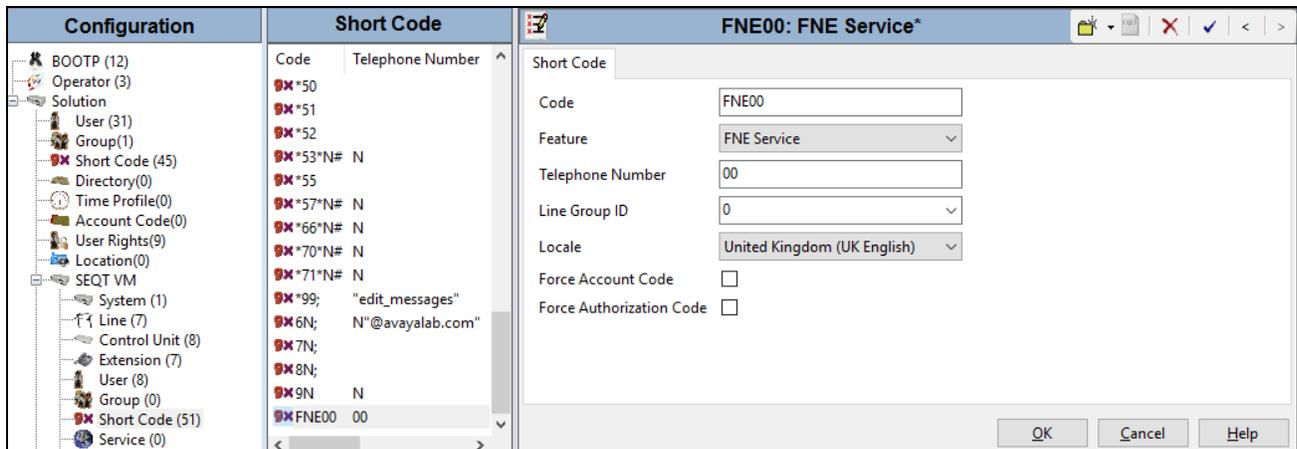
Define a short code to route outbound traffic to the SIP line. To create a short code, select **Short Code** in the left **Navigation** pane, then right-click in the **Group** pane and select **New**. On the **Short Code** tab in the **Details** pane, configure the parameters for the new short code to be created. The screen below shows the details of the previously administered “6N;” short code used in the test configuration.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **6N;** this short code will be invoked when the user dials 6 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to the value shown in the capture bellow. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value *N* represents the number dialed by the user. The host part following the “@” is the domain of the enterprise network.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4**. This short code will use this line group when placing the outbound call.
- Set **Local** to **United Kingdome (UK English)**.
- Others parameters are at default values.
- Click **OK**.



For incoming calls from mobility extension to FNE (Feature Name/Number Extension) hosted by IP Office to provide dial tone functionality, Short Code **FNE00** was created. The FNE00 was configured with the following parameters.

- In the **Code** field, enter the FNE feature code as **FNE00** for dial tone.
- Set the **Feature** field to **FNE Service**.
- Set the **Telephone Number** field to **00**.
- Set the **Line Group ID** field to **0**.
- Set **Local** to **United Kingdom (UK English)**.
- Retain default values for other fields.
- Click **OK**.



5.7. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.4**. To configure these settings, first select **User** in the left **Navigation** pane, then select the name of the user to be modified in the center **Group** pane. In the example below, the name of the user is “H323-2551”. Select the **SIP** tab in the **Details** pane.

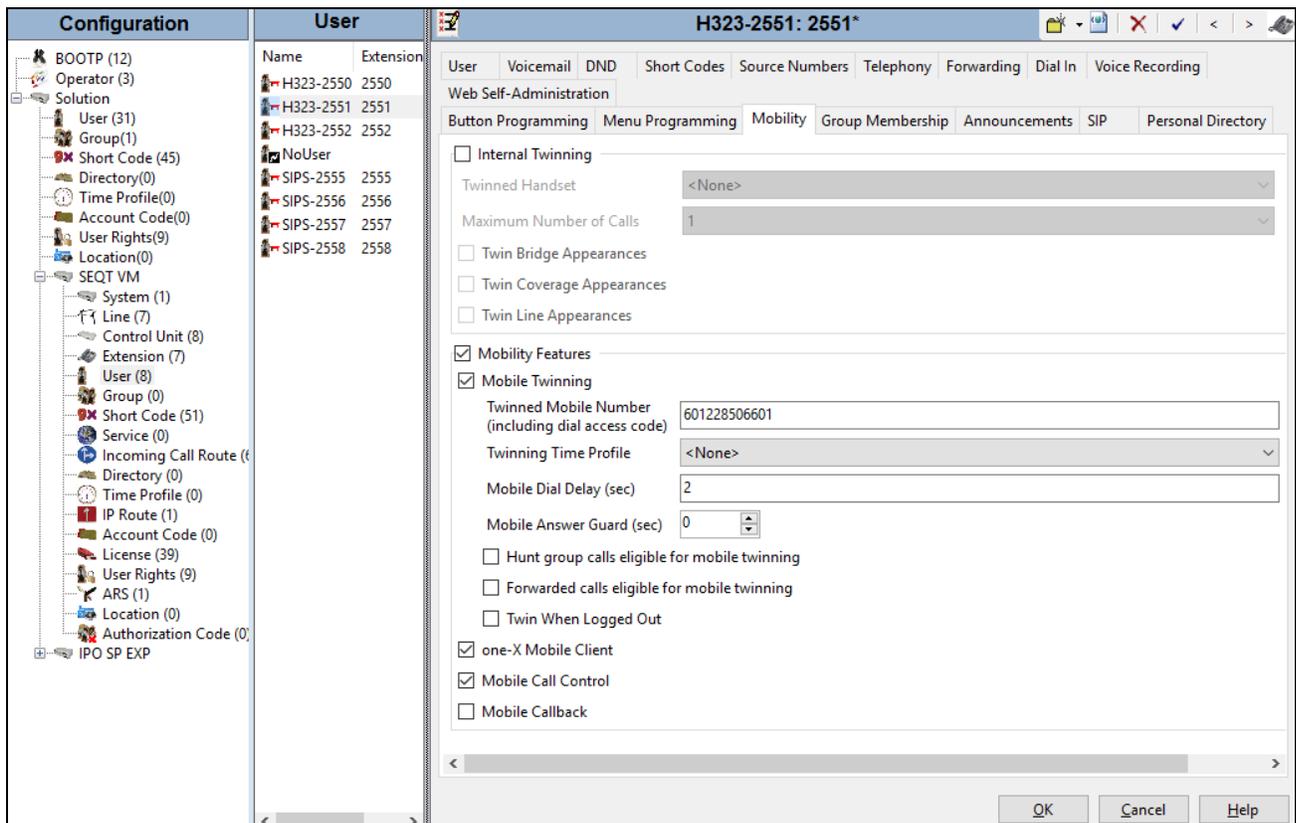
The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. They also allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.4**). The example below shows the settings for user H323-2551.

- The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise from service provider.
- The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.
- If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user’s information from the network.
- Click **OK**.

Configuration	User	Details: H323-2551: 2551
BOOTP (12)	Name	User
Operator (3)	Extension	Voicemail
Solution	H323-2550 2550	DND
User (31)	H323-2551 2551	Short Codes
Group(1)	H323-2552 2552	Source Numbers
Short Code (45)	NoUser	Telephony
Directory(0)	SIPS-2555 2555	Forwarding
Time Profile(0)	SIPS-2556 2556	Dial In
Account Code(0)	SIPS-2557 2557	Voice Recording
User Rights(9)	SIPS-2558 2558	Personal Directory
Location(0)		Web Self-Administration
SEQT VM		Button Programming
System (1)		Menu Programming
Line (7)		Mobility
Control Unit (8)		Group Membership
Extension (7)		Announcements
User (8)		SIP

One of the H.323 IP Phones at the enterprise site uses the Mobile Twinning feature. The following screen shows the **Mobility** tab for User H323-2551.

- The **Mobility Features** and **Mobile Twinning** boxes are checked.
- The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone, in this case **601228506601**.
- Check **Mobile Call Control** check-box.
- Other options can be set according to customer requirements.
- Click **OK**.

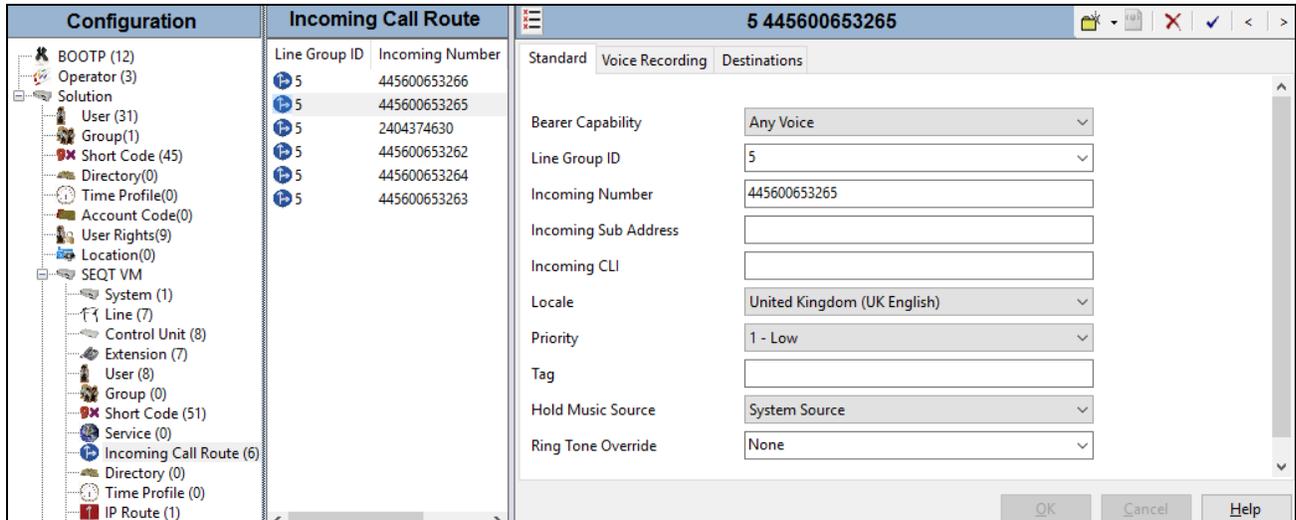


5.8. Incoming Call Route

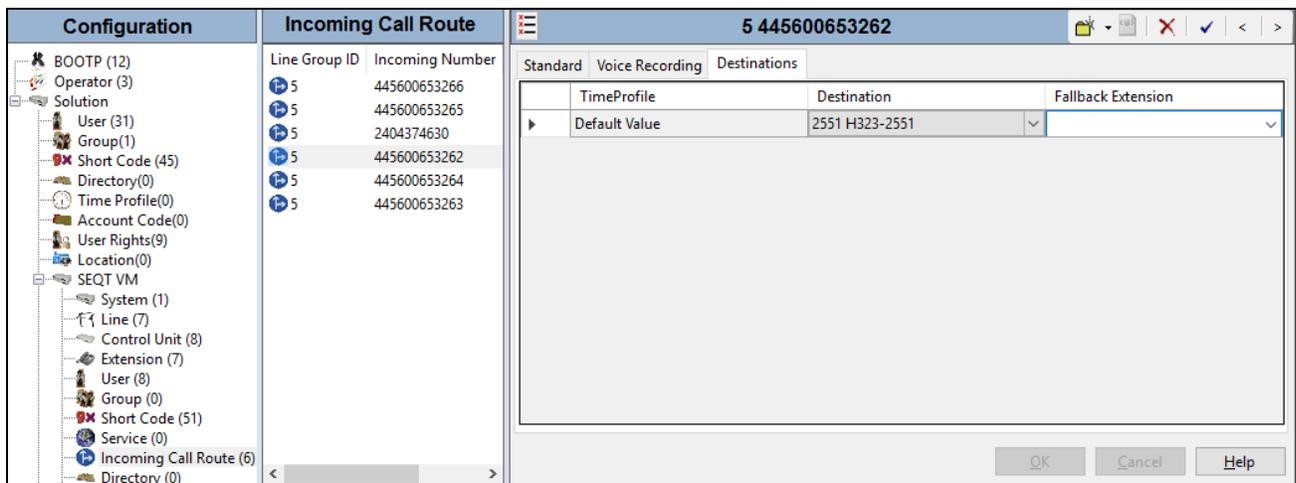
An incoming call route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by the service provider. To create an incoming call route, select **Incoming Call Route** in the left **Navigation** pane, then right-click in the center **Group** pane and select **New**. On the **Standard** tab of the **Details** pane, enter the parameters as shown below:

- Set the **Bearer Capacity** to *Any Voice*.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.4**.
- Set the **Incoming Number** to the incoming number on which this route should match.
- Set **Local** to *United Kingdom (UK English)*.
- Default values can be used for all other fields.
- Click **OK**.

An Incoming Call Route is shown below.



On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **445600653262** on line 5 are routed to extension **2551**. Click **OK**.



5.9. Save Configuration

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

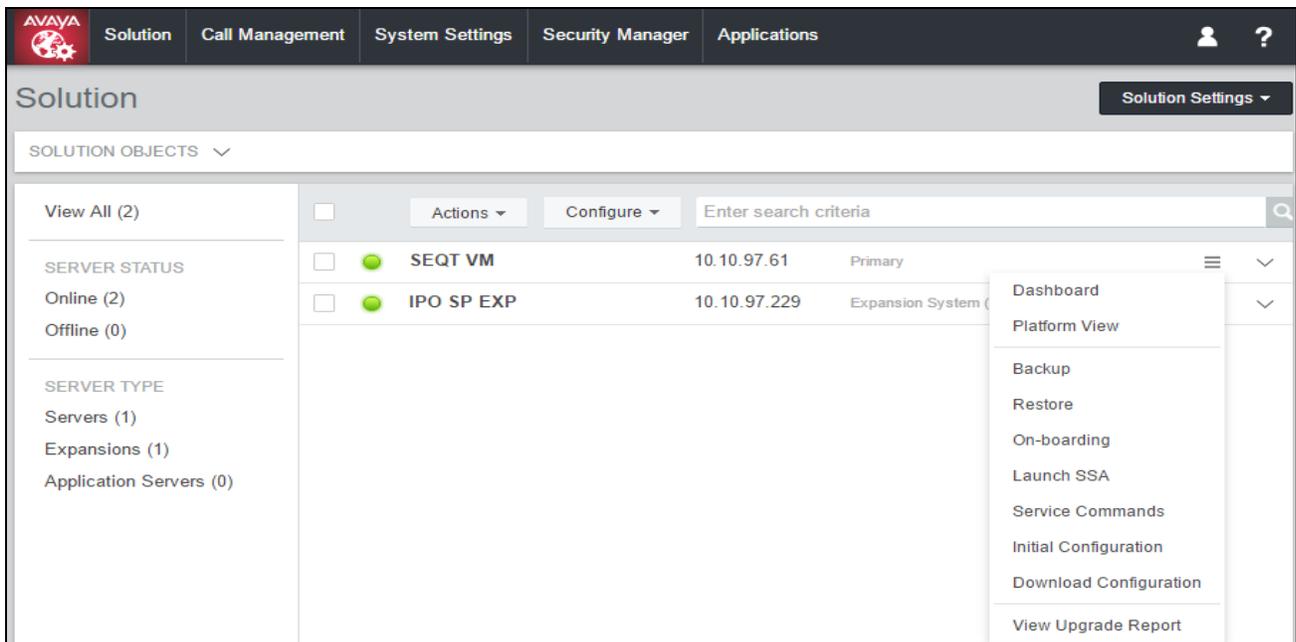
5.10. Avaya IP Office TLS Certificate Management

This section provides a procedure on how to download the IP Office certificate which is being installed on Avaya SBCE for the communication between Avaya system's components using TLS connectivity.

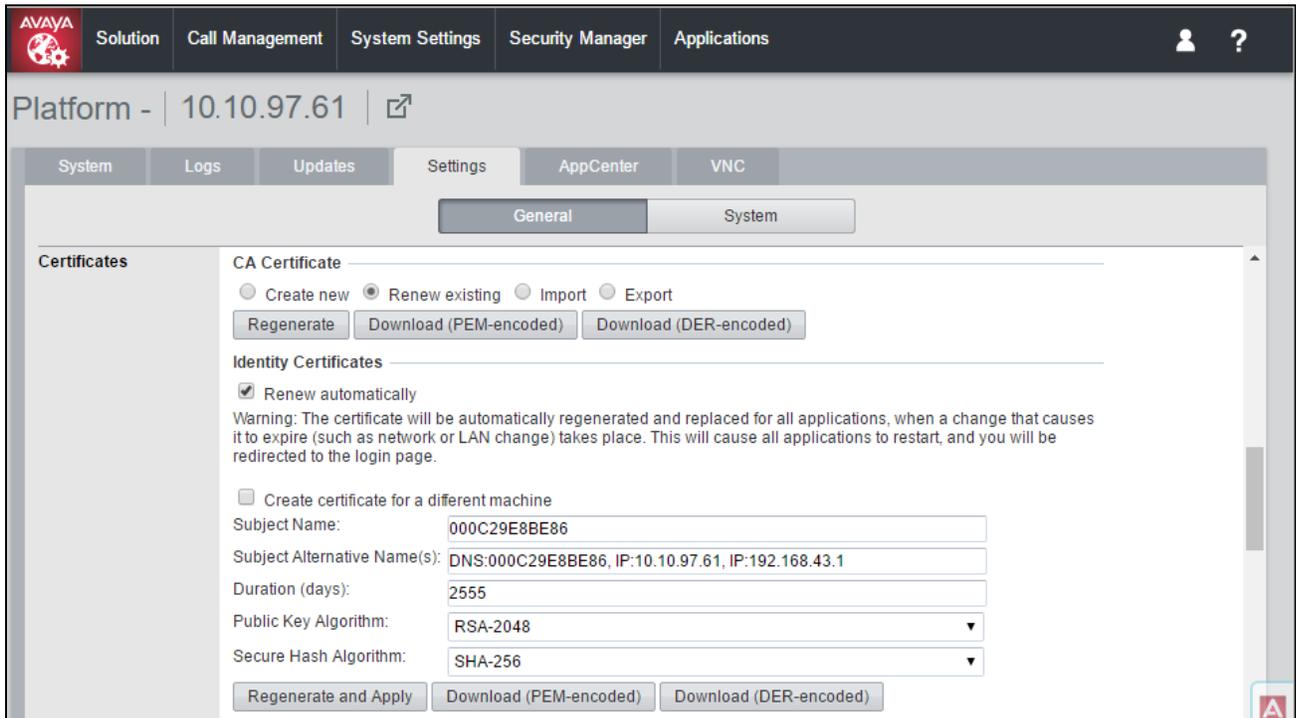
To download the IP Office certificate, launch a web browser and log in Avaya IP Office Web Management as shown below.



On the **Solution** page, click on drop-down menu on the right and select **Platform View** as shown.



On the **Platform** page, click on **Settings** and scroll down to **Certificates** section. At **CA Certificate** section, click on the **Download (PEM-encoded)** button to obtain the IP Office CA certificate.



6. Configure the Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the software has already been installed. For additional information on these configuration tasks, see **Section 10**.

The compliance testing comprised the configuration for two major components, Trunk Server for the service provider and Call Server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration is defined in the Avaya SBCE web user interface as described in the following sections.

Trunk Server configuration elements for the service provider - BT:

- Global Profiles:
 - URI Groups
 - Routing
 - Topology Hiding
 - Server Interworking
 - Signaling Manipulation
 - Server Configuration
- Domain Policies:
 - Application Rules
 - Media Rules
 - Signaling Rules
 - Endpoint Policy Group
 - Session Policy
- Device Specific Settings:
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows → Server Flows
 - Session Flows

Call Server configuration elements for the enterprise - IP Office:

- Global Profiles:
 - URI Groups
 - Routing
 - Topology Hiding
 - Server Interworking
 - Server Configuration
- Domain Policies:
 - Application Rules
 - Media Rules
 - Signaling Rules
 - Endpoint Policy Group
 - Session Policy
- TLS Management

- Certificates
- Client Profiles
- Server Profiles
- Device Specific Settings:
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows → Server Flows
 - Session Flows

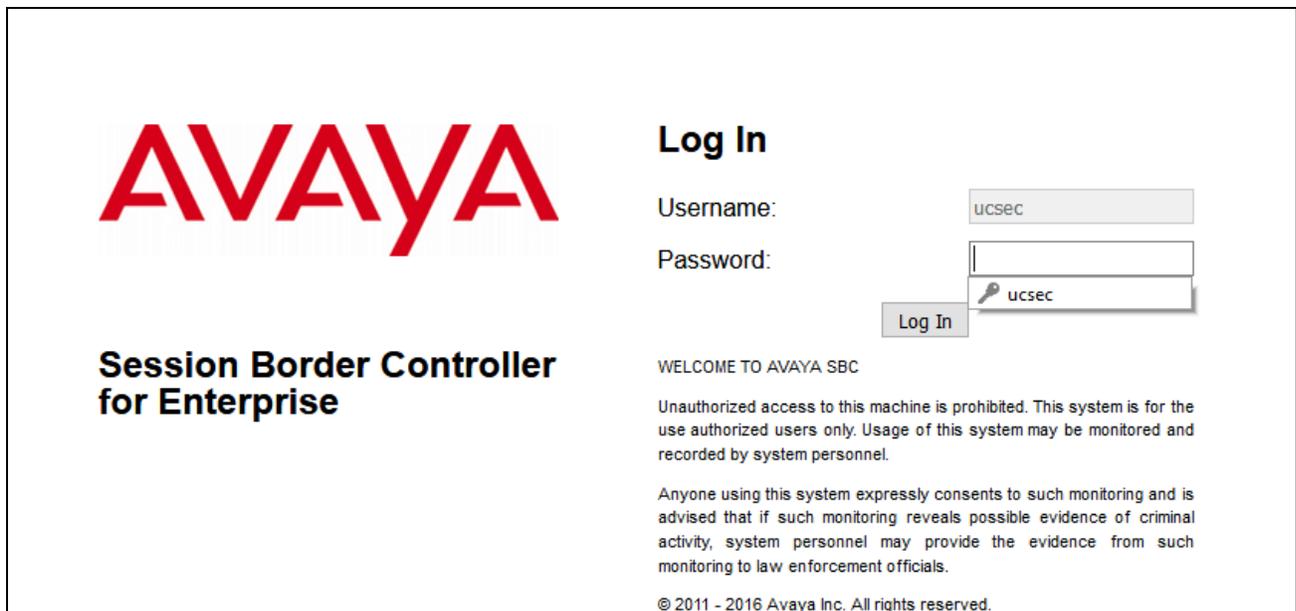
The naming convention used in this entire section is as follows:

- **SP** is stand for Service Provider, which is BT in this case.
- **EN** is stand for Enterprise Network, which refers to Avaya IP Office.

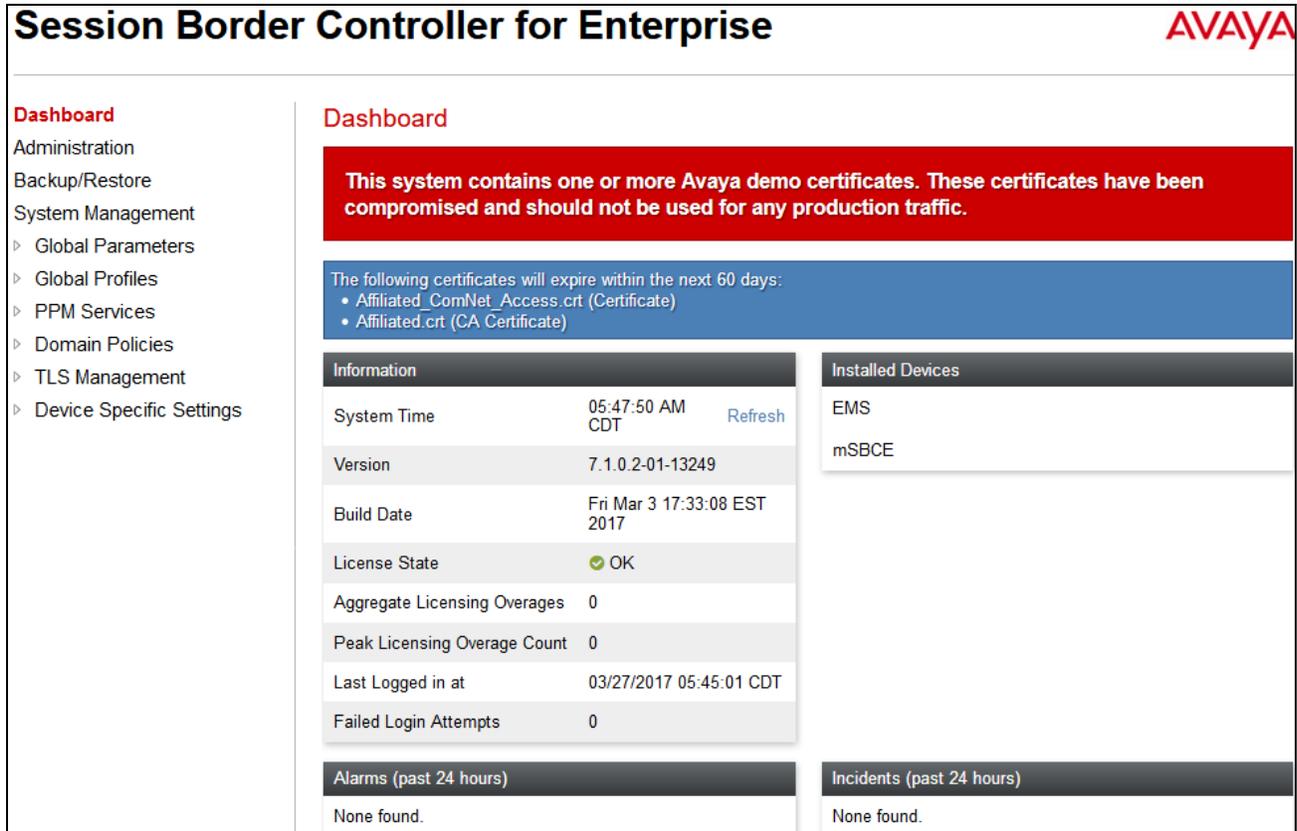
6.1. Log into the Avaya Session Border Controller for Enterprise

Use a Web browser to access the Avaya SBCE Web interface, enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the management IP address.

Enter the appropriate credentials then click **Log In**.



The **Dashboard** main page will appear as shown below.



Session Border Controller for Enterprise AVAYA

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

The following certificates will expire within the next 60 days:

- Affiliated_ComNet_Access.crt (Certificate)
- Affiliated.crt (CA Certificate)

Information	
System Time	05:47:50 AM CDT Refresh
Version	7.1.0.2-01-13249
Build Date	Fri Mar 3 17:33:08 EST 2017
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	03/27/2017 05:45:01 CDT
Failed Login Attempts	0

Installed Devices
EMS
mSBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

6.2. TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. The Avaya SBCE utilizes TLS primarily to facilitate secure communications with remote users.

Avaya SBCE is preinstalled with several certificates and profiles that can be used to quickly set up secure communication using TLS, which are listed in the Pre-installed Avaya Profiles and Certificates section. IP Office, Avaya SBCE and the 96x1 IP Deskphones are shipped with a default identity certificate to enable out-of-box support for TLS sessions. Do not use this default certificate in a production/customer environment since this certificate is common across all instances of IP Office, Avaya SBCE and the 96x1 IP Deskphones. Avaya SBCE supports the configuration of third-party certificates and TLS settings. For optimum security, Avaya recommends using third-party CA certificates for enhanced security.

Testing was done with default identity certificate. The procedure to obtain and install third party CA certificates is outside the scope of these application notes.

In this compliance testing, TLS transport is used for the communication between IP Office and Avaya SBCE. The following procedures show how to create the client and server profiles.

6.2.1. Certificates

You can use the certificate management functionality that is built into the Avaya SBCE to control all certificates used in TLS handshakes. You can access the Certificates screen from **TLS Management** → **Certificates**.

Ensure the preinstalled certificates are presented in the system as shown below.

- **AvayaSBCCA.crt** is Avaya SBCE Certificate Authority root certificate.
- **root-ca.pem** is the IP Office root certificate obtained from **Section 5.10**.

The screenshot shows the 'Certificates' management page in the Avaya Session Border Controller for Enterprise. The page title is 'Session Border Controller for Enterprise' with the AVAYA logo in the top right. A left-hand navigation menu includes: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management), Certificates (highlighted), Client Profiles, Server Profiles, and Device Specific Settings. The main content area is titled 'Certificates' and contains two buttons: 'Install' and 'Generate CSR'. Below these are four sections: 'Installed Certificates' (listing AvayaSBC.crt and SymantecClass3.pem), 'Installed CA Certificates' (listing AvayaSBCCA.crt and root-ca.pem), 'Installed Certificate Revocation Lists' (stating no lists are installed), and 'Installed Keys' (listing AvayaSBC.key). Each entry in the lists has 'View' and 'Delete' links.

Installed Certificates	
AvayaSBC.crt	View Delete
SymantecClass3.pem	View Delete

Installed CA Certificates	
AvayaSBCCA.crt	View Delete
root-ca.pem	View Delete

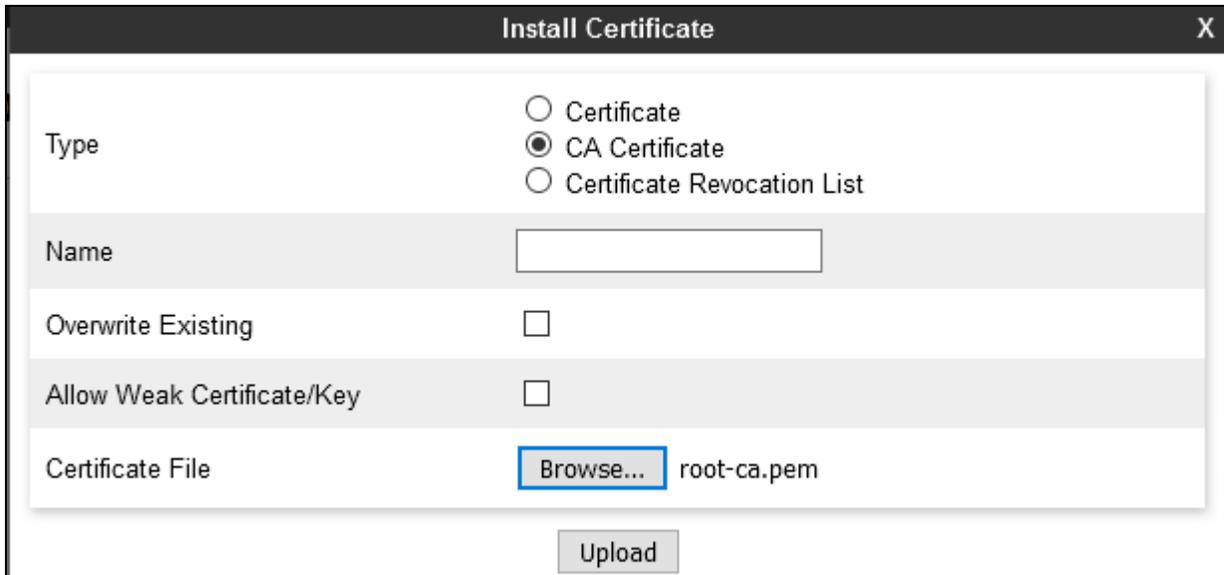
No certificate revocation lists have been installed.

Installed Keys	
AvayaSBC.key	Delete

If the IP Office Certificate Authority certificate (root-ca.pem) is not present, the following procedure will show how to install it here on Avaya SBCE.

IP Office CA certificate is obtained using procedure provided in **Section 5.10**. Then on Avaya SBCE, navigate to **TLS Management → Certificates**. Click on **Install** button.

- Select **CA Certificate**.
- Provide a descriptive **Name**. In the example below, the **Name** field was left empty and default name was used as root-ca.pem.
- **Browse** to the directory where the IP Office CA was previously saved and select it.
- Click **Upload**.



The screenshot shows a dialog box titled "Install Certificate" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Type:** Three radio button options: "Certificate" (unselected), "CA Certificate" (selected), and "Certificate Revocation List" (unselected).
- Name:** An empty text input field.
- Overwrite Existing:** An unchecked checkbox.
- Allow Weak Certificate/Key:** An unchecked checkbox.
- Certificate File:** A text field containing "root-ca.pem" and a "Browse..." button to its left.
- Upload:** A button at the bottom center of the dialog.

6.2.2. Client Profiles

This section describes the procedure to create client profile for Avaya SBCE to communicate with IP Office via TLS signalling. This will be used in **Section 6.3.3.2**.

To create Client profile, navigate to **TLS Management → Client Profiles**, click **Add**.

- Enter descriptive name in **Profile Name**.
- Select *AvayaSBC.crt* from pull down menu of **Certificate**.
- For **Peer Verification**, select IP Office CA certificate which was installed in the above section.
- Enter *1* as **Verification Depth**.
- Click **Finish**.

Capture below illustrates a client profile being created on Avaya SBCE.

Edit Profile X

The selected certificate is known to have been compromised and should not be used in a production environment.

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

TLS Profile

Profile Name

Certificate

Certificate Info

Peer Verification

Peer Certificate Authorities

Peer Certificate Revocation Lists

Verification Depth

Renegotiation Parameters

Renegotiation Time seconds

Renegotiation Byte Count

Handshake Options

Version TLS 1.2 TLS 1.1 TLS 1.0

Ciphers Default FIPS Custom

Value (What's this?)

6.2.3. Server Profiles

This section describes the procedure to create server profile for Avaya SBCE to communicate with IP Office via TLS signalling. This will be used in **Section 6.5.3**.

To create Server profile, navigate to **TLS Management → Server Profiles**, click **Add**.

- Enter descriptive name in **Profile Name**.
- Select **AvayaSBC.crt** from pull down menu of **Certificate**.
- Select **None** from pull down menu of **Peer Verification**.
- Select **Custom** for Ciphers in **Cipher Suit Options** section. And **Value ALL** is specified in the capture shown below.
- Click **Finish**.

Edit Profile

TLS Profile

Profile Name: AvayaSBCServer

Certificate: AvayaSBC.crt

Certificate Info

Peer Verification: None

Peer Certificate Authorities: AvayaSBCCA.crt, VeriSign Universal Root Certification Authority.cer, SMGRCA.pem, Affiliated.crt

Peer Certificate Revocation Lists:

Verification Depth: 0

Renegotiation Parameters

Renegotiation Time: 0 seconds

Renegotiation Byte Count: 0

Handshake Options

Version: TLS 1.2 TLS 1.1 TLS 1.0

Ciphers: Default FIPS Custom

Value (What's this?): ALL

Finish

6.3. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

6.3.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, “*” is used for all incoming and outgoing traffic.

6.3.2. Server Interworking Profile

Interworking Profile features are configured differently for Call Server and Trunk Server.

To create a Server Interworking profile, select **Global Profiles** → **Server Interworking**. Click on the **Add** button.

In the compliance testing, two Server Interworking profiles were created for SP and EN respectively.

6.3.2.1 Server Interworking Profile for SP

Profile **SP-SI** was defined to match the specification of SP. The **General**, **URI Manipulation** and **Advanced** tabs are configured with the following parameters while the other tabs for **Timers**, **Privacy** and **Header Manipulations** are kept as default.

General tab:

- **Hold Support** = *NONE*. The Avaya SBCE will not modify the hold/ resume signaling from EN to SP.
- **18X Handling** = *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from EN to SP.
- **Refer Handling** = *No*. The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from EN to SP.
- **T.38 Support** = *Yes*. SP does support T.38 fax in the compliance testing.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **SP-SI**, **General**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo on the right. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and PPM Services. The "Server Interworking" category is expanded, showing a list of profiles including "SP-SI".

The main content area is titled "Interworking Profiles: SP-SI" and includes an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." and a list of tabs: "General", "Timers", "Privacy", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is selected, showing a table of parameters:

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

An "Edit" button is located at the bottom right of the configuration area.

Advanced tab:

- **Record Routes = Both Sides.** The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Include End Point IP for Context Lookup = Yes.**
- **Extensions = None.**
- **Has Remote SBC = Yes.** This setting allows the Avaya SBCE to always use the SDP received from EN for the media.
- **DTMF Support = None.** The Avaya SBCE will send original DTMF method from SP to EN.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **SP-SI, Advanced.**

The screenshot shows the Avaya Session Border Controller for Enterprise configuration interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. On the left is a navigation menu with categories like Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and Server Interworking. The "Server Interworking" section is expanded, showing a list of profiles: IPO_42, IPO_14, IPO_48, SP4_1, and SP4. The "SP-SI" profile is selected. The main content area is titled "Interworking Profiles: SP-SI" and includes an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." and a set of tabs: "General", "Timers", "Privacy", "URI Manipulation", "Header Manipulation", and "Advanced". The "Advanced" tab is active, displaying a table of settings:

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

An "Edit" button is located at the bottom right of the settings table.

6.3.2.2 Server Interworking Profile for EN

Profile **EN-SI** was defined to match the specification of EN. The **General** and **Advanced** tabs are configured with the following parameters while the other settings for **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** are kept as default.

General tab:

- **Hold Support** = *NONE*.
- **18X Handling** = *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from SP to EN.
- **Refer Handling** = *No*. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from SP to EN.
- **T.38 Support** = *Yes*. To match with SP profile.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **EN-SI**, **General**.

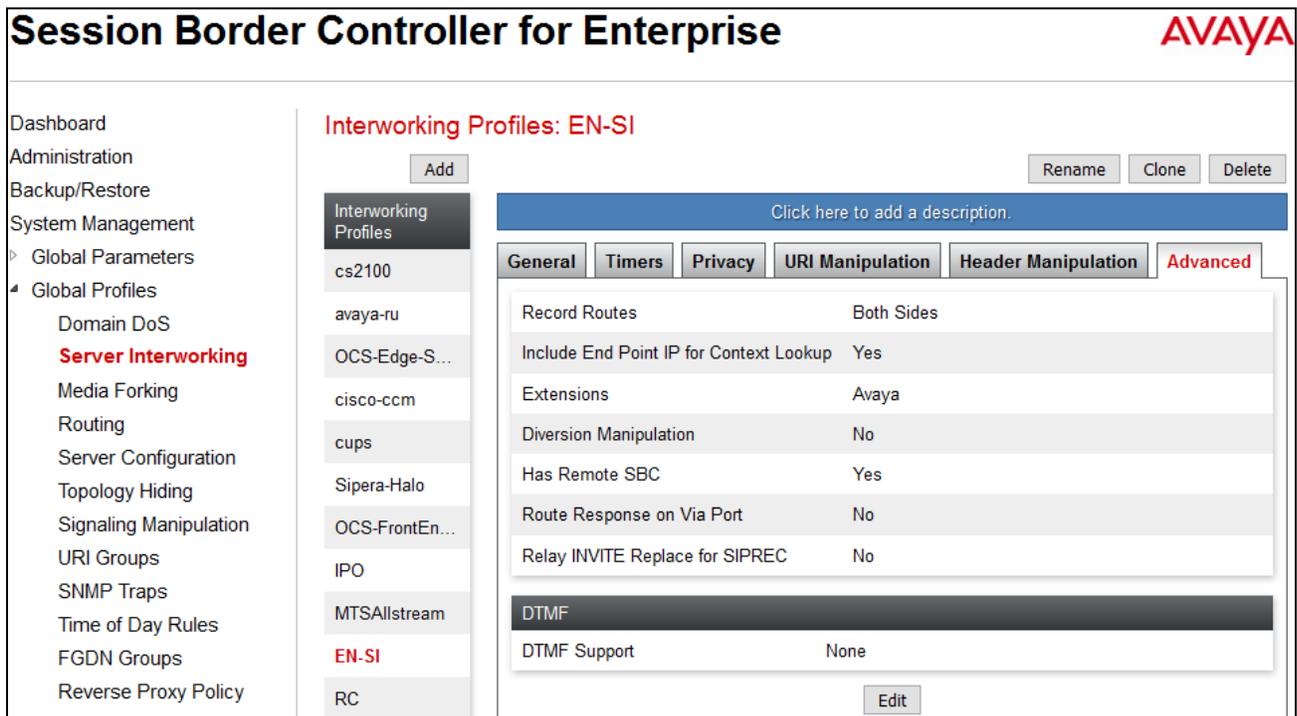
The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and PPM Services. The 'Server Interworking' option is highlighted in red. The main content area is titled 'Interworking Profiles: EN-SI' and features a list of profiles on the left, including 'EN-SI' which is highlighted in red. On the right, the configuration for the 'EN-SI' profile is displayed, showing various parameters under the 'General' tab.

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

Advanced tab:

- **Record Routes = Both Sides.** The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Include End Point IP for Context Lookup = Yes.**
- **Extensions = Avaya.**
- **Has Remote SBC = Yes.** This setting allows the Avaya SBCE to always use the SDP received from EN for the media.
- **DTMF Support = None.** The Avaya SBCE will send original DTMF method from SP to EN.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **EN-SI, Advanced.**



6.3.3. Server Configuration

Server Configuration screen contains four tabs: **General, Authentication, Heartbeat,** and **Advanced.** These tabs are used 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.

To create a Server Configuration entry, select **Global Profiles → Server Configuration.** Click **Add** button. In the compliance testing, two separate Server Configurations were created, server entry **SP-SC** for SP and server entry **EN-SC** for EN.

6.3.3.1 Server Configuration for SP

Server Configuration named **SP-SC** was created for the SP. It will be discussed in detail below.

General and **Advanced** tabs are provisioned for SP on the SIP trunk for every outbound call from enterprise to PSTN. The **Authentication** and **Heartbeat** tabs are left at default, disabled.

General tab: Click **Add** button and enter following information.

- Enter **Profile Name** *SP-SC* and click **Next** button (not shown).
- Set **Server Type** for SP as *Trunk Server*.
- Enter provided **IP Address/FQDN** of SP. Transport *UDP* and listening on port *5060*.
- Click **Next**, **Next** and **Finish** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking, Media Forking, Routing, and Server Configuration (highlighted in red). The main content area is titled "Server Configuration: SP-SC" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. Below this is a "Server Profiles" list with items IPO, RC, ThinkTel, IPO_210, EN-SC, and SP-SC (highlighted). The configuration details for SP-SC are shown in the "General" tab, which includes a "Server Type" field set to "Trunk Server" and a table for "IP Address / FQDN", "Port", and "Transport".

IP Address / FQDN	Port	Transport
ipcomms-btw-metro2.bt.com	5060	UDP

Authentication tab:

Click on the **Edit** button and enter following information.

- Check **Enable Authentication** check box.
- Enter **User Name** (provided by SP).
- Enter **Realm** (provided by SP).
- Enter **Password** and **Confirm Password** (provided by SP) (not shown).

Click **Finish**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. On the left is a navigation menu with categories: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (with sub-items: Domain DoS, Server Interworking, Media Forking, Routing, and Server Configuration), and Topology Hiding. The "Server Configuration" section is active, showing "Server Configuration: SP-SC". There are "Add", "Rename", "Clone", and "Delete" buttons. Below this is a tabbed interface with "General", "Authentication", "Heartbeat", and "Advanced" tabs. The "Authentication" tab is selected, displaying a form with the following fields: "Enable Authentication" (checked), "User Name" (avayaipoffice), and "Realm" (siptavaya.com). An "Edit" button is located at the bottom right of the form.

Heartbeat tab:

Click on the Edit button and enter following information.

- **Enable Heartbeat** is enabled.
- **Method** is *REGISTER*.
- **Frequency** is set to *60 seconds*.
- **From URI** and **To URI** are set as shown in capture.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface, similar to the previous one. The "Heartbeat" tab is selected in the tabbed interface. The form displays the following configuration: "Enable Heartbeat" (checked), "Method" (REGISTER), "Frequency" (60 seconds), "From URI" (445600653261@siptavaya.com), and "To URI" (445600653261@siptavaya.com). An "Edit" button is located at the bottom right of the form.

Advanced tab: Click **Edit** button and enter following information.

- **Interworking Profile** drop down list, select **SP-SI** as defined in **Section 6.3.2**.
- The other settings are kept as default. Click **Finish** (not shown).

The screenshot shows the configuration page for a Server Profile named 'SP-SC'. The left sidebar contains a navigation menu with 'Server Configuration' highlighted. The main content area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced', with 'Advanced' selected. The configuration table is as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-SI
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>

6.3.3.2 Server Configuration for EN

Server Configuration named **EN-SC** created for EN is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as *disabled* as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from SP to EN to query the status of the SIP trunk.

General tab: Click **Add** button then specifying the following.

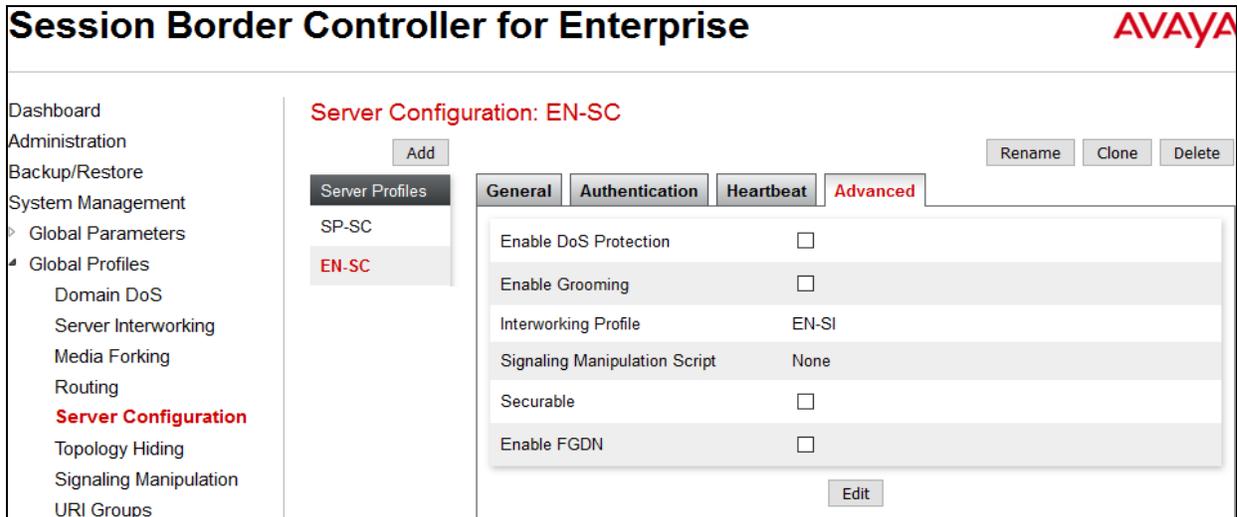
- **Server Type** for EN as **Call Server** and click **Next** button (not shown).
- **IP Address/FQDN** is IP Office WAN port IP address.
- **Transport**, between the Avaya SBCE and IP Office was **TLS**, and **Port 5061**.
- **TLS Client Profile** is the profile created in **Section 6.2.2**.
- Click **Next**, **Next** and **Finish** (not shown).

The screenshot shows the configuration page for a Server Profile named 'EN-SC'. The left sidebar contains a navigation menu with 'Server Configuration' highlighted. The main content area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced', with 'General' selected. The configuration table is as follows:

Server Type	Call Server	
TLS Client Profile	AvayaSBCCClient-Q	
IP Address / FQDN	Port	Transport
10.10.97.61	5061	TLS

Advanced tab: Click **Edit** button then enter the following information.

- **Interworking Profile** drop down list select **EN-SI** as defined in **Section** Error! Reference source not found..
- The other settings are kept as default.



The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the Avaya logo in the top right. A left-hand navigation menu includes options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking, Media Forking, Routing, **Server Configuration**, Topology Hiding, Signaling Manipulation, and URI Groups. The main content area is titled "Server Configuration: EN-SC" and features an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this, there are tabs for "General", "Authentication", "Heartbeat", and "Advanced". The "Advanced" tab is active, showing a list of configuration options: "Enable DoS Protection" (checkbox), "Enable Grooming" (checkbox), "Interworking Profile" (dropdown set to "EN-SI"), "Signaling Manipulation Script" (set to "None"), "Securable" (checkbox), and "Enable FGDN" (checkbox). An "Edit" button is located at the bottom right of the configuration area.

6.3.4. 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.

To create a Routing profile, select **Global Profiles** → **Routing** then click on the **Add** button.

In the compliance testing, routing profile **SP-RP** was created to be used in conjunction with the Server Flow (see **Section 6.5.4**) defined for EN. This entry is to route outgoing calls from the enterprise to SP.

In the opposite direction, Routing profile **EN-RP** was created to be used in conjunction with the Server Flow (see **Section 6.5.4**) defined for SP. This entry is to route incoming calls from SP to the EN.

6.3.4.1 Routing Profile for SP

The screenshot below illustrates the routing profile from Avaya SBCE to the SP network, **Global Profiles → Routing: SP-RP**. As shown in **Figure 1**, the SP SIP trunk is connected with transportation protocol **UDP**. If there is a match in the “To” or “Request URI” headers with the URI Group “*” defined in **Section Error! Reference source not found.**, the call will be routed to the **Next Hop Address** which is the IP address of SP SIP trunk.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups

Routing Profiles: SP-RP

Add Rename Clone Delete

Click here to add a description.

Routing Profile

Update Priority Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	ipcomms-btw-metro2.bt.com	UDP	Edit Delete

6.3.4.2 Routing Profile for EN

The Routing Profile for SP to EN, **EN-RP** was defined to route call where the “To” header matches the URI Group “*” defined in **Section Error! Reference source not found.** to **Next Hop Address** which is the IP address of IP Office WAN port as a destination. As shown in **Figure 1**, the SIP trunk between EN and the Avaya SBCE is connected with transportation protocol **TLS**.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Server Interworking
Media Forking
Routing

Routing Profiles: EN-RP

Add Rename Clone Delete

Click here to add a description.

Routing Profile

Update Priority Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.10.97.61	TLS	Edit Delete

6.3.5. Topology Hiding

Topology Hiding is a security feature of the Avaya SBCE which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select **Global Profiles** → **Topology Hiding** then click on the **Add Profile** (not shown).

In the compliance testing, two Topology Hiding profiles were created: **SP-TH** and **EN-TH**.

6.3.5.1 Topology Hiding Profile for SP

Topology Hiding profile **SP-TH** was defined for outgoing calls to SP as shown in the capture below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. On the left is a navigation menu with categories like Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and Reverse Proxy Policy. Under Global Profiles, "Topology Hiding" is selected and highlighted in red. The main content area is titled "Topology Hiding Profiles: SP-TH" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. A blue bar contains the text "Click here to add a description." Below this is a table titled "Topology Hiding" with the following data:

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

An "Edit" button is located at the bottom right of the table.

6.3.5.2 Topology Hiding Profile for EN

Topology Hiding profile **EN-TH** was defined for incoming calls to IP Office as shown in the capture below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. On the left is a navigation menu with categories like Administration, System Management, Global Parameters, Global Profiles, Routing, and Signaling Manipulation. The "Topology Hiding" option is highlighted in red. The main content area is titled "Topology Hiding Profiles: EN-TH" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." A table titled "Topology Hiding" lists various headers and their corresponding actions and values. An "Edit" button is located at the bottom right of the table.

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

6.4. Domain Policies

The Domain Policies feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

6.4.1. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

To clone a signaling rule, navigate to **Domain Policies** → **Signaling Rules**, select the **default** rule then click on the **Clone Rule** button (not shown).

In the compliance testing, two **Signaling Rules** were created for the SP and EN.

6.4.1.1 Signaling Rule for SP

Clone the Signaling Rule **default** with a descriptive name (e.g., **SP-SR**) and click on the **Finish** button (not shown). Verify that **General** settings of **SP-SR** with **Inbound** and **Outbound Request** are set to **Allow**, and **Enable Content-Type Checks** is enabled with **Action** and **Multipart-Action** are set to **Allow** (not shown).

On the **Signaling QoS** tab, enter the following information.

- Select the correct Quality of Service (QoS).
- The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for signaling.

The following screen shows the QoS value used for the compliance testing.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, and Signaling Rules. The main content area is titled "Signaling Rules: SP-SR" and includes an "Add" button, a "Filter By Device..." dropdown, and "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." and a list of tabs: "General UCID", "Requests", "Responses", "Request Headers", "Response Headers", and "Signaling QoS". The "Signaling QoS" tab is selected, showing a table with the following configuration:

Signaling QoS	<input checked="" type="checkbox"/>
QoS Type	DSCP
DSCP	EF

An "Edit" button is located at the bottom right of the configuration area.

6.4.1.2 Signaling Rule for EN

Clone the Signaling Rule **default** with a descriptive name (e.g., **EN-SR** for EN) and click on the **Finish** button (not shown). Verify that **General** settings of **EN-SR** with **Inbound** and **Outbound Request** are set to **Allow**, and **Enable Content-Type Checks** is enabled with **Action** and **Multipart-Action** are set to **Allow** (not shown). Similarly the Signaling QoS rules are set as shown in capture below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, and Signaling Rules. The main content area is titled "Signaling Rules: EN-SR" and includes an "Add" button, a "Filter By Device..." dropdown, and "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." and a list of tabs: "General UCID", "Requests", "Responses", "Request Headers", "Response Headers", and "Signaling QoS". The "Signaling QoS" tab is selected, showing a table with the following configuration:

Signaling QoS	<input checked="" type="checkbox"/>
QoS Type	DSCP
DSCP	EF

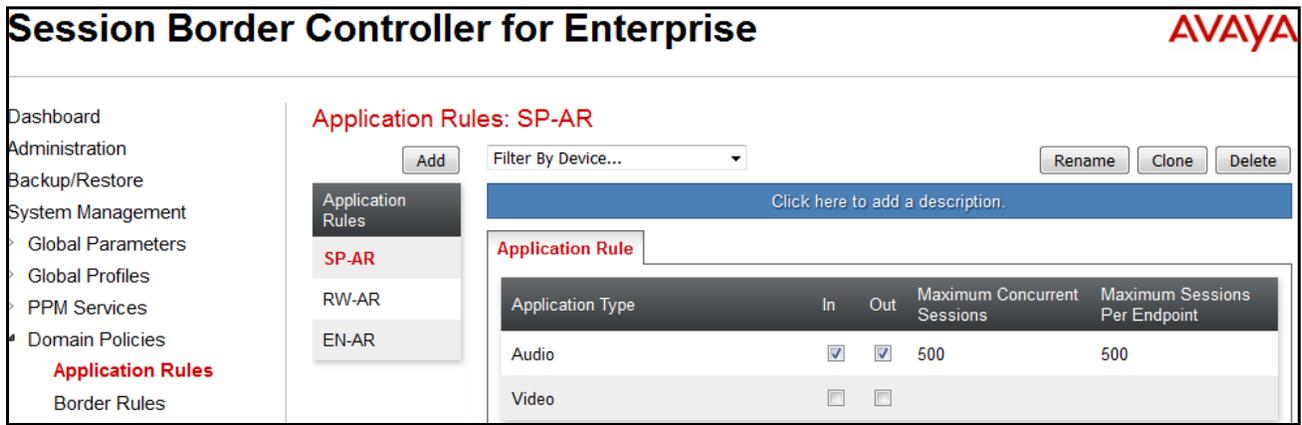
An "Edit" button is located at the bottom right of the configuration area.

6.4.2. Application Rules

Application Rules define which type of SIP based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, user can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

6.4.2.1 Application Rule for SP

Clone the Application Rule **default** with a descriptive name (e.g., **SP-AR** for service provider) and click the **Edit** button to change value of **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** to **500** respectively as shown and then click the **Finish** button (not shown). Others are left as default.

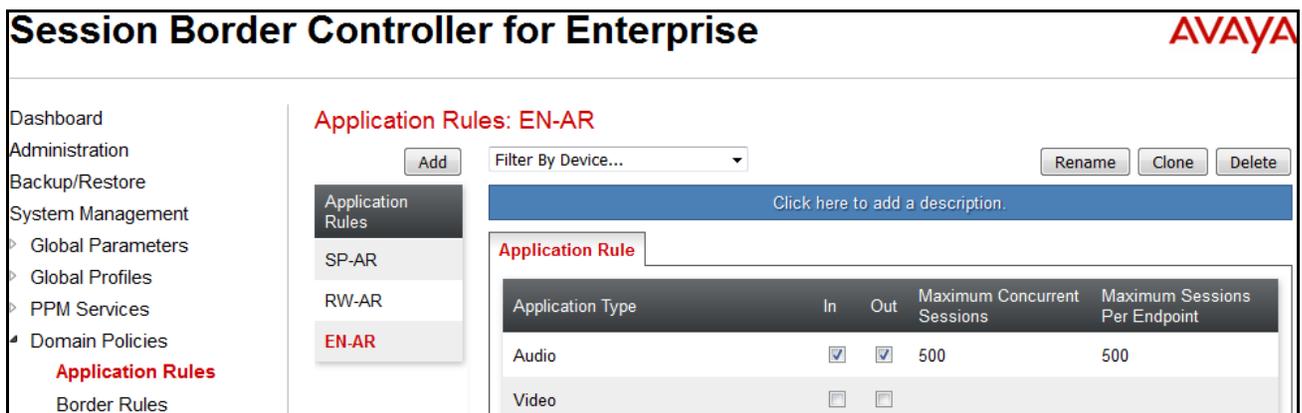


The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The title bar reads "Session Border Controller for Enterprise" and the Avaya logo is in the top right. A left-hand navigation menu includes: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, Application Rules, Border Rules). The main content area is titled "Application Rules: SP-AR". It features an "Add" button, a "Filter By Device..." dropdown, and "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." A table titled "Application Rule" displays the following data:

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	500	500
Video	<input type="checkbox"/>	<input type="checkbox"/>		

6.4.2.2 Application Rule for EN

Similarly, clone the Application Rule **default** with a descriptive name (e.g., **EN-AR** for IP Office) and click the **Edit** button to change value of **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** to **500** respectively as shown and then click the **Finish** button (not shown). Others are left as default.



The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The title bar reads "Session Border Controller for Enterprise" and the Avaya logo is in the top right. A left-hand navigation menu includes: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, Application Rules, Border Rules). The main content area is titled "Application Rules: EN-AR". It features an "Add" button, a "Filter By Device..." dropdown, and "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." A table titled "Application Rule" displays the following data:

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	500	500
Video	<input type="checkbox"/>	<input type="checkbox"/>		

6.4.3. Media Rules

Media rules can be used to 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. You can also define how Avaya SBCE must handle media packets that adhere to the set parameters.

6.4.3.1 Media Rule for SP

In this compliance testing, Secure Real-Time Transport Protocol (SRTP, media encryption) is not supported by SP. Therefore, *default-low-med* rule is used for communication between Avaya SBCE and SP.

6.4.3.2 Media Rule for EN

Secure Real-Time Transport Protocol (SRTP, media encryption) is used between Avaya SBCE and IP Office. Therefore, it is necessary to create a media rule to apply to the internal interface of Avaya SBCE, EN. Created **EN-SRTP-MR** rule is shown below.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. A left-hand navigation menu includes sections like Dashboard, Administration, Backup/Restore, System Management, Domain Policies, and TLS Management. The "Media Rules" section is highlighted in red. The main content area is titled "Media Rules: EN-SRTP-MR" and features an "Add" button, a "Filter By Device..." dropdown, and "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." The configuration is divided into three tabs: "Encryption" (selected), "Codec Prioritization", and "QoS". The "Encryption" tab contains sections for "Audio Encryption" and "Video Encryption".

Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_32 SRTP_AES_CM_128_HMAC_SHA1_80 RTP
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Formats	RTP
Interworking	<input type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input checked="" type="checkbox"/>

An "Edit" button is located at the bottom right of the configuration area.

6.4.4. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to Server Flow defined in **Section 6.5.4**.

Endpoint Policy Groups were separately created for SP and EN. To create a policy group, navigate to **Domain Policies** → **Endpoint Policy Groups** and click on the **Add** button.

6.4.4.1 Endpoint Policy Group for SP

The following screen shows **SP-PG** created for SP.

- Set Application Rule to **SP-AR** which was created in **Section 6.4.2.1**.
- Set Media Rule to **default-low-med**.
- Set Signaling Rule to **SP-SR** which was created in **Section 6.4.1.1**.
- Set Border Rule to **default**.
- Set Security Rule to **default-med**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with 'Domain Policies' expanded to 'End Point Policy Groups'. The main content area is titled 'Policy Groups: SP-PG'. It features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below these are two blue bars with instructions: 'Click here to add a description.' and 'Hover over a row to see its description.'. A 'Policy Group' section contains a table with columns: Order, Application, Border, Media, Security, Signaling, and Summary. The table has one row with the following values: Order: 1, Application: SP-AR, Border: default, Media: default-low-med, Security: default-med, Signaling: SP-SR, and an 'Edit' button.

Order	Application	Border	Media	Security	Signaling	Summary
1	SP-AR	default	default-low-med	default-med	SP-SR	Edit

6.4.4.2 Endpoint Policy Group for EN

Similarly, the following screen shows policy group **EN-PG** created for EN.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with 'Domain Policies' expanded to 'End Point Policy Groups'. The main content area is titled 'Policy Groups: EN-PG'. It features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below these are two blue bars with instructions: 'Click here to add a description.' and 'Hover over a row to see its description.'. A 'Policy Group' section contains a table with columns: Order, Application, Border, Media, Security, Signaling, and Summary. The table has one row with the following values: Order: 1, Application: EN-AR, Border: default, Media: EN-SRTP-MR, Security: default-med, Signaling: EN-SR, and an 'Edit' button.

Order	Application	Border	Media	Security	Signaling	Summary
1	EN-AR	default	EN-SRTP-MR	default-med	EN-SR	Edit

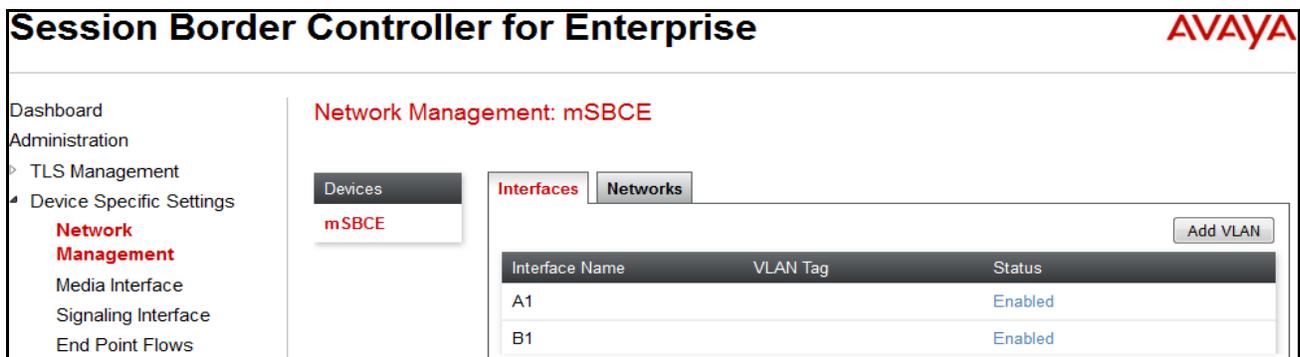
6.5. Device Specific Settings

The Device Specific Settings feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

6.5.1. Network Management

The Network Management page is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP address, public IP address, subnet mask, gateway, etc., to interface the device to the networks. This information populates the various Network Management tabs which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Network Management**, under **Interfaces** tab, enable the interfaces connecting to the inside enterprise and outside service provider networks. To enable an interface, click on “Disable” Status. The following screen shows interface **A1** and **B1** were **Enabled**.



The screenshot shows the Avaya Session Border Controller for Enterprise interface. The page title is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. The left sidebar contains a navigation menu with "Device Specific Settings" expanded to "Network Management". The main content area is titled "Network Management: mSBCE" and has two tabs: "Interfaces" (selected) and "Networks". Under the "Interfaces" tab, there is a table with the following data:

Interface Name	VLAN Tag	Status
A1		Enabled
B1		Enabled

An "Add VLAN" button is located in the top right corner of the interface table.

On the **Networks** tab, verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface was assigned to **A1** and the public interface was assigned to **B1** appropriate to the parameters shown in the **Figure 1**.



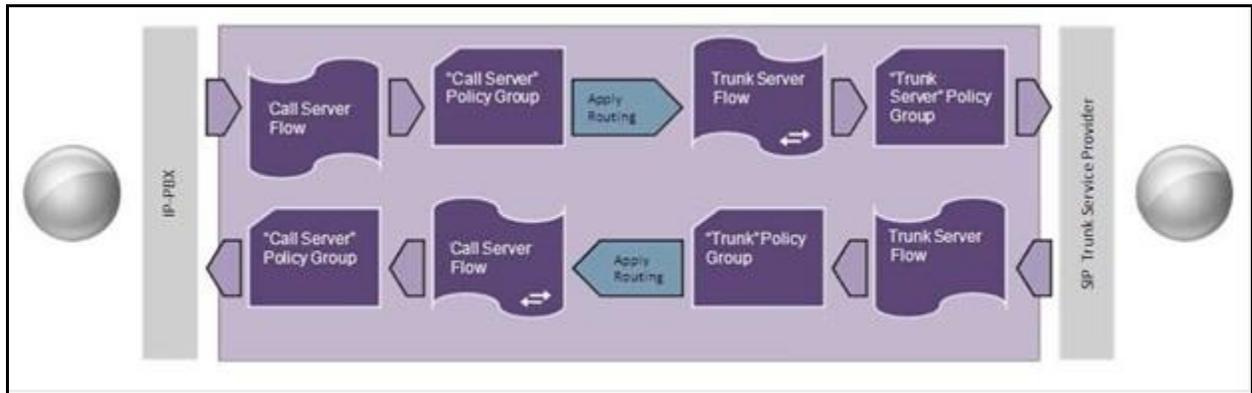
The screenshot shows the Avaya Session Border Controller for Enterprise interface. The page title is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. The left sidebar contains a navigation menu with "Device Specific Settings" expanded to "Network Management". The main content area is titled "Network Management: mSBCE" and has two tabs: "Interfaces" and "Networks" (selected). Under the "Networks" tab, there is a table with the following data:

Name	Gateway	Subnet Mask	Interface	IP Address		
Network_A1	10.10.97.129	255.255.255.192	A1	10.10.97.176	Edit	Delete
Network_B1	10.10.98.97	255.255.255.224	B1	10.10.98.103	Edit	Delete

An "Add" button is located in the top right corner of the network table.

6.5.4. End Point Flows - Server Flow

When a packet is received by the 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. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



In the compliance testing, two separate Server Flows were created for SP and EN.

To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**, select the **Server Flows** tab and click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the other fields were kept as default.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select Server Configuration created in **Section 6.3.3** which the Server Flow associates to.
- **URI Group:** Select "*".
- **Received Interface:** Select the Signaling Interface created in **Section 6.5.3** which is the Server Configuration is designed to receive SIP signaling from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 6.5.3** which is the Server Configuration is designed to send the SIP signaling to.
- **Media Interface:** Select the Media Interface created in **Section 6.5.2** which is the Server Configuration is designed to send the RTP to.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 6.4.4**.
- **Routing Profile:** Select the Routing Profile created in **Section 6.3.4**.
- **Topology Hiding Profile:** Select the Topology Hiding profile created in **Section 6.3.5** to apply toward the Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

The following screen shows the Server Flow **SP-SF** for SP.

Session Border Controller for Enterprise

- Dashboard
- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - PPM Services
 - Domain Policies
 - TLS Management
 - Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows**
 - Session Flows
 - DMZ Services
 - TURN/STUN Service
 - SNMP
 - Syslog Management
 - Advanced Options
 - Troubleshooting

End Point Flows: mSBCE

Devices

Subscriber Flows

Server Flows

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
	SP-SF	*	InsideSIG	OutsideSIG	SP-PG	EN-RP
					EN-PG	SP-RP
					RW	RW-SRTP-PG
						default_RW
					End Point Policy Group	Routing Profile
					IPO_PG	To_ThinkTel
					End Point Policy Group	Routing Profile
					SP4_IPO_42	To_SP4
					IPO_42_RW	default_RW
					End Point Policy Group	Routing Profile
					IP	RC_PG
					End Point Policy Group	Routing Profile
						EN-RP

1
SP-SF
*
InsideSIG
OutsideSIG
SP-PG
EN-RP

Edit Flow: SP-SF

Flow Name

Server Configuration

URI Group

Transport

Remote Subnet

Received Interface

Signaling Interface

Media Interface

Secondary Media Interface

End Point Policy Group

Routing Profile

Topology Hiding Profile

Signaling Manipulation Script

Remote Branch Office

Similarly, the following screen shows the Server Flow **EN-SF** for IP Office.

The screenshot displays the 'Session Border Controller for Enterprise' interface. The main heading is 'End Point Flows: mSBCE'. Below this, there are tabs for 'Devices', 'Subscriber Flows', and 'Server Flows'. The 'Server Flows' tab is active, showing a table of flows. One flow, 'EN-SF', is selected, and an 'Edit Flow: EN-SF' dialog box is open over it.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	EN-SF	*	OutsideSIG	InsideSIG	EN-PG	SP-RP

The 'Edit Flow: EN-SF' dialog box contains the following configuration fields:

- Flow Name: EN-SF
- Server Configuration: EN-SC
- URI Group: *
- Transport: *
- Remote Subnet: *
- Received Interface: OutsideSIG
- Signaling Interface: InsideSIG
- Media Interface: InMedia
- Secondary Media Interface: None
- End Point Policy Group: EN-PG
- Routing Profile: SP-RP
- Topology Hiding Profile: EN-TH
- Signaling Manipulation Script: None
- Remote Branch Office: Any

A 'Finish' button is located at the bottom of the dialog box.

6.6. System Management

To configure the Avaya SBCE device to utilize the DNS/SRV records, navigate to **System Management**. Select **Device** tab as show.

The screenshot displays the 'Session Border Controller for Enterprise' interface. The main heading is 'System Management'. Below this, there are tabs for 'Devices', 'Updates', 'SSL VPN', 'Licensing', and 'Key Bundles'. The 'Devices' tab is active, showing a table of devices.

Device Name	Management IP	Version	Status				
mSBCE	10.10.98.70	7.1.0.2-01-13249	Commissioned	Reboot	Shutdown	Restart Application	View Edit

Click **Edit** and enter the following:

- Under **DNS Settings**, enter **Primary** DNS server IP address (in this testing, public DNS was used to resolve the DNS records being pre-configured by service provider).
- **DNS Client IP** is the external interface IP address of the trunk facing service provider.
- Click **Finish**.

Alarms Incidents S... Edit Device: mSBCE X

Address and interface changes must be made in Network Management.

Any changes to the management network on this device will reboot the device.

General Settings

Appliance Name

Device Settings

High Availability (HA)

DNS Settings

Primary
Ex: 202.201.192.1

Secondary
Optional, Ex: 202.201.192.1

DNS Client IP

Session Bo

AVAYA

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Server Configuration
Topology Hiding

start Application View Edit

7. BT SIP Trunking Configuration

BT is responsible for the configuration of BT SIP Trunking service. The customer will need to provide the IP address used to reach the IP Office at the enterprise, this address will be the outside interface of the Avaya SBCE. BT will provide the customer the necessary information to configure the Avaya IP Office SIP connection to BT. The provided information from BT includes:

- IP address of the BT SIP proxy.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.
- SIP Credentials

8. Verification Steps

The following steps may be used to verify the configuration:

- Use the Avaya IP Office System Status application to verify the state of the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select the SIP line of interest from the left pane. 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).

The screenshot displays the Avaya IP Office System Status application. The left sidebar shows a navigation tree with 'System' selected. The main content area is titled 'SIP Trunk Summary' and shows the following details:

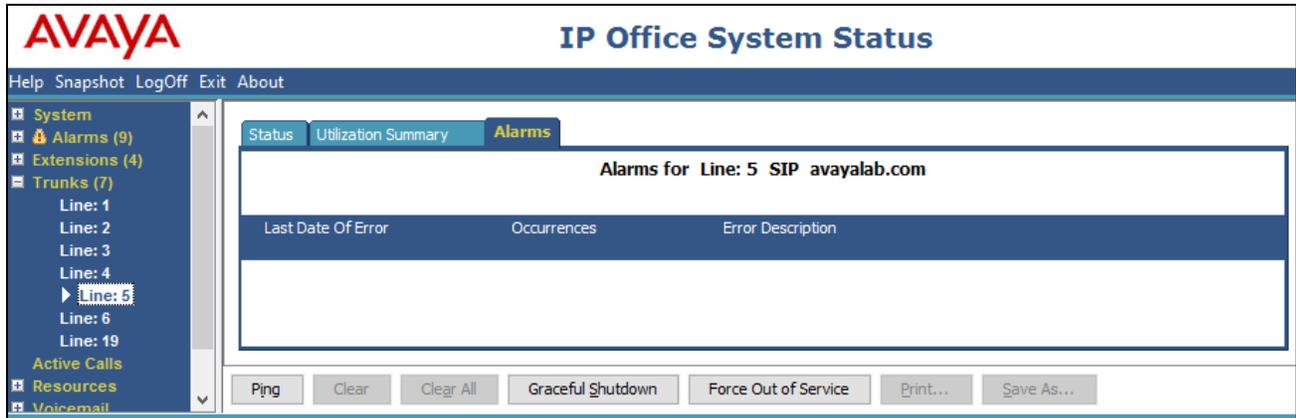
- Line Service State: In Service
- Peer Domain Name: avayalab.com
- Resolved Address: 10.10.97.176
- Line Number: 5
- Number of Administered Channels: 10
- Number of Channels in Use: 0
- Administered Compression: G711 A, G711 Mu, G722, G729 A
- Enable Faststart: Off
- Silence Suppression: Off
- Media Stream: Best Effort
- Layer 4 Protocol: TLS
- SIP Trunk Channel Licenses: 128
- SIP Trunk Channel Licenses in Use: 0 (0%)
- SIP Device Features: REFER (Incoming and Outgoing)

Below the summary is a table showing the status of six channels:

Channel Number	URI G...	Call Ref	Current State	Time in State	Remote Media Ad...	Codec	Connec...	Caller ID or Dial...	Other Party on Call	Direction of Call	Round Trip De...	Receive Jitter	Receive Packet ...	Transmit Jitter	Transmit Packet ...
1			Idle	2 days ...											
2			Idle	2 days ...											
3			Idle	2 days ...											
4			Idle	2 days ...											
5			Idle	2 days ...											
6			Idle	2 days ...											

At the bottom of the application, there are several control buttons: Trace, Trace All, Pause, Pjng, Call Details, Graceful Shutdown, Force Out of Service, Print..., and Save As... The status bar at the bottom right shows the time as 10:29:59 AM and the system as Online.

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



- Verify that a phone connected to PSTN can successfully place a call to the IP Office with two-way audio.
- Verify that a phone connected to IP Office can successfully place a call to the PSTN with two-way audio.
- Using a network sniffing tool (e.g., Wireshark) to monitor the SIP signaling between the enterprise and BT. The sniffer traces are captured at the public interface of the Avaya SBCE.

9. Conclusion

The BT Wholesale Hosted SIP Trunking Service passed compliance testing with any observations/limitations detailed in **Section 2.2**. These Application Notes describe the procedures required to configure the SIP connection between Avaya IP Office, Avaya Session Border Controller for Enterprise and the BT SIP Trunking service as shown in **Figure 1**.

10. Additional References

- [1] *Administering Avaya IP Office Platform with Manager*, Release 10.0, August 2016.
- [2] *Avaya IP Office™ Platform Server Edition Reference Configuration, Release 10.0, Issue 04.AD*, August 2016.
- [3] *Deploying IP Office™ Platform Server Edition Solution*, Release 10.0, August 2016.
- [4] *IP Office™ Platform, Using a Voicemail Pro IP Office Mode Mailbox, Issue 10D*, May 2016.
- [5] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 7.1, Issue 1, June 2016.
- [6] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.1, Issue 1, June 2016.
- [7] *Administering Avaya Session Border Controller for Enterprise*, Release 7.1, Issue 1, June 2016.
- [8] *Application Notes for configuring Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.3 to support Remote Workers*, Issue 1.0.
- [9] *Using Avaya Communicator for Web*, Release 1, Issue 1.0.6, May 2016.

Product documentation for Avaya products may be found at <http://support.avaya.com>. Additional IP Office documentation can be found at:

<http://marketingtools.avaya.com/knowledgebase/>

Product documentation for BT Wholesale Hosted SIP Trunking Service is available from BT.

©2017 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.