



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Intermedia SIP Trunking Using TLS/SRTP with Avaya IP Office 9.1 and Avaya Session Border Controller for Enterprise Release 7.0 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Intermedia Session Initiation Protocol (SIP) Trunking using TLS/SRTP with Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 7.0.

Intermedia SIP Trunking provides PSTN access via a SIP trunk between the enterprise and the Intermedia 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.

Intermedia 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 Intermedia and an Avaya IP Office solution using TLS/SRTP. In the sample configuration, Avaya IP Office solution consists of an Avaya IP Office 500v2 release 9.1.6, Avaya Session Border Controller for Enterprise release 7.0.1 (Avaya SBCE), Avaya Voicemail Pro, Avaya IP Office Softphone, and Avaya H.323, SIP, digital, and analog endpoints.

The Intermedia SIP Trunking service referenced within these Application Notes is designed for business customers. The service enables local and long distance 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 Intermedia SIP Trunking service in TLS/SRTP via 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.

2.1. Interoperability Compliance Testing

A simulated enterprise site with Avaya IP Office was connected to Intermedia SIP Trunking service via 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 with service provider.
- 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 PSTN calls to/from Avaya IP Office Softphone.
- 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.711MU 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 G.711 Pass Through modes.
- Off-net call forwarding.
- Twinning to mobile phones on inbound calls.
- Avaya Communicator for Web (WebRTC).
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

Note:

1. 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 **Reference [9]** respectively.

2.2. Test Results

Intermedia SIP Trunking passed compliance testing.

Items not supported or not tested included the following:

- Inbound toll-free is supported but was not tested as part of the compliance test.
- T.38 Fax is not supported.
- Operator Call (dial 0) and Operator Assisted (dial 0+10digits) are not supported.
- SIP OPTIONS sent by Intermedia is not supported.
- Intermedia does not support SIP Diversion Header.
- Call Redirection using SIP REFER is not supported by Intermedia.

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

- Intermedia does not send SIP OPTIONS message but responded to SIP OPTIONS message.

2.3. Support

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

For technical support on Intermedia SIP Trunking, contact Intermedia at <https://www.intermedia.net>

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to the Intermedia SIP Trunking service via 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 IP Office 500v2 as expansion 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 LAN port of Avaya IP Office is connected to the enterprise LAN while the WAN port is connected to the public IP network. Endpoints include an Avaya 9600 Series IP Telephone (with H.323 firmware), Avaya 11x0 Series IP Telephone (with SIP firmware), an Avaya 9508 Digital Telephones, an Avaya Symphony 2000 Analog Telephone and an Avaya IP Office Softphone. A separate Windows OS PC runs Avaya IP Office Manager to configure and administer Avaya IP Office.

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

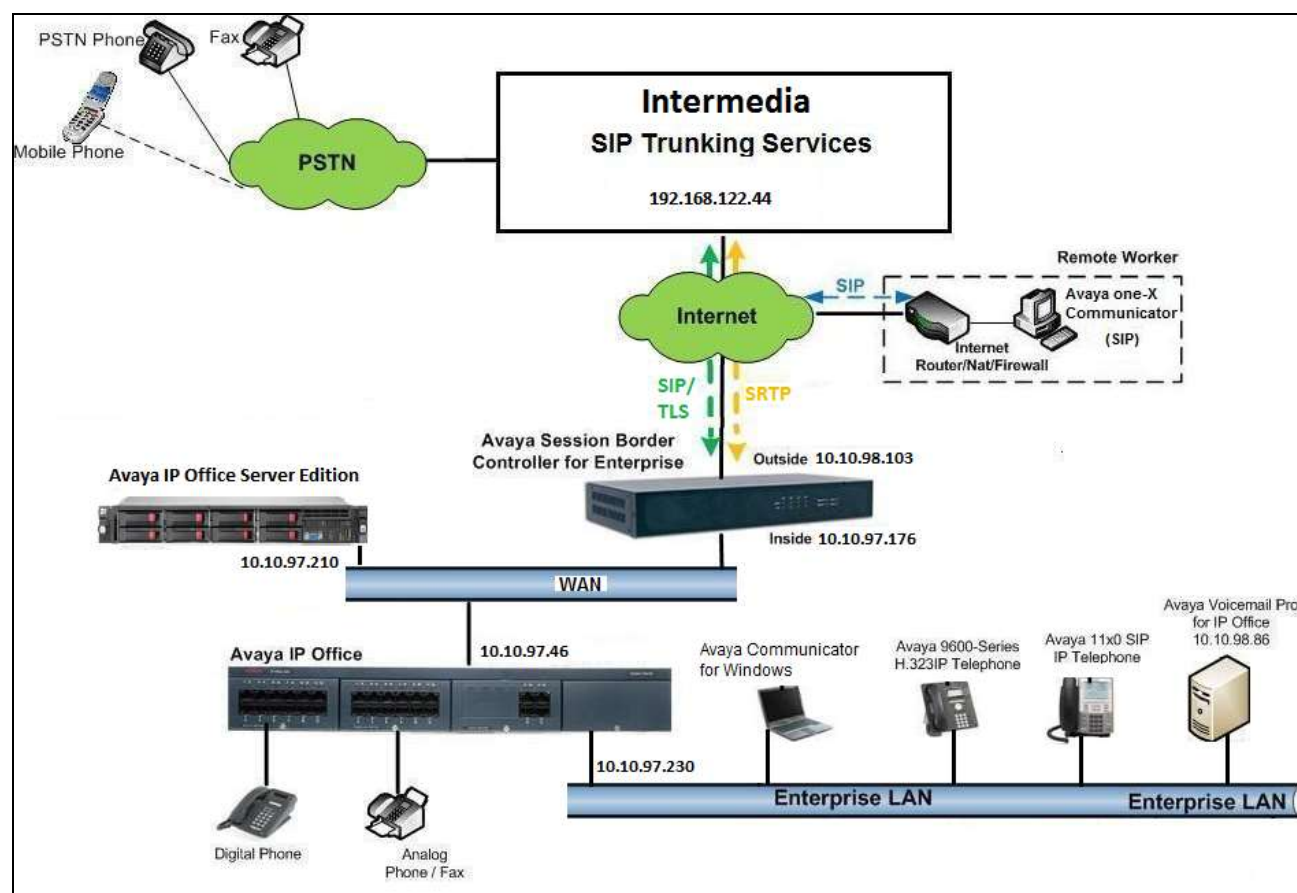


Figure 1: Test Configuration for Avaya IP Office with Intermedia SIP Trunking Service

For the purposes of the compliance test, Avaya IP Office users dialed a short code of 6 + N digits to send digits across the SIP trunk to Intermedia. The short code of 6 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Intermedia. For calls within the North American Numbering Plan (NANP), the user would dial 11 (1 + 10) digits. Thus for these NANP calls, Avaya IP Office would send 11 digits in the Request URI and the To field of an outbound SIP INVITE message. It was configured to send 10 digits in the From field. For inbound calls, Intermedia SIP Trunking sent 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

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	9.1.600.153
Avaya IP Office 500v2 (Expansion)	9.1.600.153
Avaya IP Office Manager	9.1.600.153
Avaya Voicemail Pro for IP Office	9.1.600.153
Avaya Application Server	9.1.600.153
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.0.1-03-8739
Avaya 11x0 IP Telephone (SIP)	SIP11x0e04.04.18.00
Avaya 9621G IP Telephone (H.323)	Avaya one-X® Deskphone Edition S9621
Avaya Communicator for Windows	2.0.3.40
Avaya Communicator for Web (WebRTC)	1.0.16.1217
Avaya Digital Telephone (9508)	0.45
Avaya Symphony 2000 Analog Telephone	N/A
Intermedia SIP Trunking Service Components	
Component	Release
Intermedia SBC	16.14.2
Intermedia Softswitch	16.14.2

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition without T.38 Fax Service.

5. Configure IP Office

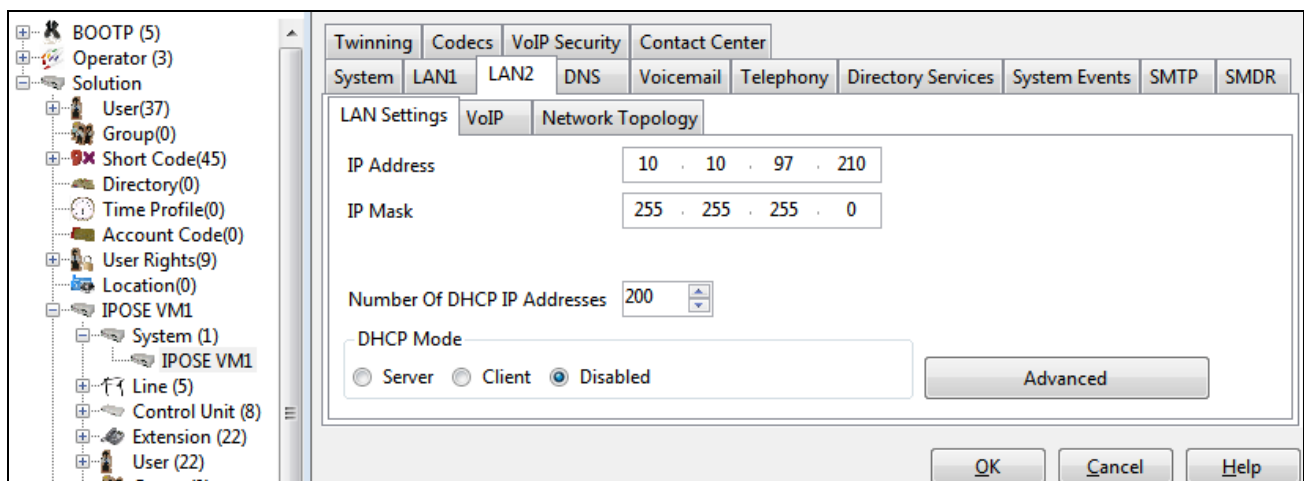
This section describes the Avaya IP Office configuration to support connectivity to Intermedia SIP Trunking service through Avaya SBCE. Avaya IP Office is configured through Avaya IP Office Manager PC application. From a PC running Avaya IP Office Manager application, select **Start → Programs → IP Office → 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 IP Office Manager can be customized using the **View** menu. In the 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. These panes will be referenced throughout the 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 and IP Office Softphone support) is assumed to be already in place.

5.1. LAN Settings

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

To access the LAN settings, first navigate to **System (1) → IPO SP** in the Navigation and Group Panes 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.

- The **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as 9600-Series IP Telephones used in the sample configuration.
- The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks to Intermedia.
- The **SIP Registrar Enable** box is checked to allow IP Office Softphone usage.
- The **Layer 4 Protocol**, check the **TLS** box and set **TLS Port** to **5061**.
- The **Keepalives**, select **RTP-RTCP** for **Scope** and **Enabled** for **Initial keepalives** from pull down menus respectively.
- **Periodic timeout** is **30**.
- All other parameters should be set according to customer requirements.
- Click **OK**.

The screenshot shows the Avaya IP Office configuration interface. The left sidebar displays a tree view of the system configuration, including sections like BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE VM1, System, IPOSE VM1, Line, Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, Directory, Time Profile, IP Route, Account Code, License, User Rights, ARS, Location, Authorization Code, IPO EXP210, System, Line, Control Unit, Extension, User, Group, Short Code, Service, RAS, Incoming Call Route, WAN Port, Time Profile, Firewall Profile, IP Route, and Account Code.

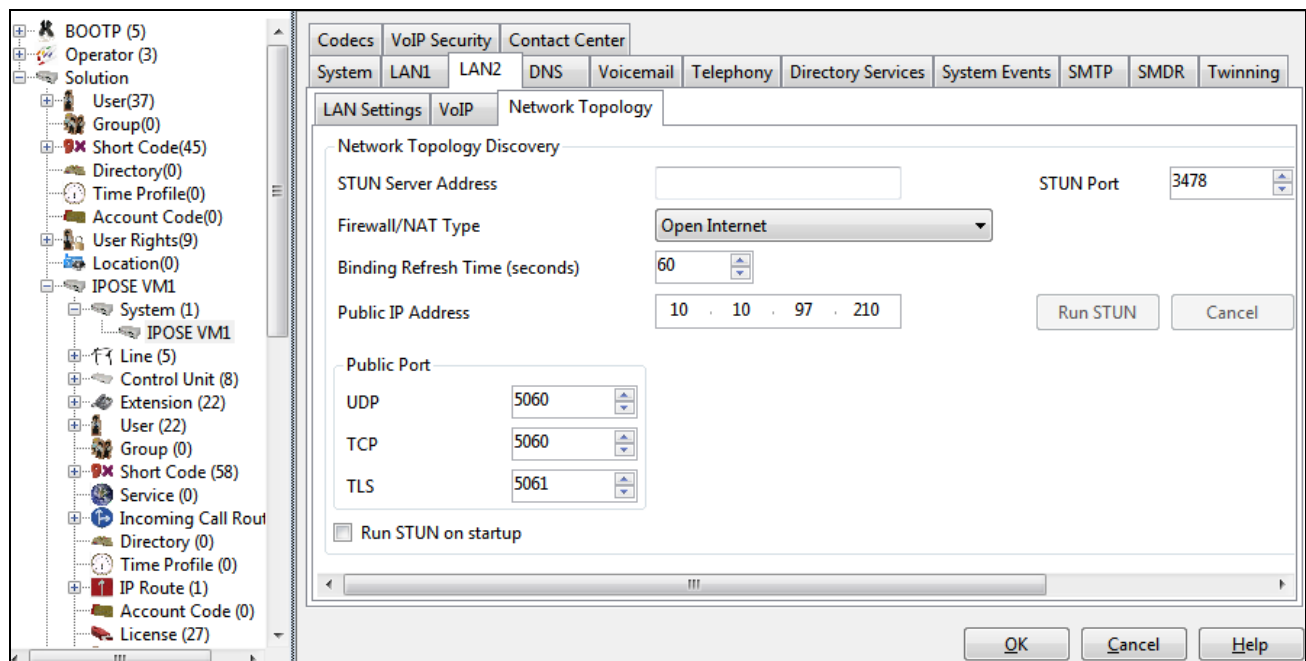
The main configuration area is titled "VoIP Security" and "Contact Center". It contains several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, and Codex. The "VoIP" tab is selected, showing the following settings:

- H323 Gatekeeper Enable**: Checked.
 - Auto-create Extn**: Unchecked.
 - Auto-create User**: Unchecked.
 - H323 Remote Extn Enable**: Unchecked.
 - Remote Call Signalling Port**: 1720.
- SIP Trunks Enable**: Checked.
- SIP Registrar Enable**: Checked.
 - Auto-create Extn/User**: Unchecked.
 - SIP Remote Extn Enable**: Unchecked.
- Domain Name**: (Empty text field).
- Layer 4 Protocol**:
 - UDP**: Checked. **UDP Port**: 5060. **Remote UDP Port**: 5060.
 - TCP**: Checked. **TCP Port**: 5060. **Remote TCP Port**: 5060.
 - TLS**: Checked. **TLS Port**: 5061. **Remote TLS Port**: 5061.
- Challenge Expiry Time (secs)**: 10.
- RTP**:
 - Port Number Range**:
 - Minimum**: 40750. **Maximum**: 50750.
 - Port Number Range (NAT)**:
 - Minimum**: 40750. **Maximum**: 50750.
 - Enable RTCP Monitoring on Port 5005**: Checked.
 - RTCP collector IP address for phones**: 0 . 0 . 0 . 0 . 0 . 0.
 - Keepalives**:
 - Scope**: RTP-RTCP. **Periodic timeout**: 30.
 - Initial keepalives**: Enabled.

At the bottom of the window are buttons for **OK**, **Cancel**, and **Help**.

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 TLS** is set to **5061**.
- All other parameters should be set according to customer requirements.
- Click **OK**.

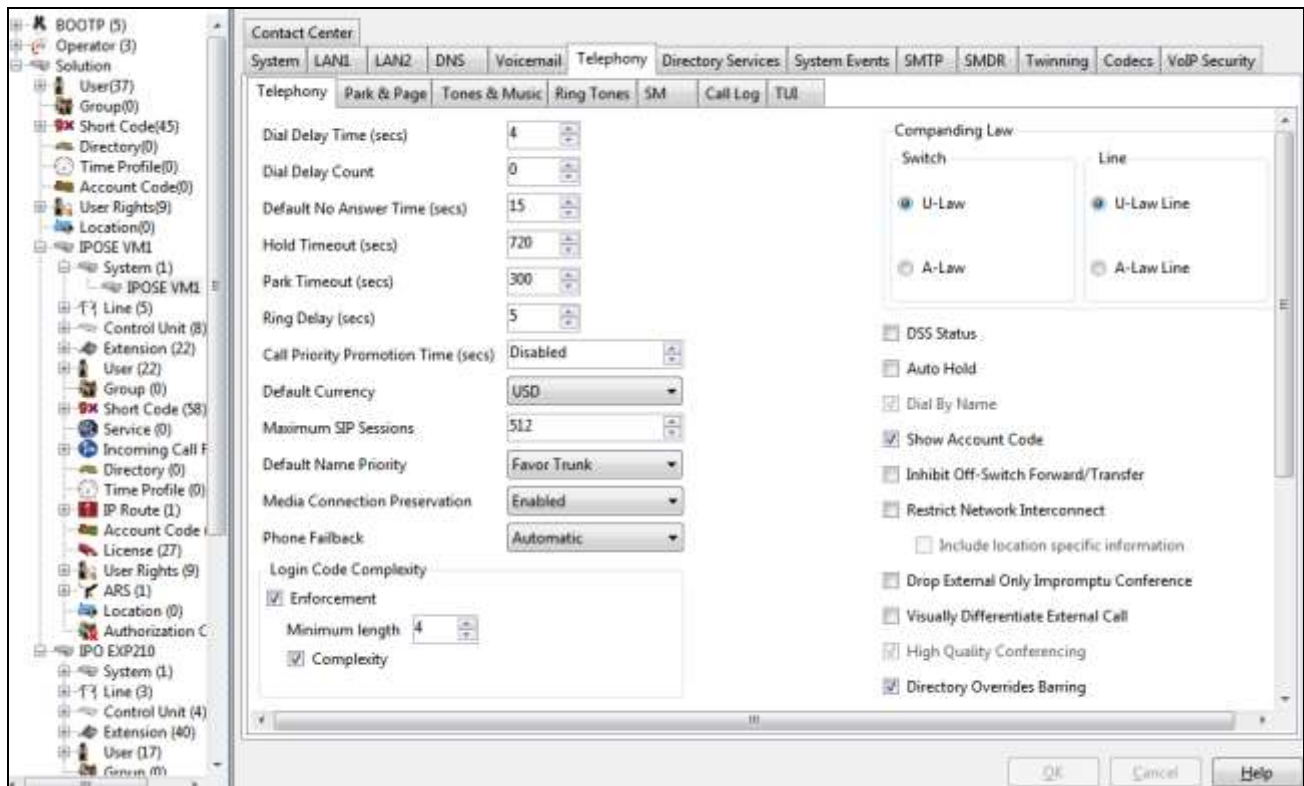


In the compliance test, the LAN1 interface was used to connect IP Office to the enterprise site IP network. The LAN1 interface configuration is not directly relevant to the interface with Intermedia SIP Trunking service, and therefore is not described in these Application Notes.

5.2. System Telephony Settings

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

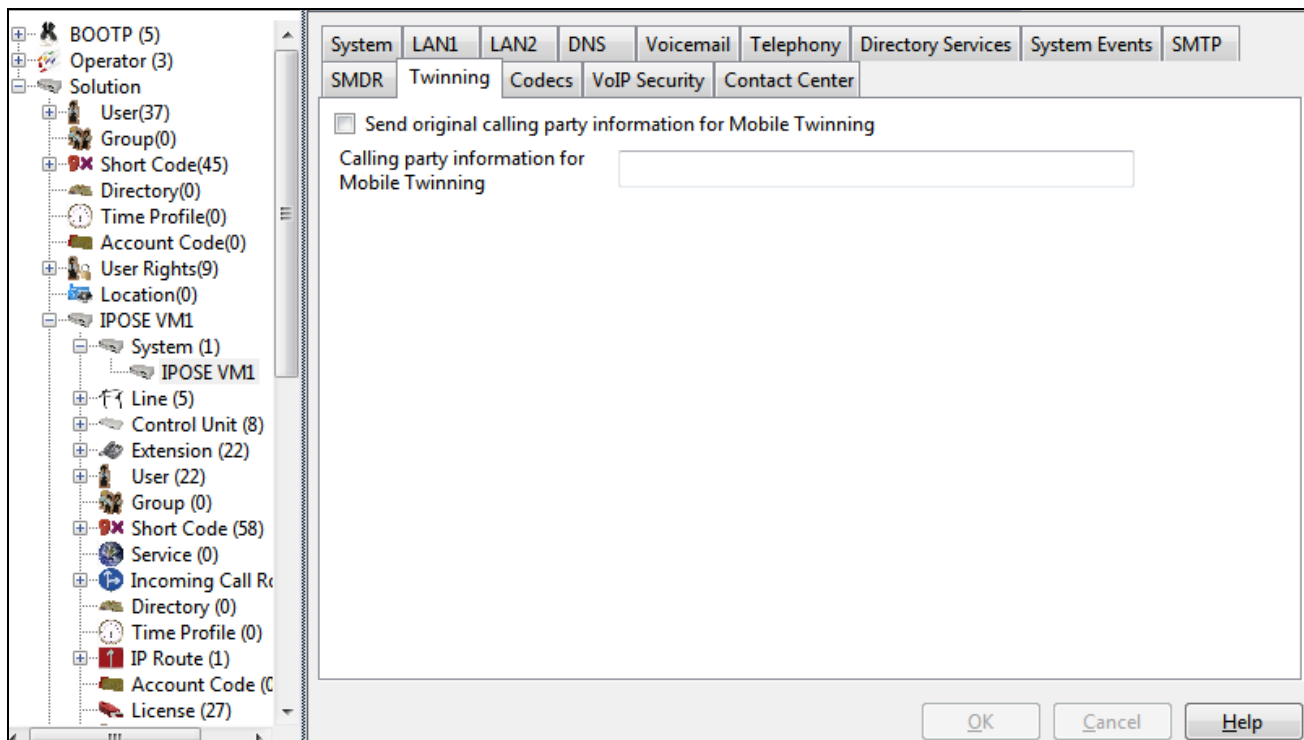
- Choose the **Companding Law** typical for the enterprise location. For North America, **ULAW** is used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the service provider across the SIP trunk.
- Uncheck the **Drop External Only Impromptu Conference** box to allow the host of 3 way conference leaving the active call without forcing all the parties off the conference.
- Other parameters are left at default.
- Click **OK**.



5.3. Twinning Calling Party Settings

When using twinning, the calling party number displayed on the twinned phone is controlled by two parameters. These parameters only affects twinning and do not impact the messaging or operation of other redirected calls such as forwarded calls. The first parameter is the **Send original calling party information for Mobile Twinning** box on the **System → Twinning** tab. The second parameter is the **Send Caller ID** parameter on the **SIP Line** form (shown in **Section 5.5**).

- For the compliance testing, the **Send original calling party information for Mobile Twinning** as shown below was unchecked. There is no requirement to use this parameter in this testing configuration.
- Click **OK**.



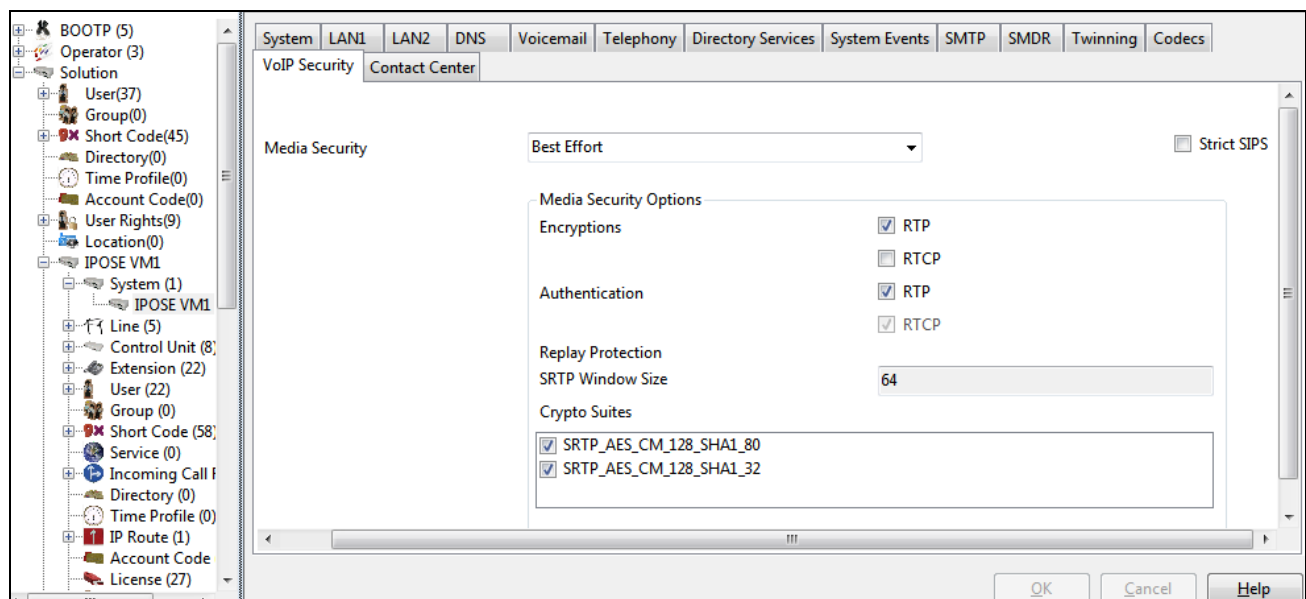
5.4. VoIP Security Settings

When enabling SRTP on the system, the recommended setting is Best Effort. 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, Best Effort is set at system level and extensions. Enforce is set at 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 follow:

- Select **Best Effort** for **Media Security**. Media security is preferred. Attempt to use secure media first and if unsuccessful, fall back to non-secure media within Avaya IP Office system.
- Other parameters are left as default.
- Click **OK**.



5.5. Administer SIP Line

A SIP line is needed to establish the SIP connection between IP Office and Intermedia 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 5.5.1** to create the SIP Line from the template.

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

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

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

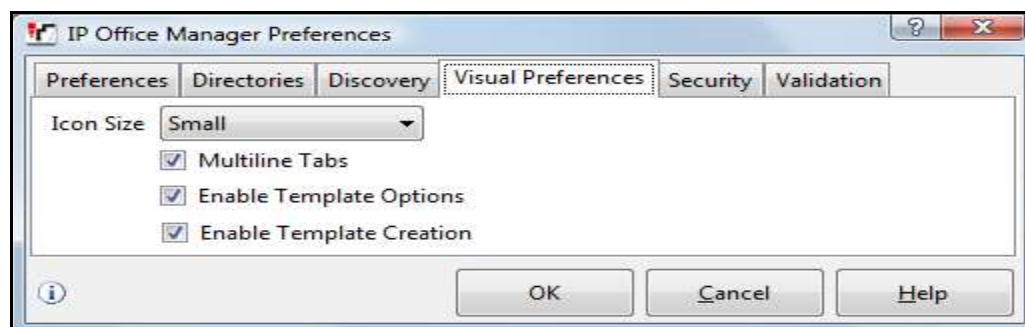
Also, the following SIP Line settings are not supported on Basic Edition:

- 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 5.5.2**.

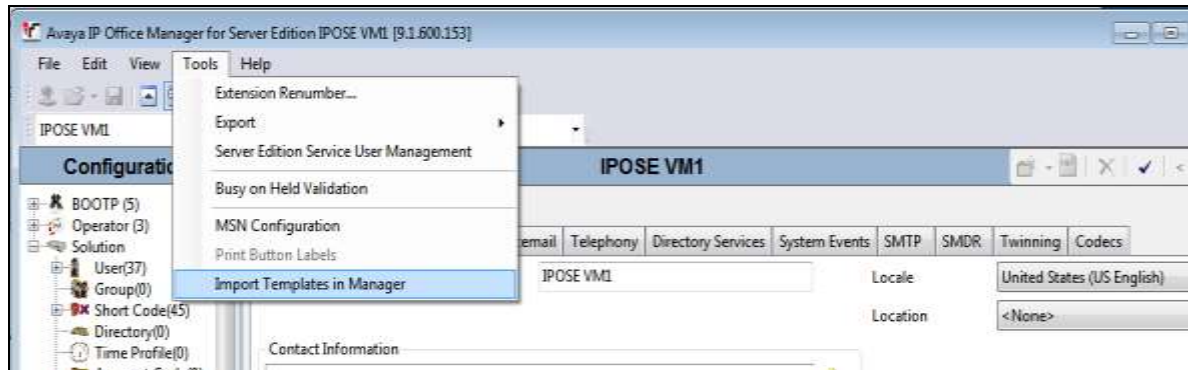
5.5.1. Create SIP line from Template

1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **AF_Intermedia_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**.
2. Verify that template options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the Visual Preferences tab. Verify that the box is checked next to **Enable Template Options** and **Enable Template Creation**. Click **OK**.



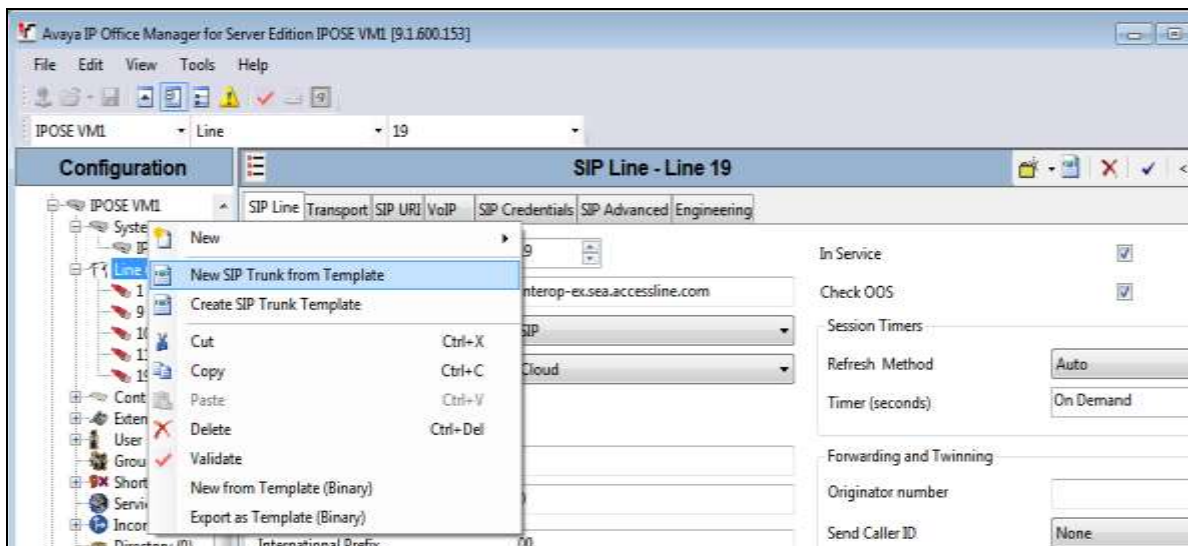
3. Import the template into IP Office Manager.

From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.

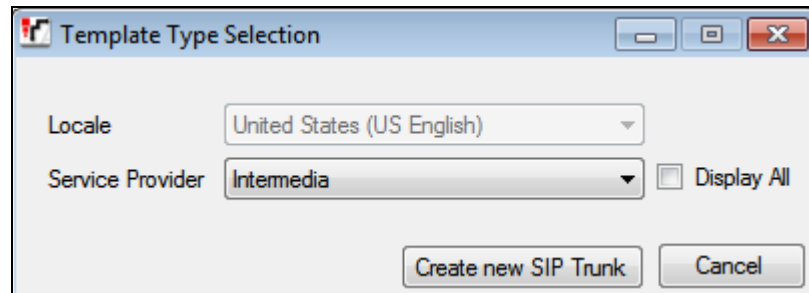


In the pop-up window that appears (not shown), select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window will appear (not shown) stating success or failure. Then click **OK** (not shown) to continue. If preferred, this step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

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



5. In the subsequent Template Type Selection pop-up window, select **Intermedia** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**AF_Intermedia_SIPTrunk.xml**) created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.



6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.5.2**.

Note: Windows 7 (and later) locks the Avaya IP Office 9.1 \Templates directory, and it cannot be viewed. To enable browsing of the \Templates directory, open Windows Explorer, navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates** (or *C:\Program Files (x86)\Avaya\IP Office\Manager\Templates*), and then click on the **Compatibility files** option shown below. The \Templates directory and its contents can then be viewed.

5.5.2. Create SIP Line Manually

To create a SIP line, begin by navigating to **Line** in the left Navigation Pane, then right-click in the Group Pane and 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.
- Set **Send Caller ID** to *None*.
- 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** was set to *Never* as Intermedia does not support REFER.
- **Outgoing Supervised REFER** was set to *Never* as Intermedia does not support REFER.
- Other parameters are set as default values.
- Click **OK**.

The screenshot shows the 'SIP Line' configuration window in IP Office. The left pane shows a tree view with 'Line (5)' selected. The main pane has tabs for 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'SIP Line' tab is active, showing the following configuration:

Field	Value
Line Number	19
ITSP Domain Name	interop-ex.sea.accessline.com
URI Type	SIP
Location	Cloud
Prefix	
National Prefix	0
International Prefix	00
Country Code	
Name Priority	System Default
Description	
In Service	<input checked="" type="checkbox"/>
Check OOS	<input checked="" type="checkbox"/>
Session Timers	
Refresh Method	Auto
Timer (seconds)	On Demand
Forwarding and Twinning	
Originator number	
Send Caller ID	None
Redirect and Transfer	
Incoming Supervised REFER	Never
Outgoing Supervised REFER	Never
Send 302 Moved Temporarily	<input type="checkbox"/>
Outgoing Blind REFER	<input type="checkbox"/>

At the bottom right are buttons for 'OK', 'Cancel', and 'Help'.

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**.

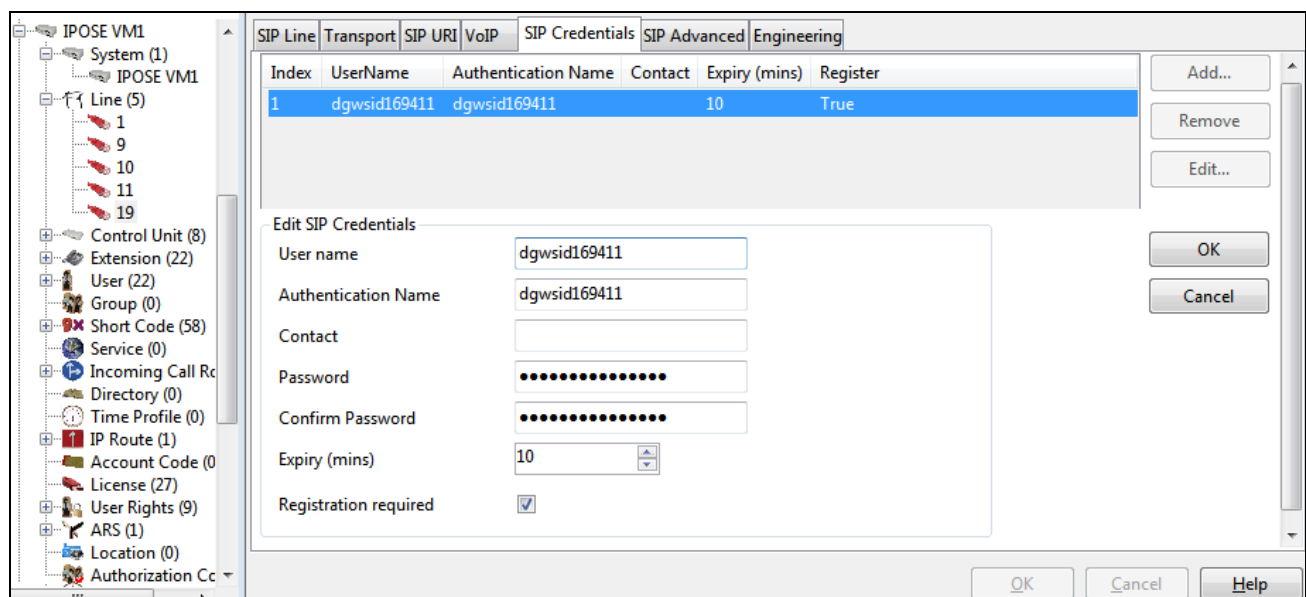
The screenshot displays the Avaya IP Office configuration window. On the left is a tree view showing the system hierarchy: IPOSE VM1, System (1), IPOSE VM1, Line (5) with sub-items 1, 9, 10, 11, and 19, Control Unit (8), Extension (22), User (22), Group (0), Short Code (58), Service (0), Incoming Call Routing, Directory (0), Time Profile (0), IP Route (1), Account Code (0), License (27), User Rights (9), ARS (1), Location (0), Authorization Codes, IPO EXP210, and System (1). The main panel has tabs for SIP Line, Transport, SIP URI, VoIP, SIP Credentials, SIP Advanced, and Engineering. The Transport tab is active, showing the following configuration:

- ITSP Proxy Address: 10.10.97.176
- Network Configuration section:
 - Layer 4 Protocol: TLS (dropdown)
 - Send Port: 5061 (spin box)
 - Use Network Topology Info: LAN 2 (dropdown)
 - Listen Port: 5061 (spin box)
- Explicit DNS Server(s): Two input fields, both containing 0 . 0 . 0 . 0
- Calls Route via Registrar: ☒
- Separate Registrar: An empty text input field

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

A SIP Credentials entry must be created for SIP trunking registration and Digest Authentication that are used by Intermedia SIP trunking service to authenticate calls from the enterprise to the PSTN. To create a SIP Credentials entry, first select the **SIP Credentials** tab. Click the **Add** button and the **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 bottom of the screen, the Edit Channel area will be opened. In the example screen below, a previously configured entry is edited. The entry was created with the parameters shown below:

- Set **User name** and **Authentication Name** to the value provided by the service provider.
- Set **Password** and **Confirmed Password** to the value provided by the service provider.
- The **Expiry (mins)** is set to **10** minutes in this case as service provider relies on registration from enterprise to keep the trunk alive.
- Check the **Registration required** option. Service provider requires registration for Digest Authentication.
- Click **OK**.



A SIP URI entry **Channel 1** is created to match incoming numbers that IP Office will accept on this line. Select the **SIP URI** tab, then click the **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:

- **Via** field is pre-populated by IP Office.
- 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**.
- **PAI** field is set to *None*.
- For **Registration**, select the account credentials previously configured on the line's **SIP Credentials** tab.
- 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 **19** was defined that only contains this line (line 19).
- Set **Max Calls per Channel** 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**.

The screenshot shows the IP Office configuration interface. On the left is a tree view of the system configuration. The main pane is titled 'SIP Line' and has several tabs: 'Transport', 'SIP URI', 'VoIP', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'SIP URI' tab is active, showing a table of SIP URI entries. Below the table is an 'Edit Channel' dialog box.

Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	19 19	1...				N...	1: dgwsi...	10
2	19 19	1...	206686...			N...	1: dgwsi...	10

Edit Channel

Via: 10.10.97.210

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

PAI: None

Registration: 1: dgwsid169411

Incoming Group: 19

Outgoing Group: 19

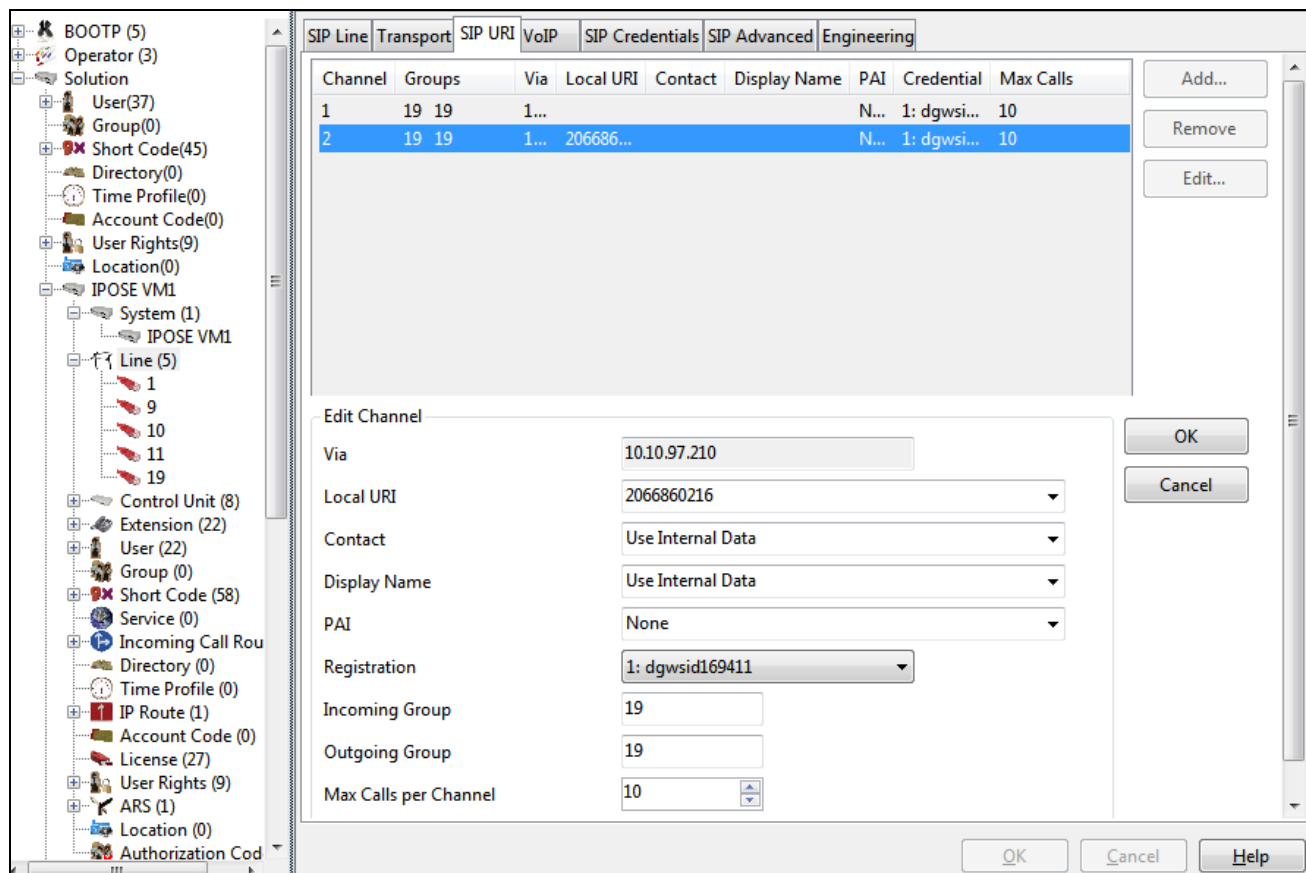
Max Calls per Channel: 10

Buttons: OK, Cancel, Help

SIP URI entry **Channel 2** was similarly created for incoming calls appropriately to pre-defined DID numbers, which is provided by service provider, to access to Feature Name Extension 00 (FNE00). The Short Codes for FNE00 are defined in **Section 5.6** to provide Dial Tone and Mobile Callback for mobility extension.

The **Channel 2**, as shown in the screenshot below, was configured with following parameters.

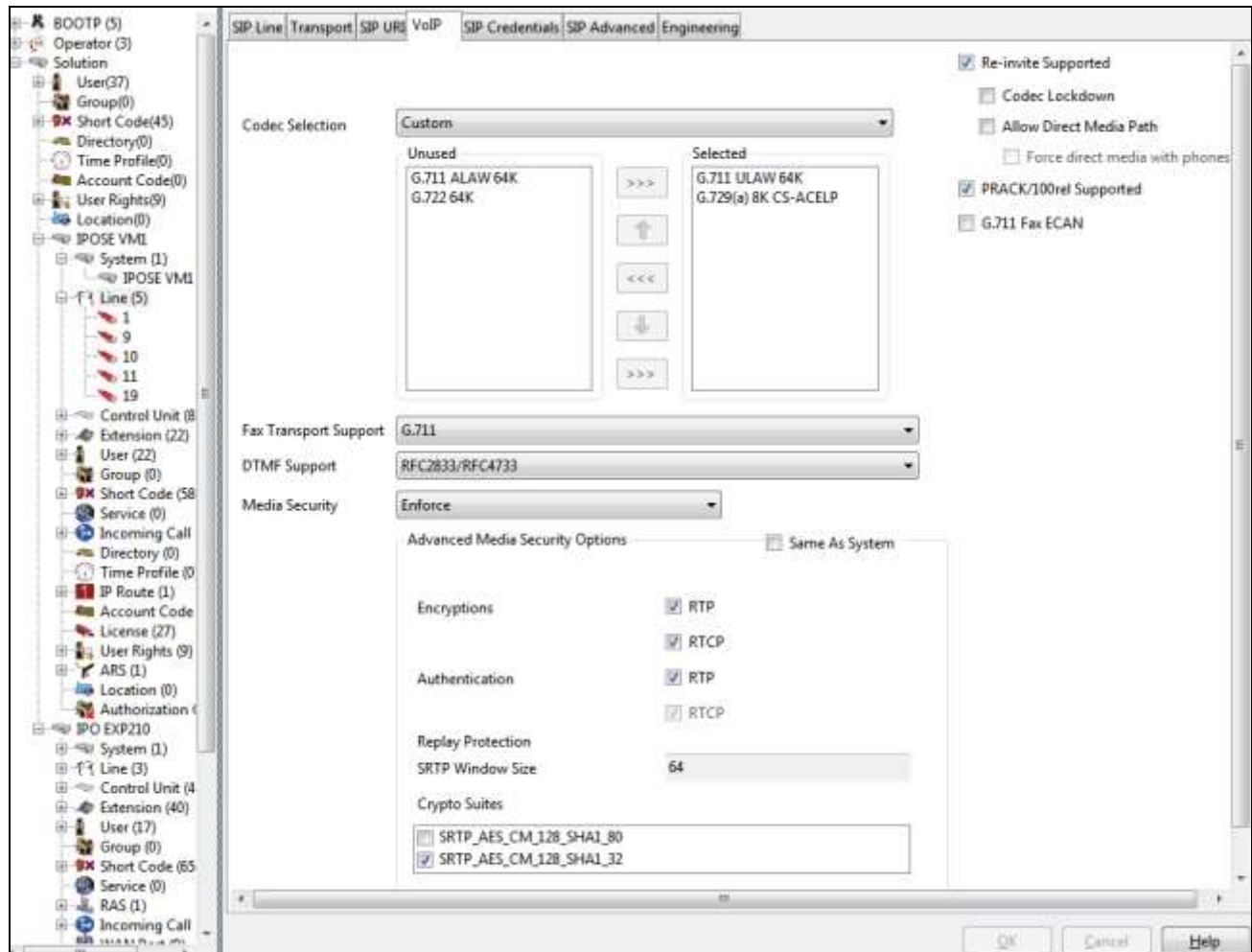
- **Via** field is pre-populated by IP Office.
- Set the **Local URI** to pre-define DID number appropriately for **Channel 2**.
- Set **Contact** and **Display Name** to *Use Internal Data*.
- **PAI** field is set to *None*.
- For **Registration**, select the account credentials previously configured on the lines **SIP Credentials** tab.
- Associate **Incoming Group** and **Outgoing Group** to SIP Line **19**.
- Set the **Max Calls per Channel** field to **10**.
- Other parameters retain default values and or set according customer requirements.
- Click **OK**.



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 ULAW** and **G.729** codec supported by the Intermedia SIP Trunking service, in the Session Description Protocol (SDP) offer.
- Set **Fax Transport Support** to **G.711** from the pull-down menu (T.38 faxing is not currently supported by service provider).
- Set the **DTMF Support** field to **RFC2833/RFT4733** from the pull-down menu. This directs IP Office to send DTMF tones using SRTP events messages as defined in RFC2833.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- Set **Media Security** to **Enforce** to ensure the use of SRTP for media communicating over the SIP trunk.
- The **Advanced Media Security Options**, uncheck the **Same As System** box to disassociate the media security settings of the SIP trunk from the media security settings of the system. Note that what is set here will over write the system and extensions settings in term of media security.
- The **Encryption**, check the **RTCP** box.
- The Crypto Suits, uncheck the **SRTP_AES_CM_128_SHA1_80** box as service provider using only **SRTP_AES_CM_128_SHA1_32**.
- Default values may be used for all other parameters.
- Click **OK**.

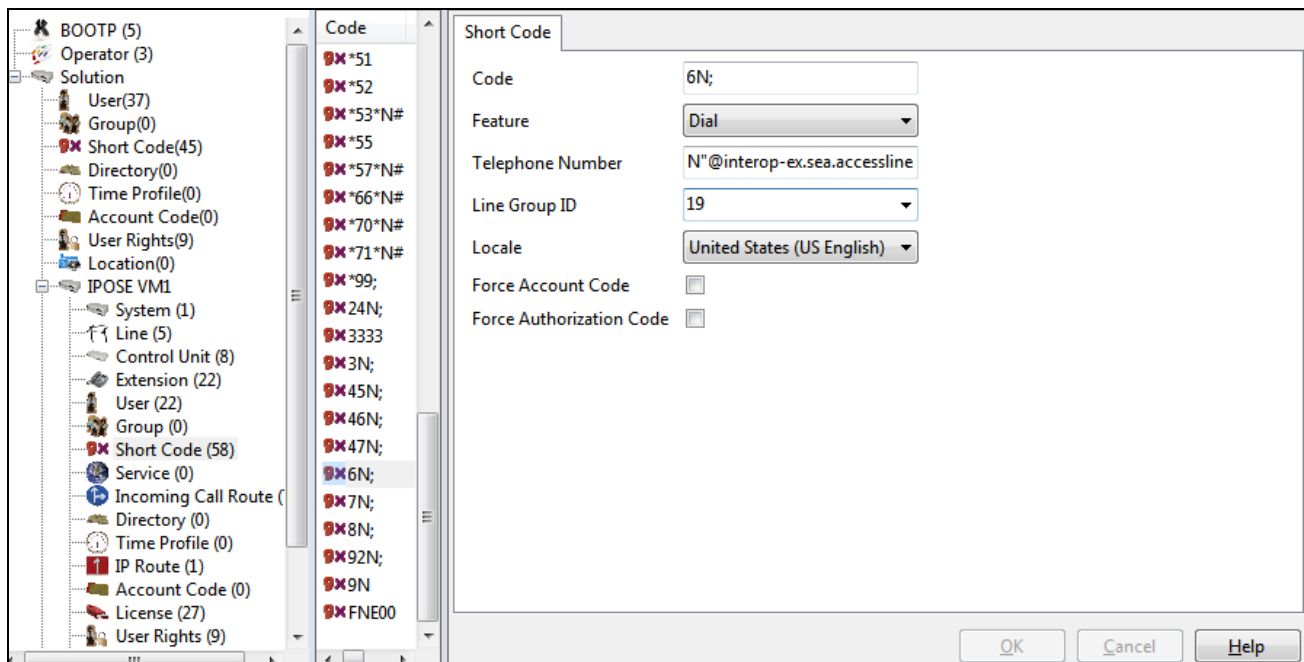
The VoIP tab capture is shown below.



5.6. Short Code

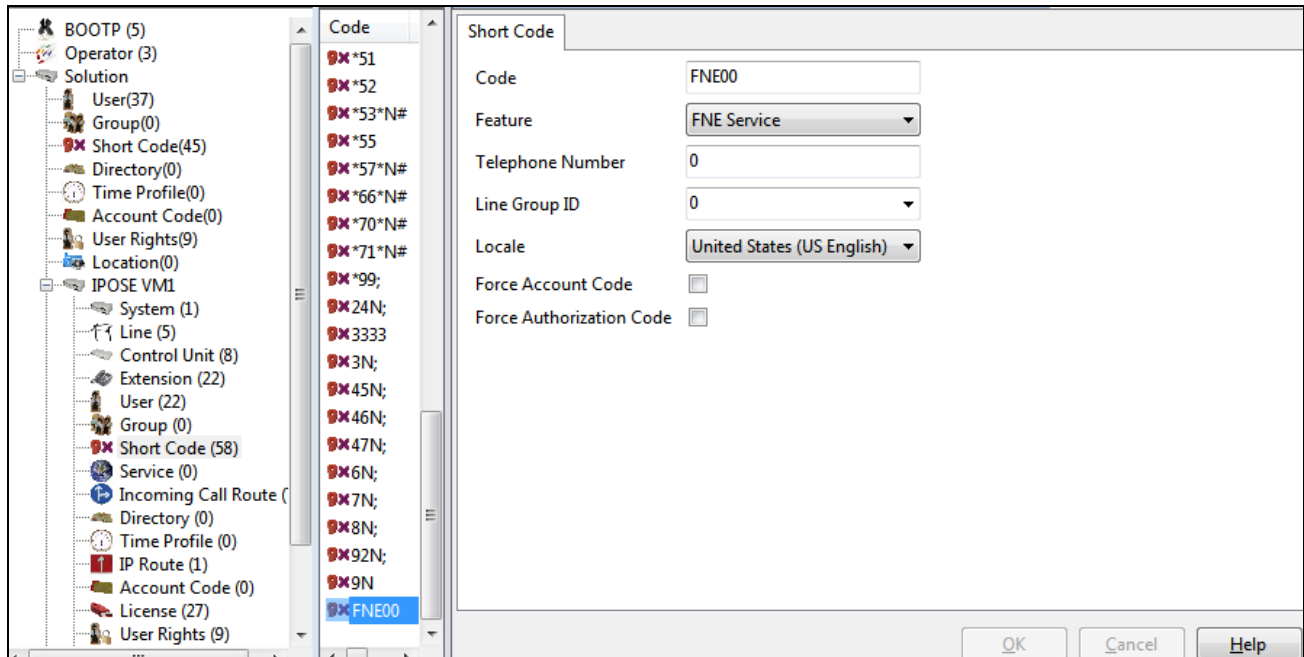
Define a short code to route outbound traffic to the SIP line. To create a short code, select **Short Code** in the left Navigation Pane, then right-click in the Group Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters for the new short code to be created. 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 service provider network.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.5**. This short code will use this line group when placing the outbound call.
- Select **United State (US English)** for **Locale**.
- Others parameters are at default values.
- Click **OK**.



For incoming calls from mobility extension to FNE features 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 **0**.
- Set the **Line Group ID** field to **0**.
- Select **United State (US English)** for **Locale**.
- Retain default values for other fields.
- Click **OK**.

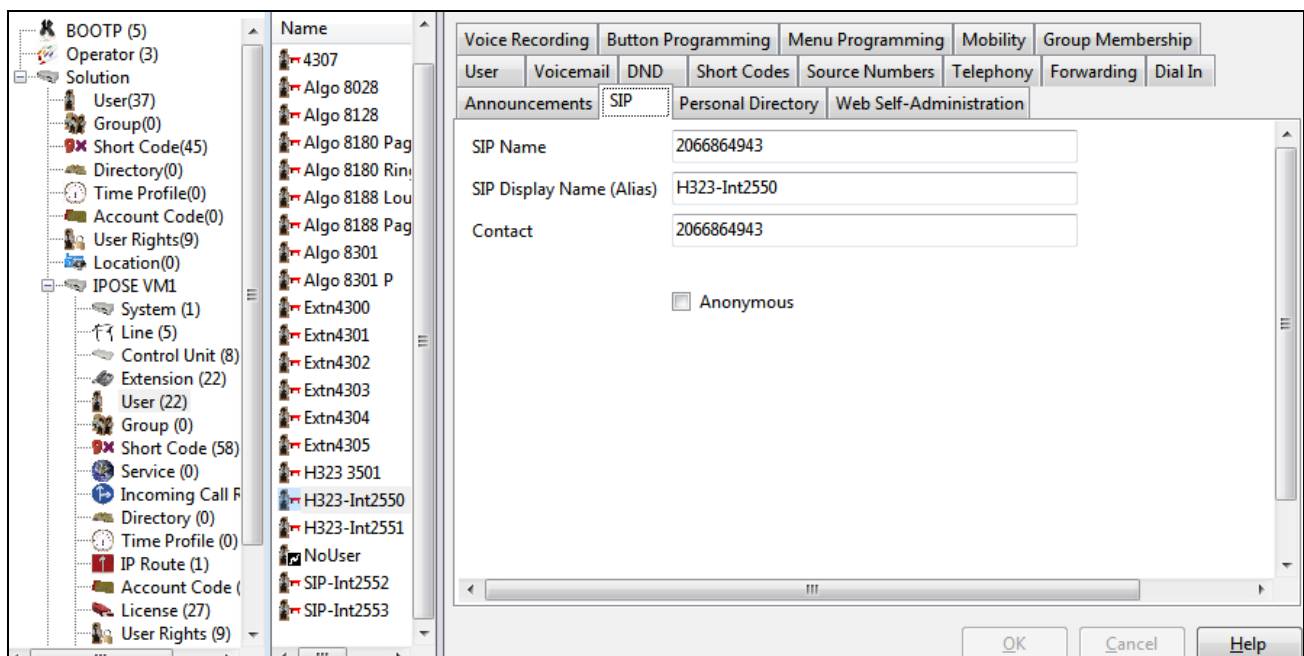


5.7. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.5**. 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-Int2550”. 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 5.5**). The example below shows the settings for user H323- Int2550.

- 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**.



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- Int2550.

- 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 **66139675205**.
- Make sure the **Mobile Call Control** box is checked.
- Other options can be set according to customer requirements.
- Click **OK**.

The screenshot displays the Avaya User Management Interface. On the left is a tree view of the system hierarchy, including BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE VM1, System, Line, Control Unit, Extension, and various other entities. The 'User' entity 'H323-Int2550' is selected. The main panel shows the 'Mobility' tab for this user. The 'Internal Twinning' section is collapsed. The 'Mobility Features' section is expanded, showing 'Mobile Twinning' checked. The 'Twinned Mobile Number' field is set to '66139675205'. The 'Twinning Time Profile' is set to '<None>'. The 'Mobile Dial Delay (secs)' is set to '2'. The 'Mobile Answer Guard (secs)' is set to '0'. The 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', and 'Twin When Logged Out' options are unchecked. The 'one-X Mobile Client', 'Mobile Call Control', and 'Mobile Callback' options are checked. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

Name	Value
Twinned Handset	<None>
Maximum Number of Calls	1
Twin Bridge Appearances	<input type="checkbox"/>
Twin Coverage Appearances	<input type="checkbox"/>
Twin Line Appearances	<input type="checkbox"/>
Mobility Features	<input checked="" type="checkbox"/>
Mobile Twinning	<input checked="" type="checkbox"/>
Twinned Mobile Number (including dial access code)	66139675205
Twinning Time Profile	<None>
Mobile Dial Delay (secs)	2
Mobile Answer Guard (secs)	0
Hunt group calls eligible for mobile twinning	<input type="checkbox"/>
Forwarded calls eligible for mobile twinning	<input type="checkbox"/>
Twin When Logged Out	<input type="checkbox"/>
one-X Mobile Client	<input checked="" type="checkbox"/>
Mobile Call Control	<input checked="" type="checkbox"/>
Mobile Callback	<input type="checkbox"/>

5.8. Incoming Call Route

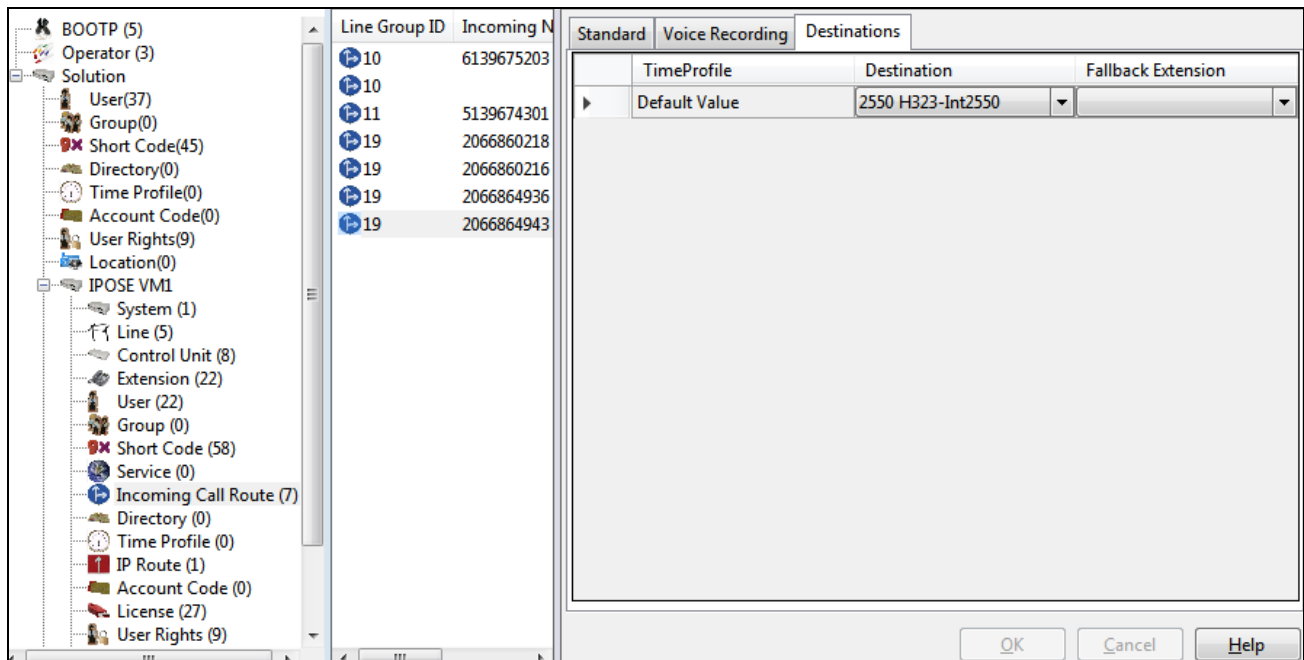
An incoming call route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by the service provider. To create an incoming call route, select **Incoming Call Route** in the left Navigation Pane, then right-click in the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

- Set the **Bearer Capability** to *Any Voice*.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.5**.
- Set the **Incoming Number** to the incoming number on which this route should match.
- Select *United States (US English)* for **Locale**.
- Default values can be used for all other fields.
- Click **OK**.

Line Group ID	Incoming N
10	6139675203
10	
11	5139674301
19	2066860218
19	2066860216
19	2066864936
19	2066864943

Field	Value
Bearer Capability	Any Voice
Line Group ID	19
Incoming Number	2066864943
Incoming Sub Address	
Incoming CLI	
Locale	United States (US English)
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **2066864943** on line 19 are routed to extension **4000**. 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.

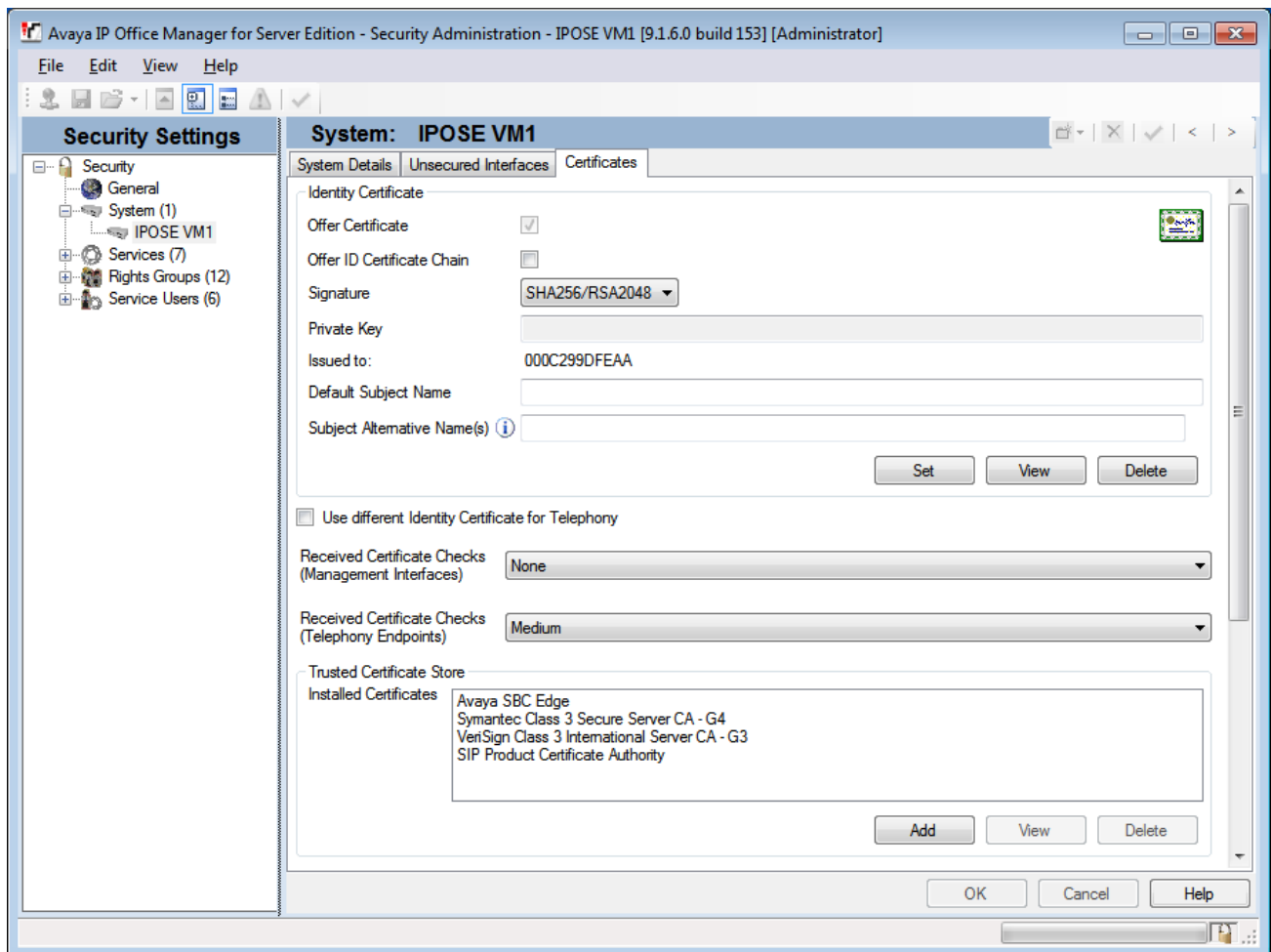
5.10. Security Settings

This setting is used with IP telephony endpoints connecting to the system. This setting is used by IP Office to validate the identity certificate offered by the other end of TLS connection. IP Office does not support mutual authentication for SIP terminals (an identity certificate is not installed in all SIP terminals). Therefore, IP Office does not require a client certificate from a SIP terminal, only SIP and SM trunks. The received certificate is tested as follows:

- **None:** No extra checks are made (The certificate must be in date).
- **Low:** Certificate minimum key size 1024 bits, in date.
- **Medium:** Certificate minimum key size 1024 bits, in date, match to store.
- **High:** Certificate minimum key size 2048 bits, in date, match to store, no self signed, no reflected, chain validation.

Navigate to **File → Advanced → Security → System**, choose **Certificates** tab.

- Select **Medium** for the **Received Certificate Checks (Telephony Endpoints)**.
- Click **Ok**.
- Click **File → Save Security Settings**.



6. Configure t Avaya Session Border Controller for Enterprise

This section covers the configuration of 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 was defined in the Avaya SBCE web user interface as described in the following sections.

Trunk Server configuration elements for the service provider - Intermedia:

- 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
- Device Specific Settings:
 - Network Management

- Media Interface
- Signaling Interface
- End Point Flows → Server Flows
- Session Flows

6.1. Log into Avaya Session Border Controller for Enterprise

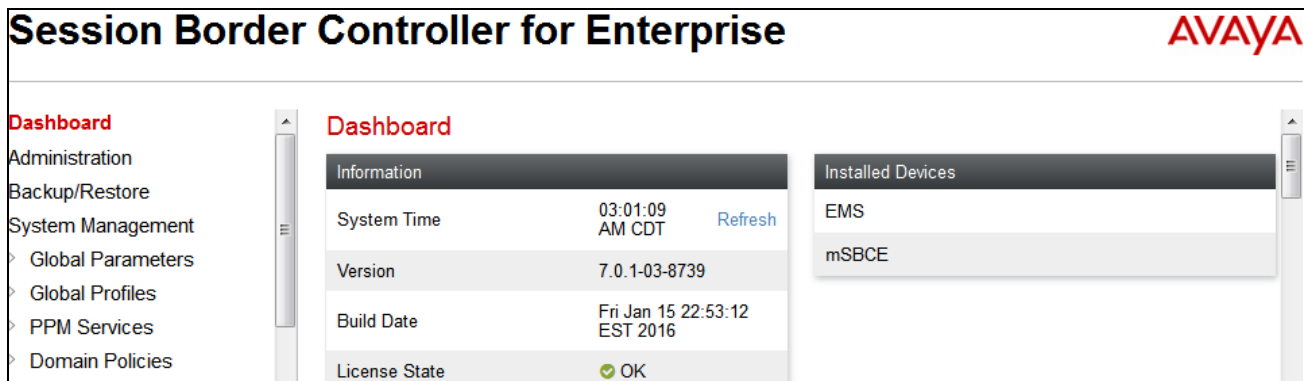
Use a Web browser to access the Avaya SBCE Web interface, enter `https://<ip-addr>/sbc` in the address field of the web browser, where `<ip-addr>` is the management IP address.

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



The image shows the login page of the Avaya Session Border Controller for Enterprise. It features the Avaya logo in red at the top left. Below the logo, the text "Session Border Controller for Enterprise" is displayed. To the right, there is a "Log In" section with a "Username:" label and a text input field. Below the input field is a "Continue" button. Further down, there is a disclaimer text: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." Below this, another paragraph states: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." At the bottom, it says: "All users must comply with all corporate instructions regarding the protection of information assets." and "© 2011 - 2015 Avaya Inc. All rights reserved."

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



The image shows the dashboard of the Avaya Session Border Controller for Enterprise. The title "Session Border Controller for Enterprise" is at the top left, and the Avaya logo is at the top right. On the left side, there is a navigation menu with the following items: "Dashboard" (highlighted in red), "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles", "PPM Services", and "Domain Policies". The main content area is titled "Dashboard" and contains two panels. The left panel is titled "Information" and displays the following data: "System Time" (03:01:09 AM CDT) with a "Refresh" link, "Version" (7.0.1-03-8739), "Build Date" (Fri Jan 15 22:53:12 EST 2016), and "License State" (OK with a green checkmark). The right panel is titled "Installed Devices" and lists "EMS" and "mSBCE".

6.2. Global Profiles

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

The naming convention in this entire section is using as follow:

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

6.2.1. 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.

6.2.2. 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.

6.2.2.1 Server Interworking profile for SP

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

General tab:

- **Hold Support** = *NONE*. Avaya SBCE will not modify the hold/ resume signaling from EN to SP.
- **18X Handling** = *None*. Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from EN to SP.
- **Refer Handling** = *No*. Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from EN to SP.
- **T.38 Support** = *No*. SP does not 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 displays 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, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. Under Global Profiles, 'Server Interworking' is highlighted. The main content area is titled 'Interworking Profiles: SP-SI' and features a list of profiles on the left, including cs2100, avaya-ru, OCS-Edge-Se..., cisco-ccm, cups, Sipera-Halo, OCS-FrontEn..., IPO, MTSAllstream, EN-SI, RC, ThinkTel, **SP-SI**, SP4, and IPO_14. The 'SP-SI' profile is selected, and its configuration is shown in the main panel. The configuration is divided into tabs: General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The 'General' tab is active, showing a table of settings.

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	No
URI Scheme	SIP
Via Header Format	RFC3261

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

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

SNMP Traps

Time of Day Rules

PPM Services

Domain Policies

Interworking Profiles: SP-SI

Add

Rename Clone Delete

Interworking Profiles

EN-SI

RC

ThinkTel

SP-SI

SP4

IPO_14

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation **Advanced**

Record Routes Both Sides

Include End Point IP for Context Lookup No

Extensions Avaya

Diversion Manipulation No

Has Remote SBC Yes

Route Response on Via Port No

DTMF

DTMF Support None

Edit

6.2.2.2 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*. Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from SP to EN.
- **Refer Handling** = *No*. Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from SP to EN.
- **T.38 Support** = *No*. EN does support T.38 fax, but SP doesn't in the compliance testing.
- Others are left as default values.

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar shows a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and PPM Services. Under Global Profiles, 'Server Interworking' is highlighted. The main content area is titled 'Interworking Profiles: EN-SI' and includes an 'Add' button and buttons for 'Rename', 'Clone', and 'Delete'. A list of profiles is shown, with 'EN-SI' selected. The 'General' tab is active, displaying a table of configuration 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	No
URI Scheme	SIP
Via Header Format	RFC3261

Advanced tab:

- **Record Routes** = *Both Sides*. Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Include End Point IP for Context Lookup** = *No*.
- **Extensions** = *Avaya*.
- **Has Remote SBC** = *Yes*. This setting allows Avaya SBCE to always use the SDP received from EN for the media.
- **DTMF Support** = *None*. 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**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar shows the navigation menu with 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: EN-SI' and shows a list of profiles on the left, including 'cs2100', 'avaya-ru', 'OCS-Edge-S...', 'cisco-ccm', 'cups', 'Sipera-Halo', 'OCS-FrontEn...', 'IPO', 'MTSAllstream', and 'EN-SI' (selected). The 'Advanced' tab is active, showing the following settings:

Setting	Value
Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
DTMF Support	None

6.2.3. 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, UDP or TLS port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

To create a Server Configuration entry, select **Global Profiles** → **Server Configuration**. Click on the **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.

6.2.3.1 Server Configuration for SP

Server Configuration named **SP-SC** was created for 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** is disabled to allow IP Office to send out authentication to SP. **Heartbeat** tab is kept as *disabled* as default to allow Avaya SBCE to forward the OPTIONS heartbeat from EN to SP to query the status of the SIP trunk.

General tab:

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

- Set **Server Type** for SP as **Trunk Server**.
- In the compliance testing, SP supported **TLS** and listened on port **5061**.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The title bar reads "Session Border Controller for Enterprise" with the Avaya logo on the right. The left sidebar contains a navigation menu with categories: 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 and "Rename", "Clone", and "Delete" buttons. Below these are tabs for "General", "Authentication", "Heartbeat", and "Advanced". The "General" tab is active, showing a "Server Type" dropdown set to "Trunk Server". Below this is a table with columns "IP Address / FQDN", "Port", and "Transport". The table contains one row: "192.168.122.44", "5061", and "TLS". An "Edit" button is located at the bottom right of the table.

IP Address / FQDN	Port	Transport
192.168.122.44	5061	TLS

Advanced tab:

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

- **Interworking Profile** drop down list, select **SP-SI** as defined in Section 6.2.2.
- The other settings are kept as default.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The title bar reads "Session Border Controller for Enterprise" with the Avaya logo on the right. The left sidebar contains a navigation menu with categories: 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 and "Rename", "Clone", and "Delete" buttons. Below these 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 "SP-SI"), "TLS Client Profile" (dropdown set to "None"), "Signaling Manipulation Script" (dropdown set to "None"), "Connection Type" (dropdown set to "SUBID"), and "Securable" (checkbox). An "Edit" button is located at the bottom right of the configuration area.

6.2.3.2 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 Avaya SBCE to forward the OPTIONS heartbeat from SP to EN to query the status of the SIP trunk.

General tab:

Click on the **Edit** button then specify the following.

- **Server Type** for EN as *Call Server*.
- **IP Address/FQDN** is IP Office IP address.
- **Transport**, the link between Avaya SBCE and EN was *TLS*. Listening on **Port 5061**.

The screenshot shows the 'Session Border Controller for Enterprise' configuration interface. The left sidebar lists navigation options: System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration (highlighted), and Topology Hiding. The main content area is titled 'Server Configuration: EN-SC' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below these are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing a 'Server Type' dropdown set to 'Call Server'. Below this is a table with columns 'IP Address / FQDN', 'Port', and 'Transport'. The table contains one entry: IP Address / FQDN: 10.10.97.210, Port: 5061, Transport: TLS. An 'Edit' button is located at the bottom right of the table.

IP Address / FQDN	Port	Transport
10.10.97.210	5061	TLS

Advanced tab:

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

- **Interworking Profile** drop down list select *EN-SI* as defined in **Section Error! Reference source not found..**
- **Signaling Manipulation Script** drop down list select *None*.
- The other settings are kept as default.

The screenshot shows the 'Session Border Controller for Enterprise' configuration interface. The left sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration (highlighted), Topology Hiding, Signaling Manipulation, URI Groups, and SNMP Traps. The main content area is titled 'Server Configuration: EN-SC' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below these 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'), 'TLS Client Profile' (dropdown set to 'None'), 'Signaling Manipulation Script' (dropdown set to 'None'), 'Connection Type' (dropdown set to 'SUBID'), and 'Securable' (checkbox). An 'Edit' button is located at the bottom right of the configuration area.

6.2.4. 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.

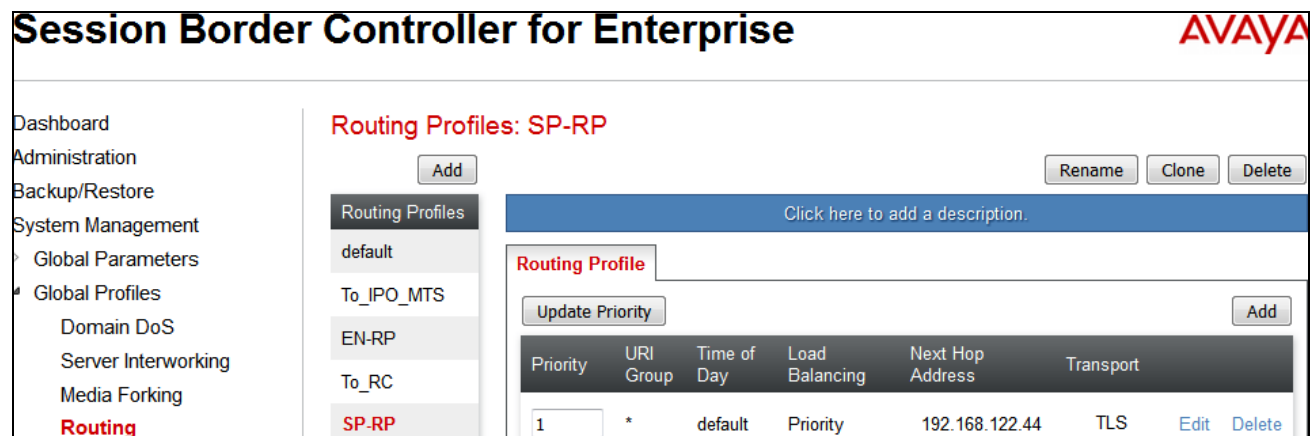
To create a Routing profile, select **Global Profiles → Routing** then click on the **Add** button.

In the compliance testing, Routing profile **SP-RP** was created to be used in conjunction with Server Flow (see **Section 6.4.4**) 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 Server Flow (see **Section 6.4.4**) defined for SP. This entry is to route incoming calls from SP to the EN.

6.2.4.1 Routing Profile for SP

The screenshot below illustrate 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 *TLS*. If there is a match in the “To” or “Request URI” headers with the URI Group **SP** 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

Routing Profiles: SP-RP

Click here to add a description.

Routing Profile

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	192.168.122.44	TLS	Edit Delete

6.2.4.2 Routing Profile for EN

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The main title is "Session Border Controller for Enterprise" with the Avaya logo in the top right corner. On the left is a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (with sub-items: Domain DoS, Server Interworking, Media Forking), and Routing (highlighted in red). The main content area is titled "Routing Profiles: EN-RP" and includes an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a list of routing profiles: "default", "To_IPO_MTS", "EN-RP" (highlighted in red), "To_RC", and "SP-RP". To the right of the list is a "Click here to add a description." link. Below the list is a "Routing Profile" section with an "Update Priority" button and an "Add" button. A table displays the configuration for the "EN-RP" profile:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.10.97.210	TLS	Edit Delete

6.2.5. Topology Hiding

Topology Hiding is a security feature of 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**.

6.2.5.1 Topology Hiding Profile for SP

Topology Hiding profile **SP-TH** was defined for outgoing calls to SP to:

- Mask URI-Host of the "Request-Line" and "To" headers with service provider SIP domain to meet the requirements of SP.
- Mask URI-Host of the "From" header to SP SIP domain as shown in capture below.

This implementation is to secure the enterprise network topology and also to meet the SIP requirements from the service provider.

The screenshots below illustrate the Topology Hiding profile **SP-TH**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar shows the navigation menu with 'Topology Hiding' selected under 'Global Profiles'. The main content area is titled 'Topology Hiding Profiles: SP-TH' and includes an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. A blue bar prompts the user to 'Click here to add a description.' Below this, a table titled 'Topology Hiding' lists the configured headers, criteria, replace actions, and overwrite values.

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

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

6.2.5.2 Topology Hiding Profile for EN

Topology Hiding profile **EN-TH** was defined for incoming calls to IP Office to:

- Mask URI-Host of the “Request-Line”, “To”, and “From” headers with the enterprise SIP domain.
- Leave the “Record-Route”, “Via” headers and SDP to default **Auto**.

The screenshots below illustrate the Topology Hiding profile **EN-TH**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: EN-TH' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A blue bar indicates 'Click here to add a description.' Below this, a table titled 'Topology Hiding' lists the configured headers, criteria, actions, and values.

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

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

6.3. 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 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.

6.3.1. Application Rules

Application Rules define which types of SIP based Unified Communications (UC) applications 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.

Select Domain Policies Application Rules from the left side menu as shown below. In the sample configuration, a single default application rule “default” was used. For field deployment create an application rule with the concurrent sessions purchased.

6.3.1.1 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 displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, Application Rules (highlighted in red), and Border Rules. The main content area is titled 'Application Rules: SP-AR' 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.' The 'Application Rule' section contains a table with 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"/>		

6.3.1.2 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 displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, Application Rules (highlighted in red), and Border Rules. The main content area is titled 'Application Rules: EN-AR' 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 tab labeled 'Application Rule'. A table lists application rules with columns: Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The table contains two entries: 'Audio' and 'Video'. The 'Audio' entry has checked boxes for 'In' and 'Out', and values of 500 for both 'Maximum Concurrent Sessions' and 'Maximum Sessions Per Endpoint'. The 'Video' entry has unchecked boxes for 'In' and 'Out'.

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"/>		

6.3.2. Media Rules

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

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

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

6.3.2.1 Media Rule for SP

Clone the Signaling Rule **default-low-med** with a descriptive name e.g. **SP-SRTP-MR** and click on the **Finish** button (not shown). Select this newly created rule and click on **Edit** to modify the parameters as shown below. Then click on **Finish** (not shown) again to save the changes.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Domain Policies, TLS Management, and Device Specific Settings. Under "Domain Policies", "Media Rules" is selected. The main content area is titled "Media Rules: SP-SRTP-MR". It features a list of media rules on the left, with "SP-SRTP-MR" highlighted. On the right, there are tabs for "Media Encryption", "Media Silencing", "Media QoS", "Media BFCP", and "Media FECC". The "Media Encryption" tab is active, showing settings for "Audio Encryption" and "Video Encryption". The "Audio Encryption" section includes "Preferred Formats" (SRTP_AES_CM_128_HMAC_SHA1_32, SRTP_AES_CM_128_HMAC_SHA1_80), "Encrypted RTCP" (checked), "MKI" (unchecked), "Lifetime" (Any), and "Interworking" (checked). The "Video Encryption" section includes "Preferred Formats" (RTP) and "Interworking" (unchecked). A "Miscellaneous" section at the bottom includes "Capability Negotiation" (unchecked). Buttons for "Add", "Filter By Device...", "Rename", "Clone", "Delete", and "Edit" are visible.

Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_32 SRTP_AES_CM_128_HMAC_SHA1_80
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 type="checkbox"/>

6.3.2.2 Media rule for EN

Clone the Media Rule **default-low-med** with a descriptive name e.g. **EN-SRTP-MR** and click on the **Finish** button (not shown). Select this newly created rule and click on **Edit** to modify the parameters as shown below. Then click on **Finish** again to save the changes.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Media Rules' highlighted. The main content area is titled 'Media Rules: EN-SRTP-MR'. It includes an 'Add' button, a 'Filter By Device...' dropdown, and buttons for 'Rename', 'Clone', and 'Delete'. Below these is a link to 'Click here to add a description.' The configuration is divided into several sections: 'Media Encryption' (selected), 'Media Silencing', 'Media QoS', 'Media BFCP', and 'Media FECC'. The 'Media Encryption' section is further divided into 'Audio Encryption' and 'Video Encryption'. The 'Audio Encryption' section shows 'Preferred Formats' as 'SRTP_AES_CM_128_HMAC_SHA1_32' and 'SRTP_AES_CM_128_HMAC_SHA1_80', 'Encrypted RTCP' checked, 'MKI' unchecked, 'Lifetime' as 'Any', and 'Interworking' checked. The 'Video Encryption' section shows 'Preferred Formats' as 'RTP' and 'Interworking' unchecked. The 'Miscellaneous' section shows 'Capability Negotiation' unchecked. An 'Edit' button is at the bottom right.

6.3.3. Signaling Rules

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

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 SP and EN.

6.3.3.1 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** were

set to **Allow**, and **Enable Content-Type Checks** was enabled with **Action** and **Multipart-Action** were set to **Allow** (not shown).

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

- Select the proper Quality of Service (QoS).
- 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 left sidebar contains a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, and Signaling Rules (highlighted in red). The main content area is titled "Signaling Rules: SP-SR" and includes an "Add" button, a "Filter By Device..." dropdown, and buttons for "Rename", "Clone", and "Delete". 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" (highlighted in red). The "Signaling QoS" tab is active, showing a table with the following data:

Signaling QoS	
QoS Type	DSCP
DSCP	EF

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

6.3.3.2 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** were set to **Allow**, and **Enable Content-Type Checks** was enabled with **Action** and **Multipart-Action** were set to **Allow** (not shown). Similarly the Signaling QoS rules are set as shown in Figure below.

Similarly the Signaling QoS rules are set as shown in Figure below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, and Signaling Rules (highlighted in red). The main content area is titled "Signaling Rules: EN-SR" and includes an "Add" button, a "Filter By Device..." dropdown, and buttons for "Rename", "Clone", and "Delete". 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" (highlighted in red). The "Signaling QoS" tab is active, showing a table with the following data:

Signaling QoS	
QoS Type	DSCP
DSCP	EF

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

6.3.4. 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 6.4.4**.

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 Group** button (not shown).

6.3.4.1 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 6.3.1.1**.
- Set Media Rule to **SP-SRTP-MR** which was created in **Section 6.3.2.1**.
- Set Signaling Rule to **SP-SR** which was created in **Section 6.3.3.1**.
- 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 lists navigation options: Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, End Point Policy Groups (highlighted), Session Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Policy Groups: SP-PG'. It includes an 'Add' button, a 'Filter By Device...' dropdown, and buttons for 'Rename', 'Clone', and 'Delete'. Below these are two blue bars with text: '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 a Summary button. The table has one row with the following values: Order 1, Application SP-AR, Border default, Media SP-SRTP-MR, Security default-med, Signaling SP-SR, and an Edit button.

Order	Application	Border	Media	Security	Signaling
1	SP-AR	default	SP-SRTP-MR	default-med	SP-SR

6.3.4.2 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 lists navigation options: Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, End Point Policy Groups (highlighted), Session Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Policy Groups: EN-PG'. It includes an 'Add' button, a 'Filter By Device...' dropdown, and buttons for 'Rename', 'Clone', and 'Delete'. Below these are two blue bars with text: '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 a Summary button. 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
1	EN-AR	default	EN-SRTP-MR	default-med	EN-SR

6.4. 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.

6.4.1. Network Management

The Network Management page is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address, 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 'Network Management: mSBCE' page with the 'Interfaces' tab selected. A table lists two interfaces, A1 and B1, both with a status of 'Enabled'. An 'Add VLAN' button is visible in the top right corner of the table area.

Interface Name	VLAN Tag	Status
A1		Enabled
B1		Enabled

On the **Networks** tab and verify the IP addresses assigned to the interfaces and that the interfaces were 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 'Network Management: mSBCE' page with the 'Networks' tab selected. A table lists two networks, Network_A1 and Network_B1, with their respective gateway, subnet mask, interface, and IP address. 'Edit' and 'Delete' buttons are available for each network entry.

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

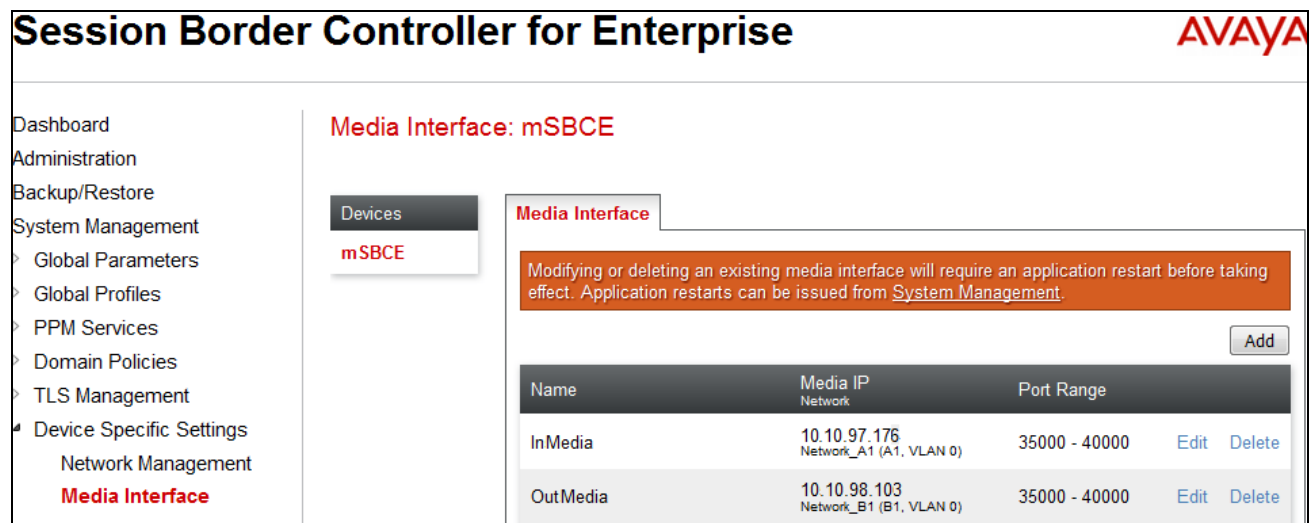
6.4.2. Media Interface

The Media Interface screen is where the media ports are defined. Avaya SBCE will open connection for RTP traffic on the defined ports.

To create a new **Media Interface**, navigate to **Device Specific Settings → Media Interface** and click on the **Add Media Interface** button (not shown).

Two separate Media Interfaces are needed for both the inside and outside interfaces. The following screen shows the Media Interfaces **InsideMedia** and **OutsideMedia** were created for the compliance testing.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.



The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The main title is "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar contains navigation links: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings, Network Management, and Media Interface (highlighted). The main content area is titled "Media Interface: mSBCE" and includes a sub-tab "Media Interface". A warning message states: "Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below this is an "Add" button and a table of media interfaces.

Name	Media IP Network	Port Range	
InMedia	10.10.97.176 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
OutMedia	10.10.98.103 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit Delete

6.4.3. Signaling Interface

The Signaling Interface screen is where the SIP signaling port is defined. Avaya SBCE will listen for SIP requests on the defined port.

To create a new **Signaling Interface**, navigate to **Device Specific Settings → Signaling Interface** and click on the **Add Signaling Interface** button (not shown).

Two separate Signaling Interfaces are needed for both inside and outside interfaces. The following screen shows the Signaling Interfaces **InsideSIP** and **OutsideSIP** were created in the compliance testing with **TLS/5061** and **TLS/5061** respectively configured for inside and outside interfaces.

Session Border Controller for Enterprise AVAYA

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

Signaling Interface: mSBCE

Devices
mSBCE

Signaling Interface

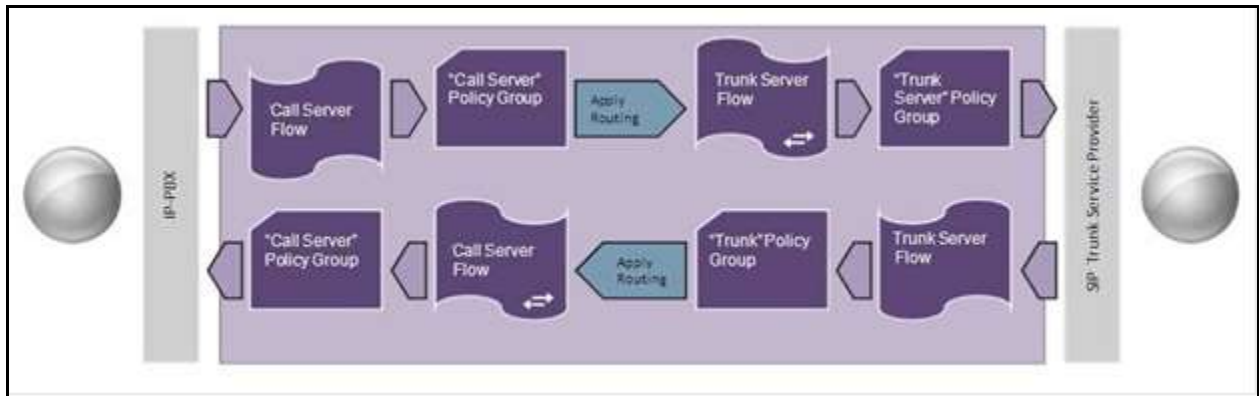
Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIG	10.10.97.176 Network_A1 (A1, VLAN 0)	5060	5060	5061	AvayaSBCServer	Edit Delete
OutsideSIG	10.10.98.103 Network_B1 (B1, VLAN 0)	5060	5060	5061	AvayaSBCServer	Edit Delete

6.4.4. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through 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 6.2.3** which the Server Flow associates to.
- **URI Group:** Select “*”.
- **Received Interface:** Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration is designed to receive SIP signaling from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration is designed to send the SIP signaling to.
- **Media Interface:** Select the Media Interface created in **Section 6.4.2** 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 6.3.4**.
- **Routing Profile:** Select the Routing Profile created in **Section 6.2.4**.
- **Topology Hiding Profile:** Select the Topology Hiding profile created in **Section 6.2.5** 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.

Edit Flow: SP-SF

X

Flow Name	<input type="text" value="SP-SF"/>
Server Configuration	<input type="text" value="SP-SC"/>
URI Group	<input type="text" value="*/"/>
Transport	<input type="text" value="*/"/>
Remote Subnet	<input type="text" value="*/"/>
Received Interface	<input type="text" value="InsideSIG"/>
Signaling Interface	<input type="text" value="OutsideSIG"/>
Media Interface	<input type="text" value="OutMedia"/>
End Point Policy Group	<input type="text" value="SP-PG"/>
Routing Profile	<input type="text" value="EN-RP"/>
Topology Hiding Profile	<input type="text" value="SP-TH"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Remote Branch Office	<input type="text" value="Any"/>

Finish

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

Edit Flow: EN-SF

X

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

Finish

7. Intermedia SIP Trunking Configuration

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

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

8. Verification Steps

The following steps may be used to verify the configuration:

- Use 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).

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System
Alarms (19)
Extensions (26)
Trunks (4)
Line:1
Line:2
Line:17
Line:19
Active Calls
Resources
Voicemail
IP Networking
Locations

Status Utilization Summary Alarms

SIP Trunk Summary

Line Service State: In Service
Peer Domain Name: avayalab.com
Resolved Address: 135.10.97.176
Line Number: 19
Number of Administered Channels: 20
Number of Channels in Use: 0
Administered Compression: G711 Mu
Enable Faststart: Off
Silence Suppression: Off
Media Stream: RTP
Layer 4 Protocol: UDP
SIP Trunk Channel Licenses: Unlimited
SIP Trunk Channel Licenses in Use: 0
SIP Device Features:

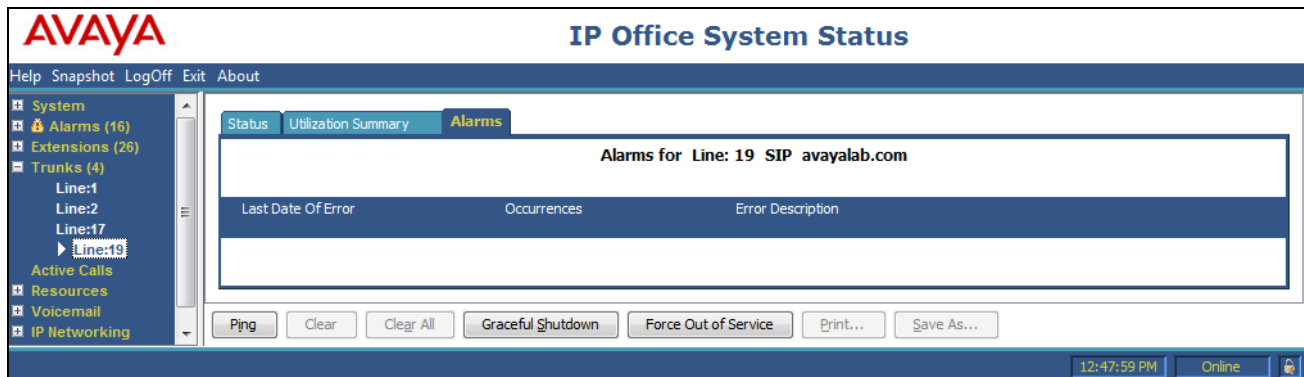
0%

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	00:24:32											
2			Idle	00:49:27											
3			Idle	20:23:27											
4			Idle	20:23:27											
5			Idle	20:23:27											

Trace Trace All Pause Ping Call Details Graceful Shutdown Force Out of Service Print... Save As...

12:44:34 PM 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 Avaya IP Office with two-way audio.
- Verify that a phone connected to Avaya 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 Intermedia. The sniffer traces are captured at the public interface of Avaya SBCE.

9. Conclusion

The Intermedia SIP Trunking passed compliance testing. These Application Notes describe the procedures required to configure the SIP connection between Avaya IP Office, Avaya SBCE and the Intermedia SIP Trunking service as shown in **Figure 1**.

10. Additional References

- [1] *IP Office 9.1 Administering Avaya IP Office Platform with Manager*, Release 9.1.0, Issue 10.03, February 2015.
- [2] *Administering Avaya IP Office™, Platform Voicemail Pro IP Office™ Platform 9.115-601063*, Issue 10c - (09 December 2014).
- [3] */ IP Office Embedded Voicemail User Guide (IP Office Mode)*, Document number 15-604067, Issue 9.0, 10 September 2013.
- [4] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 7.0, Issue 1, August 2015.
- [5] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 1, August 2015.
- [6] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.0, Issue 1, August 2015.
- [7] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 1, August 2015.
- [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 1.0.4, October 2015.

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 Intermedia SIP Trunking is available from Intermedia.

©2016 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.