



Application Notes for Configuring Avaya IP Office Release 11.1 with Avaya Session Border Controller for Enterprise Release 8.1 to support Telenor IPT Multi-User SIP Trunk – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Telenor IPT Multi-User SIP Trunk and Avaya IP Office R11.1 with Avaya Session Border Controller for Enterprise R8.1.

The Telenor IPT Multi-User SIP Trunk Platform provides PSTN access via a SIP trunk connected to the Telenor Voice over Internet Protocol (VoIP) network as an alternative to legacy analogue or digital trunks. Telenor is a member of the Avaya DevConnect Service Provider program.

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

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

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Telenor IPT Multi-User SIP Trunk service and Avaya IP Office R11.1 with Avaya Session Border Controller for Enterprise (Avaya SBCE) R8.1.

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

Avaya Session Border Controller for Enterprise (Avaya SBCE) is the point of connection between Avaya IP Office and Telenor IPT Multi-User SIP Trunk service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signalling for interoperability.

Telenor IPT Multi-User SIP Trunk service provides PSTN access via a SIP trunk connected to the Telenor network as an alternative to legacy Analog or Digital trunks. This approach generally results in lower cost for customers

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office and Avaya SBCE to connect to the Telenor IPT Multi-User SIP Platform. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with this Application Note, the interface between Avaya systems and the Telenor SIP Trunk do not include use of any specific encryption features. Encryption TLS and SRTP was used internal to the enterprise between Avaya products.

2.1. Interoperability Compliance Testing

Avaya IP Office was connected to the Telenor IPT Multi-User SIP Trunk. To verify SIP trunking interoperability the following features and functionality were exercised during the interoperability compliance test:

- Incoming PSTN calls to various phone types including 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 including 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.
- Calls using the G.722 and G.711A codecs.
- Inbound and outbound PSTN calls to/from Avaya IX Workplace™ for Windows Softphone client.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using G.711 fax transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail for inbound and outbound calls.
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, transfer, and conference.
- Call transfer to PSTN.
- Off-net call forwarding and mobile twinning.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Telenor IPT Multi-User SIP Trunk with the following observations:

- It was observed during failover testing that when Telenor's priority A SIP trunk server is down, the Avaya SBCE is not re-routing the call to Telenor's next Priority B or priority C SIP trunk server until 32 seconds later. Telenor have indicated that this will create issues with some of their customer SIP platform set-ups. As requested by Telenor, the "Trans Expire" value on the Telenor Server Interworking profile needs to be set to 5 seconds as per **Section 6.5.2**. This enables Timer B on the SIP INVITE and the Avaya SBCE will only wait 5 seconds before re-routing to the next priority SIP trunk server.
- The use of SIP REFER method for call redirection and call transfer to PSTN is not recommended for this solution. SIP reINVITE method should be used for call redirection and call transfers to PSTN and has been tested successfully. Please ensure "Incoming Supervised REFER" and "Outgoing Supervised REFER" are set to "Never" on the SIP Line as per **Section 5.6.2**. This ensures SIP reINVITE method will always be used for call redirection and call transfer to PSTN.
- T.38 fax is not supported by Telenor and therefore was not tested.
- No inbound toll-free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked by the Service Provider with the Emergency Services Operator.

2.3. Support

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

For technical support on Telenor products please use the following web link: <https://www.telenor.no/bedrift/kundeservice/>

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Telenor IPT Multi-User SIP Trunk. Located at the enterprise site is an Avaya IP Office Server Edition, an Avaya IP Office 500 V2 as an Expansion and an Avaya Session Border Controller for Enterprise. Endpoints include Avaya 1600 Series IP Telephones (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware), Avaya J179 SIP Telephones, Avaya 1140e SIP Telephones, Avaya 1400 Series Digital Deskphones, Analog Telephone and a fax machine. The site also has a Windows 7 PC running Avaya IP Office Manager to configure the Avaya IP Office as well as Avaya IX Workplace™ for Windows softphone client.

For security purposes, all Service Provider IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes. Instead, all IP addresses have been changed to a private format and all phone numbers have been obscured beyond the city code.

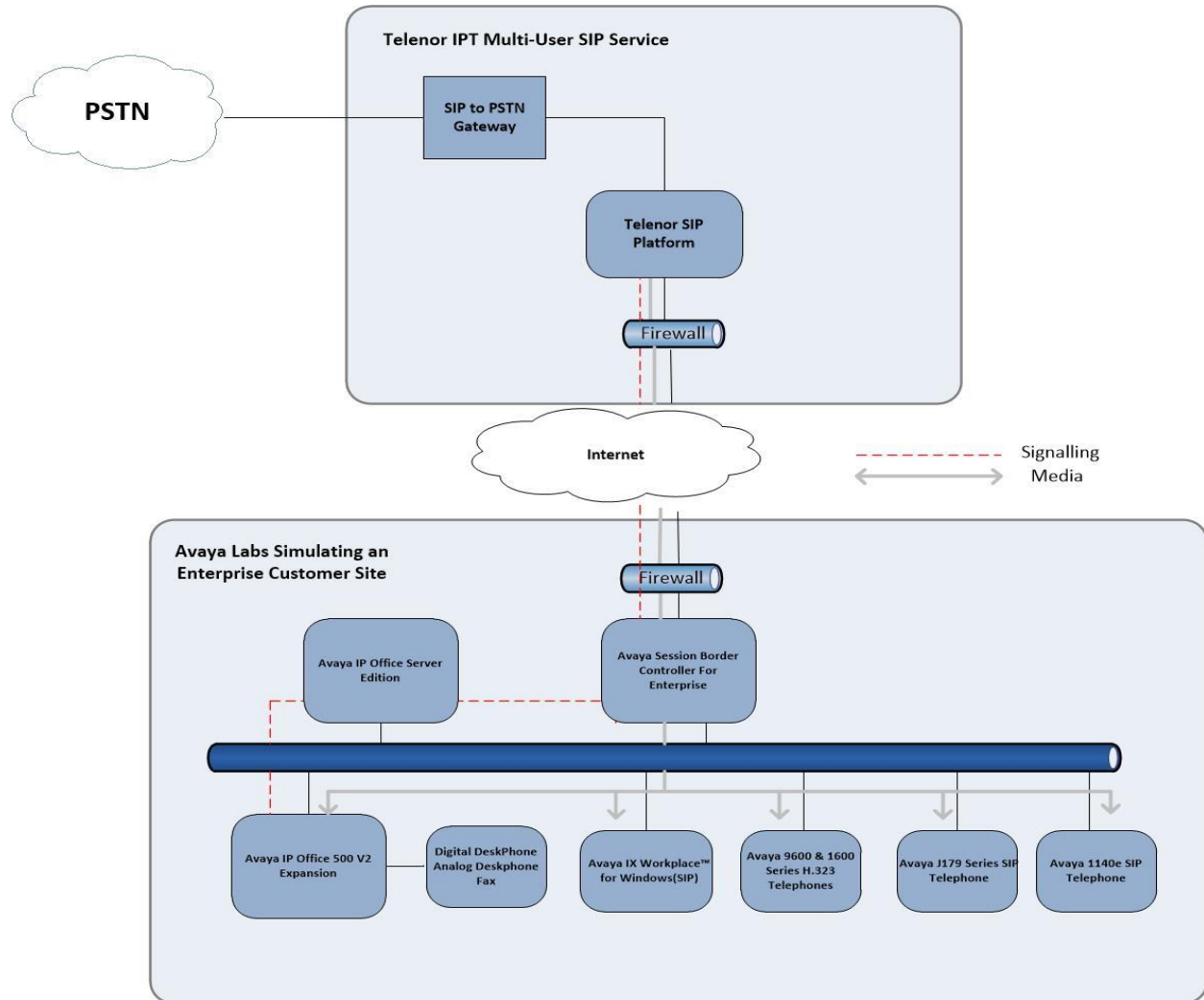


Figure 1: Telenor IPT Multi-User SIP Trunk to Avaya IP Office Topology

4. Equipment and Software Validated

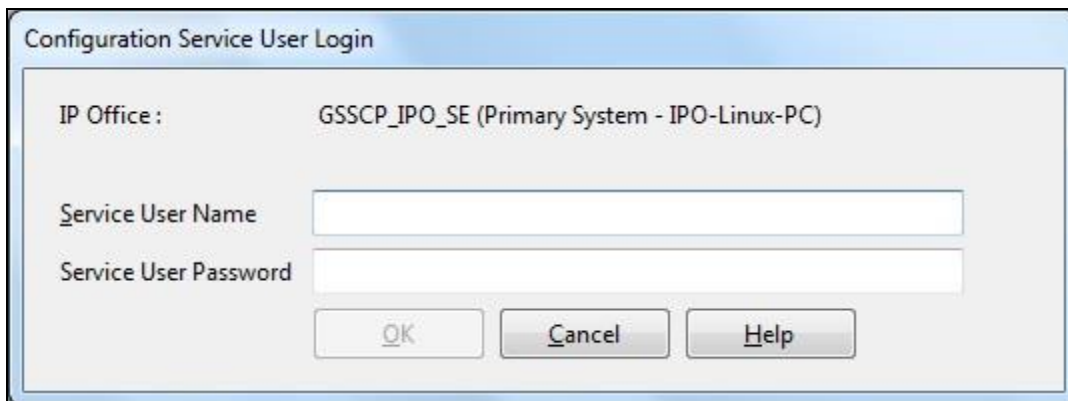
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	Version 11.1.0..0.0 build 237
Avaya IP Office 500 V2	Version 11.1.0..0.0 build 237
Avaya IP Office Manager	Version 11.1.0..0.0 build 237
Avaya Session Border Controller for Enterprise	8.1.0.0-14-18490
Avaya 1608 Phone (H.323)	1.3.12
Avaya 9611G Series Phone (H.323)	6.8.0
Avaya J179 Series Phone (SIP)	4.0.4.0.10
Avaya 1140e (SIP)	FW: 04.04.23.00.bin
Avaya IX Workplace™ for Windows(SIP)	3.11.0.44.25
Avaya 1408 Digital Telephone	R48
Avaya Analogue Phone	N/A
Telenor	
IPT Version	1.15.277

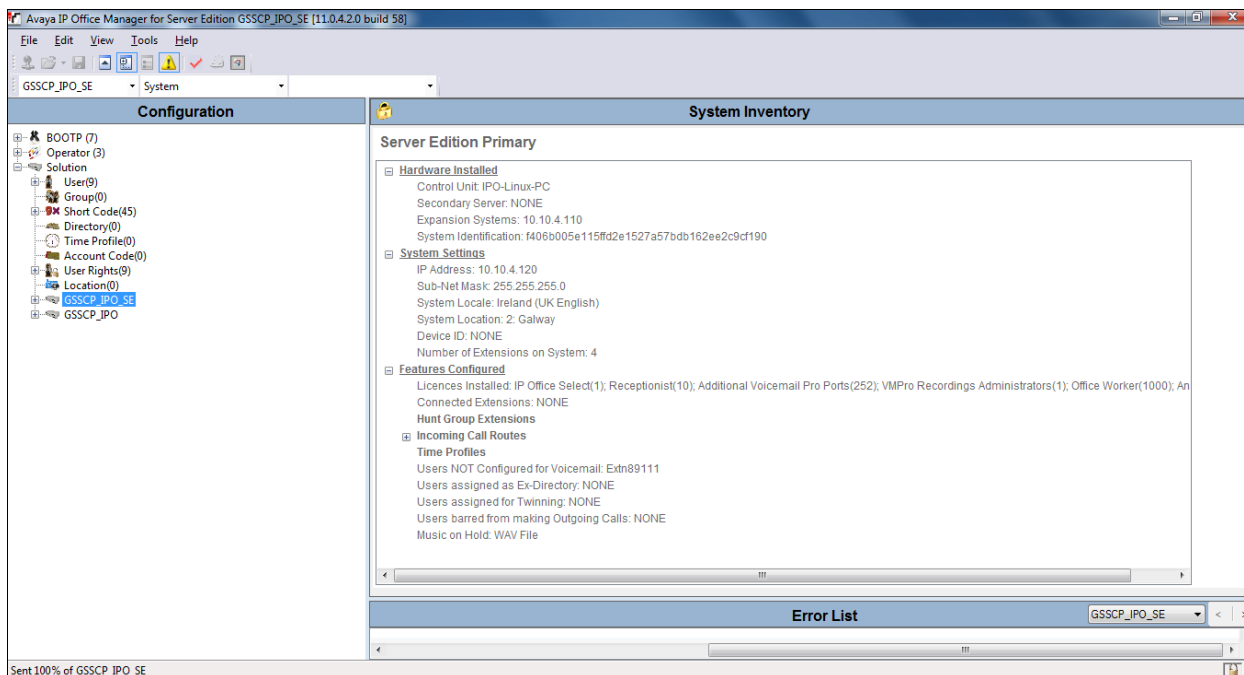
Note – Testing was performed with IP Office Server Edition with 500 V2 Expansion R11.1. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. **Note:** that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks, this includes T.38 fax.

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to the Telenor IPT Multi-User SIP platform. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the appropriate 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 in the next section. All the Avaya IP Office configurable components are shown in the left pane known as the Navigation Pane. The pane on the right is the Details Pane. These panes will be referenced throughout the Avaya IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the Service Provider is assumed to already be in place.



5.1. Verify System Capacity

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

Licence Remote Server

Licence Mode Licence Normal

Licensed Version 11.0

PLDS Host ID 647560473402

PLDS File Status Valid

Feature	Instances	Status	Expiry Date	Source
Receptionist	10	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	252	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	1	Valid	Never	PLDS Nodal
Office Worker	1000	Valid	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	1	Obsolete	Never	PLDS Nodal
Power User	1000	Valid	Never	PLDS Nodal
Customer Service Agent	100	Dormant	Never	PLDS Nodal
Customer Service Supervisor	100	Dormant	Never	PLDS Nodal
Avaya IP endpoints	1000	Valid	Never	PLDS Nodal
SIP Trunk Channels	256	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	1	Valid	Never	PLDS Nodal
Wave User	16	Obsolete	Never	PLDS Nodal
3rd Party IP Endpoints	1000	Valid	Never	PLDS Nodal
Server Edition	150	Valid	Never	PLDS Nodal
UMS Web Services	1000	Valid	Never	PLDS Nodal
Avaya Mac Softphone	1000	Valid	Never	PLDS Nodal

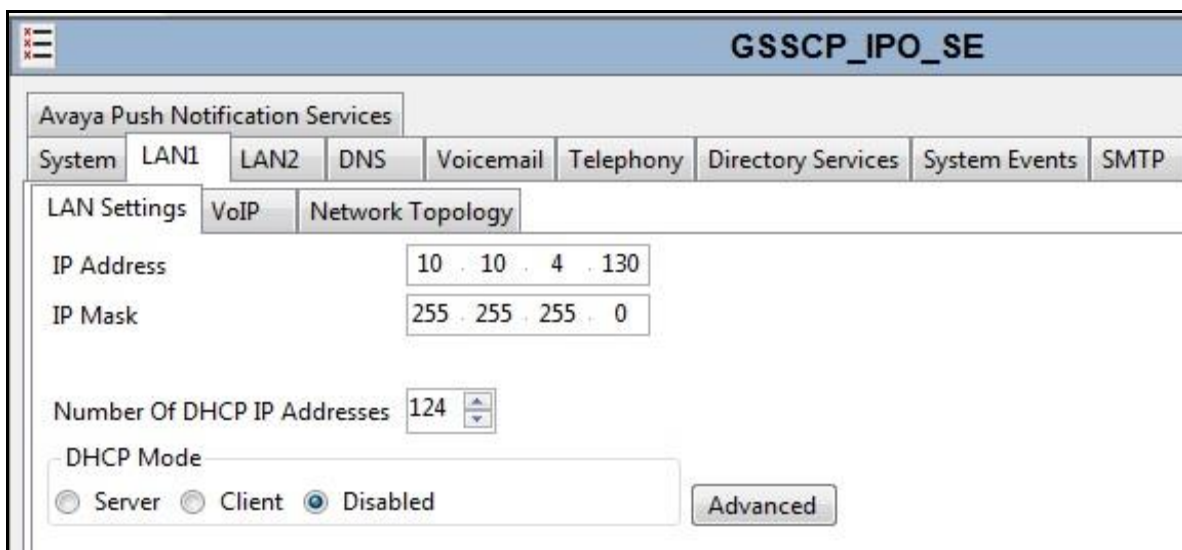
Add...

Remove

5.2. LAN1 Settings

In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to connect the Avaya IP Office to the internal side of the Avaya SBCE as these are on the same LAN, **LAN2** was not used.

To access the LAN1 settings, first navigate to **System → GSSCP_IPO_SE** in the Navigation Pane where GSSCP_IPO_SE is the name of the IP Office. Navigate to the **LAN1 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the private interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).



The screenshot shows the configuration interface for GSSCP_IPO_SE. The top navigation bar includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, and SMTP. The LAN1 tab is selected, and the LAN Settings sub-tab is active. The IP Address is set to 10.10.4.130 and the IP Mask is 255.255.255.0. The Number Of DHCP IP Addresses is set to 124. The DHCP Mode is set to Disabled. An Advanced button is visible at the bottom right.

On the **VoIP** tab in the Details Pane, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol. Set **H.323 Signalling over TLS** to **Preferred** to allow IP Office H323 endpoints to use TLS for signalling. Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. If SIP Endpoints are to be used such as the Avaya Communicator for Windows and the Avaya 1140e, the **SIP Registrar Enable** box must also be checked. The **Domain Name** has been set to the customer premises equipment domain “**avaya.com**”. If the **Domain Name** is left at the default blank setting, SIP registrations may use the IP Office LAN1 IP Address. All other parameters shown are default values.

The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Set **Scope** to **RTP-RTCP** and **Initial keepalives** to **Enabled** and **Periodic timeout** to **30**. This will cause the IP Office to send RTP and RTCP keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP/RTCP traffic is present.

Avaya IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for both signalling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signalling. The specific values used for the compliance test are shown in the example below. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).

The screenshot displays the 'GSSCP_IPO_SE' configuration window. The 'VoIP' tab is selected, showing 'SIP' and 'Network Topology' sub-tabs. The 'SIP' sub-tab is active, displaying various configuration options for SIP services. Below the SIP settings, the 'RTP' section is visible, showing port ranges and monitoring options. At the bottom, the 'DiffServ Settings' section is partially visible.

GSSCP_IPO_SE

Avaya Push Notification Services

System LAN1 LAN2 DNS Voicemail Telephony Directory Services System Events SMTP SMDR VoIP Contact Center Avaya Cloud Services

LAN Settings VoIP Network Topology

☒ H323 Gatekeeper Enable
☐ Auto-create Extn ☐ Auto-create User ☐ H323 Remote Extn Enable
H.323 Signalling over TLS Preferred Remote Call Signalling Port 1720

☒ SIP Trunks Enable
☒ SIP Registrar Enable
☐ Auto-create Extn/User ☐ SIP Remote Extn Enable Allowed SIP User Agents Allow All

SIP Domain Name avaya.com
SIP Registrar FQDN avaya.com

Layer 4 Protocol
☒ UDP UDP Port 5060 Remote UDP Port 5060
☒ TCP TCP Port 5060 Remote TCP Port 5060
☒ TLS TLS Port 5061 Remote TLS Port 5061

Challenge Expiry Time (secs) 10

RTP
Port Number Range
Minimum 49152 Maximum 53246
Port Number Range (NAT)
Minimum 49152 Maximum 53246
☒ Enable RTCP Monitoring on Port 5005
RTCP collector IP address for phones 0 . 0 . 0 . 0
Keepalives
Scope RTP-RTCP Periodic timeout 30
Initial keepalives Enabled

DiffServ Settings
B8 DSCP(Hex) B8 Video DSCP(Hex) FC DSCP Mask (Hex) 88 SIG DSCP (Hex)
46 DSCP 46 Video DSCP 63 DSCP Mask 34 SIG DSCP

On the **Network Topology** tab, set the **Firewall/NAT Type** from the pulldown menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used as NAT was not required for this configuration, therefore resulting in no requirement for a STUN server. The **Use Network Topology Info** in the **SIP Line** was set to **None** in **Section 5.6.2**. Set **Binding Refresh Time (seconds)** to **60**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider. Default values were used for all other parameters. On completion, click the **OK** button (not shown).

The screenshot shows the 'GSSCP_IPO_SE' configuration window with the 'Network Topology' tab selected. The window has a title bar with standard OS controls and a menu bar with options like System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, Contact Center, and Avaya Cloud Services. Below the menu bar, there are sub-tabs for LAN Settings, VoIP, and Network Topology. The 'Network Topology' sub-tab is active, showing a 'Network Topology Discovery' section. This section contains several fields: 'STUN Server Address' (0.0.0.0), 'STUN Port' (3478), 'Firewall/NAT Type' (Open Internet), 'Binding Refresh Time (seconds)' (60), and 'Public IP Address' (0.0.0.0). There are also 'Run STUN' and 'Cancel' buttons. Below these fields, there is a 'Public Port' section with three rows: 'UDP' (5060), 'TCP' (5060), and 'TLS' (5061). At the bottom left, there is a checkbox labeled 'Run STUN on startup' which is currently unchecked.

Network Topology Discovery	
STUN Server Address	0.0.0.0
STUN Port	3478
Firewall/NAT Type	Open Internet
Binding Refresh Time (seconds)	60
Public IP Address	0 . 0 . 0 . 0
<input type="button" value="Run STUN"/> <input type="button" value="Cancel"/>	
Public Port	
UDP	5060
TCP	5060
TLS	5061
<input type="checkbox"/> Run STUN on startup	

5.3. System Telephony Settings

Navigate to the **Telephony** → **Telephony** tab on the Details Pane. Choose the **Companding Law** typical for the enterprise location. For Europe, **ALAW** 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. On completion, click the **OK** button (not shown).

The screenshot displays the 'GSSCP_IPO_SE*' configuration window. The 'Telephony' tab is selected, showing various settings for telephony services. The 'Companding Law' section is highlighted, showing 'A-Law' selected for the 'Switch' and 'A-Law Line' selected for the 'Line'. Other settings include 'Dial Delay Time (secs)' set to 1, 'Dial Delay Count' set to 4, 'Default No Answer Time (secs)' set to 15, 'Hold Timeout (secs)' set to 0, 'Park Timeout (secs)' set to 300, 'Ring Delay (secs)' set to 5, 'Call Priority Promotion Time (secs)' set to Disabled, 'Default Currency' set to EUR, 'Default Name Priority' set to Favour Trunk, 'Media Connection Preservation' set to Enabled, 'Phone Failback' set to Automatic, 'Login Code Complexity' set to Enforcement, 'Minimum length' set to 4, and 'Complexity' checked. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked.

System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	VoIP	Contact Center	Avaya Cloud Services
Avaya Push Notification Services												
Telephony Park & Page Tones & Music Ring Tones SM Call Log TUI												
Dial Delay Time (secs) 1												
Dial Delay Count 4												
Default No Answer Time (secs) 15												
Hold Timeout (secs) 0												
Park Timeout (secs) 300												
Ring Delay (secs) 5												
Call Priority Promotion Time (secs) Disabled												
Default Currency EUR												
Default Name Priority Favour Trunk												
Media Connection Preservation Enabled												
Phone Failback Automatic												
Login Code Complexity												
Enforcement												
Minimum length 4												
Complexity												
Companding Law												
Switch												
U-Law												
A-Law												
Line												
U-Law Line												
A-Law Line												
DSS Status												
Auto Hold												
Dial By Name												
Show Account Code												
Inhibit Off-Switch Forward/Transfer												
Restrict Network Interconnect												
Include location specific information												
Drop External Only Impromptu Conference												
Visually Differentiate External Call												
High Quality Conferencing												

5.4. VoIP Settings

Navigate to the **VoIP** tab on the Details Pane. Check the available Codecs boxes as required. Note that **G.711 ULAW 64K** and **G.711 ALAW 64K** are greyed out and always available. Once available codecs are selected, they can be used or unused by using the horizontal arrows as required. Note that in test, **G.722 64K** is set as the priority codec and **G.711 ALAW 64K** set as the secondary codec as per screenshot below.

The screenshot displays the 'GSSCP_IPO_SE' configuration window. The 'VoIP' tab is selected, and the 'VoIP Security' sub-tab is active. The 'Ignore DTMF Mismatch For Phones' checkbox is checked, and 'Allow Direct Media Within NAT Location' is unchecked. The 'RFC2833 Default Payload' is set to 101. Under 'Available Codecs', G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, and G.729(a) 8K CS-AC are all checked. The 'Default Codec Selection' section shows 'Unused' codecs (G.711 ULAW 64K, G.729(a) 8K CS-A) and 'Selected' codecs (G.722 64K, G.711 ALAW 64K). Navigation buttons (right arrow, up arrow, left arrow, down arrow, and right arrow) are positioned between the 'Unused' and 'Selected' lists.

GSSCP_IPO_SE										
Avaya Push Notification Services										
System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	VoIP
VoIP										
VoIP Security Access Control Lists										
Ignore DTMF Mismatch For Phones <input checked="" type="checkbox"/>										
Allow Direct Media Within NAT Location <input type="checkbox"/>										
RFC2833 Default Payload: 101										
<div><div>Available Codecs</div><div><input checked="" type="checkbox"/> G.711 ULAW 64K <input checked="" type="checkbox"/> G.711 ALAW 64K <input checked="" type="checkbox"/> G.722 64K <input checked="" type="checkbox"/> G.729(a) 8K CS-AC</div></div> <div><div>Default Codec Selection</div><div><div>Unused</div><div>G.711 ULAW 64K G.729(a) 8K CS-A</div></div><div><div>Selected</div><div>G.722 64K G.711 ALAW 64K</div></div></div>										

5.5. VoIP Security

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

In the compliance testing, **Preferred** is selected as this allows IP Office to fall back to non-secure media if the attempt to use secure media is unsuccessful.

Navigate to **System → VoIP Security** tab and configure as follows:

- Select **Preferred** for **Media**.
- Check **RTP** for **Encryptions**.
- Check **RTP** for **Authentication**.
- Check **SRTP_AES_CM_128_SHA1_80** for **Crypto Suites**.
- Other parameters are left as default.
- Click **OK**.

The screenshot shows the 'GSSCP_IPO_SE' configuration window. The 'VoIP' tab is selected, and within it, the 'VoIP Security' sub-tab is active. The 'Access Control Lists' sub-tab is also visible. The 'Default Extension Password' and 'Confirm Default Extension Password' fields are both masked with dots. The 'Media' dropdown is set to 'Preferred'. The 'Strict SIPS' checkbox is unchecked. Under 'Media Security Options', the 'Encryptions' section has 'RTP' checked and 'RTCP' unchecked. The 'Authentication' section has 'RTP' checked and 'RTCP' unchecked. The 'Replay Protection' section is empty. The 'SRTP Window Size' is set to 64. The 'Crypto Suites' section has 'SRTP_AES_CM_128_SHA1_80' checked and 'SRTP_AES_CM_128_SHA1_32' unchecked.

5.6. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Telenor IPT Multi-User SIP platform. 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 5.6.1** to create the SIP Line from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.6.2**.

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

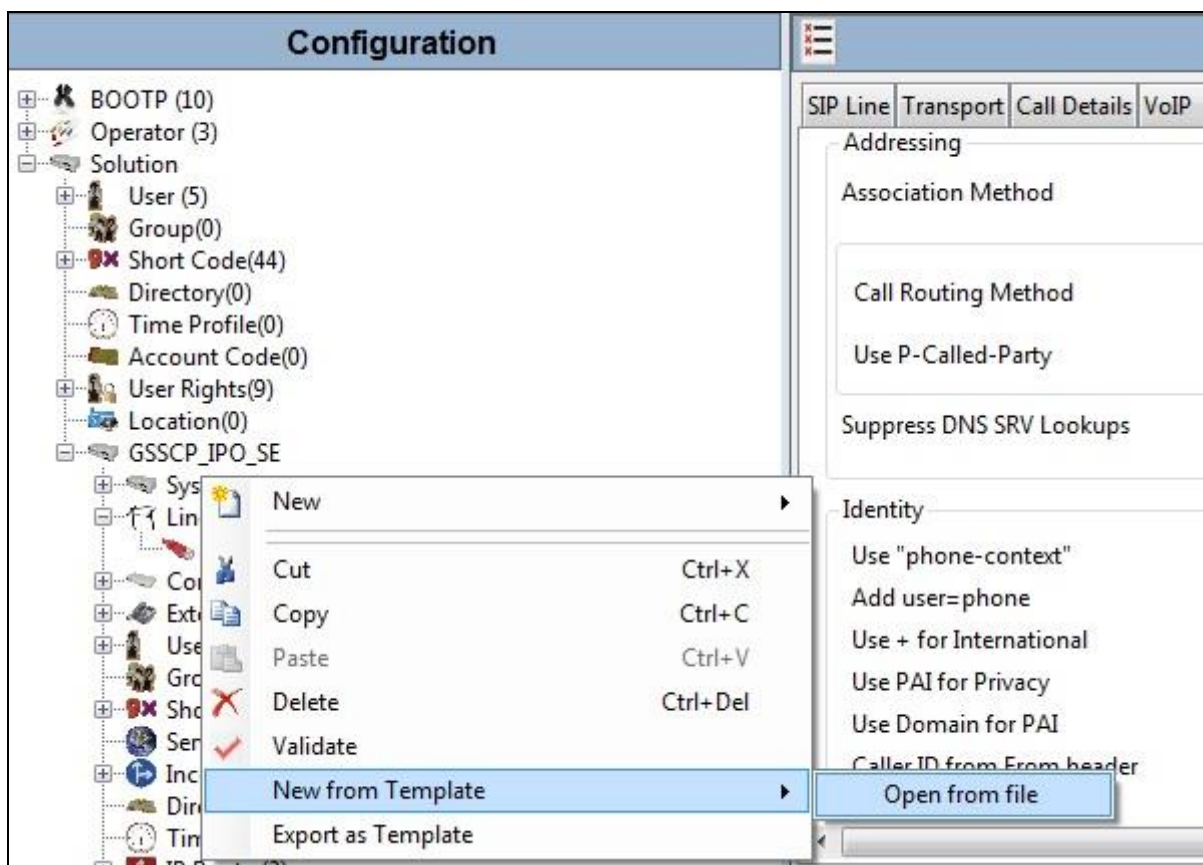
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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 **Section 5.6.2**.

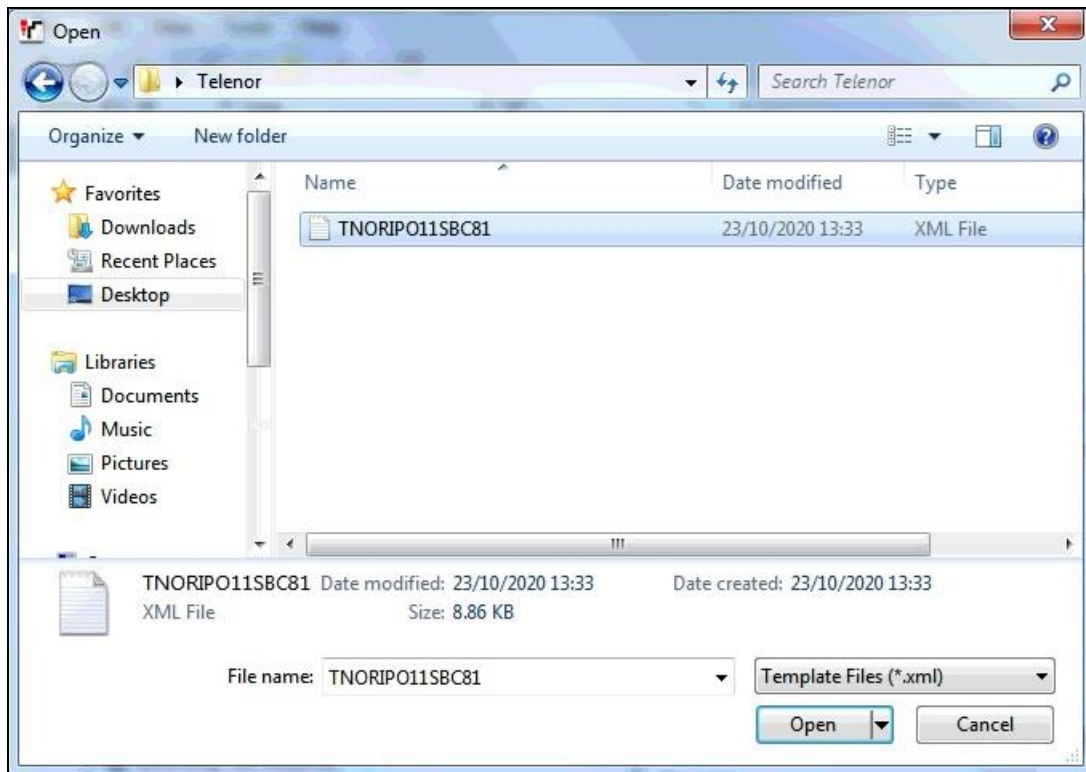
5.6.1. SIP Line From Template

DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

Copy a previously created template file to a location (e.g., *\temp*) on the same computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New** → **New from Template**.



Navigate to the directory on the local machine where the template was copied and select the template as required.



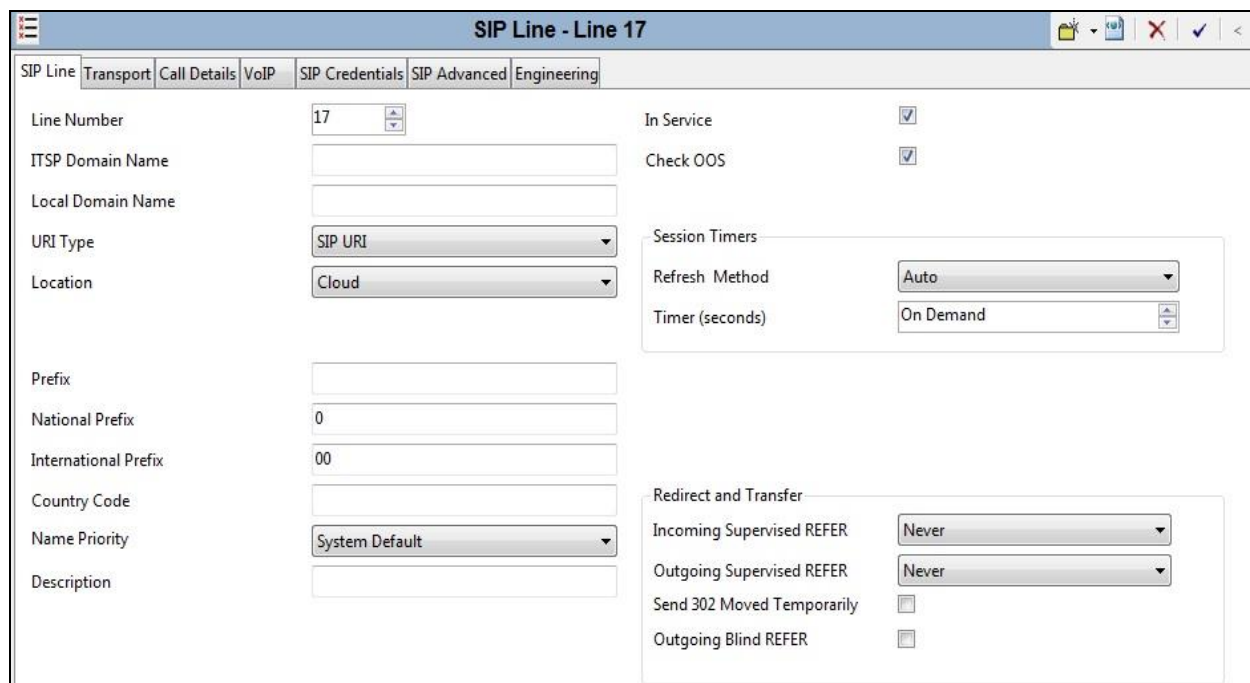
The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.6.2**.

5.6.2. Manual SIP Line Configuration

On the **SIP Line** tab in the Details Pane, configure the parameters below to connect to the SIP Trunking service.

- Set **ITSP Domain Name** to a domain name provided by the Service Provider if required, however no ITSP Domain Name was used in this configuration.
- Set **National Prefix** to **0** and **International Prefix** to **00** for number conversion as follows: outbound national and international called party numbers are converted to E.164 format; inbound national and international calling party numbers are converted to diallable format.
- Ensure the **In Service** box is checked.
- Ensure the **Check OSS** box is checked.
- Leave the **Refresh Method** at the default value of **Auto**.
- Leave **Timer (seconds)** at the default value of **On Demand**. This value allows the Session Refresh interval to be set by the network.
- Set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never** as per **Section 2.2**.
- Default values may be used for all other parameters.

On completion, click the **OK** button (not shown).



The screenshot shows the 'SIP Line - Line 17' configuration window. The 'SIP Line' tab is selected. The configuration fields are as follows:

Field	Value
Line Number	17
ITSP Domain Name	
Local Domain Name	
URI Type	SIP URI
Location	Cloud
Prefix	
National Prefix	0
International Prefix	00
Country Code	
Name Priority	System Default
Description	
In Service	<input checked="" type="checkbox"/>
Check OSS	<input checked="" type="checkbox"/>
Session Timers	
Refresh Method	Auto
Timer (seconds)	On Demand
Redirect and Transfer	
Incoming Supervised REFER	Never
Outgoing Supervised REFER	Never
Send 302 Moved Temporarily	<input type="checkbox"/>
Outgoing Blind REFER	<input type="checkbox"/>

On completion, click the **OK** button (not shown).

Select the **Transport** tab and set the following:

- Set **ITSP Proxy Address** to the inside interface IP address (**10.10.4.35**) of the Avaya SBCE as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **TLS**.
- Set **Send Port** to **5061** and **Listen Port** to **5061**.
- Set **Use Network Topology Info** to **None**.

On completion, click the OK button (not shown).

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '10.10.4.35'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'TLS', 'Send Port' is '5061', 'Use Network Topology Info' is set to 'None', and 'Listen Port' is '5061'. 'Explicit DNS Server(s)' are set to '0.0.0.0'. 'Calls Route via Registrar' is checked. There is a 'Separate Registrar' field which is currently empty.

After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, select the **Call Details** tab and click on **Add**.

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'Call Details' tab selected. The 'SIP URIs' section is visible, showing a table with columns: URI, Groups, Credential, Local URI, Contact, P Asserted ID, P Preferred ID, Diversion Header, and Remote Party ID. To the right of the table are buttons for 'Add...', 'Remove', and 'Edit...'.

A SIP URI is shown in this example that is used for calls to and from extensions that have a DDI number assigned to them. Additional SIP URI's may be required for calls to services such as Voicemail Collect and the Mobile Twinning FNE, these would be for incoming calls only.

For the compliance test, SIP URI entries were created that matched any number assigned to an Avaya IP Office user. The entry was created with the parameters shown below.

- Set **Incoming Group**. This is the value assigned for incoming calls that's analysed in the Incoming Call Route settings described in **Section 5.8**. In the test environment a value of **17** was used for the Telenor IPT Multi-User SIP platform.
- Set **Outgoing Group**. This is the value assigned for outgoing calls that can be selected directly in the short code settings described in **Section 5.7**. In the test environment a value of **17** was used.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Set **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** to **Use Internal Data** for both the **Display** name and **Content**. On incoming calls, this will analyse the Request-Line sent by Telenor and match to the SIP settings in the User profile as described in **Section 5.7**. On outgoing calls this will insert the SIP settings in the User profile into the relevant headers in the SIP messages.
- Leave the **Outgoing Calls**, **Forwarding/Twinning** and **Incoming Calls** at their respective default values of **Caller**, **Original Caller** and **Called** for the **Local URI**, **Contact** and **P Asserted ID** call details.

The following screenshot shows the completed configuration:

URI	Groups	Credential	Local URI	Contact	P Asserted ID	P Preferred ID	Diversion Header	Remote Party ID
1	17 17	0: <None>	Use Internal Data	Use Internal Data	Use Internal Data		Use Internal Data	

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

- Select **System Default** from the drop-down menu as system default codecs were already defined in **Section 5.4**.
- Set the **Fax Transport Support** box to **G.711** as this is the preferred method of fax transmission for Telenor.
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check **Media Security to Same as System (Preferred)** and ensure that the **Same as System** box is checked. This ensures that system level media security is set to **Preferred** specifying that SRTP is preferred over RTP as configured in **Section 5.5**.
- Check the **Local Hold Music** box.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of the incoming call or transfer does not support the codec originally negotiated.
- Check the **PRACK/100rel Supported** box if early media is required. This was checked during compliance testing.
- On completion, click the **OK** button (not shown).

Default values may be used for all other parameters.

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'VoIP' tab selected. The window has a tabbed interface with 'SIP Line', 'Transport', 'Call Details', 'VoIP', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'VoIP' tab is active, displaying various configuration options. On the left, there is a 'Codec Selection' section with a dropdown menu set to 'System Default'. Below this are two lists: 'Unused' (containing G.711 ULAW 64K and G.729(a) 8K CS-ACELP) and 'Selected' (containing G.722 64K and G.711 ALAW 64K), with arrows for moving items between them. Below the codec lists are fields for 'Fax Transport Support' (set to G.711), 'DTMF Support' (set to RFC2833/RFC4733), and 'Media Security' (set to Same as System (Preferred)). At the bottom, there is an 'Advanced Media Security Options' section with a checked 'Same As System' checkbox. On the right side of the window, there are several checkboxes: 'Local Hold Music' (checked), 'Re-invite Supported' (checked), 'Codec Lockdown' (unchecked), 'Allow Direct Media Path' (unchecked), 'Force direct media with phones' (unchecked), and 'PRACK/100rel Supported' (checked).

Select the **SIP Advanced** tab and set the following:

- Check the **Add user=phone** box to send SIP parameter user with the value phone to the From and To Headers in outgoing calls.
- Check the **Use + for International** as E.164 numbering is used on the SIP Trunk.
- Default values may be used for all other parameters.

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'SIP Advanced' tab selected. The window is divided into several sections:

- Addressing:** Association Method is set to 'By Source IP address'. Call Routing Method is set to 'Request URI'. Use P-Called-Party and Suppress DNS SRV Lookups are unchecked.
- Identity:** Use "phone-context" is unchecked. Add user=phone and Use + for International are checked. Use PAI for Privacy, Use Domain for PAI, Caller ID from From header, and Send From In Clear are unchecked. Cache Auth Credentials is checked. User-Agent and Server Headers is empty. Send Location Info is set to 'Never'.
- Media:** Allow Empty INVITE, Send Empty re-INVITE, and Allow To Tag Change are unchecked. P-Early-Media Support is set to 'None'. Send SilenceSupp=Off and Force Early Direct Media are unchecked. Media Connection Preservation is set to 'Disabled'. Indicate HOLD is unchecked.
- Call Control:** Call Initiation Timeout (s) is 4. Call Queuing Timeout (m) is 5. Service Busy Response is '486 - Busy Here'. on No User Responding Send is '408-Request Timeout'. Action on CAC Location Limit is 'Allow Voicemail'. Suppress Q.850 Reason is unchecked.

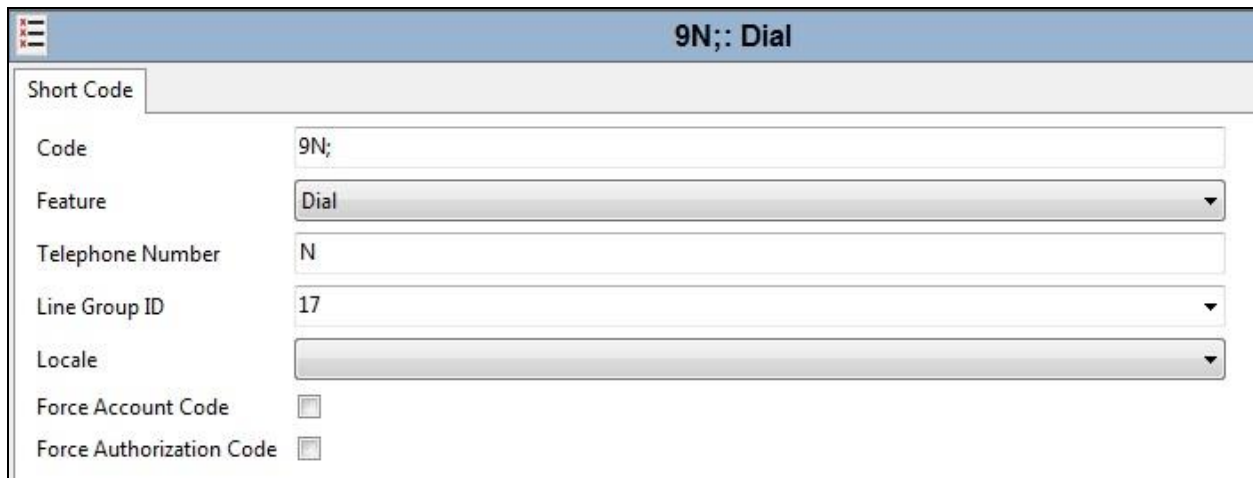
Note: It is advisable at this stage to save the configuration as described in **Section 5.11** to make the Line Group ID defined in **Section 5.6.2** available.

5.7. Short Codes

Define a short code to route outbound traffic to the SIP line. To create a short code, right-click **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as required. The example below shows the configuration used during testing for national numbers.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. The example shows **9N;** which will be invoked when the user dials 9 followed by the dialled number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message.
- Set the **Line Group Id** to the outgoing line group number defined on the SIP URI tab on the SIP Line in **Section 5.6.2**.

On completion, click the **OK** button (not shown).



The screenshot shows a configuration window titled "9N;; Dial". The window has a tab labeled "Short Code". Below the tab, there are several fields and checkboxes:

Field	Value
Code	9N;
Feature	Dial
Telephone Number	N
Line Group ID	17
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

5.8. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.6.2**. To configure these settings, first navigate to **User** in the Navigation Pane. Select the **User** tab if any changes are required.

The following example shows the configuration required for a SIP Endpoint.

- Change the **Name** of the User if required.
- Set the **Password** and **Confirm Password**.
- Select the required profile from the **Profile** drop down menu. **Basic User** is commonly used; **Power User** can be selected for SIP softphone, WebRTC and Remote Worker endpoints.

Extn89110: 89110									
Group Membership	Announcements	SIP	Personal Directory	Web Self-Administration					
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Name	Extn89110								
Password	••••••••								
Confirm Password	••••••••								
Unique Identity									
Audio Conference PIN									
Confirm Audio Conference PIN									
Account Status	Enabled ▼								
Full Name	Extn89110								
Extension	89110								
Email Address									
Locale	▼								
Priority	5 ▼								
System Phone Rights	None ▼								
Profile	Power User ▼								
<input type="checkbox"/> Receptionist									

SIP endpoints require setting of the **SIP Registrar Enable** as described in **Section 5.2**.

Next, select the **SIP** tab in the Details Pane. To reach the **SIP** tab click the right arrow on the right-hand side of the Details Pane until it becomes visible. 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. These 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 5.6.2**). As such, these fields should be set to one of the DDI numbers assigned to the enterprise from Telenor.

The screenshot shows the configuration page for 'Ext89110: 89110*'. The 'SIP' tab is selected. The 'SIP Name' field contains '+47xxxxxx31', the 'SIP Display Name (Alias)' field contains 'Ext89110', and the 'Contact' field contains '+47xxxxxx31'. There is an unchecked checkbox labeled 'Anonymous'.

Note: The **Anonymous** box can be used to restrict Calling Line Identity (CLIR).

The following screen shows the Mobility tab for user 89110. The **Mobility Features** and **Mobile Twinning** are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone over the SIP Trunk. Other options can be set accordingly to customer requirements.

The screenshot shows the configuration page for 'Ext89110: 89110*' with the 'SIP' tab selected. The 'Twinned Handset' dropdown is set to '<None>'. The 'Maximum Number of Calls' is set to '1'. There are three unchecked checkboxes: 'Twin Bridge Appearances', 'Twin Coverage Appearances', and 'Twin Line Appearances'. The 'Mobility Features' section is expanded and contains several checked items: 'Mobile Twinning', 'Twinned Mobile Number (including dial access code)' (0035389xxxxxx1), 'Twining Time Profile' (<None>), 'Mobile Dial Delay (secs)' (3), 'Mobile Answer Guard (secs)' (0), 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', 'Twin When Logged Out', 'one-X Mobile Client', 'Mobile Call Control', and 'Mobile Callback'. There are also unchecked checkboxes for 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', and 'Twin When Logged Out'.

5.9. Incoming Call Routing

An incoming call route maps an inbound DDI number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation 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 5.6.2**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left.
- Default values can be used for all other fields.

The screenshot shows a configuration window titled "17 +47xxxxxx31". It has three tabs: "Standard", "Voice Recording", and "Destinations". The "Standard" tab is active. The fields and their values are:

Field	Value
Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	+47xxxxxx31
Incoming Sub Address	
Incoming CLI	
Locale	
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. On completion, click the **OK** button (not shown). In this example, incoming calls to the test DDI number **+4722xxxxxx31** on line 17 are routed to extension 89110.

The screenshot shows the same configuration window, but with the "Destinations" tab active. It displays a table with two columns: "TimeProfile" and "Destination".

TimeProfile	Destination
Default Value	89110 Extn89110

5.10. G.711 Fax

At Release 11, both G.711 and T.38 Fax is supported on IP Office Server Edition when using an IP Office Expansion (500 V2). The Telenor SIP Trunk testing was carried out using this configuration with only the analogue extension for the fax machine on the Expansion. In this configuration, the G.711 fax settings are configured on the SIP line between the Expansion and the Server.

5.10.1. Analogue User

To configure the settings for the fax User, first navigate to **User** in the Navigation Pane for the Expansion. In the test environment, the 500V2 Expansion is called **GSSCP_IPO**. Select the **User** tab. The following example shows the configuration required for an analog Endpoint.

- Change the **Name** of the User if required.
- The **Password** and **Confirm Password** fields are set but are not required for analog endpoints.
- Select the required profile from the **Profile** drop down menu. **Basic User** is sufficient for fax.

Configuration

- [-] BOOTP (7)
 - [-] Operator (3)
 - [-] Solution
 - [-] User (9)
 - [-] Group (0)
 - [-] Short Code (45)
 - [-] Directory (0)
 - [-] Time Profile (0)
 - [-] Account Code (0)
 - [-] User Rights (9)
 - [-] Location (0)
 - [-] GSSCP_IPO_SE
 - [-] GSSCP_IPO
 - [-] System (1)
 - [-] Line (6)
 - [-] Control Unit (5)
 - [-] Extension (20)
 - [-] User (6)
 - ☒ NoUser
 - ☐ 89101 89101
 - ☐ 89102 89102
 - ☐ 89103 89103
 - ☒ 89119 Analog89119
 - ☐ 89104 ChrisMc
 - [-] Group (0)
 - [-] Short Code (57)
 - [-] Service (0)
 - [-] RAS (1)
 - [-] Incoming Call Route (0)
 - [-] WanPort (0)
 - [-] Time Profile (0)

Analog89119 : 89119

Group Membership
Announcements
SIP
Personal Directory
Web Self-Administration

User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Name	Analog89119								
Password	••••••••								
Confirm Password	••••••••								
Unique Identity									
Audio Conference PIN									
Confirm Audio Conference PIN									
Account Status	Enabled								
Full Name									
Extension	89119								
Email Address									
Locale									
Priority	5								
System Phone Rights	None								
Profile	Basic User								
<input type="checkbox"/> Receptionist <input type="checkbox"/> Enable Softphone									

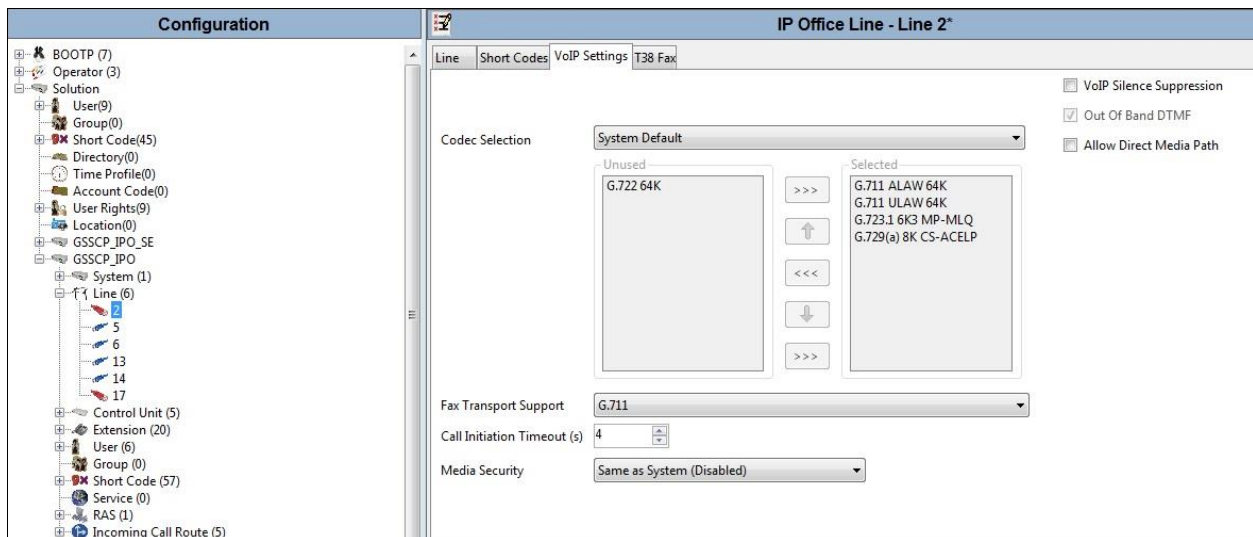
Configure other settings as described in **Section 5.7**.

5.10.2. G.711 Fax Settings

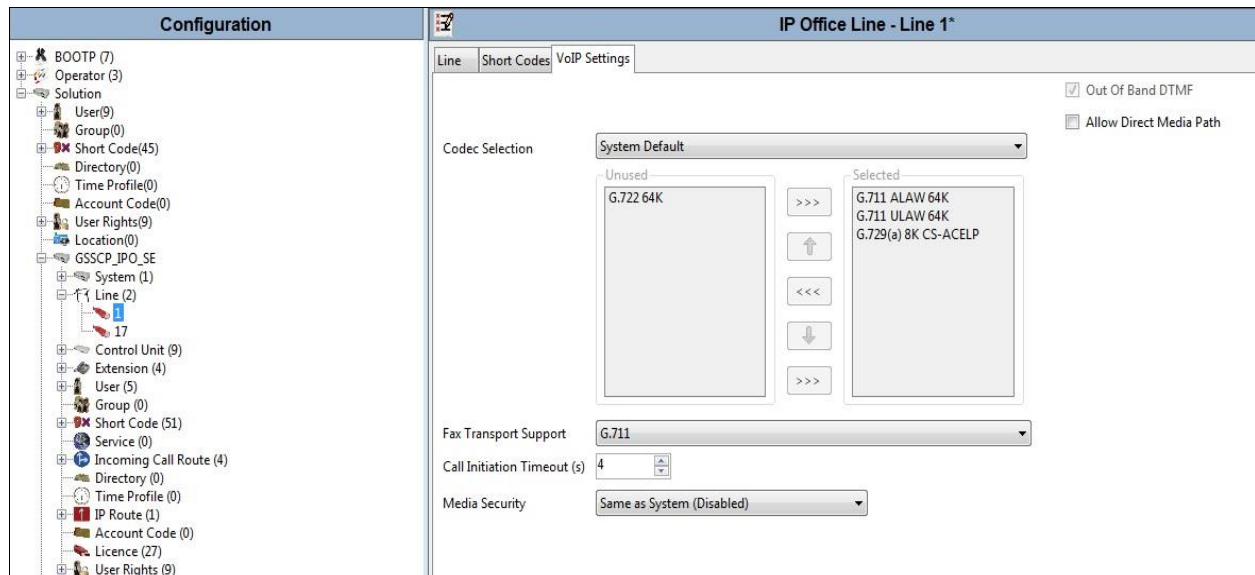
The G.711 Fax settings are defined on the SIP Line between the Expansion and the Server. Note that the VoIP settings for G.711 Fax are required in three places in this configuration:

- The SIP Line for the Telenor SIP Trunk as described in **Section 5.6.2**.
- The IP Office Line between the Server and the Expansion on the Expansion.
- The IP Office Line between the Server and the Expansion on the Server.

In all the above cases, the **Fax Transport Support** was set to **G.711**. The following screenshot shows the VoIP Settings for the IP Office Line between the Server and the Expansion on the Expansion:



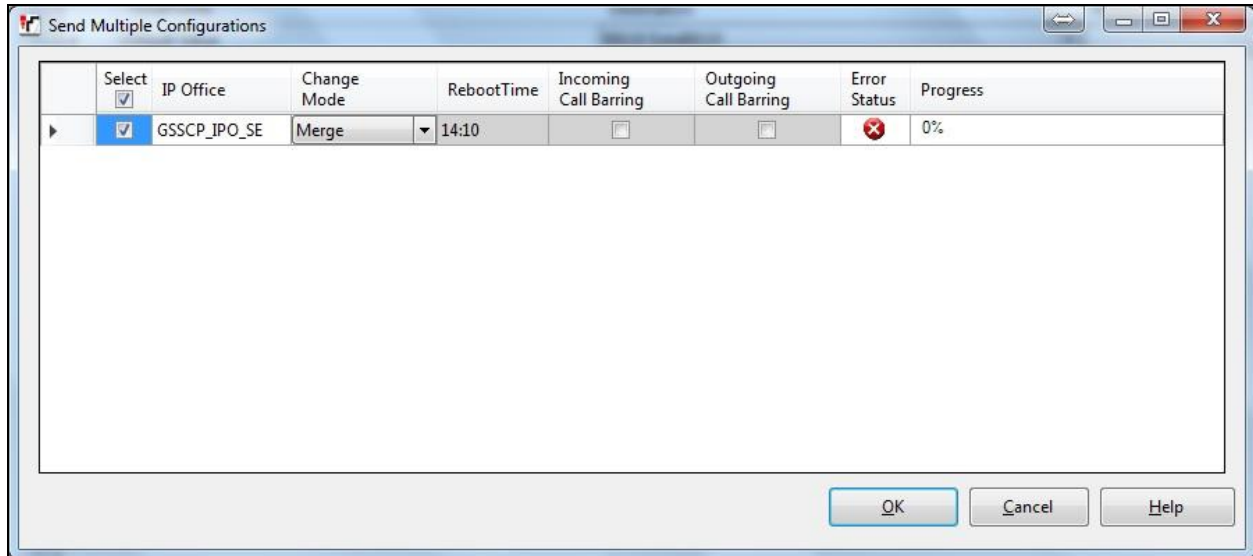
The following shows the **VoIP Settings** tab in the IP Office Line for the Expansion in the Server configuration:



Refer to **Section 5.6.2** for the VoIP Settings on the SIP Line for the Telenor SIP Trunk.

5.11. 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. A screen like the one shown below is displayed where the system configuration has been changed and needs to be saved on the system. **Merge, Reboot, Timed** or **RebootWhen Free** can be selected from the **Change Mode** drop-down menu based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to save the configuration.



5.12. TLS Certificates

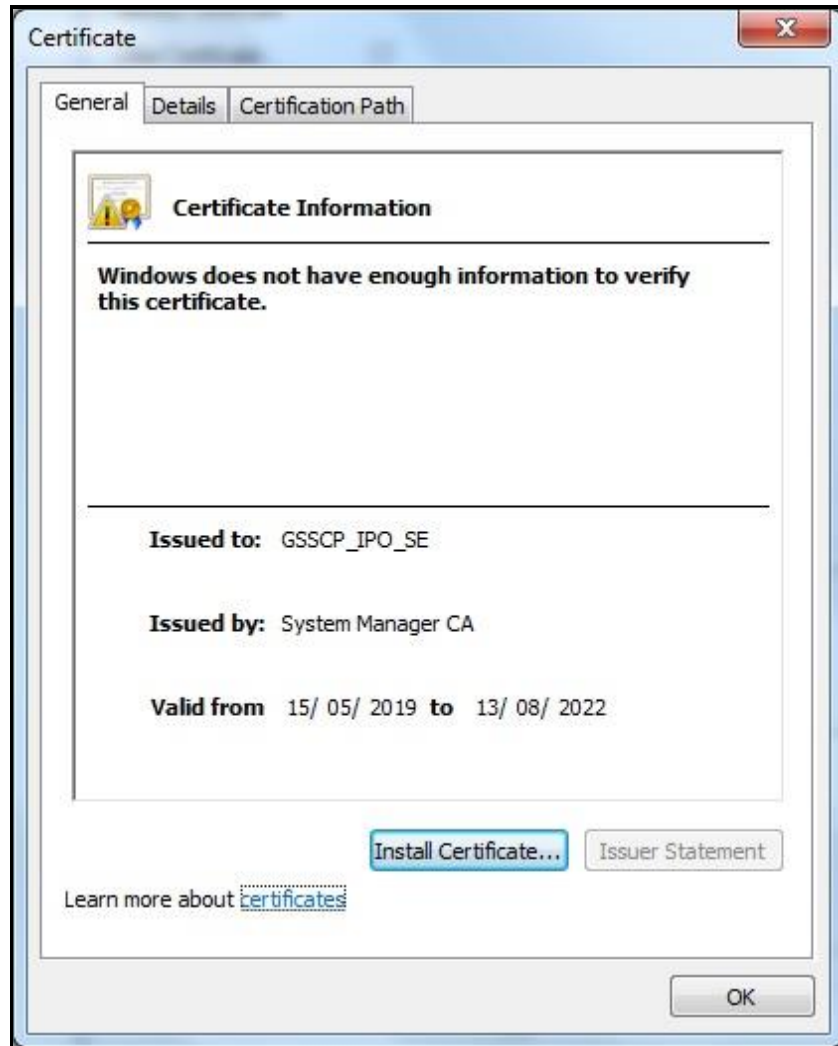
For the compliance test, TLS signalling was used internally to the enterprise wherever possible. Testing was done using identity certificates signed by a local certificate authority **System Manager CA**. The generation and installation of these certificates are beyond the scope of these Application Notes.

To view the certificate currently installed on IP Office, navigate to **File → Advanced → Security Settings**. In the Security Settings window, navigate to **Security → System** and select the **Certificates** tab.

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



A pop-up window displays the certificate that is issued to the Avaya IP Office (GSSCP_IPO_SE) and issued by **System Manager CA**. Click **OK** to close the pop-up window.



To verify the trusted certificates, return to the **Security → System → Certificates** tab and scroll down to the **Trusted Certificate Store** section. Verify that **System Manager CA** is displayed as an **Installed Certificate**.

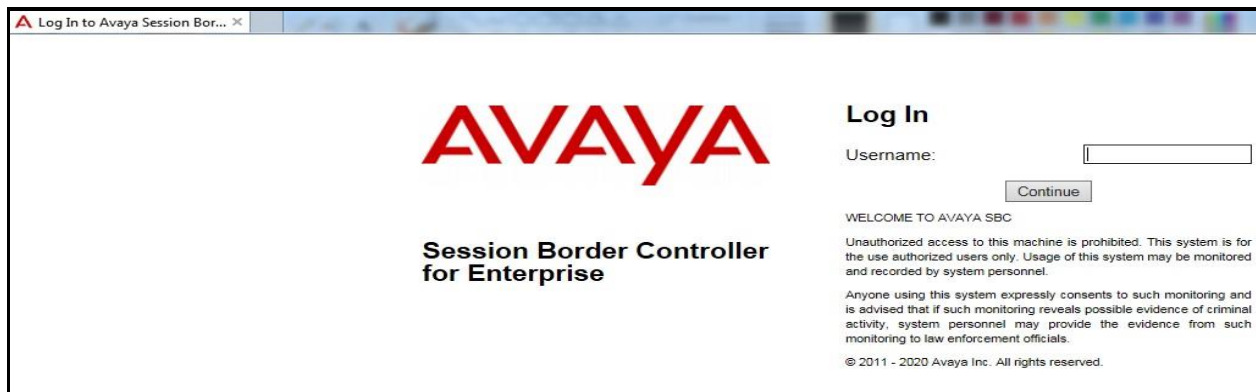


6. Configure Avaya Session Border Controller for Enterprise

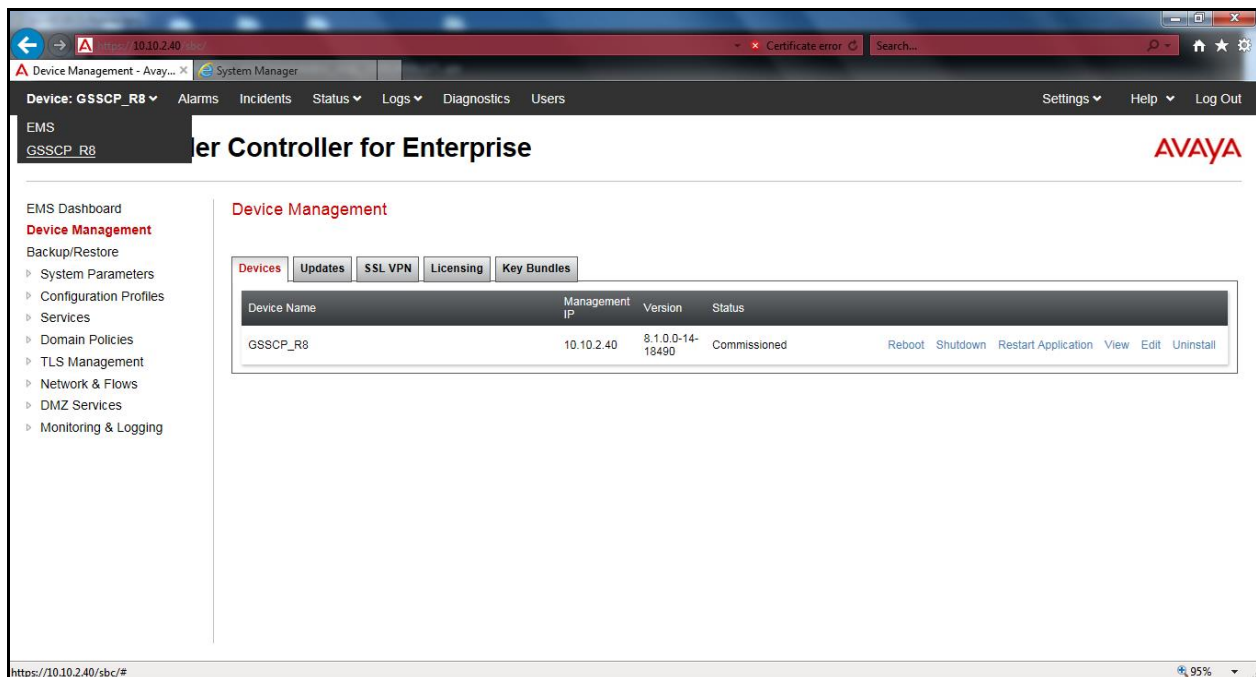
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

6.1. Access Avaya Session Border Controller for Enterprise

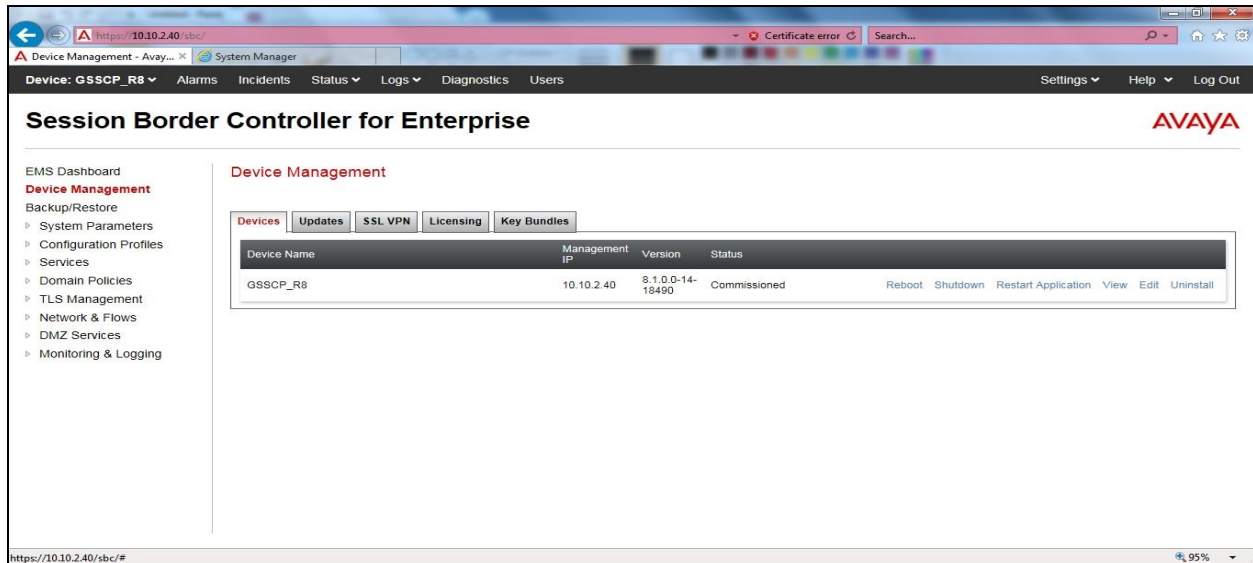
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



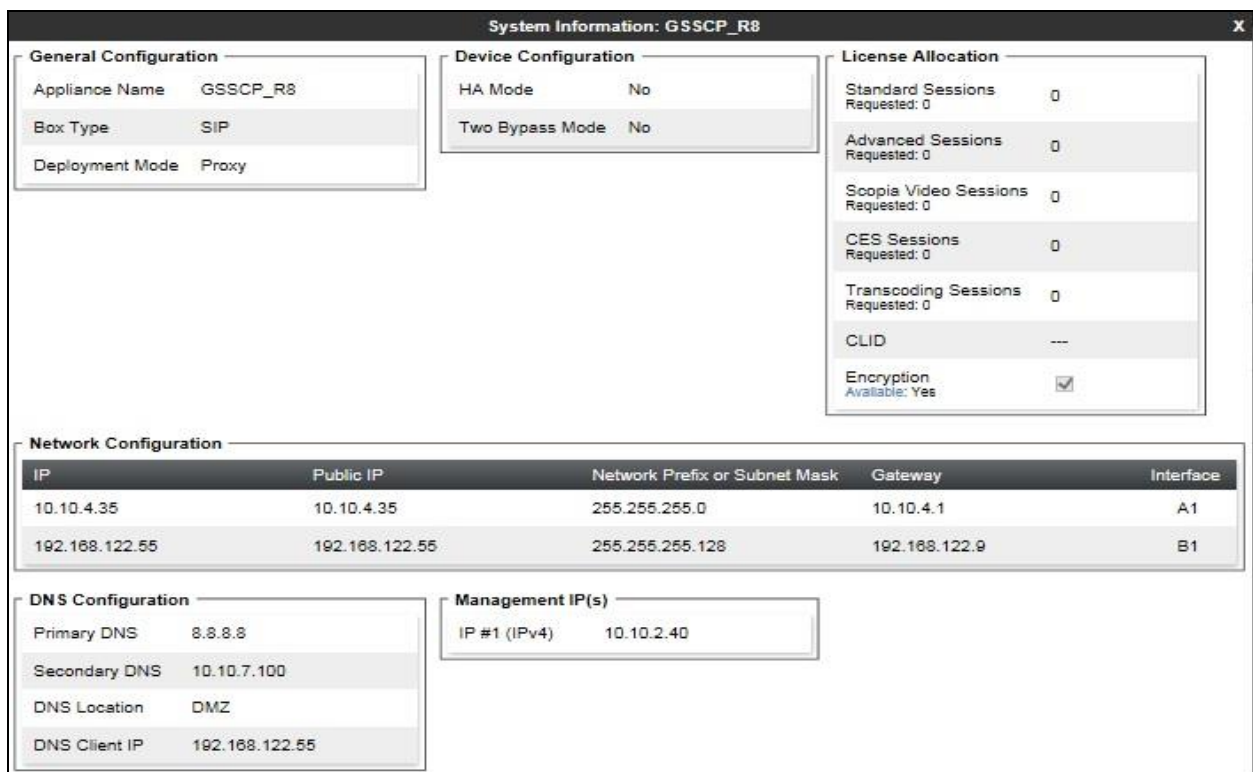
Once logged in, on the top-left of the screen, under **Device:** select the required device from the drop-down menu. with a menu on the left-hand side. In this case, **GSSCP_R8** is used as a starting point for all configuration of the Avaya SBCE.



To view system information that was configured during installation, navigate to **Device Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_R8** is shown. To view the configuration of this device, click **View** (the third option from the right).



The **System Information** screen shows the **General Configuration**, **Device Configuration**, **License Allocation**, **Network Configuration**, **DNS Configuration** and **Management IP** information.



6.2. Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one physical interface assigned.

To define the network information, navigate to **Network & Flows → Network Management** in the main menu on the left-hand side and click on **Add**. Enter details for the external interfaces in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Network Prefix or Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The screenshot shows a 'Network' dialog box with a warning banner at the top: 'Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped.' Below the banner are four input fields: 'Name' (B1_External), 'Default Gateway' (192.168.122.9), 'Network Prefix or Subnet Mask' (255.255.255.128), and 'Interface' (B1). An 'Add' button is to the right of the 'Interface' field. Below these fields is a table with three columns: 'IP Address', 'Public IP', and 'Gateway Override'. The first row contains the values '192.168.122.55', 'Use IP Address', and 'Use Default'. A 'Delete' button is to the right of the first row. At the bottom of the dialog is a 'Finish' button.

IP Address	Public IP	Gateway Override
192.168.122.55	Use IP Address	Use Default

Click on **Add** to define the internal interfaces or Edit if it was defined during installation of the Avaya SBCE. Enter details in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Network Prefix or Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

Network

Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped.

Name: A1_Internal

Default Gateway: 10.10.4.1

Network Prefix or Subnet Mask: 255.255.255.0

Interface: A1

Add

IP Address	Public IP	Gateway Override
10.10.4.35	Use IP Address	Use Default

Delete

Finish

The following screenshot shows the completed Network Management configuration:

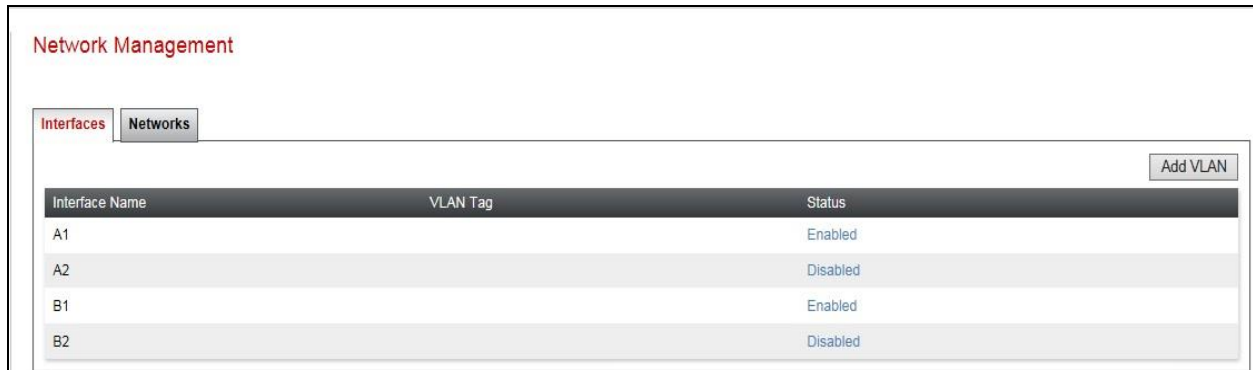
Network Management

Interfaces Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
A1_Internal	10.10.4.1	255.255.255.0	A1	10.10.4.35	Edit	Delete
B1_External	192.168.122.9	255.255.255.128	B1	192.168.122.55	Edit	Delete

Select the **Interfaces** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.



Network Management

Interfaces Networks

Add VLAN

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

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **Device Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear that will indicate when the restart is complete.

6.3. Define TLS Profiles

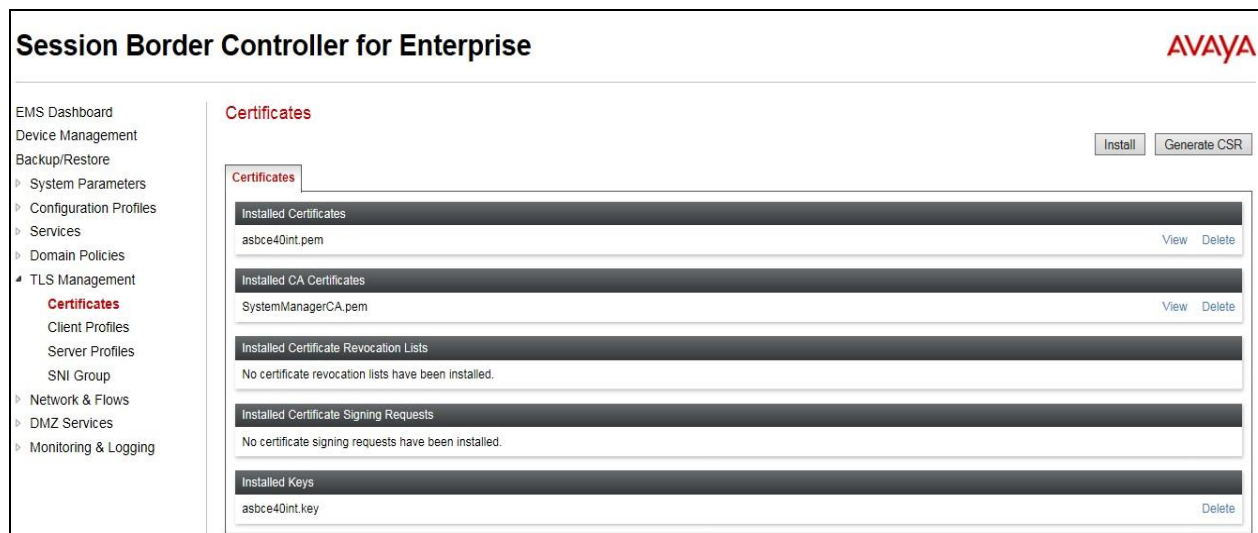
For the compliance test, TLS transport is used for signalling on the SIP trunk between IP Office and the Avaya SBCE. Compliance testing was done using identity certificates signed by a local certificate authority. The generation and installation of these certificates are beyond the scope of these Application Notes.

The following procedures show how to view the certificates and configure the Client and Server profiles to support the TLS connection.

6.3.1. Certificates

To view the certificates currently installed on the Avaya SBCE, navigate to **TLS Management** → **Certificates**:

- Verify that an Avaya SBCE identity certificate (**asbce40int.pem**) is present under **Installed Certificates**.
- Verify that certificate authority root certificate (**SystemManagerCA.pem**) is present under **Installed CA certificates**.
- Verify that private key associated with the identity certificate (**asbce40int.key**) is present under **Installed Keys**.



6.3.2. Client Profile

To create a new client profile, navigate to **TLS Management** → **Client Profile** in the left pane and click **Add** (not shown).

- Set **Profile Name** to a descriptive name. **GSSCP_Client** was used in the compliance testing.
- Set **Certificate** to the identity certificate **asbce40int.pem** used in the compliance testing.
- **Peer Verification** is automatically set to **Required**.
- Set **Peer Certificate Authorities** to the **SystemManagerCA.pem** identity certificate.
- Set **Verification Depth** to **1**.

Click **Next** to accept default values for the next screen and click **Finish** (not shown).

Client Profiles: GSSCP_Client

[Add](#) [Delete](#)

Client Profiles

- GSSCP_Client**

Client Profile

Click here to add a description.

TLS Profile

Profile Name	GSSCP_Client
Certificate	asbce40int.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	<input checked="" type="checkbox"/> TLS 1.2 <input checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

[Edit](#)

6.3.3. Server Profile

To create a new server profile, navigate to **TLS Management** → **Server Profile** in the left pane and click **Add** (not shown).

- Set **Profile Name** to a descriptive name. **GSSCP_Server** was used in the compliance testing
- Set **Certificate** to the identity certificate **asbce40int.pem** used in the compliance testing.
- Set **Peer Verification** to **Optional**.

Click **Next** to accept default values for the next screen and click **Finish** (not shown).

The screenshot shows a web-based configuration interface for a server profile named "GSSCP_Server". The interface is divided into a left sidebar and a main content area. The sidebar contains a "Server Profiles" section with a list of profiles, including "GSSCP_Server", and buttons for "Add" and "Delete". The main content area is titled "Server Profiles: GSSCP_Server" and contains a "Server Profile" tab. The "Server Profile" tab is expanded, showing the following configuration details:

TLS Profile	
Profile Name	GSSCP_Server
Certificate	asbce40int.pem
SNI Options	None

Certificate Verification	
Peer Verification	Optional
Peer Certificate Authorities	---
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:IMD5:1aNULL:1eNULL:@STRENGTH

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

6.4. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

6.4.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Network & Flows** → **Signaling Interface** from the menu on the left-hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

To enter details of transport protocol and ports for the SIP signalling on the internal interface:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **Signaling IP**, select the **A1_Internal** signalling interface IP addresses defined in **Section 6.2**.
- Select **TLS** port number, **5061** is used for IP Office.
- Select a **TLS Profile** defined in **Section 6.3.3** from the drop-down menu.
- Click **Finish**.

To enter details of transport protocol and ports for the SIP signalling on the external interface:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **Signaling IP**, select the **B1_external** signalling interface IP address defined in **Section 6.2**.
- Select **UDP** port number, **5060** is used for the Telenor SIP Trunk.
- Click **Finish**.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Int	10.10.4.35 A1_Internal (A1, VLAN 0)	5060	---	5061	GSSCP_Server	Edit Delete
Sig_Ext	192.168.122.55 B1_External (B1, VLAN 0)	---	5060	---	None	Edit Delete

6.4.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Network & Flows → Media Interface** from the menu on the left-hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

To enter details of the media IP and RTP port range for the internal interface to be used in the server flow:

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **A1_Internal** media interface IP address defined in **Section 6.2**.
- For **Port Range**, enter **35000-40000**.
- Click **Finish**.

To enter details of the media IP and RTP port range on the external interface to be used in the server flow:

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select the **B1_External** media interface IP address defined in **Section 6.2**.
- Select **Port Range**, enter **10000-10999** as specified by Telenor.
- Click **Finish**.

Name	Media IP Network	Port Range	
Media_Int	10.10.4.35 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
Media_Ext	192.168.122.55 B1_External (B1, VLAN 0)	10000 - 10999	Edit Delete

6.5. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, Telenor is connected as the Trunk Server and the IP Office is connected as the Call Server.

6.5.1. Server Interworking Avaya

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Configuration Profiles**

→ **Server Interworking** and click on **Add**.

- Enter profile name such as Avaya and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- All other options on the **General** Tab can be left at default.

Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▼
Send Hold	<input type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = Avaya**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.
- Click **Finish**.

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides <input type="radio"/> Dialog-Initiate Only (Single Side) <input type="radio"/> Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	<input checked="" type="checkbox"/>
Extensions	Avaya ▼
Diversion Manipulation	<input type="checkbox"/>
Diversion Condition	None ▼
Diversion Header URI	<input type="text"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Relay INVITE Replace for SIPREC	<input type="checkbox"/>
MOBX Re-INVITE Handling	<input type="checkbox"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP Notify <input type="radio"/> RFC 2833 Relay & SIP Notify <input type="radio"/> SIP Info <input type="radio"/> RFC 2833 Relay & SIP Info <input type="radio"/> Inband
<input type="button" value="Finish"/>	

6.5.2. Server Interworking – Telenor

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Configuration Profiles**

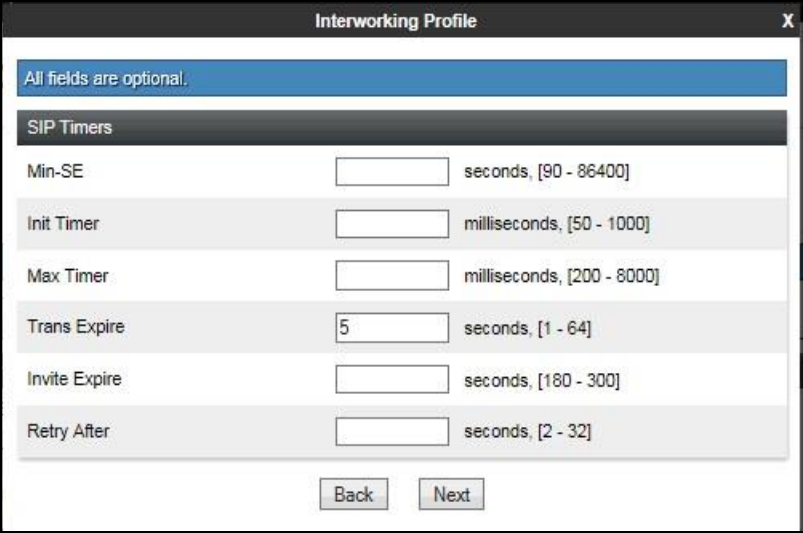
→ **Server Interworking** and click on **Add**.

- Enter profile name such as Telenor and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- All other options on the **General** Tab can be left at default.

Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▼
Send Hold	<input type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

On the **Timers** Tab:

- For Trans Expire, enter **5** as discussed in **Section 2.2**.
- Click **Next**.



The screenshot shows a window titled "Interworking Profile" with a close button (X) in the top right corner. Below the title bar is a blue banner that reads "All fields are optional." Below this is a section titled "SIP Timers" with a dark header. The section contains six rows, each with a label, a text input field, and a unit/range. The "Trans Expire" row has the value "5" entered in the input field. At the bottom of the form are two buttons: "Back" and "Next".

SIP Timers		
Min-SE	<input type="text"/>	seconds, [90 - 86400]
Init Timer	<input type="text"/>	milliseconds, [50 - 1000]
Max Timer	<input type="text"/>	milliseconds, [200 - 8000]
Trans Expire	<input type="text" value="5"/>	seconds, [1 - 64]
Invite Expire	<input type="text"/>	seconds, [180 - 300]
Retry After	<input type="text"/>	seconds, [2 - 32]

Back Next

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.
- Click **Finish**.

Record Routes

☐ None
☐ Single Side
☒ Both Sides
☐ Dialog-Initiate Only (Single Side)
☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup ☒

Extensions None ▾

Diversion Manipulation ☐

Diversion Condition None ▾

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

Relay INVITE Replace for SIPREC ☐

DTMF

DTMF Support

☒ None
☐ SIP Notify
☐ SIP Info
☐ Inband

Finish

6.6. Define Servers

Servers are defined for each server connected to the Avaya SBCE. In this case, Telenor is connected as the Trunk Server and IP Office is connected as the Call Server.

6.6.1. Server Configuration – Avaya

From the left-hand menu select **Services** → **SIP Servers** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profiles** tab, set the following:

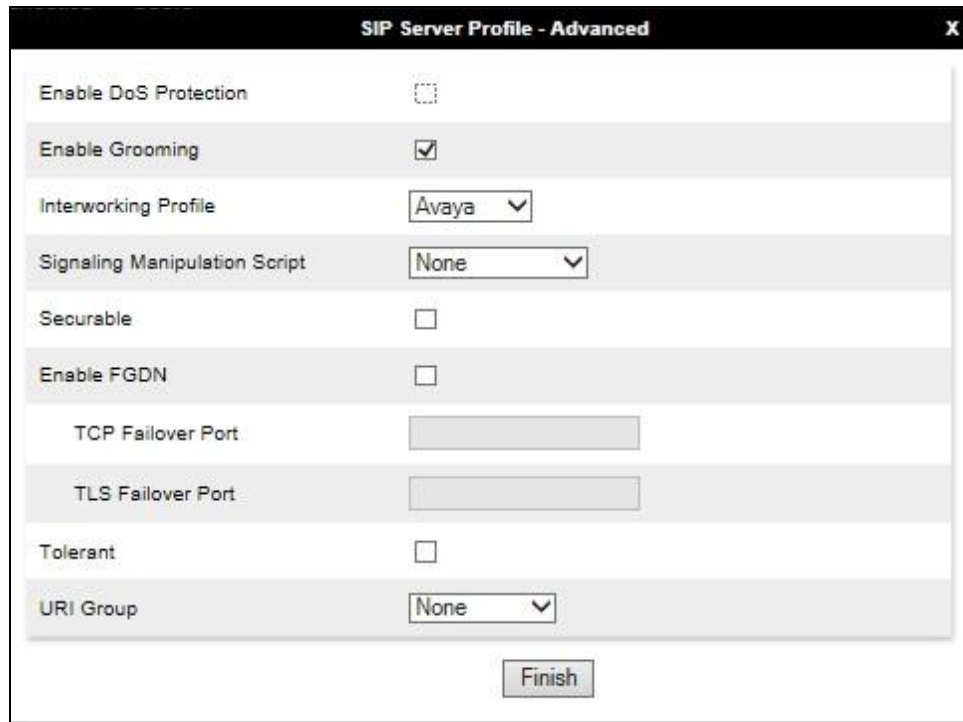
- Select **Server Type** to be **Call Server**.
- Select **TLS Client Profile** to be **GSSCP_Client** as defined in **Section 6.3.2**.
- Enter **IP Address / FQDN** to **10.10.4.130** (IP Office IP Address).
- For **Port**, enter **5061**.
- For **Transport**, select **TLS**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

The screenshot shows the 'SIP Server Profile - General' configuration window. At the top, a blue banner states: 'Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.' Below this, the 'Server Type' is set to 'Call Server' in a dropdown menu. The 'SIP Domain' field is empty. The 'DNS Query Type' is set to 'NONE/A' in a dropdown menu. The 'TLS Client Profile' is set to 'GSSCP_Client' in a dropdown menu. An 'Add' button is located to the right of these fields. Below the main configuration area is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The first row contains the values '10.10.4.130', '5061', and 'TLS' (selected in a dropdown). A 'Delete' button is located to the right of the table.

IP Address / FQDN	Port	Transport
10.10.4.130	5061	TLS

On the **Advanced** tab:

- Check **Enable Grooming**.
- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.



The screenshot shows a configuration window titled "SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several settings:

Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None

At the bottom right of the window is a "Finish" button.

6.6.2. Server Configuration – Telenor

To define the Telenor Trunk Server, navigate to **Services → SIP Servers** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **192.168.97.216** (Telenor SIP Platform).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click **Add** and repeat the steps for IP addresses **192.168.97.200** and **192.168.97.232**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

SIP Server Profile - General

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

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport	
192.168.97.216	5060	UDP	Delete
192.168.97.200	5060	UDP	Delete
192.168.97.232	5060	UDP	Delete

On the Advanced tab:

- Select **Telenor** for **Interworking Profile**.
- Click **Finish**.

The screenshot shows a configuration window titled "SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several settings:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Telenor ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼

At the bottom right of the window is a button labeled "Finish".

6.7. Routing


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.

Routing information is required for routing to IP Office on the internal side and Telenor address on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

6.7.1. Routing – Avaya

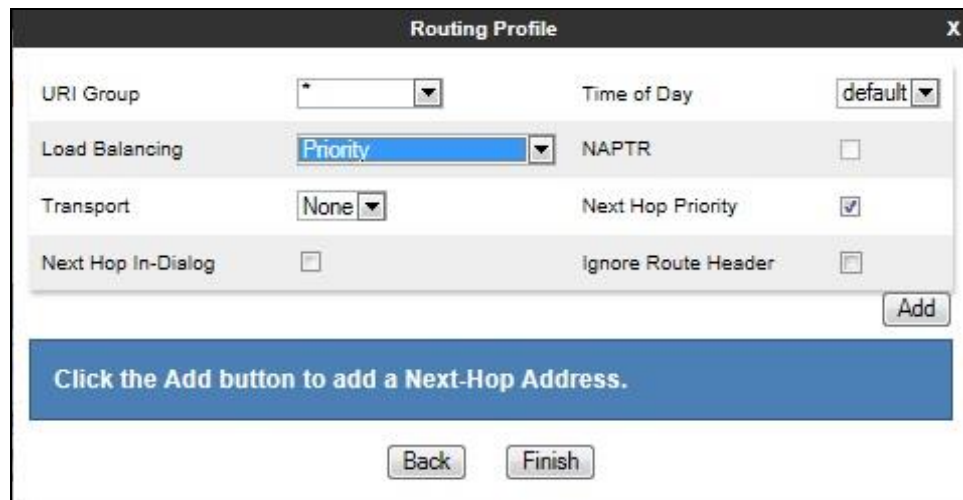
Create a Routing Profile for IP Office.

- Navigate to **Configuration Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.



The image shows a 'Routing Profile' window. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text input field labeled 'Profile Name' containing the text 'Avaya'. Below the input field is a 'Next' button.

The Routing Profile window will open. Use the default values displayed and click **Add**.



The image shows a 'Routing Profile' window with various configuration options. The title bar has 'Routing Profile' and a close button 'X'. The options are arranged in a grid-like fashion:

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>

Below the grid is an 'Add' button. At the bottom, there is a blue banner with the text 'Click the Add button to add a Next-Hop Address.' and two buttons: 'Back' and 'Finish'.

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **SIP Server Profile = Avaya (Section 6.6.1)** from drop down menu.
- **Next Hop Address = Select 10.10.4.130:5061(TLS)** from drop down menu.
- Click **Finish**.

Profile : Avaya

URI Group: *
Time of Day: default
Load Balancing: Priority
NAPTR: ☐
Transport: None
LDAP Routing: ☐
LDAP Server Profile: None
LDAP Base DN (Search): None
Matched Attribute Priority: ☐
Alternate Routing: ☐
Next Hop Priority: ☒
Next Hop In-Dialog: ☐
Ignore Route Header: ☐
ENUM: ☐
ENUM Suffix:
Add
Priority / Weight: 1
LDAP Search Attribute:
LDAP Search Regex Pattern:
LDAP Search Regex Result:
SIP Server Profile: Avaya
Next Hop Address: 10.10.4.130:5061 (TLS)
Transport: None
Delete
Finish

6.7.2. Routing – Telenor

Create a Routing Profile for Telenor SIP network.

- Navigate to **Configuration Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

Routing Profile

Profile Name: Telenor
Next

The Routing Profile window will open. Use the default values displayed and click **Add**.

Routing Profile

URI Group: * Time of Day: default

Load Balancing: Priority NAPTR: ☐

Transport: None Next Hop Priority: ☒

Next Hop In-Dialog: ☐ Ignore Route Header: ☐

Add

Click the Add button to add a Next-Hop Address.

Back Finish

On the **Next Hop Address** window, set the following:

- **Load Balancing = Round Robin.**
- **SIP Server Profile = Telenor (Section 6.6.2)** from drop down menu.
- **Next Hop Address = Select 192.168.96.216 (UDP)** from drop down menu.
- Click **Add** and repeat the steps for IP addresses **192.168.97.200** and **192.168.97.232**.
- Click **Finish**.

Profile - Telenor

URI Group: * Time of Day: default

Load Balancing: Round-Robin NAPTR: ☐

Transport: None LDAP Server Profile: None

LDAP Base DN (Search): None

Matched Attribute Priority: ☐ Alternate Routing: ☐

Next Hop Priority: ☐ Next Hop In-Dialog: ☐

Ignore Route Header: ☐

ENUM: ☐ ENUM Suffix:

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
0				Telenor	192.168.97.216:5060 (UDP)	None	Delete
0				Telenor	192.168.97.200:5060 (UDP)	None	Delete
0				Telenor	192.168.97.232:5060 (UDP)	None	Delete

Finish

6.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for IP Office, navigate to **Configuration Profiles → Topology Hiding** from menu on the left-hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Avaya

Add

Topology Hiding Profiles

default

cisco_th_profile

Avaya

Telenor

RenameCloneDelete

Click here to add a description.

Topology Hiding

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

Edit

To define Topology Hiding for Telenor, navigate to **Configuration Profiles → Topology Hiding** from the menu on the left-hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for Telenor and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Auto** under **Replace Action**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Telenor

Buttons: Add, Rename, Clone, Delete

Topology Hiding Profiles: default, cisco_th_profile, Avaya, **Telenor**

Click here to add a description.

Topology Hiding

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

Edit

6.9. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

In the reference configuration, only new Media Rules were defined. All other rules under Domain Policies, linked together on End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one of the defaults and then make the necessary changes to the new rule.

6.9.1. Media Rules

A media rule defines the processing to be applied to the selected media. For the compliance test, a media rule was created for Avaya IP Office to use SRTP, while the predefined **default-low-med** media rule was used for the Telenor SIP trunk.

To define the Media Rule for IP Office, navigate to **Domain Policies → Media Rules** in the main menu on the left-hand side. Click on **Add** and enter details in the Media Rule pop-up box (not shown)

- In the **Rule Name** field enter a descriptive name such as **Avaya_SRTP**.
- Set **Preferred Format #1** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Set **Preferred Format #3** to **RTP**.
- Uncheck **Encrypted RTCP**.
- Check **Capability Negotiation** under **Miscellaneous** (not shown).

Default values were used for all other fields. Click **Finish** (not shown).

The screenshot shows the 'Media Rules: Avaya_SRTP' configuration window. On the left is a sidebar with a 'Media Rules' section containing a list of rules: 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', and 'Avaya_SRTP' (which is highlighted in red). Above this list is an 'Add' button. The main area of the window has a title bar with 'Rename', 'Clone', and 'Delete' buttons. Below the title bar is a blue bar with the text 'Click here to add a description.' Underneath this are four tabs: 'Encryption' (selected), 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active and shows two sections: 'Audio Encryption' and 'Video Encryption'. The 'Audio Encryption' section has a table with the following rows: 'Preferred Formats' (SRTP_AES_CM_128_HMAC_SHA1_80, RTP), 'SRTP Context Reset on SSRC Change' (checkbox), 'Encrypted RTCP' (checkbox), 'MKI' (checkbox), 'Lifetime' (Any), and 'Interworking' (checkbox). The 'Video Encryption' section has a table with the following rows: 'Preferred Formats' (RTP) and 'Interworking' (checkbox).

For the compliance test, the default media rule **default-low-med** was used for Telenor.

The screenshot shows the 'Media Rules: default-low-med' configuration window. On the left is a sidebar with a list of media rules: 'default-low-med' (highlighted), 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', and 'Avaya_SRTP'. The main area has tabs for 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing 'Audio Encryption' and 'Video Encryption' sections. Both sections have 'Preferred Formats' set to 'RTP' and 'Interworking' checked. A 'Miscellaneous' section at the bottom has 'Capability Negotiation' unchecked. An 'Edit' button is at the bottom right. A warning banner at the top states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.'

6.10. End Point Policy Groups

An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the Telenor SIP trunk. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 6.11**.

6.10.1. End Point Policy Group – Avaya IP Office

To define an End Point policy for IP Office, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left-hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name, in this case **Avaya**, and click **Next** (not shown).
- Leave the **Application Rule**, **Border Rule**, **Security Rule** and **Signalling Rule** fields at their default values.
- In the **Media Rule** drop down menu, select the recently added Media Rule called **Avaya_SRTP**.
- Click **Finish**.

The screenshot shows the 'Policy Set' configuration window. It contains five rows, each with a label and a dropdown menu: 'Application Rule' (default), 'Border Rule' (default), 'Media Rule' (Avaya_SRTP), 'Security Rule' (default-low), and 'Signaling Rule' (default). A 'Finish' button is located at the bottom center.

6.10.2. End Point Policy Group – Telenor

For the compliance test, the predefined End Point Policy **default-low** was used for the Telenor End Point Policy Group.

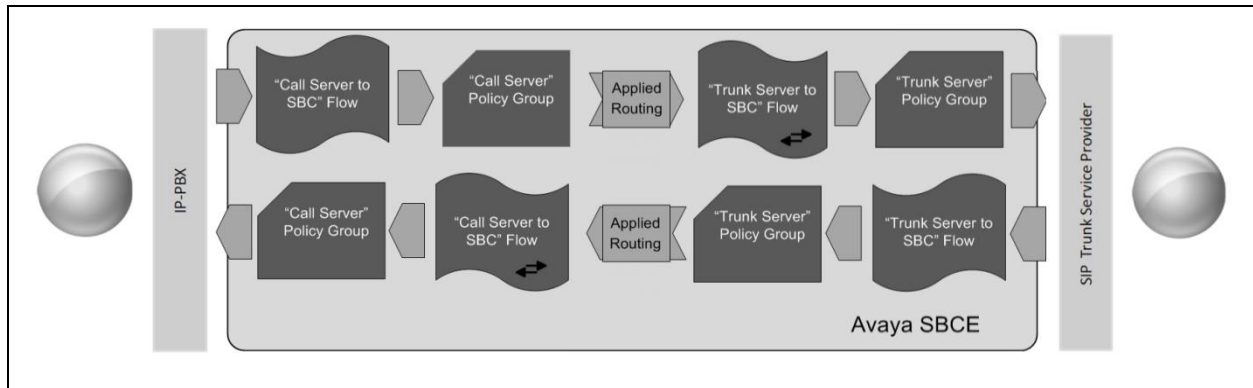
The screenshot shows a 'Policy Set' configuration window with a black title bar and a close button (X) in the top right corner. The window contains a list of five rules, each with a corresponding dropdown menu. The 'Security Rule' dropdown is currently set to 'default-low'. Below the list is a 'Finish' button.

Rule Type	Selected Policy
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default

Finish

6.11. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from IP Office to Telenor's SIP Trunk and incoming flows from Telenor's SIP Trunk to IP Office. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



This configuration ties all the previously entered information together so that calls can be routed from IP Office to Telenor SIP Trunk and vice versa. The following screenshot shows all configured flows.

End Point Flows

Subscriber Flows **Server Flows** Add

Modifications made to a Server Flow will only take effect on new sessions.

Click here to add a row description.

SIP Server: Avaya						
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	Call_Server	*	Sig_Ext	Sig_Int	Avaya	Telenor View Clone Edit Delete

SIP Server: Telenor						
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	Trunk_Server	*	Sig_Int	Sig_Ext	default-low	Avaya View Clone Edit Delete

To define a Server Flow for the Telenor SIP Trunk, navigate to **Network & Flows → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Telenor SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Telenor server configuration defined in **Section 6.6.2**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 6.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 6.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **default-low**.
- In the **Routing Profile** drop-down menu, select the routing profile of the IP Office defined in **Section 6.7.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Telenor SIP Trunk defined in **Section 6.8** and click **Finish** (not shown).

Flow: Trunk_Server

Criteria	
Flow Name	Trunk_Server
Server Configuration	Telenor
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Int

Profile	
Signaling Interface	Sig_Ext
Media Interface	Media_Ext
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	Telenor
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

To define an incoming server flow for IP Office from the Telenor network, navigate to **Network & Flows → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for IP Office, in the test environment **Call_Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for IP Office defined in **Section 6.6.1**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 6.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 6.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **Avaya**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Telenor SIP Trunk defined in **Section 6.7.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of IP Office defined in **Section 6.8** and click **Finish** (not shown).

Flow: Call_Server X

Criteria		Profile	
Flow Name	Call_Server	Signaling Interface	Sig_Int
Server Configuration	Avaya	Media Interface	Media_Int
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	Avaya
Remote Subnet	*	Routing Profile	Telenor
Received Interface	Sig_Ext	Topology Hiding Profile	Avaya
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	<input type="checkbox"/>

7. Telenor IPT Multi-User SIP Trunk Configuration

The configuration of the Telenor equipment used to support Telenor's SIP platform is outside of the scope of these Application Notes and will not be covered. To obtain further information on Telenor equipment and system configuration please contact an authorized Telenor representative.

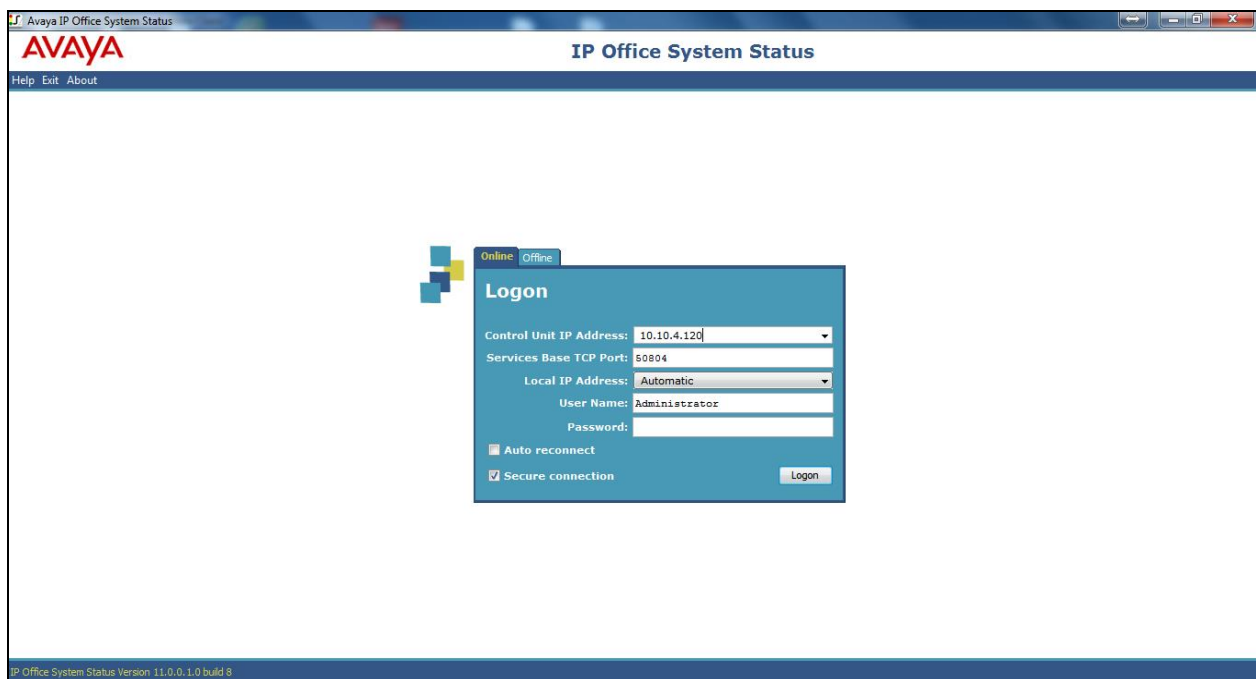
8. Verification Steps

This section includes steps that can be used to verify that the configuration has been done correctly.

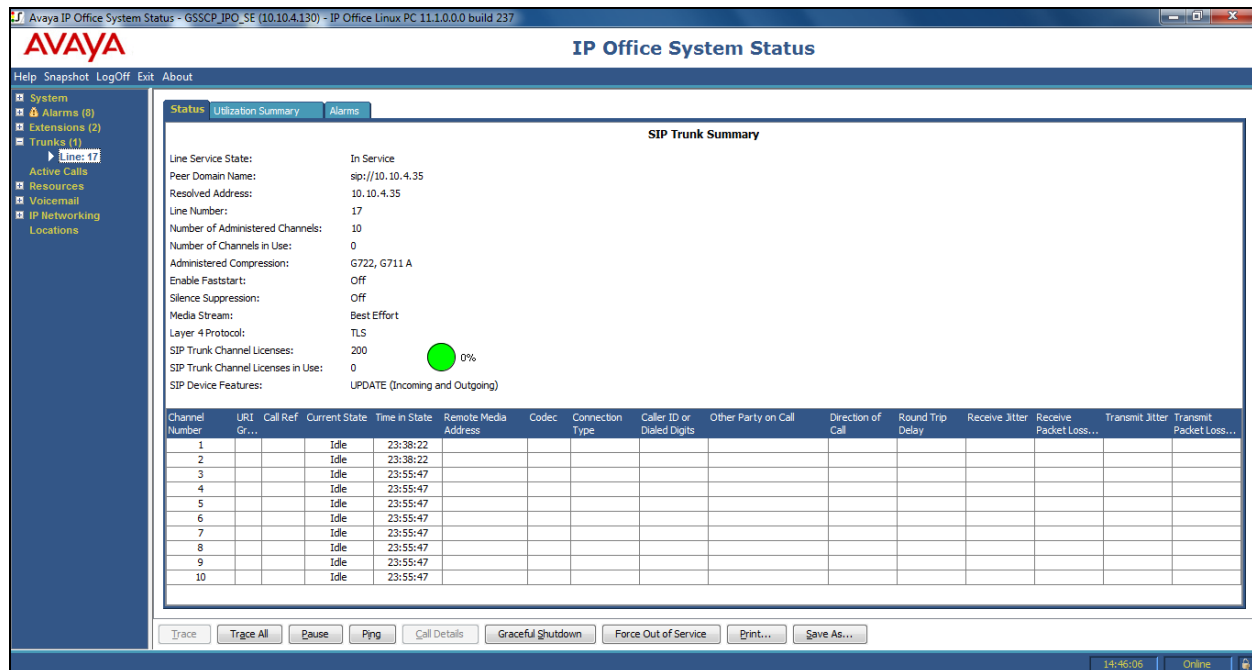
8.1. SIP Trunk status

The status of the SIP trunk can be verified by opening the System Status application. This is found on the PC where IP Office Manager is installed in PC programs under **Start → All Programs → IP Office → System Status** (not shown).

Log in to IP Office System Status at the prompt using the **Control Unit IP Address** for the IP Office. The **User Name** and **Password** are the same as those used for IP Office Manager.

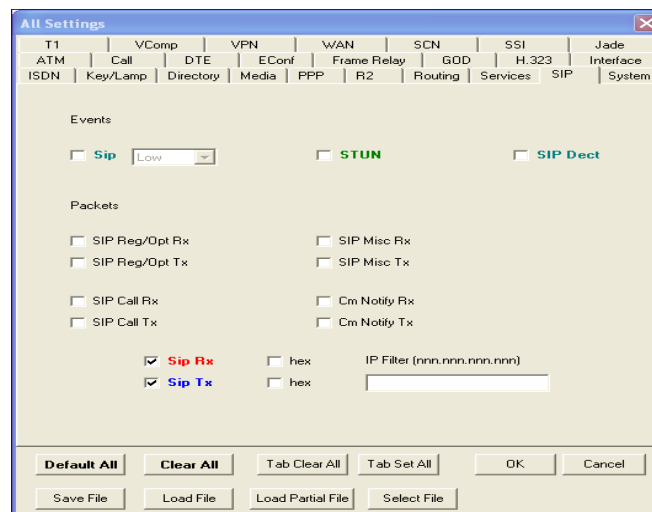


From the left-hand menu expand **Trunks** and choose the SIP trunk (**17** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational.



8.2. Monitor

The Monitor application can also be used to monitor and troubleshoot IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select the button that is third from the right in the screen below, or select **Filters → Trace Options**. The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, the **SIP Rx** and **SIP Tx** boxes are checked. All SIP messages will appear in the trace with the color blue. To customize the color, right-click on **SIP Rx** or **SIP Tx** and select the desired color.



As an example, the following shows a portion of the monitoring window of OPTIONS being sent between IP Office and the Service Provider.



```
Avaya IP Office SysMonitor - [STOPPED] Monitoring 10.10.4.120 (GSSCP_IPO_10 (Server Edition(P))) Log Settings - C:\Users\...\sysmonitorsettings.ini
File Edit View Filters Status Help
***** SysMonitor v10.1.0.2.0 build 2 [connected to 10.10.4.120 (GSSCP_IPO_10 (Server Edition(P)))] *****
336128685mS SIP Rx: TCP 10.10.4.30:43844 -> 10.10.4.120:5060
  OPTIONS sip:avaya.com SIP/2.0
  From: <sip:avaya.com>;tag=1c1904606935
  To: <sip:avaya.com>
  CSeq: 1 OPTIONS
  Call-ID: 07a0401e5c819c50fc33700dd0e04846
  Contact: <sip:10.10.4.30:5060;transport=tcp>
  Record-Route: <sip:10.10.4.30:5060;ipca=line=2;lr;transport=tcp>
  Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, FRACK, REFER, INFO, SUBSCRIBE, UPDATE
  Supported: replaces
  User-Agent: M800B/v.7.20A.155.056
  Max-Forwards: 69
  Via: SIP/2.0/TCP 10.10.4.30:5060;branch=z9hG4bK-s1632-000939282561-1--s1632-
  Accept: application/sdp, application/simple-message-summary, message/sipfrag
  Content-Length: 0

336128686mS Sip: Association found trunk: SIP Line (17)
336128686mS Sip: Update SipICPUser->trunk SIP Line (17)
336128686mS Sip: SIPDialog f6e2cdd0 created, dialogs 1 twn_keys 1
336128686mS Sip: (f6e2cdd0) SetUnintTransactionCondition to Unint_None
336128686mS Sip: SipICPUser 8430 has 1 dialog open (AttachDialogToSipICPUser)
336128686mS Sip: SIPDialog:ExtractResponseParamsFromViaHeader remote sent_by: 10.10.4.30:5060 trunk
336128686mS Sip: SIPDialog:ExtractResponseParamsFromViaHeader remote sent by transport: SIP/2.0/TCP trunk
336128686mS Sip: (f6e2cdd0) SendSIPResponse: OPTIONS code 200 SENT TO 10.10.4.30 43844
336128686mS SIP Tx: TCP 10.10.4.120:5060 -> 10.10.4.30:43844
  SIP/2.0 200 OK
  Via: SIP/2.0/TCP 10.10.4.30:5060;branch=z9hG4bK-s1632-000939282561-1--s1632-
  Record-Route: <sip:10.10.4.30:5060;ipca=line=2;lr;transport=tcp>
  From: <sip:avaya.com>;tag=1c1904606935
  Call-ID: 07a0401e5c819c50fc33700dd0e04846
  CSeq: 1 OPTIONS
  Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, INFO, NOTIFY, UPDATE
  Supported: timer
  Server: IP Office 10.1.0.2.0 build 2
  To: <sip:avaya.com>;tag=895dd2b8d0f38743
  Content-Type: application/sdp
  Content-Length: 169

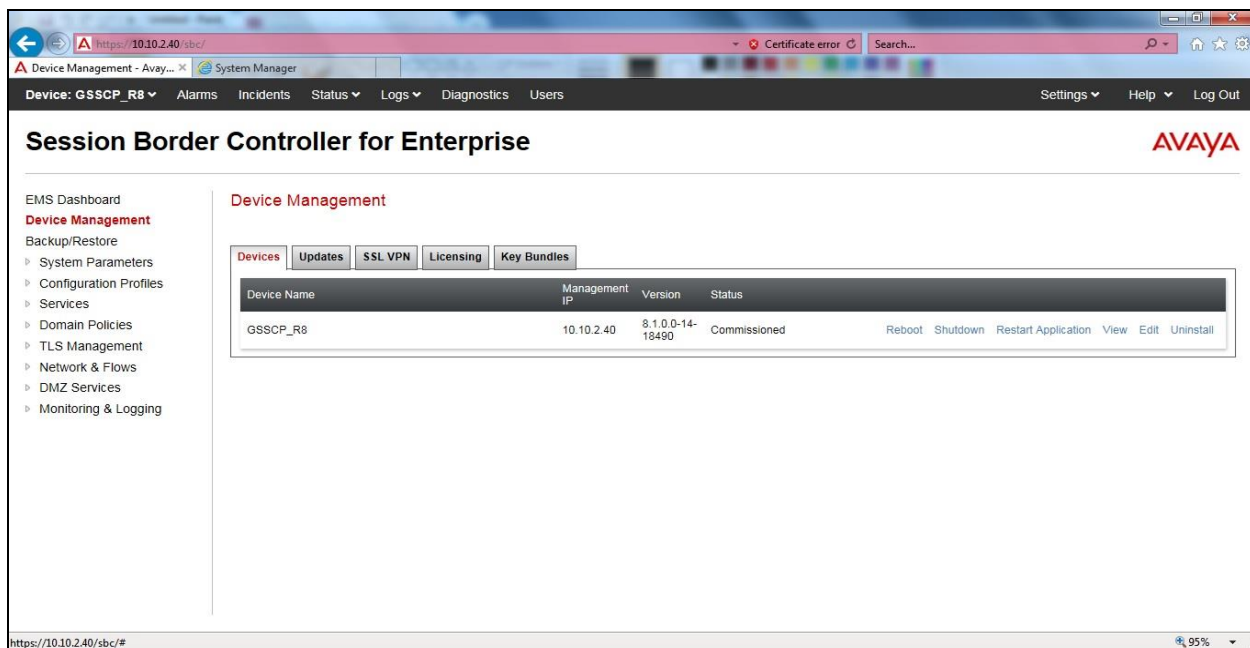
  v=0
  o=UserA 1712183164 1334060956 IN IP4 10.10.4.120
  s=Session SDP
  c=IN IP4 10.10.4.120
  t=0 0
```

8.3. Avaya SBCE

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

8.3.1. Incidents

The Incident Viewer can be accessed from the Avaya SBCE dashboard as highlighted in the screen shot below.



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

Incident Viewer

AVAYA

Device All ▼ Category All ▼ Clear Refresh Generate Report

Displaying results 1 to 15 out of 2000.

Type	ID	Date	Time	Category	Device	Cause
Routing Failure	686948871165253	7/15/13	2:15 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden
Routing Failure	686948811180314	7/15/13	2:13 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden
ACK Message Out of Dialog	686948761299324	7/15/13	2:12 PM	Protocol Discrepancy	VLAN3_MicroSBC	General Method not allowed Out-Of-Dialog
Message Dropped	686948761299222	7/15/13	2:12 PM	Policy	VLAN3_MicroSBC	No Subscriber Flow Matched
Call Denied	686948761263328	7/15/13	2:12 PM	Policy	VLAN3_MicroSBC	No Subscriber Flow Matched
Routing Failure	686948751195370	7/15/13	2:11 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden

8.3.2. Trace Capture

To define the trace, navigate to **Device Specific Settings → Troubleshooting → Trace** in the menu on the left-hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select **All** from the **Local Address** drop down menu.
- Enter the IP address of the Service Provider's SBC in the **Remote Address** field or enter a * to capture all traffic.
- Specify the **Maximum Number of Packets to Capture**, 1000 is shown as an example.
- Specify the filename of the resultant .pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

Trace: GSSCP_R8

Packet Capture
Captures

Packet Capture Configuration

Status

Ready

Interface

B1

Local Address
IP:Port

All

Remote Address
*, *.Port, IP, IP:Port

*

Protocol

UDP

Maximum Number of Packets to Capture

10000

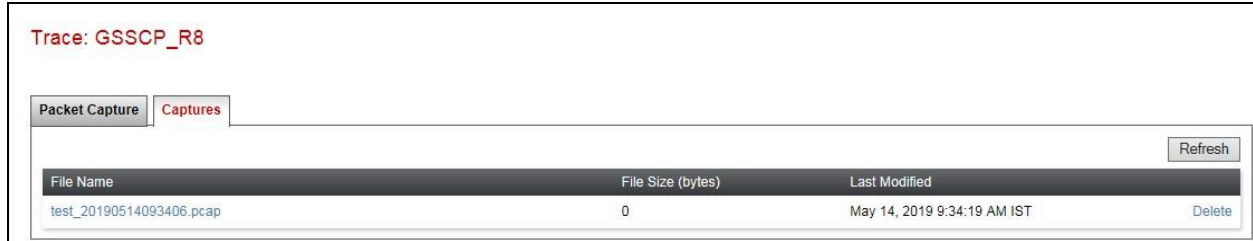
Capture Filename
Using the name of an existing capture will overwrite it.

test.pcap

Start Capture

Clear

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.



The trace is viewed as a standard .pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response in the form of a 200 OK will be seen from the Telenor network.

9. Conclusion

These Application Notes demonstrated how IP Office R11.1 and Avaya Session Border Controller for Enterprise R8.1 can be successfully combined with Telenor IPT Multi-User SIP Trunk Service as shown in **Figure 1**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and demonstrates Avaya IP Office with Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with Telenor IPT Multi-User SIP Trunk Service. This solution provides IP Office and Avaya Session Border Controller for Enterprise users the ability to access the Public Switched Telephone Network (PSTN) via a SIP trunk using the with Telenor IPT Multi-User SIP Trunk Service thus eliminating the costs of analogue or digital trunk connections previously required to access the PSTN. The service was successfully tested with a number of observations listed in **Section 2.2**.

10. Additional References

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

- [1] *Avaya IP Office™ Platform Start Here First*, Release 11.1, Apr 2020.
- [2] *Avaya IP Office™ Platform Server Edition Reference Configuration*, Release 11.1, Apr 2020.
- [3] *Deploying IP Office™ Platform Server Edition Solution*, Release 11.1, May 2020.
- [4] *IP Office™ Platform 11.1, Deploying IP Office Essential Edition*, May 2020.
- [5] *IP Office™ Platform 11.1 Installing and Maintaining the Avaya IP Office™ Platform Application Server*, May 2020.
- [6] *Administering Avaya IP Office™ Platform with Web Manager*, Release 11.1, Apr 2020.
- [7] *Administering Avaya IP Office™ Platform with Manager*, Release 11.1, Apr 2020.
- [8] *IP Office™ Platform 11.1 Using Avaya IP Office™ Platform System Status*, Apr 2020.
- [9] *IP Office™ Platform 11.1 Using IP Office System Monitor*, Apr 2020.
- [10] *Using Avaya Equinox for Windows on IP Office*, Jun 2020.
- [11] *IP Office™ Platform 11.1 - Third-Party SIP Extension Installation Notes*, Jun 2020.
- [12] *Avaya IP Office Knowledgebase*, <http://marketingtools.avaya.com/knowledgebase>
- [13] *Deploying Avaya Session Border Controller for Enterprise Release 8.1*, Jun 2020.
- [14] *Upgrading Avaya Session Border Controller for Enterprise Release 8.1*, Apr 2020.
- [15] *Administering Avaya Session Border Controller for Enterprise Release 8.1*, Apr 2020.
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2020 Avaya Inc. All Rights Reserved.

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

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