



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Server Edition R11.1 with Avaya Session Border Controller for Enterprise R8.1 to support Swisscom Smart Business Connect - 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between the Swisscom Smart Business Connect and Avaya IP Office Server Edition R11.1 with Avaya Session Border Controller for Enterprise R8.1.

The Swisscom Smart Business Connect SIP Trunk provides PSTN access via a SIP trunk connected to the Swisscom Smart Business Connect Voice Over Internet Protocol (VoIP) network as an alternative to legacy Analog or Digital trunks. Swisscom 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 Swisscom Smart Business Connect and Avaya IP Office Server Edition with Avaya Session Border Controller for Enterprise (Avaya SBCE).

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

The Avaya Session Border Controller for Enterprise (Avaya SBCE) is the point of connection between Avaya IP Office and Swisscom Smart Business Connect SIP Trunk service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signalling for interoperability.

Swisscom Smart Business Connect service provides PSTN access via a SIP trunk connected to the Swisscom 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 Server Edition and Avaya SBCE to connect to the Swisscom Smart Business Connect SIP Trunk. 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 this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For security, TLS and SRTP was used internally to the enterprise between Avaya products.

2.1. Interoperability Compliance Testing

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.
- Incoming and Outgoing PSTN calls to/from Avaya Workplace Client for Windows soft phone.
- Calls using the G.711A, G.729 and G.722 codecs.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using both T38 Fallback and G.711 pass-through transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation 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, call mute, transfer, and conference.
- Off-net call forwarding and mobile twinning.

2.2. Test Results

Interoperability testing of the test configuration was completed with successful results for Swisscom's SIP Trunk service with the following observations:

- During testing it was observed that when an inbound call from a PSTN number terminates on an IP Office user that is call forwarded to another external PSTN number that is not in service or voicemail enabled, the external PSTN will respond to IP Office with a "183 Session Progress" that can contain an announcement "e.g. This number is not in service". However, IP Office responds to the "183 Session Progress" with "180 Ringing" so the PSTN caller that initially made the inbound call does not hear this announcement and will just hear continuous ringback until the Call Queueing Timers expire and busytone is then heard. However, in this particular call scenario, IP Office is behaving as designed as IP Office does not support playing announcements from non-primary targets (forwarding, twinning etc.) as the call is still anchored on IP Office.
- During T.38 fax testing, it was observed that when Swisscom sent a reINVITE to negotiate to T.38 fax calls, IP Office responded with a 200OK with 2 x media lines in the SDP. The first media line had an attribute value of "inactive" which made the second media line active. However, Swisscom would respond to the 200OK from IP Office with a BYE and the call was terminated. Therefore, T.38 fax is not supported on the Swisscom Smart Business Connect SIP platform.

- The Privacy Header as required by Swisscom is not included in the SIP INVITE for outbound calls with Calling Line Identity (CLIR) when using an IP Office short code (*67 was used in the test configuration). As a workaround, the anonymous button can be enabled on the SIP tab in **Section 5.8** to restrict CLIR and include a Privacy Header as required by Swisscom.
- 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 Swisscom products please contact the Swisscom support team: Email: PBX-Technical.Partner@swisscom.com.

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to the Swisscom 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 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 Workplace Client for Windows for softphone testing.

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.

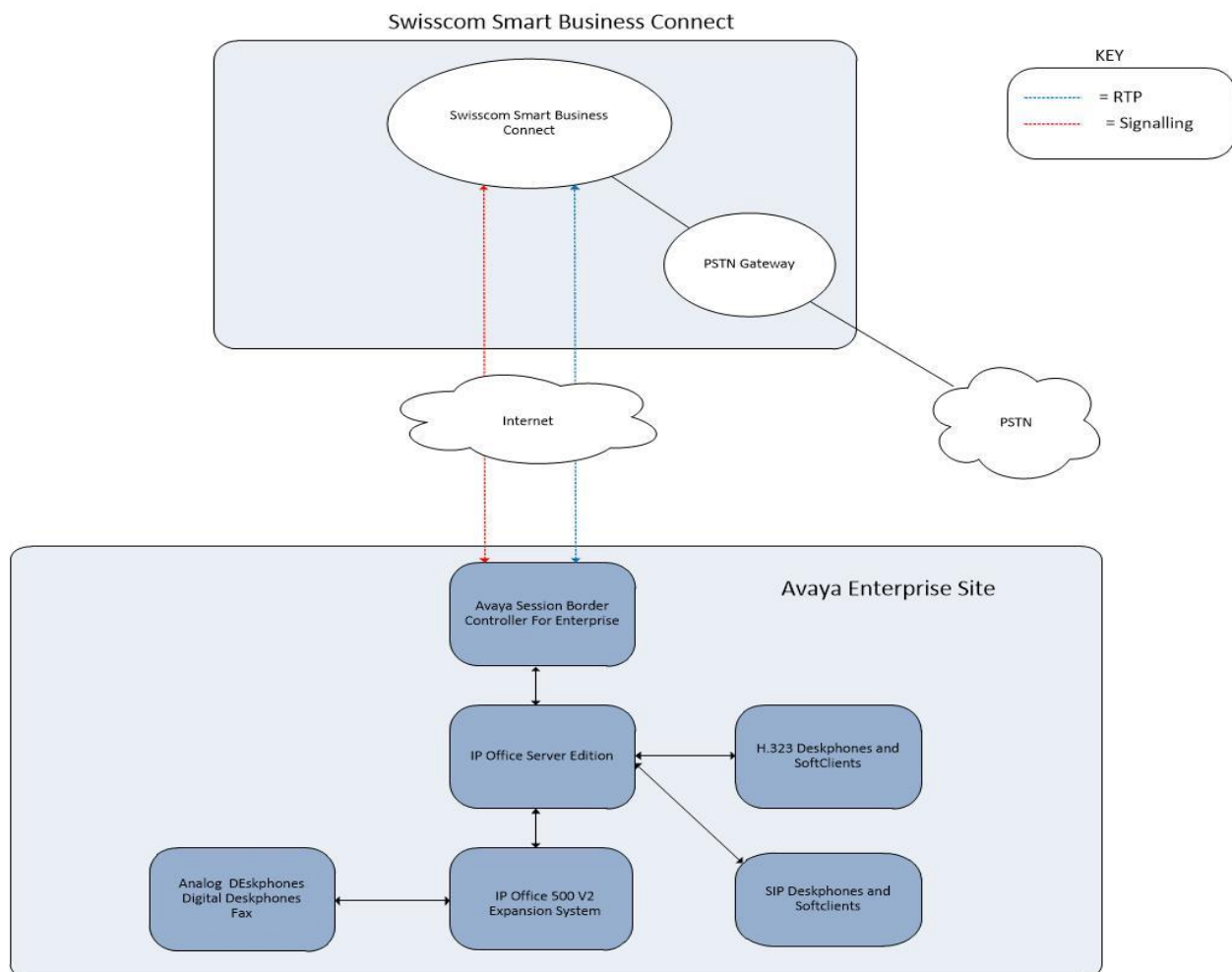


Figure 1: Test setup Swisscom Smart Business Connect to simulated Avaya Enterprise

4. Equipment and Software Validated

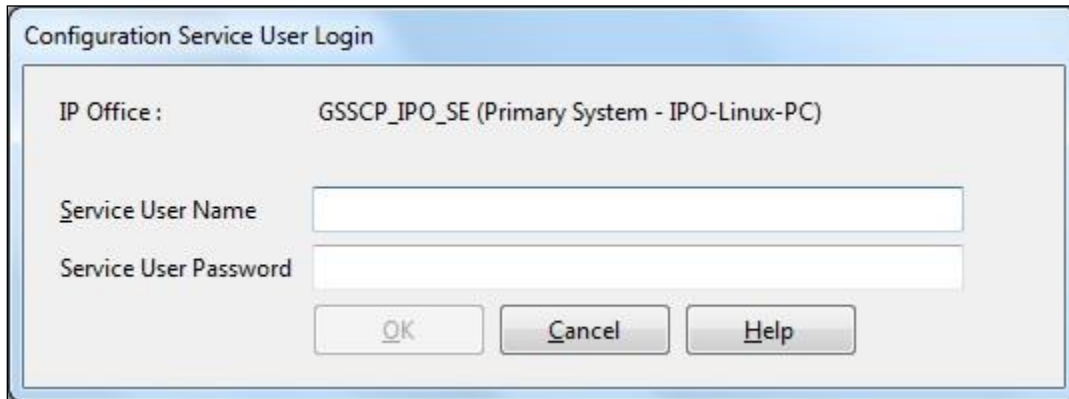
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	Version 11.1.1.0.0 build 209
Avaya IP Office 500 V2	Version 11.1.1.0.0 build 209
Avaya Voicemail Pro Client	Version 11.1.1000.152
Avaya IP Office Manager	Version 11.1.1.0.0 build 209
Avaya Session Border Controller for Enterprise	8.1.2.0-31-19809
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 Workplace Client for Windows (SIP)	3.17.0.65.16
Avaya 1140e (SIP)	FW: 04.04.23.00.bin
Avaya 1408 Digital Telephone	R48
Avaya Analogue Phone	N/A
Swisscom	
Cisco C881-K9	Cisco IOS Software, Version 15.6(3)M4

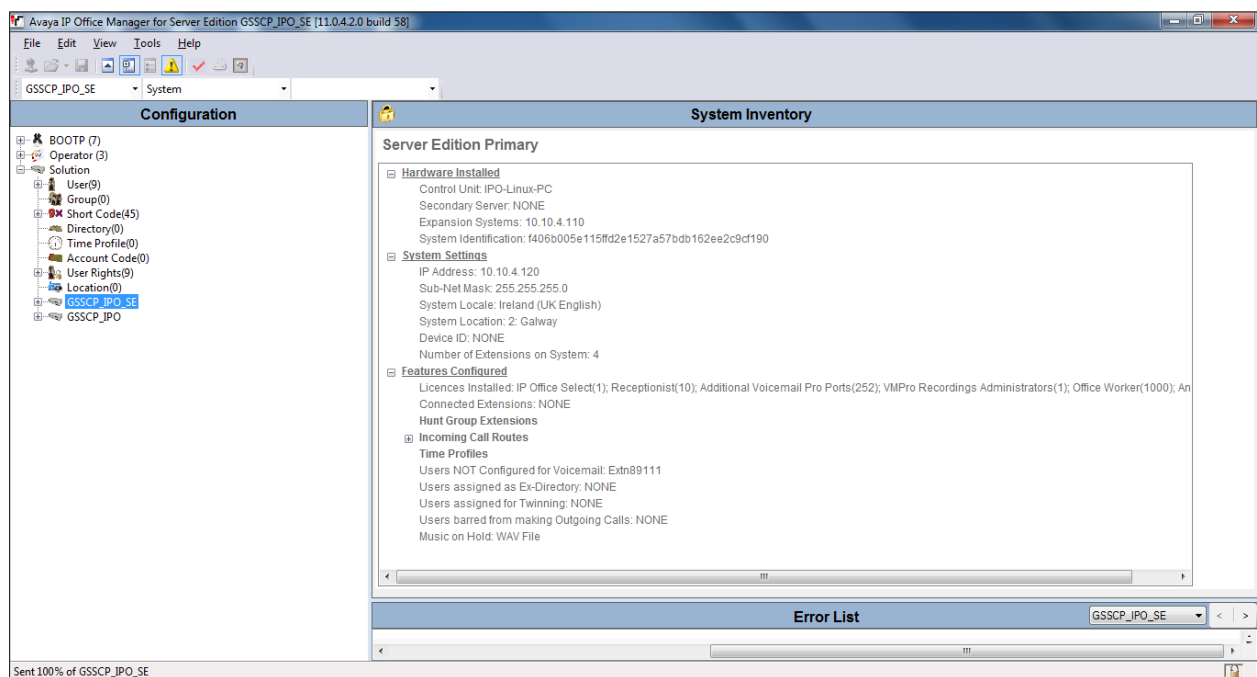
Note – Testing was performed with IP Office Server Edition with 500 V2 Expansion R11.1. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires 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 Swisscom SIP Trunk service. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials.



A management window will appear similar to the one 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 (such as twinning) is assumed to already be in place.



5.1. Verify System Capacity

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

Licence Remote Server

Licence Mode Licence Normal

Licensed Version 11.0

PLDS Host ID 213429294550

PLDS File Status Valid

Feature	Instances	Status	Expiry Date	Source
Receptionist	10	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	10	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	10	Obsolete	Never	PLDS Nodal
VMPro TTS (Generic)	40	Obsolete	Never	PLDS Nodal
Teleworker	384	Obsolete	Never	PLDS Nodal
Mobile Worker	384	Obsolete	Never	PLDS Nodal
Office Worker	384	Valid	Never	PLDS Nodal
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	40	Obsolete	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	10	Obsolete	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Customer Service Agent	10	Dormant	Never	PLDS Nodal
Customer Service Supervisor	10	Dormant	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal
SIP Trunk Channels	128	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	10	Valid	Never	PLDS Nodal
Wave User	16	Obsolete	Never	PLDS Nodal
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal
Centralized Endpoints	10	Obsolete	Never	PLDS Nodal

Add...

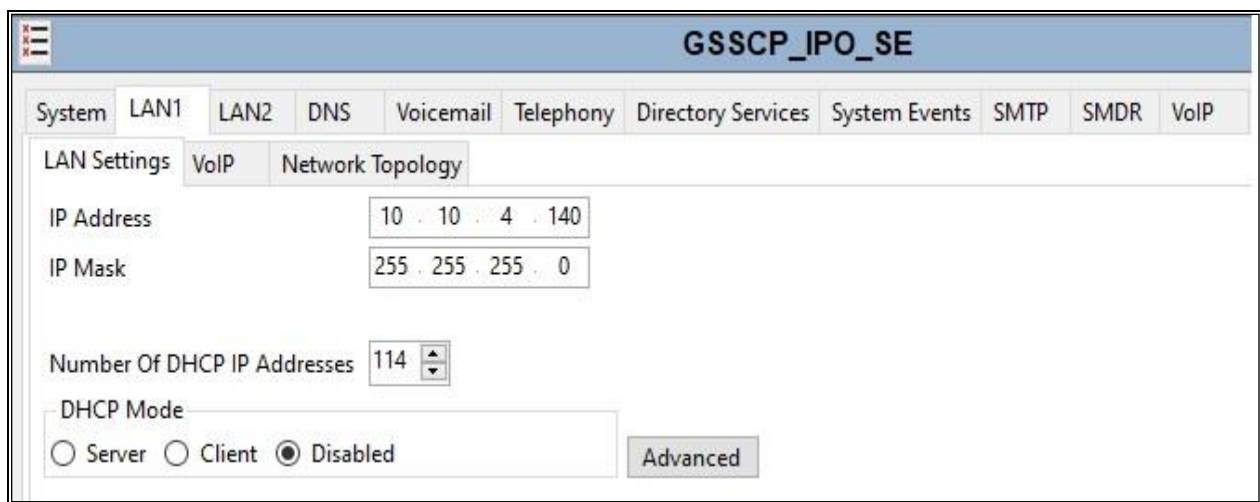
Remove

OK Cancel Help

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 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 'GSSCP_IPO_SE' configuration window with the 'LAN1' tab selected. Under the 'LAN Settings' sub-tab, the 'IP Address' is set to '10 . 10 . 4 . 140' and the 'IP Mask' is set to '255 . 255 . 255 . 0'. The 'Number Of DHCP IP Addresses' is set to '114'. The 'DHCP Mode' is set to 'Disabled' (indicated by a selected radio button). There are also radio buttons for 'Server' and 'Client', and an 'Advanced' button.

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 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**.

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 shows the 'GSSCP_IPO_SE*' configuration window with the following settings:

- System Tab:** LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, Contact Center.
- LAN Settings Tab:**
 - ☒ H323 Gatekeeper Enable
 - ☐ Auto-create Extn ☐ Auto-create User ☐ H323 Remote Extn Enable
 - H.323 Signalling over TLS: Preferred (dropdown)
 - Remote Call Signalling Port: 1720 (spin box)
- VoIP Tab:**
 - ☒ SIP Trunks Enable
 - ☒ SIP Registrar Enable
 - ☐ Auto-create Extn/User ☐ SIP Remote Extn Enable
 - Allowed SIP User Agents: Block blacklist only (dropdown)
 - SIP Domain Name: avaya.com (text box)
 - SIP Registrar FQDN: avaya.com (text box)
 - Layer 4 Protocol:
 - ☒ UDP UDP Port: 5060 (spin box) Remote UDP Port: 5060 (spin box)
 - ☒ TCP TCP Port: 5060 (spin box) Remote TCP Port: 5060 (spin box)
 - ☒ TLS TLS Port: 5061 (spin box) Remote TLS Port: 5061 (spin box)
 - Challenge Expiry Time (secs): 10 (spin box)
- RTP Tab:**
 - Port Number Range:
 - Minimum: 40750 (spin box) Maximum: 50750 (spin box)
 - Port Number Range (NAT):
 - Minimum: 40750 (spin box) Maximum: 50750 (spin box)
 - ☒ Enable RTCP Monitoring on Port 5005
 - RTCP collector IP address for phones: 0 . 0 . 0 . 0 (text box)
 - Keepalives:
 - Scope: RTP-RTCP (dropdown) Periodic timeout: 30 (spin box)
 - Initial keepalives: Enabled (dropdown)

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 **30**. 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 'Network Topology Discovery' section contains the following settings:

- STUN Server Address:** 0.0.0.0
- STUN Port:** 3478
- Firewall/NAT Type:** Open Internet (selected from a dropdown menu)
- Binding Refresh Time (seconds):** 0 (with up/down arrows)
- Public IP Address:** 0 . 0 . 0 . 0
- Public Port:**
 - UDP: 5060
 - TCP: 5060
 - TLS: 5061

At the bottom, there is a checkbox labeled 'Run STUN on startup' which is currently unchecked. To the right of the IP address field are 'Run STUN' and 'Cancel' buttons.

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 shows the 'GSSCP_IPO_SE*' configuration window with the 'Telephony' tab selected. The window has a top navigation bar with tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and Contact Center. Below this is a sub-tab bar for the Telephony section: Telephony, Park & Page, Tones & Music, Ring Tones, SM, Call Log, and TUI. The main configuration area is divided into several sections:

- General Settings:** Dial Delay Time (secs) is 1; Dial Delay Count is 4; Default No Answer Time (secs) is 15; Hold Timeout (secs) is 0; Park Timeout (secs) is 300; Ring Delay (secs) is 5; Call Priority Promotion Time (secs) is Disabled; Default Currency is EUR; Default Name Priority is Favour Trunk; Media Connection Preservation is Enabled; Phone Failback is Automatic.
- Login Code Complexity:** Enforcement is checked; Minimum length is 4; Complexity is checked.
- RTCP Collector Configuration:** Send RTCP to an RTCP Collector is unchecked; Server Address is 0.0.0.0; UDP Port Number is 5005; RTCP reporting interval (secs) is 5.
- Companding Law:** Switch is set to A-Law (radio button selected); Line is set to A-Law Line (radio button selected).
- Advanced Settings:** DSS Status is unchecked; Auto Hold is checked; Dial By Name is checked; Show Account Code is checked; Inhibit Off-Switch Forward/Transfer is unchecked; Restrict Network Interconnect is unchecked; Include location specific information is unchecked; Drop External Only Impromptu Conference is checked; Visually Differentiate External Call is unchecked; High Quality Conferencing is checked; Directory Overrides Barring is checked; Advertise Callee State To Internal Callers is unchecked; Internal Ring on Transfer is unchecked.

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.711 ALAW 64K** is set as the priority codec, **G.729(a) 8K CS-ACELP** set as the secondary codec and **G.722 64K** as the third codec selection.

The screenshot shows the 'GSSCP_IPO_SE' configuration window with the 'VoIP' tab selected. The interface includes several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. Under the 'VoIP' tab, there are sub-tabs for 'VoIP Security' and 'Access Control Lists'. The 'VoIP Security' sub-tab is active, showing options for 'Ignore DTMF Mismatch For Phones' (checked), 'Allow Direct Media Within NAT Location' (unchecked), and 'RFC2833 Default Payload' (set to 101). Below these options are three panels: 'Available Codecs', 'Default Codec Selection', and 'Selected'. The 'Available Codecs' panel lists four codecs with checkboxes: G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, and G.729(a) 8K CS-AC. The 'Default Codec Selection' panel has two sub-sections: 'Unused' and 'Selected'. The 'Unused' section contains 'G.711 ULAW 64K'. The 'Selected' section contains 'G.711 ALAW 64K', 'G.729(a) 8K CS-A', and 'G.722 64K'. Between the 'Unused' and 'Selected' sections are five buttons: '>>>', '<<<', and two arrows pointing up and down.

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 with the 'VoIP Security' tab selected. The 'Media' dropdown is set to 'Preferred'. Under 'Media Security Options', 'Encryptions' has 'RTP' checked and 'RTCP' unchecked. 'Authentication' has 'RTP' checked and 'RTCP' unchecked. 'Replay Protection' is unchecked. 'SRTP Window Size' is set to 64. Under 'Crypto Suites', 'SRTP_AES_CM_128_SHA1_80' is checked and 'SRTP_AES_CM_128_SHA1_32' is unchecked. The 'Strict SIPS' checkbox is also unchecked.

System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	VoIP
VoIP Security										
Default Extension Password: [Masked]										
Confirm Default Extension Password: [Masked]										
Media: Preferred										
Media Security Options										
Encryptions: [X] RTP, [] RTCP										
Authentication: [X] RTP, [X] RTCP										
Replay Protection: []										
SRTP Window Size: 64										
Crypto Suites: [X] SRTP_AES_CM_128_SHA1_80, [] SRTP_AES_CM_128_SHA1_32										
[] Strict SIPS										

5.6. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Swisscom Smart Business Connect service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.6.1** 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:

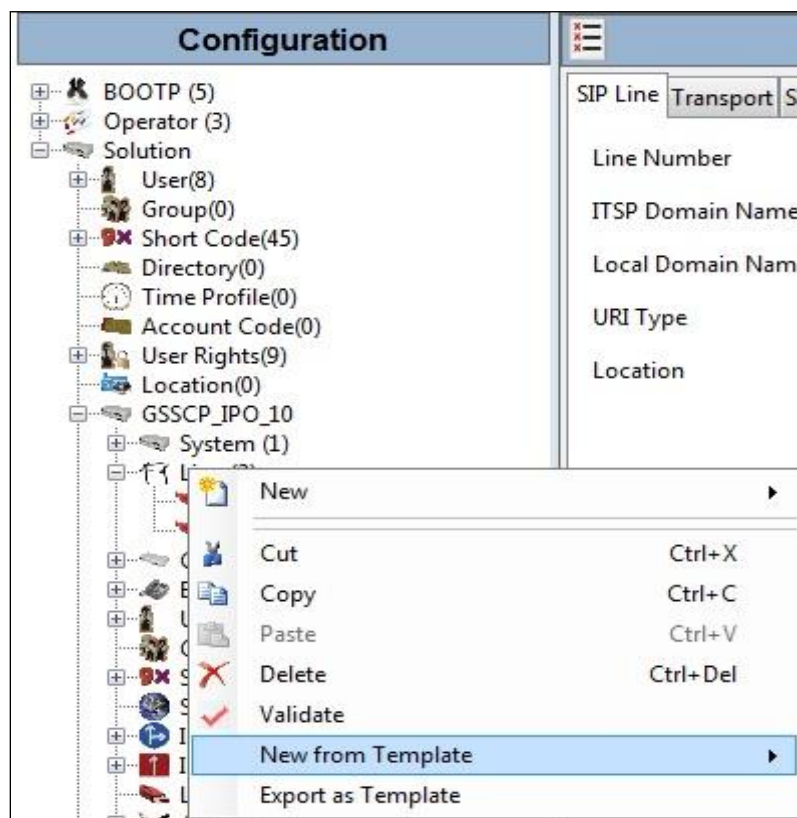
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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**.

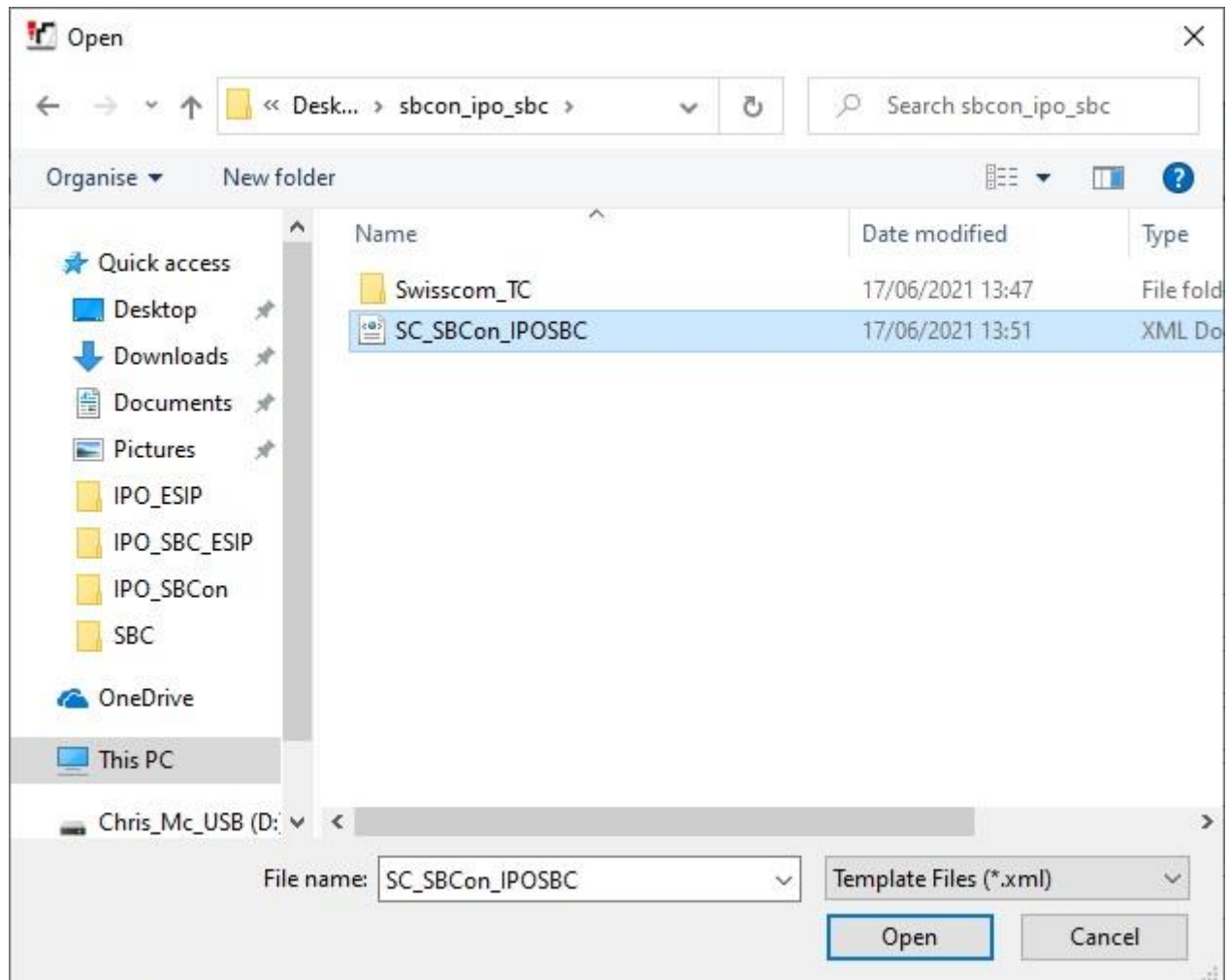
5.6.1. SIP Line From Template

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.



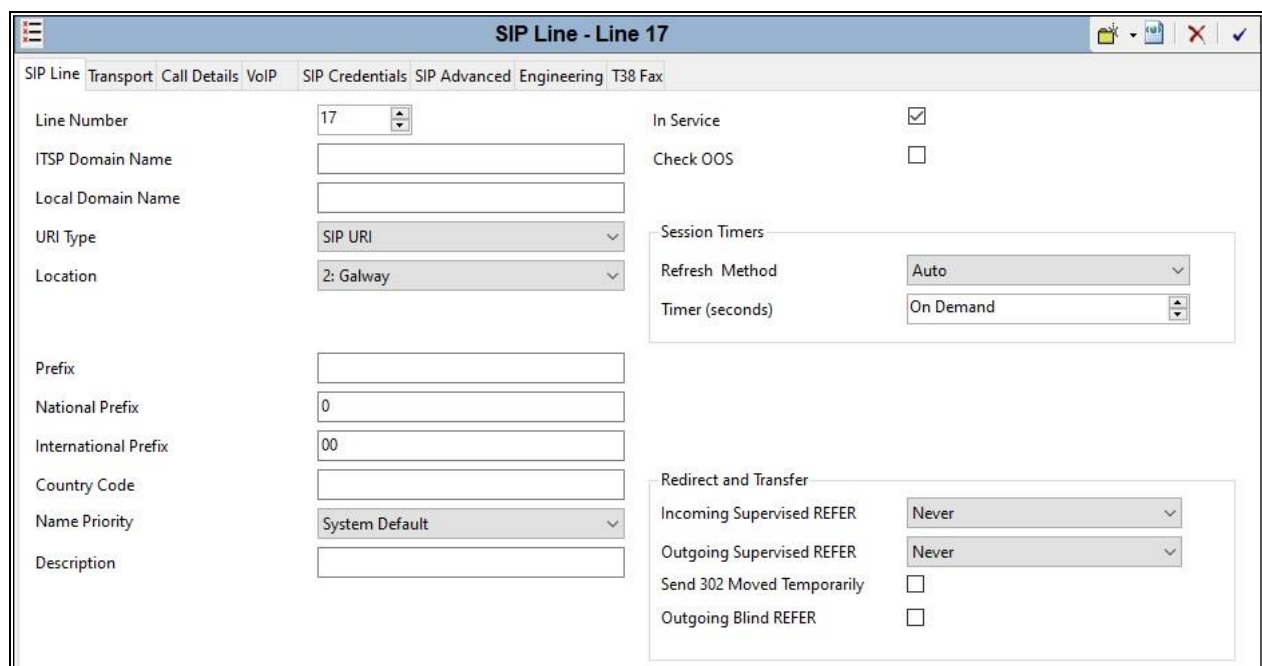
The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.6.2**.

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 provider by the Service Provider if required, however no ITSP Domain Name was used in this configuration.
- Set **Location** to that defined for Emergency calls as described in **Section 5.9**.
- 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.
- Leave the **Refresh Method** at the default value of **Auto** which results in re-INVITE being used for Session Refresh.
- 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 Supervise REFER** to **Never**. REFER is not supported by Swisscom SIP platform.
- Default values may be used for all other parameters.

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



SIP Line - Line 17	
SIP Line Transport Call Details VoIP SIP Credentials SIP Advanced Engineering T38 Fax	
Line Number	17
ITSP Domain Name	
Local Domain Name	
URI Type	SIP URI
Location	2: Galway
Prefix	
National Prefix	0
International Prefix	00
Country Code	
Name Priority	System Default
Description	
In Service	<input checked="" type="checkbox"/>
Check OOS	<input 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"/>

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. 'Separate Registrar' is 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 empty, and the 'Add...' button is visible.

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 5.9**. In the test environment a value of **17** was used for the Swisscom 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** and **P Asserted ID** to **Use Internal Data** for both the **Display** name and **Content**. On incoming calls, this will analyse the Request-Line sent by Swisscom and match to the SIP settings in the User profile as described in **Section 5.8**. 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	
2	17 2	0: <None>	Auto	Auto				

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 **T38 Fallback** as this is the preferred method of fax transmission for Swisscom.
- 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 menu bar 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 two lists: 'Unused' and 'Selected'. The 'Unused' list contains 'G.711 ULAW 64K'. The 'Selected' list contains 'G.711 ALAW 64K', 'G.729(a) 8K CS-ACELP', and 'G.722 64K'. Between the lists are buttons for moving items: '>>>', '<<<', and '<<<'. Below the codec lists are three dropdown menus: 'Fax Transport Support' set to 'T38 Fallback', 'DTMF Support' set to 'RFC2833/RFC4733', and 'Media Security' set to 'Same as System (Preferred)'. 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).

After the SIP line parameters are defined, the SIP credentials used for registration and authorisation on this line must be created. To define SIP credentials, first select the **SIP Credentials** tab. Click the **Add** button and the **New SIP Credentials** area will appear at the bottom of the pane.

SIP Line - Line 17*							
SIP Line	Transport	Call Details	VoIP	T38 Fax	SIP Credentials	SIP Advanced	Engineering
Index	UserName	Authentication Name	Contact	Expiry (mins)	Register		
						Add... Remove Edit...	

Enter the registration credentials provided by Swisscom as shown below. Click the **OK** button.

Edit SIP Credentials

User name

+414xxxxxx20

Authentication Name

xxxx

Contact

+414xxxxxx20

Password

••••••••

Confirm Password

••••••••

Expiry (mins)

60

Registration required

☒

OK

Cancel

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

- Select **To Header** from the **Call Routing Method** drop down menu. In the test environment, Swisscom were sending the group number in the Request URI and the DDI number in the To Header.
- 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.
- Select **Emergency Calls** from the **Send Location Info** drop down menu if required
- 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: By Source IP address (dropdown)
 - Call Routing Method: To Header (dropdown)
 - Use P-Called-Party: ☐
 - Suppress DNS SRV Lookups: ☐
- Identity:**
 - Use "phone-context": ☐
 - Add user=phone: ☒
 - Use + for International: ☒
 - Use PAI for Privacy: ☐
 - Use Domain for PAI: ☐
 - Caller ID from From header: ☐
 - Send From In Clear: ☐
 - Cache Auth Credentials: ☒
 - User-Agent and Server Headers:
 - Send Location Info: Emergency Calls (dropdown)
 - Add UUI header: ☐
 - Add UUI header to redirected calls: ☐
- Media:**
 - Allow Empty INVITE: ☐
 - Send Empty re-INVITE: ☐
 - Allow To Tag Change: ☐
 - P-Early-Media Support: None (dropdown)
 - Send SilenceSupp=Off: ☐
 - Force Early Direct Media: ☐
 - Media Connection Preservation: Disabled (dropdown)
 - Indicate HOLD: ☐
- Call Control:**
 - Call Initiation Timeout (s): 4 (spinner)
 - Call Queuing Timeout (m): 5 (spinner)
 - Service Busy Response: 503 - Service Unavailable (dropdown)
 - on No User Responding Send: 408-Request Timeout (dropdown)
 - Suppress Q.850 Reason Header: ☐
 - Emulate NOTIFY for REFER: ☐
 - No REFER if using Diversion: ☐

Note: It is advisable at this stage to save the configuration as described in **Section 5.11** to add 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 and route incoming calls from mobility extensions to access Feature Name Extensions (FNE) hosted on IP Office. 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 shown below.

- 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". It has a "Short Code" tab selected. The fields are as follows:

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"/>

A further example is shown for an emergency number.

The screenshot shows a configuration window titled "086756;; Dial Emergency". It has a "Short Code" tab selected. The fields are as follows:

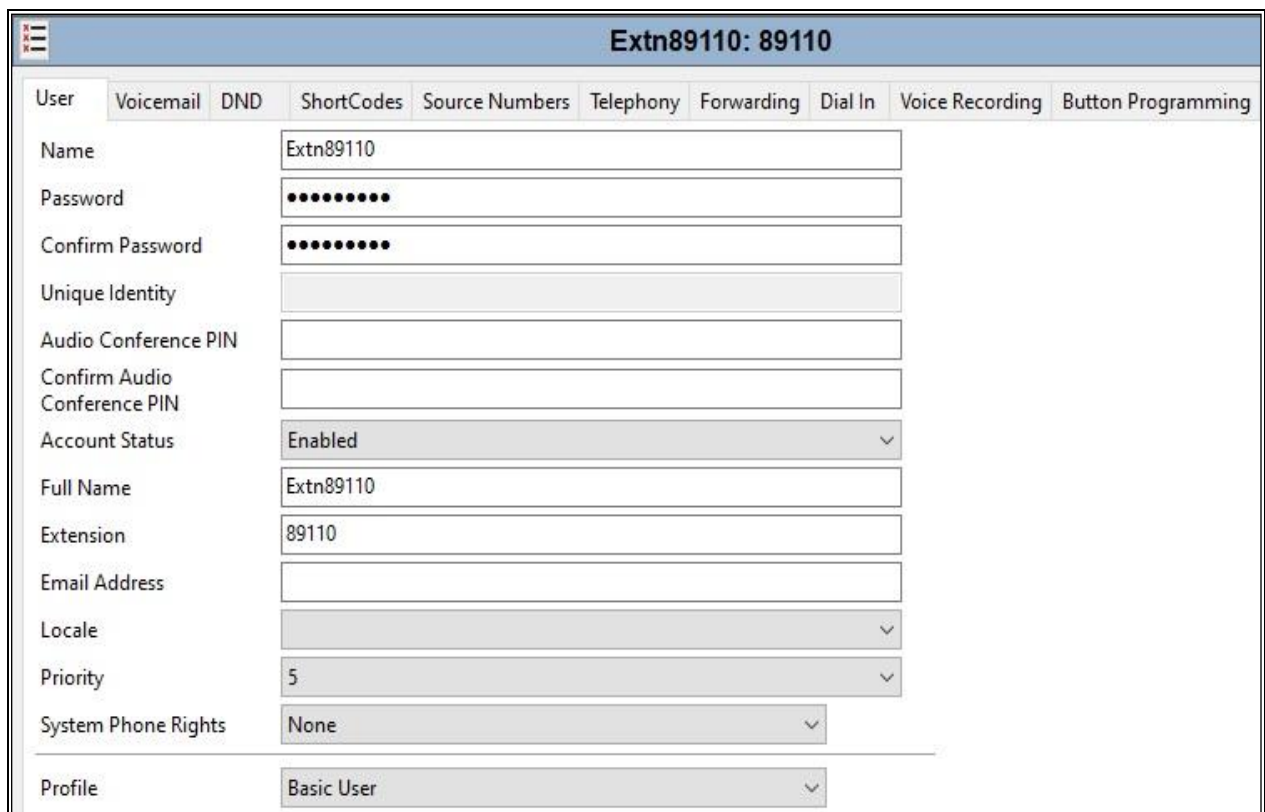
Field	Value
Code	086756;
Feature	Dial Emergency
Telephone Number	086756
Line Group ID	100
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

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.



Ext89110: 89110	
User	Voicemail DND ShortCodes Source Numbers Telephony Forwarding Dial In Voice Recording Button Programming
Name	Ext89110
Password	••••••••
Confirm Password	••••••••
Unique Identity	
Audio Conference PIN	
Confirm Audio Conference PIN	
Account Status	Enabled
Full Name	Ext89110
Extension	89110
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Basic User

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 Swisscom.

The screenshot shows the configuration interface for 'Ext89110: 89110*'. The 'SIP' tab is selected. The configuration fields are as follows:

Field	Value
SIP Name	+414xxxxxx20
SIP Display Name (Alias)	+414xxxxxx20
Contact	+414xxxxxx20
Anonymous	<input checked="" type="checkbox"/>

Note: The **Anonymous** box can be used to restrict Calling Line Identity (CLIR) as discussed **Section 2.2**.

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.

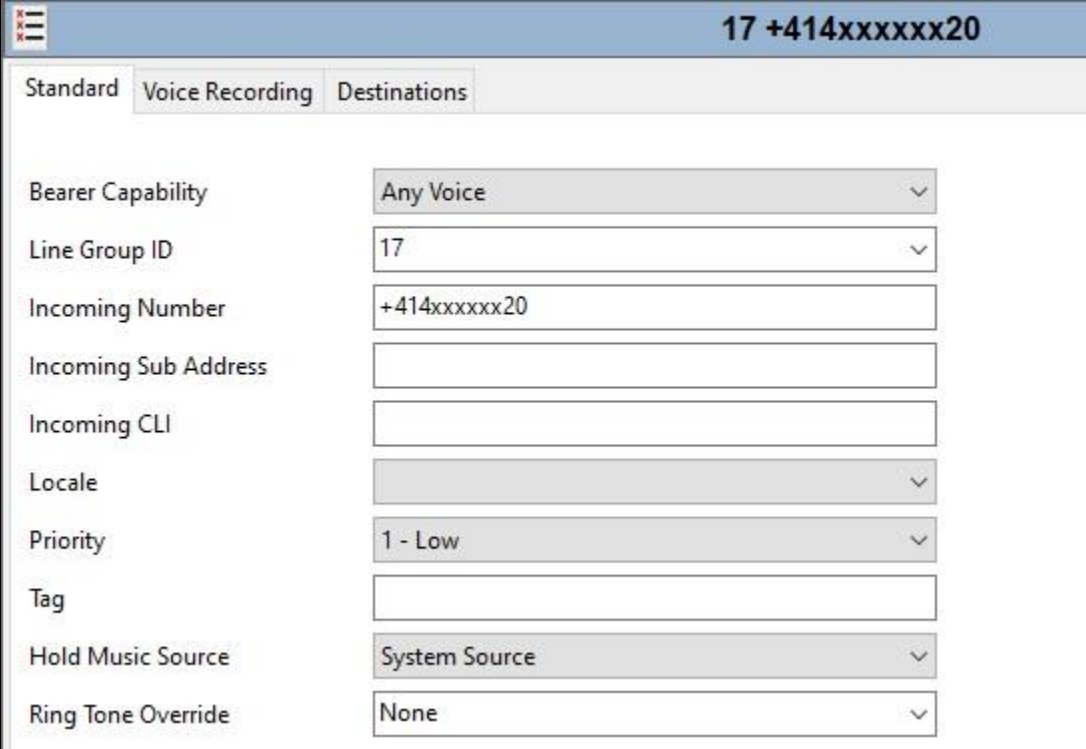
The screenshot shows the configuration interface for 'Ext89110: 89110*'. The 'Mobility' tab is selected. The configuration fields are as follows:

Field	Value
Internal Twinning	<input type="checkbox"/>
Twinned Handset	<None>
Maximum Number of Calls	1
Twin Bridge Appearances	<input type="checkbox"/>
Twin Coverage Appearances	<input type="checkbox"/>
Twin Line Appearances	<input type="checkbox"/>
Mobility Features	<input checked="" type="checkbox"/>
Mobile Twinning	<input checked="" type="checkbox"/>
Fallback Twinning	<input type="checkbox"/>
Twinned Mobile Number (including dial access code)	90035387xxxxxx
Twinning Time Profile	<None>
Mobile Dial Delay (secs)	3
Mobile Answer Guard (secs)	0
Hunt group calls eligible for mobile twinning	<input type="checkbox"/>
Forwarded calls eligible for mobile twinning	<input type="checkbox"/>
Twin When Logged Out	<input type="checkbox"/>
one-X Mobile Client	<input type="checkbox"/>
Mobile Call Control	<input checked="" type="checkbox"/>
Mobile Callback	<input checked="" type="checkbox"/>

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 displays the configuration interface for an incoming call route. At the top, a blue header bar contains a menu icon on the left and the text "17 +414xxxxxx20" on the right. Below the header, there are three tabs: "Standard", "Voice Recording", and "Destinations". The "Standard" tab is currently selected. The configuration fields are as follows:

Field	Value
Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	+414xxxxxx20
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 **+414xxxxxx20** on line 17 are routed to extension 89110.

17 +414xxxxxx20	
Standard	Voice Recording
Destinations	
TimeProfile	Destination
▶ Default Value	89110 Extn89110

5.10. Location

If Location information is required for calls to Emergency Services, right-click **Location** in the Navigation Pane and select **New**, (not shown). On the **Location** tab of the Details Pane, enter the parameters as required. An example used during testing is shown below:

- Define a **Location Name**.
- Define a **Subnet Address** and **Subnet Mask** as required. In the test environment, there was no differentiation based on subnet.
- In the example, all other fields were left at default values.

Galway	
Location	Address
Location Name	Galway
Location ID	2
Subnet Address	0 . 0 . 0 . 0
Subnet Mask	0 . 0 . 0 . 0
Emergency ARS	<None>
Parent Location for CAC	<None>
Call Admission Control	
Total Maximum Calls	Unlimited
External Maximum Calls	Unlimited
Internal Maximum Calls	Unlimited
Time Settings	
Time Zone	Same as System
Local Time Offset from UTC	00:00
Automatic DST	<input type="checkbox"/>
Clock Forward/Back Settings (Start Date - End Date(DST Offset))	<Add New Entry>
<div> <div>Edit</div> <div>Delete</div> </div>	

Click on the **Address** tab and enter data as required. The following screenshot shows an example used during testing:

The screenshot displays the 'Galway' application window with the 'Address' tab selected. At the top, there is a 'Country Code' dropdown menu set to 'IE'. A yellow warning icon is present next to a message: 'Please refer to the help for Information regarding this screen. Failure to format the address properly could result in improper address association.' Below this, the form is organized into several sections. On the left, there are six address lines labeled A1 through A6, with A1 containing 'Connacht', A2 and A3 containing 'Galway', A4 containing 'Mervue', A5 containing 'Business Park', and A6 containing 'Unit 25-29'. Below these are eight additional fields labeled RD, RDSEC, RDBR, RDSUBBR, PRD, POD, STS, PRM, and POM, each with an empty input box. On the right side, there are fields for HNO, HNS, LMK, BLD, LOC, PLC, FLR, UNIT (containing 'GSSCP Unit'), ROOM, and SEAT. At the bottom right, there is a section with fields for NAM (containing 'GSSCP'), ADDCODE, PCN, PC, and POBOX.

Galway	
Location Address	
Country Code	IE
Please refer to the help for Information regarding this screen. Failure to format the address properly could result in improper address association.	
A1	Connacht
A2	Galway
A3	Galway
A4	Mervue
A5	Business Park
A6	Unit 25-29
RD	
RDSEC	
RDBR	
RDSUBBR	
PRD	
POD	
STS	
PRM	
POM	
HNO	
HNS	
LMK	
BLD	
LOC	
PLC	
FLR	
UNIT	GSSCP Unit
ROOM	
SEAT	
NAM	GSSCP
ADDCODE	
PCN	
PC	
POBOX	

5.11. 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 Swisscom SIP Trunk testing was carried out using this configuration with only the analog extension for the fax machine on the Expansion. In this configuration, the T38 Fallback fax settings are configured on the SIP line between the Expansion and the Server.

5.11.1. Analog 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**.

5.11.2. T38 Fallback Fax Settings

The T38 Fallback 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 Swisscom 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 **T38 Fallback**. The following screenshot shows the VoIP Settings for the IP Office Line between the Server and the Expansion on the Expansion:

The screenshot shows the 'IP Office Line - Line 1' configuration window with the 'VoIP Settings' tab selected. The window has a header bar with a menu icon and the title 'IP Office Line - Line 1'. Below the header are three tabs: 'Line', 'Short Codes', and 'VoIP Settings'. The 'VoIP Settings' tab is active. In the top right corner, there are two checkboxes: 'Out Of Band DTMF' (checked) and 'Allow Direct Media Path' (unchecked). The main area is divided into two sections. The top section is 'Codec Selection', which features a 'System Default' dropdown menu. Below this are two lists: 'Unused' and 'Selected'. The 'Unused' list contains 'G.711 ULAW 64K'. The 'Selected' list contains 'G.711 ALAW 64K', 'G.729(a) 8K CS-ACELP', and 'G.722 64K'. Between these lists are five buttons: '>>>', '<<<', '<<<', '>>>', and '>>>'. The bottom section contains three settings: 'Fax Transport Support' set to 'T38 Fallback', 'Call Initiation Timeout (s)' set to '4', and 'Media Security' set to 'Same as System (Preferred)'.

Line	Short Codes	VoIP Settings
<div><div>Out Of Band DTMF <input checked="" type="checkbox"/></div><div>Allow Direct Media Path <input type="checkbox"/></div><div><div>Codec Selection</div><div>System Default</div><div><div>Unused</div><div>G.711 ULAW 64K</div></div><div><div>Selected</div><div>G.711 ALAW 64K G.729(a) 8K CS-ACELP G.722 64K</div></div></div><div><div>Fax Transport Support</div><div>T38 Fallback</div></div><div><div>Call Initiation Timeout (s)</div><div>4</div></div><div><div>Media Security</div><div>Same as System (Preferred)</div></div></div>		

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

The screenshot displays the 'IP Office Line - Line 2*' configuration window with the 'VoIP Settings' tab selected. The window has a tabbed interface with 'Line', 'Short Codes', 'VoIP Settings', and 'T38 Fax'. The 'VoIP Settings' tab contains the following elements:

- Codec Selection:** A dropdown menu set to 'System Default'. Below it are two lists: 'Unused' and 'Selected'.
 - Unused:** G.711 ULAW 64K, G.723.1 6K3 MP-MLQ
 - Selected:** G.711 ALAW 64K, G.729(a) 8K CS-ACELP, G.722 64K
 - Between the lists are five buttons: '>>>', an up arrow, '<<<', a down arrow, and '>>>'.
- Fax Transport Support:** A dropdown menu set to 'T38 Fallback'.
- Call Initiation Timeout (s):** A numeric input field with the value '4'.
- Media Security:** A dropdown menu set to 'Same as System (Preferred)'.
- Checkboxes (top right):**
 - ☐ VoIP Silence Suppression
 - ☒ Out Of Band DTMF
 - ☐ Allow Direct Media Path

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

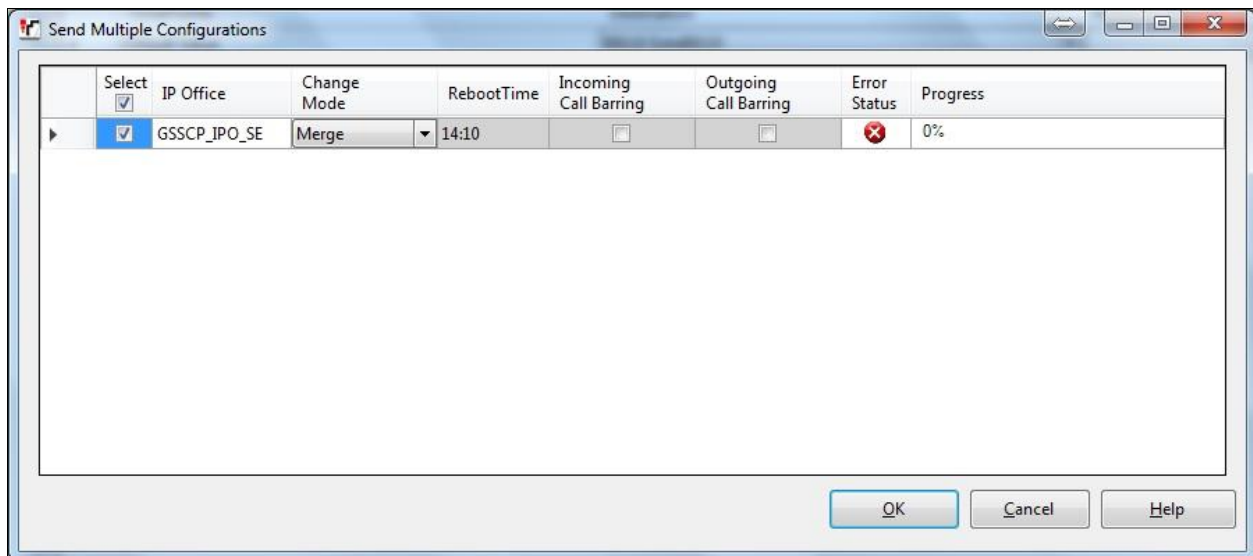
5.12. Save Configuration

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, Immediate, When Free or Timed is shown under the **Configuration Reboot Mode** column, 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

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.



5.13. TLS Certificates

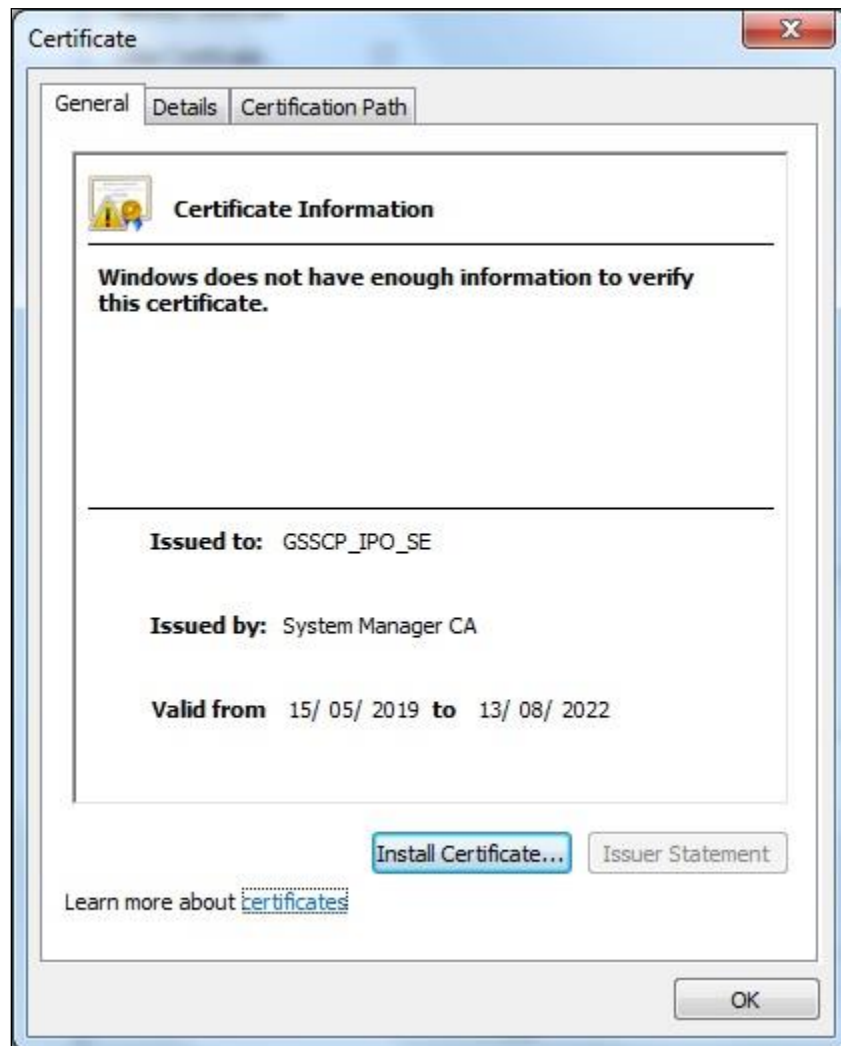
For the compliance test, TLS signalling was used internally to the enterprise wherever possible. Testing was done using identity certificates signed by a local certificate authority **System Manager CA**. The generation and installation of these certificates are beyond the scope of these Application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



6. Configure Avaya Session Border Controller for Enterprise

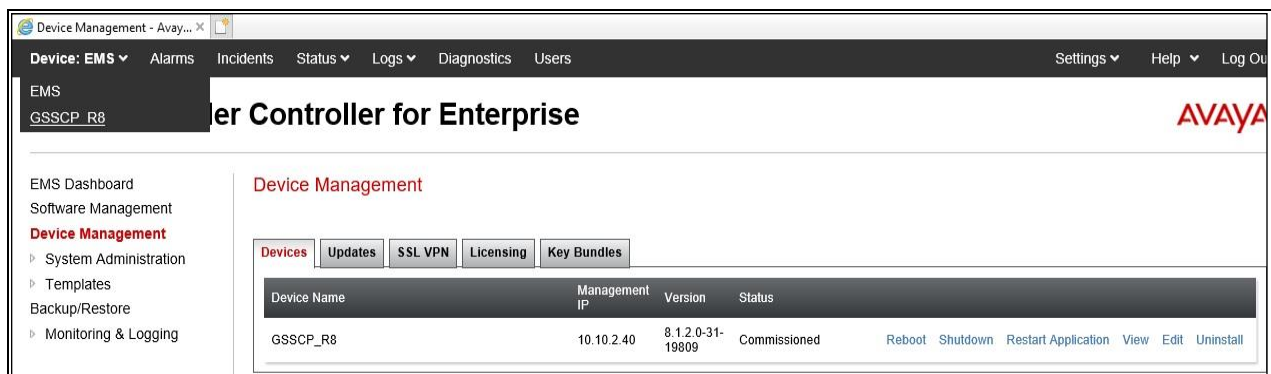
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP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

6.1. Accessing 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).

Device Management - Avaya... X

Device: GSSCP_R8 Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows
DMZ Services
Monitoring & Logging

Device Management

Devices Updates SSL VPN Licensing Key Bundles License Compliance

Device Name	Management IP	Version	Status	
GSSCP_R8	10.10.2.40	8.1.2.0-31-19809	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

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

System Information: GSSCP_R8 X

General Configuration

Appliance Name: GSSCP_R8

Box Type: SIP

Deployment Mode: Proxy

Device Configuration

HA Mode: No

Two Bypass Mode: No

License Allocation

Standard Sessions Requested: 0

Advanced Sessions Requested: 0

Scopia Video Sessions Requested: 0

CES Sessions Requested: 0

Transcoding Sessions Requested: 0

Premium Sessions Requested: 0

CLID: ---

Encryption Available: Yes ☒

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.10.4.35	10.10.4.35	255.255.255.0	10.10.4.1	A1
192.168.37.2	192.168.37.2	255.255.255.240	192.168.37.1	B1

DNS Configuration

Primary DNS: 8.8.8.8

Secondary DNS: 10.10.7.100

DNS Location: DMZ

DNS Client IP: 192.168.37.2

Management IP(s)

IP #1 (IPv4): 10.10.2.40

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' (192.168.37.1), 'Network Prefix or Subnet Mask' (255.255.255.240), 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 '192.168.37.2', 'Use IP Address', and 'Use Default'. A 'Delete' link is to the right of the first row. At the bottom is a 'Finish' button.

IP Address	Public IP	Gateway Override
192.168.37.2	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:

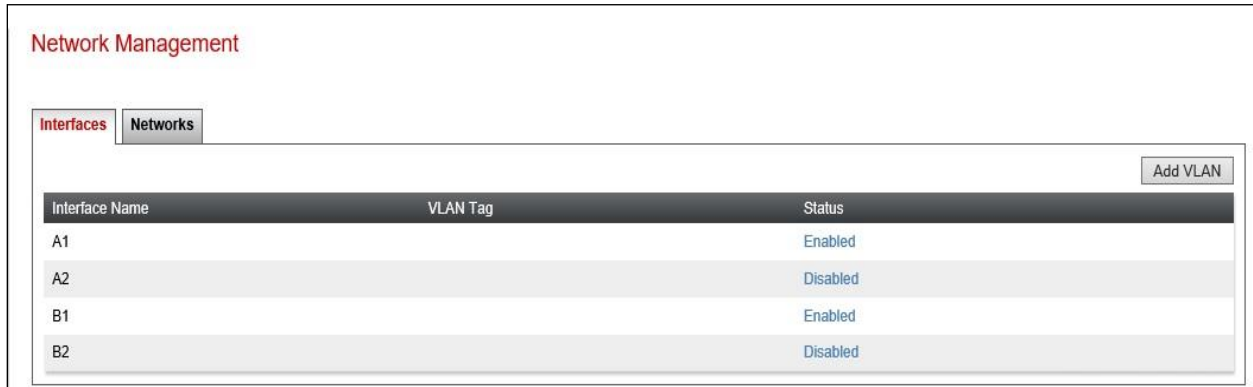
Network Management

Interfaces Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
A1_Internal	10.10.4.1	255.255.255.0	A1	10.10.4.35	Edit Delete
B1_External	192.168.37.1	255.255.255.240	B1	192.168.37.2	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.



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**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left is a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Certificates (selected), Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled "Certificates" and includes "Install" and "Generate CSR" buttons. It contains five sections: "Installed Certificates" with a table listing "asbce40int.pem" with "View" and "Delete" links; "Installed CA Certificates" with a table listing "SystemManagerCA.pem" with "View" and "Delete" links; "Installed Certificate Revocation Lists" with a message "No certificate revocation lists have been installed."; "Installed Certificate Signing Requests" with a message "No certificate signing requests have been installed."; and "Installed Keys" with a table listing "asbce40int.key" with a "Delete" link.

Installed Certificates	
asbce40int.pem	View Delete

Installed CA Certificates	
SystemManagerCA.pem	View Delete

No certificate revocation lists have been installed.

No certificate signing requests have been installed.

Installed Keys	
asbce40int.key	Delete

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).

The screenshot displays the 'Client Profiles: GSSCP_Client' configuration window. On the left, a sidebar shows 'Client Profiles' with 'GSSCP_Client' selected. The main area is divided into two sections. The top section, 'Client Profile', contains fields for 'Profile Name' (GSSCP_Client), 'Certificate' (asbce40int.pem), and 'SNI' (Enabled). Below this is the 'Certificate Verification' section, which includes 'Peer Verification' (Required), 'Peer Certificate Authorities' (SystemManagerCA.pem), 'Peer Certificate Revocation Lists' (---), 'Verification Depth' (1), and 'Extended Hostname Verification' (disabled). The bottom section, 'Renegotiation Parameters', shows 'Renegotiation Time' and 'Renegotiation Byte Count' both set to 0. The 'Handshake Options' section includes 'Version' (TLS 1.2, 1.1, and 1.0 checked), 'Ciphers' (Default selected), and 'Value' (HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH). An 'Edit' button is located at the bottom right of the configuration area.

Client Profile	
Profile Name	GSSCP_Client
Certificate	asbce40int.pem
SNI	<input checked="" 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

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 displays the configuration interface for a server profile named 'GSSCP_Server'. The interface is divided into two main sections. The top section, titled 'Server Profile', contains the following fields: 'Profile Name' (GSSCP_Server), 'Certificate' (asbce40int.pem), 'SNI Options' (None), 'Peer Verification' (Optional), 'Peer Certificate Authorities' (---), 'Peer Certificate Revocation Lists' (---), 'Verification Depth' (1), and 'Extended Hostname Verification' (unchecked). The bottom section, titled 'Renegotiation Parameters' and 'Handshake Options', contains the following fields: 'Renegotiation Time' (0), 'Renegotiation Byte Count' (0), 'Version' (checked for TLS 1.2, TLS 1.1, and TLS 1.0), 'Ciphers' (Default selected, FIPS and Custom unselected), and 'Value' (HIGH:DH:ADH:MD5:1aNULL:1eNULL:@STRENGTH). An 'Edit' button is located at the bottom right of the configuration area.

Server Profiles: GSSCP_Server	
Click here to add a description.	
Server Profile	
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:MD5:1aNULL:1eNULL:@STRENGTH

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 **IP Address**, select the **B1_external** signalling interface IP address defined in **Section 6.2**.
- Select **UDP** port number, **5060** is used for the Swisscom SIP trunk.
- Click **Finish**.

Signaling Interface						
Signaling Interface						
Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Ext	192.168.37.2 B1_External (B1, VLAN 0)	---	5060	---	None	Edit Delete
Sig_Int	10.10.4.35 A1_Internal (A1, VLAN 0)	---	---	5061	GSSCP_Server	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 **35000-40000**.
- 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	192.168.37.2 B1_External (B1, VLAN 0)	35000 - 40000	Edit Delete

6.5. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, Swisscom 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.

The screenshot shows the 'General' configuration tab for Server Interworking. It contains various settings for SIP call server capabilities. The 'Hold Support' is set to 'None'. The '180 Handling', '181 Handling', '182 Handling', and '183 Handling' are all set to 'None'. 'Refer Handling' is unchecked. 'URI Group' is set to 'None'. 'Send Hold', 'Delayed Offer', '3xx Handling', 'Diversion Header Support', 'Delayed SDP Handling', 'Re-Invite Handling', 'Prack Handling', and 'Allow 18X SDP' are all unchecked. 'T.38 Support' is checked. 'URI Scheme' is set to 'SIP'. 'Via Header Format' is set to 'RFC3261'.

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - s=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 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 – Swisscom

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 Swisscom and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- All other options on the **General** Tab can be left at default.

The screenshot shows the 'General' configuration tab for a server interworking profile. The settings are as follows:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - a=sendsonly
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 (dropdown menu)
Send Hold	<input type="checkbox"/>
Delayed Offer	<input 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"/> RFC3281 <input type="radio"/> RFC2543

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, Swisscom 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:

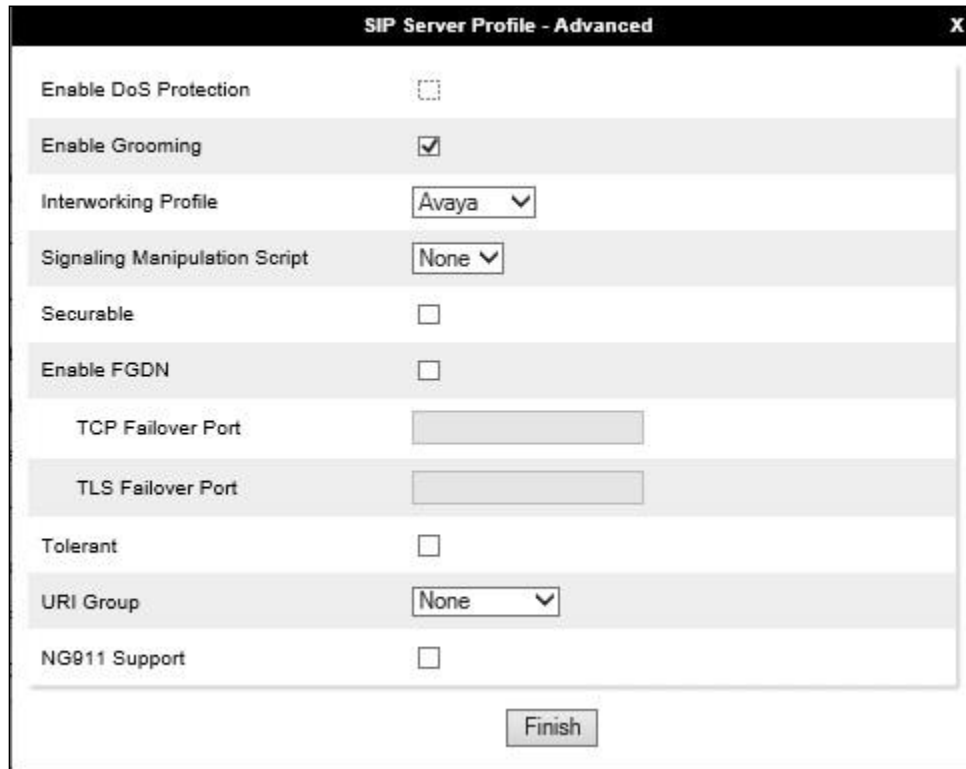
- Select **Server Type** to be **Call Server**.
- Select **TLS Client Profile** to be **GSSCP_Client** as defined in **Section 6.3.2**.
- Enter **IP Address / FQDN** to **10.10.4.140** (IP Office IP Address).
- For **Port**, enter **5061**.
- For **Transport**, select **TLS**.
- Click on **Next** (not 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'. The 'SIP Domain' field is empty. The 'DNS Query Type' is set to 'NONE/A'. The 'TLS Client Profile' is set to 'GSSCP_Client'. An 'Add' button is located to the right of these fields. Below the fields is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The first row contains the values '10.10.4.140', '5061', and 'TLS'. A 'Delete' button is located to the right of the first row.

IP Address / FQDN	Port	Transport
10.10.4.140	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, each with a label and a control element:

Setting	Value/Control
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya (dropdown menu)
Signaling Manipulation Script	None (dropdown menu)
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	(empty text field)
TLS Failover Port	(empty text field)
Tolerant	<input type="checkbox"/>
URI Group	None (dropdown menu)
NG911 Support	<input type="checkbox"/>

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

6.6.2. Server Configuration – Swisscom

To define the Swisscom 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 **192.168.110.16** (Swisscom SIP Network).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click on **Next** (not shown).

Edit SIP Server Profile - General

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

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
192.168.110.16	5060	UDP

Delete

In the new Authentication window that appears, enter the following values as Swisscom require authentication to connect to their network:

- **Enabled Authentication:** Checked
- **User Name:** Enter username provided by the Service Provider.
- **Realm:** Enter realm details provided by the Service Provider or leave blank to be detected by the server challenge.
- **Password** Enter password provided by the Service Provider.
- **Confirm Password** Re-enter password provided by the Service Provider.

Click **Next** to continue (not shown).



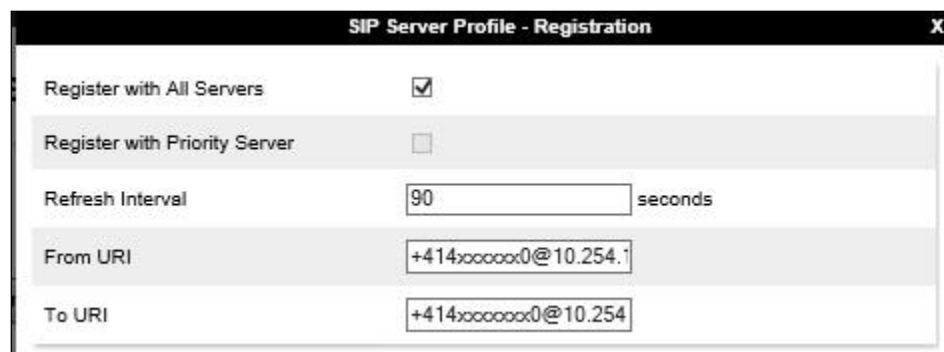
The screenshot shows a window titled "SIP Server Profile - Authentication". It contains the following fields and controls:

- Enable Authentication:** A checkbox that is checked.
- User Name:** A text input field containing "xxxxxx".
- Realm:** A text input field with the placeholder text "(Leave blank to detect from server challenge)".
- Password:** A text input field with the placeholder text "(Leave blank to keep existing password)".
- Confirm Password:** A text input field.

In the new Registration window that appears, enter the following values.

- **Register with Priority Server:** Check.
- **Refresh Interval** Choose the desired frequency in seconds the Avaya SBCE will send SIP REGISTERS.
- **From URI:** Enter an URI to be sent in the FROM header for SIP REGISTERS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP REGISTERS.

Click **Next** to continue (not shown).

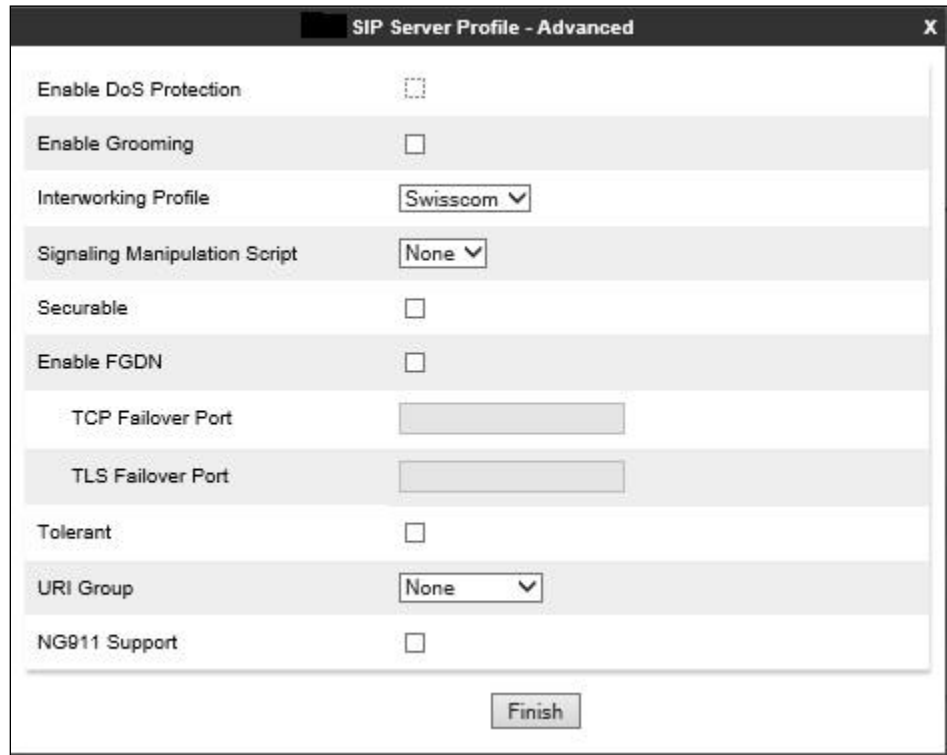


The screenshot shows a window titled "SIP Server Profile - Registration". It contains the following fields and controls:

- Register with All Servers:** A checkbox that is checked.
- Register with Priority Server:** A checkbox that is unchecked.
- Refresh Interval:** A text input field containing "90" followed by the label "seconds".
- From URI:** A text input field containing "+414xxxxxx0@10.254.1".
- To URI:** A text input field containing "+414xxxxxx0@10.254".

On the Advanced tab:

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



The screenshot shows a configuration window titled "SIP Server Profile - Advanced". It contains several settings, most of which are disabled (checkboxes are unchecked). The "Interworking Profile" is set to "Swisscom" via a dropdown menu. The "Signaling Manipulation Script" is set to "None" via a dropdown menu. The "URI Group" is also set to "None" via a dropdown menu. At the bottom right, there is a "Finish" button.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Swisscom ▼
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 ▼
NG911 Support	<input type="checkbox"/>

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 Swisscom 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

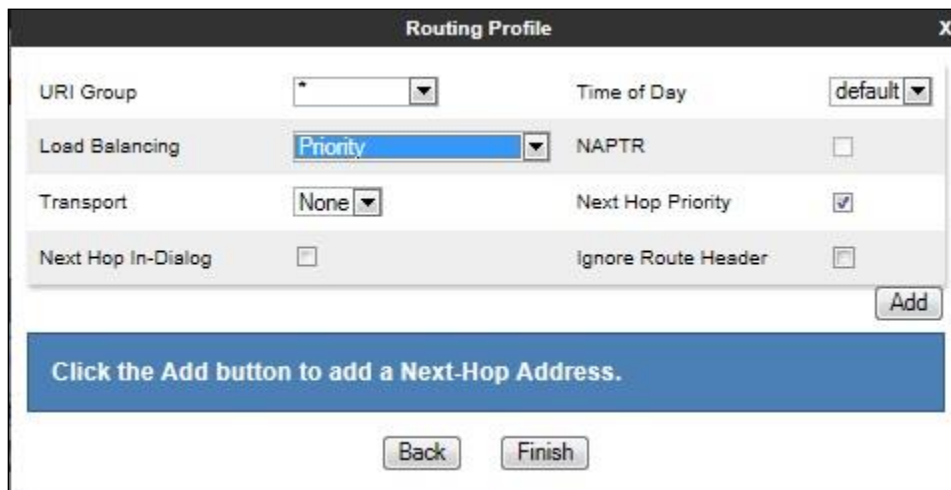
Create a Routing Profile for IP Office.

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



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "Avaya". Below the input field is a button labeled "Next".

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



The screenshot shows the "Routing Profile" window with various settings. The settings are as follows:

URI Group	Time of Day
*	default

Load Balancing	NAPTR
Priority	<input type="checkbox"/>

Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>

Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

At the bottom right of the settings area is an "Add" button. Below the settings area is a blue banner with the text "Click the Add button to add a Next-Hop Address." At the bottom of the window are 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 10.10.4.140:5061 (TLS)** from drop down menu.
- Click **Finish**.

6.7.2. Routing – Swisscom

Create a Routing Profile for Swisscom SIP network.

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

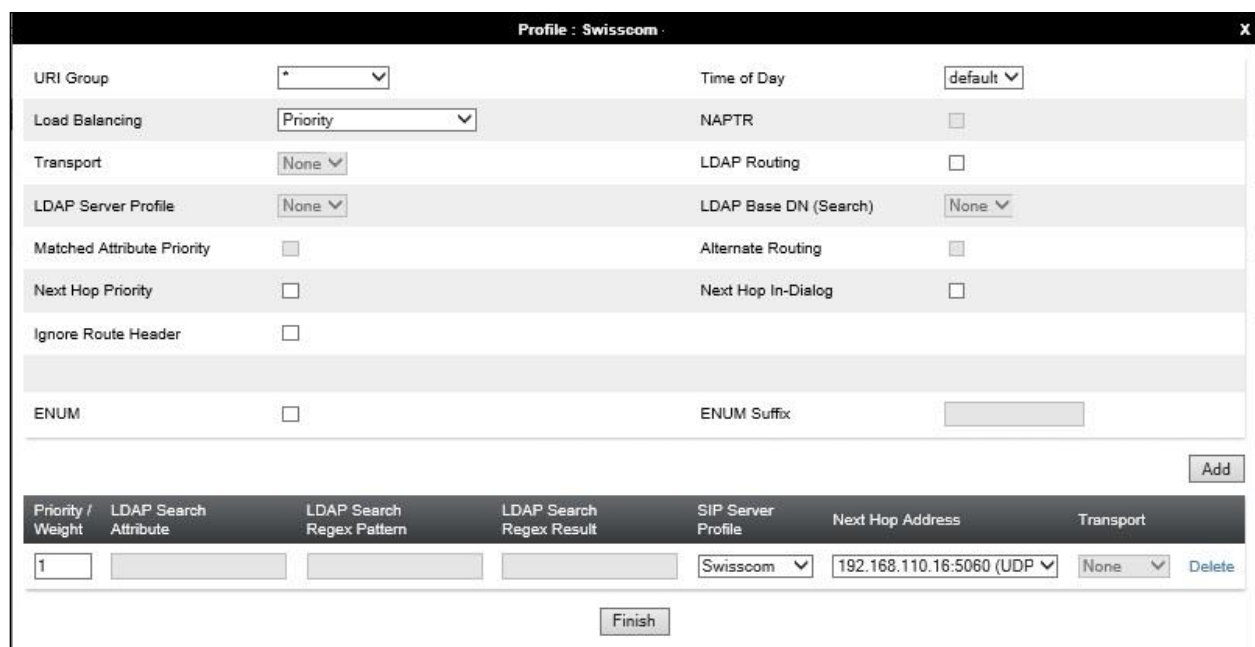
The Routing Profile window will open. Use the default values displayed and click **Add**.



The screenshot shows the 'Routing Profile' window. It contains several configuration fields: 'URI Group' (dropdown with '*'), 'Time of Day' (dropdown with 'default'), 'Load Balancing' (dropdown with 'Priority'), 'NAPTR' (checkbox), 'Transport' (dropdown with 'None'), 'Next Hop Priority' (checkbox checked), 'Next Hop In-Dialog' (checkbox), and 'Ignore Route Header' (checkbox). An 'Add' button is located at the bottom right. Below the form is a blue banner with the text 'Click the Add button to add a Next-Hop Address.' At the very bottom are 'Back' and 'Finish' buttons.

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

- **Priority/Weight = 1.**
- **SIP Server Profile = Swisscom** (Section 6.6.2) from drop down menu.
- **Next Hop Address = Select 192.168.110.16 (UDP)** from drop down menu.
- Click **Finish**.



The screenshot shows the 'Profile : Swisscom' window. It contains configuration fields for 'URI Group', 'Time of Day', 'Load Balancing', 'NAPTR', 'Transport', 'LDAP Server Profile', 'LDAP Base DN (Search)', 'Matched Attribute Priority', 'Alternate Routing', 'Next Hop Priority', 'Next Hop In-Dialog', 'Ignore Route Header', 'ENUM', and 'ENUM Suffix'. An 'Add' button is at the bottom right. Below the form is a table with the following columns: 'Priority / Weight', 'LDAP Search Attribute', 'LDAP Search Regex Pattern', 'LDAP Search Regex Result', 'SIP Server Profile', 'Next Hop Address', and 'Transport'. The table contains one row with the following values: '1', an empty field, an empty field, an empty field, 'Swisscom', '192.168.110.16:5060 (UDP)', and 'None'. A 'Delete' link is next to the last cell. At the bottom is a 'Finish' button.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				Swisscom	192.168.110.16:5060 (UDP)	None

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

Rename Clone Delete

Topology Hiding Profiles

default

cisco_th_profile

Avaya

Swisscom

Click here to add a description.

Topology Hiding

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

Edit

To define Topology Hiding for Swisscom, 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 Swisscom 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: Swisscom

Buttons: Add, Rename, Clone, Delete

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

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
To	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, Signalling, 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, media rules were created for both Avaya IP Office and Swisscom to use SRTP.

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 #2** 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 list of media 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 the following settings: 'Preferred Formats' set to 'SRTP_AES_CM_128_HMAC_SHA1_80' and 'RTP'; 'SRTP Context Reset on SSRC Change' with an unchecked checkbox; 'Encrypted RTCP' with an unchecked checkbox; 'MKI' with an unchecked checkbox; 'Lifetime' set to 'Any'; and 'Interworking' with an unchecked checkbox. The 'Video Encryption' section has 'Preferred Formats' set to 'RTP' and 'Interworking' with an unchecked checkbox.

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

The screenshot shows the 'Media Rules: default-low-med' configuration page. 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 a top bar with 'Add', 'Filter By Device...', and 'Clone' buttons. Below this is a warning: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' The configuration is divided into four tabs: 'Encryption' (selected), 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab contains sections for 'Audio Encryption' and 'Video Encryption'. Each section has 'Preferred Formats' set to 'RTP' and 'Interworking' checked. There is also a 'Miscellaneous' section with 'Capability Negotiation' unchecked. An 'Edit' button is at the bottom right.

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 signalling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the Swisscom 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' dialog box with a close button (X) in the top right corner. It contains five rows of configuration options, 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.

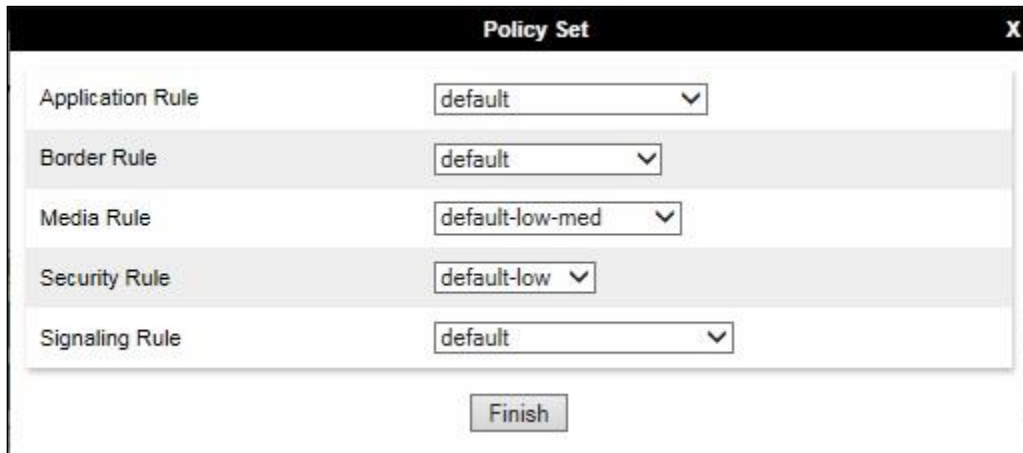
6.10.2. End Point Policy Group – Swisscom

For the compliance test, the end point policy group **Swisscom** was created for the Swisscom SIP trunk. Default values were used for each of the rules which comprise the group.

In the **Group Name** field enter a descriptive name, in this case **Swisscom** and click **Next** (not shown).

- Leave the **Application Rule**, **Border Rule**, **Media Rule**, **Security Rule** and **Signaling Rule** fields at their default values.

Click **Finish**.



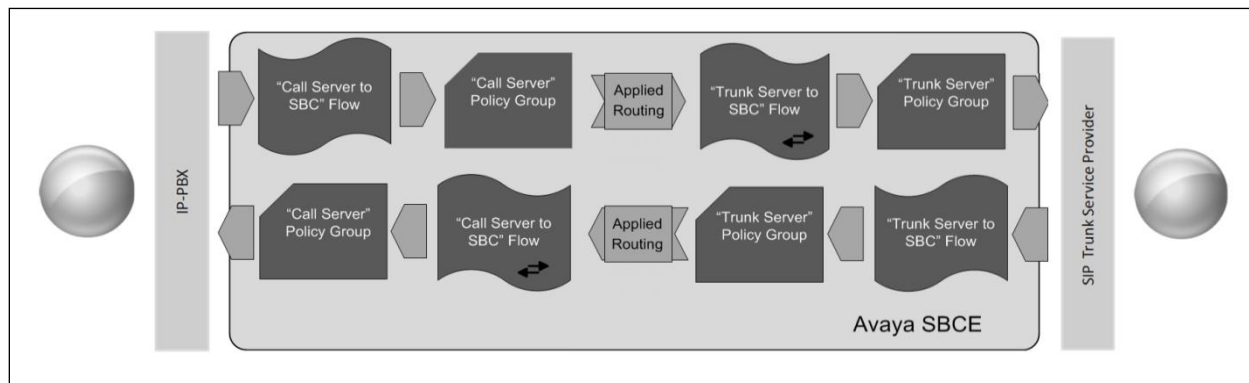
The screenshot shows a window titled "Policy Set" with a close button (X) in the top right corner. Inside the window, there are five rows, each with a rule name on the left and a dropdown menu on the right. The dropdown menus are set to the following values: "default" for Application Rule, "default" for Border Rule, "default-low-med" for Media Rule, "default-low" for Security Rule, and "default" for Signaling Rule. At the bottom center of the window is a button labeled "Finish".

Rule Name	Value
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 Swisscom's SIP Trunk and incoming flows from Swisscom'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 Swisscom 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.

Hover over a row to see its 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	Swisscom	View Clone Edit Delete

SIP Server: Swisscom

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 Swisscom 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 Swisscom SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Swisscom 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 Swisscom SIP Trunk defined in **Section 6.8** and click **Finish** (not shown).

The screenshot shows a configuration window titled "Flow: Trunk_Server" with a close button (X) in the top right corner. The window is divided into two main sections: "Criteria" and "Profile".

Criteria Section:

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

Profile Section:

Signaling Interface	Sig_Ext
Media Interface	Media_Ext
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	Swisscom
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 Swisscom 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 Swisscom 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).

The screenshot shows a configuration window titled "Flow: Call_Server" with a close button (X) in the top right corner. The window is divided into two main sections: "Criteria" on the left and "Profile" on the right. Each section contains a table of configuration parameters.

Criteria	
Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Ext

Profile	
Signaling Interface	Sig_Int
Media Interface	Media_Int
Secondary Media Interface	None
End Point Policy Group	Avaya
Routing Profile	Swisscom
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

7. Swisscom SIP Trunk Configuration

The configuration of the Swisscom equipment used to support Swisscom's SIP trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on Swisscom equipment and system configuration please contact an authorized Swisscom representative as per **Section 2.3**.

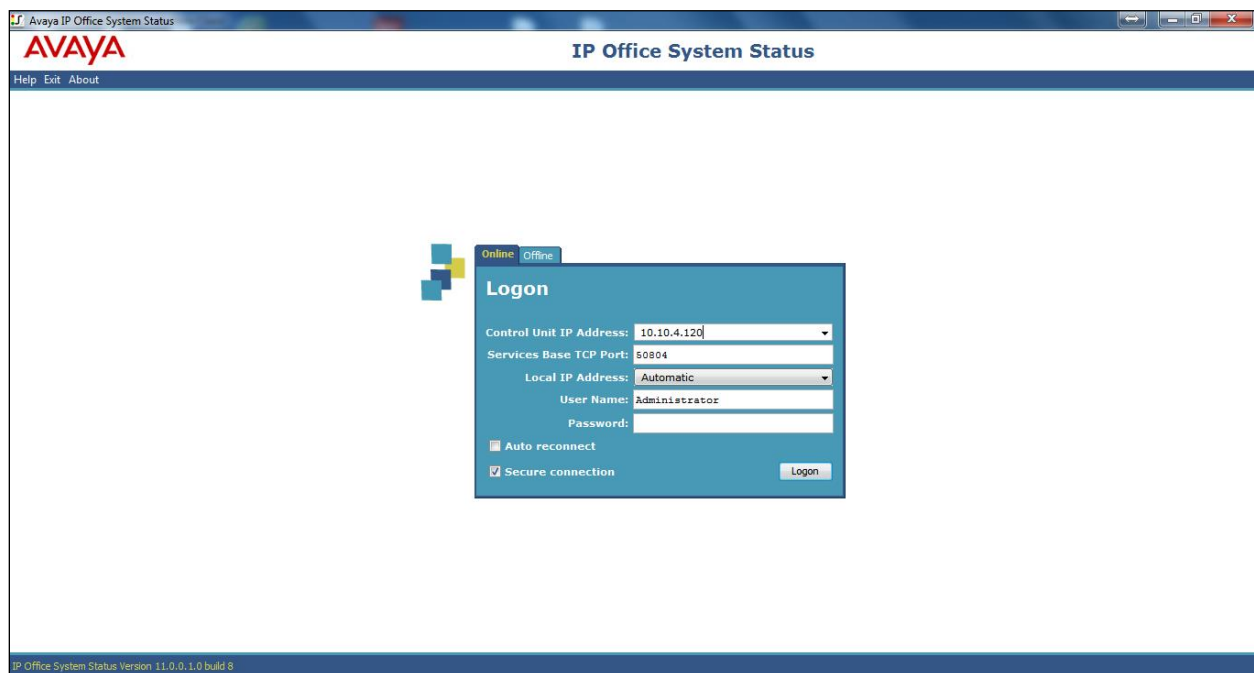
8. Verification Steps

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

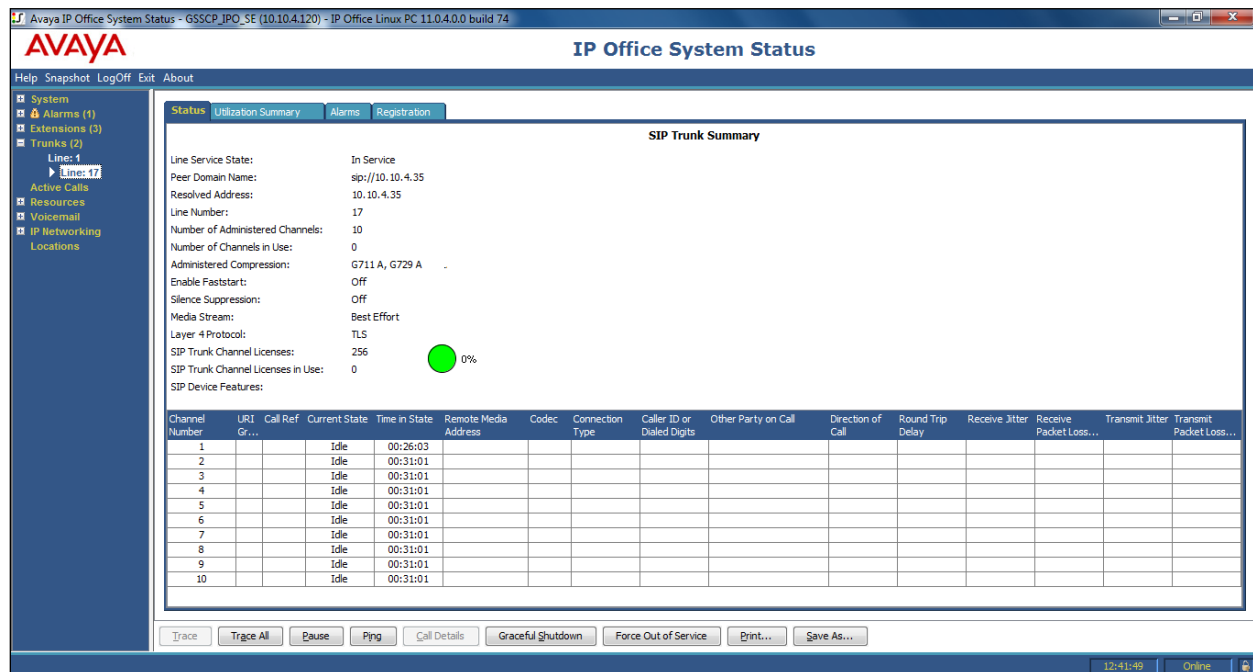
8.1. SIP Trunk status

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.

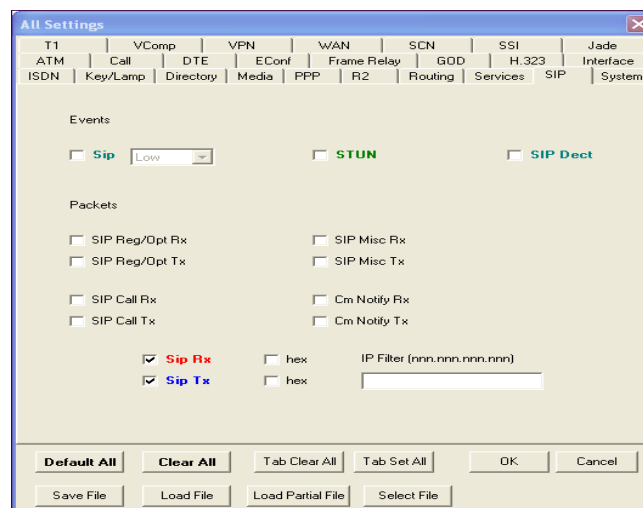


From the left-hand menu expand **Trunks** and choose the SIP trunk (**17** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational.



8.1.1. 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\...sysmonsettings.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)))] *****
336128686mS 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;pcp-line=2;lr;transport=tcp>
  Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
  Supported: replaces
  User-Agent: M0005/v.7.20A.158.056
  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 SipTCPUser-trunk SIP Line (17)
336128686mS Sip: SIPDialog f6e2cdd0 created, dialogs 1 txn_keys 1
336128686mS Sip: (f6e2cdd0) SetUnintTransactionCondition to Unint_None
336128686mS Sip: SipTCPUser 8430 has 1 dialog open (AttachDialogToSipTCPUser)
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;pcp-line=2;lr;transport=tcp>
  From: <sip:avaya.com>tag=1c1904606935
  To: <sip:avaya.com>tag=895d62b8d0f38743
  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=895d62b8d0f38743
  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
  
```

8.2. Avaya SBCE

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

8.2.1. Incidents

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

The screenshot shows the Avaya SBCE dashboard for device GSSCP_R8. The 'Device Management' section is active, displaying a table of device details.

Device Name	Management IP	Version	Status	Actions
GSSCP_R8	10.10.2.40	8.1.2.0-31-19809	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

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

Incident Viewer					
Device	All	Category	All	Clear Filters	Refresh
Displaying results 1 to 15 out of 2001.					
ID	Device	Date & Time	Category	Type	Cause
808935850202406	GSSCP_R8	Apr 8, 2021, 9:48:20 AM	Policy	Routing Failure	Timeout while contacting DNS servers voip.de
808935701001417	GSSCP_R8	Apr 8, 2021, 9:43:22 AM	Policy	Routing Failure	Timeout while contacting DNS servers voip.de
808935550301024	GSSCP_R8	Apr 8, 2021, 9:38:20 AM	Policy	Routing Failure	Timeout while contacting DNS servers voip.de
808900351634588	GSSCP_R8	Apr 7, 2021, 2:05:03 PM	Policy	Server Registration	Registration Failed, Server is Down
808634079618563	GSSCP_R8	Apr 1, 2021, 10:09:19 AM	Media Anomaly Detection	Media Type Unsupported	Media Not Acceptable
808633992019632	GSSCP_R8	Apr 1, 2021, 10:06:24 AM	Media Anomaly Detection	Media Type Unsupported	Media Not Acceptable
808633926635990	GSSCP_R8	Apr 1, 2021, 10:04:13 AM	Media Anomaly Detection	Media Type Unsupported	Media Not Acceptable

8.2.2. 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 ▾ : <input type="text"/>
Remote Address *, *:Port, IP, IP:Port	<input type="text" value="*"/>
Protocol	All ▾
Maximum Number of Packets to Capture	<input type="text" value="1000"/>
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	<input type="text" value="test.pcap"/>

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

Trace: GSSCP_R8

Packet Capture | **Captures**

File Name	File Size (bytes)	Last Modified	
test_20210408095534.pcap	12,288	April 8, 2021 at 9:55:56 AM IST	Delete

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 Swisscom network.

9. Conclusion

These Application Notes demonstrated how IP Office Server Edition R11.1 and Avaya Session Border Controller for Enterprise R8.1 can be successfully combined with Swisscom Smart Business Connect 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 Swisscom Smart Business Connect. 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 with Swisscom Smart Business Connect thus eliminating the costs of analog 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, Mar 2021.
- [2] *Avaya IP Office™ Platform Server Edition Reference Configuration*, Release 11.1, Mar 2021.
- [3] *Deploying IP Office™ Platform Server Edition Solution*, Release 11.1, Mar 2021.
- [4] *IP Office™ Platform 11.1, Deploying IP Office Essential Edition*, Mar 2021.
- [5] *IP Office™ Platform 11.1 Installing and Maintaining the Avaya IP Office™ Platform Application Server*, Mar 2021.
- [6] *Administering Avaya IP Office™ Platform with Web Manager*, Release 11.1, Mar 2021.
- [7] *Administering Avaya IP Office™ Platform with Manager*, Release 11.1, Mar 2021.
- [8] *IP Office™ Platform 11.1 Using Avaya IP Office™ Platform System Status*, Mar 2021.
- [9] *IP Office™ Platform 11.1 Using IP Office System Monitor*, Mar 2021.
- [10] *Using Avaya Workplace Client for Windows on IP Office*, Feb 2021.
- [11] *IP Office™ Platform 11.1 - Third-Party SIP Extension Installation Notes*, Mar 2021.
- [12] *Avaya IP Office Knowledgebase*, <http://marketingtools.avaya.com/knowledgebase>
- [13] *Deploying Avaya Session Border Controller for Enterprise Release 8.1*, Dec 2020.
- [14] *Upgrading Avaya Session Border Controller for Enterprise Release 8.1*, Dec 2020.
- [15] *Administering Avaya Session Border Controller for Enterprise Release 8.1*, Dec 2020.
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2021 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.