



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.0 with Avaya Session Border Controller for Enterprise Release 7.2.2 to support Swisscom Enterprise SIP Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya IP Office R11.0 and Avaya Session Border Controller for Enterprise R7.2.2 to support Swisscom Enterprise SIP Service.

The Swisscom Enterprise SIP service provides PSTN access via a SIP trunk connected to the Swisscom Voice Over Internet Protocol (VoIP) network as an alternative to legacy Analogue 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 the Swisscom SIP Trunk (Enterprise SIP) and Avaya IP Office R11.0 and Avaya Session Border Controller for Enterprise R7.2.2.

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 Enterprise SIP service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

Customers using this Avaya SIP-enabled enterprise solution with Swisscom's SIP Trunk are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office and Avaya SBCE to connect to the Swisscom 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 the testing associated with this Application Note, the interface between Avaya systems and the Swisscom Enterprise SIP Trunk do not include use of any specific encryption features. Encryption (TLS/SRTP) was used internal 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 calls to the enterprise site from PSTN phones using the Swisscom Enterprise SIP Service, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the Swisscom Enterprise SIP Service to PSTN destinations, calls made from SIP and H.323 telephones.
- Calls using the G.711A and G.729 codecs.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using G.711 fax transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail for inbound and outbound calls.
- Inbound and outbound PSTN calls to/from Avaya Equinox Softphone client.
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, transfer, and conference.
- Call transfer to PSTN.
- Off-net call forwarding and mobile twinning.

2.2. Test Results

Interoperability testing of the 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 Queuing 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 Enterprise SIP service.
- The Privacy Header 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). This is a known issue currently under investigation. As a workaround, the anonymous button can be enabled on the SIP tab in **Section 5.8** to restrict CLIR.

- Off-net call forwarding was tested successfully, but the original calling party number was not sent to the forwarded PSTN phone. This is a known issue with IP Office R11 that is currently under investigation.
- 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: ent.incident-voice@swisscom.com.

3. Reference Configuration

Figure 1 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 an Avaya 1600 Series IP Telephone (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware), an Avaya 1140e SIP Telephone, an Avaya Analogue 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 Equinox for Windows for mobility 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.

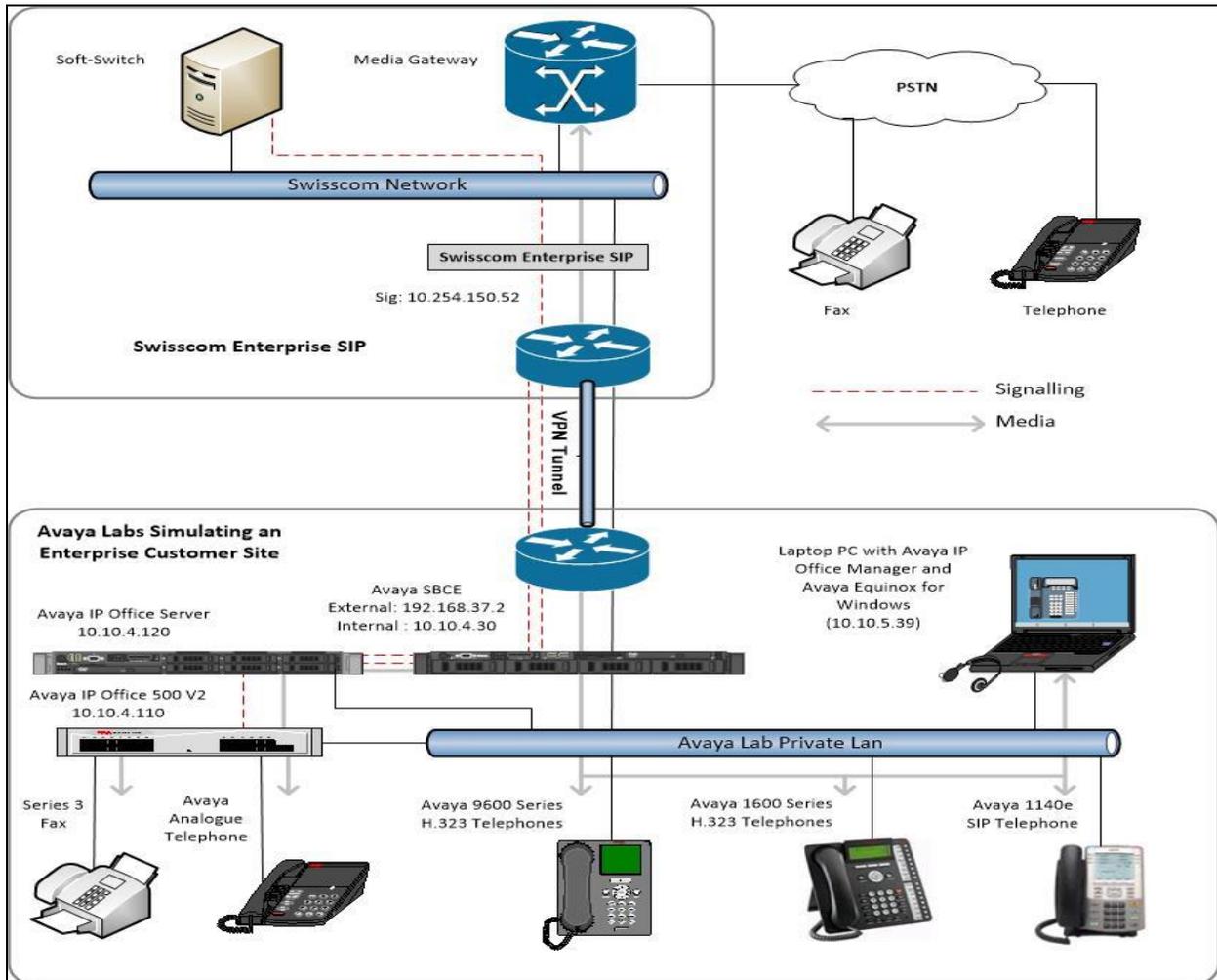


Figure 1: Test setup Swisscom Enterprise SIP to simulated Avaya Enterprise

4. Equipment and Software Validated

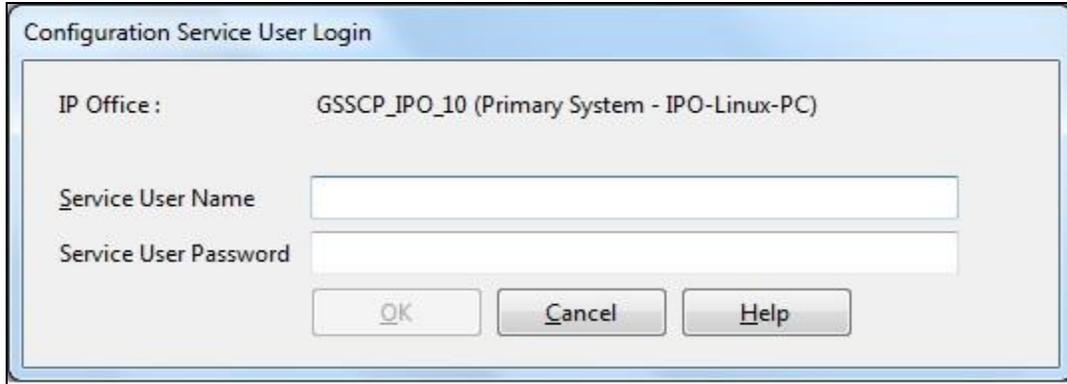
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	Version 11.0.0.1.0 build 8
Avaya IP Office 500 V2	Version 11.0.0.1.0 build 8
Avaya Voicemail Pro Client	Version 11.0.200.1
Avaya IP Office Manager	Version 11.0.0.1.0 build 8
Avaya Session Border Controller for Enterprise	7.2.2.1-04-16104
Avaya 1608 Phone (H.323)	1.3.12
Avaya 9611G Series Phone (H.323)	6.6.0
Avaya 9608 Series Phone (H.323)	6.6.0
Avaya Communicator for Equinox (SIP)	3.3.1.60
Avaya 1140e (SIP)	FW: 04.04.30.00.bin
Avaya 98390 Analogue Phone	N/A
Swisscom	
eSBC	Cisco 897VA 15.5 (3) M6a
C-SBC	ACME Net-Net 6300 Firmware 7.4.0 MR 1 P 5
SESM	Genband MCP_19.0.20.9_2018-08-03-0638

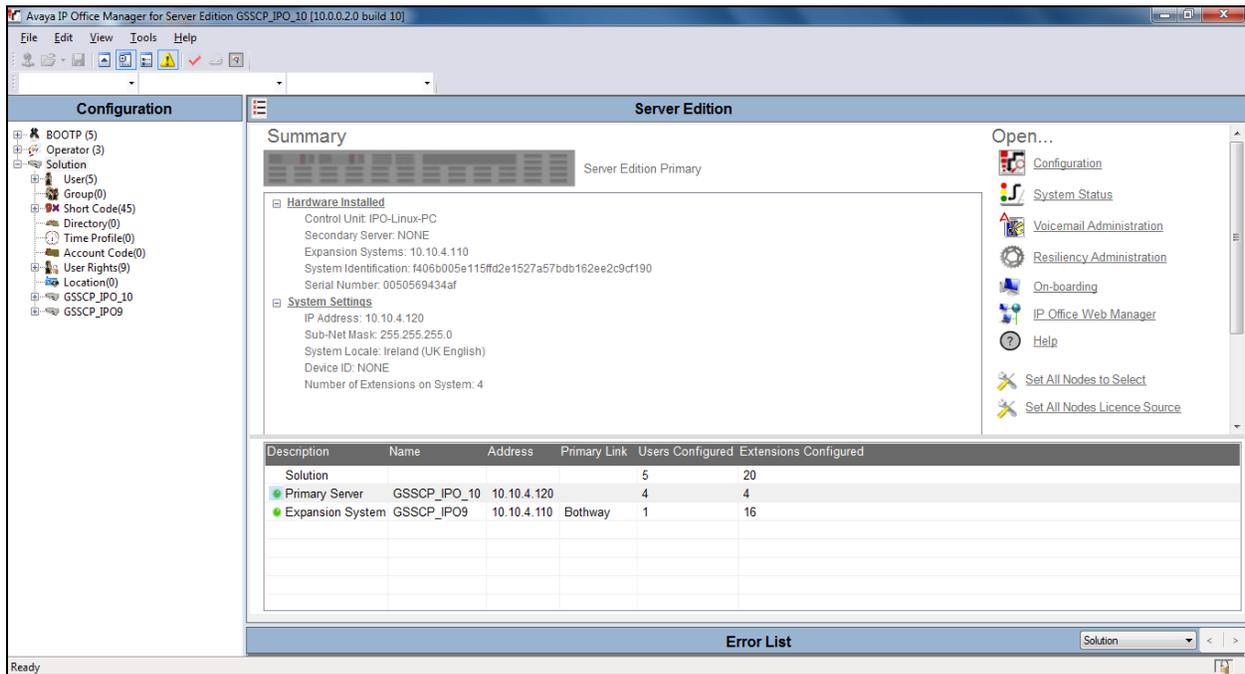
Note – Testing was performed with IP Office Server Edition with 500 V2 Expansion R11.0. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. **Note:** that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analogue 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 Enterprise SIP 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 appropriate Avaya IP Office system from the pop-up window and log in with the appropriate credentials.



A management window will appear similar to the one in the next section. All the Avaya IP Office configurable components are shown in the left pane known as the Navigation Pane. The pane on the right is the Details Pane. These panes will be referenced throughout the Avaya IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the Service Provider is assumed to already be in place.



5.1. Verify System Capacity

Navigate to **License** → **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.

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

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 from 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_10** in the Navigation Pane where GSSCP_IPO_10 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 displays the configuration page for GSSCP_IPO_10. The 'LAN1' tab is selected, and the 'LAN Settings' sub-tab is active. The 'IP Address' field is set to 10.10.4.120 and the 'IP Mask' field is set to 255.255.255.0. The 'Number Of DHCP IP Addresses' is set to 134. 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).

GSSCP_IPO_10

System | **LAN1** | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | VoIP | VoIP Security | Contact Center

LAN Settings | VoIP | Network Topology

H323 Gatekeeper Enable

Auto-create Extn Auto-create User H323 Remote Extn Enable

H.323 Signalling over TLS: Preferred Remote Call Signalling Port: 1720

SIP Trunks Enable

SIP Registrar Enable

Auto-create Extn/User SIP Remote Extn Enable

SIP Domain Name: avaya.com

SIP Registrar FQDN: avaya.com

Layer 4 Protocol:

- UDP UDP Port: 5060 Remote UDP Port: 5060
- TCP TCP Port: 5060 Remote TCP Port: 5060
- TLS TLS Port: 5061 Remote TLS Port: 5061

Challenge Expiry Time (secs): 10

RTP

Port Number Range

Minimum: 49152 Maximum: 53246

Port Number Range (NAT)

Minimum: 49152 Maximum: 53246

Enable RTCP Monitoring on Port 5005

RTCP collector IP address for phones: 0 . 0 . 0 . 0

Keepalives

Scope: RTP-RTCP Periodic timeout: 30

Initial keepalives: Enabled

DiffServ Settings

B8 DSCP (Hex) B8 Video DSCP (Hex) FC DSCP Mask (Hex) 88 SIG DSCP (Hex)

46 DSCP 46 Video DSCP 63 DSCP Mask 34 SIG DSCP

On the **Network Topology** tab, set the **Firewall/NAT Type** from the pulldown menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used as NAT was not required for this configuration, therefore resulting in no requirement for a STUN server. The **Use Network Topology Info** in the **SIP Line** was set to **None** in **Section 5.6.2**. Set **Binding Refresh Time (seconds)** to **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 configuration window for GSSCP_IPO_10. The 'Network Topology' tab is active. Under 'Network Topology Discovery', the 'Firewall/NAT Type' is set to 'Open Internet'. The 'Binding Refresh Time (seconds)' is set to 30. The 'Public IP Address' is set to 0.0.0.0. The 'STUN Port' is set to 3478. There are 'Run STUN' and 'Cancel' buttons. A 'Public Port' section contains UDP, TCP, and TLS ports, all set to 0. A checkbox for 'Run STUN on startup' is present at the bottom.

5.3. System Telephony Settings

Navigate to the **Telephony** → **Telephony** tab on the Details Pane. Choose the **Companding Law** typical for the enterprise location. For Europe, **ALAW** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the Service Provider across the SIP trunk. On completion, click the **OK** button (not shown).

The screenshot displays the configuration interface for GSSCP_IPO_10, specifically the Telephony settings. The interface is divided into several sections:

- System Navigation:** Includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony (selected), Directory Services, System Events, SMTP, SMDR, VoIP, VoIP Security, and Contact Center.
- Telephony Sub-tabs:** Includes Telephony (selected), Park & Page, Tones & Music, Ring Tones, SM, Call Log, and TUI.
- Configuration Parameters:**
 - Dial Delay Time (secs): 1
 - Dial Delay Count: 4
 - Default No Answer Time (secs): 15
 - Hold Timeout (secs): 0
 - Park Timeout (secs): 300
 - Ring Delay (secs): 5
 - Call Priority Promotion Time (secs): Disabled
 - Default Currency: EUR
 - Default Name Priority: Favour Trunk
 - Media Connection Preservation: Enabled
 - Phone Failback: Automatic
- Companding Law:**
 - Switch:** Radio buttons for U-Law and A-Law (selected).
 - Line:** Radio buttons for U-Law Line and A-Law Line (selected).
- Additional Settings:**
 - Login Code Complexity:** Enforced (checked), Minimum length: 4, Complexity (checked).
 - Other Options:** DSS Status (unchecked), Auto Hold (checked), Dial By Name (checked), Show Account Code (checked), Inhibit Off-Switch Forward/Transfer (unchecked), Restrict Network Interconnect (unchecked), Include location specific information (unchecked), Drop External Only Impromptu Conference (checked), Visually Differentiate External Call (unchecked), High Quality Conferencing (checked).

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 and **G.729(a) 8K CS-ACELP** set as the secondary codec as per screenshot below.

GSSCP_IPO_10*

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | **VoIP** | VoIP Security | Contact Center

Ignore DTMF Mismatch For Phones

Allow Direct Media Within NAT Location

RFC2833 Default Payload: 101

Available Codecs

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

Default Codec Selection

Unused

- G.711 ULAW 64K
- G.722 64K

Selected

- G.711 ALAW 64K
- G.729(a) 8K CS-ACELP

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** and **SRTP_AES_CM_128_SHA1_32** for **Crypto Suites**.
- Other parameters are left as default.
- Click **OK**.

The screenshot shows the configuration interface for VoIP Security on a system named GSSCP_IPO_10*. The interface has a top navigation bar with tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and VoIP Security. The VoIP Security tab is active. Below the navigation bar, there is a 'Media' dropdown menu set to 'Preferred' and a 'Strict SIPs' checkbox which is unchecked. A 'Media Security Options' section contains several settings: 'Encryptions' with 'RTP' checked and 'RTCP' unchecked; 'Authentication' with 'RTP' and 'RTCP' both checked; 'Replay Protection' with 'SRTP Window Size' set to '64'; and 'Crypto Suites' with 'SRTP_AES_CM_128_SHA1_80' and 'SRTP_AES_CM_128_SHA1_32' both checked.

5.6. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Swisscom Enterprise SIP 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:

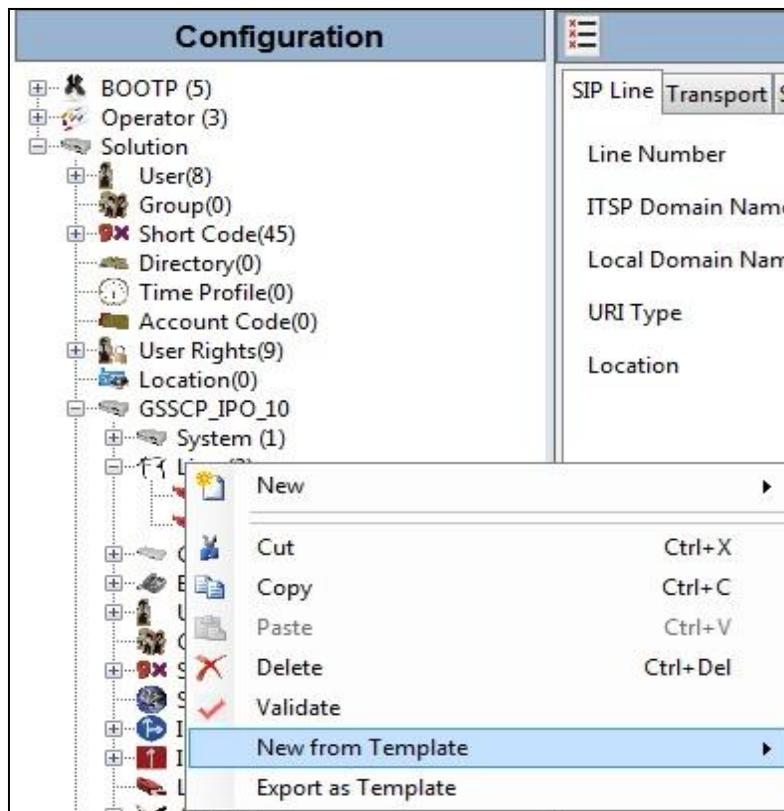
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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**.

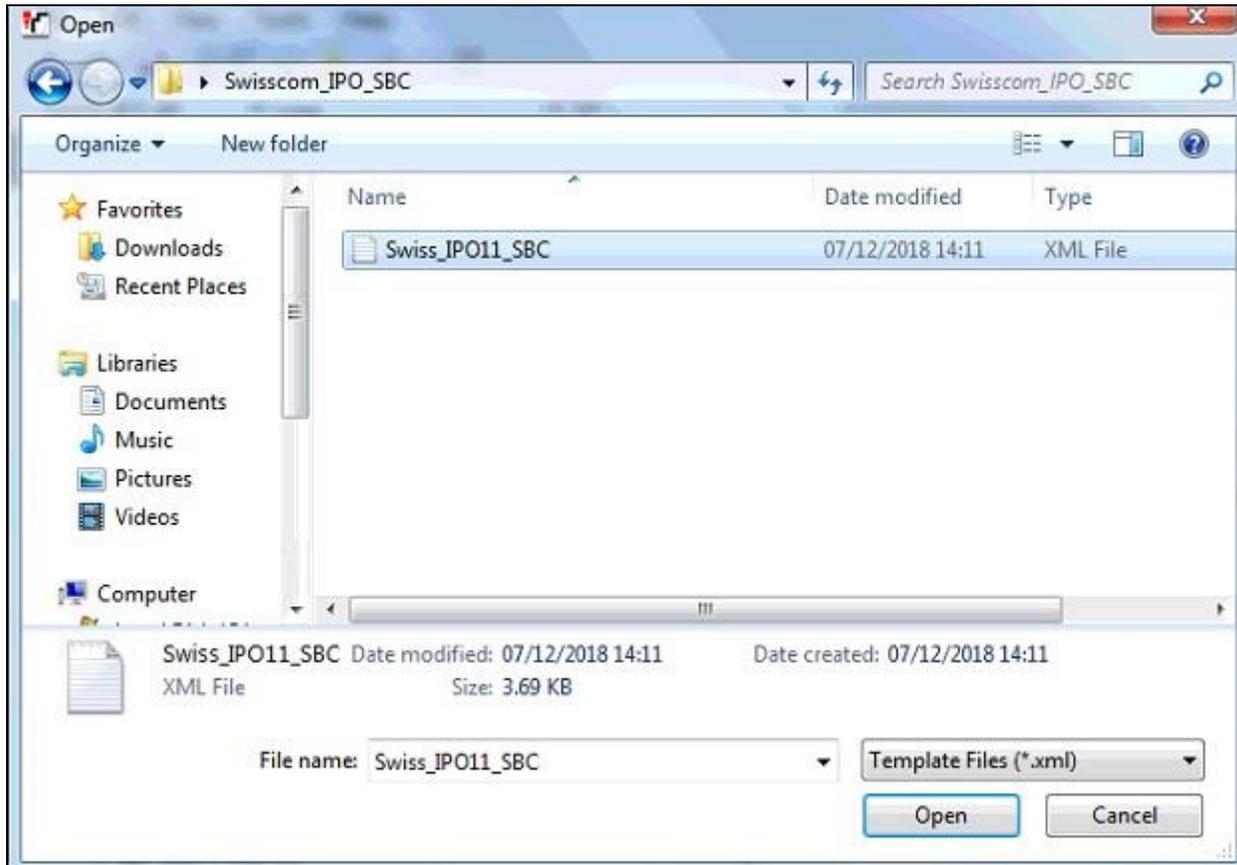
5.6.1. SIP Line From Template

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.



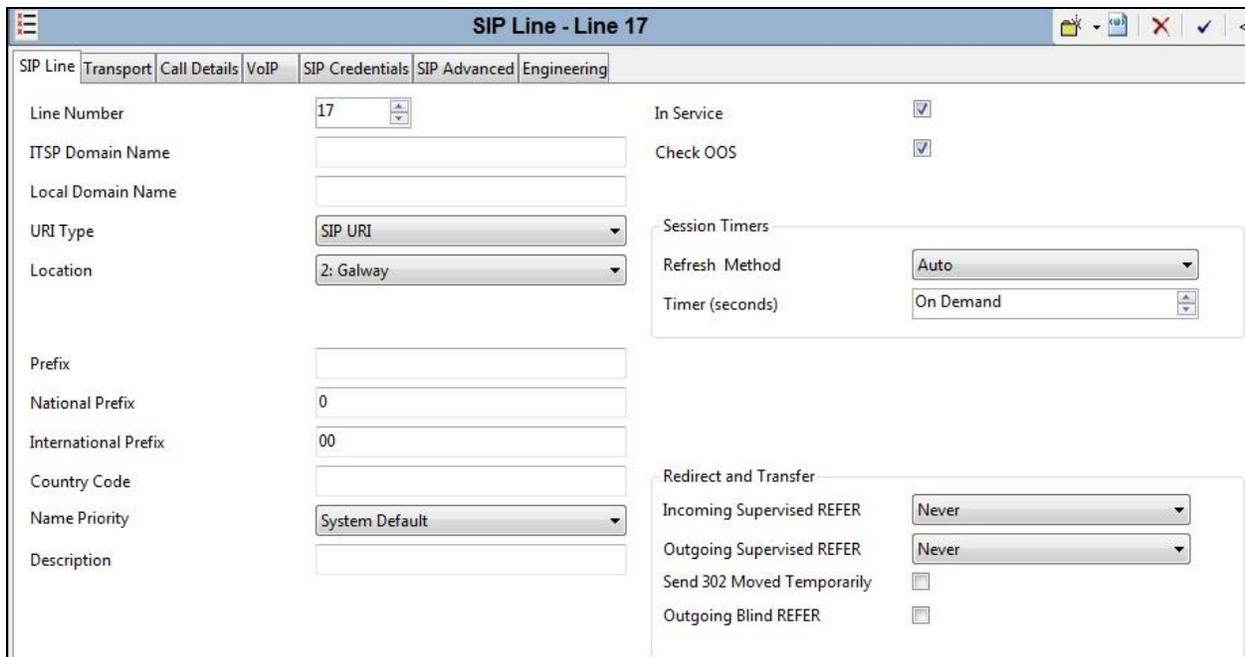
The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.6.2**.

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 5.10**.
- Set **National Prefix** to **0** and **International Prefix** to **00** for number conversion as follows: outbound national and international called party numbers are converted to E.164 format; inbound national and international calling party numbers are converted to diallable format.
- Ensure the **In Service** box is checked.
- Ensure the **Check OSS** box is checked.
- Leave the **Refresh Method** at the default value of **Auto** 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 Enterprise SIP.
- Default values may be used for all other parameters.

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



SIP Line - Line 17	
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 OSS	<input checked="" type="checkbox"/>
Session Timers	
Refresh Method	Auto
Timer (seconds)	On Demand
Redirect and Transfer	
Incoming Supervised REFER	Never
Outgoing Supervised REFER	Never
Send 302 Moved Temporarily	<input type="checkbox"/>
Outgoing Blind REFER	<input type="checkbox"/>

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

- Set **ITSP Proxy Address** to the inside interface IP address (**10.10.4.30**) 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 '10.10.4.30'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'TLS', 'Send Port' is '5061', and 'Use Network Topology Info' is set to 'None'. 'Listen Port' is also '5061'. 'Explicit DNS Server(s)' are both '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**.

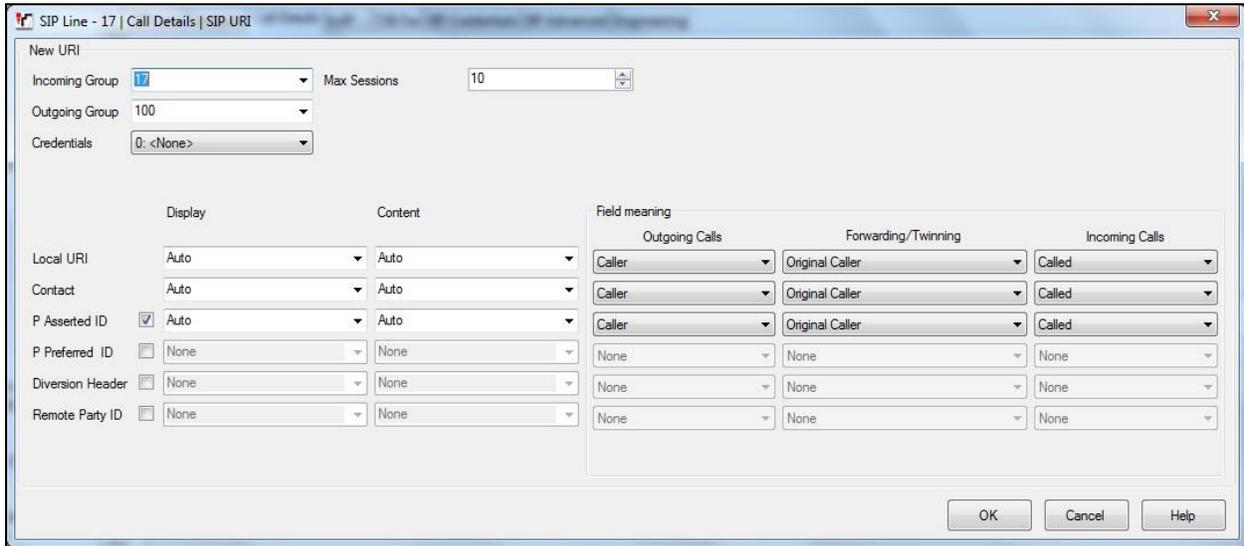
The screenshot shows the 'SIP Line - Line 17*' configuration window with the 'Call Details' tab selected. The 'SIP URIs' section is visible, showing a table with columns: URI, Groups, Credential, Local URI, Contact, P Asserted ID, P Preferred ID, Diversion Header, and Remote Party ID. To the right of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

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.

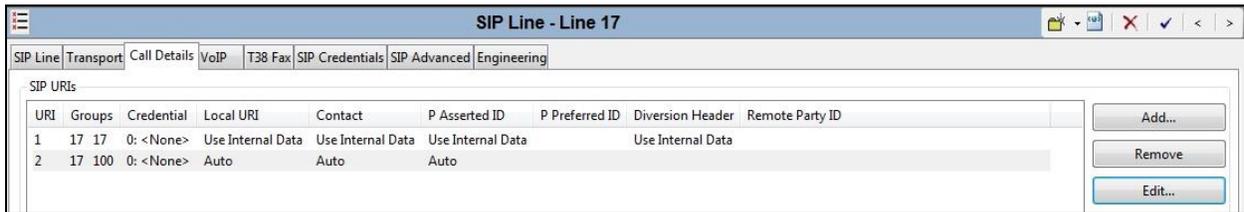
- Set **Incoming Group**. This is the value assigned for incoming calls that's analysed in the Incoming Call Route settings described in **Section 5.9**. In the test environment a value of **17** was used for the Swisscom Enterprise SIP service.
- Set **Outgoing Group**. This is the value assigned for outgoing calls that can be selected directly in the short code settings described in **Section 5.7**. In the test environment a value of **17** was used.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern
- Set **Local URI, Contact, P Asserted ID** and **Diversion Header** to **Use Internal Data** for both the **Display** name and **Content**. On incoming calls, this will analyse the Request-Line sent by 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. This ensures that the original called party number is sent for forwarded calls, though this is not currently working as described in **Section 2.2**.

	Display	Content	Field meaning		
			Outgoing Calls	Forwarding/Twinning	Incoming Calls
Local URI	Use Internal Data	Use Internal Data	Caller	Original Caller	Called
Contact	Use Internal Data	Use Internal Data	Caller	Original Caller	Called
P Asserted ID	<input checked="" type="checkbox"/> Use Internal Data	Use Internal Data	Caller	Original Caller	Called
P Preferred ID	<input type="checkbox"/> None	None	None	None	None
Diversion Header	<input checked="" type="checkbox"/> Use Internal Data	Use Internal Data	Caller	Original Caller	None
Remote Party ID	<input type="checkbox"/> None	None	None	None	None

Note: If required a SIP URI can be created for calls to services such as the Mobile Twinning FNE: The numbers used for these services may not be associated with a User so the incoming calls would not match the SIP settings in the User profile as described in **Section 5.8**. In order to match the incoming calls with a SIP URI, the Local URI can be set either to **Auto** which will match any number, or to the specific number used for the service. As this SIP URI would be used for incoming calls only, the **Outgoing Group** is set to an unused value, for example **100**. The following screenshot shows an example:



The following screenshot shows the completed configuration:



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

- Select **System Default** from the drop-down menu as system default codecs were already defined in **Section 5.4**.
- Set the **Fax Transport Support** box to **G.711** as this is the preferred method of fax transmission for 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 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 configuration interface for SIP Line - Line 17, specifically the VoIP tab. The interface includes several sections:

- Codec Selection:** A dropdown menu is set to "System Default". Below it are two columns: "Unused" containing "G.711 ULAW 64K" and "G.722 64K", and "Selected" containing "G.711 ALAW 64K" and "G.729(a) 8K CS-ACELP". Navigation buttons (right arrow, up arrow, down arrow, left arrow, and right arrow) are positioned between the columns.
- Local Hold Music:** A checked checkbox.
- Re-invite Supported:** A checked checkbox.
- Codec Lockdown:** An unchecked checkbox.
- Allow Direct Media Path:** An unchecked checkbox.
- Force direct media with phones:** An unchecked checkbox.
- PRACK/100rel Supported:** A checked checkbox.
- Fax Transport Support:** A dropdown menu set to "G.711".
- DTMF Support:** A dropdown menu set to "RFC2833/RFC4733".
- Media Security:** A dropdown menu set to "Same as System (Disabled)".

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

- Check the **Add user=phone** box to send SIP parameter user with the value phone to the From and To Headers in outgoing calls.
- Check the **Use + for International** as E.164 numbering is used on the SIP Trunk.
- 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 configuration window for 'SIP Line - Line 17*'. The 'SIP Advanced' tab is selected. The configuration is divided into several sections:

- Addressing:** Association Method is set to 'By Source IP address' and Call Routing Method is set to 'Request URI'. Suppress DNS SRV Lookups is unchecked.
- Identity:** Use "phone-context" is unchecked. Add user=phone is checked. Use + for International is checked. Use PAI for Privacy, Use Domain for PAI, Caller ID from From header, and Send From In Clear are unchecked. Cache Auth Credentials is checked. User-Agent and Server Headers is empty. Send Location Info is set to 'Emergency Calls'. Add UII header and Add UII header to redirected calls are unchecked.
- Media:** Allow Empty INVITE, Send Empty re-INVITE, and Allow To Tag Change are unchecked. P-Early-Media Support is set to 'None'. Send SilenceSupp=Off is unchecked. Force Early Direct Media is unchecked. Media Connection Preservation is set to 'Disabled'. Indicate HOLD is unchecked.
- Call Control:** Call Initiation Timeout (s) is 4. Call Queuing Timeout (m) is 5. Service Busy Response is set to '486 - Busy Here'. on No User Responding Send is set to '408-Request Timeout'. Action on CAC Location Limit is set to 'Allow Voicemail'. Suppress Q.850 Reason Header and Emulate NOTIFY for REFER are unchecked.

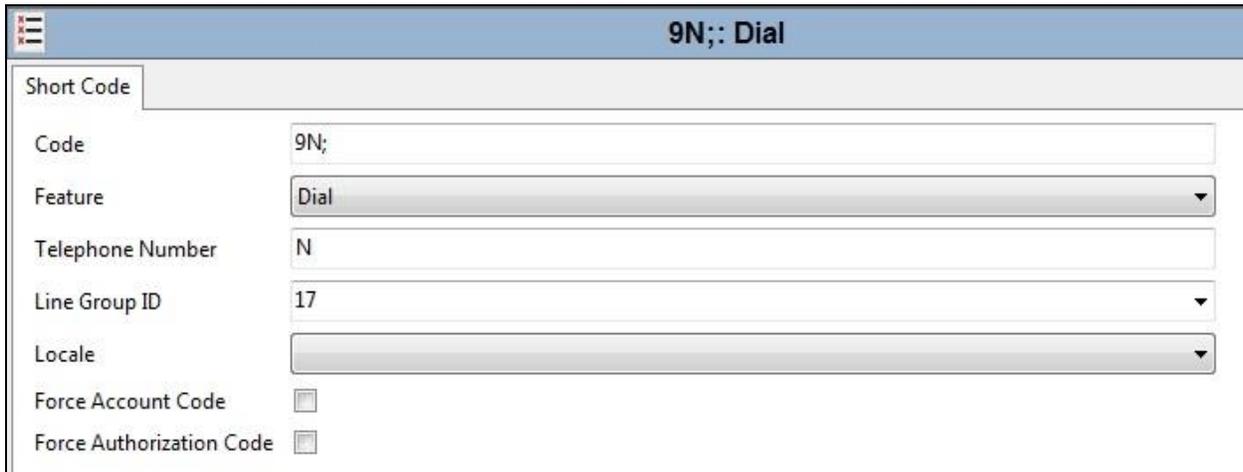
Note: It is advisable at this stage to save the configuration as described in **Section 5.12**.

5.7. ShortCodes

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**.

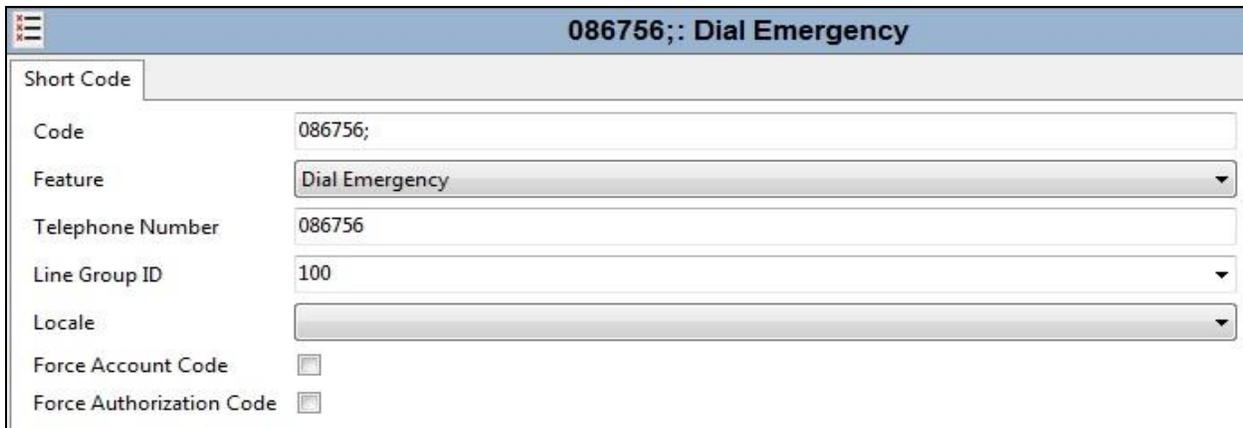
On completion, click the **OK** button (not shown).



The screenshot shows a configuration window titled "9N;; Dial". The "Short Code" tab is active. The fields are as follows:

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". The "Short Code" tab is active. The fields are as follows:

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**. 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.

The screenshot displays the configuration page for user 'Extn89110: 89110'. The page has a blue header with the user name. Below the header is a navigation bar with tabs: Group Membership, Announcements, SIP, Personal Directory, Web Self-Administration, User, Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, and Button Programming. The 'User' tab is selected. The main content area contains the following fields and options:

Name	Extn89110
Password	••••••••
Confirm Password	••••••••
Unique Identity	
Audio Conference PIN	
Confirm Audio Conference PIN	
Account Status	Enabled
Full Name	Extn89110
Extension	89110
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Power User
	<input type="checkbox"/> Receptionist

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

Next, select the **SIP** tab in the Details Pane. To reach the **SIP** tab click the right arrow on the right-hand side of the Details Pane until it becomes visible. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. These allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.6.2**). As such, these fields should be set to one of the DDI numbers assigned to the enterprise from Swisscom.

Ext89110: 89110								
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording
Group Membership	Announcements	SIP	Personal Directory	Web Self-Administration				
SIP Name	+414xxxxxx80							
SIP Display Name (Alias)	+414xxxxxx80							
Contact	+414xxxxxx80							
<input type="checkbox"/> Anonymouse								

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

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

Ext89110: 89110*									
Announcements	SIP	Personal Directory	Web Self-Administration						
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Twinned Handset	<None>								
Maximum Number of Calls	1								
<input type="checkbox"/> Twin Bridge Appearances									
<input type="checkbox"/> Twin Coverage Appearances									
<input type="checkbox"/> Twin Line Appearances									
<input checked="" type="checkbox"/> Mobility Features									
<input checked="" type="checkbox"/> Mobile Twinning									
Twinned Mobile Number (including dial access code)	0035389xxxxxx1								
Twinning Time Profile	<None>								
Mobile Dial Delay (secs)	3								
Mobile Answer Guard (secs)	0								
<input type="checkbox"/> Hunt group calls eligible for mobile twinning									
<input type="checkbox"/> Forwarded calls eligible for mobile twinning									
<input type="checkbox"/> Twin When Logged Out									
<input type="checkbox"/> one-X Mobile Client									
<input checked="" type="checkbox"/> Mobile Call Control									
<input checked="" type="checkbox"/> Mobile Callback									

5.9. Incoming Call Routing

An incoming call route maps an inbound DDI number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.6.2**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left.
- Default values can be used for all other fields.

The screenshot shows a configuration window for an incoming call route. The title bar displays '17 +414xxxxxx80'. The 'Standard' tab is selected, with other tabs being 'Voice Recording' and 'Destinations'. The form contains the following fields:

Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	+414xxxxxx80
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 **+414xxxxxx80** on line 17 are routed to extension 89110.

The screenshot shows the 'Destinations' tab of the configuration window. The title bar remains '17 +414xxxxxx80'. The 'Destinations' tab is selected. The form contains the following fields:

TimeProfile	Destination
Default Value	89110

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.

The screenshot shows a web-based configuration interface for a location named "Galway". The interface is titled "Galway" and has two tabs: "Location" (selected) and "Address". The "Location" tab contains the following fields and settings:

- 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>

Below these fields is a section for **Call Admission Control** with three settings:

- Total Maximum Calls:** Unlimited
- External Maximum Calls:** Unlimited
- Internal Maximum Calls:** Unlimited

At the bottom is a **Time Settings** section:

- Time Zone:** Same as System
- Local Time Offset from UTC:** 00:00
- Automatic DST:**
- Clock Forward/Back Settings (Start Date - End Date(DST Offset)):** <Add New Entry>

At the bottom right of the form are two buttons: "Edit" and "Delete".

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

The screenshot shows a web application window titled "Galway" with a standard browser toolbar. The application has two tabs: "Location" and "Address", with "Address" being the active tab. The form is organized into several sections:

- Location Section:** A vertical list of location codes (A1 through A6) on the left, each with a corresponding text input field on the right. The values entered are: A1: Connacht, A2: Galway, A3: Galway, A4: Mervue, A5: Business Park, A6: Unit 25-29.
- RD Section:** A vertical list of codes (RD, RDSEC, RDBR, RDSUBBR, PRD, POD, STS, PRM, POM) on the left, each with an empty text input field on the right.
- UNIT Section:** A vertical list of codes (HNO, HNS, LMK, BLD, LOC, PLC, FLR, UNIT, ROOM, SEAT) on the left. The input fields for HNO, HNS, LMK, BLD, LOC, PLC, and FLR are empty. The input field for UNIT contains the text "GSSCP lab". The input fields for ROOM and SEAT are empty.
- NAM Section:** A vertical list of codes (NAM, ADDCODE, PCN, PC, POBOX) on the left. The input field for NAM contains the text "GSSCP". The input fields for ADDCODE, PCN, PC, and POBOX are empty.

5.11. G.711 Fax

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

5.11.1. Analogue User

To configure the settings for the fax User, first navigate to **User** in the Navigation Pane for the Expansion. In the test environment, the 500V2 Expansion is called **GSSCP_IPO9**. Select the **User** tab. The following example shows the configuration required for an analogue Endpoint.

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

The screenshot displays the configuration interface for a user named 'Analog89119: 89119'. The left-hand side shows a navigation tree with 'User' selected under the 'Solution' folder. The right-hand side shows the configuration form with the following fields and values:

Analog89119: 89119	
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

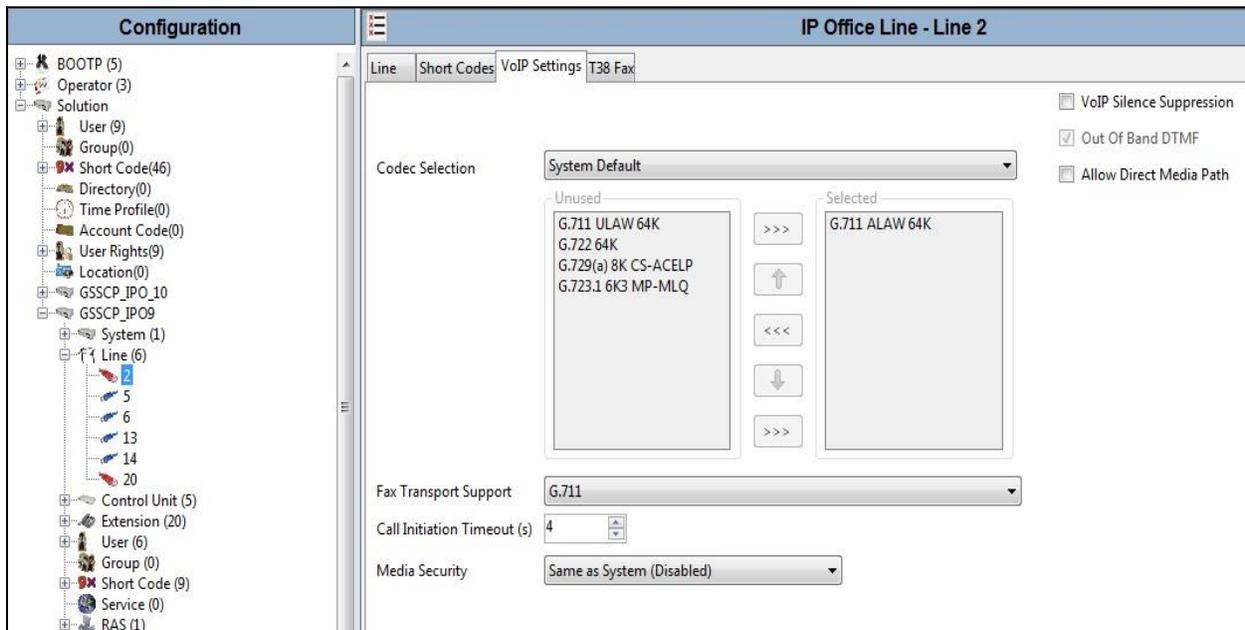
Configure other settings as described in **Section 5.8**.

5.11.2. G.711 Fax Settings

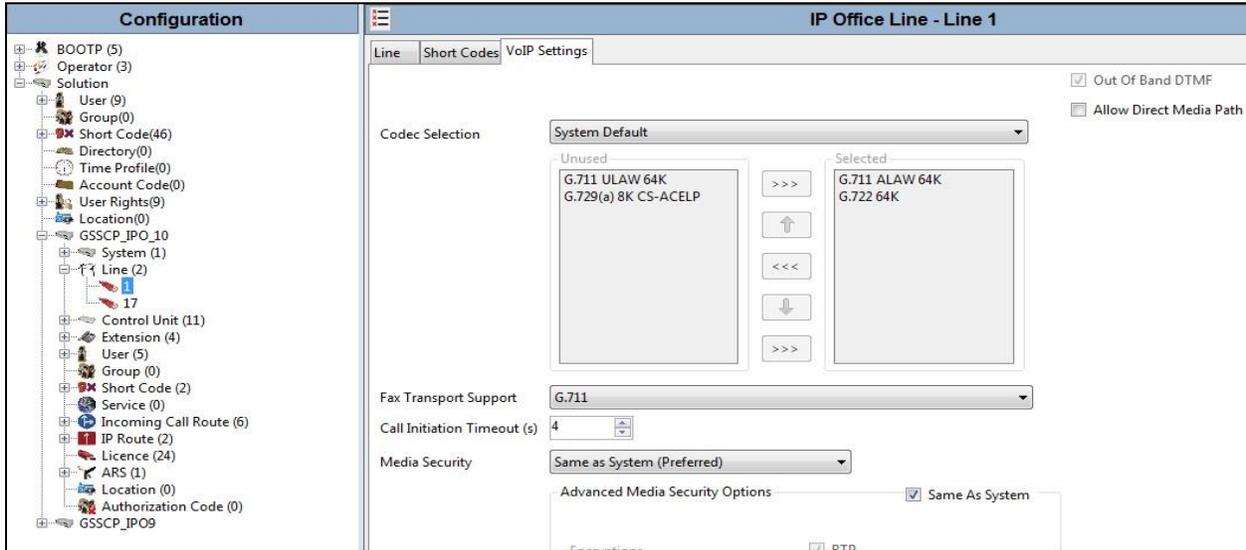
The G.711 Fax settings are defined on the SIP Line between the Expansion and the Server. Note that the VoIP settings for G.711 Fax are required in three places in this configuration:

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

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



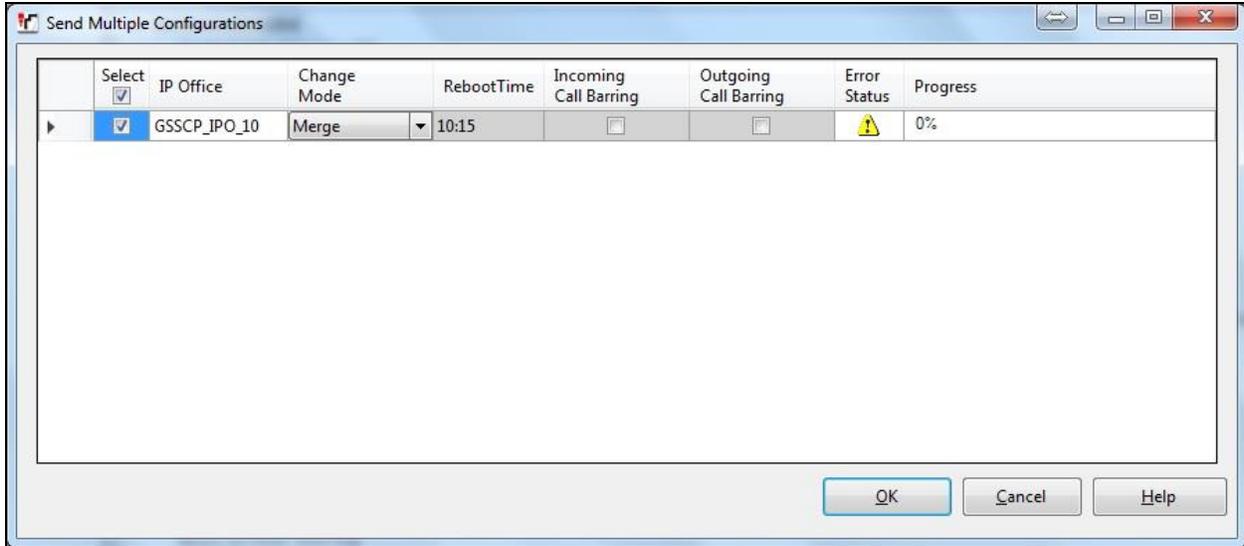
The following shows the **VoIP Settings** tab in the IP Office Line for the Expansion in the Server configuration:



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

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, 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

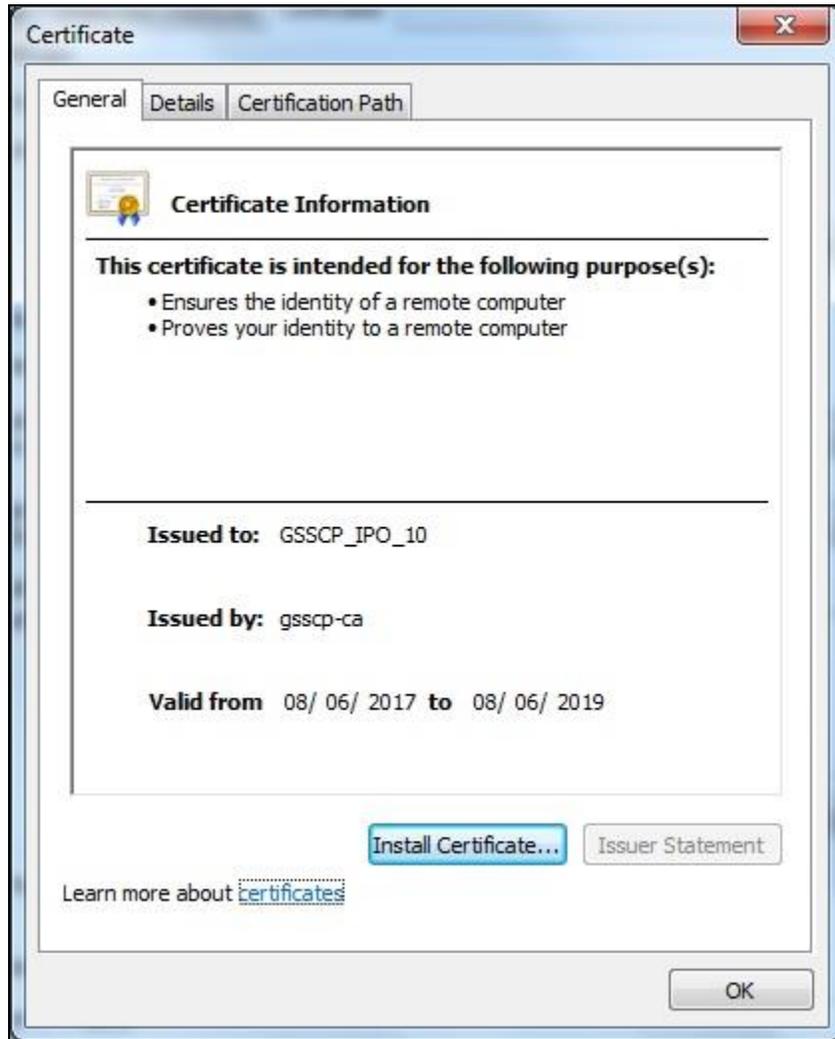
For the compliance test, TLS signalling was used internally to the enterprise wherever possible. Testing was done using identity certificates signed by a local certificate authority **gsscp-ca**. The generation and installation of these certificates are beyond the scope of these Application Notes.

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_10) and issued by gsscp-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 **gsscp-ca** is displayed as an **Installed Certificate**.



6. Configure Avaya Session Border Controller for Enterprise

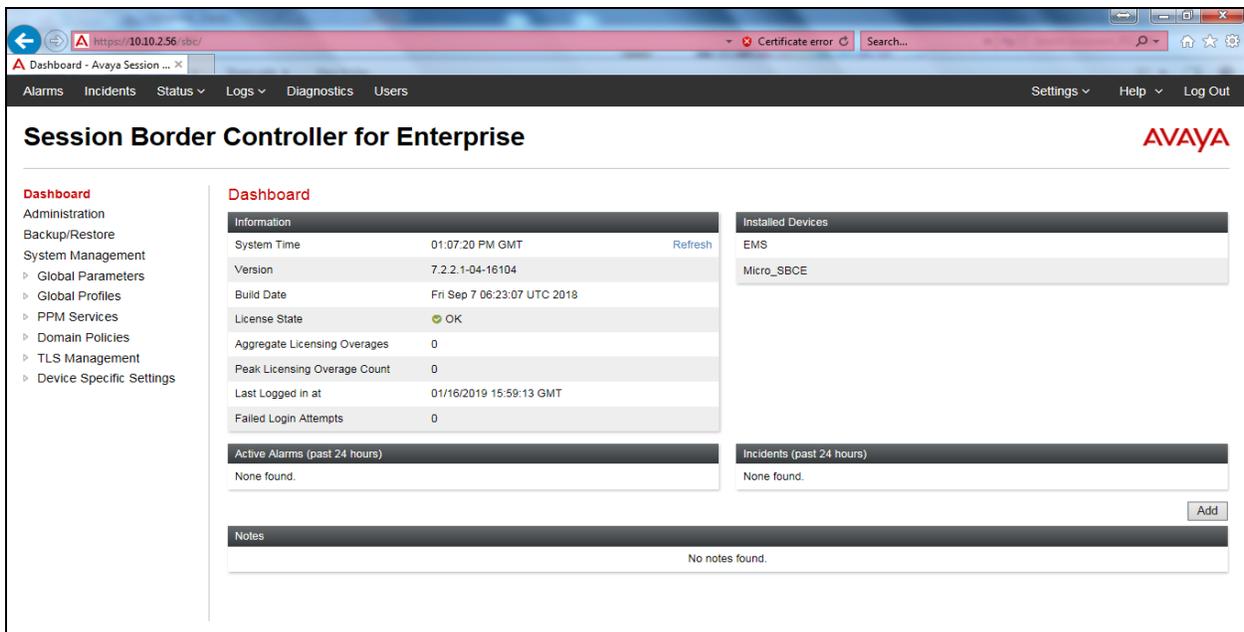
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP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

6.1. Accessing Avaya Session Border Controller for Enterprise

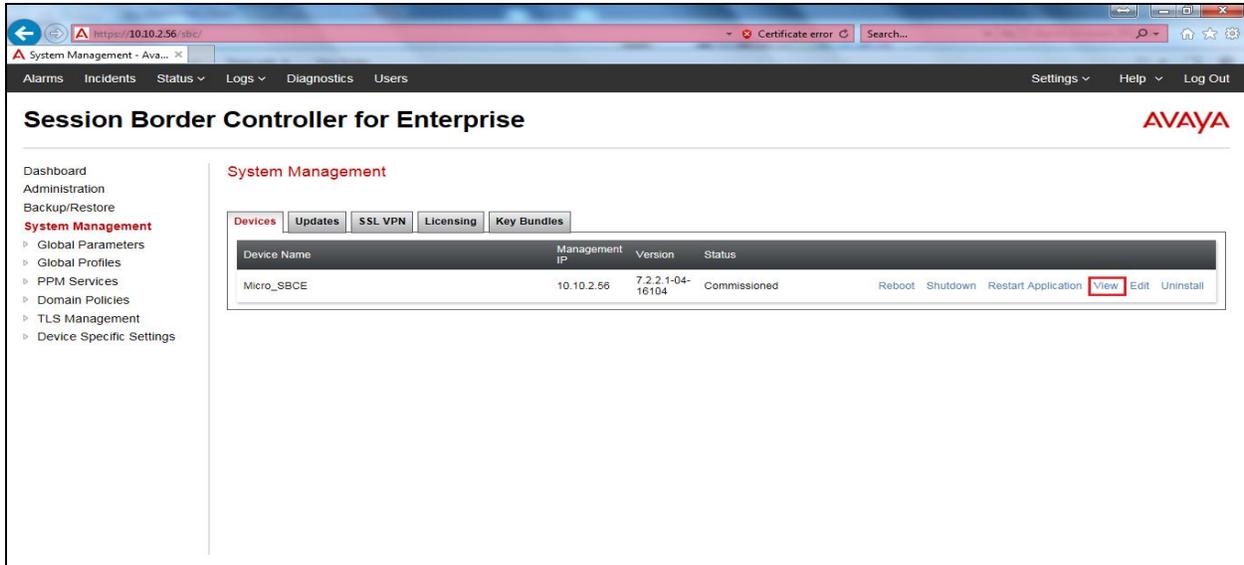
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



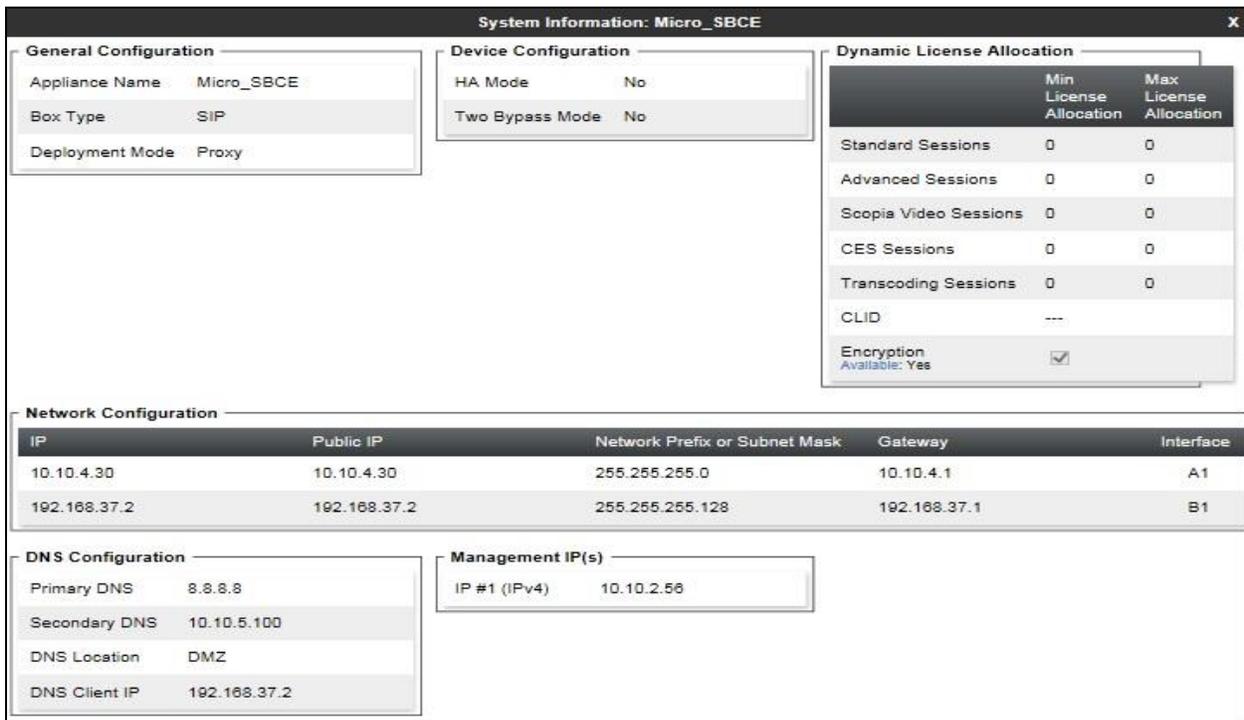
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



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



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



6.2. Define Network Management

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

To define the network information, navigate to **Device Specific Settings → 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 **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' configuration dialog box with the following fields and options:

- Name:** B1_External
- Default Gateway:** 192.168.37.1
- Network Prefix or Subnet Mask:** 255.255.255.128
- Interface:** B1 (selected from a dropdown menu)

Below these fields is an **Add** button. Below the **Add** button is a table with three columns: **IP Address**, **Public IP**, and **Gateway Override**.

IP Address	Public IP	Gateway Override	
192.168.37.2	Use IP Address	Use Default	Delete

At the bottom of the dialog box is a **Finish** button.

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 **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.

The following screenshot shows the completed Network Management configuration:

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
A1_Internal	10.10.4.1	255.255.255.0	A1	10.10.4.30	Edit	Delete
B1_External	192.168.37.1	255.255.255.128	B1	192.168.37.2	Edit	Delete

6.3. TLS Management

For the compliance test, TLS transport is used for signalling on the SIP trunk between Avaya 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 (**Micro_SBCE.crt**) is present under **Installed Certificates**.
- Verify that certificate authority root certificate (**GSSCP_Root.crt**) is present under **Installed CA certificates**.
- Verify that private key associated with the identity certificate (**Micro_SBCE.key**) is present under **Installed Keys**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The page title is "Session Border Controller for Enterprise" and the AVAYA logo is in the top right corner. A left-hand navigation menu includes: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies), TLS Management (with sub-items: Certificates, Client Profiles, Server Profiles), and Device Specific Settings. The "Certificates" page is active, showing a sub-menu for "Certificates" and two buttons: "Install" and "Generate CSR". The main content area is divided into three sections: "Installed Certificates" with a table listing "Micro_SBCE.crt" and "View Delete" links; "Installed CA Certificates" with a table listing "GSSCP_Root.crt" and "View Delete" links; and "Installed Certificate Revocation Lists" with the message "No certificate revocation lists have been installed." Below these is the "Installed Keys" section with a table listing "Micro_SBCE_avaya.com.key" and "Micro_SBCE.key", each with a "Delete" link.

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 **Micro_SBCE.crt** used in the compliance testing.
- **Peer Verification** is automatically set to **Required**.
- Set **Peer Certificate Authorities** to the **GSSCP_Root.crt** identity certificate.
- Set **Verification Depth** to **1**.
- Click **Next** to accept default values for the next screen and click **Finish** (not shown).

The screenshot shows a web interface for managing client profiles. The main heading is "Client Profiles: GSSCP_Client". On the left, there is a sidebar with "Client Profiles" and "GSSCP_Client" listed. The main content area shows the configuration for the "GSSCP_Client" profile. The configuration is organized into several sections:

- TLS Profile**: Profile Name: GSSCP_Client, Certificate: Micro_SBCE.crt
- Certificate Verification**: Peer Verification: Required, Peer Certificate Authorities: GSSCP_Root.crt, Peer Certificate Revocation Lists: ---, Verification Depth: 1, Extended Hostname Verification:
- Renegotiation Parameters**: Renegotiation Time: 0, Renegotiation Byte Count: 0
- Handshake Options**: Version: TLS 1.2 TLS 1.1 TLS 1.0

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 **Micro_SBCE.crt** used in the compliance testing.
- Set **Peer Verification** to **None**.

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

The screenshot shows the configuration page for a server profile named 'GSSCP_Server'. The page is titled 'Server Profiles: GSSCP_Server' and includes an 'Add' button and a 'Delete' button. The main content area is divided into several sections:

- Server Profile**: A blue header bar with the text 'Click here to add a description.'
- TLS Profile**:
 - Profile Name: GSSCP_Server
 - Certificate: Micro_SBCE.crt
- Certificate Verification**:
 - Peer Verification: None
 - Extended Hostname Verification:
- Renegotiation Parameters**:
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**:
 - Version: TLS 1.2 TLS 1.1 TLS 1.0
 - Ciphers: Default FIPS Custom
 - Value: HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@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 **Device Specific Settings** → **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 **IP Address**, 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 **TCP** port number, **5060** is used for the Swisscom Enterprise SIP.
- Click **Finish**.

Signaling Interface: Micro_SBCE

Devices

Micro_SBCE

Signaling Interface

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

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Ext_Sig	192.168.37.2 B1_External (B1, VLAN 0)	5060	---	---	None	Edit Delete
Int_Sig	10.10.4.30 A1_Internal (A1, VLAN 0)	5060	---	5061	GSSCP_Server	Edit Delete

6.4.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **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 **IP Address**, select the **A1_Internal** media interface IP address defined in **Section 6.2**.
- For **Port Range**, enter required values or leave as default **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 **IP Address**, select the **B1_External** media interface IP address defined in **Section 6.2**.
- For **Port Range**, enter required values or leave as default **35000-40000**.
- Click **Finish**.

Media Interface: Micro_SBCE

Devices

Micro_SBCE

Media Interface

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

Add

Name	Media IP Network	Port Range	
Ext_Media	192.168.37.2 B1_External (B1, VLAN 0)	35000 - 40000	Edit Delete
Int_Media	10.10.4.30 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete

6.5. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38.

6.5.1. Server Interworking Avaya

From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add**.

- Enter profile name such as Avaya and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

The screenshot shows the 'General' configuration tab for Server Interworking. 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"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None (dropdown)
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

From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add**.

- Enter profile name such as Swisscom and click **Next** (Not Shown).
- Check **Hold Support = None**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▾
Send Hold	<input type="checkbox"/>
Delayed Offer	<input 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 = None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

The screenshot displays the 'Advanced' configuration tab with the following settings:

- Record Routes:** Radio buttons for None, Single Side, **Both Sides** (selected), Dialog-Initiate Only (Single Side), and Dialog-Initiate Only (Both Sides).
- Include End Point IP for Context Lookup:**
- Extensions:** Dropdown menu set to **None**.
- Diversion Manipulation:**
- Diversion Condition:** Dropdown menu set to **None**.
- Diversion Header URI:** Empty text input field.
- Has Remote SBC:**
- Route Response on Via Port:**
- Relay INVITE Replace for SIPREC:**

A dark grey header labeled **DTMF** is present below the main settings. Underneath it:

- DTMF Support:** Radio buttons for **None** (selected), SIP Notify, SIP Info, and Inband.

A **Finish** button is located at the bottom center of the configuration area.

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 **Global Profiles** → **Server Configuration** and click on **Add** (not shown) and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Select **TLS Client Profile** to be **GSSCP_Client**.
- Enter **IP Address / FQDN** to **10.10.4.120** (IP Office LAN1 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.

Server Configuration Profile - General

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Call Server

SIP Domain: []

DNS Query Type: NONE/A

TLS Client Profile: GSSCP_Client

Add

IP Address / FQDN	Port	Transport	
10.10.4.120	5061	TLS	Delete

On the **Advanced** tab:

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

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

6.6.2. Server Configuration – Swisscom Enterprise SIP

To define the Swisscom Trunk Server, navigate to **Global Profiles** → **Server Configuration** and click on **Add** (not shown) 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 **10.254.150.52** (Swisscom SIP Network).
- For **Port**, enter **5060**.
- For **Transport**, select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

IP Address / FQDN	Port	Transport	
10.254.150.52	5060	TCP	Delete

On the Advanced tab:

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

The screenshot shows a dialog box titled "Server Configuration Profile - Advanced" with a close button (X) in the top right corner. The dialog contains the following configuration options:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" 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 ▼

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

6.7. Routing

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

Routing information is required for routing to IP Office on the internal side and Swisscom Enterprise SIP addresses 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 **Global 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. Below the title bar, there is a text input field labeled "Profile Name" containing the text "Avaya". Below the input field is a "Next" button.

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



The screenshot shows the "Routing Profile" window with the following configuration options:

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

Below the configuration options is an "Add" button. A blue message box contains the text: "Click the Add button to add a Next-Hop Address." At the bottom of the window are "Back" and "Finish" buttons.

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

- **Priority/Weight = 1.**
- **Server Configuration = Avaya (Section 6.6.1)** from drop down menu.
- **Next Hop Address = Select 10.10.4.120:5061(TLS)** from drop down menu.
- Click **Finish.**

The screenshot shows the 'Profile : Avaya' configuration window. The settings are as follows:

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

Below the settings is an 'Add' button and a table for the Next Hop Address:

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Avaya	10.10.4.120:5061 (TLS)	None	Delete

At the bottom of the window is a 'Finish' button.

6.7.2. Routing – Swisscom Enterprise SIP

Create a Routing Profile for Swisscom SIP network.

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

The screenshot shows the 'Routing Profile' configuration window. The 'Profile Name' field contains the text 'Swisscom'. Below the field is a 'Next' button.

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

The screenshot shows the 'Routing Profile' configuration window. It contains several settings: 'URI Group' is set to '*', 'Time of Day' is 'default', 'Load Balancing' is 'Priority', 'NAPTR' is unchecked, 'Transport' is 'None', 'Next Hop Priority' is checked, 'Next Hop In-Dialog' is unchecked, and 'Ignore Route Header' is unchecked. There is an 'Add' button at the bottom right. Below the settings is a blue banner with the text 'Click the Add button to add a Next-Hop Address.' and 'Back' and 'Finish' buttons at the bottom.

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

- **Priority/Weight = 1.**
- **Server Configuration = Swisscom (Section 6.6.2)** from drop down menu.
- **Next Hop Address = Select 10.254.150.52:5060(TCP)** from drop down menu.
- Click **Finish**.

The screenshot shows the 'Profile : Swisscom' configuration window. It contains several settings: 'URI Group' is set to '*', 'Time of Day' is 'default', 'Load Balancing' is 'Priority', 'NAPTR' is unchecked, 'Transport' is 'None', 'Next Hop Priority' is checked, 'Next Hop In-Dialog' is unchecked, 'Ignore Route Header' is unchecked, 'ENUM' is unchecked, and 'ENUM Suffix' is empty. There is an 'Add' button at the bottom right. Below the settings is a table with the following data:

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Swisscom	10.254.150.52:5060 (TCP)	None	Delete

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 **Global 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).

The screenshot shows the 'Topology Hiding Profiles: Avaya' configuration page. On the left, there is a sidebar with a list of profiles: 'default', 'cisco_th_profile', 'Avaya' (highlighted), and 'Swisscom'. An 'Add' button is located above the list. The main area contains a table with the following columns: 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The table lists several headers and their corresponding configurations. Below the table is an 'Edit' button. At the top right of the main area, there are 'Rename', 'Clone', and 'Delete' buttons. A blue bar at the top of the main area contains the text 'Click here to add a description.'

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

To define Topology Hiding for Swisscom, navigate to **Global 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
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---

Buttons: Edit

6.9. Domain Policies

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

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

6.9.1. Media Rules

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

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 **SRTP_AES_CM_128_HMAC_SHA1_32**.
- Set **Preferred Format #3** to **RTP**.
- Check **Encrypted RTCP**.
- Check **Capability Negotiation** under **Miscellaneous**.

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

The screenshot shows the 'Media Rules: Avaya_SRTP' configuration page. On the left is a sidebar with a list of media rules: 'Media Rules', 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', and 'Avaya_SRTP' (highlighted in red). The main area has a title 'Media Rules: Avaya_SRTP' and buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete'. Below the title is a blue bar with the text 'Click here to add a description.' and a tabbed interface with 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS' tabs. The 'Encryption' tab is active and contains two sections: 'Audio Encryption' and 'Video Encryption'. The 'Audio Encryption' section has fields for 'Preferred Formats' (SRTP_AES_CM_128_HMAC_SHA1_80, SRTP_AES_CM_128_HMAC_SHA1_32, RTP), 'Encrypted RTCP' (checked), 'MKI' (unchecked), 'Lifetime' (Any), and 'Interworking' (unchecked). The 'Video Encryption' section has fields for 'Preferred Formats' (RTP) and 'Interworking' (unchecked).

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



6.10. End Point Policy Groups

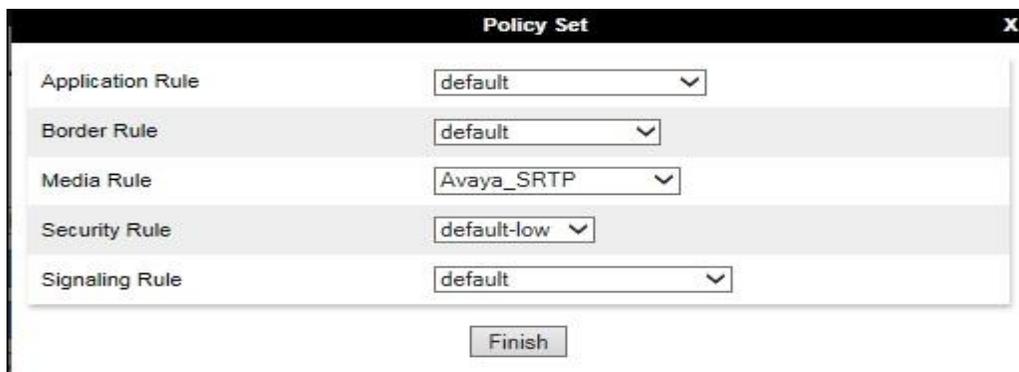
An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signalling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the Swisscom Enterprise SIP. The end point policy group is applied to 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 **Signaling Rule** fields at their default values.
- In the **Media Rule** drop down menu, select the recently added Media Rule called **Avaya_SRTP**.

Click **Finish**.



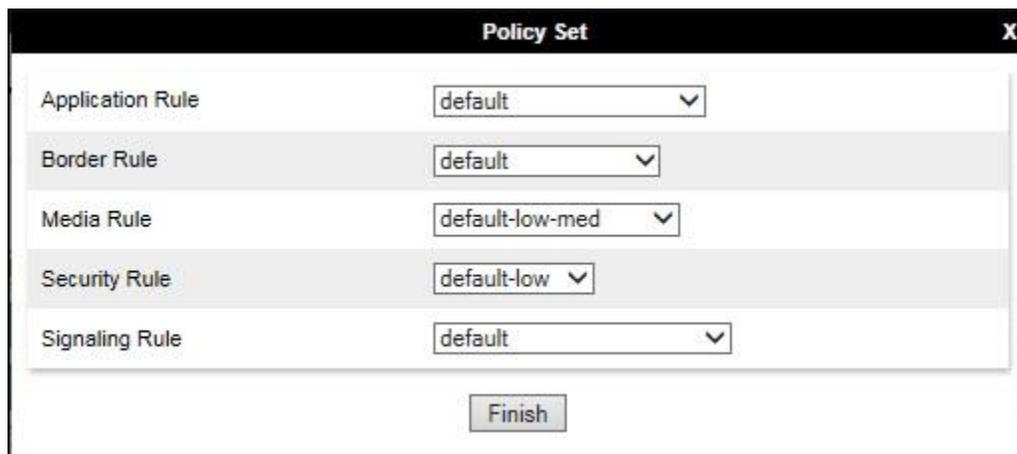
6.10.2. End Point Policy Group – Swisscom Enterprise SIP

For the compliance test, the end point policy group **Swisscom** was created for the Swisscom Enterprise SIP server. 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**.



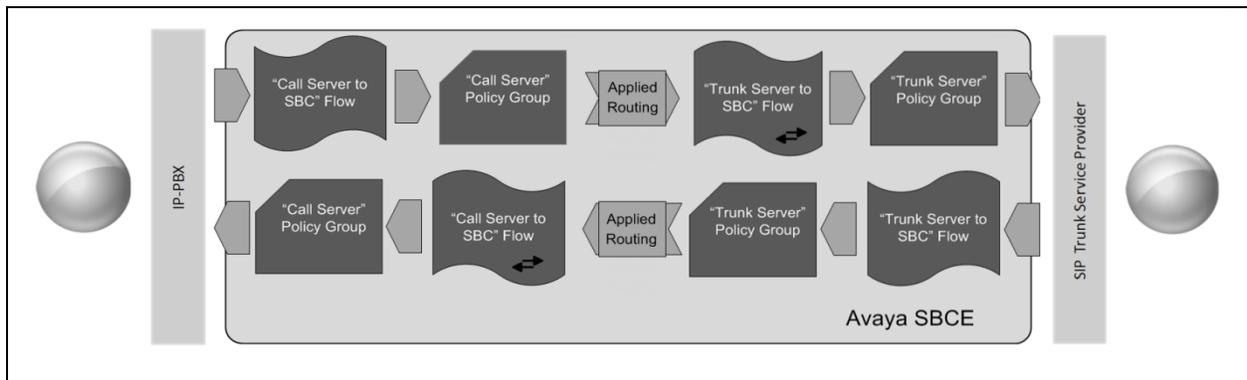
The screenshot shows a window titled "Policy Set" with a close button (X) in the top right corner. The window contains five rows of configuration options, each with a label on the left and a dropdown menu on the right. The dropdown menus are set to the following values: "default" for Application Rule, "default" for Border Rule, "default-low-med" for Media Rule, "default-low" for Security Rule, and "default" for Signaling Rule. Below these rows is a "Finish" button.

Rule Type	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 Enterprise SIP and incoming flows from Swisscom Enterprise SIP to IP Office. This configuration ties all the previously entered information together so that signalling can be routed from the IP Office to the PSTN via the Swisscom Enterprise SIP network and vice versa. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



The following screenshot shows all configured flows.

Subscriber Flows **Server Flows** Add

Click here to add a row description.

Server Configuration: Avaya

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Call_Server	*	Ext_Sig	Int_Sig	Avaya	Swisscom	View Clone Edit Delete

Server Configuration: Swisscom

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Trunk_Server	*	Int_Sig	Ext_Sig	Swisscom	Avaya	View Clone Edit Delete

To define a Server Flow for the Swisscom Enterprise SIP, navigate to **Device Specific Settings** → **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 **Swisscom**.
- In the **Routing Profile** drop-down menu, select the routing profile of IP Office defined in **Section 6.7.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Swisscom Enterprise SIP defined in **Section 6.8** and click **Finish** (not shown).

The screenshot shows a configuration window titled "Flow: Trunk_Server". It is divided into two main sections: "Criteria" and "Profile".

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

Profile	
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
Secondary Media Interface	None
End Point Policy Group	Swisscom
Routing Profile	Avaya
Topology Hiding Profile	Swisscom
Signaling Manipulation Script	None
Remote Branch Office	Any

To define a server flow for IP Office, navigate to **Device Specific Settings → 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 external SIP signalling interface defined in **Section 6.4.1**.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**.
- In the **Media Interface** drop-down menu, select the internal 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 Enterprise SIP 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". It is divided into two main sections: "Criteria" and "Profile".

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

Profile	
Signaling Interface	Int_Sig
Media Interface	Int_Media
Secondary Media Interface	None
End Point Policy Group	Avaya
Routing Profile	Swisscom
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any

7. Swisscom Enterprise SIP 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.

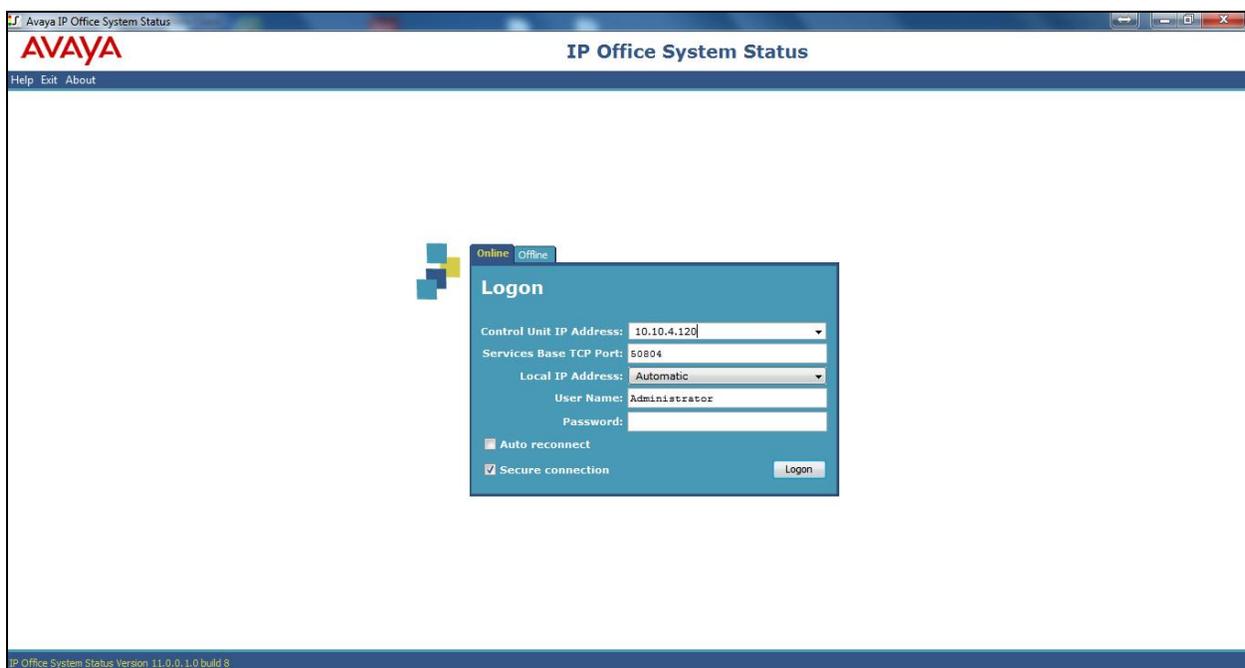
8. Verification Steps

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

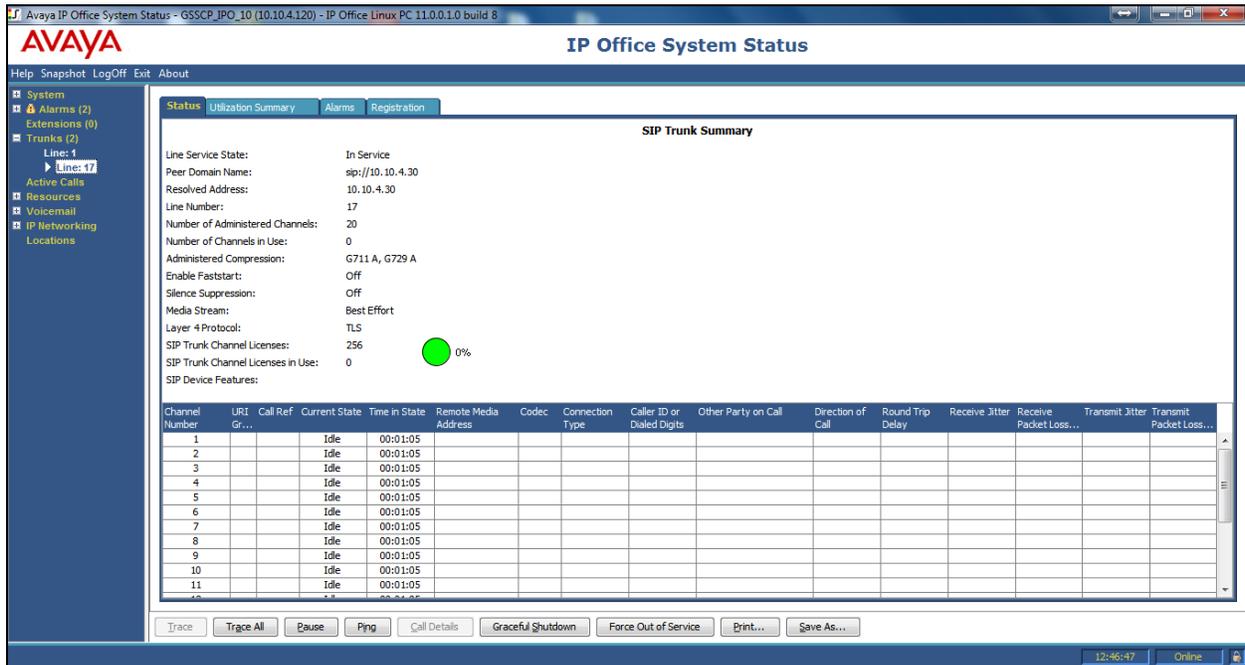
8.1. SIP Trunk status

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

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

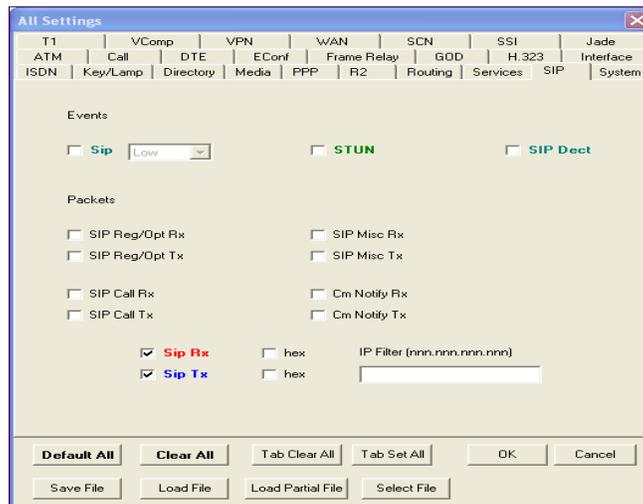


From the left-hand menu expand **Trunks** and choose the SIP trunk (**17** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational.



8.2. Monitor

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



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

```

Avaya IP Office SysMonitor - [STOPPED] Monitoring 10.10.4.120 (GSSCP_IPO_10 (Server Edition(P))) Log Settings - C:\Users\... \sysmonitorsettings.ini
File Edit View Filters Status Help
***** SysMonitor v10.1.0.2.0 build 2 [connected to 10.10.4.120 (GSSCP_IPO_10 (Server Edition(P)))] *****
336128686mS SIP Rk: 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: 07a0401e5c819c50f33700dd0e04846
Contact: <sip:10.10.4.30:5060;transport=tcp>
Record-Route: <sip:10.10.4.30:5060;ipcs-line=2;lr;transport=tcp>
Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, FRACK, REFER, INFO, SUBSCRIBE, UPDATE
Supported: replaces
User-Agent: MS008/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 SIPUser--trunk SIP Line (17)
336128686mS Sip: SIPDialog f6e2cdd0 created, dialogs 1 txn_keys 1
336128686mS Sip: (f6e2cdd0) SetUnintTransactionCondition to Unint_None
336128686mS Sip: SIPUser f430 has 1 dialog open (AttachDialogToSIPUser)
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;ipcs-line=2;lr;transport=tcp>
From: <sip:avaya.com;tag=1c1904606935>
To: <sip:avaya.com;tag=895dd2b8d0f38743>
Call-ID: 07a0401e5c819c50f33700dd0e04846
CSeq: 1 OPTIONS
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, INFO, NOTIFY, UPDATE
Supported: timer
Server: IP Office 10.1.0.2.0 build 2
To: <sip:avaya.com;tag=895dd2b8d0f38743>
Content-Type: application/sdp
Content-Length: 169

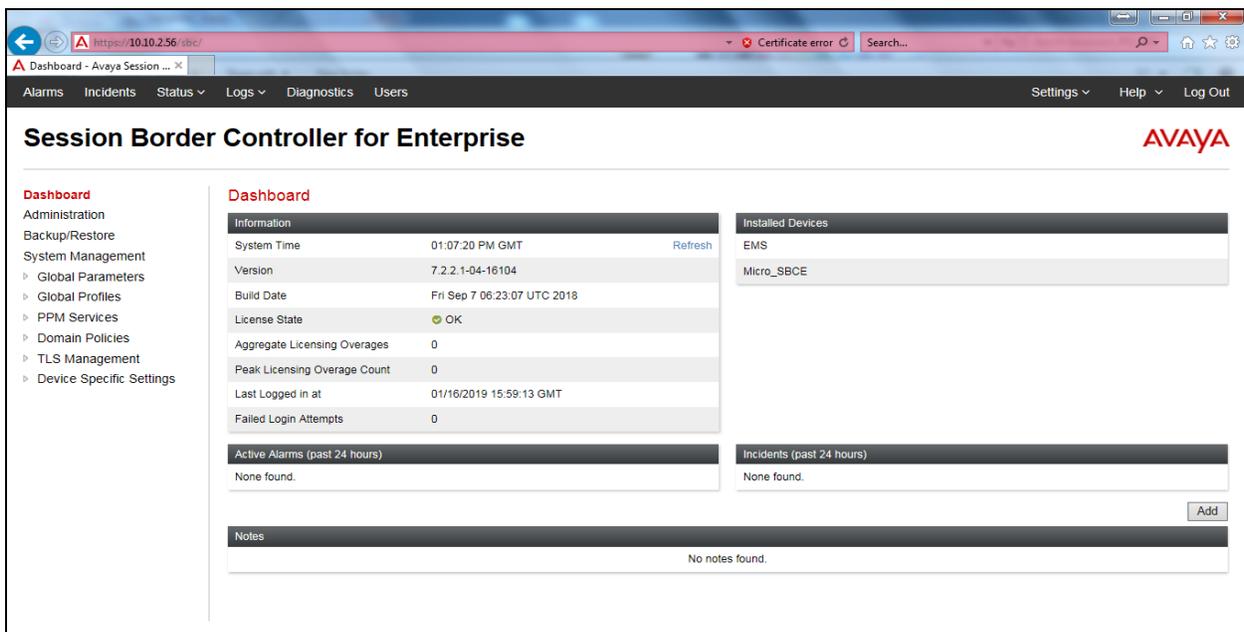
v=0
o=UserA 1712183164 1334060956 IN IP4 10.10.4.120
s=Session SDP
c=IN IP4 10.10.4.120
t=0
  
```

8.3. Avaya SBCE

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

8.3.1. Incidents

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



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

Incident Viewer							AVAYA
Device	All	Category	All			Clear	Refresh Generate Report
Displaying results 1 to 15 out of 2000.							
Type	ID	Date	Time	Category	Device	Cause	
Routing Failure	686948871165253	7/15/13	2:15 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden	
Routing Failure	686948811180314	7/15/13	2:13 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden	
ACK Message Out of Dialog	686948761299324	7/15/13	2:12 PM	Protocol Discrepancy	VLAN3_MicroSBC	General Method not allowed Out-Of-Dialog	
Message Dropped	686948761299222	7/15/13	2:12 PM	Policy	VLAN3_MicroSBC	No Subscriber Flow Matched	
Call Denied	686948761263328	7/15/13	2:12 PM	Policy	VLAN3_MicroSBC	No Subscriber Flow Matched	
Routing Failure	686948751195370	7/15/13	2:11 PM	Policy	VLAN3_MicroSBC	Neither target nor source is Call Server, Sending 403 Forbidden	

8.3.2. Trace Capture

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

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

Trace: Micro_SBCE

Devices

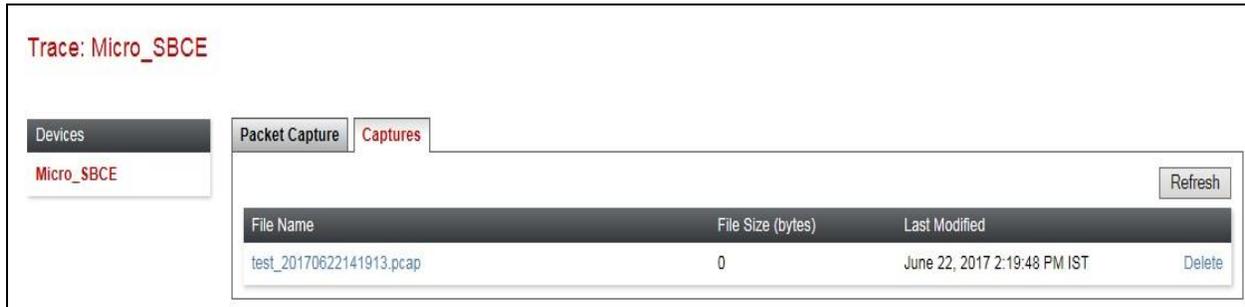
Packet Capture

Captures

Micro_SBCE

Packet Capture Configuration	
Status	Ready
Interface	B1
Local Address <small>IP[:Port]</small>	All : <input type="text"/>
Remote Address <small>*, *:Port, IP, IP:Port</small>	<input type="text" value="*"/>
Protocol	All
Maximum Number of Packets to Capture	1000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	test.pcap
<input type="button" value="Start Capture"/> <input type="button" value="Clear"/>	

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



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

9. Conclusion

These Application Notes demonstrated how IP Office Release 11.0 and Avaya Session Border Controller for Enterprise R7.2 can be successfully combined with Swisscom Enterprise SIP service solution 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 the Swisscom Enterprise SIP service. This solution provides IP Office and Avaya Session Border Controller for Enterprise users the ability to access the Public Switched Telephone Network (PSTN) via a SIP trunk using the Swisscom Enterprise SIP service thus eliminating the costs of analogue or digital trunk connections previously required to access the PSTN. The service was successfully tested with a number of observations listed in **Section 2.2**.

10. Additional References

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

- [1] *Avaya IP Office™ Platform Start Here First*, Release 11.0, May 2018.
- [2] *Avaya IP Office™ Platform Server Edition Reference Configuration*, Release 11.0, May 2018.
- [3] *Deploying IP Office™ Platform Server Edition Solution*, Release 11.0, May 2018.
- [4] *IP Office™ Platform 10.1, Deploying IP Office Essential Edition*, Document number 15-601042, May 2018.
- [5] *IP Office™ Platform 10.1 Installing and Maintaining the Avaya IP Office™ Platform Application Server*, Document number 15-601011, May 2018.
- [6] *Administering Avaya IP Office™ Platform with Web Manager*, Release 11.0, May 2018.
- [7] *Administering Avaya IP Office™ Platform with Manager*, Release 11.0, May 2018.
- [8] *IP Office™ Platform 10.1 Using Avaya IP Office™ Platform System Status*, Document number 15-601758, Apr 2018.
- [9] *IP Office™ Platform 11.0 Using IP Office System Monitor*, Document number 15-601019, May 2018.
- [10] *Using Avaya Equinox for Windows on IP Office*, Release 10.0, Mar 2018.
- [11] *IP Office™ Platform 11.0 - Third-Party SIP Extension Installation Notes*, Apr 2018.
- [12] *Avaya IP Office Knowledgebase*, <http://marketingtools.avaya.com/knowledgebase>
- [13] *Deploying Avaya Session Border Controller for Enterprise Release 7.2.2*, Oct 2018
- [14] *Upgrading Avaya Session Border Controller for Enterprise Release 7.2.2*, Oct 2018
- [15] *Administering Avaya Session Border Controller for Enterprise Release 7.2.2*, Jun 2018
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2019 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.