



DevConnect Program

Application Notes for Configuring Avaya IP Office Server Edition R12.0 with Swisscom Smart Business Connect – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Swisscom Smart Business Connect and Avaya IP Office Server Edition R12.0.

Swisscom Smart Business Connect 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.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Swisscom Smart Business Connect and Avaya IP Office Server Edition R12.0.

Avaya IP Office Server Edition R12.0 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.

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 Server Edition R12.0 to connect to the Swisscom Smart Business Connect SIP trunk. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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

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

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

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability the following features and functionality were exercised during the interoperability compliance test:

- Incoming PSTN calls to various phone types including H.323, SIP, Digital and Analog telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, Digital, and Analog telephones at the enterprise.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to the Service Provider.
- Incoming and Outgoing PSTN calls to/from Avaya Workplace Client for Windows soft phone.
- Calls using the G.711A and G.729.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using G.711 pass-through transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, call mute, transfer, and conference.
- Off-net call forwarding and mobile twinning.

2.2. Test Results

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

- During 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 200 OK 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 200 OK from IP Office with a BYE and the call was terminated. Therefore, T.38 fax is not currently supported on the Swisscom Smart Business Connect service.
- The Privacy Header as required by Swisscom is not included in the SIP INVITE for outbound calls with Calling Line Identity (CLIR) when using an IP Office short code (*67 was used in the test configuration). As a workaround, the anonymous button can be enabled on the SIP tab in **Section 5.7** to restrict CLIR and include a Privacy Header as required by Swisscom.
- No inbound toll free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked by the Service Provider with the Emergency Services Operator.

2.3. Support

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

For technical support on Swisscom products please contact the Swisscom support team: Email: PBX-Technical.Partner@swisscom.com.

3. Reference Configuration

Figure 1 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 and Avaya IP Office 500 V2 as an expansion. Endpoints include Avaya 1600 Series IP Telephones (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware), Avaya 1140e SIP Telephones, Avaya 1400 Series Digital Deskphones, Analog Telephone and a fax machine. The site also has a Windows PC running Avaya IP Office Manager to configure the Avaya IP Office as well as Avaya Workplace Client for Windows for softphone testing.

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

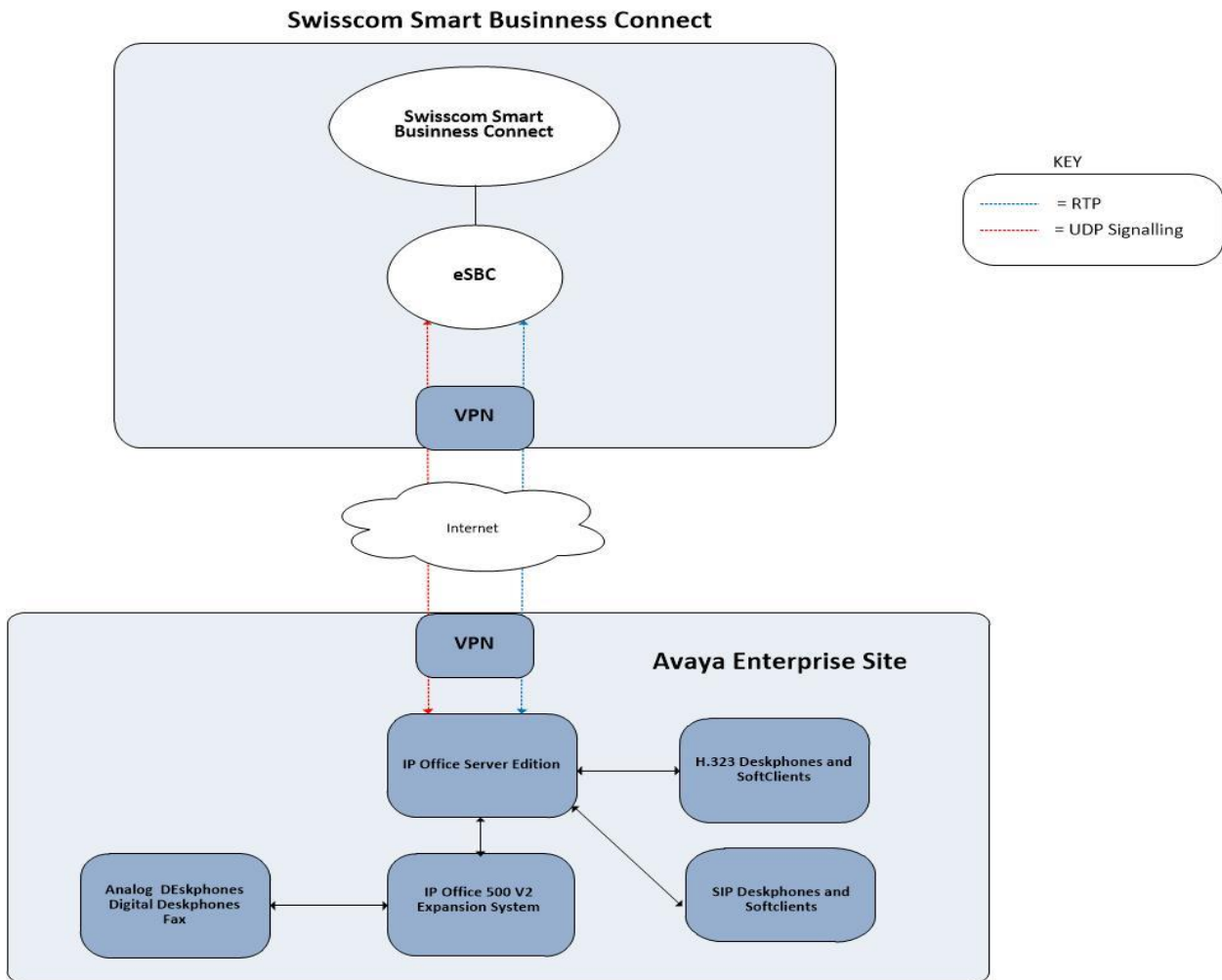


Figure 1: Swisscom Smart Business Connect to Avaya IP Office Server Edition Topology

4. Equipment and Software Validated

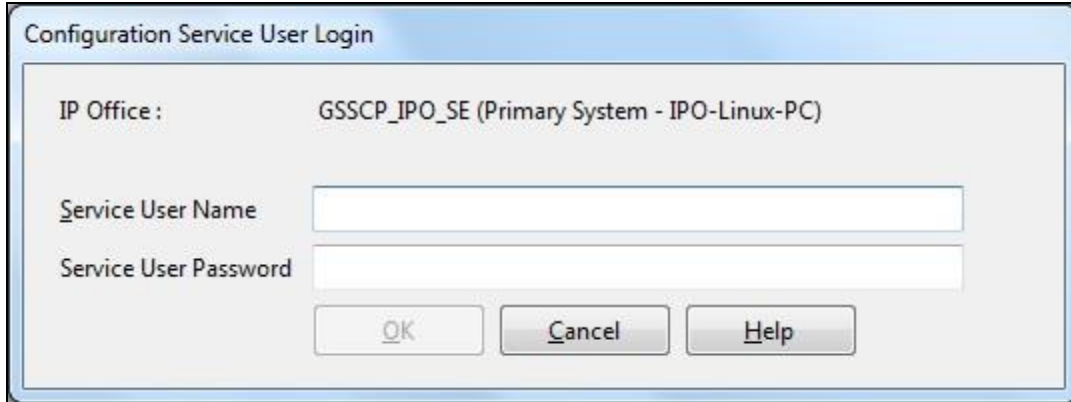
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	Version 12.0.0.0.0 build 55
Avaya IP Office 500 V2	Version 12.0.0.0.0 build 55
Avaya Voicemail Pro Client	Version 12.0.0.26
Avaya IP Office Manager	Version 12.0.0.0.0 build 55
Avaya 1608 Phone (H.323)	1.3.12
Avaya 9611G Series Phone (H.323)	6.8.3
Avaya 9608 Series Phone (H.323)	6.8.3
Avaya J179 IP Phone (SIP)	4.0.10
Avaya Workplace for Windows (SIP)	3.36.0
Avaya 1140e (SIP)	FW: 04.04.30.00.bin
Avaya 1408 Digital Telephone	R48
Avaya 98390 Analogue Phone	N/A
Swisscom	
eSBC	Cisco C881-K9: version 15.7(3)M6

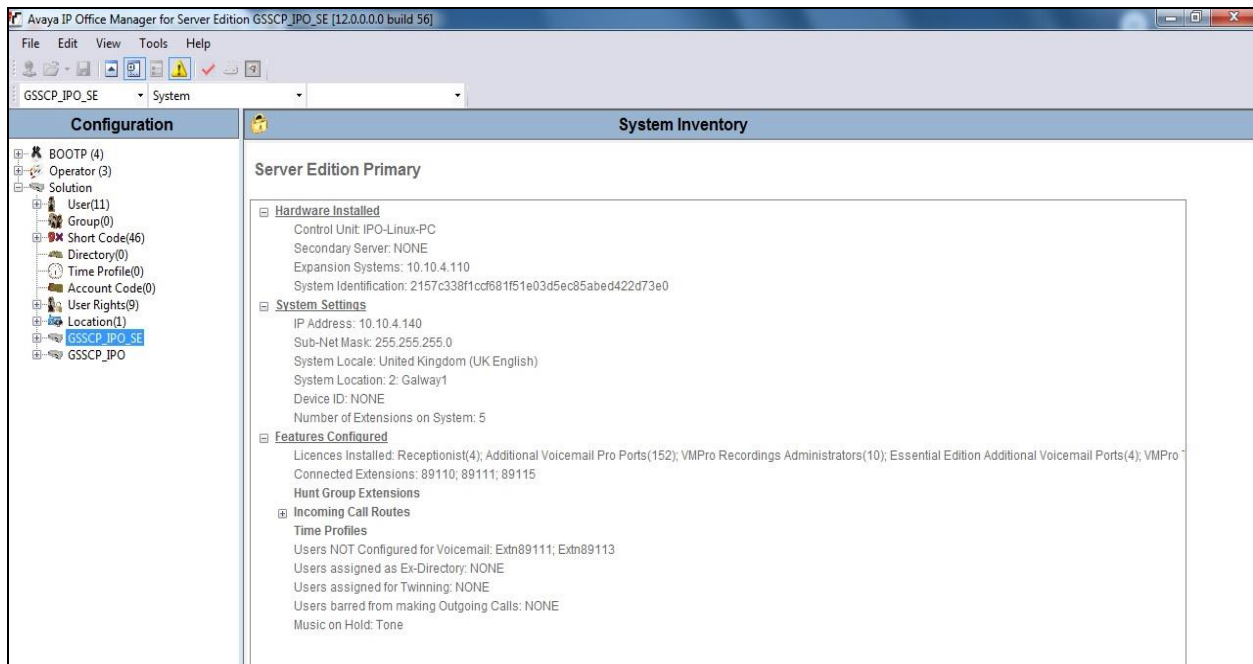
Note – Testing was performed with IP Office Server Edition with 500 V2 Expansion R12.0. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. **Note:** that IP Office Server 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 SIP Trunk service. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials.



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



5.1. Verify System Capacity

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

Licence Remote Server					
Licence Mode		Licence Normal			
Licensed Version		12.0			
PLDS Host ID		338645006189			
PLDS File Status		Valid			
Feature	Instances	Status	Expiry Date	Source	
Receptionist	4	Valid	Never	PLDS Nodal	
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal	
VMPro Recordings Administrators	10	Valid	Never	PLDS Nodal	
Essential Edition Additional Voice...	4	Obsolete	Never	PLDS Nodal	
VMPro TTS (Generic)	40	Obsolete	Never	PLDS Nodal	
Teleworker	384	Obsolete	Never	PLDS Nodal	
Mobile Worker	384	Obsolete	Never	PLDS Nodal	
Office Worker	384	Valid	Never	PLDS Nodal	
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal	
VMPro TTS (Scansoft)	40	Obsolete	Never	PLDS Nodal	
VMPro TTS Professional	40	Valid	Never	PLDS Nodal	
IPSec Tunnelling	10	Obsolete	Never	PLDS Nodal	
Power User	384	Valid	Never	PLDS Nodal	
Customer Service Agent	5	Dormant	Never	PLDS Nodal	
Customer Service Supervisor	5	Dormant	Never	PLDS Nodal	
Avaya IP endpoints	384	Valid	Never	PLDS Nodal	
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal	
SIP Trunk Channels	300	Valid	Never	PLDS Nodal	
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal	
CTI Link Pro	10	Valid	Never	PLDS Nodal	
Wave User	16	Obsolete	Never	PLDS Nodal	
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal	
Centralized Endpoints	10	Obsolete	Never	PLDS Nodal	

5.2. LAN2

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 **LAN2** interface was used to the Avaya IP Office to the Swisscom SIP platform.

To access the LAN2 settings, first navigate to **System** → **GSSCP_IPO_SE** in the Navigation Pane where GSSCP_IPO_SE is the name of the IP Office. Navigate to the **LAN1** → **LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the private interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).



The screenshot displays the configuration page for GSSCP_IPO_SE. The top navigation bar includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. The LAN2 tab is active, and the LAN Settings sub-tab is selected. The IP Address field is set to 192.168.37.2, and the IP Mask field is set to 255.255.255.0. The Number Of DHCP IP Addresses is set to 200. The DHCP Mode is set to Disabled, with radio buttons for Server, Client, and Disabled. An Advanced button is visible at the bottom right of the configuration area.

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

The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Set **Scope** to **RTP-RTCP** and **Initial keepalives** to **Enabled** and **Periodic timeout** to **30**.

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

The screenshot displays the configuration page for **GSSCP_IPO_SE**. The interface includes a navigation bar with tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and Contact Center. The **VoIP** tab is active, and the **Network Topology** sub-tab is selected.

SIP Settings:

- H323 Gatekeeper Enable
- Auto-create Extn Auto-create User H323 Remote Extn Enable
- H.323 Signalling over TLS: **Disabled** (dropdown)
- Remote Call Signalling Port: **1720** (spin box)
- SIP Trunks Enable
- SIP Registrar Enable
- Auto-create Extn/User SIP Remote Extn Enable
- Allowed SIP User Agents: **Block blacklist only** (dropdown)
- SIP Domain Name: **avaya.com** (text box)
- SIP Registrar FQDN: **avaya.com** (text box)
- Layer 4 Protocol:
 - UDP: UDP Port **5060** (spin box), Remote UDP Port **5060** (spin box)
 - TCP: TCP Port **5060** (spin box), Remote TCP Port **5060** (spin box)
 - TLS: TLS Port **5061** (spin box), Remote TLS Port **5061** (spin box)
- Challenge Expiry Time (secs): **10** (spin box)

RTP Settings:

- Port Number Range:
 - Minimum: **40750** (spin box), Maximum: **50750** (spin box)
- Port Number Range (NAT):
 - Minimum: **40750** (spin box), Maximum: **50750** (spin box)
- Enable RTCP Monitoring on Port 5005
- RTCP collector IP address for phones: **0 . 0 . 0 . 0** (text box)
- Keepalives:
 - Scope: **RTP-RTCP** (dropdown)
 - Periodic timeout: **30** (spin box)
 - Initial keepalives: **Enabled** (dropdown)

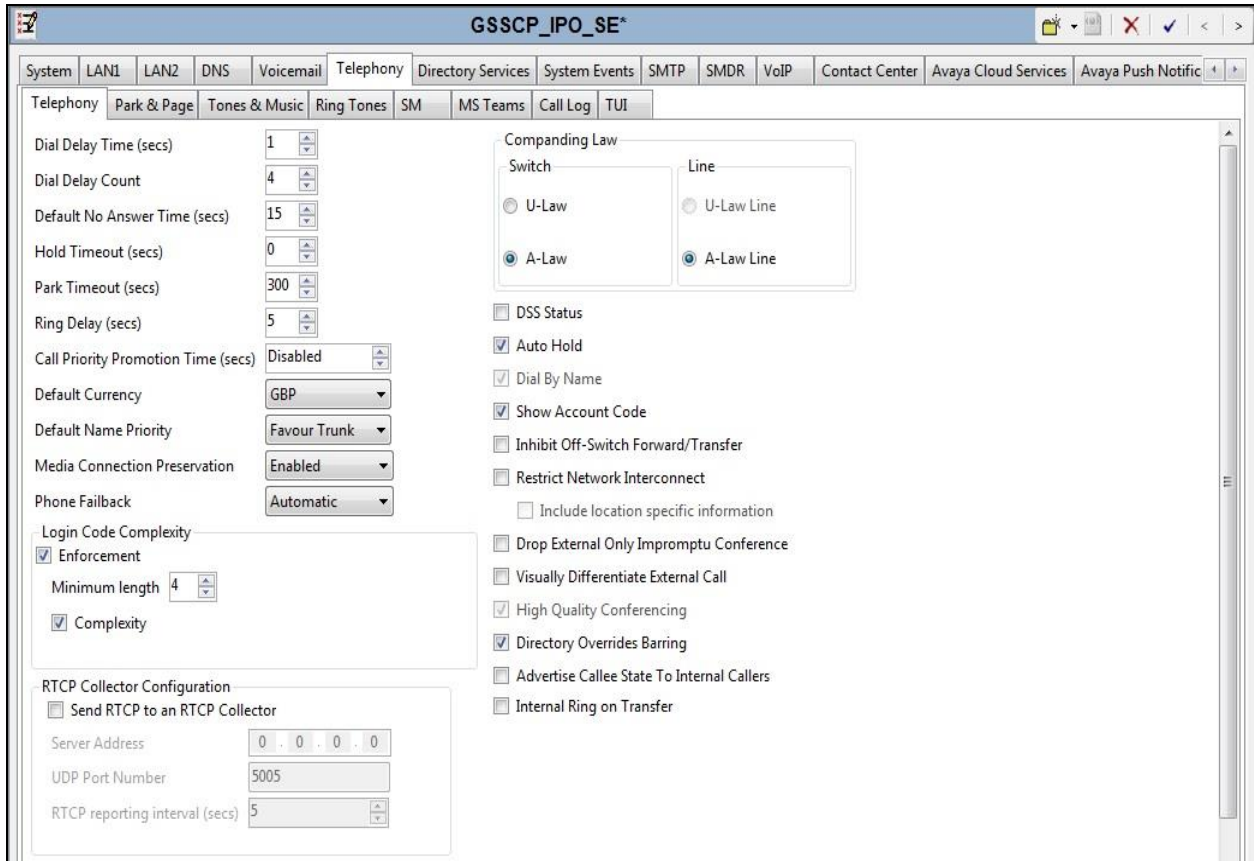
On the **Network Topology** tab, set the **Firewall/NAT Type** from the pulldown menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used as NAT was not required for this configuration, therefore resulting in no requirement for a STUN server. The **Use Network Topology Info** in the **SIP Line** was set to **None** in **Section 5.5.2**. 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_SE, specifically the Network Topology tab. The window has a menu bar with options: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, Contact Center, Avaya Cloud Services, and Avaya Push Notific. Below the menu bar, there are sub-tabs: LAN Settings, VoIP, and Network Topology. The main content area is divided into several sections:

- Network Topology Discovery:** Contains fields for IP Office STUN Server (0.0.0.0), Port (3478), and a checkbox for Run STUN on startup. There are Run STUN and Cancel buttons.
- WebRTC:** Contains fields for WebRTC Client STUN Server and WebRTC Client TURN Server, both currently empty, and a Port field set to 3478.
- NAT:** Contains a Firewall/NAT Type dropdown menu set to Open Internet, a Binding Refresh Time (seconds) spinner set to 30, and a Public IP Address field set to 0.0.0.0. To the right, there is a SIP Registrar Public Ports section with UDP (5060), TCP (5060), and TLS (5061) ports.
- SBC:** Contains Public IP Address (IPv4) set to 0.0.0.0, Public IP Address (IPv6) (empty), Private IP Address (IPv4) set to 0.0.0.0, and FQDN (empty). To the right, there is an SBC Registrar Public Ports section with UDP (0), TCP (0), and TLS (0) ports.

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).



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.

GSSCP_IPO_SE*

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | VoIP

VoIP | VoIP Security | Access Control Lists

Ignore DTMF Mismatch For Phones

Allow Direct Media Within NAT Location

Disable Direct Media For Simultaneous Clients

RFC2833 Default Payload 101

OPUS Default Payload 116

Available Codecs

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

Default Codec Selection

Unused

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

Selected

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

5.5. Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Swisscom Smart Business Connect. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.5.1** to create the SIP Line from the template.

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

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

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

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

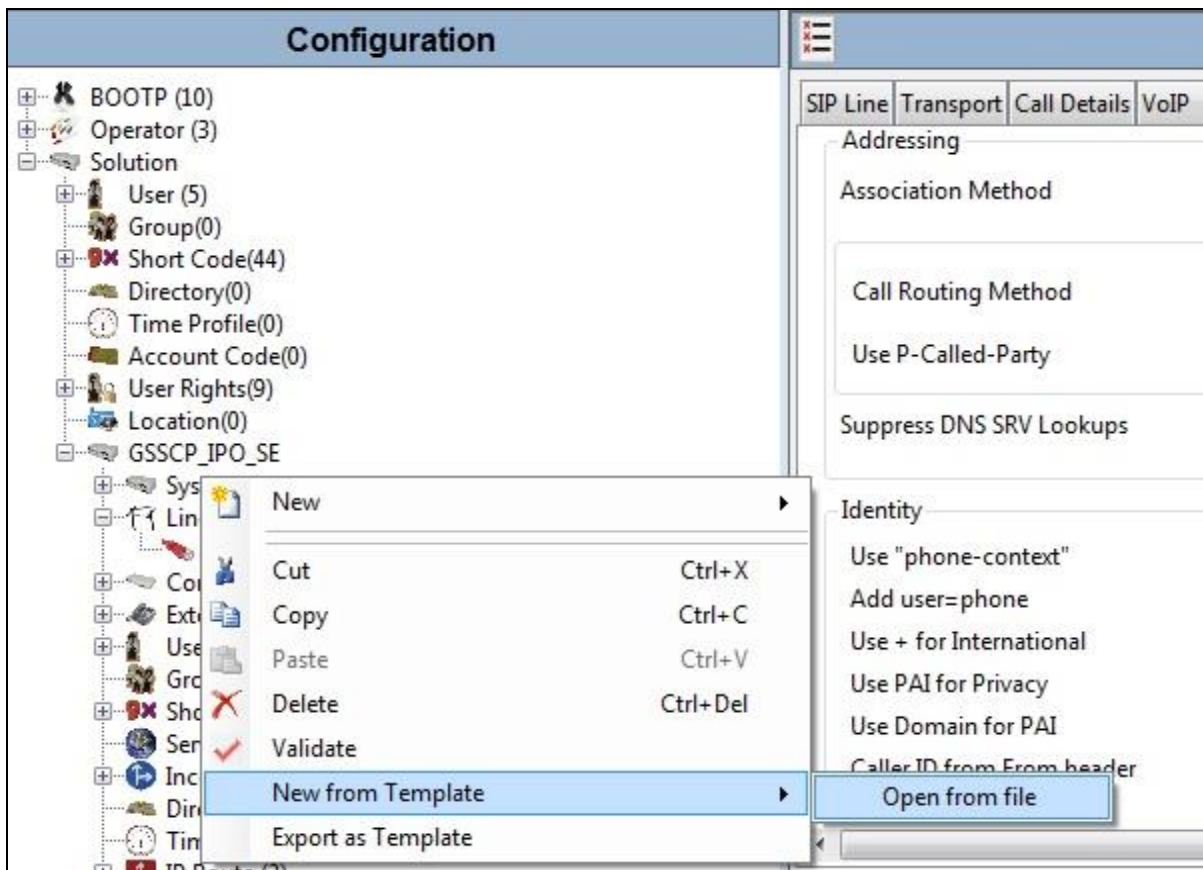
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Section 5.5.2**.

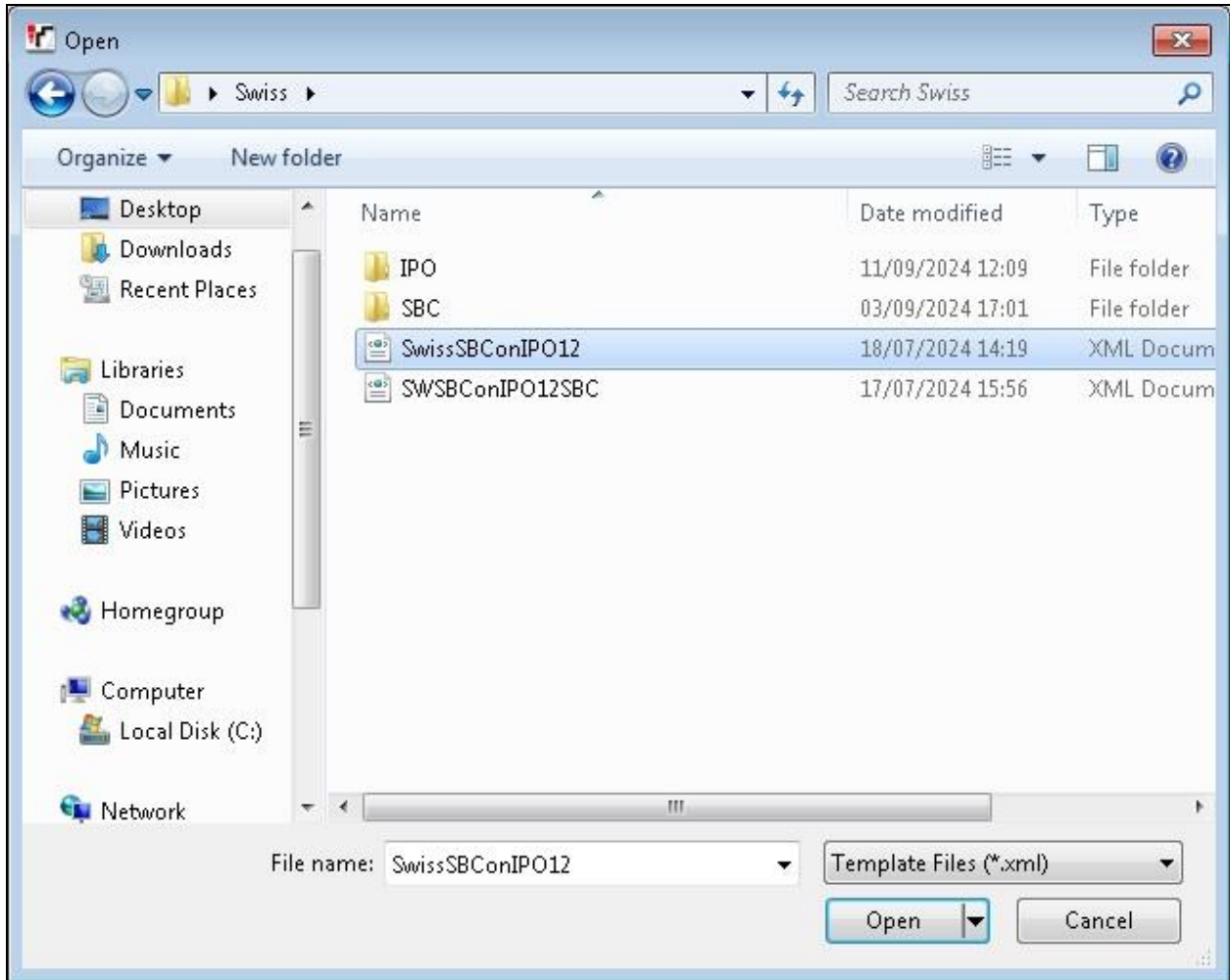
5.5.1. SIP Line From Template

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 5.5.2**.

5.5.2. 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. **join.swisscom.com** was used for the compliance testing as per the screenshot below.
- Set **Location** to that defined for Emergency calls as described in **Section 5.9**.
- Set **National Prefix** to **0** and **International Prefix** to **00** for number conversion as follows: outbound national and international called party numbers are converted to E.164 format; inbound national and international calling party numbers are converted to diallable format.
- Ensure the **In Service** box is checked.
- Leave the **Refresh Method** at the default value of **Auto** which results in re-INVITE being used for Session Refresh.
- Leave **Timer (seconds)** at the default value of **On Demand**. This value allows the Session Refresh interval to be set by the network.
- Set **Incoming Supervised REFER** and **Outgoing Supervise REFER** to **Never**. REFER is not supported by Swisscom Smart Business Connect SIP platform.
- Default values may be used for all other parameters.

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

The screenshot displays the configuration interface for a SIP Line, titled "SIP Line - Line 17". The interface is organized into several sections:

- Line Identification:** Line Number is set to 17.
- ITSP Configuration:** ITSP Domain Name is set to join.swisscom.com.
- Location and Prefixes:** Location is set to 2: Galway1. National Prefix is 0, and International Prefix is 00.
- Session Timers:** Refresh Method is set to Auto, and Timer (seconds) is set to On Demand.
- Service Status:** The In Service checkbox is checked.
- Redirect and Transfer:** Incoming Supervised REFER and Outgoing Supervised REFER are both set to Never.
- Other Options:** Check OOS, Send 302 Moved Temporarily, and Outgoing Blind REFER are all unchecked.

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

- Set **ITSP Proxy Address** to the IP Address for Swisscom Smart Business Connect.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Send Port** to **5060** and **Listen Port** to **5060**.
- Set **Use Network Topology Info** to **None** as NAT is not used in this configuration and the Network Topology settings defined in **Section 5.2** are not required.

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

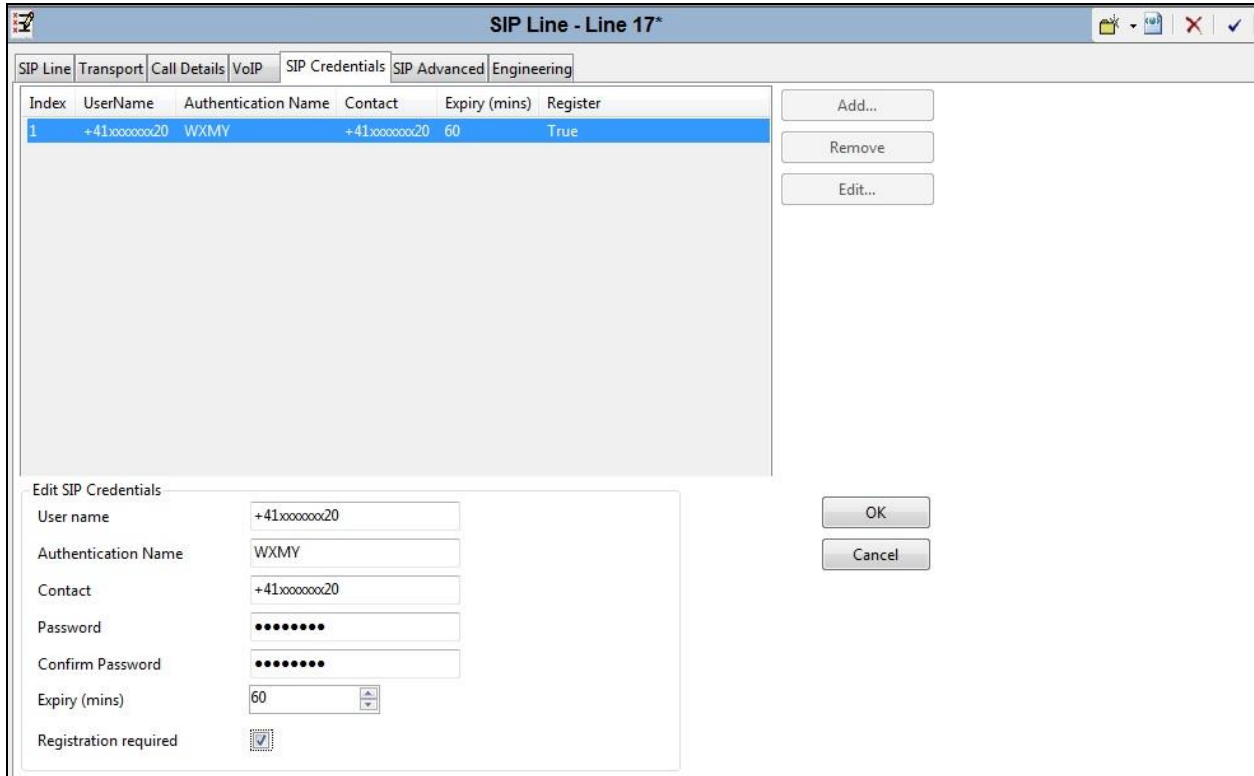
The screenshot shows the 'SIP Line - Line 17*' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '10.254.110.16'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'TCP', 'Send Port' is '5060', and 'Use Network Topology Info' is 'None'. 'Listen Port' is also '5060'. '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 credentials used for registration and authorisation on this line must be created. To define SIP credentials, first select the **SIP Credentials** tab. Click the **Add** button and the **New SIP Credentials** area will appear at the bottom of the pane.

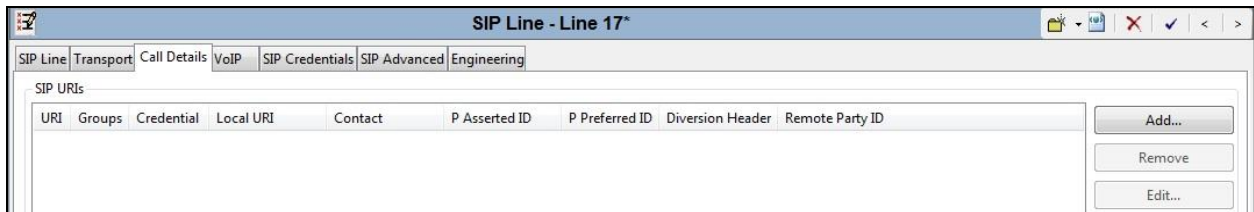
The screenshot shows the 'SIP Line - Line 17*' configuration window with the 'SIP Credentials' tab selected. The table below shows the columns for SIP credentials: Index, UserName, Authentication Name, Contact, Expiry (mins), and Register. To the right of the table are three buttons: 'Add...', 'Remove', and 'Edit...'.

Index	UserName	Authentication Name	Contact	Expiry (mins)	Register
-------	----------	---------------------	---------	---------------	----------

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



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**.



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

- Set **Incoming Group**. This is the value assigned for incoming calls that's analysed in the Incoming Call Route settings described in **Section 5.8**. In the test environment a value of **17** was used for the Swisscom SIP platform.
- Set **Outgoing Group**. This is the value assigned for outgoing calls that can be selected directly in the short code settings described in **Section 5.6**. 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
- For **Credentials**, select **1: <+41xxxxxx20>** from the pull-down menu since this configuration uses SIP registration
- Set **Local URI**, **Contact** and **P Asserted ID** to **Use Internal Data** for both the **Display** name and **Content**. On incoming calls, this will analyse the Request-Line sent by Swisscom and match to the SIP settings in the User profile as described in **Section 5.7**. On outgoing calls this will insert the SIP settings in the User profile into the relevant headers in the SIP messages.
- Set the **Outgoing Calls**, **Forwarding/Twinning** and **Incoming Calls** at their respective values of **Caller**, **Original Caller** and **Called** for the **Local URI** setting call details. Set the **Outgoing Calls**, **Forwarding/Twinning** and **Incoming Calls** at their respective values of **Caller**, **Caller** and **Called** for the **Contact** and **P Asserted ID** setting call details.

The screenshot shows the configuration window for a SIP Line. The 'New URI' section includes:

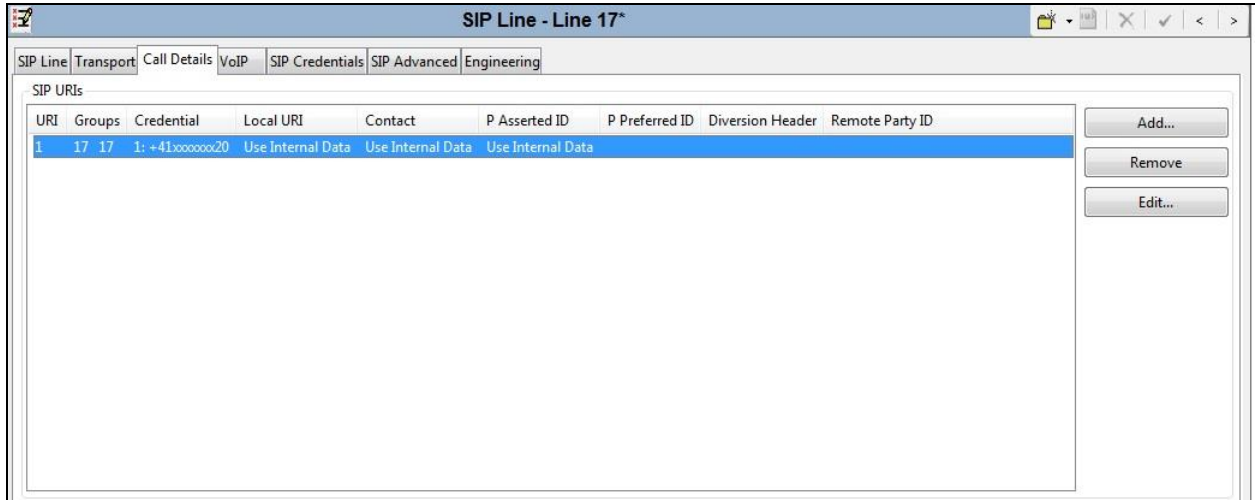
- Incoming Group: 17
- Outgoing Group: 17
- Max Sessions: 10
- Credentials: 1: +41xxxxxx20

The 'Field meaning' section is organized as follows:

	Outgoing Calls	Forwarding/Twinning	Incoming Calls
Local URI	Caller	Original Caller	Called
Contact	Caller	Caller	Called
P Asserted ID	Caller	Caller	Called
P Preferred ID	None	None	None
Diversion Header	None	None	None
Remote Party ID	None	None	None

Buttons at the bottom: OK, Cancel, Help.

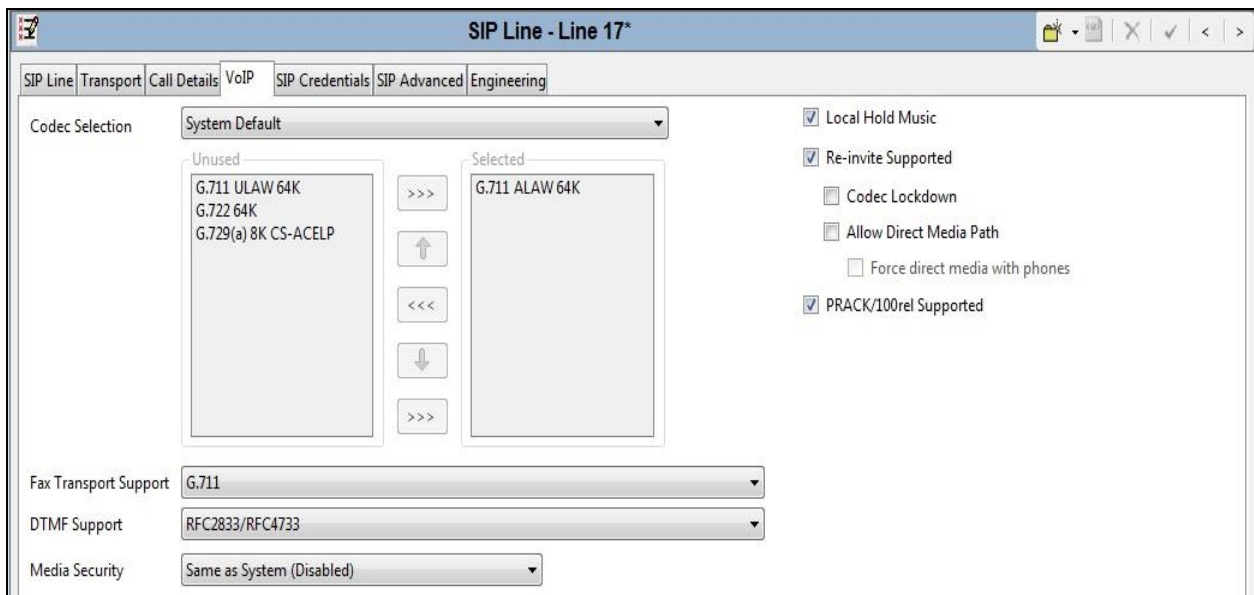
The following screenshot shows the completed configuration:



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 **Media Security to Same as System (Disabled)**.
- 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.



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

- Select **To Header** from the **Call Routing Method** drop down menu. In the test environment, Swisscom were sending the group number in the Request URI and the DDI number in the To Header.
- Check the **Use + for International** as E.164 numbering is used on the SIP Trunk.
- Select **Emergency Calls** from the **Send Location Info** drop down menu if required
- Default values may be used for all other parameters.

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

- Addressing:**
 - Association Method: By Source IP address
 - Call Routing Method: To Header
 - Use P-Called-Party:
 - Suppress DNS SRV Lookups:
- Identity:**
 - Use "phone-context":
 - Add user=phone:
 - Use + for International:
 - Use PAI for Privacy:
 - Use Domain for PAI:
 - Caller ID from From header:
 - Send From In Clear:
 - Cache Auth Credentials:
 - User-Agent and Server Headers:
 - Send Location Info: Emergency Calls
 - Add UUI header:
 - Add UUI header to redirected calls:
- Media:**
 - Allow Empty INVITE:
 - Send Empty re-INVITE:
 - Allow To Tag Change:
 - P-Early-Media Support: None
 - Send SilenceSupp=Off:
 - Force Early Direct Media:
 - Media Connection Preservation: Disabled
 - Indicate HOLD:
 - Media Security:
- Call Control:**
 - Call Initiation Timeout (s): 4
 - Call Queuing Timeout (m): 5
 - Service Busy Response: 503 - Service Unavailable
 - on No User Responding Send: 408-Request Timeout
 - Suppress Q.850 Reason Header:
 - Emulate NOTIFY for REFER:
 - No REFER if using Diversion:
- Calling Number Verification:**
 - Incoming Calls Handling: System

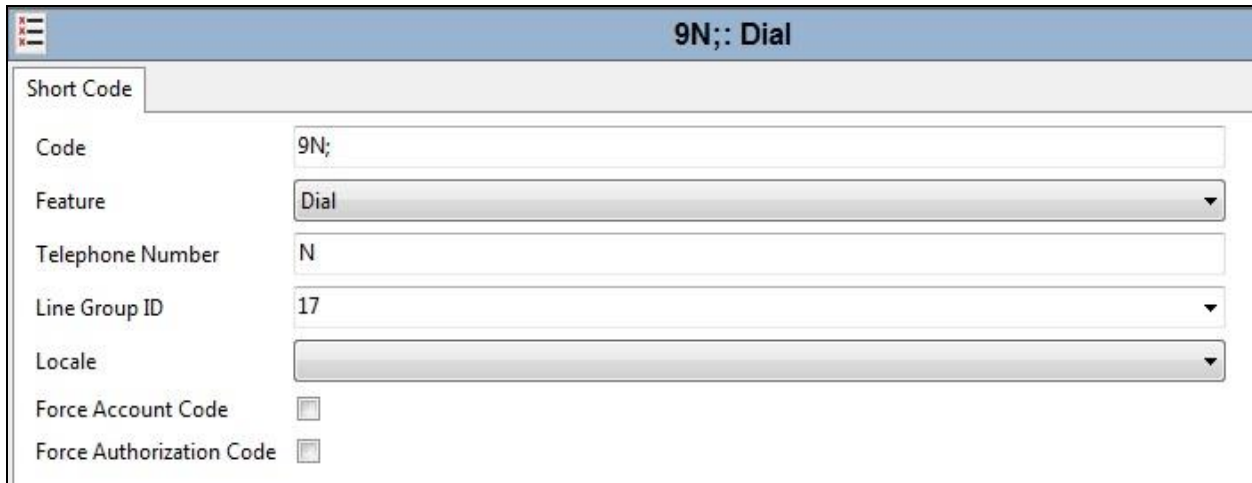
It is advisable at this stage to save the configuration as described in **Section 5.11**.

5.6. 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 5.5.2**.

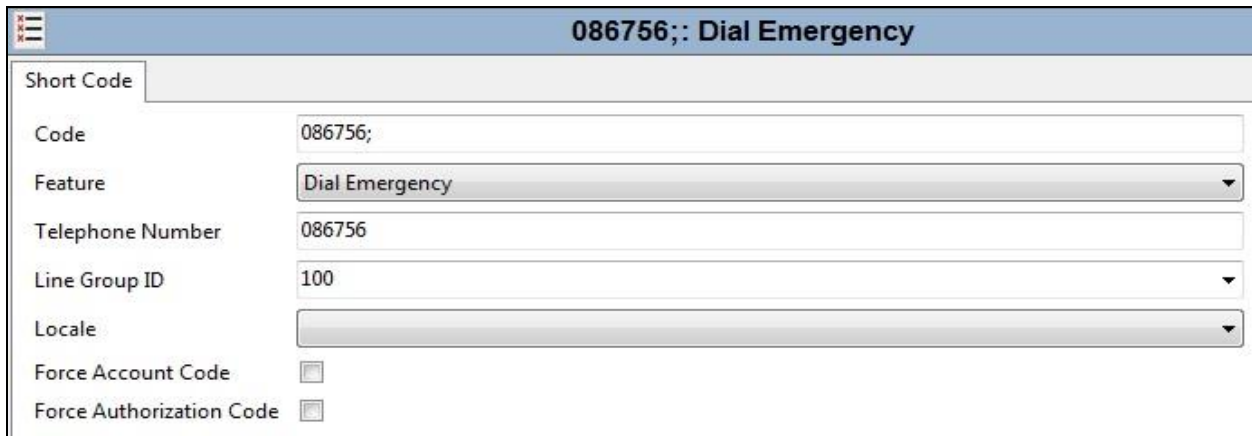
On completion, click the **OK** button (not shown).



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"/>

5.7. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.5.2**. To configure these settings, first navigate to **User** in the Navigation Pane. Select the **User** tab if any changes are required.

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

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

The screenshot displays the configuration page for a user named 'Ext89110: 89110'. The page is divided into several tabs: User, Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, and Button Programming. The 'User' tab is active, showing the following configuration fields:

- Name: Ext89110
- Password: [Redacted]
- Confirm Password: [Redacted]
- Unique Identity: [Empty]
- Audio Conference PIN: [Empty]
- Confirm Audio Conference PIN: [Empty]
- Account Status: Enabled
- Full Name: Ext89110
- Extension: 89110
- Email Address: [Empty]
- Locale: [Empty]
- Priority: 5
- System Phone Rights: None
- Profile: Basic User

Below the Profile dropdown, there are several checkboxes for additional features:

- Receptionist
- Enable Softphone
- Enable one-X Portal Services
- Enable one-X TeleCommuter
- Enable Remote Worker
- Enable Desktop/Tablet VoIP client
- Enable Mobile VoIP Client
- Enable MS Teams Client
- Send Mobility Email
- Web Collaboration

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 5.5.2**). As such, these fields should be set to one of the DDI numbers assigned to the enterprise from Swisscom.

The screenshot shows the configuration for the SIP tab of Ext89110: 89110*. The fields are as follows:

Field	Value
SIP Name	+414xxxxxx21
SIP Display Name (Alias)	+414xxxxxx21
Contact	+414xxxxxx21
Anonymous	<input checked="" type="checkbox"/>

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

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

The screenshot shows the configuration for the Mobility tab of Ext89110: 89110. The fields are as follows:

Field	Value
Simultaneous Coverage Delay (secs)	0
MS Teams URI	
Internal Twinning	<input type="checkbox"/>
Twinned Handset	<None>
Maximum Number of Calls	1
Twin Bridge Appearances	<input type="checkbox"/>
Twin Coverage Appearances	<input type="checkbox"/>
Twin Line Appearances	<input type="checkbox"/>
Mobility Features	<input checked="" type="checkbox"/>
Mobile Twinning	<input checked="" type="checkbox"/>
Fallback Twinning	<input type="checkbox"/>
Twinned Mobile Number (including dial access code)	900353xxxxxx52
Twinning Time Profile	<None>
Mobile Dial Delay (secs)	3
Mobile Answer Guard (secs)	0
Hunt group calls eligible for mobile twinning	<input type="checkbox"/>
Forwarded calls eligible for mobile twinning	<input type="checkbox"/>
Twin When Logged Out	<input type="checkbox"/>
one-X Mobile Client	<input type="checkbox"/>
Mobile Call Control	<input checked="" type="checkbox"/>
Mobile Callback	<input checked="" type="checkbox"/>

5.8. 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 5.5.2**.
- 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 the configuration form for an incoming call route. The title bar displays '17 +414xxxxxx21'. The 'Standard' tab is selected. The fields are as follows:

Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	+414xxxxxx21
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 **+414xxxxxx21** on line 17 are routed to extension 89110.

The screenshot shows the 'Destinations' tab of the configuration form. The title bar displays '17 +414xxxxxx21'. The 'Destinations' tab is selected. The table below shows the destination configuration:

TimeProfile	Destination
▶ Default Value	89110 Extn89110

5.9. 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 the configuration page for a location named 'Galway'. The interface is divided into several sections:

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

Buttons for 'Edit' and 'Delete' are visible at the bottom right of the configuration area.

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

The screenshot displays the 'Galway' application interface with the 'Address' tab selected. At the top, there are tabs for 'Location' and 'Address'. Below the tabs, the 'Country Code' is set to 'IE'. A warning message states: 'Please refer to the help for Information regarding this screen. Failure to format the address properly could result in improper address association.' The address fields are organized into several sections:

A1	Connacht	HNO	
A2	Galway	HNS	
A3	Galway	LMK	
A4	Mervue	BLD	
A5	Business Park	LOC	
A6	Unit 25-29	PLC	
		FLR	
		UNIT	GSSCP Unit
		ROOM	
		SEAT	
RD		NAM	GSSCP
RDSEC		ADDCODE	
RDBR		PCN	
RDSUBBR		PC	
PRD		POBOX	
POD			
STS			
PRM			
POM			

5.10. Fax

At Release 12.0, both G.711 and T.38 Fax is supported on IP Office Server Edition when using an IP Office Expansion (500 V2). The Swisscom Smart Business Connect testing was carried out using this configuration with only the analog extension for the fax machine on the Expansion. In this configuration, the G.711 fax settings are configured on the SIP line between the Expansion and the Server.

5.10.1. Analog User

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is a navigation tree under 'Configuration' with 'User (6)' selected. The main area shows the configuration for 'Analog89119: 89119'. The 'User' tab is active, showing fields for Name, Password, Confirm Password, Unique Identity, Audio Conference PIN, Confirm Audio Conference PIN, Account Status (set to 'Enabled'), Full Name, Extension (89119), Email Address, Locale, Priority (5), System Phone Rights (None), and Profile (Basic User). There are also checkboxes for 'Receptionist' and 'Enable Softphone'.

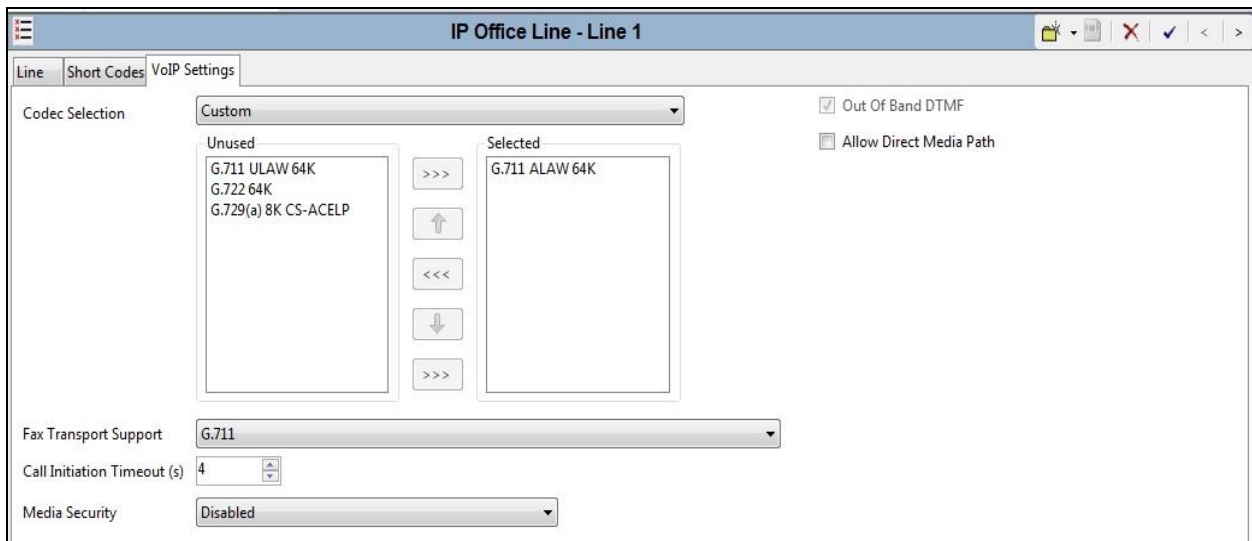
Configure other settings as described in **Section 5.7**.

5.10.2. G.711 Fax Settings

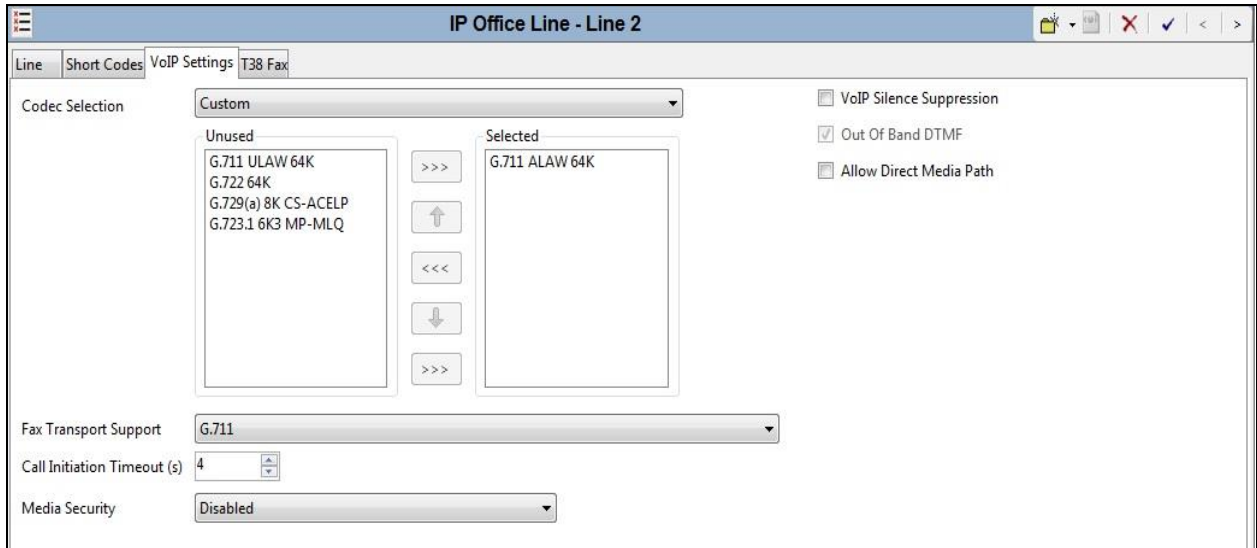
The G.711 Fax settings are defined on the SIP Line between the Expansion and the Server. Note that the VoIP settings for G.711 are required in three places in this configuration:

- The SIP Line for the Swisscom Smart Business Connect SIP platform as described in **Section 5.5.2**.
- 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 **G711**. The following screenshot shows the VoIP Settings for the IP Office Line between the Server and the Expansion on the Expansion:



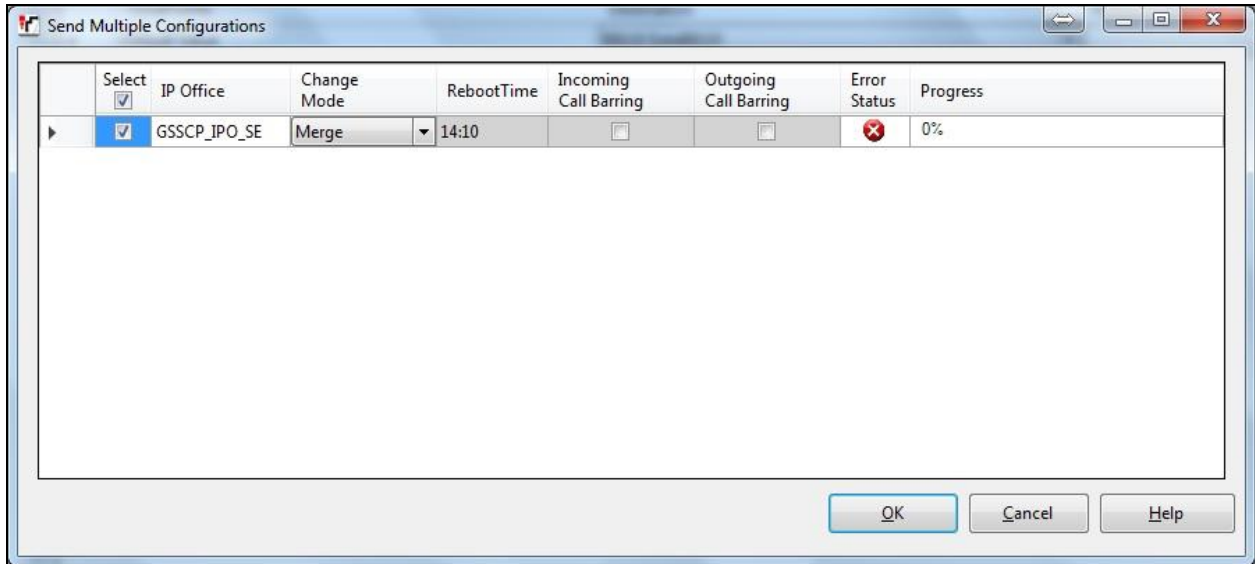
The following shows the **VoIP Settings** tab in the IP Office Line for the Expansion in the Server configuration:



Refer to **Section 5.5.2** for the VoIP Settings on the SIP Line for the Swisscom SIP Trunk.

5.11. Save Configuration

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



6. Configure the Swisscom Equipment

The configuration of the Swisscom Smart Business Connect equipment used to support the SIP Trunk is outside 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.

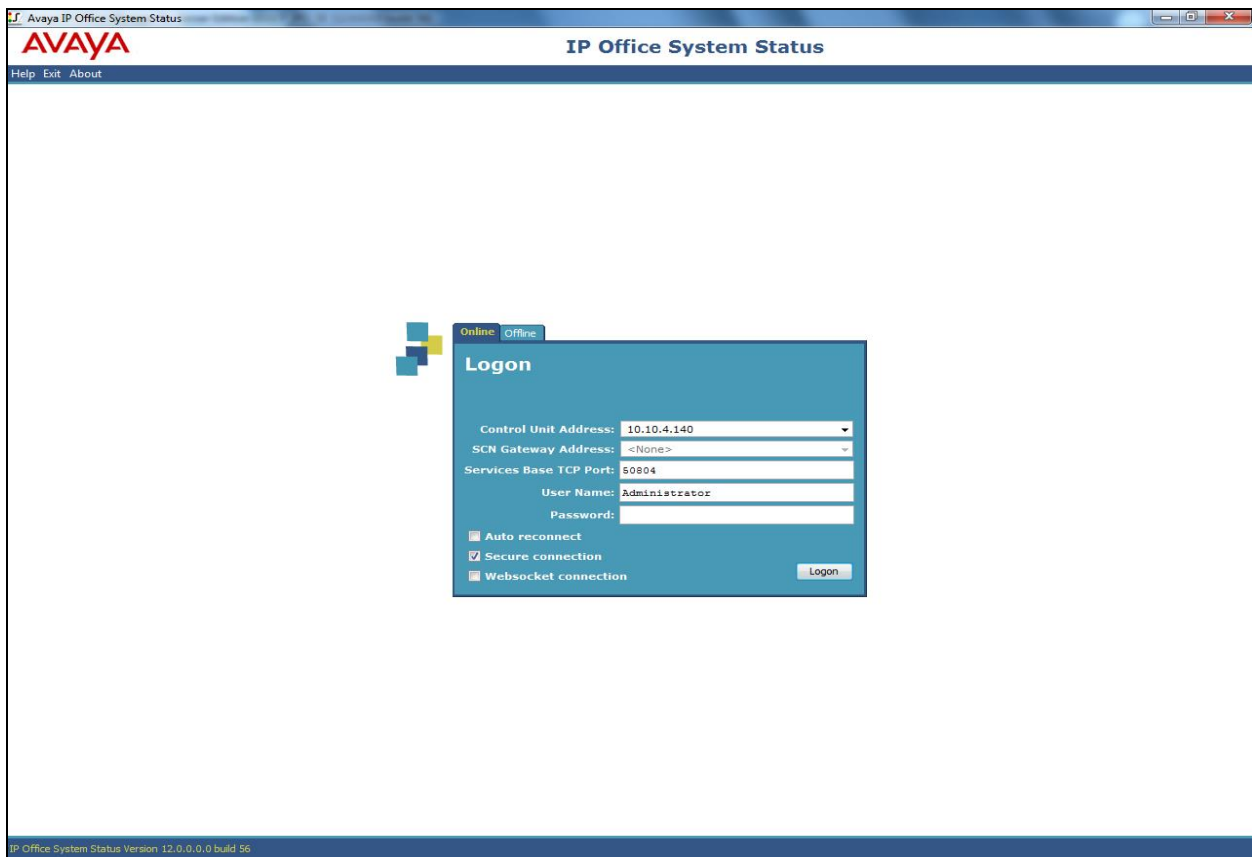
7. Verification Steps

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

7.1. 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.

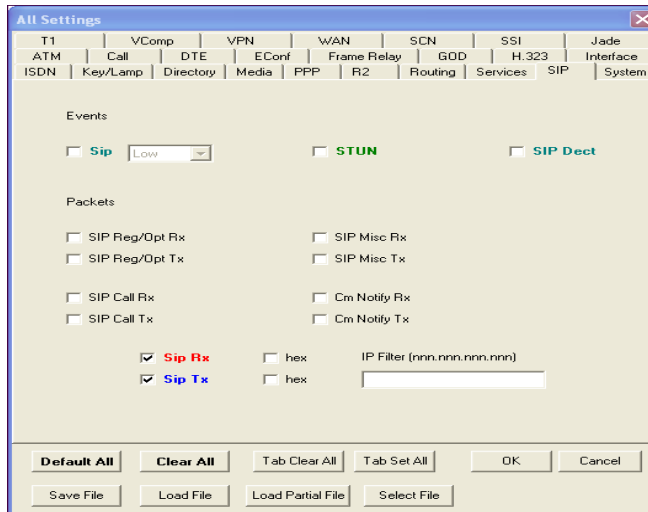
SIP Trunk Summary

Line Service State: In Service
Peer Domain Name: join.swisscom.com
Resolved Address: 10.254.110.16
Line Number: 17
Number of Administered Channels: 10
Number of Channels in Use: 0
Administered Compression: G711 A
Silence Suppression: Off
Media Stream: RTP
Layer 4 Protocol: UDP
SIP Trunk Channel Licenses: 300
SIP Trunk Channel Licenses in Use: 0  0%

Channel Number	URI Gr...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Los...	Transmit Jitter	Transmit Packet Los...
1			Idle	02:31:30											
2			Idle	02:31:30											
3			Idle	02:31:30											
4			Idle	02:31:30											
5			Idle	02:31:30											
6			Idle	02:31:30											
7			Idle	02:31:30											
8			Idle	02:31:30											
9			Idle	02:31:30											
10			Idle	02:31:30											

7.2. 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 REGISTERS being sent between IP Office and a SIP phone.

```

Avaya IP Office SysMonitor - [STOPPED] Monitoring 10.10.4.140 (GSSCP_IPO_SE (Server Edition(P))); Log Settings - C:\Users\...\sysmonitorsettings.ini
File Edit View Filters Status Help
11:57:17 522168690mS SIP Rx: TCP 10.10.5.62:55982 -> 10.10.4.140:5060
REGISTER sip:avaya.com SIP/2.0
From: <sip:89115@avaya.com>;tag=666ae2b9407b2376e3c6512w3g25c1zr5v2_F89115
To: <sip:89115@avaya.com>
Call-ID: 1_666ae2b969ec034251711256115a105q1neul4_R89115
CSeq: 408 REGISTER
Max-Forwards: 70
Via: SIP/2.0/TCP 10.10.5.62:55982;branch=z9hG4bKod_6672c79c-277f4e876q50335f3448495t4y212952_R89115;keep
Supported: eventlist,feature-ref,replaces,tdialog,vnd.avaya.stimulus-ipo
Allow: INVITE,ACK,BYE,CANCEL,SUBSCRIBE,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
User-Agent: Avaya 1179 IP Phone 4.0.10.3.2 c81feac884d4
Contact: <sip:89115@10.10.5.62:55982>;transport=tcp;avaya-sc-enabled;q=1;expires=900;avaya-actions="presence.initiate-pubsub,presence.redirect";+avaya.gmtoffset=4.0.10.3.2";+av.ip.mode=4;+av.sdp.anat;+av.sip.sig=4;+av.sip.media=4;+av.sip.ipc tolerance;+sip.instance="urn:uuid:00000000-0000-1000-8000-c81feac884d4";reg-id=1
Authorization: Digest realm="ipoffice",nonce="415b70be55e8b05d66c7",uri="sip:avaya.com",response="c5e8a5cc543983187cfd30bca85529",username="89115"
Content-Length: 0

11:57:17 522168690mS Sip: TCP packet known set owner
11:57:17 522168690mS Sip: SIP REG: 89115 +sip.instance="urn:uuid:00000000-0000-1000-8000-c81feac884d4"
11:57:17 522168690mS Sip: SIP REG: 89115 reg-id=1
11:57:17 522168690mS Sip: SIP FindUserFromAuthentication, <89115> cfg_user d00d4b50 from_unregister 0 is_ipo_behind_nat 0 is_phone_behind_nat 0
11:57:17 522168691mS Sip: authenticateChallengeRtn 1 cfg_user d00d4b50
11:57:17 522168691mS Sip: SIP REG: user 89115 authenticated
11:57:17 522168691mS Sip: (98039ae0) SendSIPResponse: REGISTER code 200 SENT TO 10.10.5.62 55982
11:57:17 522168691mS SIP Tx: TCP 10.10.4.140:5060 -> 10.10.5.62:55982
SIP/2.0 200 OK
Via: SIP/2.0/TCP 10.10.5.62:55982;branch=z9hG4bKod_6672c79c-277f4e876q50335f3448495t4y212952_R89115;keep
From: <sip:89115@avaya.com>;tag=666ae2b9407b2376e3c6512w3g25c1zr5v2_F89115
Call-ID: 1_666ae2b969ec034251711256115a105q1neul4_R89115
CSeq: 408 REGISTER
User-Agent: IP Office 12.0.0.0 build 55
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Contact: <sip:89115@10.10.5.62:55982>;transport=tcp;avaya-sc-enabled
Content-Type: application/vnd.avaya.stimulus-ipo
Date: Wed, 19 Jun 2024 10:57:17 GMT
Expires: 3600
Supported: vnd.avaya.stimulus-ipo
Server: IP Office 12.0.0.0 build 55
To: <sip:89115@avaya.com>;tag=31021a6dacdae0a2
Content-Length: 50

<ipo>
backup_ipoffice_server="0.0.0.0";
</ipo>

```

8. Conclusion

These Application Notes describe the procedures required to configure the connectivity between Avaya IP Office Server Edition R12.0 and Swisscom Smart Business Connect SIP 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 Server Edition R12.0 can be configured to interoperate successfully with Swisscom's SIP Trunk service. Swisscom's Smart Business Connect is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

9. Additional References

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

- [1] *Deploying IP Office as Virtual Servers*, Release 12.0, Apr 2024.
- [2] *Deploying IP Office Server Edition Servers*, Release 12.0, Apr 2024.
- [3] *Deploying an IP500 V2 IP Office System*, Release 12.0, Apr 2024.
- [4] *Administering Avaya IP Office with IP Office Web Manager*, Release 12.0, May 2024.
- [5] *Administering Avaya IP Office with IP Office Manager*, Release 12.0, May 2024.
- [6] *Using Avaya IP Office System Status*, Apr 2024.
- [7] *Using IP Office System Monitor*, Apr 2024.
- [8] *Administrating Voicemail Pro*, Release 12.0, May 2024.
- [9] *Using Avaya Workplace Client for Windows*, Nov 2023.
- [10] *IP Office SIP Phone Installation Notes*, Apr 2024..
- [11] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

2024 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.