Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office 10.1 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.

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 at the Avaya Solution and Interoperability Test Lab.

1. Introduction

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

Avaya IP Office was connected to the Swisscom Smart Business Connect SIP trunk via a VPN established over the internet.

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 and analogue telephones at the enterprise. Calls routed to the enterprise via the SIP trunk from Swisscom.
- Outgoing PSTN calls from various phone types including H.323, SIP and analogue telephones at the enterprise. Calls routed from the enterprise via the SIP trunk to Swisscom.
- Inbound and outbound PSTN calls to/from an Avaya Communicator for Windows client.
- Various call types including: local, international, toll free (outbound) and directory assistance.
- Calls using G.711A, G.711MU and G.729A codec's.
- Caller ID presentation and Caller ID restriction.
- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobile twinning.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Swisscom Smart Business Connect. The following observations were made during the test:

- When making an outbound call that was not answered, after ninety seconds the ringback tone stopped and there was silence. Expected behaviour is a failure tone or an announcement.
- When making an outbound call to an invalid number, the network sent 200 OK (Answer) before playing an announcement. The behaviour more commonly observed is for a backwards transmission path established using SIP 183 Session Progress to be used to play a tone or announcement to the caller. Using 200 OK completes the SIP dialogue and establishes the call making it indistinguishable from a successful call.
- When making some calls with multiple PSTN endpoints, for example conferencing, audio delays were observed. These were deemed to be a characteristic of the test environment and not a SIP interoperability issue.

2.3. Features Not Tested

The following features and functionality were not tested:

- No inbound toll-free access was available for testing
- Emergency Calls were not tested as the IP Office location data was not defined.
- Fax was not tested as this is not offered to Swisscom customers on IP Office.

2.4. 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: cbu.incident-voice@swisscom.com.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to Swisscom Smart Business Connect. Located at the enterprise site are an Avaya IP Office Server Edition and an Avaya IP Office 500 v2 as an Expansion. 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 and an Avaya Analogue Telephone. The site also has a Windows 7 PC running Avaya IP Office Manager to configure the Avaya IP Office as well as Avaya Communicator for Windows for mobility testing. For security purposes, PSTN routable phone numbers used in the compliance test are not shown in full.

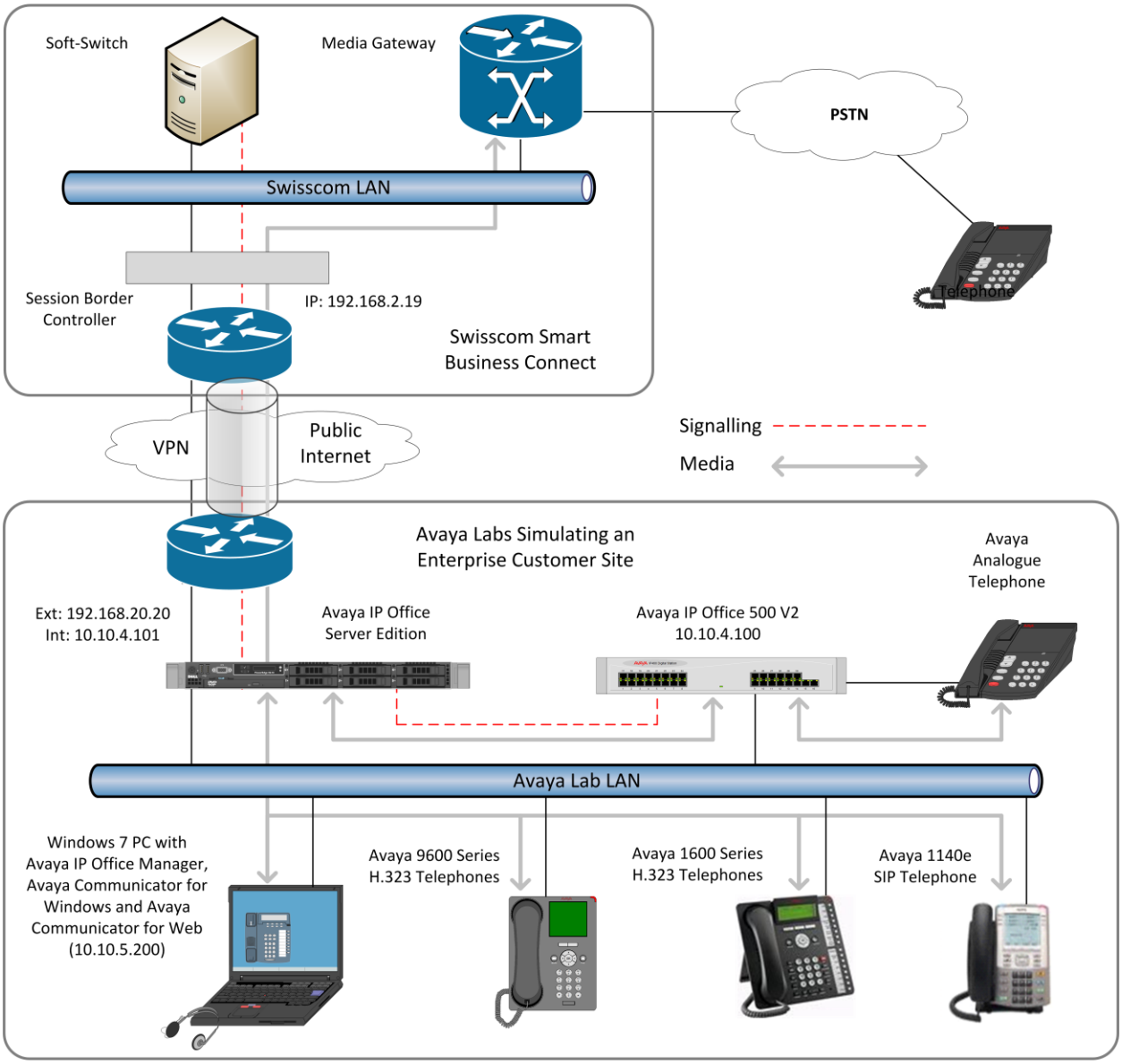


Figure 1: Swisscom Smart Business Connect to Avaya IP Office Topology

4. Equipment and Software Validated

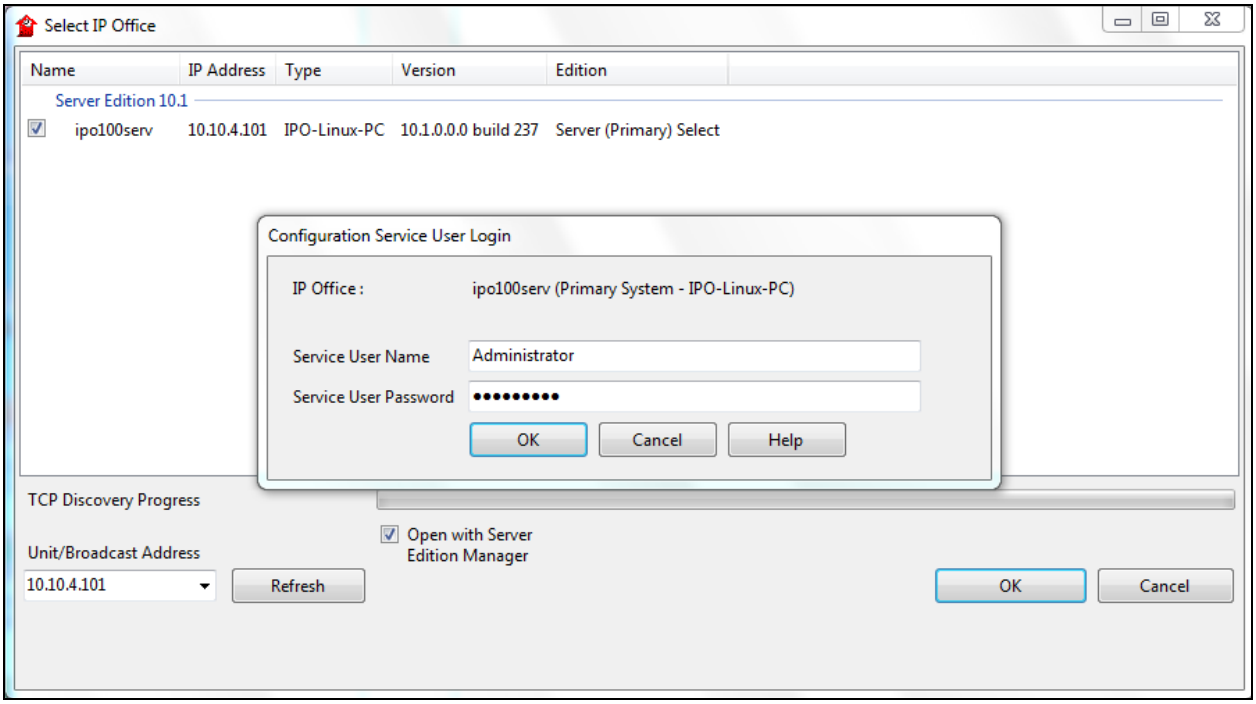
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	10.1.0.0.0 build 237
Avaya IP Office 500 V2 Expansion	10.1.0.0.0 build 237
Avaya 1140e IP SIP Telephone	04.04.23.00
Avaya 1608 IP Phone (H.323)	1.350B
Avaya 9611 IP Phone (H.323)	6.6.4.01
Avaya 98390 Analogue Phone	N/A
Avaya Communicator for Windows	2.1.4.0
Avaya IP Office Server Edition Manager	Version 10.1.0.0.0 build 237
Swisscom Smart Business Connect	
Cisco C881-K9 Integrated Services Router	IOS 15.6

Testing was performed with IP Office Server Edition with 500 V2 Expansion R10.1. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. Note that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks.

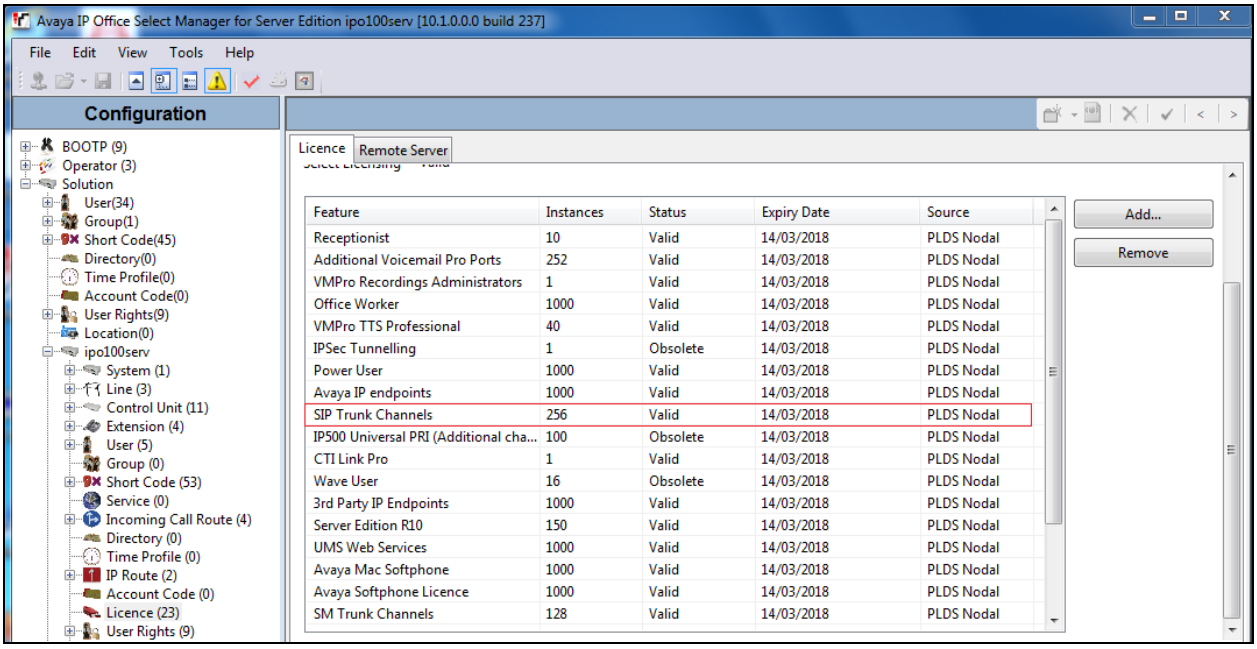
5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to Swisscom Smart Business Connect. 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** (not shown), 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 (such as mobile twinning) is assumed to already be in place.



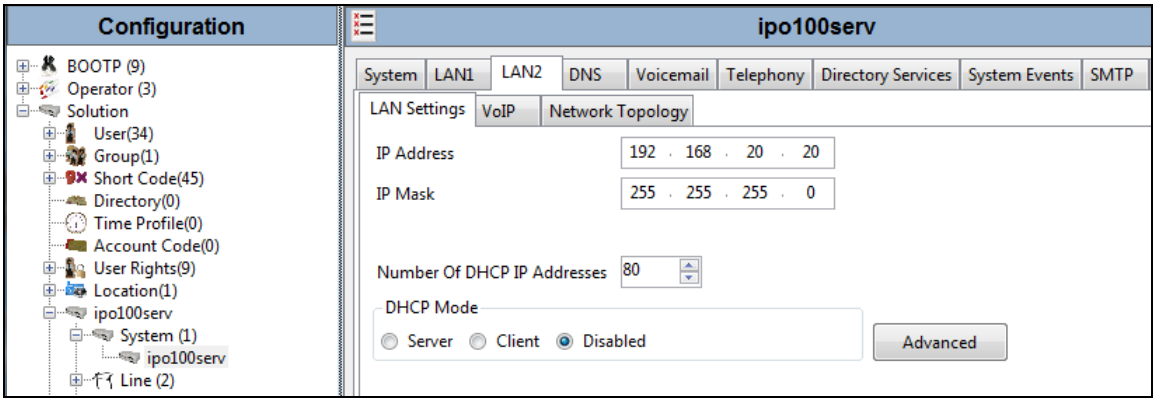
5.1. Verify System Capacity

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

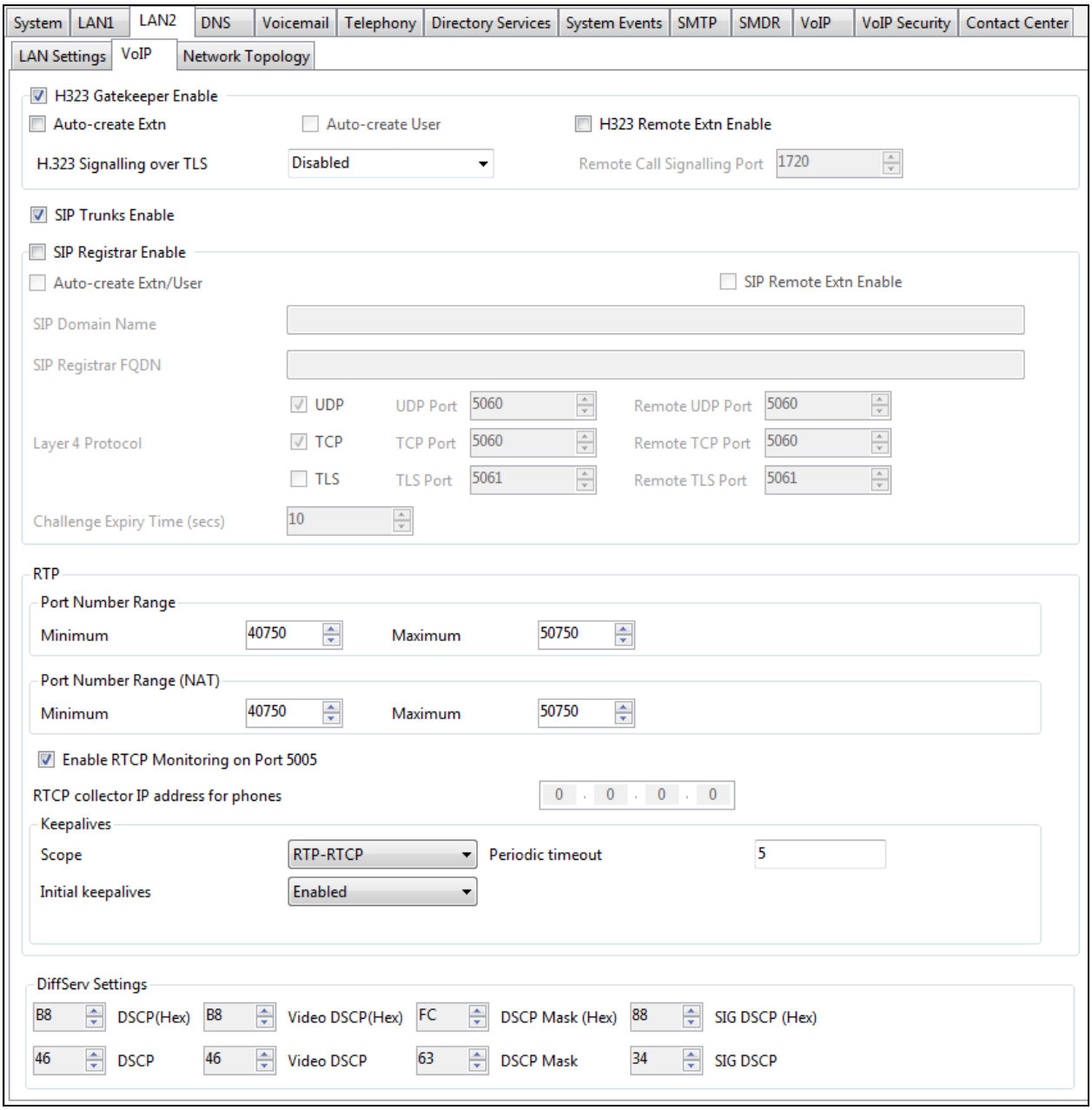


5.2. LAN2

In the sample configuration, the LAN2 port was used to connect the Avaya IP Office to Swisscom Smart Business Connect. To access the LAN2 settings, first navigate to **System → <IP Office Name>** in the Navigation Pane where <IP Office Name> is the name of the IP Office. This is **ipo100serv** for the Server Edition in the GSSCP test environment. Navigate to the **LAN2 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the external interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the OK button (not shown).



On the **VoIP** tab in the Details Pane, check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. Scroll down for further configuration. Define **Keepalives** as required, during testing **RTP-RTCP** was used with a **Periodic Timeout** of **5**. The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Based on this setting, Avaya IP Office requests RTP media to be sent to a UDP port in the configurable range for calls using LAN2. The range used for testing was the Linux default setting of **40750** to **50750**.

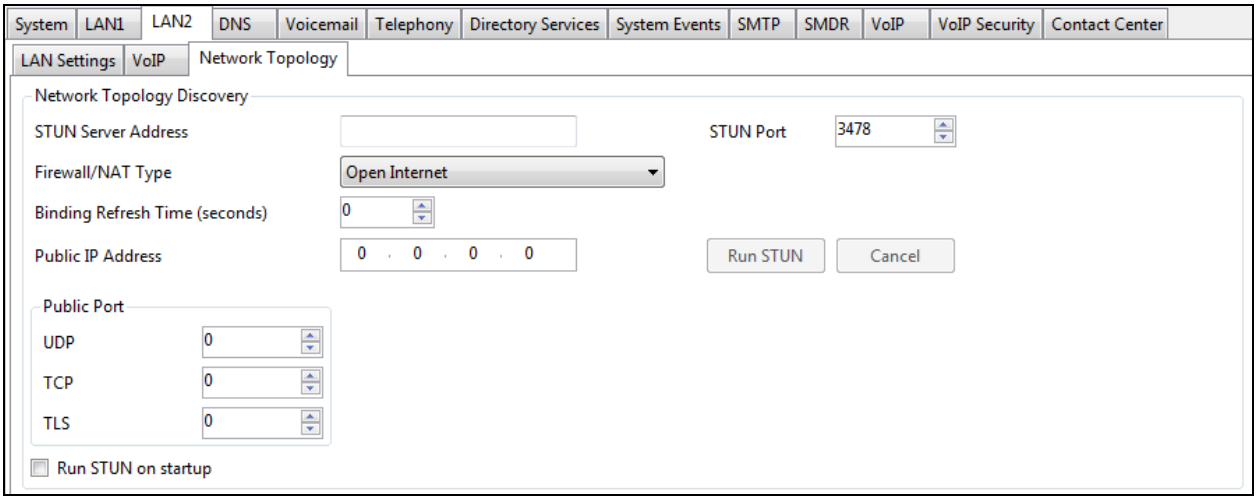


Note: Avaya IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP header with specific values to support Quality of Services policies for both signalling and media (not shown). DSCP for media can be set for both voice and video. The **DSCP** field is the value used for voice and the **SIG DSCP** is the value used for signalling. For the compliance test, the DSCP values were left at their default values.

All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).

On the **Network Topology** tab in the Details Pane, leave the **STUN Server Address** blank and the Firewall/NAT Type at **Open Internet** as NAT is not required in this configuration.

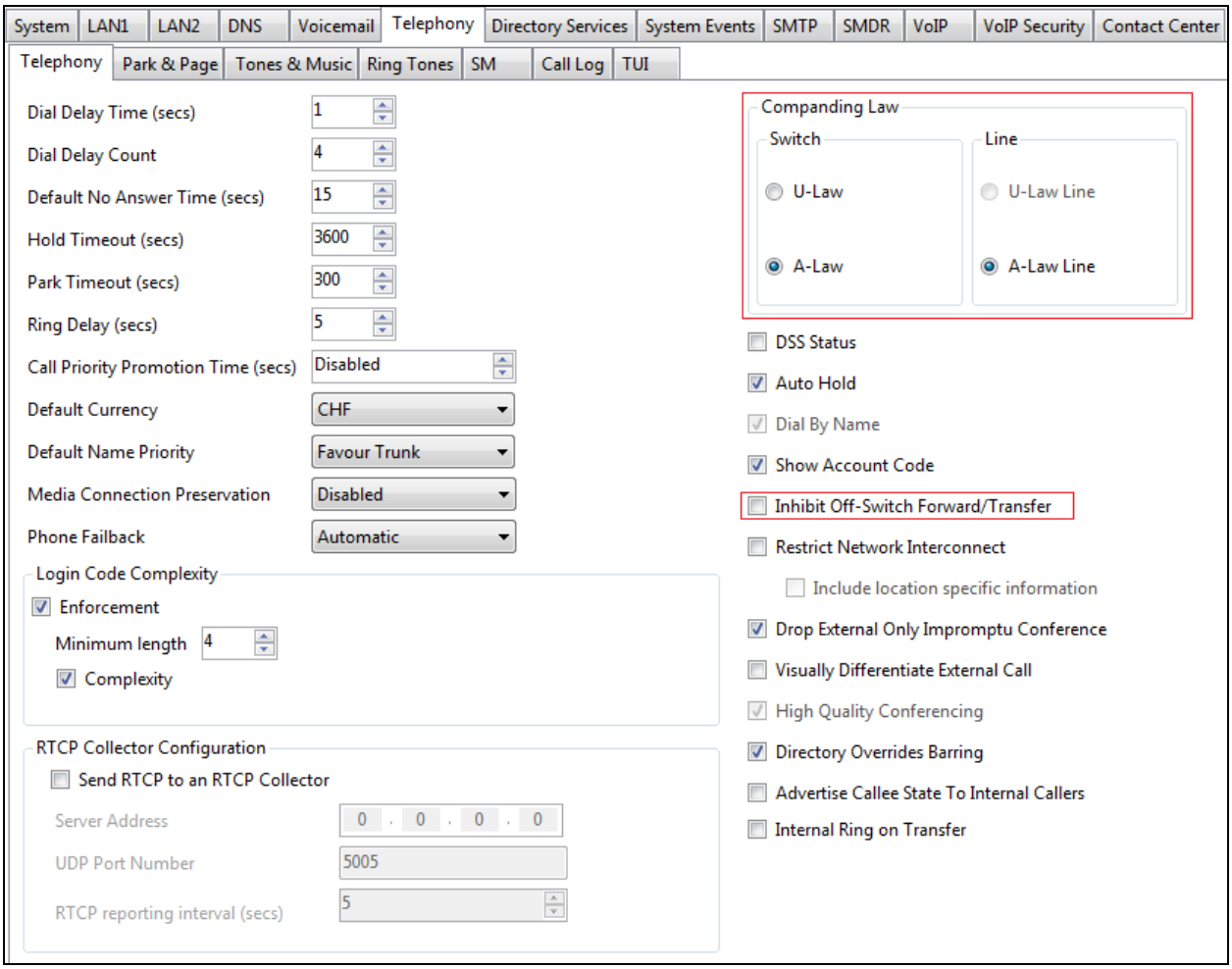
The Network Topology tab can be used to set the **Binding Refresh Time** for the periodic sending of OPTIONS. This is intended for use where OPTIONS are required at intervals of less than 300 seconds. A value of **0** uses the default of 300 seconds.



Note: During compliance testing, registration was used with REGISTER messages sent at intervals defined in the SIP URI settings described in **Section 5.6.2**. These REGISTER messages act as a check of the SIP Trunk so that OPTIONS messages are not critical.

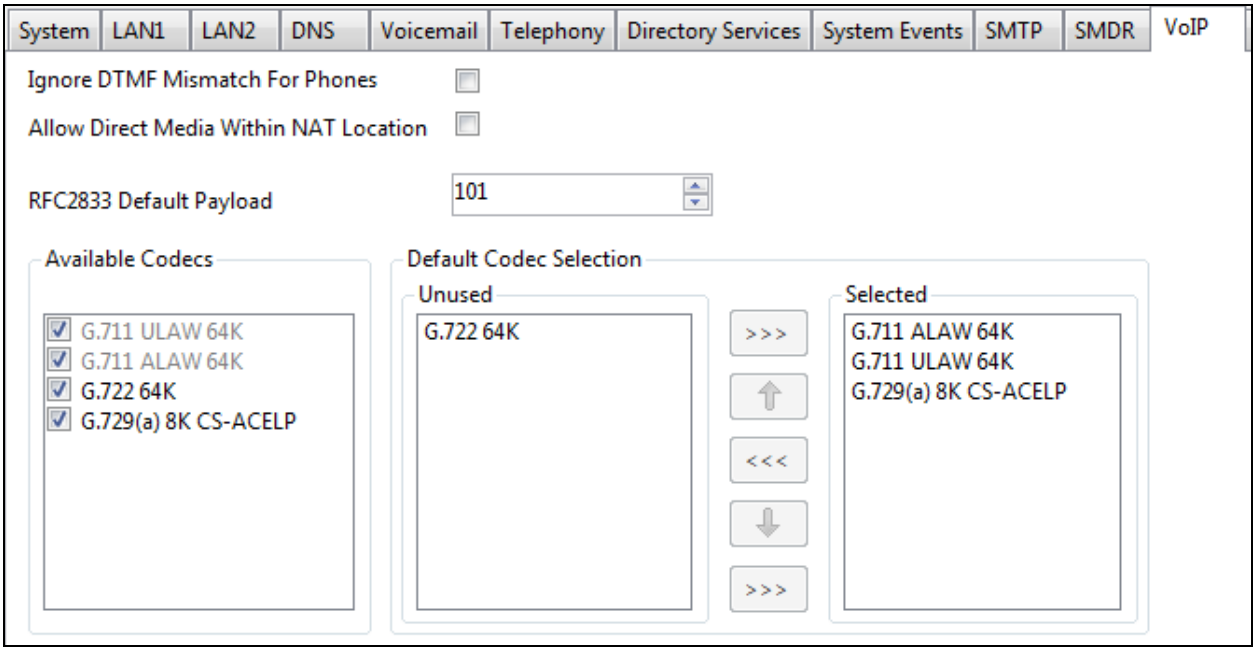
5.3. System Telephony Settings

Navigate to the **Telephony → Telephony** tab on the Details Pane. Choose the **Companding Law** typical for the enterprise location. For Europe, **A-Law** 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. Codec Settings

Navigate to the **VoIP** tab on the Details Pane. Check the **Available Codecs** boxes as required for the IP endpoints. 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**, **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** were used as the default codec's. The order of priority can be changed using the vertical arrows. On completion, click the **OK** button (not shown).



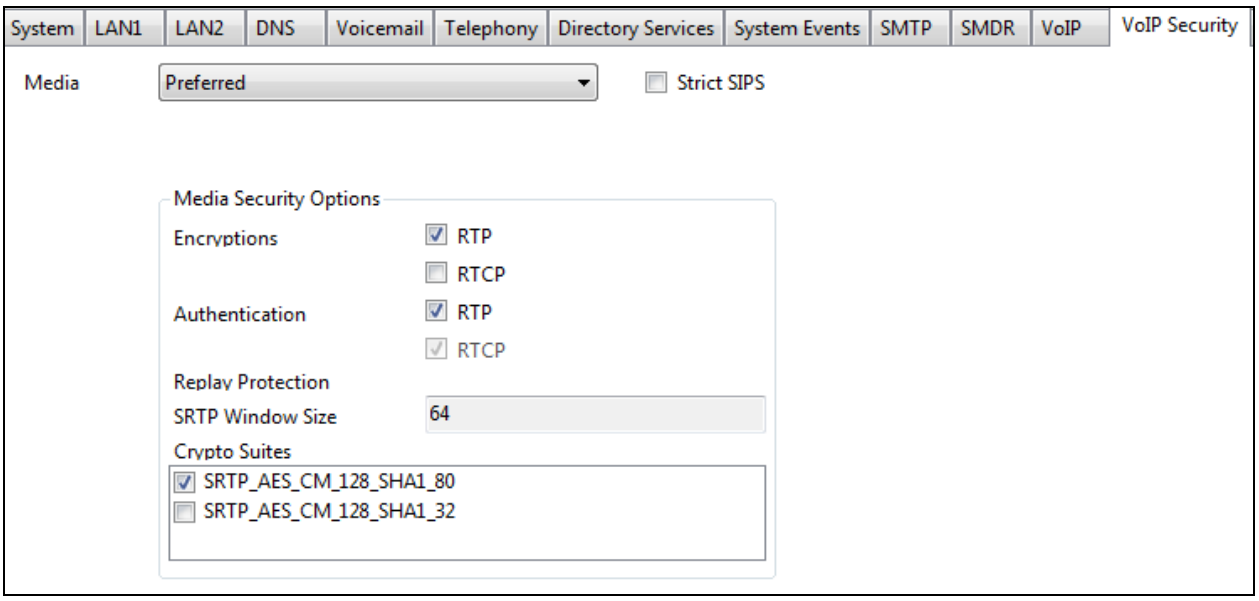
Note: The codec settings for IP endpoints can also be used for the SIP Trunk by selecting **System Default** in the **Codec Selection** as shown in **Section 5.6.2**.

5.5. VoIP Security

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. To secure media using SRTP, navigate to the **VoIP Security** tab on the Details Pane. Select the required level of security in the **Media** dropdown menu, in the test environment **Preferred** was selected.

Selecting Preferred allows further configuration of media security. In the test environment, **Encryption** and **Authentication** was applied to **RTP**. The **SRTP Window Size** was left at the default value of **64** and in the **Crypto Suites** box, only **SRT_AES_CM_128_SHA1_80** was selected. These settings only applied within the enterprise, VoIP Security was not used on the SIP Trunk.

VoIP Security is set according to customer requirements; the example shows the Lab settings:



5.6. 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 5.6.1** 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**.

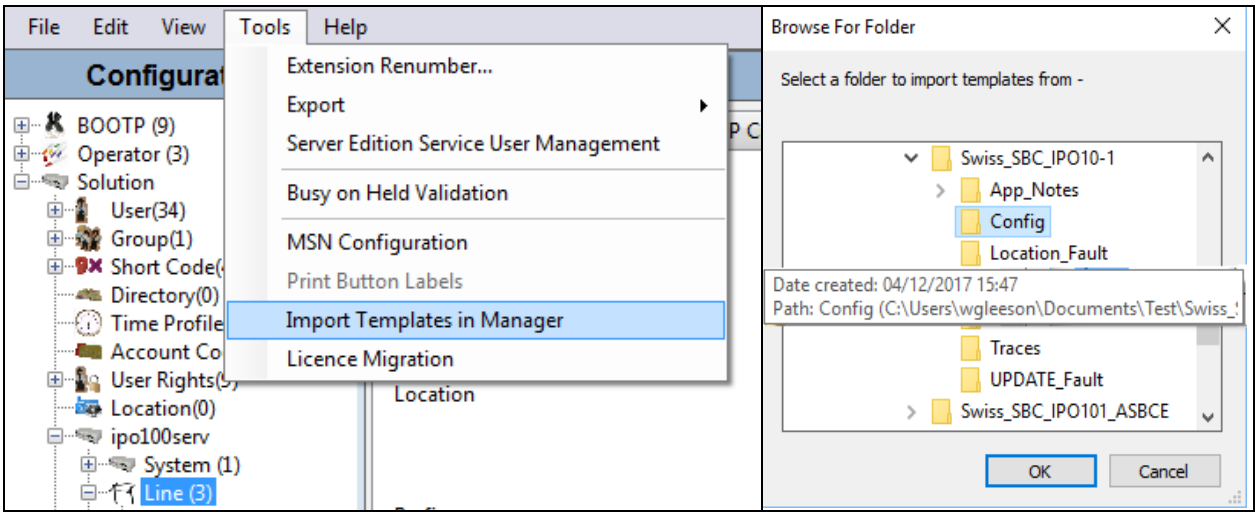
Also, the following SIP Line settings are not supported on Basic Edition:

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

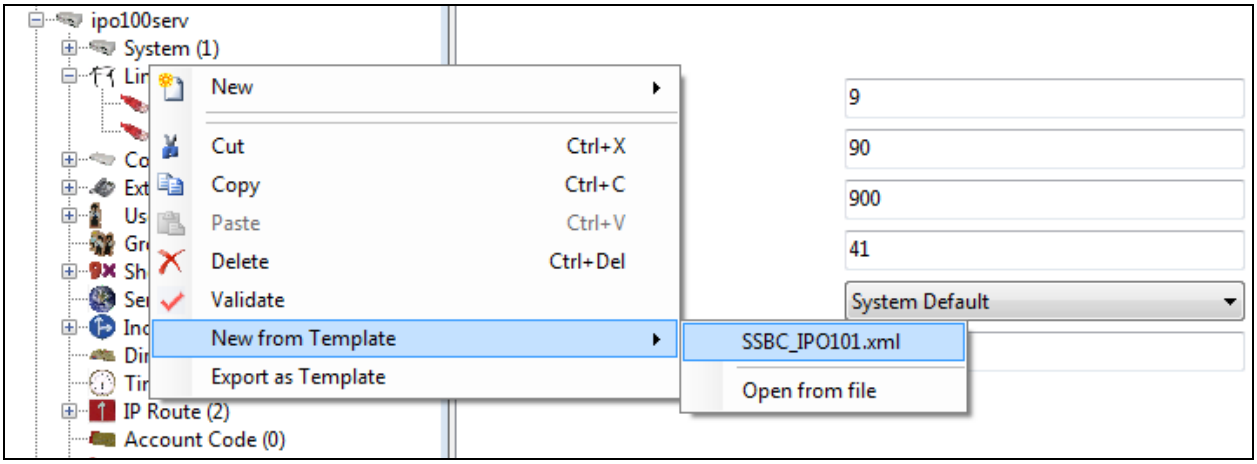
Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New→SIP Line** (not shown). Then, follow the steps outlined in **Section 5.6.2**.

5.6.1. SIP Line From Template

Copy the template file to the computer where IP Office Manager is installed. The template can be used in one of two ways: import it and select directly as an option when creating the SIP Line; create the SIP Line from the template as a file on the local machine. To import the file, click on the **Tools** tab and select **Import Templates in Manager**.

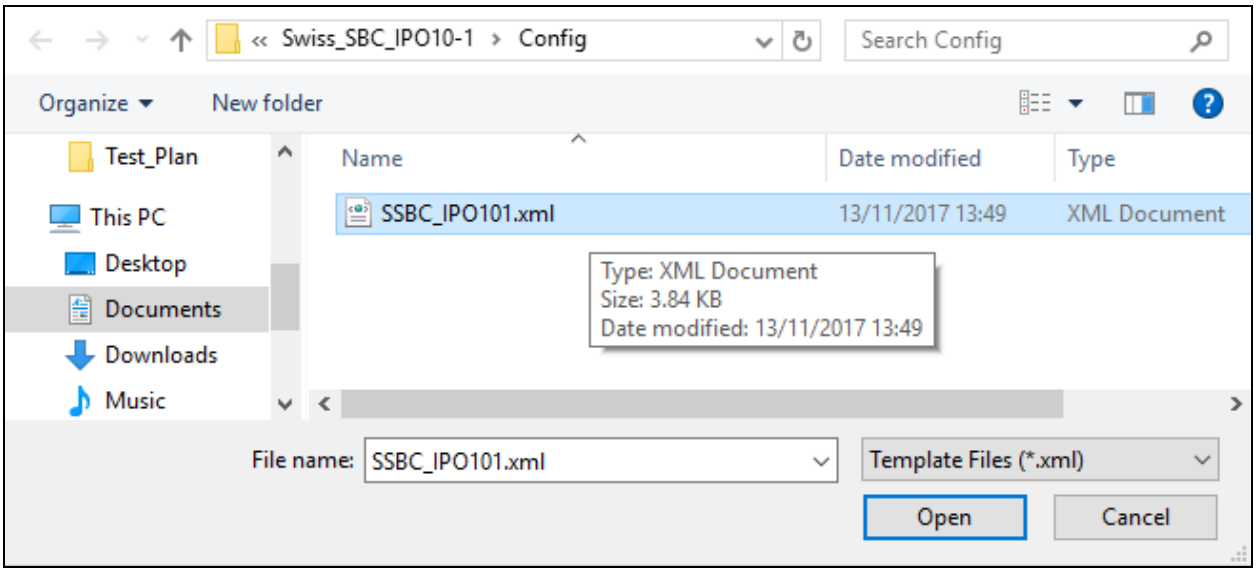


To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New from Template**. If the template file was imported as shown above, select it directly:



Alternatively, if the template file was not imported, select **Open from file**.

Browse to the appropriate folder on the local machine and select **Template Files (*.xml)** from the drop down menu:

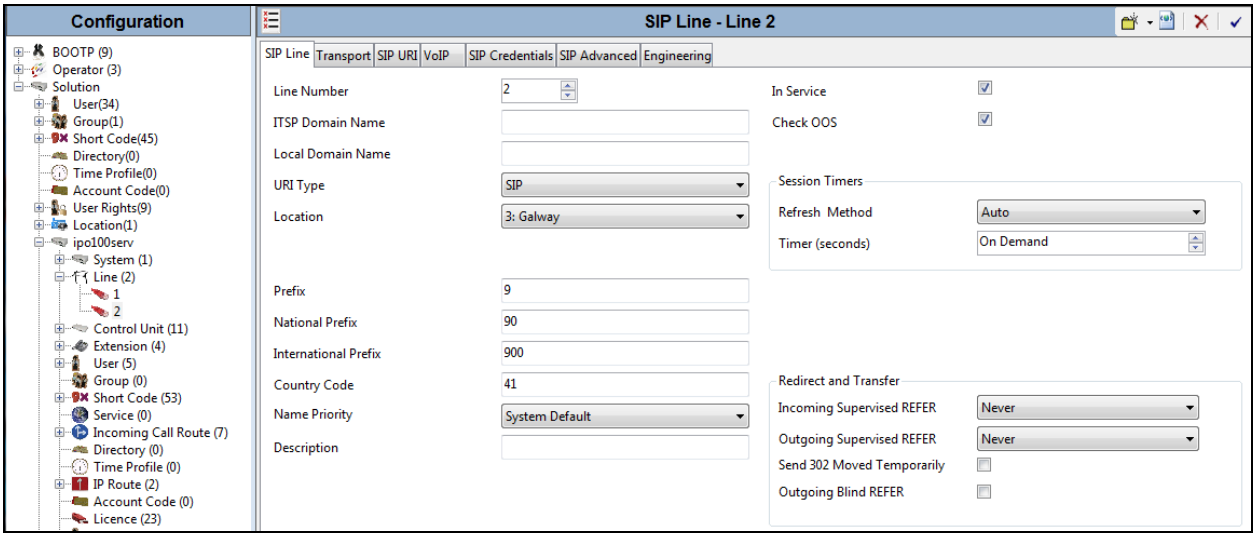


The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.6.2**.

5.6.2. Manual SIP Line Configuration

To create a SIP Line or to modify a SIP Line previously created from the template, navigate to **Line** in the Navigation Pane. Right click on **Line** and select **New** (not shown) or select a SIP Line previously created. On the **SIP Line** tab in the Details Pane, configure the parameters below to connect to Swisscom Smart Business Connect.

- Set **Prefix** to the digit, if any, used to access an outside line. In the test environment, this was **9**.
- Set **Location** to that defined for Emergency calls as described in **Section 5.11**.
- 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. If a prefix digit is used for outbound calls it should be included here. The example shows **90** and **900** respectively.
- Set **Country Code** to **41** for Switzerland for number conversion, in conjunction with the above prefixes, as follows: outbound national called party numbers are converted to E.164 format using this country code; inbound E.164 calling party numbers are identified as national numbers using this country code and are converted to national format.
- Ensure the **In Service** and **Check OOS** boxes are 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 the Swisscom Smart Business Connect
- Leave all other fields at default settings.

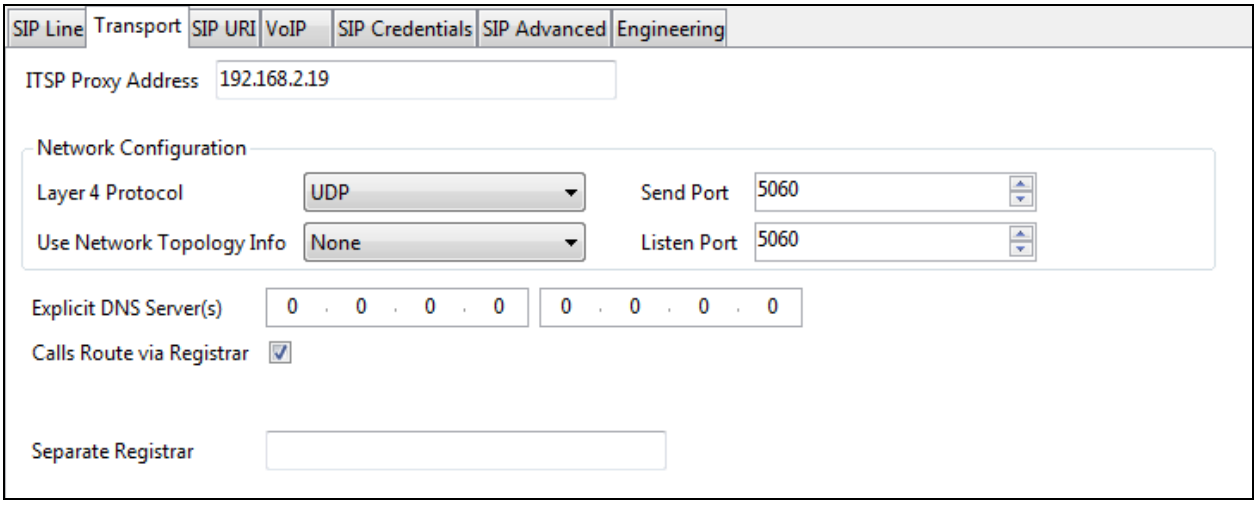


On completion, click the **OK** button (not shown).

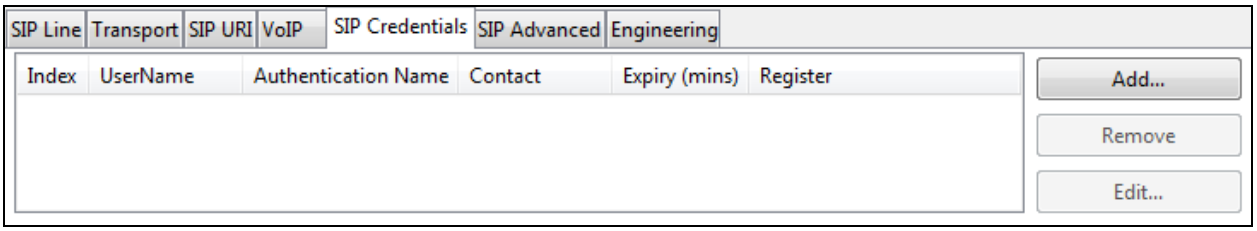
Select the **Transport** tab and set the following:

- Set **ITSP Proxy Address** to the IP Address for Swisscom Smart Business Connect.
- Set **Layer 4 Protocol** as required. During testing, **UDP** was used.
- Set **Send Port** and **Listen Port** as required. During testing, **5060** was used.
- 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.

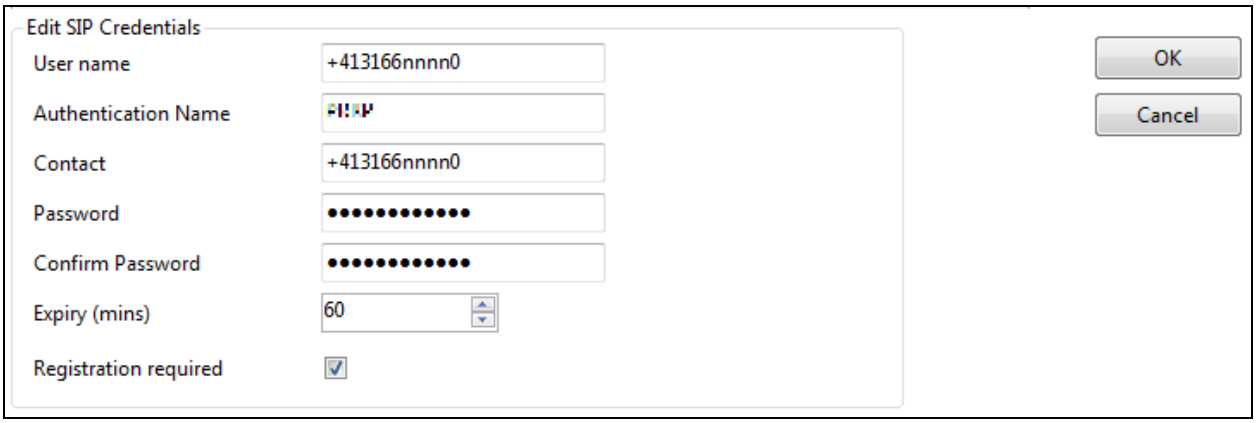
On completion, click the OK button (not shown).



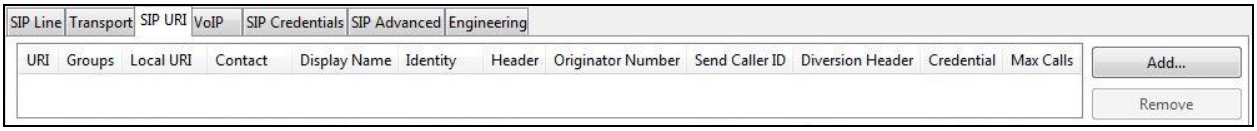
After the SIP line parameters are defined, the SIP credentials used for registration and authorisation on this line must be created. To define SIP credentials, first select the **SIP Credentials** tab. Click the **Add** button and the **New SIP Credentials** area will appear at the bottom of the pane.



Enter the SIP ID, SIP-USER and SIP-Password provided by Swisscom here.
The SIP ID is used for the **User name** and **Contact fields**. The SIP-USER is used for the **Authentication Name**. The **Expiry** is not used as the registration timeout is taken from the value provided in the 200 OK Contact header received from the network. Ensure that the **Registration required** checkbox is ticked.



After the SIP Credentials are defined, the SIP URIs that Avaya IP Office will receive and transmit on this line must be created. To create a SIP URI entry, first select the **SIP URI** tab. Click the **Add** button and the **New URI** area will appear at the bottom of the pane.

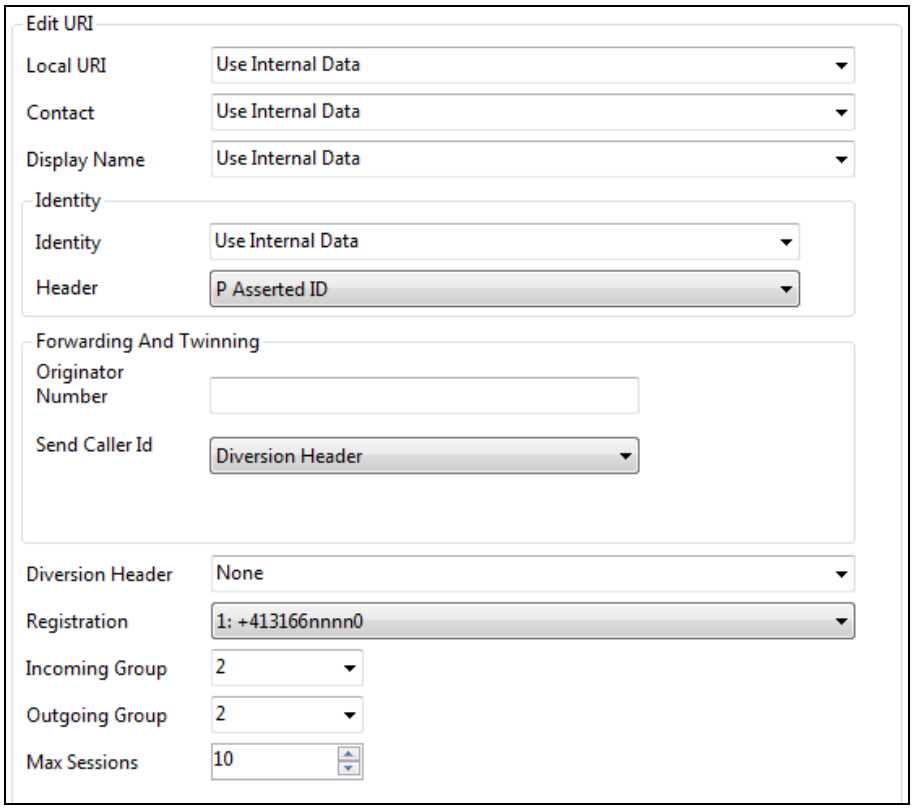


A SIP URI is shown in this example that is used for calls to and from extensions that have a DDI number assigned to them. Additional SIP URI's may be required for calls to services such as Voicemail Collect and the Mobile Twinning FNE, these would be for incoming calls only.

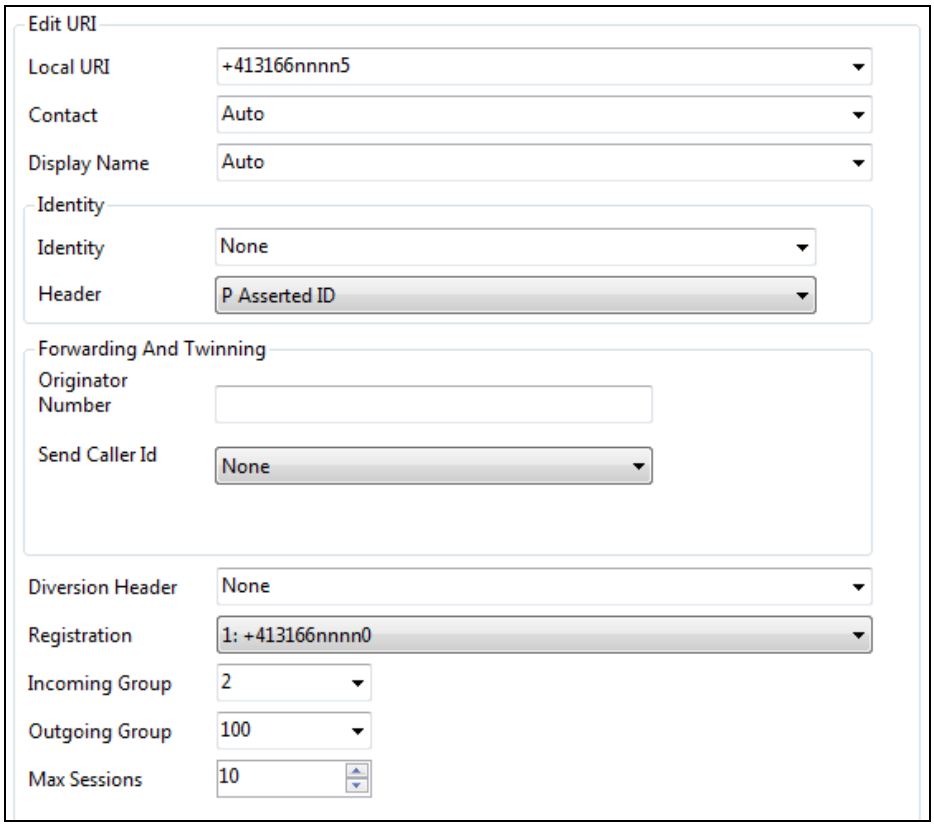
The SIP URI for calls to and from extensions that have DDI numbers associated with them was created with the parameters shown below.

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**. 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 **Originator Number** for **Forwarding and Twinning** blank so that the originating number is sent as the calling party number. Select **Diversion Number** as the **Send Caller ID** value to ensure that the DDI number assigned to the forwarding extension is sent in the Diversion header.
- Select the SIP Credentials defined previously in the **Registration** drop down menu.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. For the compliance test, a new incoming group **2** was defined that was associated to a single line (line 2).
- Associate this line with an outgoing line group by entering a line group number in the **Outgoing Group** field. For the compliance test, a new outgoing group **2** was defined that was associated to a single line (line 2)
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Leave other fields at default values.

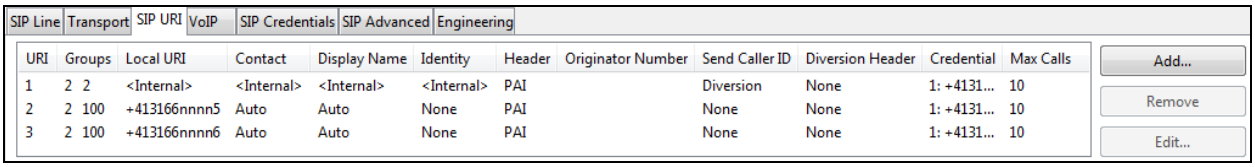
On completion, click the **OK** button.



Note: If required a SIP URI can be created for calls to services such as Voicemail Collect and 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:

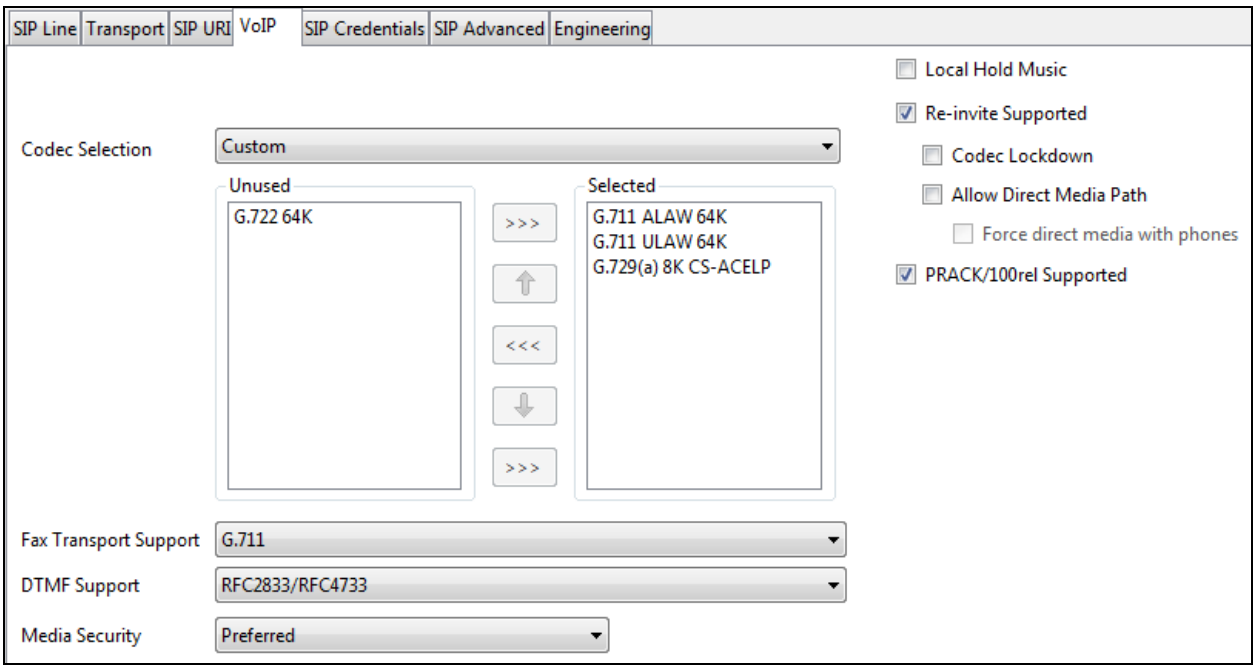


The following screenshot shows the completed configuration:

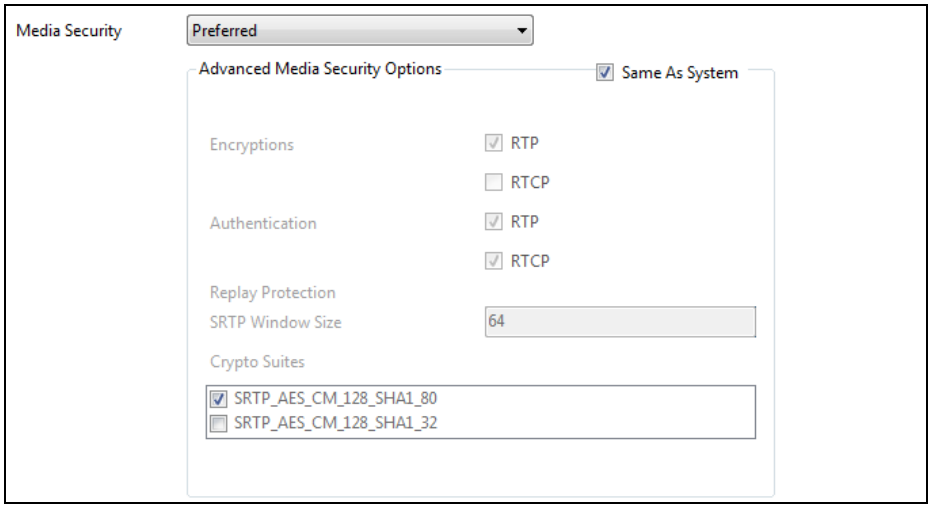


Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- In **Section 5.4**, system default codecs were defined. If any other codec combination is required for this SIP Line, select **Custom** in the **Codec Selection** drop down menu.
- Highlight codecs in the **Unused** box that are to be used on this line and click on the right arrows to move them to the **Selected** box.
- Highlight codecs in the **Selected** box that are not to be used and click on the left arrows to move them to the **Unused** box.
- Highlight codecs in the **Selected** box and use the up and down arrows to change the priority order of the offered codecs if required, for testing with Swisscom, **G.711 ALAW 64K**, **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** were used. This reflected the codec list received from the network.
- Select **RFC2833/RFC4733** in the **DTMF Support** drop down menu. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- 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.
- Leave the **Allow Direct Media Path** box unchecked. Direct Media is not supported where the network used for endpoints is different to that used for the SIP Trunk.
- Check the **PRACK/100rel Supported** box if early media is required. This was checked during compliance testing.
- Select **Media Security** as required. In the test environment, **Preferred** was selected from the drop down menu. Scroll down to define the security settings if required.

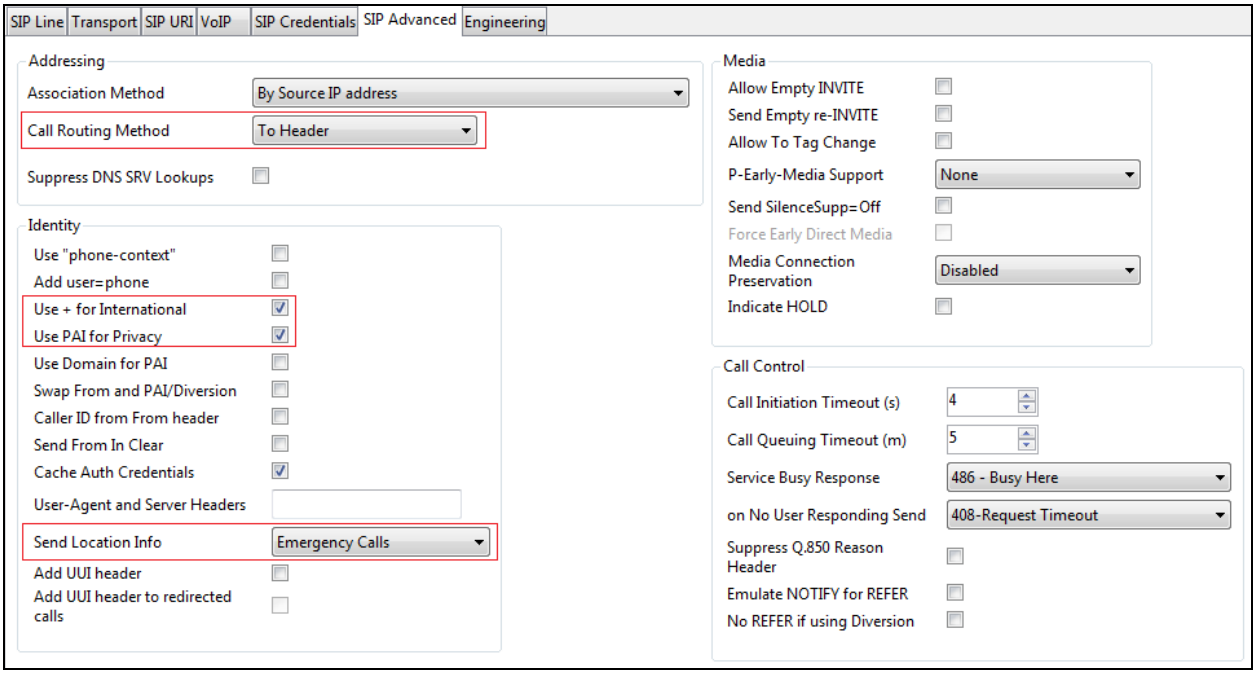


In the test environment, the system security settings were used by checking the **Same As System** box. This setting uses the values described in **Section 5.5**. On completion, click the **OK** button (not shown).



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.
- Check the **Use PAI for Privacy** box to send the calling party number for outbound calls with CLI Restricted in the P-Asserted-Identity header.
- Select **Emergency Calls** from the **Send Location Info** drop down menu if required.



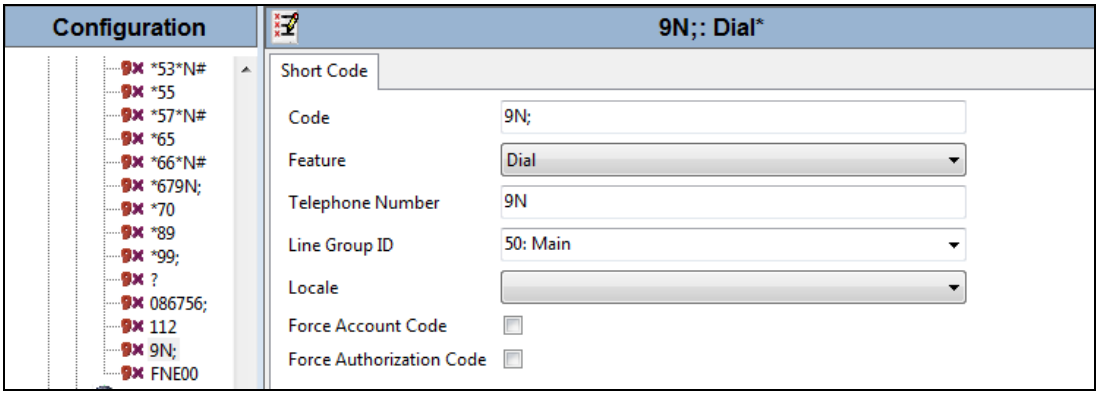
Note: The configuration shown in the previous page shows Location Info sent for Emergency calls. This was not tested, but is shown for information. The settings for Location data are shown in **Section 5.11**.

It is advisable at this stage to save the configuration as described in **Section 5.12** to make the Line Group ID defined in **Section 5.6** available.

5.7. Short Codes

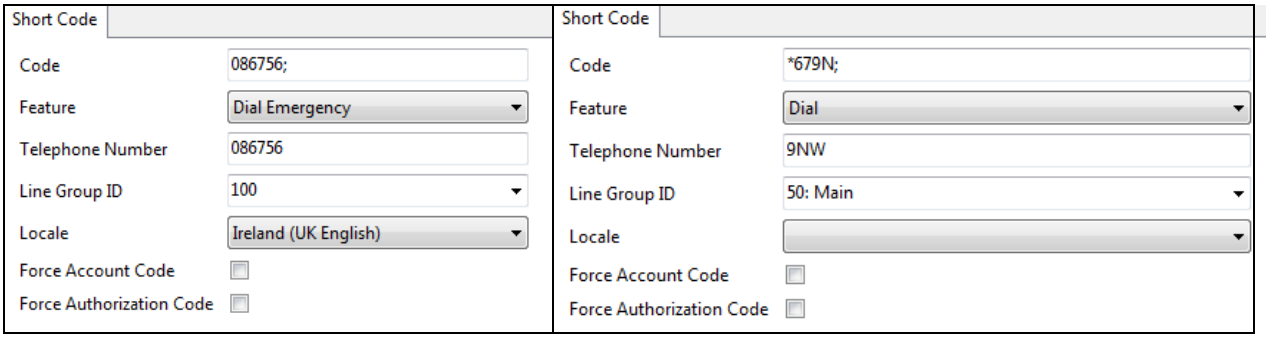
Define a short code to route outbound traffic to the SIP line. To create a short code, right-click **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as shown in the example below for public numbers.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon.
- The example shows **9N** which will be invoked when the user dials 9 followed by a public number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **9N** so that the call is passed to the ARS function with the dialled number unchanged.
- Set the **Line Group Id** to the ARS route number described in **Section 5.10**.
- On completion, click the **OK** button (not shown).



A further two examples are shown for an emergency number and withholding CLI:

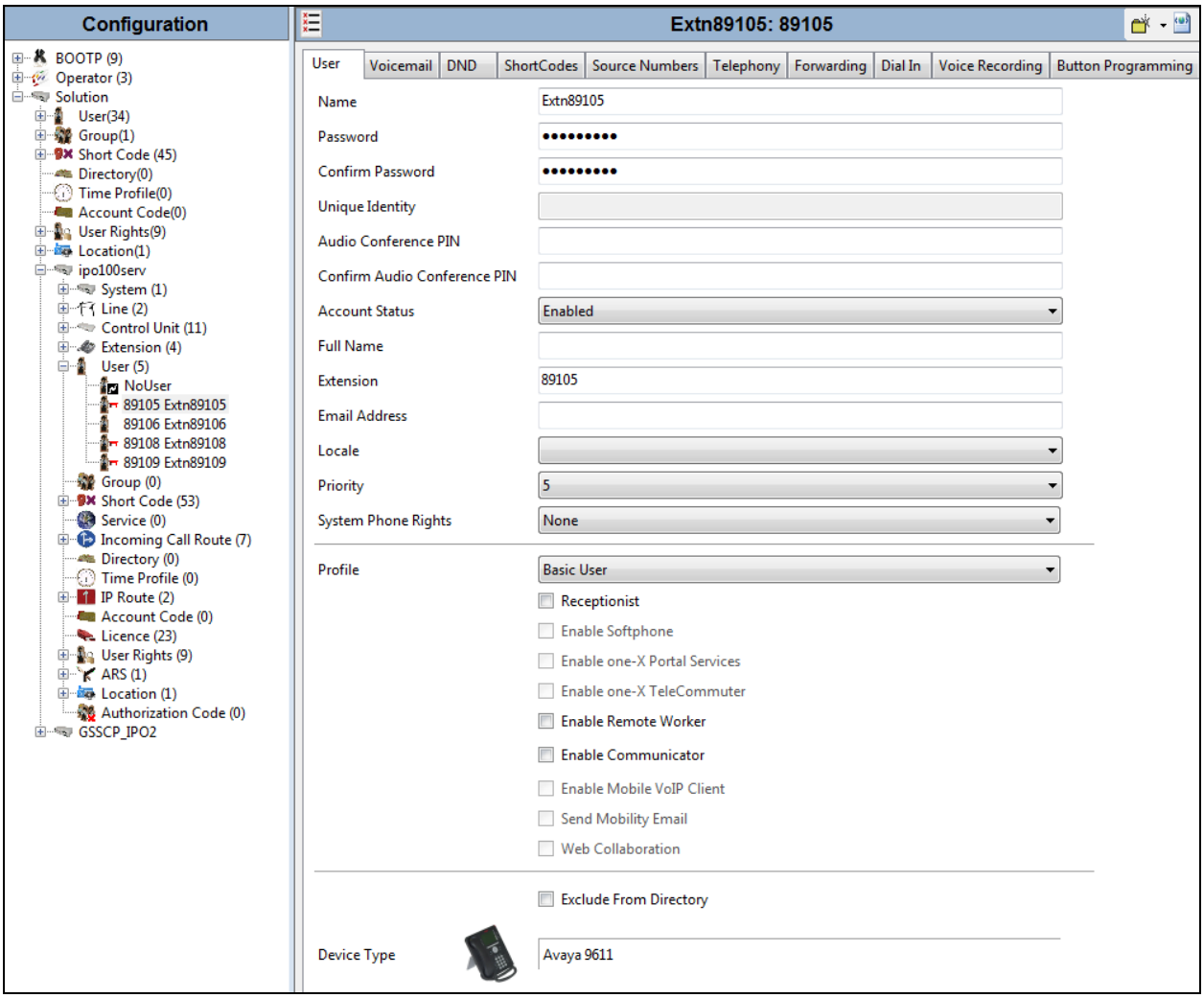
Code	***Feature***	***Telephone Number***	***Line Group ID***	***Description***
086756;	Dial Emergency	086756	100	Emergency Services Test Number. Feature uses Location data. Line Group ID is not used.
*679N;	Dial	9NW	50:Main	Public Number with *67 prefix. "W" suffix in Telephone Number withholds CLI.



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. The following example shows the **User** tab for an H.323 Endpoint:

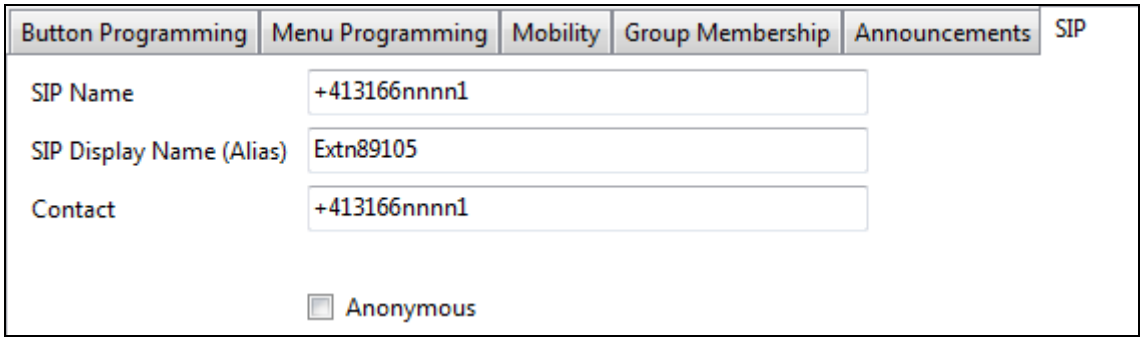
- Change the **Name** of the User if required.
- Set the **Password** and **Confirm Password**.
- Select the required profile from the **Profile** drop down menu. **Basic User** is commonly used; **Power User** can be selected for SIP softphone, WebRTC and Remote Worker endpoints.



Note: SIP endpoints require setting of the SIP Registrar Enable in the LAN1 settings. Navigate to **System → <IP Office Name>** (not shown) in the Navigation Pane where <IP Office Name> is the name of the IP Office. Navigate to the **LAN1 → VoIP** tab in the Details Pane (not shown) and check the **SIP Registrar Enable** check box.

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 fields should be set to the DDI numbers assigned to the enterprise from Swisscom in international format. In the example below, one of the DDI numbers in the test range is used, though some of the digits have been obscured. On completion, click the **OK** button (not shown).



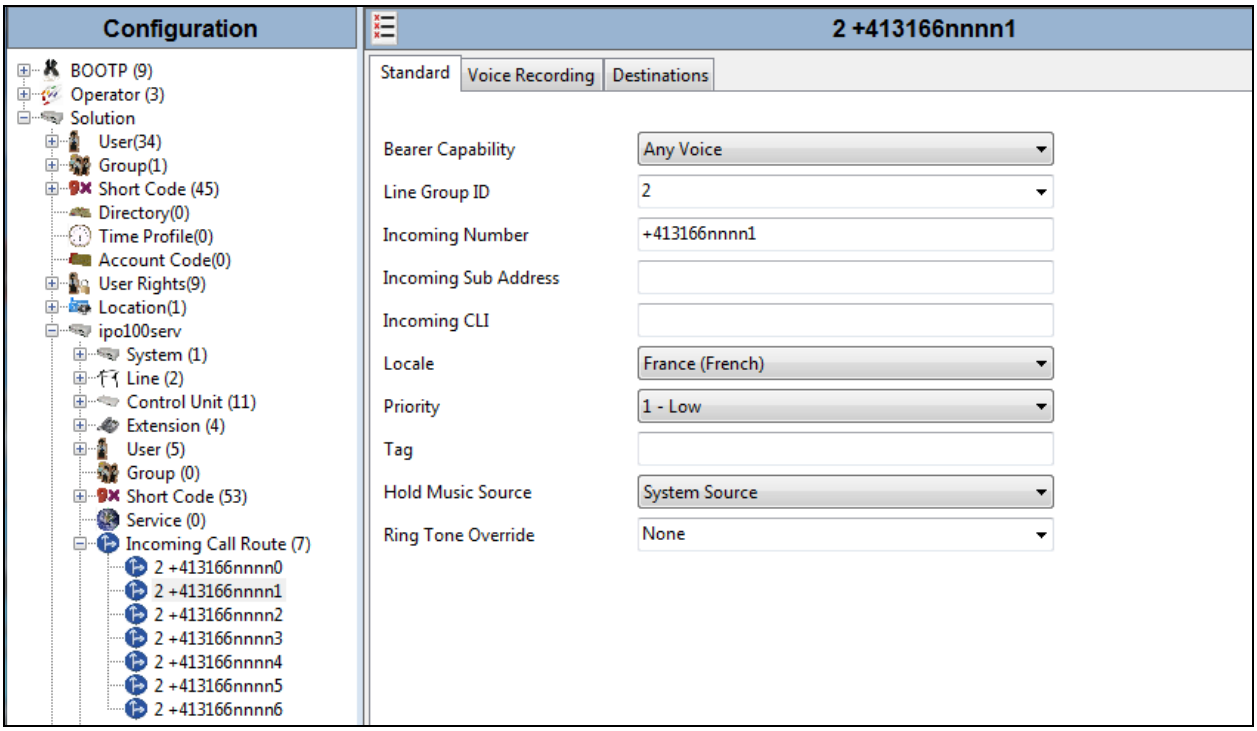
Note: The **Anonymous** box can be used to restrict Calling Line Identity (CLIR).

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 Route** in the Navigation Pane and select **New**, (not shown).

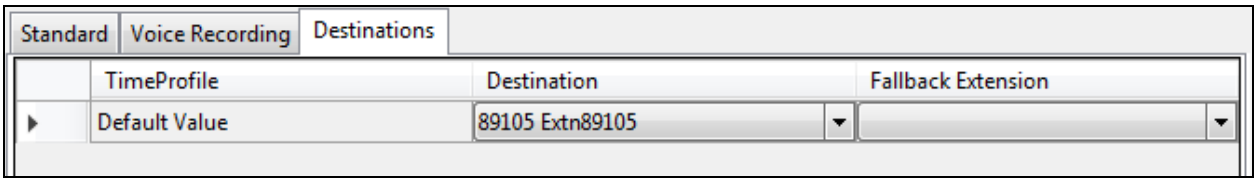
On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- 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**.
- 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.



Note: A number of digits of the DDI have been obscured. Number format for incoming calls is E.164 with leading "+".

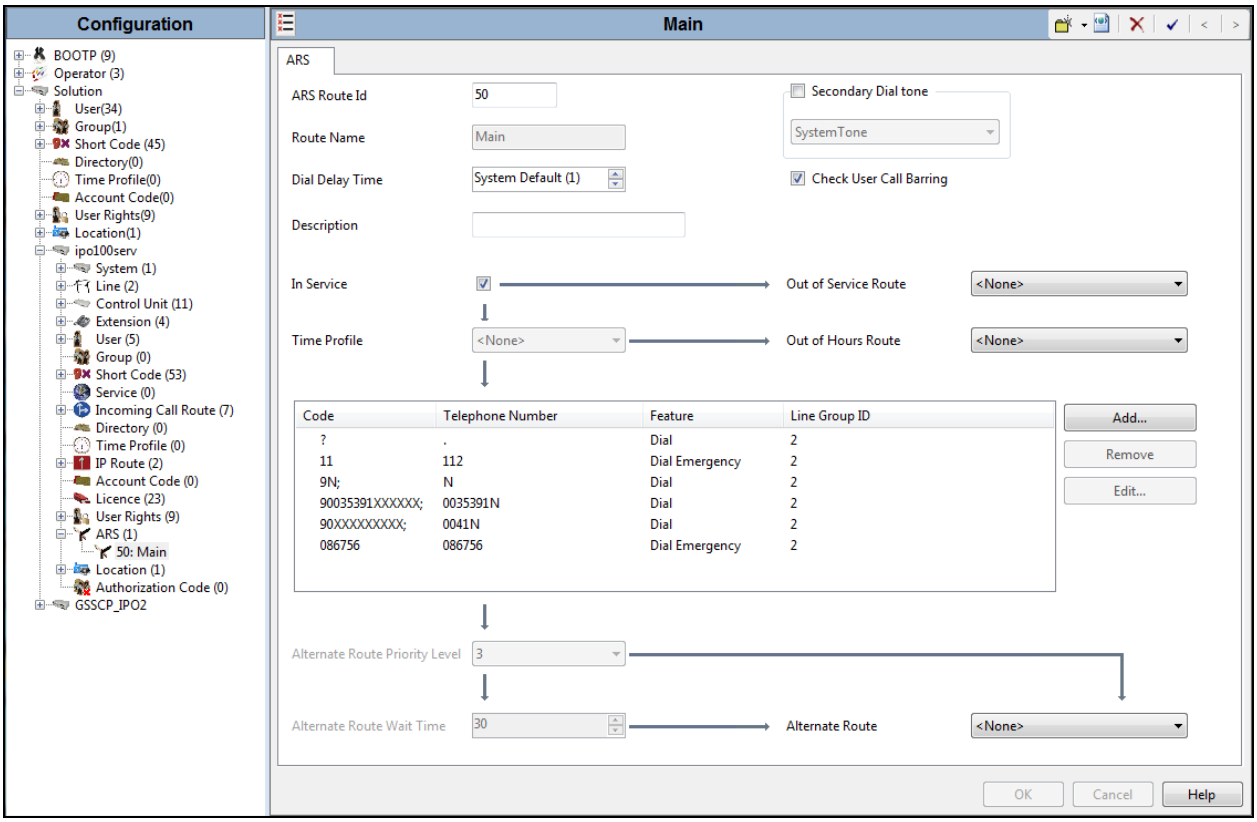
On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. On completion, click the **OK** button (not shown). In this example, incoming calls to the test DDI number on line **2** are routed to extension **89105**.



Note: Calls coming in to destinations not associated with an extension such as Voice Mail and FNE also appear on line 2 in this configuration. The destinations are defined as the short codes for Voicemail Collect and the FNE Service.

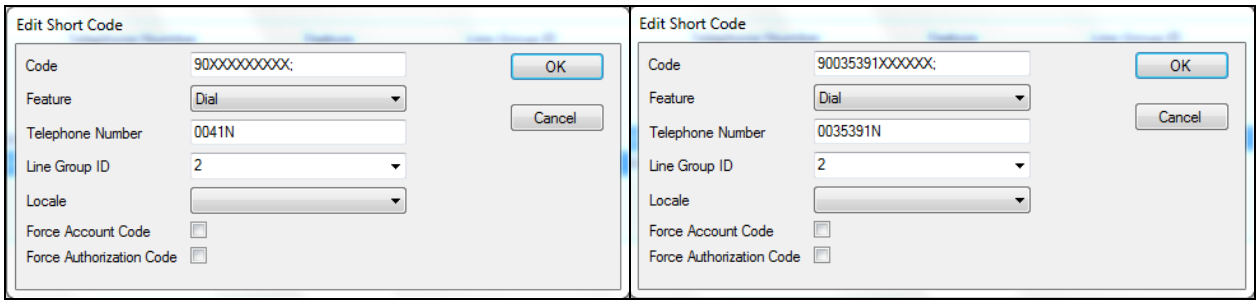
5.10. ARS

The Main ARS route exists by default and requires editing. Select the ARS **Main** route and click on **Add**.

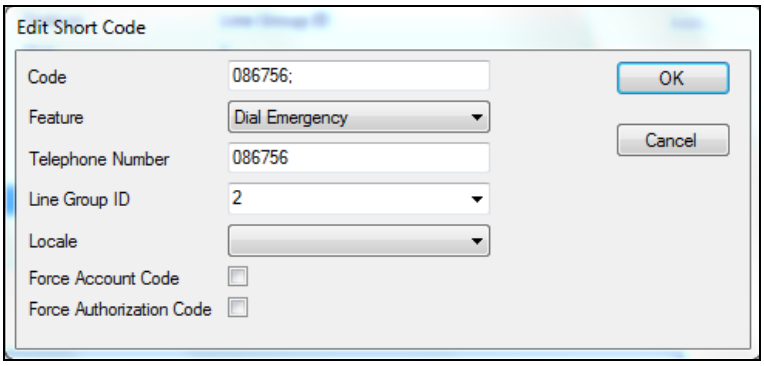


Define numbers as required. An example for national numbers is as follows:

- Define the Short **Code**, the example shows both a 10 digit national number and an international number with country code and city code prefixed with **9** for an outside line. Select **Dial** in the **Feature** drop down menu.
- Define the **Telephone Number** without the **9** which removes it and sends the number as dialled. All **X** characters can be replaced with a single **N**.
- Select the **Line Group ID** defined in the SIP Line URI described in **Section 5.6**. During testing this was **2** for the SIP Trunk. Click on **OK**



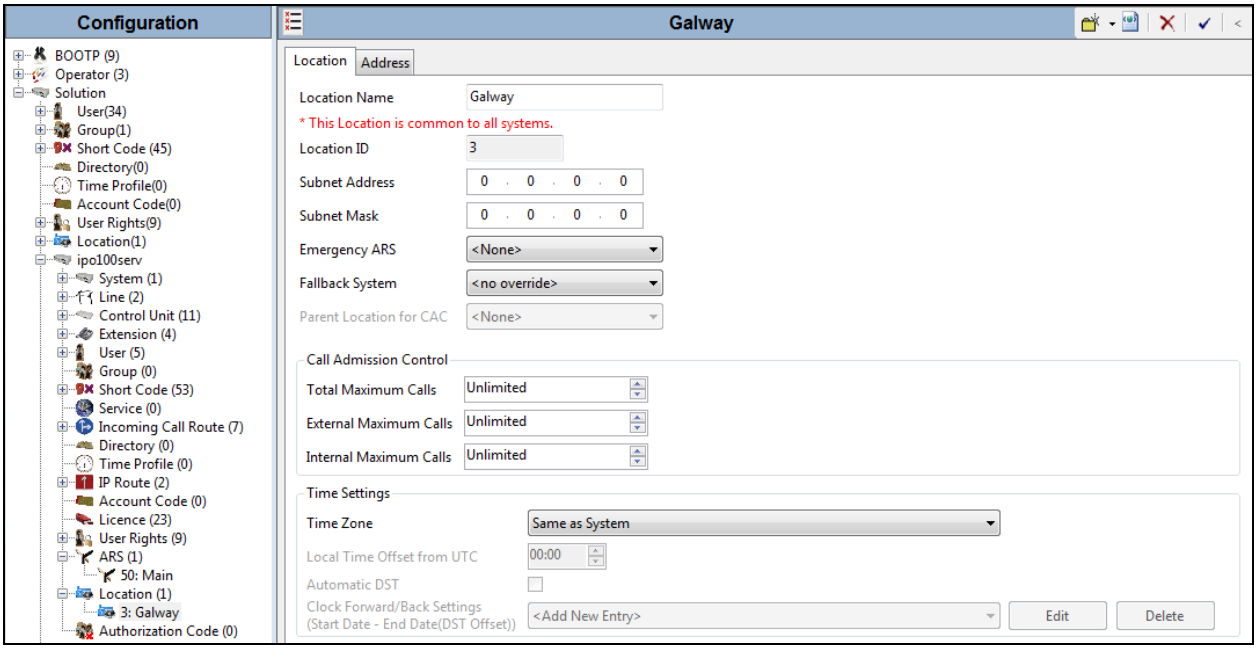
The **X** used in the Code indicates any digit and "**;**" causes the system to wait for the full number to be dialled or a "#". The next example shows an emergency number. Set **Feature** to **Dial Emergency**. The number shown is not a valid Emergency Services number, it is a test number used to check Location data.



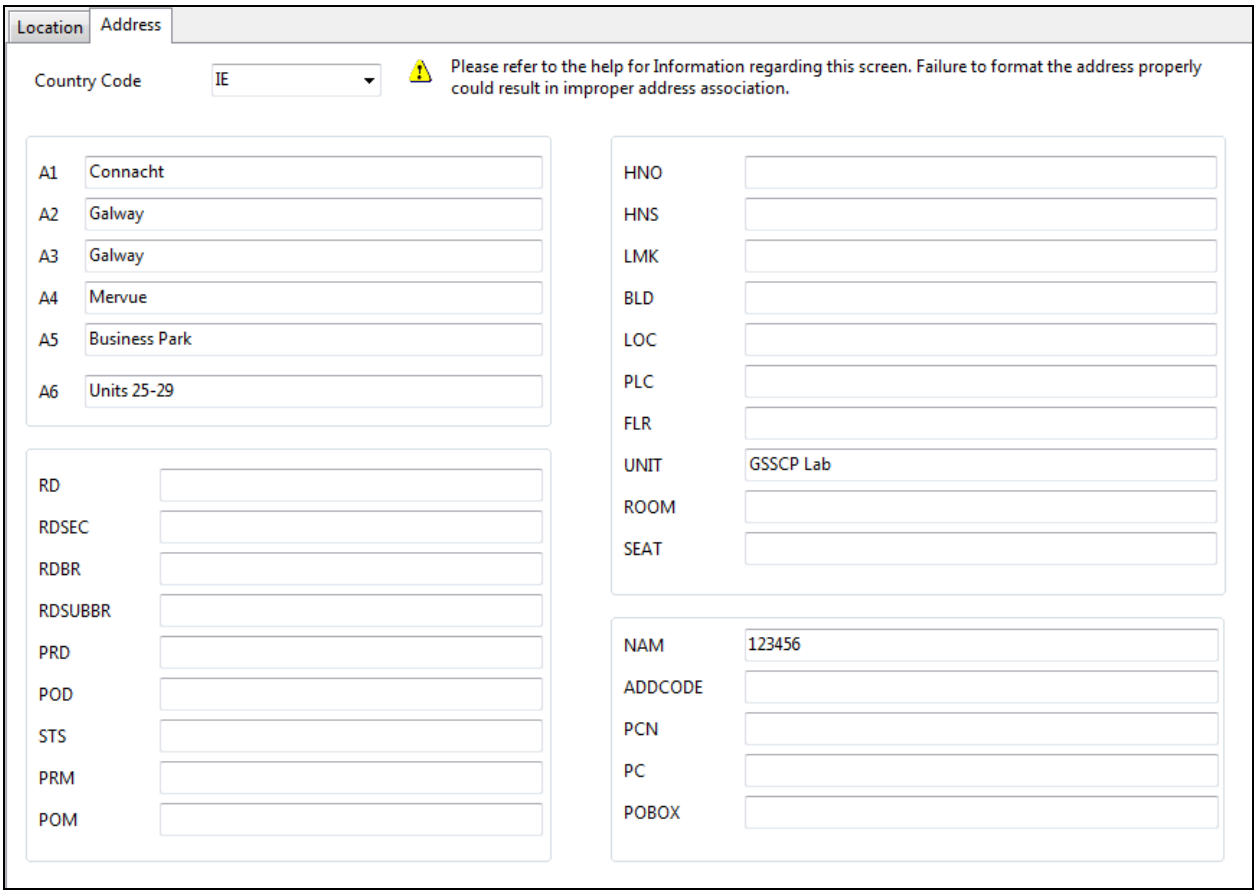
5.11. Location

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.
- Select the **Emergency ARS** from the drop down menu. In the test environment default ARS of **50: Main** was used.
- In the example, all other fields were left at default values.



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

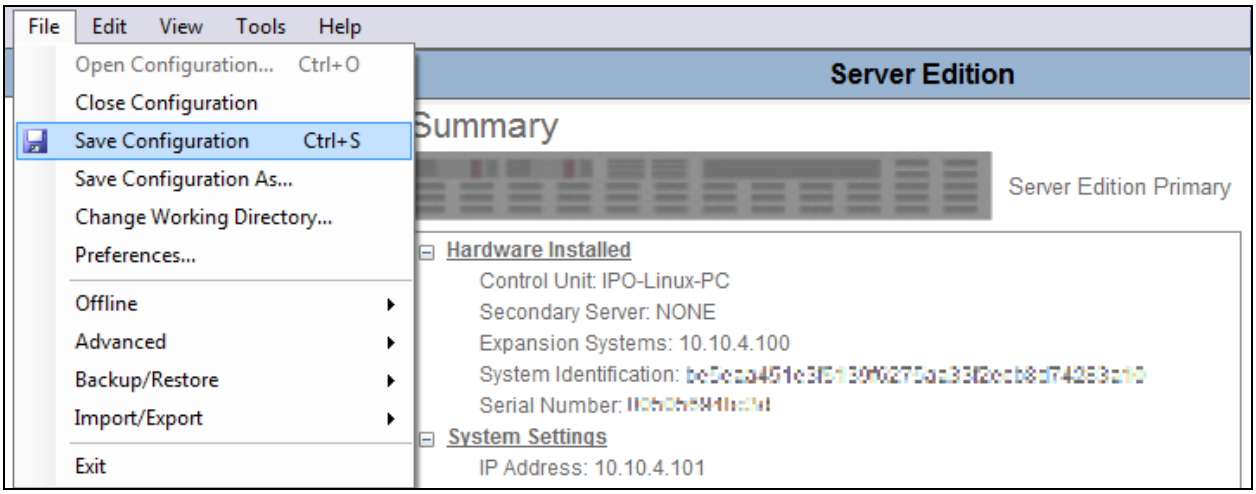


Note: The above example bears no relation to the information that would be used in the live environment. It was specified for the sole purpose of being identifiable in the SIP messages of the test calls.

The location data defined in the test environment is applied to the whole IP office. This can be refined according to subnet and also individual extensions. The SIP Line is configured to send location data as described in **Section 5.6.2**.

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.



6. Configure the Swisscom Equipment

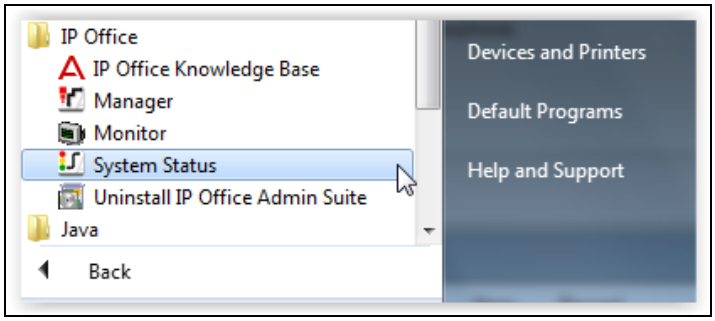
The configuration of the Swisscom Smart Business Connect equipment used to support the SIP Trunk is outside the scope of these Application Notes and will not be covered. To obtain further information on Swisscom equipment and system configuration please contact an authorized Swisscom representative.

7. Verification Steps

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

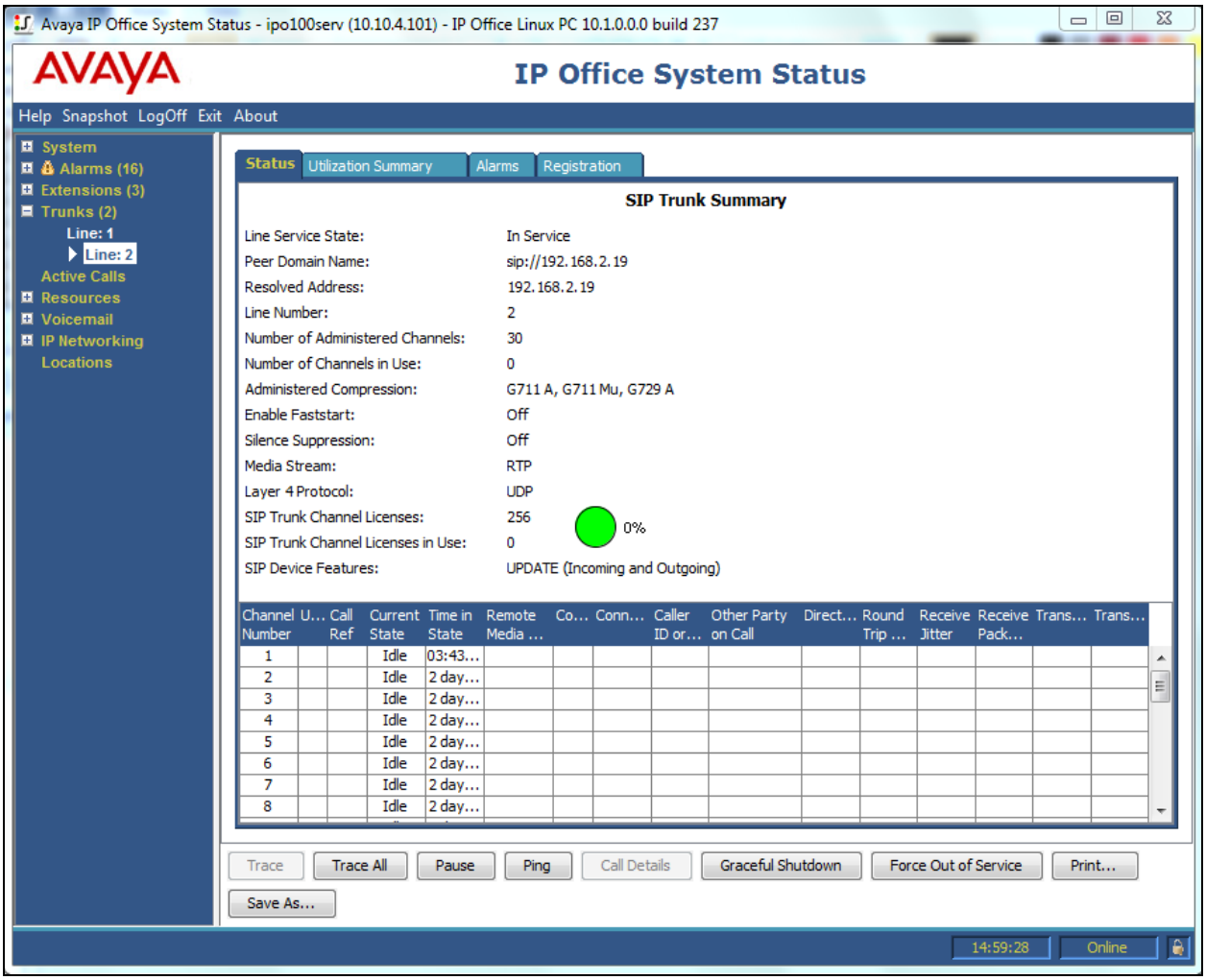
7.1. SIP Trunk status

The status of the SIP trunk can be verified by opening the System Status application. A Windows 7 PC was used for testing and the application was opened by pressing the Start button and selecting **All Programs→ IP Office → System Status**.



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 (**2** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational.



8. Conclusion

All tests for Swisscom Smart Business Connect were completed. Observations for the testing are listed in **Section 2.2**.

9. Additional References

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

[1] *Avaya IP Office™ Platform Start Here First*, Release 10.1, Sep 2017.
[2] *Avaya IP Office™ Platform Server Edition Reference Configuration*, August 2016
[3] *Deploying IP Office™ Platform Server Edition Solution*, Release 10.1, Jun 2017
[4] *IP Office™ Platform 10.1, Deploying Avaya IP Office™ Platform IP500 V2*, Sep 2017.
[5] *IP Office™ Platform 10.1 Installing and Maintaining the Avaya IP Office™ Platform Application Server*, Document number 15-601011, Sep 2017.
[6] *Administering Avaya IP Office™ Platform with Web Manager*, Release 10.1, Jun 2017.
[7] *Administering Avaya IP Office™ Platform with Manager*, Release 10.1, Jun 2017.
[8] *IP Office™ Platform 10.1 Using Avaya IP Office™ Platform System Status*, Document number15-601758, Jul 2017.
[9] *IP Office™ Platform 10.1 Using IP Office System Monitor*, Document number 15-601019, Jun 2017.
[10] *Using Avaya Communicator for Windows on IP Office*, Release 10.0, August 2016.
[11] *Avaya Communicator for Web- IP Office™ Platform: User Guide*, October 2016.
[12] *Avaya Communicator for Web- IP Office™ Platform: Administering Guide*, October 2016.
[13] *IP Office™ Platform 10.0 - Third-Party SIP Extension Installation Notes*, June 2016.
[14] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/