Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office 10.1 and Avaya Session Border Controller for Enterprise Release 7.2 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 with Avaya Session Border Controller for Enterprise.

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

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office and Avaya SBCE to connect to the Swisscom 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 the Avaya SBCE and 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 the Swisscom Smart Business Connect. The following observations were made during the test:

- 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 outbound calls, in particular calls to mobile phones, an UPDATE message was received from the network within the initial INVITE dialogue that reversed the From and To headers. IP Office rejected these with "500 Internal Server Error". This did not adversely affect call set-up.
- Emergency Calls to a test number were attempted and the location data could be seen in the body of the initial INVITE message in xml format. These calls were not answered.
- When putting inbound calls on hold for over 15 minutes, the outbound audio was lost when the call was taken off hold. This fault was intermittent and disappeared altogether when encryption between the IP Office and the Avaya SBCE was removed. This is assumed to be related to an existing issue on the Avaya SBCE, raised as fault report AURORA-12076, with conversion between encrypted and unencrypted media.
- When putting outbound calls on hold for over 15 minutes, calls were released from the network. This was resolved by changing the configuration of the IP Office so that call hold was not indicated by the use of re-INVITE messages.
- There were a small number of instances where although an outbound test call was answered, there was no 200 OK message received from the network. This was assumed to be an issue in 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 testing was not required as this is not offered to Swisscom customers on IP Office. Although not required, some fax calls were attempted but these failed.

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.

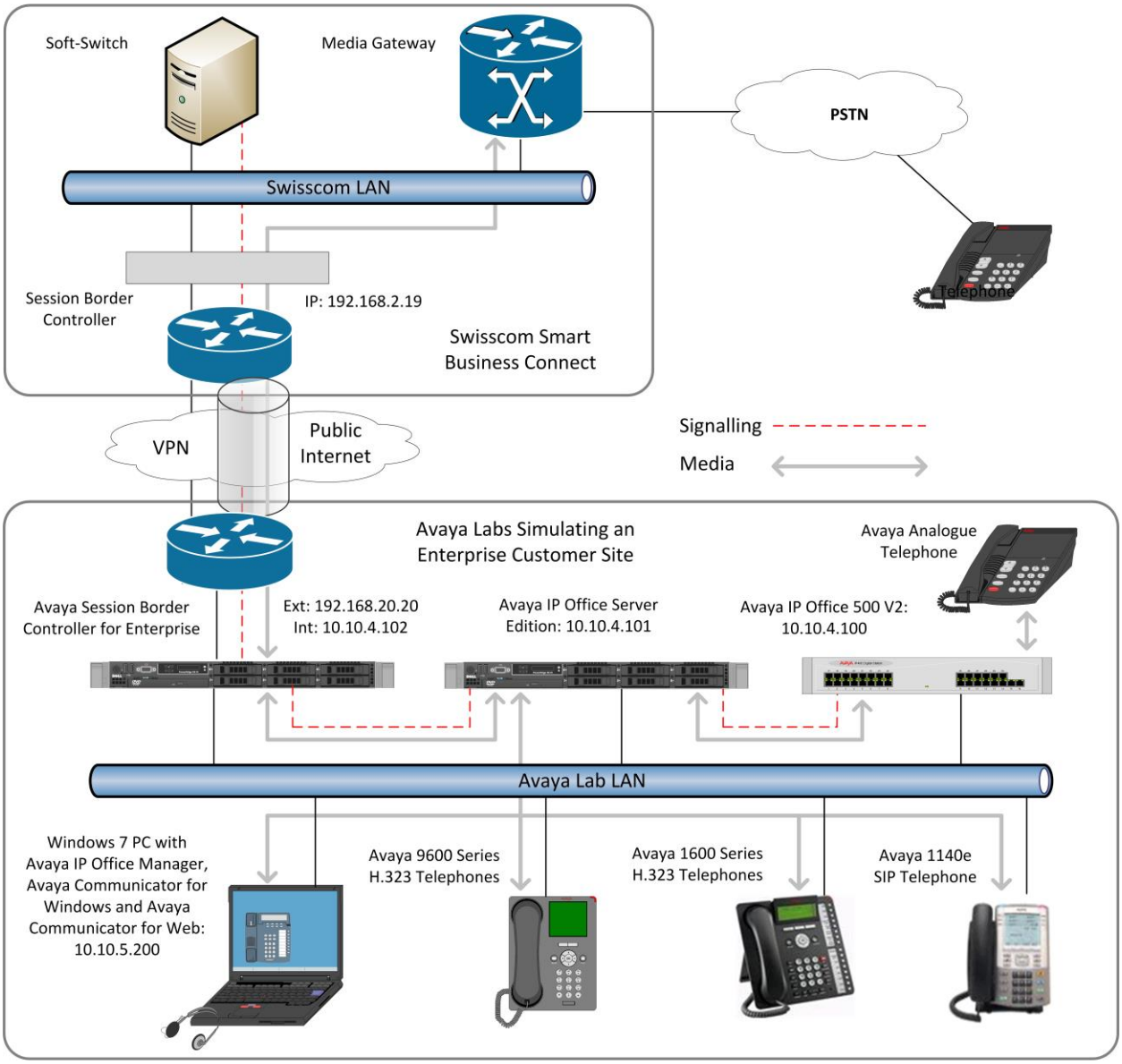


Figure 1: Swisscom Smart Business Connect to Avaya IP Office via Avaya SBCE Topology

4. Equipment and Software Validated

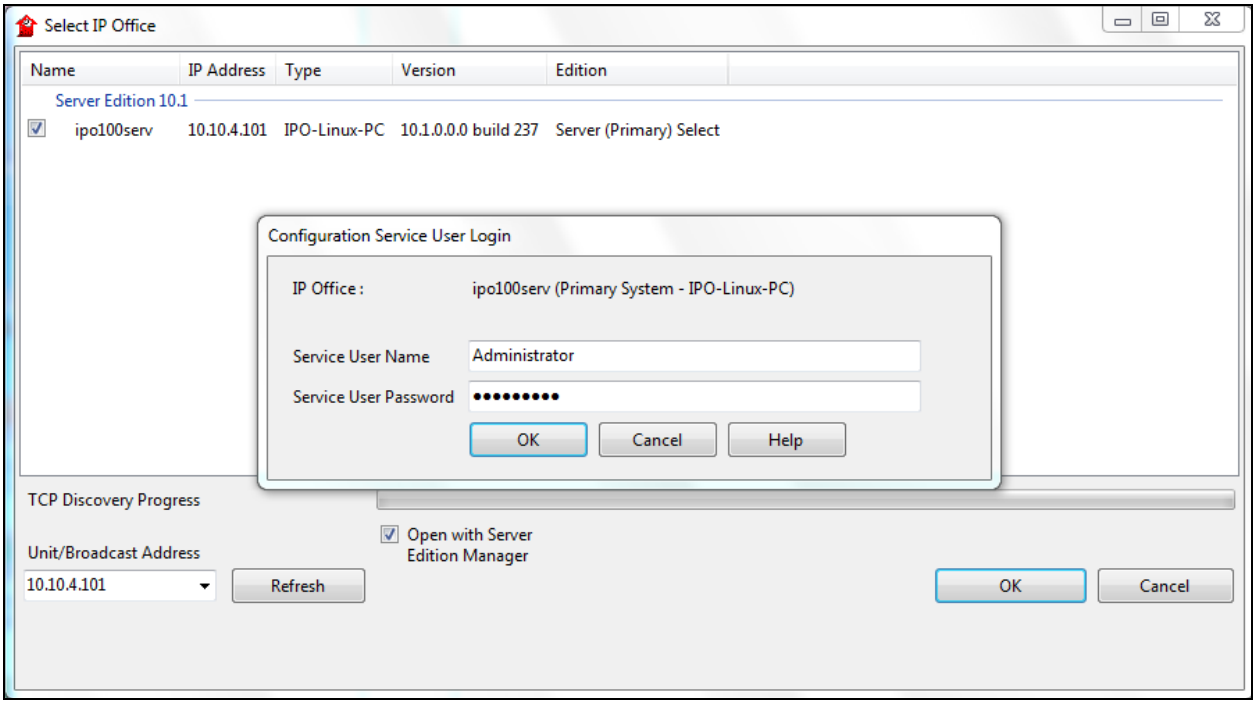
The following equipment and software were used for the sample configuration provided:

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.

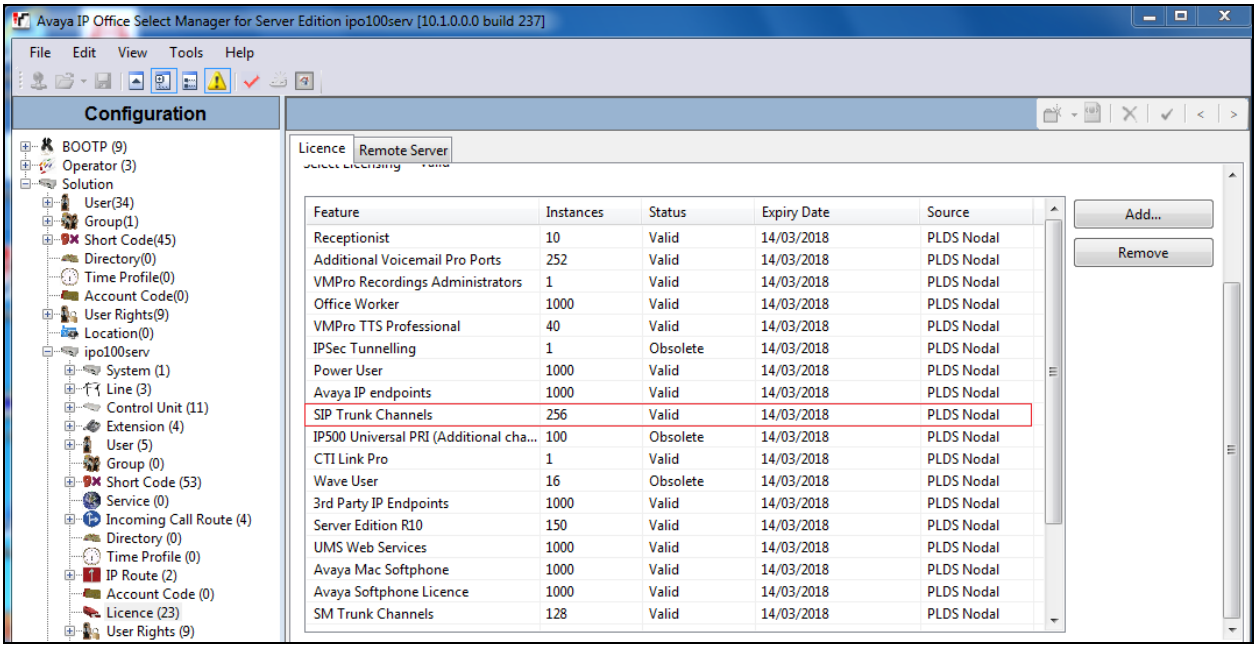
5. Configure Avaya IP Office

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

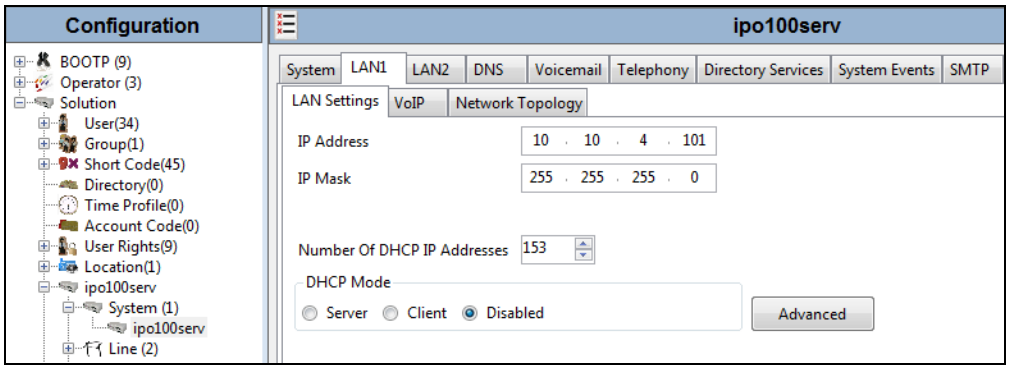
Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of channels provisioned for the SIP trunk.



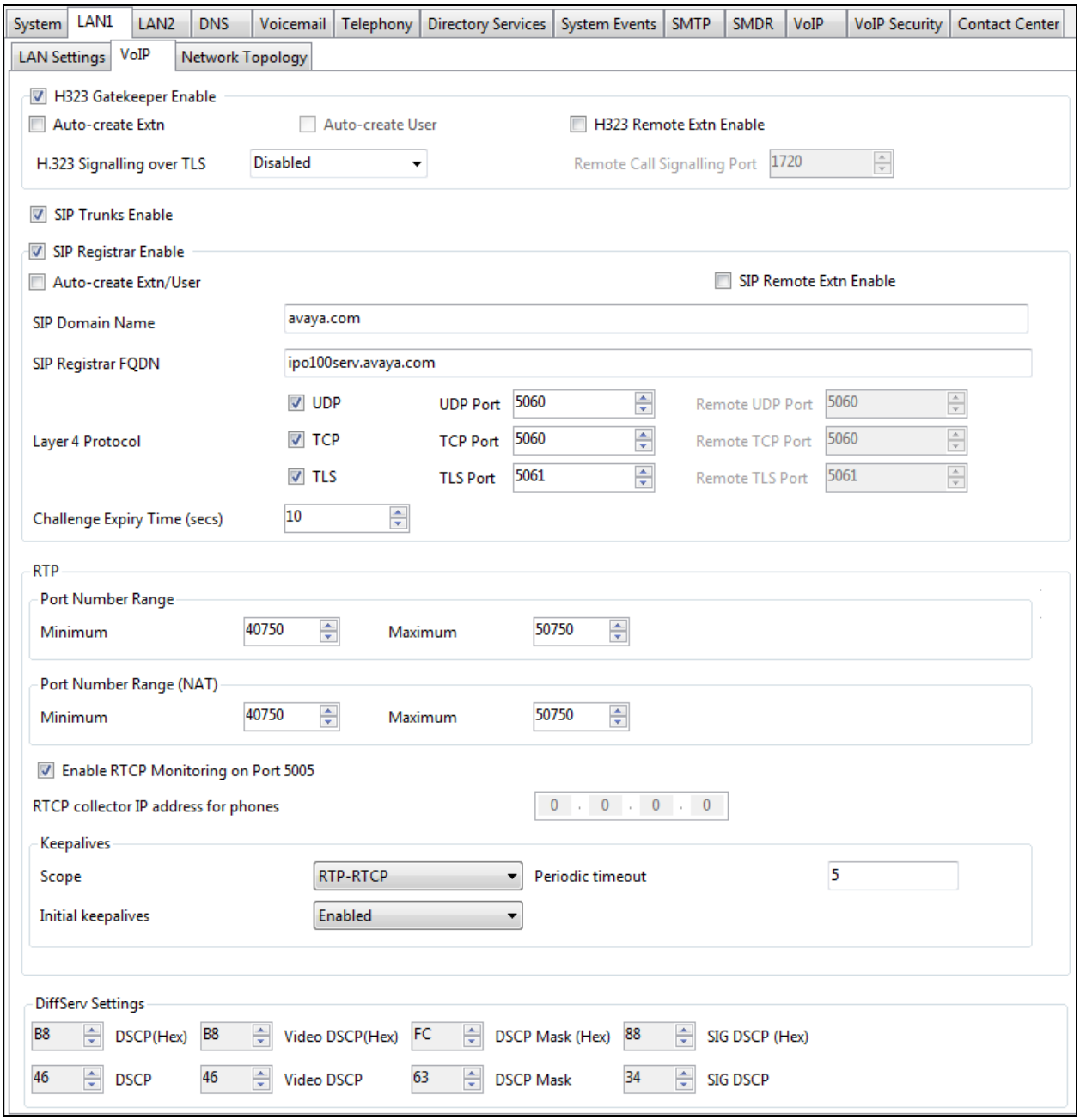
Feature	Instances	Status	Expiry Date	Source
Receptionist	10	Valid	14/03/2018	PLDS Nodal
Additional Voicemail Pro Ports	252	Valid	14/03/2018	PLDS Nodal
VMPro Recordings Administrators	1	Valid	14/03/2018	PLDS Nodal
Office Worker	1000	Valid	14/03/2018	PLDS Nodal
VMPro TTS Professional	40	Valid	14/03/2018	PLDS Nodal
IPSec Tunnelling	1	Obsolete	14/03/2018	PLDS Nodal
Power User	1000	Valid	14/03/2018	PLDS Nodal
Avaya IP endpoints	1000	Valid	14/03/2018	PLDS Nodal
SIP Trunk Channels	256	Valid	14/03/2018	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	14/03/2018	PLDS Nodal
CTI Link Pro	1	Valid	14/03/2018	PLDS Nodal
Wave User	16	Obsolete	14/03/2018	PLDS Nodal
3rd Party IP Endpoints	1000	Valid	14/03/2018	PLDS Nodal
Server Edition R10	150	Valid	14/03/2018	PLDS Nodal
UMS Web Services	1000	Valid	14/03/2018	PLDS Nodal
Avaya Mac Softphone	1000	Valid	14/03/2018	PLDS Nodal
Avaya Softphone Licence	1000	Valid	14/03/2018	PLDS Nodal
SM Trunk Channels	128	Valid	14/03/2018	PLDS Nodal

5.2. LAN1

In the sample configuration, the LAN1 port was used to connect the Avaya IP Office to the Avaya SBCE. Note that this is the local LAN port also used for connection to endpoints. To access the LAN1 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 **LAN1 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the internal 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**.

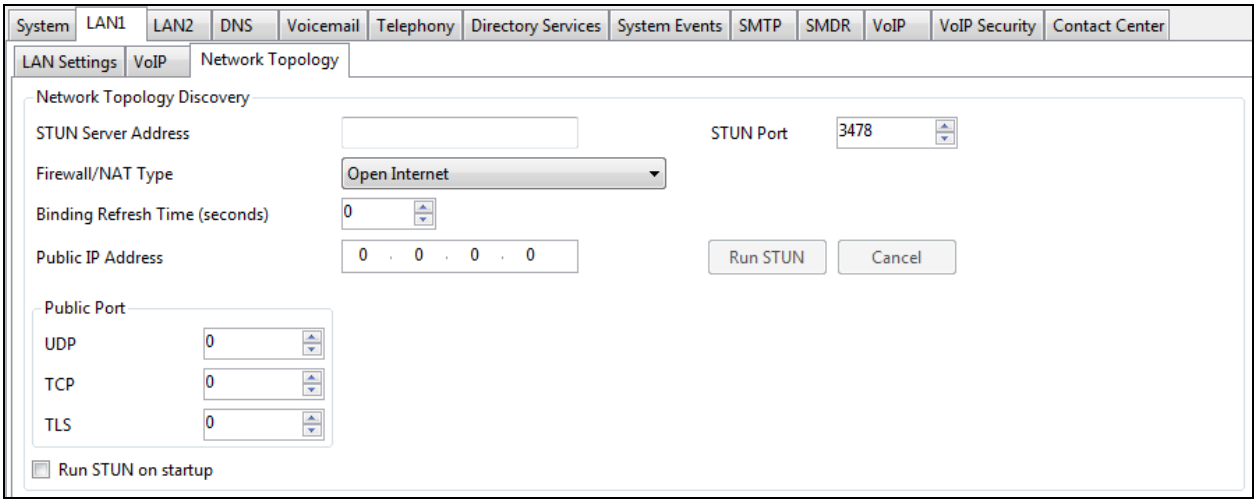


Note: Avaya IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP header with specific values to support Quality of Services policies for both signalling and media (not shown). DSCP for media can be set for both voice and video. The **DSCP** field is the value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

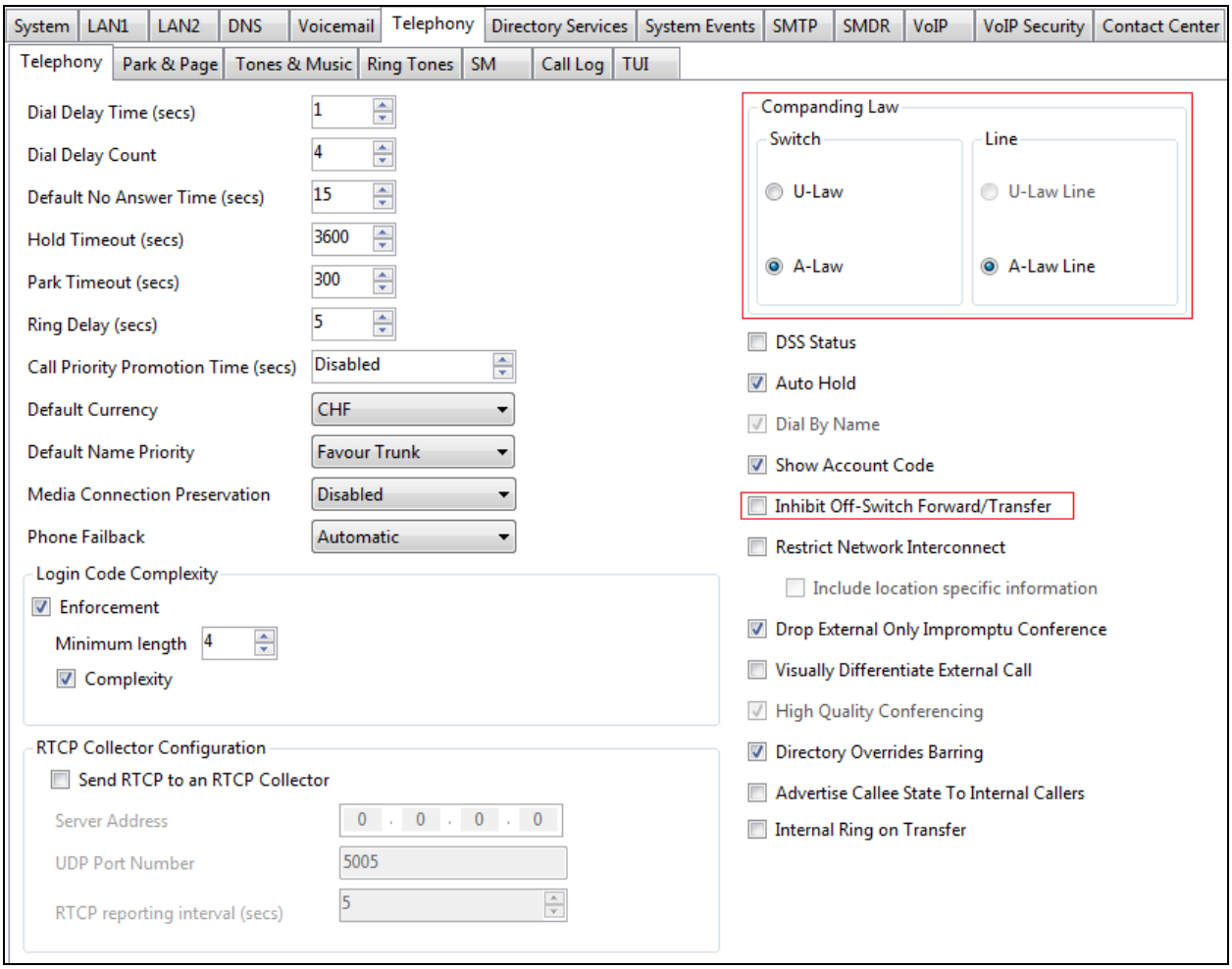
The Network Topology tab can be used to set the **Binding Refresh Time** for the periodic sending of OPTIONS. This is intended for use where OPTIONS are required at intervals of less than 300 seconds. A value of **0** uses the default of 300 seconds.



Note: During compliance testing, registration was used with REGISTER messages sent by the Avaya SBCE as described in **Section 6.6**. These REGISTER messages act as a check of the SIP Trunk so that OPTIONS messages are not critical.

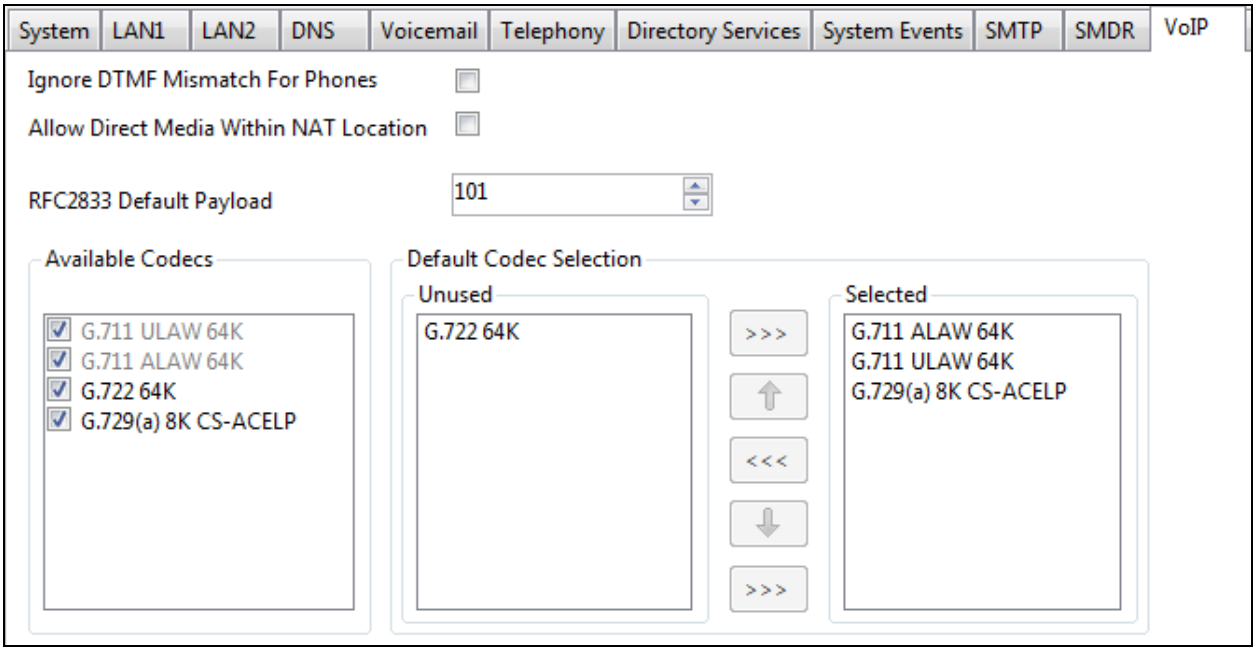
5.3. System Telephony Settings

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).



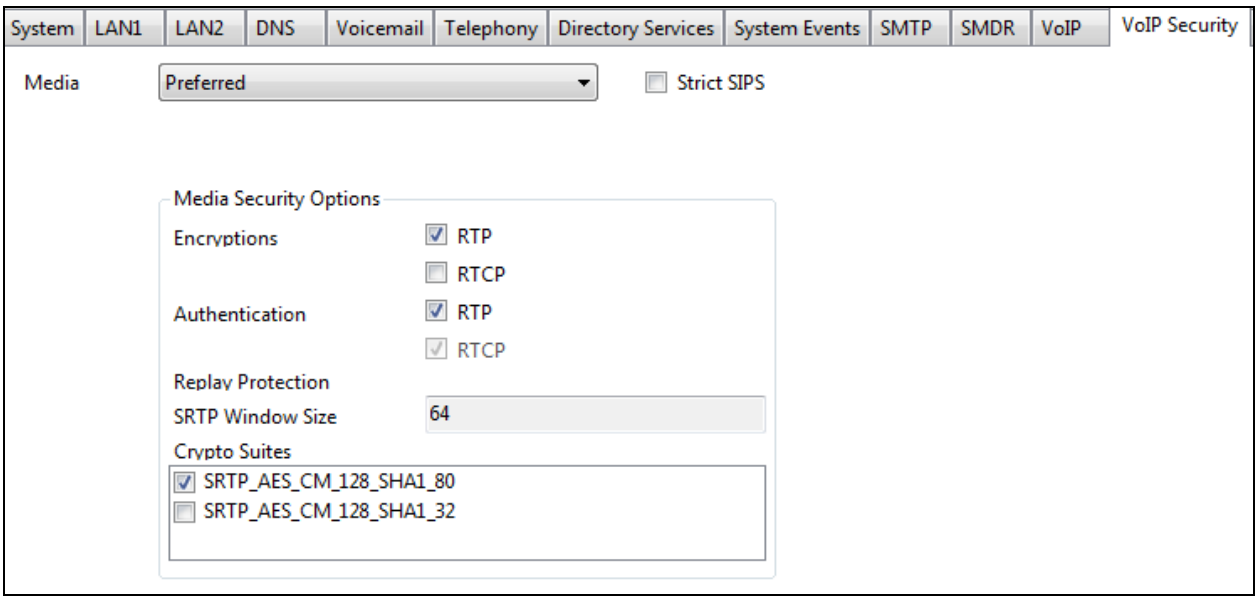
Note: The codec settings for IP endpoints can also be used for the SIP Trunk by selecting **System Default** in the **Codec Selection** as shown in **Section 5.6.2**.

5.5. VoIP Security

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. To enable 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 to the Avaya SBCE due to an issue described in **Section 2.2**.

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 via the Avaya SBCE. 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**.

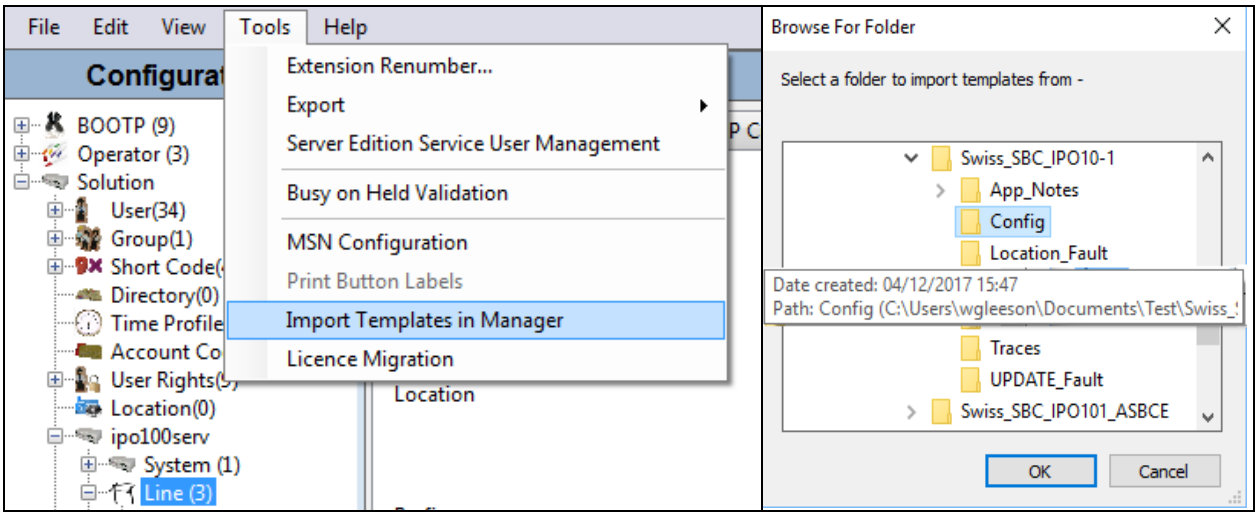
Also, the following SIP Line settings are not supported on Basic Edition:

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

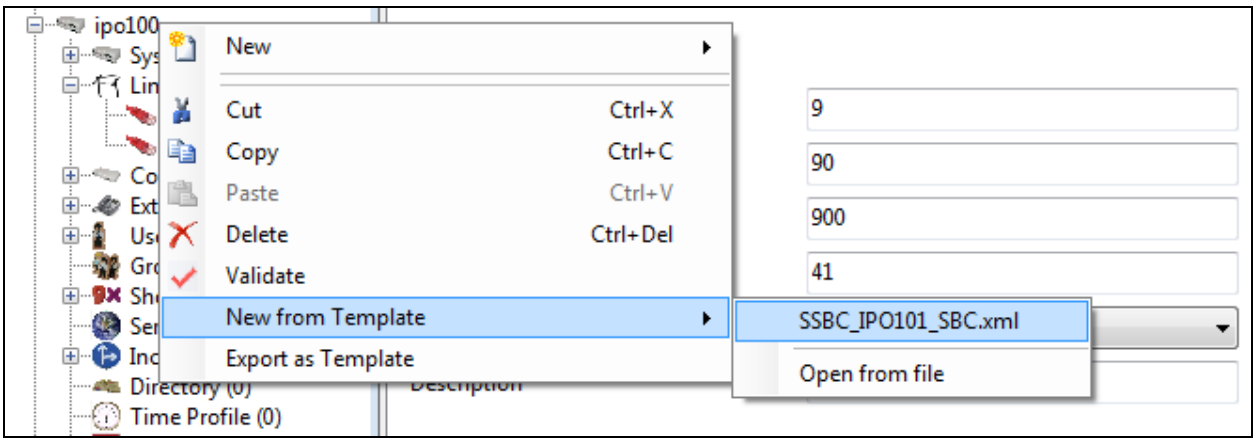
Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New→SIP Line** (not shown). Then, follow the steps outlined in **Section 5.6.2**.

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**.

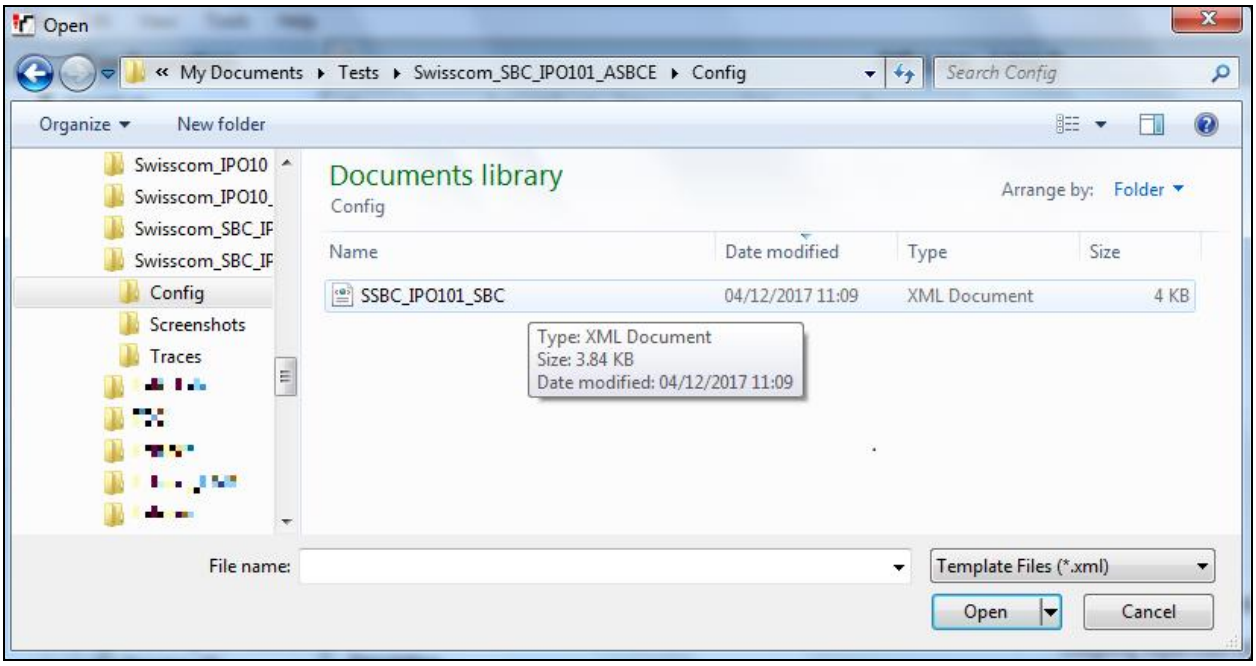


To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New from Template**. If the template file was imported as shown above, select it directly:



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:

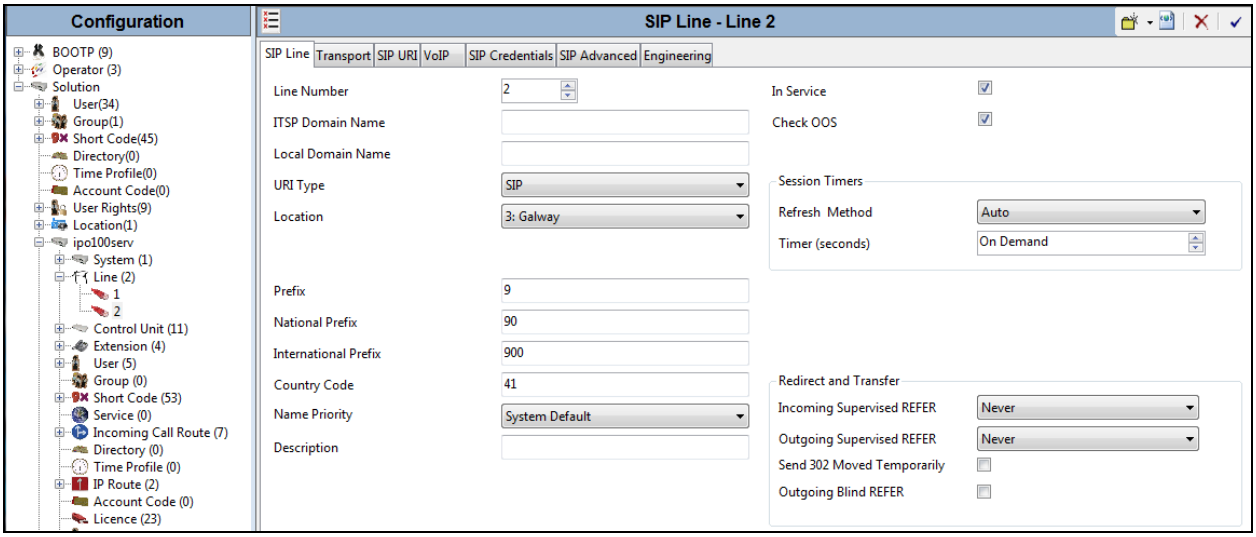


The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.6.2**.

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 the Avaya SBCE.

- 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.

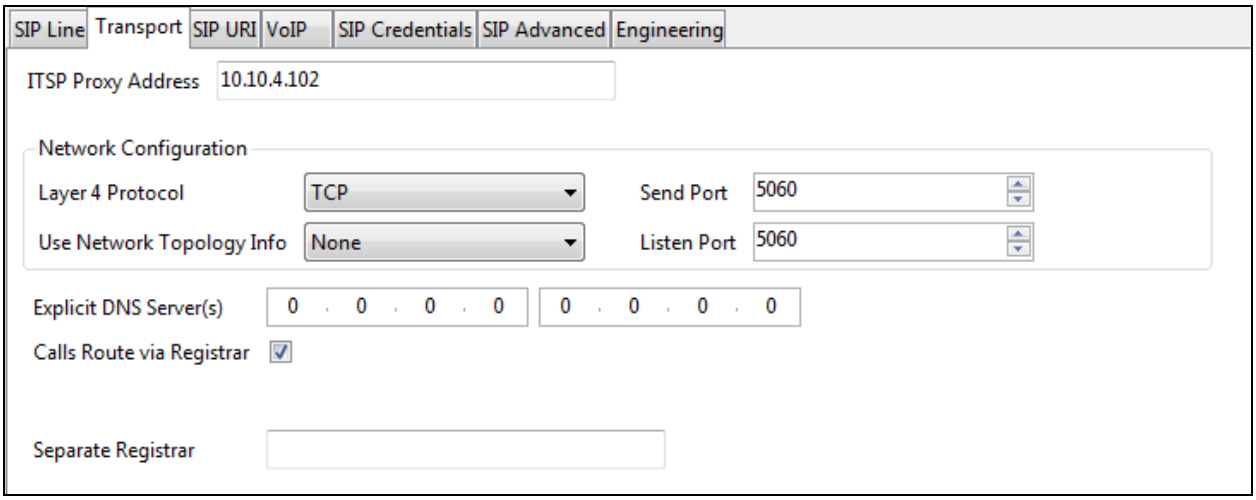


On completion, click the **OK** button (not shown).

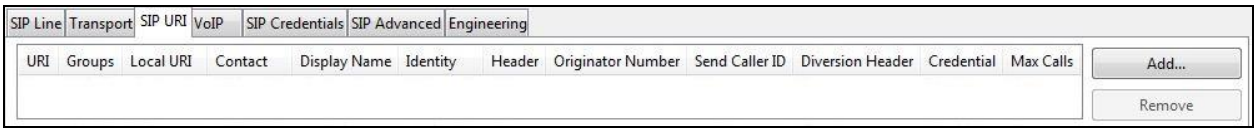
Select the **Transport** tab and set the following:

- Set **ITSP Proxy Address** to the internal IP Address of the Avaya SBCE.
- Set **Layer 4 Protocol** as required. During testing **TCP** was used though TLS is recommended once the RTP to SRTP conversion issue described in **Section 2.2** is resolved.
- 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 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.

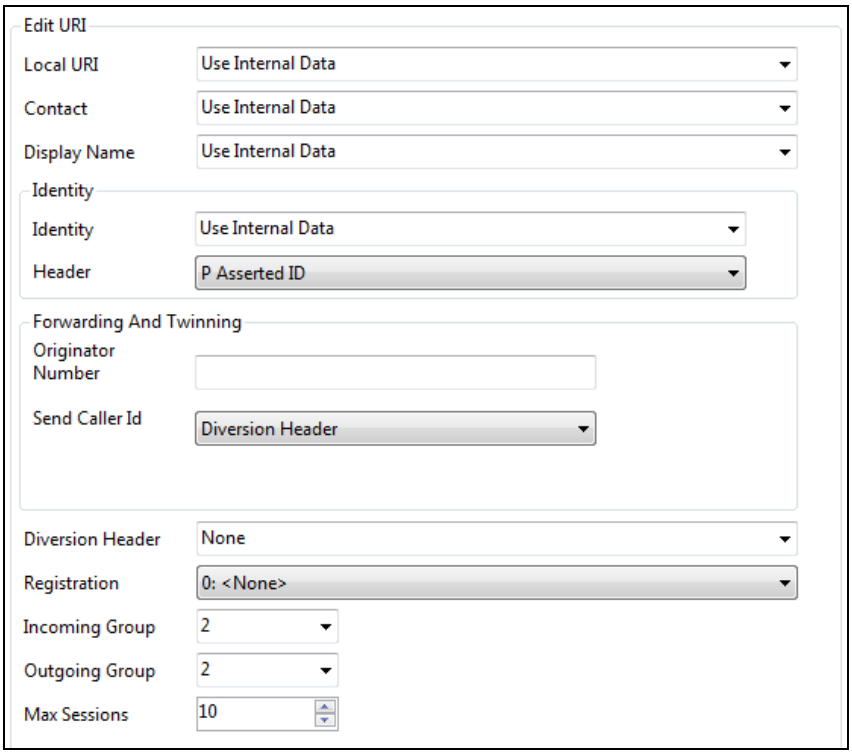


A SIP URI is shown in this example that is used for calls to and from extensions that have a DDI number assigned to them. Additional SIP URI's may be required for calls to services such as Voicemail Collect and the Mobile Twinning FNE, these would be for incoming calls only.

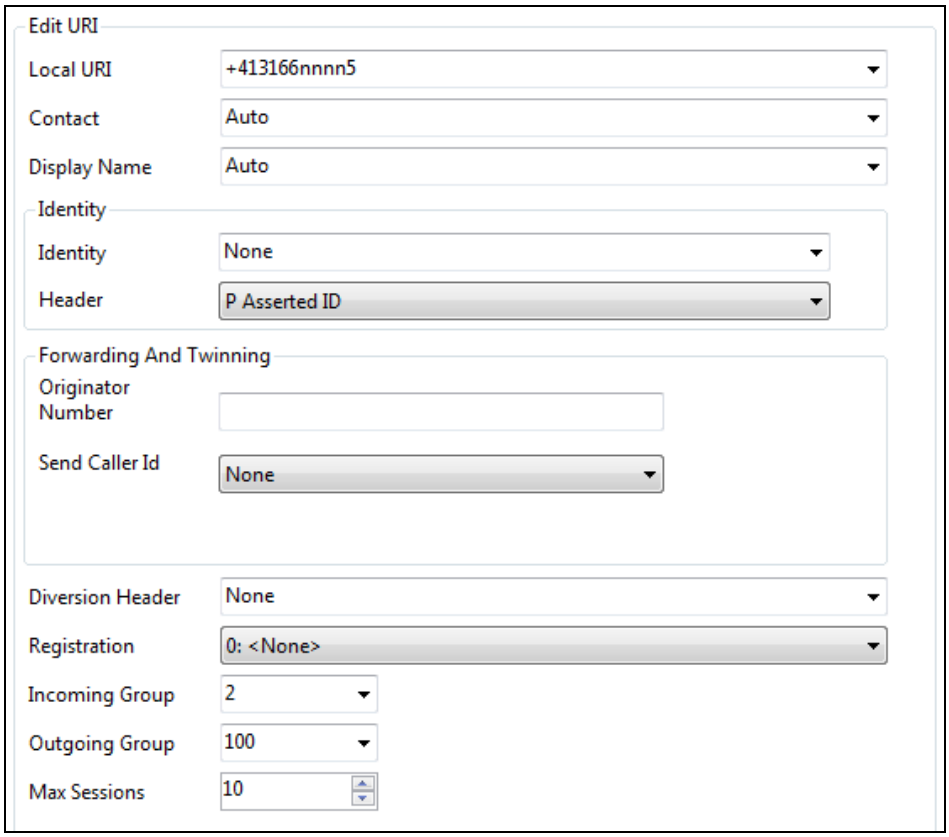
The SIP URI for calls to and from extensions that have DDI numbers associated with them was created with the parameters shown below.

- 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.
- Leave the **Registration** drop down menu at the default value of **0: <None>**. Although registration and authorisation are used, the function is provided by the Avaya SBCE as described in **Section 6.6**.
- 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.

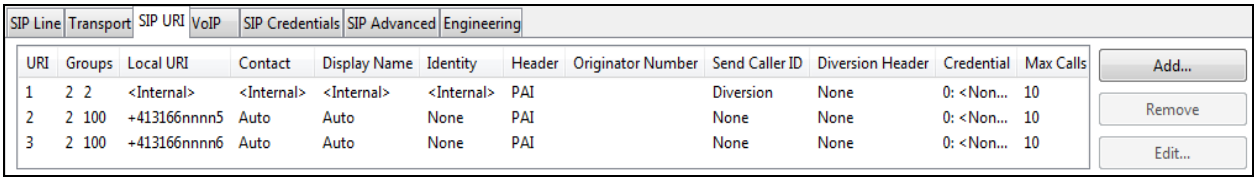
On completion, click the **OK** button.



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:

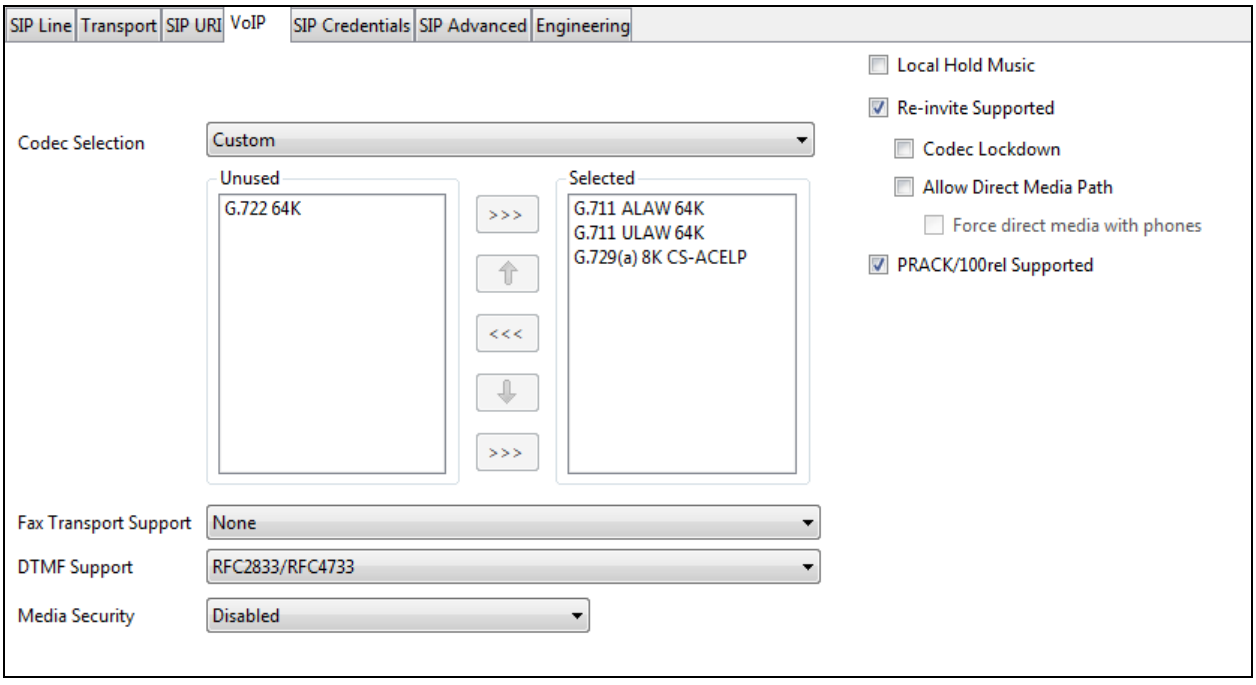


The following screenshot shows the completed configuration:



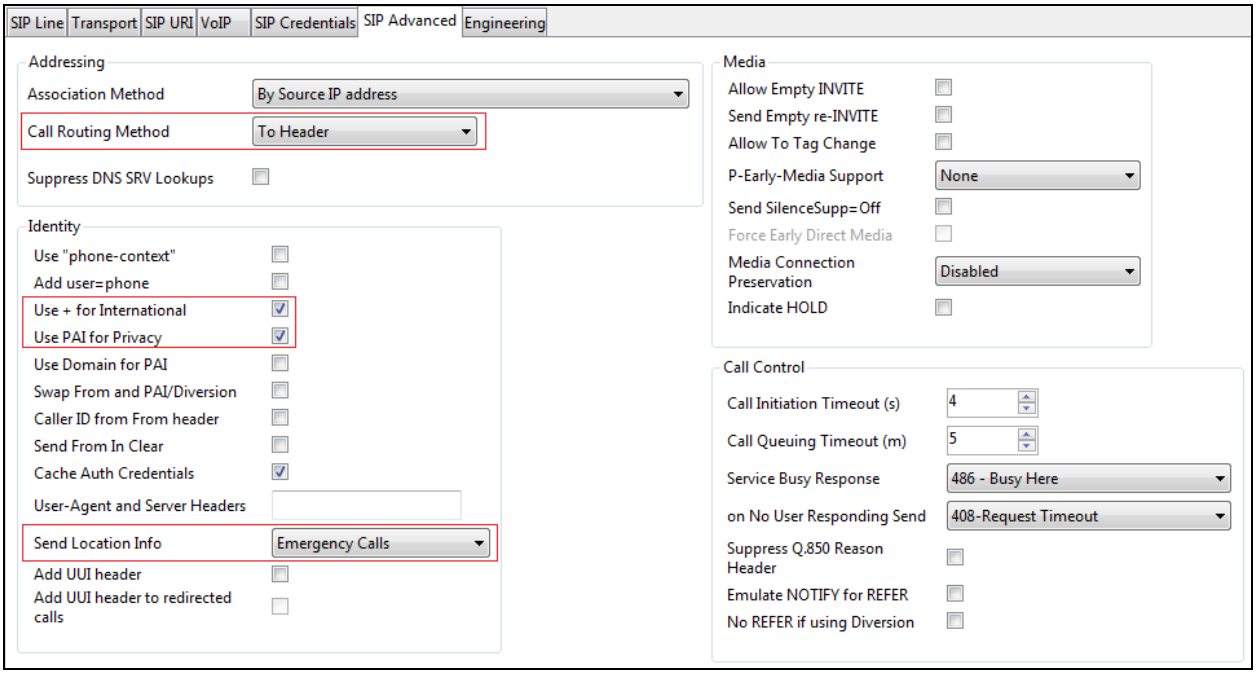
Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- 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 can be used where the endpoints are in the same network as the internal interface of the Avaya SBCE, though this was not used during testing.
- 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 it was **Disabled** as there was an issue with conversion between RTP and SRTP on the Avaya SBCE as described in **Section 2.2**.



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.



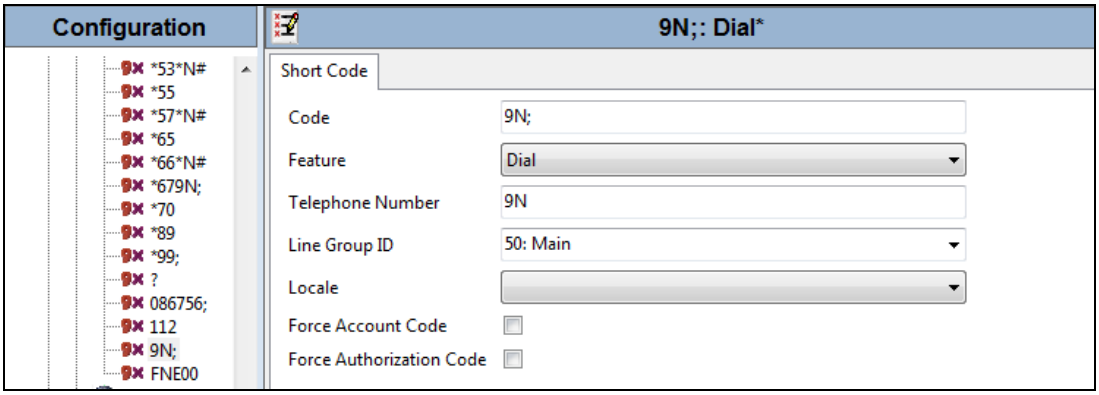
Note: The configuration shown above shows Location Info sent for Emergency calls. This was not tested, but is shown for information. The settings for Location data are shown in **Section 5.11**.

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

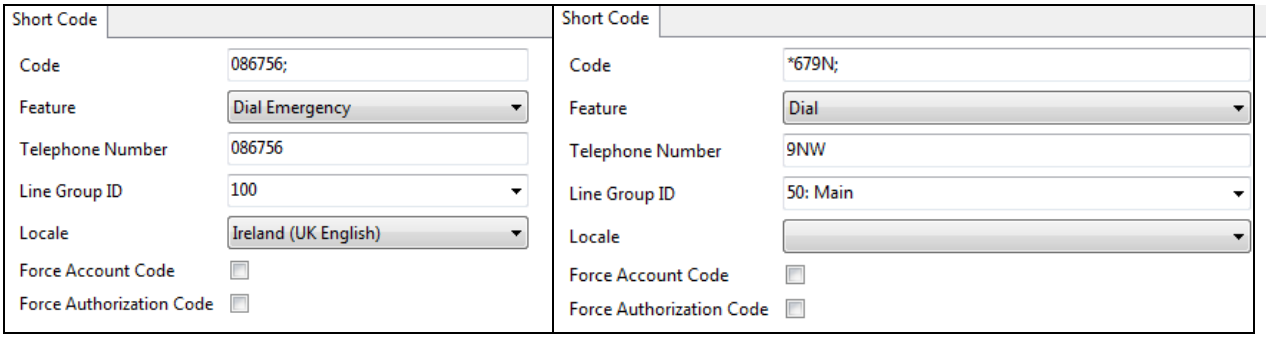
Define a short code to route outbound traffic to the SIP line. To create a short code, right-click **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as shown in the example below for public numbers.

- 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:

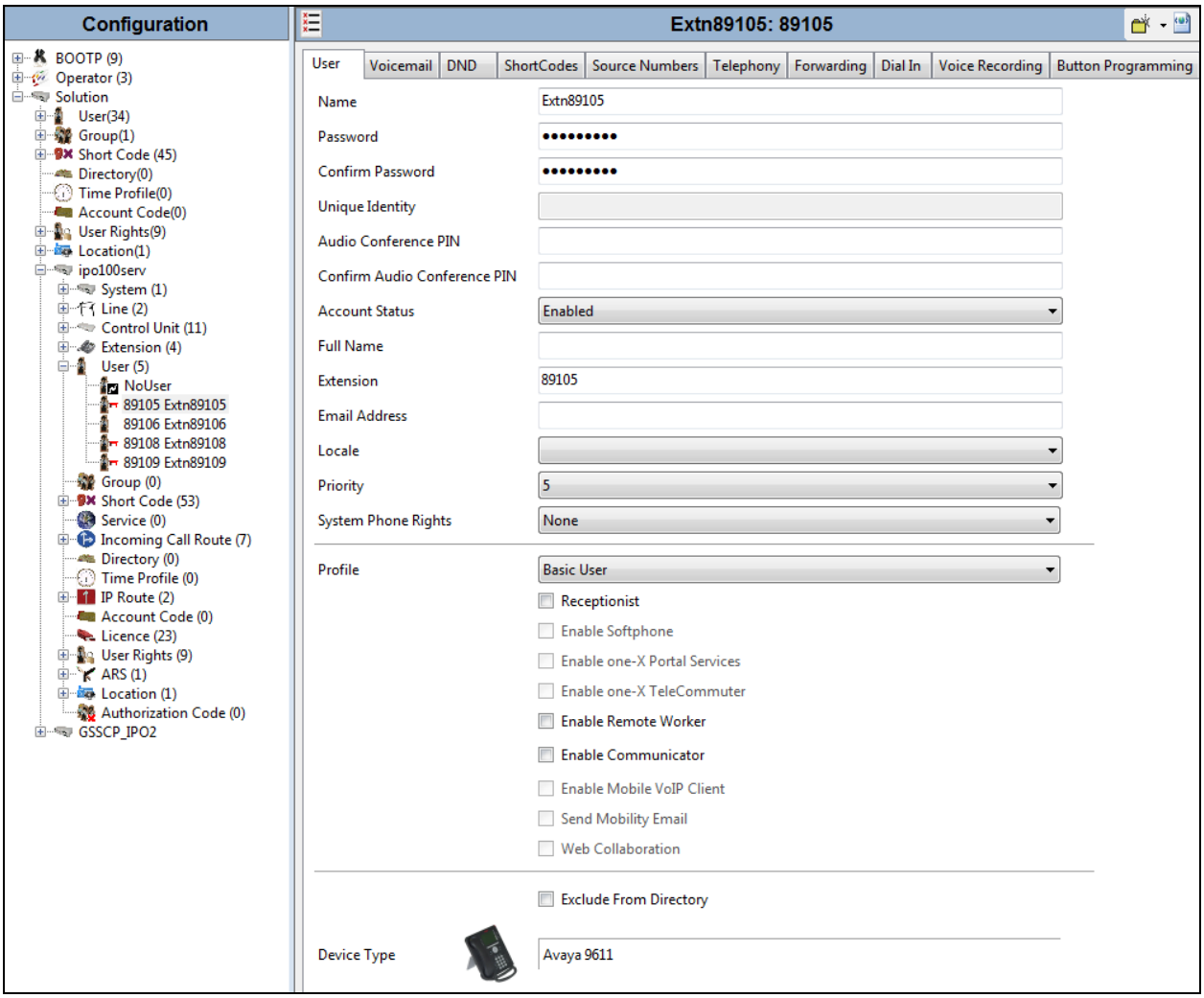
Code	***Feature***	***Telephone Number***	***Line Group ID***	***Description***
086756;	Dial Emergency	086756	100	Emergency Services Test Number. Feature uses Location data. Line Group ID is not used.
*679N;	Dial	9NW	50:Main	Public Number with *67 prefix. "W" suffix in Telephone Number withholds CLI.



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:

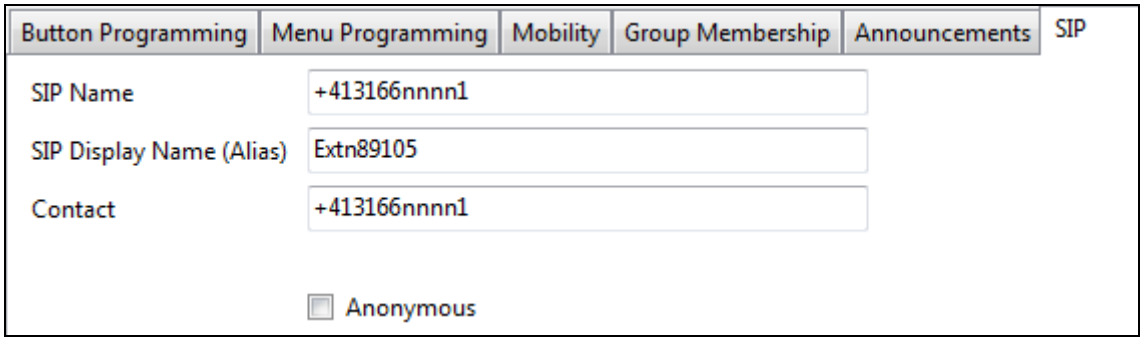
- Change the **Name** of the User if required.
- Set the **Password** and **Confirm Password**.
- Select the required profile from the **Profile** drop down menu. **Basic User** is commonly used; **Power User** can be selected for SIP softphone, WebRTC and Remote Worker endpoints.



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).



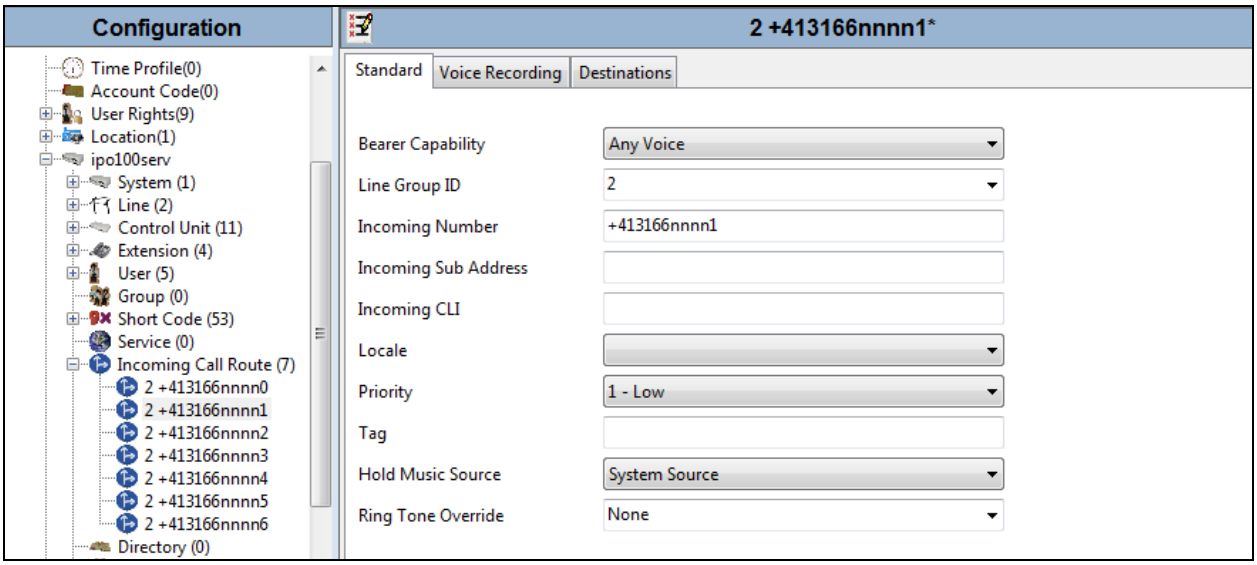
Note: The **Anonymous** box can be used to restrict Calling Line Identity (CLIR).

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).

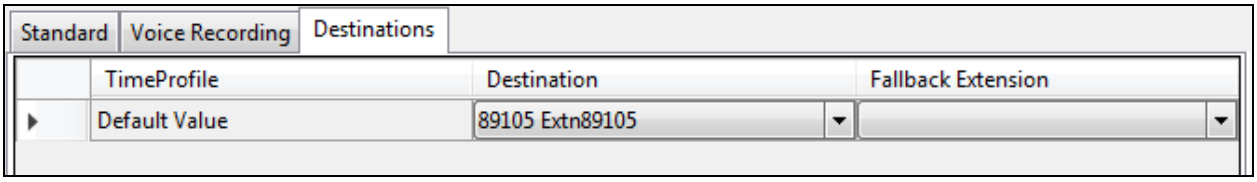
On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- 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 "+".

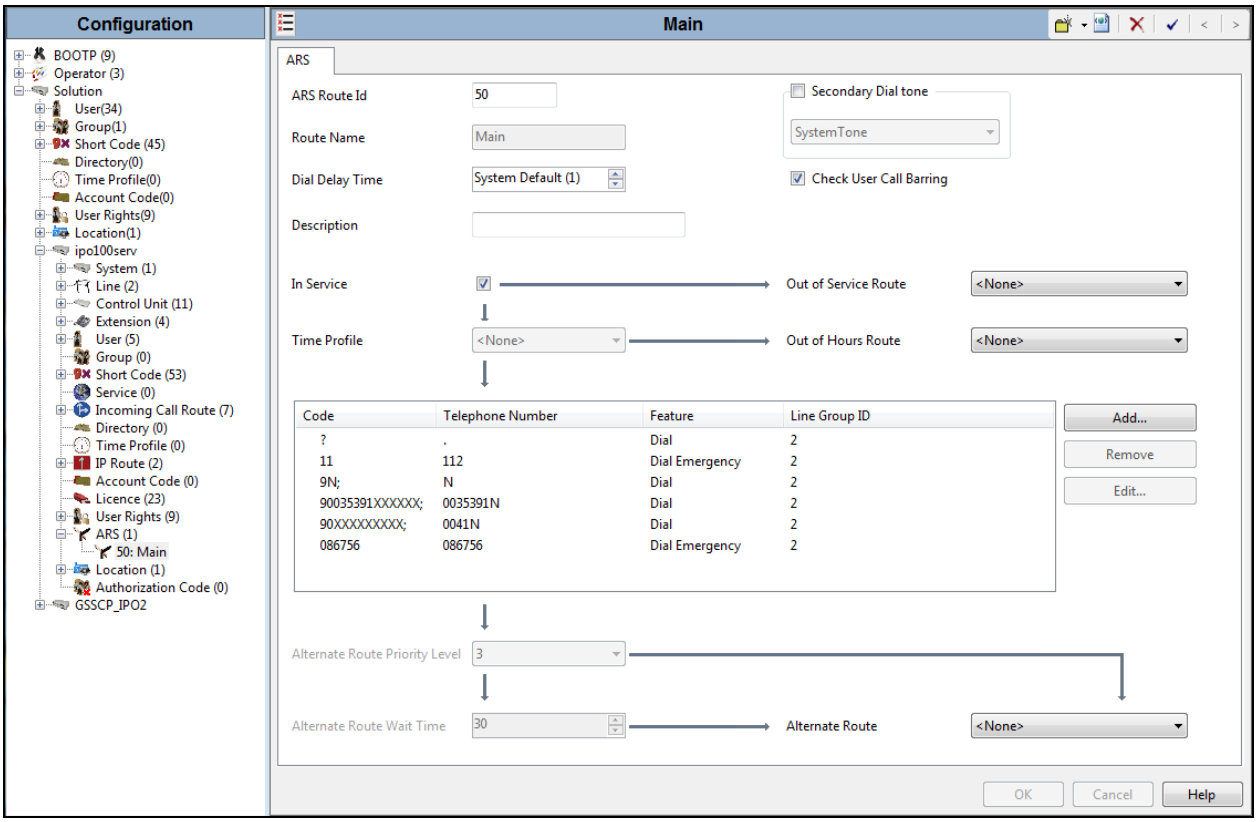
On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. On completion, click the **OK** button (not shown). In this example, incoming calls to the test DDI number on line **2** are routed to extension **89105**.



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.

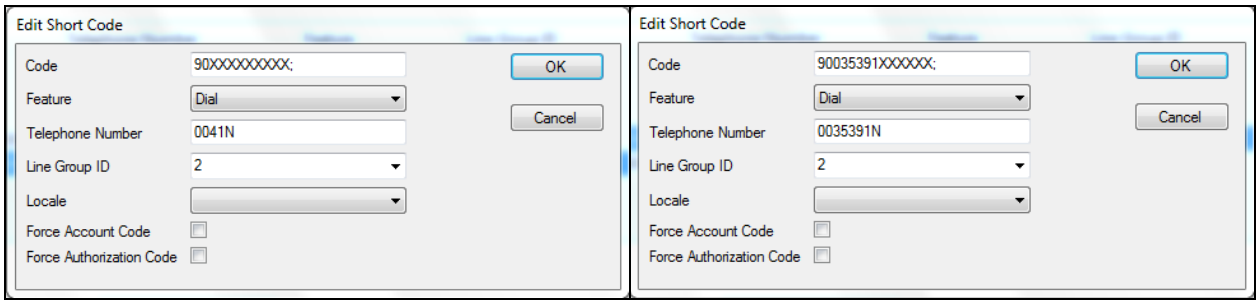
5.10. ARS

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

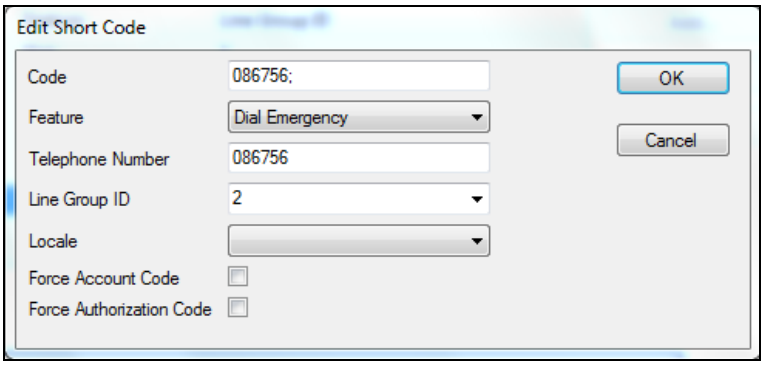


Define numbers as required. An example for national numbers is as follows:

- 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**



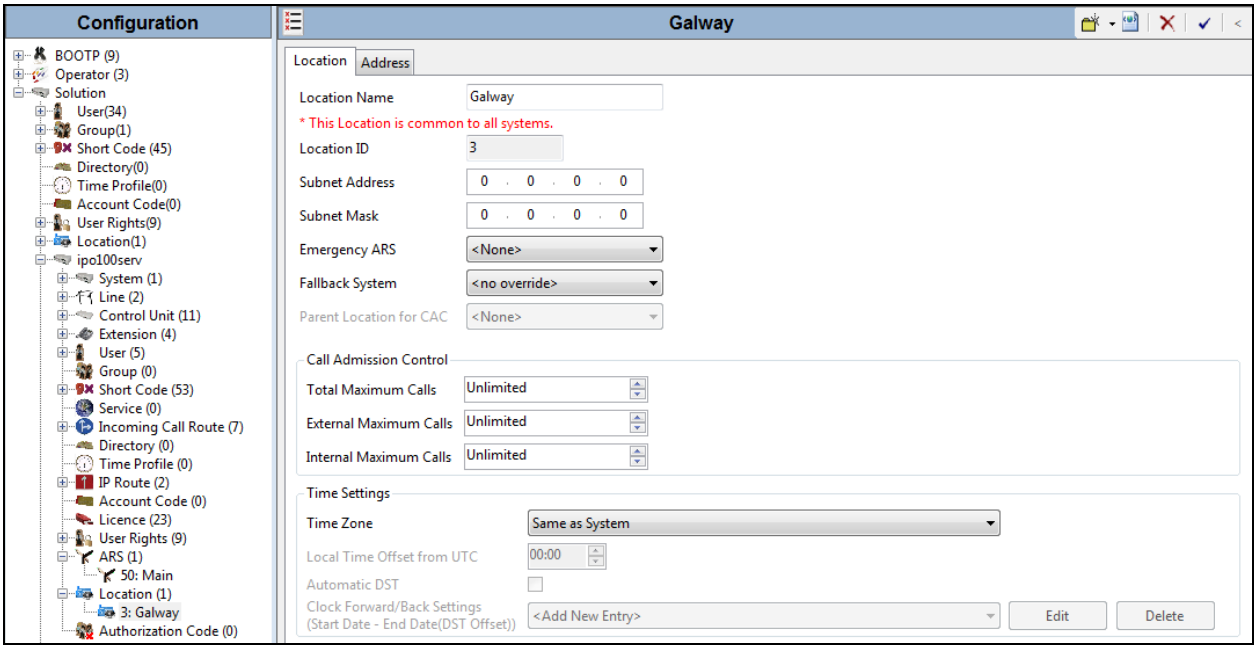
The **X** used in the Code indicates any digit and "**;**" causes the system to wait for the full number to be dialled or a "#". The next example shows an emergency number. Set **Feature** to **Dial Emergency**. The number shown is not a valid Emergency Services number, it is a test number used to check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



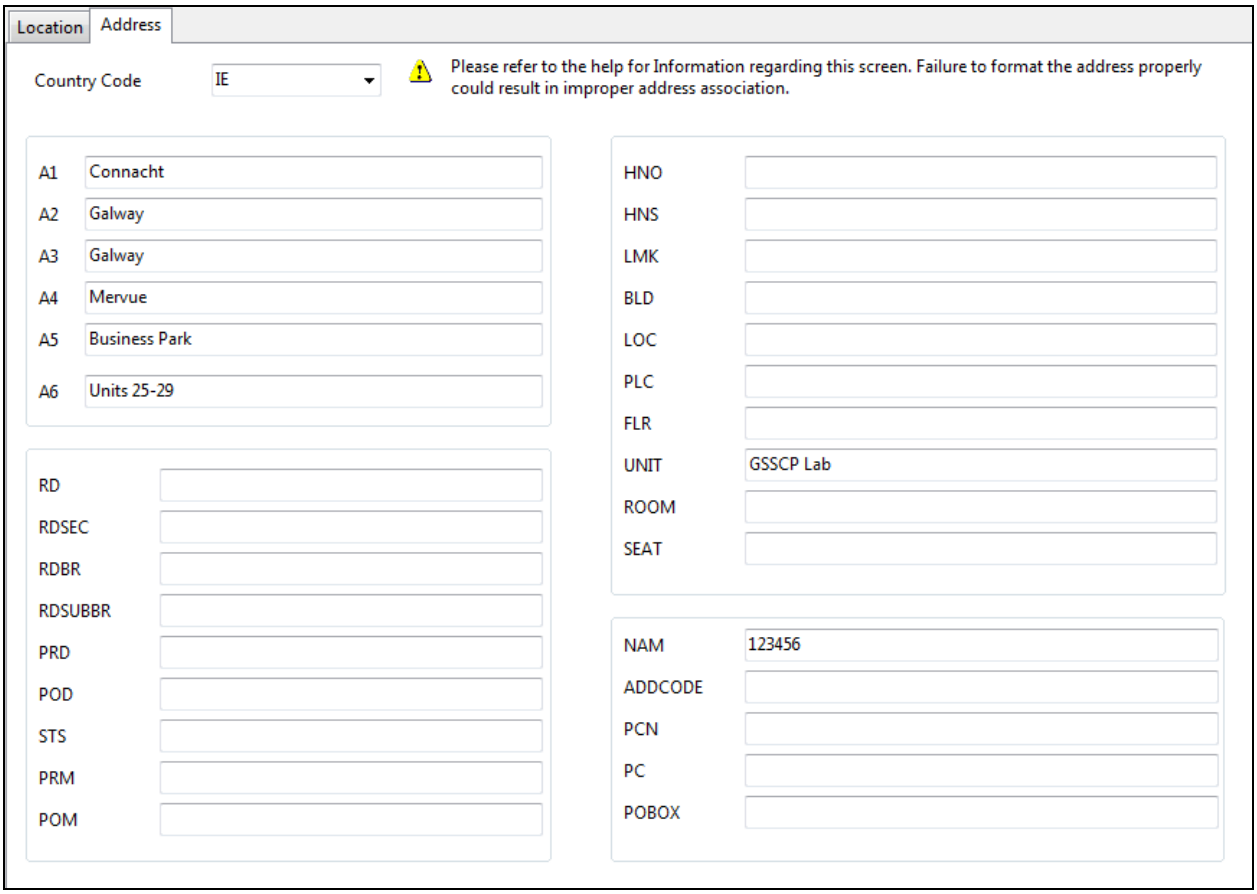
5.11. Location

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:

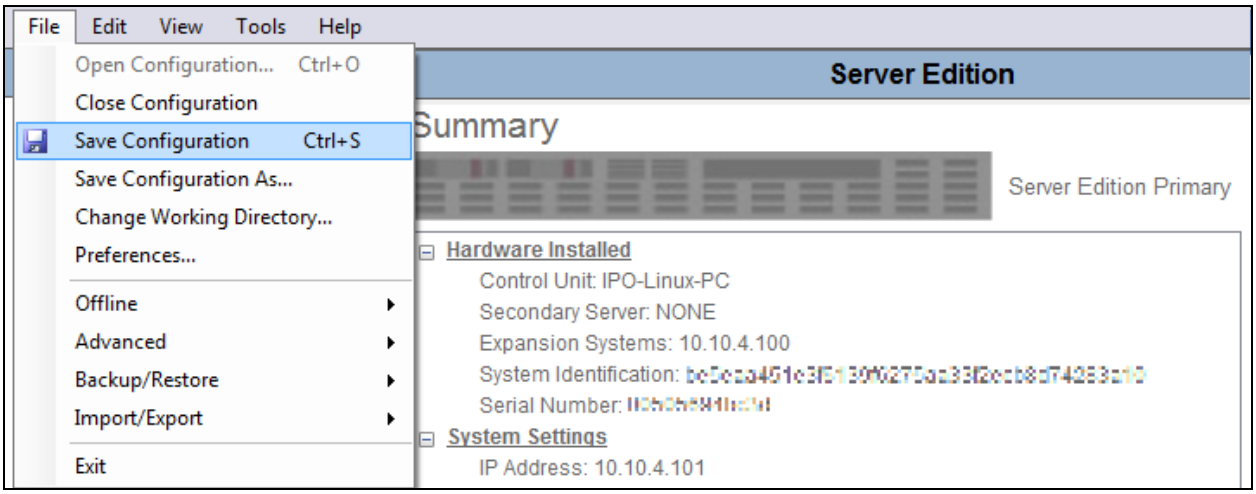


Note: The above example bears no relation to the information that would be used in the live environment. It was specified for the sole purpose of being identifiable in the SIP messages of the test calls.

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.



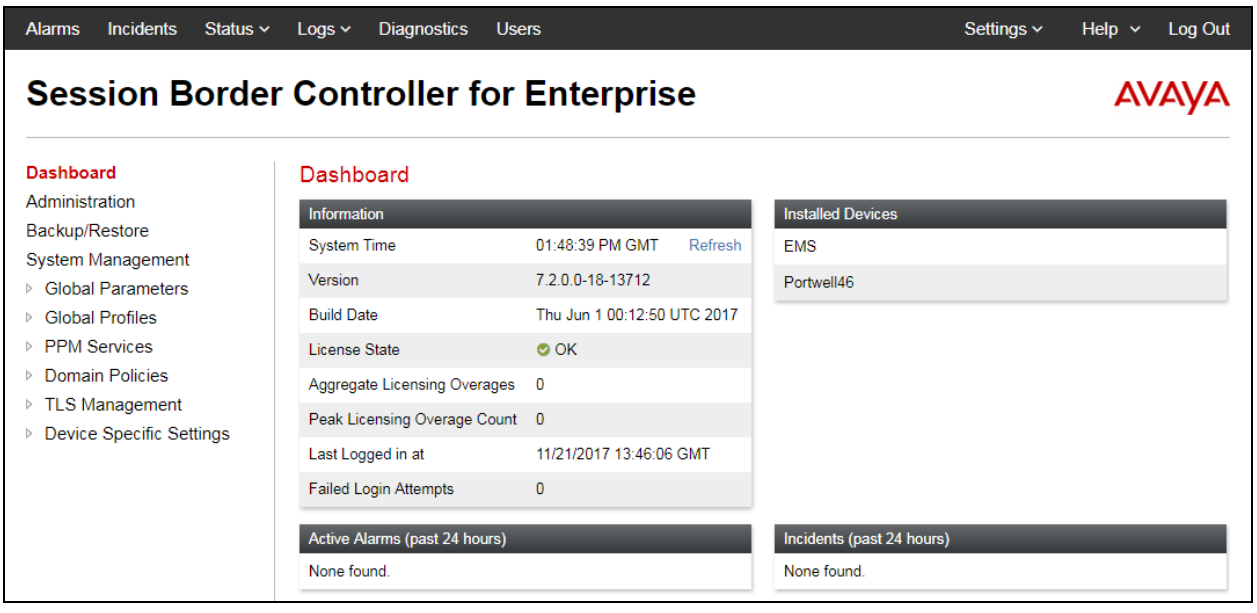
6. Configure Avaya Session Border Controller for Enterprise

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

6.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using the appropriate username and password.

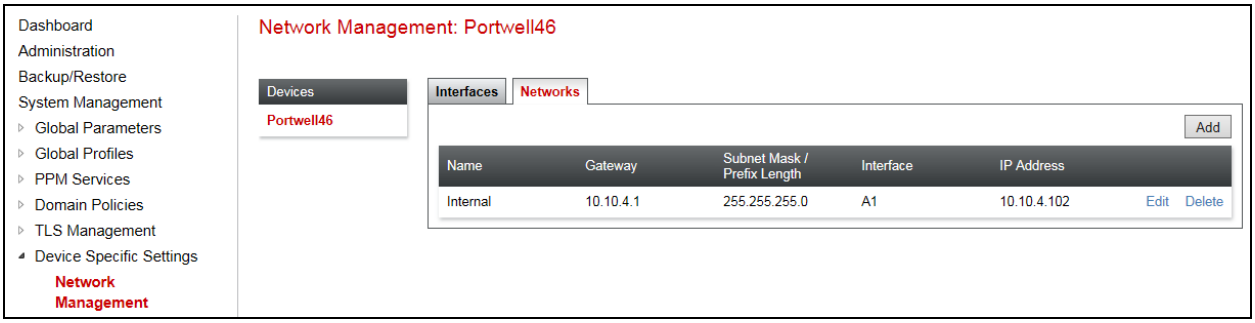
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



6.2. Define Network Management

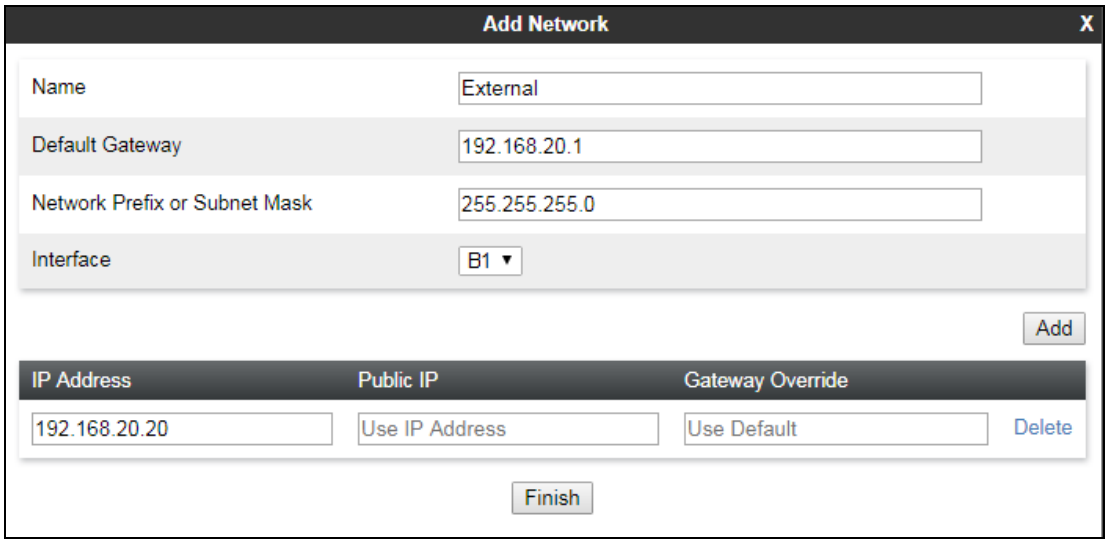
Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external.

To define the network information, navigate to **Device Specific Settings → Network Management** in the main menu on the left hand side and click on **Add**.



Enter details for the external interface in the dialogue box:

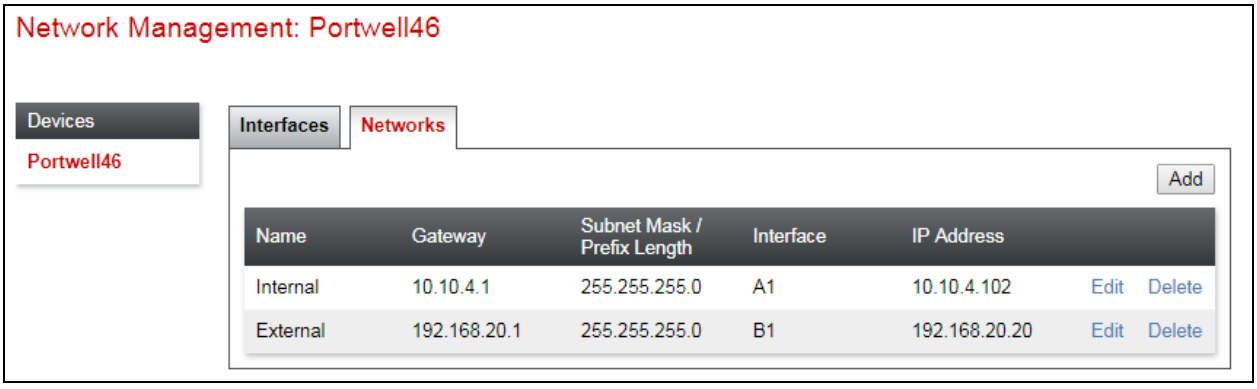
- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field. In the test environment, this was the IP address of the VPN server.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external physical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



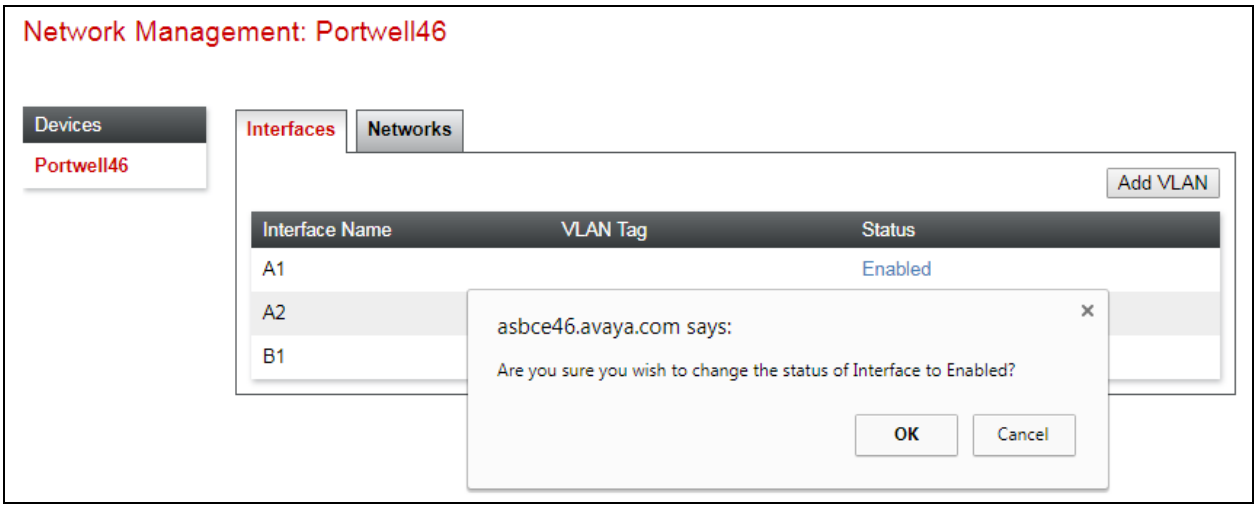
Click on **Add** again to define the internal interface if required. Enter details in the dialogue box (not shown):

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

The following screenshot shows the completed Network Management configuration:



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



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

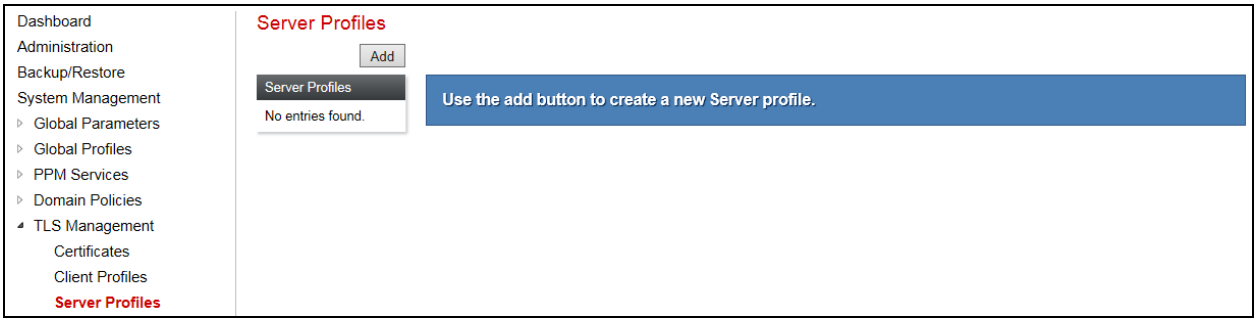
- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

6.3. Define TLS Profiles

TLS profiles are required to support TLS on the interfaces. The implementation of certificates is beyond the scope of this document and is assumed to be already in place. The signalling interfaces require a TLS server profile and the server configuration requires a TLS client profile.

6.3.1. Server Profile

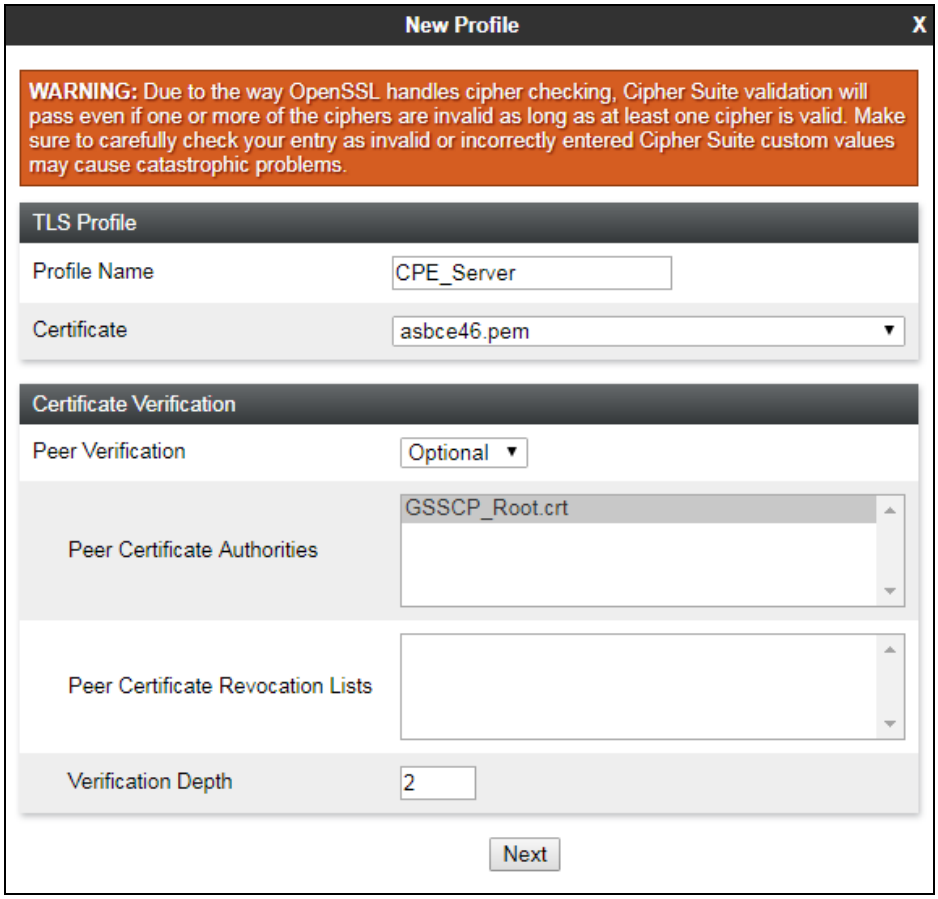
To define a TLS server profile on the Avaya SBCE, navigate to **TLS Management → Server Profiles** in the main menu on the left hand side. Click on **Add.**



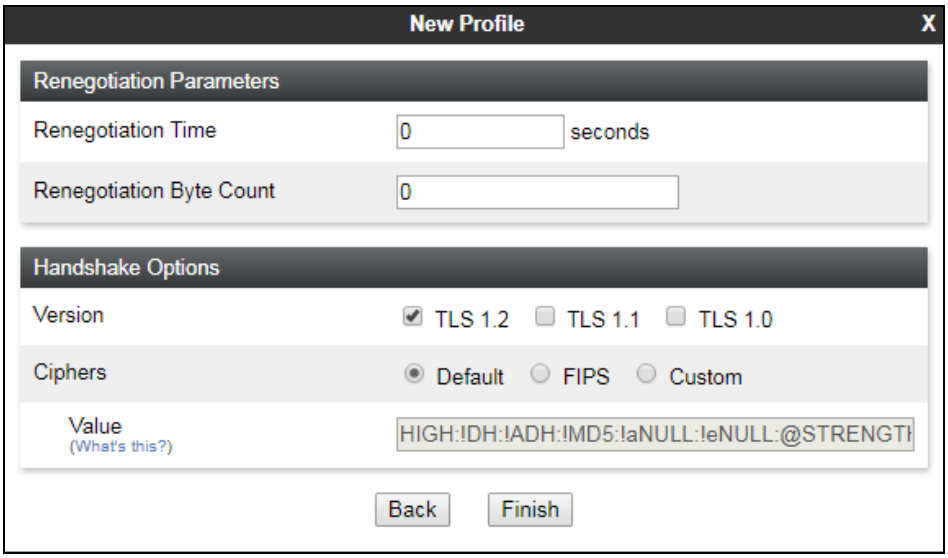
Details of the TLS server profile for the signalling interfaces are entered here.

- In the **Name** field enter a descriptive name for the server profile.
- In the **Certificate** drop down menu, select the Avaya SBCE identity certificate to be used for this profile.
- Select **Peer Verification** as required. In the test environment peer verification was made optional by selecting **Optional** in the drop down menu.
- Highlight the trusted root certificate in the **Peer Certificate Authorities** field.
- Set the **Verification Depth** as required. The example shown is for the link with IP Office which has an identity certificate provided by a System Manager implemented as a sub-CA. This means that the IP Office identity certificate is signed by an intermediate certificate which is in turn signed by a root certificate. This gives it a depth of **2**.

Once the server profile details are entered, click on **Next**.

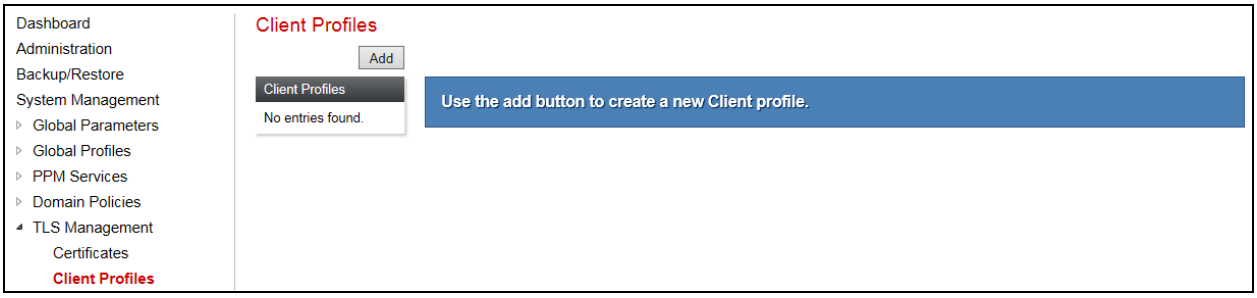


The next dialogue box completes the server profile configuration. In the test environment, these parameters were left at default values. Click on **Finish**.



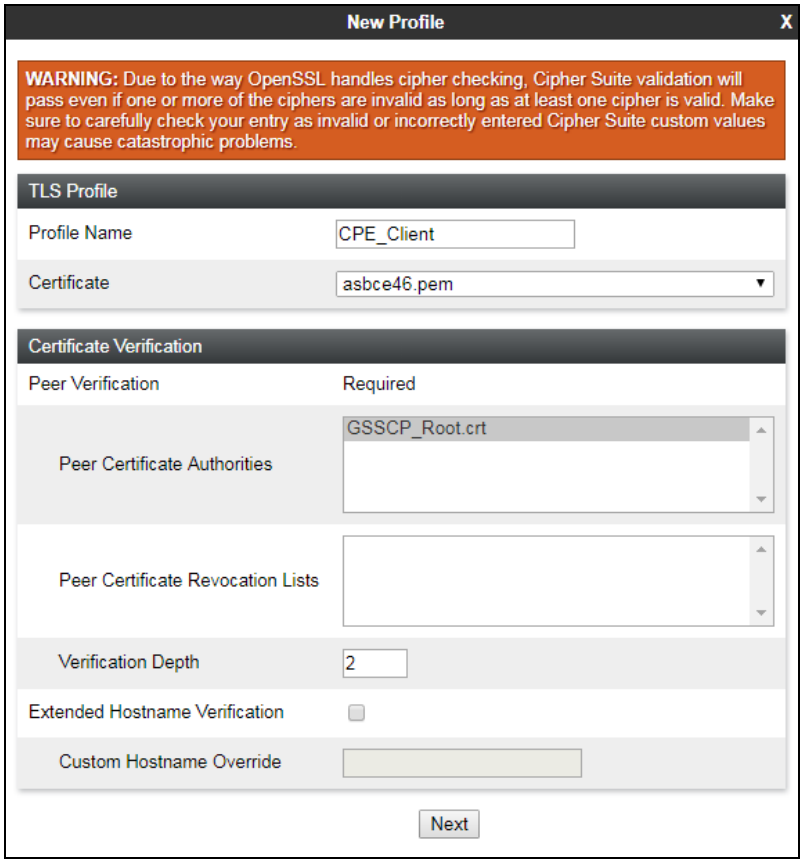
6.3.2. Client Profile

To define a TLS client profile on the Avaya SBCE, navigate to **TLS Management → Client Profiles** in the main menu on the left hand side. Click on **Add.**



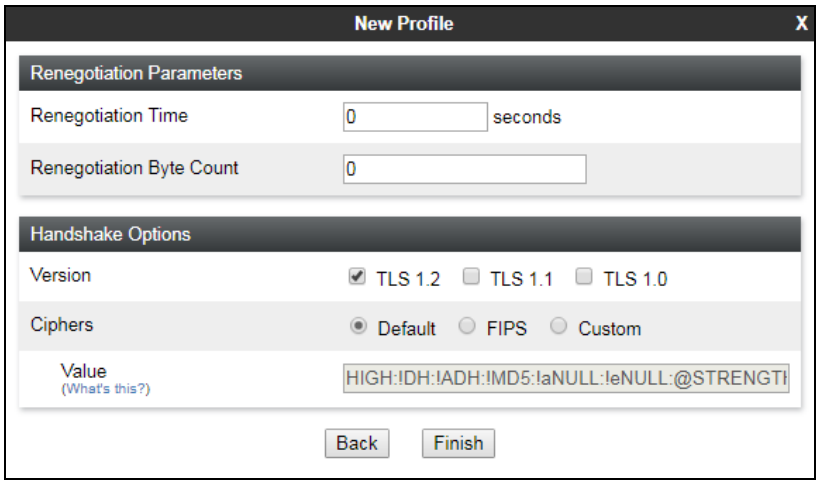
Details of the TLS client profile for the signalling interfaces are entered here.

- In the **Name** field enter a descriptive name for the client profile.
- In the **Certificate** drop down menu, select the Avaya SBCE identity certificate to be used for this profile.
- Highlight the trusted root certificate in the **Peer Certificate Authorities** field.
- Set the **Verification Depth** as required. This was **2** in the test environment as explained in the Server Profile configuration.



Note: Peer Verification is always **Required** for the client profile.

Click on **Next** to complete the client profile configuration. In the test environment, these parameters were left at default values. Click on **Finish**.

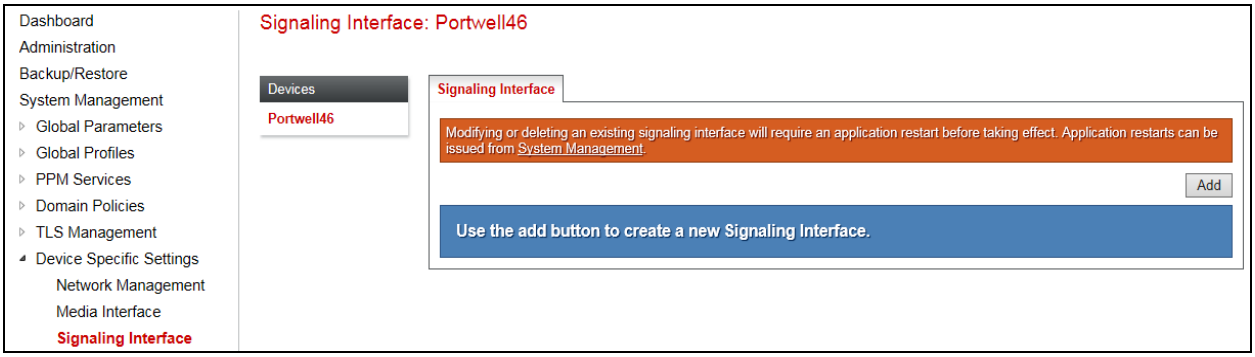


6.4. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces. Testing was carried out using TCP for transport of signalling between IP Office and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and Swisscom Smart Business Connect. Signalling and media interfaces were required on both the internal and external sides of the Avaya SBCE to handle traffic between the Avaya SBCE and IP Office, and Avaya SBCE and Swisscom Smart Business Connect.

6.4.1. Signalling Interfaces

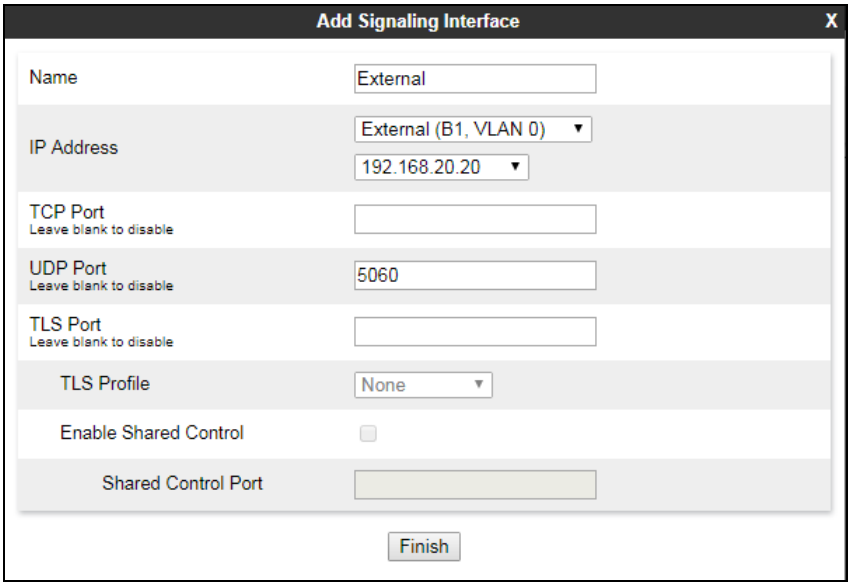
To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Signaling Interface** in the main menu on the left hand side. Click on **Add**.



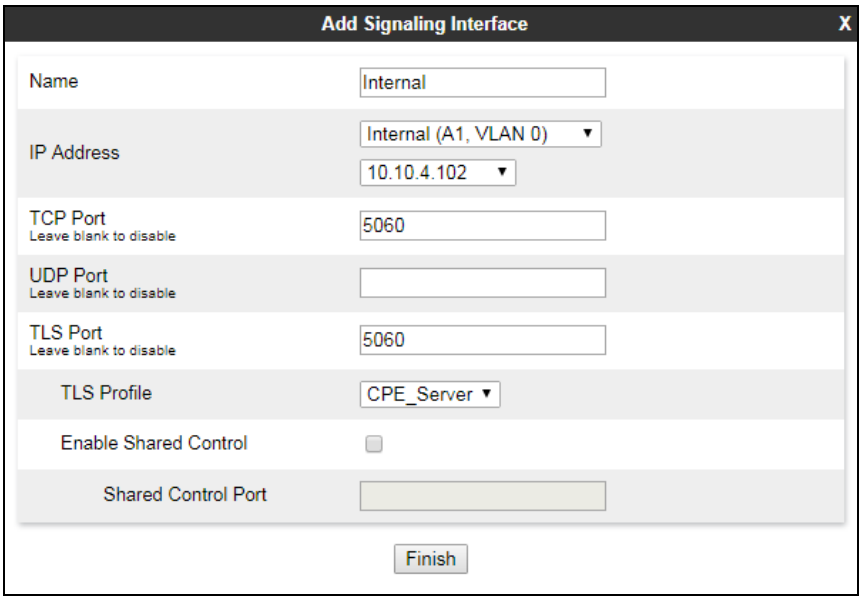
Details of transport protocol and ports for the external and internal SIP signalling are entered in the dialogue box. Note that in the test environment, the internal interface was enabled for both TCP and TLS.

Enter details for the signalling interface as follows:

- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 6.2**. In the test environment, this was IP address **192.168.20.20**.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for Swisscom.

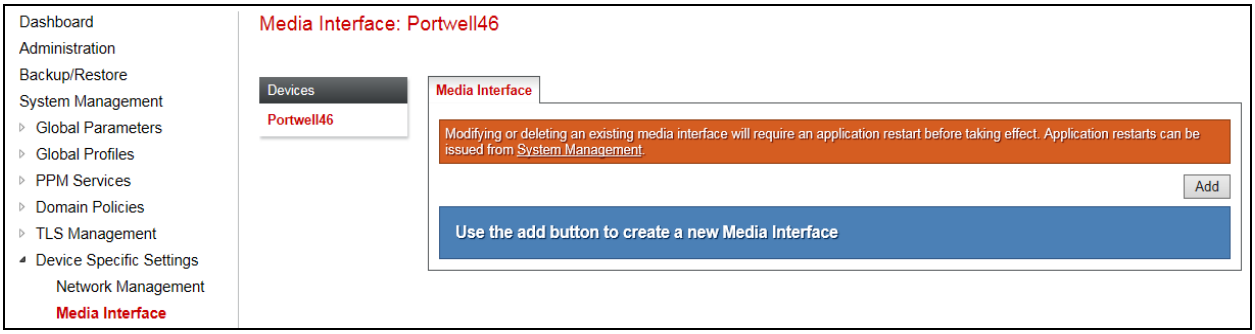


The internal signalling interfaces are defined in the same way. In the **IP Address** drop down menus, select the internal network interface and IP address. Additionally, if TLS is used between the Avaya SBCE and the IP Office, enter the port number and select the **TLS Profile** created in **Section 6.3.1** in the drop down menu. Click on **Finish**.



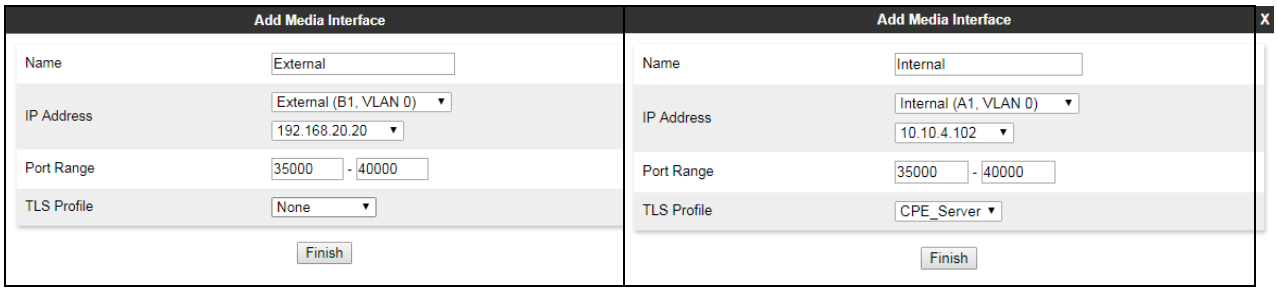
6.4.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Media Interface** in the main menu on the left hand side. Click on **Add**.



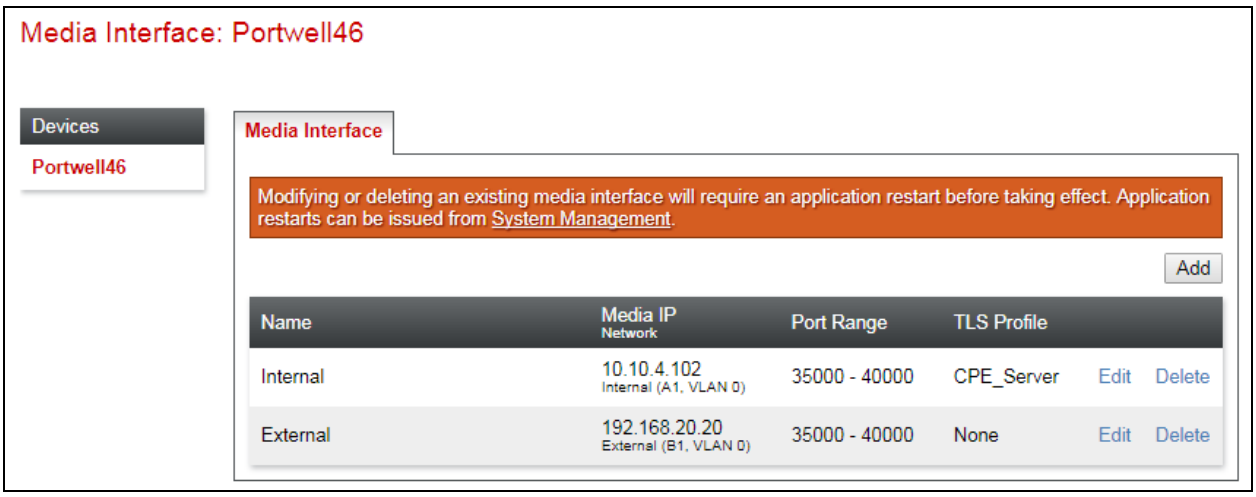
Details of the RTP port ranges for the internal and external media streams are entered in the dialogue box. The IP addresses for media can be the same as those used for signalling.

- In the **Name** field enter a descriptive name for the media interface.
- In the **IP Address** drop down menus, select the network interface and IP address. Note that when the network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 6.2**. In the test environment, this was **192.168.20.20** for the external and **10.10.4.102** for the internal interfaces.
- Define the RTP **Port Range** for the media path with Swisscom Smart Business Connect (external) or IP Office (internal), during testing this was left at default values of **35000** to **40000**.
- Click on **Finish**.



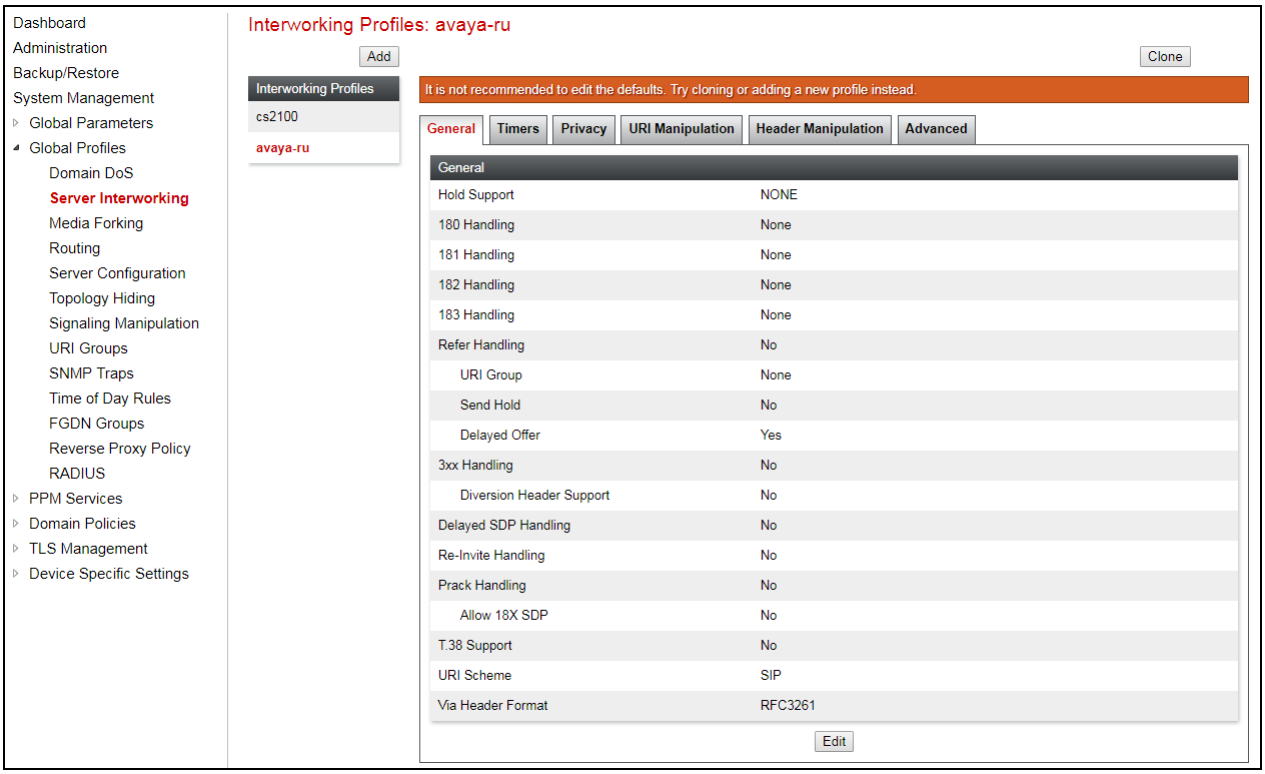
Note: If TLS and SRTP are used between the Avaya SBCE and the IP Office, the **TLS Profile** created in **Section 6.3.1** can be selected in the drop down menu. TLS and SRTP were not used in the test environment because of the issue described in **Section 2.2**.

The screenshot shows the completed configuration:

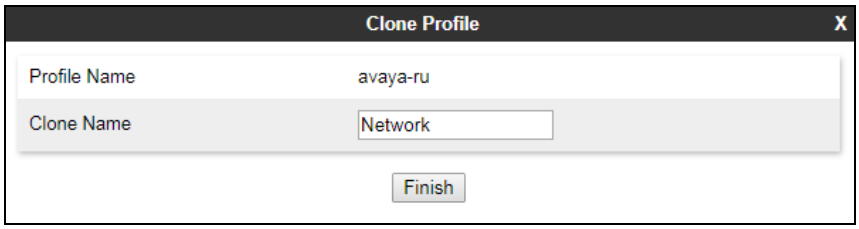


6.5. Define Server Interworking

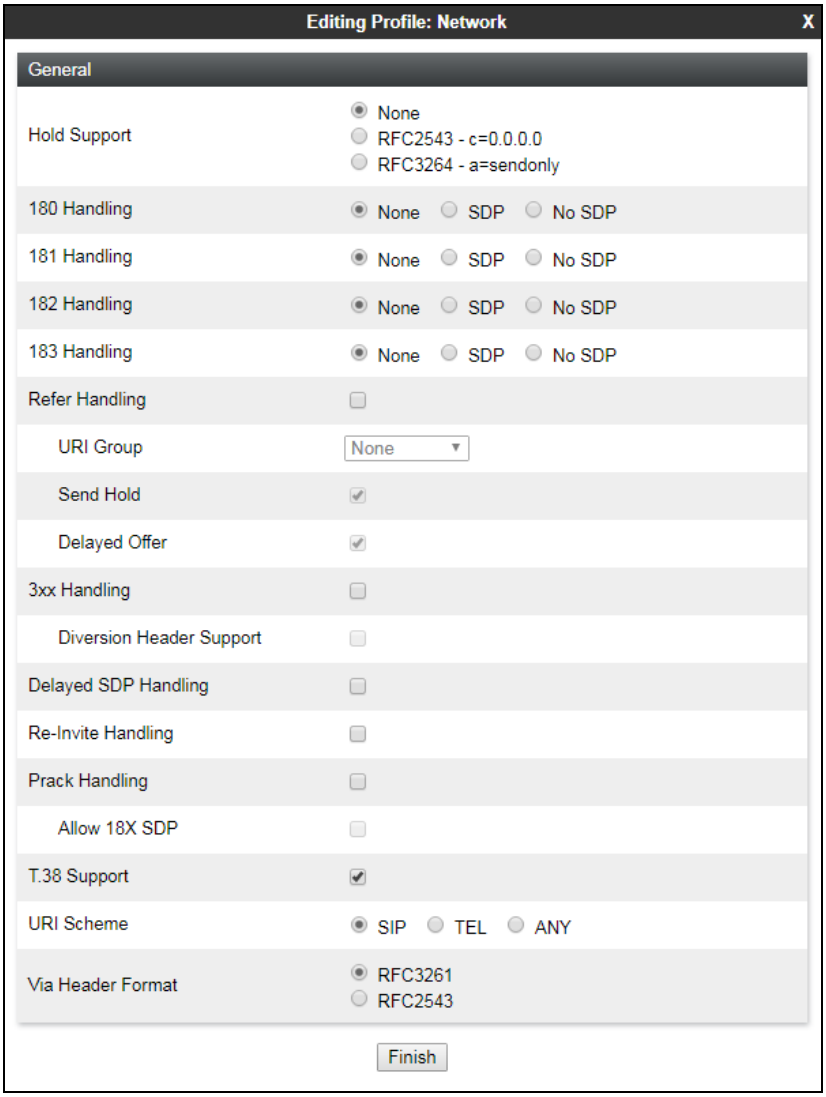
Server interworking is defined for servers connected to the Avaya SBCE. To define server interworking, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. Server Interworking for Swisscom Smart Business Connect can be defined by cloning a default profile. Highlight the **avaya-ru** profile and click on **Clone**.



A dialogue box is displayed. In the **Name** field enter a descriptive name for the SIP Trunk, in the test environment **Network** was used. Click on **Finish**.

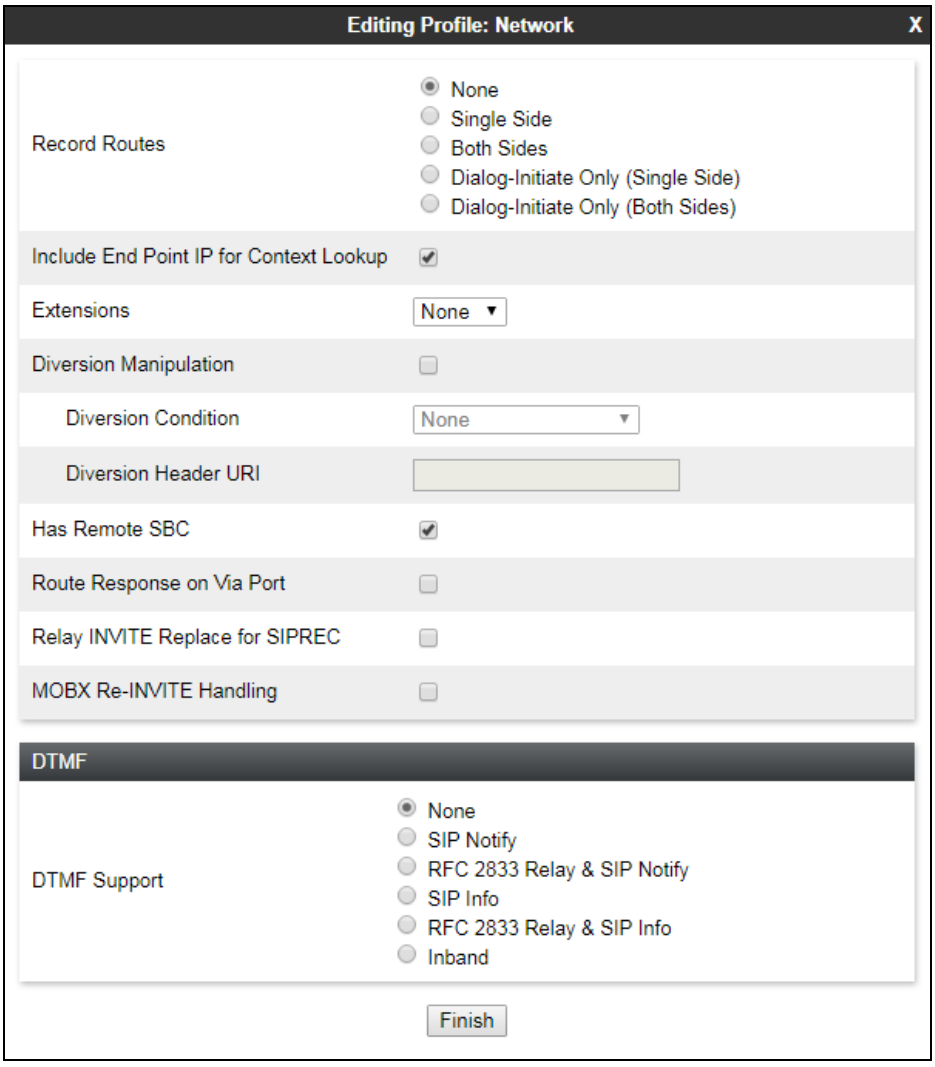


The profile is created and can be edited from the main menu. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions. Select the **General** tab and click on **Edit** (not shown). In the test environment, the **T.38 Support** box was checked even though T.38 fax is not supported. All the rest of the settings were left at default values. Click on **Finish**.



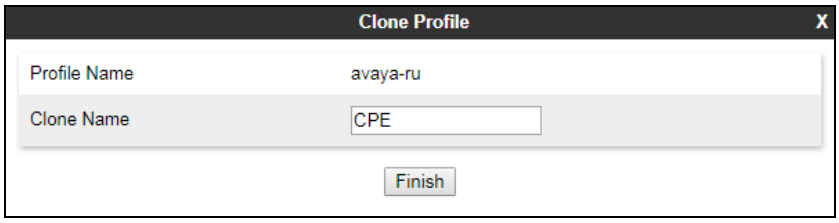
Select the **Advanced** tab (not shown) and click on **Edit**. Define the following settings in the dialogue box:

- Check the **None** radio button in the **Record Routes** field.
- Select **None** in the **Extensions** drop down menu.
- Ensure that the **Has Remote SBC** box is checked.
- Click on **Finish.**



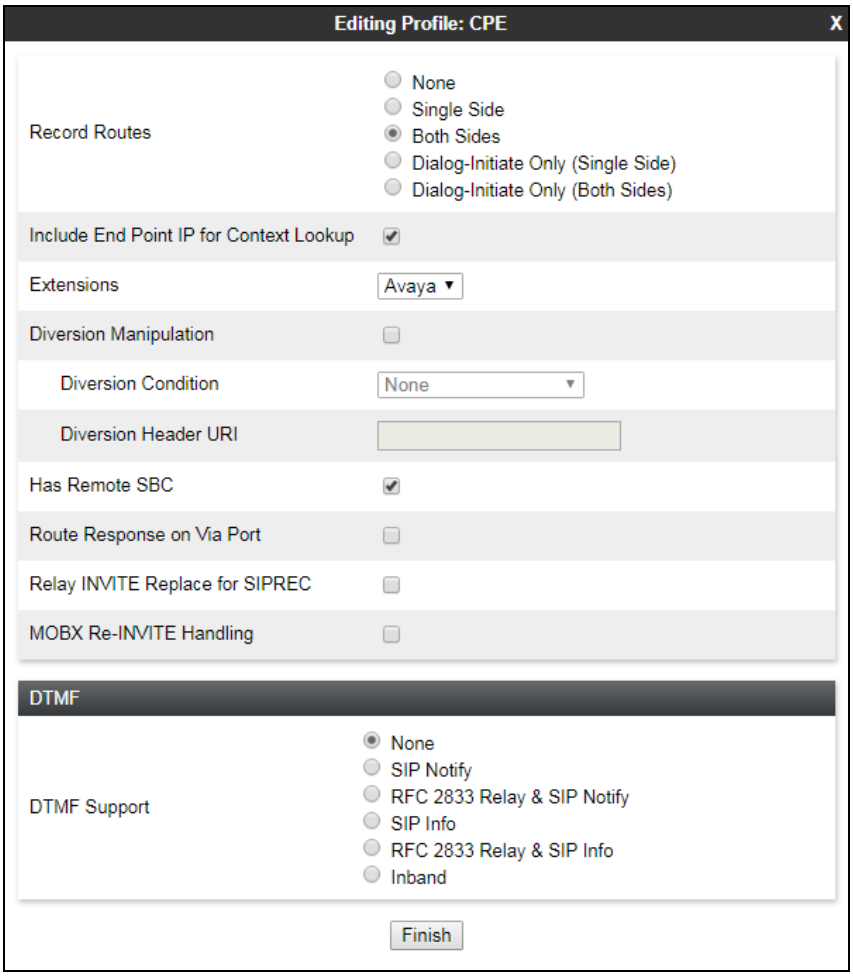
Repeat the process to define Server Interworking for IP Office. Navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. Highlight the **avaya-ru** profile and click on **Clone.**

In the **Name** field of the dialogue box, enter a descriptive name for IP Office. In the test environment **CPE** was used. Click on **Finish**.



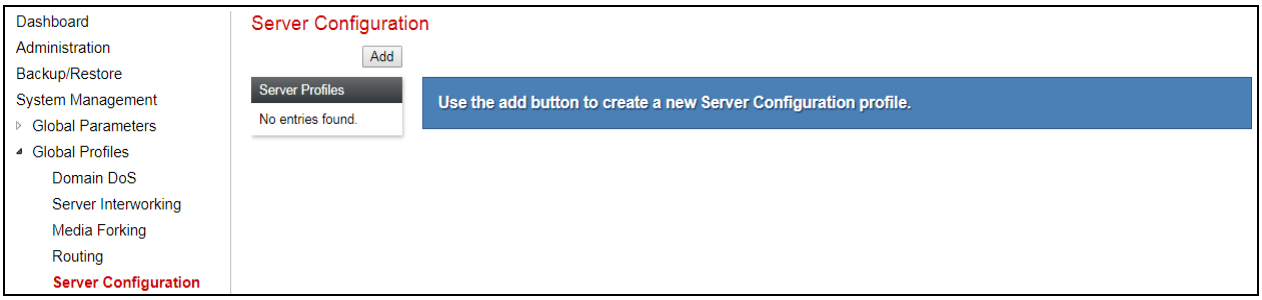
The profile is created and can be edited from the main menu. Select the **General** tab (not shown) and click on **Edit**. In the dialogue box (not shown) the settings can be left at default values, though the **T.38 Support** box was checked in the test environment. Select the **Advanced** tab (not shown) and click on **Edit**. Define the following settings in the dialogue box:

- Check the **Both Sides** radio button in the **Record Routes** field.
- Select **Avaya** in the **Extensions** drop down menu.
- Ensure that the **Has Remote SBC** box is checked.
- Click on **Finish.**

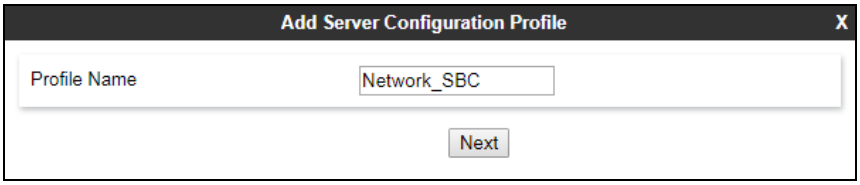


6.6. Define Servers

A server definition is required for each SIP Trunk connected to the Avaya SBCE. In the case of the test environment, this was IP Office on the enterprise side and the Swisscom SIP Trunk on the network side. To define the Swisscom Smart Business Connect server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add**.

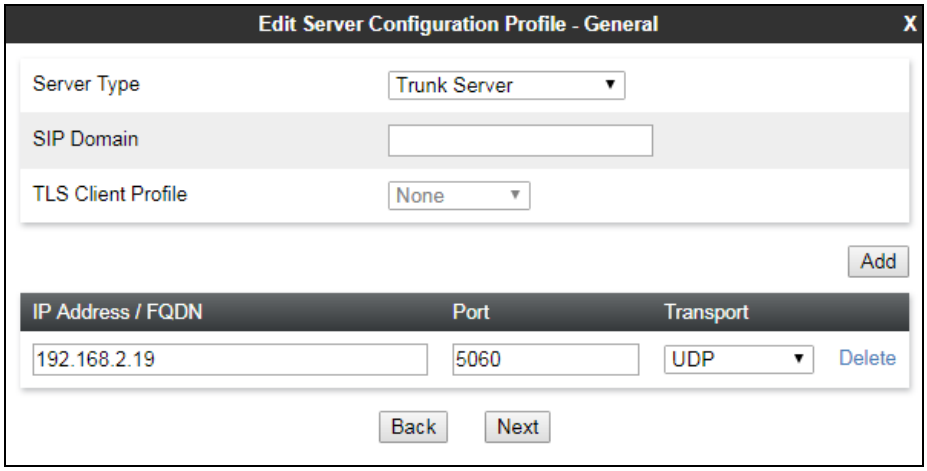


Enter an appropriate name in the dialogue box displayed. Note that for the purposes of documentation, an assumption was made that that the Avaya SBCE was connecting to an SBC in the Swisscom Smart Business Connect network.

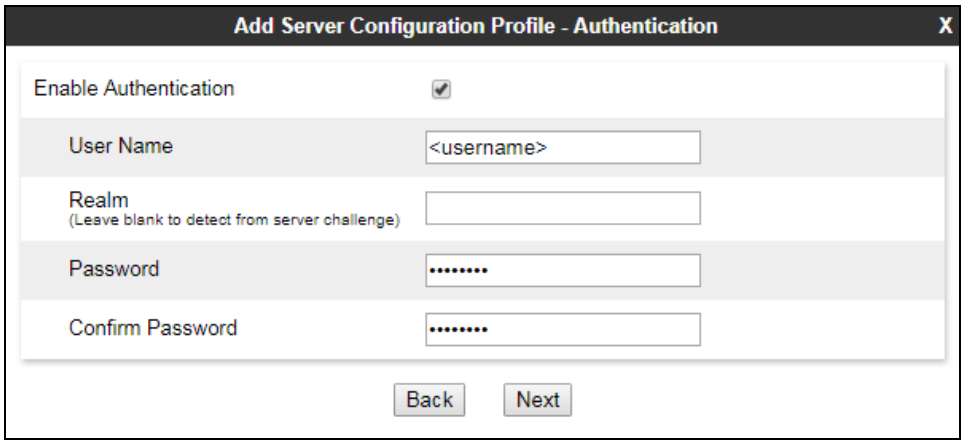


Click on **Next** and enter configuration settings in the dialogue box displayed:

- In the **Server Type** drop down menu, select **Trunk Server**.
- Click on **Add** to enter an IP address or FQDN.
- In the **IP Address / FQDN** box, type the IP address of the Swisscom network SBC.
- In the **Port** box, enter the port to be used for the SIP Trunk, typically **5060** for UDP.
- In the **Transport** drop down menu, select **UDP**.

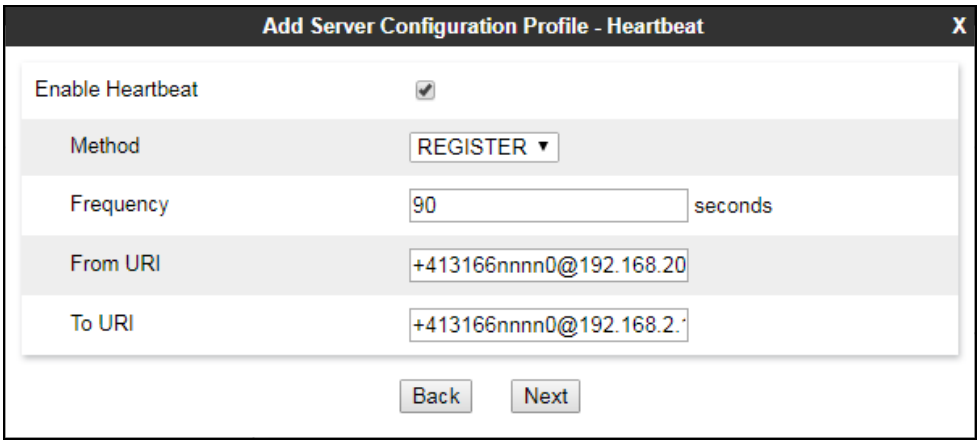


Click on **Next** and enter the SIP USER and SIP-Password provided by Swisscom into the dialogue box. The SIP USER is used for the **User Name** and the **Realm** is left blank.



Click on **Next** again and enter registration details in the dialogue box:

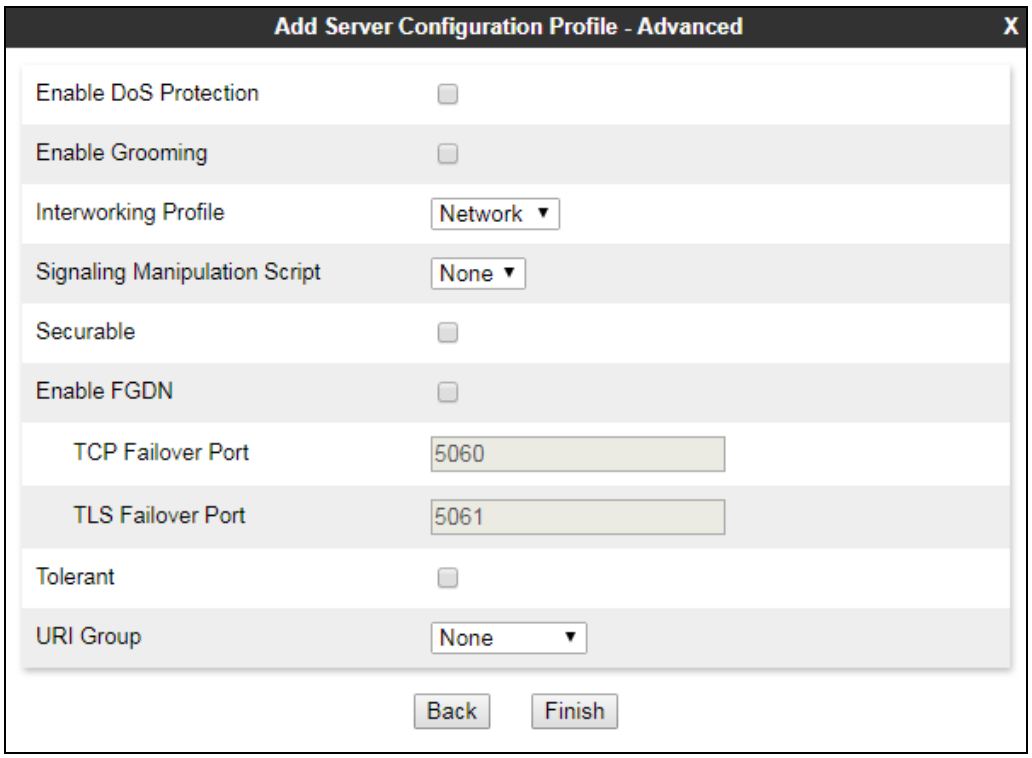
- Check the **Enable Heartbeat** box.
- Select **REGISTER** from the **Method** drop down menu.
- Enter the **Frequency** for registration, during testing **90** was used so that the Avaya SBCE registered with Swisscom Smart Business Connect every 90 seconds.
- Enter the **From URI** and **To URI** as the <User Name>@<IP Address> where the User Name is the SIP ID provided by Swisscom and the IP Address is the external interface of the Avaya SBCE and the Swisscom SBC respectively.
- Click on **Next**



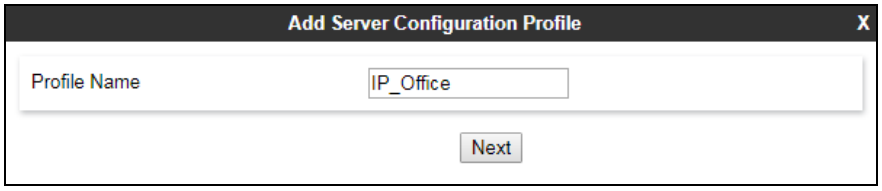
Click on **Next** again to get to the final dialogue box.

The final dialogue box contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the profile for Swisscom Smart Business Connect defined in **Section 6.5**.
- Leave the other fields at default settings.
- Click on **Finish**.

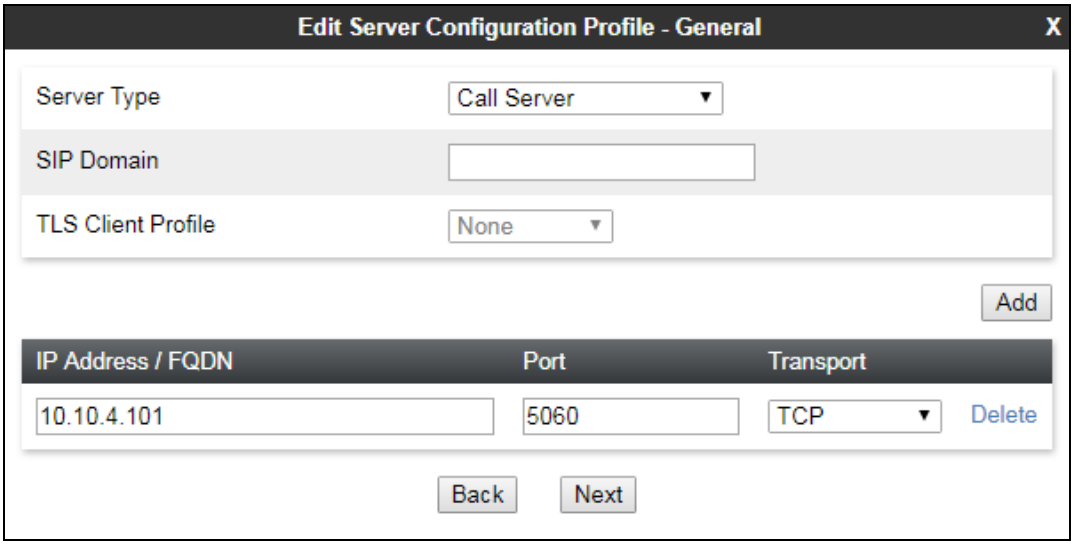


Use the previous process to define the Call Server configuration for IP Office if not already defined. Navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** (not shown). Enter an appropriate name in the dialogue box displayed.



Click on **Next** and enter configuration settings in the dialogue box displayed:

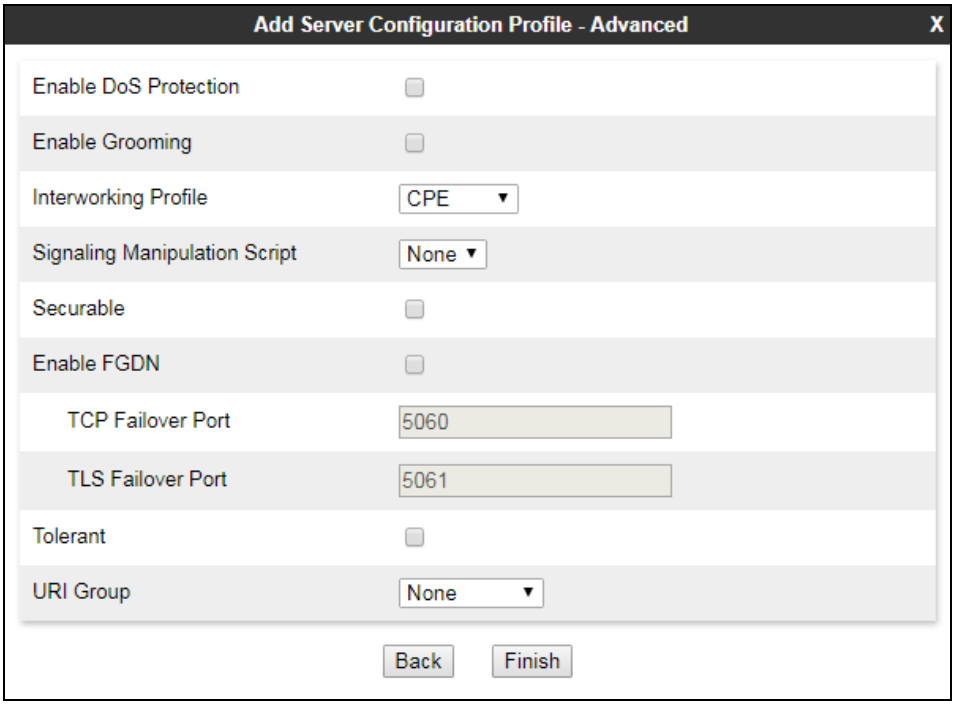
- In the **Server Type** drop down menu, select **Call Server**.
- If using TLS, select the **TLS Client Profile** created in **Section 6.3.2**. in the drop down menu
- Click on **Add** to enter an IP address or FQDN.
- In the **IP Address / FQDN** box, type the IP address of the IP Office.
- In the **Port** box, enter the port to be used for IP Office. In the test environment, this was **5060** for TCP.
- In the **Transport** drop down menu, select the signalling transport to be used. In the test environment, this was **TCP**.



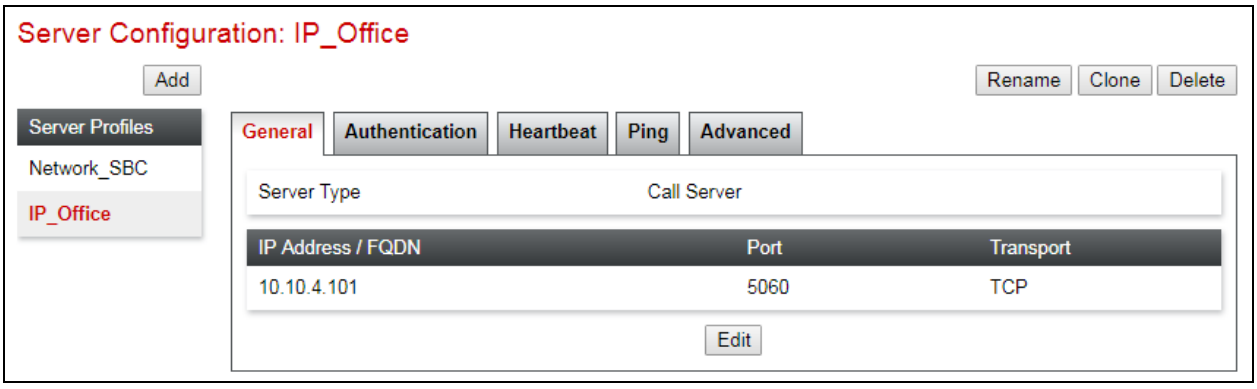
Click on **Next** again to get to the final dialogue box.

The final dialogue box contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the profile for IP Office defined in **Section 6.5**.
- Leave the other fields at default settings.
- Click on **Finish**.



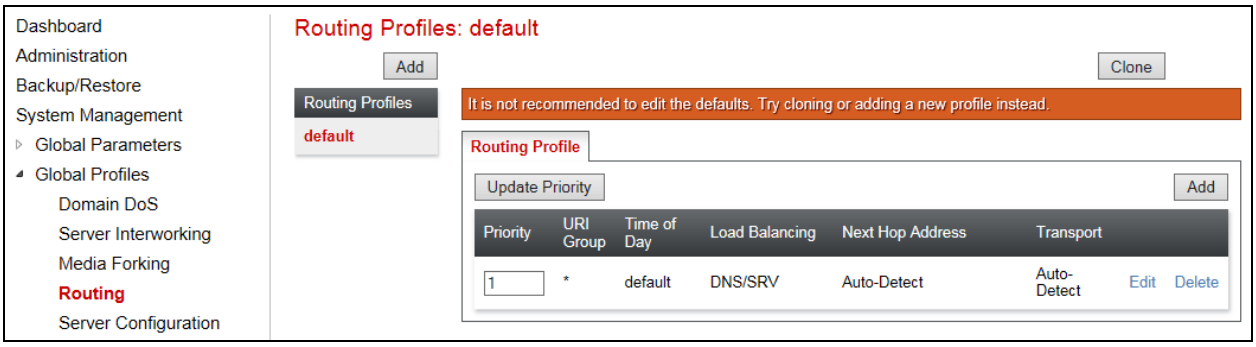
The following screenshot shows the **General** tab of the completed Server Configuration for IP Office:



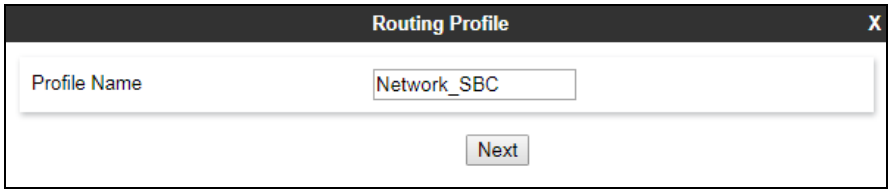
6.7. Define Routing

Routing information is required for routing to the Swisscom Smart Business Connect network SBC on the external side and IP Office on the internal side. The IP addresses and ports defined here will be used as the destination addresses for signalling.

To define routing to the Swisscom network SBC, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add.**

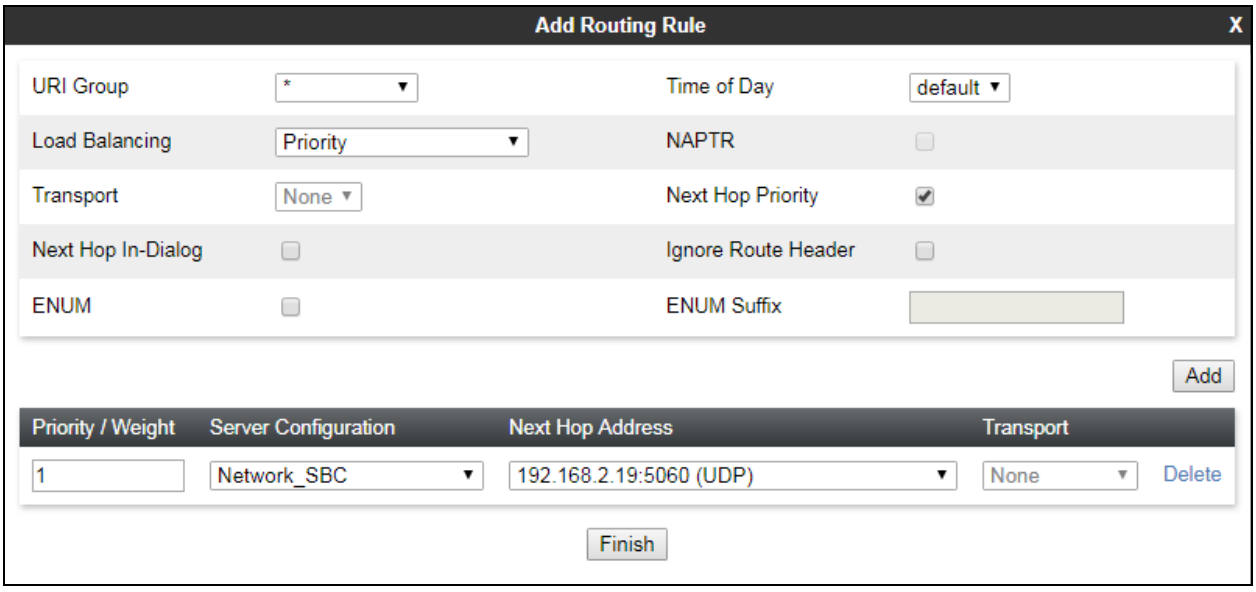


Enter an appropriate name in the dialogue box.

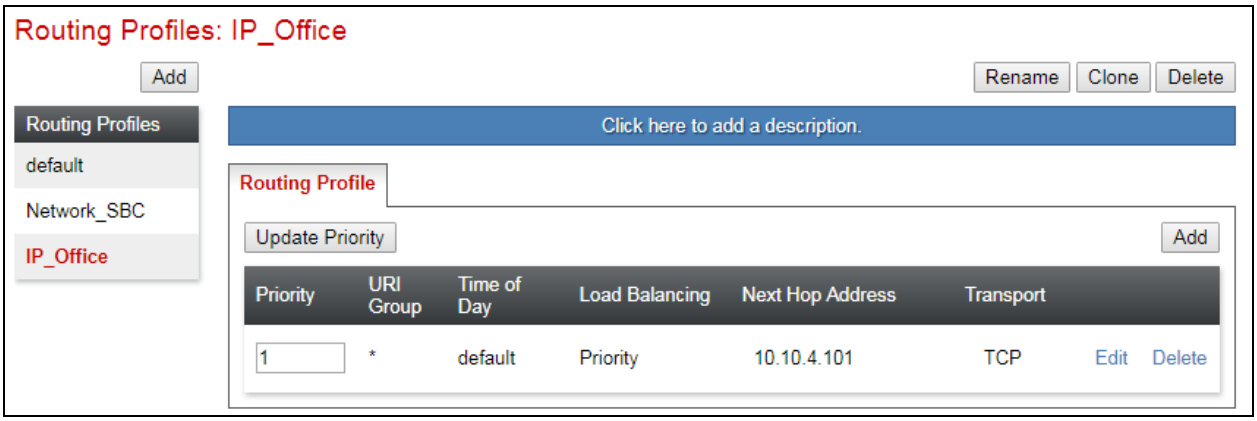


Click on **Next** and enter details for the Routing Profile for the SIP Trunk:

- Leave the **Load Balancing** drop down menu at default of **Priority**.
- Click on **Add** to specify the next hop address for the SIP Trunk.
- Assign priority in the **Priority / Weight** field. In the test environment, **1** was used.
- Select the Server Configuration defined in **Section 6.6** in the **Server Configuration** drop down menu, the **Next Hop Address** field will be automatically populated.
- Click on **Finish**.



Repeat the process for the Routing Profile for IP Office: The following screenshot shows the completed profile:

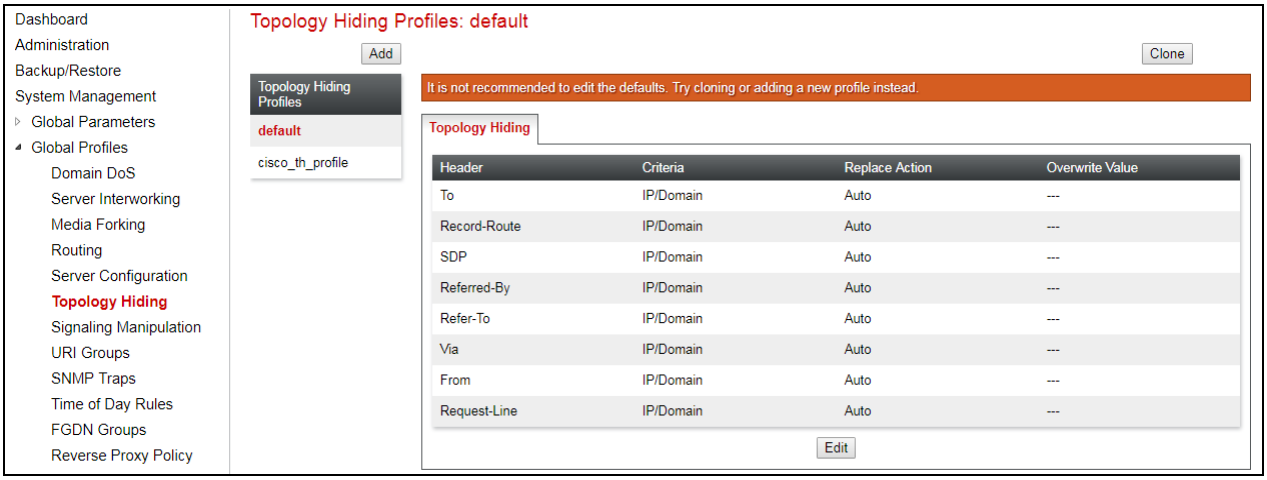


Note: The Name is **IP_Office** and the **Next Hop Address** is **10.10.4.101** in this configuration.

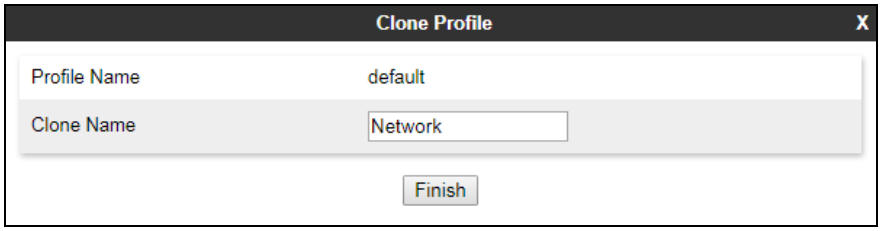
6.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop for terminating addresses or Avaya SBCE interfaces for originating addresses.

To define Topology Hiding for Swisscom Smart Business Connect, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side. Highlight the default profile and click on **Clone**.

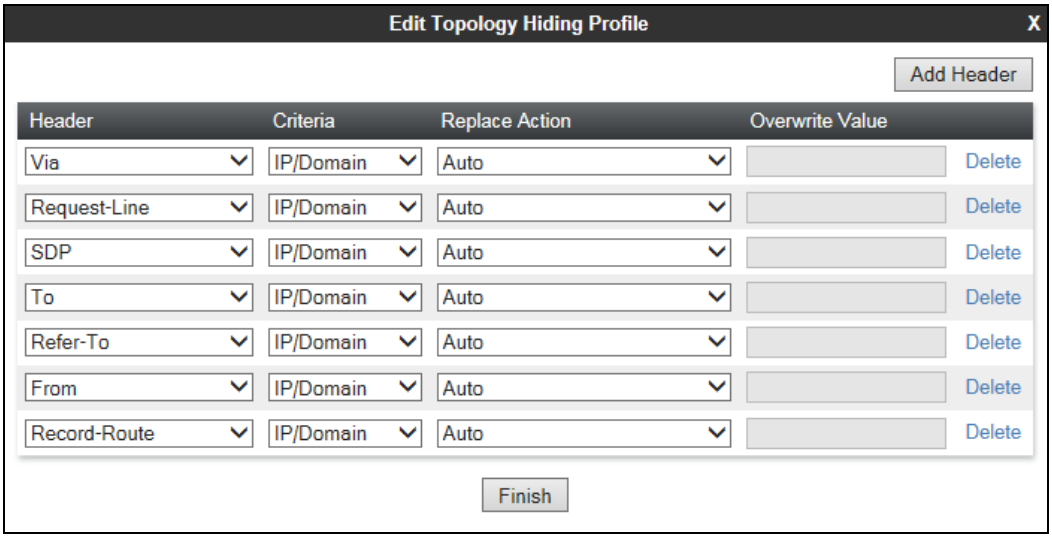


Enter a suitable name in the **Clone Profile** dialogue box:

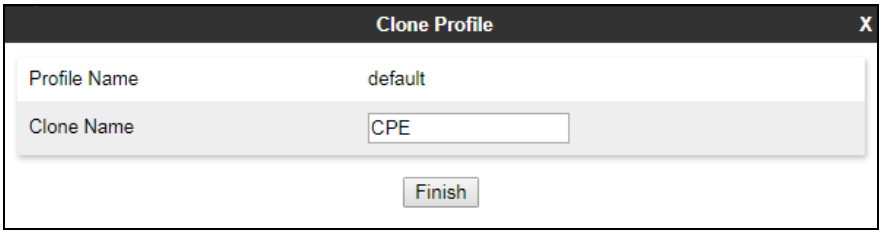


Edit the clone and enter details in the **Topology Hiding Profile** pop-up menu if required.

- Click on **Add Header** and **s**elect from the **Header** drop down menu.
- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required in which case select **Overwrite** and enter the domain in the **Overwrite Value** field. Click on **Finish**.



To define Topology hiding for IP Office, follow the same process. Navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side, highlight the default profile and click on **Clone** (not shown). Enter a suitable name in the **Clone Profile** dialogue box:



Edit the clone and enter details in the **Topology Hiding Profile** pop-up menu (not shown) if required. Note that during testing, the Topology Hiding for both Swisscom Smart Business Connect and IP Office was left at default values.

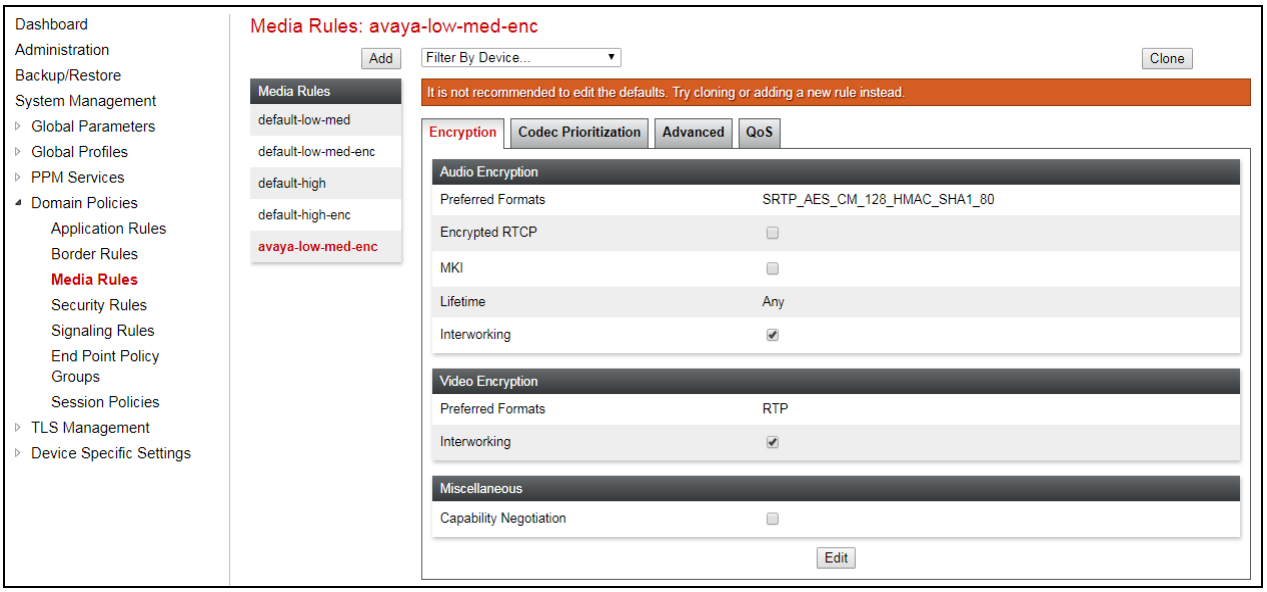
6.9. Domain Policies

Domain policies are used to bring together a number of different rules for use in a server flow described in **Section 6.10**. Swisscom Smart Business Connect testing was carried out without security on the signalling and media between the Avaya SBCE and the IP Office because of an issue with RTP / SRTP conversion described in **Section 2.2**. The process of media encryption is carried out on the media by using a specific Media Rule and is described here for information.

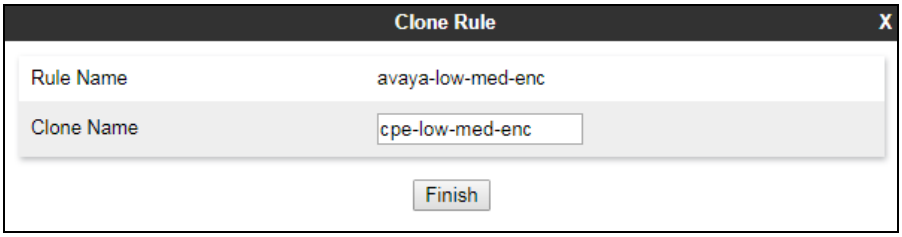
6.9.1. Media Rules

Media rules can be used to manipulate media in a number of ways including encryption. Although there are default media rules for encryption, a bespoke one is described here that allows fallback to unencrypted media.

To define the media rule, navigate to **Domain Policies →Signaling Rules** in the main menu on the left hand side. Highlight the default **avaya-low-med-enc** media rule for encrypted media and click on **Clone**.



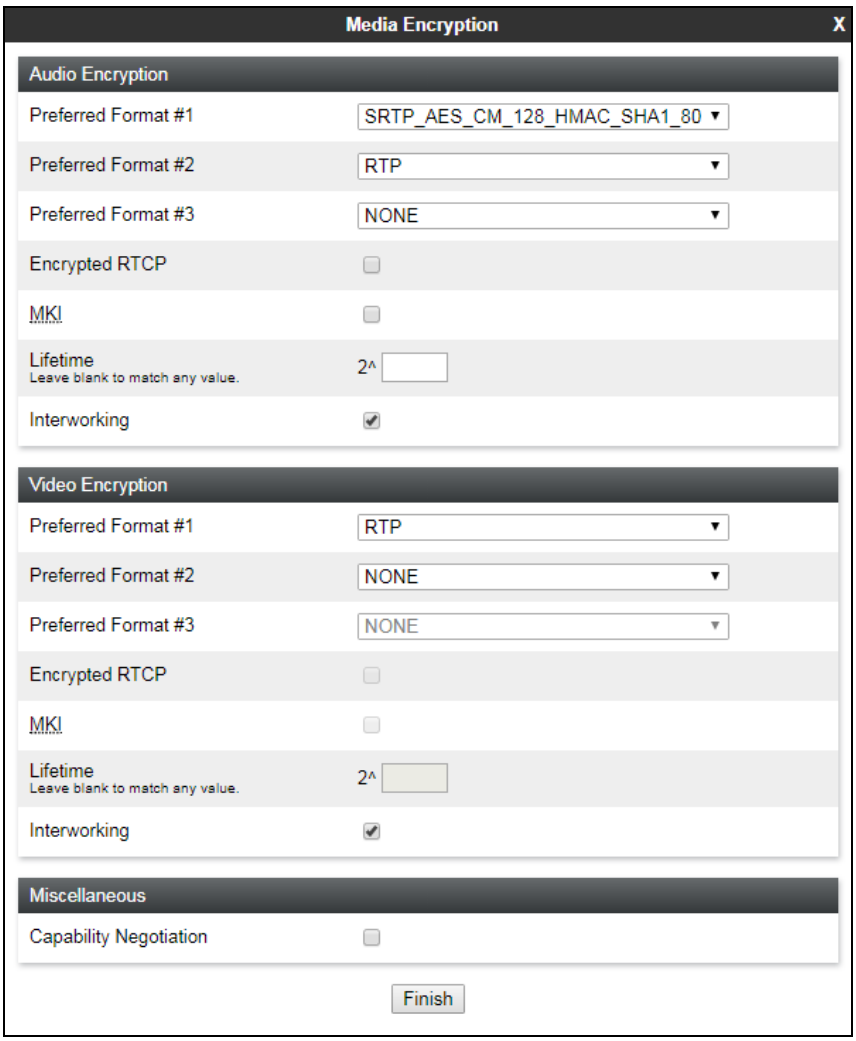
Enter a **Rule Name** in the **Clone Rule** dialogue box and click on **Finish**.



The only change applied in this example is to add unencrypted media as a second choice.

To add unencrypted media as a second choice, highlight the recently created Media Rule click on the **Encryption** tab and click on **Edit** (not shown).

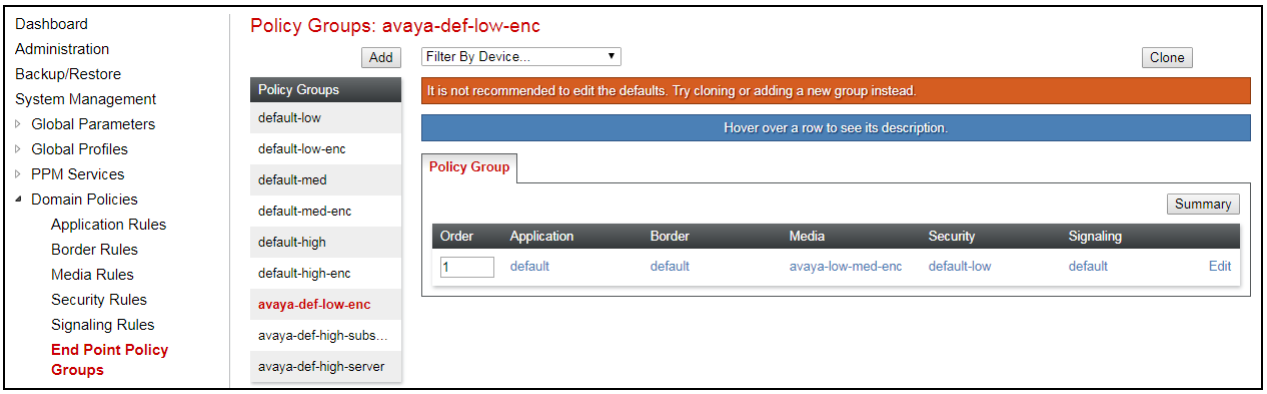
- Select the required encryption in the **Preferred Format #1** drop down menu. The example shows **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Select the **RTP** in the **Preferred Format #2** drop down menu.
- Other fields can be left at default values.
- Click on **Finish**.



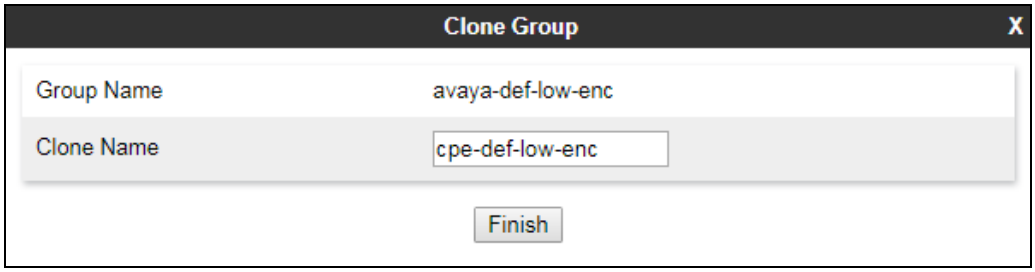
6.9.2. End Point Policy Group

An End Point Policy Group is required to implement the media rule. To define one for use in the IP Office server flow, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side.

Select an appropriate pre-defined Policy Group for encryption, in the test environment this was **avaya-default-low-enc**, and click on **Clone**.

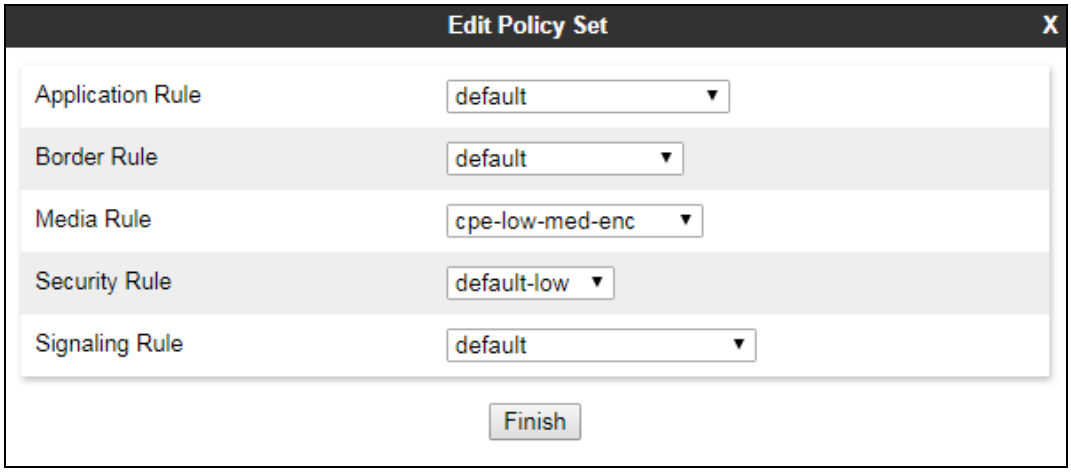


Enter an appropriate name in the pop-up box.

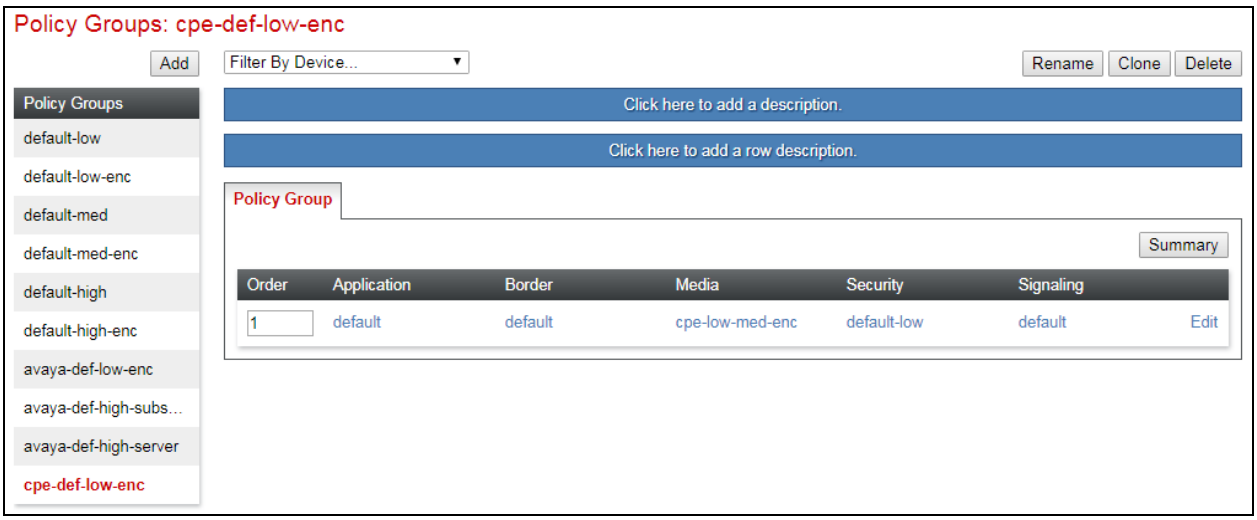


Highlight the resulting Policy Group and click on **Edit** (not shown). Enter details as follows:

- Leave the **Application Rule**, **Border Rule**, **Security Rule** and **Signaling Rule** at their default values.
- Select the **Media Rule** created in the **Section 6.9.1** in the drop down menu.
- Click on **Finish**.

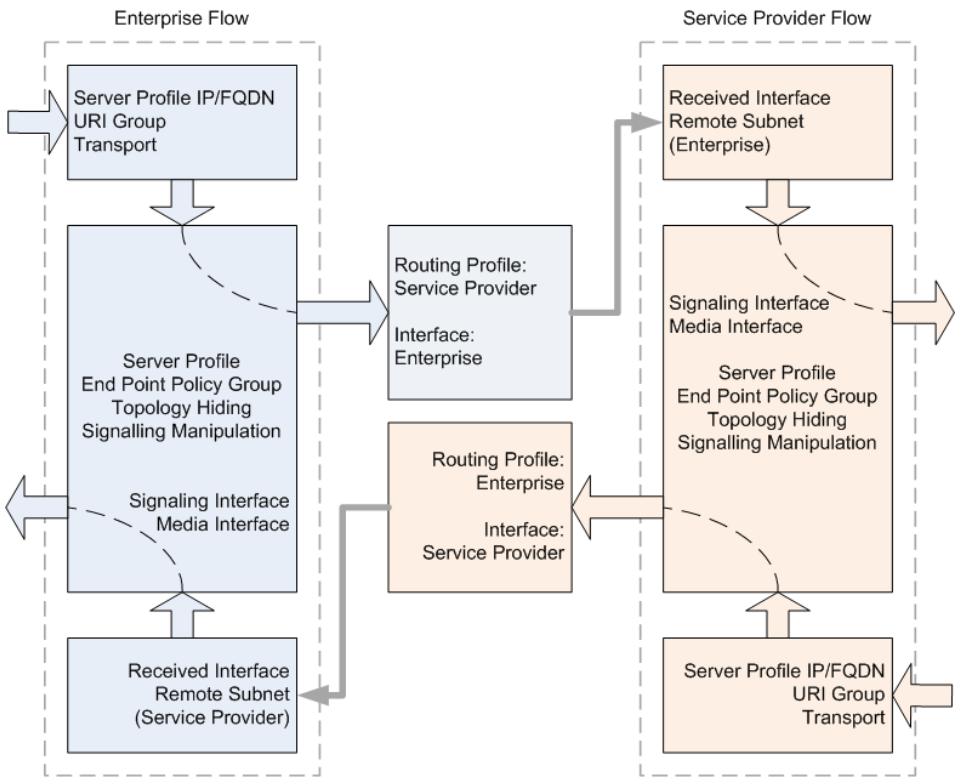


The completed Policy Group is shown in the following screenshot:



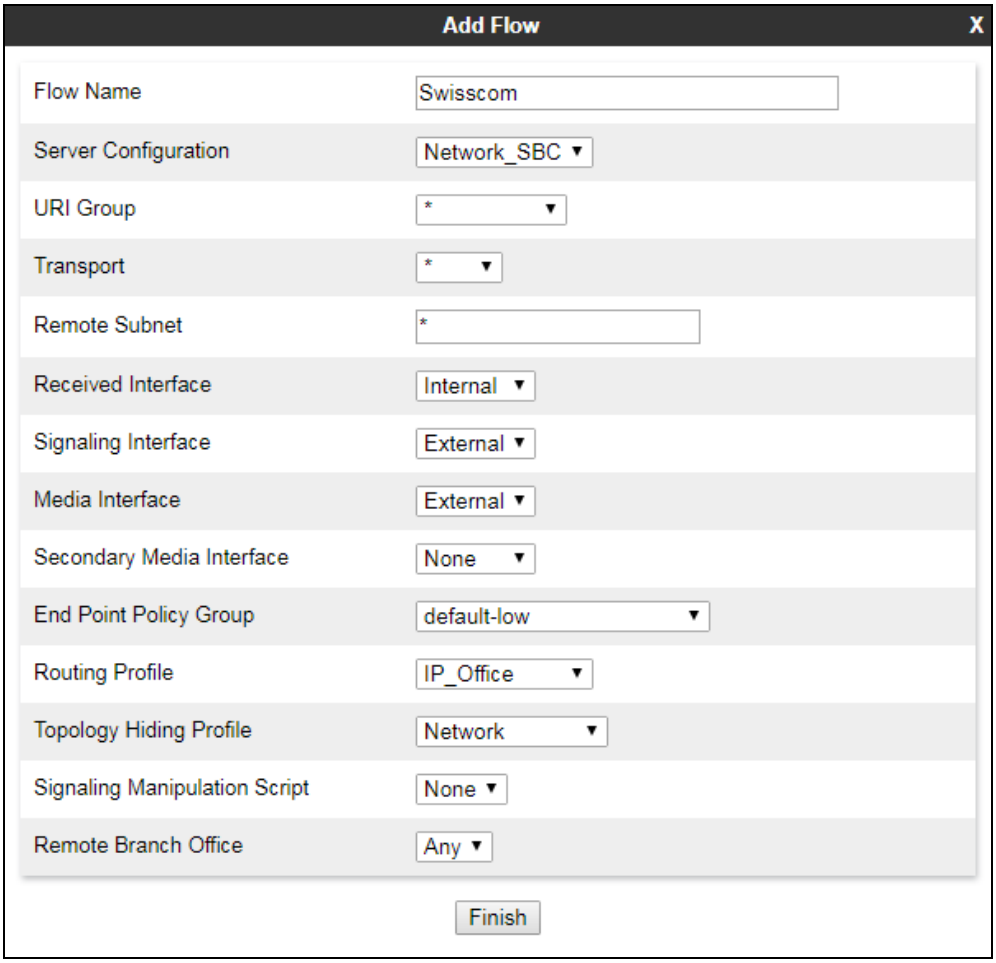
6.10. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for Swisscom Smart Business Connect and the other for IP Office. These End Point Server Flows allow calls to be routed from IP Office to Swisscom and vice versa. The following diagram, gives an overview of the Server Flows for the Enterprise (IP Office) and the Service Provider (Swisscom Smart Business Connect):



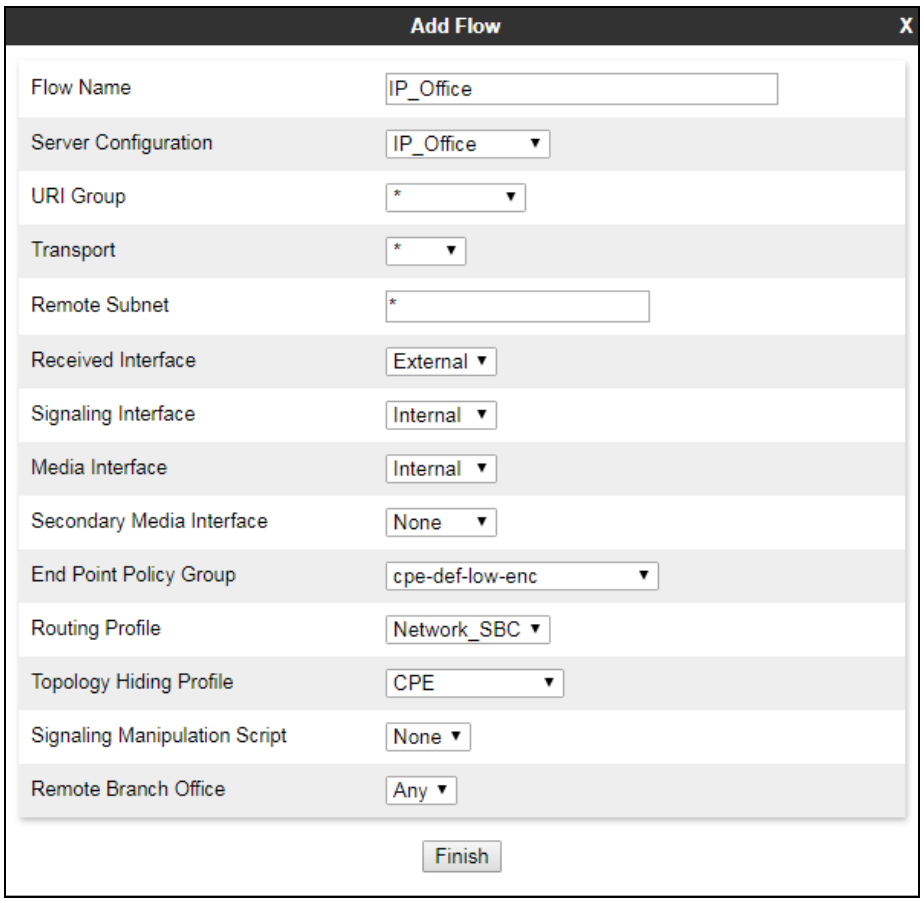
To define a Server Flow for Swisscom Smart Business Connect, navigate to **Device Specific Settings → End Point Flows**. Click on the **Server Flows** tab and click on **Add** (not shown).

- In the **Flow Name** field enter a descriptive name for the server flow for Swisscom Smart Business Connect, in the test environment **Swisscom** was used.
- In the **Server Configuration** field drop-down menu, select the server profile for the Swisscom network SBC defined in **Section 6.6**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**. This is the interface that signalling bound for Swisscom is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 6.4.1**. This is the interface that signalling bound for Swisscom is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 6.4.2**. This is the interface that media bound for Swisscom is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of IP Office defined in **Section 6.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile for Swisscom defined in **Section 6.8** and click on **Finish**.

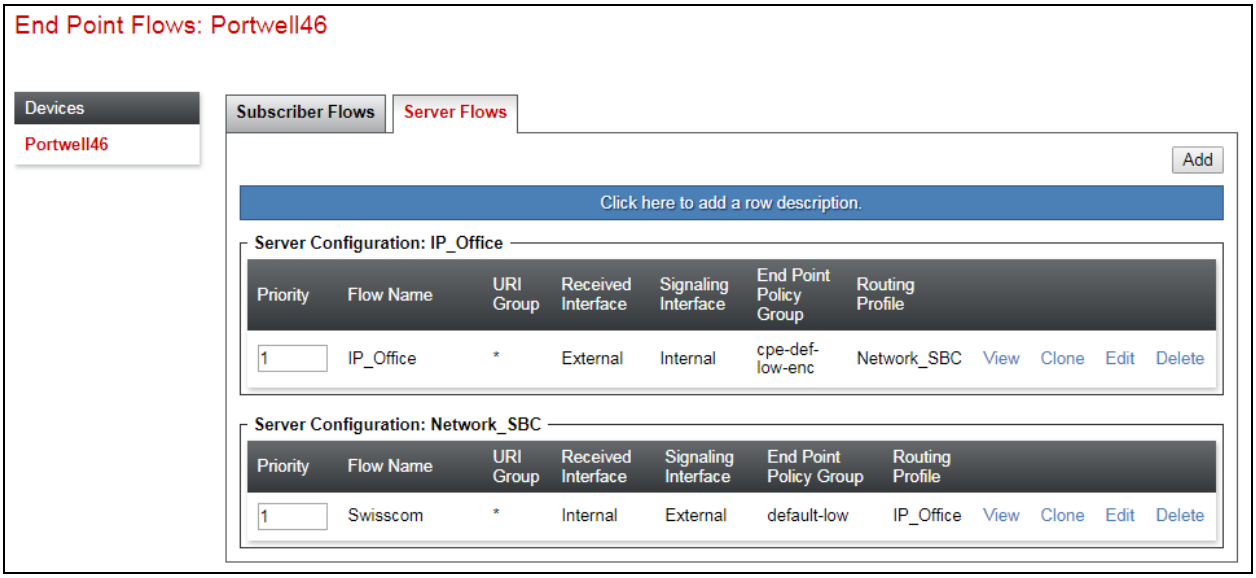


To define a Server Flow for IP Office, navigate to **Device Specific Settings → End Point Flows**. Click on the **Server Flows** tab and click on **Add** (not shown).

- In the **Flow Name** field enter a descriptive name for the server flow for IP Office, in the test environment **IP_Office** was used.
- In the **Server Configuration** field drop-down menu, select the server profile for IP Office defined in **Section 6.6**.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 6.4.1**. This is the interface that signalling bound for IP Office is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**. This is the interface that signalling bound for IP Office is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 6.4.2**. This is the interface that media bound for IP Office is sent on.
- If secure media is used within the enterprise, select the **End Point Policy Group** defined in **Section 6.9** in the drop-down menu. Alternatively, select **default-low**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Swisscom network SBC defined in **Section 6.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of IP Office defined in **Section 6.8**.



Click on **Finish**. The following screenshot shows the completed configuration:



7. Configure the Swisscom Equipment

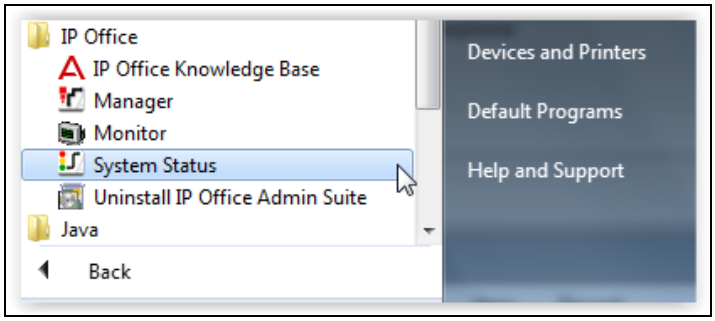
The configuration of the Swisscom Smart Business Connect equipment used to support the SIP Trunk is outside the scope of these Application Notes and will not be covered. To obtain further information on Swisscom equipment and system configuration please contact an authorized Swisscom representative.

8. Verification Steps

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

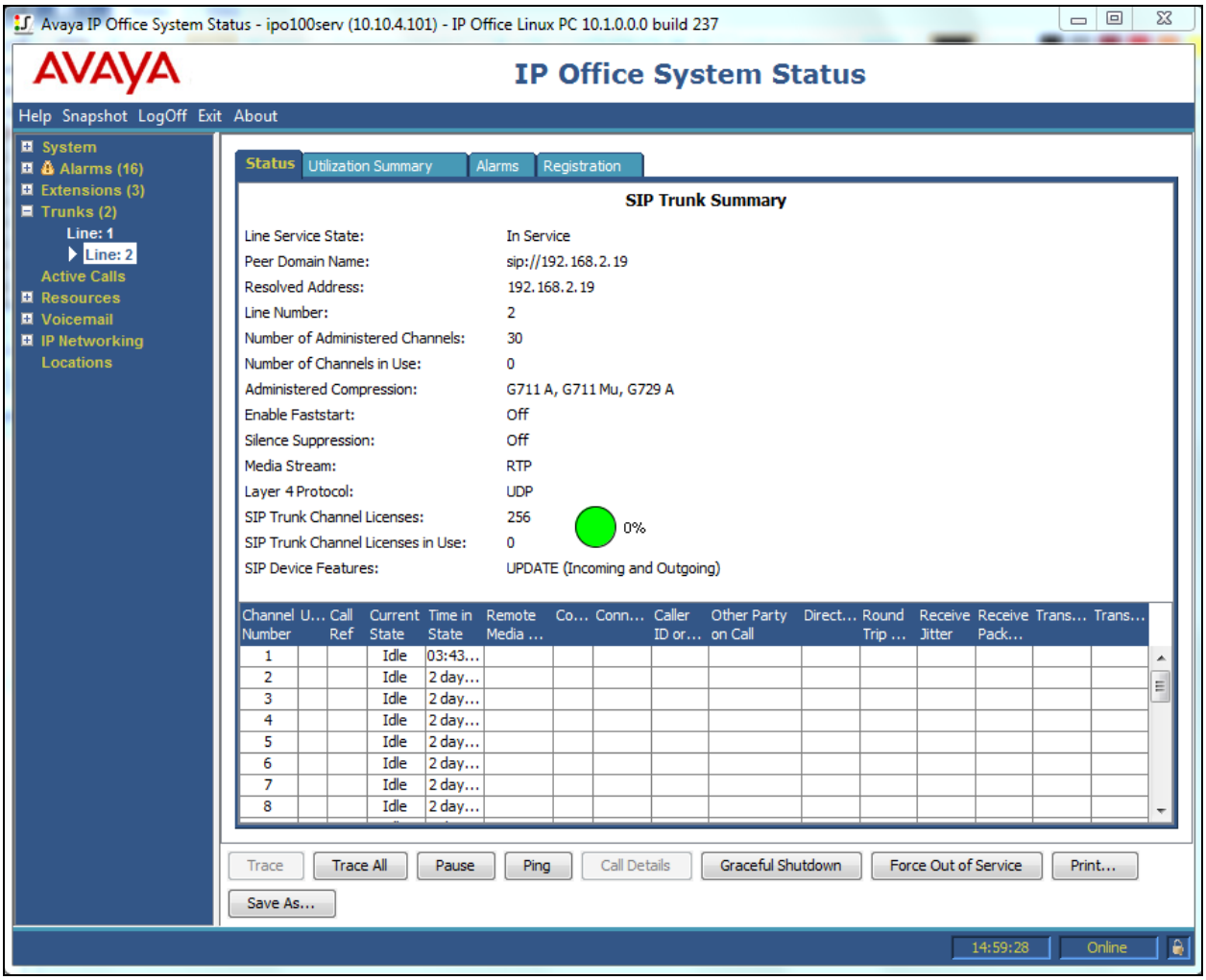
8.1. SIP Trunk status

The status of the SIP trunk can be verified by opening the System Status application. 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.

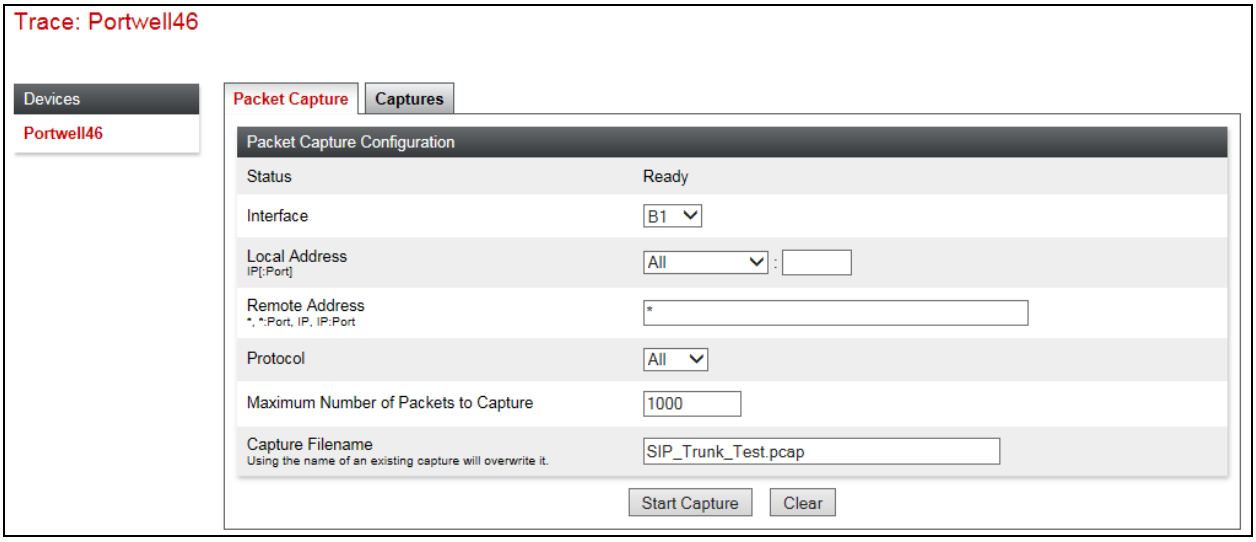
From the left hand menu expand **Trunks** and choose the SIP trunk (**2** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational.



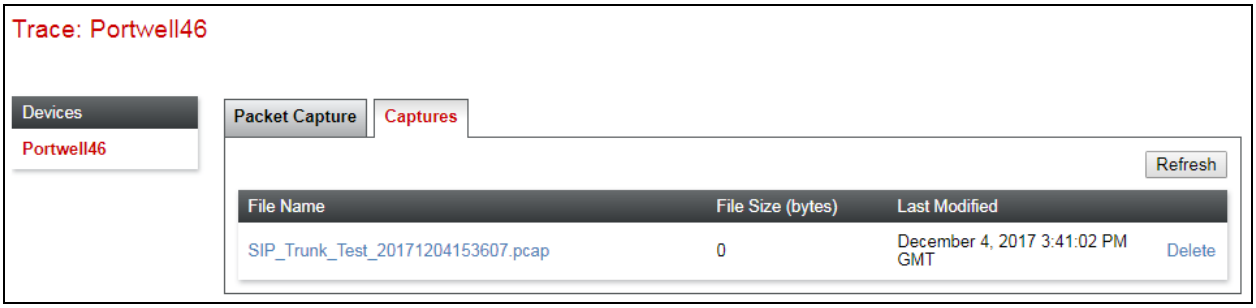
Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from IP Office via the Avaya SBCE to the Swisscom Smart Business Connect network are receiving a response.

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

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



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



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

9. Conclusion

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

10. Additional References

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

[1] *Avaya IP Office™ Platform Start Here First*, Release 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] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.2, Sept 2017
[15] *Upgrading Avaya Session Border Controller for Enterprise*, Release 7.2, Aug 2017
[16] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2, Sept 2017
[17] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/

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.