Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 8.1 with Avaya Session Border Controller for Enterprise Release 6.2 to support Telenor SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya IP Office R8.1 and the Avaya Session Border Controller for Enterprise 6.2 to support Telenor SIP Trunk Service.

The Telenor SIP Trunk Service provides PSTN access via a SIP trunk connected to the Telenor Voice Over Internet Protocol (VoIP) network as an alternative to legacy Analogue or Digital trunks. Telenor are a member of the Avaya DevConnect Service Provider program.

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 Telenor SIP Trunk Service and Avaya IP Office. In the sample configuration, the Avaya IP Office solution consists of an Avaya Session Border Controller for Enterprise Release 6.2, and Avaya IP Office 500 v2 Release 8.1 Essential Edition, Avaya Voicemail Pro, Avaya IP Office Softphone, and Avaya H.323, SIP, digital, and analog endpoints.

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

The Avaya Session Border Controller for Enterprise (SBCE) is the point of connection between Avaya IP Office and Telenor SIP Trunk Service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

Telenor SIP Trunk Service provides PSTN access via a SIP trunk connected to the Telenor network as an alternative to legacy Analogue or Digital trunks. This approach generally results in lower cost for customers.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office and Avaya SBCE to connect to the Telenor SIP Trunk Service. 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.

2.1. Interoperability Compliance Testing

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

- Incoming PSTN calls to various phone types including H.323, SIP, Digital and Analogue telephones at the enterprise
- All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider
- Outgoing PSTN calls from various phone types including H.323, SIP, Digital, and Analogue telephones at the enterprise

- All outbound PSTN calls were routed from the enterprise across the SIP trunk to the Service Provider
- Inbound and outbound PSTN calls to/from an IP Office Softphone client
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance
- Codecs G.711A and G.711MU
- 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 twinning
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 transport mode

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Telenor SIP Trunk Service with the following observations:

- No inbound toll free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- No emergency calls to the operator were tested.
- Inbound and Outbound fax was tested using T.38 standard.

2.3. Support

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

For technical support on Telenor products please contact the following website: http://www.telenor.com/

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to Telenor SIP Trunk Service. Located at the enterprise site is an Avaya IP Office 500v2 with Avaya SBCE. Endpoints include two Avaya 1600 Series IP Telephones (with H.323 firmware), one Avaya 1140e SIP Telephone, Avaya 2420 Digital Telephone, Avaya Analogue Telephone and fax machine. The site also has a Windows XP PC running Avaya IP Office Manager to configure the Avaya IP Office as well as an IP Office Softphone client for mobility testing. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes. Instead, public IP addresses have been changed to a private format and all phone numbers have been obscured beyond the city code.

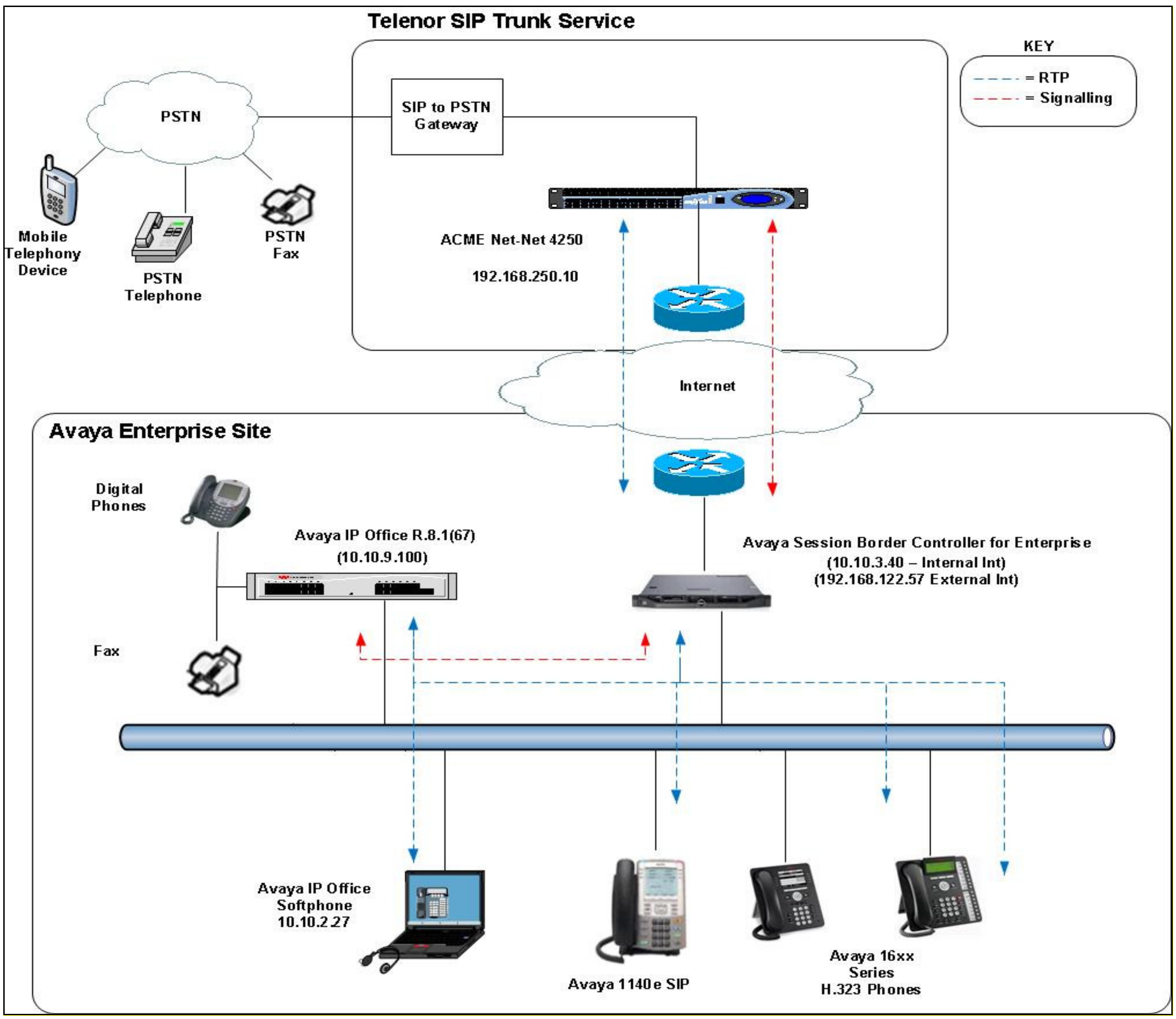


Figure 1: Test Setup Telenor SIP Trunk Service to Simulated Enterprise

Avaya IP Office was configured to connect to a static IP address at the Service Provider. For the purposes of the compliance test, users dialed a short code of 9N digits to send digits across the SIP trunk to the Telenor network. The short code of 9 is stripped off by Avaya IP Office and the remaining N digits sent.

4. Equipment and Software Validated

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

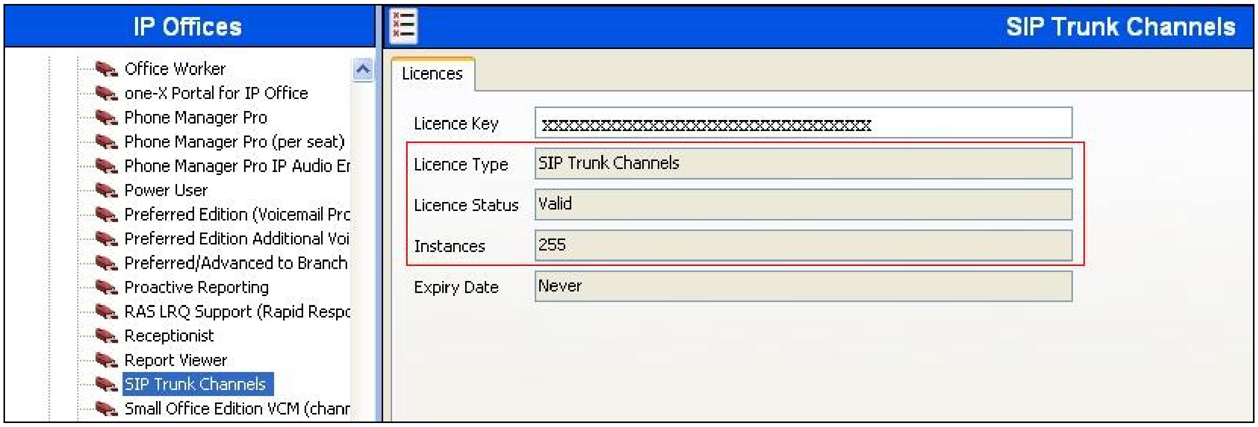
Equipment/Software	Release/Version
Avaya	
Avaya Session Border Controller for Enterprise	Release 6.2 (Q48)
Avaya IP Office 500 V2	Avaya IP Office R8.1(10.1.67)
Avaya 1603 Phone (H.323)	1.3100
Avaya 1608 Phone (H.323)	1.3100
Avaya SoftPhone (SIP)	3.056516
Avaya 1140e (SIP)	FW: 04.01.13.00.bin
Avaya 2420 Digital Phone	R6.0
Avaya 98390 Analogue Phone	N/A
Telenor	
ACME Net-Net 4250	Firmware SC6.2.0 Patch 3
Lucent Session Manager	14.28.00.18
Telenor IPT	Version 3.1.3.132

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to Telenor SIP Trunk Service. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials. A management window will appear similar to the one in the next section. All the Avaya IP Office configurable components are shown in the left pane known as the Navigation Pane. The pane on the right is the Details Pane. These panes will be referenced throughout the Avaya IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the Service Provider (such as twinning) is assumed to already be in place.

5.1. Verify System Capacity

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



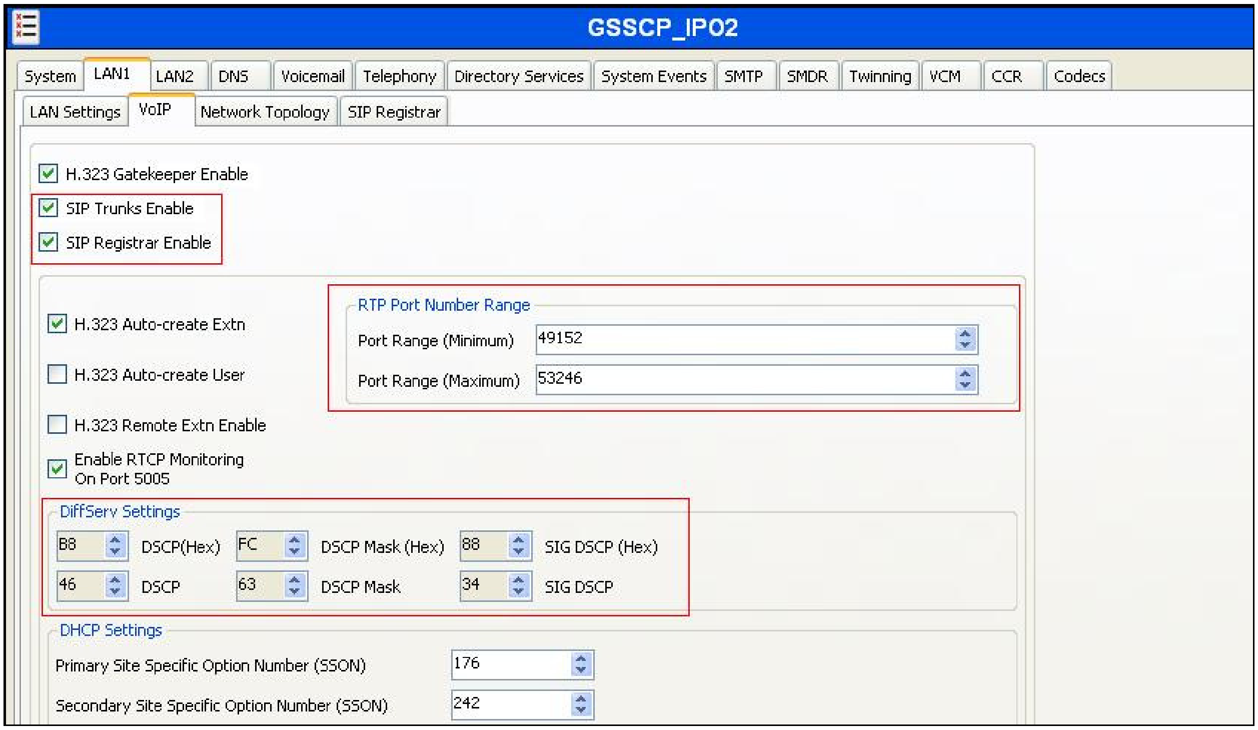
5.2. LAN Settings

The IP500/IP500 V2 control units have 2 RJ45 Ethernet ports, physically marked as LAN and WAN. Within the system configuration, the physical LAN port is LAN1, the physical WAN port is LAN2.

In the sample configuration, the LAN1 port was used to connect the Avaya IP Office to the enterprise network. To access the LAN1 settings, first navigate to **System → GSSCP_IPO2** in the Navigation Pane where GSSCP_IPO2 is the name of the IP Office. Navigate to the **LAN1 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the management interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the OK button (not shown).

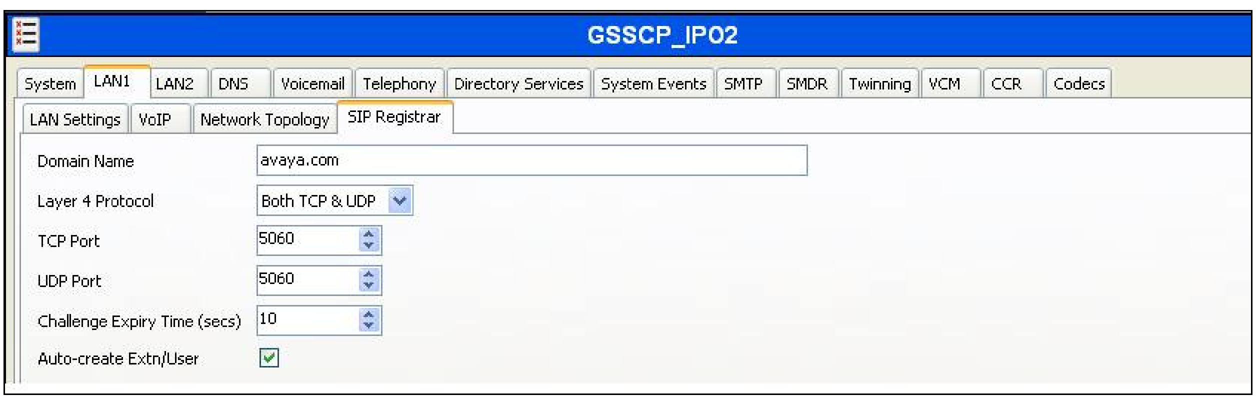
On the **VoIP** tab in the Details Pane, check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. The IP Office Softphone uses SIP. If Softphone along with any other SIP endpoint is to be used, the **SIP Registrar Enable** box must also be checked. The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Based on this setting, Avaya IP Office would request RTP media be sent to a UDP port in the configurable range for calls using LAN1.

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



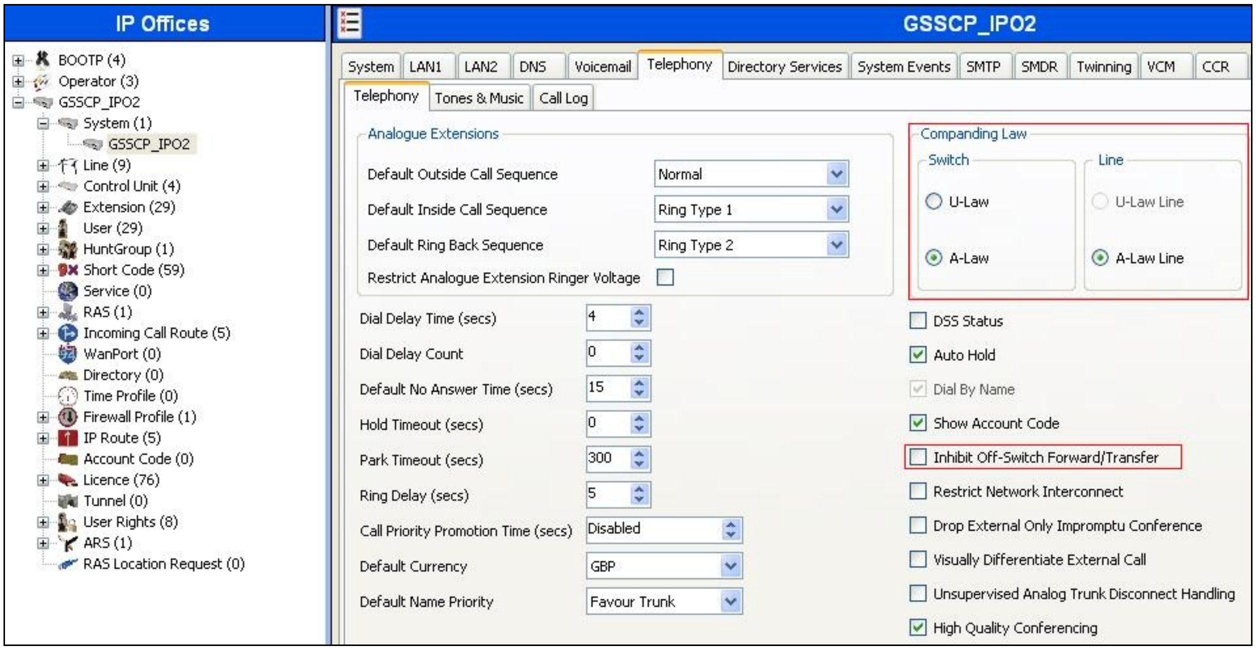
Select the **Network Topology** tab as shown in the following screen. In the sample configuration, the default settings were used and the **Use Network Topology Info** in the **SIP Line** was set to "None" in **Section 5.6**. The **Binding Refresh Time (seconds)** can still be used to lower the SIP OPTIONS timing from the default of 300 seconds. During the testing, the Binding Refresh Time was varied (e.g., 30 seconds, 90 seconds to test SIP OPTIONS timing).

Optionally, select the **SIP Registrar** tab. The following screen shows the settings used in the sample configuration. The **Domain Name** has been set to the customer premises equipment domain "**avaya.com**". If the **Domain Name** is left at the default blank setting, SIP registrations may use the IP Office LAN 1 IP Address. All other parameters shown are default values.



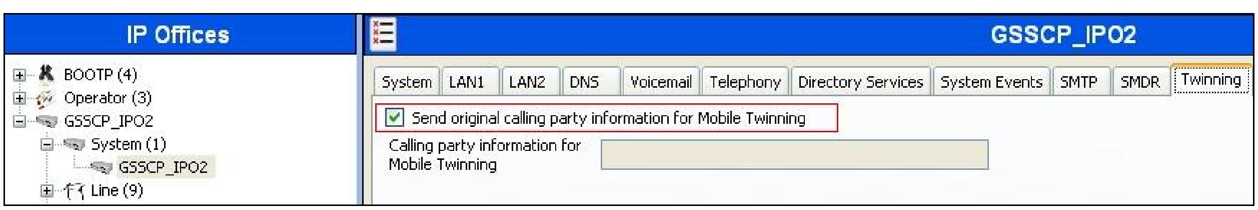
5.3. System Telephony Settings

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



5.4. System Twinning Settings

Navigate to the **Twinning** tab, check the box labeled **Send original calling party information for Mobile Twinning**. With this setting, Avaya IP Office will send the original calling party number to the twinned phone in the SIP From header (not the associated desk phone number) for calls that originate from an internal extension. On calls from the PSTN to a twinned phone, Avaya IP Office will send the calling party number of the host phone associated with the twinned destination (instead of the number of originating caller).This setting only affects twinning and does not impact the messaging of other redirected calls such as forwarded calls. If this box is checked, it will also override any setting of the **Send Caller ID** parameter on the SIP line (**Section 5.6**). On completion, click the **OK** button (not shown).



5.5. Codec Settings

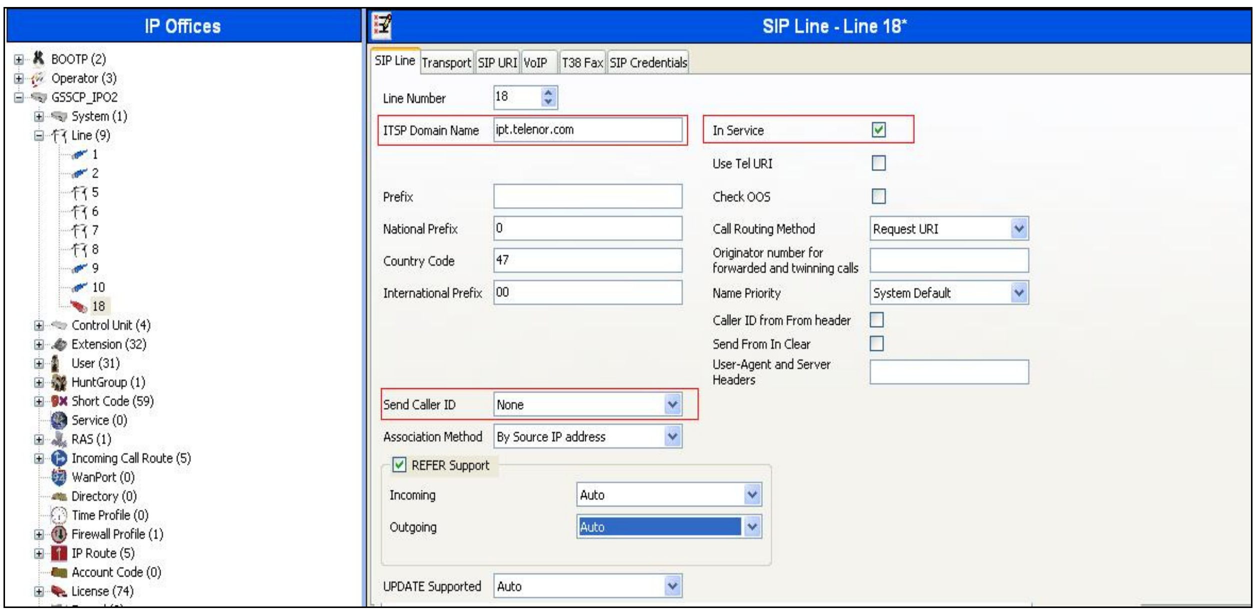
Navigate to the **Codecs** tab on the Details Pane. Check the Available Codecs boxes as required. Note that **G.711 ULAW 64K** and **G.711 ALAW 64K** are greyed out and always available. Once available codecs are selected, they can be used or unused by using the horizontal arrows as required. Note that in test, **G.711 ALAW 64K**, and **G.711 ULAW 64K** were used. The order of priority can be changed using the vertical arrows. On completion, click the **OK** button (not shown).

5.6. Administer SIP Line

A SIP Line is needed to establish the SIP connection between Avaya IP Office and the Telenor SIP Trunk Service. To create a SIP line, begin by navigating to **Line** in the Navigation Pane. Right-click and select **New→SIP Line** (not shown). On the **SIP Line** tab in the Details Pane, configure the parameters below to connect to the SIP Trunking service.

- Set the **ITSP Domain Name** to the domain name provided by Telenor SIP Trunk Service
- Set **Send Caller ID** to ***None***. This parameter determines how the calling party number is sent in the SIP messaging for twinning if the box labeled **Send original calling party information for Mobile Twinning** is unchecked in **Section 5.4**.This parameter was set to ***None*** and the box in **Section 5.4** was checked.
- Ensure the **In Service** box is checked
- Default values may be used for all other parameters

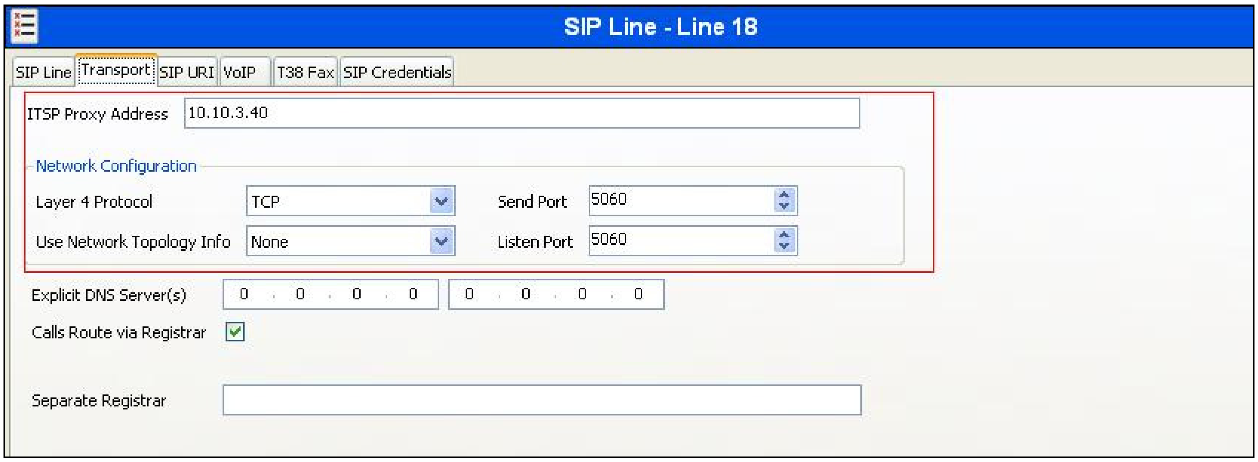
On completion, click the **OK** button (not shown).



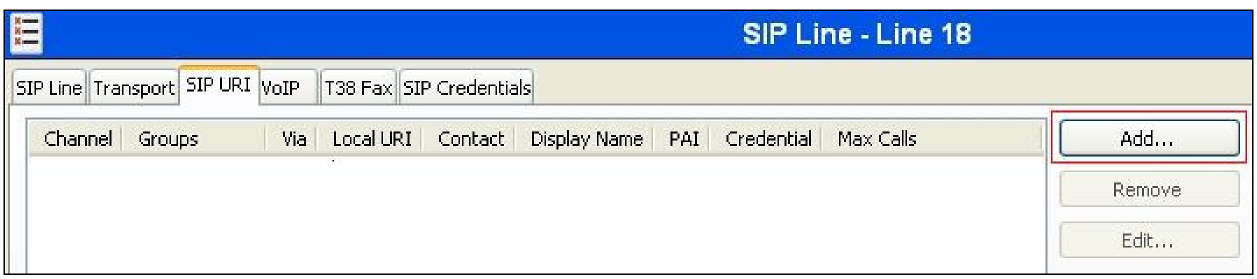
Select the **Transport** tab and set the following:

- Set **ITSP Proxy Address** to the inside IP address of the Avaya SBCE as shown in **Figure 1**
- Set **Layer 4 Protocol** to **TCP**
- Set **Send Port** to **5060** and **Listen Port** to **5060**
- Set **Use Network Topology Info** to **None**

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

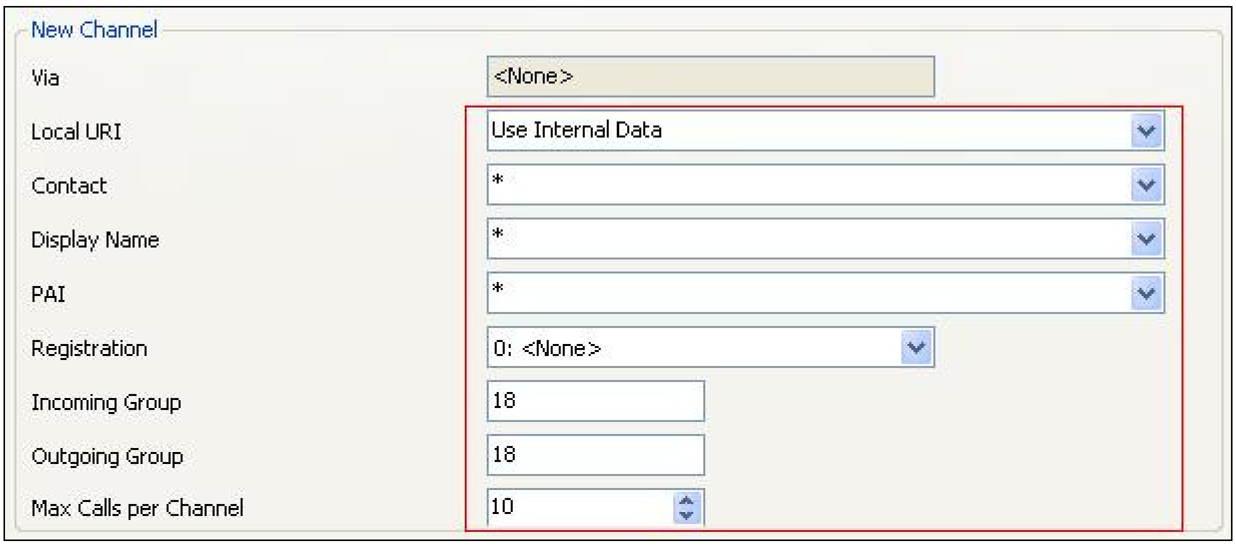


After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, first select the **SIP URI** tab. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane.



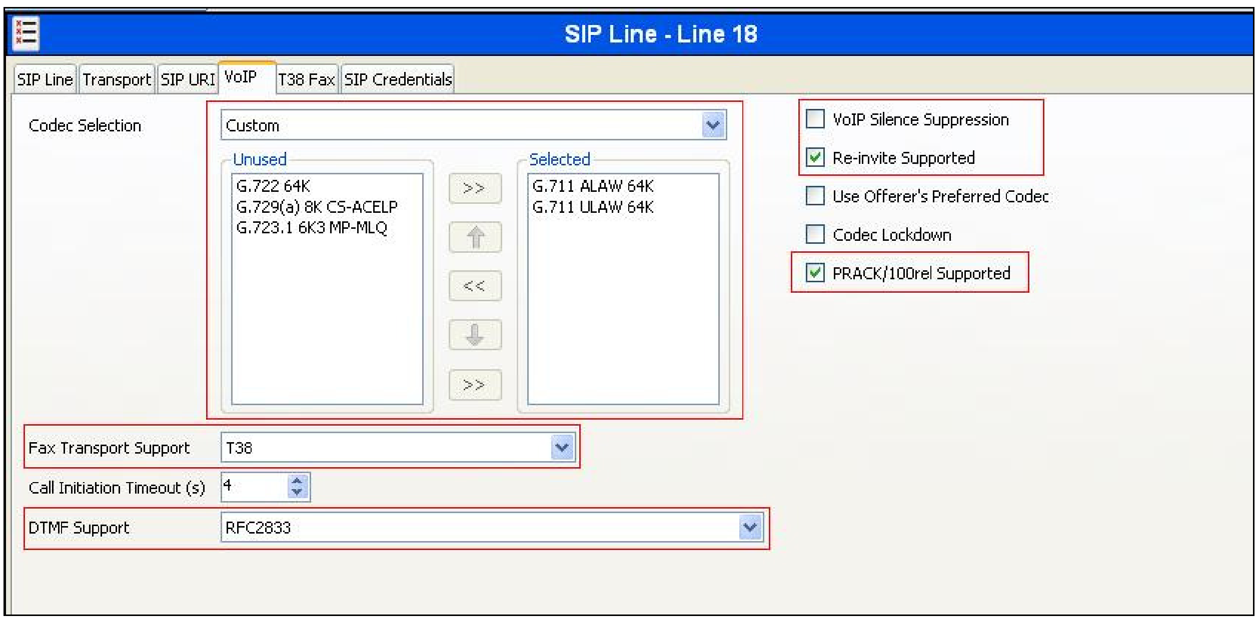
For the compliance test, a single SIP URI entry was created that matched any number assigned to an Avaya IP Office user. The entry was created with the parameters shown below.

- Set **Local URI** to **Use Internal Data**. This setting allows calls on this line whose SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.7**.
- Set **Contact**, **Display Name** and **PAI** to the wildcard *.
- For **Registration**, select **0: <None>** from the pull-down menu since this configuration does not use SIP registration.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **18** was defined that was associated to a single line (line 18).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

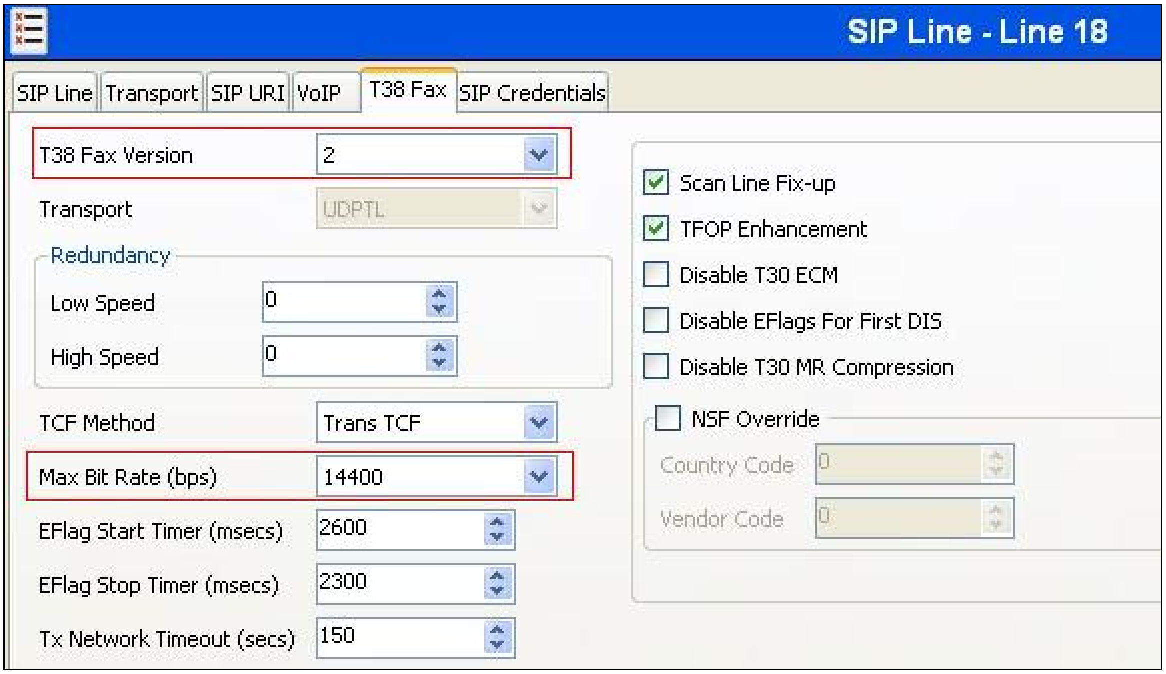


Select the **VoIP** tab, to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- Select **Custom** from the drop-down menu.
- Select **G.711 ALAW 64K,** and **G.711 ULAW 64K** codec.
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Uncheck the **VoIP Silence Suppression** box.
- Select the **Fax Transport Support** box to **T.38**.
- 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 on the trunk.
- Check **PRACK/100rel Supported** to advertise the support for provisional responses and Early Media to the Telenor network.
- Default values may be used for all other parameters.



Select the **T.38 Fax** tab, to set the T.38 parameters for the line. Un-check the Use Default Values box (not shown) and select **2** from the **T38 Fax Version** drop down menu. Set the **Max Bit Rate (bps)** to **14400**. All other field may retain their default values. On completion, click the **OK** button (not shown).



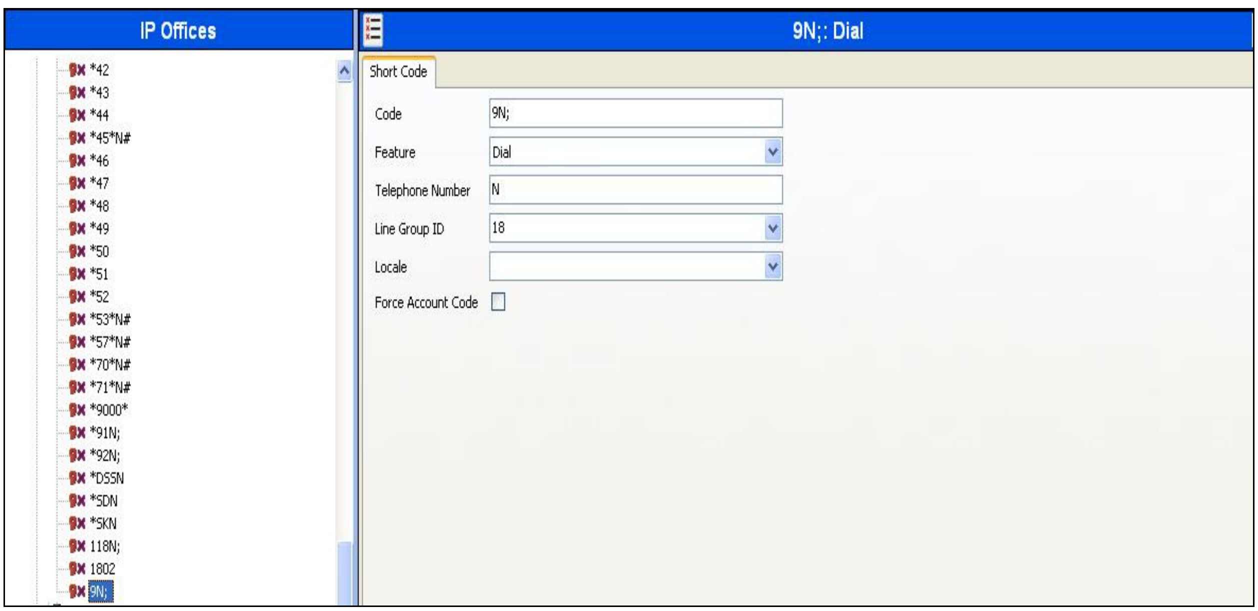
Note: It is advisable at this stage to save the configuration as described in **Section 5.11** to make the Line Group ID defined in **Section 5.6** available.

5.7. Short Codes

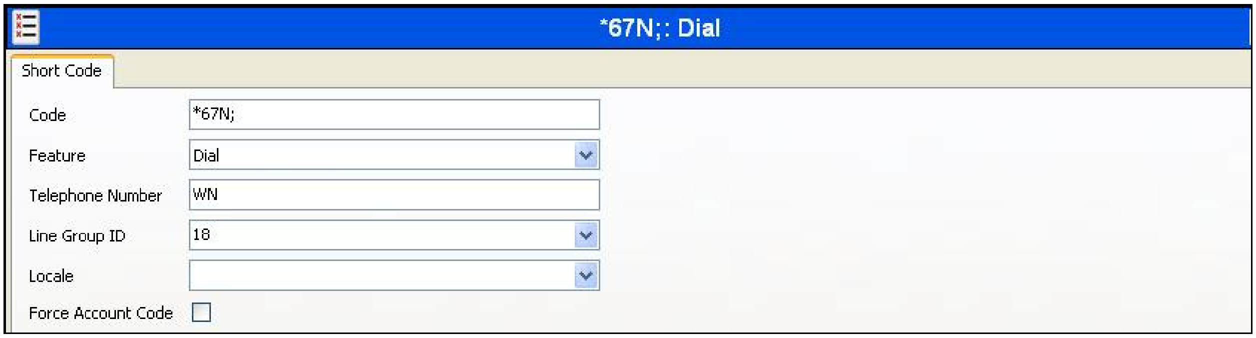
Define a short code to route outbound traffic to the SIP line. To create a short code, right-click **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as shown below.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon
- The example shows **9N**; which will be invoked when the user dials 9 followed by the dialed number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N** which will allow an IP Office user to dial the digit 9 followed by any telephone number, symbolized by the letter N. The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message.
- Set the **Line Group Id** to the outgoing line group number defined on the SIP URI tab on the SIP Line in **Section 5.6**

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



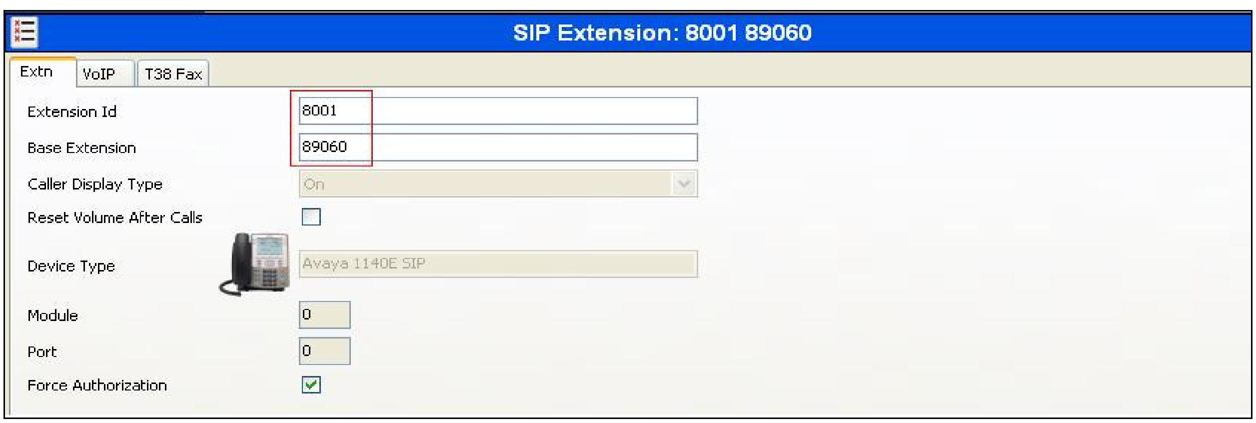
The screenshot below displays an example of a short code ***67N;** that can be used to withhold the sending of the calling ID number. **W** is a Telephone Number Field Character used to withhold outgoing CLI. The short code is similar to the shortcode **9N;** code used to route outbound traffic to the SIP line except that the Telephone Number field begins with **W** which will withhold the sending of the calling ID number. **Note:** This operation is service provider dependent.



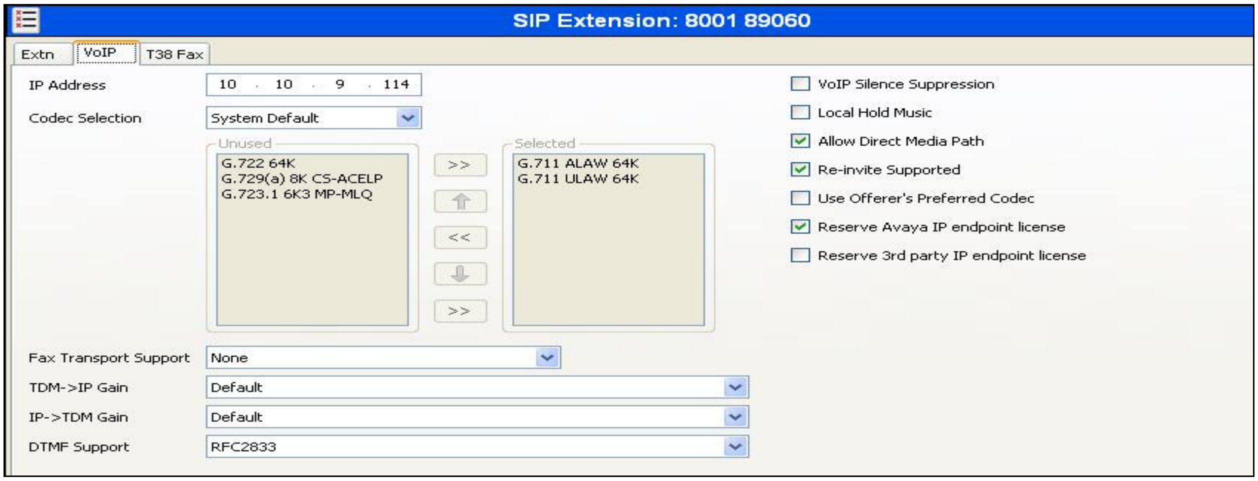
5.8. Users and Extensions

In this section, examples of IP Office Users, Extensions, and Hunt Groups will be illustrated. In the interests of brevity, not all users and extensions shown in **Figure 1** will be presented, since the configuration can be easily extrapolated to other users.

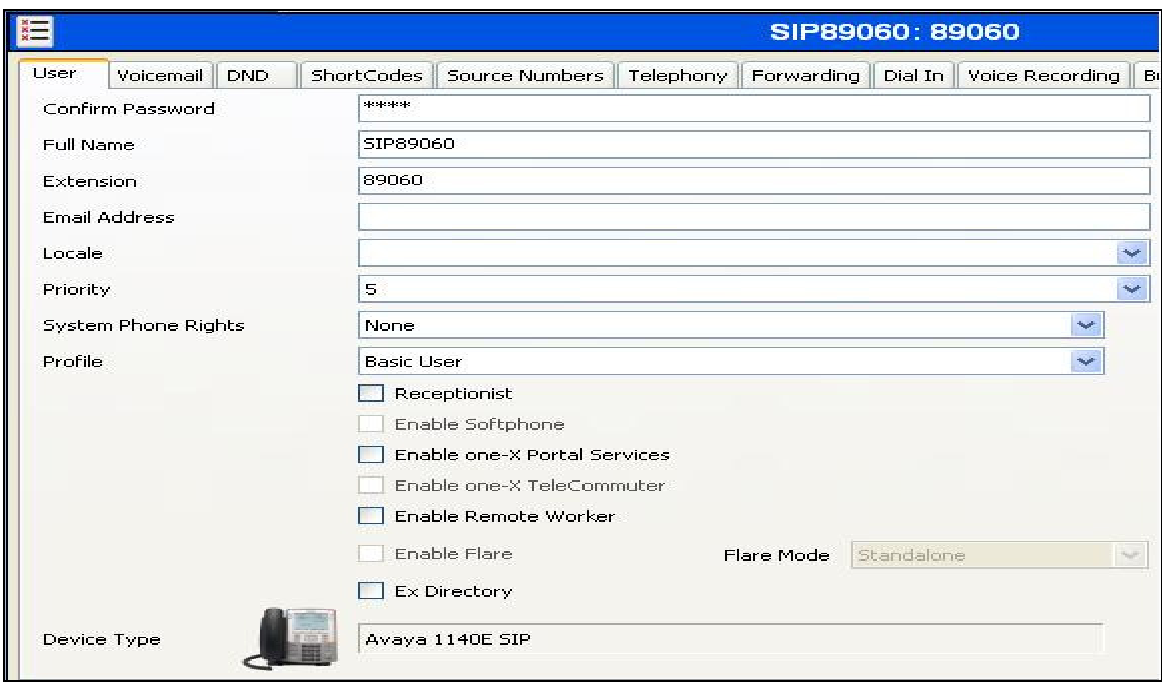
A new SIP extension may be added by right-clicking on **Extension** in the Navigation pane and selecting **New SIP Extension**. Alternatively, an existing SIP extension may be selected in the group pane. The following screen shows the **Extn** tab for the extension corresponding to an Avaya 1140E. The **Base Extension** field is populated with 89060, the extension assigned to the Avaya 1140E. Ensure the **Force Authorization** box is checked.



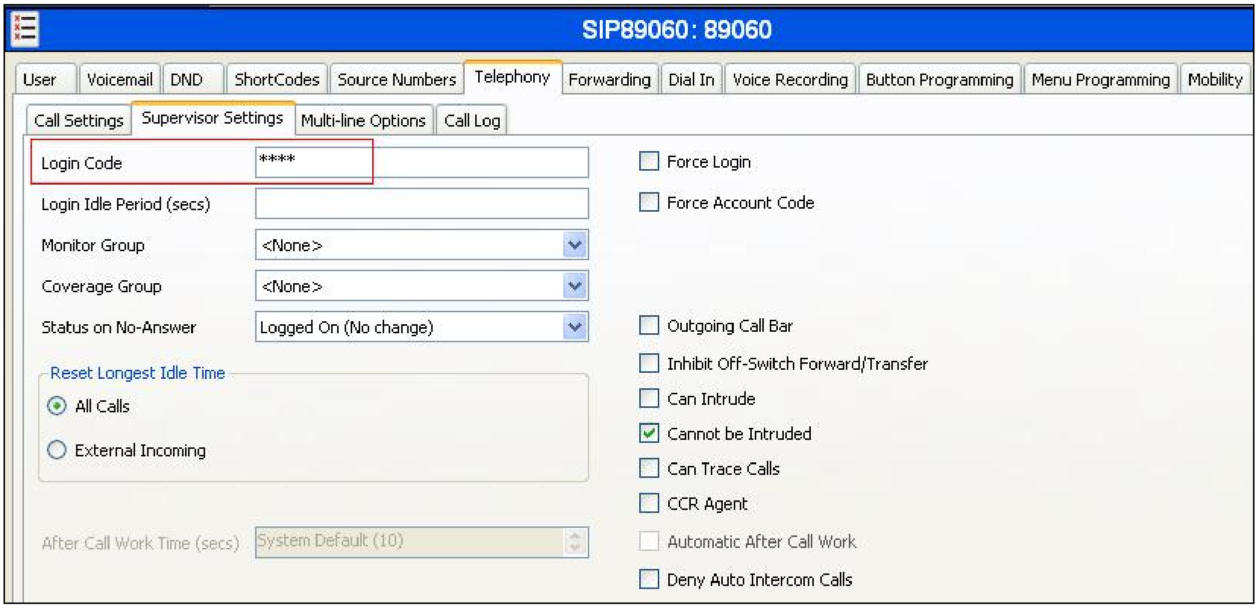
The following screen shows the **VoIP** tab for the extension. The **IP Address** field may be left blank or populated with a static IP address. Check the **Reserve Avaya IP endpoint license** box. The new **Codec Selection** parameter may retain the default setting “System Default” to follow the system configuration shown in **Section 5.5**. Alternatively, “Custom” may be selected to allow the codecs to be configured for this extension, using the arrow keys to select and order the codecs. Other fields may retain default values.



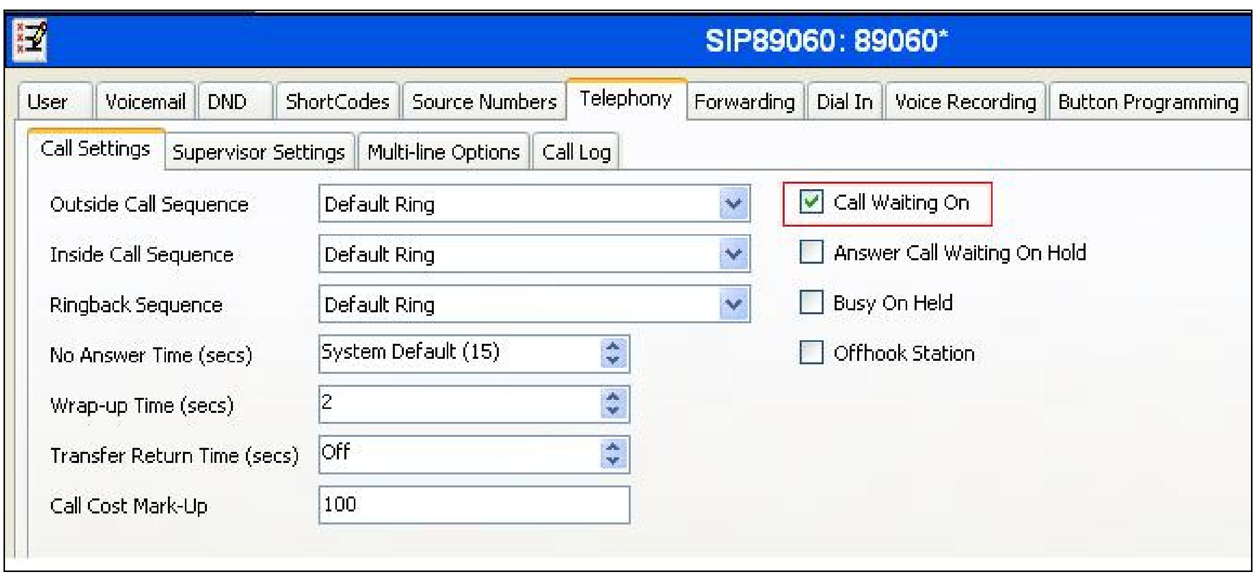
To add a User, right click on **User** in the Navigation pane, and select **New**. To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured in the Group pane. Configure the SIP parameters for each User that will be placing and receiving calls via the SIP line defined in **Section 5.6**. To configure these settings, select the **User** tab if any changes are required. The example below shows the changes required to use Avaya 1140E which was used in test.



Select the **Telephony** tab. Then select the **Supervisor Settings** tab as shown below. The **Login Code** will be used by the Avaya 1140E telephone user as the login password.



Remaining in the **Telephony** tab for the user, select the **Call Settings** tab as shown below. Check the **Call Waiting On** box to allow multiple call appearances and transfer operations.



Next select the **SIP** tab in the Details Pane. To reach the **SIP** tab click the right arrow on the right hand side of the Details Pane until it becomes visible. The values entered for the SIP **Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. These allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.6**). As such, these fields should be set to one of the DDI numbers assigned to the enterprise from Telenor.

In the example below, one of the DDI numbers in the test range is used, though only country code, city code and least significant digit are shown. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. On completion, click the **OK** button (not shown).

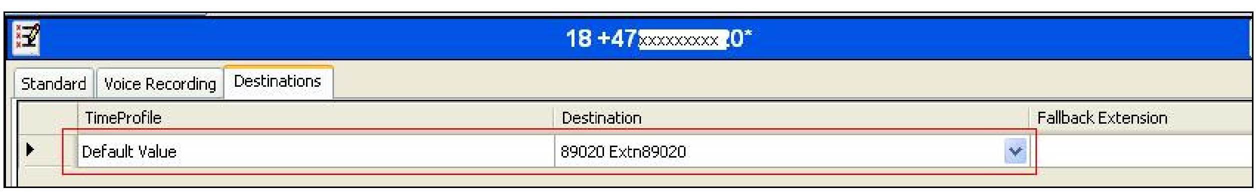
Note: The **Contact** field must be in E.164 format for the caller ID on the called phone to display properly.

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**s in the Navigation Pane and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capacity** 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

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 18 are routed to extension 89010.



5.10. Privacy / Anonymous Calls

There are multiple methods for a user to withhold outgoing identification:

- Dialing the short code *67 to access the SIP Line. (Section 5.7).
- Specific users may be configured to always withhold calling line identification by checking the **Anonymous** field in the **SIP** tab for the user (**Section 5.8**).
- Avaya Telephones equipped with a "Features" button can also request privacy for a specific call, without dialing a unique short code, using **Features → Call Settings → Withhold Number**, on the phone itself.

To configure IP Office to include the caller's DID number in the P-Asserted-Identity SIP header, required by Telenor SIP Trunk Service to admit an otherwise anonymous caller to the network, the following procedure may be used.

From the Navigation pane, select **User**. From the Group pane, scroll down past the configured users and select the user named **NoUser**. From the NoUser Details pane, select the tab **Source Numbers**. Press the **Add** button to the right of the list of any previously configured Source Numbers. In the **Source Number** field, type **SIP_USE_PAL_FOR_PRIVACY**. Click **OK**.

The source number **SIP_USE_PAI_FOR_PRIVACY** should now appear in the list of Source Numbers as shown below.

5.11. Save Configuration

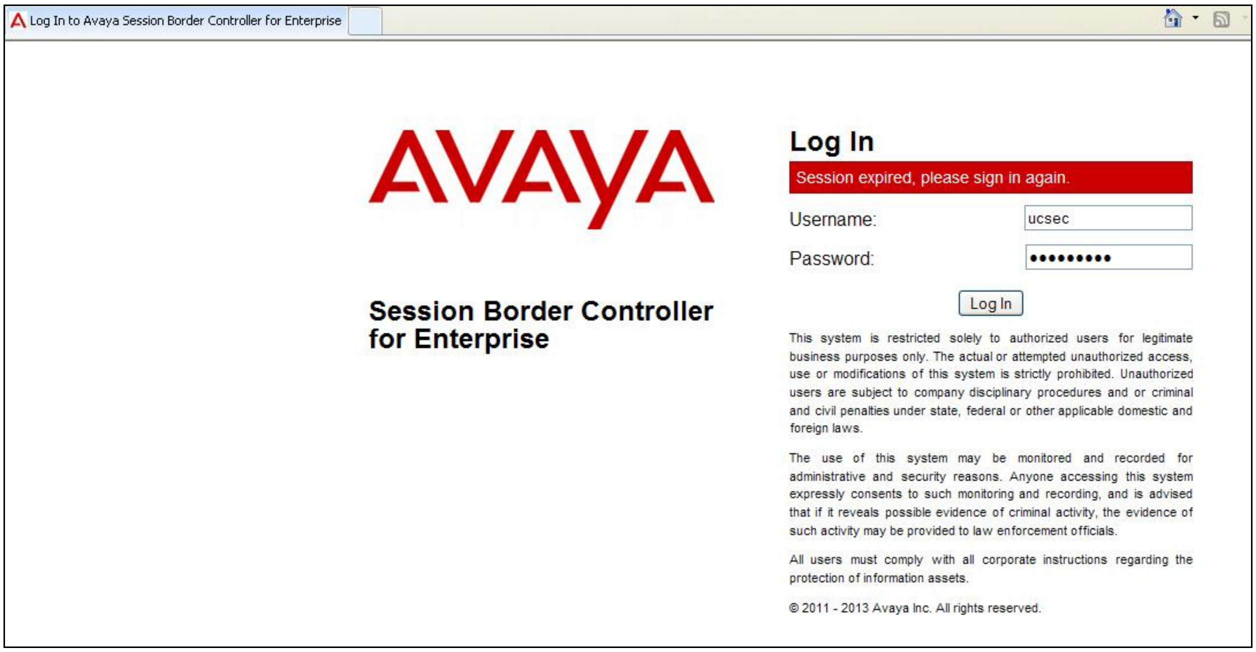
Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections.

6. Configure Avaya Session Border Controller for Enterprise

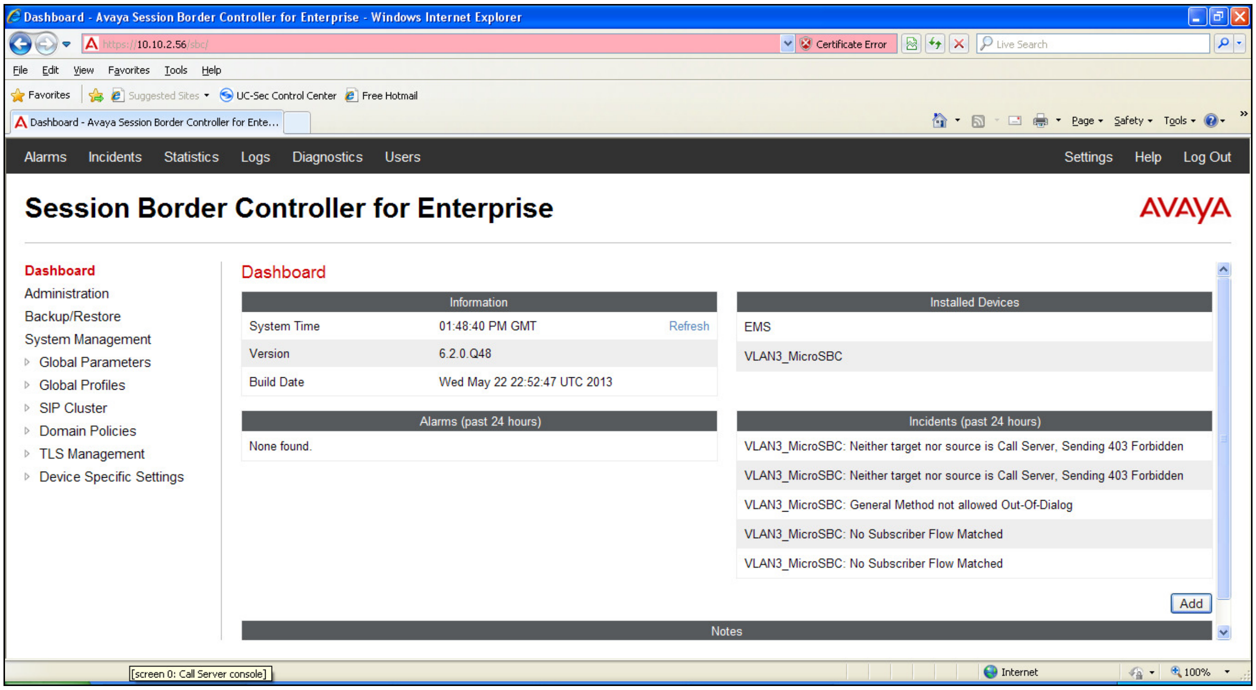
This section describes the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed.

6.1. Accessing Avaya Session Border Controller for Enterprise

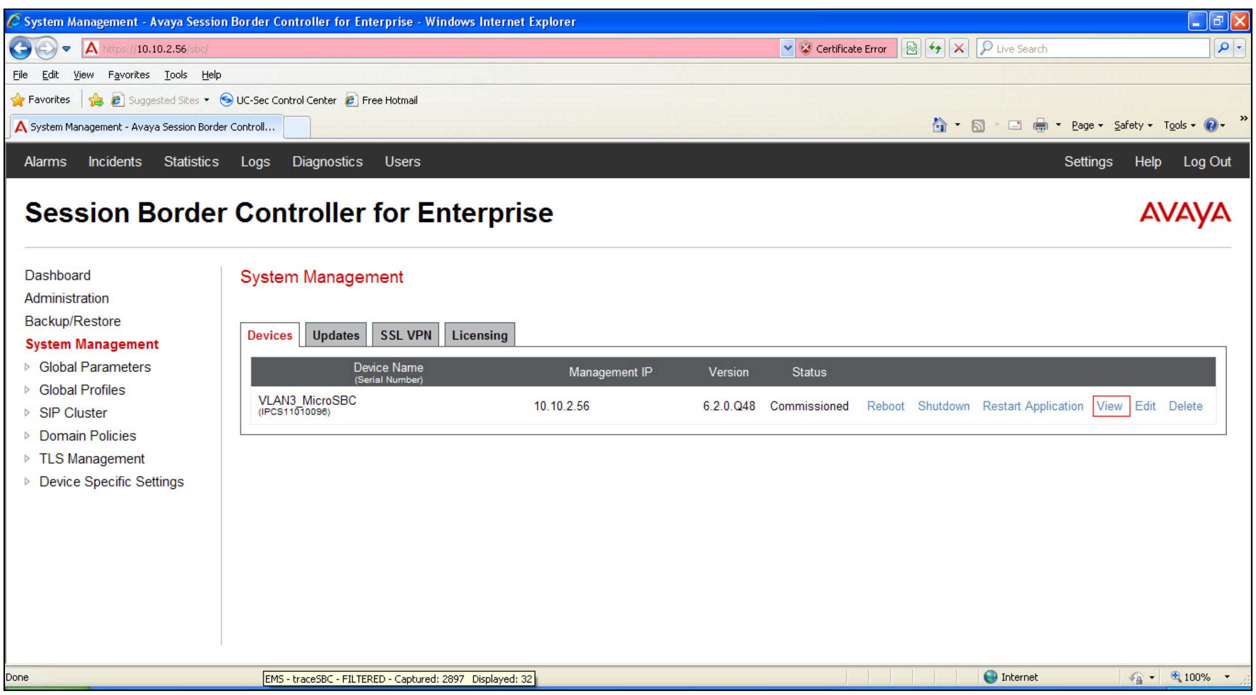
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



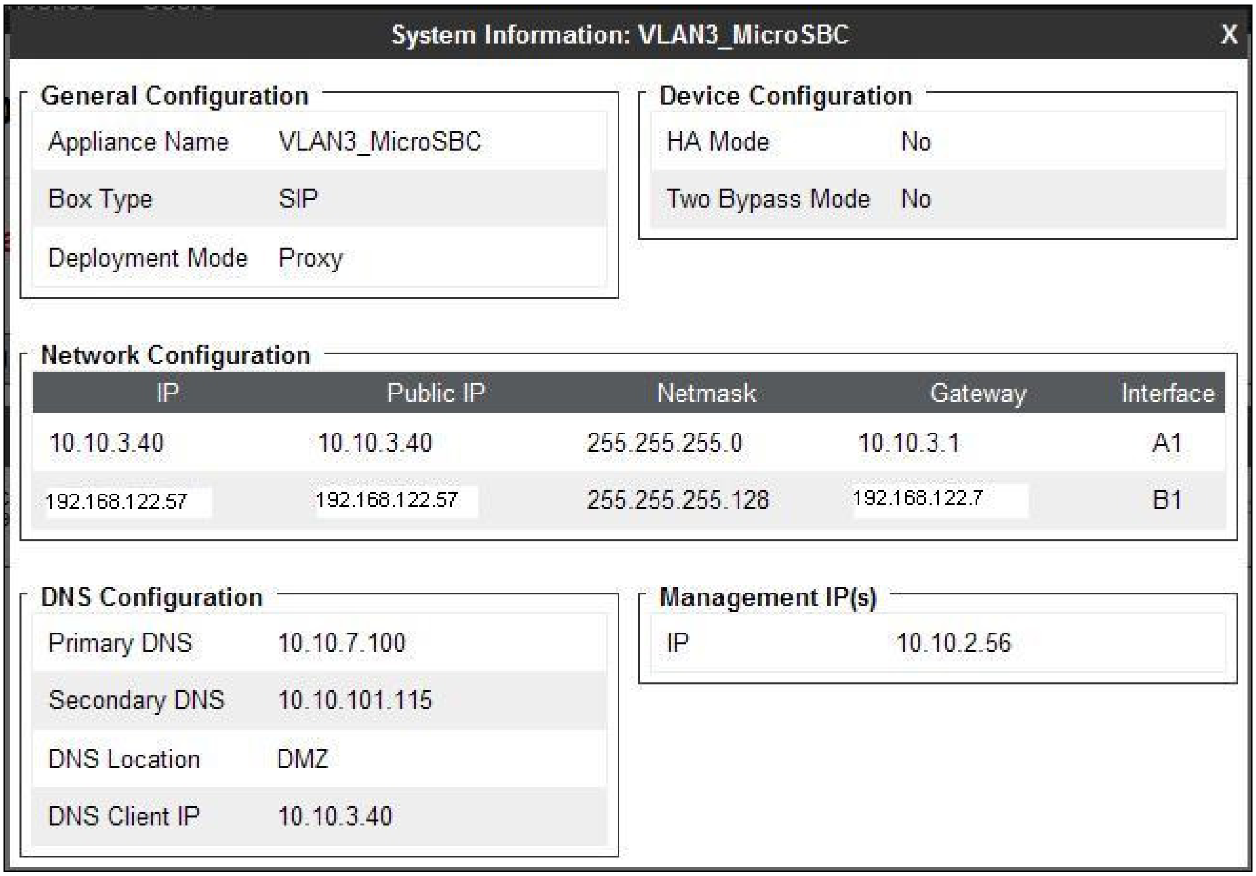
The dashboard of the Avaya SBCE will appear.



To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **VLAN3_MicroSBC** is shown. To view the configuration of this device, click **View** (the third option from the right).



The **System Information** screen shows the **Network Configuration, DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.



6.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

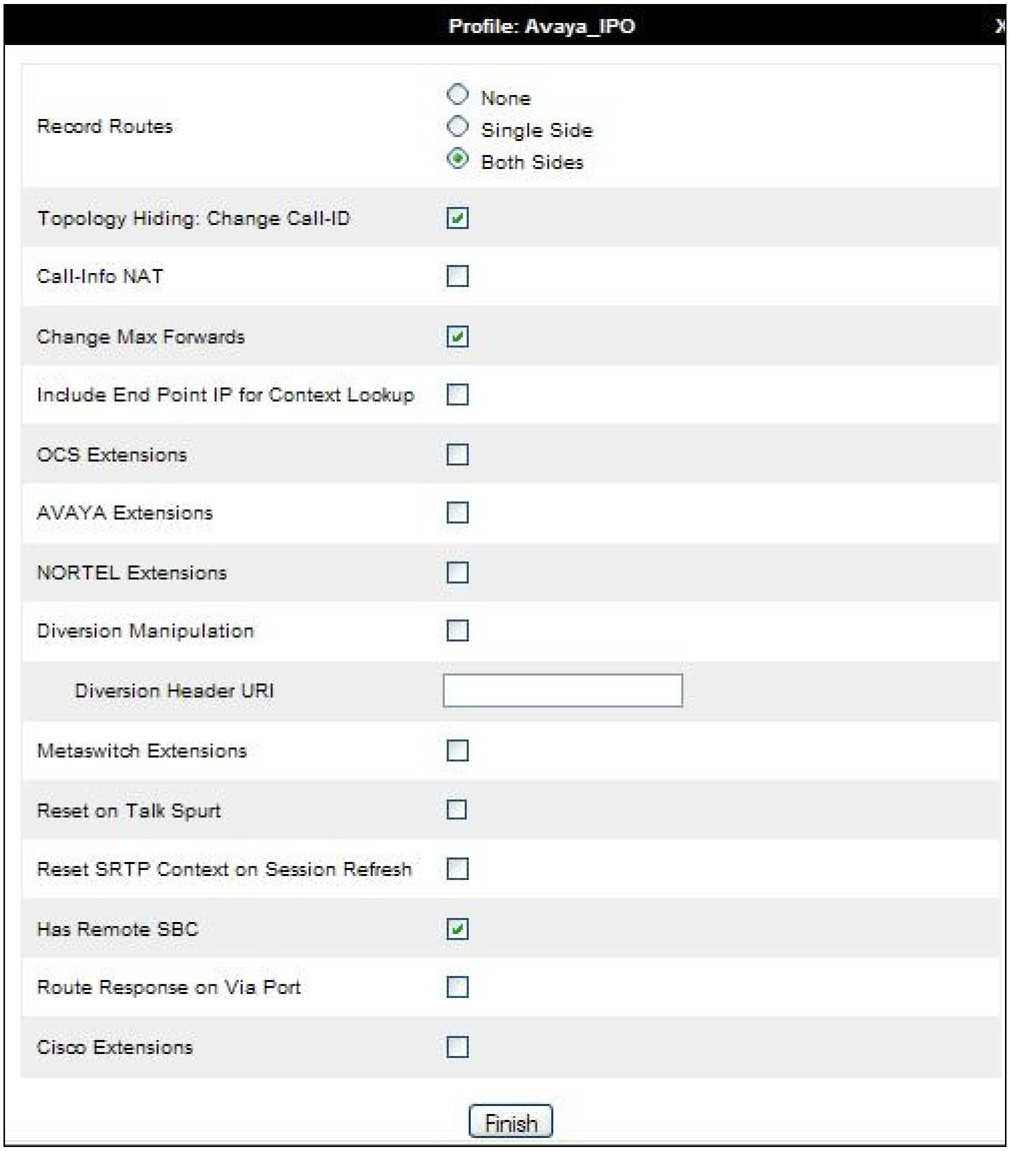
6.2.1. Server Internetworking Avaya

Server Internetworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles → Server Interworking** and click on **Add**.

- Enter profile name such as **Avaya_IPO** and click **Next** (not shown)
- Check **Hold Support= RFC3264**
- Check **T.38 Support**
- All other options on the **General** Tab can be left at default

Click on **Next** on the following screens and then **Finish**.

Default values can be used for the **Advanced Settings** window. Click **Finish**

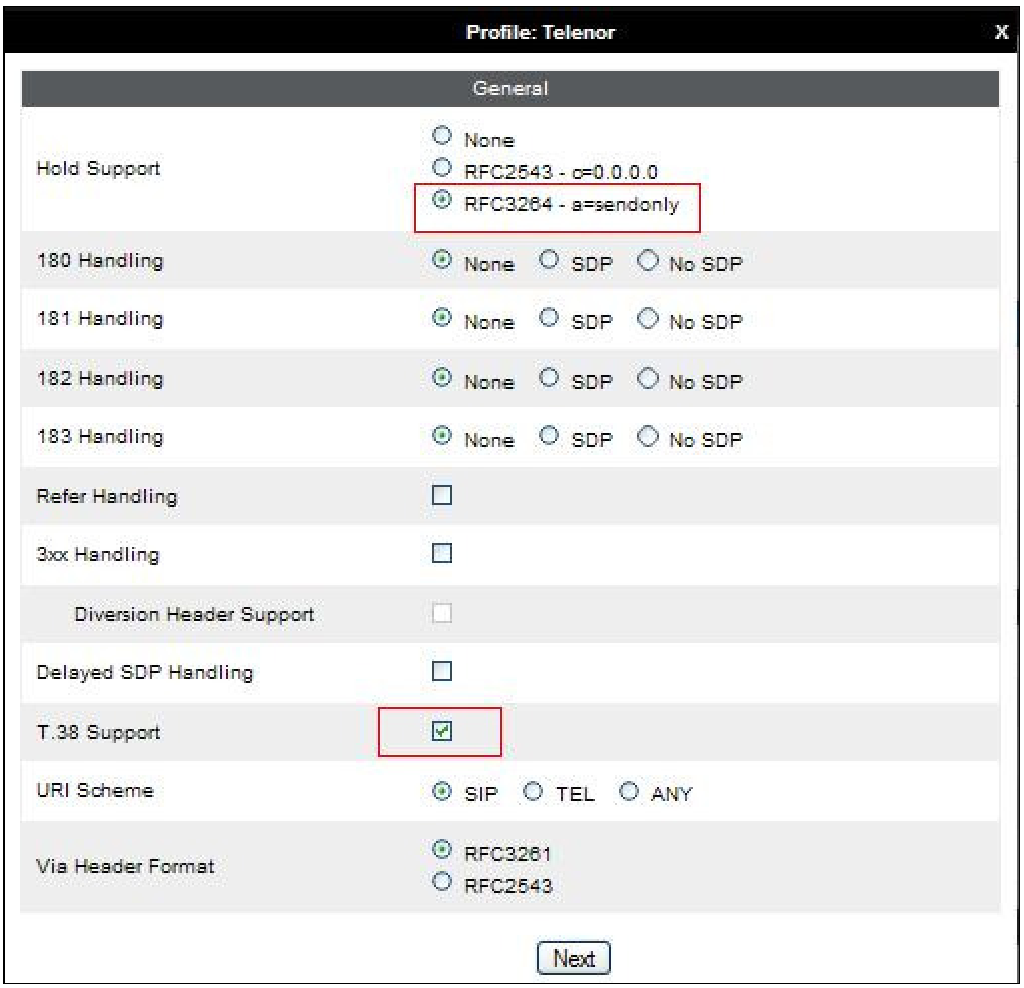


6.2.2. Server Internetworking – Telenor

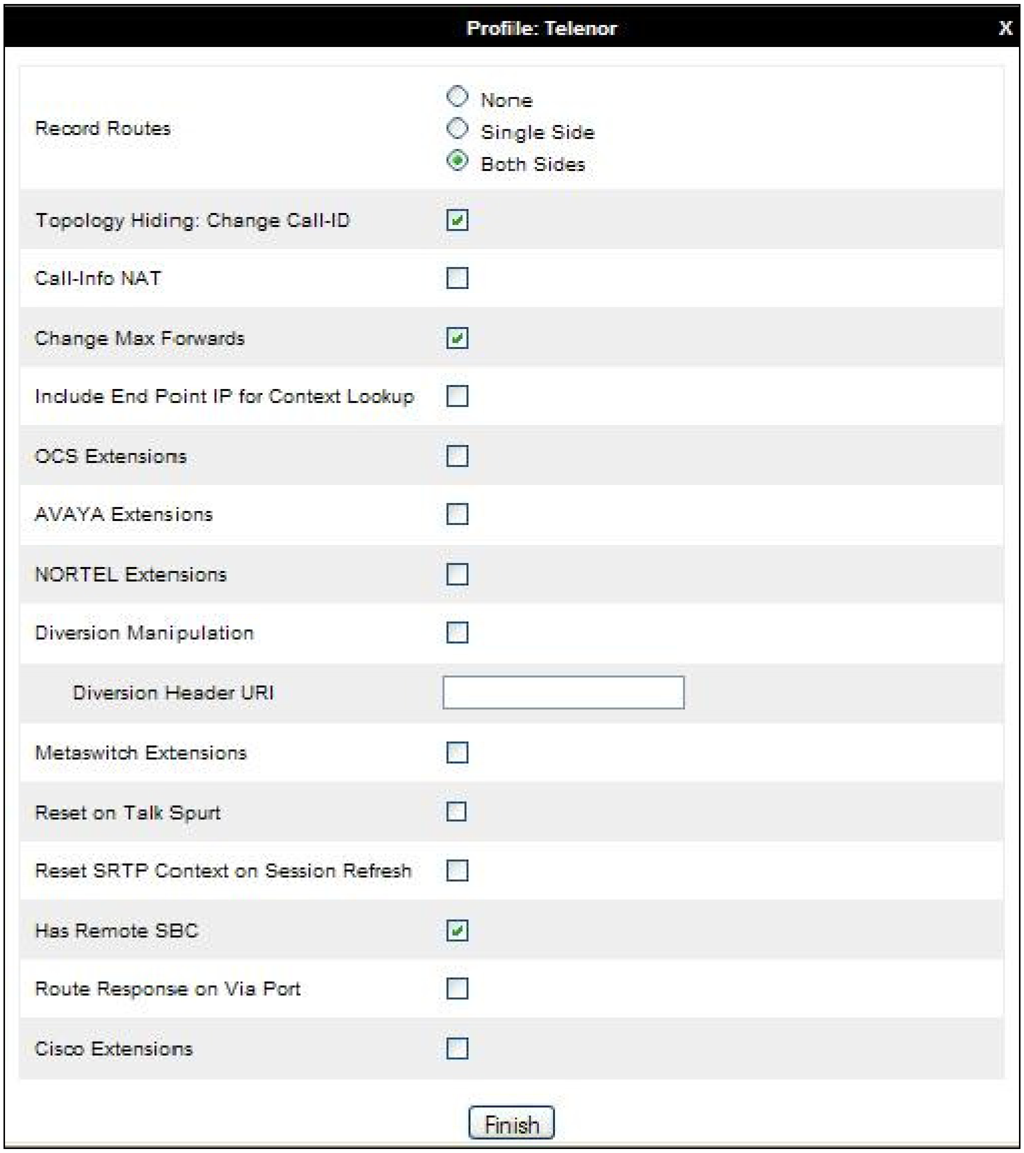
Server Internetworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles → Server Interworking** and click on **Add**.

- Enter profile name such as **Telenor** and click **Next** (not shown)
- Check **Hold Support= RFC3264**
- Check **T.38 Support**
- All other options on the **General** Tab can be left at default

Click on **Next** on the following screens and then **Finish**.



Default values can be used for the **Advanced Settings** window. Click **Finish**.



6.2.3. Routing

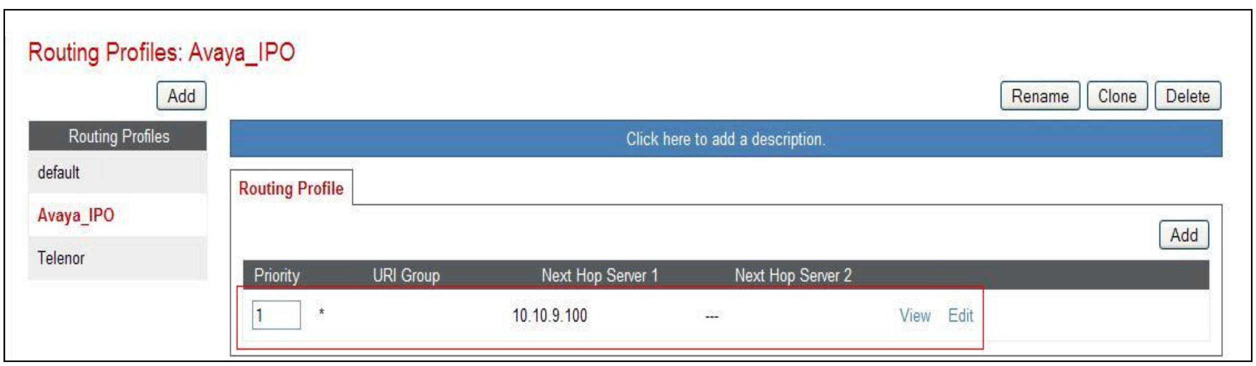
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

Create a Routing Profile for IP Office and a Routing Profile for Telenor. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.
In the new window that appears, enter the following values. Use default values for all remaining fields:

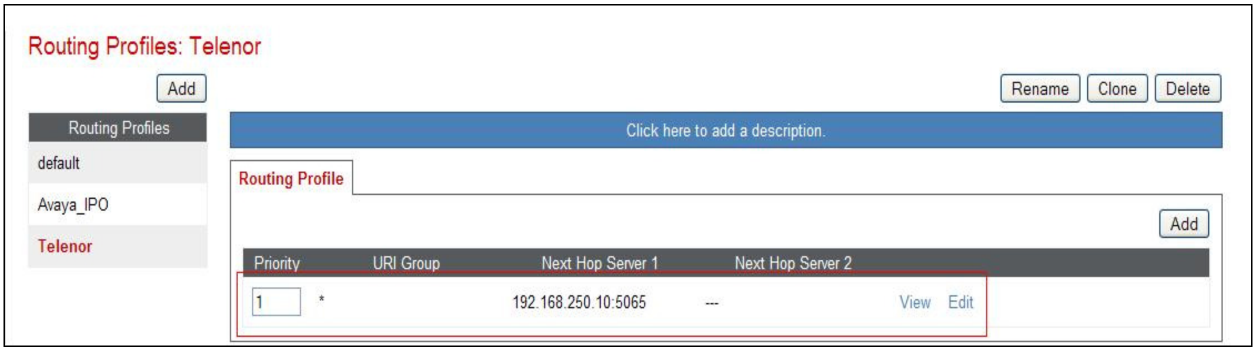
- **URI Group:** Select "*" from the drop down box
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server
- **Routing Priority Based on Next Hop Server**: Checked
- **Use Next Hop for In-Dialog Messages**: Select only if there is no secondary Next Hopserver
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets

Click **Finish**.

The following screen shows the Routing Profile to IP Office.



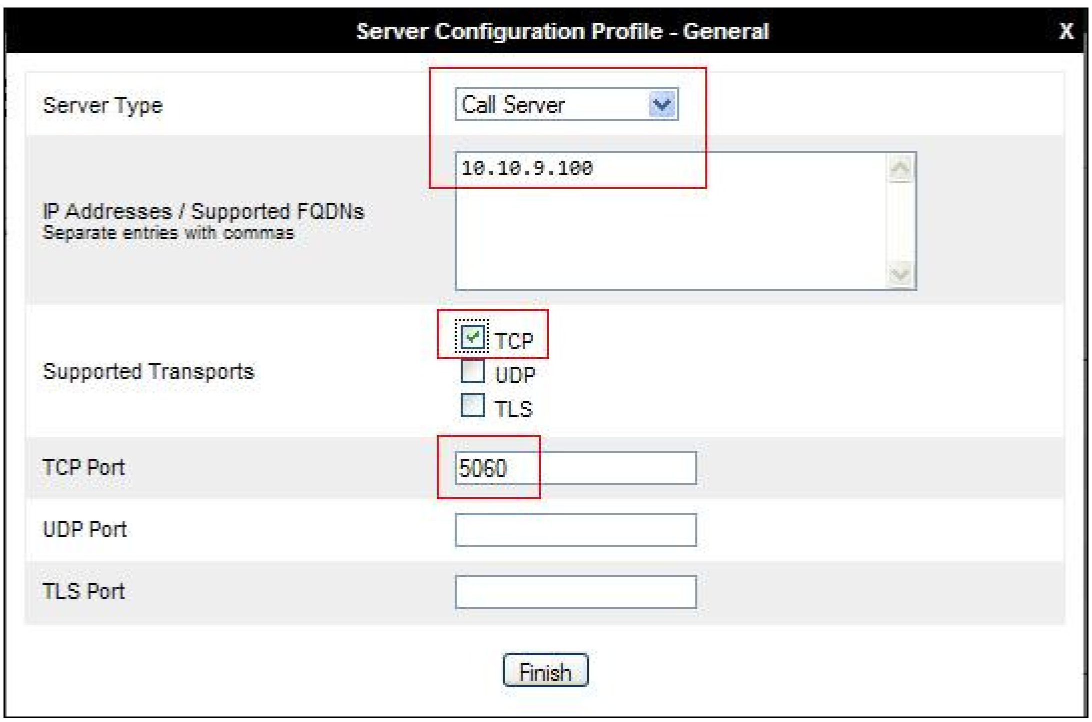
The following screen shows the Routing Profile to Telenor.



6.2.4. Server Configuration– Avaya IP Office

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add**. Enter **Profile Name: Avaya_IPO**. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**
- Enter **IP Addresses / Supported FQDNs** to **10.10.9.100**
- For **Supported Transports**, check **TCP**
- **TCP Port: 5060**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



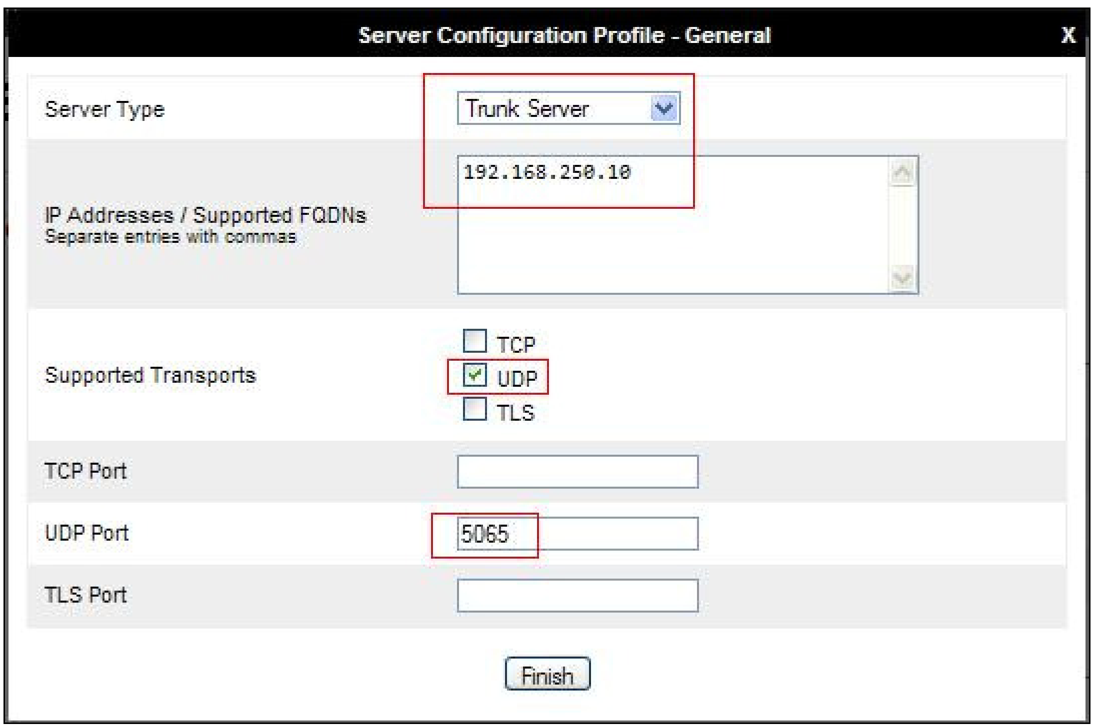
On the **Advanced** tab:

- Select **Avaya_IPO** for **Interworking Profile**
- Click **Finish**

6.2.5. Server Configuration – Telenor

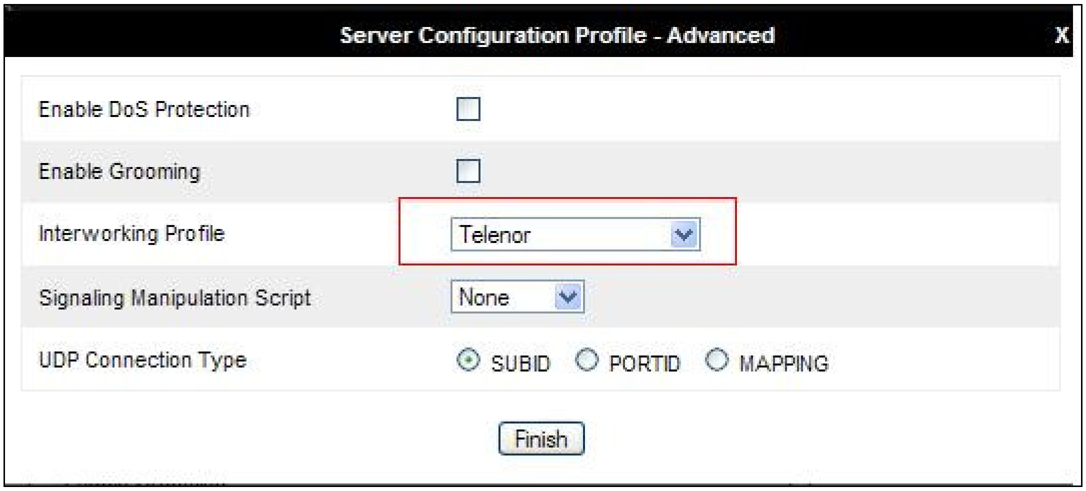
The **Server Configuration** screen contains fourtabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add**. Enter Name as **Telenor**. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** as **Trunk Server**
- Enter **IP Addresses / Supported FQDNs** to **192.168.250.10**
- **Supported Transports**: Check **UDP**
- **UDP Port: 5065** as specified by Telenor
- Click on **Next** (not shown)



On the Advanced tab:

- Select **Telenor** for Interworking Profile
- Click Finish



6.2.6. Topology Hiding

The **Topology Hiding** screen manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. Navigate to **Global Profiles → Topology Hiding** (not shown).

- Click **default** profile and select **Clone** (not shown)
- Enter a descriptive Profile Name
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Auto** under **Replace Action**
- Click **Finish** (not shown)

The screen below is a result of the details configured above for both Avaya IP Office and Telenor Topology Profiles.

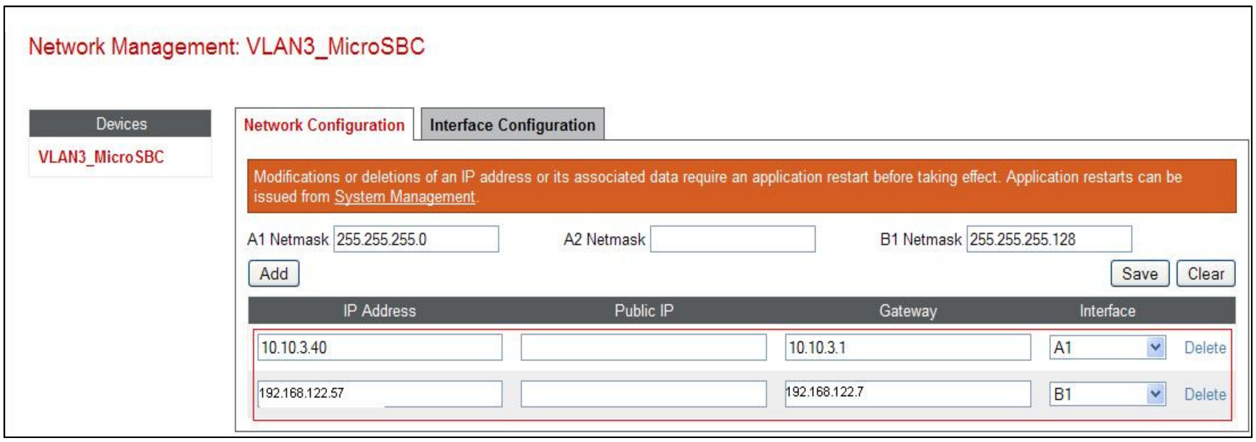
6.3. Device Specific Settings

The Device Specific Settings feature allows aggregation of system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network.

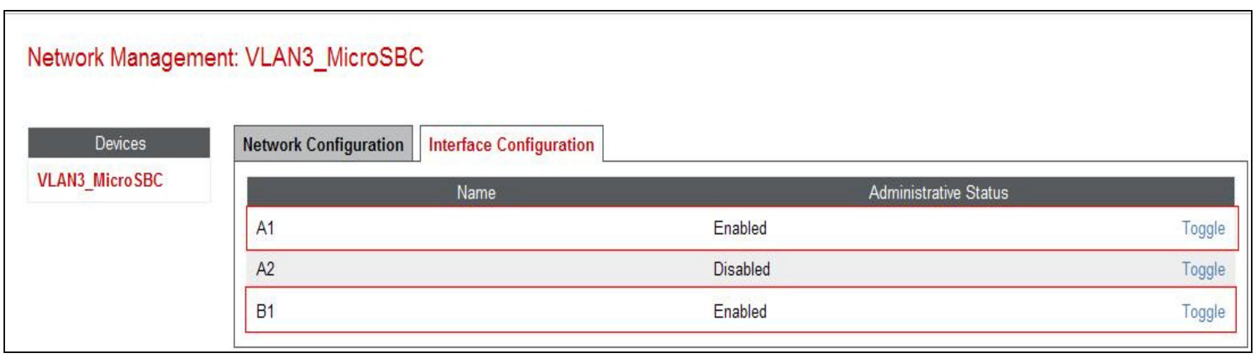
6.3.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the external interface is assigned to **B1**.



Select the **Interface Configuration** Tab and use the **Toggle** button to enable the interfaces.

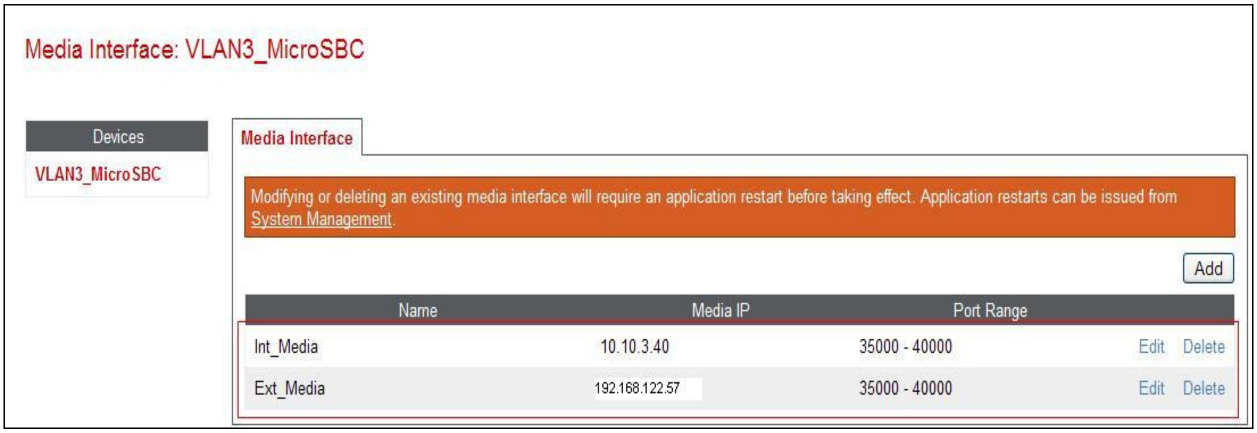


6.3.2. Media Interface

The Media Interface screen allows the IP address and ports to be set for transporting Media over the SIP trunk. The Avaya SBCE listens for SIP media on the defined ports.
To create a new Media Interface, navigate to **Device Specific Settings → Media Interface**.

- Select **Add**
- **Name**: **Int_Media**
- **Media IP**: **10.10.3.40** (Internal address for calls toward IP Office)
- **Port Range**: **35000-40000**
- Click **Finish**
- Select **Add**
- **Name**: **Ext_Media**
- **Media IP**: **192.168.122.57** (External address for calls toward Telenor)
- **Port Range**: **35000-40000**
- Click **Finish**

The following screen shows the Media Interfaces created in the sample configuration for the inside and outside IP interfaces.

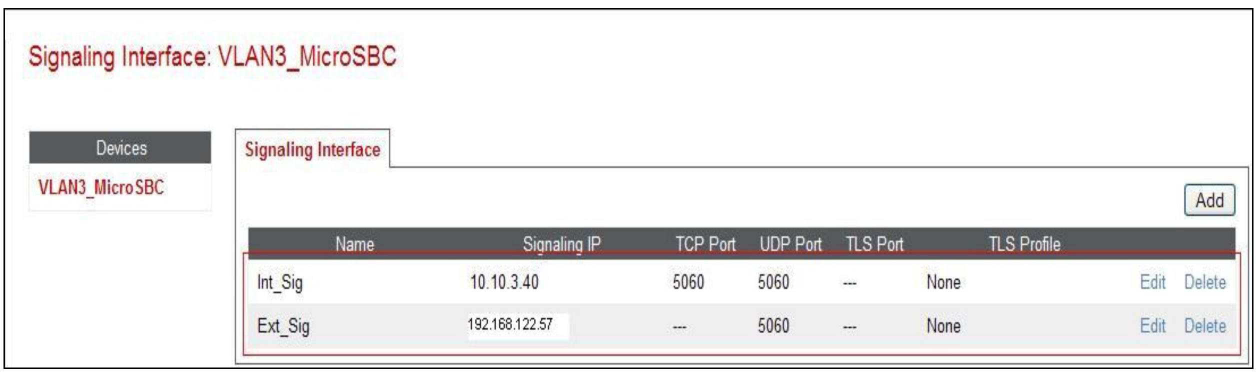


6.3.3. Signalling Interface

The Signalling Interface screen allows the IP Address and ports to be set for transporting signaling messages over the SIP trunk. The Avaya SBCE listens for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** and click **Add**.

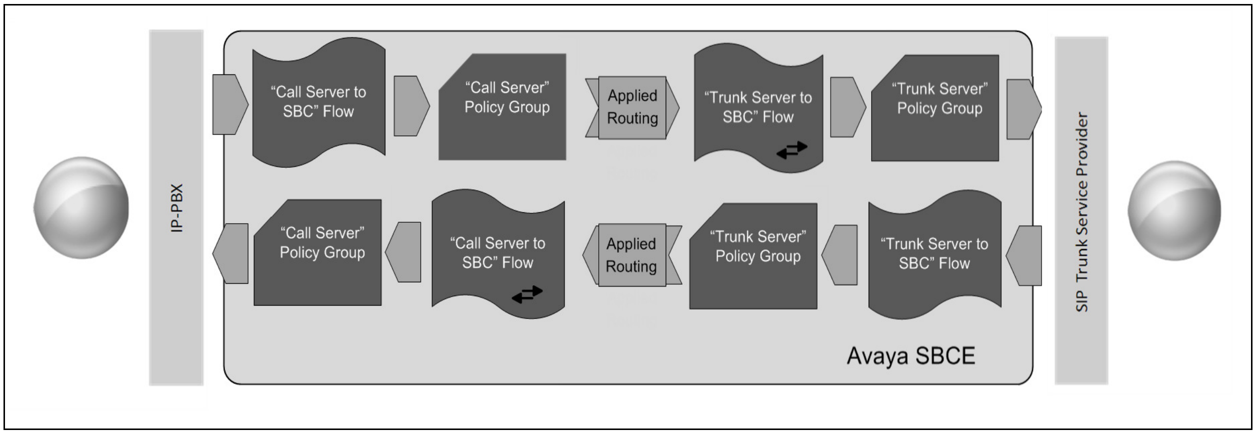
- **Name**: **Int_Sig**
- **Signaling IP**: **10.10.3.40** (Internal address for calls toward IP Office)
- **TCP Port**: **5060**
- **UDP Port**: **5060**
- Click **Finish**
- Select **Add**
- **Name**: **Ext_Sig**
- **Signaling IP: 192.168.122.57** (External address for calls toward Telenor)
- **UDP Port**: **5060**
- Click **Finish**

The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.



6.3.4. End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

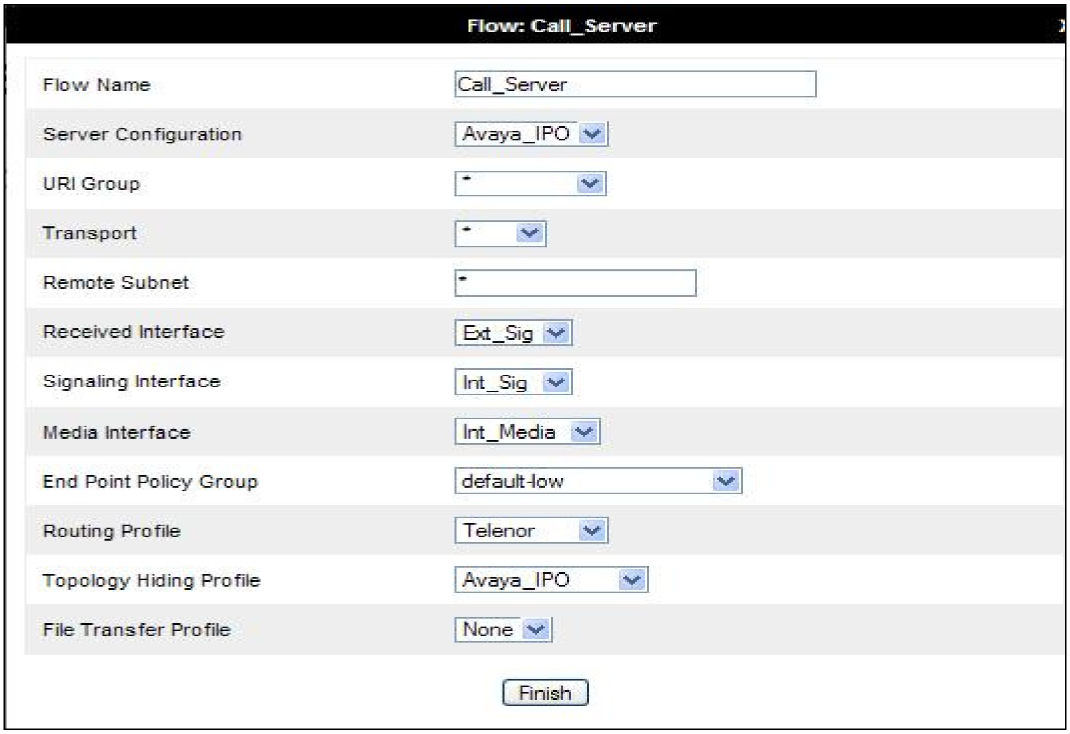


To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow**.

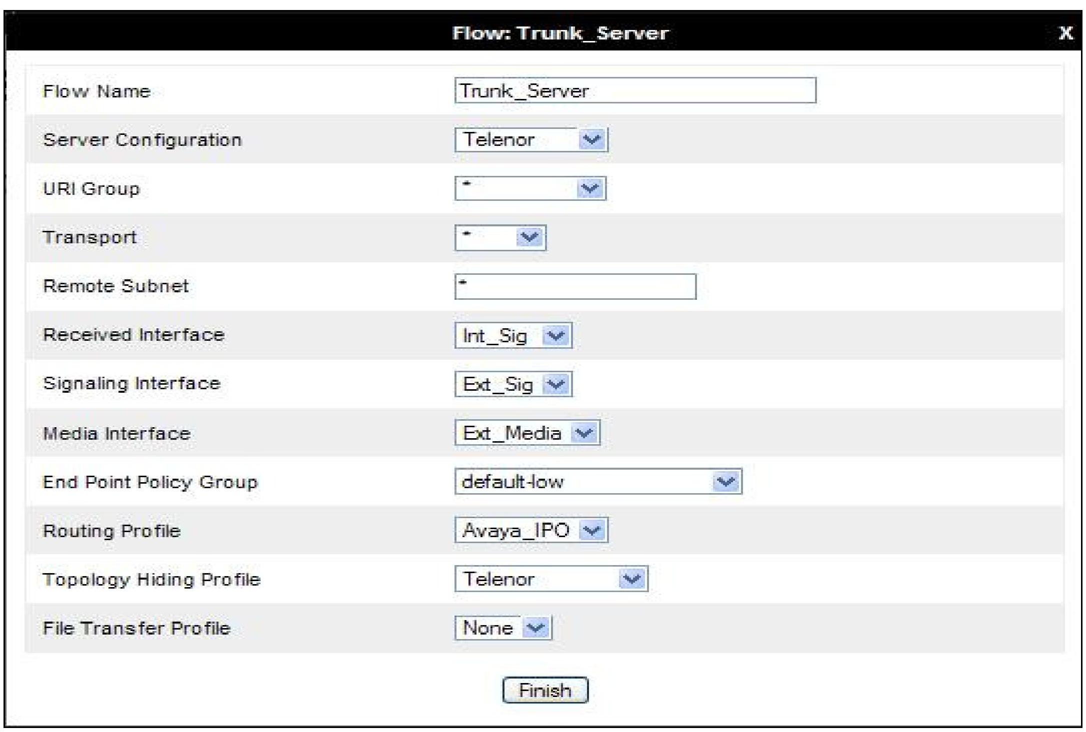
- **Flow Name:** Enter a descriptive name
- **Server Configuration:** Select a Server Configuration created in **Section 6.2.4** and **6.2.5** and assign to the Flow
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration
- **End Point Policy Group:** Select the policy assigned to the Server Configuration
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration

Click **Finish** to save and exit.

The following screen shows the Sever Flow for IP Office.



The following screen shows the Sever Flow for Telenor.



7. Telenor SIP Trunk Service Configuration

Telenor is responsible for the configuration of the SIP Trunk Service. The customer will need to provide the public IP address used to reach the Avaya IP Office at the enterprise. Telenor will provide the customer the necessary information to configure the SIP connection to the SIP Trunking service including:

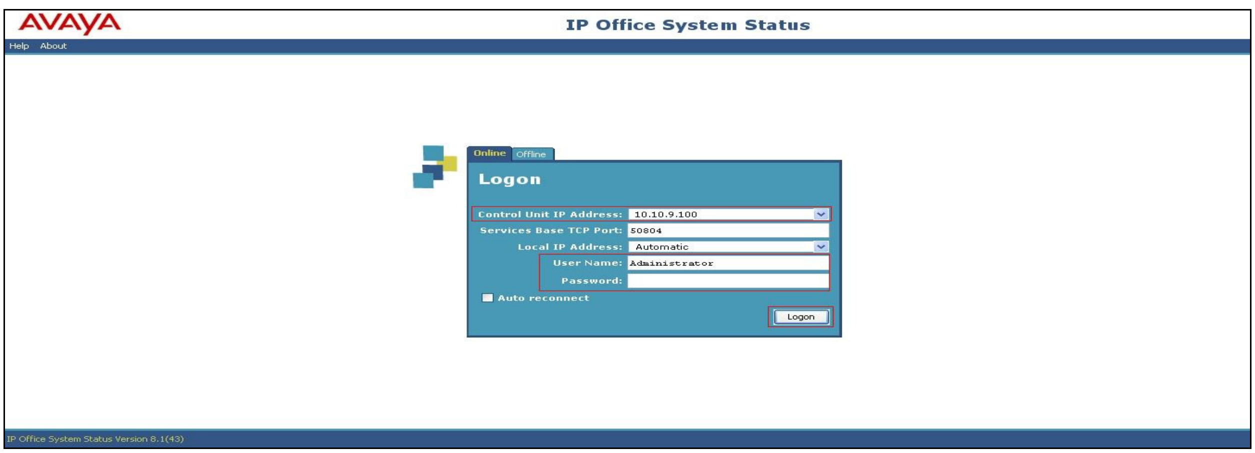
- IP address of SIP Trunking SIP proxy
- Network SIP Domain
- Supported codecs
- DDI numbers
- All IP addresses and port numbers used for signalling or media that will need access to the enterprise network through any security devices.

8. Verification Steps

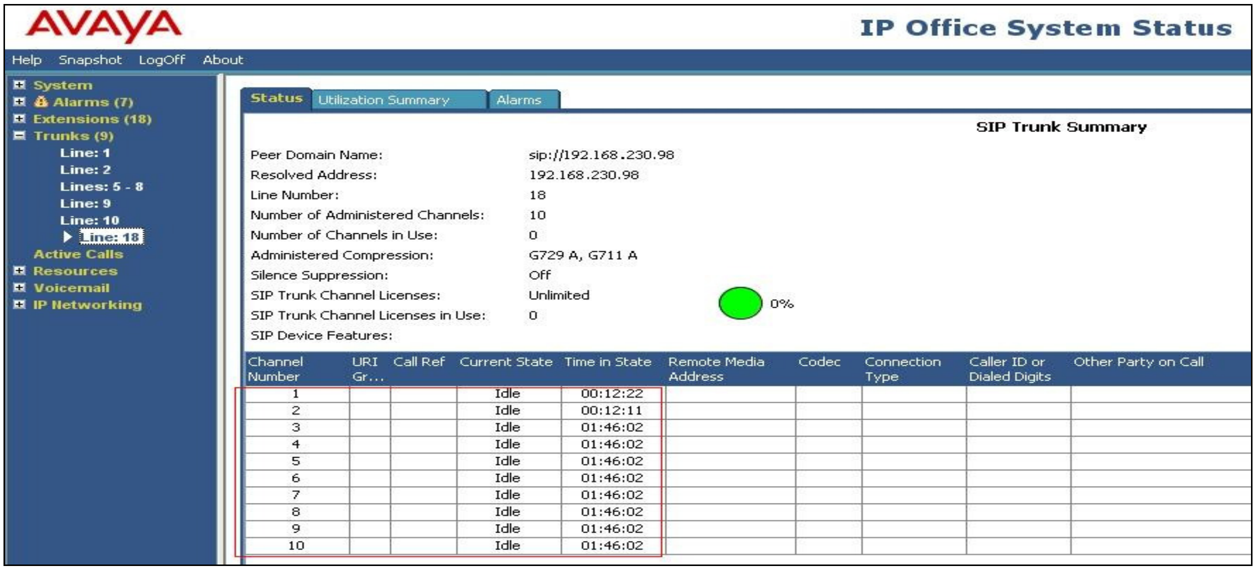
This section includes steps that can be used to verify that the configuration has been done correctly.

8.1. SIP Trunk status

The status of the SIP trunk can be verified by opening the System Status application. This is found on the PC where IP Office Manager is installed in PC programs under **Start →All Programs →IP Office →System Status** (not shown).
Log in to IP Office System Status at the prompt using the **Control Unit IP Address** for the IP office. The **User Name** and **Password** are the same as those used for IP Office Manager.



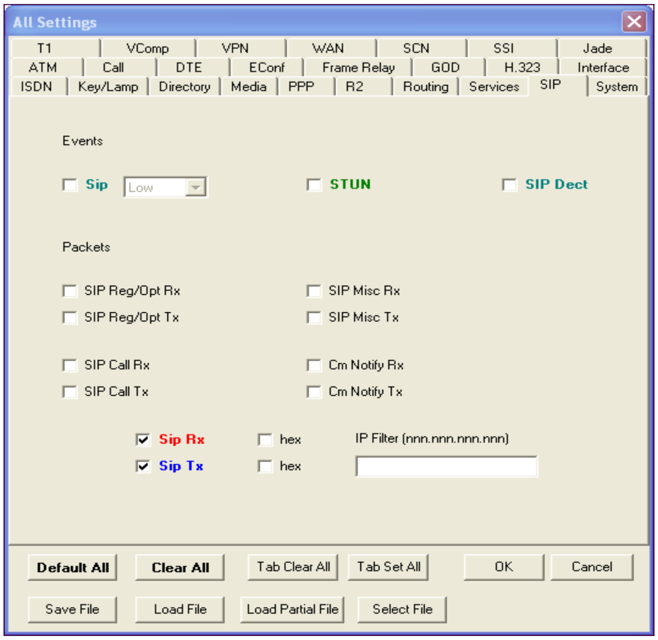
From the left hand menu expand **Trunks** and choose the SIP trunk (**18** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational. IP address has been changed.



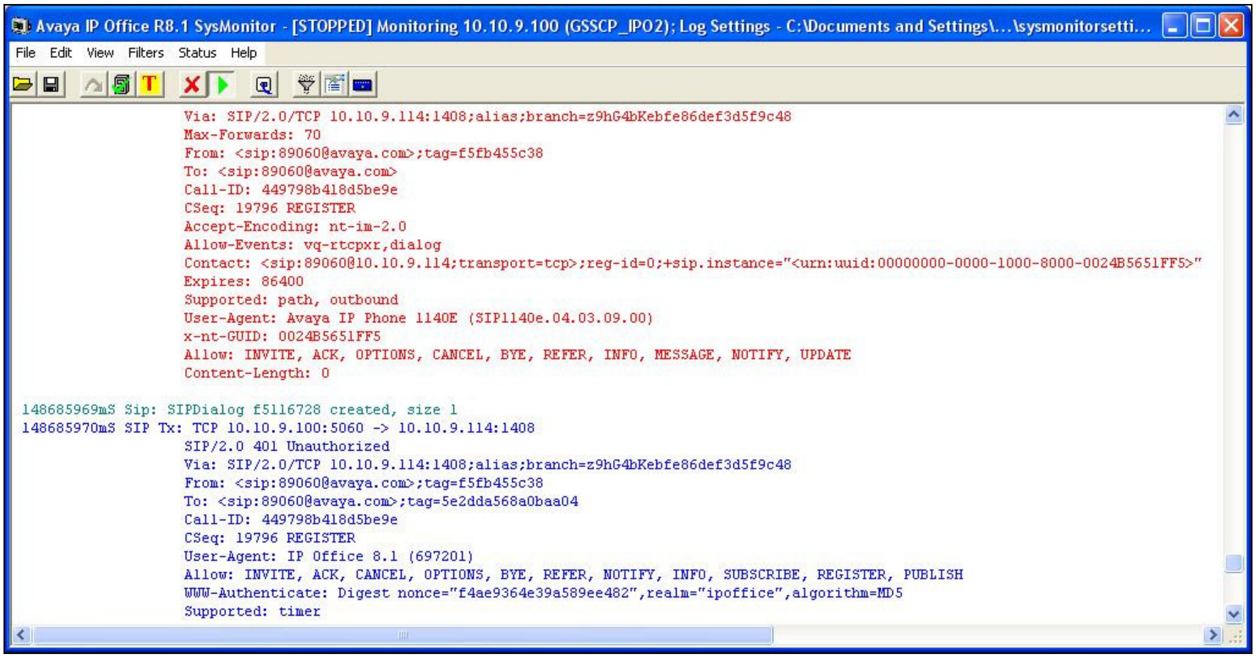
8.2. Monitor

The Monitor application can also be used to monitor and troubleshoot IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select the button that is third from the right in the screen below, or select **Filters →Trace Options**.

The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, the **SIP Rx** and **SIP Tx** boxes are checked. All SIP messages will appear in the trace with the color blue. To customize the color, right-click on **SIP Rx** or **SIP Tx** and select the desired color.



As an example, the following shows a portion of the monitoring window for a Registration attempt to the SIP trunk.

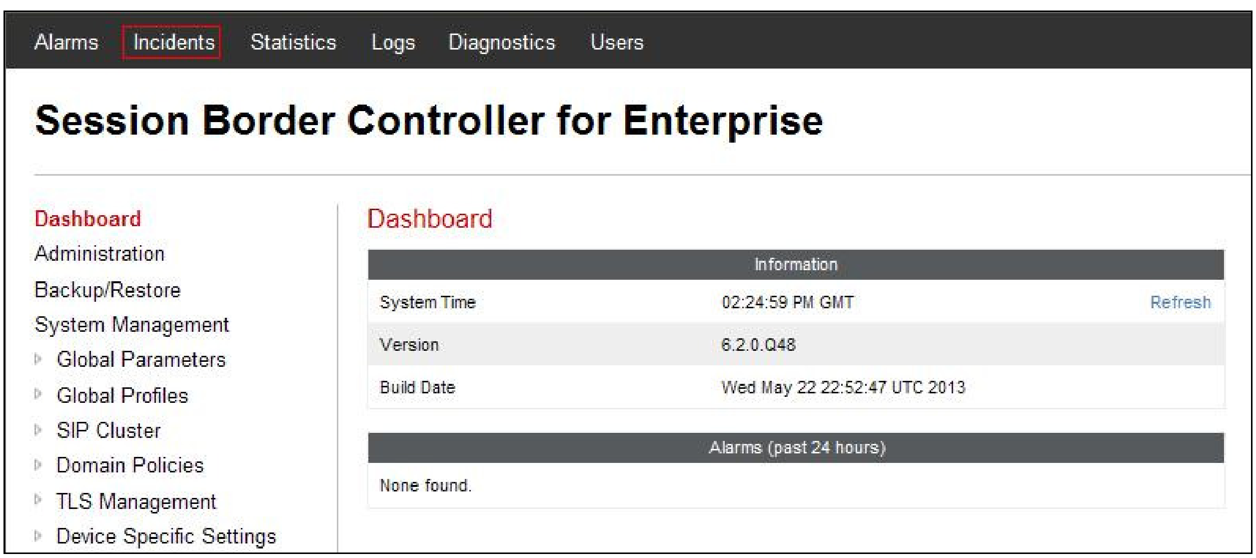


8.3. Avaya SBCE

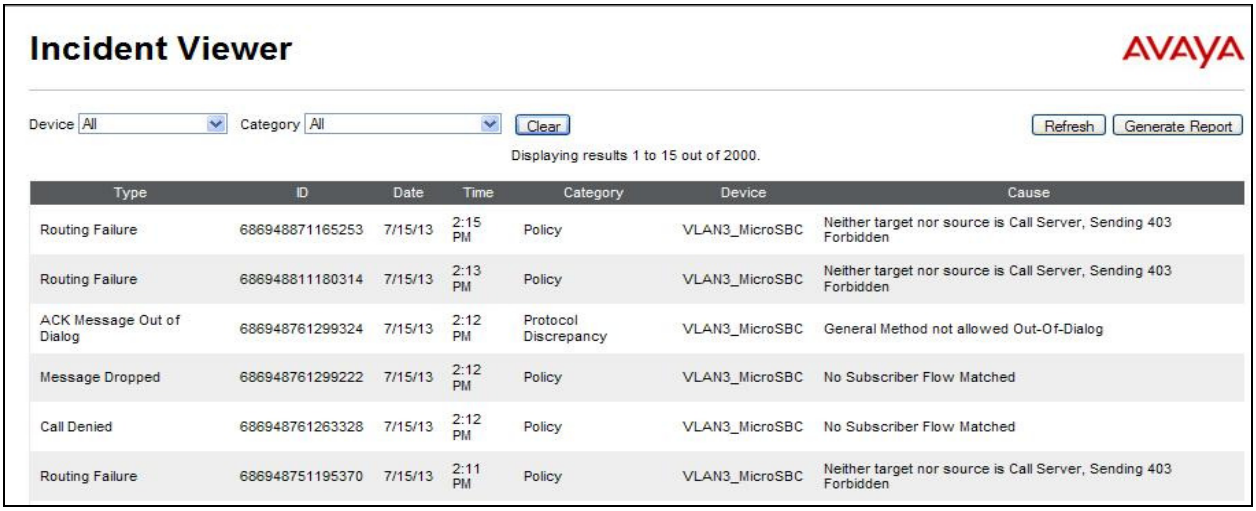
This section provides verification steps that may be performed with the Avaya SBCE.

8.3.1. Incidents

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



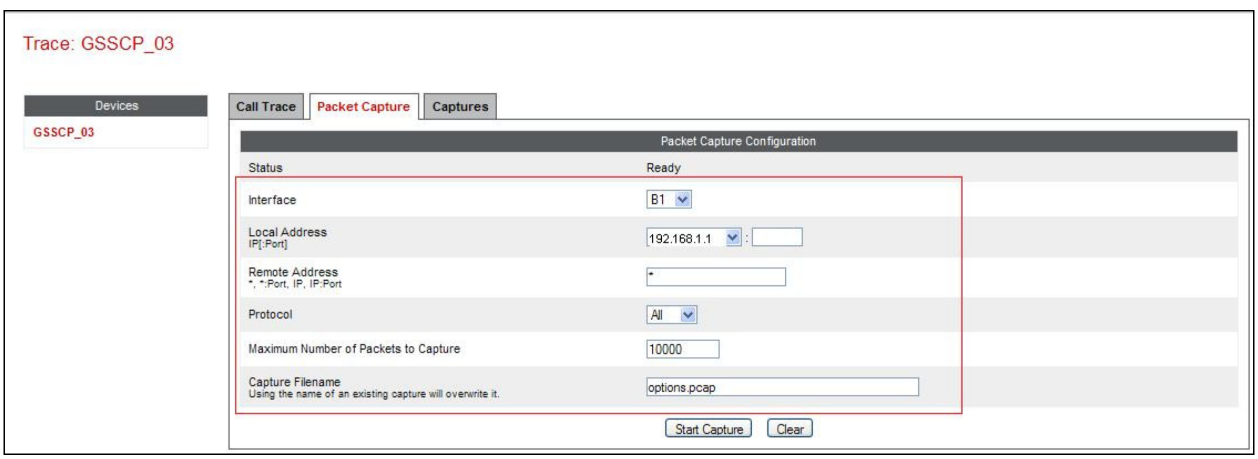
Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures.



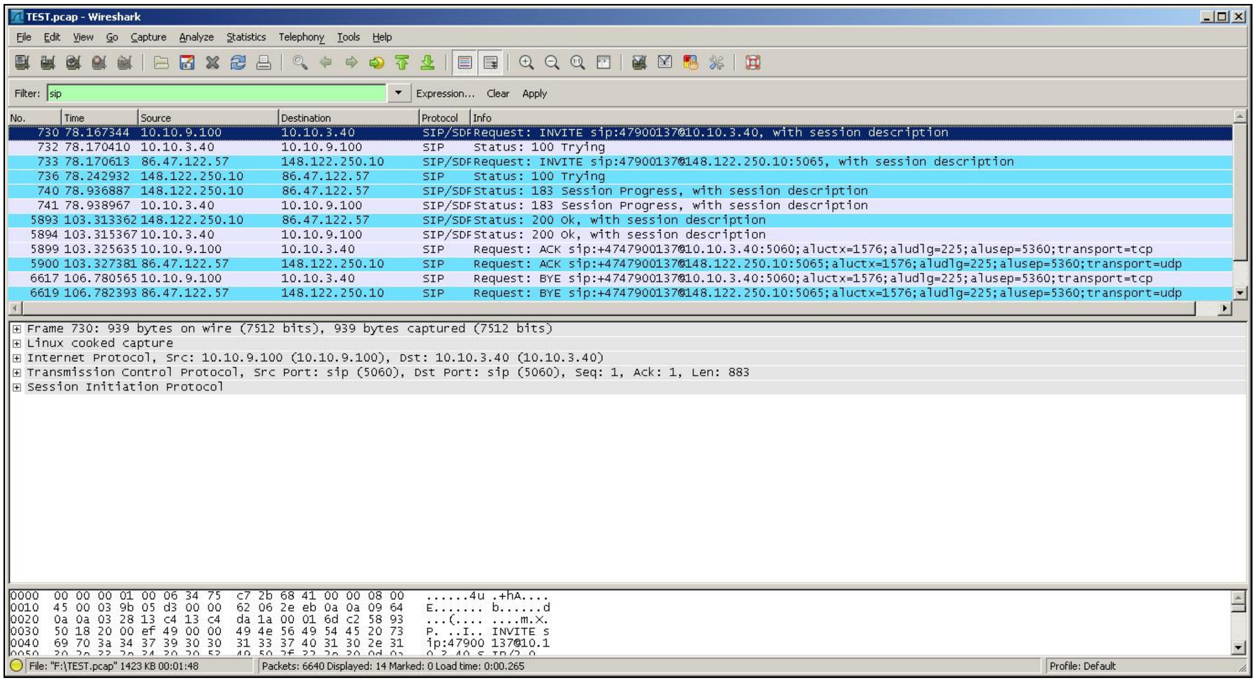
8.3.2. Trace Capture

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

- Select the SIP Trunk interface from the **Interface** drop down menu
- Select the signalling interface IP address from the **Local Address** drop down menu
- Enter the IP address of the Service Provider's SBC in the **Remote Address** field or enter a ***** to capture all traffic
- Specify the **Maximum Number of Packets to Capture**, 10000 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 as per screenshot below.



9. Conclusion

These Application Notes demonstrated how IP Office Release 8.1 and Avaya Session Border Controller for Enterprise can be successfully combined with Telenor SIP trunk service solution as shown in **Figure 1**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and demonstrates Avaya IP Office with Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with Telenor SIP Trunk Service. This solution provides IP Office and Avaya Session Border Controller for Enterprise users the ability to access the Public Switched Telephone Network (PSTN) via a SIP trunk using the Telenor SIP Trunk thus eliminating the costs of analog or digital trunk connections previously required to access the PSTN.

10. Additional References

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

[1] *Avaya IP Office 8.1* Documentation CD, 16th July 2012.
[2] *IP Office 8.1 Installation Manual,* Document Number 15-601042, August 2012.
[3] *IP Office Manager Manual 10.0,* Document Number 15-601011, August 2012
[4] *IP Office Release 8.1 Implementing Voicemail Pro*, Document Number 15-601064, June 2012
[5] *System Status Application,* Document number15-601758, 12th November 2011
[6] *IP Office Softphone Installation*, 28th September 2011
[7] *IP Office SIP Extension Installation*, 3rd October 2011
[8] *Avaya IP Office Knowledgebase,* http://marketingtools.avaya.com/knowledgebase
[9] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2
[10] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2

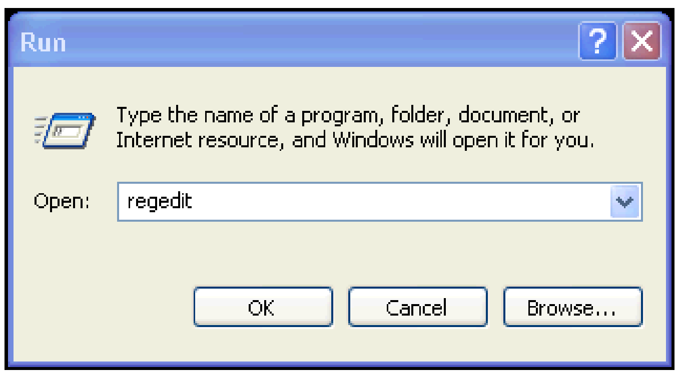
11. Appendix A: SIP Line Template

Avaya IP Office Release 8.1 supports a SIP Line Template (in xml format) that can be created from an existing configuration and imported into a new installation to simplify configuration procedures as well as to reduce potential configuration errors.

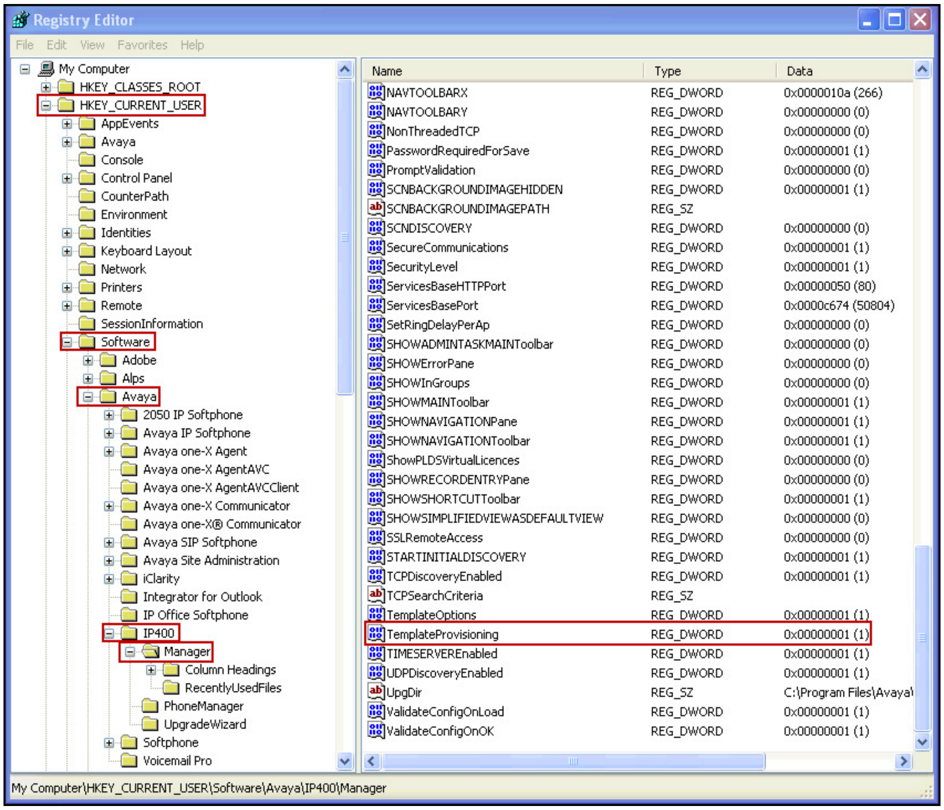
Note that not all of the configuration information, particularly items relevant to a specific installation environment, is included in the SIP Line Template. Therefore, it is critical that the SIP Line configuration be verified/updated after a template has been imported and additional configuration be supplemented using the settings provided in this Application Note as a reference.

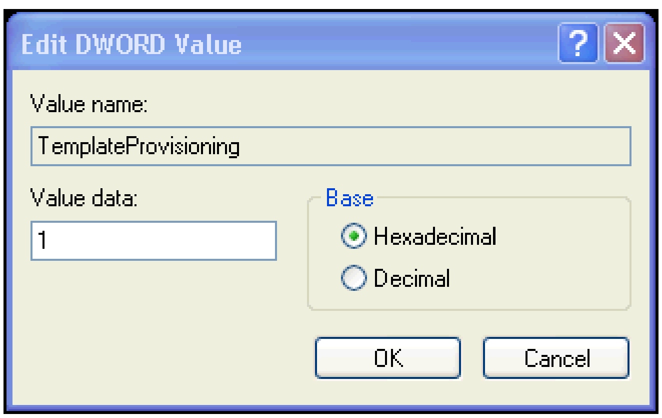
Create a new registry entry called **TemplateProvisioning** and set the **Value data** to **1**, as follows:

Select **Start**, and then **Run**. Type **regedit** as shown below



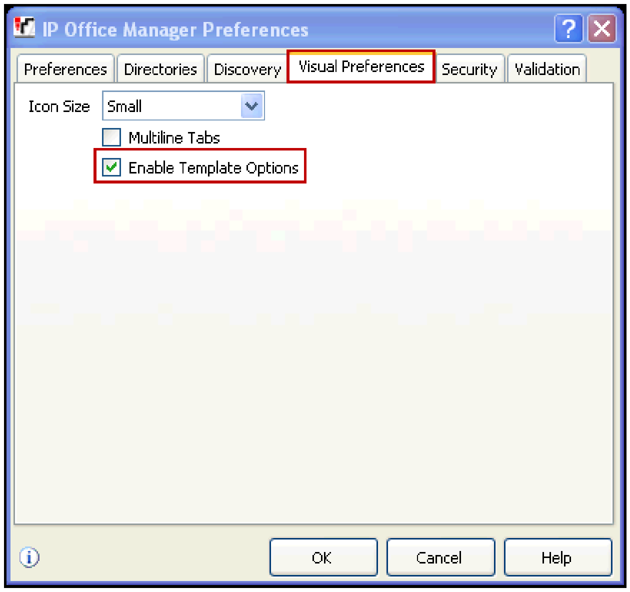
Under **HKEY_CURRENT_USER, Software, Avaya, IP400**, right click on **Manager**, then select **New, DWORD value,** then rename the newly created entry to: **TemplateProvisioning.** Right click on the newly created entry and select **Modify,** change the value under **Value Data** from "**0**" to "**1**".





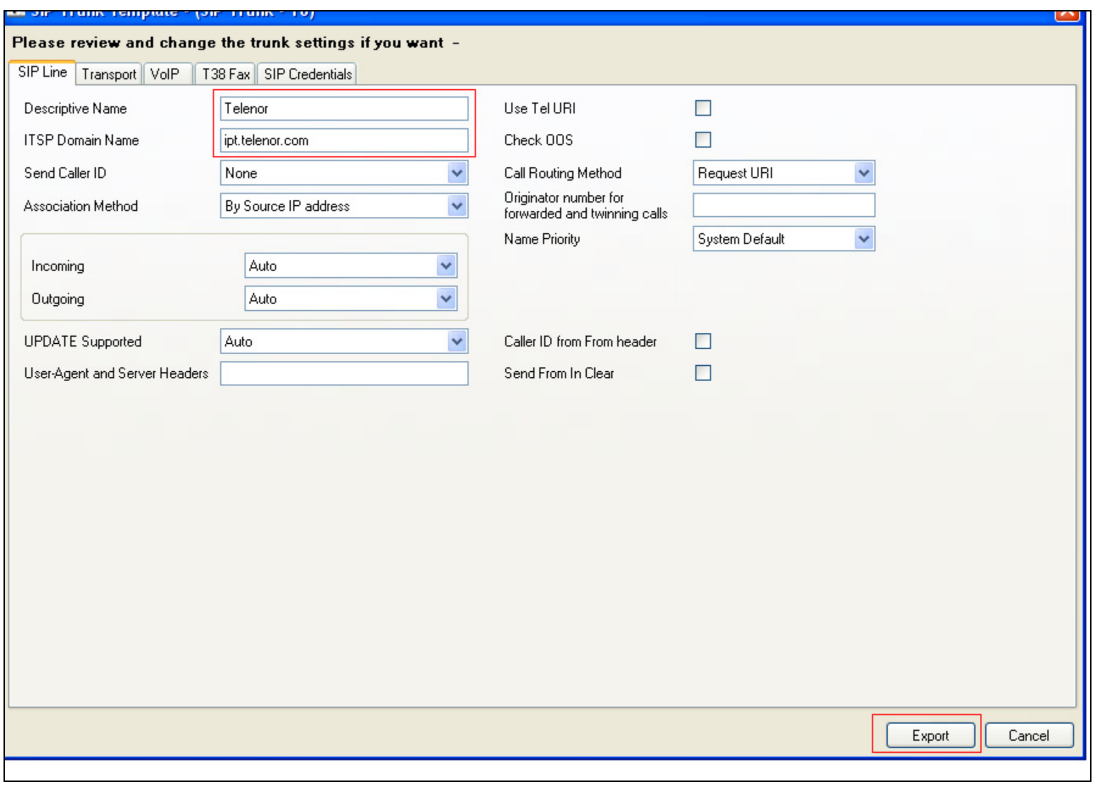
Reboot the computer

When the computer comes back up, enable the template by opening **IP Office Manager**, select **File**, and then **Preferences**. On the **Visual Preferences** tab, check the **Enable Template Options** box, and click **OK**.

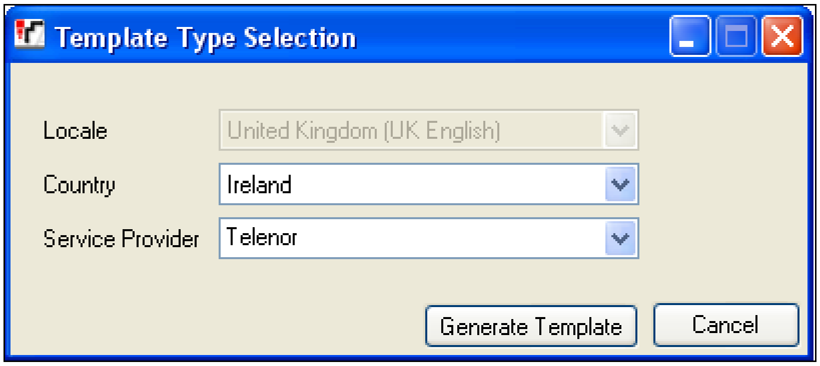


To create a SIP Line Template from the configuration, on the left Navigation Pane, right click on the Sip Line (**18**), and select **Generate SIP Trunk Template** (not shown).

Enter a descriptive name; **Telenor** was used in the sample template. To generate the template click on **Export**.



On the next screen, **Template Type Selection**, select the **Country**, enter the name for the **Service Provider** and click **Generate Template**.



The following is an example of the exported SIP Line Template file.


```xml
<?xml version="1.0" encoding="utf-8" ?>
<Template xmlns="urn:SIPTrunk-schema">
<TemplateType>SIPTrunk</TemplateType>
<Version>20130725</Version>
<SystemLocale>eng</SystemLocale>
<DescriptiveName>Telenor</DescriptiveName>
<ITSPDomainName>ipt.Telenor.com</ITSPDomainName>
<SendCallerID>CallerIDNone</SendCallerID>
<ReferSupport>true</ReferSupport>
<ReferSupportIncoming>2</ReferSupportIncoming>
<ReferSupportOutgoing>2</ReferSupportOutgoing>
<RegistrationRequired>false</RegistrationRequired>
<UseTelURI>false</UseTelURI>
<CheckOOS>false</CheckOOS>
<CallRoutingMethod>1</CallRoutingMethod>
<OriginatorNumber />
<AssociationMethod>SourceIP</AssociationMethod>
<LineNamePriority>SystemDefault</LineNamePriority>
<UpdateSupport>UpdateAuto</UpdateSupport>
<UserAgentServerHeader />
<CallerIDfromFromheader>false</CallerIDfromFromheader>
<PerformUserLevelPrivacy>false</PerformUserLevelPrivacy>
<ITSPProxy>10.10.3.40</ITSPProxy>
<LayerFourProtocol>SipUDP</LayerFourProtocol>
<SendPort>5060</SendPort>
<ListenPort>5060</ListenPort>
<DNSServerOne>0.0.0.0</DNSServerOne>
<DNSServerTwo>0.0.0.0</DNSServerTwo>
<CallsRouteViaRegistrar>true</CallsRouteViaRegistrar>
<SeparateRegistrar />
<CompressionMode>AUTOSELECT</CompressionMode>
<UseAdvVoiceCodecPrefs>true</UseAdvVoiceCodecPrefs>
<AdvCodecPref>G.711 ALAW 64K,G.711 ULAW 64K</AdvCodecPref>
<CallInitiationTimeout>4</CallInitiationTimeout>
```

<DTMFSupport>**DTMF_SUPPORT_RFC2833**</DTMFSupport>
<VoipSilenceSupression>**false**</VoipSilenceSupression>
<ReinviteSupported>**true**</ReinviteSupported>
<FaxTransportSupport>**FOIP_T38**</FaxTransportSupport>
<UseOffererPrefferedCodec>**false**</UseOffererPrefferedCodec>
<CodecLockdown>**false**</CodecLockdown>
<Rel100Supported>**true**</Rel100Supported>
<T38FaxVersion>**2**</T38FaxVersion>
<Transport>**UDPTL**</Transport>
<LowSpeed>**0**</LowSpeed>
<HighSpeed>**0**</HighSpeed>
<TCFMethod>**Trans_TCF**</TCFMethod>
<MaxBitRate>**FaxRate_14400**</MaxBitRate>
<EflagStartTimer>**2600**</EflagStartTimer>
<EflagStopTimer>**2300**</EflagStopTimer>
<UseDefaultValues>**false**</UseDefaultValues>
<ScanLineFixup>**true**</ScanLineFixup>
<TFOPEnhancement>**true**</TFOPEnhancement>
<DisableT30ECM>**false**</DisableT30ECM>
<DisableEflagsForFirstDIS>**false**</DisableEflagsForFirstDIS>
<DisableT30MRCompression>**false**</DisableT30MRCompression>
<NSFOverride>**false**</NSFOverride>
<SIPCredentials>
<Expiry>**60**</Expiry>
<RegistrationRequired>**true**</RegistrationRequired>
</SIPCredentials>
</Template>

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.