Avaya Solution & Interoperability Test Lab

Application Notes for Avaya IP Office 11 and Avaya Session Border Controller for Enterprise 8.0 with Optus Evolve Voice SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Avaya IP Office 11 and Avaya Session Border Controller (Avaya SBCE) 8.0 with Optus Evolve Voice.

The Optus Evolve Voice provides PSTN access via a SIP trunk connected to the Optus Voice over Internet Protocol (VoIP) network as an alternative to legacy analogue or digital trunks. Optus 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 any 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.

Table of Contents

1. Introduction

These Application Notes describe the procedures for configuring Avaya IP Office and Avaya Session Border Controller for Enterprise with Optus Evolve Voice SIP Trunking service. Customers using this Avaya SIP-enabled enterprise solution with Optus Evolve Voice 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 R11.0 and Avaya Session Border Controller for Enterprise 8.0 to connect to the Optus Evolve Voice. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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

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

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

For the testing associated with this Application Note, the interface between Avaya systems and the Optus Evolve Voice do not include use of any specific encryption features.

2.1 Interoperability Compliance Testing

The compliance testing was based on the standard Avaya GSSCP test plan. The testing covered functionality required for compliance as a solution supported on the Optus Evolve Voice network. Calls were made to and from the PSTN across the Optus Evolve Voice network. The following standard features were tested as part of this effort:

- PSTN incoming and outgoing calls to/from various phone types supported by Avaya IP Office including H.323, SIP, analog and digital stations; and Avaya Equinox Softphone.
- Passing of DTMF events and their recognition by navigating Interactive Voice Response menus.
- PBX features such as hold, resume, conference and transfer.
- G.711A and G.729A audio codecs.
- Network Call Redirection.
- Dialing plan including local 8-digit number and 10-digit Full Nation Number (FNN), international number.
- Caller ID presentation and restriction.
- Faxing (T.38 fallback to G.711).
- Mobility: forwarding and mobile twining.

2.2 Test Results

Interoperability testing of Optus Evolve Voice SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

Please refer to the test case document for a complete list of solution issues found when tested.

- **Faxing** – Optus Evolve Voice supports Fax t.38 fallback to G.711 mode. At the time of compliance testing, there are circumstances t.38 was successfully negotiated between Optus Evolve Voice and Avaya Aura, but there is no t.38 fax data transmitted toward Avaya IP Office. Optus should continue investigating the issue from Optus Evolve Voice network to understand the issue.
- **Calling Party Number Restriction** – the Privacy header is not included in the outbound SIP INVITE when IP Office user uses WITHHOLD feature (or *67 short code) to make outbound call via SIP trunk. This results in pilot number is displayed on PSTN phone. In order to hide calling party number for outbound call via SIP trunk, Anonymous option should be checked under SIP tab of IP Office user configuration.
- **Off-net call forwarding** does not present original calling party number on the forward target. The pilot number is presented.
- **Transfer** – Original caller ID is not presented to transfer target in blind transfer scenario. While REFER is disabled, IP Office does not include the Diversion header in the outbound INVITE to transfer target, thus there is no original caller ID presented to transfer target.
- **Emergency '000' Services Limitations and Restrictions** – Although Optus provides Emergency Services dialing on '000", Optus does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with Optus Evolve SIP Trunking Service to complete '000' calls; therefore, it is the customer's responsibility to ensure proper operation with its equipment/software vendor.
  While the Optus Evolve SIP Trunking Service does support '000' calling capabilities under certain Calling Plans, there are circumstances when that '000' service may not be available. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the customer's location in the automatic location information database.
- **REFER must be disabled** on the Avaya IP Office SIP trunk to the Optus Evolve Voice Service as Optus Evolve Voice does not support REFER.

2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com
- **Optus:** Customers should contact their Optus Business representative or follow the support links available on http://www.optus.com.au

3. Reference Configuration

The reference configuration used in these Application Notes is shown in the diagram below and consists of several components.

- Avaya IP Office Application Server running on VMware ESXi 6.0.
- Avaya IP Office 500 V2.
- Avaya IP phones are represented with Avaya 9600 Series IP Telephones running SIP / H.323 software, Avaya 1600 Series IP Telephones running H.323 software
- Avaya Communicator for Windows 3.5.
- Avaya 1400 Series Digital Telephones.
- The Avaya SBCE 8.0 provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the Optus Evolve Voice Service and the enterprise internal network.
- Optus Evolve Voice Service provided one trunk group. DID range assigned by Optus for this testing: 02xxxxx3xx (10 digits).

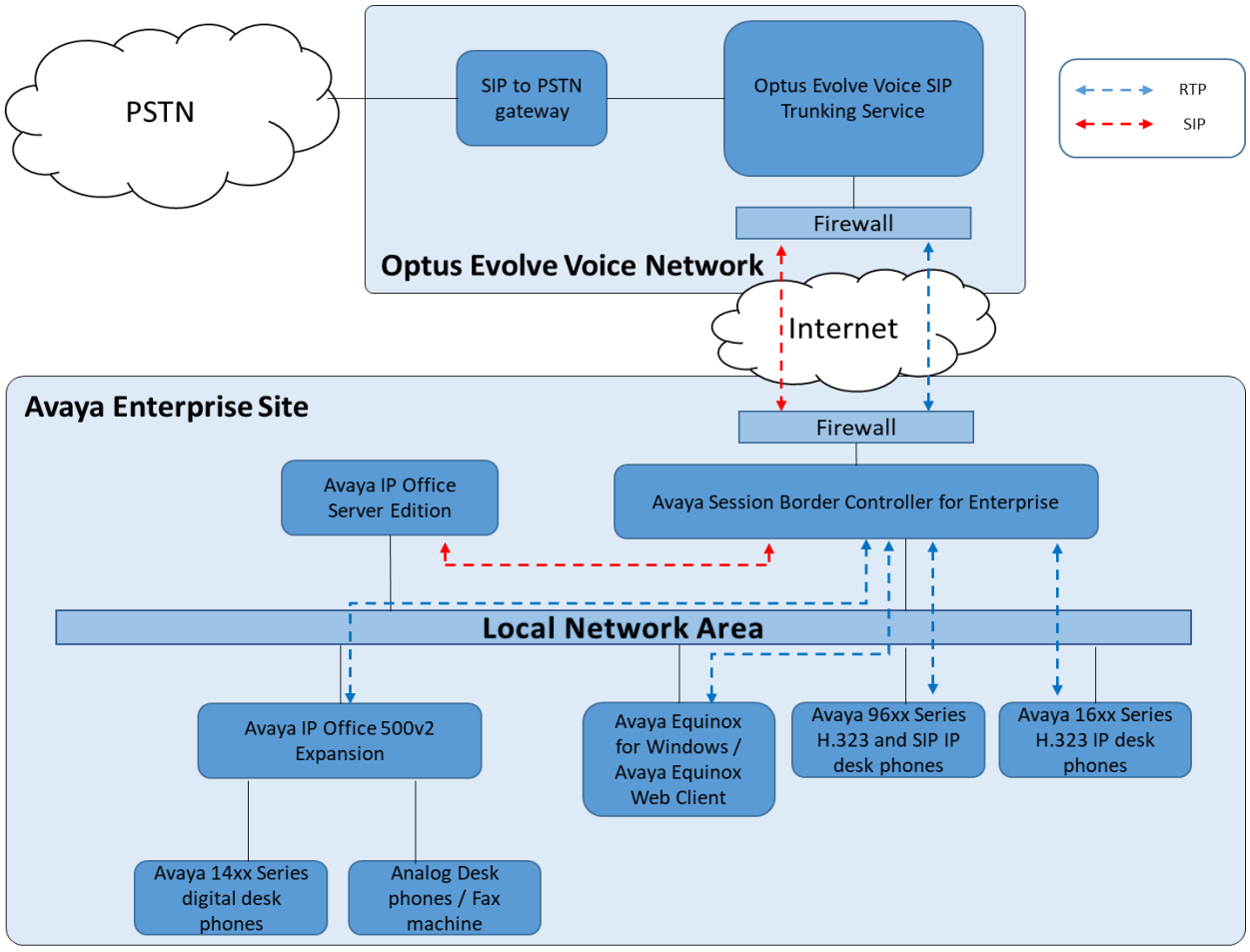


Figure 1: Test Setup Optus Evolve Voice to Avaya Enterprise

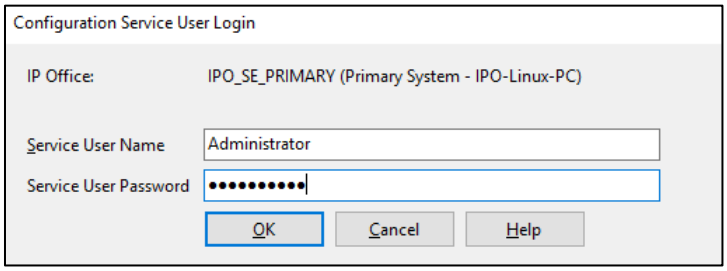
4. Equipment and Software Validated

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

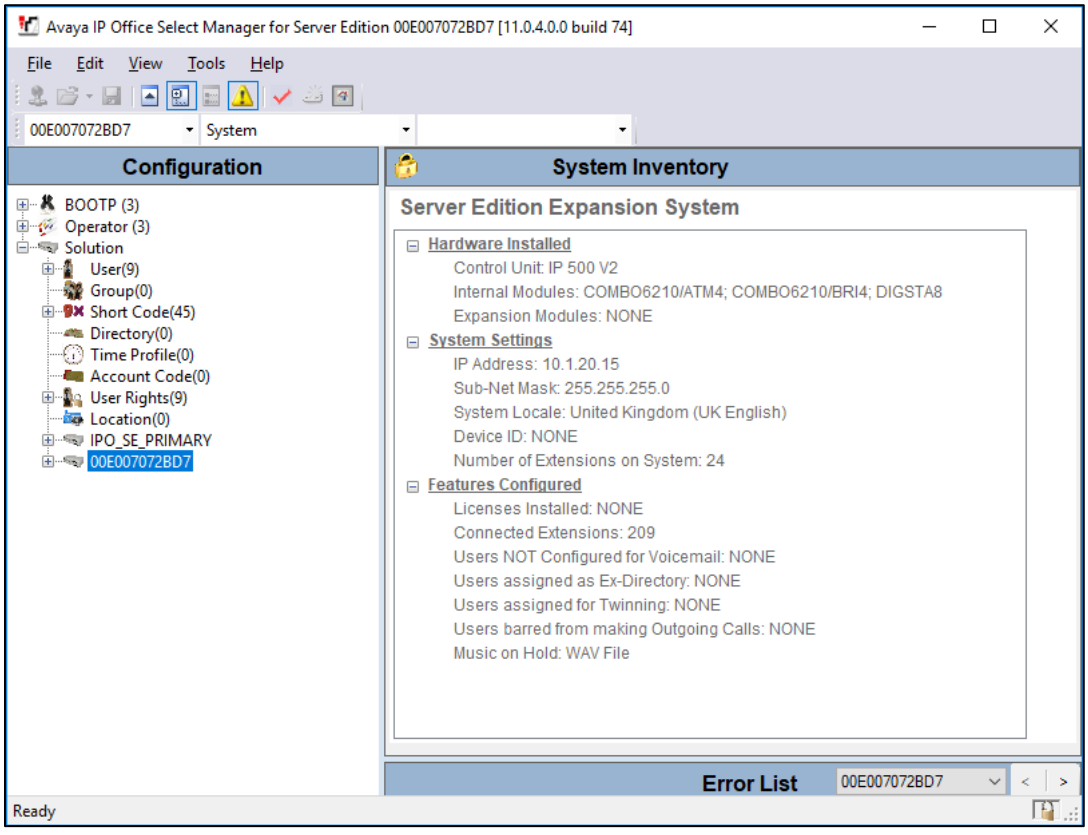
Component	Version
Avaya	
Avaya IP Office Server Edition 11	11.0.4.0.74
Avaya IP Office 500 v2	11.0.4.0.74
Avaya Session Border Controller for Enterprise 8.0	8.0 - 8.0.0.0-19-16991
Avaya Equinox for Windows 3.5	3.5.7.30.1
Avaya 96x1 series – SIP phone	7.1.5
Avaya 96xx series – H.323 phone	3.2.8
Avaya 16xx series – H.323 phone	1.3.12
Service Provider – Optus Evolve Voice	
Genband CS2000	Release 18
Acme Packet SBC	SCZ7.2.0 MR-2 GA (Build 252)

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to Avaya SBCE. 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.

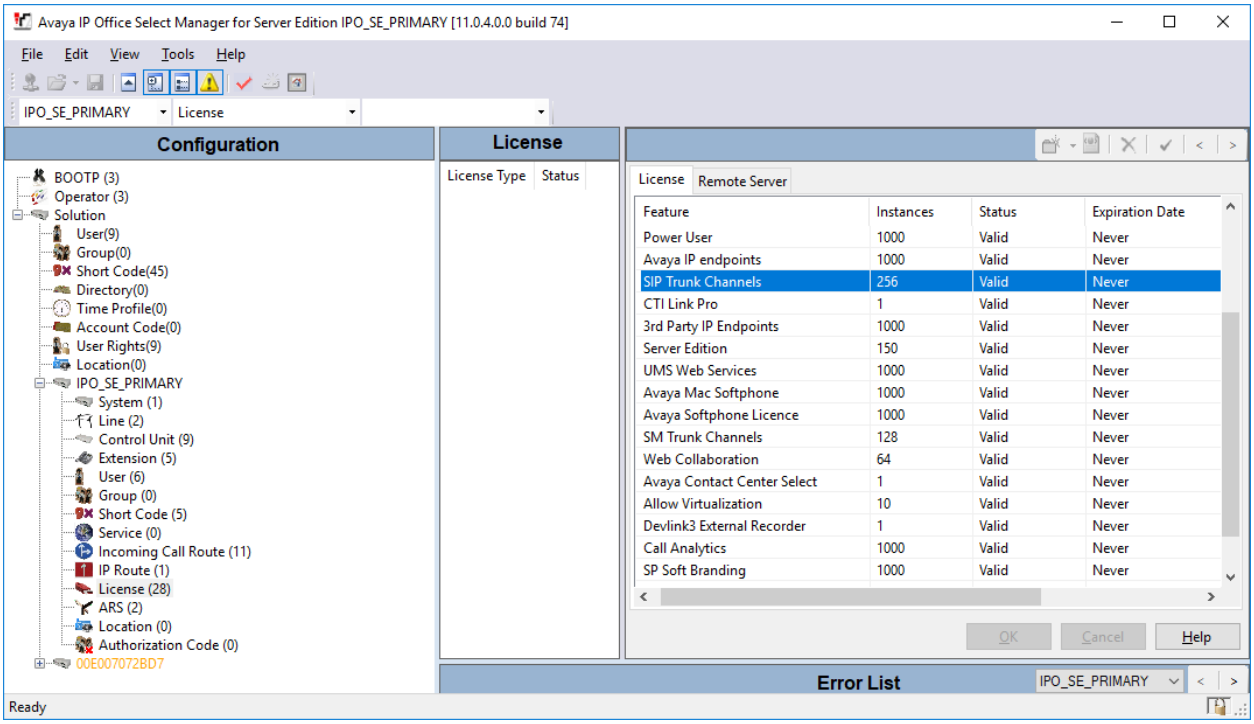


A management window will appear similar to the one in the next section. All the Avaya IP Office configurable components are shown in the left pane known as the Navigation Pane. The pane on the right is the Details Pane. These panes will be referenced throughout the Avaya IP Office configuration. All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



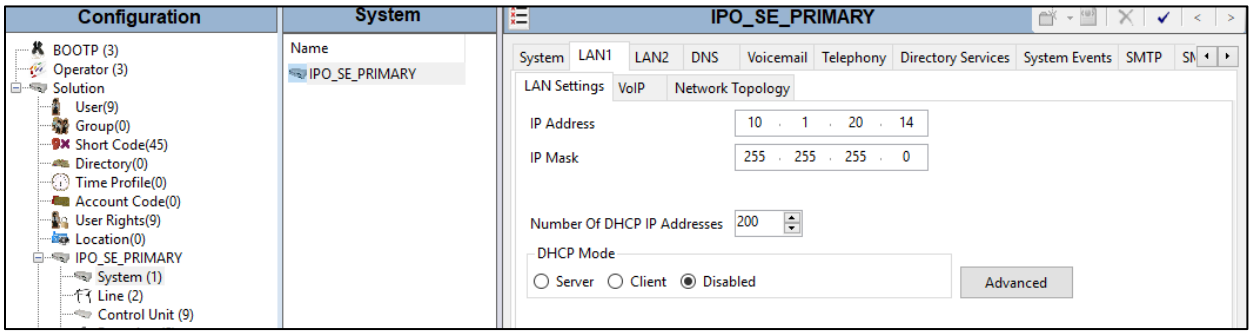
5.1 Verify System Capacity

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 SIP trunk channels provisioned by Optus Evolve Voice Services.

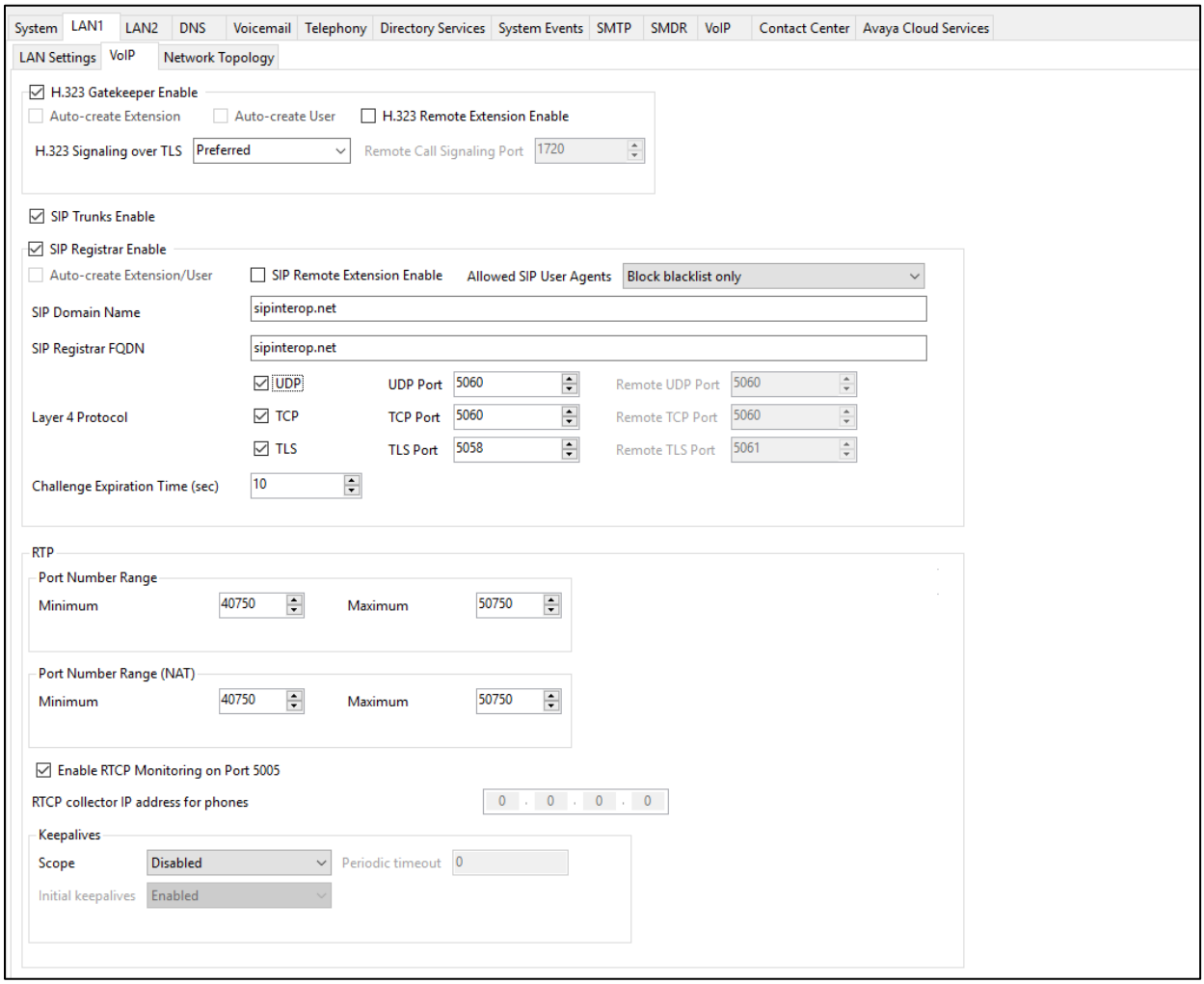


5.2 LAN1 Settings

In the sample configuration, the LAN1 port was used to connect to Avaya SBCE. To access the LAN1 settings, first navigate to **System (1) > IPO_SE_PRIMARY** in the **Navigation** and **Group** panes and then navigate to the **LAN1 > LAN Settings** tab in the **Details** pane. Set the **DHCP Mode** to **Disabled**, then set the **IP Address** field to the IP address of the Avaya IP Office LAN port. Set the **IP Mask** field to the mask used on the network. Other parameters are set as default values.

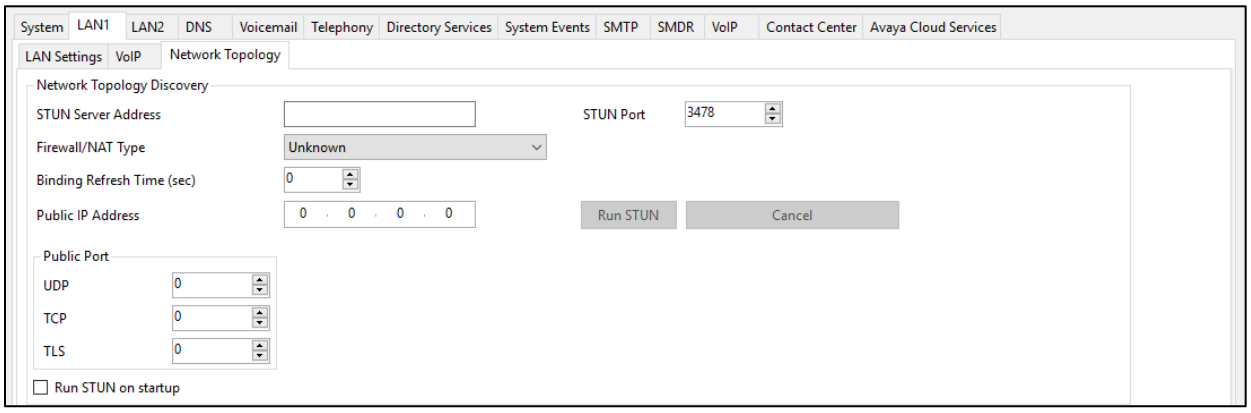


Select the **VoIP** tab as shown in the following screen. The **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the 9600-Series IP Telephones used in the sample configuration. The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks to Avaya SBCE. The **SIP Registrar Enable** box is checked to allow Avaya IP Office SIP phones usage. The **SIP Domain Name** is set to desired IP Office SIP domain. The **Layer 4 Protocol** use **UDP/TCP** with port **5060** and **TLS** with port **5061**. The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. The **Enable RTCP Monitoring on Port 5005** is checked. The specific values used for the compliance test are shown in the example below. All other parameters should be set according to customer requirements.



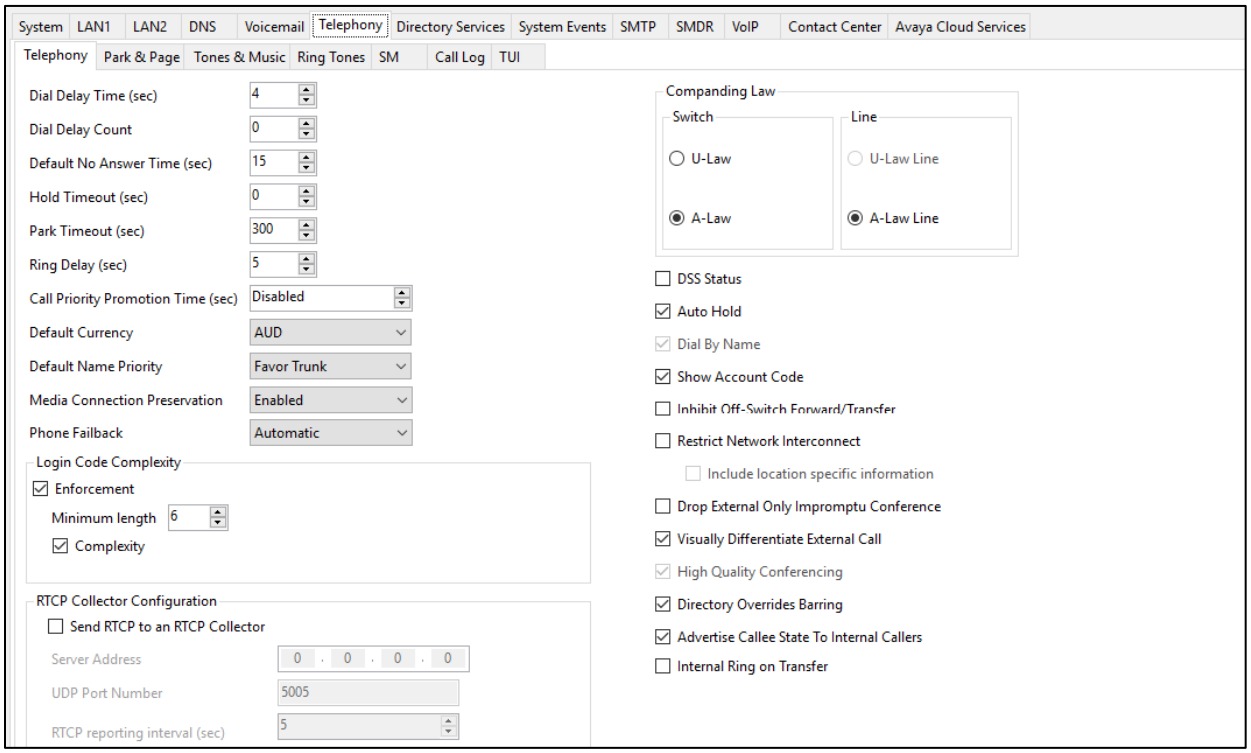
On the **Network Topology** tab in the **Details** Pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. The parameter was set to **Unknown**. All other parameters should be set according to customer requirements.



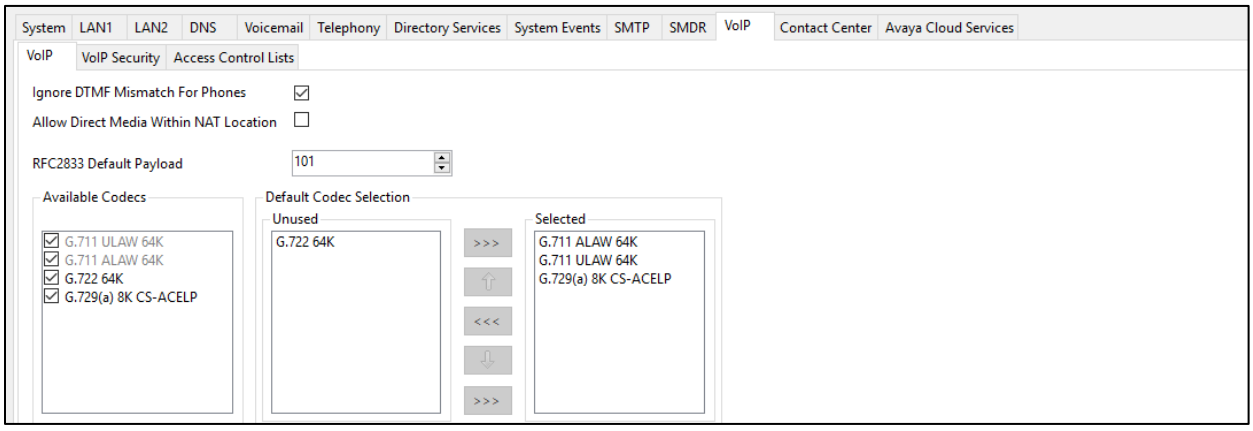
5.3 System Telephony Settings

Navigate to **System (1) > IPO_SE_PRIMARY** in the **Navigation** and **Group** panes and then navigate to the **Telephony > Telephony** tab in the **Details** pane. Choose the **Companding Law** typical for the enterprise location. For Australia, **A-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the service provider across the SIP trunk. Set **Dial Delay Time (sec)** to desired number.



5.4 VoIP Settings

Navigate to **System (1) > IPO_SE_PRIMARY** in the **Navigation** and **Group** panes and then navigate to the **VoIP** tab in the **Details** pane. Choose the **RFC2833 Default Payload** as IP Office default of **101**. Select codecs **G.711 ALAW 64K, G.11 ULAW 64K** and **G.729(a) 8K CS-ACELP** that Optus Evolve Voice supports.



5.5 SIP Line

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

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

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

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

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

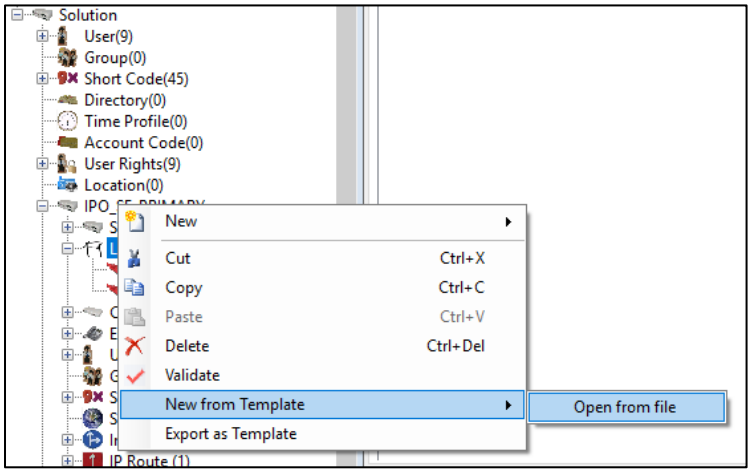
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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

5.5.1 SIP Line From Template

DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

Copy a previously created template file to a location (e.g., \temp) on the same computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the **Navigation Pane**, then navigate to **New → New from Template → Open from file**

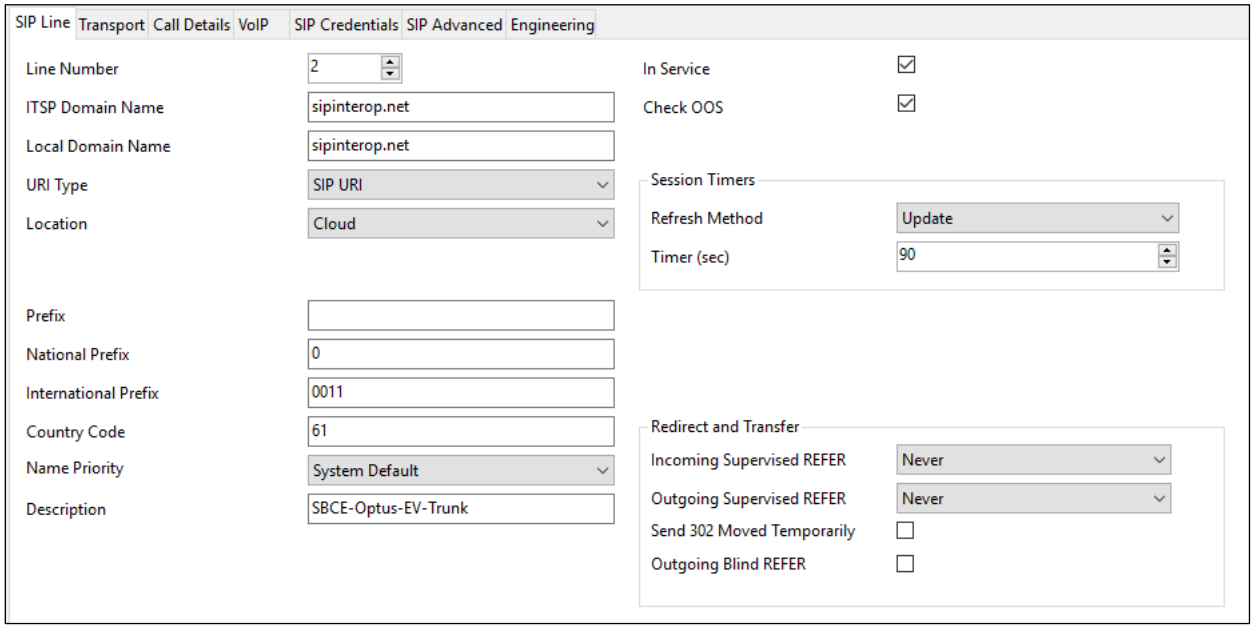


Navigate to the directory on the local machine where the template was copied and select the template (Not Shown). The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.5.2**.

5.5.2 Manual SIP Line Configuration

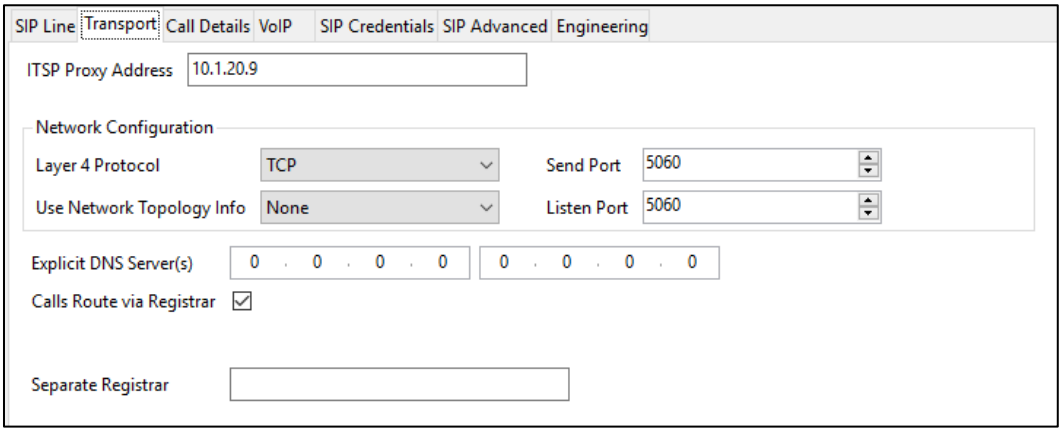
To create a SIP line, begin by navigating to **Line** in the left **Navigation** pane, then right-click in the **Group** pane and select **New > SIP Line** (not shown) and enter the desired number for **Line number** (here **2** was chosen). On the **SIP Line** tab in the **Details** pane, configure the parameters as shown below:

- Set **ITSP Domain Name** to the enterprise domain so that IP Office uses this domain as the host portion of the SIP URI in SIP headers such as the From header.
- Set **Local Domain Name** to the same domain set in **LAN1**.
- Check the **In Service** box.
- Set **URI Type** to SIP.
- Check the **Check OOS** box. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Set **Location** to **Cloud**.
- Set **Country Code** to **61** (Country Code of Australia).
- Set **International Prefix** to **0011**.
- Set **National Prefix** to **0**.
- Set **Incoming Supervised REFER** to **Never**.
- Set **Outgoing Supervised REFER** to **Never**.



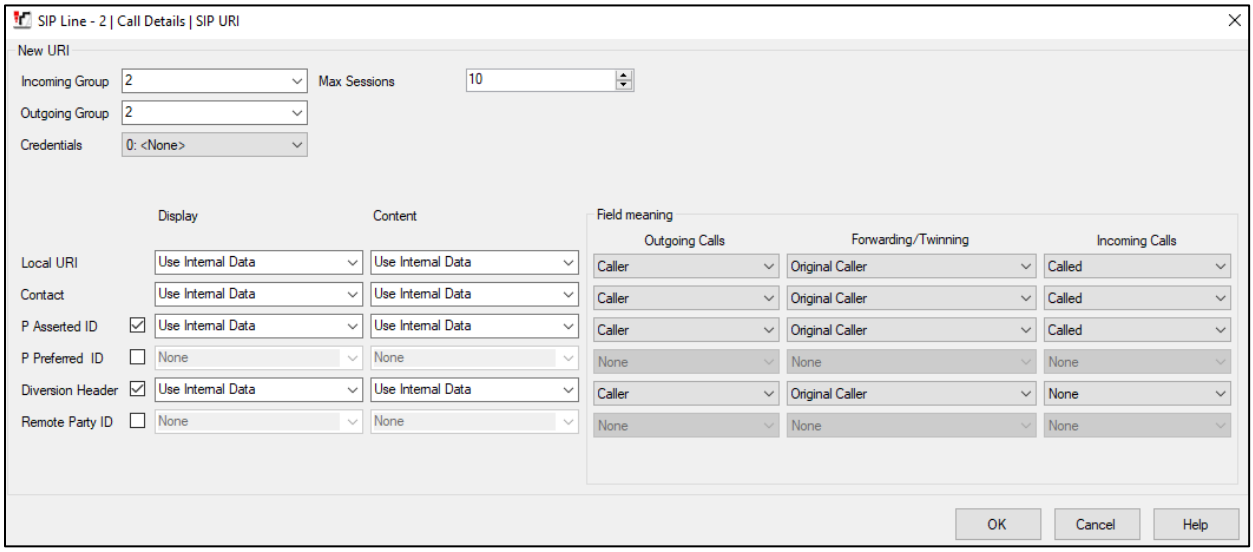
Select the **Transport** tab:

- The **ITSP Proxy Address** is set to the IP address of Avaya SBCE A1 Interface. As shown in **Figure 1**, this IP address is 10.1.20.9.
- In the **Network Configuration** area, **TCP** is selected as the Layer 4 Protocol, and the **Send Port** is set to **5060**. The **Use Network Topology Info** parameter is set to **None**. Other parameters retain default values in the screen below.
- Check **Calls Route via Registrar**.



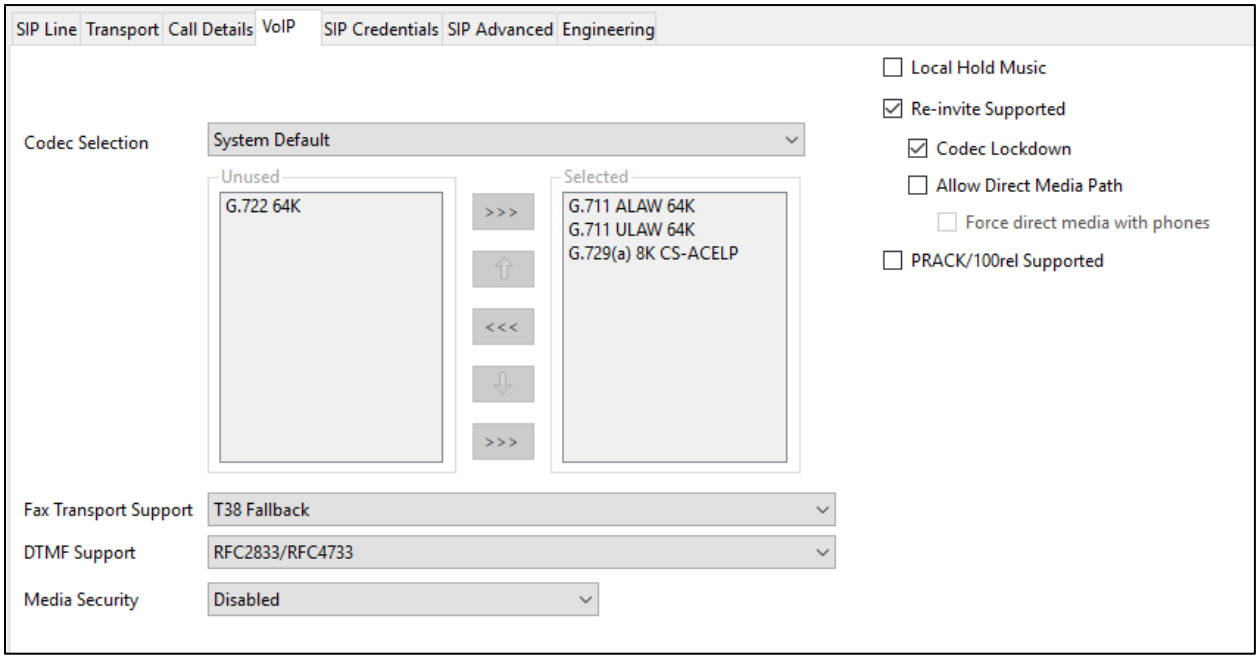
For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

- Set **Incoming Group**. This is the value assigned for incoming calls that is analyzed in the **Incoming Call Route** settings described in **Section 5.9**. In the test environment a value of **2** was used for the Optus Evolve Voice Service.
- Set **Outgoing Group**. This is the value assigned for outgoing calls that can be selected directly in the short code settings described in **Section 5.6**. In the test environment a value of **2** was used.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Set **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** to **Use Internal Data** for both the **Display name** and **Content**. On incoming calls, this will analyze the Request-Line sent by Optus Evolve Voice Service 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.
- Set the **Outgoing Calls**, **Forwarding/Twinning** and **Incoming Calls** at their respective values of **Caller**, **Original Caller** and **Called** for the **Local URI**, **Contact** and **P Asserted ID** call details. This ensures that the original called party number is sent for forwarded calls.



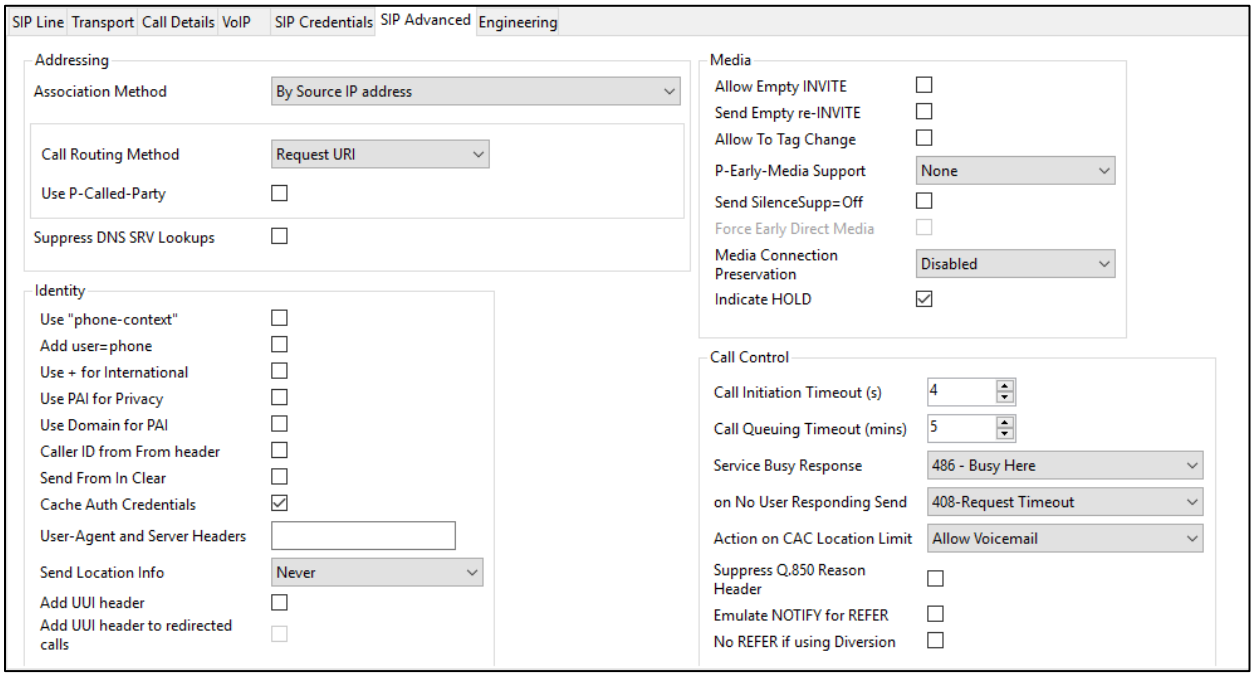
Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- The Codec Selection can be selected by choosing Custom from the pull-down menu, allowing an explicit ordered list of codecs to be specified. Selecting **G.711 ALAW 64K**, **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** codecs causes Avaya IP Office to include these codecs, which are supported by Optus Evolve Voice Service.
- Check the **Re-invite Supported** box.
- Check **Codec Lockdown** box.
- Uncheck **Allow Direct Media Path** box.
- Set **Fax Transport Support** to **T38 Fallback** from the pull-down menu as Optus Evolve Voice Service support T.38 fallback to G.711 pass-thru. At the time this testing happens, T.38 Fax is unsuccessful, the root cause is still unknown.
- Set the **DTMF Support** to **RFC2833/RFC4733** from the pull-down menu.
- Default values may be used for all other parameters.



Select **SIP Advanced** tab:

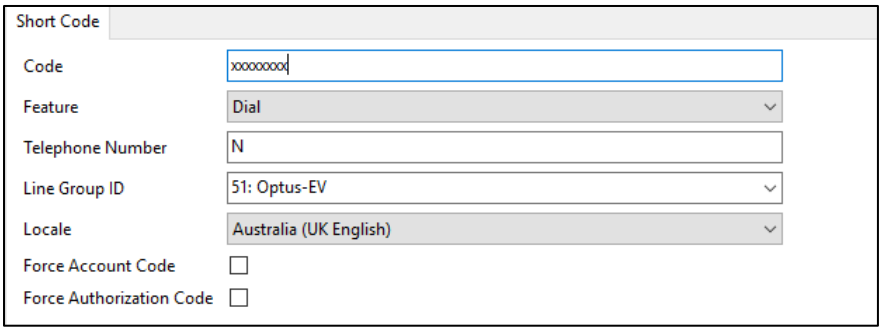
- Check **Indicate HOLD** box.
- Default values may be used for all other parameters.



5.6 Short Codes

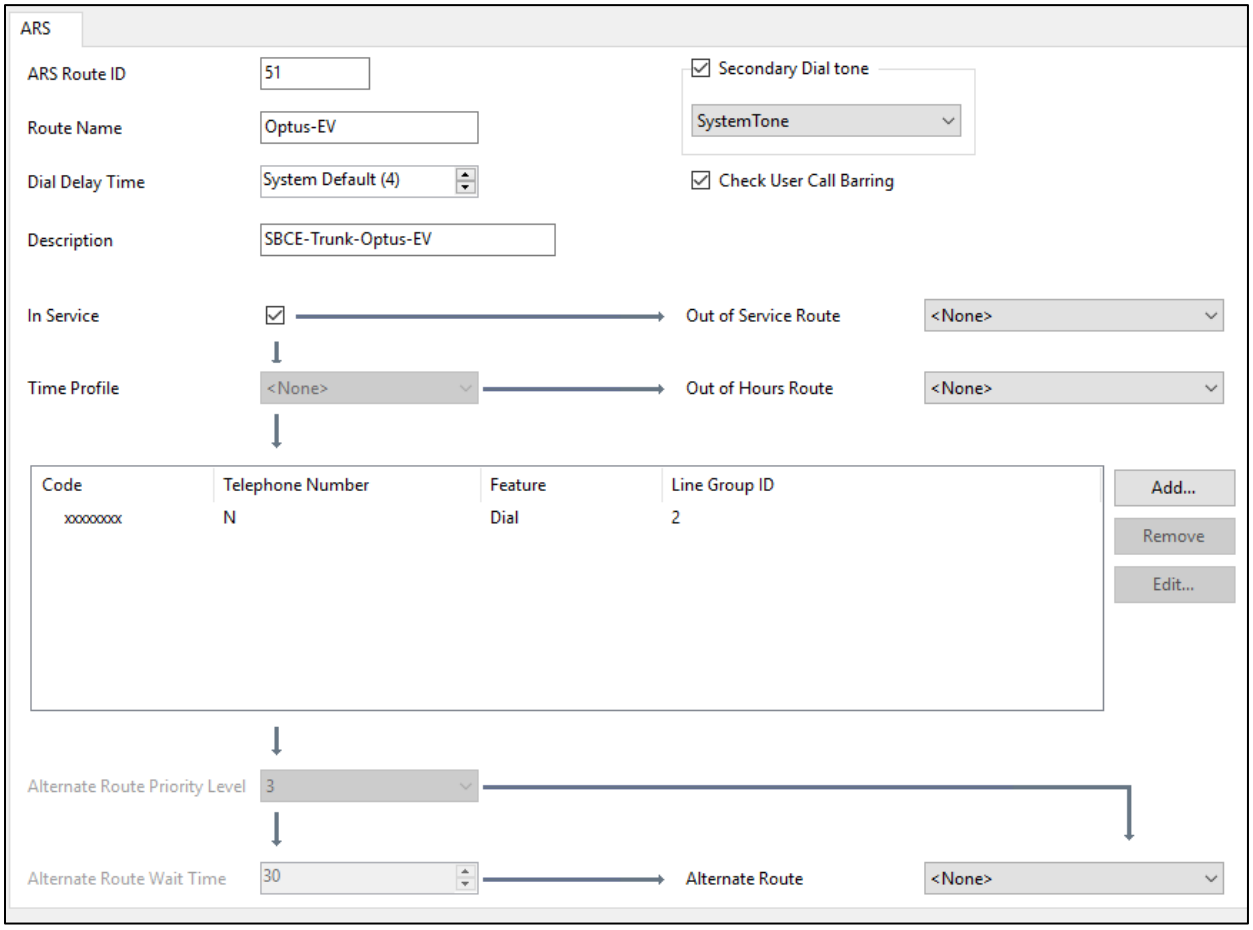
Define a short code to route outbound traffic to the SIP line. To create a short code, right-click **Short Code** in the Navigation pane and select **New** (not shown). On the **Short Code** tab in the **Details** pane, configure the parameters as shown below:

- In the **Code** field, enter the dial string which will trigger this short code. The example shows "**xxxxxxxx**" which will be invoked when the user dials any 8-digit number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to "**N**".
- Set the **Line Group Id** to **51: Optus-EV**.
- Set **Locale** to **Australia (UK English)**.



5.7 ARS table

ARS Route ID 51 was selected to route outbound calls as defined in the Short Code in **Section 5.6**. That Short Code and the SIP Line created in **Section 5.5** must be added to this ARS Route ID as shown below.

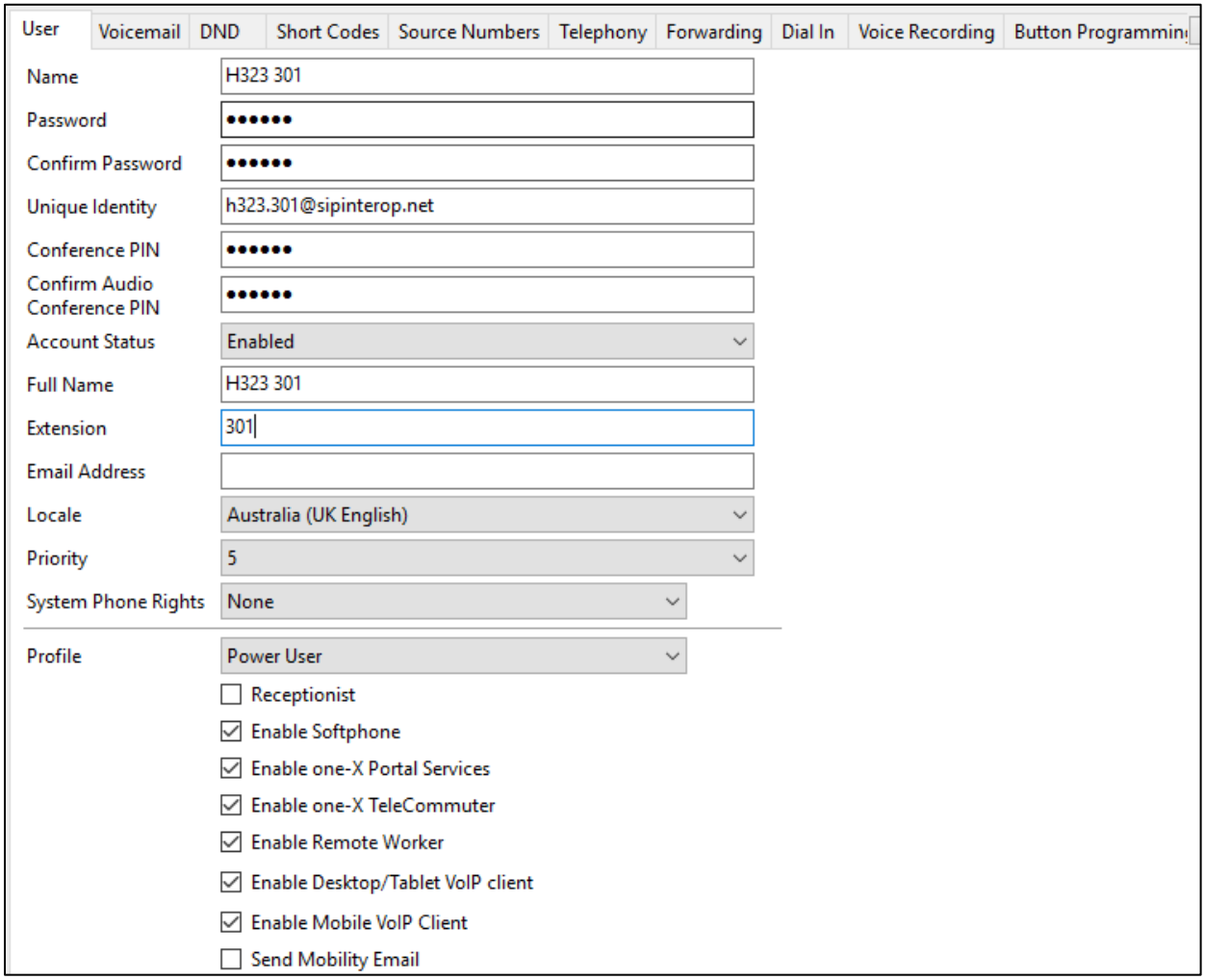


5.8 User

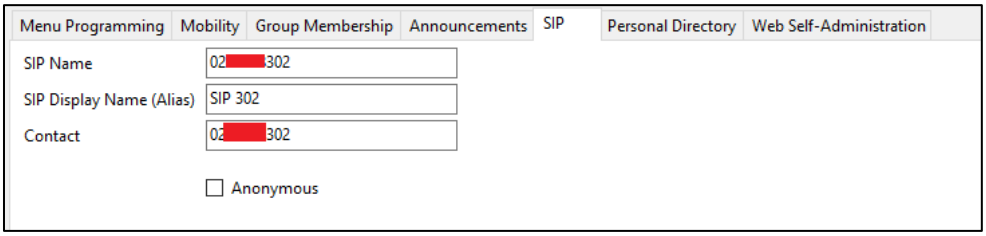
Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.5.** To configure these settings, first navigate to **User** in the Navigation Pane. Select the **User** tab if any changes are required.

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

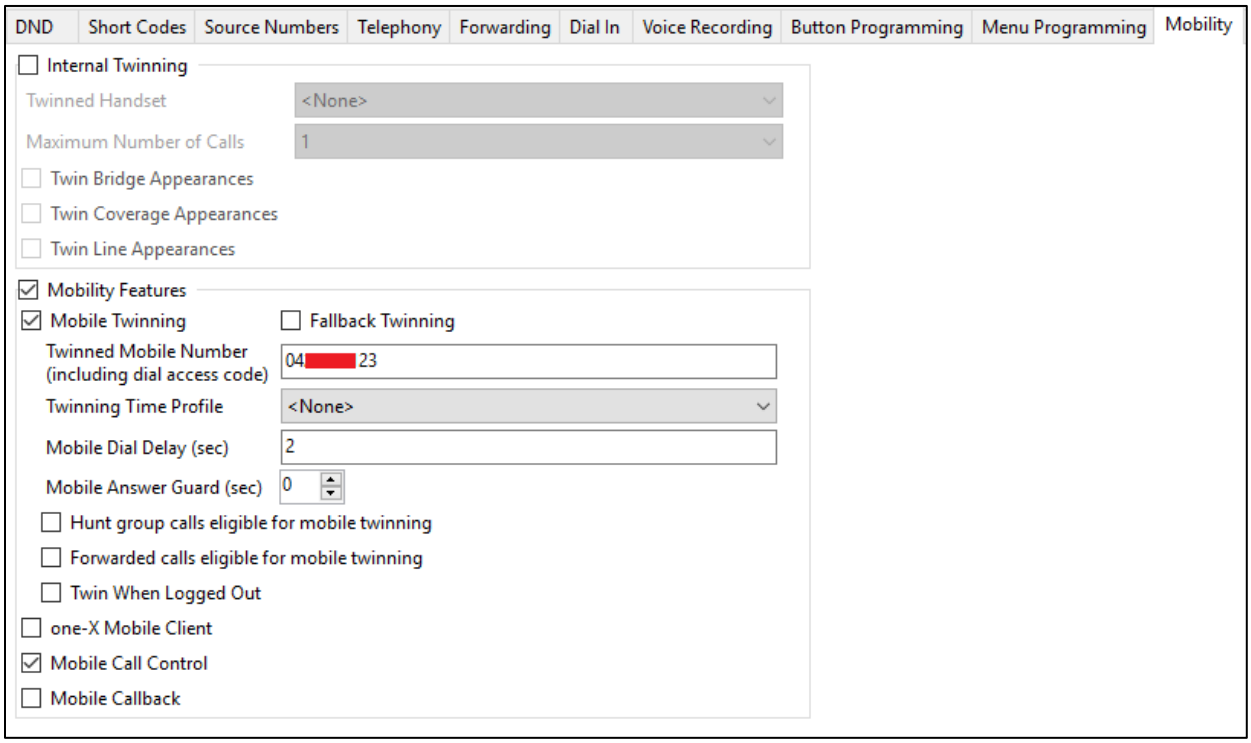
- Change the **Name** of the User if required.
- Set the **Password** and **Confirm Password**.
- Select the required profile from the **Profile** drop down menu. **Basic User** is commonly used; **Power User** can be selected for SIP softphone, WebRTC and Remote Worker endpoints.



SIP endpoints require setting of the **SIP Registrar Enable** as described in **Section 5.2**. 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/P-Asserted-Identity/Contact** header for outgoing SIP trunk calls. These allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.5.2**). As such, these fields should be set to one of the DDI numbers assigned to the enterprise from Optus Evolve Voice.



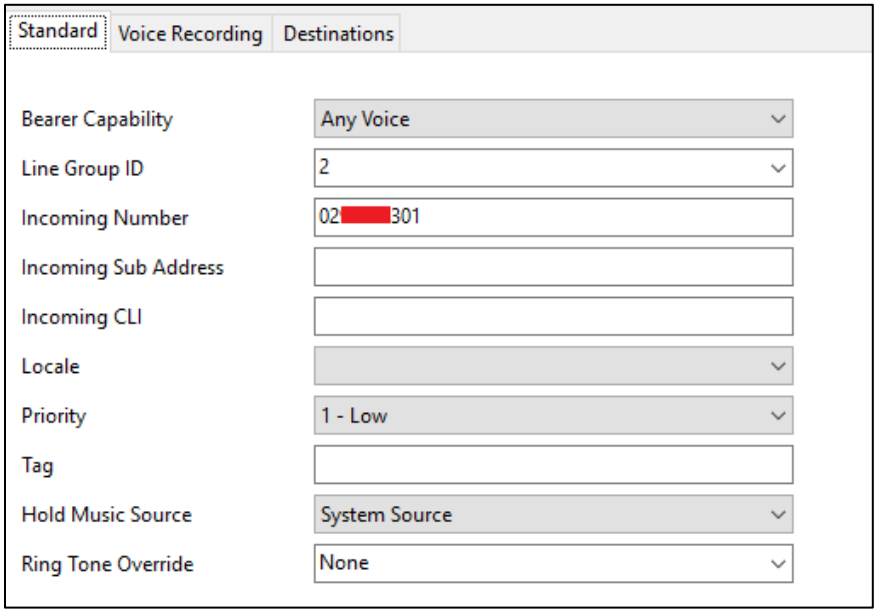
Optional: The following screen shows the **Mobility** tab for user 302. The **Mobility Features** and **Mobile Twinning** are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone over the SIP Trunk. Other options can be set accordingly to customer requirements.



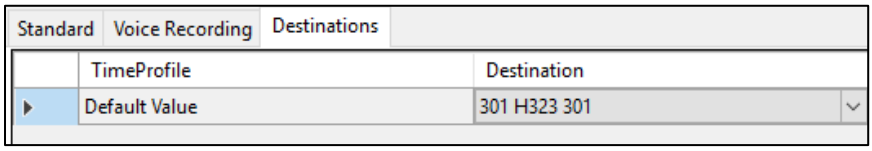
5.9 Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Routes** in the **Navigation** pane and select **New** (not shown). On the **Standard** tab of the **Details** pane, enter the parameters as shown below:

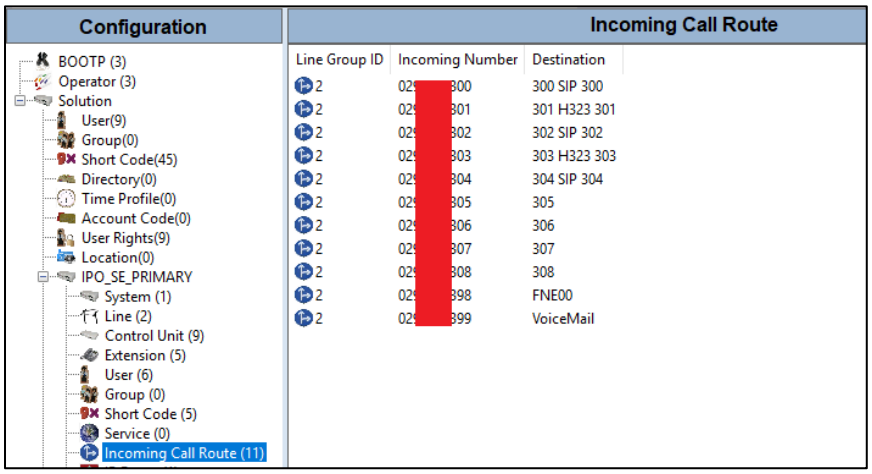
- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.5**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left. In this sample configuration, assigned DID numbers starting with 02 have been masked due to security reasons.



Select 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 DID number 02xxxxx301 on line 2 are routed to extension 301



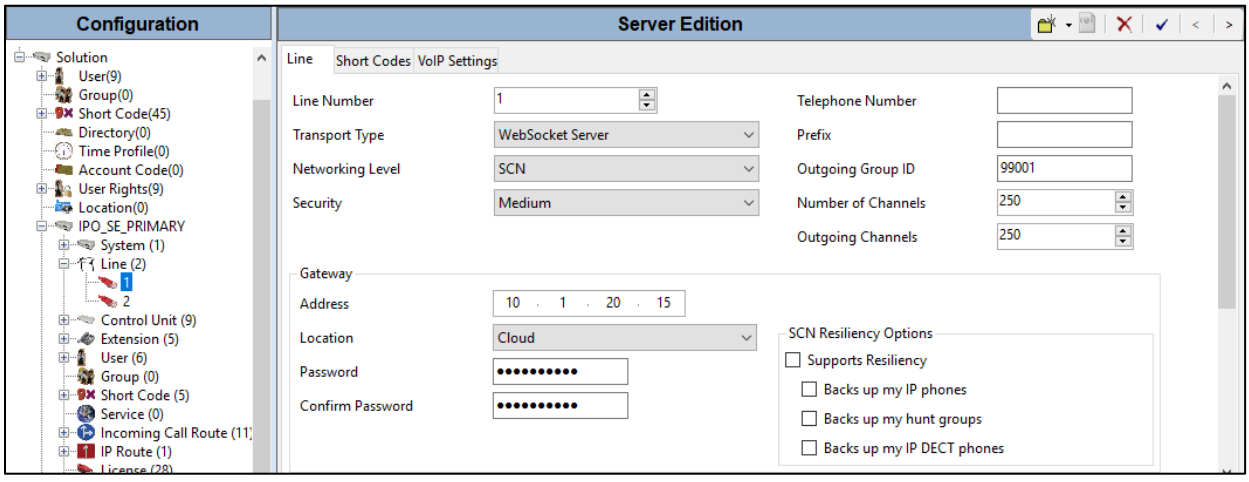
The following screen shows all the administered **Incoming Call Route** entries those are used in the compliance test



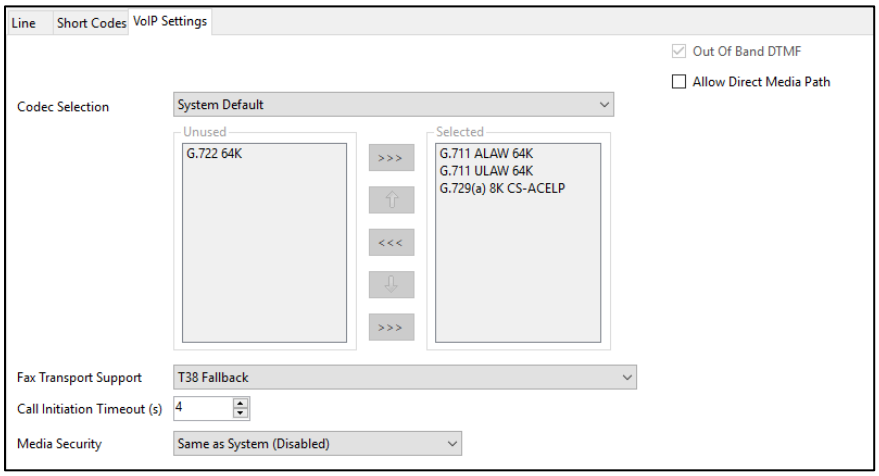
5.10 Digital, Analog and T.38 Fax Extensions

The compliance test with Optus Evolve Voice testing was also carried out with digital extensions and analog extensions including Fax machine on the IP Office Expansion. An IP Office line must be administered between IP Office Server Edition and IP Office Expansion (IP Office 500v2) with **T.38 Fallback** is configured as the fax transport

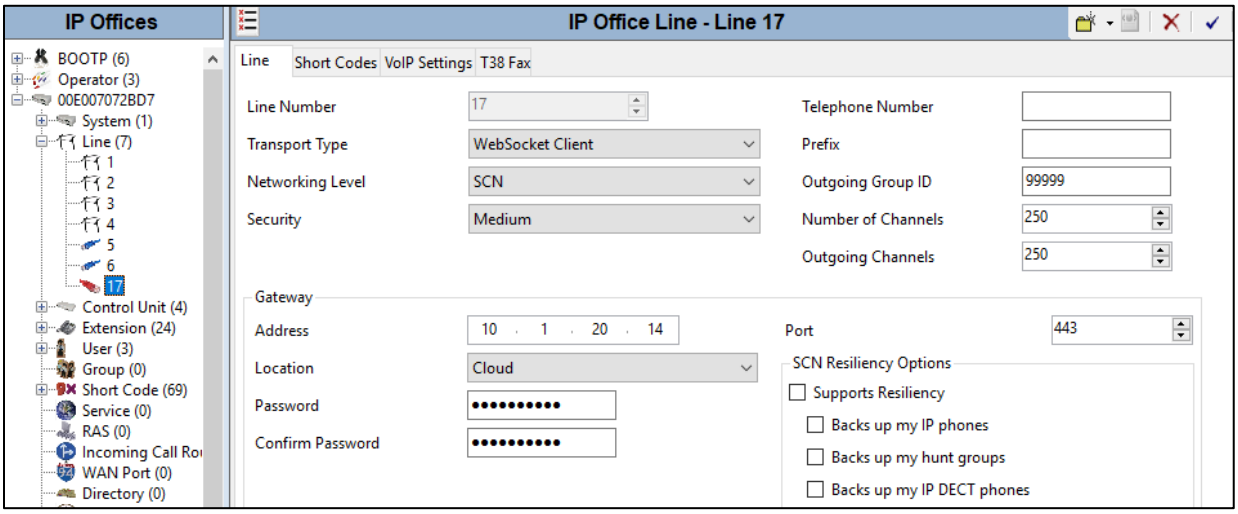
In **Line** tab, configure the **IP Office Line** as in screenshot below on the IP Office Server Edition.



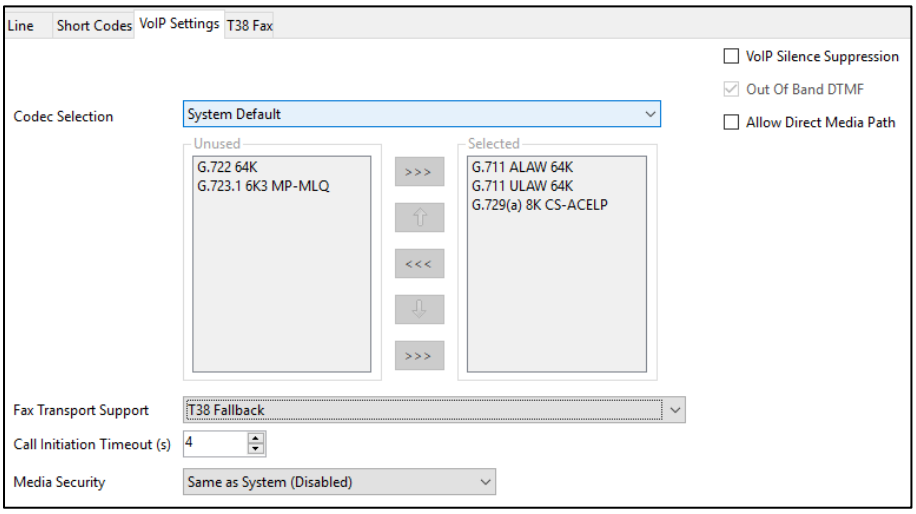
In the **VoIP Settings** tab, select **T38 Fallback** from the **Fax Transport Support** drop down menu.



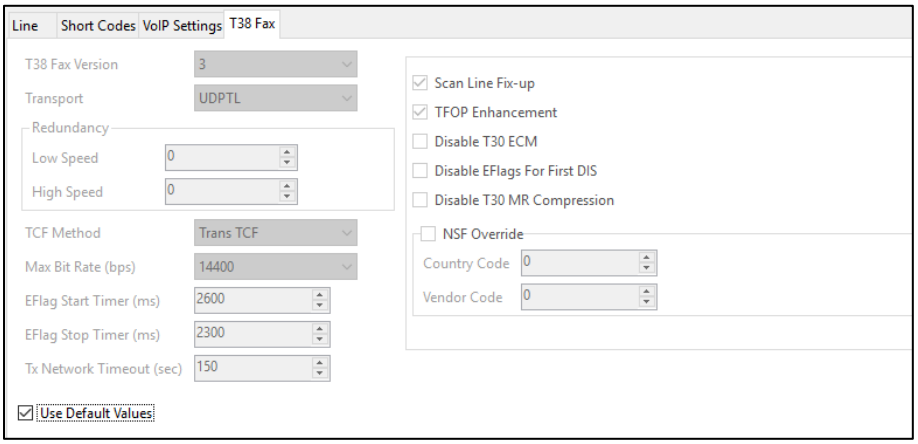
In **Line** tab, configure the **IP Office Line** as in screenshot below on the IP Office Expansion.



In the **VoIP Settings** tab, select **T38 Fallback** from the **Fax Transport Support** drop down menu.

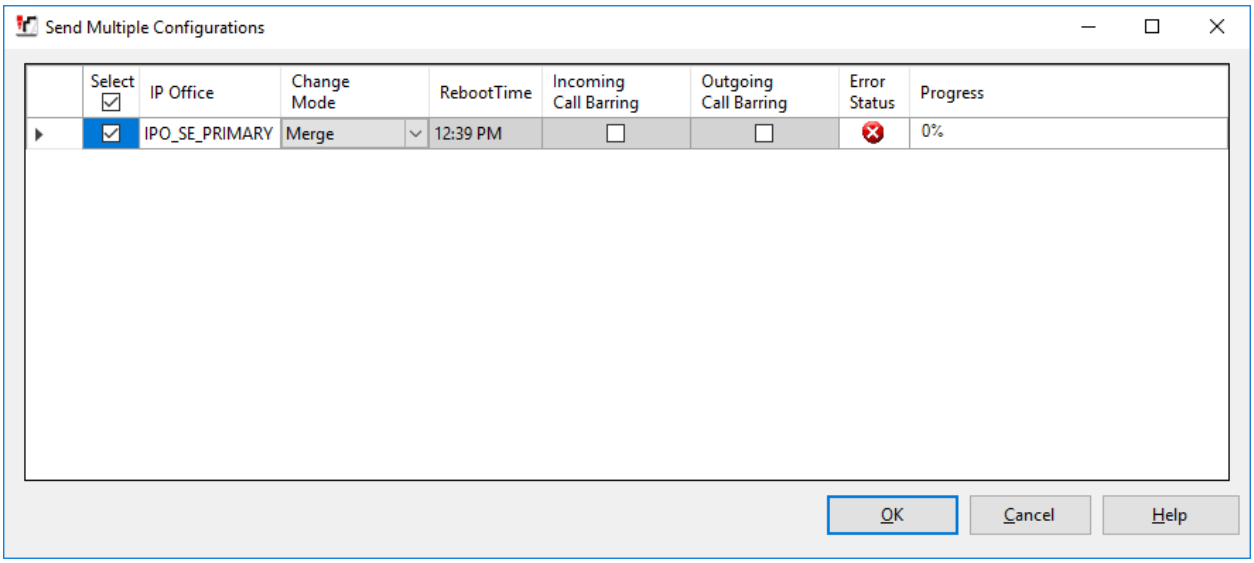


In the **T38 Fax** tab, check **Use Default Value**s.



5.11 Save Configuration

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



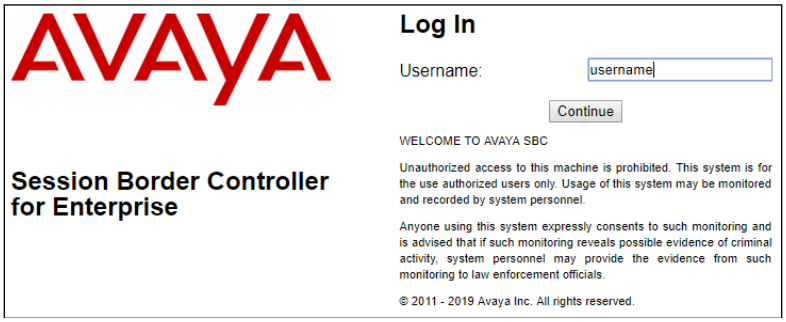
6. Configure Avaya Session Border Controller for Enterprise

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document.

IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition resolved.

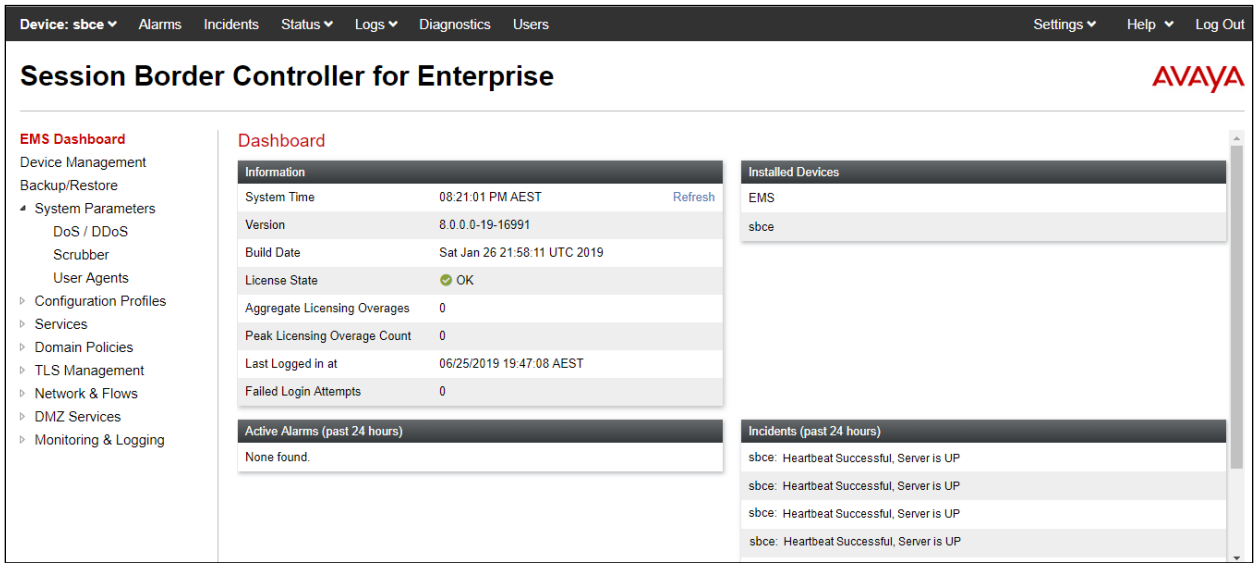
As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (10.1.20.9), with access to the **Optus** site. The connection to Optus uses the Avaya SBCE public interface B1 (IP address 192.168.1.2). The follow provisioning is performed via the Avaya SBCE GUI interface, using the "M1" management LAN connection on the chassis.

1. Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Enter the **Username** and click on **Continue**.



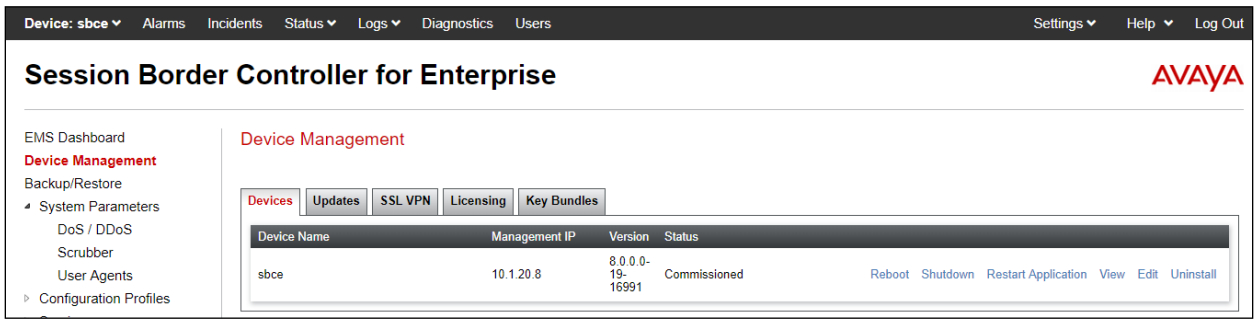
3. Enter the password and click on **Log In**.

The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

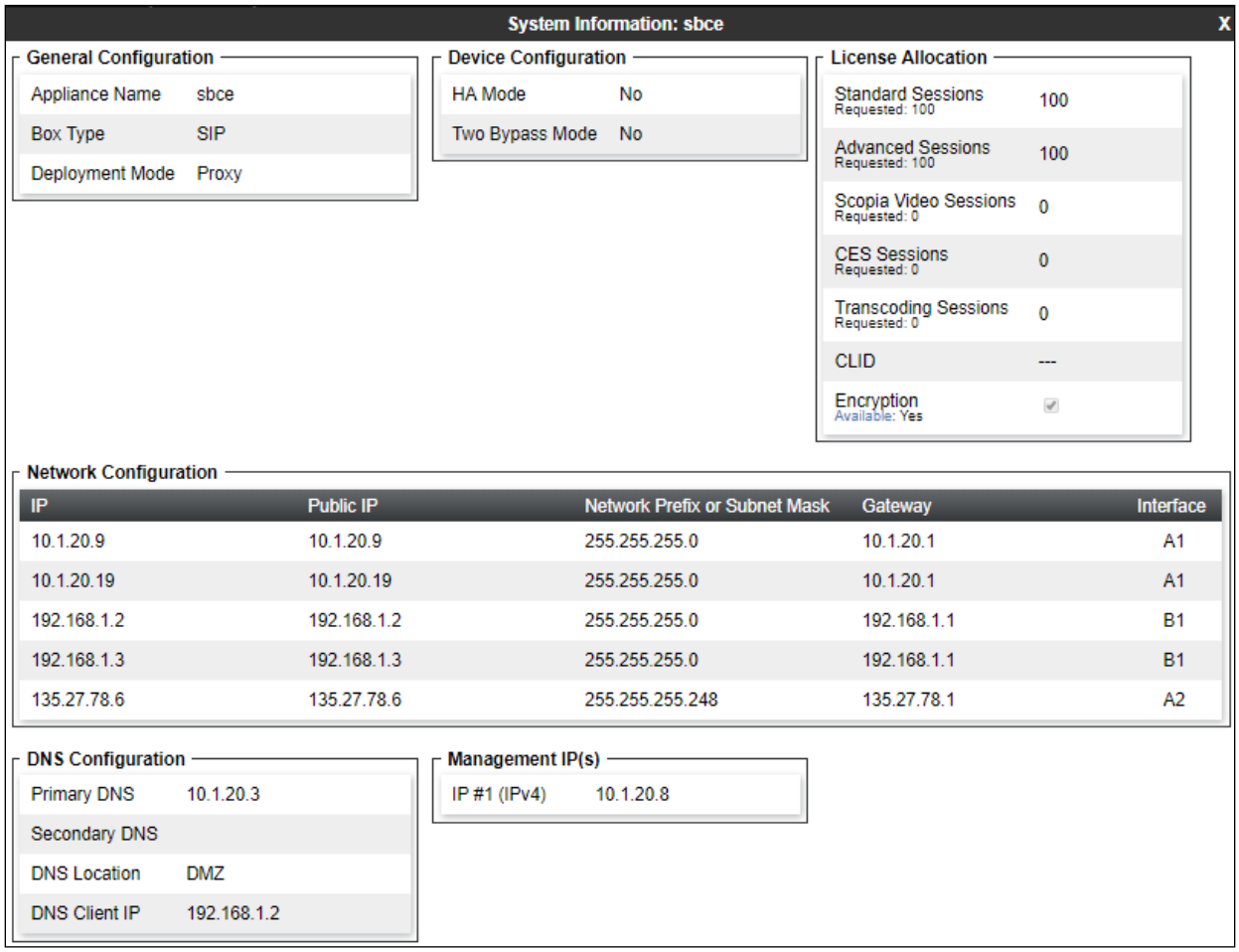


6.1 Device Management – Status

1. Select **Device Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative.



2. Click on **View** (shown above) to display the **System Information** screen. Note that DNS servers are Optus DNS servers and DNS client must be B1 IP address that is used for SIP trunk with Optus

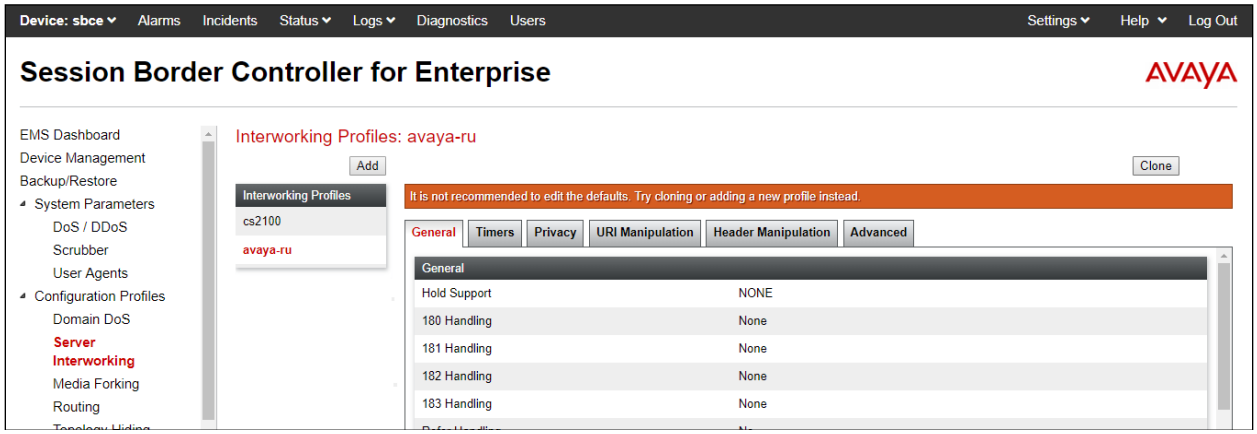


6.2 Server Interworking Profiles

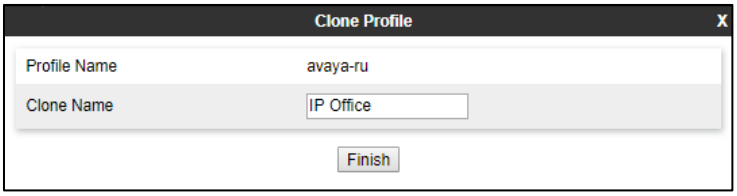
6.2.1 Server Interworking – IP Office

Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the profile for the connection to IP Office.

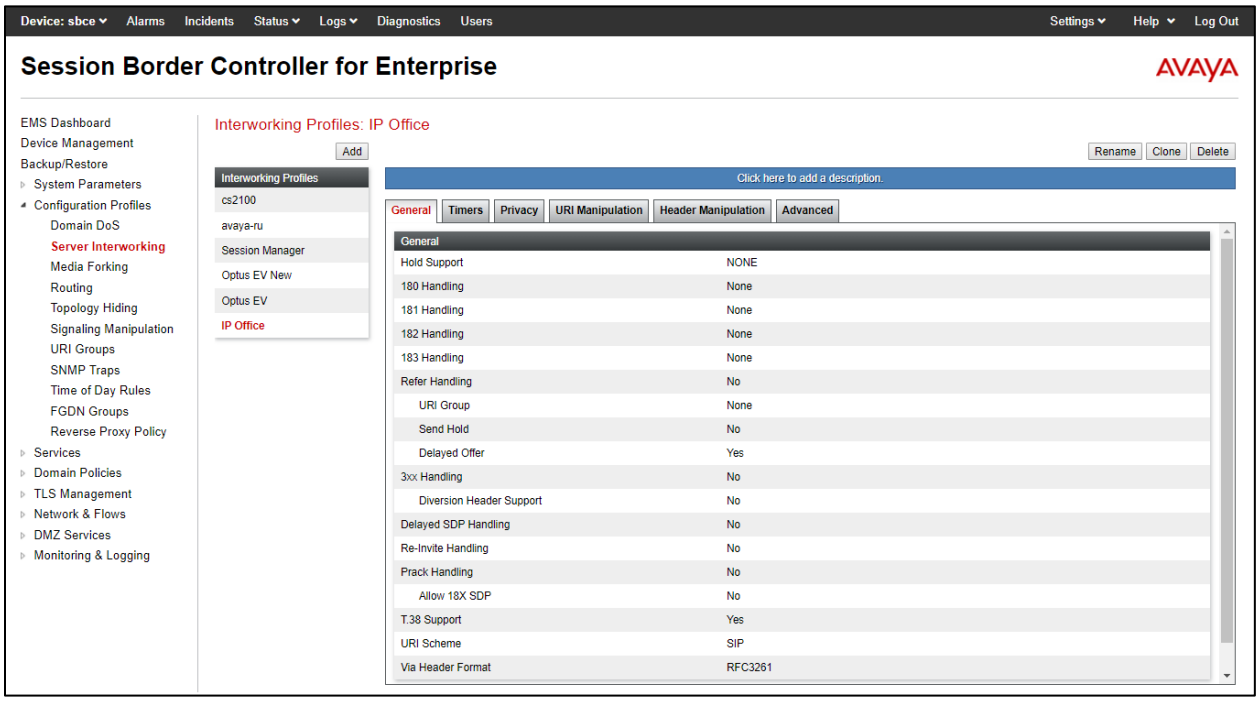
1. Select **Configuration Profiles → Server Interworking** from the left-hand menu.
2. Select the pre-defined **avaya-ru** profile and click the **Clone** button.



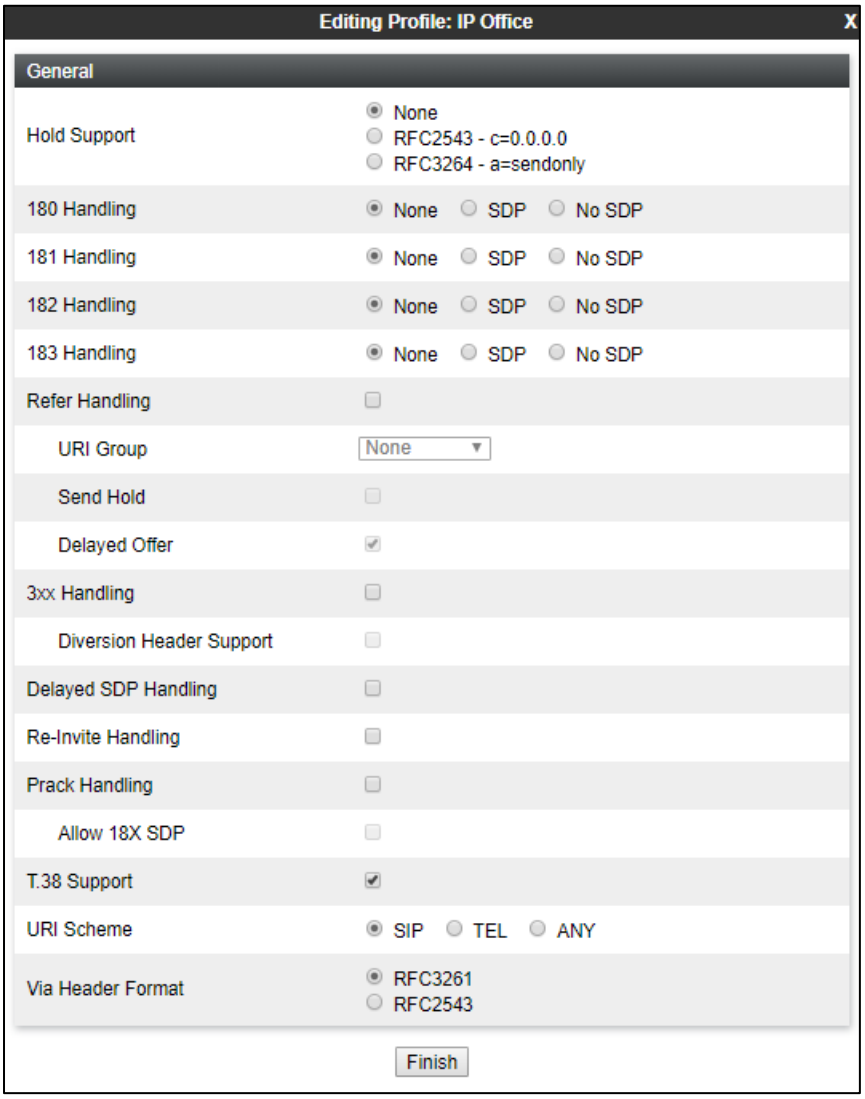
3. Enter profile name: (e.g., **IP Office**), and click **Finish**.



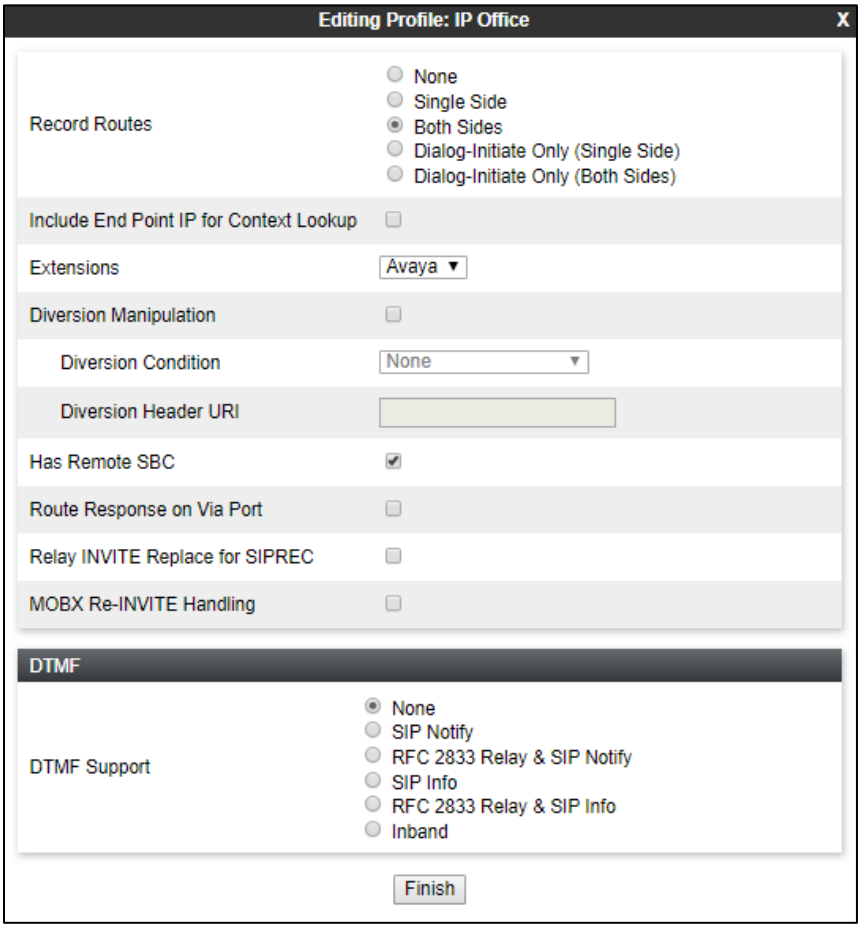
4. The new **IP Office** profile will be listed. Select it, scroll to the bottom of the Profile screen, and click on **Edit**.



5. The **General** screen will open.
   - Check **T.38 Support**.
   - All other options can be left with default values, and click **Finish**.



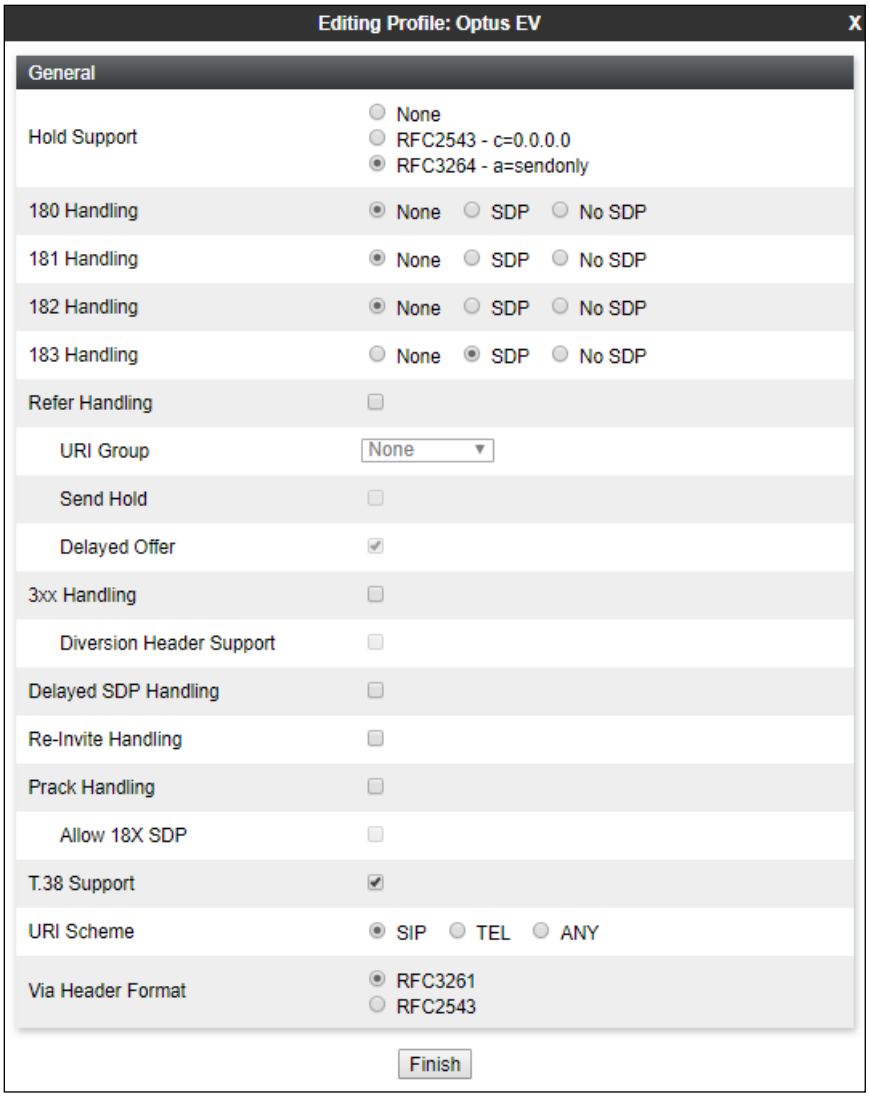
6. Leave settings in **Timer**, **Privacy**, **URI Manipulation**, **Header Manipulation** windows as default.
7. On the **Advanced** window, configure;
   - **Record Routes**: choose **Both Sides**.
   - **Has Remote SBC**: choose **Yes**.



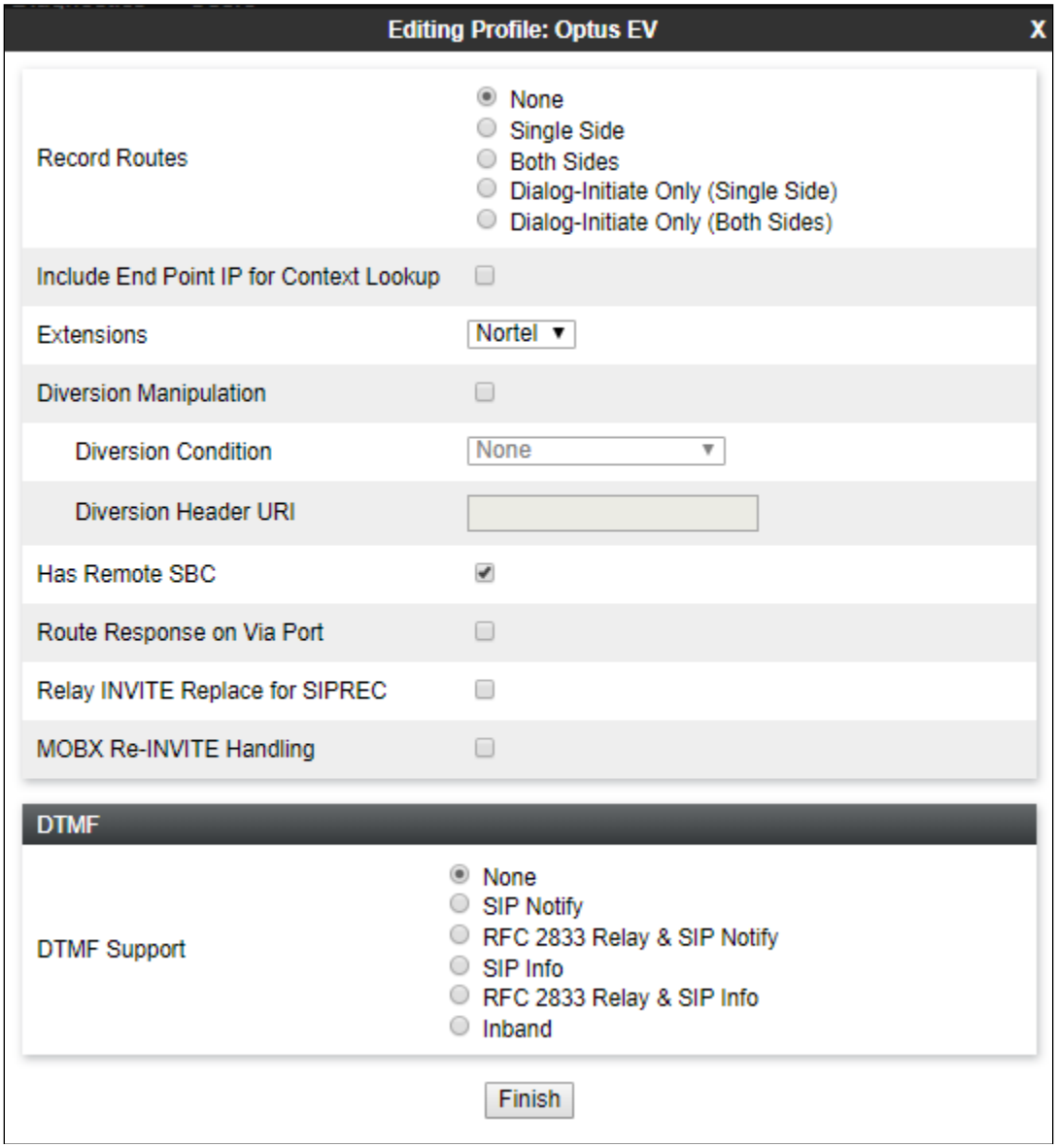
6.2.2 Server Interworking – Optus EV

Repeat the steps shown in **Section 6.2.1** to add an Interworking Profile for the connection to Optus via the public network, with the following changes:

1. Click **Add** to add a new profile, enter **Optus EV** then click **Next** (not shown).
2. The **General** screen will open:
   - Check **T.38 Support**.
   - All other options can be left as default.
   - Click **Next**.
   - The **Privacy/DTMF, SIP Timers/Transport Timers** screens will open (not shown), accept default values for all the screens by clicking **Next**.



The **Advanced** window is configured as below, click **Finish** to save the profile:

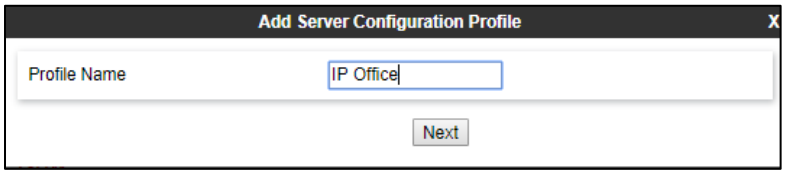


6.3 SIP Server Profiles

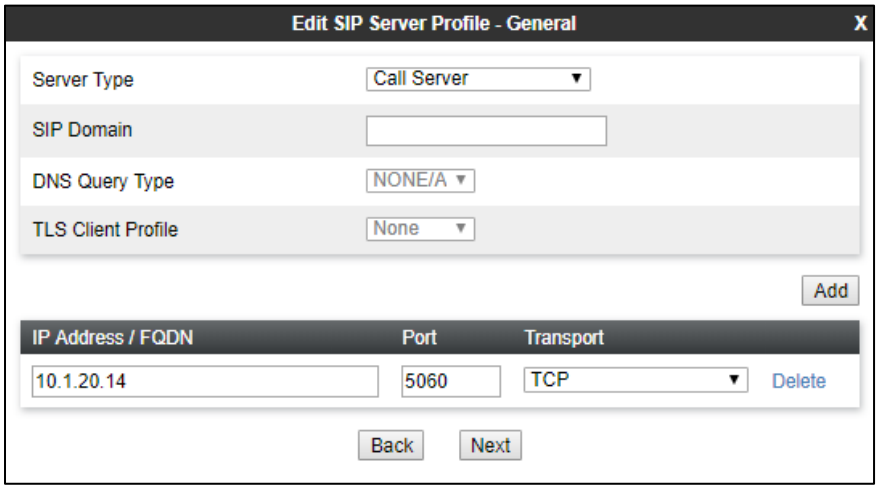
6.3.1 SIP Server – IP Office

This section defines the SIP Server Profile for the Avaya SBCE connection to IP Office.

1. Select **Services → SIP Server** from the left-hand menu.
2. Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **IP Office**) and click **Next**.

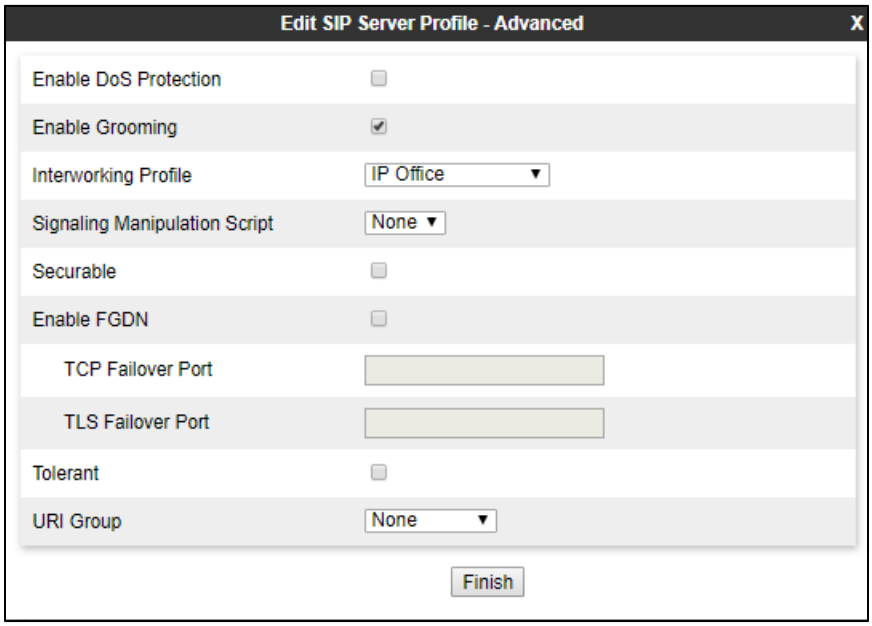


3. The **Add SIP Server Profile** window will open.
   - Select **Server Type**: **Call Server**.
   - **IP Address / FQDN**: **10.1.20.14** (IP Office Server LAN1 IP Address)
   - **Transport**: Select **TCP**.
   - **Port**: **5060**.
   - Select **Next**.



4. The **Authentication** and **Heartbeat** windows will open (not shown).
   - Select **Next** to accept default values.

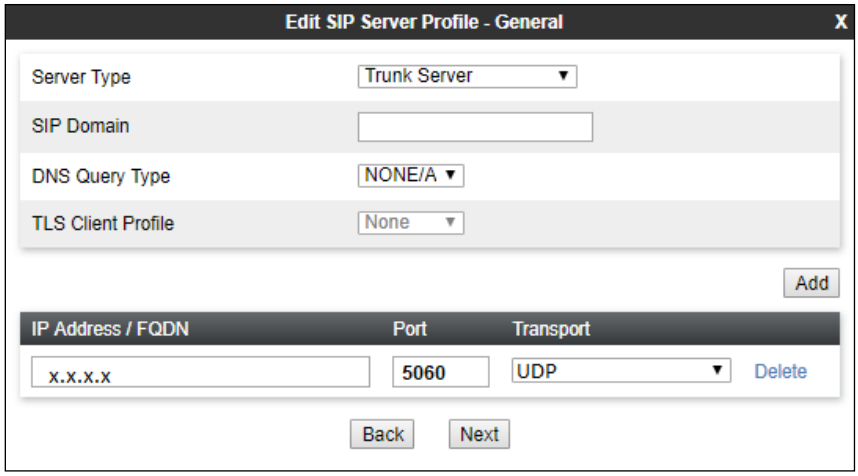
5. The **Advanced** window will open.
   - For **Interworking Profile**, select the profile created for IP Office in **Section 6.2.1**.
   - Check **Enable Grooming**.
   - Select **Finish**.



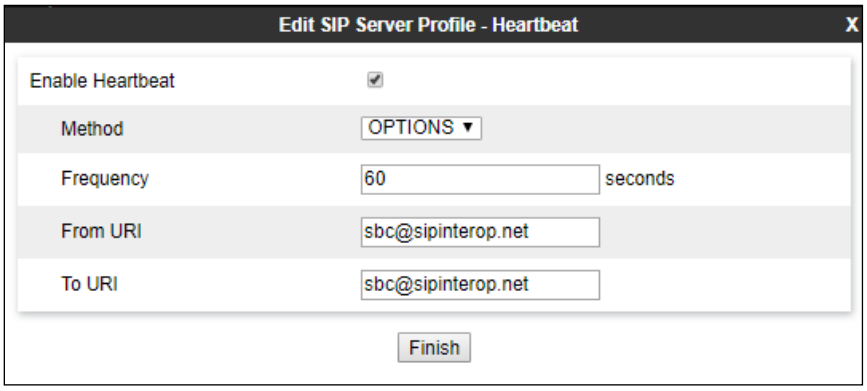
6.3.2 SIP Server – Optus EV

Repeat the steps in **Section 6.3.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to Optus EV Trunk Group.

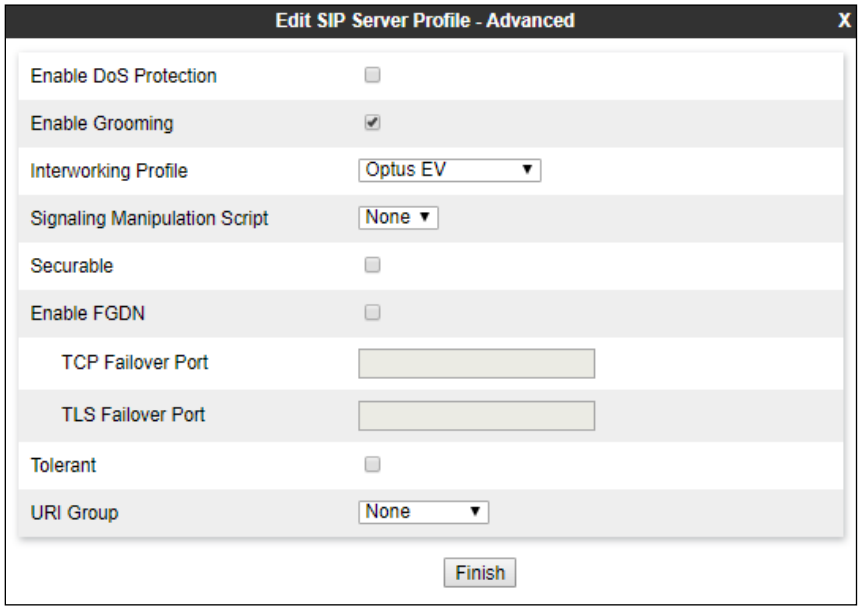
1. Select **Add Profile** and enter a Profile Name (e.g., **Optus EV**) and select **Next**.
2. On the **General** window (not shown), enter the following.
   - Select Server Type**: Trunk Server**.
   - **IP Address / FQDN: x.x.x.x** (outbound proxy of Optus).
   - **Transport**: Select **UDP**.
   - **Port: 5060**.
   - Select **Next**.



3. Under **Heartbeat** window:
   - Select **Enable Heartbeat**.
   - **Method**: choose **OPTIONS**.
   - **Frequency**: enter **60**.
   - **From URI** and **To URI**: enter **sbc@sipinterop.net**.



4. Under Advanced window:
    - Check **Enable Grooming**.
    - Select **Optus EV** for Interworking Profile.

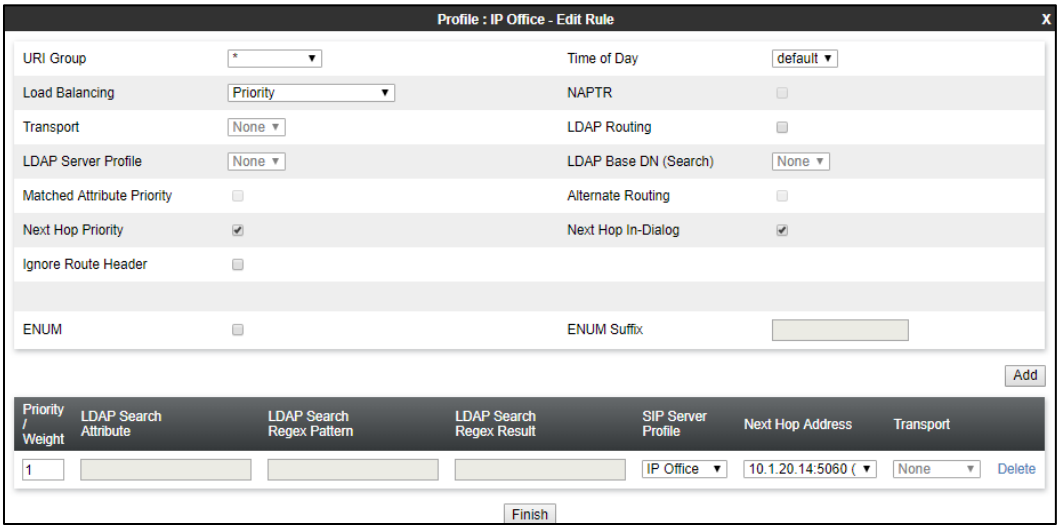


6.4 Routing Profiles

6.4.1 Routing – To IP Office

This provisioning defines the Routing Profile for the connection to IP Office.

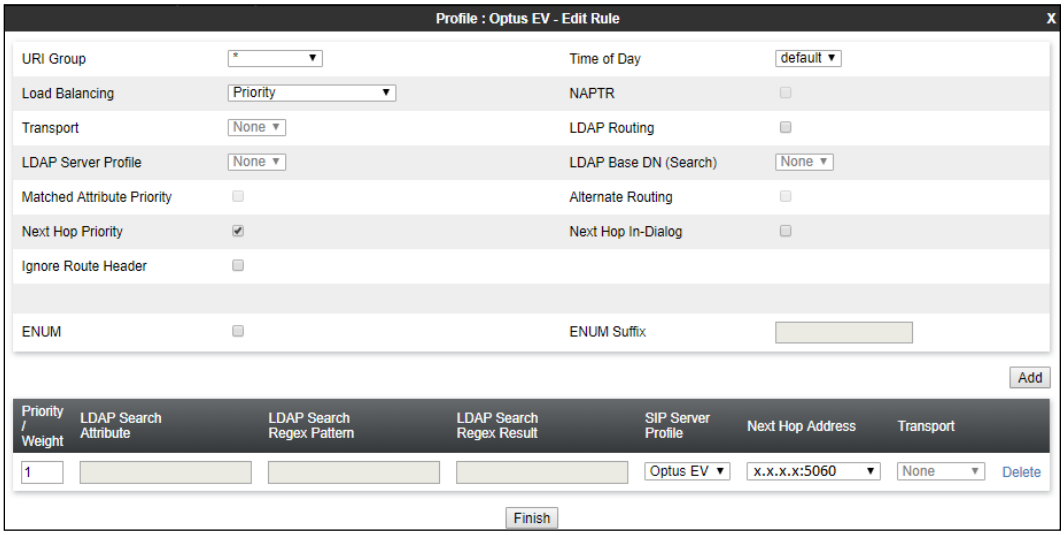
1. Select **Configuration Profiles → Routing** from the left-hand menu, and select **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **IP Office)** and click **Next**.
3. The Routing Profile window will open. Using the default values shown, click on **Add.**
4. The Next-Hop Address window will open. Populate the following fields:
   - **Priority/Weight** = **1**.
   - **SIP Server Profile** = **IP Office**.
   - **Next Hop Address:** Verify that the **10.1.20.14:5060 (TCP)** entry from the drop down menu is selected (IP Office Server LAN1 IP address). Also note that the **Transport** field is grayed out.
   - Click on **Finish**.



6.4.2 Routing – To Optus EV

Repeat the steps in **Section 6.4.1**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to Optus.

1. On the **Configuration Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **Optus EV)**.
2. Load Balancing: select **Priority**.
3. On the **Next-Hop Address** window (not shown), populate the following fields:
   - **SIP Server Profile** = **Optus EV**.
   - **Next Hop Address:** Verify that the **x.x.x.x:5060** entry from the drop down menu is selected. Also note that the **Transport** field is grayed out.
   - Use default values for the rest of the parameters.
4. Click **Finish**.

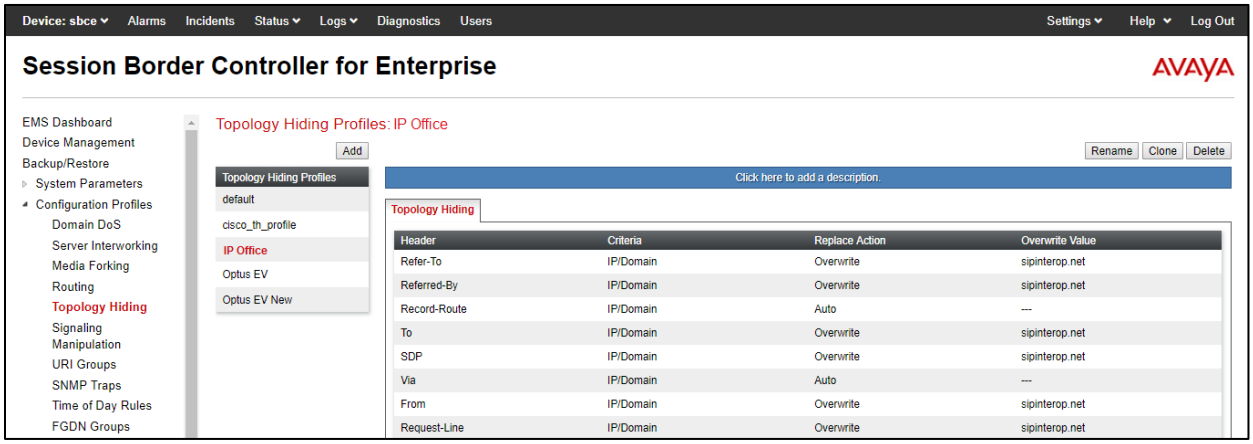


6.5 Topology Hiding

6.5.1 Topology Hiding – IP Office

The **Topology Hiding** screen allows users to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

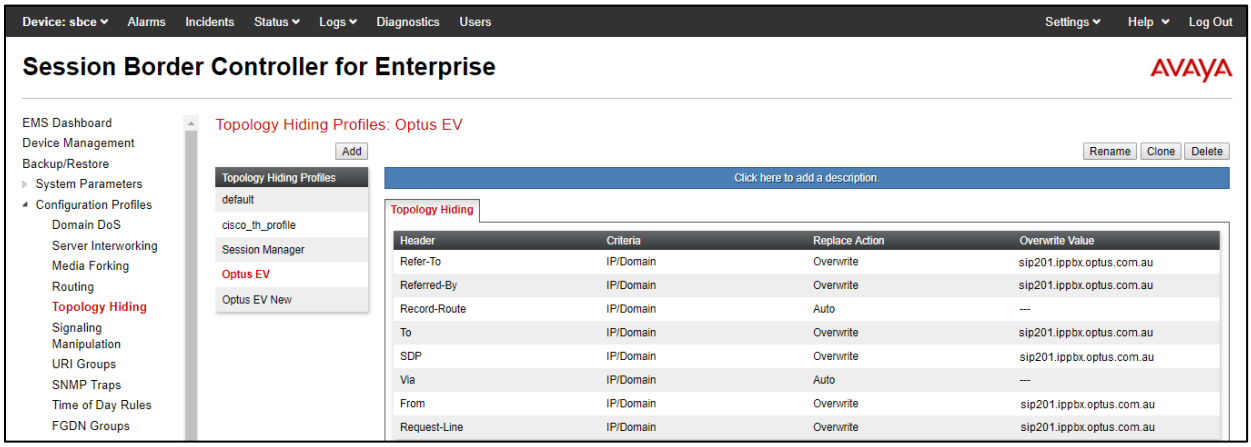
1. Select **Configuration Profiles → Topology Hiding** from the left-hand side menu.
2. Select the **Add** button, enter **Profile Name**: (e.g., **IP Office**), and click **Next**.
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly for all the headers.
4. Populate the fields as shown below, and click **Finish**.



6.5.2 Topology Hiding – Optus

Repeat the steps in **Section 6.5.1,** with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to Optus.

1. Enter a **Profile Name**: (e.g., **Optus EV**).
2. Click on the **Add Header** button repeatedly until all headers are added.
3. Populate the fields as shown below, and click **Finish**.

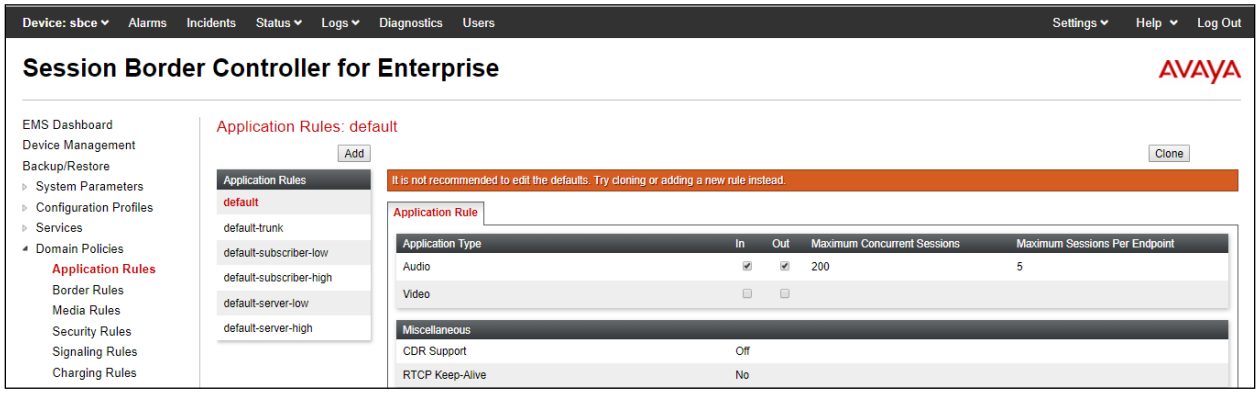


6.6 Domain Policies

The Domain Policies feature allows users to configure, apply and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. Avaya SBCE has pre-defined / default Rules and Policies under Domain Policies. Although the default Rules and Policies are editable, it is highly recommended to clone the Rules and/or Policies before modification as needed. The compliance test was commenced using the default rules and policies without any modification.

6.6.1 Application Rules

Ensure that the Application Rule used in the End Point Policy Group reflects the licensed sessions that the customer has purchased. In the lab setup, the Avaya SBCE was licensed for 200 Voice sessions, and the default rule was amended accordingly. Other Application Rules could be utilized on an as needed basis.

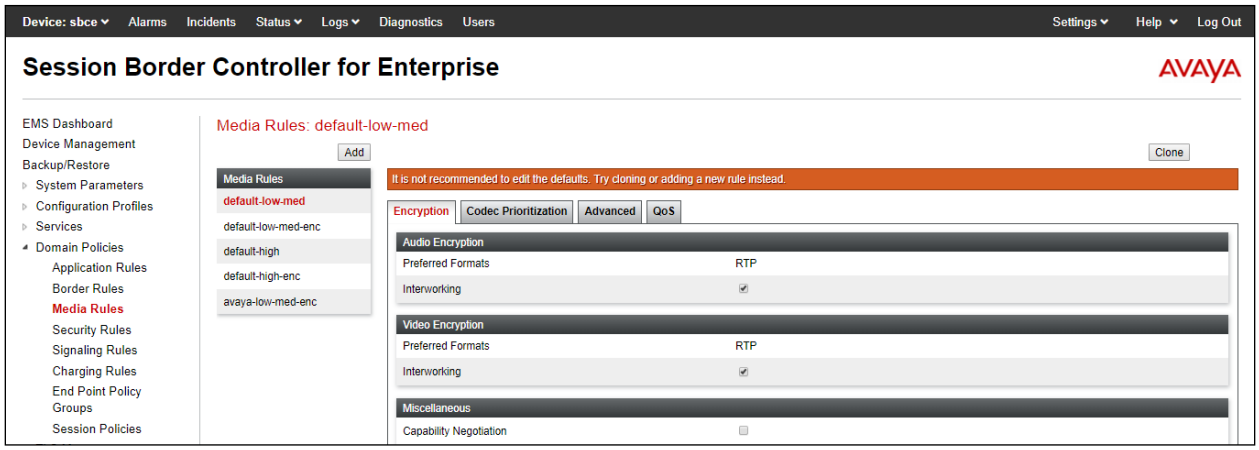


6.6.2 Border Rules

The Border Rule specifies if NAT is utilized (on by default), as well as detecting SIP and SDP Published IP addresses.

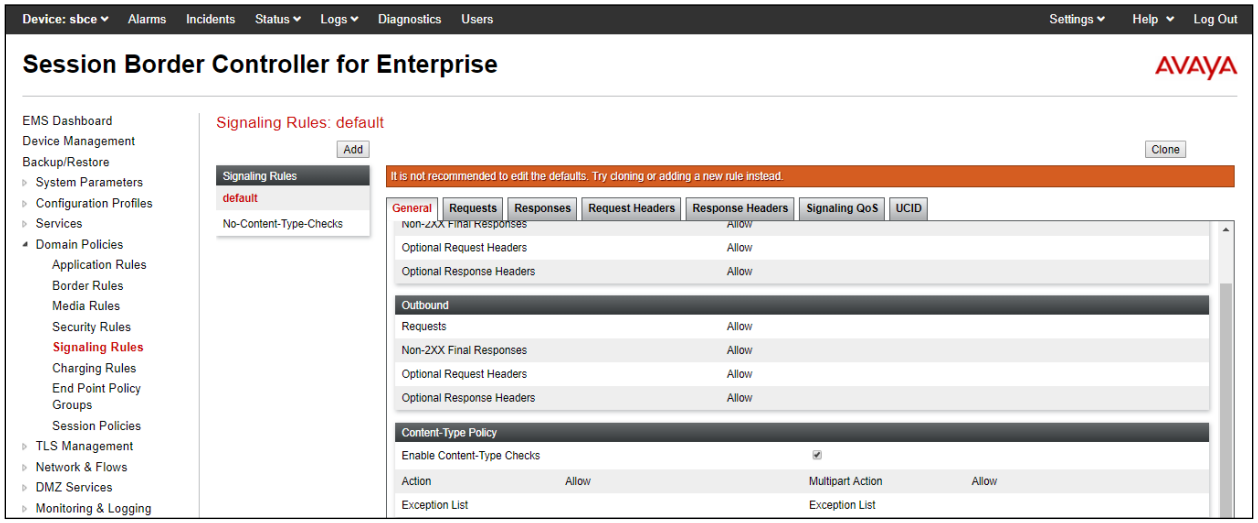
6.6.3 Media Rules

This Media Rule will be applied to both directions and therefore, only one rule is needed.
In the solution as tested, the **default-low-med** rule was utilized. No customization was required.



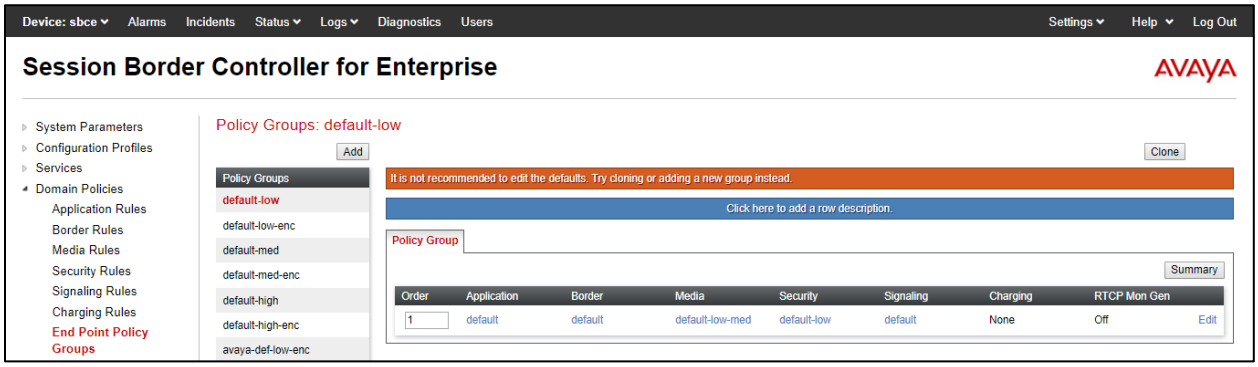
6.6.4 Signaling Rules

The default Signaling Rule was utilized. No customization was required.



6.6.5 Endpoint Policy Groups

In the solution as tested, the **default-low** rule was utilized. This rule incorporated the media and Signaling Rules specified above, as well as other policies.



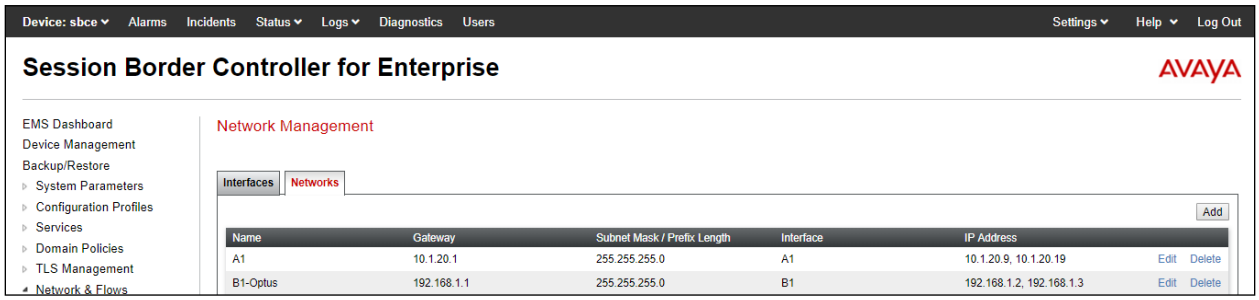
6.7 Network & Flows

The **Network & Flows** feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows.

6.7.1 Network Management

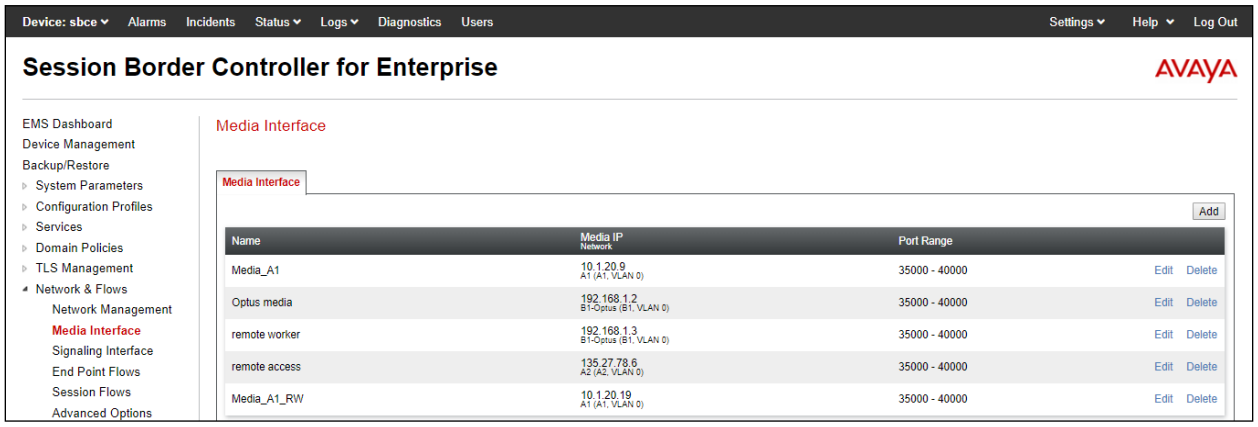
1. Select **Network & Flows** → **Network Management** from the menu on the left-hand side.
2. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.
3. Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit.** However, some of these values may not be changed if associated provisioning is in use.

Note: B1 has two IP Addresses configured for each interface. One is used for SIP trunking, another one is used for Remote worker. Configuration for Remote worker is out of scope of this document.



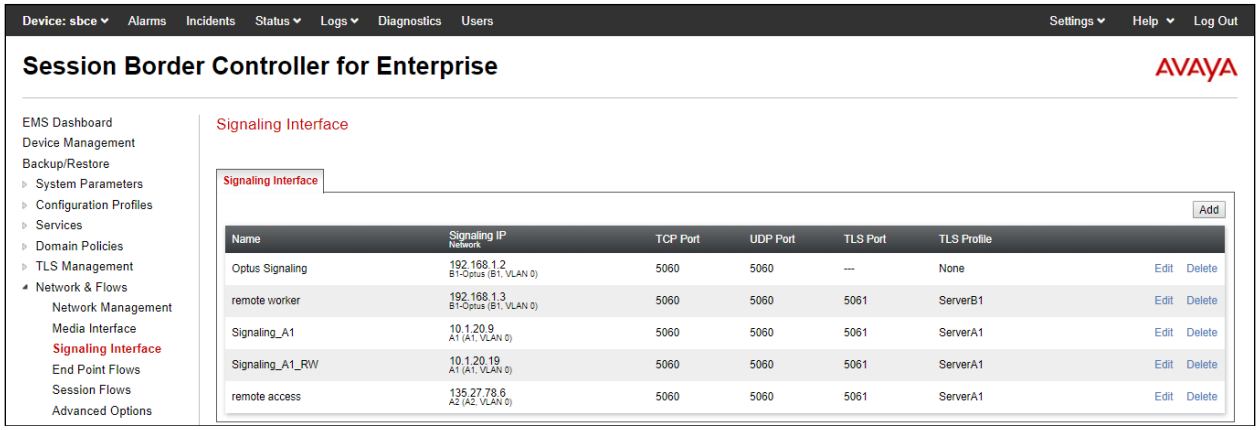
6.7.2 Media Interfaces

1. Select **Network & Flows** from the menu on the left-hand side (not shown).
2. Select **Media Interface**.
3. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
   - **Name**: **Media_A1**.
   - **IP Address**: **10.1.20.9** (Avaya SBCE A1 address).
   - **Port Range**: **35000-40000**.
4. Click **Finish** (not shown).
5. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
   - **Name**: **Optus media**.
   - **IP Address**: **192.168.1.2** (Avaya SBCE B1 address).
   - **Port Range**: **35000-40000**.
6. Click **Finish** (not shown). Note that changes to these values require an application restart. The completed **Media Interface** screen is shown below.



6.7.3 Signaling Interface

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Select **Add** (not shown) and enter the following:
   - **Name**: **Signaling_A1**.
   - **IP Address**: **10.1.20.9** (Avaya SBCE A1 address).
   - **TCP Port**: **5060**.
   - **UDP Port**: **5060**.
   - **TLS Port**: **5060**.
4. Click **Finish** (not shown).
5. Select **Add** again, and enter the following:
   - **Name**: **Optus Signaling**.
   - **IP Address**: **192.168.1.2** (Avaya SBCE B1 address).
   - **TCP Port**: **5060**.
   - **UDP Port**: **5060**.
6. Click **Finish** (not shown). Note that changes to these values require an application restart.



6.7.4 Endpoint Flows – For IP Office

1. Select **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Select **Add**, (not shown) and enter the following:
   - **Name**: **IP Office**.
   - **SIP Server Profile**: **IP Office**.
   - **URI Group**: *****.
   - **Transport**: *****.
   - **Remote Subnet**: *****.
   - **Received Interface**: **Optus Signaling**.
   - **Signaling Interface**: **Signaling_A1**.
   - **Media Interface**: **Media_A1**.
   - **End Point Policy Group**: **default-low**.
   - **Routing Profile**: **Optus EV**.
   - **Topology Hiding Profile**: **IP Office**.
   - Let other values default.
4. Click **Finish**.

6.7.5 Endpoint Flows – For Optus EV

Repeat step **1** through **4** from **Section 6.7.4**, with the following changes:

- **Name**: **Optus EV**.
- **SIP Server Profile**: **Optus EV**.
- **URI Group**: *****.
- **Transport**: *****.
- **Remote Subnet**: *****.
- **Received Interface**: **Signaling_A1**.
- **Signaling Interface**: **Optus Signaling**.
- **Media Interface**: **Optus media**.
- **End Point Policy Group**: **default-low**.
- **Routing Profile**: **IP Office**.
- **Topology Hiding Profile**: **Optus EV**.

7. Verification Steps

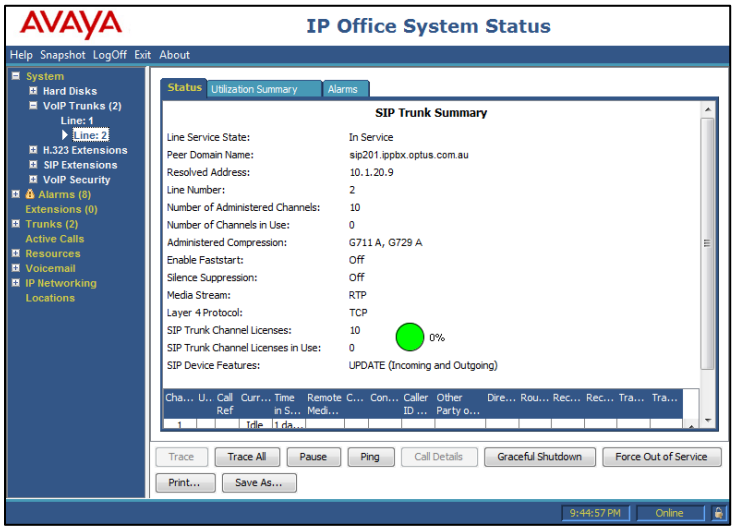
The following steps may be used to verify the configuration.

7.1 IP Office Verification

The following steps can also be used to verify the configuration.

Use the **Avaya IP Office System Status** application to verify the state of SIP connections. Launch the application from **Start → Programs → IP Office→ System Status** on the PC where **Avaya IP Office System Status** is installed, log in with the proper credentials.

Select the **SIP Line** under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current State** is **Idle** for each channel.



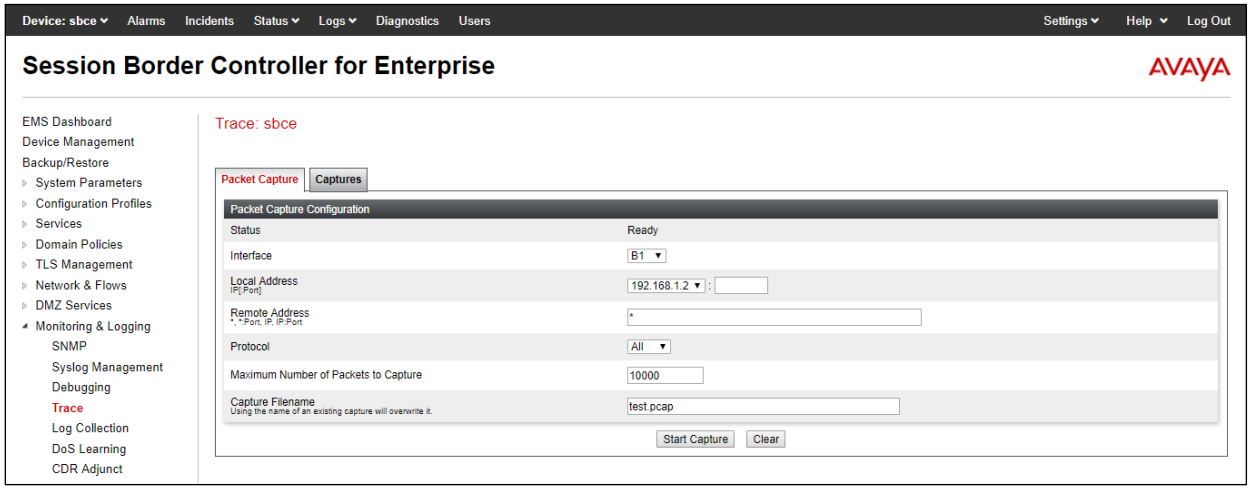
7.2 Avaya Session Border Controller for Enterprise Verification

Log into the Avaya SBCE as shown in **Section 6**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.

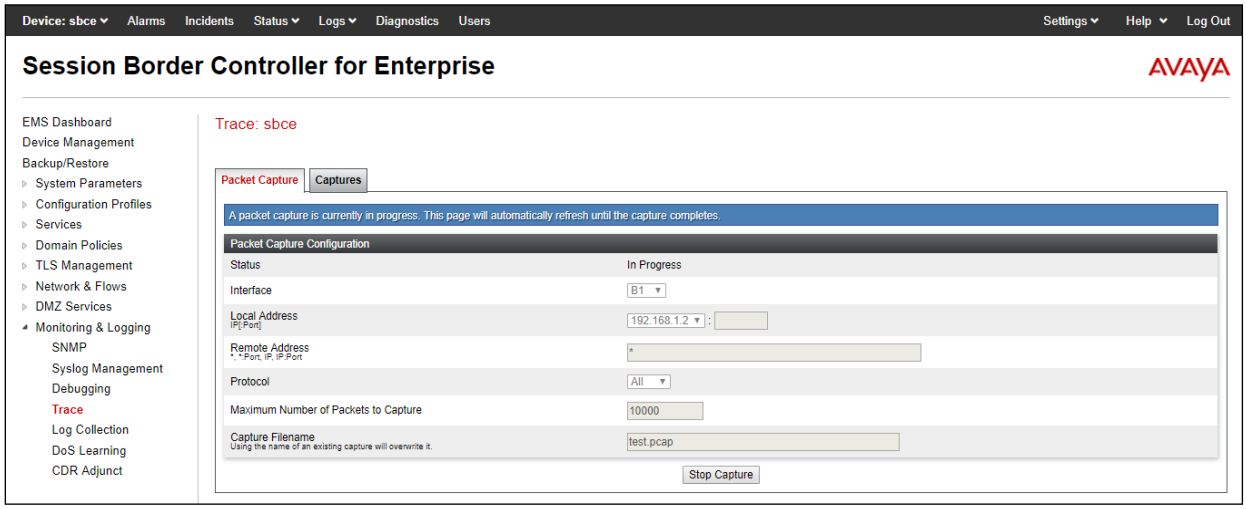
Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

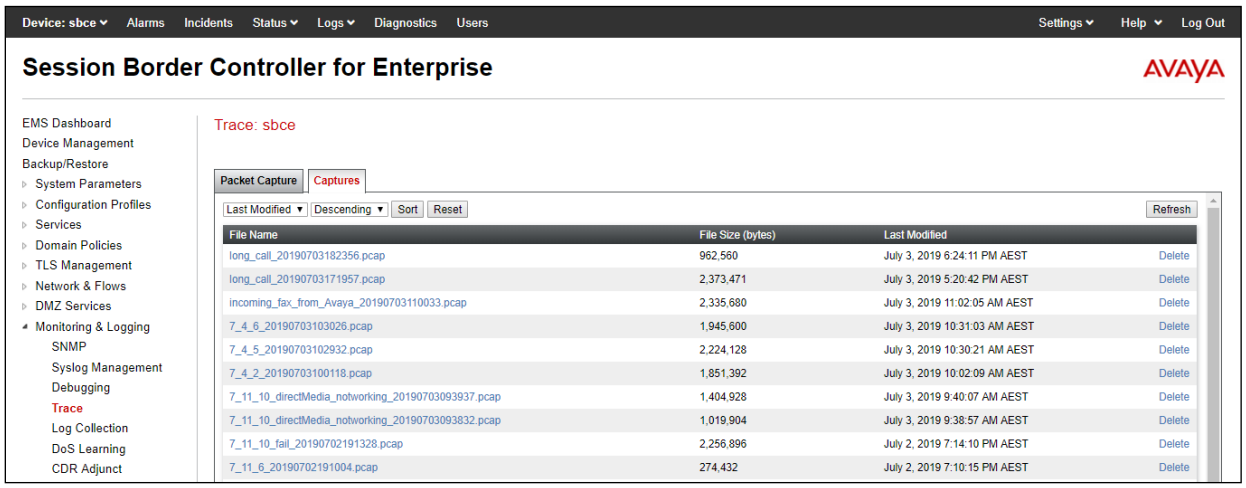
1. Navigate to **Monitoring & Logging → Trace**.
2. Select the **Packet Capture** tab and select the following:
   - Select the desired **Interface** from the drop down menu (e.g., **B1**).
   - Specify the **Maximum Number of Packets to Capture** (e.g., **10000**).
   - Specify a **Capture Filename** (e.g., **test.pcap**).
   - Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
   - Click **Start Capture** to begin the trace.



The capture process will initialize and then display the following **In Progress** status window:



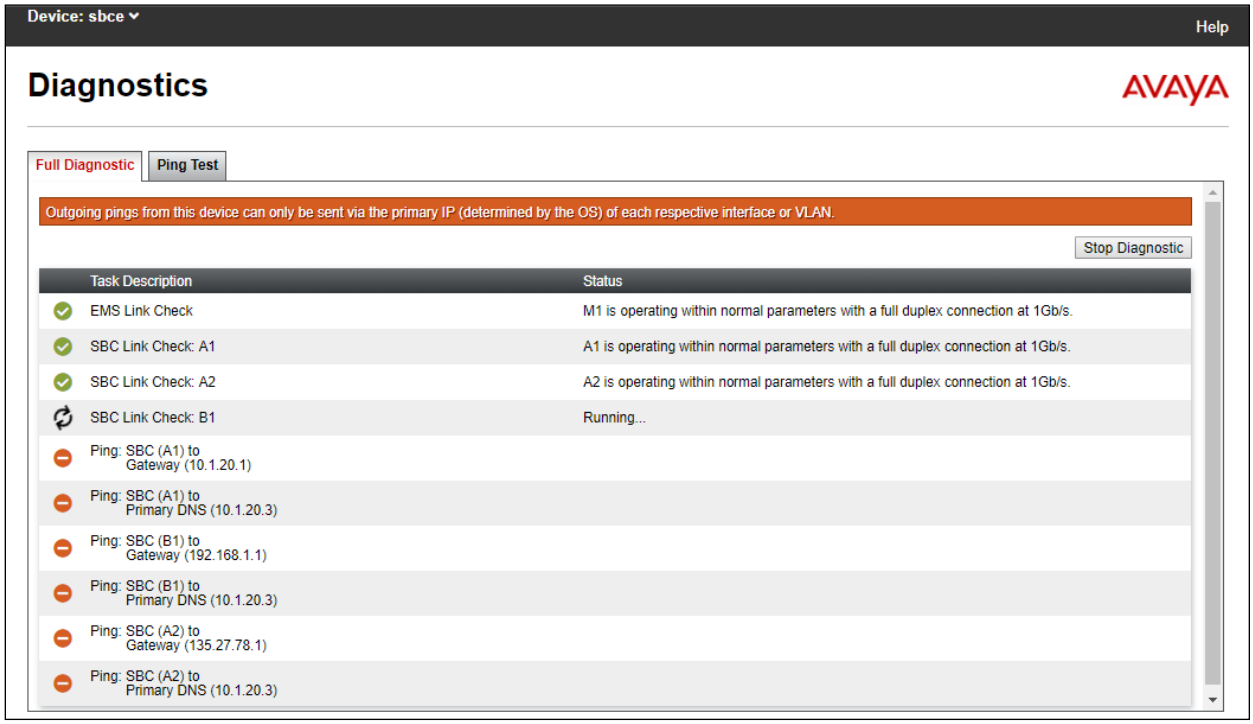
3. Run the test.
4. When the test is completed, select the **Stop Capture** button shown above.
5. Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.
6. Click on the **File Name** link to download the file and use Wireshark to open the trace.

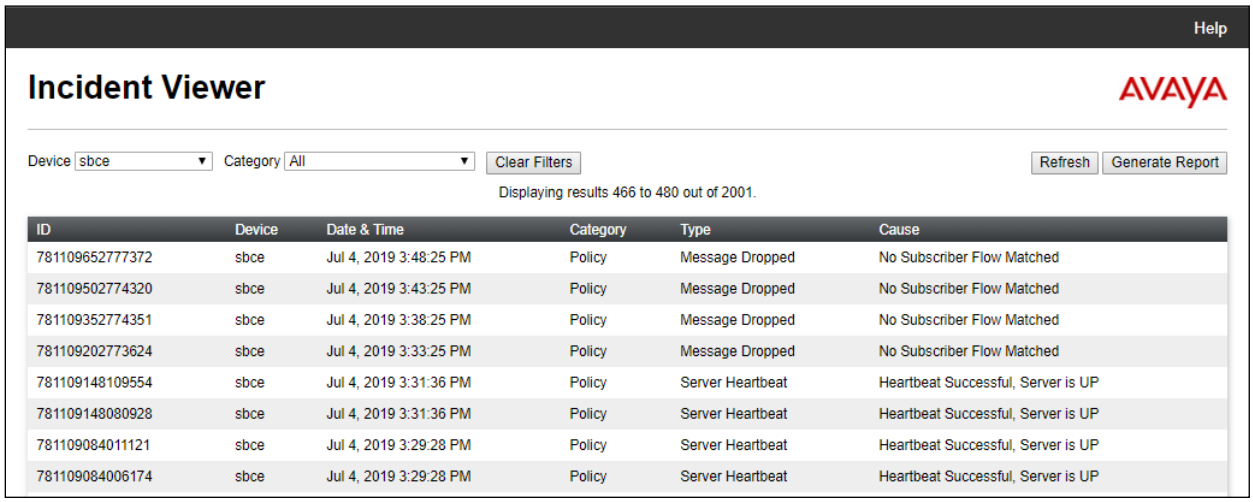


The following section details various methods and procedures to help diagnose call failure or service interruptions. As detailed in previous sections, the demarcation point between the Optus Evolve Voice Service and the customer SIP PABX is the customer SBC.
On either side of the SBC, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

- Ping from the SBC to the Optus network gateway.
- Ping from the SBC to the IP Office.

- Ping from the Optus network towards the customer SBC.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.





8. Conclusion

As illustrated in these Application Notes, Avaya IP Office 11 and Avaya Session Border Control for Enterprise 8.0 can be configured to interoperate successfully with Optus Evolve Voice SIP Trunking service. This solution allows enterprise users access to the PSTN using the Optus Evolve Voice SIP Trunking service connection. Please refer to **Section 2.2** for exceptions.

9. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Avaya IP Office™ Platform Start Here First, Release* 11.0, May 2018.
[2] *Avaya IP Office™ Platform Server Edition Reference Configuration*, Release 11.0, May 2018.
[3] *Deploying IP Office™ Platform Server Edition Solution*, Release 11.0, May 2018.
[4] *IP Office™ Platform 11.0, Deploying IP Office Essential Edition (IP500 V2)*, Document number 15- 601042, Feb 2019.
[5] *IP Office™ Platform 11.0, Installing and Maintaining the Avaya IP Office™ Platform Application Server*, Document number 15-601011, Apr 2019.
[6] *Administering Avaya IP Office™ Platform with Web Manager*, Release 11.0, May 2018.
[7] *Administering Avaya IP Office™ Platform with Manager*, Release 11.0, May 2018.
[8] *IP Office™ Platform 11.0, Using Avaya IP Office™ Platform System Status*, Document number 15-601758, Apr 2018.
[9] *IP Office™ Platform 11.0, Using IP Office System Monitor*, Document number 15-601019, May 2018.
[10] *Using Avaya Equinox for Windows on IP Office*, Release 11.0, Jun 2018.
[11] *IP Office™ Platform 11.0 - Third-Party SIP Extension Installation Notes*, Apr 2018.
[12] *Avaya IP Office Knowledgebase*, http://marketingtools.avaya.com/knowledgebase

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.