Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Vodafone DE (Germany) SIP Trunk Service with Avaya IP Office 10.0 and Avaya Session Border Controller for Enterprise 7.1 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking for an enterprise solution using Avaya IP Office 10.0 and Avaya Session Border Controller for Enterprise 7.1 to interoperate with the Vodafone DE SIP Trunk Service.

The Vodafone DE SIP Trunk Service provides PSTN access via a SIP trunk connected to the Vodafone DE Voice Over Internet Protocol (VoIP) network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise. Vodafone DE is a member of the Avaya DevConnect Service Provider program.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking for an enterprise solution using Avaya IP Office 10.0 and the Avaya Session Border Controller for Enterprise 7.1 (Avaya SBCE) to interoperate with the Vodafone DE SIP Trunk Service.

The Vodafone DE SIP Trunk Service referenced within these Application Notes is designed for business customers. Customers using this service with the IP Office solution are able to place and receive PSTN calls via a broadband WAN connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Avaya IP Office, Avaya SBCE and various Avaya endpoints listed in **Section 4**.

The Vodafone DE SIP Trunk Service passed compliance testing with observations/ limitations described in **Section 2.2**.

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 Vodafone DE SIP Trunk Service did not include use of any specific encryption features as requested by Vodafone DE.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products wherever possible (see **Section 2.2**).

2.1. Interoperability Compliance Testing

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

- Establishment of the SIP trunk
- SIP OPTIONS queries and responses
- Incoming PSTN calls (via the SIP trunk) to SIP and H.323 telephones at the enterprise
- Outgoing PSTN calls (via the SIP trunk) from SIP and H.323 telephones at the enterprise
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows and Avaya Communicator for Web
- Various call types including: local, long distance, international, outbound toll-free, operator, and local directory assistance
- Codec G.711A and G.729
- Caller ID presentation and Caller ID restriction
- DTMF transmission using RFC 2833
- Response to incomplete call attempts and trunk errors
- Voicemail navigation using DTMF input for inbound and outbound calls
- Voicemail message waiting indicator (MWI)
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and twinning (mobility)
- G.711 fax
- Long duration calls and simultaneous active calls
- Remote worker

The following items are not supported or were not tested:

- The REFER method and T.38 Fax are not supported by the Vodafone DE SIP Trunk Service.
- Inbound toll-free calls and emergency calls were not tested.

2.2. Test Results

Interoperability testing of the Vodafone DE SIP Trunk Service was successful with the following observations.

- **Outbound Caller ID**: On outbound calls, the calling party number is shown as the pilot/base number of the account and not the actual DDI sent by Avaya IP Office. The trunk was configured by Vodafone DE with a length that was longer than the set of numbers provided for testing. In this case, it is expected behavior that the pilot/base number is used as the calling party.
- **Call Forward and Caller ID**: For inbound PSTN calls that are call forwarded to another PSTN endpoint, the forwarding party number is shown as the calling party instead of the original PSTN caller (forwarded party). This also impacts enterprise users with Twinning (mobility) enabled. These users have their inbound calls also ring a mobile

phone. On the mobile phone, the enterprise host number is shown as the calling party instead of the original PSTN caller.

- **Call Forward and SRTP**: For inbound PSTN calls that are call forwarded to another PSTN endpoint, the call results in no audio if SRTP is used on the connection between Avaya IP Office and the Avaya SBCE. This is believed to be an Avaya issue and is under investigation. As a workaround, this connection can be set to use TCP and RTP (**Sections 5.5.3** and **5.5.6**).
- **G.711 fax**: Some G.711 fax calls failed due to excessive jitter on the trunks used in the test environment.
- **G.729 and SRTP**: Inbound or outbound calls from an Avaya 96x1 H.323 phone to the PSTN using G.729 and encrypted media inside the enterprise results in one-way audio in the outbound direction from the enterprise. On an outbound call with G.729 selected, Vodafone requests a ptime of 30 and cannot be changed on a per customer basis. Inbound calls requests a ptime of 20 but the failure is the same. This issue is believed to be an issue with the Avaya 96x1 H323 phone. The issue has been raised to the Avaya development team and is under investigation. Other phone types tested (Avaya 16xx H.323 and Avaya 11xx SIP phones) did not have this issue. Workarounds include **one** of the following:
    - Do not use G.729 on the trunk to Vodafone DE (**Section 5.5.6**).
    - Do not use encryption TLS/SRTP internal to the enterprise (**Sections 5.3.1** for signaling and **Section 5.3.4** for media).
- **Intermittent loss of audio in one direction after session refresh in some call scenarios**: An outbound call from an Avaya 1100 Series SIP phone or Avaya Communicator for Web to the PSTN which is blind transferred to a local extension, would intermittently lose audio in one direction when a session refresh reINVITE was sent by Avaya IP Office. Audio may not be impacted on the first session refresh but may be impacted on subsequent session refreshes. A failure occurred approximately one in twelve calls. The issue has been raised to the Avaya development team and is under investigation. As a workaround, session refresh should be disabled (**Section 5.5.2**).

2.3. Support

For technical support on Vodafone DE products please visit the website at www.vodafone.de or contact an authorized Vodafone DE representative.

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

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The sample configuration shows an enterprise site connected to the Vodafone DE SIP Trunk Service.

Located at the enterprise is the Avaya SBCE. It has a public side that connects to the Vodafone DE SIP Trunk Service. The private side of the Avaya SBCE connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In

this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers.

The enterprise site contains an Avaya IP Office 500 V2 with various endpoints and a Windows PC running both Avaya IP Office Manager to configure Avaya IP Office and Avaya VoiceMail Pro for voicemail. In addition, the Avaya IP Office Application Server is present to support use of Avaya Communicator for Web (WebRTC client).

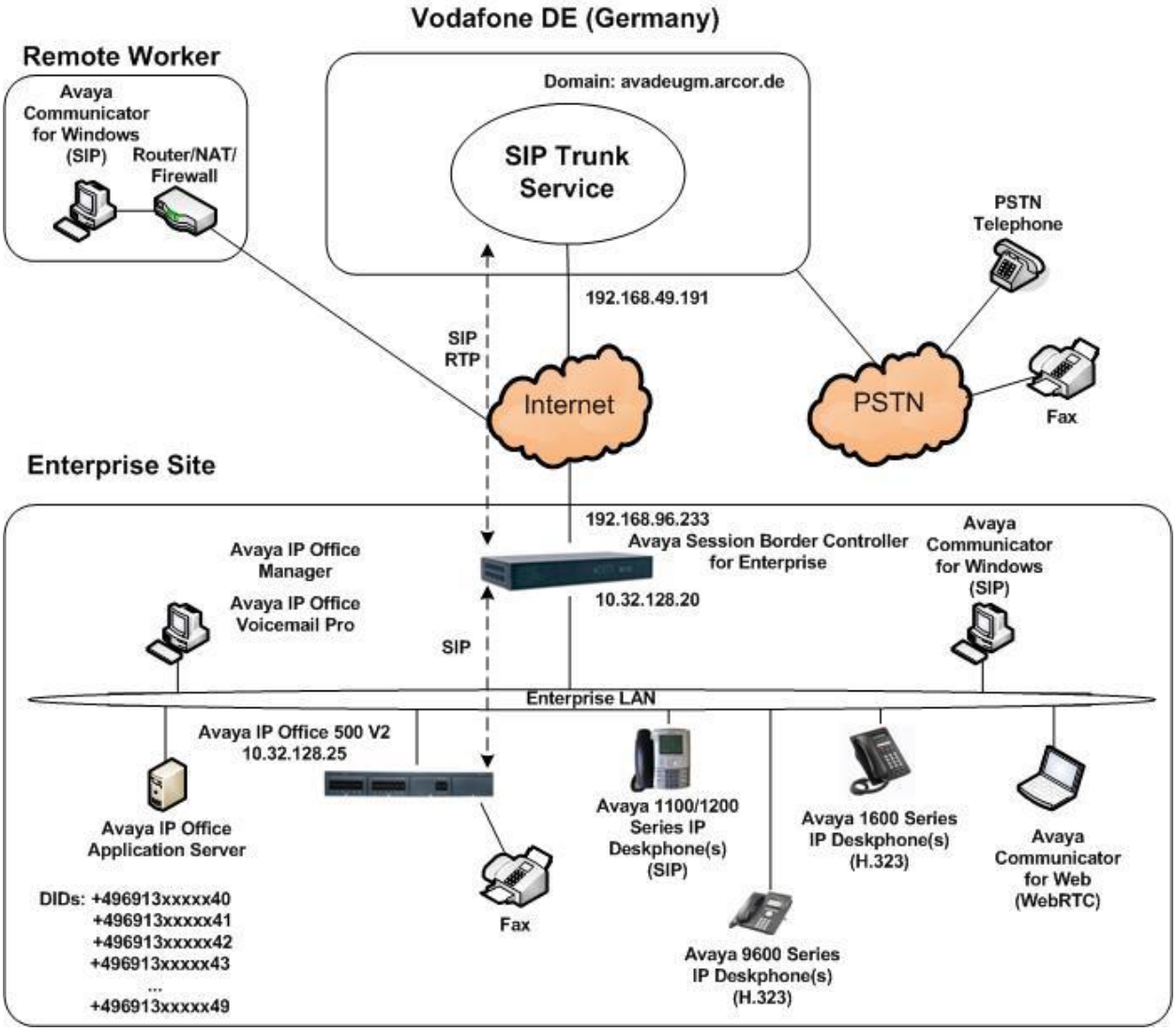


Figure 1: Avaya Interoperability Test Lab Configuration

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 replaced with private addresses and all phone numbers have been partially masked or replaced with numbers that cannot be routed over the PSTN.

For the purposes of the compliance test, users dialed a prefix digit 9 plus N digits to send an outbound call to the number N across the SIP trunk to the service provider. The short code of 9 was stripped off by Avaya IP Office and the remaining N digits were sent to the service provider network. For international calls, Avaya IP Office was configured to replace the dialed international access code (00) with a + sign in the SIP headers (**Section 5.5.8**). In the source headers (e.g., From, PAI, and Contact), Avaya IP Office was configured to send the DDI number assigned by Vodafone DE in international format (e.g., +496913xxxxxxx) (**Section 5.7**).

The Vodafone DE SIP Trunk Service sends the destination number in international format (e.g., +496913xxxxxxx) in the Request-Line and the To header in an inbound SIP INVITE message.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the enterprise network such as a data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that SIP and RTP traffic between the service provider and Avaya IP Office must be allowed to pass through these devices.

The administration of the Avaya Voicemail Pro messaging service and endpoints on Avaya IP Office are standard. Since these configuration tasks are not directly related to the interoperation with the Vodafone DE SIP Trunk Service, they are not included in these Application Notes.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment	**Software**
Avaya IP Office 500 v2	10.0 SP3 (10.0.0.3.0 Build 5)
Avaya IP Office Manager	10.0 SP3 (10.0.0.3.0 Build 5)
Avaya IP Office VoiceMail Pro	10.0 SP3 (10.0.0.3.0 Build 5)
Avaya IP Office Application Server • one-X® Portal • WebRTC Gateway	10.0 SP3 (10.0.0.3.0 Build 5) (10.0.0.3.0 Build 5) (10.0.0.3.0 Build 10)
Avaya Session Border Controller for Enterprise running on a Portwell CAD-0208 server	7.1 SP2 (7.1.0.2-01-13249)
Avaya 1140E IP Deskphone (SIP)	4.4 SP4 (4.04.23)
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3.5 (1.3.50B)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.6.4 (6.6401)
Avaya Communicator for Windows	2.1.3 (2.1.3.237)
Avaya Communicator for Web	1.0.16.1718

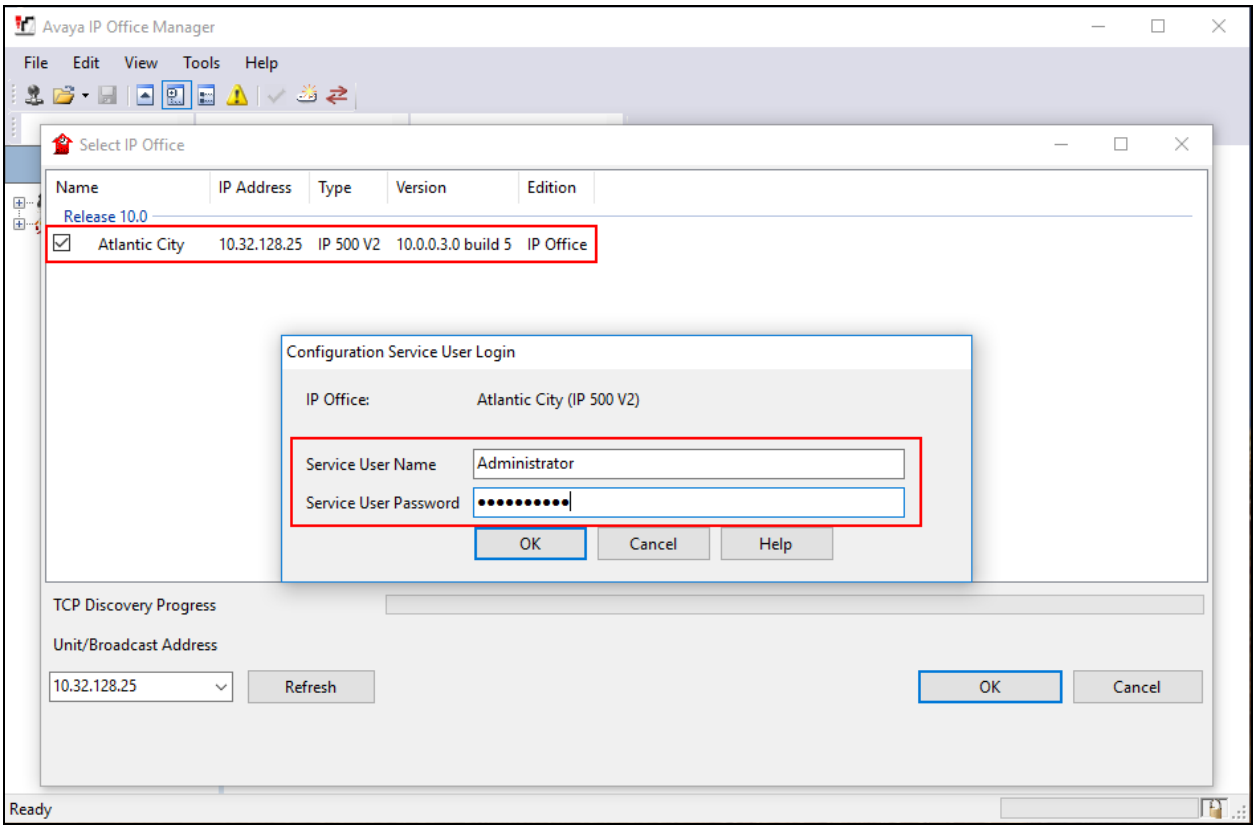
Vodafone DE Components	
Equipment	**Software**
Oracle Session Border Controller	7.2
Italtel Softswitch	20.50.52

Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with IP Office Server Edition in all configurations.

Avaya IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog/digital endpoints or analog/digital trunks.

5. Configure Avaya IP Office

Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the PC running Avaya IP Office Manager, select **Start → All Programs → IP Office → Manager** to launch the application. Select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials.



If the above screen does not appear, the configuration may be alternatively opened by navigating to **File → Open Configuration** at the top of the Avaya IP Office Manager window.

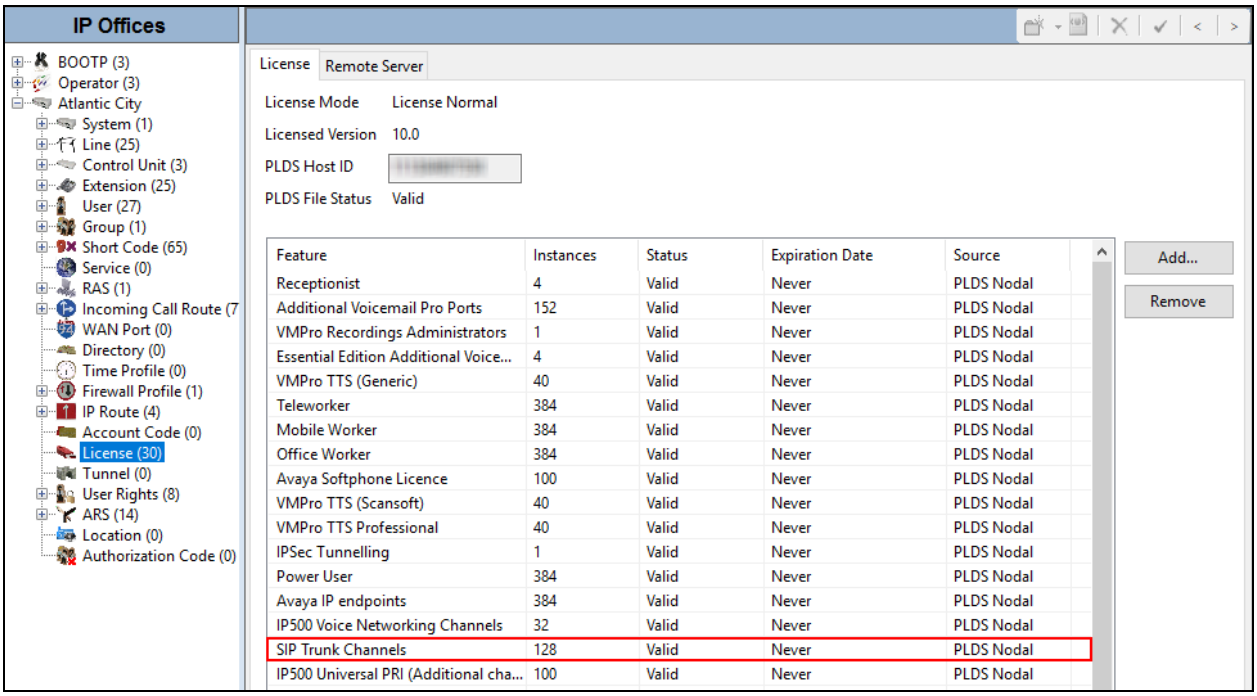
The appearance of the Avaya IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation pane on the left side, omit the Group pane in the center, and show the Details pane on the right side. Since the Group Pane has been omitted, its content is shown as submenus in the Navigation pane. The Navigation and Details 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 and Avaya Communicator support) is assumed to already be in place.

In the sample configuration, **Atlantic City** was used as the system name. All navigation described in the following sections (e.g., **License → SIP Trunk Channels**) appears as submenus underneath the system name **Atlantic City** in the Navigation Pane.

5.1. Licensing

The configuration and features described in these Application Notes require Avaya IP Office to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License** in the Navigation pane. Confirm a valid license with sufficient **Instances** (trunk channels) appears in the Details pane.

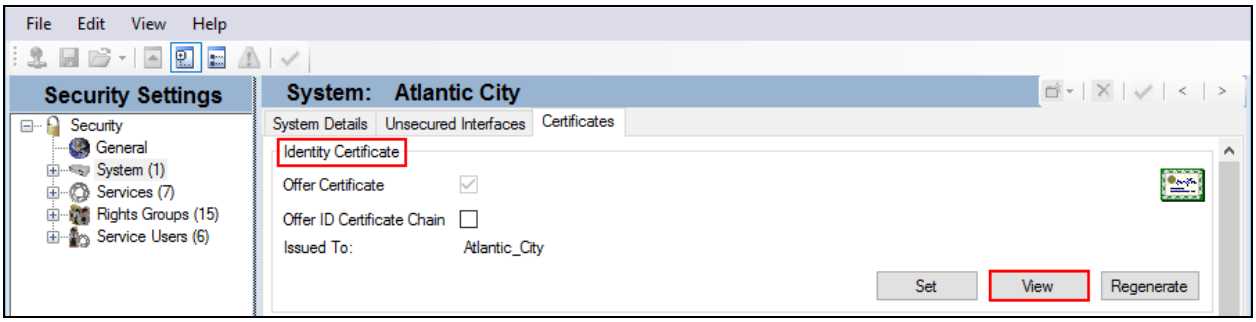


5.2. TLS Management

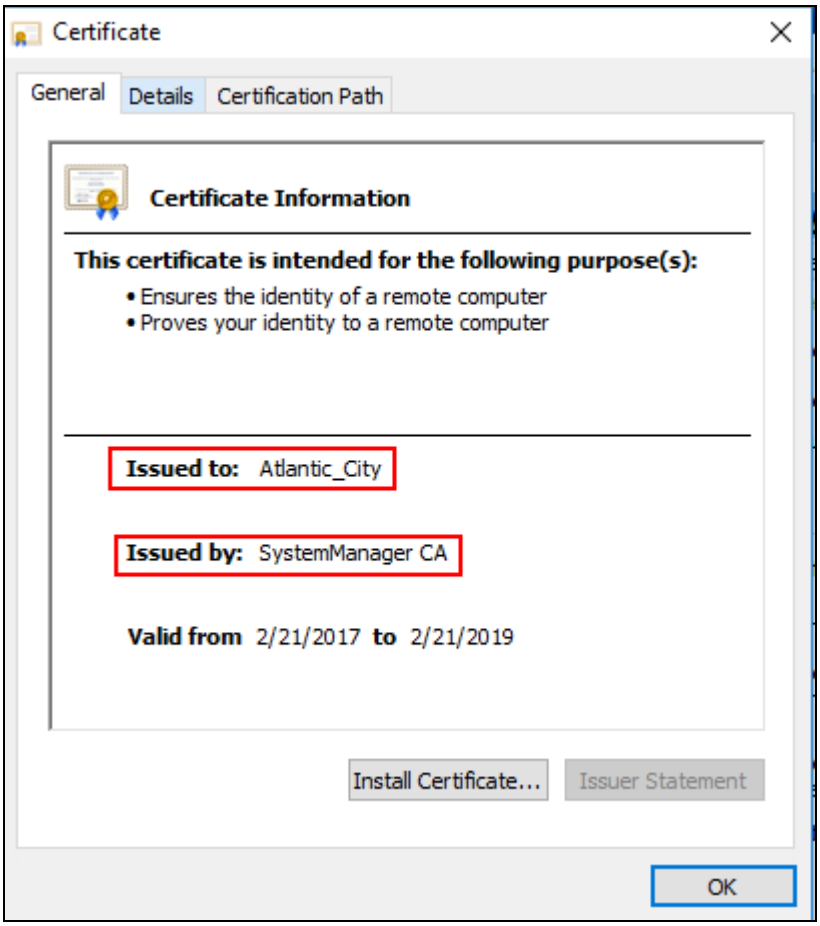
For the compliance test, the signaling on the SIP trunk between Avaya IP Office and the Avaya SBCE was secured using TLS. Testing was done using identity certificates signed by a local certificate authority **SystemManager CA**. The generation and installation of these certificates are beyond the scope of these Application Notes. However, once the certificates are available they can be viewed on the Avaya IP Office in the following manner.

To view the certificates currently installed on Avaya IP Office, navigate to **File → Advanced → Security Settings**. In the Security Settings window, navigate to **Security → System** and select the **Certificates** tab.

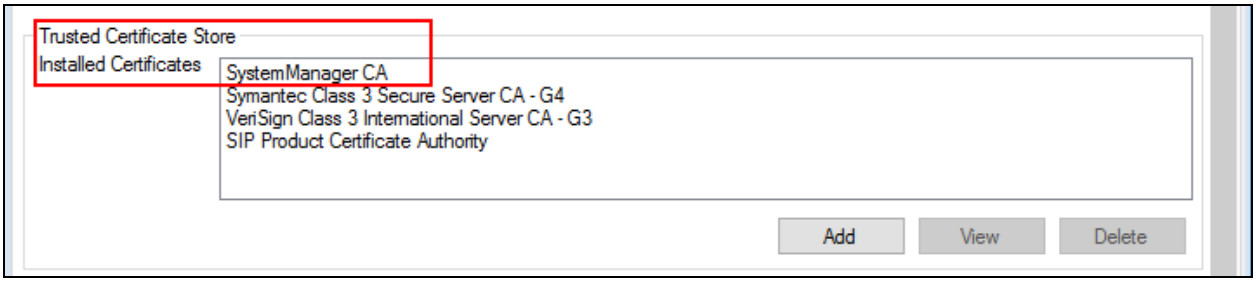
To verify the identity certificate, locate the **Identity Certificate** section and click **View** to see the details of the certificate.



A pop-up window will appear showing that the certificate is issued to the Avaya IP Office (**Atlantic_City**) and signed/issued by **SystemManager CA**. Click **OK** to close the pop-up window.



To verify the trusted certificates, return to the **Security → System →Certificates** tab and scroll down to the **Trusted Certificate Store** section. Verify that **SystemManager CA** is listed as an **Installed Certificate**.

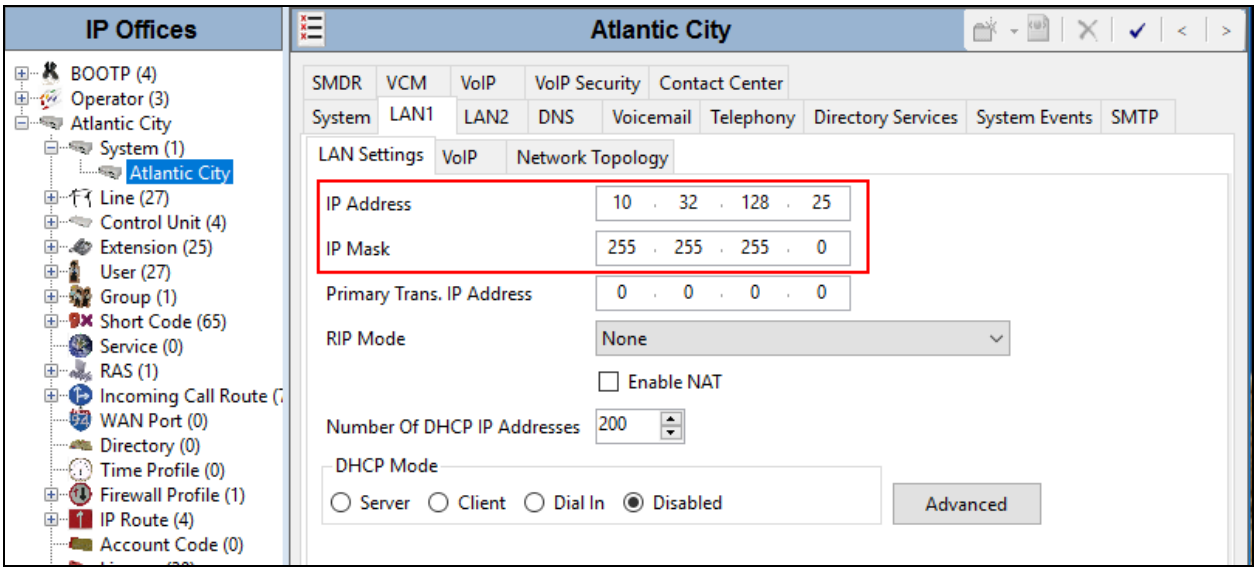


5.3. System

Configure the necessary system settings.

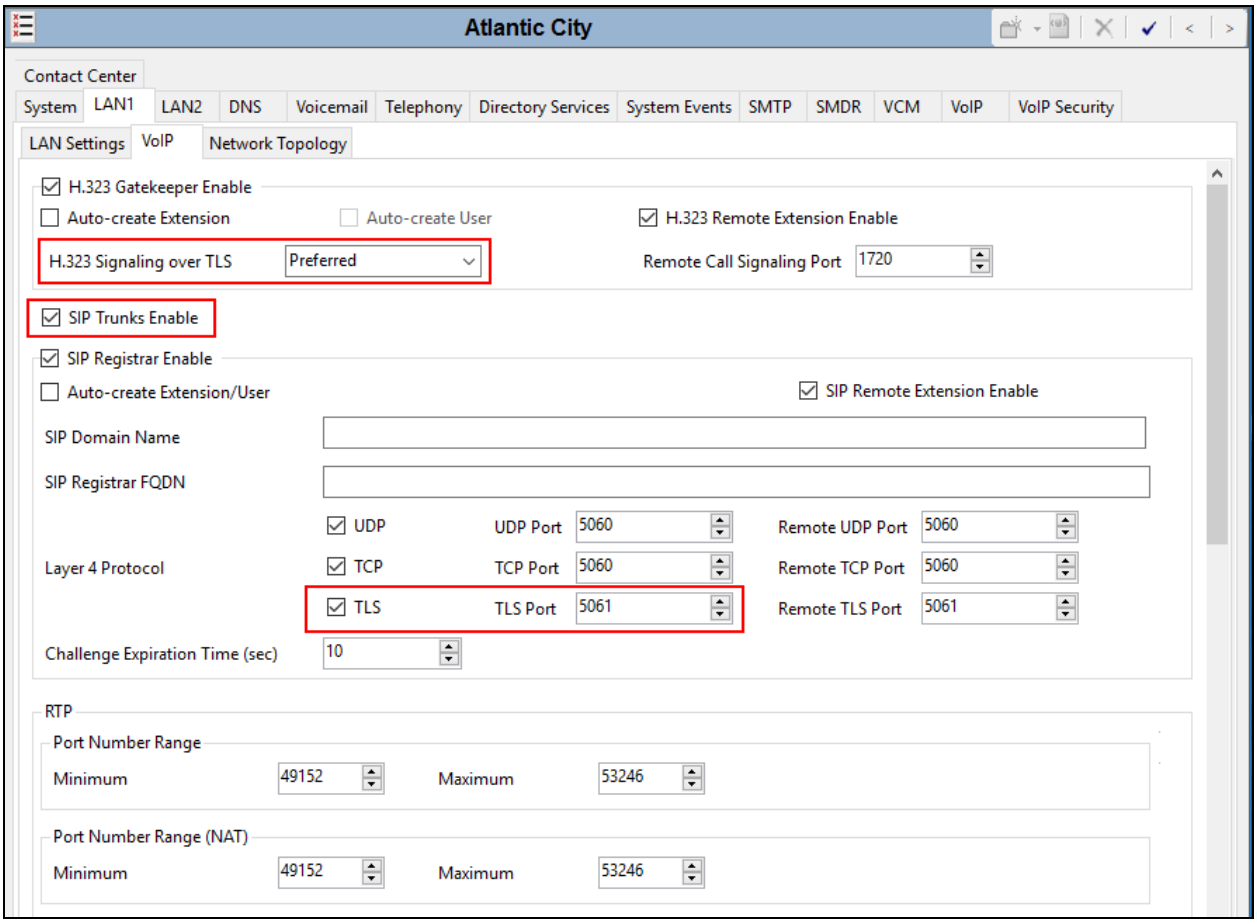
5.3.1. System – LAN1 Tab

In the sample configuration, the Avaya IP Office LAN port was used to connect to the enterprise network. The LAN1 settings correspond to the LAN port on the Avaya IP Office 500 V2. To access the LAN1 settings, first navigate to **System** → <*Name*>, where <*Name*> is the system name assigned to the Avaya IP Office. In the case of the compliance test, the system name is **Atlantic City**. Next, navigate to the **LAN1** → **LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office LAN port. Set the **IP Mask** field to the mask used on the enterprise network. All other parameters should be set according to customer requirements.



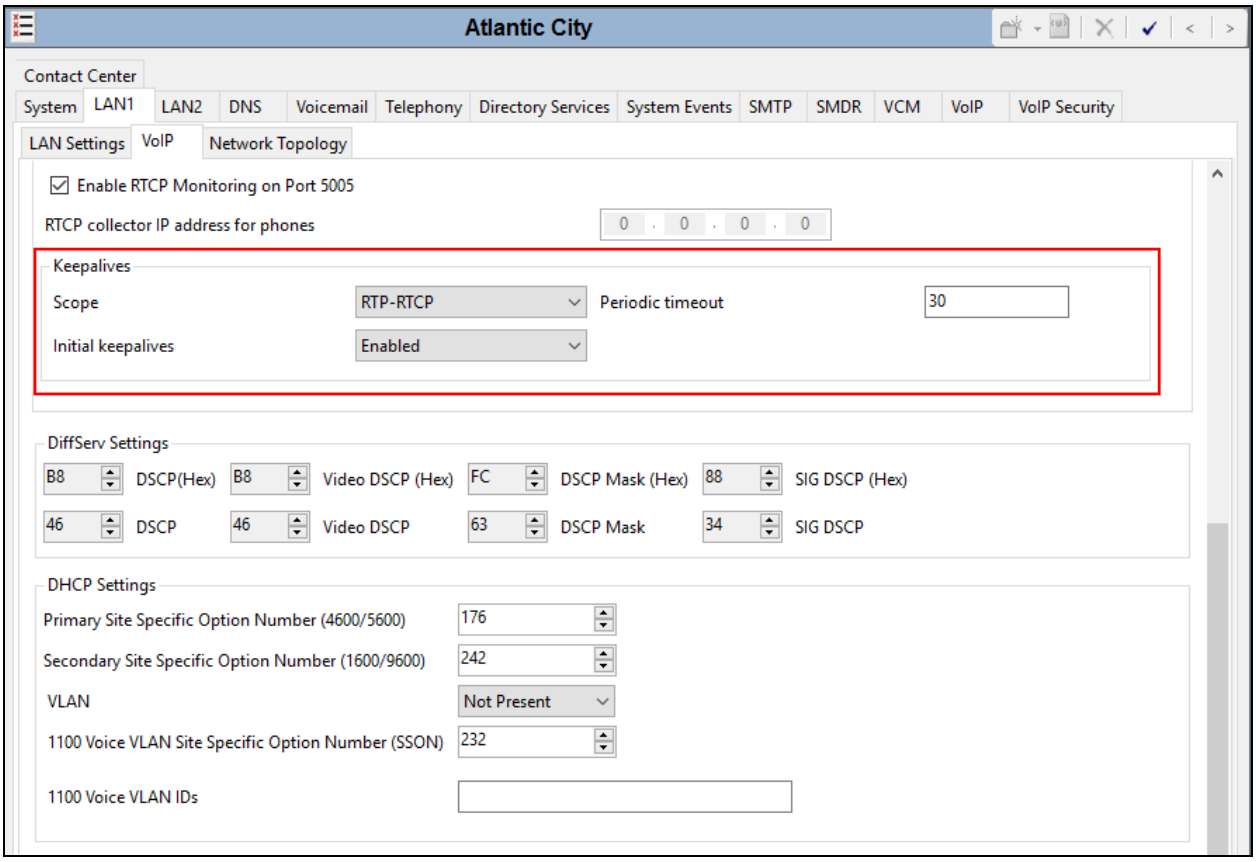
On the **VoIP** tab in the Details Pane configure the following parameters:

- In the test environment, Avaya IP Office endpoints used TLS for signaling. As a result, the **H.323 Signaling over TLS** was set to **Preferred**. To disable TLS on H.323 phones, then set **H.323 Signaling over TLS** to **Disabled**.
- Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks.
- To enable TLS for SIP endpoints, in the **Layer 4 Protocol** section, the **TLS** box was checked and the **TLS Port** was set to **5061**. To disable TLS on SIP phones, then uncheck the **TLS** box.



Scroll down the page.

- In the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the periodic timeout to **30** and the **Initial keepalives** parameter to **Enabled**. These settings will cause Avaya IP Office to send RTP and RTCP keepalive packets starting at the time of initial connection and every 30 seconds thereafter if no other RTP/RTCP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting to see media from the other, as well as helping to keep firewall ports open for the duration of the call.
- All other parameters should be set according to customer requirements.

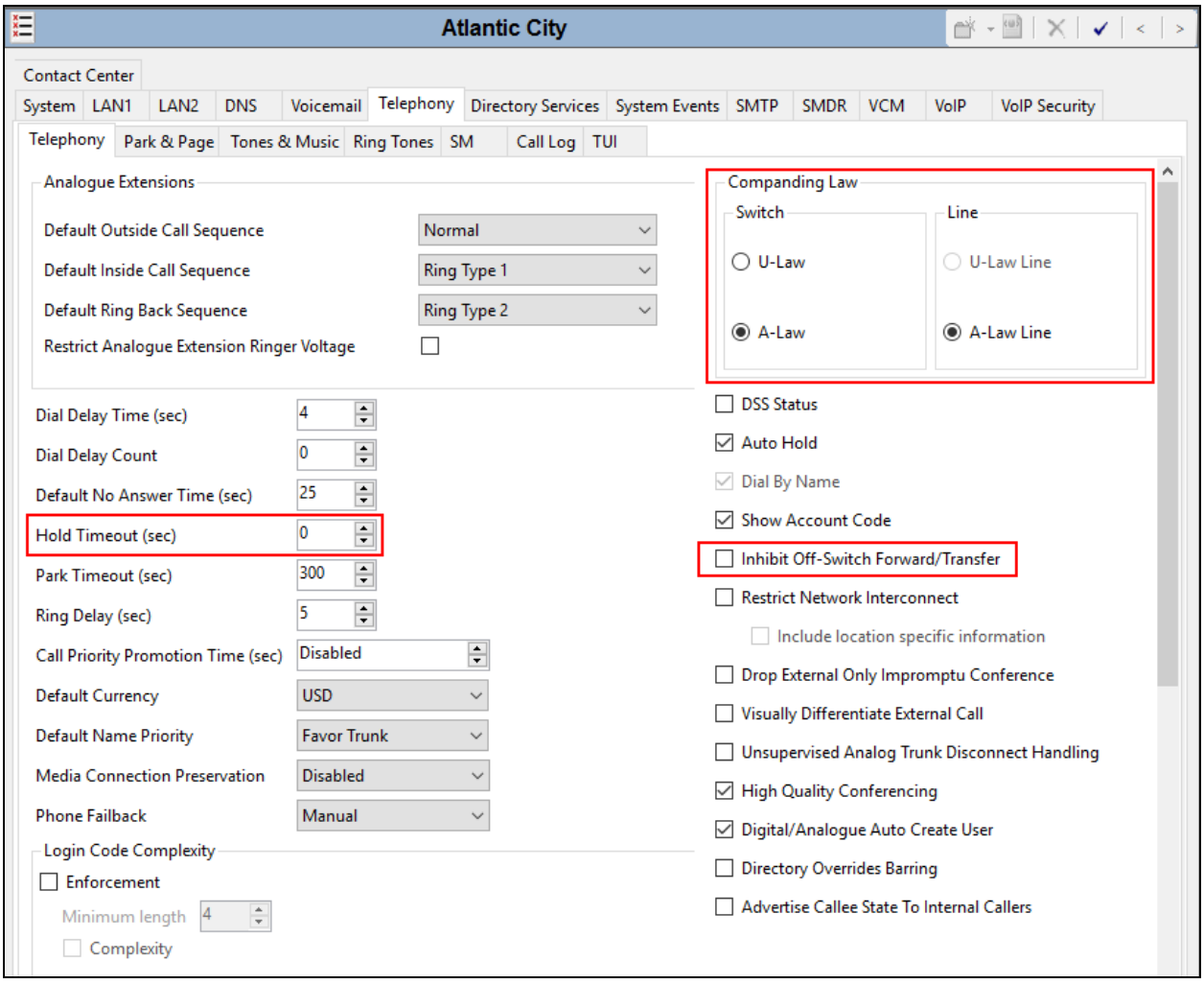


No configuration was necessary on the **LAN2 → Network Topology** tab for SIP Trunking since the **SIP Line → Transport** tab has the **Use Network Topology Info** field set to **None** (**Section 5.5.3**).

5.3.2. System - Telephony Tab

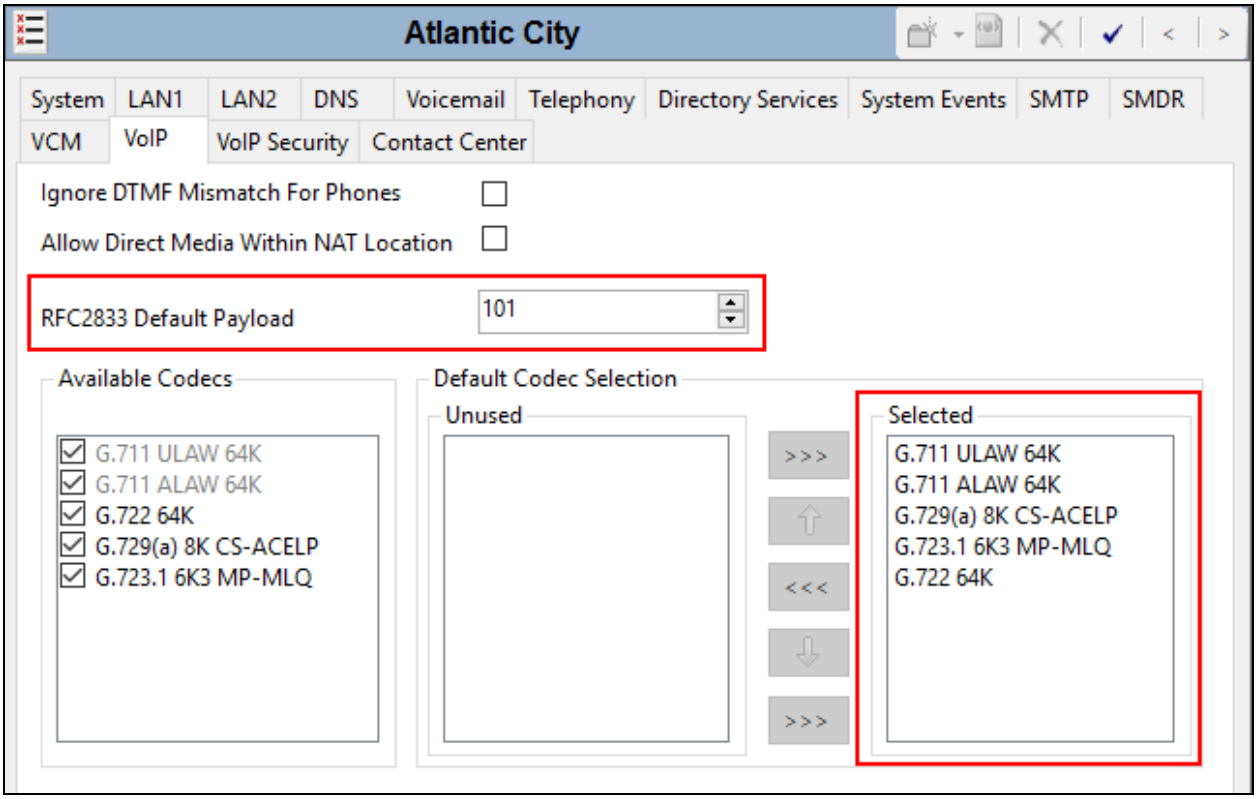
To access the System Telephony settings, navigate to the **Telephony → Telephony** tab in the Details Pane.

- Choose the **Companding Law** typical for the enterprise location. For the compliance test, **A-Law** was used for both **Switch** and **Line**.
- Enter or select **0** for **Hold Timeout (sec)** so that calls on hold will not time out.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN. If for security reasons incoming calls should not be allowed to transfer back to the PSTN then leave this setting checked.
- All other parameters should be set according to customer requirements.



5.3.3. System – VoIP

For the compliance test, all codecs were checked under **Available Codecs** and all were moved to the **Selected** group using the arrow buttons. The group of **Selected** codecs are the codecs which are available to the system for use. The list can be further restricted for the SIP trunk on the **SIP Line → VoIP** tab (**Section 5.5.6**). The **RFC2833 Default Payload** was left at the system default of **101**. Vodafone sends 106 as the payload value. For each call, the payload value was negotiated to 101 or 106; both values were used successfully.

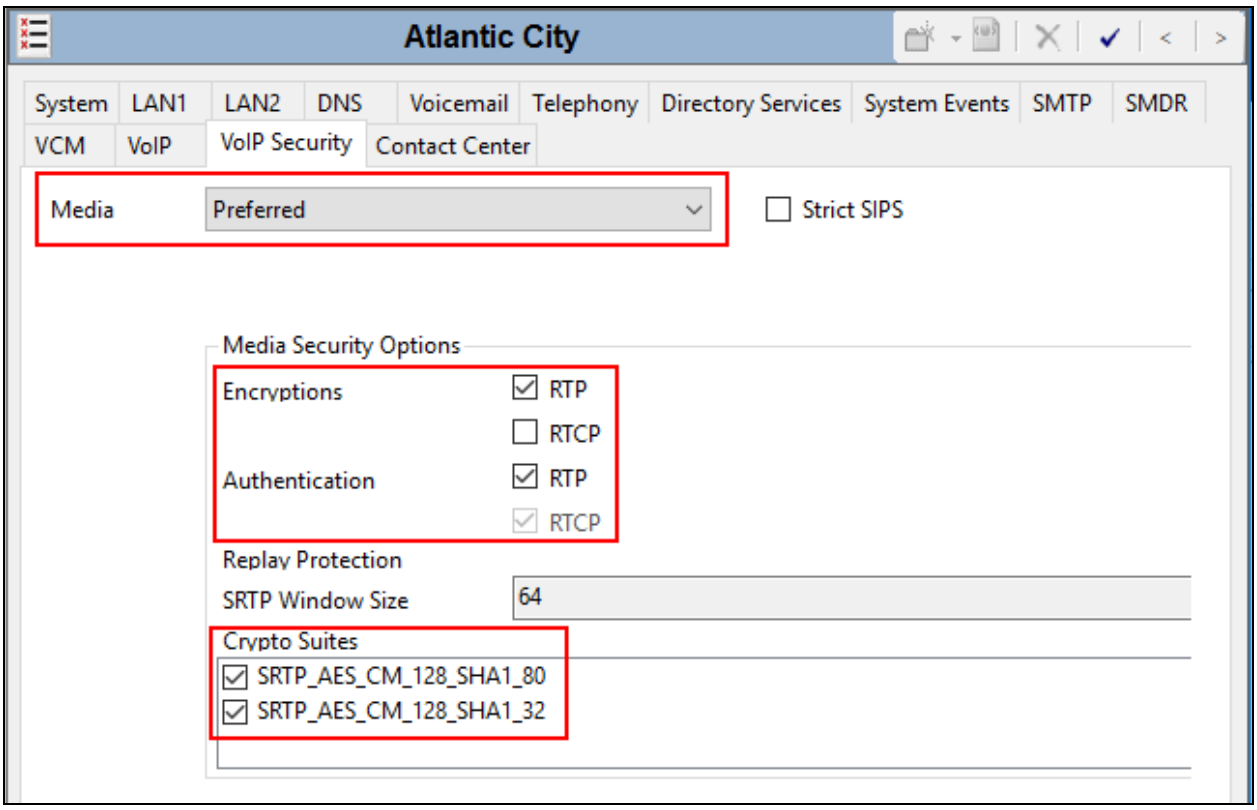


5.3.4. System – VoIP Security

For the compliance test, SRTP was used internal to the enterprise wherever possible. Thus, the **Media** parameter was set to **Preferred**, specifying that SRTP is preferred before RTP. One way to avoid the issue with Avaya 96x1 H.323 phones using SRTP and G.729 documented in **Section 2.2** is to set the **Media** parameter to **Disabled**. This will disable the use of SRTP to the enterprise phones. If SRTP is disabled for media, then TLS should be disabled for signaling (**Section 5.3.1**).

For the compliance test, **Media** was set to **Preferred** and the Media Security Options were set as follows:

- Under **Encryptions**, check **RTP**.
- Under **Authentications**, check **RTP**.
- Under **Crypto Suites**, both **SRTP_AES_CM_128_SHA1_80** and **SRTP_AES_CM_128_SHA1_32** were selected.
- Click **OK** to commit (not shown).

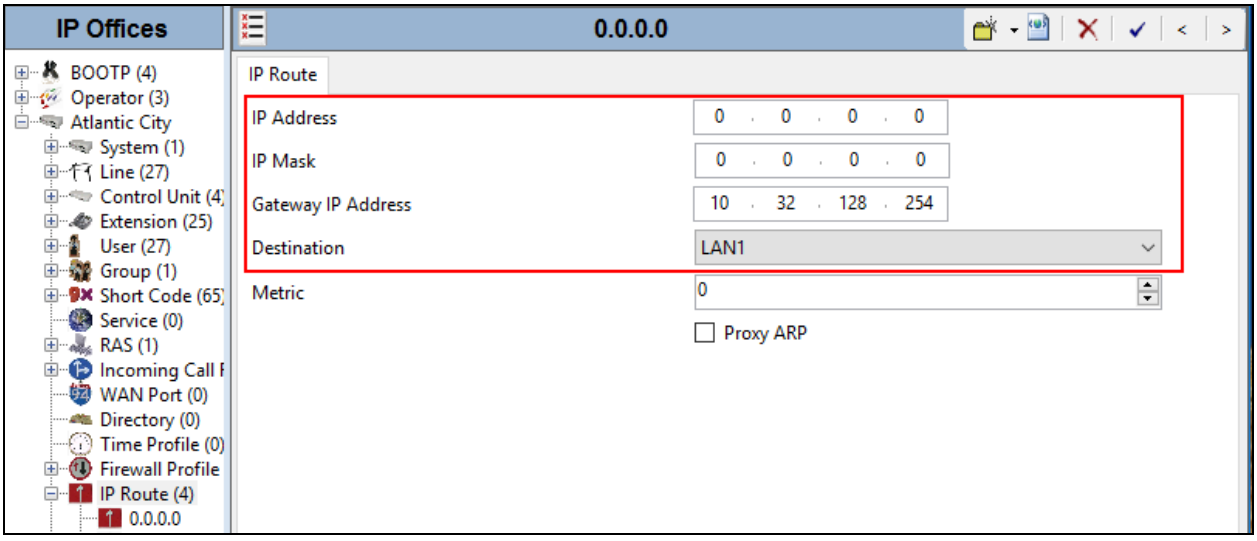


5.4. IP Route

A default route is needed so IP Office can reach other network subnets other than the one where it resides. Since IP Office and the private side of the Avaya SBCE reside on the same subnet, the default route is not specifically used for SIP Trunking. Navigate to **IP Route → 0.0.0.0** in the left Navigation Pane if a default route already exists. Otherwise, to create the default route, right-click on **IP Route** and select **New**. Create/verify a default route with the following parameters:

- Set **IP Address** and **IP Mask** to **0.0.0.0**.
- Set **Gateway IP Address** to the IP address of the default router on the network where Avaya IP Office is connected.
- For the **Destination**, select from the drop-down list the Avaya IP Office LAN interface that is used for this route (**LAN1)**.

Click the **OK** button at the bottom of the page (not shown).



5.5. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Avaya SBCE. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.5.1** 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 **Sections 5.5.2** – **5.5.8**.

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

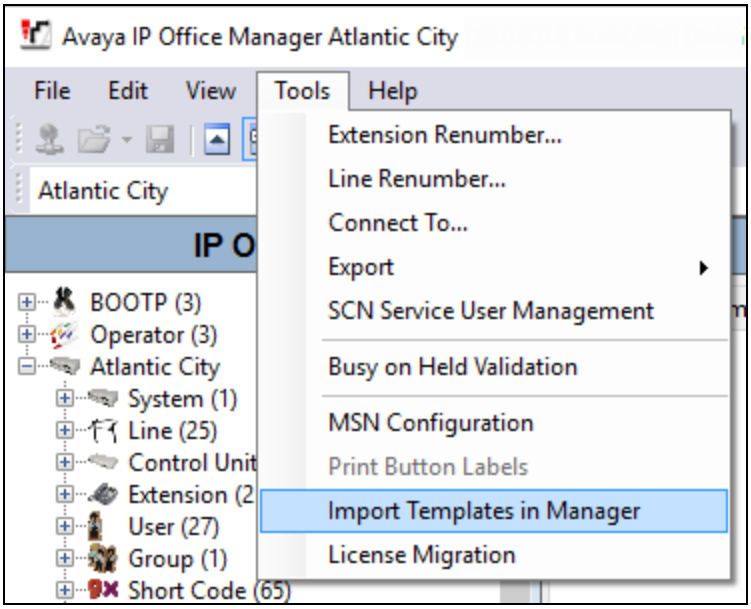
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required
- SIP Advanced
- Engineering

To create a SIP Line manually, right-click **Line** in the Navigation Pane and select **New → SIP Line**; then, follow the steps outlined in **Sections 5.5.2** – **5.5.8**.

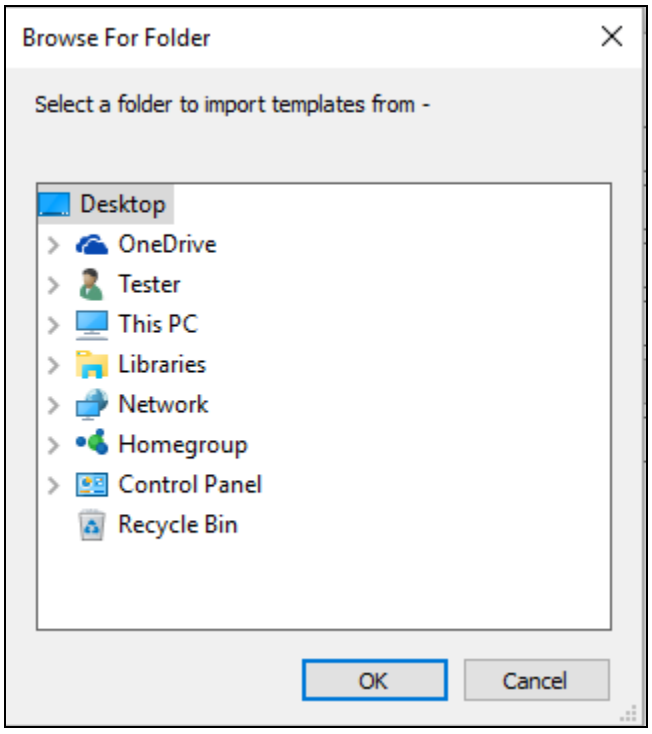
5.5.1. SIP Line From Template

1. Copy the template file to the computer where IP Office Manager is installed. Place it in an empty directory. This is important because **Step 2** will import all templates located in this directory not just the template file associated with these Application Notes.

2. Import the template into IP Office Manager. From IP Office Manager, select **Tools** → **Import Templates in Manager**. This action will copy all the template files located in the selected directory into the IP Office template directory and make the templates available in the IP Office Manager pull-down menus in **Step 3**.



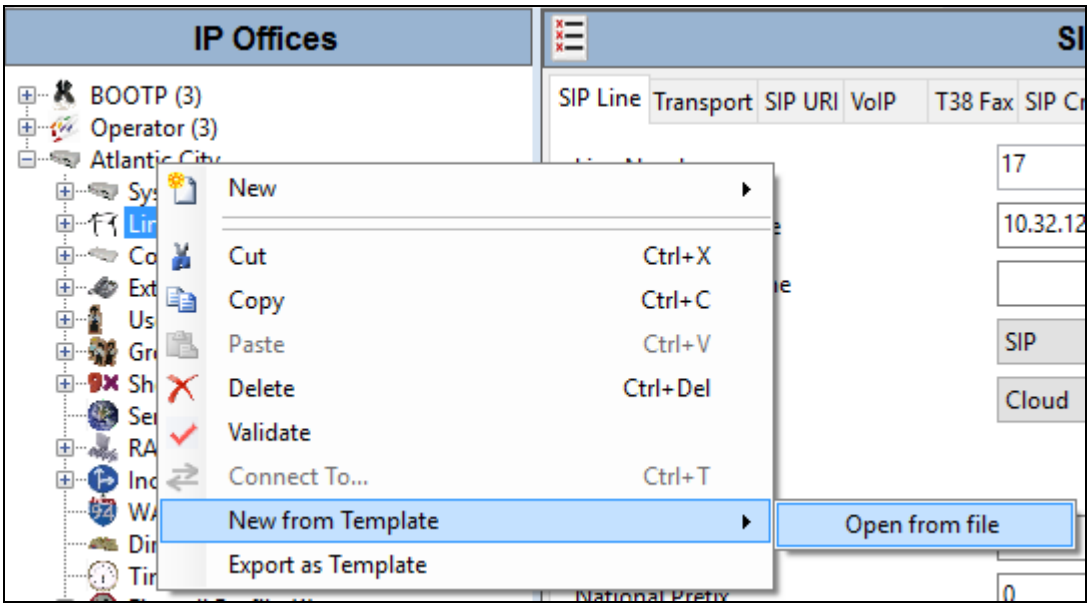
In the pop-up window that appears, select the directory where the template file was copied in **Step 1**, then click **OK**.



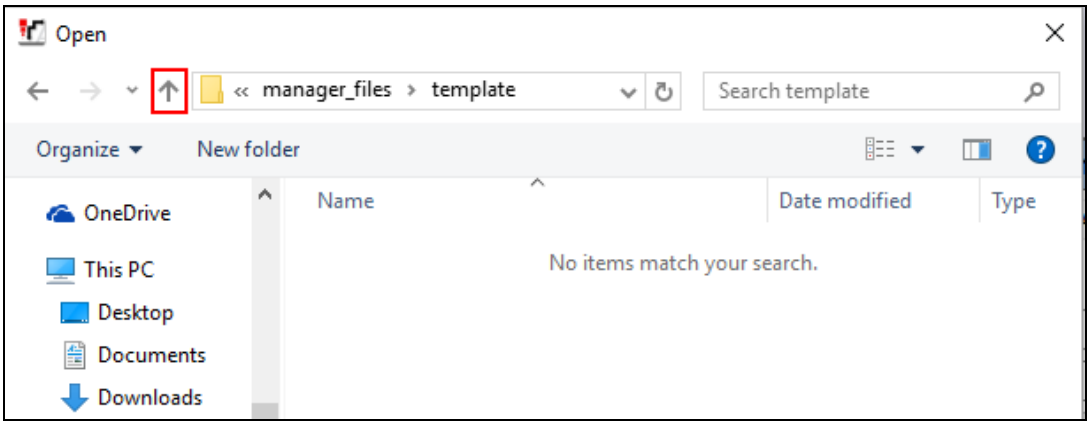
After the import is complete, a final import status pop-up window will appear stating success or failure (not shown). Click **OK** (not shown) to continue.

Note - Within Avaya IP Office Manager menus, the template directory may be accessed by navigating to **C:\Program Files\Avaya\IP Office\Manager\Templates**. However, the template directory is physically located in the User Access Control Virtual Store area of Windows. To view the directory from outside Avaya IP Office Manager (e.g., Windows Explorer), replace the **C:** portion of the template path above with **%UserProfile%\AppData\Local\VirtualStore**.

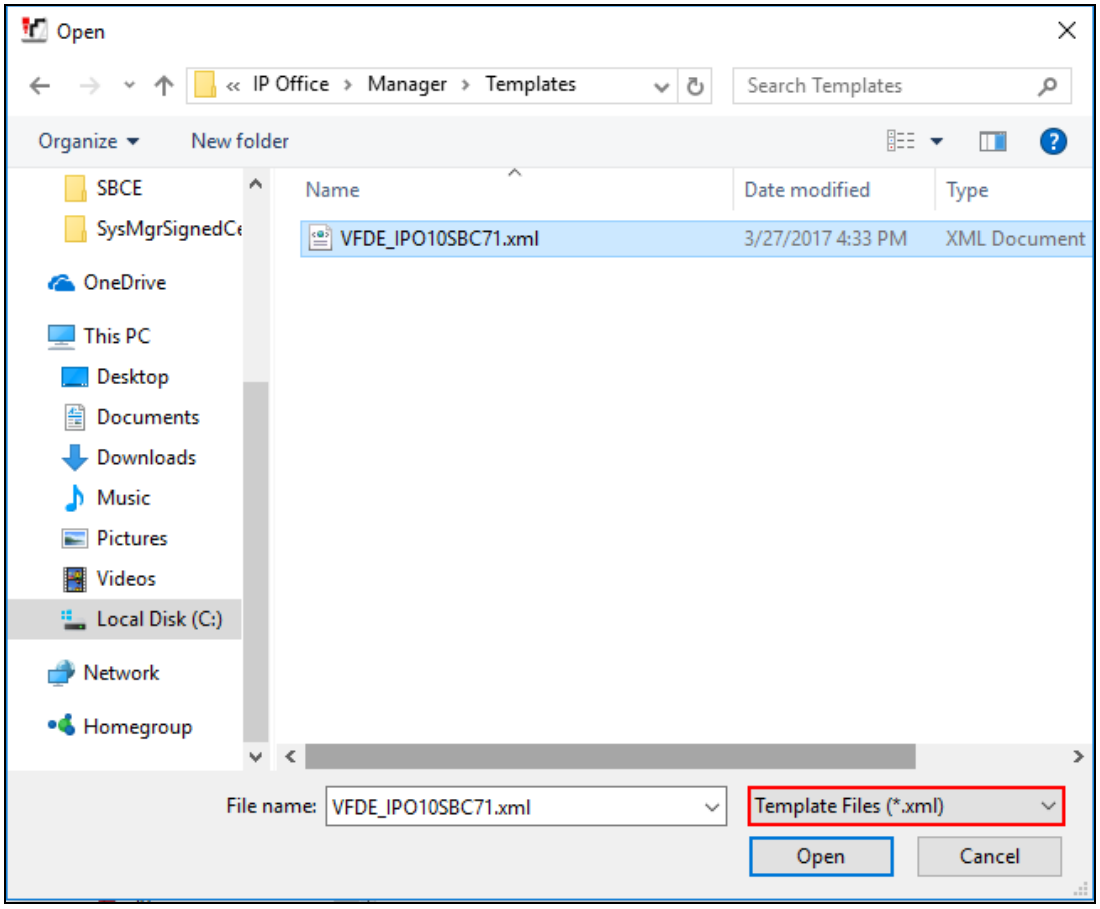
3. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, and select **New From Template → Open File**.



4. The subsequent pop-up window opens to **C:\Program Files\Avaya\IP Office\Manager\manager_files\template**. Navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates**. The up arrow icon can be used to move up through the directory tree.



5. Once reaching the correct directory, select **Template Files (.xml)** in the lower right corner to ensure that .xml template files are displayed. From the list of template files, select the one to be used and click **Open**.



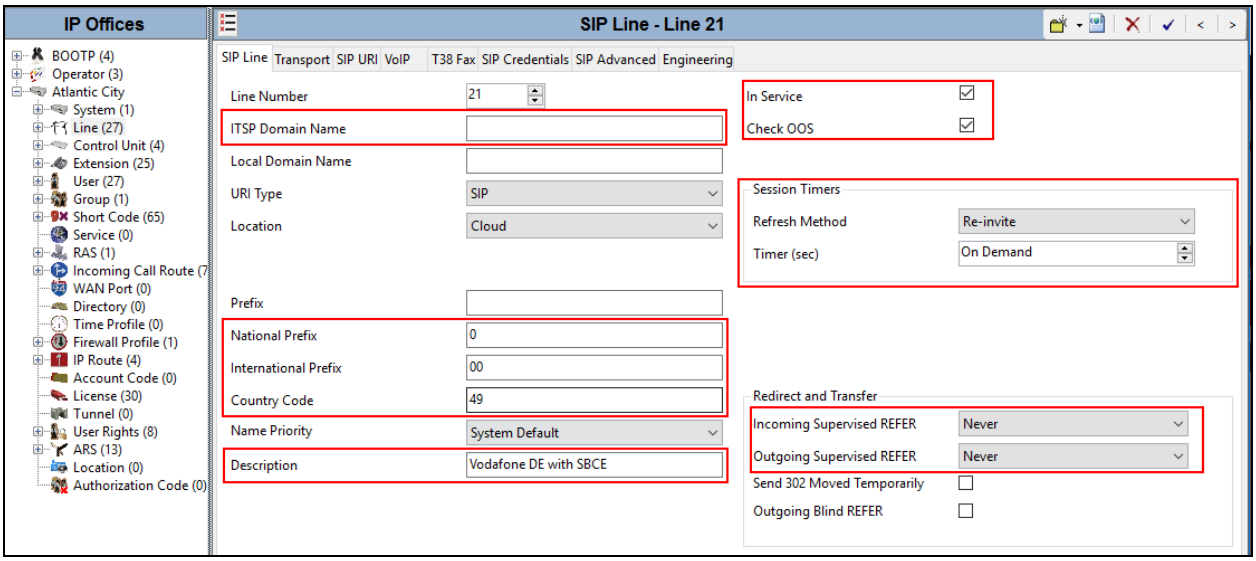
A final status pop-up window will appear stating whether the trunk creation was a success or failure (not shown). Click **OK** (not shown) to continue.

6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.5.2 – 5.5.8**.

5.5.2. SIP Line – SIP Line Tab

On the **SIP Line** tab in the Details Pane, configure or verify the parameters as shown below.

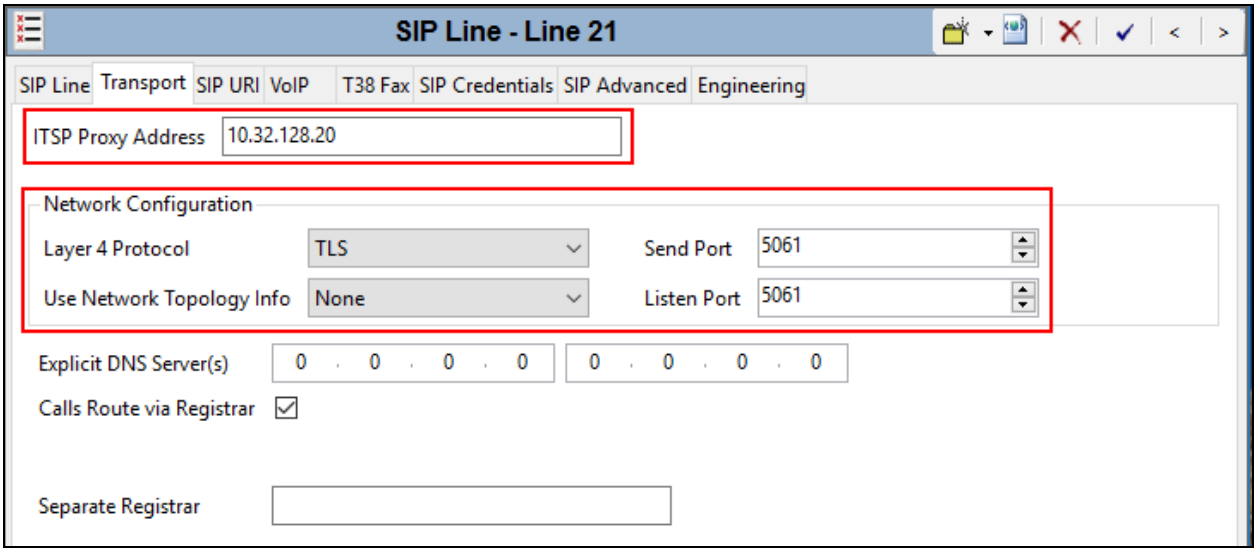
- Set the **ITSP Domain Name** to the IP address of the internal signaling interface of the Avaya SBCE or this field may be left blank. If left blank, Avaya IP Office will automatically use the **ITSP Proxy Address (Section 5.5.3)** for this value which is also set to the IP address of the internal signaling interface of the Avaya SBCE.
- Check the **In Service** box. This makes the trunk available to incoming and outgoing calls.
- Check the **Check OOS** box. Avaya IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Set the **Refresh Method** to **Re-invite** and the **Timer (seconds)** to **On Demand**. This setting will disable session refresh messages from Avaya IP Office. This is recommended based on intermittent failures observed during testing (**Section 2.2**).
- Set the **National Prefix**, **International Prefix**, and **Country Code** to values appropriate for the location. In the case of the compliance test, the **National Prefix** was set to **0**, the **International Prefix** was set to **00** and the **Country Code** was set to **49** (Germany).
- Enter a **Description** for the trunk (optional).
- Set the **Incoming Supervised REFER** field and **Outgoing Supervised REFER** field to **Never** since Vodafone does not support the REFER method.
- Default values may be used for all other parameters.



5.5.3. SIP Line - Transport Tab

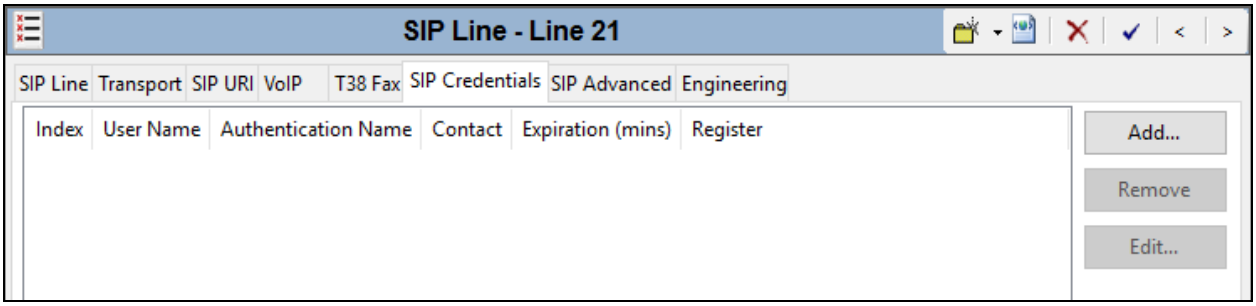
Select the **Transport** tab. Set or verify the parameters as shown below. TLS was used for the signaling connection between Avaya IP Office and the Avaya SBCE.

- Set the **ITSP Proxy Address** to the IP address of the internal signaling interface of the Avaya SBCE.
- Set **Layer 4 Protocol** to **TLS**. To avoid the issue of loss of audio on inbound calls from the PSTN that are call forwarded back to the PSTN (**Section 2.2**), the **Layer 4 Protocol** can be set to **TCP**, as well as setting the media to use RTP instead of SRTP (**Section 5.5.6**)
- Set **Use Network Topology Info** to **None**.
- If **Layer 4 Protocol** is set to **TLS**, then set the **Send Port** and **Listen Port** to **5061**. If **Layer 4 Protocol** is set to **TCP**, then the **Send Port** and **Listen Port** should be set to **5060**.
- Default values may be used for all other parameters.



5.5.4. SIP Line – SIP Credentials

The Vodafone DE SIP Trunk Service does not require SIP credentials for registration or authentication so the **SIP Credentials** tab has no entry.



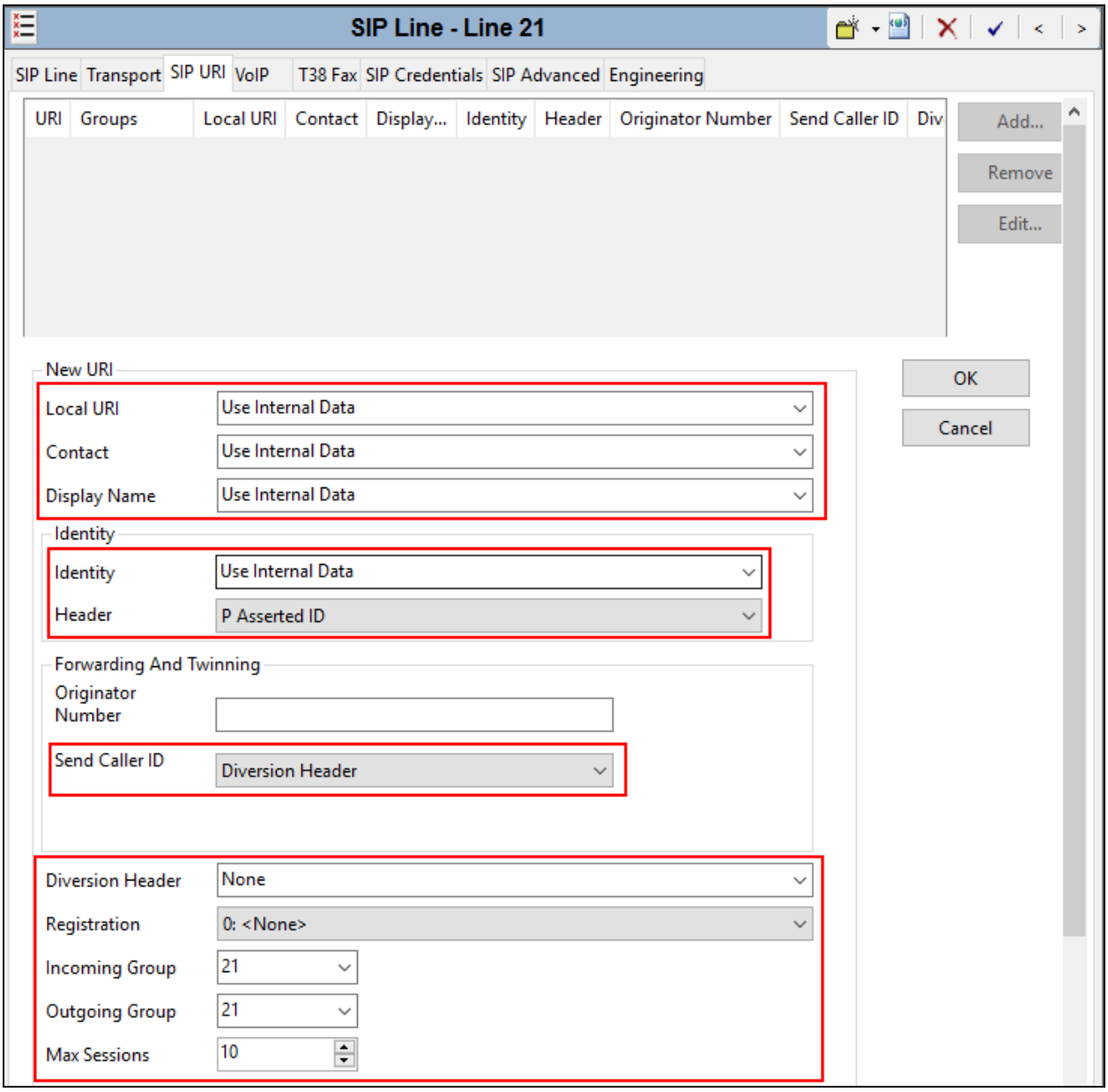
5.5.5. SIP Line - SIP URI Tab

The set of SIP URI entries define which incoming calls will be accepted on the line and provide configuration control of various SIP headers for outbound calls. A single SIP URI can be used for both incoming and outgoing calls but this requires that the **SIP Name** setting on the **User → SIP** tab (used in the From header for outbound calls) must match exactly with what the service provider sends in the Request-Line for inbound calls.

To create the entry for inbound and outbound calls, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**. For outbound calls, these settings will populate the user portion of the From and Contact headers as well as the display name with the contents of the **User → SIP** tab (**Section 5.7**). The From header is populated from the **SIP Name** field, while the Contact header and Display Name are populated from the **Contact** and **Display Name** fields respectively. The **User → SIP** tab is only present if a trunk in the system has a SIP URI using **Internal Data**. The **Local URI** setting also impacts inbound calls. In this case, an inbound call is only accepted if the user portion of the inbound INVITE Request-Line header matches a value configured on the system for a user (**User → SIP**), hunt group (**Hunt Group → SIP**) or voicemail (**System → Voicemail**).
- Under **Identity**, set **Identity** to **Use Internal Data** and **Header** to **P Asserted ID**. This enables the sending of the P-Asserted Identity (PAI) header in each outbound INVITE. The user portion of the PAI header will be populated from the **SIP Name** field on the **User → SIP** tab (**Section 5.7**).
- Under **Forwarding and Twinning**, set **Send Caller ID** to **Diversion Header**. With this setting, Avaya IP Office will include the Diversion header for calls that are forwarded or directed via Mobile Twinning out the SIP Line. The Diversion header will contain the redirecting party which is a DDI provided by the service provider.
- Set **Diversion Header** to **None**. This disables the sending of the Diversion header in each outbound INVITE. The Diversion header is only sent for **Forwarding and Twinning** as described above.
- For the **Registration** field, select **0: <None>** from the pull-down menu.
- 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 in **Section 5.8.1**. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining Automatic Route Selection (ARS) or short code entries for routing outbound traffic to this line in **Section 5.6**. For the compliance test, a new incoming and outgoing group **21** was defined that only contained this line (line 21).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

Click **OK**.

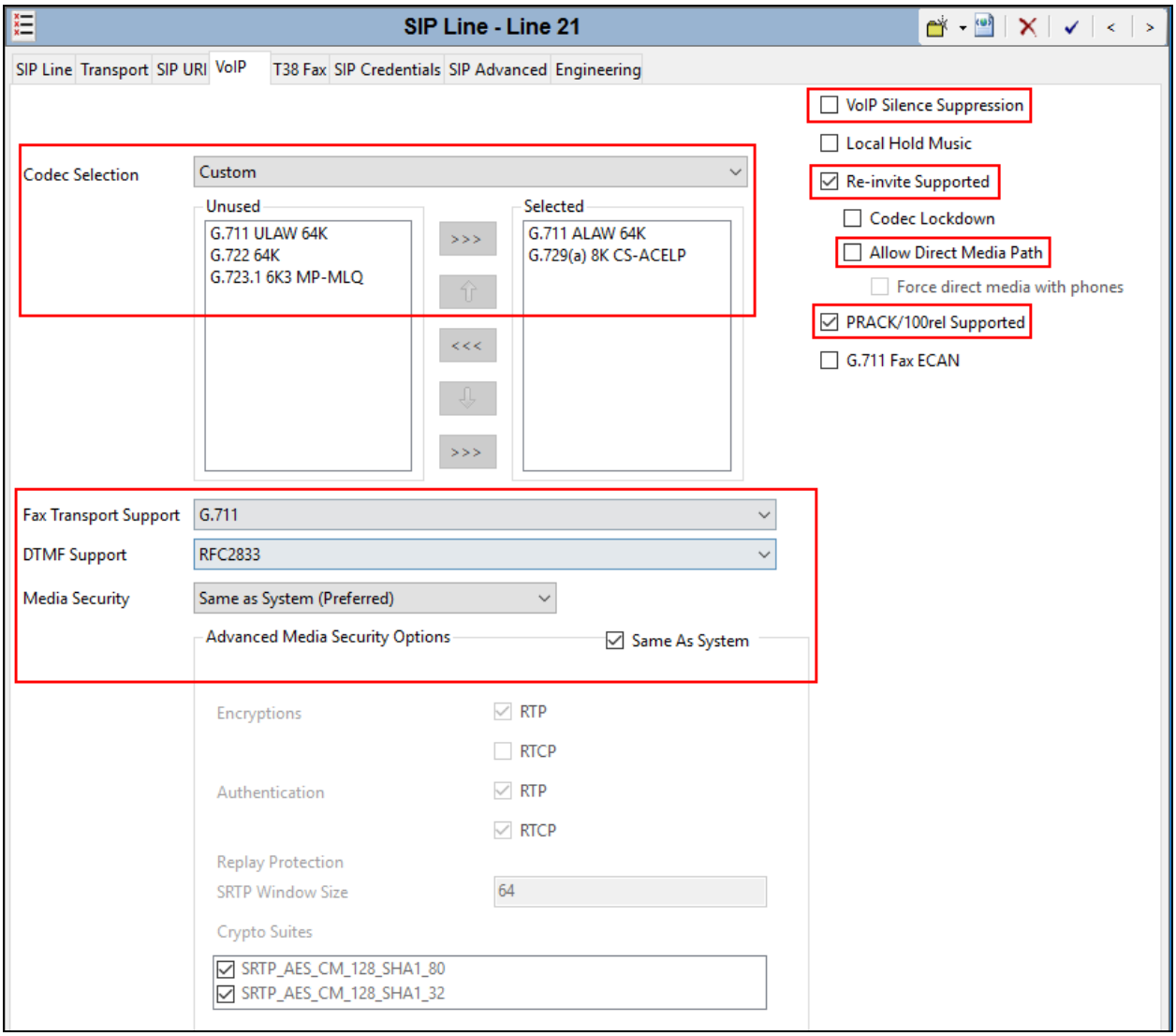


If **Use Internal Data** is selected, additional SIP URIs may be required to allow inbound calls to numbers not associated with a user, such as a short code. These URIs are created in the same manner as shown above with the exception that the incoming DDI number is entered directly in the **Local URI**, **Contact**, and **Display Name** fields.

5.5.6. SIP Line - VoIP Tab

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

- For **Codec Selection**, select **System Default** from the pull-down menu to use the default list of codecs. A list of the codecs in their current order of preference will be shown on the right in the **Selected** column. To use a custom list of codecs, select **Custom** for **Codec Selection**. Next, move unwanted codecs from the **Selected** column to the **Unused** column. Lastly, move the codecs up or down the list in the **Selected** column to achieve the desired order of preference. The example below shows the codecs used for the compliance test. One way to avoid the issue with Avaya 96x1 H.323 phones using SRTP and G.729 documented in **Section 2.2**, is to exclude G.729 in the **Selected** column.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box.
- Verify that **Allow Direct Media Path** is unchecked.
- Check the **PRACK/100rel Supported** option box. This setting enables support by Avaya IP Office for the PRACK (Provisional Reliable Acknowledgement) message on SIP trunks.
- Set the **Fax Transport Support** to **G.711**. T.38 fax is not supported by the Vodafone DE SIP Trunk Service.
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- To use SRTP on the SIP Trunk, set **Media Security** to **Same as System (Preferred)** and verify that the **Same as System** box is checked. The system level media security is set to **Preferred** specifying that SRTP is preferred over RTP. To avoid the issue of loss of audio on inbound calls from the PSTN that are call forwarded back to the PSTN (**Section 2.2**), the SIP trunk can be configured to use RTP. To use RTP on the SIP Trunk, set **Media Security** to **Disabled**. If the trunk is set to use RTP for media, then signaling should be set to use TCP instead of TLS (**Section 5.5.3**).
- Default values may be used for all other parameters.



5.5.7. SIP Line – T38 Fax Tab

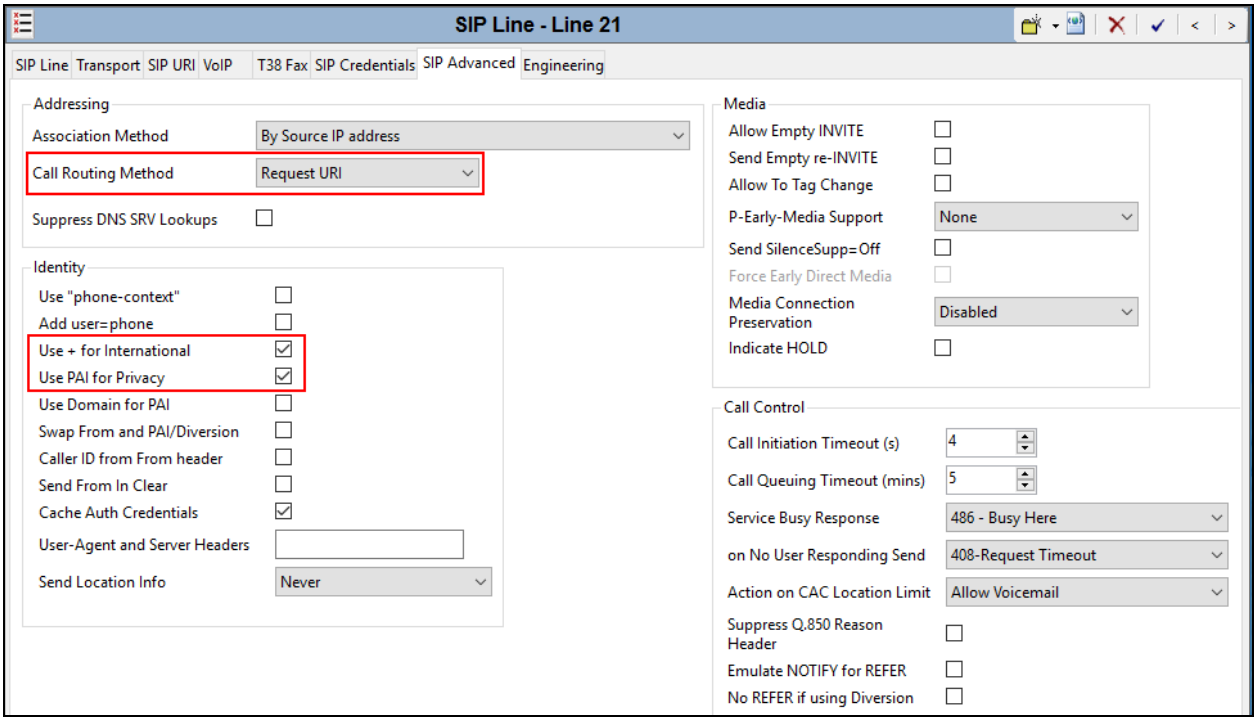
Vodafone DE does not support T.38, so no changes are needed on the **T38 Fax** tab.

5.5.8. SIP Line – SIP Advanced

Select the **SIP Advanced** tab. Set the parameters as shown below.

- Set **Call Routing Method** to **Request URI**. Avaya IP Office will route calls based on the contents of the Request URI in the incoming INVITE.
- Check the **Use + for International** box. In outbound SIP headers, the user dialed international code (in this case 00) will be replaced with a + sign. For example, 0019085551234 will become +19085551234.
- Check the **Use PAI for Privacy** box. By default, Avaya IP Office uses the P-Preferred-ID header (PPI) for privacy calls. When this box is checked, the PAI header is used instead.

Click the **OK** button at the bottom of the page (not shown).

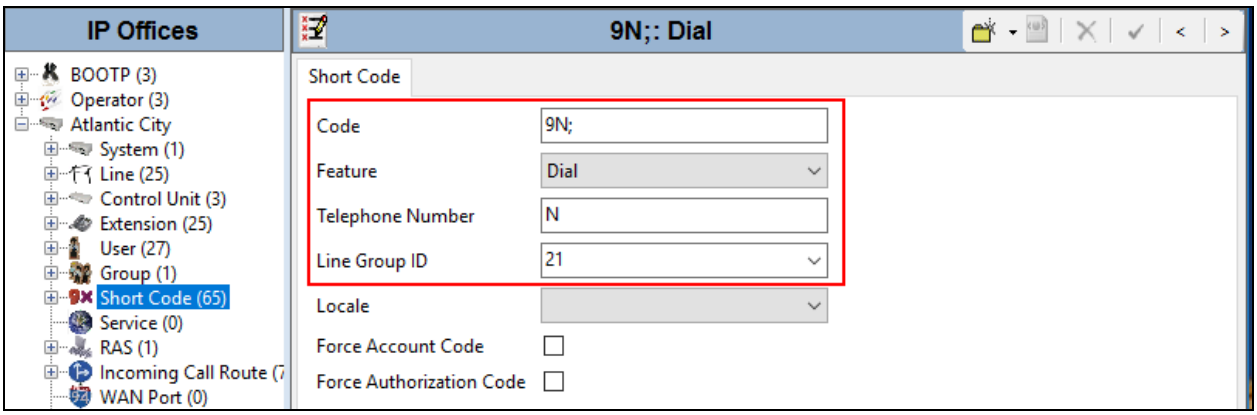


5.6. Short Codes

A short code is a dial pattern that triggers a specific function. A short code is used by the caller to route outbound traffic to a specific trunk or ARS route. To create a short code, right-click on **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.

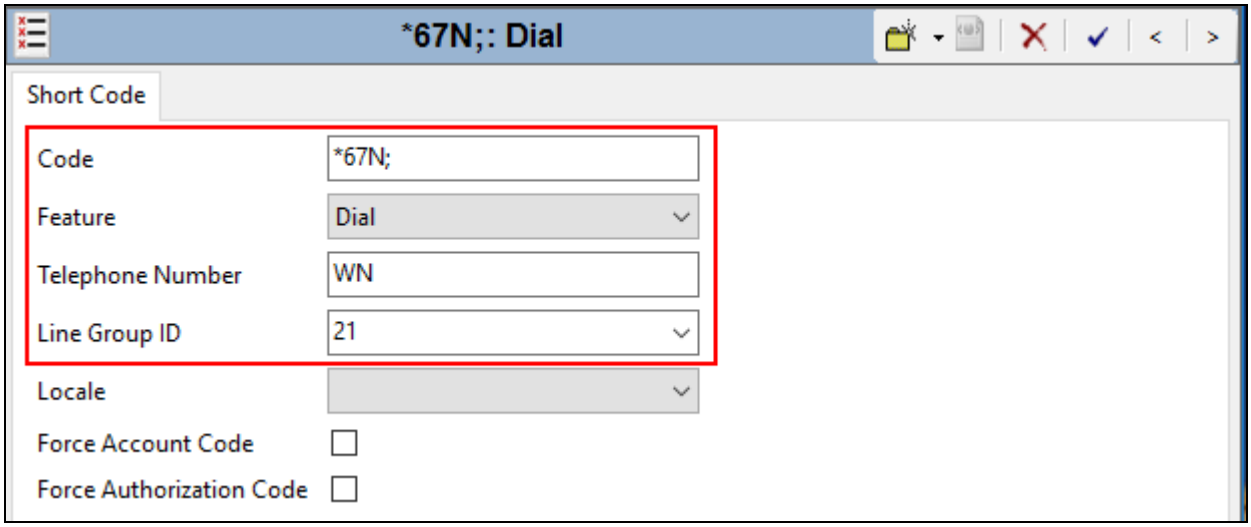
- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **9N;**. This short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to **Dial.** This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value forms the user portion of the Request-Line and To headers of an outbound INVITE.
- Set the **Line Group Id** to the outgoing line group number defined on the SIP URI tab on the SIP Line in **Section 5.5.5**. Alternatively, the **Line Group ID** may point to an ARS route which allows for more comprehensive routing decisions based on the number dialed and available trunks. More information on using ARS may be found in [2].

Click the **OK** button (not shown).



Optionally, add or edit a short code that can be used to access the SIP Line anonymously. In the screen shown below, the short code ***67N;*** is illustrated. This short code is similar to the **9N;** short code except that the **Telephone Number** field begins with the letter **W**, which means "withhold the outgoing calling line identification".

In the case of the SIP Line documented in these Application Notes, when a user dials *67 plus the number, Avaya IP Office will include the calling number in the P-Asserted-Identity (PAI) header and will include the Privacy Id header.



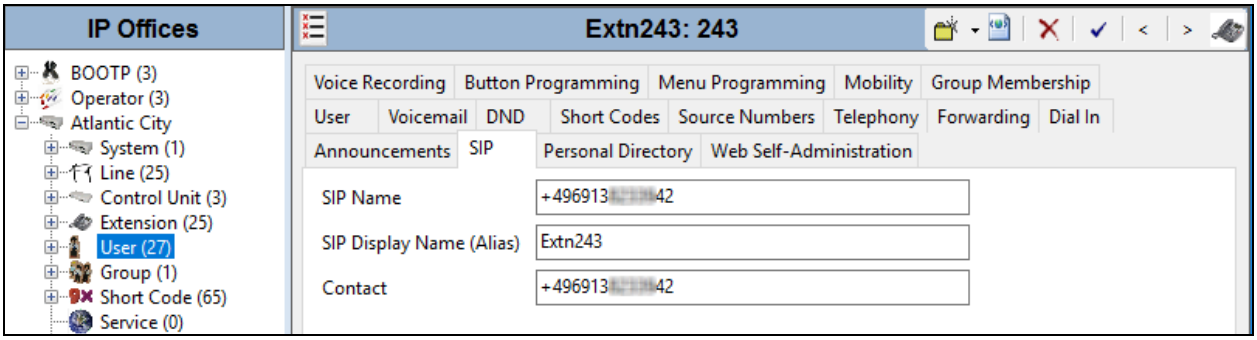
5.7. User

If the SIP Line is configured to use the **Use Internal Data** setting in **Section 5.5.5**, then configure the SIP parameters for each user that will be placing and receiving calls via the SIP line. To configure these settings, first navigate to **User** → *Name* in the Navigation Pane where *Name* is the name of the user to be modified. In the example below, the name of the user is **Extn243**. Select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers for outgoing SIP trunk calls. The value entered in the **SIP Name** field is also used in the PAI and Diversion headers.

The example below shows the settings for user **Extn243**. The **SIP Name** and **Contact** are set to one of the DDI numbers assigned to the enterprise from Vodafone DE in international format.

The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network.

Click the **OK** button (not shown).



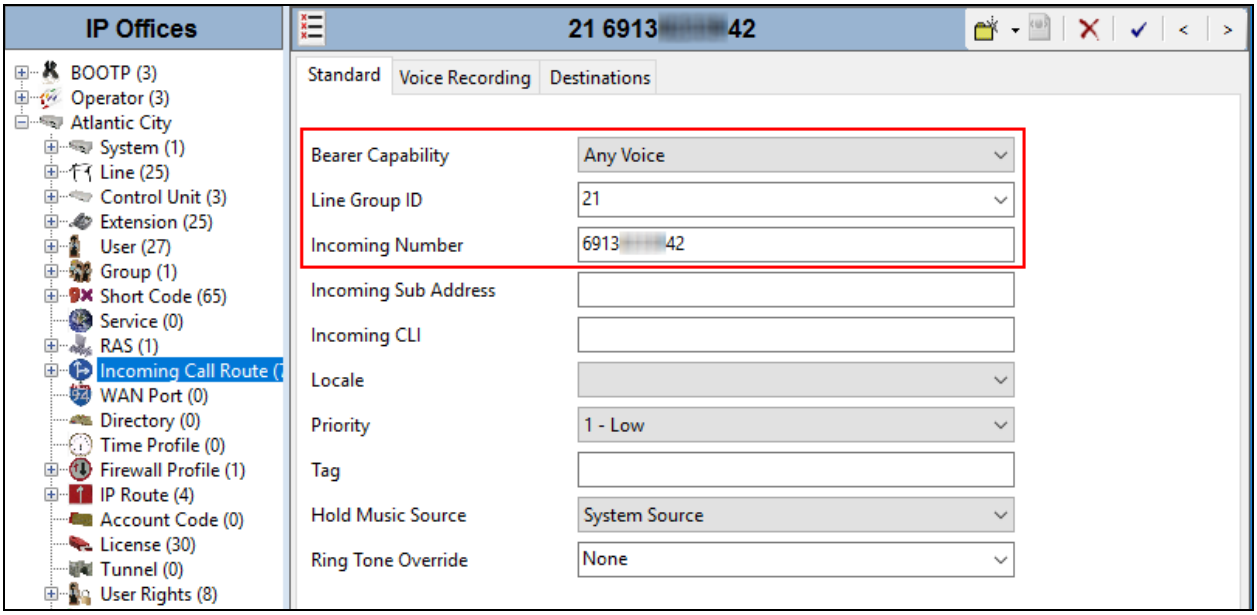
5.8. Incoming Call Route

An incoming call route maps an inbound DDI number on a specific line to an internal extension. This procedure should be repeated for each DDI number provided by the service provider. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**.

5.8.1. Incoming Call Route – Standard Tab

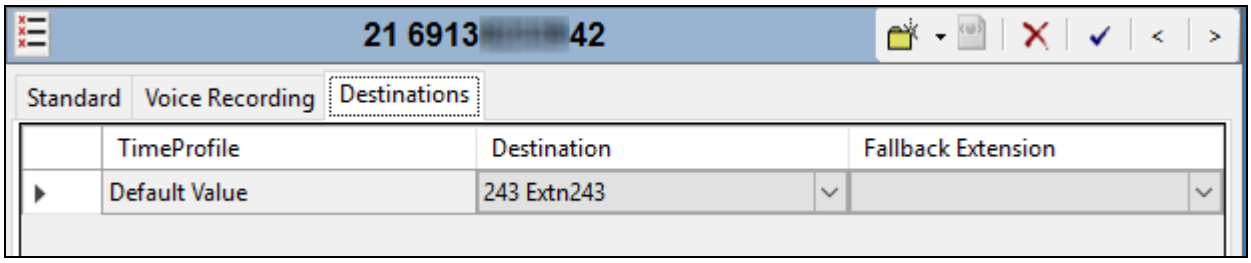
On the **Standard** tab of the Details Pane, enter the parameters as shown below.

- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.5.5**.
- Set the **Incoming Number** to the incoming number on which this route should match. The matching is performed from right to left. Thus, the local number was entered without the 0 prefix so it would match the number in local format (06913xxxxx42) or international format (+496913xxxxx42).
- Default values can be used for all other fields.



5.8.2. Incoming Call Route – Destinations Tab

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. Click the **OK** button (not shown). In this example, incoming calls to this number on line **21** are routed to extension **243**.

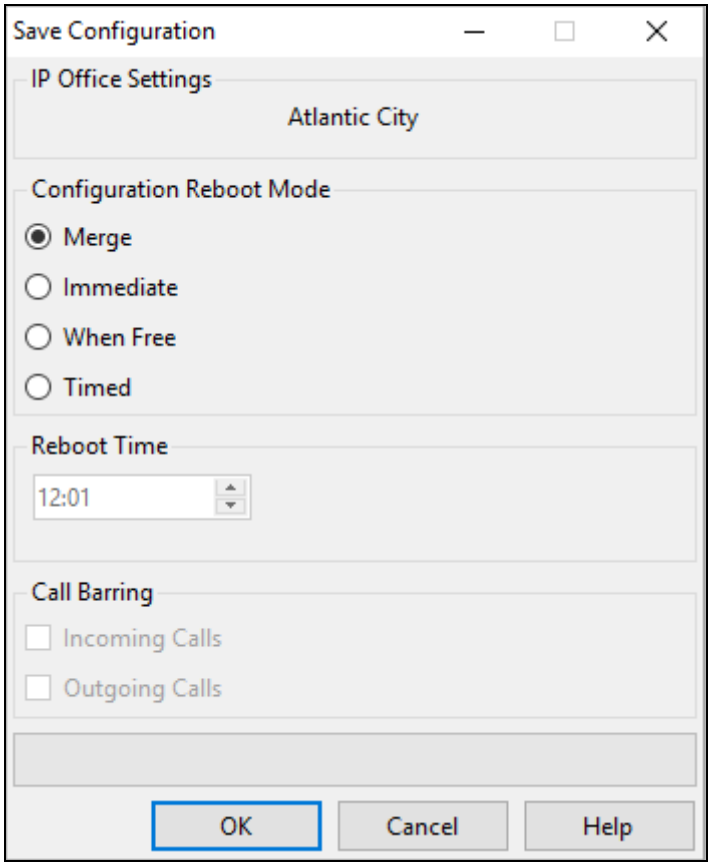


Incoming Call Routes for other direct mappings of DDI numbers to Avaya IP Office users listed in **Figure 1** are omitted here, but can be configured in the same fashion.

5.9. 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.

The following will appear, with either **Merge** or **Immediate** selected, 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 proceed.



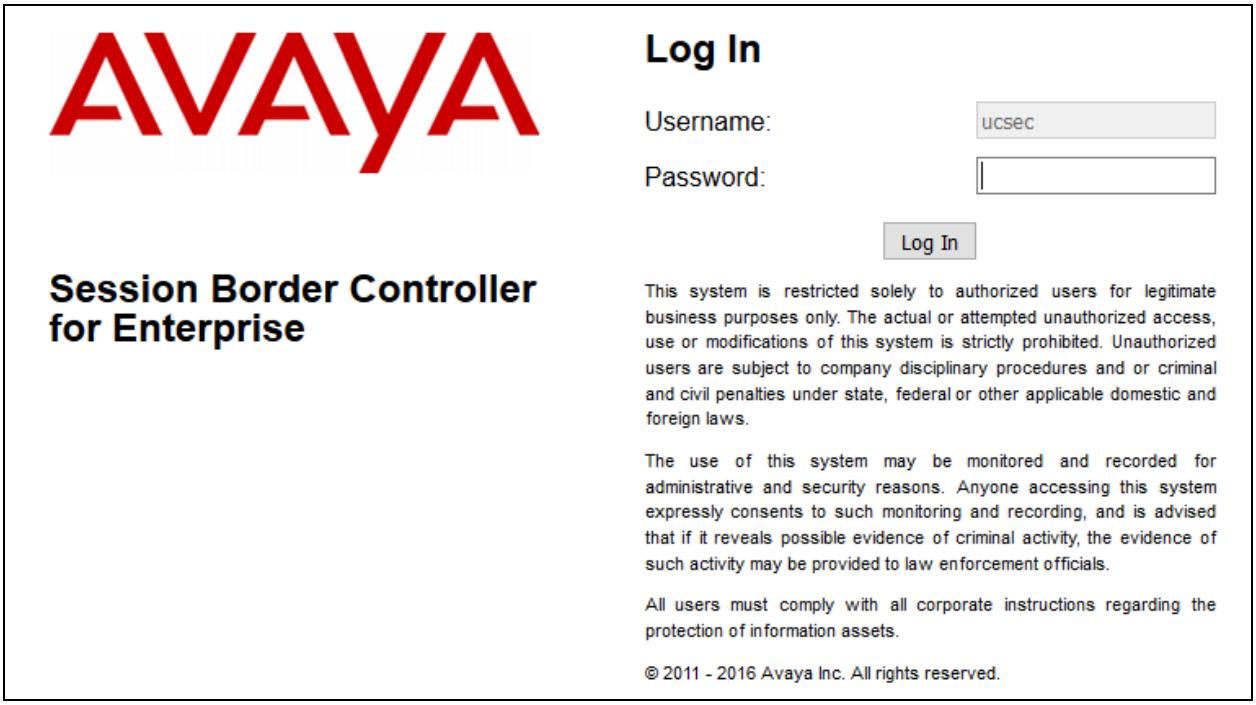
6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed, including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (i.e., A1 and B1).

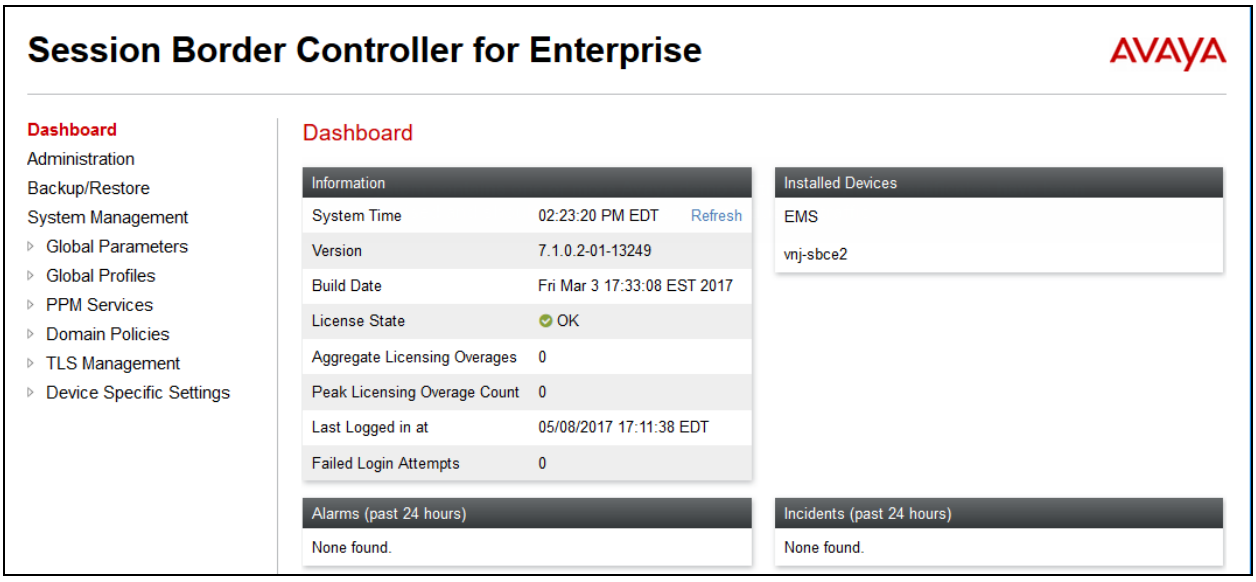
On all screens described in this section, it is to be assumed that parameters are left at their default values unless specified otherwise.

6.1. Access the Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The Avaya SBCE login page will appear as shown below. Log in with the appropriate credentials.

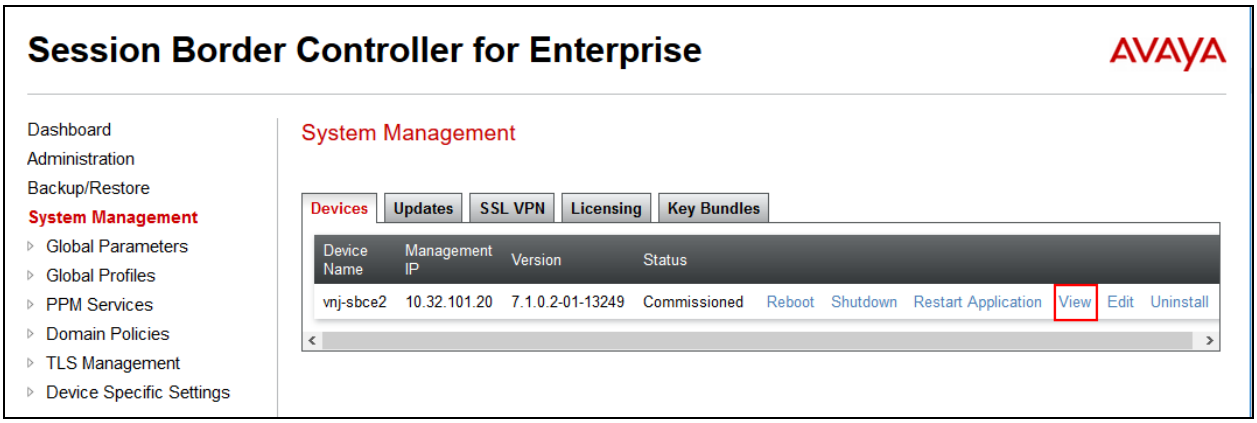


After logging in, the Dashboard screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

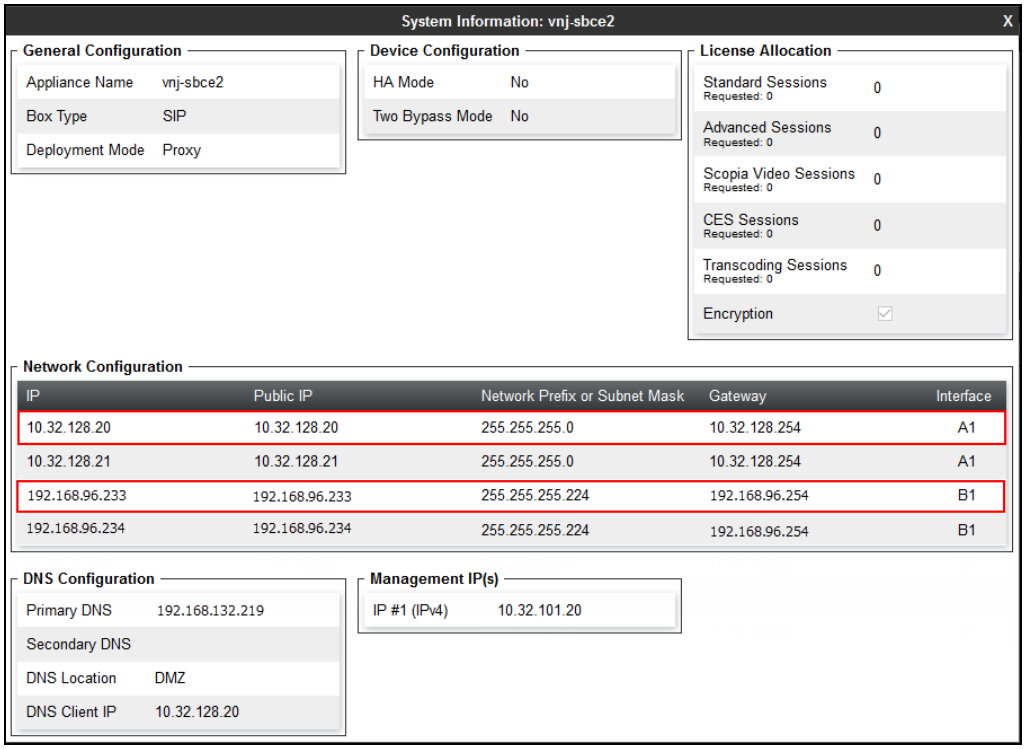


6.2. Verify Network Configuration and Enable Interfaces

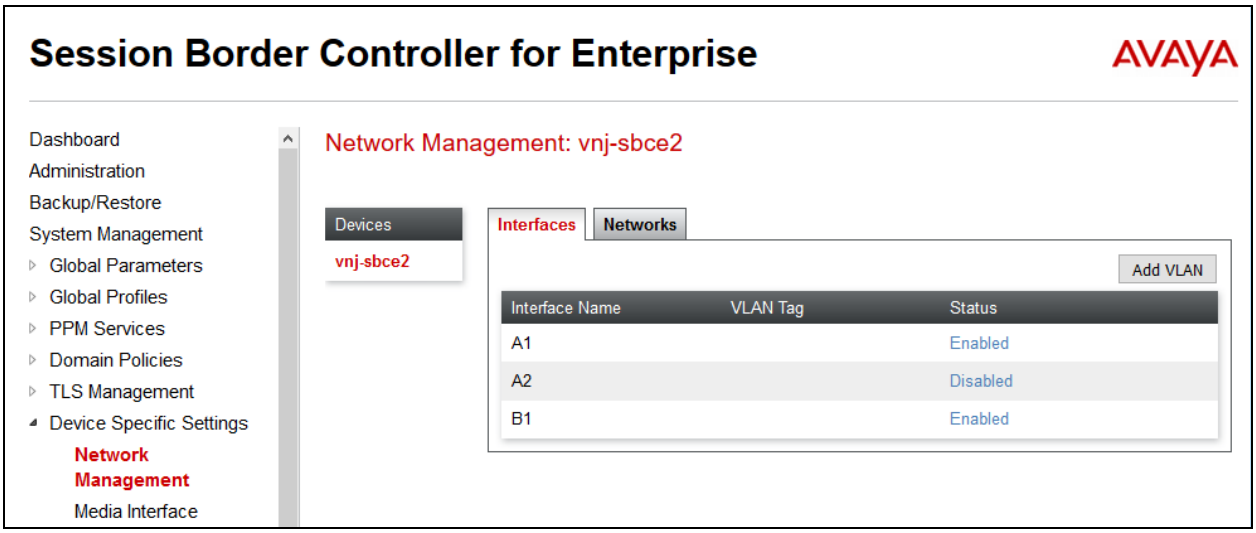
To view the network information provided during installation, navigate to **System Management**. In the right pane, click **View** highlighted below.



A System Information page will appear showing the information provided during installation. The **Appliance Name** field is the name of the device (**vnj-sbce2**). This name will be referenced in other configuration screens. Interfaces **A1** and **B1** highlighted below represent the private (or internal) and public (or external) interfaces of the Avaya SBCE for SIP Trunking. Each of these interfaces must be enabled after installation. Note that the **Management IP** is on a different subnet than either the A1 and B1 interfaces.



To enable the interfaces, first navigate to **Device Specific Settings → Network Management** in the left pane and select the device being managed in the center pane. In the right pane, click on the **Interfaces** tab. Verify the **Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click the **Disabled** status to enable the interface.



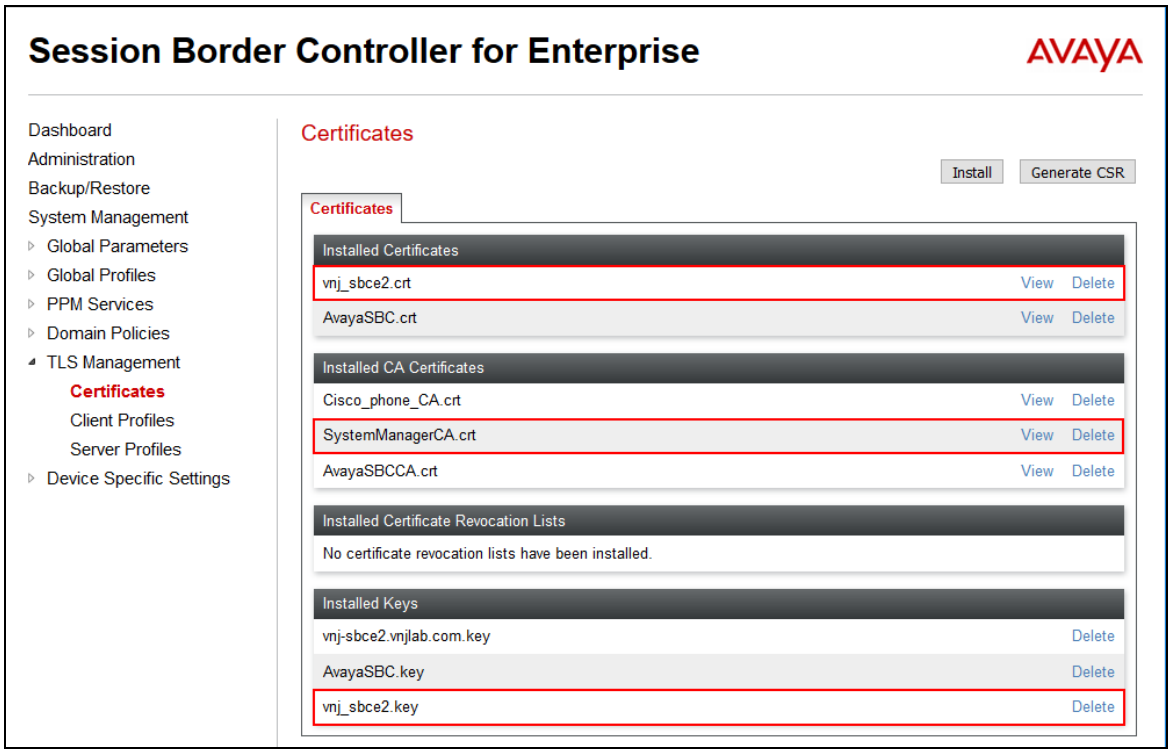
6.3. TLS Management

For the compliance test, the signaling on the SIP trunk between Avaya IP Office and the Avaya SBCE was secured using TLS. Testing was done using identity certificates signed by a local certificate authority **SystemManager CA**. The generation and installation of these certificates are beyond the scope of these Application Notes. However, once the certificates are available, the following sections show how to view the certificates and configure the profiles to support the TLS connection.

6.3.1. Certificates

To view the certificates currently installed on the Avaya SBCE, navigate to **TLS Management → Certificates**. Perform the following:

- Verify that an Avaya SBCE identity certificate (**vnj_sbce2.crt**) is present under **Installed Certificates**.
- Verify that certificate authority root certificate (**System ManagerCA.crt**) is present under **Installed CA certificates**.
- Verify that private key associated with the identity certificate (**vnj_sbce2.key**) is present under **Installed Keys**.



Lastly, verify the Avaya SBCE identity certificate (**vnj_sbce2.crt**) was signed/issued by the certificate authority **System Manager CA**. Click **View** next to the identity certificate (**vnj_sbce2.crt**) to see the details of the certificate.

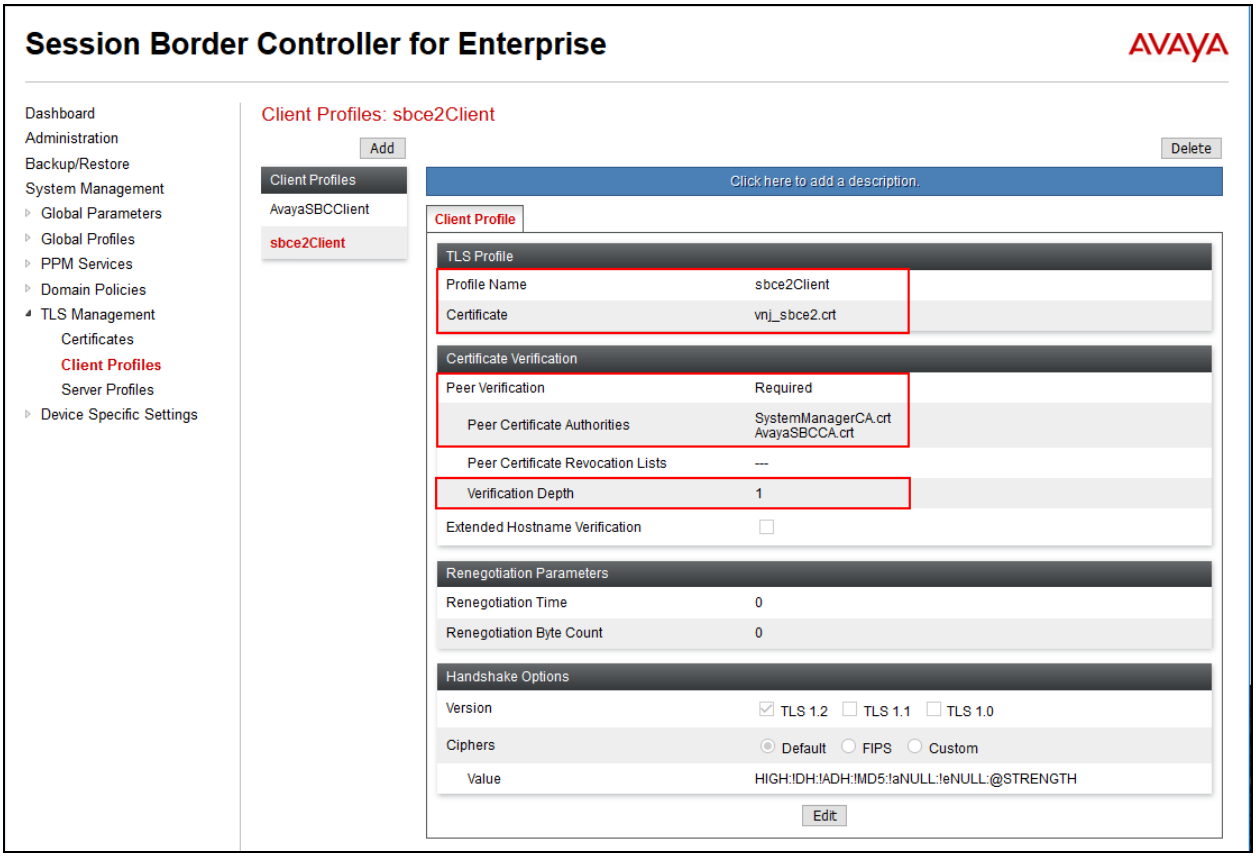
A pop-up window will appear showing that the **vnj_sbce2.crt** identity certificate was signed by **SystemManager CA**. Close the pop-up window.

6.3.2. Client Profile

To create a new profile, navigate to **TLS Management → Client Profile** in the left pane. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, client profile **sbce2Client** was created. This profile will be applied to the Avaya IP Office server configuration in **Section 6.7.1**. When configuring the profile, configure the parameters as follows:

- Set **Profile Name** to a descriptive name.
- Set **Certificate** to the identity certificate (**vnj_sbce2.crt**) to be sent by the Avaya SBCE.
- Set **Peer Verification** to **Required**.
- From the list of **Peer Certificate Authorities**, select the certificate authorities which will be accepted as signers of an incoming identity certificate from the far-end. For the test environment, the list must include **SystemManagerCA.crt** who is the signer of the Avaya IP Office identity certificate.
- Set **Verification Depth** to **1**.

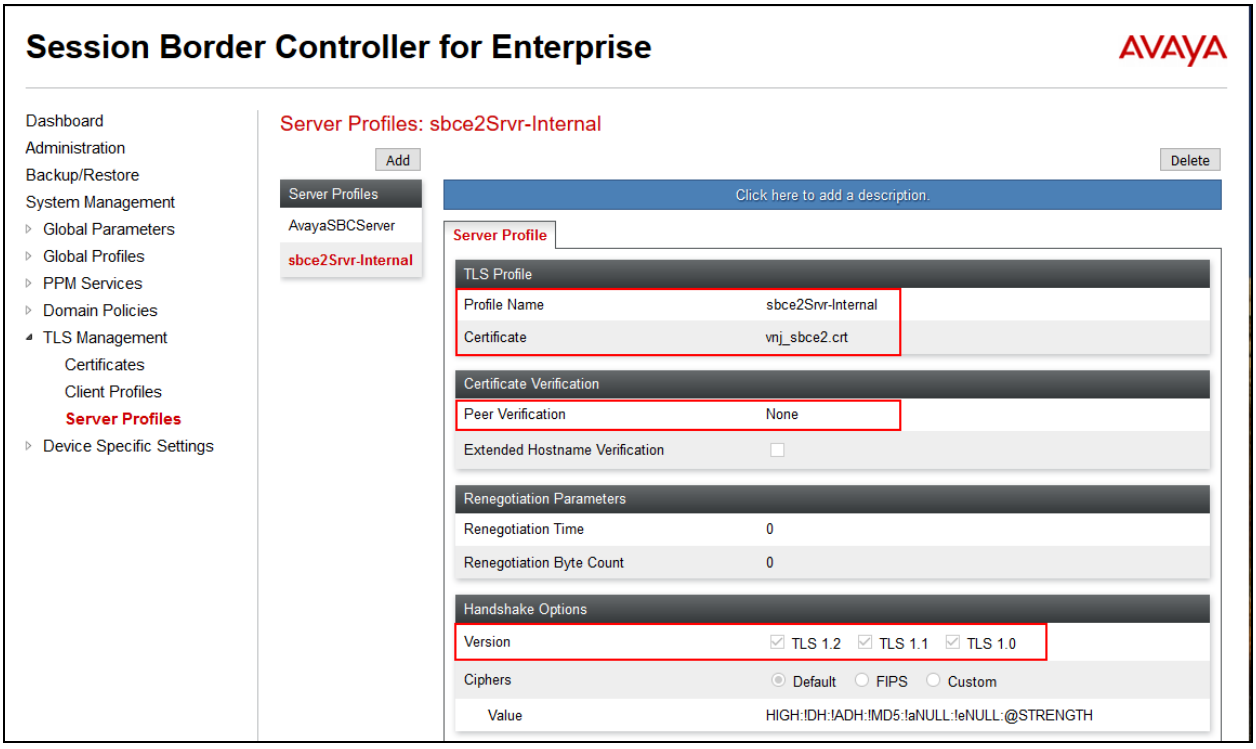


6.3.3. Server Profile

To create a new profile, navigate to **TLS Management → Server Profile** in the left pane. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, client profile **sbce2Srvr-Internal** was created. This profile will be applied to the Avaya SBCE internal signaling interface in **Section 6.4**. When configuring the profile, configure the parameters as follows:

- Set **Profile Name** to a descriptive name.
- Set **Certificate** to the identity certificate (**vnj_sbce2.crt**) to be sent by the Avaya SBCE.
- Set **Peer Verification** to **None**.
- Set **Verification Depth** to **1**.
- Under Handshake Options, for **Version** check the **TLS 1.0** box in addition to the **TLS 1.2** and **TLS 1.1** boxes to include TLS 1.0 as an acceptable TLS version for the connection. This is needed to support Avaya Communicator for Windows as a remote worker since it only supports TLS 1.0.



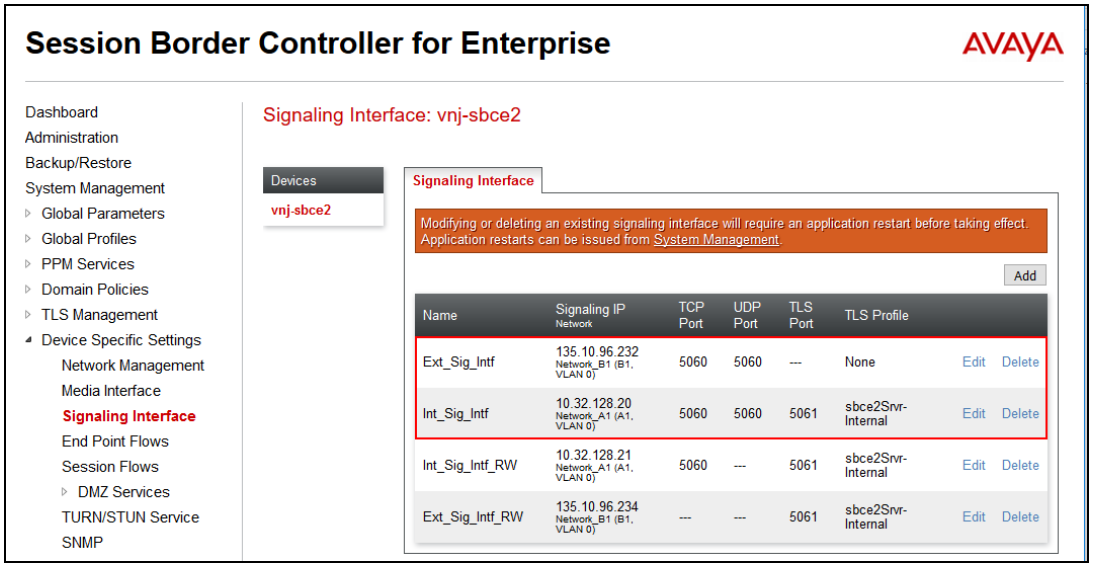
6.4. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**vnj-sbce2**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int_Sig_Intf** was created for the Avaya SBCE internal interface and signaling interface **Ext_Sig_Intf** was created for the Avaya SBCE external interface. These two signaling interfaces are highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Signaling IP** to the IP address associated with the private interface (A1) specified in **Section 6.2**. For the external interface, set the **Signaling IP** to the IP address associated with the public interface (B1) specified in **Section 6.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port the Avaya SBCE will listen on for each transport protocol. The internal interface was configured to listen for UDP or TCP on port **5060** and TLS on **5061**. Since TLS was selected, the **TLS profile** was set to **sbce2Svr-Internal** which point to the proper TLS certificate. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port **5060**. Since Vodafone DE uses UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE external interface for UDP only.



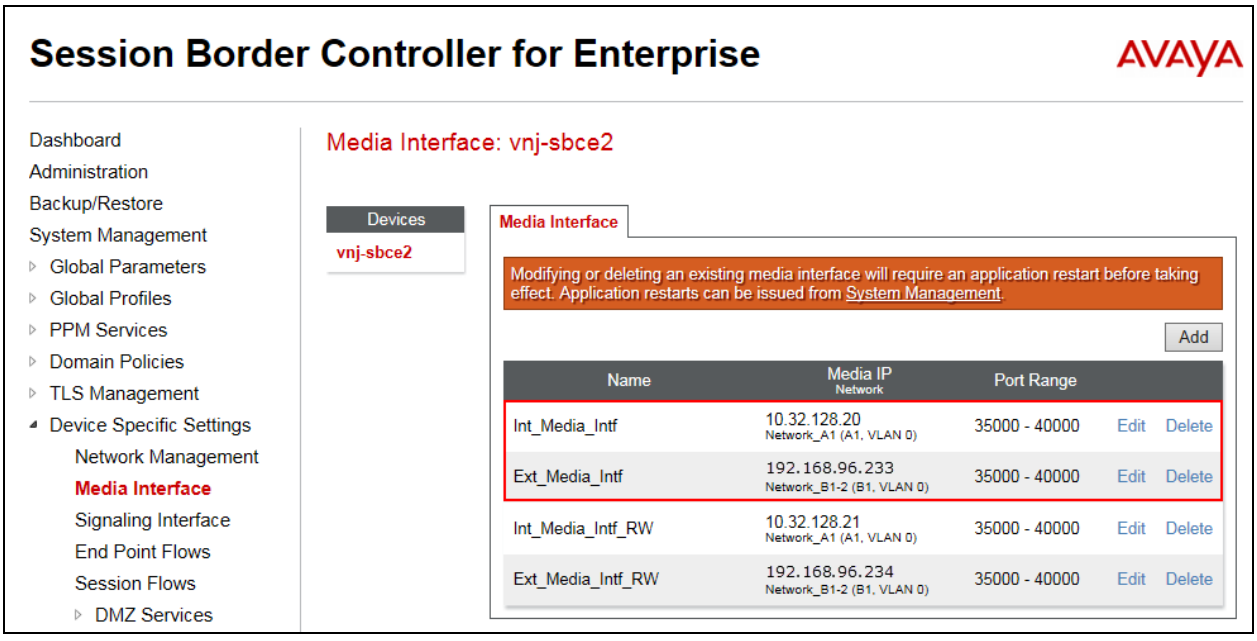
6.5. Media Interface

A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**vnj-sbce2**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, media interface **Int_Media_Intf** was created for the Avaya SBCE internal interface and media interface **Ext_Media_Intf** was created for the Avaya SBCE external interface. Each is highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Media IP** to the IP address associated with the private interface (A1) specified in **Section 6.2**. For the external interface, set the **Media IP** to the IP address associated with the public interface (B1) specified in **Section 6.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the far end. For the compliance test, the default port range was used for both interfaces.



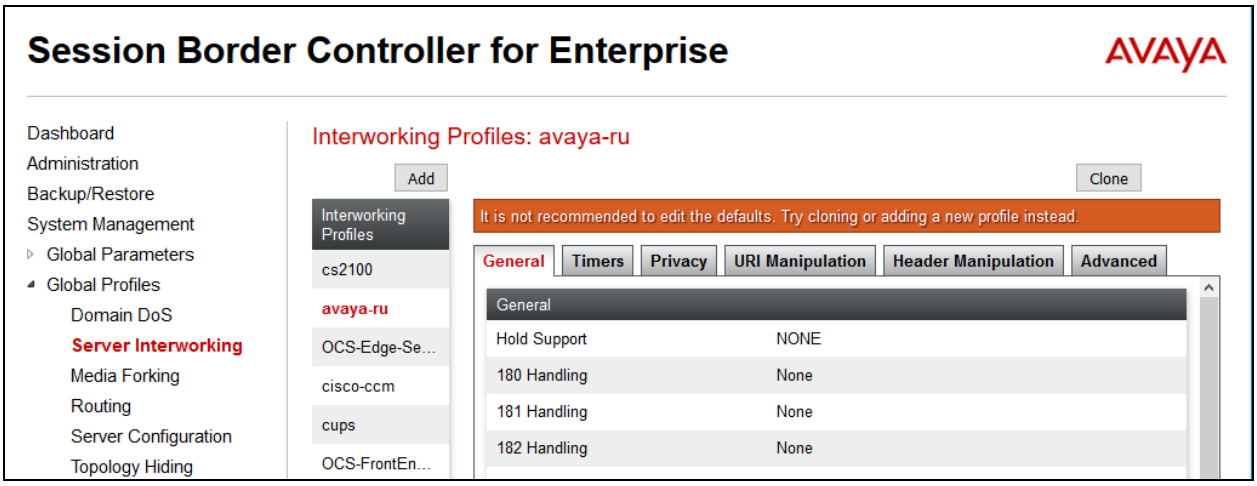
6.6. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create one server interworking profile for Avaya IP Office and another for the service provider SIP server. These profiles will be applied to the appropriate servers in **Section 6.7.1** and **6.7.2**.

To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed.

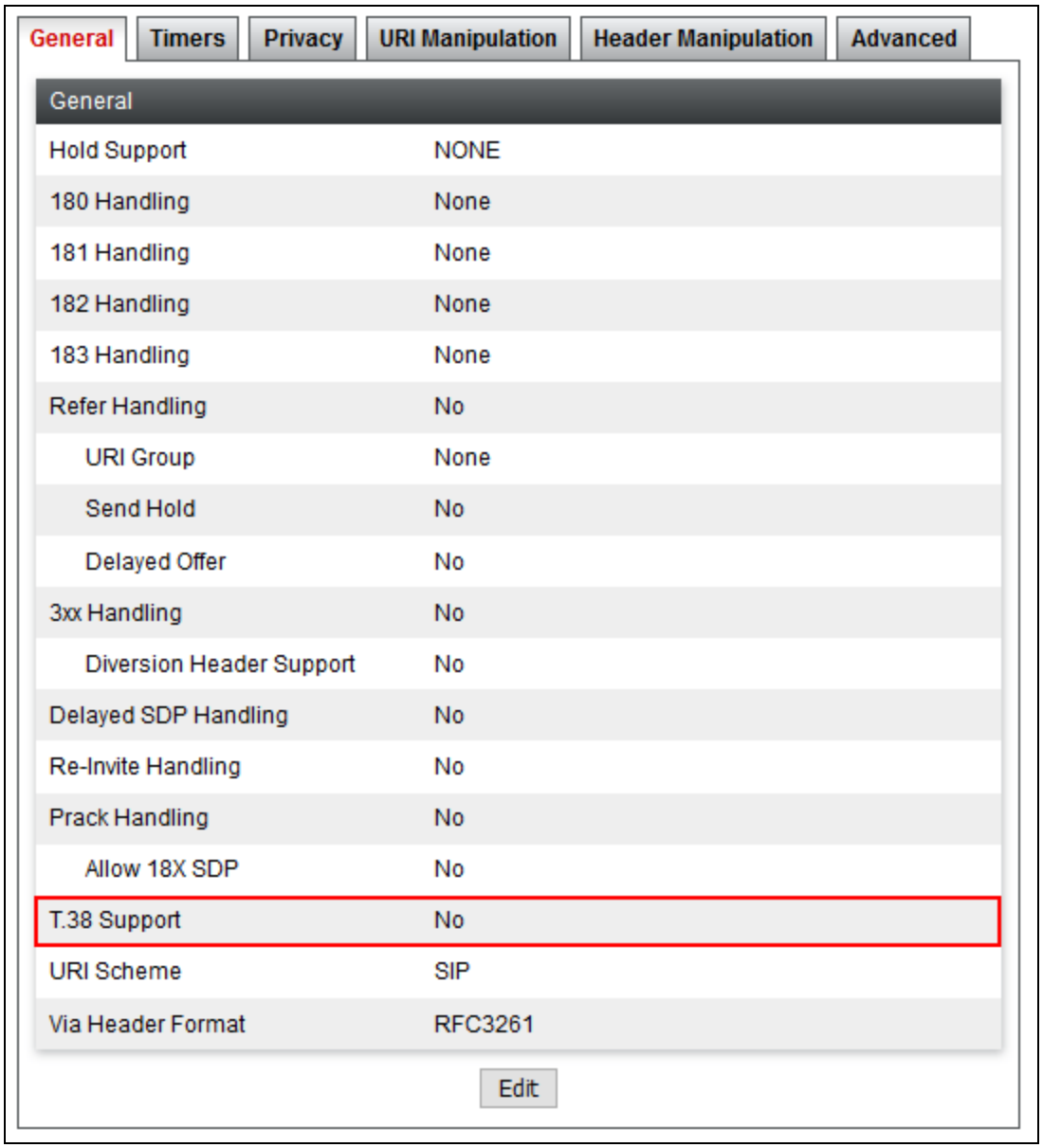
To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the user interface as described above, before creating the specific server interworking profiles used for the compliance test.



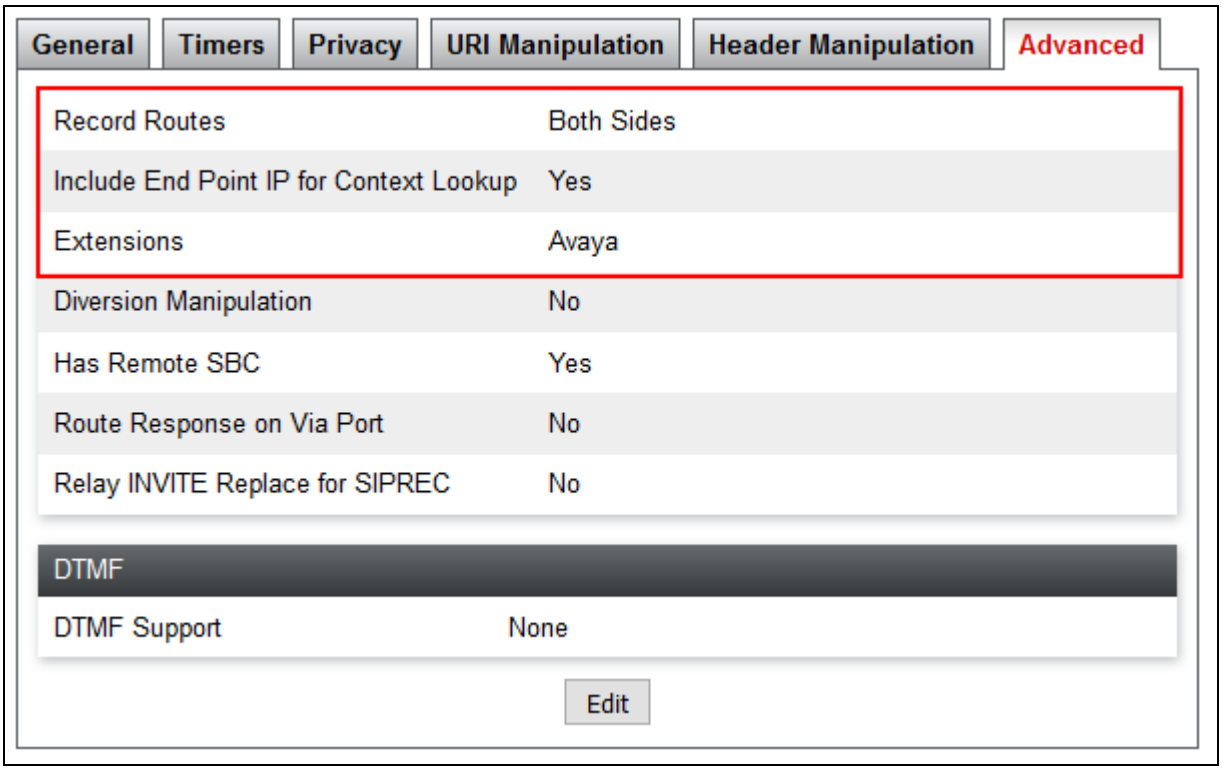
6.6.1. Server Interworking – Avaya IP Office

The recommended method of creating a server interworking profile for Avaya IP Office is to first clone the predefined profile **avaya-ru** and then make any changes necessary to support a specific service provider. For the compliance test, server interworking profile **IPOffice** was created for Avaya IP Office using this approach and **T.38 Support** parameter was set to **No**. The **General** tab parameters are shown below.



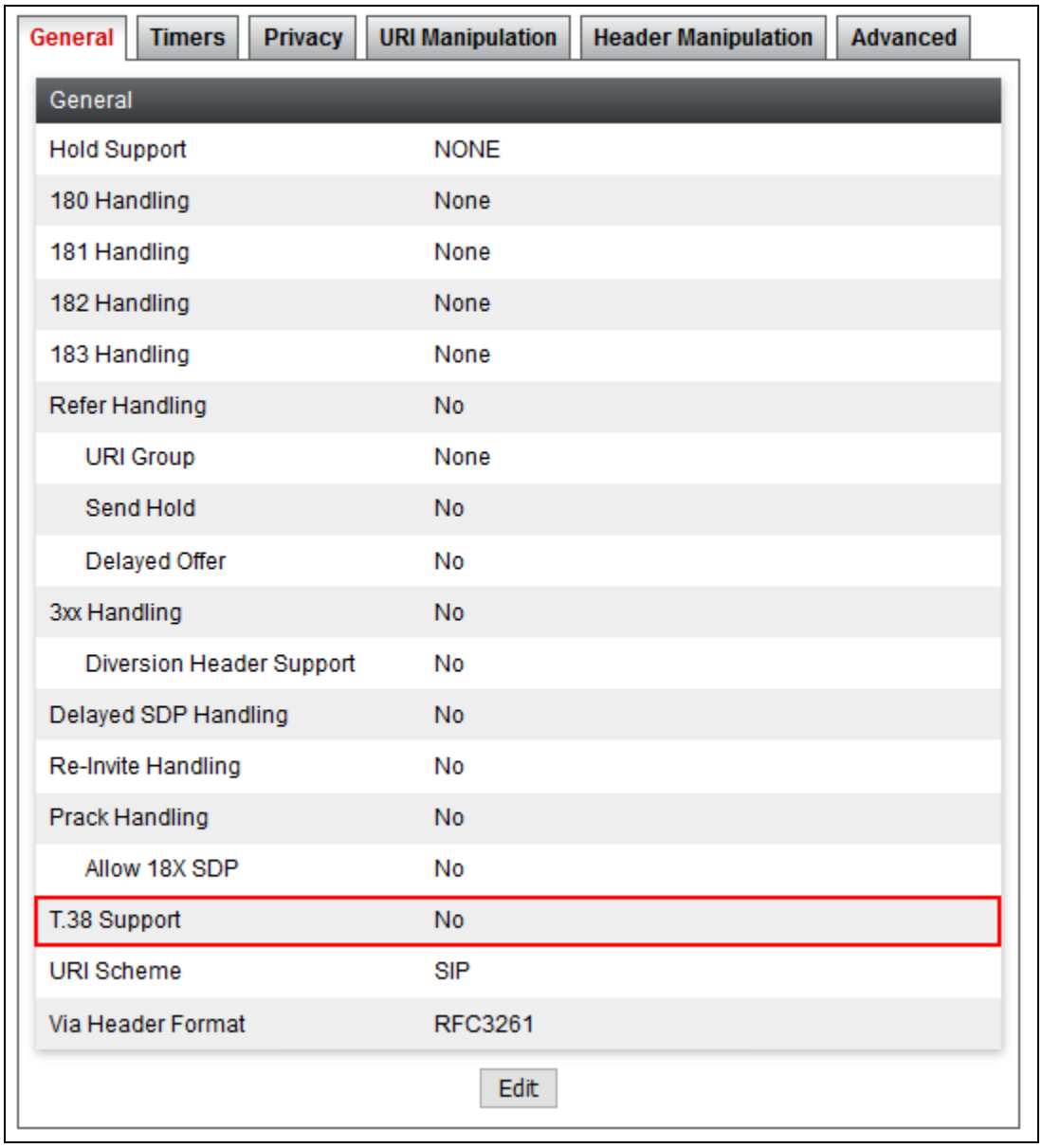
The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs use default values.

The **Advanced** tab parameters are shown below. Highlighted values below indicate differences between the cloned profile and the default value.



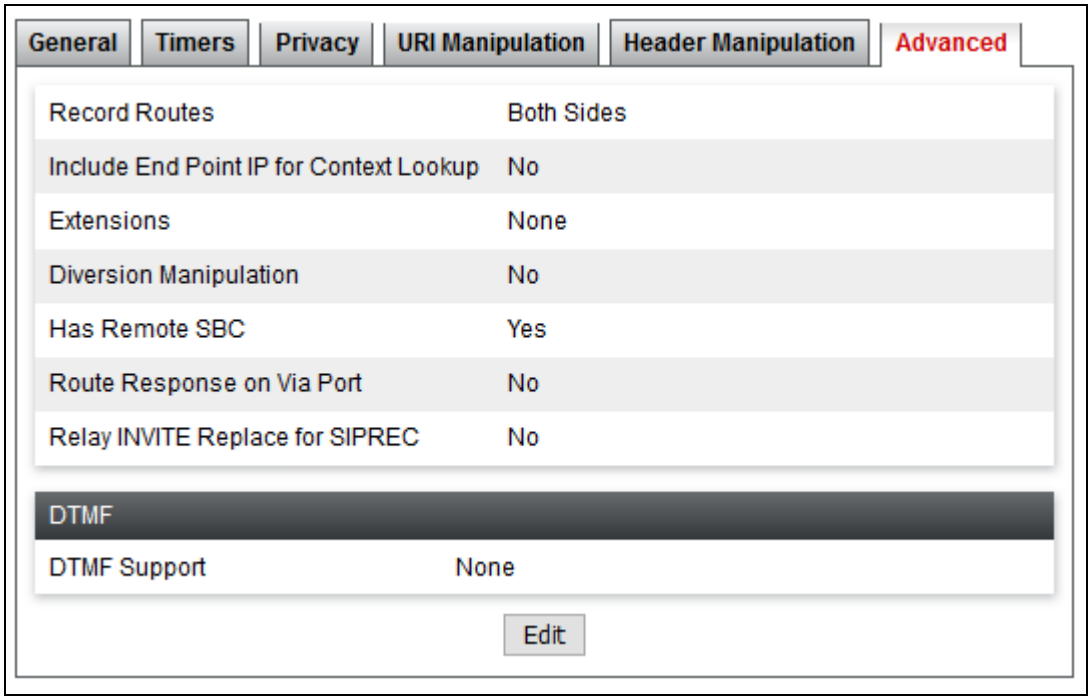
6.6.2. Server Interworking – Vodafone DE

For the compliance test, server interworking profile **VF-DE-Intwk** was created for the Vodafone DE SIP server. To create the profile, click **Add** (not shown). When creating the profile, the default values were used for all parameters including that the **T.38 Support** parameter was set to **No**. The **General** tab parameters are shown below.



The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs use default values.

The **Advanced** tab parameters are shown below.

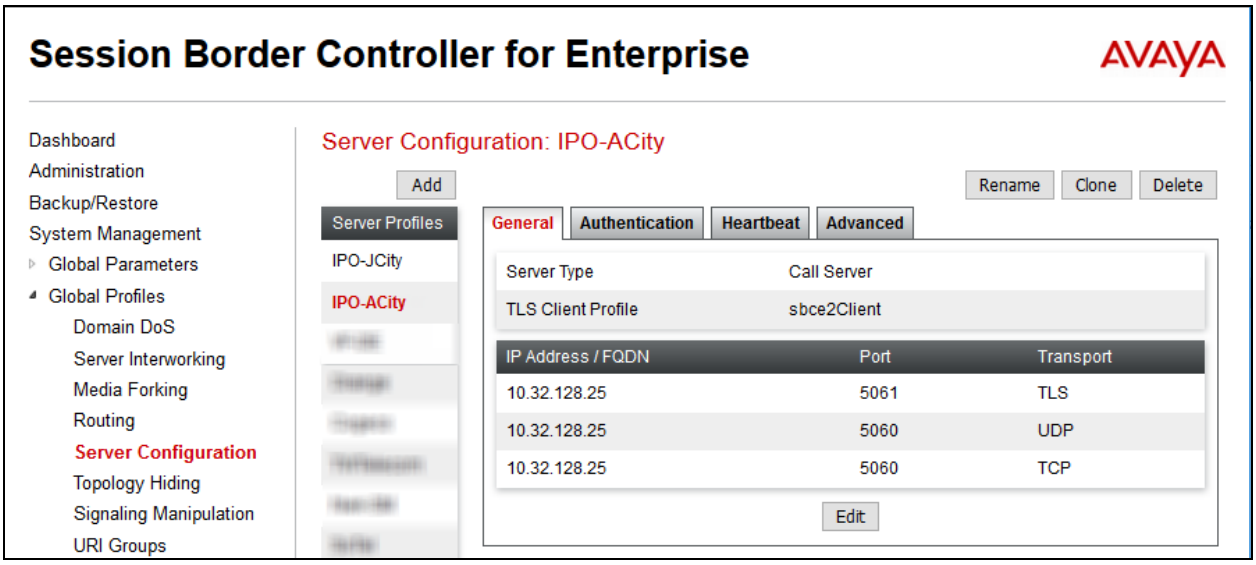


6.7. Server Configuration

A server configuration profile defines the attributes of the physical server. Create one server configuration profile for Avaya IP Office and another for the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the profile name will appear under **Server Profiles** in the center pane and the settings are shown in the far right pane.

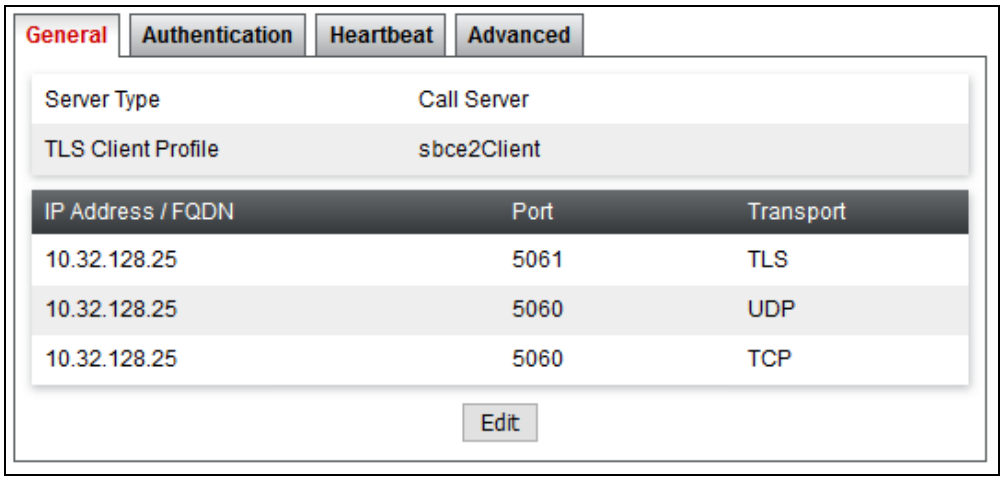
To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.



6.7.1. Server Configuration – Avaya IP Office

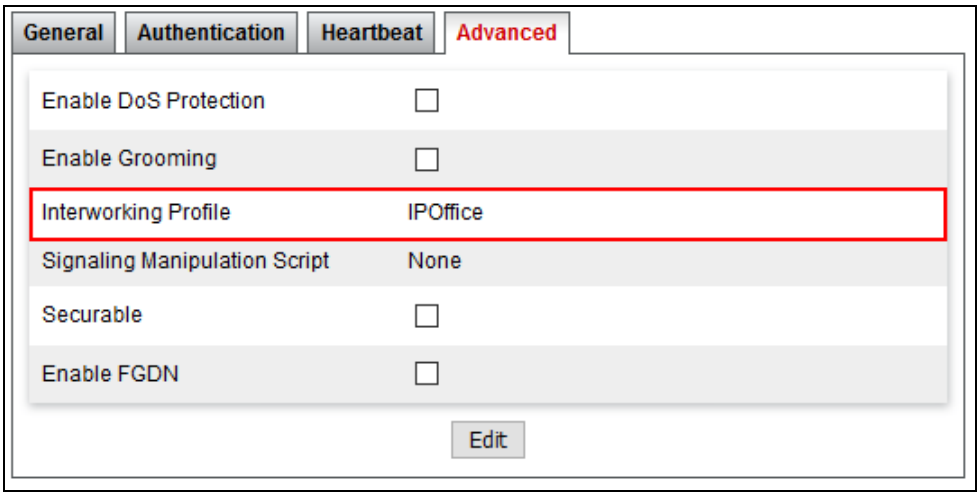
For the compliance test, the server configuration profile **IPO-ACity** was created for Avaya IP Office. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Call Server**.
- Set **TLS Client Profile** to **sbce2Client** (**Section 6.3.2**).
- Set **IP Address / FQDN** to the Avaya IP Office LAN1 address (**Section 5.3.1**).
- Enter a valid combination of **Port** and **Transport** that Avaya IP Office may use to listen for SIP requests. For the compliance test, Avaya IP Office was configured to use port **5060** for **UDP/TCP** or port **5061** for **TLS**.



The **Authentication** and **Heartbeat** tabs use the default values.

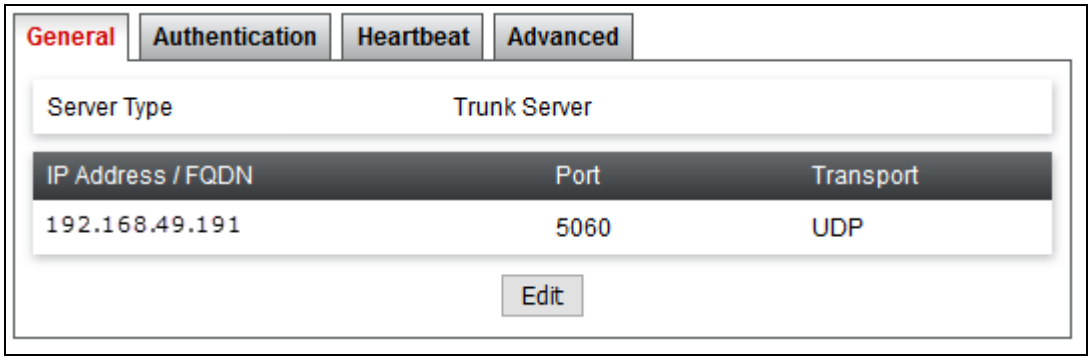
On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Avaya IP Office defined in **Section 6.6.1**. Leave the other fields at the default values.



6.7.2. Server Configuration – Vodafone DE

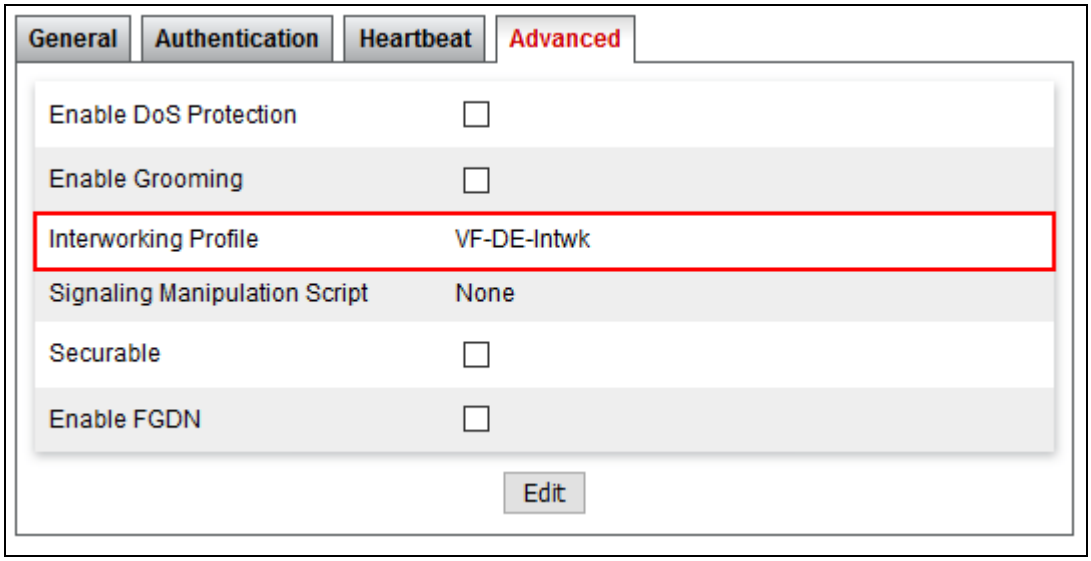
For the compliance test, the server configuration profile **VF-DE** was created for the Vodafone DE SIP Server. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Trunk Server**.
- Set **IP Address / FQDN** to the Vodafone DE SIP proxy IP address provided by Vodafone DE.
- Enter a valid combination of **Port** and **Transport** that the Vodafone DE SIP proxy may use to listen for SIP requests. Additional combinations can be entered by clicking the **Add** button (not shown).



The **Authentication** and **Heartbeat** tabs use the default values.

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Vodafone DE defined in **Section 6.6.2**. Leave the other fields at the default values.



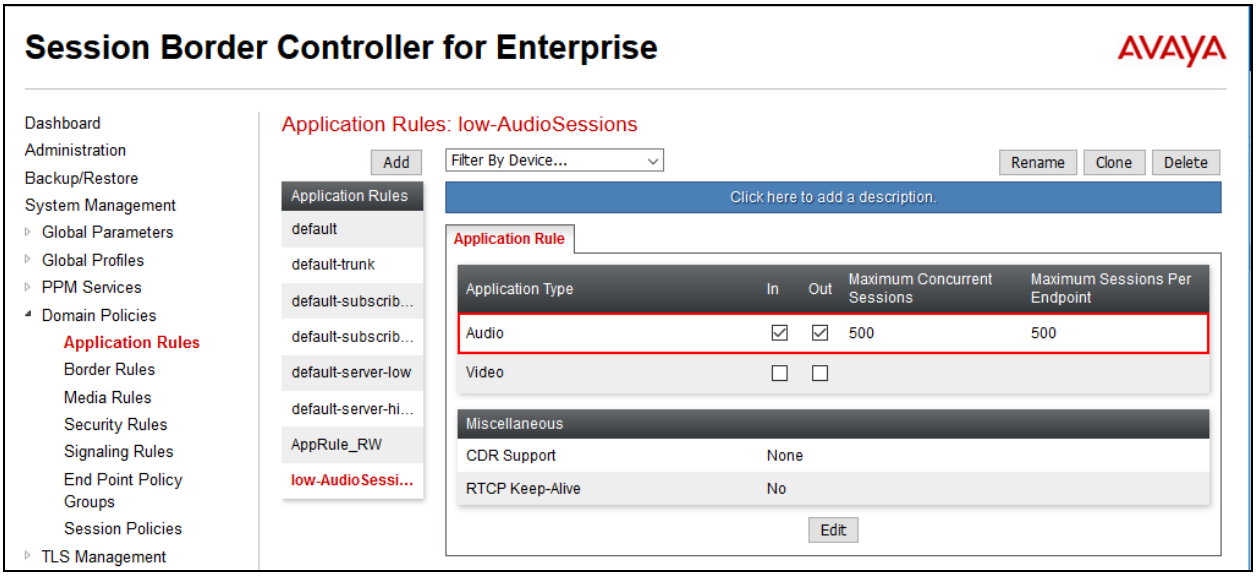
6.8. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 6.11**.

To create a new profile, navigate to **Domain Policies → Application Rules** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed.

To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

For the compliance test, the application rules profile named **low-AudioSessions** was cloned from the **default-trunk** profile in which the settings for both **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** were adjusted down to **500** (from 2000) for **Audio**. This change was to accommodate the maximum capacity on the Avaya SBCE running on the Portwell CAD-0208 server. The **low-AudioSessions** application rules profile was used for both Avaya IP Office and the Vodafone DE SIP server.

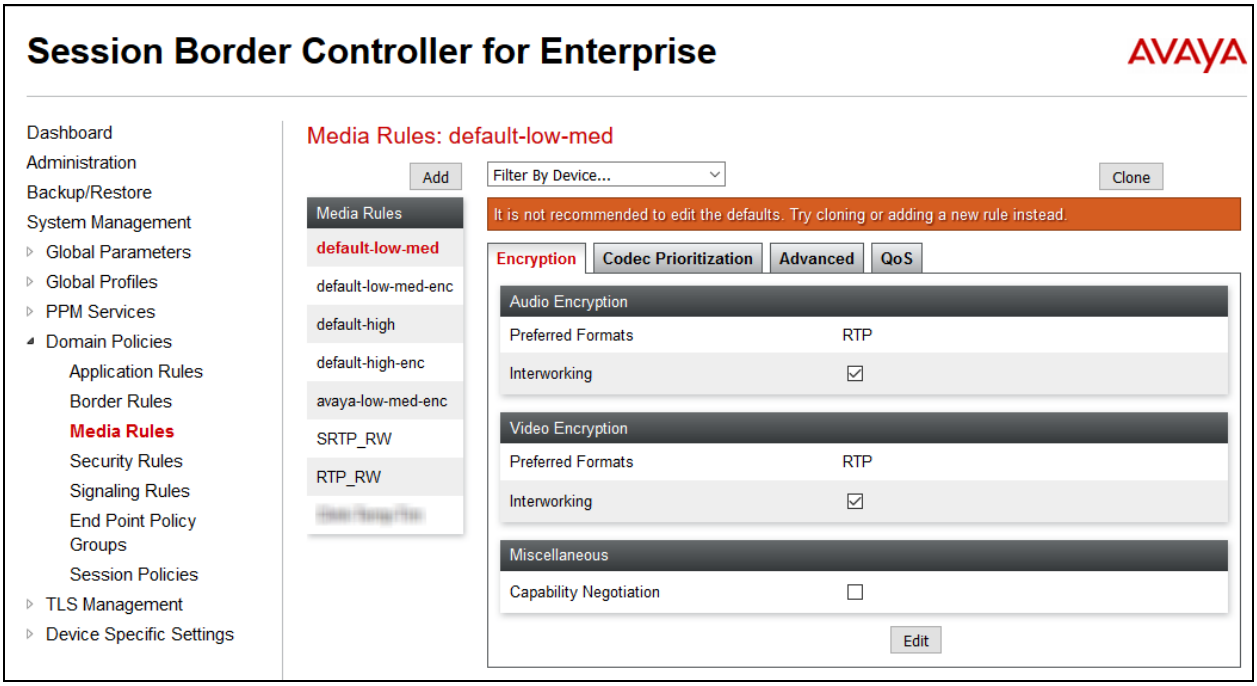


6.9. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger end point policy group defined in **Section 6.11**. For the compliance test, a media rule was created for Avaya IP Office to use SRTP, while the predefined **default-low-med** media rule was used for the Vodafone DE SIP server.

To create a new profile, navigate to **Domain Policies → Media Rules** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane.

To view an existing rule, navigate to **Domain Policies → Media Rules** in the left pane. In the center pane, select the rule (e.g., **default-low-med**) to be viewed.



6.9.1. Media Rules – Avaya IP Office

For the compliance test, the media rule **IPO-SRTP-Pref** was created for Avaya IP Office. When creating the rule, configure the **Encryption** tab parameters as follows:

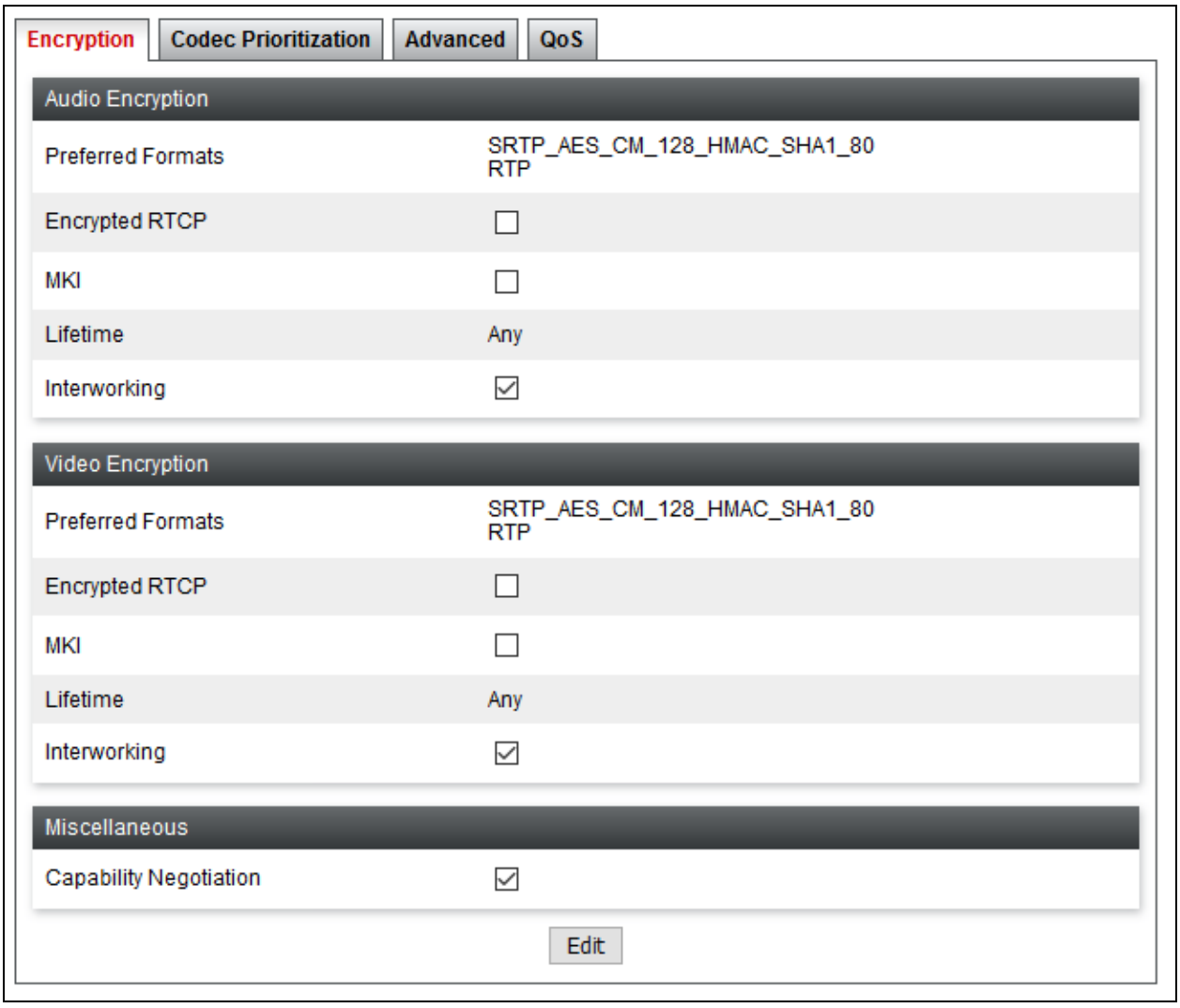
Under Audio Encryption and Video Encryption:

- Set **Preferred Formats** to **SRTP_AES_CM_128_HMAC_SHA1_80** followed by **RTP**. The use of SRTP or RTP will be determined by the **Media Security** setting on the Avaya IP Office SIP Line described in **Section 5.5.6**.
- Check the **Interworking** box.

Under Miscellaneous:

- Check the **Capability Negotiation** box.

Default values were used for all other fields on this tab and the other **Media Rule** tabs.



6.9.2. Media Rules – Vodafone DE

For the compliance test, the default media rule **default-low-med** was used for Vodafone DE SIP server. The **Encryption** tab parameters are as follows:

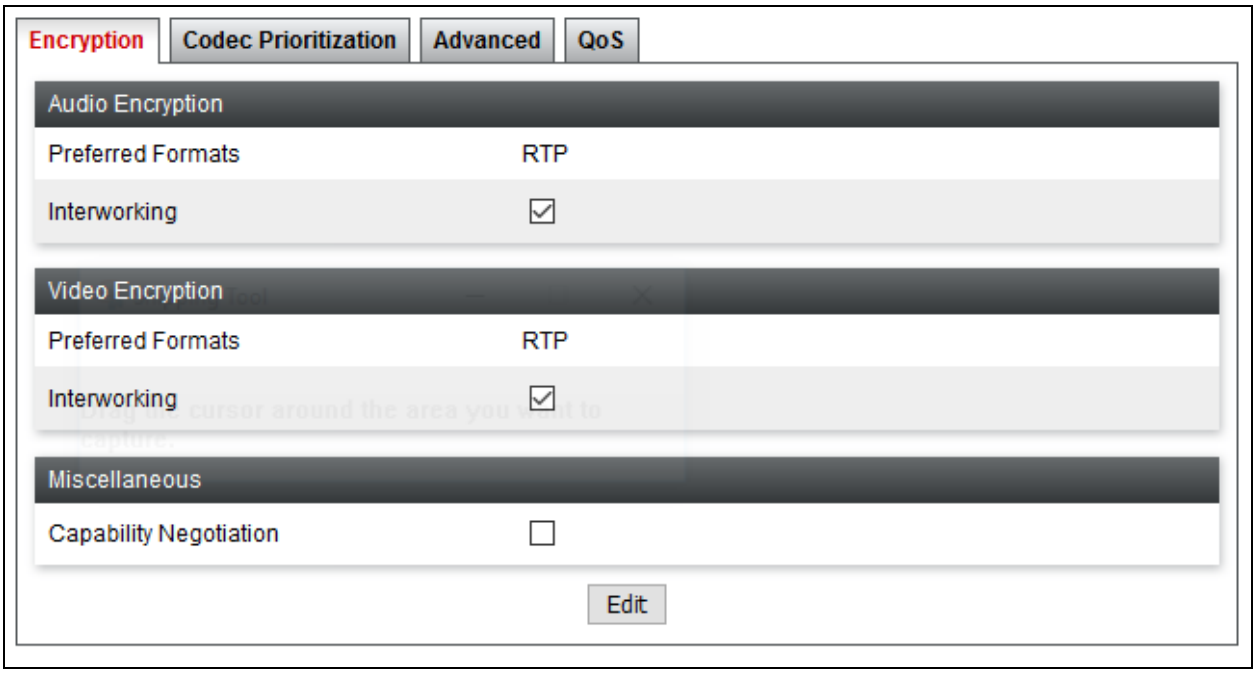
Under Audio Encryption and Video Encryption:

- The **Preferred Formats** is set to **RTP**.
- The **Interworking** box is checked.

Under Miscellaneous:

- The **Capability Negotiation** box is unchecked.

Default values were used for all other fields on this tab and the other **Media Rule** tabs.

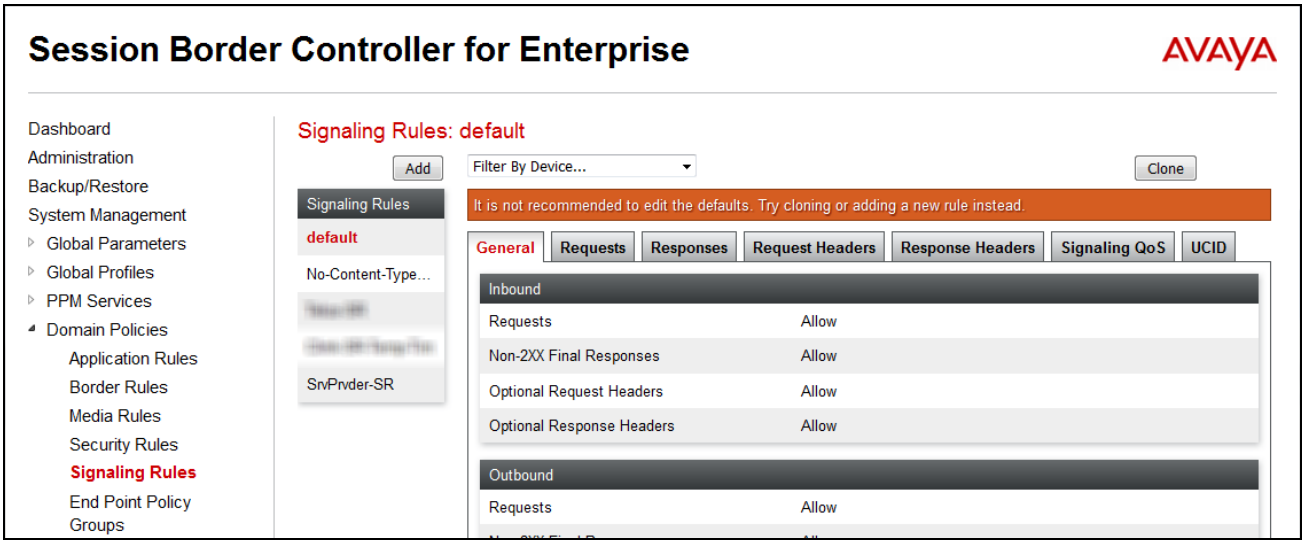


6.10. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger end point policy group defined in **Section 6.11**. For the compliance test, the predefined **default** media rule (shown below) was used for both Avaya IP Office and the Vodafone DE SIP server.

To create a new profile, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane.

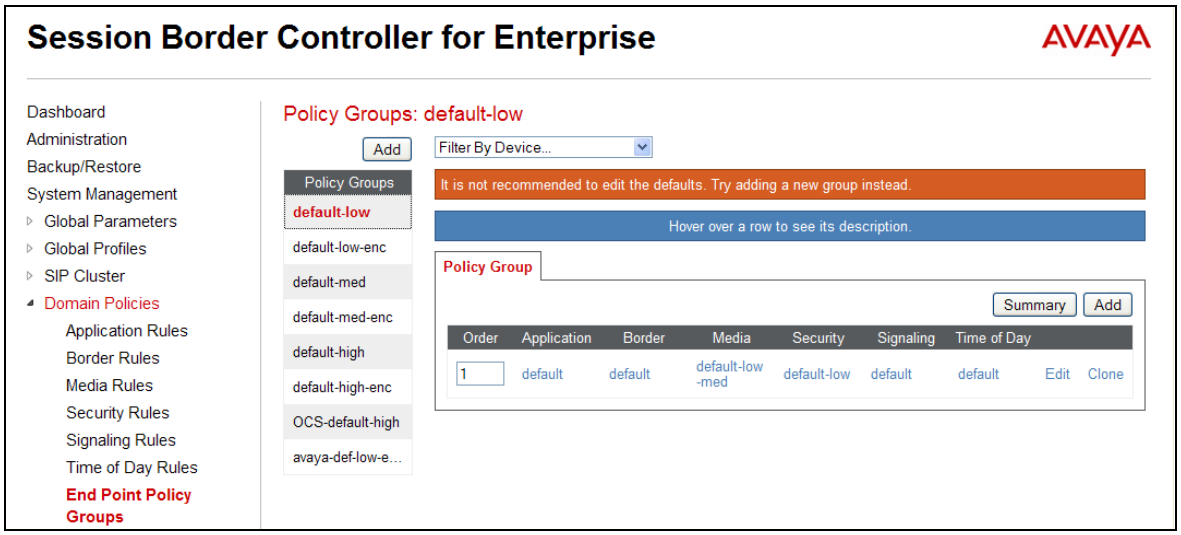
To view an existing rule, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select the rule (e.g., **default**) to be viewed.



6.11. End Point Policy Groups

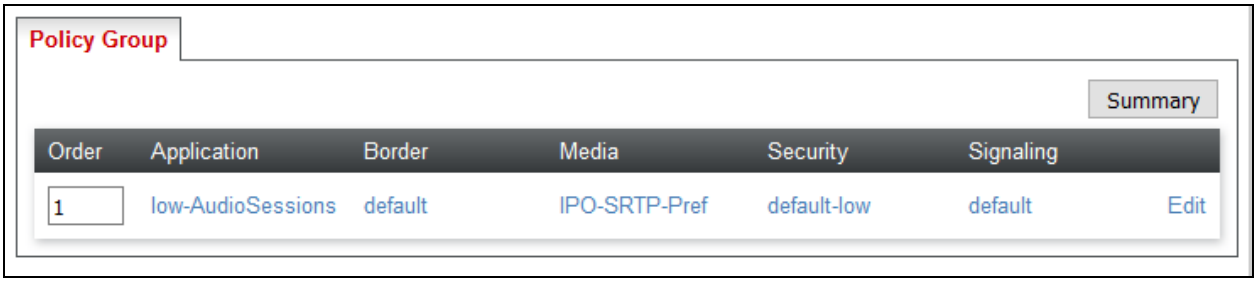
An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the service provider SIP server. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 6.14**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by series of pop-up windows in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.



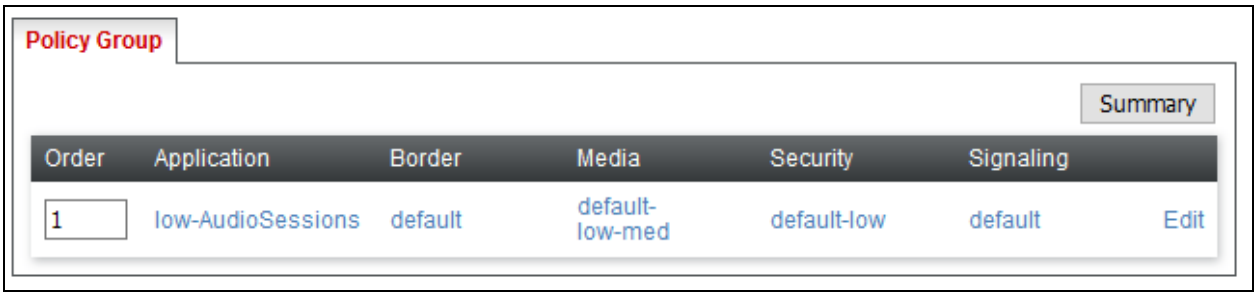
6.11.1. End Point Policy Group – Avaya IP Office

For the compliance test, the end point policy group **IPO-EP-Policy** was created for Avaya IP Office. Default values were used for each of the rules which comprise the group with the exception of **Application** and **Media**. For **Application**, enter the application rule specified in **Section 6.8**. For **Media**, enter the media rule defined in **Section 6.9.1**.



6.11.2. End Point Policy Group – Vodafone DE

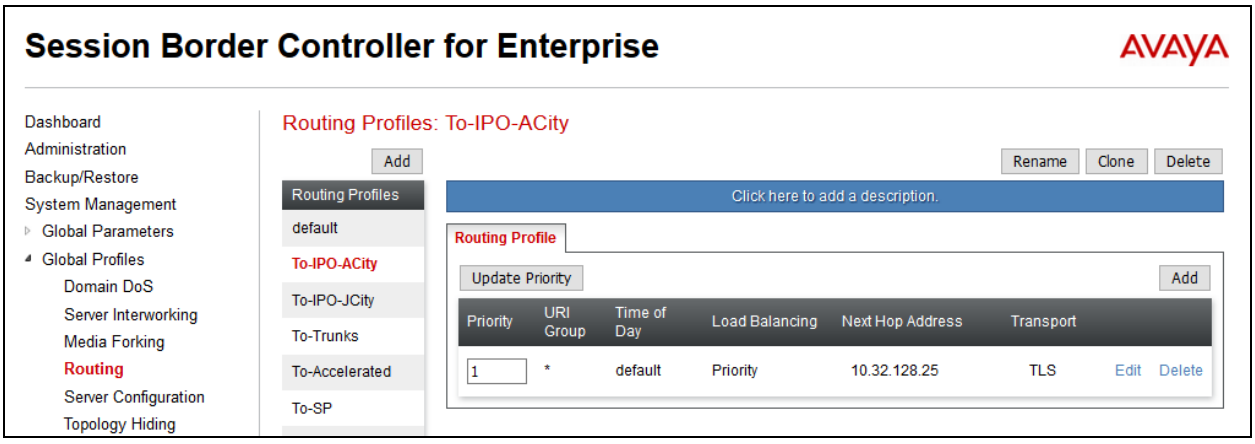
For the compliance test, the end point policy group **VF-DE-EP-Policy** was created for the Vodafone DE SIP server. Default values were used for each of the rules which comprise the group with the exception of **Application**. For **Application**, enter the application rule specified in **Section 6.8**.



6.12. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 6.14**. Create one routing profile for Avaya IP Office and another for the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

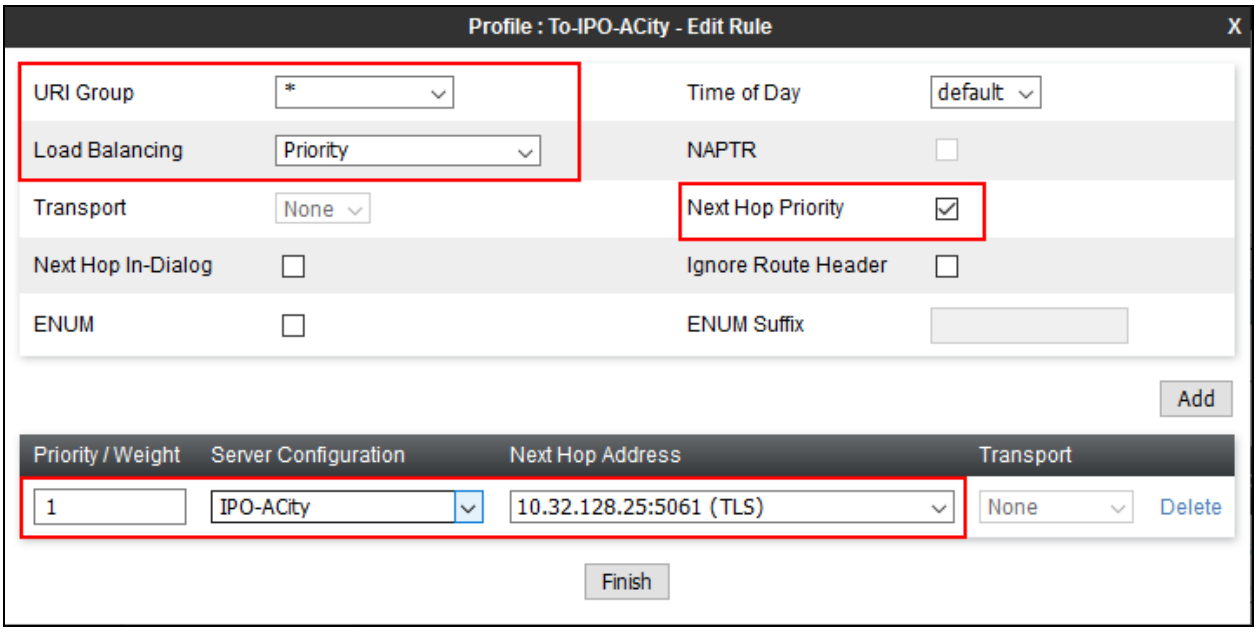


6.12.1. Routing - Avaya IP Office

For the compliance test, the routing profile **To-IPO-ACity** was created for Avaya IP Office. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card ***** to match on any URI.
- Set **Load Balancing** to **Priority** from the pull-down menu.
- Enable **Next Hop Priority**.
- Click **Add** to enter the following for the Next Hop Address:
    - Set **Priority/Weight** to **1**.
    - For **Server Configuration**, select **IPO-ACity** (**Section 6.7.1**) from the pull-down menu. The **Next Hop Address** pull-down menu will show each entry of Address/Port/Transport defined in the **Server Configuration** selected. For the **Next Hop Address**, select the entry that represents the connection between Avaya IP Office and the Avaya SBCE. In this case, the connection used **TLS** on port **5061**.

Click **Finish**.

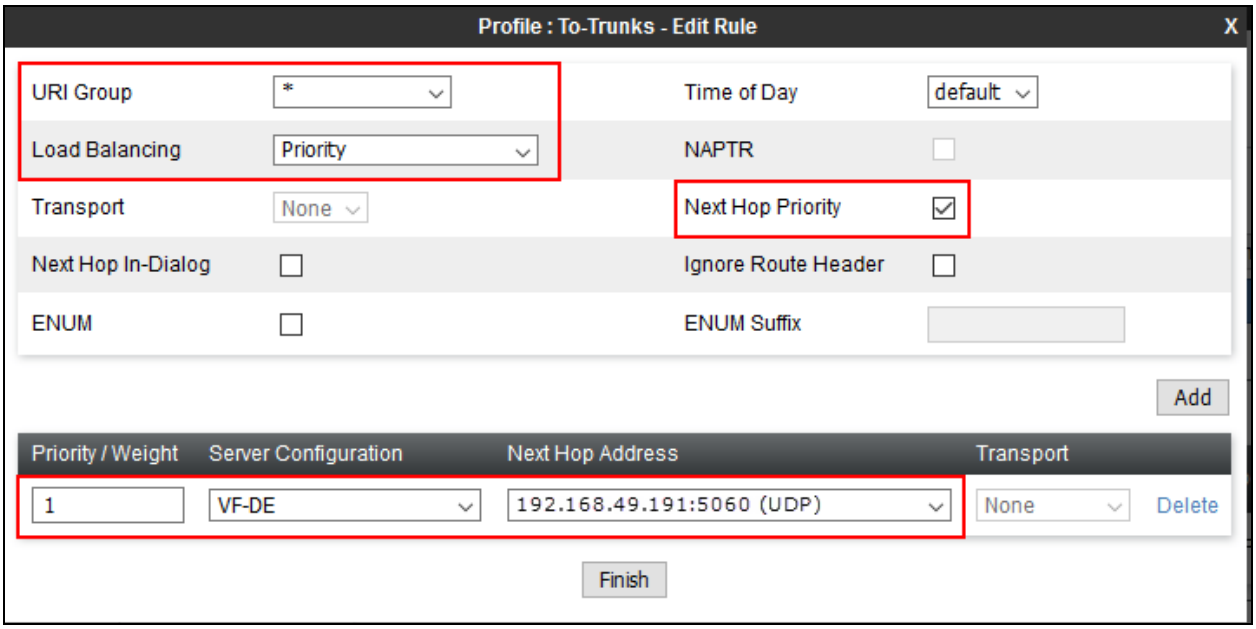


6.12.2. Routing – Vodafone DE

For the compliance test, the routing profile **To-Trunks** was created for Vodafone DE. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card ***** to match on any URI.
- Set **Load Balancing** to **Priority** from the pull-down menu.
- Enable **Next Hop Priority**.
- Click **Add** to enter the following for the Next Hop Address:
    - Set **Priority/Weight** to **1**.
    - For **Server Configuration**, select **VF-DE** (**Section 6.7.2**) from the pull-down menu. The **Next Hop Address** pull-down menu will show each entry of Address/Port/Transport defined in the **Server Configuration** selected. For the **Next Hop Address**, select the entry that represents the connection between Vodafone DE and the Avaya SBCE. This connection used **UDP** on port **5060**.

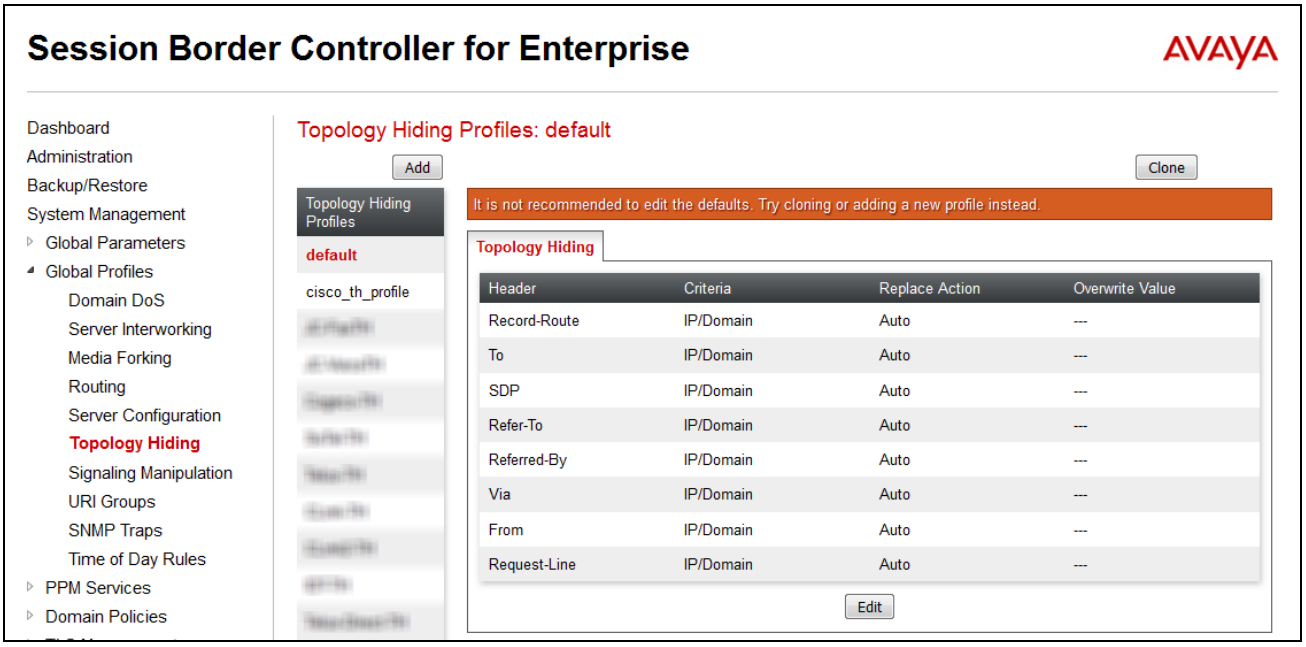
Click **Finish**.



6.13. Topology Hiding

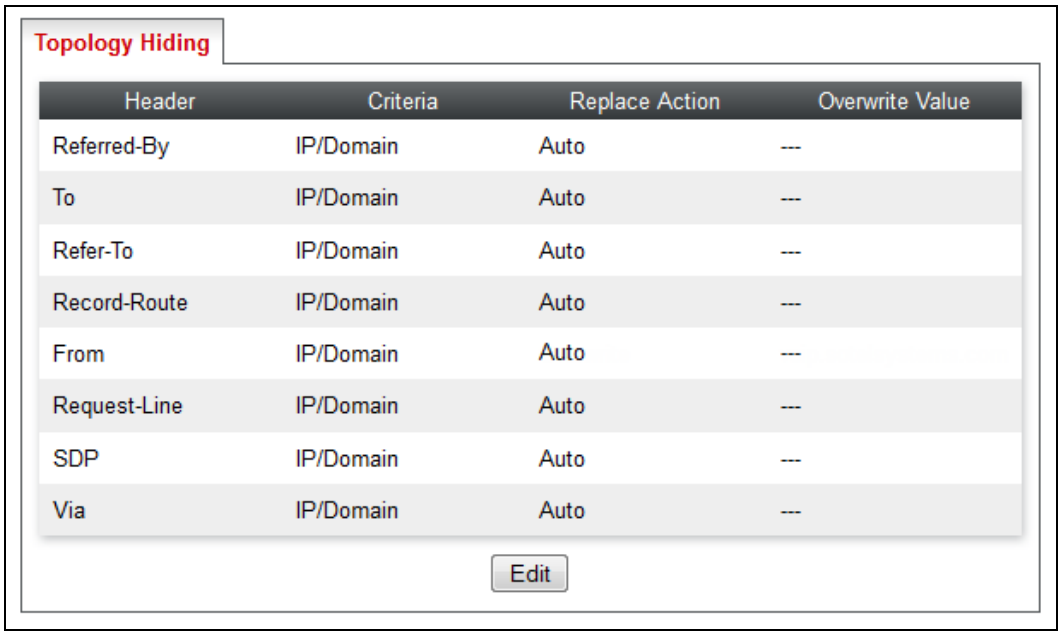
Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the end point flow in **Section 6.14**.

To add a new profile or view an existing profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add** to add a new profile, or select an existing profile (e.g., **default**) to be viewed.



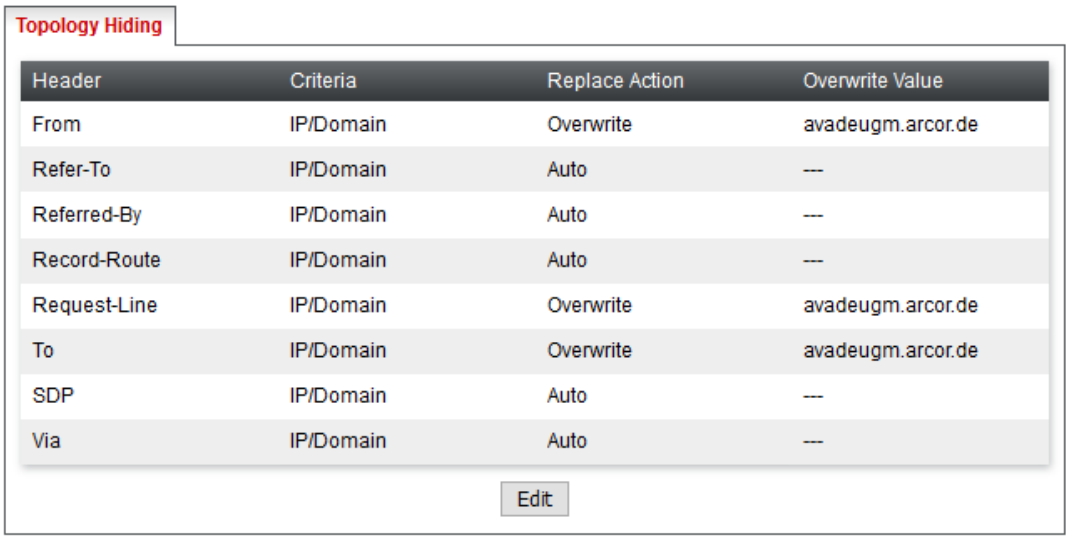
6.13.1. Topology Hiding – Avaya IP Office

Avaya IP Office used the predefined **default** topology hiding profile shown below.



6.13.2. Topology Hiding – Vodafone DE

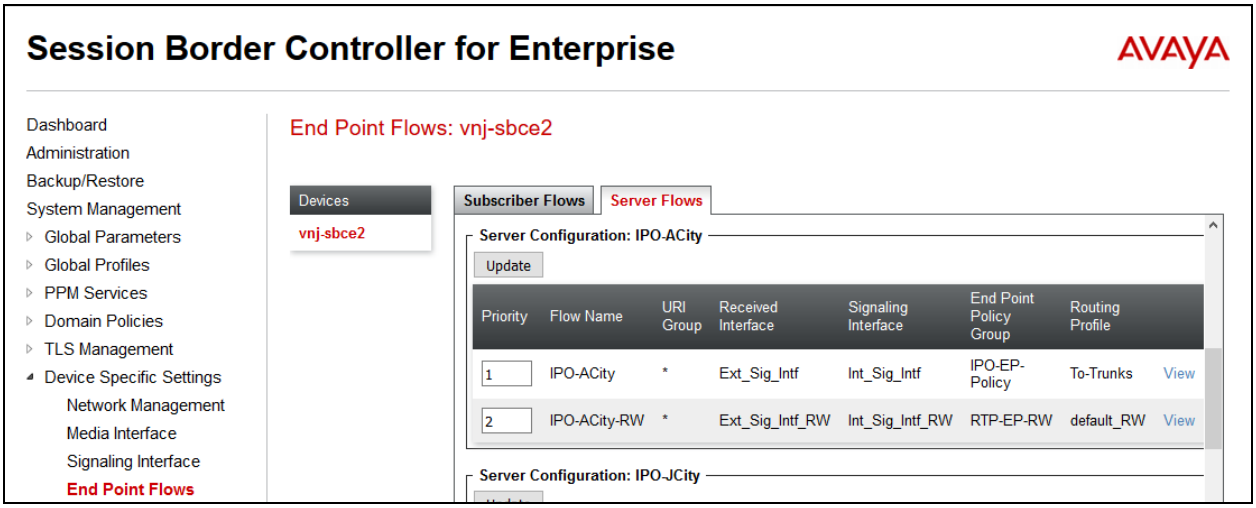
The topology hiding profile for Vodafone DE (**VF-DE-TH**) was created by cloning the predefined **default** profile and changing the value of the **Request-Line**, **To** and **From** headers. The profile is configured to overwrite the host part of these headers with the Vodafone DE domain.



6.14. End Point Flows

Endpoint flows are used to determine the signaling endpoints (connected servers) involved in a call in order to apply the appropriate policies. When a packet arrives at the 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 policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source end point flow and the destination end point flow. In the case of the compliance test, the signaling endpoints are Avaya IP Office and the service provider SIP server.

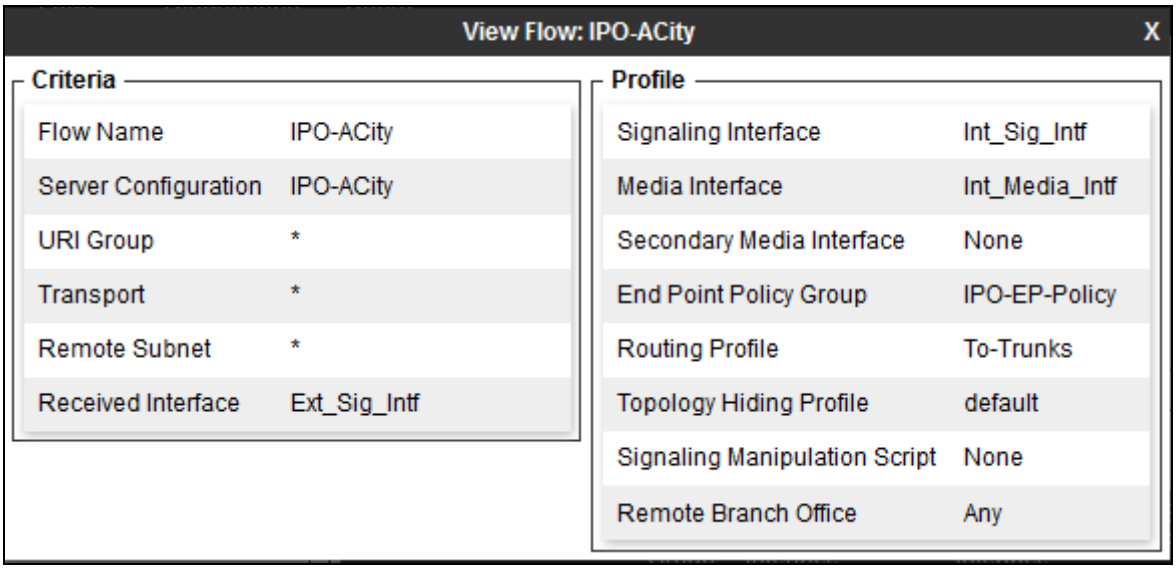
To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device to be managed. In the right pane, select the **Server Flows** tab and click the **Add** button. A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters. Once complete, the settings are shown in the far right pane.



6.14.1. End Point Flow – Avaya IP Office

For the compliance test, the end point flow **IPO-ACity** was created for Avaya IP Office. All traffic from Avaya IP Office will match this flow as the source flow and use the specified routing profile **To-Trunks** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

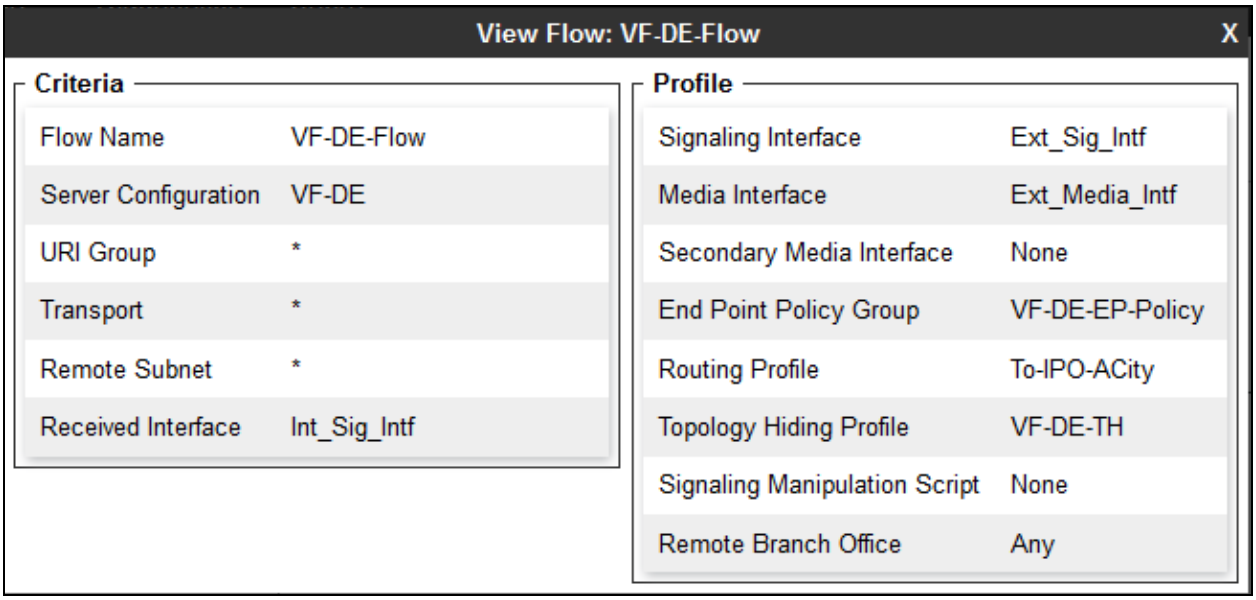
- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Avaya IP Office server created in **Section 6.7.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set the **Received Interface** to the external signaling interface.
- Set the **Signaling Interface** to the internal signaling interface.
- Set the **Media Interface** to the internal media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Avaya IP Office in **Section 6.11.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.12.2** used to direct traffic to the Vodafone DE SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Avaya IP Office in **Section 6.13.1**.



6.14.2. End Point Flow – Vodafone DE

For the compliance test, the end point flow **VF-DE-Flow** was created for the Vodafone DE SIP server. All traffic from Vodafone DE will match this flow as the source flow and use the specified routing profile **To-IPO-ACity** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Vodafone DE SIP server created in **Section 6.7.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set the **Received Interface** to the internal signaling interface.
- Set the **Signaling Interface** to the external signaling interface.
- Set the **Media Interface** to the external media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Vodafone DE in **Section 6.11.2**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.12.1** used to direct traffic to Avaya IP Office.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Vodafone DE in **Section 6.13.2**.



7. Vodafone DE SIP Trunk Service Configuration

Vodafone DE is responsible for the configuration of the Vodafone DE SIP Trunk Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise. In the case of the compliance test, this is the public IP address of the Avaya SBCE. Vodafone DE will provide the customer the necessary information to configure Avaya IP Office and the Avaya SBCE including:

- Vodafone DE SIP proxy IP address
- Transport protocol and port
- SIP Domain
- Supported codecs and order of preference
- DDI numbers

In addition, to configure any possible firewall/security devices at the enterprise, Vodafone DE will provide the IP address and port of any media sources that will need access to the enterprise.

8. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

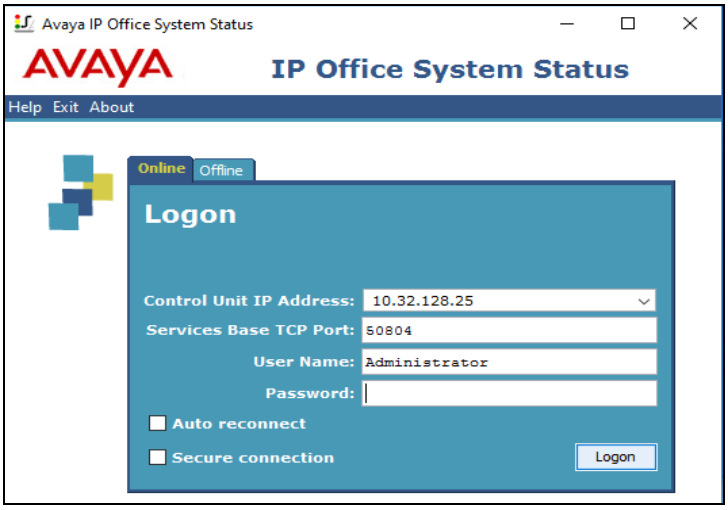
8.1. Avaya IP Office

Avaya IP Office has several tools that can be used to verify and troubleshoot the system operation. Two of these tools are described in the following subsections.

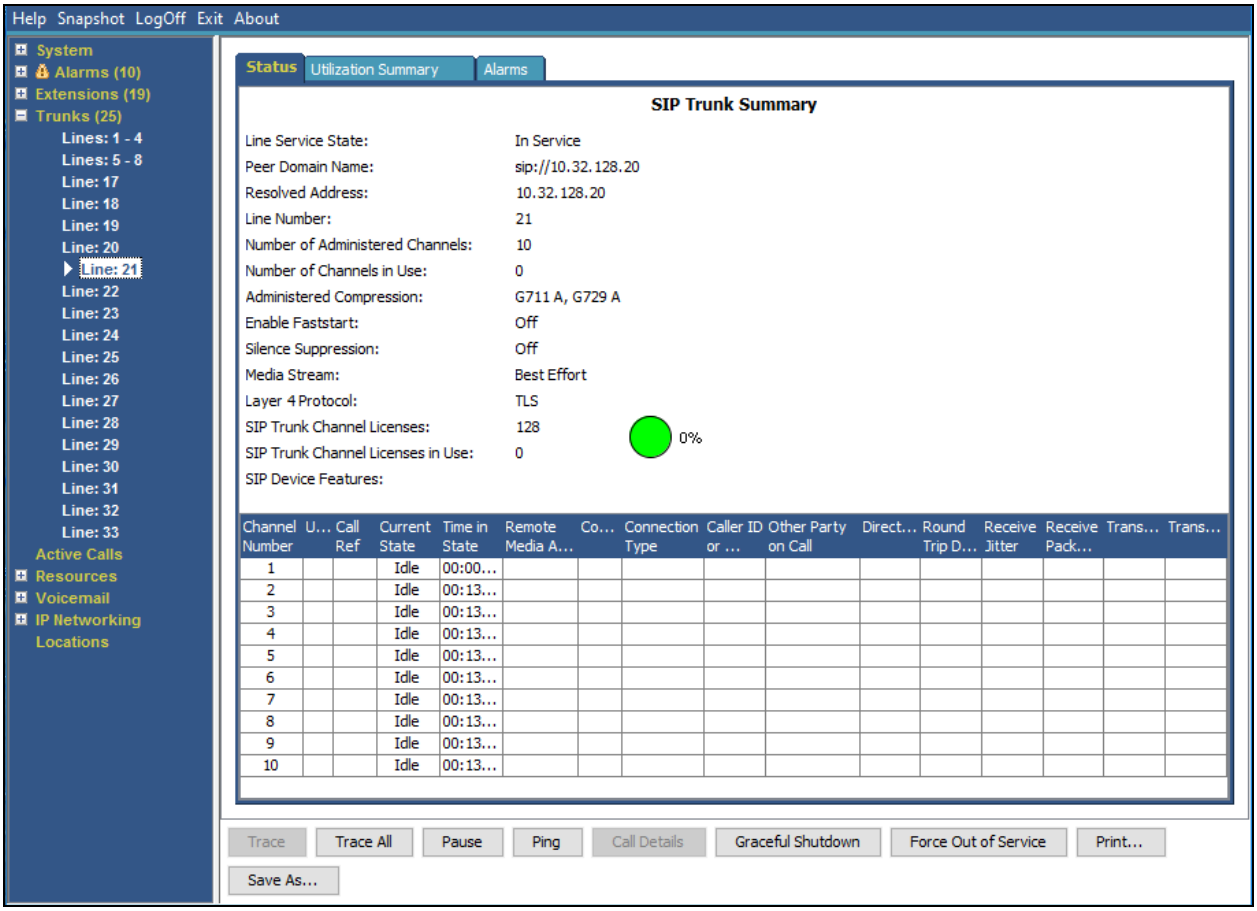
8.1.1. System Status

The System Status application is used to monitor and troubleshoot Avaya IP Office. Use the System Status application to verify the state of the SIP trunk. System Status can be accessed from **Start → All Programs → IP Office → System Status**.

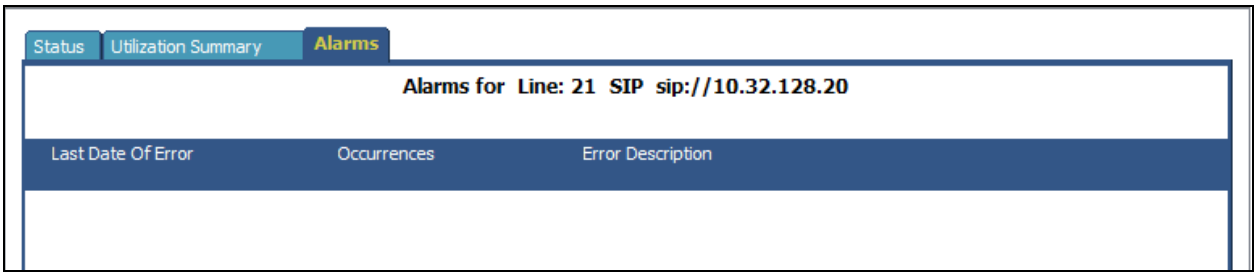
The following screen shows an example **Logon** screen. Enter the Avaya IP Office IP address in the **Control Unit IP Address** field, and enter an appropriate **User Name** and **Password**. Click **Logon**.



Select the SIP line under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current State** does not indicate an error. The state of **Idle** indicates the channel does not have an active call.



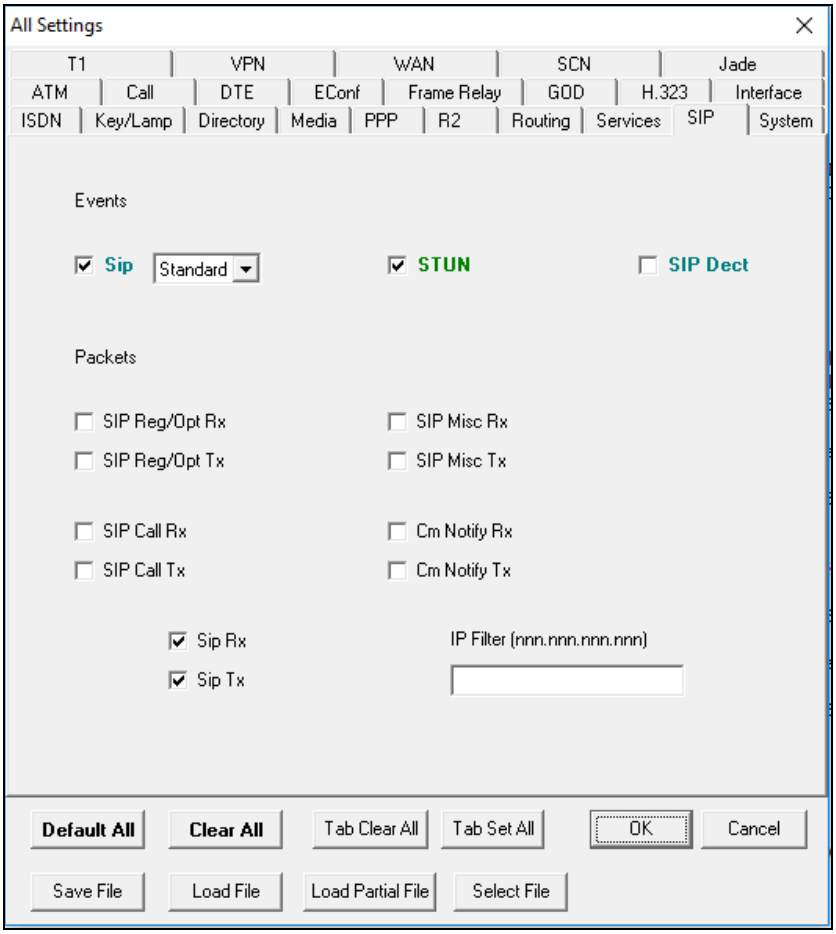
Select the **Alarms** tab and verify that no alarms are active on the SIP line.



8.1.2. Monitor

The Monitor application can also be used to monitor and troubleshoot Avaya IP Office. The Monitor application can be accessed from **Start → All Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select **Filters → Trace Options**.

The following screen shows the **SIP** tab, allowing configuration of SIP monitoring.



8.2. Avaya Session Border Controller for Enterprise

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

- **Alarms**: This option provides information about active alarms.
- **Incidents**: This option provides detailed reports of anomalies, errors, policies violations, etc.
- **Status**: This option provides statistical and current status information.
- **Diagnostics**: This option provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office 10.0 and Avaya Session Border Controller for Enterprise 7.1 to the Vodafone DE SIP Trunk Service. The Vodafone DE SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks. The Vodafone DE SIP Trunk Service passed compliance testing. Please refer to **Section 2.2** for any observations/exceptions.

10. Additional References

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

[1] *Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 31q, February 6, 2017.
[2] *Administering Avaya IP Office Platform with Manager*, Release 10, September 2016.
[3] *Using System Status*, Document Number 15-601758, Issue 11f, February 6, 2017.
[4] *Administering Avaya IP Office Platform Voicemail Pro*, Document Number 15-601063, Issue 11f, November 22, 2016.
[5] *Using IP Office System Monitor*, Document Number 15-601019, Issue 08b, November 25, 2016.
[6] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.1, Issue 2, January 2017.
[7] *Administering Avaya Session Border Controller for Enterprise*, Release 7.1, Issue 3, May 2017.

Additional Avaya IP Office documentation can be found at:
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.