Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 7.0 to support Clearcom SIP Trunking Service using TLS - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 9.1 and Avaya Session Border Controller for Enterprise Release 7.0 to support Clearcom SIP Trunking Service using TLS.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints. For privacy, TLS for Signaling was used inside of the enterprise (private network side) and outside of the enterprise (public network side).

Clearcom SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Clearcom's network as an alternative to legacy analog or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

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.

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

©2016 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction 4
2. General Test Approach and Test Results 4
   2.1 Interoperability Compliance Testing 5
   2.2 Test Results 6
   2.3 Support 7
3. Reference Configuration 7
4. Equipment and Software Validated 10
5. Configure IP Office 11
   5.1 Licensing 11
   5.2 System 12
      5.2.1 System - LAN1 Tab 12
      5.2.2 System - Telephony Tab 15
      5.2.3 System - Twinning Tab 16
      5.2.4 System - Codecs Tab 17
      5.2.5 System – VoIP Security Tab 18
   5.3 IP Route 19
   5.4 SIP Line 20
      5.4.1 Importing a SIP Line Template 20
      5.4.2 Creating a SIP Trunk from an XML Template 24
      5.4.3 SIP Line - SIP Line Tab 26
      5.4.4 SIP Line - Transport Tab 27
      5.4.5 SIP Line - SIP URI Tab 28
      5.4.6 SIP Line - VoIP Tab 29
      5.4.7 SIP Line – SIP Advanced Tab 31
   5.5 Extension 32
   5.6 Users 34
   5.7 Incoming Call Route 38
   5.8 Outbound Call Routing 40
      5.8.1 Short Codes and Automatic Route Selection 40
   5.9 Save Configuration 43
6. IP Office Certificates 44
   6.1 IP Office Identity Certificate for Telephony 44
   6.2 IP Office Trusted Certificate Store 45
   6.3 Save Security Settings 48
7. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE) 50
   7.1 Log in Avaya SBCE 50
   7.2 TLS Management 53
      7.2.1 TLS Certificates 53
      7.2.2 TLS Client Profile – IP Office 53
      7.2.3 TLS Client Profile – Service Provider 55
      7.2.4 TLS Server Profile – IP Office 57
      7.2.5 TLS Server Profile – Service Provider 59
   7.3 Global Profiles 61
      7.3.1 Server Interworking – Avaya-IPO 62
      7.3.2 Server Interworking - SP-General 65
      7.3.3 Server Configuration 68

©2016 Avaya Inc. All Rights Reserved.

7.3.4 Routing Profiles 78
7.3.5 Topology Hiding 81
7.4 Domain Policies 85
7.4.1 Application Rules 85
7.4.2 Media Rules 88
7.4.3 End Point Policy Groups 93
7.5 Device Specific Settings 97
7.5.1 Network Management 97
7.5.2 Media Interface 99
7.5.3 Signaling Interface 101
7.5.4 End Point Flows 104
8. Clearcom SIP Trunking Service Configuration 108
9. Verification and Troubleshooting 109
9.1 Verification Steps 109
9.2 Protocol Traces 109
9.3 IP Office System Status 110
9.4 IP Office Monitor 113
9.5 Avaya Session Border Controller for Enterprise (Avaya SBCE) 114
9.6 TraceSBC Tool 118
10. Conclusion 120
11. References 121

©2016 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Clearcom and an Avaya SIP-enabled enterprise solution using Transport Layer Security (TLS).

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office 500v2 Release 9.1 (hereafter referred to as IP Office), Avaya Session Border Controller for Enterprise Release 7.0 (hereafter referred to as Avaya SBCE), Avaya Communicator for Windows and Avaya Deskphones, including SIP, H.323.

For privacy, TLS transport for Signaling was used inside of the enterprise (private network side) and outside of the enterprise (public network side). RTP was used inside of the enterprise (private network side) and outside of the enterprise (public network side) (refers to **Section 2.2**).

The Clearcom SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the Avaya 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.

The terms “service provider” or “Clearcom” will be used interchangeable throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Solution & Interoperability Test Lab by connecting IP Office and the Avaya SBCE to the Clearcom SIP Trunking service via the public Internet, as depicted in **Figure 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.

©2016 Avaya Inc. All Rights Reserved.

2.1 Interoperability Compliance Testing

To verify the Clearcom SIP Trunking service offering with Avaya IP Office and the Avaya SBCE using TLS transport for signaling, and RTP for media, the following features and functionalities were exercised during the compliance testing:

- SIP Trunk Registration (Dynamic Authentication).
- Incoming PSTN calls to various Avaya endpoints, including SIP and H.323 telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323 telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider network.
- Incoming and outgoing PSTN calls to/from Avaya Communicator for Windows.
- Dialing plans including local calls (within Mexico), international, outbound toll-free, etc.
- Caller ID presentation.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two way speech-path. Testing was performed with codecs: G.729A, G.711A and G.711U, Clearcom's preferred codec order.
- Proper response to no matching codecs.
- Fax.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.

Note: Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

Items not supported or not tested included the following:

- Operator (0) and operator assisted calls (0+10).

©2016 Avaya Inc. All Rights Reserved.

2.2 Test Results

Interoperability testing with Clearcom SIP Trunking service was successfully completed with the exception of observations/limitations described below:

- **Secure Real-time Transport Protocol (SRTP)**: SRTP supports RTP media protection on a point to point basis providing confidentiality, message authentication and replay protection. As SRTP is point to point, all individual links involved in the VoIP call, including key exchange/signaling, must be secure for the call to be secure from end to end. During the compliance test it was observed that RTP, instead of SRTP, was always used. Calls would fail if the use of SRTP was enforced. This behavior may be caused by the far-end not supporting TLS/SRTP. Thus **Best Effort** was used during the compliance test, allowing IP Office and the Avaya SBCE to use SRTP if supported by the far-end, otherwise it defaults to RTP.
- **Caller ID on outbound calls**: On calls originating from IP Office extensions to PSTN telephones, the caller ID number shown on the PSTN endpoint was always the main DID number assigned by Clearcom to the SIP trunk, not the specific DID assigned to that extension. This includes calls to "twinned" mobile phones, and calls that were forwarded or transferred back on the SIP trunk to the PSTN, where the number displayed on the PSTN endpoint was the main DID number on the trunk, not the originator's caller's ID. This may be a requirement of the Clearcom service for all outbound calls, it is listed here simply as an observation.
- **Caller ID on inbound calls**: On inbound calls made from the test lab in the U.S., the caller ID shown on the enterprise extensions occasionally showed "Unavailable", while in other cases showed numbers corresponding to local PSTN numbers in Mexico, not the number of the original caller. Calls made from a test number in Mexico showed the correct caller ID.
- **Outbound Calling Party Number (CPN) Block**: Clearcom did not allow outbound calls with privacy enabled. When an IP Office user activated "Withhold Number" to enable user privacy on an outbound call, IP Office sent "anonymous" in the "From" header and the "Privacy:id" header, while the caller information was still being sent in the **"**P-Asserted-Identity" header. Clearcom responded with a "403 PSTN calls are forbidden" message and the call was rejected.
- **Outbound call from an enterprise extension to a busy PSTN number**: Clearcom did not send a "486 Busy Here" message on an outbound call to a PSTN number that was busy, as it was expected on this condition. There was no direct impact to the user, who heard busy tone.
- **Call transfer to the PSTN using REFER**: PSTN calls that were transferred back to the network using REFER messages did not work properly. Calls that were blind transferred dropped. On attended transfers, the REFER message was accepted by Clearcom with a 202 message, but the trunks were not released. Due to these reasons, REFER was left disabled in the Avaya IP Office for the tests. With REFER disabled, blind and attended call transfers to the PSTN were allowed to complete, with the caveat that the IP Office was not released from the call path, and two trunks remained busy for the complete duration of the call.
- **Fax support**: Fax calls using the T.38 protocol failed during the test. G.711 fax was also tested, but it behaved unreliably. Fax should not be used in this solution.
- **Incoming Call, SIP Trunk Signaling Failure**: When the SIP trunk was forced to an "Out of Service" condition, and an incoming call was attempted to one of the DID numbers, it took

©2016 Avaya Inc. All Rights Reserved.

from 15 to 30 seconds, depending on the source of the call, for the caller to receive an error recording from the network. This amount of time seems excessive in these conditions.

2.3 Support

For support on Clearcom SIP Trunking service visit the corporate Web page at:
http://www.clearcom.mx/

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates the test configuration used. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the Clearcom SIP Trunking service through the public Internet.

The Avaya components used to create the simulated enterprise customer site includes:

- Avaya IP Office 500v2.
- Avaya IP Office Voicemail Pro.
- Avaya Session Border Controller for Enterprise.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 1100 Series SIP IP Deskphones.
- Avaya Communicator for Windows.

Located at the edge of the enterprise is the Avaya SBCE. The Avaya SBCE has two physical interfaces, interface **B1** is used to connect to the public network, interface **A1** is used to connect to the private network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. The Avaya SBCE provides network address translation at both the IP and SIP layers.

Also located at the enterprise site is Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codec's. The IP Office **LAN1** interface connects to the inside (A1) interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE (B1) connects to Clearcom's network via the public Internet.

For inbound calls, the calls flowed from the PSTN to Clearcom's network to the Avaya SBCE, then to IP Office.

Outbound calls to the PSTN were first processed by IP Office. Once IP Office selected the proper SIP trunk; the call was routed to the Avaya SBCE, across the public Internet, to Clearcom's network.

The transport protocol between the Avaya SBCE and Clearcom, across the public Internet, is SIP over TLS. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network, is also SIP over TLS.

©2016 Avaya Inc. All Rights Reserved.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Clearcom. The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to the network

In an actual customer configuration, the enterprise site may also include additional network components between Clearcom and the enterprise. 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 the enterprise must be allowed to pass through these devices.

For confidentiality and privacy purposes, actual public IP addresses and DID numbers used during the compliance test have been replaced with fictitious IP addresses and DID numbers throughout these Application Notes.

©2016 Avaya Inc. All Rights Reserved.

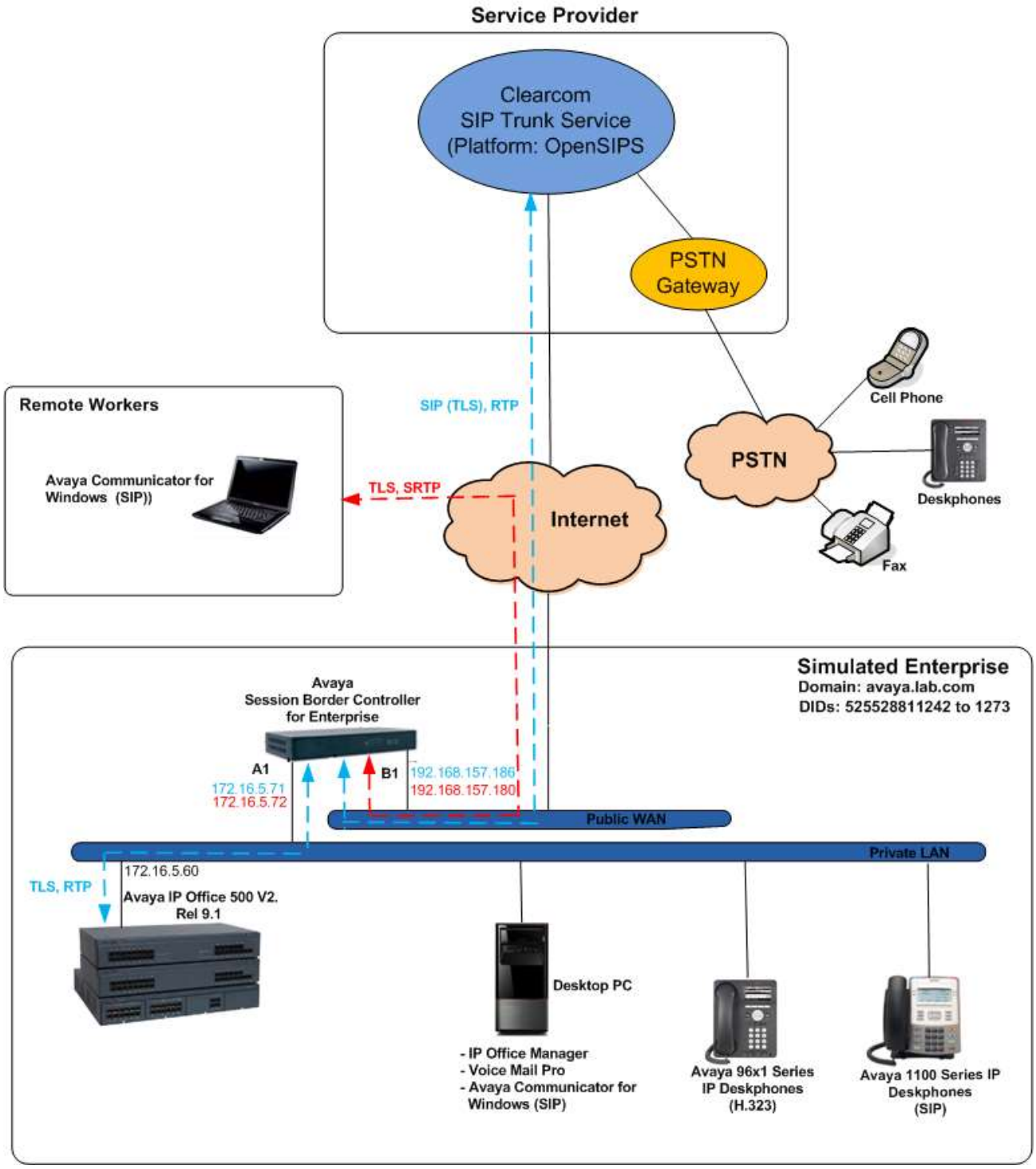


Figure 1: Avaya Interoperability Test Lab Configuration.

©2016 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

The following equipment and software/firmware were used for the compliance testing.

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	9.1.6.0 Build 153
Avaya IP Office DIG DCPx16 V2	9.1.6.0 Build 153
Avaya IP Office Manager	9.1.6.0 Build 153
Avaya Voicemail Pro Client	9.1.6.0 Build 2
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.0.1-03-8739
Avaya 96x1 Series IP Deskphones (H.323)	6.6029
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.18.00
Avaya Communicator for Windows	2.0.3.40
Clearcom	
OpenSIPS Softswitch	1.9
OpenSIPS Session Border Controller	1.9

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500v2 and also when deployed with all configurations of IP Office Server Edition without T.38 Fax Service.

©2016 Avaya Inc. All Rights Reserved.

5. Configure IP Office

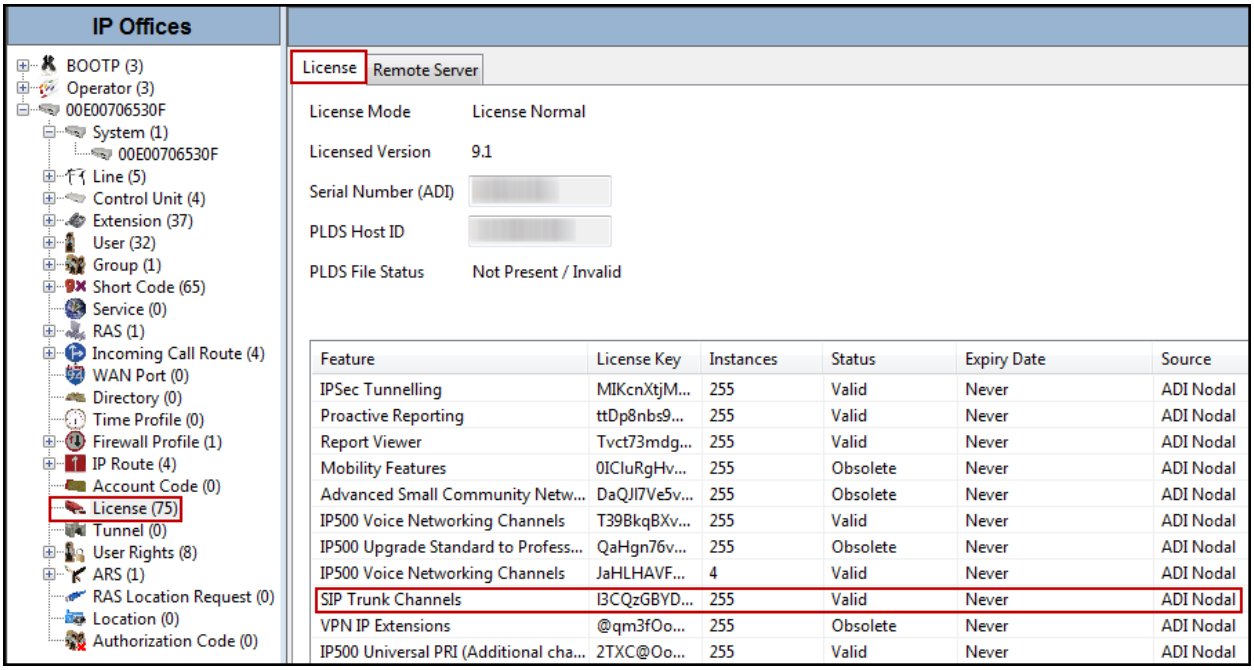
This section describes the IP Office configuration required to interwork with Clearcom SIP Trunking service. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP Office Manager. Navigate to **File → Open Configuration**, select the proper IP Office from the pop-up window, and log in with the appropriate credentials. A management window will appear as shown in the next sections. The appearance of IP Office Manager can be customized using the **View** menu (not shown). In the screenshots presented in this section, the **View** menu was configured to show the **Navigation Pane** on the left side and the **Details Pane** on the right side. These panes will be referenced throughout these Application Notes.

These Application Notes assume the basic installation and configuration of IP Office have already been completed and are not discussed here. For further information on IP Office, please consult References in **Section 11**.

5.1 Licensing

The configuration and features described in these Application Notes require the IP Office system 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**, then from the license tab, locate **SIP Trunk Channels**. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the Details pane. Note that the full License Keys in the screen below is not shown for security purposes.



©2016 Avaya Inc. All Rights Reserved.

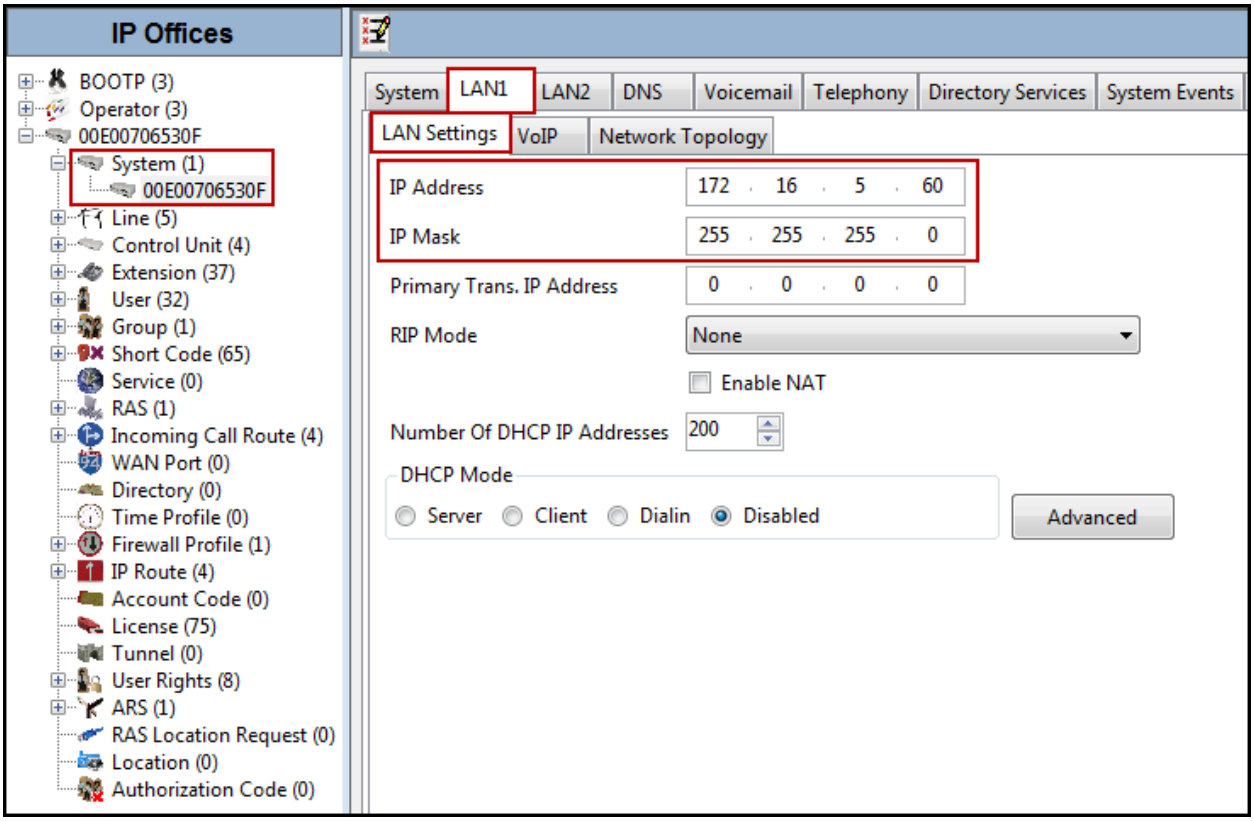
5.2 System

Configure the necessary system settings. In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to connect Avaya IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.1 System - LAN1 Tab

In the sample configuration, the MAC address **00E00706530F** was used as the system name. The **LAN** port connects to the Avaya SBCE across the enterprise LAN (private) network. The **LAN1** settings correspond to the **LAN** port in IP Office. To access the **LAN1** settings, navigate to **System (1) → 00E00706530F** in the Navigation Pane, then in the Details Pane, navigate to the **LAN1→ LAN Settings** tab. The **LAN1** settings for the compliance testing were configured with following parameters:

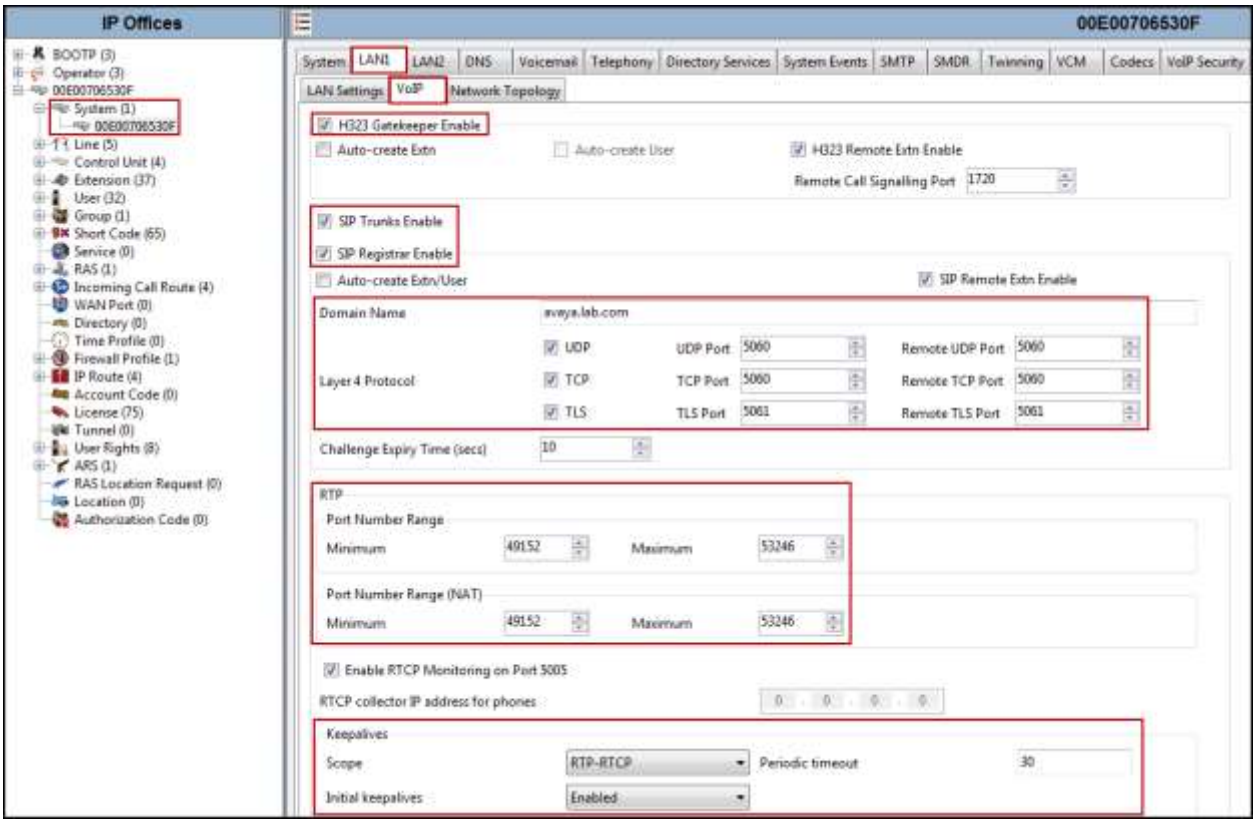
- Set the **IP Address** field to the LAN IP address, e.g., **172.16.5.60**.
- Set the **IP Mask** field to the subnet mask of the private network, e.g., **255.255.255.0**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).



The **VoIP** tab as shown in the screenshot below was configured with following settings:

©2016 Avaya Inc. All Rights Reserved.

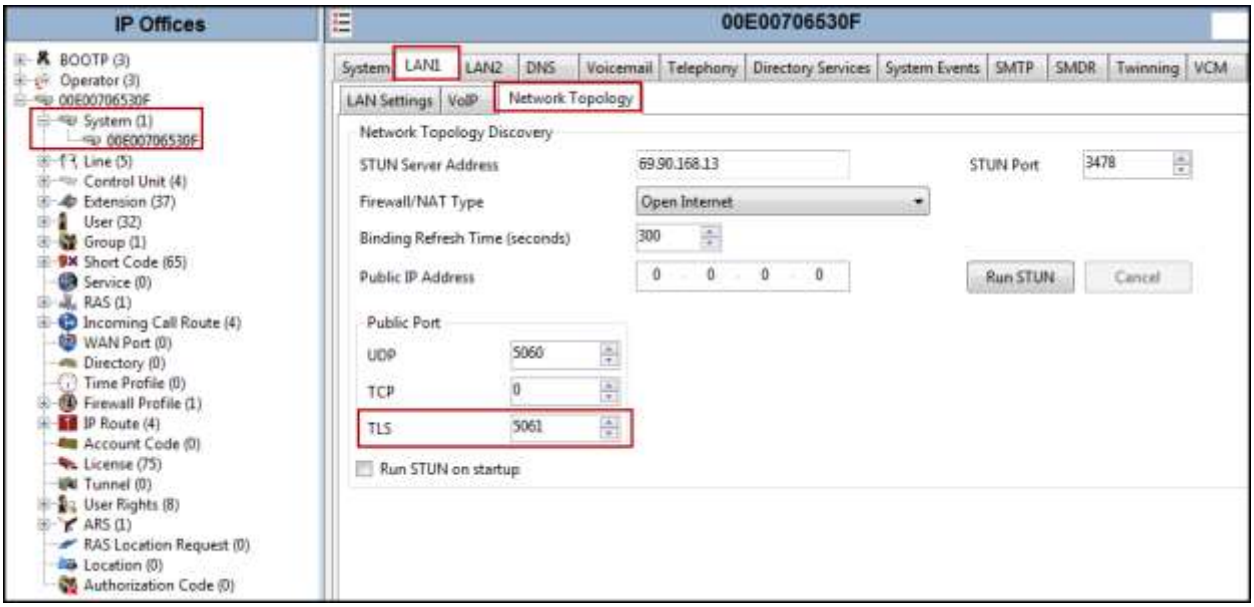
- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Clearcom.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name of the enterprise under **Domain Name**.
- Verify the **UDP Port**, **TCP Port** numbers under **Layer 4 Protocol** are set to **5060** and **TLS** port is set to **5061**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP-RTCP**, **Periodic Timeout** to **30**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP traffic is present.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).



In the **Network Topology** tab, configure the following parameters:

©2016 Avaya Inc. All Rights Reserved.

- Select the **Firewall/NAT Type** from the pull-down menu to the option that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even though the default STUN settings are populated, they will not be used.
- Set the **Binding Refresh Time (seconds)** to a desired value. The value of **300** (or every 5 minutes) was used during the compliance testing. This value is used to determine the **frequency** that IP Office will send OPTIONS heartbeats to the service provider.
- Verify the **Public IP Address** is set to **0.0.0.0**.
- Set the **Public Port** to **5061** for **TLS**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

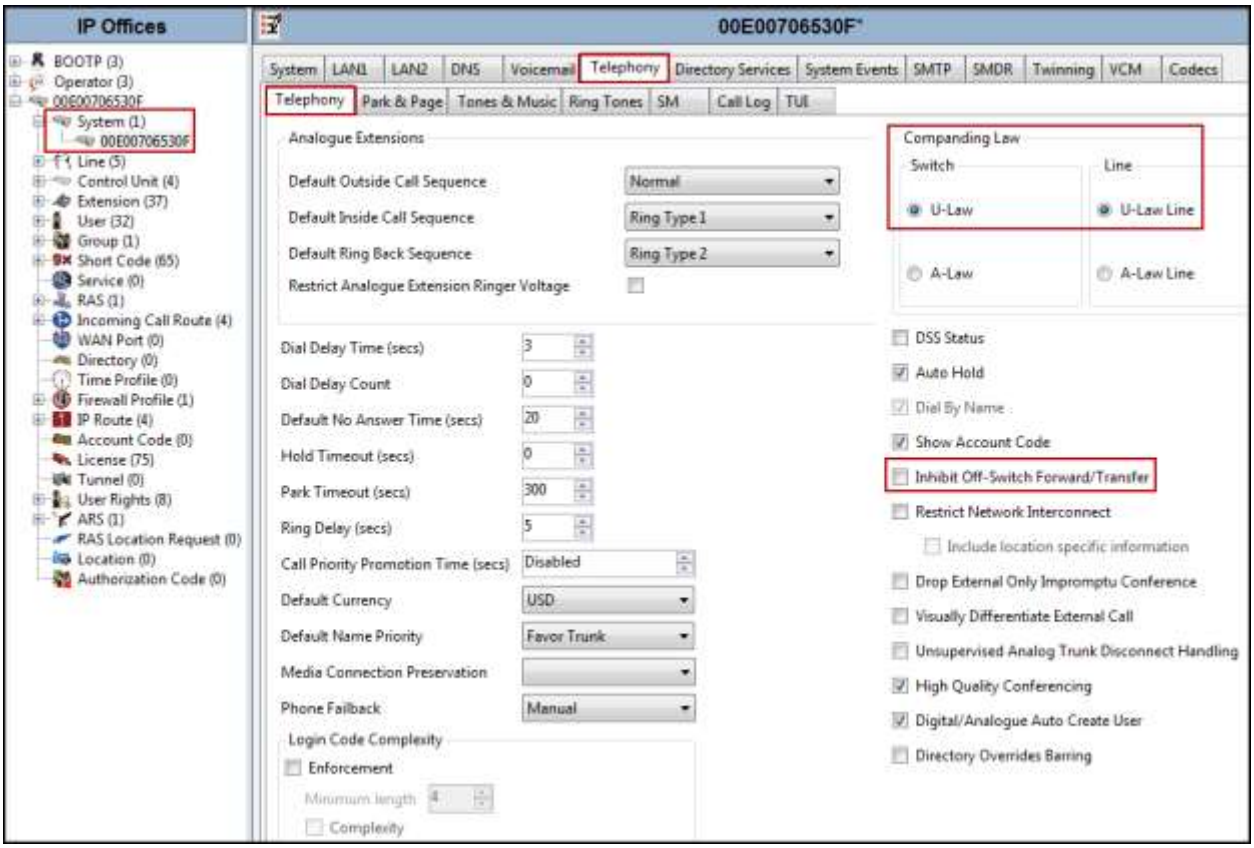


©2016 Avaya Inc. All Rights Reserved.

5.2.2 System - Telephony Tab

Navigate to the **Telephony → Telephony** Tab in the Details Pane, configure the following parameters:

- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).



©2016 Avaya Inc. All Rights Reserved.

5.2.3 System - Twinning Tab

Navigate to the **Twinning** tab on the Details Pane, configure the following parameters:

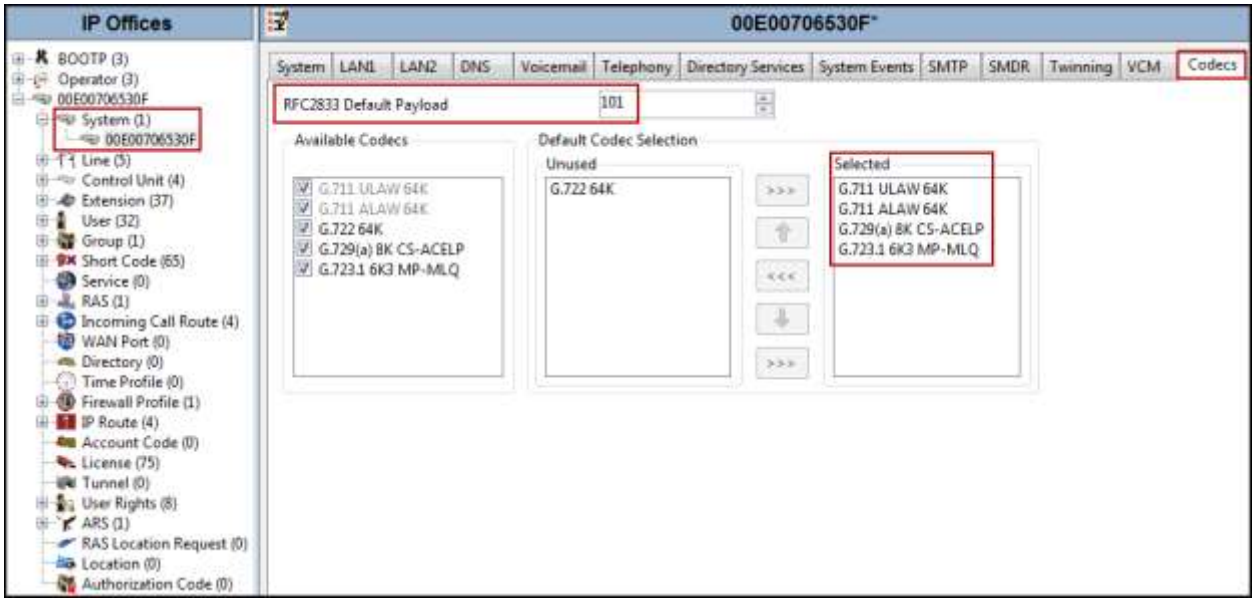
- Uncheck the **Send original calling party information for Mobile Twinning** box. This will allow the Caller ID for Twinning to be controlled by the setting on the SIP Line (**Section 5.4**). This setting also impacts the Caller ID for call forwarding.
- Click **OK** to commit (not shown).

©2016 Avaya Inc. All Rights Reserved.

5.2.4 System - Codecs Tab

For **Codecs** settings, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **Codecs** tab and configure the following parameters:

- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used.
- For **Codec Selection**, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order was used.
- Click **OK** to commit (not shown).



Note: The codec selections defined under this section (System – Codecs Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.6** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

©2016 Avaya Inc. All Rights Reserved.

5.2.5 System – VoIP Security Tab

Secure Real-Time Transport Protocol (SRTP) refers to the application of additional encryption and or authentication to VoIP calls (SIP and H.323). SRTP can be applied between telephones, between ends of an IP trunk or in various other combinations.

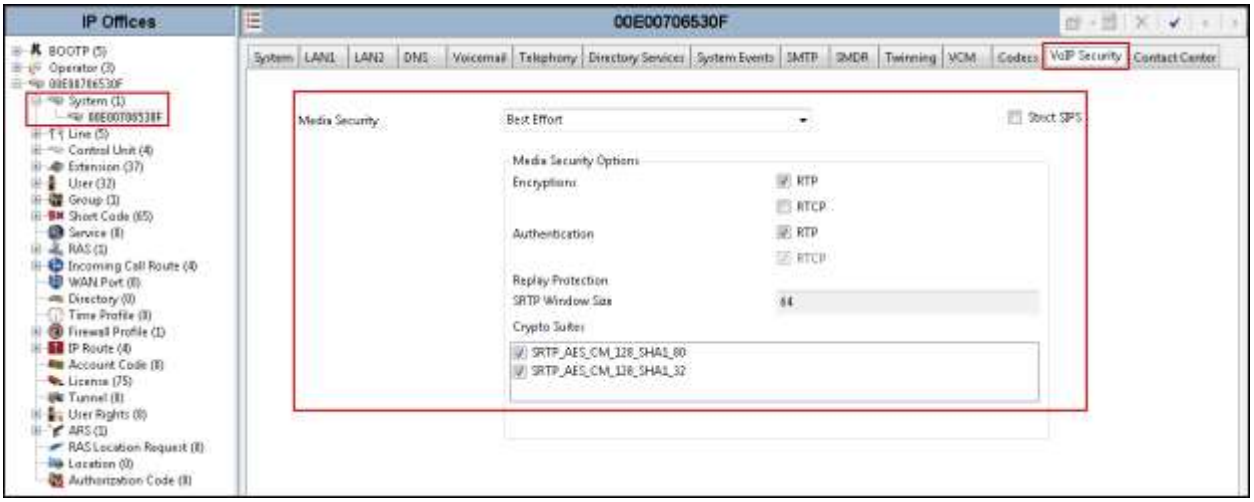
Configuring the use of SRTP at the system level is done on the **System VoIP Security** tab using the Media Security setting. The options are:

- Best Effort
- Disabled (default)
- Enforced

When enabling SRTP on the system, the recommended setting is **Best Effort**. In this scenario, IP Office uses SRTP if supported by the far-end, otherwise uses RTP. If the **Enforced** setting is used, and SRTP is not supported by the far-end, the call is not established (**Section 2.2**).

To configure the use of SRTP, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **VoIP Security** tab and configure the following parameters:

- Under **Media Security** select **Best Effort** from the pull down menu.
- Under **Media Security Options** ensure that **RTP** is checked under **Encryptions** and **Authentication**.
- Under Crypto Suites ensure that **SRTP_AES_CM_128_SHA1_80** and **SRTP_AES_CM_128_SHA1_32** are checked.
- Verify that Strict **SIPS** is not checked.
- Click **OK** to commit (not shown).



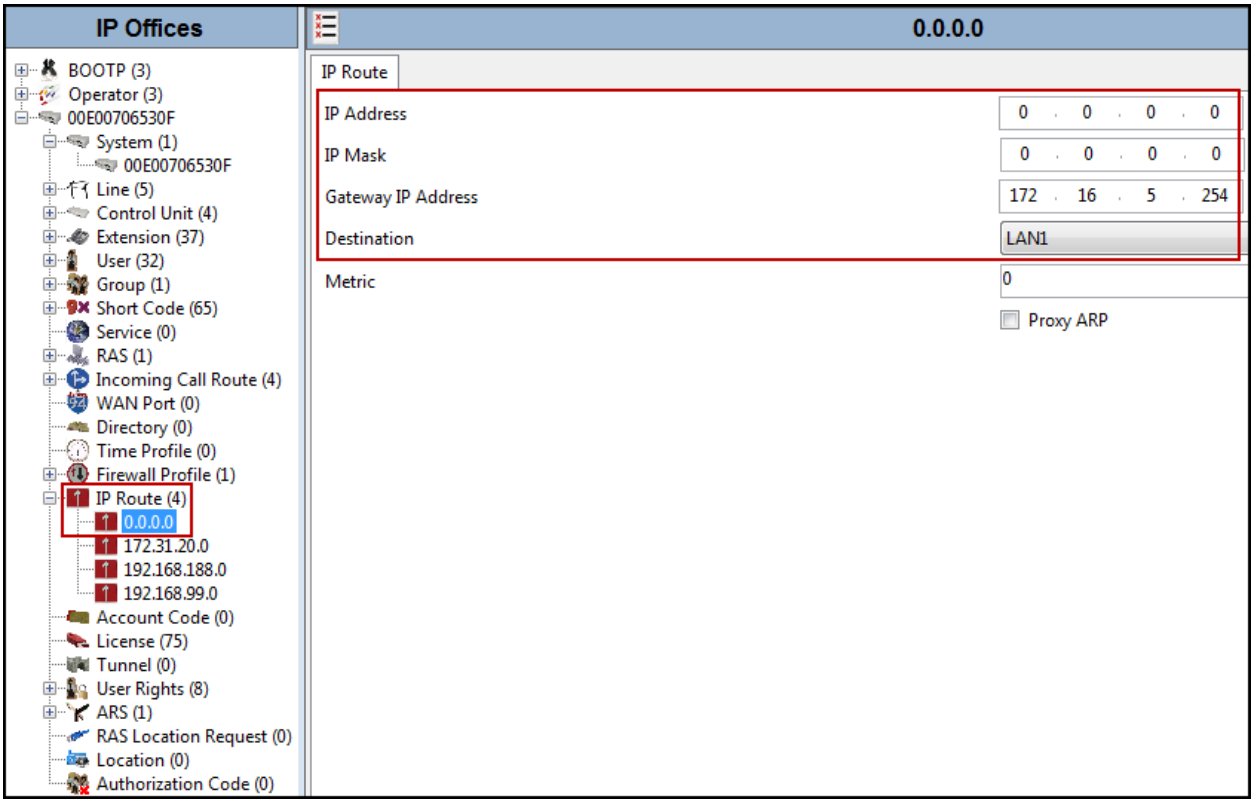
©2016 Avaya Inc. All Rights Reserved.

5.3 IP Route

In the reference configuration, the IP Office LAN1 interface and the private interface of the Avaya SBCE resided on the same IP subnet, so an IP route was not necessary. In an actual customer configuration, these two interfaces may be in different IP subnets, and in that case an IP route would have to be created to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to reach the IP subnet where the Avaya SBCE resides.

To create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to reach the IP subnet where the Avaya SBCE resides (if located in different subnets), on the left navigation pane, right-click on **IP Route** and select **New**.

- Set the **IP Address** and **IP Mask** of the subnet of the private side of the Avaya SBCE, or enter **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).



©2016 Avaya Inc. All Rights Reserved.

5.4 SIP Line

A SIP Line is needed to establish the SIP connection between IP Office and Clearcom SIP Trunking Service. 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 Avaya IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.4.1** and **5.4.2** 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 trunk Registration Credentials.
- 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 5.4.3** to **5.4.7**.

Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.3** to **5.4.7**.

5.4.1 Importing a SIP Line Template

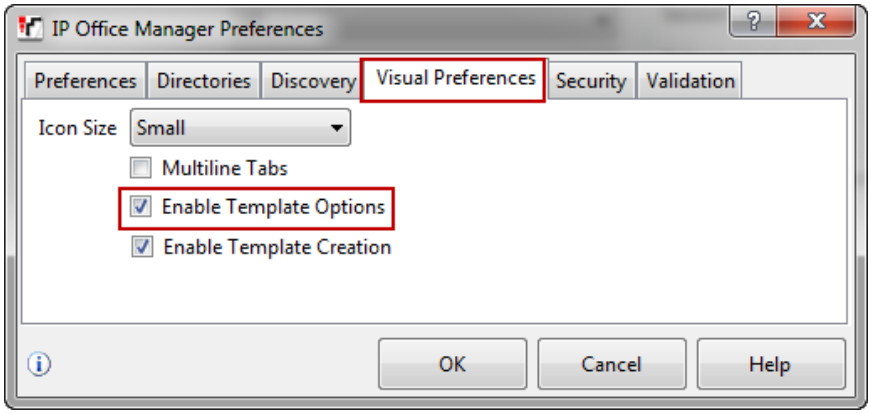
Note: DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500v2) 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.

1. Copy a previously created template file to a location (e.g., C:*Temp*) on the same computer where IP Office Manager is installed. By default, the template file name will have the format **AF_<*user supplied text*>_SIPTrunk.xml**, where the **<*user supplied text*>** portion is entered during template file creation.

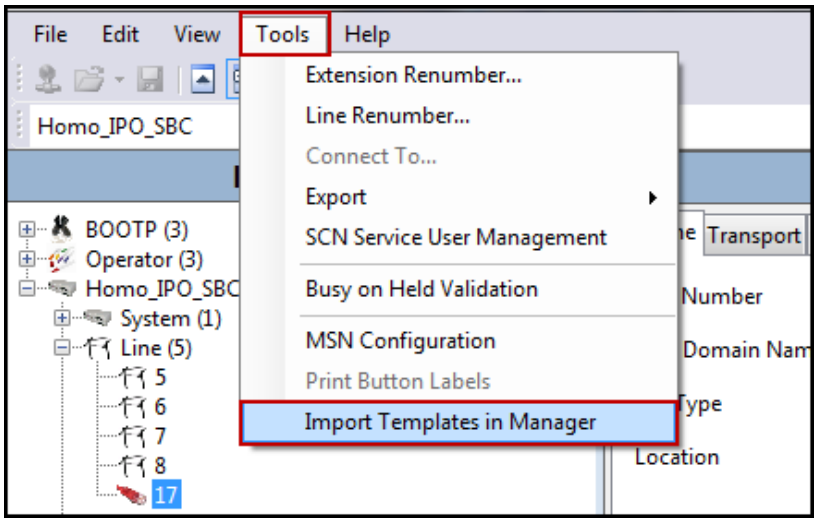
Note: If necessary, the **<*user supplied text*>** portion of the template file name may be modified, however the **AF_<*user supplied text*>_SIPTrunk.xml** format of the file name must be maintained. For example, an original template file **AF_*TEST* _SIPTrunk.xml** could be changed to **AF_*Test1*_SIPTrunk.xml**. The template file name is selected in **Section 5.4.2**, **step 2**, to create a new SIP Line.

©2016 Avaya Inc. All Rights Reserved.

2. Verify that Template Options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the **Visual Preferences** tab. Check the box next to **Enable Template Options**. Click **OK**.

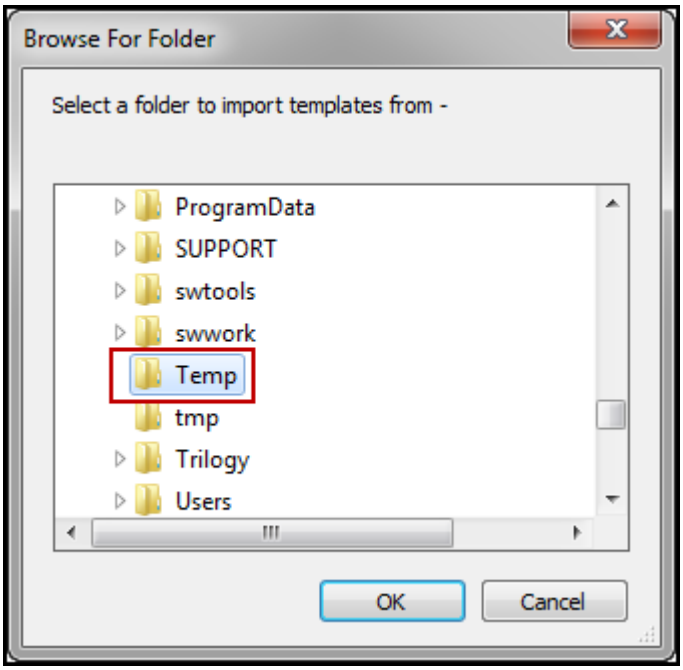


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**.



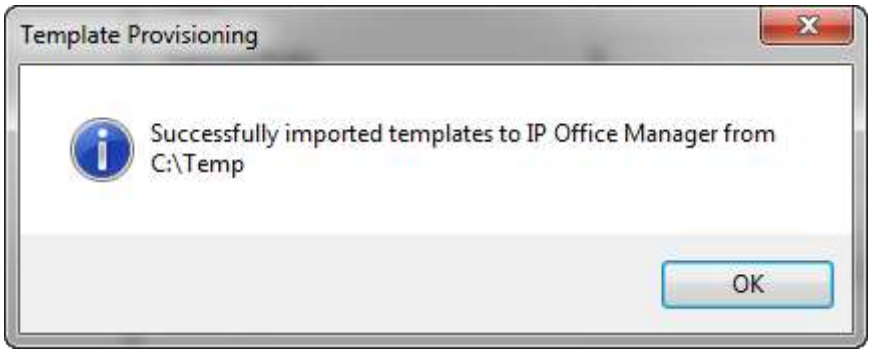
©2016 Avaya Inc. All Rights Reserved.

4. A folder browser will open. Select the directory used in **step 1** to store the template(s) (e.g., C:*Temp*).



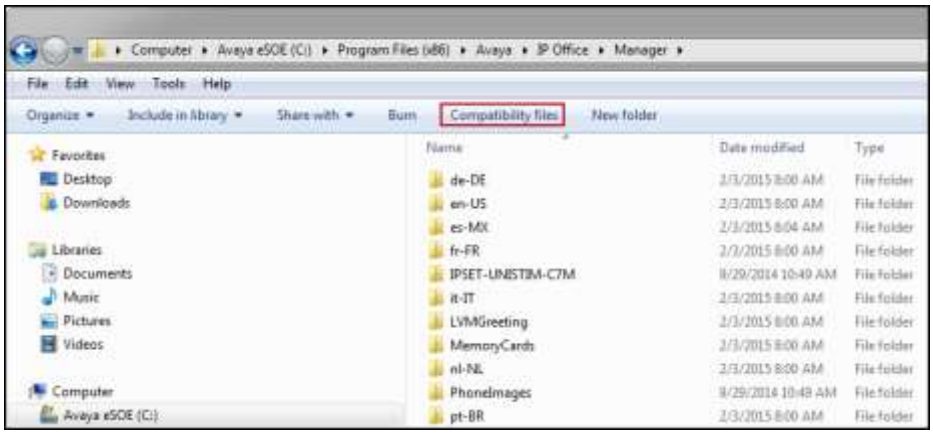
In the reference configuration, template files **AF_CLTLSIPO91SBCE7_SIPTrunk.xml** was imported. The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.

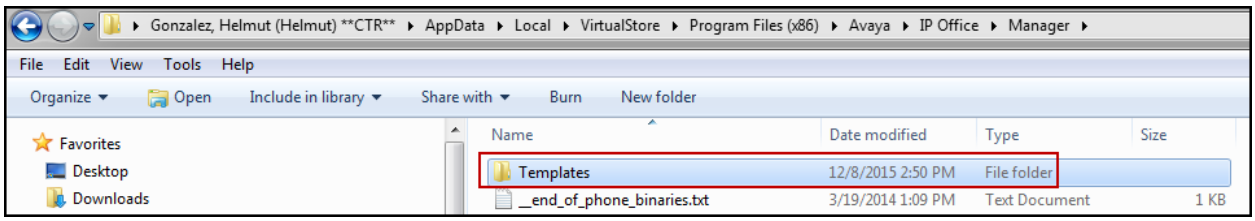
5. After the import is complete, a final import status pop-up window will open stating success or failure. Click **OK**.

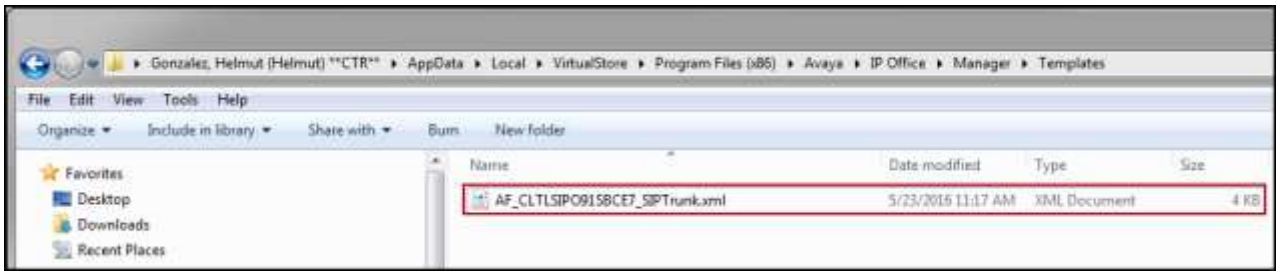


©2016 Avaya Inc. All Rights Reserved.

Note: Windows 7 (and later) locks the Avaya IP Office 9.1 **Templates** directory, and it cannot be viewed. To enable browsing of the **Templates** directory, open Windows Explorer, navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates** (or C:*Program Files (x86)*\Avaya\IP Office\Manager\Templates), and then click on the **Compatibility files** option shown below. The **Templates** directory and its contents can then be viewed.



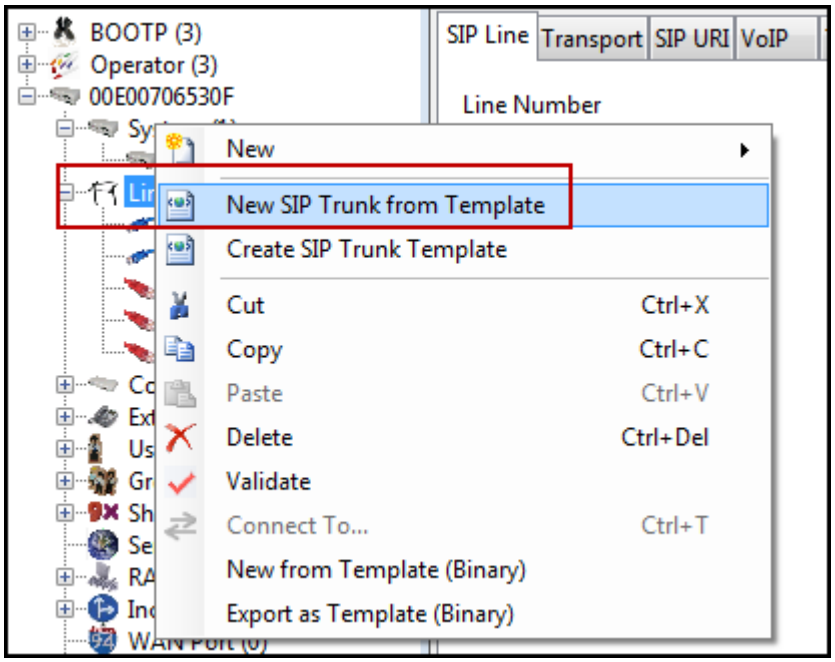




©2016 Avaya Inc. All Rights Reserved.

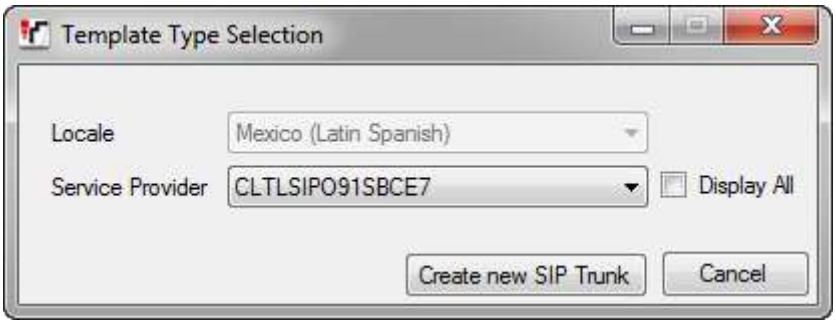
5.4.2 Creating a SIP Trunk from an XML Template

1. To create the SIP Trunk from a template, right-click on **Line** in the Navigation Pane, and select **New SIP Trunk from Template**.



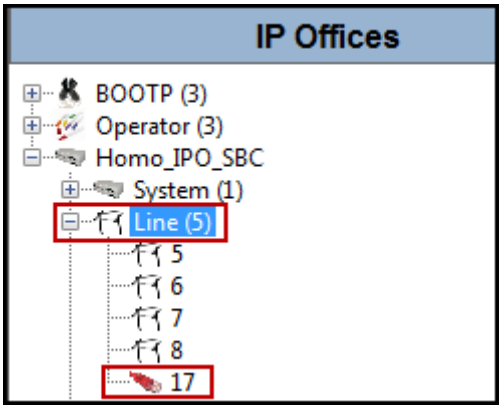
2. In the subsequent **Template Type Selection** pop-up window, from the **Service Provider** pull-down menu, select the XML template name from **Section 5.4.1**. Click **Create new SIP Trunk**.

Note: The drop down menu will display the ***<user supplied text>*** part of the template file name (see **Section 5.4.1**). If you check the **Display All** box, then the full template file name is displayed.



©2016 Avaya Inc. All Rights Reserved.

The newly created SIP Line will appear in the Navigation pane (e.g., SIP Line **17**).



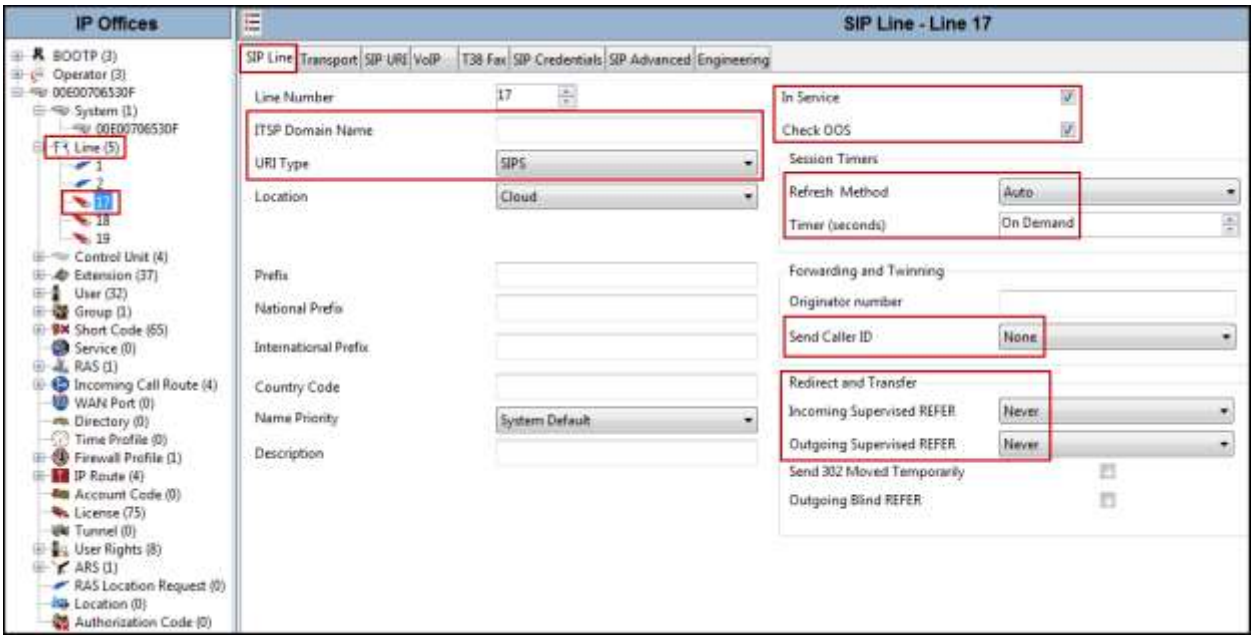
It is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.3** to **5.4.7**.

©2016 Avaya Inc. All Rights Reserved.

5.4.3 SIP Line - SIP Line Tab

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

- Leave the **ITSP Domain Name** blank. Note that if this field is left blank, then IP Office inserts the ITSP Proxy Address from the Transport tab as the ITSP Domain in the SIP messaging.
- Verify that **URI Type** is set to **SIPS**.
- Verify that **In Service** box is checked, which is the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line. The time between SIP OPTIONS sent by IP Office will use the Binding Refresh Time for LAN1, as shown in **Section 5.2.1**.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (seconds)** is set to **On Demand**.
- Set **Send Caller ID** to **Diversion Header**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** Support and **Outgoing Supervised REFER** to **Never** (Refer to **Section 2.2**).
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

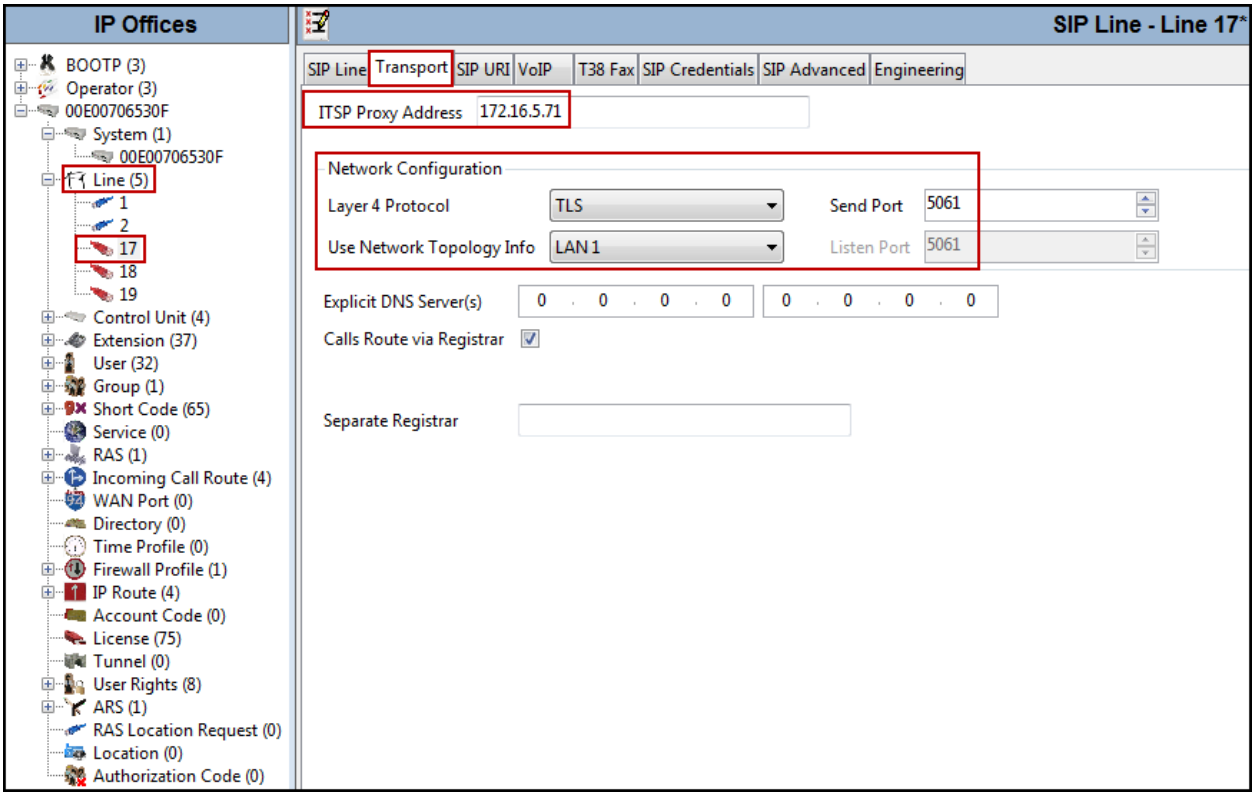


©2016 Avaya Inc. All Rights Reserved.

5.4.4 SIP Line - Transport Tab

Select the **Transport** tab; configure the parameters as shown below:

- Set the **ITSP Proxy Address** to the IP address of the inside interface (or private side) assigned to the Avaya SBCE, as shown on **Figure 1** (**Note**: On interface **A1** of the Avaya SBCE, IP address **172.16.5.71** was used to connect to IP Office, refer to **Section 7.5.1**).
- Set the **Layer 4 Protocol** to **TLS**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2.1**.
- Set the **Send Port** to **5061**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



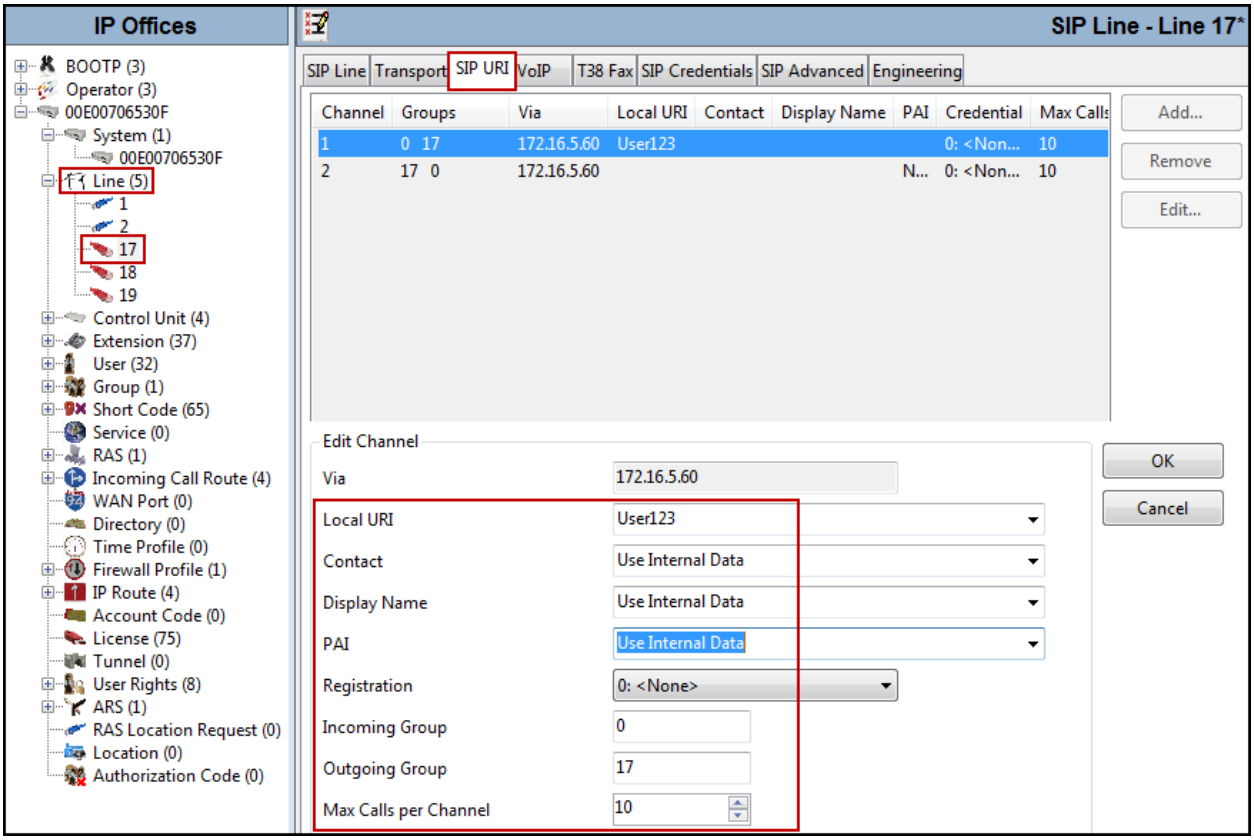
©2016 Avaya Inc. All Rights Reserved.

5.4.5 SIP Line - SIP URI Tab

Two SIP URI entries must be created to match each outgoing number that Avaya IP Office will send on this line and incoming numbers that Avaya IP Office will accept on this line.

To set the SIP URI for outgoing numbers, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. The entry was created with the parameters shown below:

- Set **Local URI** to the user name associated with the SIP trunk credentials provided by Clearcom. Clearcom required the user name to be sent in the "From" header.
- Set **Contact**, **Display Name and PAI** to **Use Internal Data**.
- Under **Registration**, select **0: <None>** from the pull-down menu.
- Set **Incoming Group** to **0**.
- Set **Outgoing Group** to **17** (SIP Line number being used).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern
- Click **OK**.
- Click **OK** again to commit (not shown).

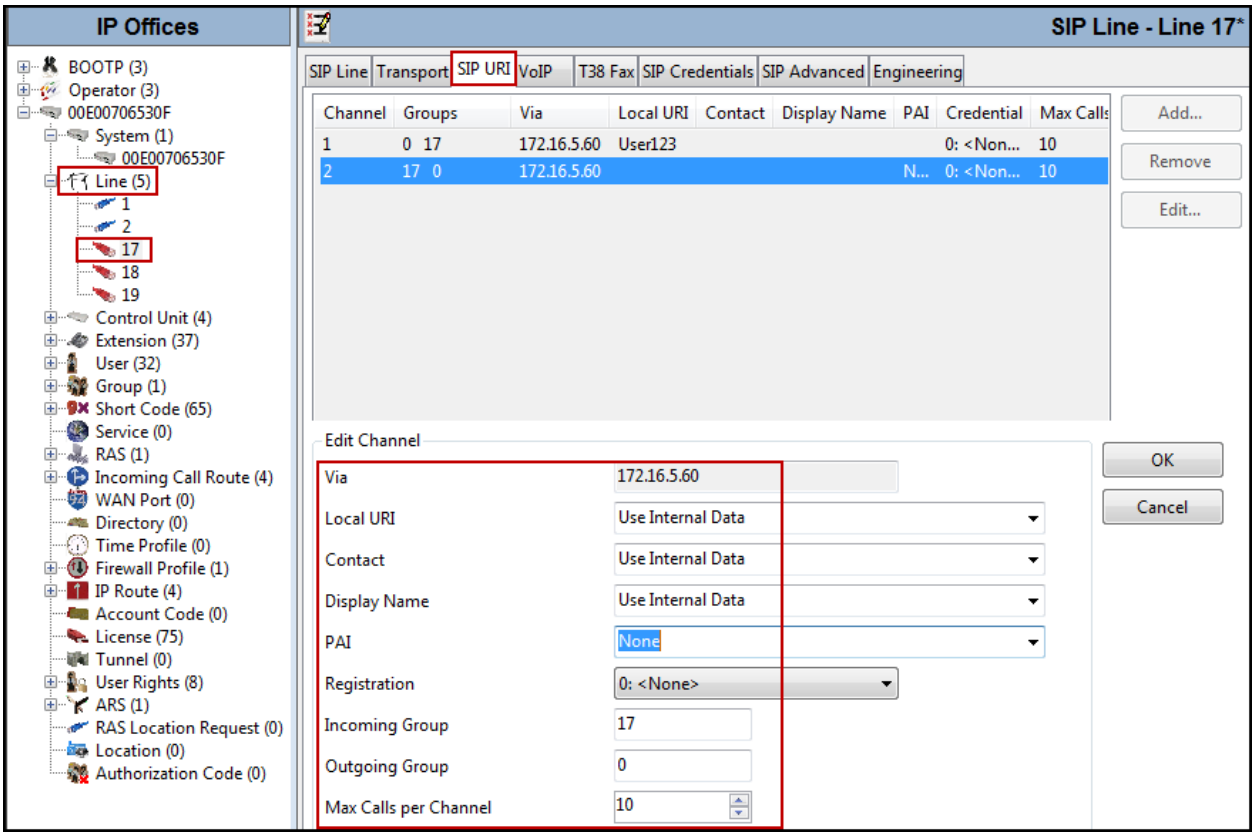


To set the SIP URI for inbound calls, select the **SIP URI** tab and click the **Add** button. The **New**

©2016 Avaya Inc. All Rights Reserved.

Channel area will appear at the bottom of the pane. Set the parameters as shown below:

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**. This setting allows calls on this line that have a SIP URI that matches the number set in the **SIP** tab of any user as shown later in **Section 5.6**.
- Set **PAI** to ***None***.
- Under **Registration**, select **0: <None>** from the pull-down menu.
- Set **Incoming Group** to **17** (SIP Line number being used).
- Leave the **Outgoing Group** field with the default value ***0***.
- Set **Max Calls per Channel** to the number of simultaneous calls to be allowed on the SIP trunk using this SIP URI pattern.
- Click **OK**.
- Click **OK** again to commit (not shown).



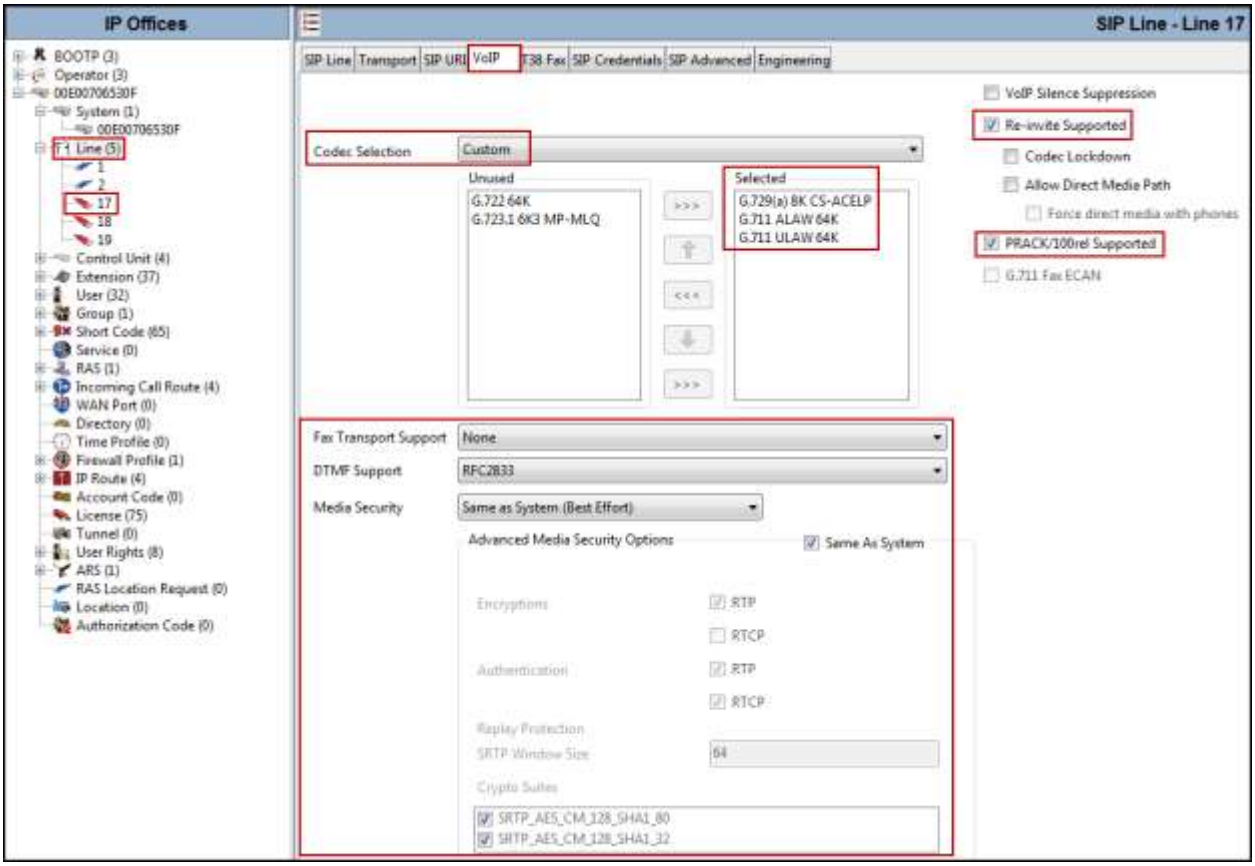
5.4.6 SIP Line - VoIP Tab

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** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line, as shown. Clearcom supports codec G.729(a), G.711 ALAW and G.711ULAW for audio, with G.729(a) being the preferred codec.
- Select **None** for **Fax Transport Support** (Refer to **Section 2.2**).

©2016 Avaya Inc. All Rights Reserved.

- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set the **Media Security** field to **Same as System (Best Effort)**. Use the same setting as the system setting configured on the **System | VoIP Security** tab.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.
- Check the **PRACK/100rel Supported** box, to advertise the support for reliable provisional responses and Early Media to Clearcom.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



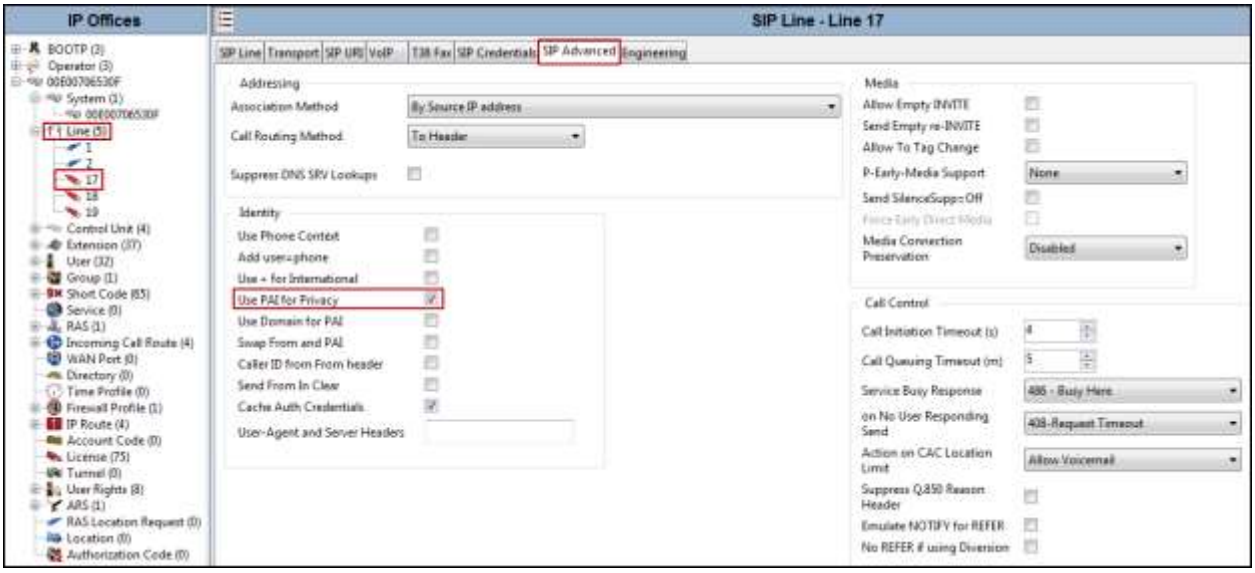
Note: The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.4** (System – Codecs tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

©2016 Avaya Inc. All Rights Reserved.

5.4.7 SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab. For outbound calls with privacy enabled, Avaya IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with "anonymous". IP Office can be configured to use the P-Preferred-Identity (PPI) or P-Asserted-Identity (PAI) header to pass the actual calling party information for authentication and billing purposes. By default, IP Office will use the PPI header for privacy. To configure IP Office to use the PAI header for privacy calls:

- Check the box for **Use PAI for Privacy**.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

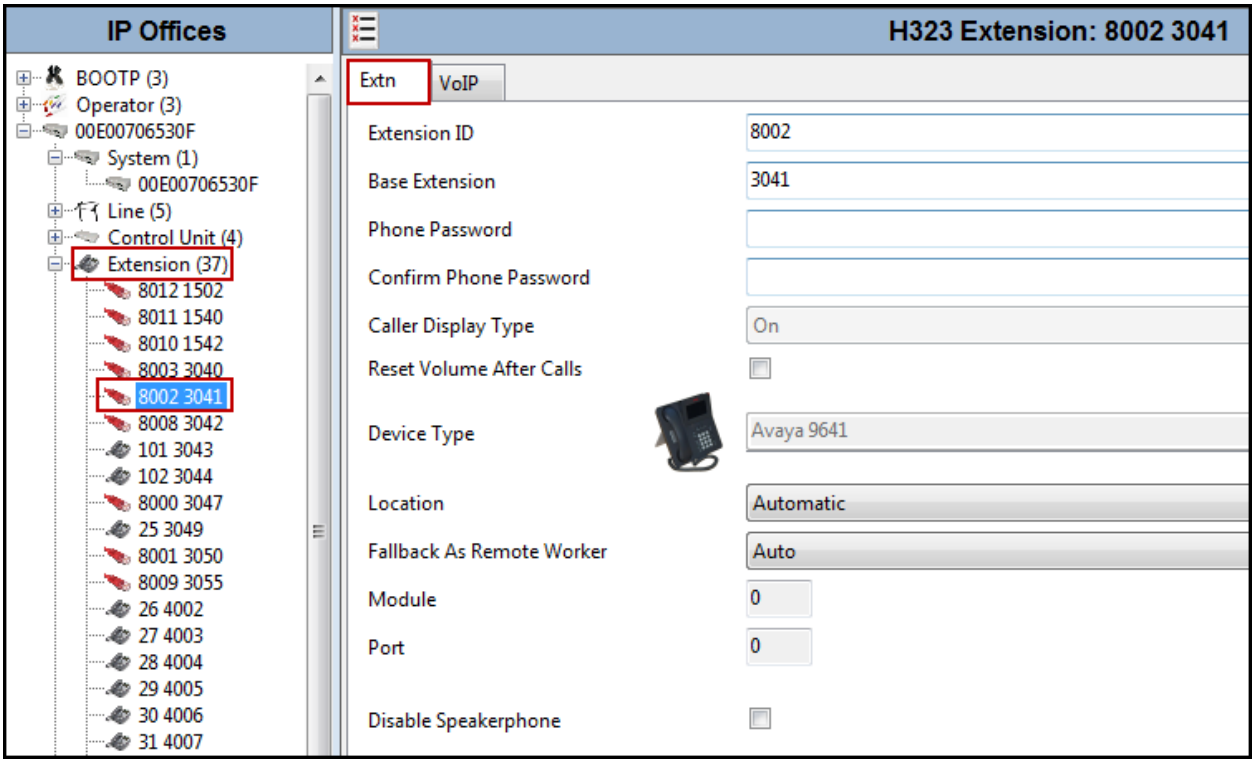


©2016 Avaya Inc. All Rights Reserved.

5.5 Extension

In this section, an example of an Avaya IP Office extension will be illustrated. In the interests of brevity, not all users and extensions will be presented, since the configuration can be easily extrapolated to other users and extensions. To add an extension, right click on **Extension** then select **New → Select H323 or SIP**.

Select the **Extn** tab. Following is an example of extension 3041; this extension corresponds to an H.323 extension.

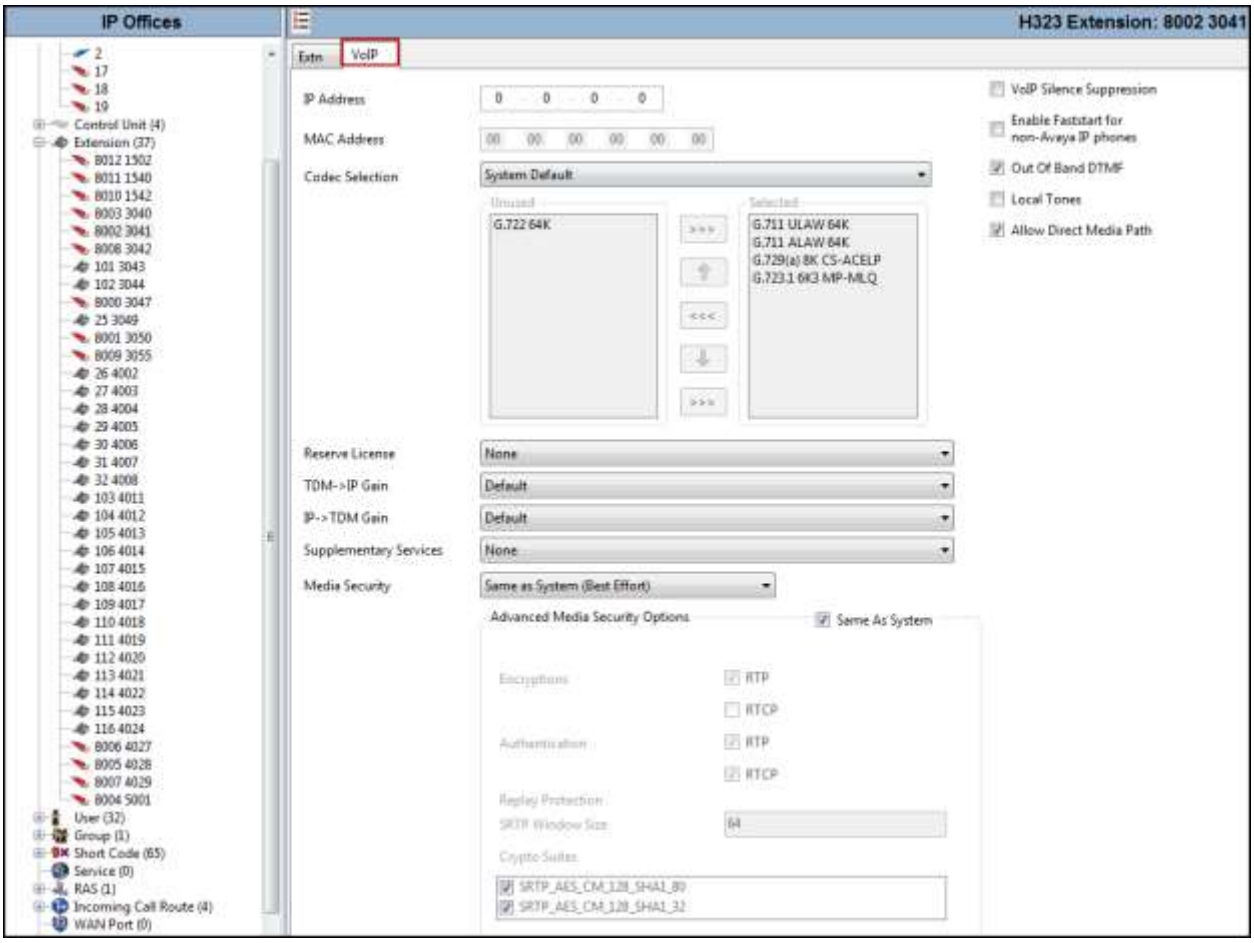


©2016 Avaya Inc. All Rights Reserved.

Select the **VOIP** tab. Use default values on VoIP tab. Following is an example for extension 3041; this extension corresponds to an H.323 extension.

By default, all IP phones (SIP and H.323) will use the system default codec selection configured under the System Codecs tab (**Section 5.2.4**), unless configured otherwise for a specific extension by selecting **Custom** under **Codec Selection** on the screenshot shown below. The example below shows the codecs used for IP phones (SIP and H.323).

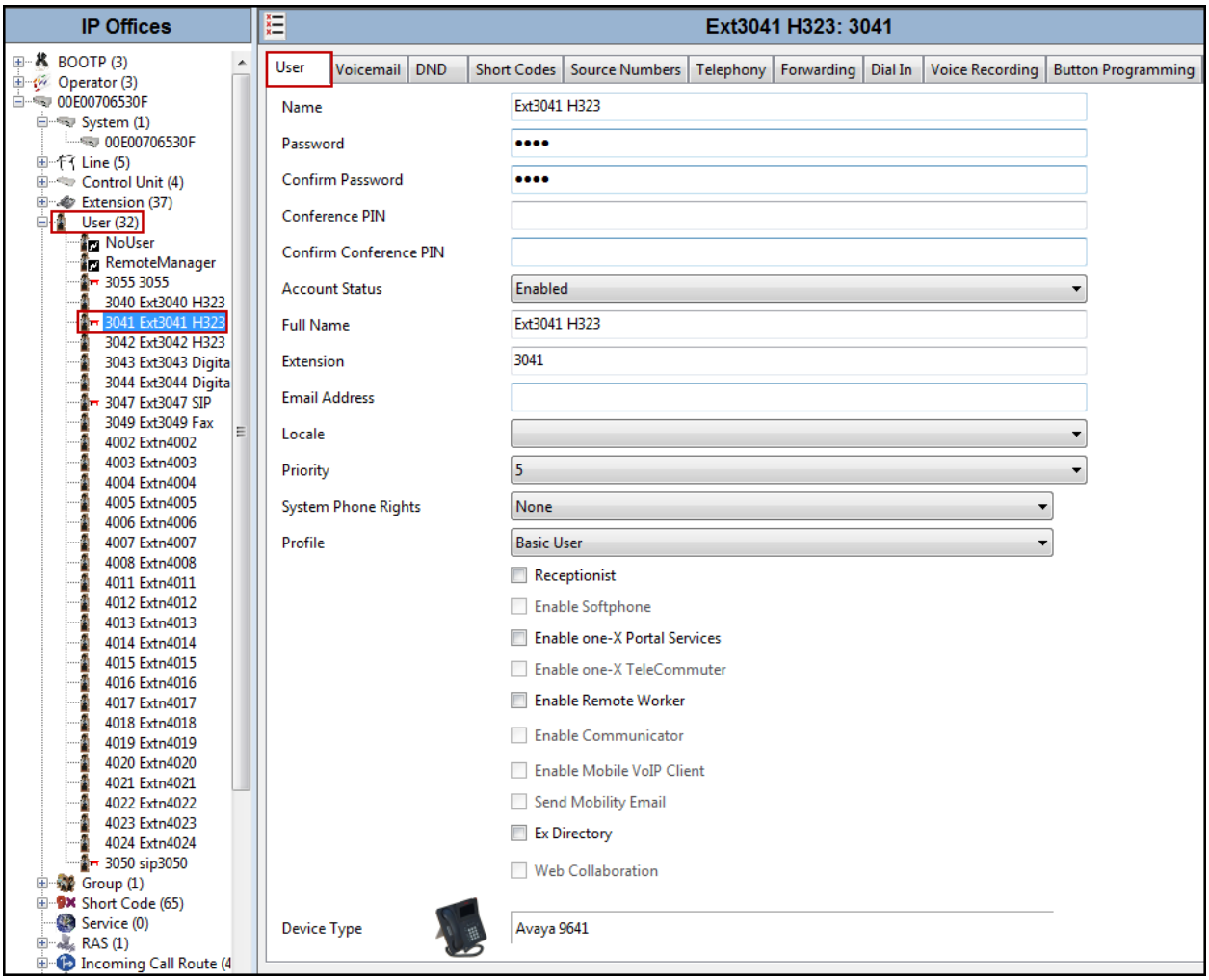
By default, all IP phones (SIP and H.323) will use the system default Media Security selection configured under the System **VoIP Security** tab (**Section 5.2.5**), unless configured otherwise for a specific extension by selecting **Media Security** under **VoIP** tab on the screenshot shown below. The **Media Security** field was set to **Same as System (Best Effort)**. The example below shows the Media Security used for IP phones (SIP and H.323).



©2016 Avaya Inc. All Rights Reserved.

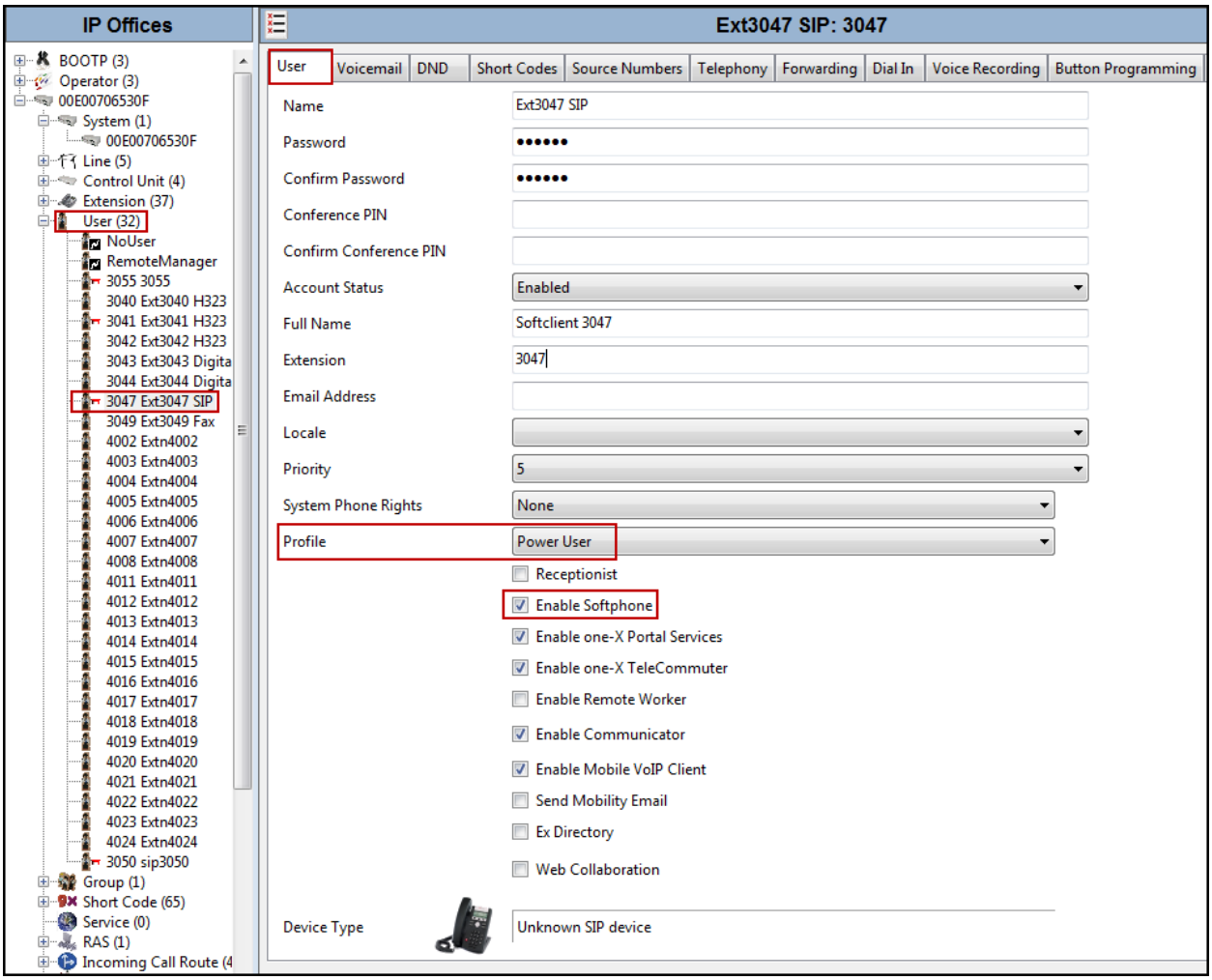
5.6 Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.4**. To configure these settings, first navigate to **User** in the left Navigation Pane, and then select the name of the user to be modified. In the example below, the name of the user is **Ext3041 H323**.



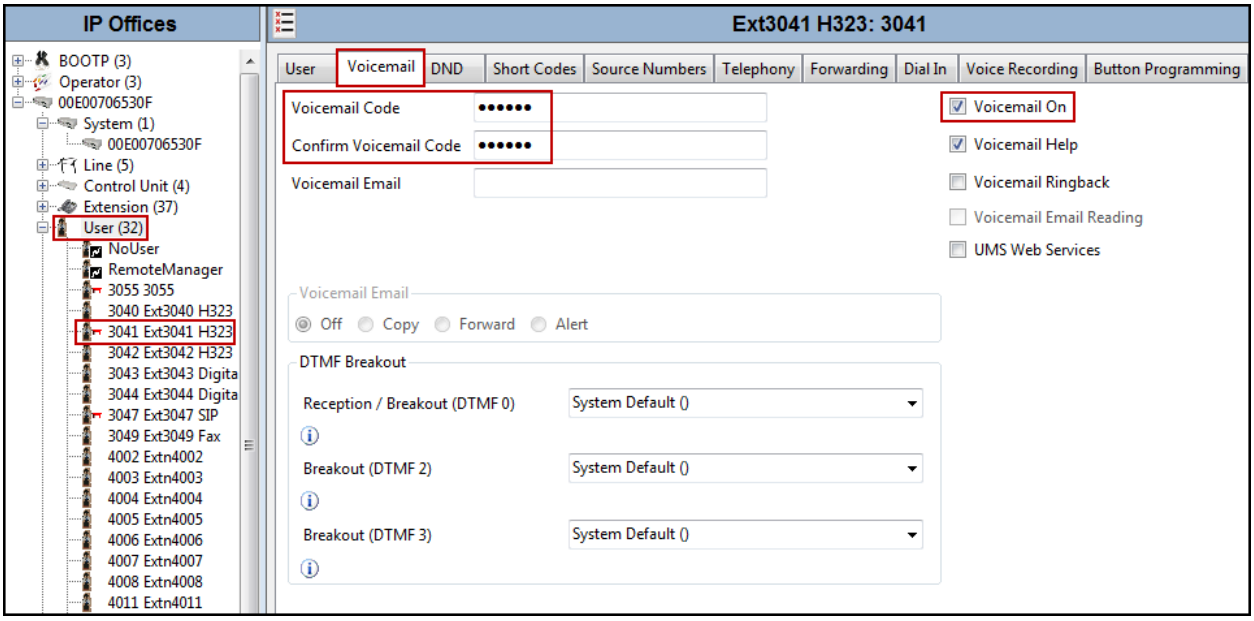
©2016 Avaya Inc. All Rights Reserved.

In the example below, the name of the user is **Ext3047 SIP**. This is a Softphone user, set the **Profile** to **Power User** and check **Enable Softphone**.

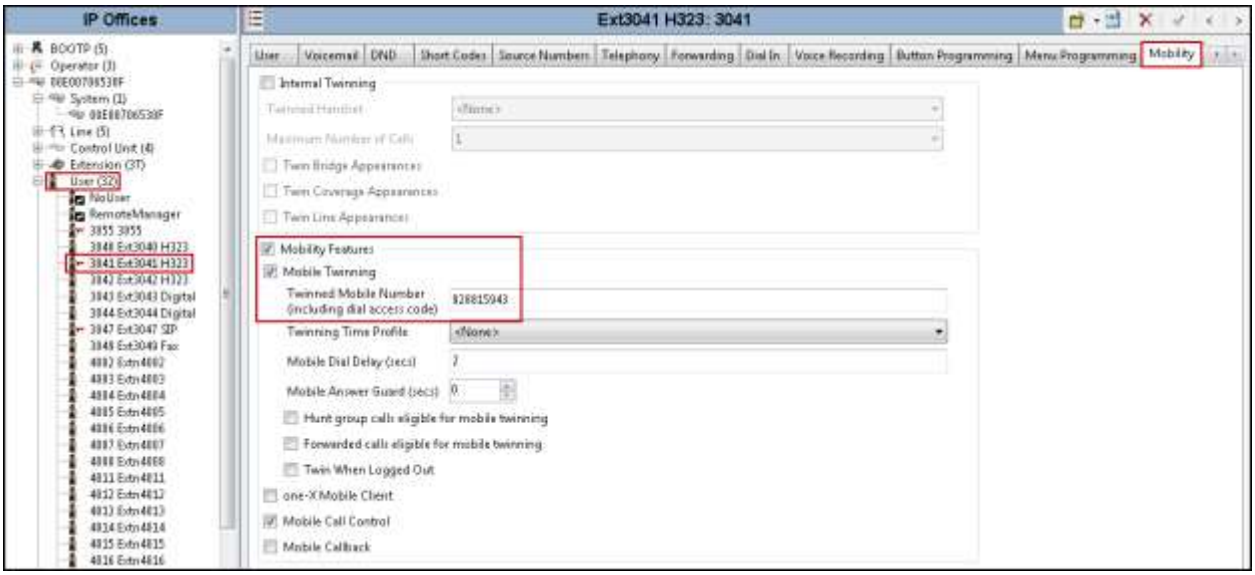


©2016 Avaya Inc. All Rights Reserved.

Select the **Voicemail** tab. The following screen shows the **Voicemail** tab for the user with extension 3041. The **Voicemail On** box is checked. Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters. In the verification of these Application Notes, incoming calls from Clearcom to this user were redirected to Voicemail Pro after no answer. Voicemail messages were recorded and retrieved successfully. Voice mail navigation and retrieval were performed locally and from PSTN telephones to test DTMF using RFC 2833.

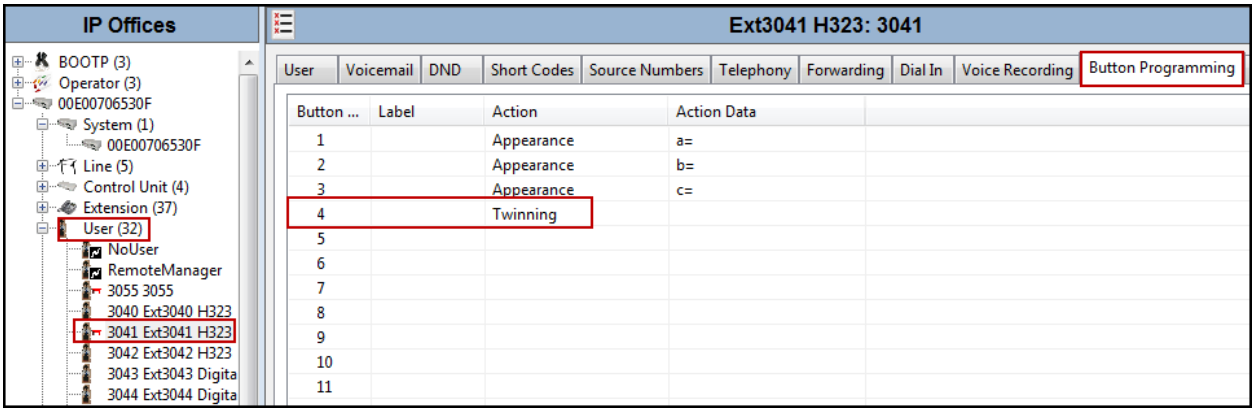


Select the **Mobility** tab. In the sample configuration user 3041 was one of the users configured to test the Mobile Twinning feature. The following screen shows the **Mobility** tab for user 3041. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned telephone, including the dial access code "9", in this case **928815943**. Other options can be set according to customer requirements.



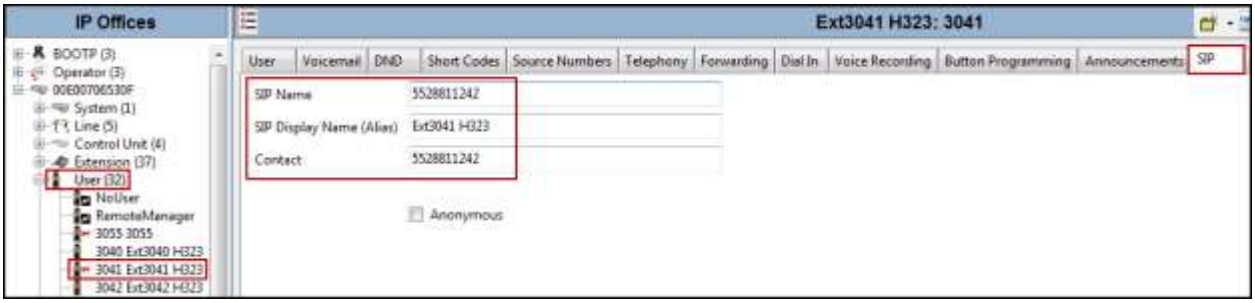
©2016 Avaya Inc. All Rights Reserved.

To program a key on the telephone to turn Mobile Twinning on and off, select the **Button Programming** tab on the user, then select the button to program to turn Mobile Twinning on and off, click on **Edit →Action→Emulation**, select **Twinning** (not shown). In the sample below, button **4** was programmed to turn Mobile Twinning on and off for user 3041.



Select the **SIP** tab. 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. In addition, these settings are used to match against the SIP URI of incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.4**). The example below shows the settings for user "Ext3040 H323". The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Clearcom. In the example, DID number **5528811242** was used. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.

If all calls involving this user should be considered private, then the **Anonymous** box may be checked to withhold the Caller ID information from the network.



©2016 Avaya Inc. All Rights Reserved.

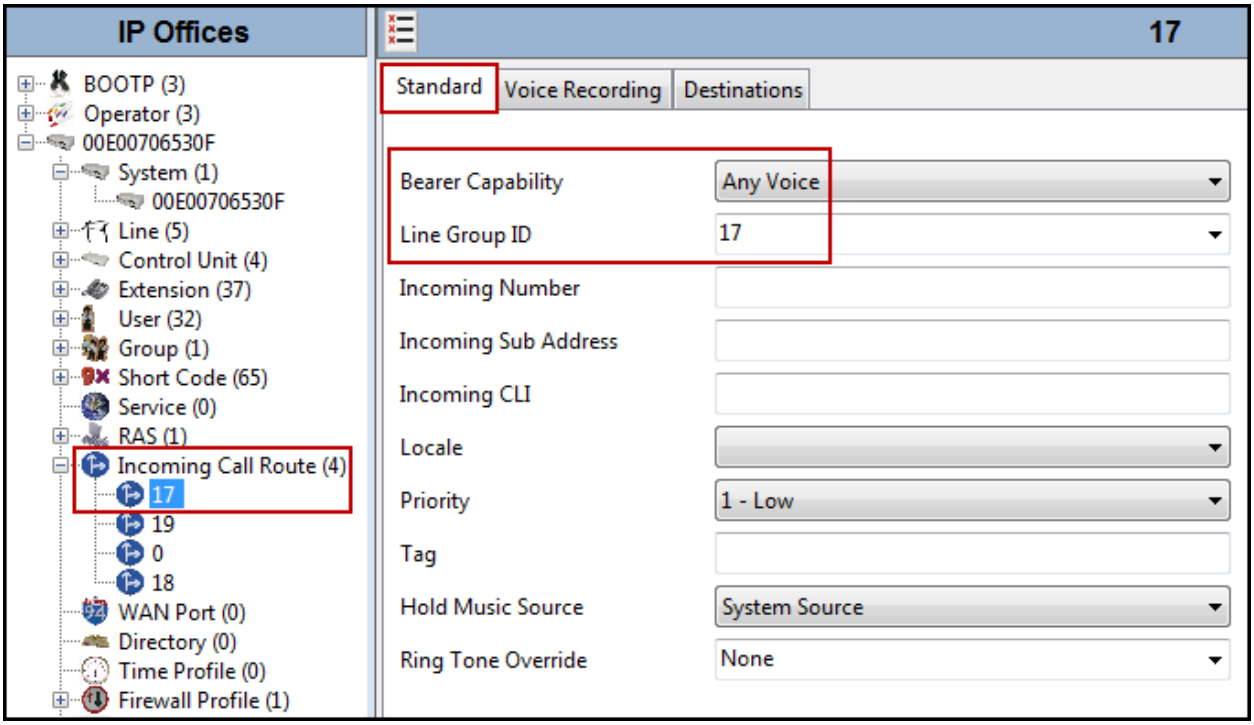
5.7 Incoming Call Route

An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system.

In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in IP Office. The routing decision for the call is based on the parameters previously configured for **Call Routing Method** and **SIP URI** (**Section 5.4.5** and **5.4.7**) and the users **SIP Name** and **Contact**, already populated with the assigned Clearcom DID numbers (**Section 5.6**).

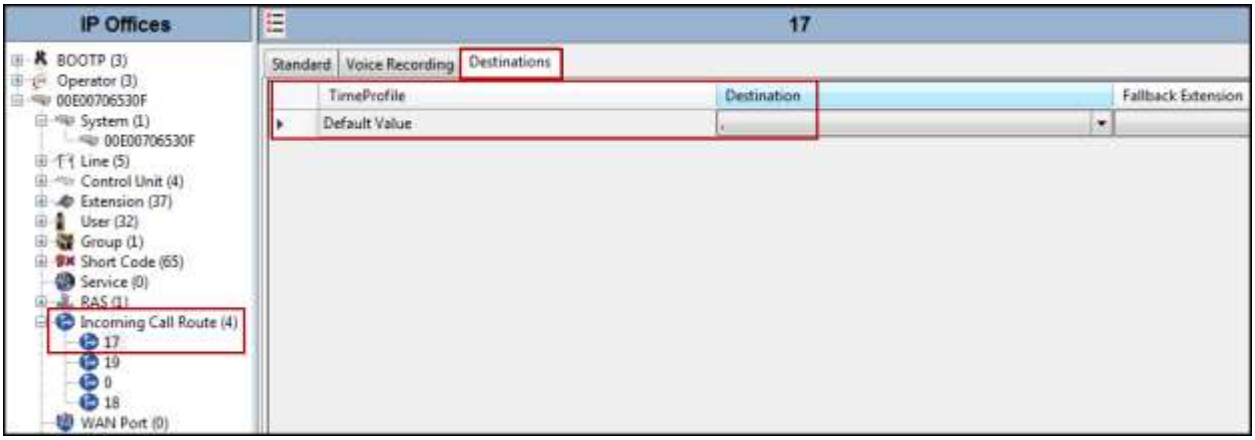
From the left Navigation Pane, right-click on **Incoming Call Route** and select **New**.
On the Details Pane (not shown), under the **Standard** tab, set the parameters as show below:

- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group ID** to the incoming line group of the SIP line defined in **Section 5.4**.
- Default values may be used for all other parameters.



©2016 Avaya Inc. All Rights Reserved.

- Under the **Destinations** tab, enter "**.**" for the **Destination**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of that **User**, which matches the number present on the user part of the incoming Request URI.
- Click **OK** to commit (not shown).



©2016 Avaya Inc. All Rights Reserved.

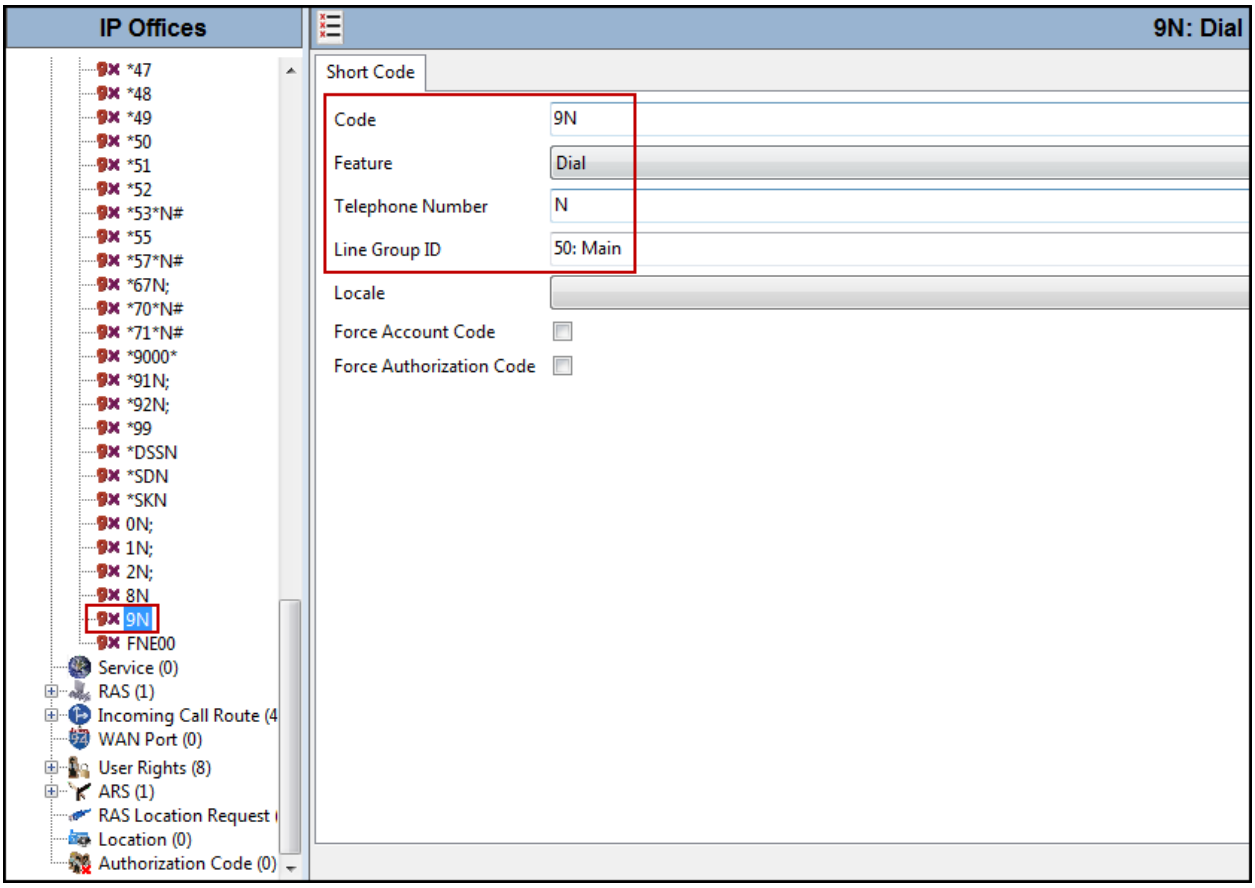
5.8 Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used.

5.8.1 Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code** on the Navigation Pane and select **New**. The screen below shows the short code **9N** created (Note that the semi-colon is not used here). In this case, when the Avaya IP Office user dials 9 plus any number **N**, instead of being directed to a specific Line Group ID, the call is directed to **Line Group 50: Main**, which is configurable via ARS. Configure the following parameters:

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **9N** was used (Note that the semi-colon is not used here).
- 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 is passed to ARS.
- Set the **Line Group Id** to **50: Main** to be directed to **Line Group 50: Main**, this is configurable via ARS.
- Click the **OK** to commit (not shown).

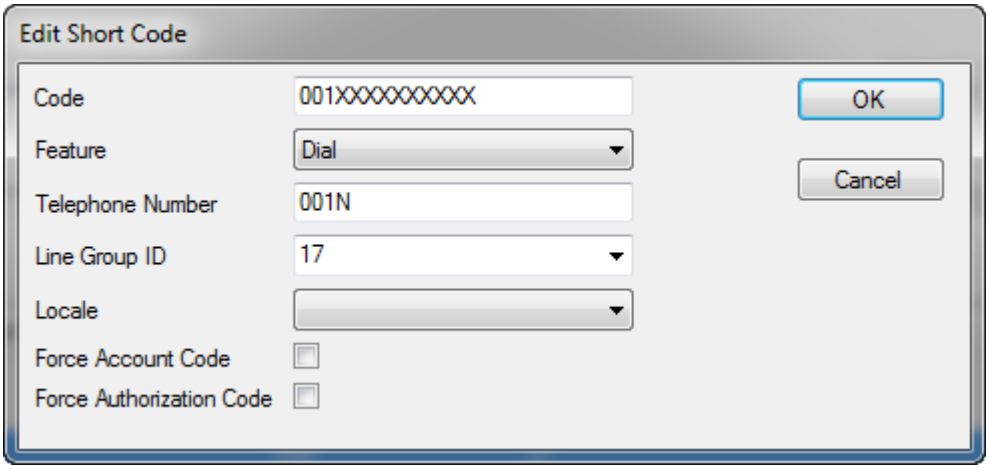


©2016 Avaya Inc. All Rights Reserved.

The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **X**s used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office.

To create a short code to be used for ARS, select **ARS → 50: Main** on the Navigation Pane and click **Add**. Configure the following parameters:

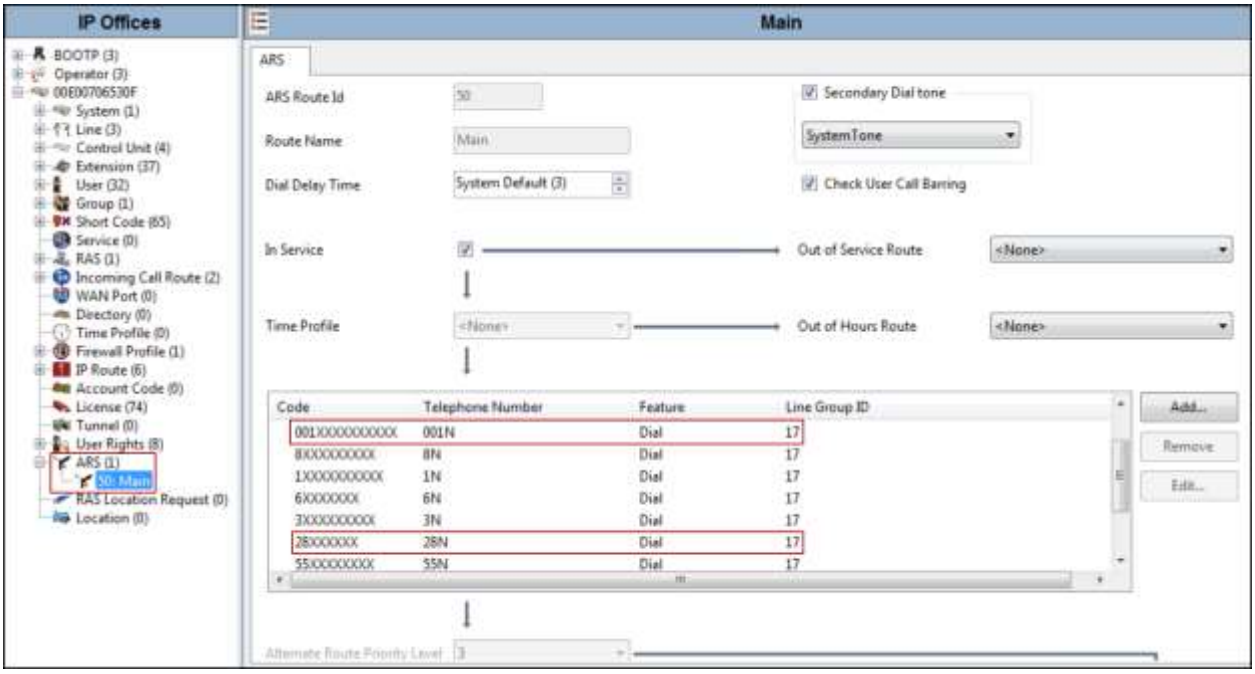
- In the **Code** field, enter the dial string which will trigger this short code. In this case, **001** followed by **10 Xs** to represent the exact number of digits. Note that **001** is used for international calls from Mexico to North America (U.S.).
- Set **Feature** to **Dial.** This is the action that the short code will perform.
- Set **Telephone Number** to **001N**. The value **N** represents the additional number of digits dialed by the user after dialing **001** (The **9** will be stripped off).
- Set the **Line Group Id** to the Line Group number being used for the SIP Line, in this case **Line Group ID 17** was used.
- Click OK to commit.



Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

©2016 Avaya Inc. All Rights Reserved.

The first example highlighted below shows that for calls from Mexico to the North American Numbering Plan, the user dialed **9**, followed by **001** and **10** digits (represented by **10 Xs**). The second example highlighted shows an eight digit number starting with a **28**, which is for local calls in Mexico. The user dialed **9**, followed by the local number (e.g., 28811234). In each case the **9** is stripped off, the remaining digits, including the **001** and **28** shown in the examples below, are included in the SIP INVITE message IP Office sends to Clearcom.



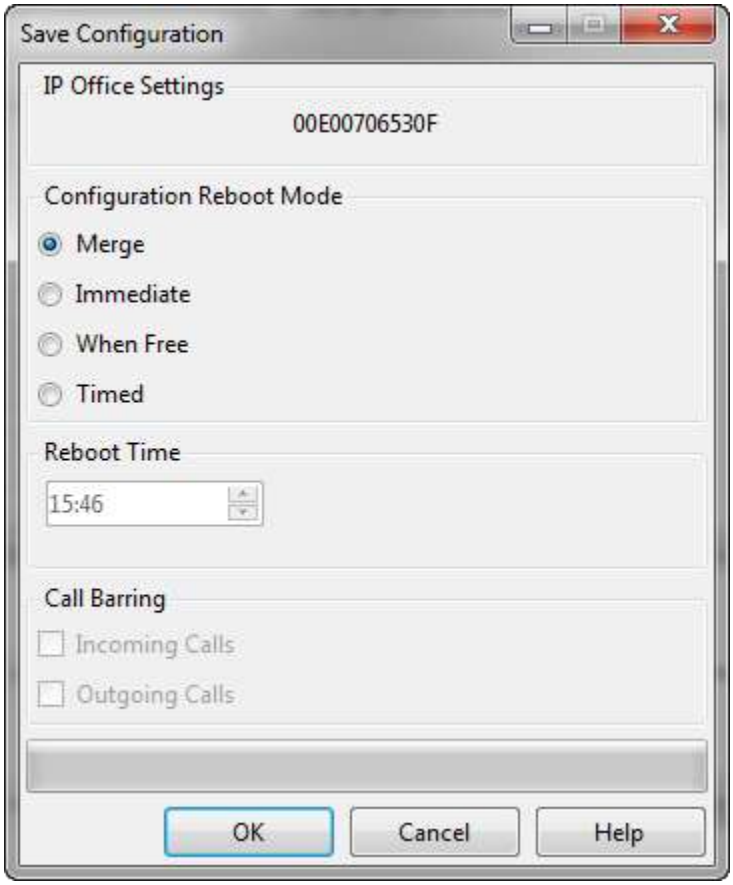
©2016 Avaya Inc. All Rights Reserved.

5.9 Save Configuration

When desired, send the configuration changes made in Avaya IP Office Manager to the Avaya IP Office server in order for the changes to take effect.

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

Once the configuration is validated, a screen similar to the following will appear, with either the **Merge** or the **Immediate** radio button chosen based on the nature of the configuration changes made since the last save. Note that clicking OK may cause a service disruption due to system reboot. Click **OK** if desired.



©2016 Avaya Inc. All Rights Reserved.

6. IP Office Certificates

Services between the system and applications may, depending on the settings of the service being used for the connection, require the exchange of security certificates. The system can either generate its own certificate or certificates provided from a trusted source can be loaded.

6.1 IP Office Identity Certificate for Telephony

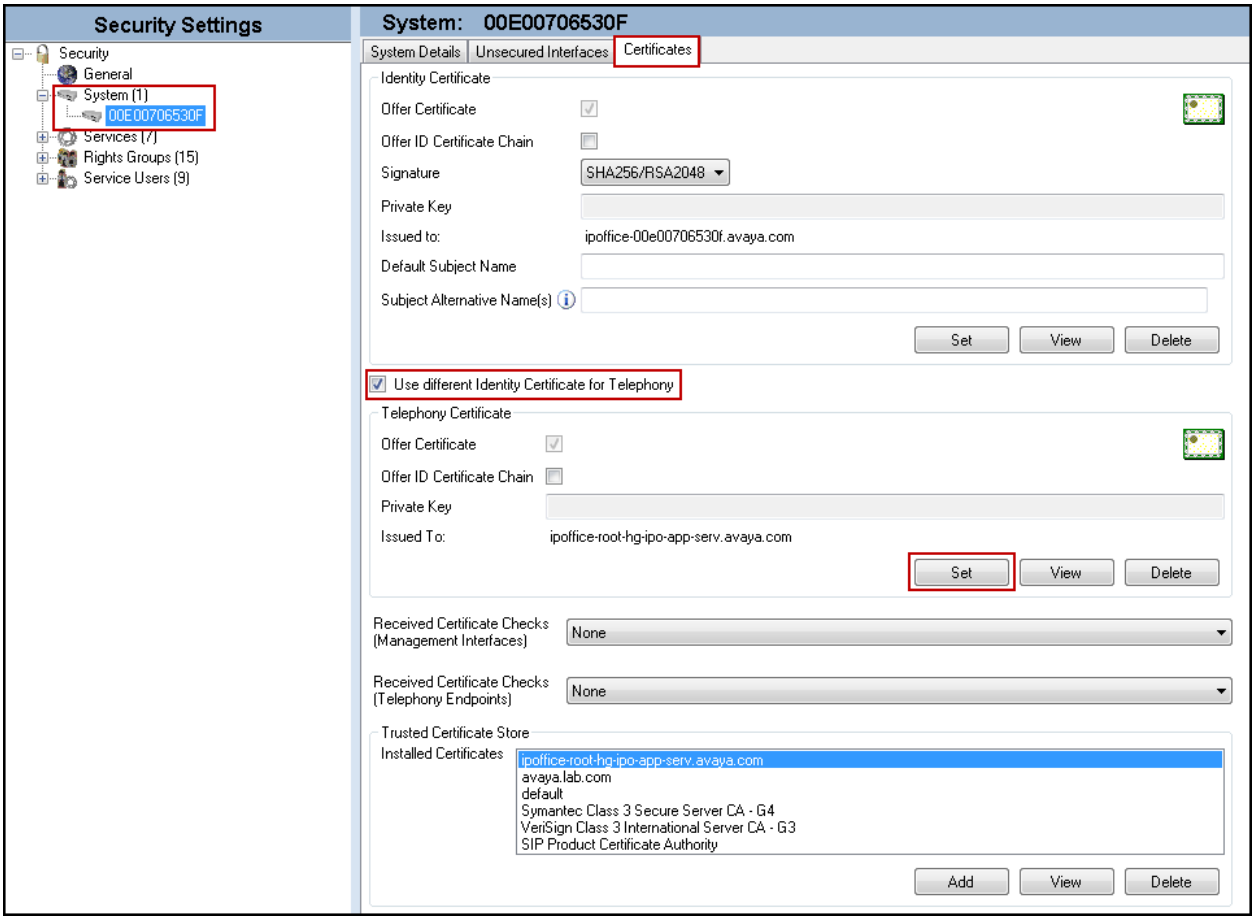
During the compliance test a separate identity certificate was used for telephony related secure communications, instead of the default identity certificate and setting created during the initial installation of IP Office.

It is assumed that the generation of certificates for IP Office has been previously completed, and is not discussed in this document. Refer to items [5, 6 and 7] in **Section 11**.

In the sample configuration, the MAC address **00E00706530F** was used as the system name.

To install a separate identity certificate for Telephony in IP Office, access the IP Office **Security Settings →System→00E00706530F→Certificates**:

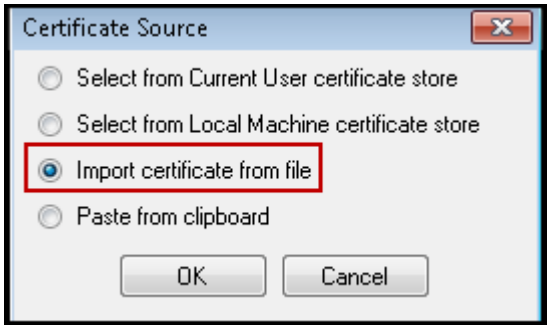
- Check **Use different Identity Certificate for Telephony**.
- Under **Use different Identity Certificate for Telephony**, click **Set**.



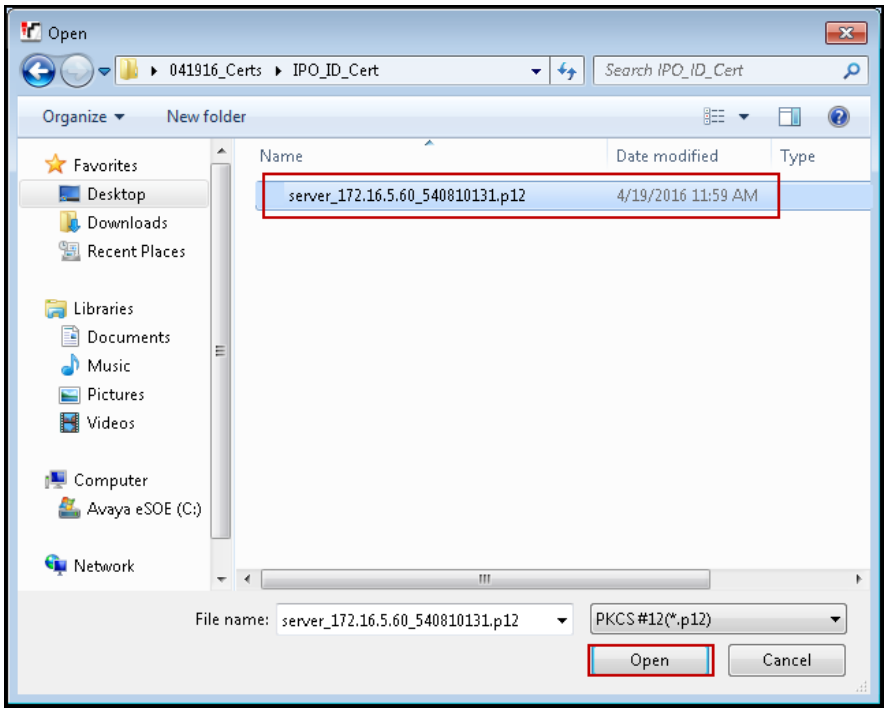
- Select the source where the certificate is located.

©2016 Avaya Inc. All Rights Reserved.

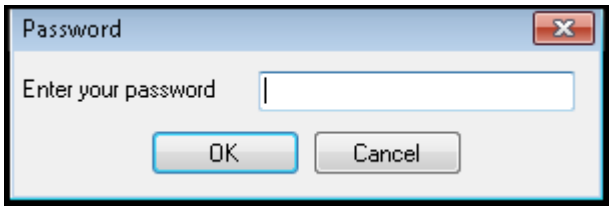
- **Import certificate from file** was selected.



- Navigate to the location where the certificate is located in the PC, select the certificate, and click **Open**.



- Enter the Password provided during the creation of the certificate, click **OK**.



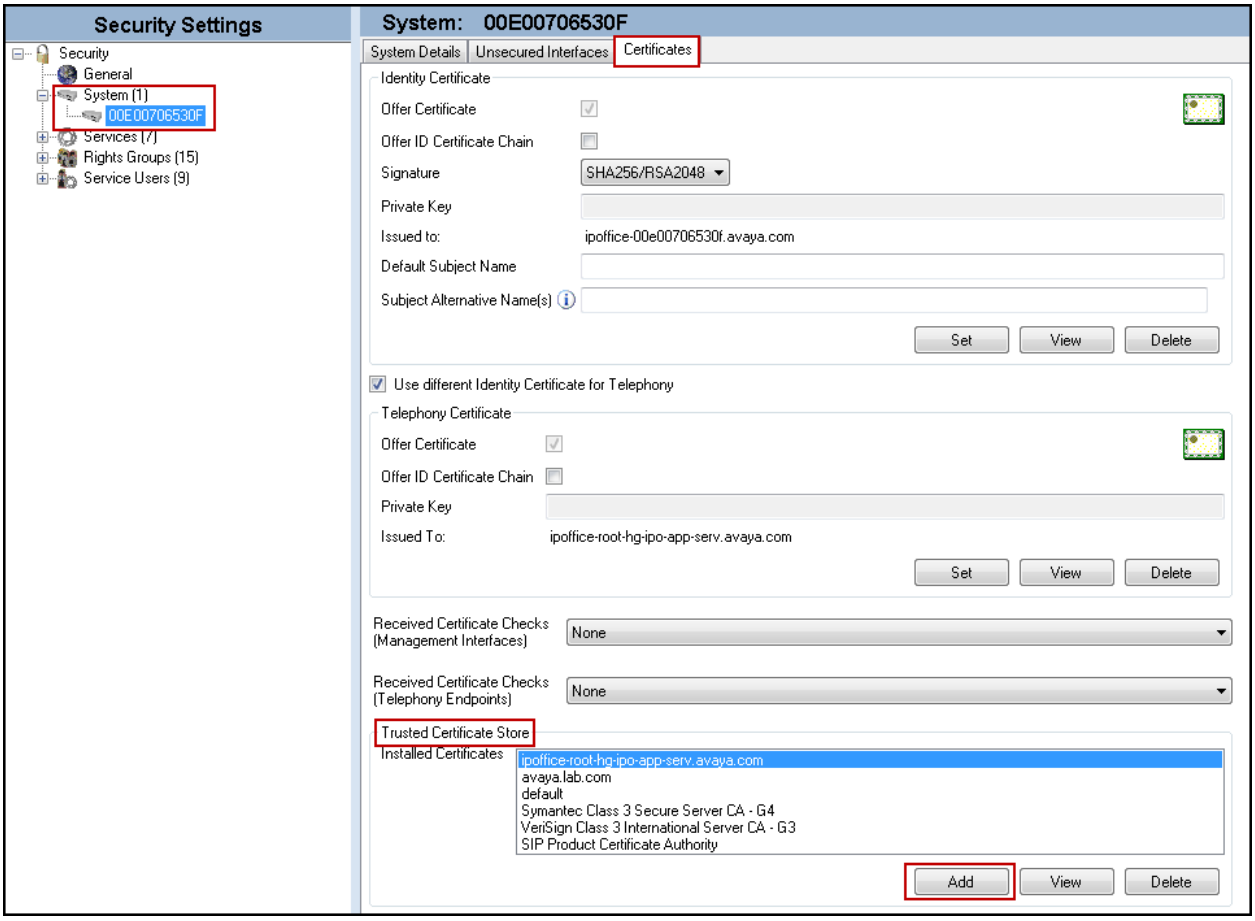
6.2 IP Office Trusted Certificate Store

The certificate store contains a set of trusted certificates used to evaluate received client certificates. Up to 25 X.509v3 certificates may be installed.

©2016 Avaya Inc. All Rights Reserved.

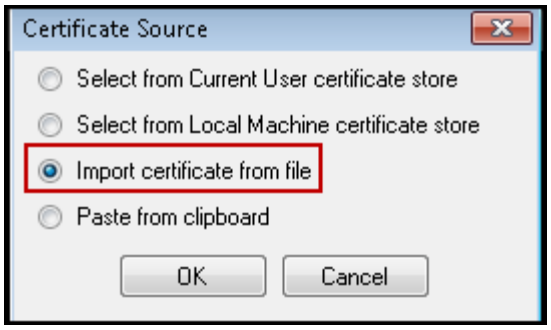
In addition to the identity certificate installed in **Section 6.1** above, a Root Certificate Authority (CA) certificate was installed in the IP Office trusted certificate store, as follows: Access IP Office **Security Settings →System→00E00706530F→Certificates**:

- Under **Trusted Certificate Store**, click **Add**.



- Select the source where the certificate is located.
- **Import certificate from file** was selected.

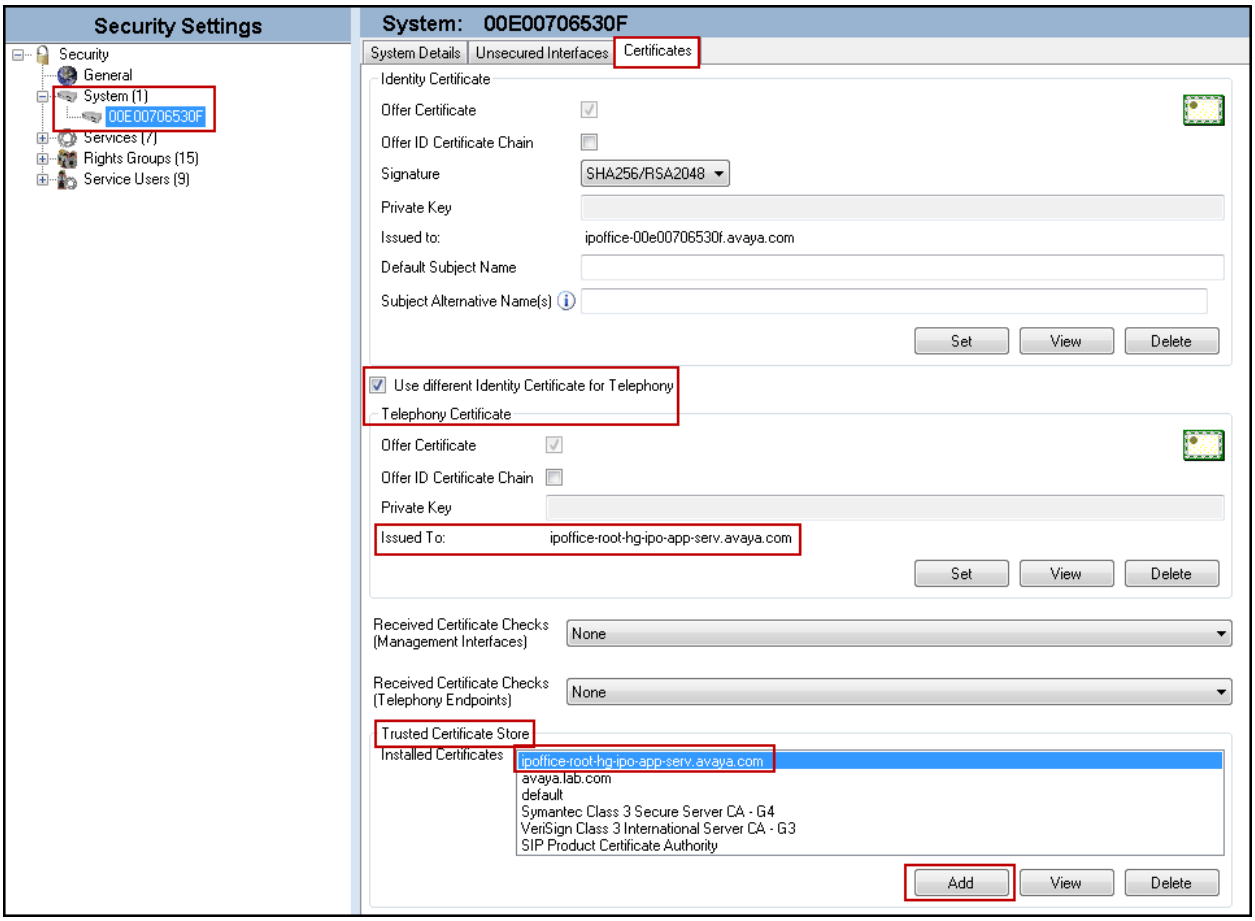
©2016 Avaya Inc. All Rights Reserved.



- Navigate to the location where the certificate is located in the PC, select the certificate, and click **Open**.

The following screen capture shows the identity certificate for Telephony and the Root CA certificate that were installed.

©2016 Avaya Inc. All Rights Reserved.

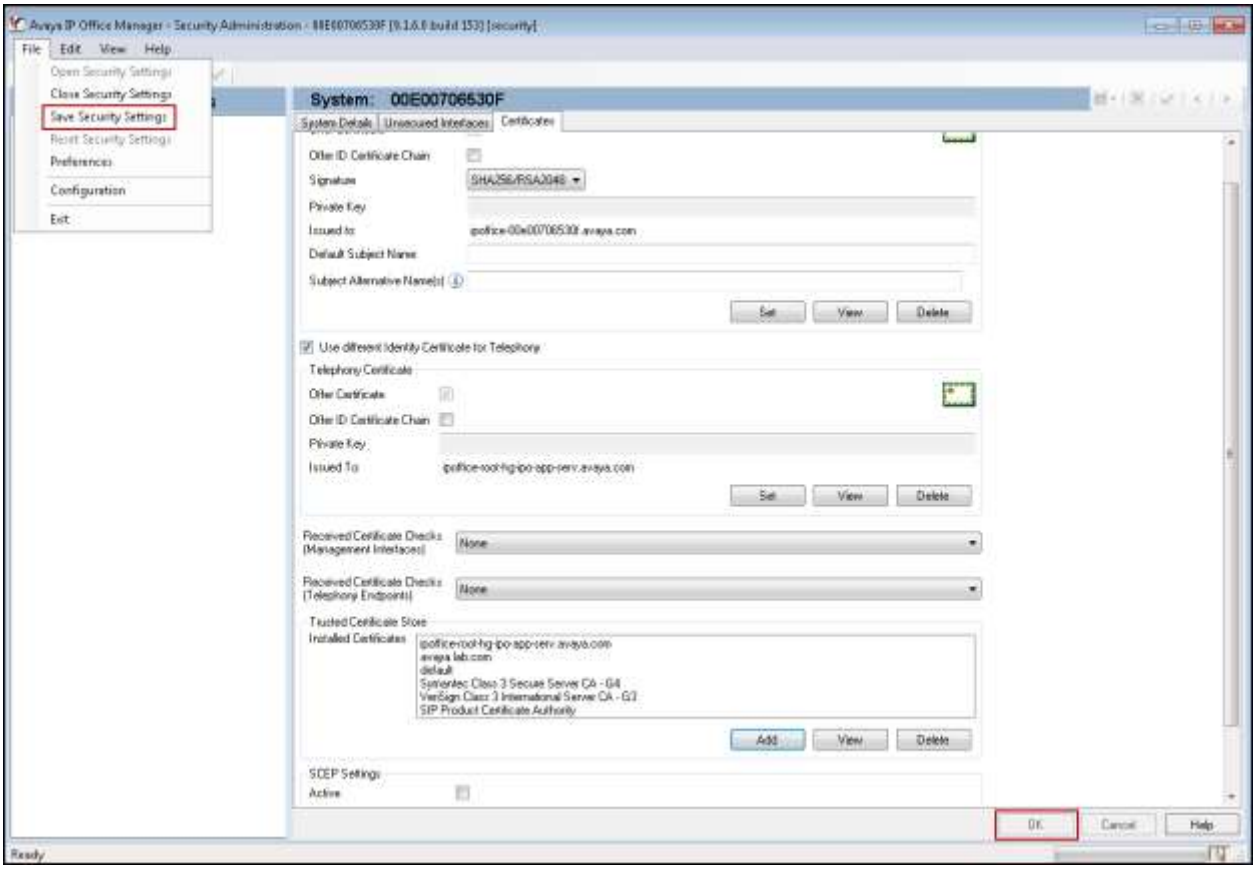


6.3 Save Security Settings

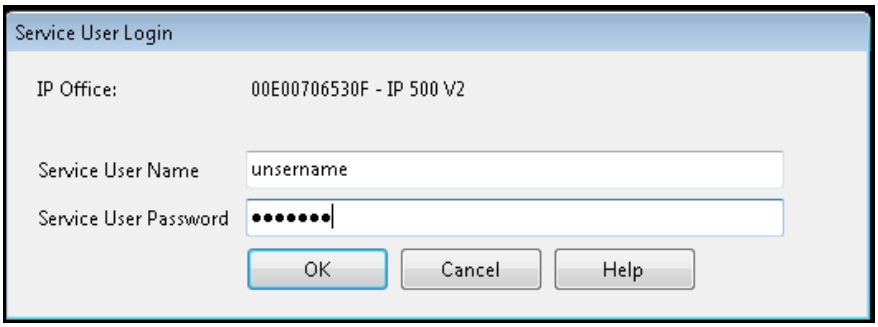
When desired, send the changes made to the security settings to the Avaya IP Office server in order for the changes to take effect, as follows:

©2016 Avaya Inc. All Rights Reserved.

- To commit the changes click **OK** at the bottom right of the screen.
- Next navigate to **File→Save Security Settings** in the menu bar at the top left of the screen to save the settings performed in the preceding sections.



Once the configuration is validated, a screen similar to the following will appear. Note that clicking OK may cause a service disruption due to system reboot. Click **OK** if desired.



©2016 Avaya Inc. All Rights Reserved.

7. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE)

This section describes the required configuration of the Avaya SBCE to connect to Clearcom SIP Trunking Service.

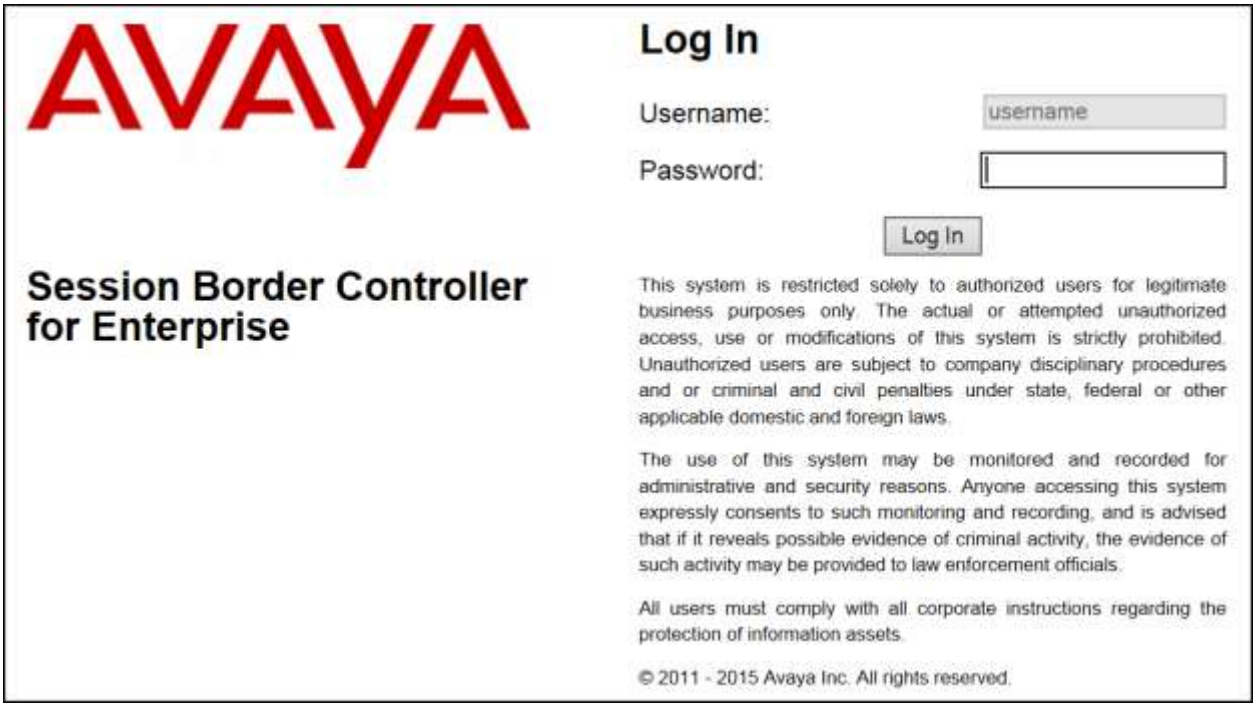
It is assumed that the Avaya SBCE was provisioned and is ready to be used. The configuration shown here is accomplished using the Avaya SBCE web interface.

Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

7.1 Log in Avaya SBCE

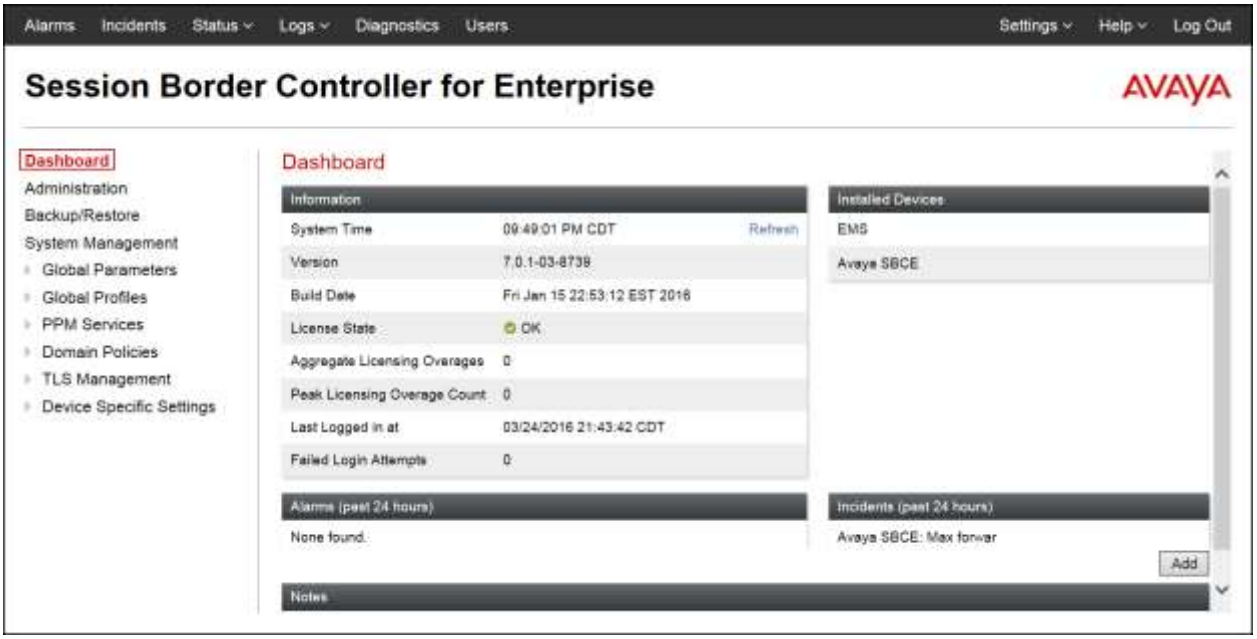
Use a Web browser to access the Avaya SBCE Web interface. Enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the Avaya SBCE management IP address.

Enter the appropriate credentials and click **Log In**.

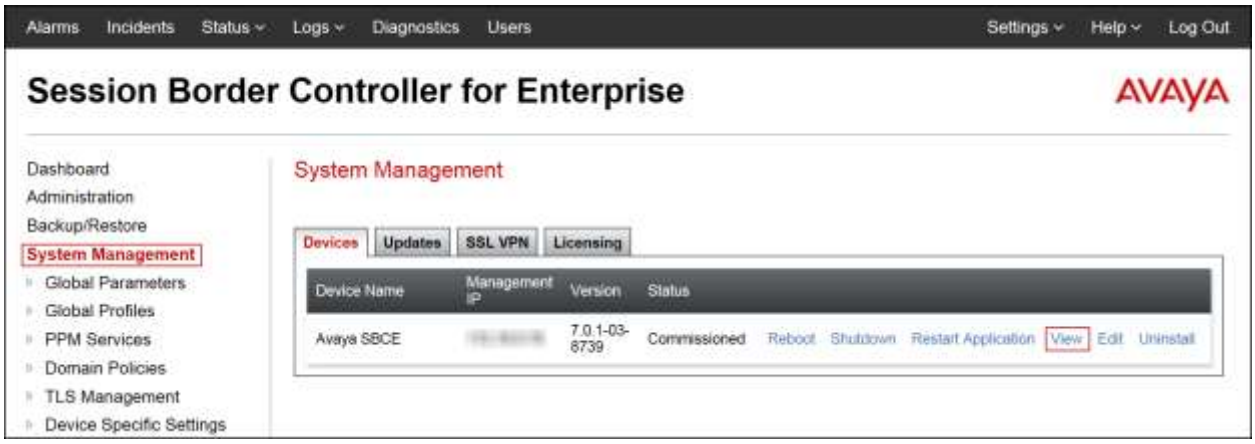


©2016 Avaya Inc. All Rights Reserved.

The **Dashboard** main page will appear as shown below.



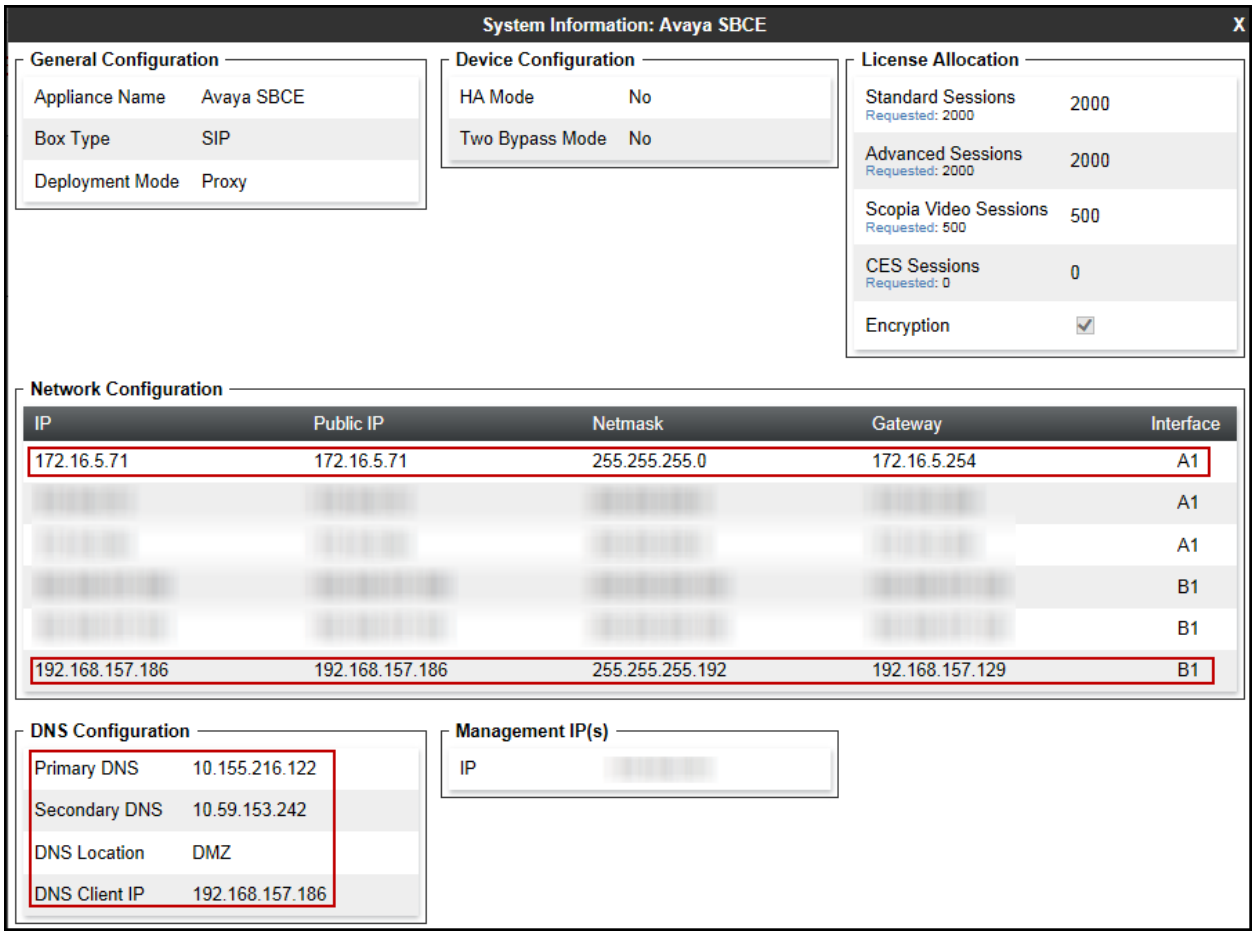
To view the system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Avaya SBCE** was already added. To view the configuration of this device, click on **View** as shown in the screenshot below.



©2016 Avaya Inc. All Rights Reserved.

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed as shown below.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**.



On the previous screen, note that **A1** corresponds to the inside interface (Private Network side) and **B1** corresponds to the outside interface (Public Network side) of the Avaya SBCE. (Use **Figure 1** as reference for IP addresses assignments). The configuration required for Remote Worker is beyond the scope of these Application Notes and is not discussed in these Application Notes, thus IP addresses used for Remote Worker assigned to interfaces **A1** and **B1** were blurred out. The management IP address was also blurred out for security reasons.

Note: Valid public DNS IP addresses are required with this solution.

IMPORTANT! – During the Avaya SBCE installation, the Management interface (labeled "M1") of the Avaya SBCE <u>must</u> be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).

©2016 Avaya Inc. All Rights Reserved.

7.2 TLS Management

7.2.1 TLS Certificates

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

This section describes the TLS profiles that were created for the Avaya SBCE, including the following:

- Create TLS client and server profiles to identify which certificates will be used in various TLS connections on the Avaya SBCE.

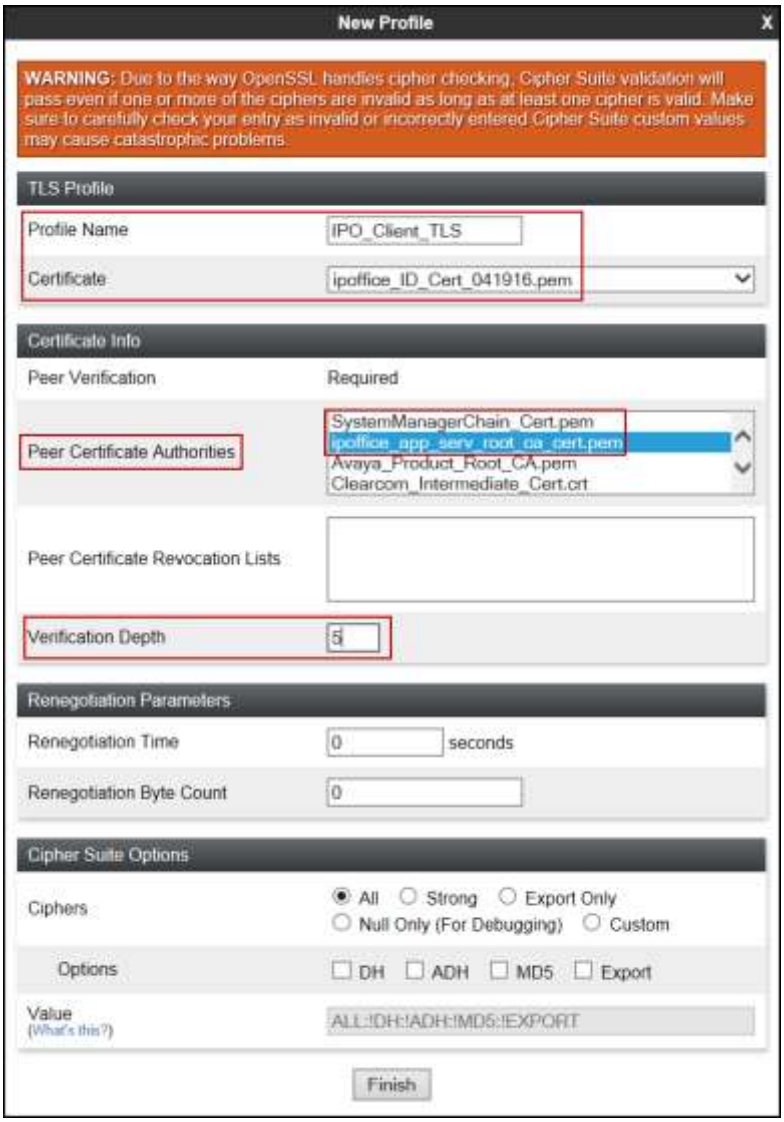
It is assumed that generation and installation of certificates on the Avaya SBCE, and the exchange of TLS Certificate Authority (CA) certificates with the Service Provider, have been previously completed, and is not discussed in this document. Refer to item [9] in **Section 11**.

7.2.2 TLS Client Profile – IP Office

To create a TLS client profile toward IP Office, navigate to **TLS Management → Client Profiles** and click **Add**. Configure the following parameters:

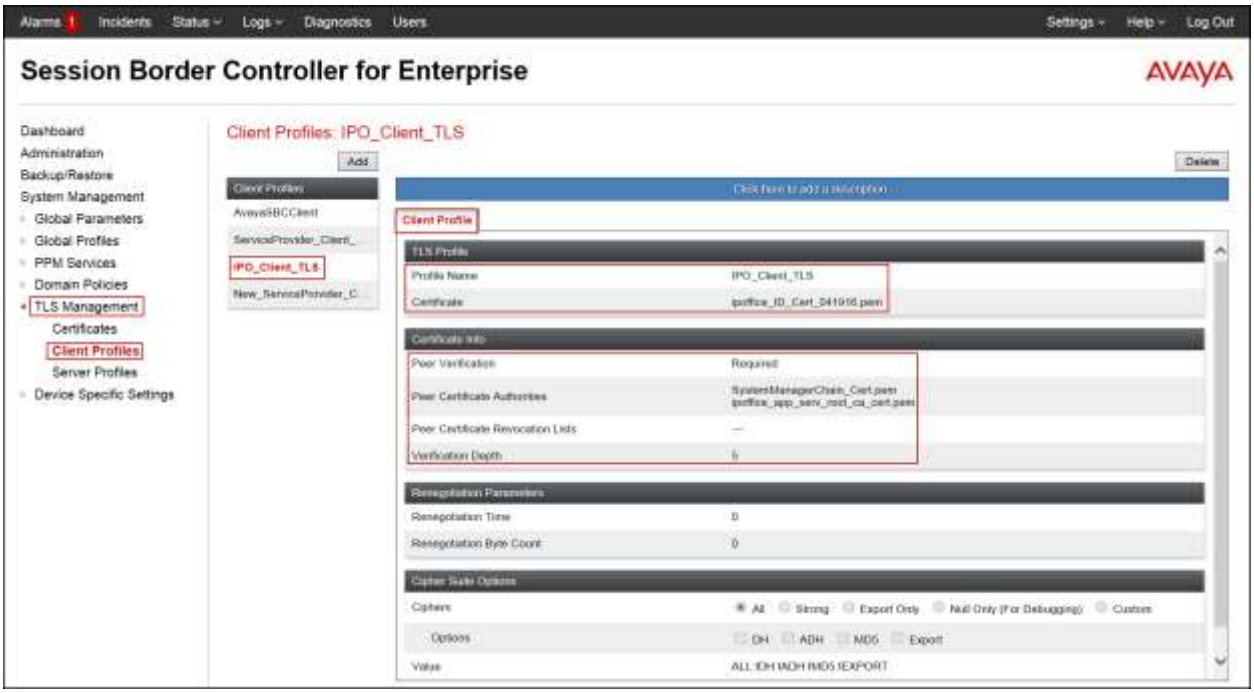
©2016 Avaya Inc. All Rights Reserved.

- Under TLS Profile enter the **profile name**; the name of **IPO_Client_TLS** was used in this example.
- Under TLS Profile select the **Certificate** to be used from the pull down menu; **ipoffice_ID_Cert_041916.pem** was selected in the sample configuration.
- Under Certificate Info, by using Crtl+Click, select the CA certificates to be used for the **Peer Certificate Authorities** field, **SystemManagerChain_Cert.pem** and **ipoffice_app_serv_root_ca_cert.pem** were selected in the sample configuration.
- Set the **Verification Depth** to **5**.
- Default values can be used for the remaining fields.
- Click **Finish**.



The following screen capture shows the newly created **IPO_Client_TLS** client Profile.

©2016 Avaya Inc. All Rights Reserved.



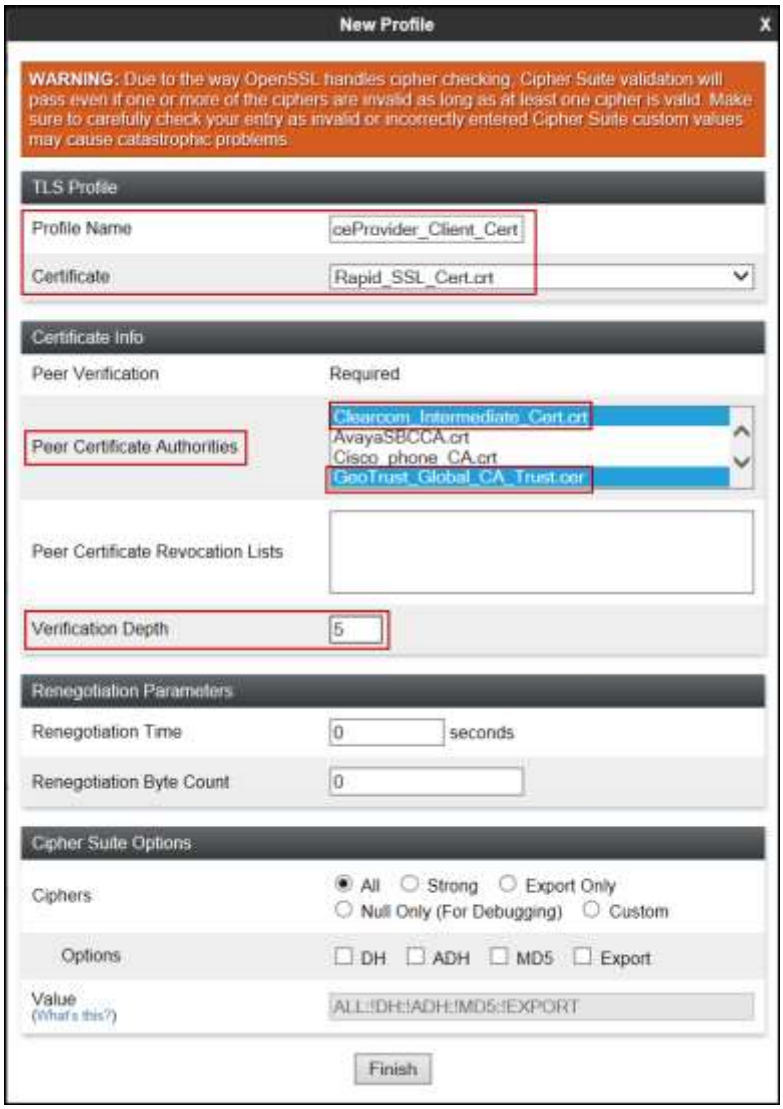
7.2.3 TLS Client Profile – Service Provider

To create a TLS client profile toward the Service Provider, navigate to **TLS Management → Client Profiles** and click **Add**. Configure the following parameters:

- Under TLS Profile enter the **profile name**; the name of **New_ServiceProvider_Client_Cert** was used in this example.

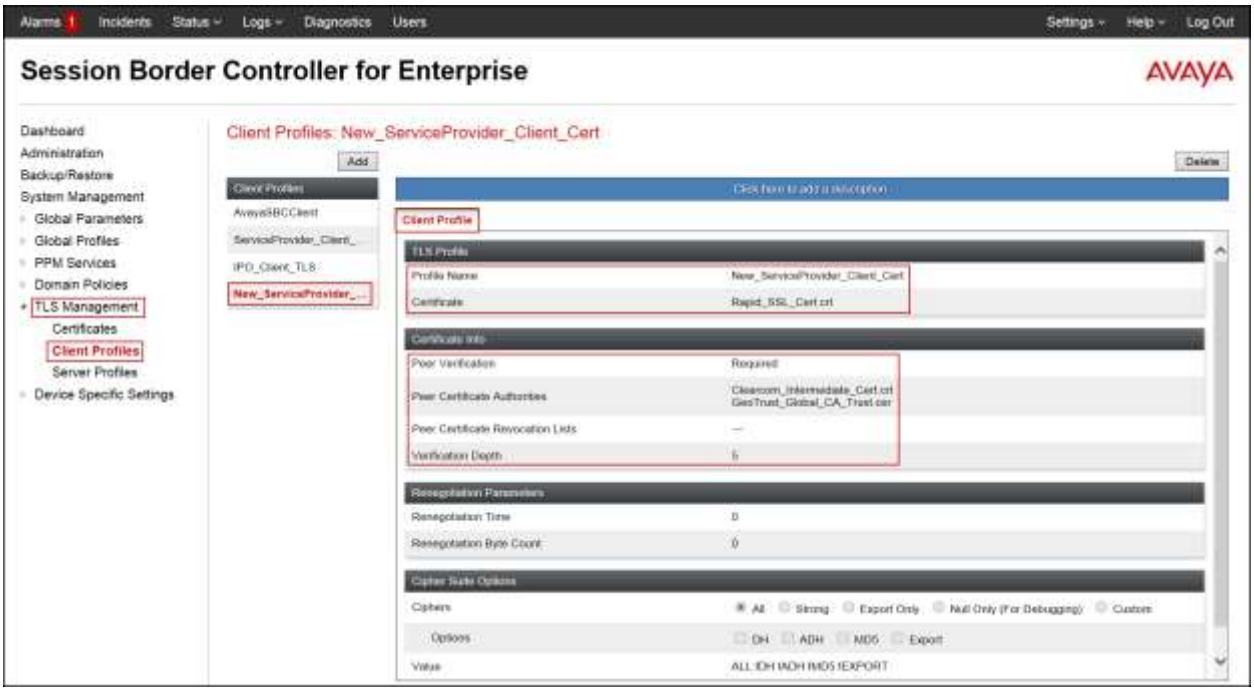
©2016 Avaya Inc. All Rights Reserved.

- Under TLS Profile select the **Certificate** to be used from the pull down menu; **Rapid_SSL_Cert.crt** was selected in the sample configuration.
- Under Certificate Info, by using Crtl+Click, select the CA certificates to be used for the **Peer Certificate Authorities** field, **Clearcom_Intermediate_Cert.crt** and **GeoTrust_Global_CA_Trust.cer** were selected in the sample configuration.
- Set the **Verification Depth** to **5**.
- Default values can be used for the remaining fields.
- Click **Finish**.



The following screen capture shows the newly created **New_ServiceProvider_Client_Cert** client Profile.

©2016 Avaya Inc. All Rights Reserved.



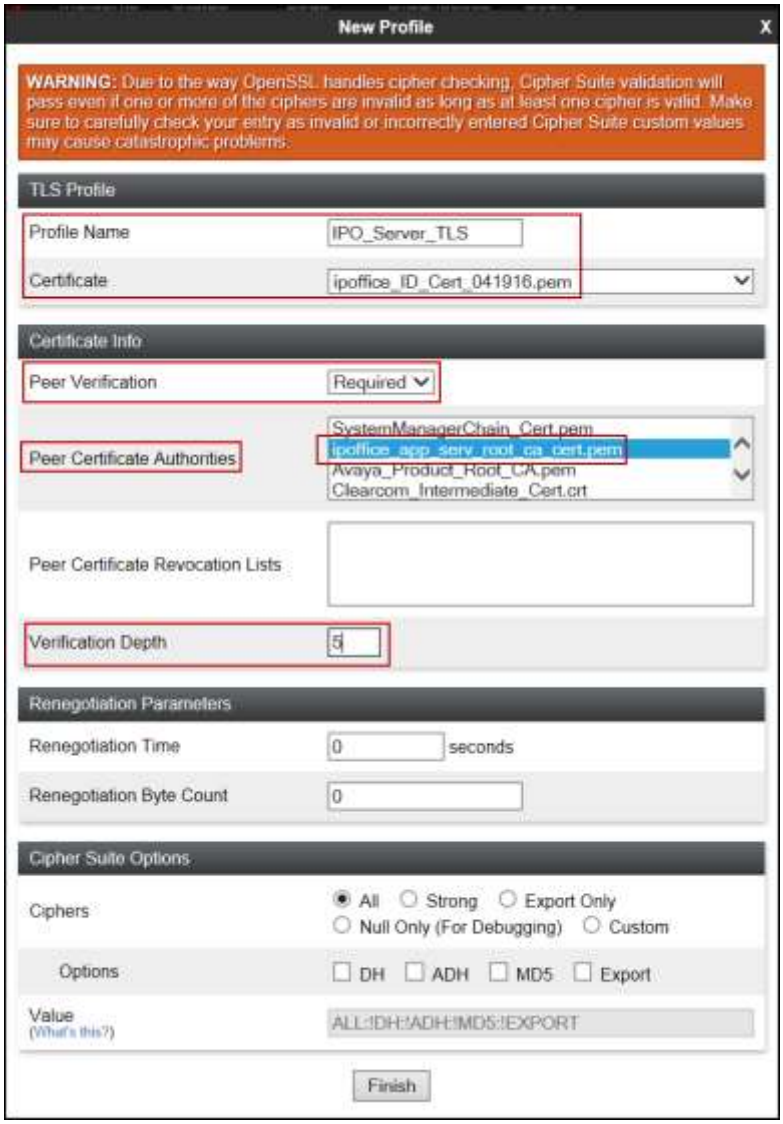
7.2.4 TLS Server Profile – IP Office

To create a TLS server profile toward the IP Office, navigate to **TLS Management → Server Profiles** and click **Add**. Configure the following parameters:

- Under TLS Profile enter the **profile name**; the name of **IPO_Server_TLS** was used in this example.

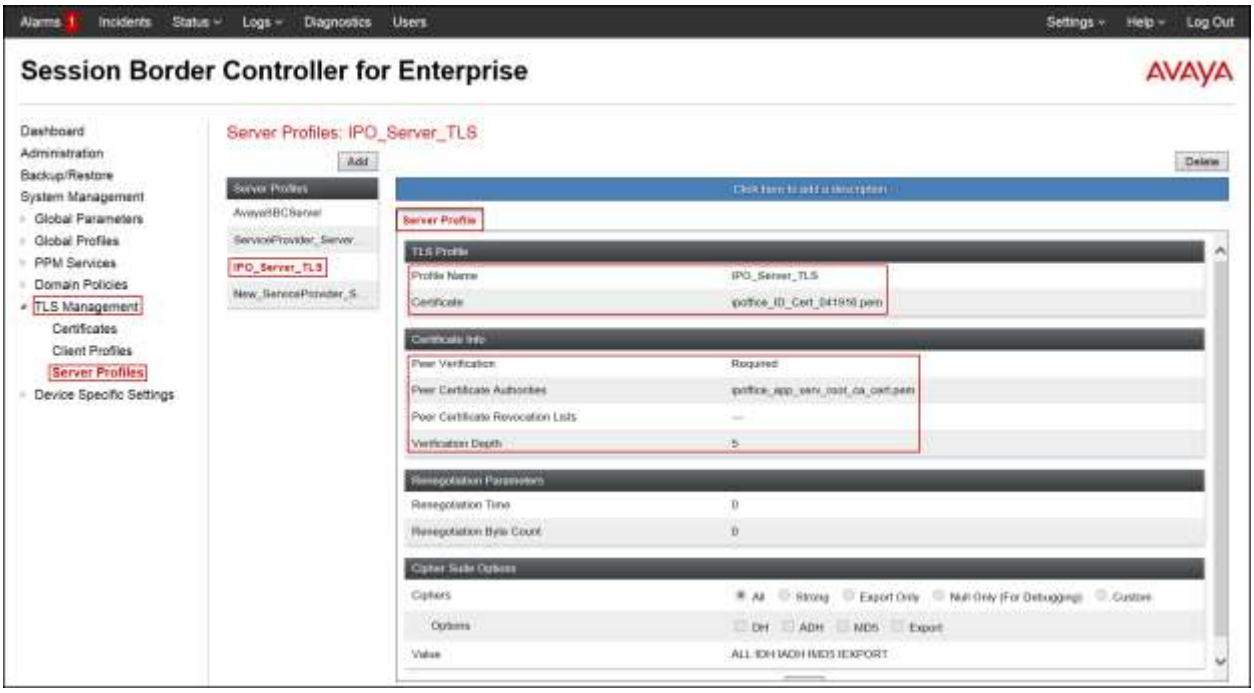
©2016 Avaya Inc. All Rights Reserved.

- Under TLS Profile select the **Certificate** to be used from the pull down menu; **ipoffice_ID_Cert_041916.pem** was selected in the sample configuration.
- Under Certificate Info, **Peer Verification**, select **Required** from the pull down menu.
- Under Certificate Info, by using Crtl+Click, select the CA certificates to be used for the **Peer Certificate Authorities** field, **ipoffice_app_serv_root_ca_cert.pem** was selected in the sample configuration.
- Set the **Verification Depth** to **5**.
- Default values can be used for the remaining fields.
- Click **Finish**.



The following screen capture shows the newly created **IPO_Server_TLS** server Profile.

©2016 Avaya Inc. All Rights Reserved.



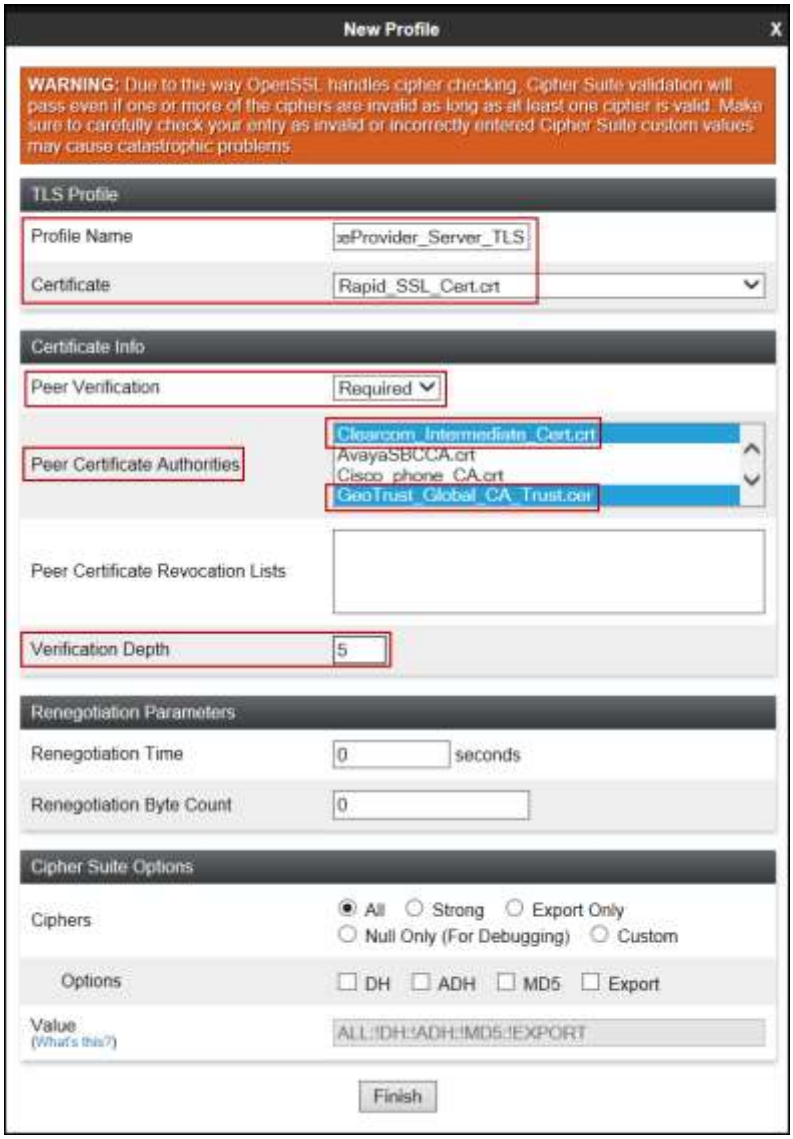
7.2.5 TLS Server Profile – Service Provider

To create a TLS server profile toward the Service Provider, navigate to **TLS Management → Server Profiles** and click **Add**. Configure the following parameters:

- Under TLS Profile enter the **profile name**; the name of **New_ServiceProvider_Server_TLS** was used in this example.

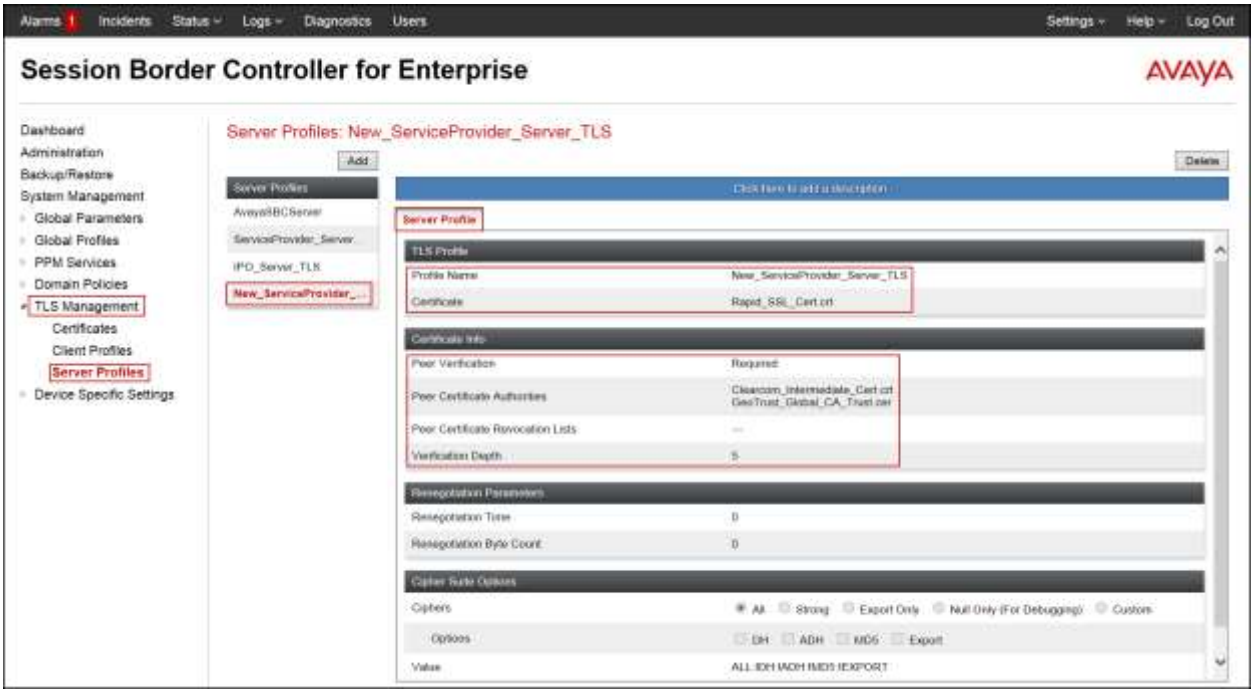
©2016 Avaya Inc. All Rights Reserved.

- Under TLS Profile select the **Certificate** to be used from the pull down menu; **Rapid_SSL_Cert.crt** was selected in the sample configuration.
- Under Certificate Info, **Peer Verification**, select **Required** from the pull down menu.
- Under Certificate Info, by using Crtl+Click, select the CA certificates to be used for the **Peer Certificate Authorities** field, **Clearcom_intermediate_Cert.crt** and **GeoTrust_Global_CA_Trust.cer** were selected in the sample configuration.
- Set the **Verification Depth** to **5**.
- Default values can be used for the remaining fields.
- Click **Finish**.



The following screen capture shows the newly created **New_ServiceProvider_Server_TLS** server Profile.

©2016 Avaya Inc. All Rights Reserved.



7.3 Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

©2016 Avaya Inc. All Rights Reserved.

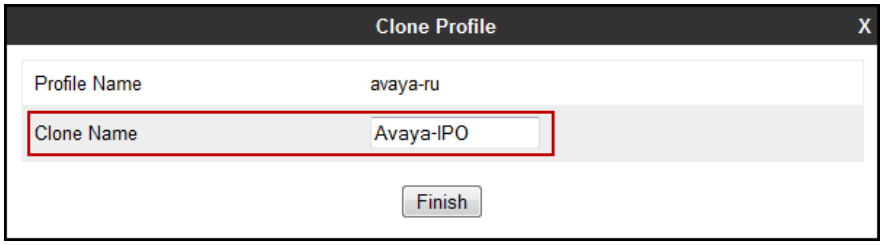
7.3.1 Server Interworking – Avaya-IPO

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or "cloned". Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or "cloned". If needed, the profile can then be modified to meet specific requirements for the enterprise SIP-enabled solution. For Clearcom, this profile was left with the **avaya-ru** default values.

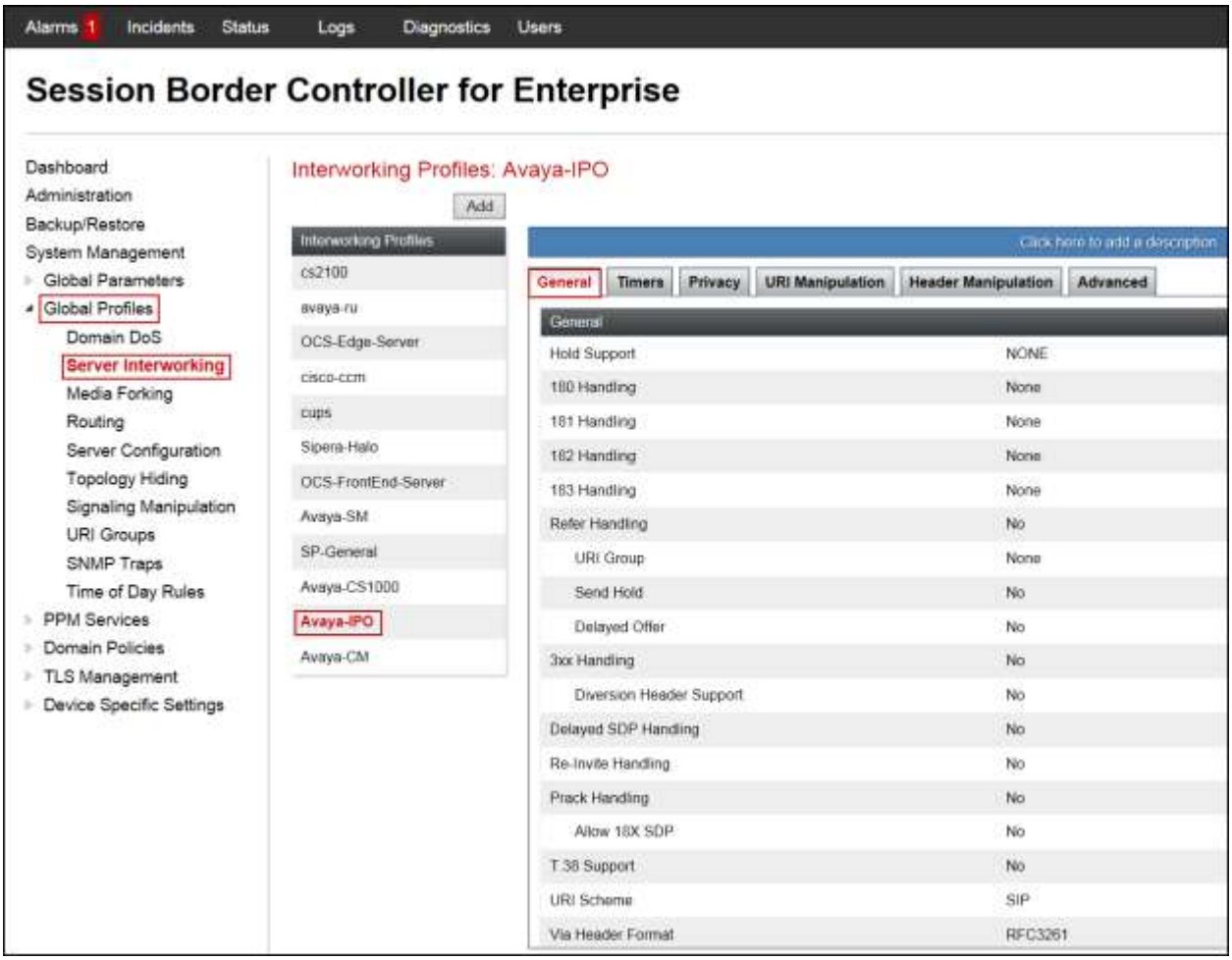
On the left navigation pane, select **Global Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **avaya-ru**. Click **Clone** on top right of the screen (not shown).

Enter the new profile name in the **Clone Name** field; the name of **Avaya-IPO** was chosen in this example. Click **Finish**.



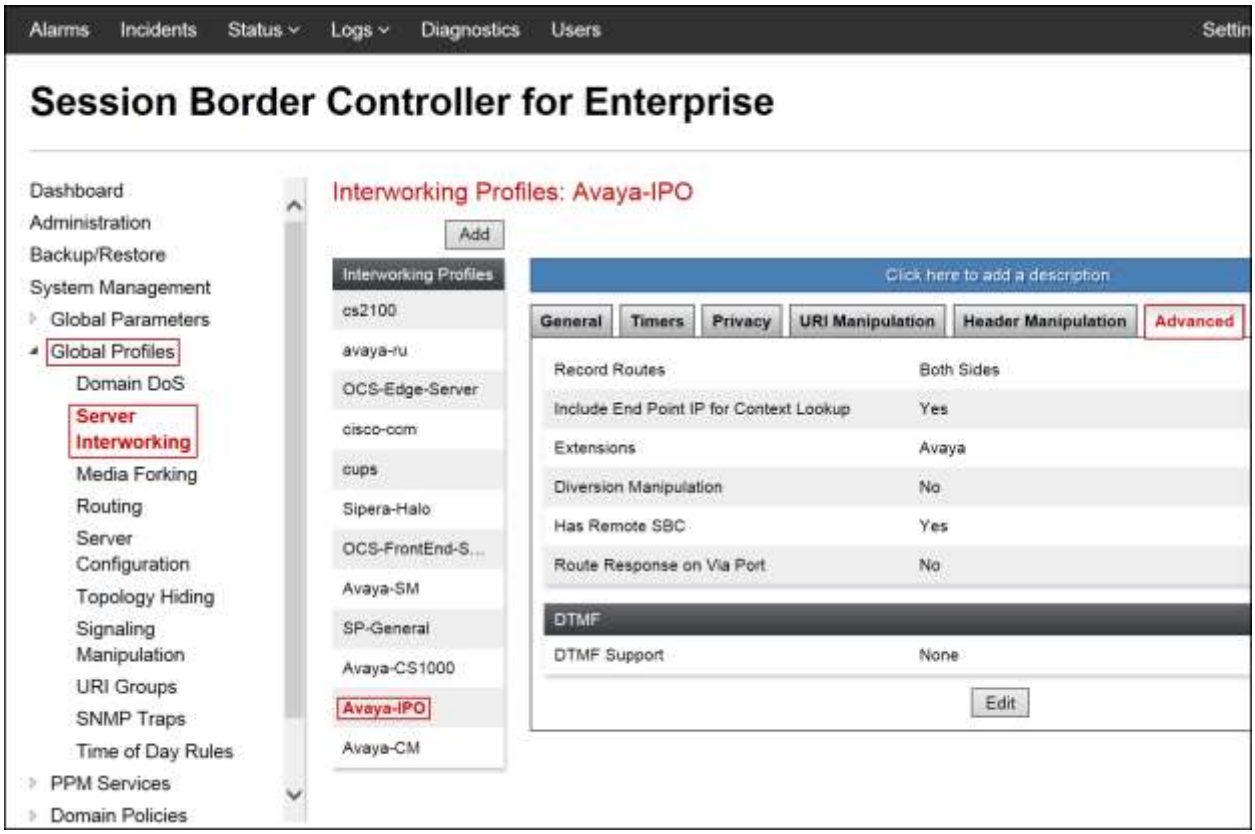
The following screen capture shows the **General** tab of the newly created **Avaya-IPO** Server Interworking Profile.

©2016 Avaya Inc. All Rights Reserved.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **Avaya-IPO** Server Interworking Profile.



©2016 Avaya Inc. All Rights Reserved.

7.3.2 Server Interworking - SP-General

A second Server Interworking profile named **SP-General** was created for the service provider.

On the left navigation pane, select **Global Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **Add** (not shown) (note that **Add** is being used to create the SP-General profile instead of cloning the avaya-ru profile).

Enter the new profile name; the name of **SP-General** was chosen in this example.

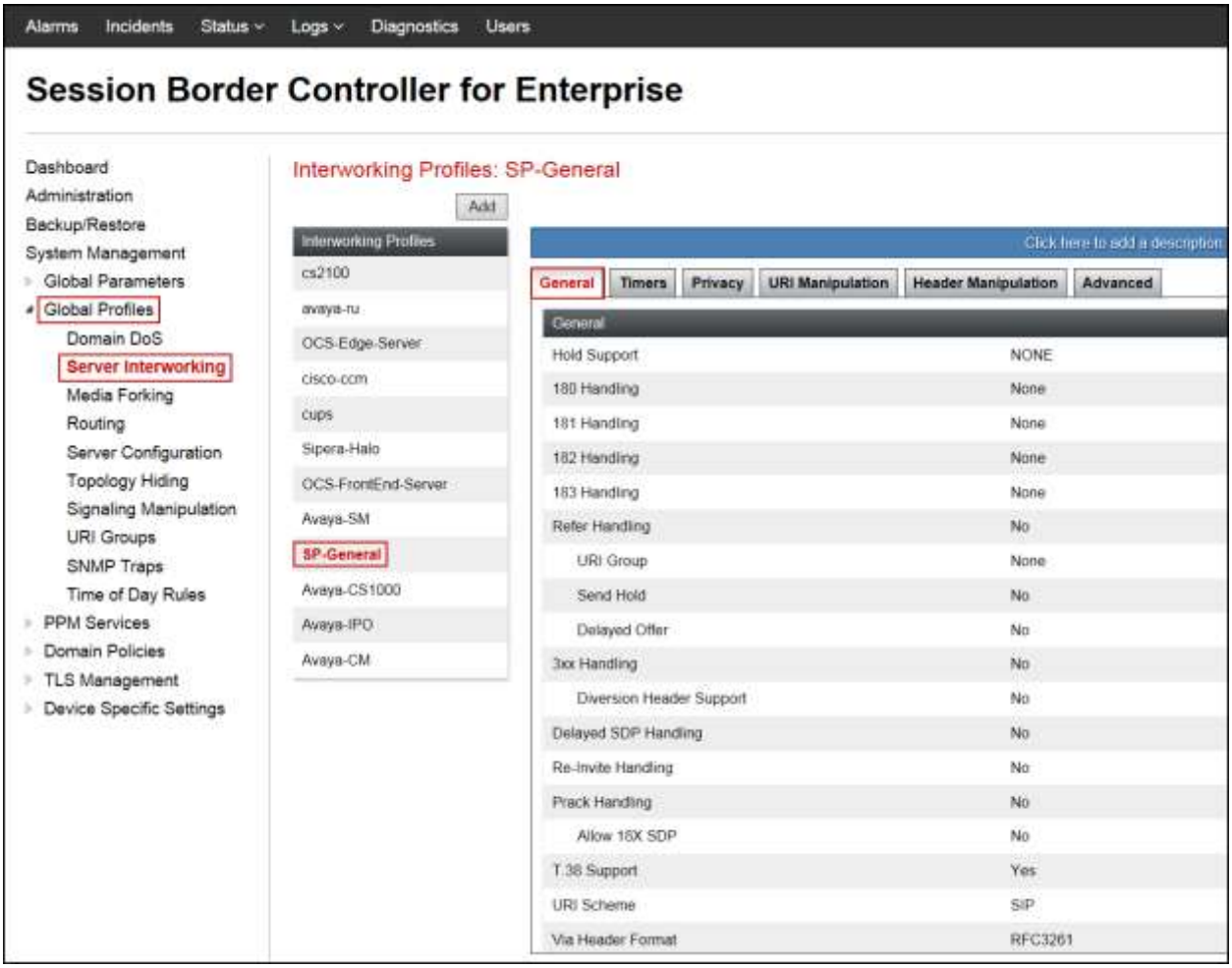
- Click **Next**.

- Click **Next**.

©2016 Avaya Inc. All Rights Reserved.

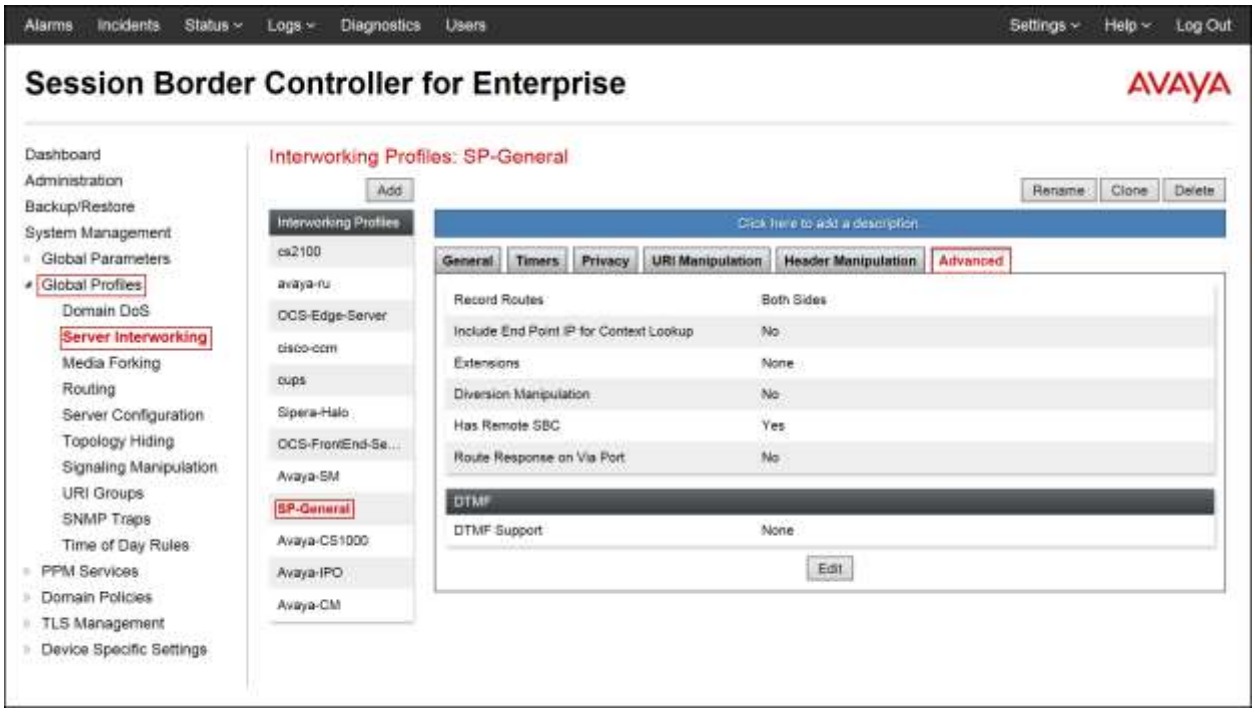
- Leaving other fields with their default values, click **Next** until the Advanced tab is reached, check **Both Sides** then click **Finish** on the Advanced tab.

The following screen capture shows the **General** tab of the newly created **SP-General** Server Interworking Profile.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the newly created **SP-General** Server Interworking Profile.



©2016 Avaya Inc. All Rights Reserved.

7.3.3 Server Configuration

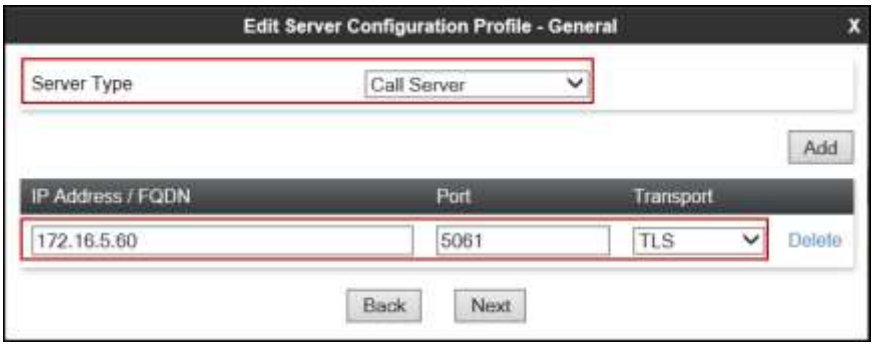
Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (IP Office) and the Trunk Server or SIP Proxy at the service provider's network.

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** (not shown). Click **Add Profile** (not shown) and enter the profile name: **IP Office**.

- Click **Next**.

On the **Edit Server Configuration Profile – General** window:

- **Server Type**: Select **Call Server**.
- **IP Address / FQDN**: **172.16.5.60** (IP Address of IP Office).
- **Port**: **5061** (This port must match the port number defined in **Section 5.4.4**).
- **Transports**: Select **TLS**.
- Click **Next**.

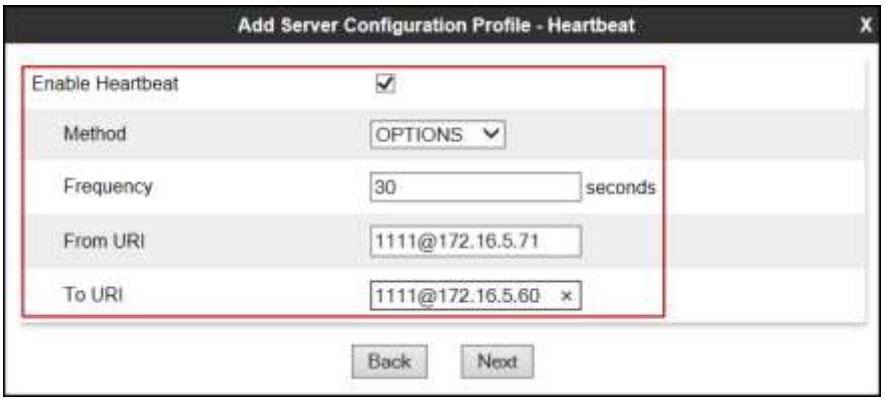


- Click **Next** on the **Authentication** window (not shown).

On the **Add Server Configuration Profile - Heartbeat** window:

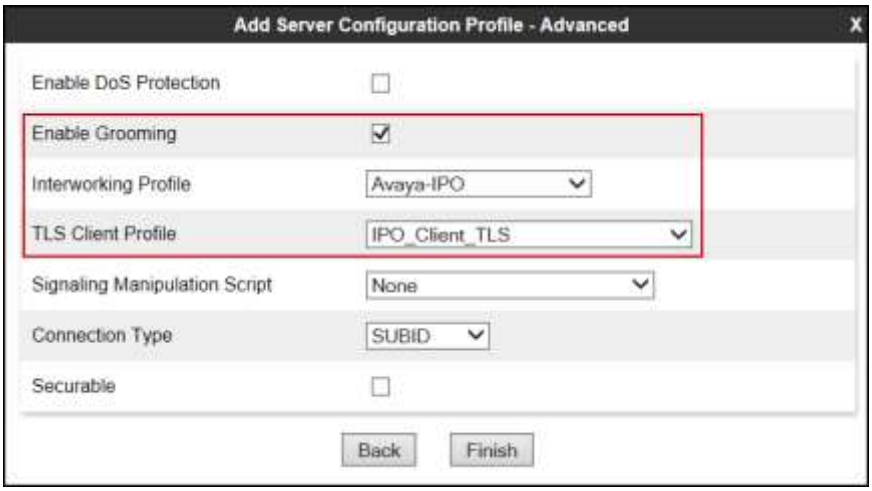
©2016 Avaya Inc. All Rights Reserved.

- Check **Enable Heartbeat**.
- Under **Method** select **OPTIONS** from the drop down menu.
- Under **Frequency** enter **30** (30 seconds was used during the compliance test; the time frequency can be increased).
- Under **From URI** enter **1111@172.16.5.71** (inside IP address of the Avaya SBCE).
- Under **To URI** enter **1111@172.16.5.60** (IP address of IP Office).
- Click Next.



On the **Add Server Configuration Profile - Advanced** window:

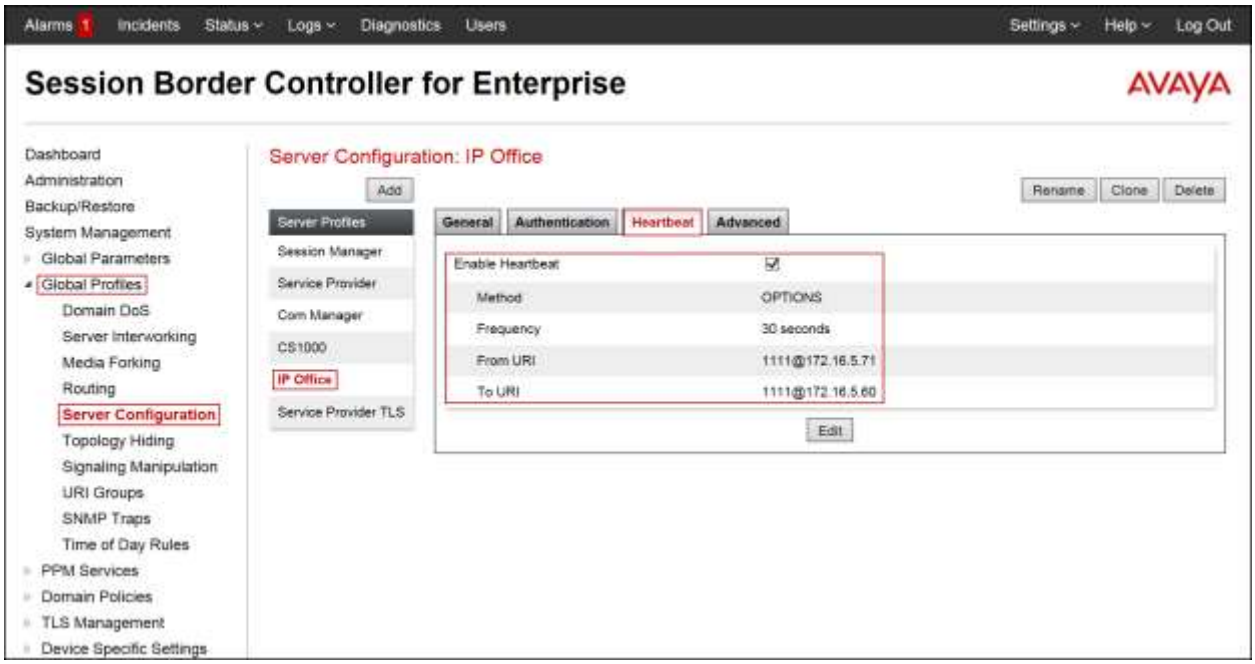
- Select **Avaya-IPO** from the **Interworking Profile** drop down menu.
- Select **IPO_Cleint_TLS** from the **TLS Client Profile** (**Section 7.2.2**).
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

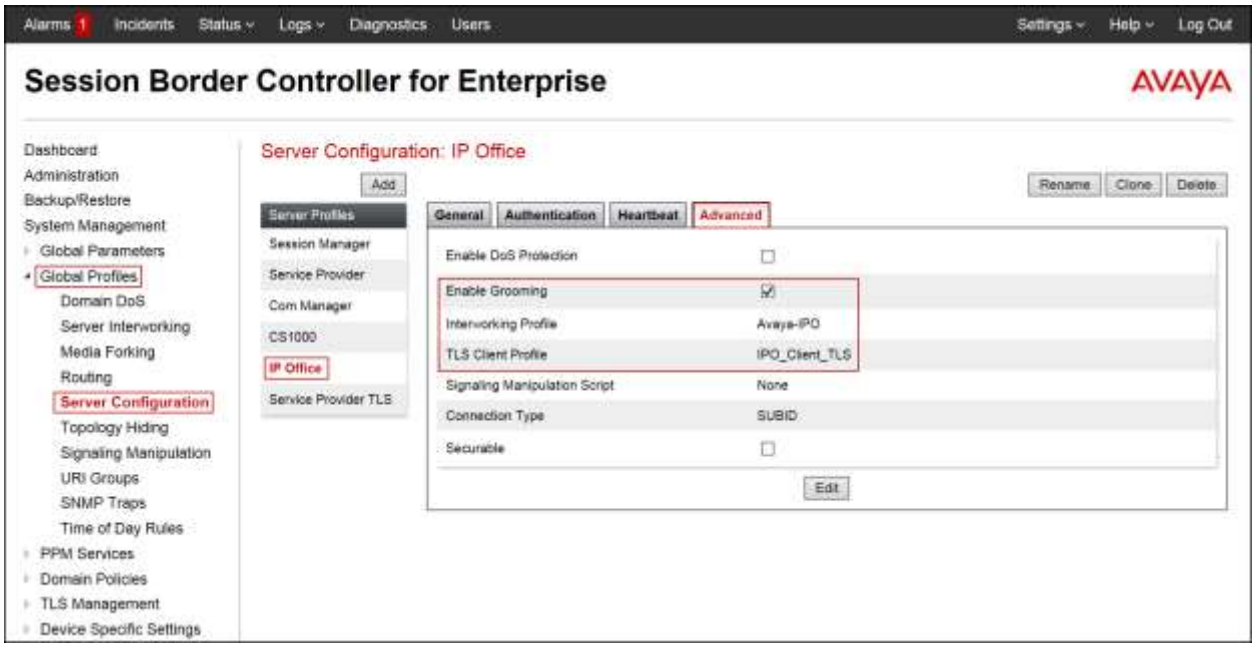
The following screen capture shows the **General** tab of the newly created **IP Office** Server Configuration Profile.

The following screen capture shows the **Heartbeat** tab of the newly created **IP Office** Server Configuration Profile.



©2016 Avaya Inc. All Rights Reserved.

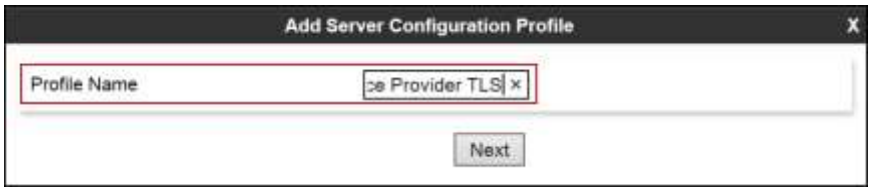
The following screen capture shows the **Advanced** tab of the newly created **IP Office** Server Configuration Profile.



©2016 Avaya Inc. All Rights Reserved.

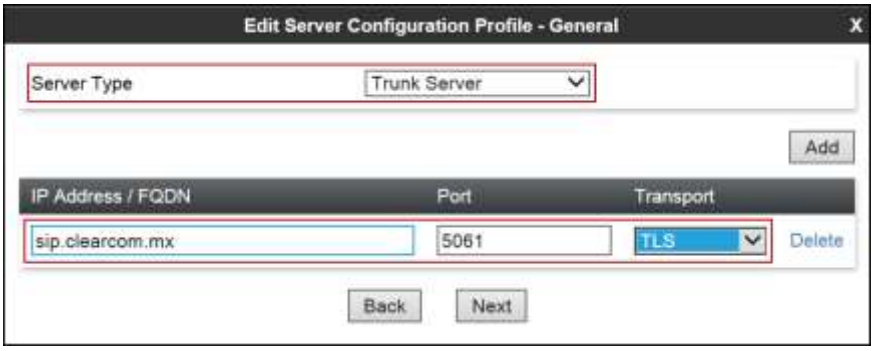
To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** (not shown) section and enter the profile name: **Service Provider TLS**.

- Click **Next**.



On the **Edit Server Configuration Profile – General** window:

- **Server Type**: Select **Trunk Server**.
- **IP Address / FQDN**: **sip.clearcom.mx** (Clearcom's SIP proxy server FQDN).
- **Port: 5061**.
- **Transports**: Select **TLS**.
- Click **Next**.



©2016 Avaya Inc. All Rights Reserved.

On the **Authentication** tab:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Enter the **Realm** credential provided by the service provider for SIP trunk registration. Note that the Service Provider's Domain Name was used.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

©2016 Avaya Inc. All Rights Reserved.

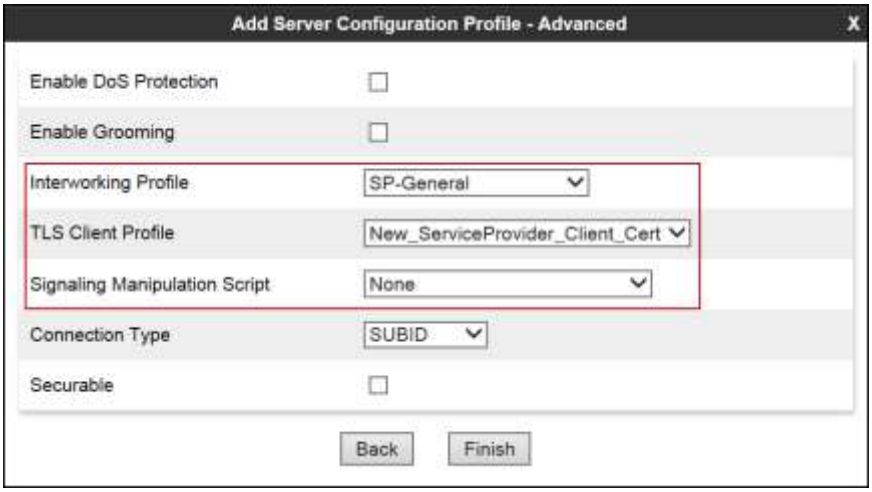
On the **Heartbeat** tab:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. **120** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
  - **From URI**: Use the **User Name** entered above in the **Authentication** screen (**User123**) and the Service Provider's domain name (**clearcom.mx**), as shown on the screen below.
  - **To URI**: Use the **User Name** entered above in the **Authentication** screen (**User123**) and the Service Provider Proxy Provider's domain name (**clearcom.mx**), as shown on the screen below.
  - Click **Next**.

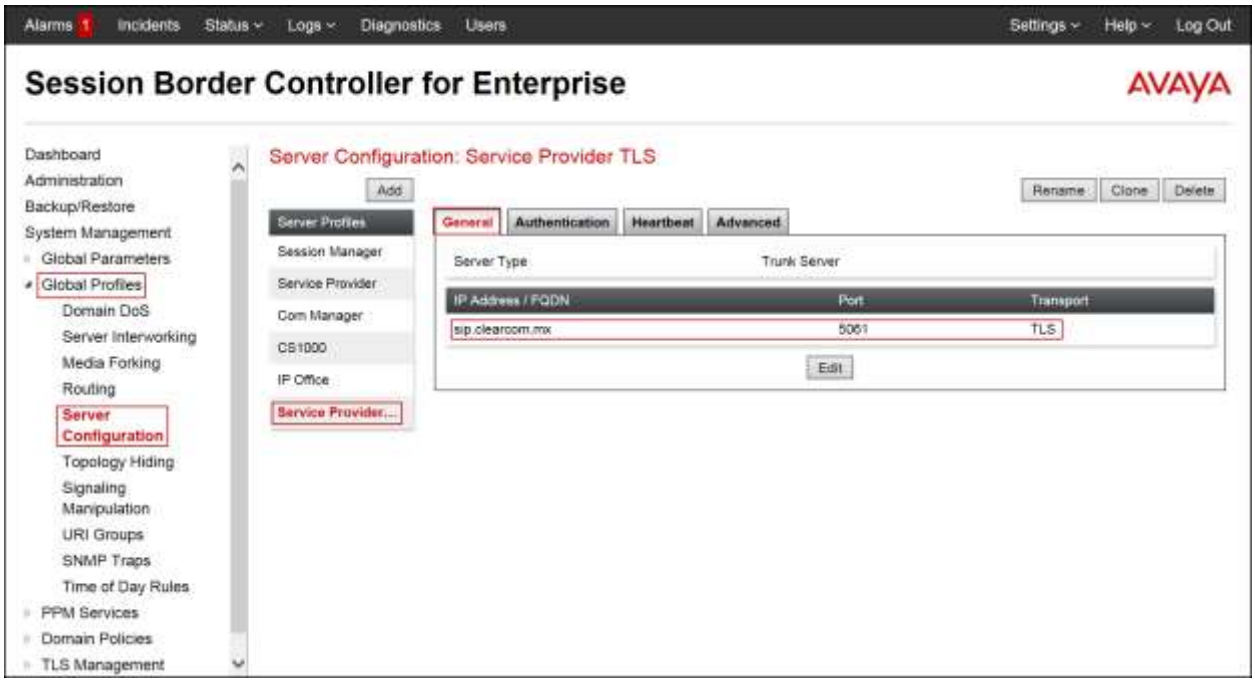
©2016 Avaya Inc. All Rights Reserved.

On the **Add Server Configuration Profile - Advanced** window:

- Select **SP-General** from the **Interworking Profile**.
- Select **New_ServiceProvider_Client_Cert** from the **TLS Client Profile** (**Section 7.2.3**).
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

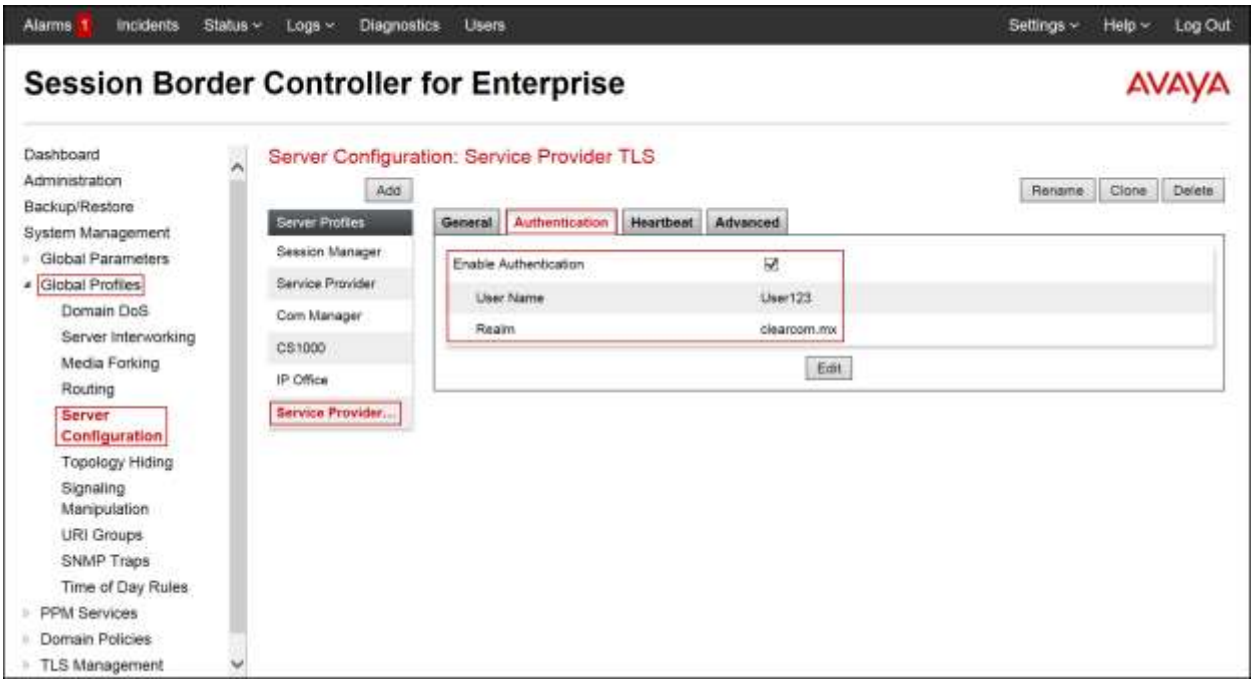


The following screen capture shows the **General** tab of the newly created **Service Provider TLS** Server Configuration Profile.

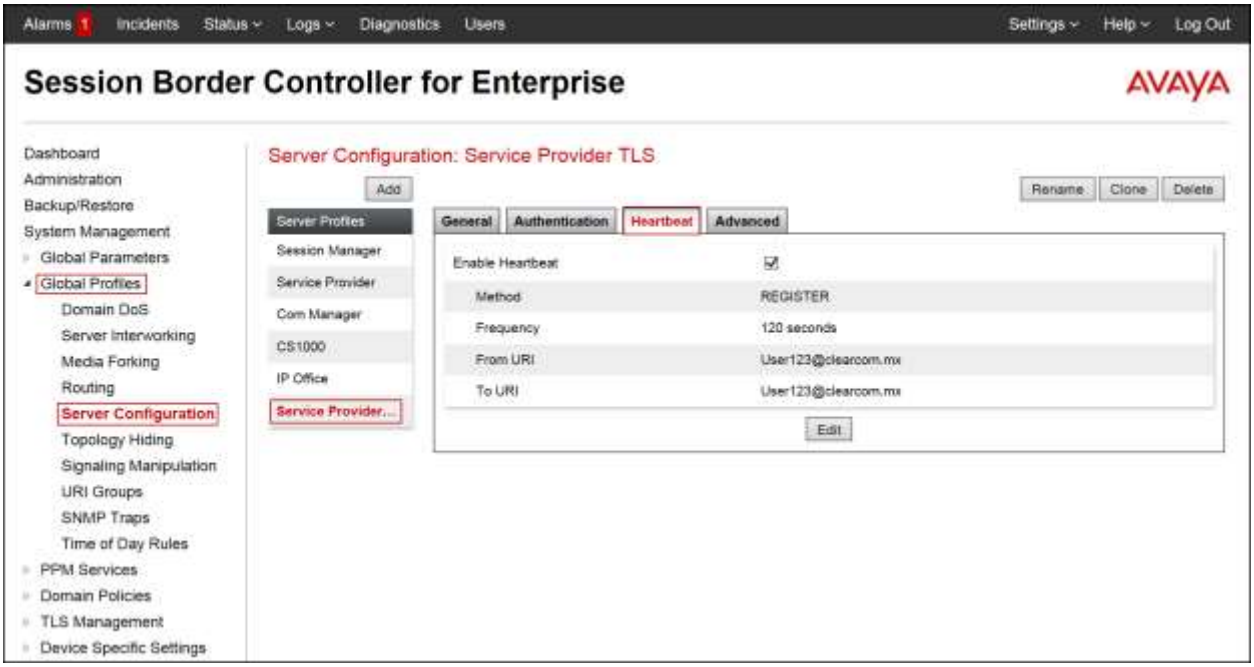


©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Authentication** tab of the newly created **Service Provider TLS** Server Configuration Profile.



The following screen capture shows the **Heartbeat** tab of the newly created **Service Provider TLS** Server Configuration Profile.



The following screen capture shows the **Advanced** tab of the newly created **Service Provider TLS** Server Configuration Profile.

©2016 Avaya Inc. All Rights Reserved.

©2016 Avaya Inc. All Rights Reserved.

7.3.4 Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

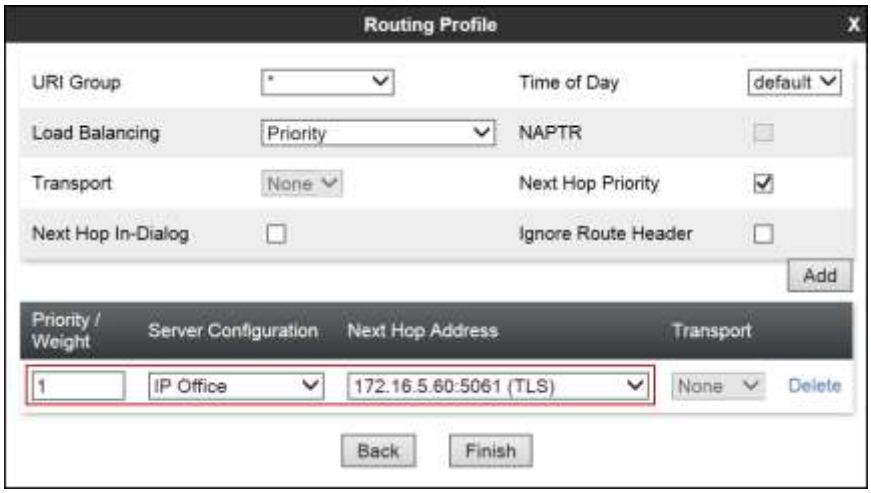
Two Routing profiles were created; one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are sent to Clearcom.

To create the inbound route, from the **Global Profiles** menu on the left-hand side (not shown):

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route_to_IPO_TLS**.
- Click **Next**.

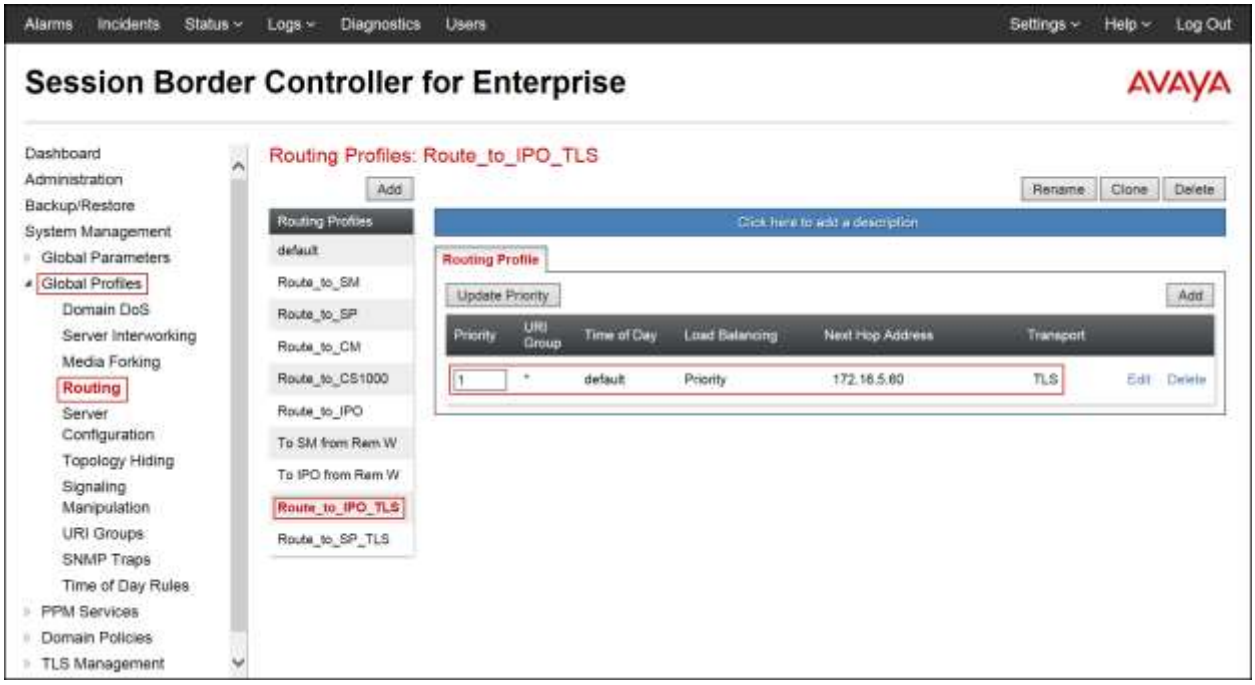
On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: **1**
- **Server Configuration**: Select **IP Office**.
- The **Next Hop Address** is populated automatically with **172.16.5.60:5061 (TLS)** (IP Office IP address, Port and Transport).
- Click **Finish**.



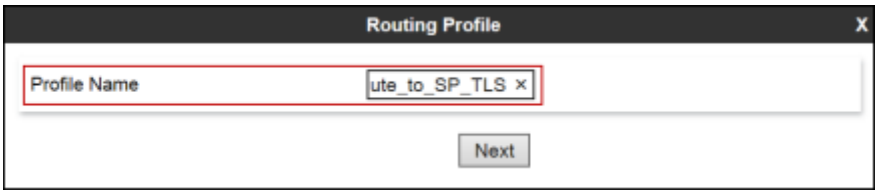
©2016 Avaya Inc. All Rights Reserved.

The following screen shows the newly created **Route_to_IPO_TLS** Routing Profile.



Similarly, for the outbound route:

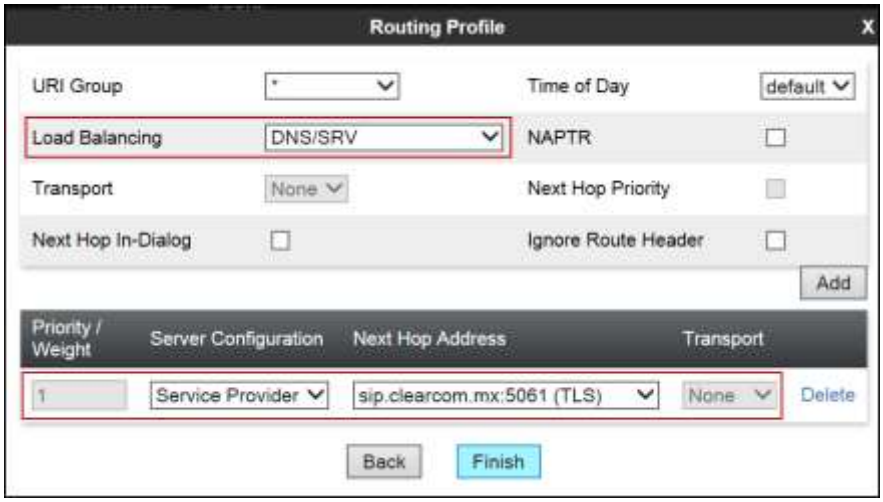
- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route_to_SP_TLS**.
- Click **Next**.



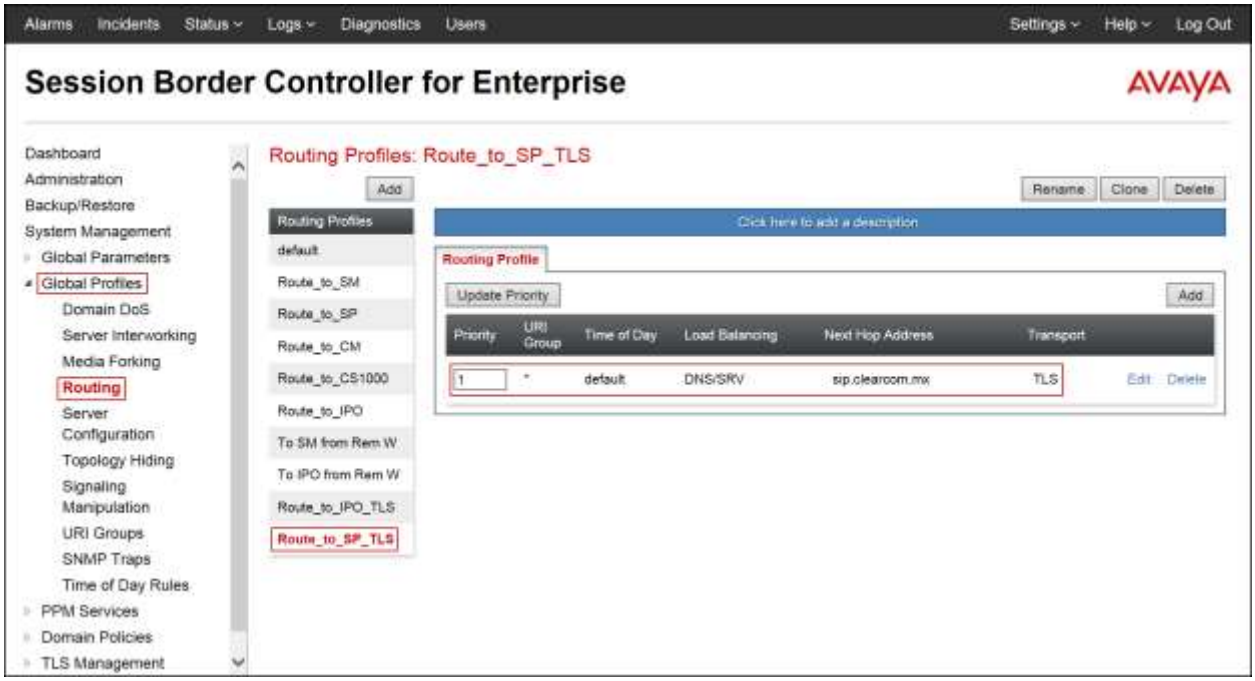
On the Routing Profile screen complete the following:

©2016 Avaya Inc. All Rights Reserved.

- Click on the **Add** button to add a **Next-Hop Address**.
- **Load Balancing**: Select **DNS/SRV**.
- **Priority / Weight**: **1**
- **Server Configuration**: Select **Service Provider TLS**.
- The **Next Hop Address** is populated automatically with **sip.clearcom.mx:5061 (TLS)** **(**Clearcom's SIP Proxy FQDN, port and transport).
- Click **Finish**.



The following screen capture shows the newly created **Route_to_SP_TLS** Routing Profile.



©2016 Avaya Inc. All Rights Reserved.

7.3.5 Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

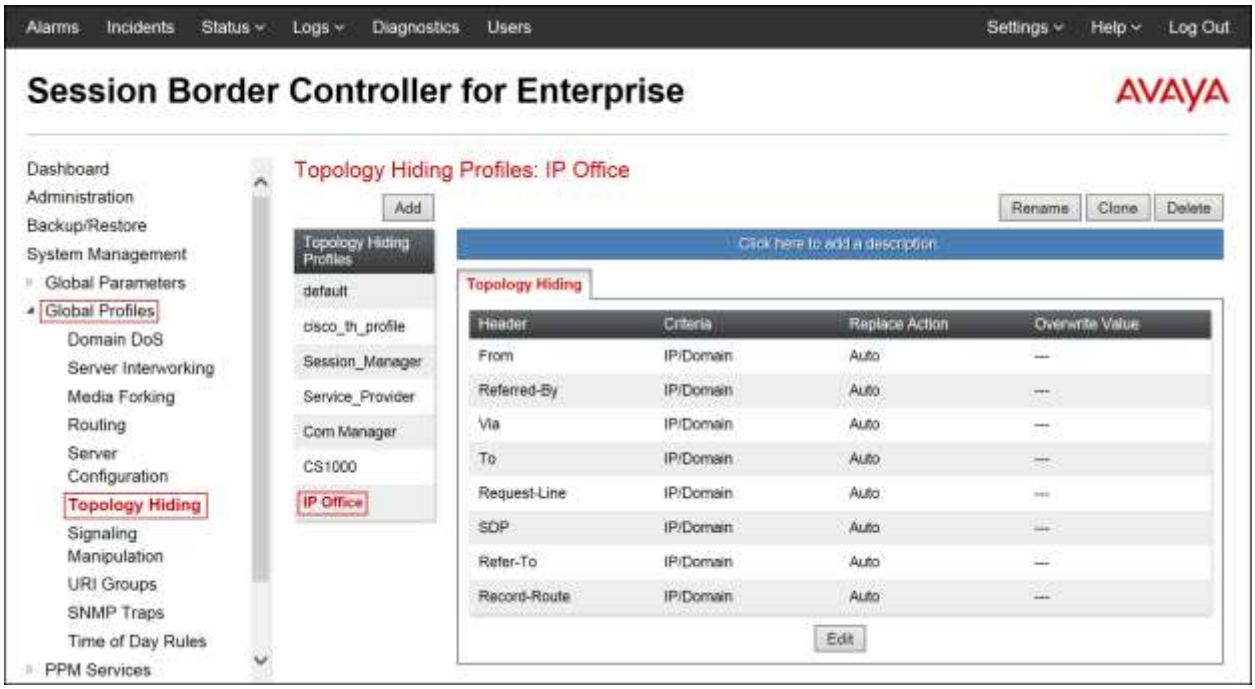
Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by IP Office and the SIP trunk service provider, allowing the call to be accepted in each case.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Clone Name**: **IP Office**.
- Click **Finish**.

©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly added **IP Office** Topology Hiding Profile. Note that for IP Office no values were overwritten (left with default values).

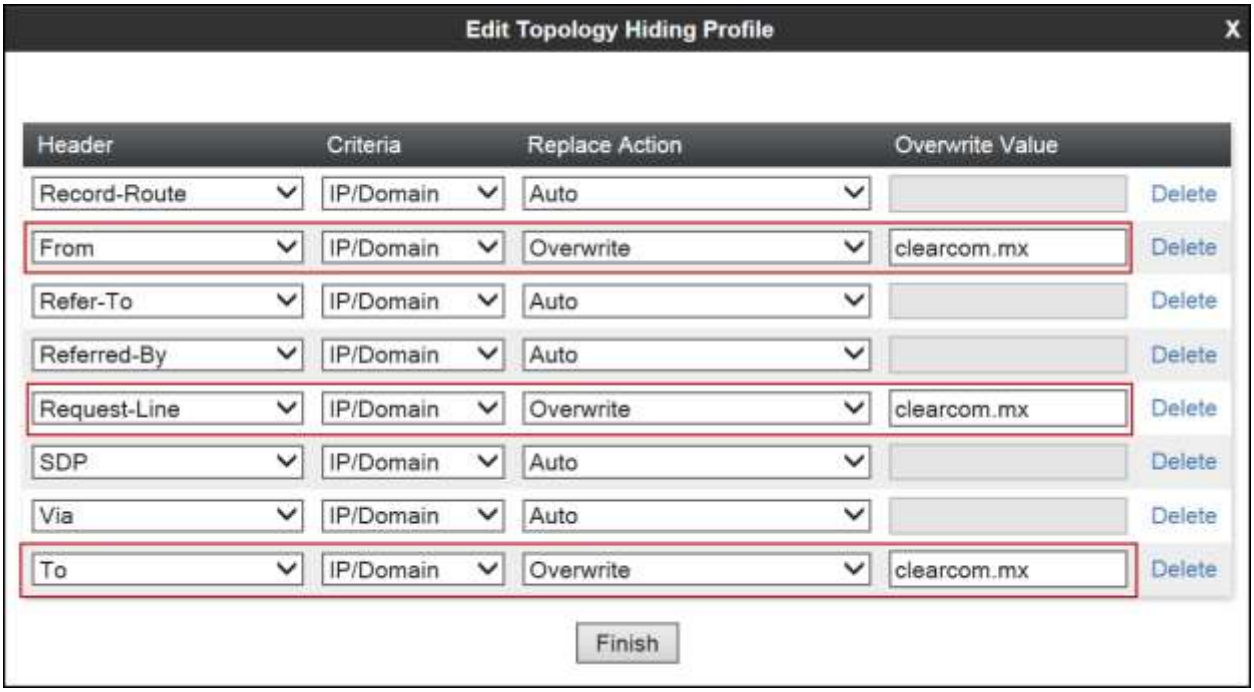


To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Clone Name**: **Service_Provider**.
- Click **Finish**.

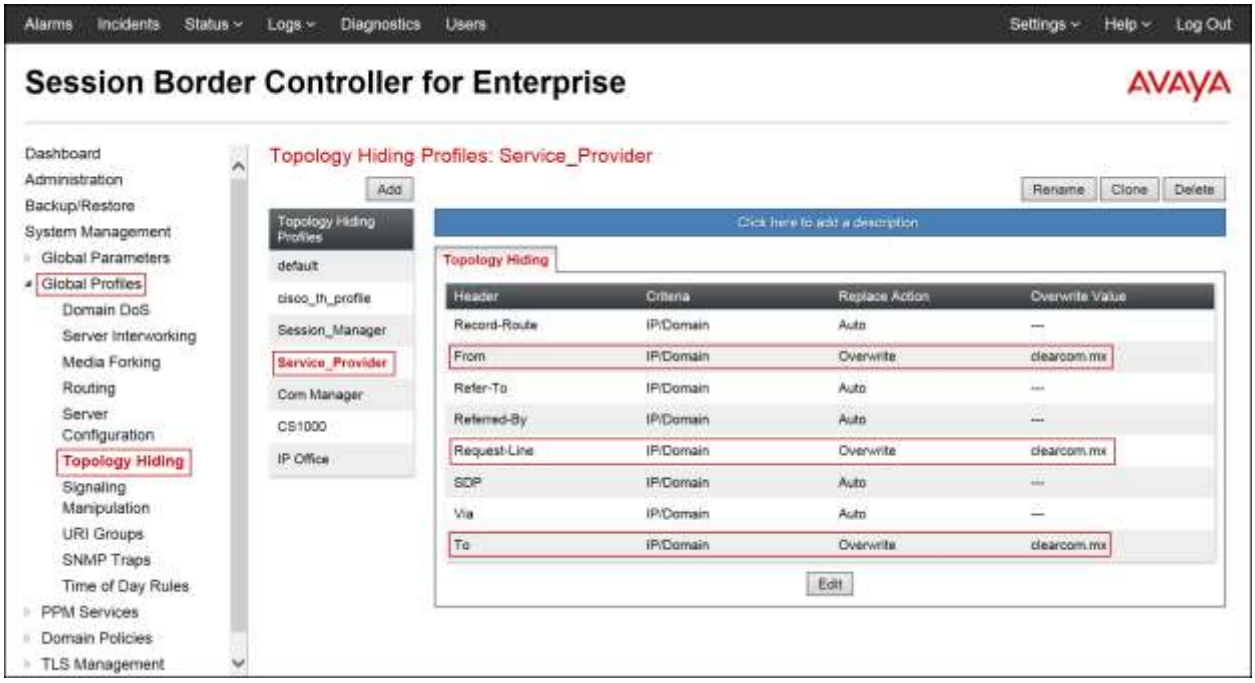
©2016 Avaya Inc. All Rights Reserved.

- Click **Edit** on the newly created **Service_Provider** Topology Hiding profile.
- On the **From** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (**clearcom.mx**) under **Overwrite Value**
- On the **To** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (**clearcom.mx**) under **Overwrite Value**.
- On the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (**clearcom.mx**) under **Overwrite Value**.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly added **Service_Provider** Topology Hiding Profile.



©2016 Avaya Inc. All Rights Reserved.

7.4 Domain Policies

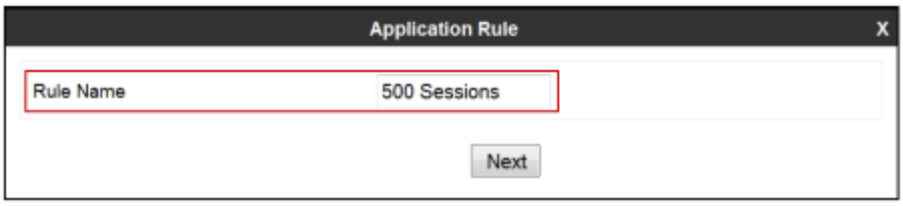
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.4.1 Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the Avaya SBCE will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

From the menu on the left-hand side, select **Domain Policies → Application Rules** (not shown).

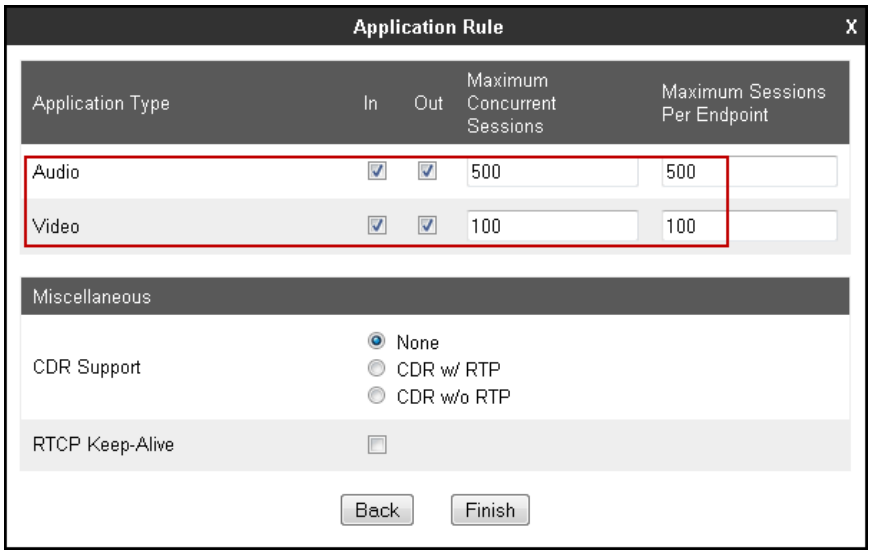
- Click on the **Add** button to add a new rule (not shown).
- **Rule Name:** enter the name of the profile, e.g., **500 Sessions**.
- Click **Next**.



- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values; the value of **500** was used in the sample configuration.

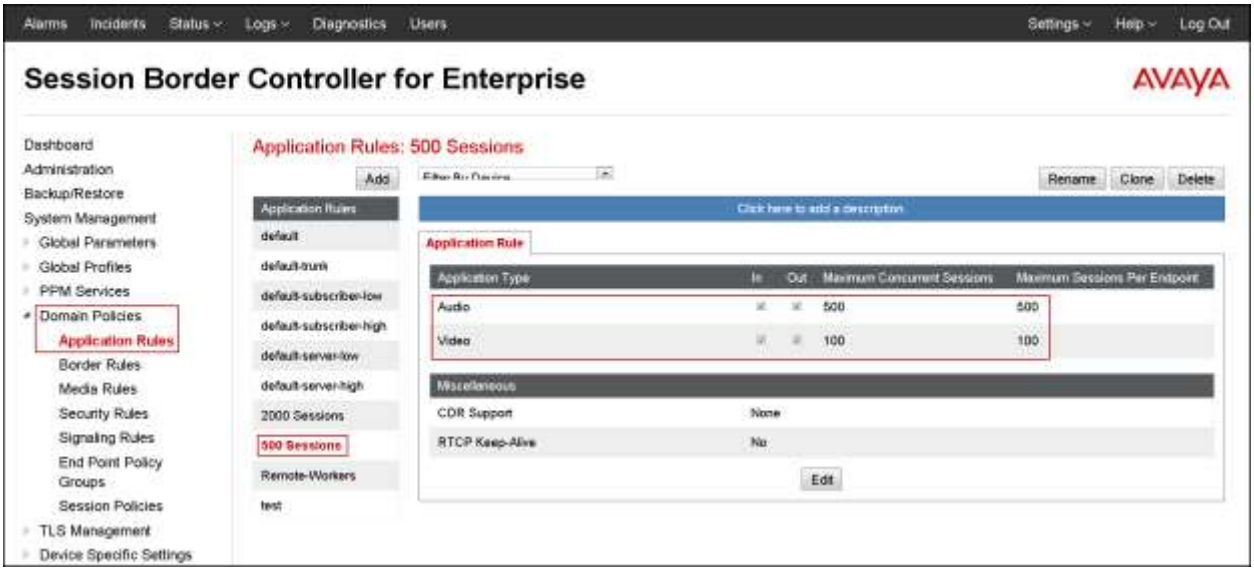
©2016 Avaya Inc. All Rights Reserved.

- Under **Video** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values; the value of **100** was used in the sample configuration.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **500 Sessions** Application Rule.



©2016 Avaya Inc. All Rights Reserved.

7.4.2 Media Rules

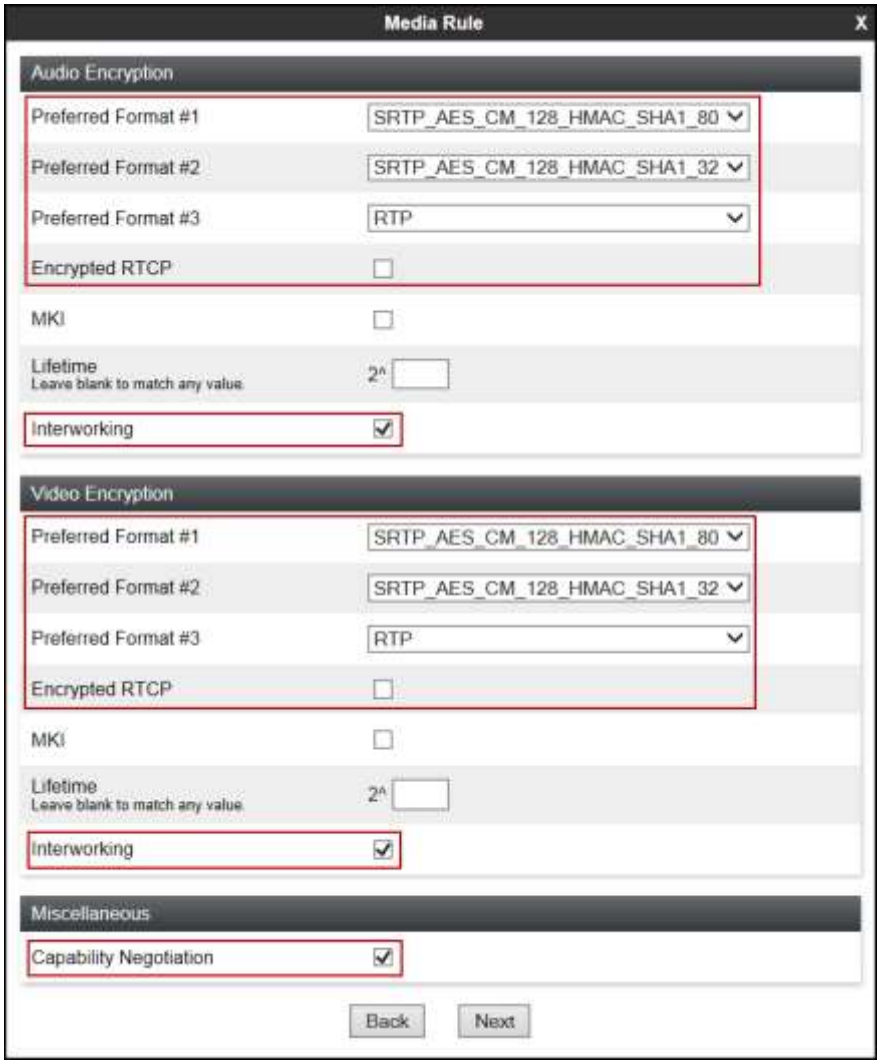
Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, two media rules (shown below) were used; one toward IP Office and one toward the Service Provider.

To add a media rule in the IP Office direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **IPO_SRTP**.
- Click Next.

©2016 Avaya Inc. All Rights Reserved.

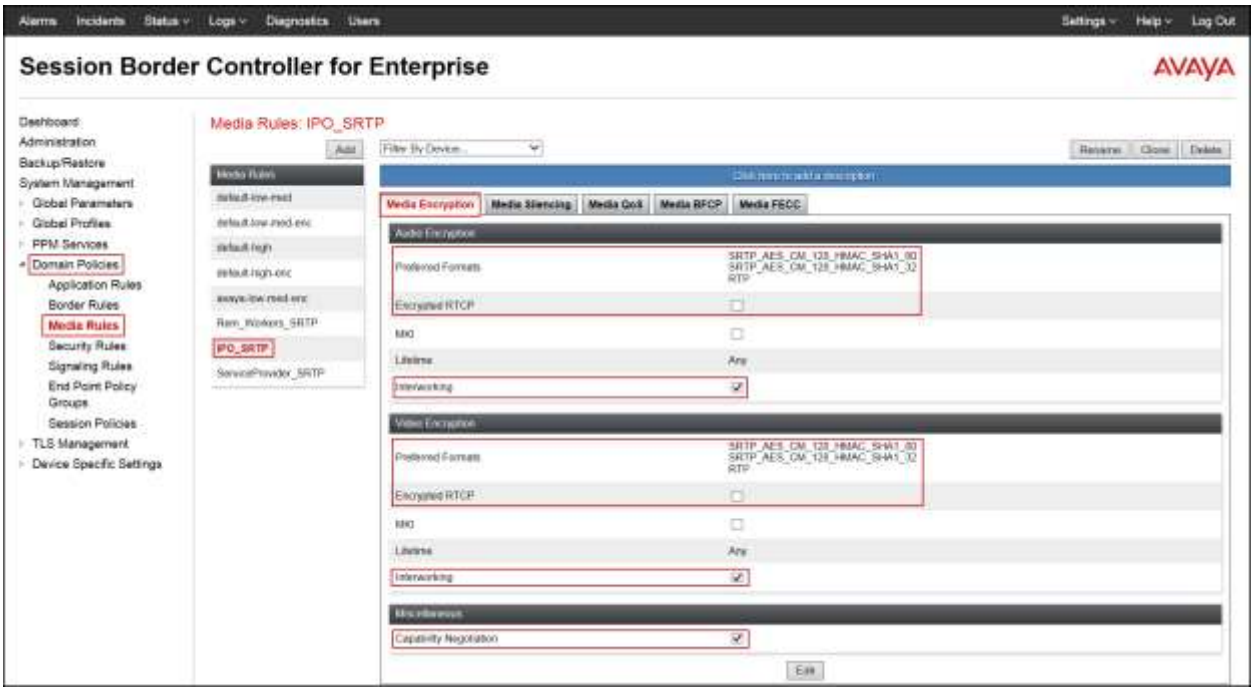
- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **SRTP_AES_CM_128_HMAC_SHA1_32**.
- Under Audio Encryption, **Preferred Format #3**, select **RTP**.
- Under Audio Encryption**,** uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous check **Capability Negotiation**.
- Click **Next**.



- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

The following screen capture shows the newly created **IPO_SRTP** Media Rule.

©2016 Avaya Inc. All Rights Reserved.



To add a media rule in the Service Provider direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

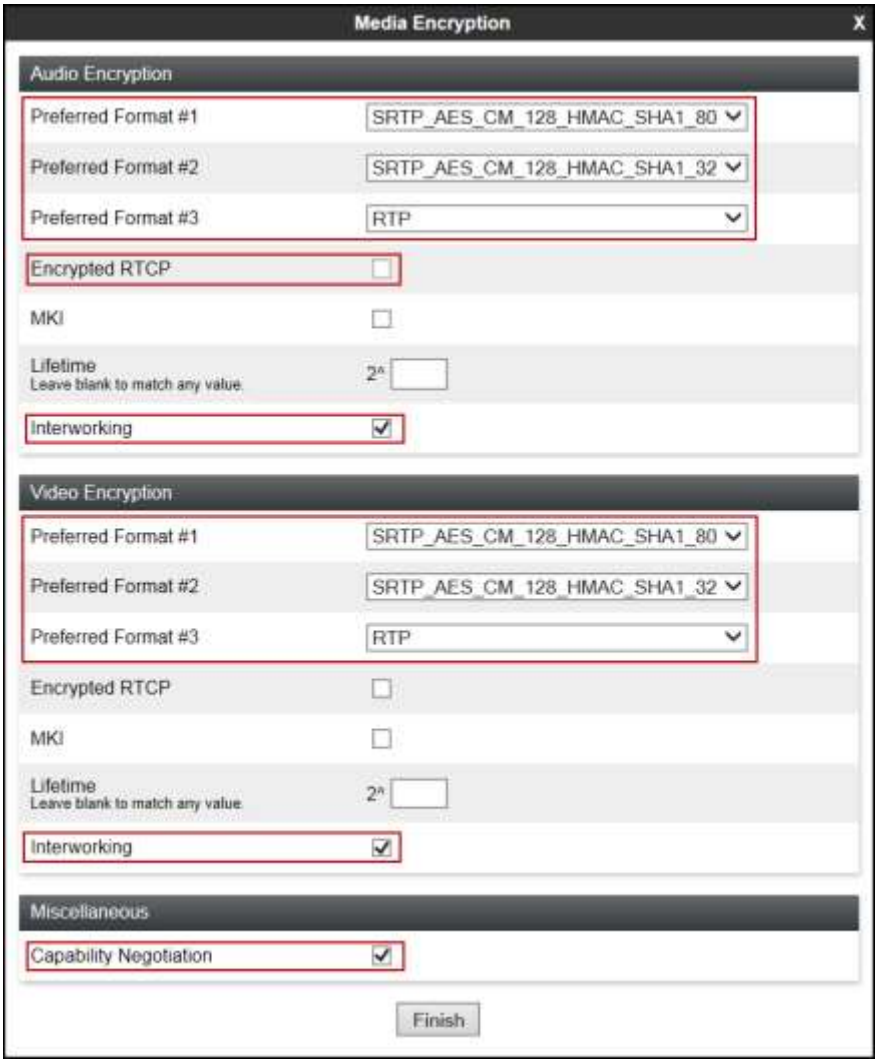
©2016 Avaya Inc. All Rights Reserved.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **ServiceProvider_SRTP**.
- Click Next.

- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.

©2016 Avaya Inc. All Rights Reserved.

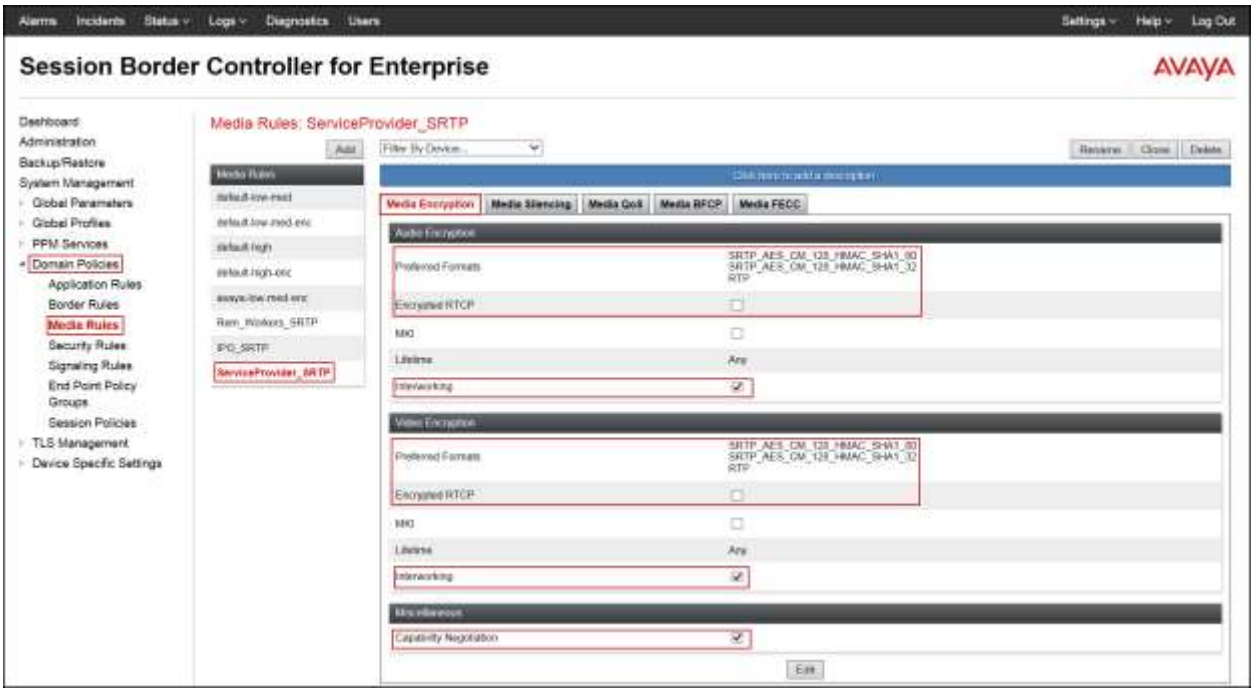
- Under Audio Encryption, **Preferred Format #2**, select **SRTP_AES_CM_128_HMAC_SHA1_32**.
- Under Audio Encryption, **Preferred Format #3**, select **RTP**.
- Under Audio Encryption**,** uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous check **Capability Negotiation**.
- Click **Finish**.



- Accept default values in the remaining sections by clicking **Next (**not shown), and then click **Finish** (not shown).

The following screen capture shows the newly created **ServiceProvider_SRTP** Media Rule.

©2016 Avaya Inc. All Rights Reserved.

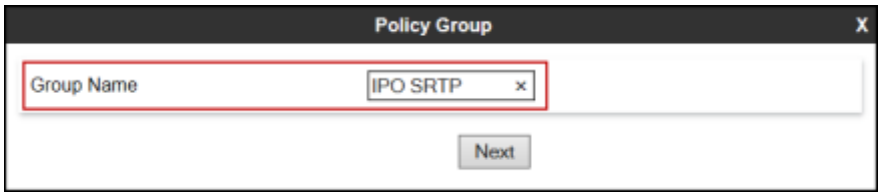


7.4.3 End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

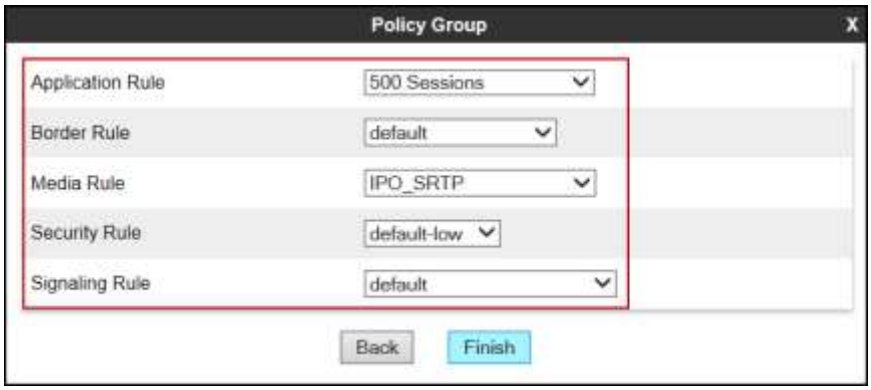
To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups** (not shown).

- Click on the **Add** button to add a new policy group (not shown).
- **Group Name: IPO SRTP**.
- Click **Next**.

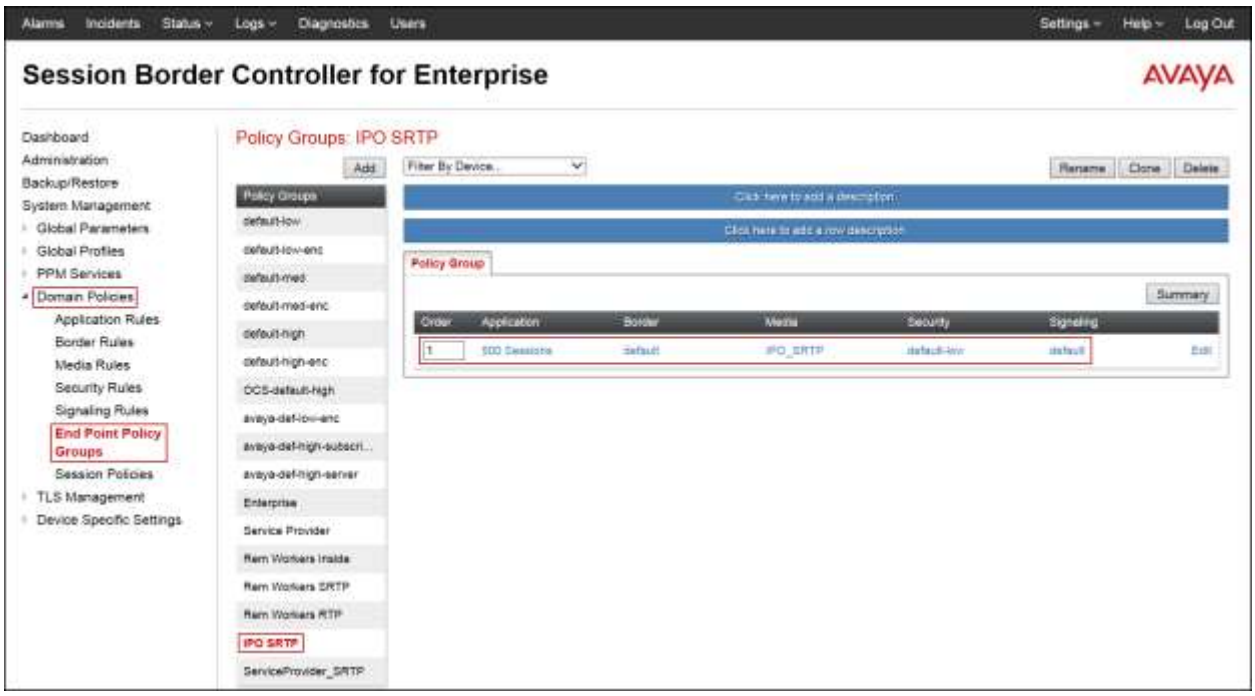


©2016 Avaya Inc. All Rights Reserved.

- **Application Rule: 500 Sessions**.
- **Border Rule: default**.
- **Media Rule: IPO_SRTP**.
- **Security Rule: default-low**.
- **Signaling Rule: default**.
- Click **Finish**.



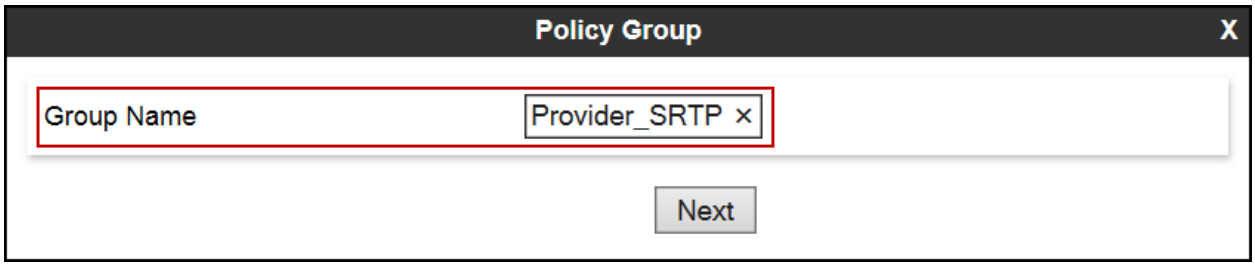
The following screen capture shows the newly created **IPO_SRTP** End Point Policy Group.



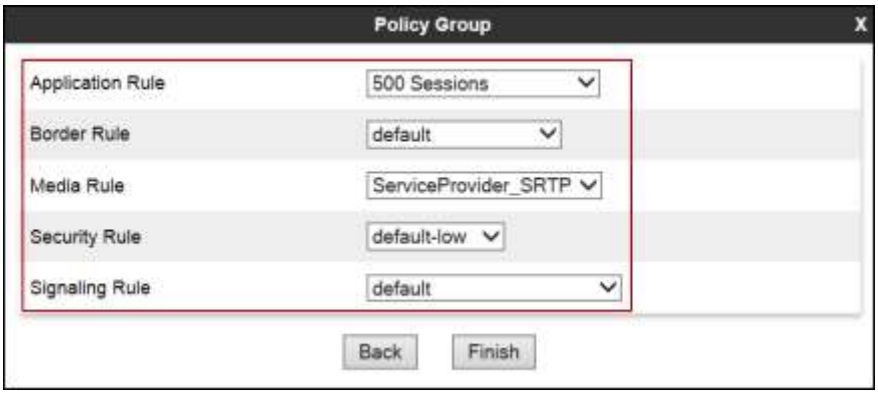
©2016 Avaya Inc. All Rights Reserved.

Similarly, to create an End Point Policy Group toward the Service Provider.

- Click on the **Add** button to add a new policy group (not shown).
- **Group Name: ServiceProvider_SRTP**.
- Click **Next**.

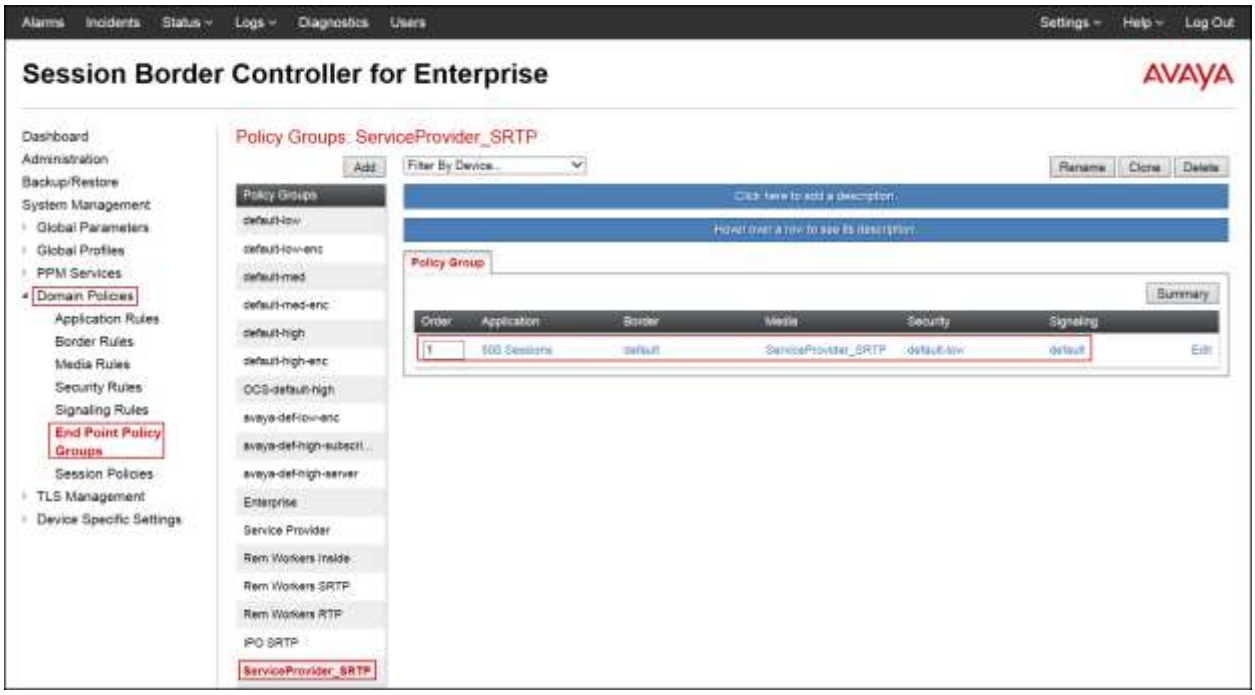


- **Application Rule: 500 Sessions**.
- **Border Rule: default**.
- **Media Rule: ServiceProvider_SRTP**.
- **Security Rule: default-low**.
- **Signaling Rule: default**.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **ServiceProvider_SRTP** End Point Policy Group.



©2016 Avaya Inc. All Rights Reserved.

7.5 Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc., are defined here.

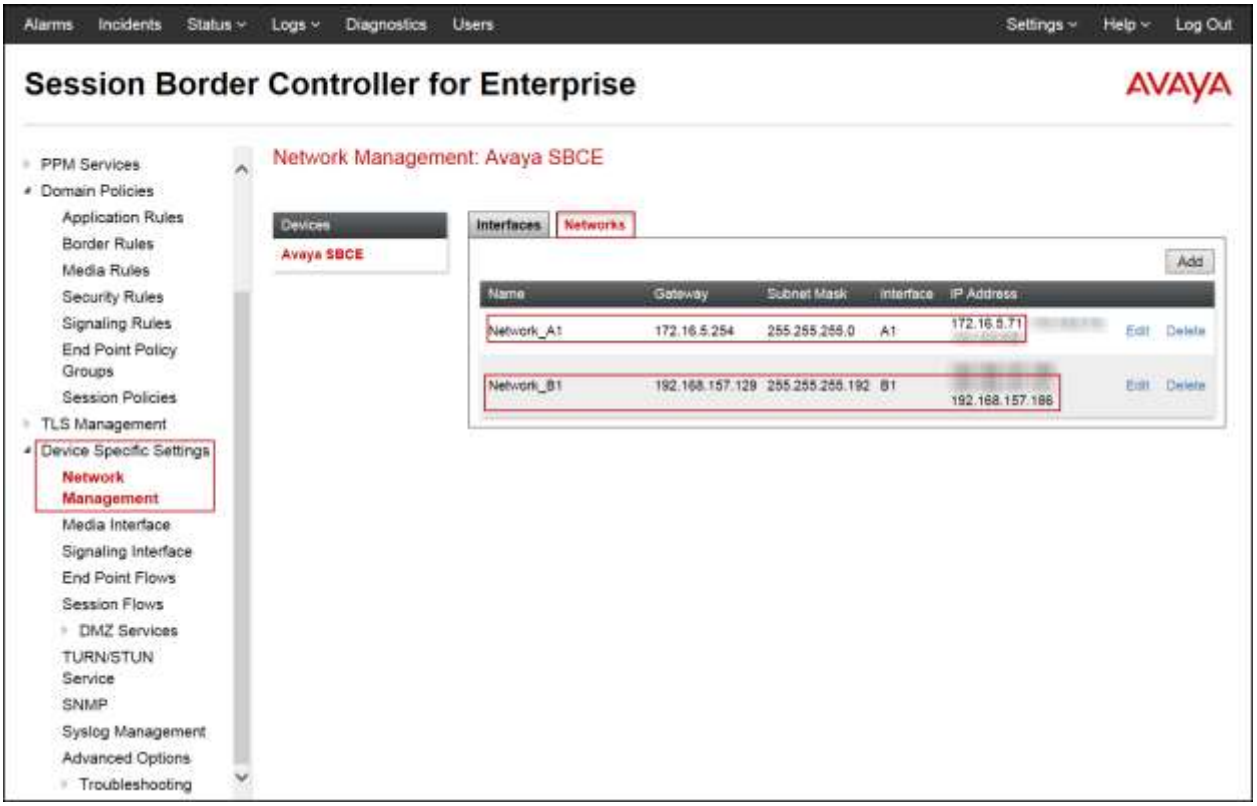
7.5.1 Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** under **Device Specific Settings** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.

In the event that changes need to be made to the network configuration information, they can be entered here.

Use **Figure 1** as reference for IP address assignments.

Note: Only the highlighted items were created for the compliance test, and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in these Application Notes.



©2016 Avaya Inc. All Rights Reserved.

On the Interface Configuration tab, click the **Status** for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **Disabled**, so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.

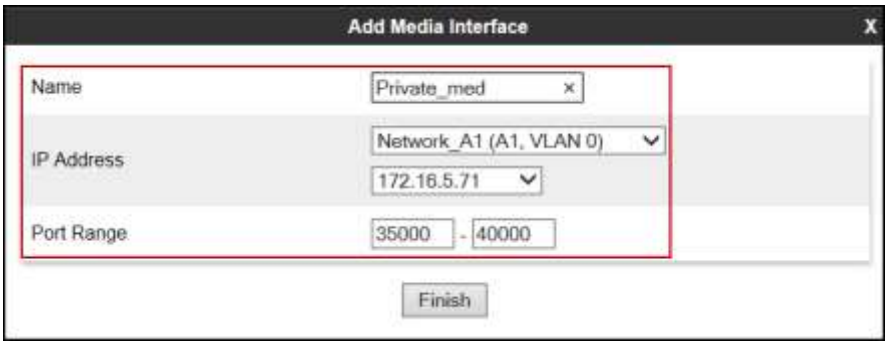
©2016 Avaya Inc. All Rights Reserved.

7.5.2 Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

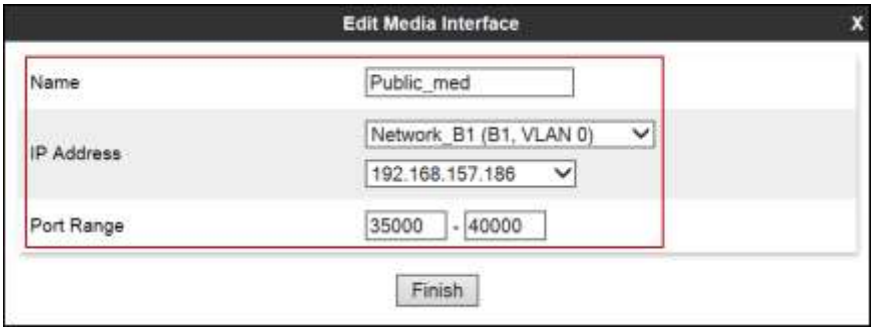
From the **Device Specific Settings** menu on the left-hand side, select **Media Interface** (not shown).

- Select **Add** in the **Media Interface** area (not shown).
- **Name**: **Private_med**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**.
- Select **IP Address**: **172.16.5.71** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office)
- **Port Range**: **35000-40000**.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

- Select **Add** in the **Media Interface** area (not shown)**.**
- **Name**: **Public_med**.
- Under **IP Address** select: **Network_B1 (B1, VLAN 0)**.
  Select **IP Address**: **192.168.157.186** (Outside IP Address of the Avaya SBCE, toward Clearcom).
- **Port Range**: **35000-40000**.
- Click **Finish**.



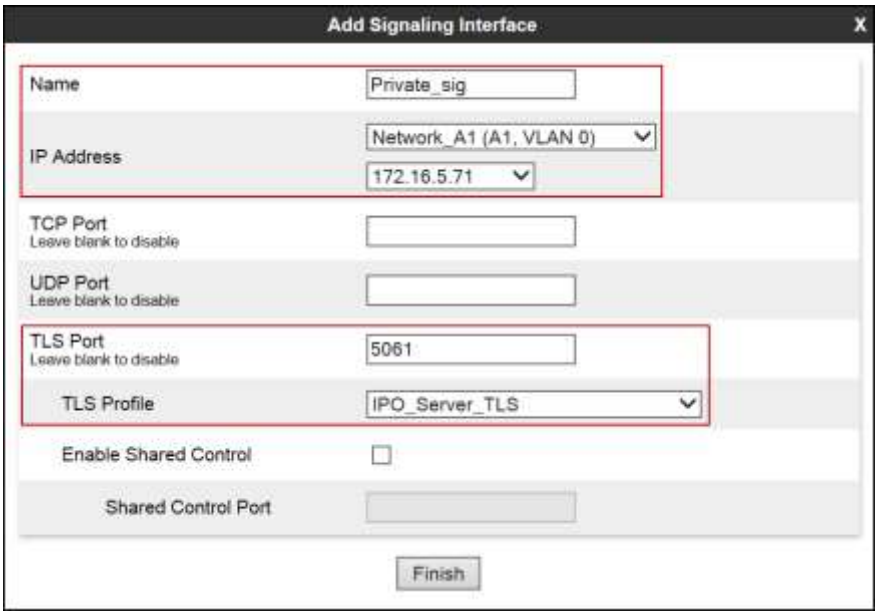
The following screen capture shows the newly created Media Interfaces.

©2016 Avaya Inc. All Rights Reserved.

7.5.3 Signaling Interface

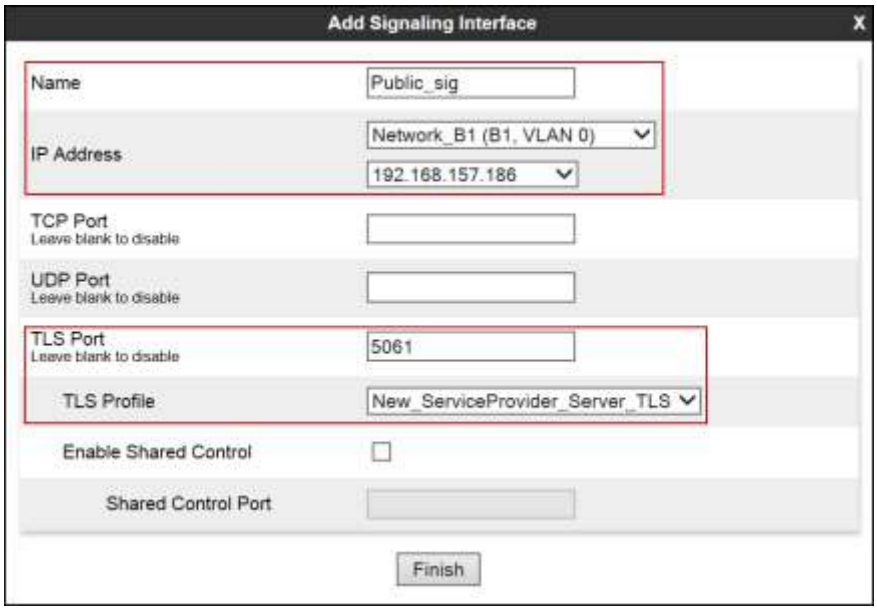
To create the Signaling Interface toward IP Office, from the **Device Specific** menu on the left hand side, select **Signaling Interface** (not shown).

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name**: **Private_sig**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**.
- Select **IP Address**: **172.16.5.71** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office).
- **TLS Port**: **5061**.
- Under **TLS Profile** select: **IPO_Server_TLS**.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name**: **Public_sig**.
- Under **IP Address** select: **Network_B1 (B1, VLAN 0)**.
- Select **IP Address**: **192.168.157.186** (Outside or B1 IP Address of the Avaya SBCE, toward Clearcom).
- **TLS Port**: **5061**.
- Under **TLS Profile** select: **New_ServiceProvider_Server_TLS**.
- Click **Finish**.



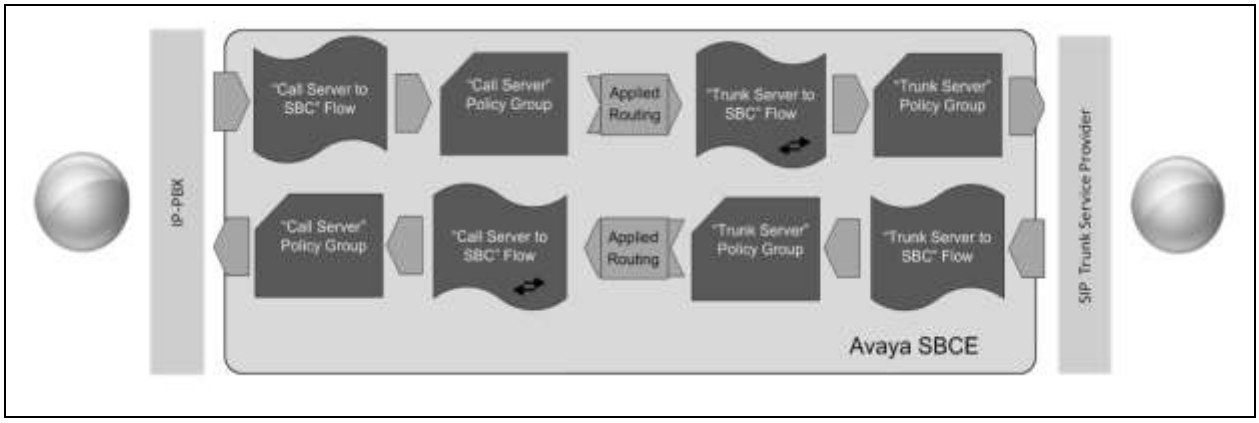
The following screen capture shows the newly created Signaling Interfaces.

©2016 Avaya Inc. All Rights Reserved.

©2016 Avaya Inc. All Rights Reserved.

7.5.4 End Point Flows

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

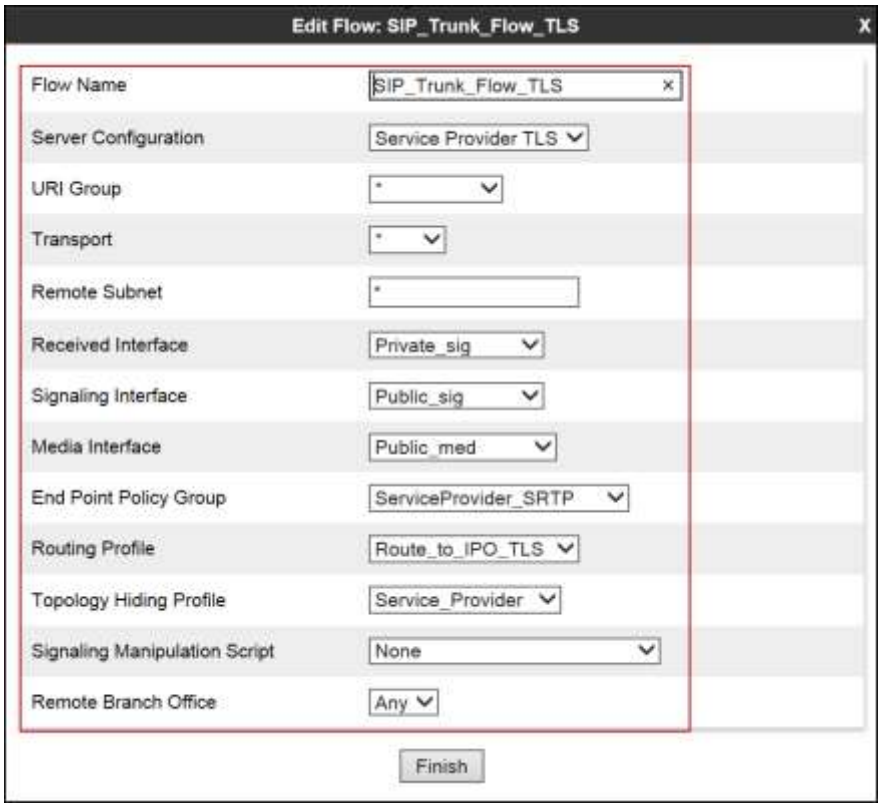


©2016 Avaya Inc. All Rights Reserved.

The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward Clearcom, from the **Device Specific Settings** menu, select **End Point Flows** (not shown), then the **Server Flows** tab. Click **Add** (not shown).

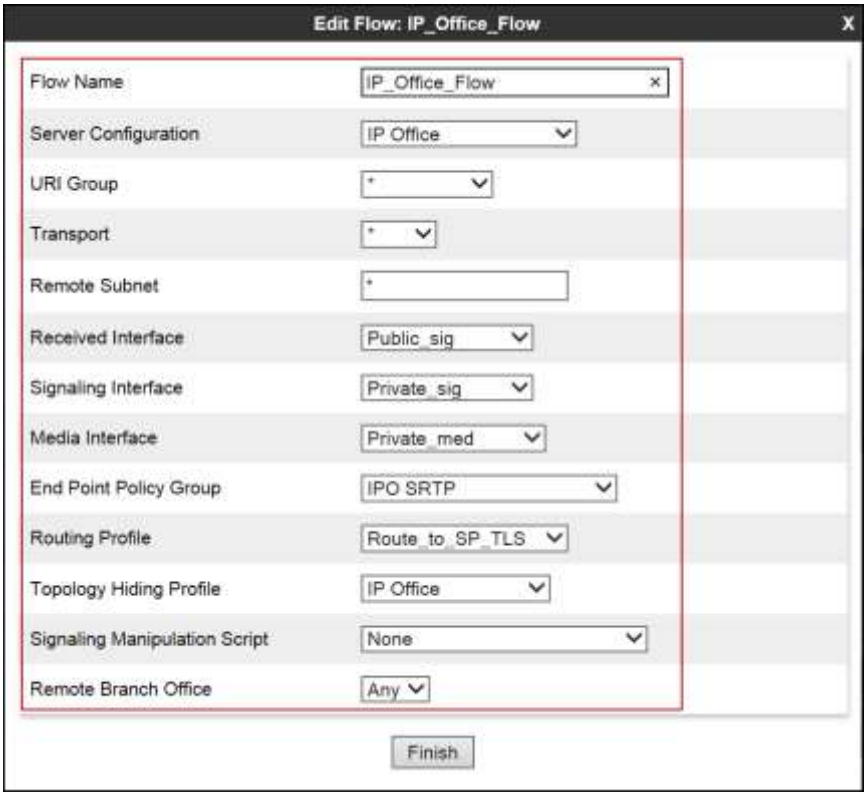
- **Name: SIP_Trunk_Flow_TLS**.
- **Server Configuration**: **Service Provider TLS**.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Private_sig**.
- **Signaling Interface: Public_sig**.
- **Media Interface**: **Public_med**.
- **End Point Policy Group: ServiceProvider_SRTP**.
- **Routing Profile: Route_to_IPO_TLS** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service_Provider**.
- **Signaling Manipulation Script: None**.
- **Remote Branch Office: Any**.
- Click **Finish**.



To create the call flow toward IP Office, click **Add** (not shown).

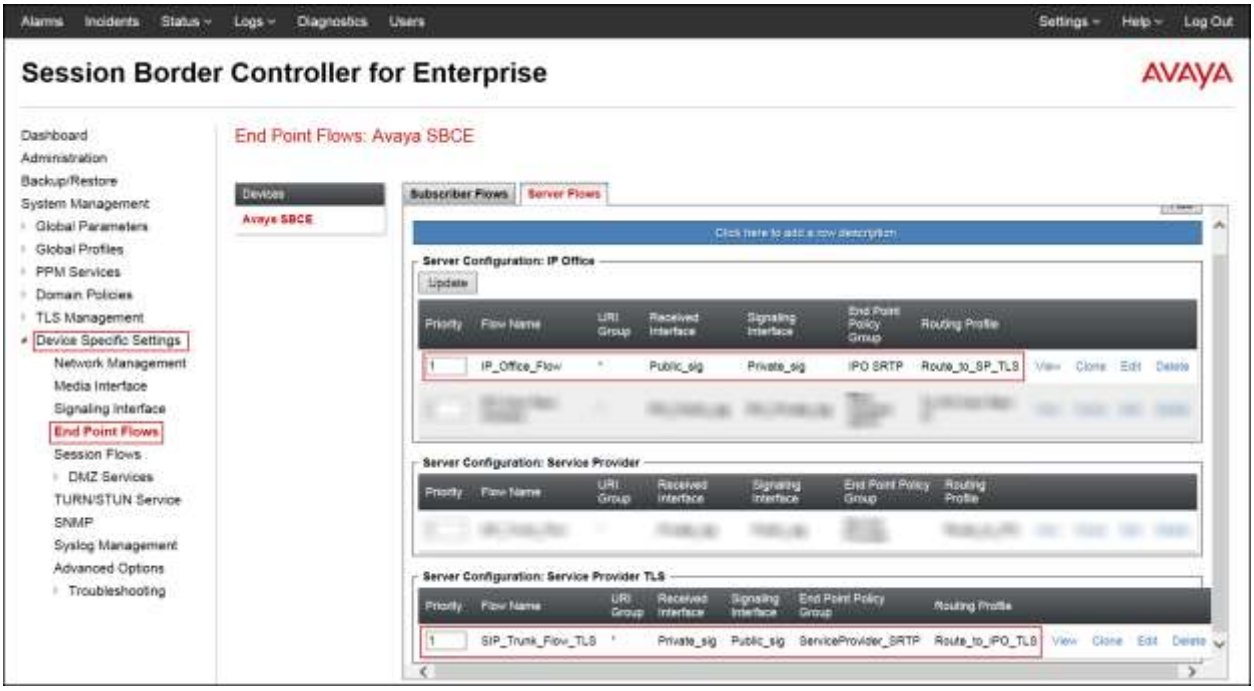
©2016 Avaya Inc. All Rights Reserved.

- **Name: IP_Office_Flow**.
- **Server Configuration**: **IP Office**.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Public_sig**.
- **Signaling Interface: Private_sig**.
- **Media Interface**: **Private_med**.
- **End Point Policy Group: IPO SRTP**.
- **Routing Profile: Route_to_SP_TLS** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: IP Office**.
- **Signaling Manipulation Script: None**.
- **Remote Branch Office: Any**.
- Click **Finish**.



©2016 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly created **End Point Flows**.



©2016 Avaya Inc. All Rights Reserved.

8. Clearcom SIP Trunking Service Configuration

To use Clearcom's SIP Trunk service, a customer must request the service from Clearcom using the established sales processes. The process can be started by contacting Clearcom via the corporate web site at: http://www.clearcom.mx/ and requesting information.

During the signup process, Clearcom and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Clearcom's network.

Clearcom is responsible for the configuration of Clearcom SIP Services. The customer will need to provide a public IP address to be used to reach the Avaya SBCE at the enterprise. In the case of the compliance test, this is the outside or public IP address of the Avaya SBCE (B1 interface). The customer will also need the IP addresses for the primary and the secondary public DNS servers, these addresses can be obtained from the local ISP in Mexico.

Clearcom will provide the customer the necessary information to configure Avaya IP Office and the Avaya SBCE following the steps discussed in the previous sections, including:

- SIP Trunk registration credentials (User Name, Password, etc.).
- Clearcom's Domain Name and SIP Proxy FQDN.
- DID numbers, etc.

©2016 Avaya Inc. All Rights Reserved.

9. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting tips that can be used to troubleshoot the solution.

9.1 Verification Steps

The following steps may be used to verify the configuration:

- Verify that endpoints at the enterprise site can place calls to PSTN and that calls remain active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from PSTN and that calls can remain active for more than 35 seconds.
- Verify that the user on the PSTN side can end an active call by hanging up.
- Verify that an Avaya endpoint at the enterprise site can end an active call by hanging up.

9.2 Protocol Traces

The following SIP message headers are inspected using a sniffer trace analysis tool:

- Request-URI: Verify the request number and SIP domain.
- From: Verify the display name and display number.
- To: Verify the display name and display number.
- P-Asserted-Identity: Verify the display name and display number.
- Privacy: Verify privacy masking with “user, id”.
- Diversion: Verify the display name and display number.

The following attributes in SIP message body are inspected using a sniffer trace analysis tool:

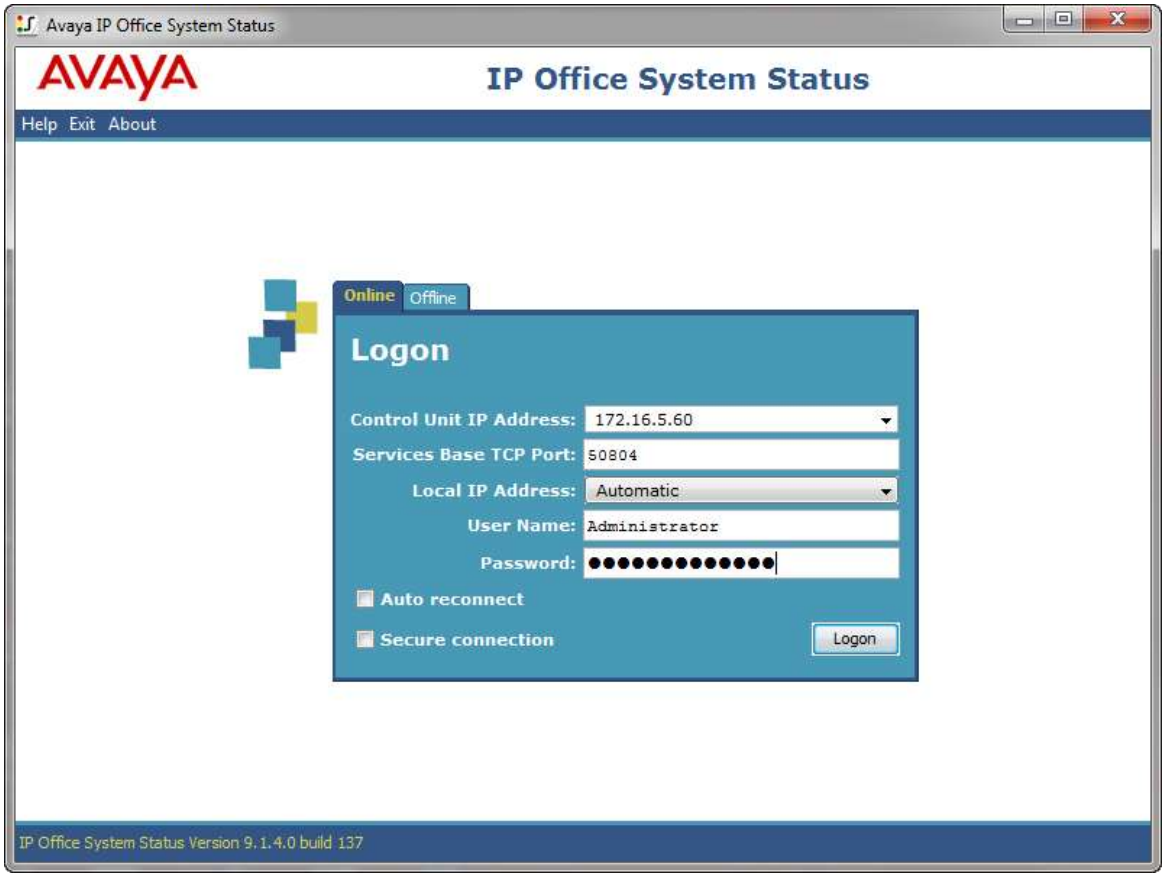
- Connection Information (c line): Verify IP addresses of near end and far end endpoints.
- Time Description (t line): Verify session timeout value of near end and far end endpoints.
- Media Description (m line): Verify audio port, codec, DTMF event description.
- Media Attribute (a line): Verify specific audio port, codec, ptime, send/ receive ability, DTMF events.

©2016 Avaya Inc. All Rights Reserved.

9.3 IP Office System Status

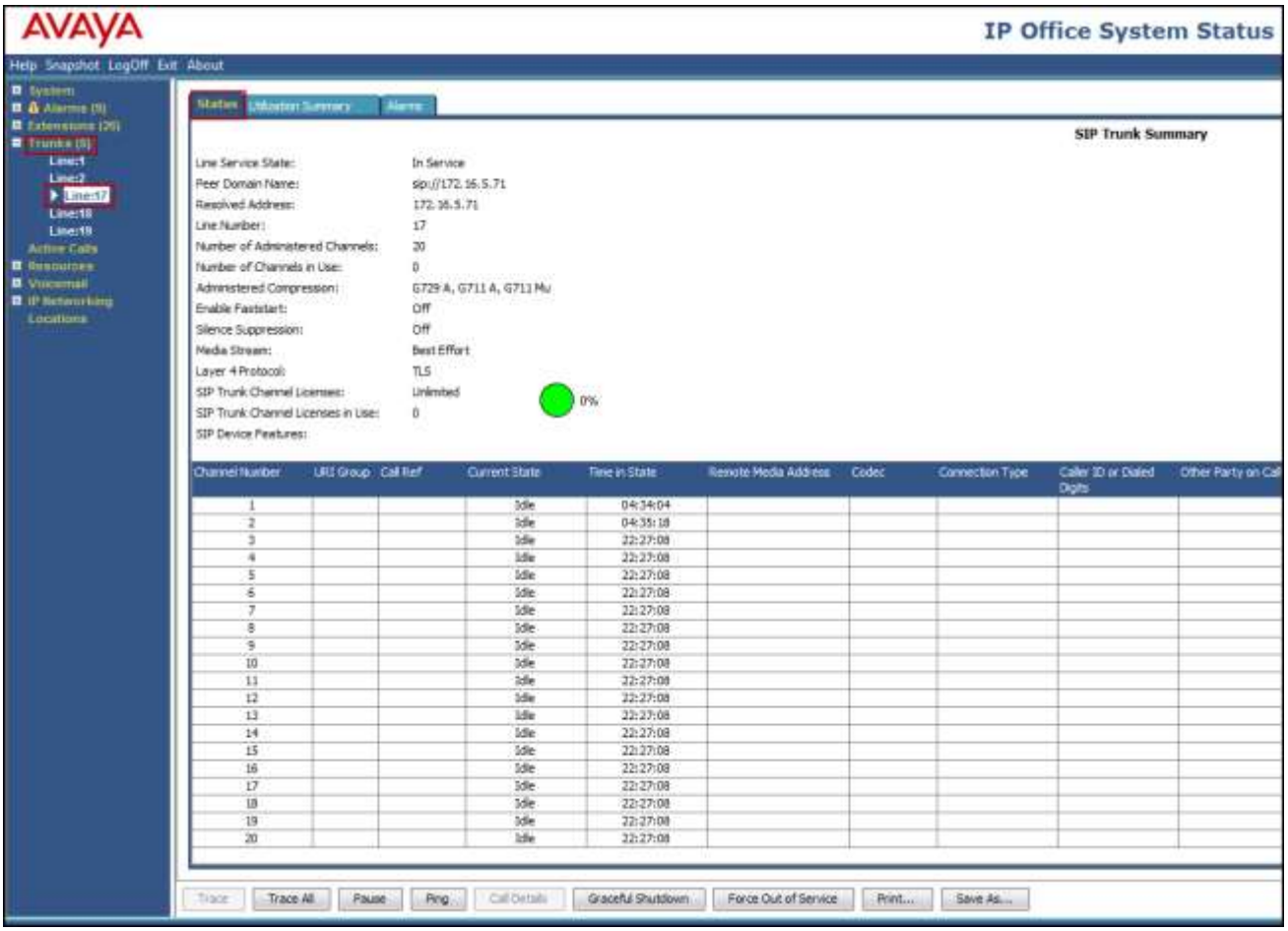
The following steps can also be used to verify the configuration.

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 IP Office Manager is installed, log in with the proper credentials.



1. Select the SIP Line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** is **Idle** for each channel (assuming no active calls at present time).

©2016 Avaya Inc. All Rights Reserved.



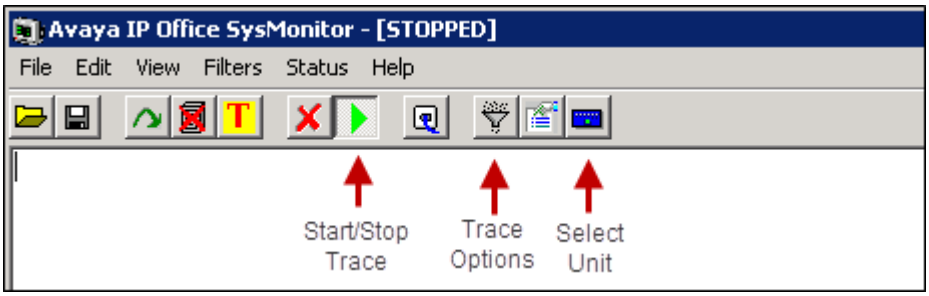
2. Select the **Alarms** tab and verify that no alarms are active on the SIP Line.

©2016 Avaya Inc. All Rights Reserved.

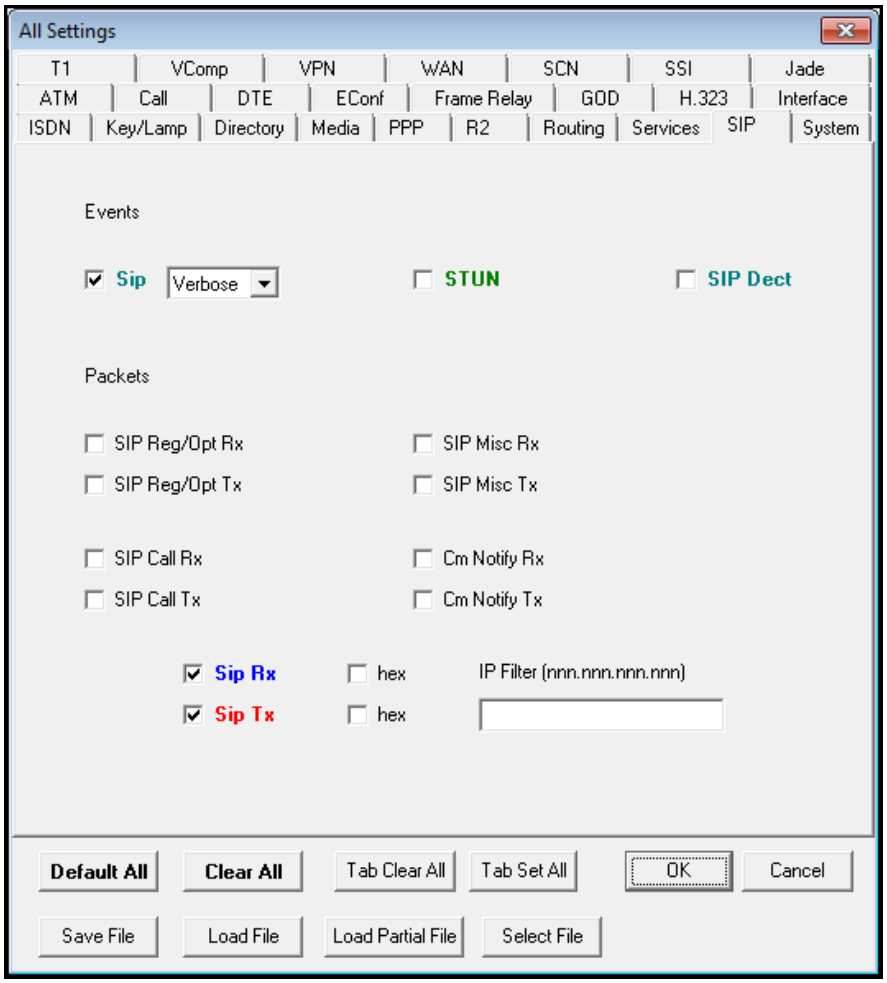
©2016 Avaya Inc. All Rights Reserved.

9.4 IP Office Monitor

The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where Avaya IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and select the IP address of the IP Office system under verification.



Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting to the desired color.

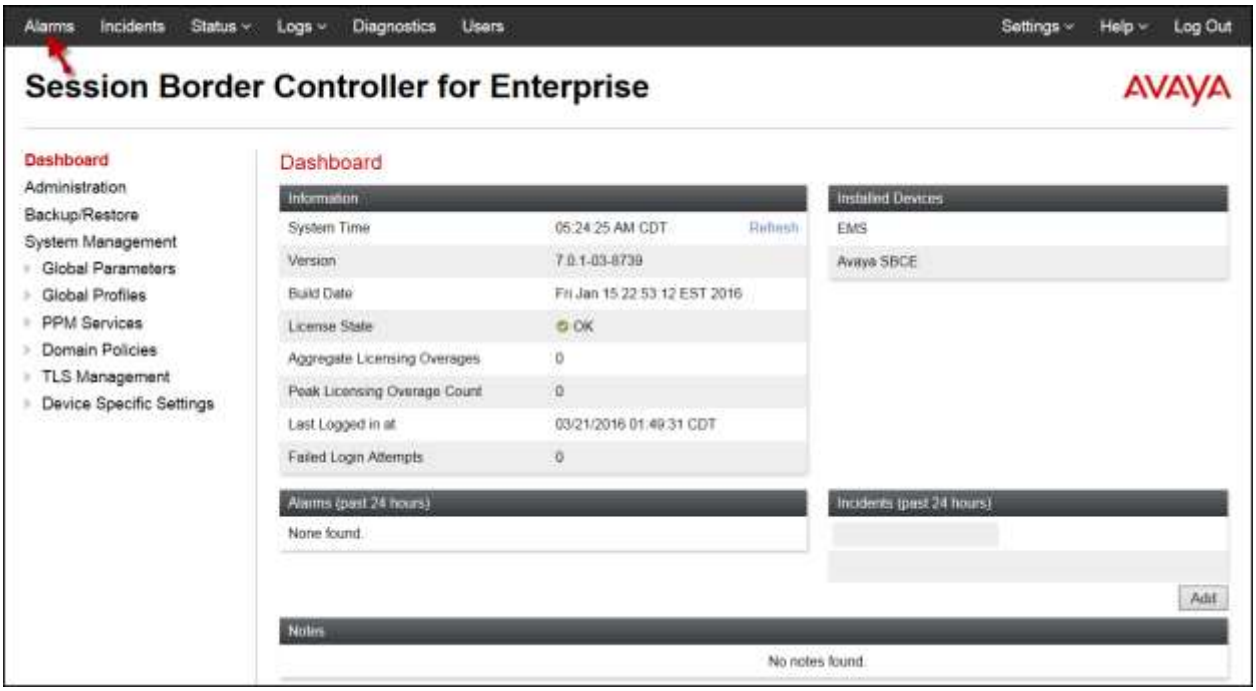


©2016 Avaya Inc. All Rights Reserved.

9.5 Avaya Session Border Controller for Enterprise (Avaya SBCE)

There are several links and menus located on the taskbar at the top of the screen of the web interface that can be used for diagnostic and troubleshooting.

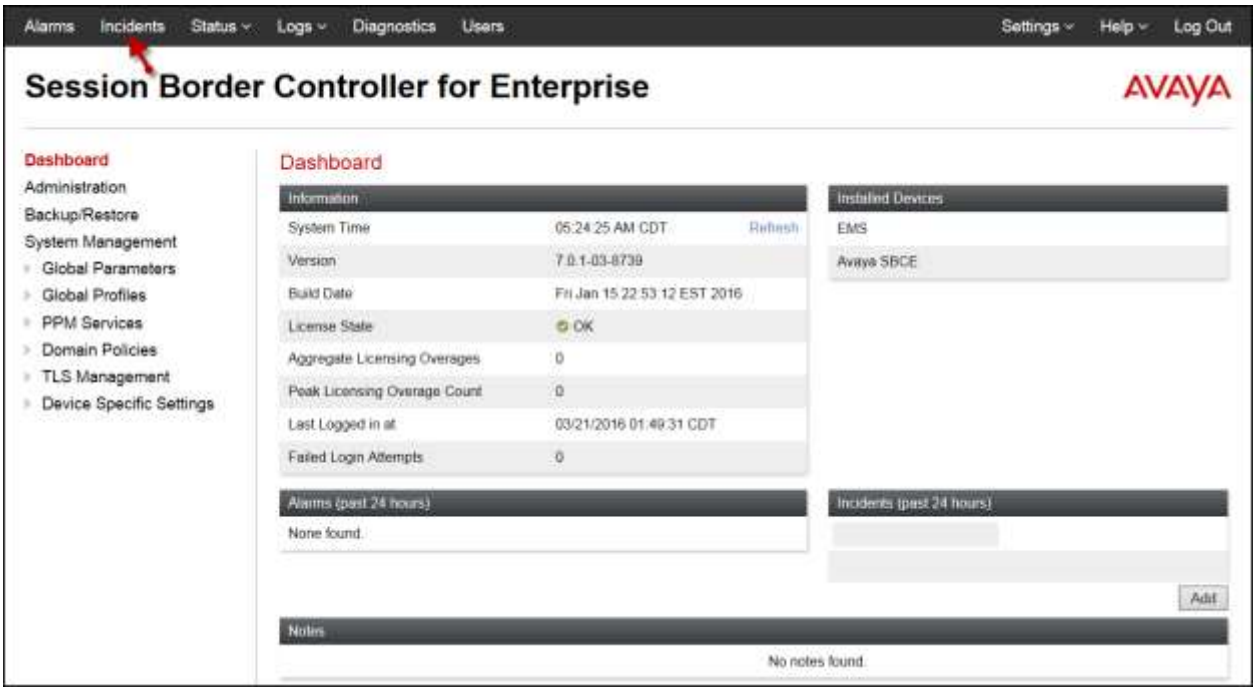
Alarms: Provides information about the health of the Avaya SBCE.



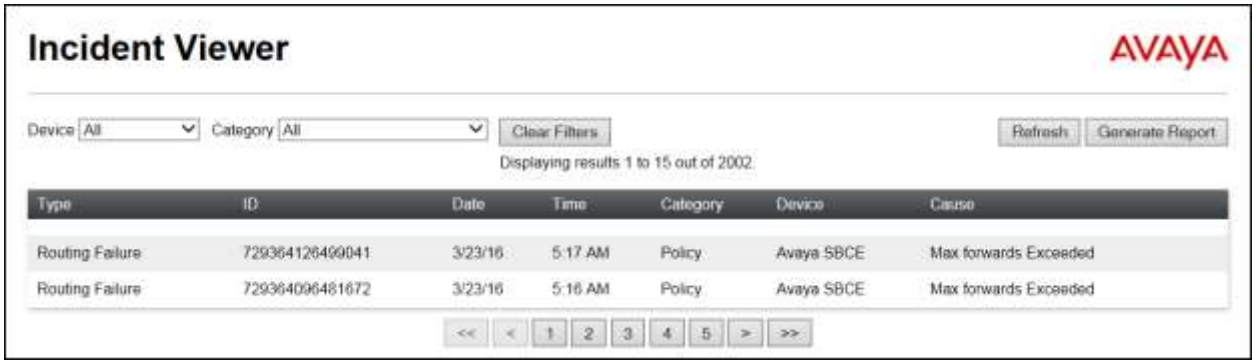
The following screen shows the **Alarm Viewer** page.

©2016 Avaya Inc. All Rights Reserved.

Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.

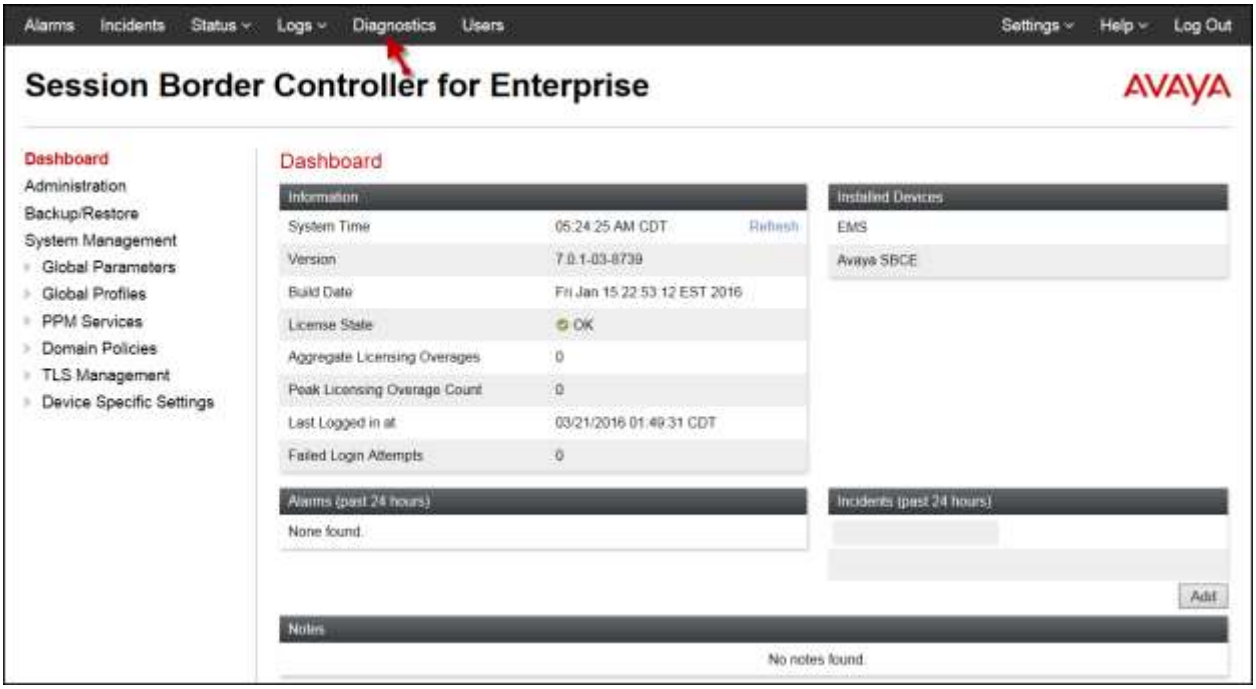


The following screen shows the Incident Viewer page.

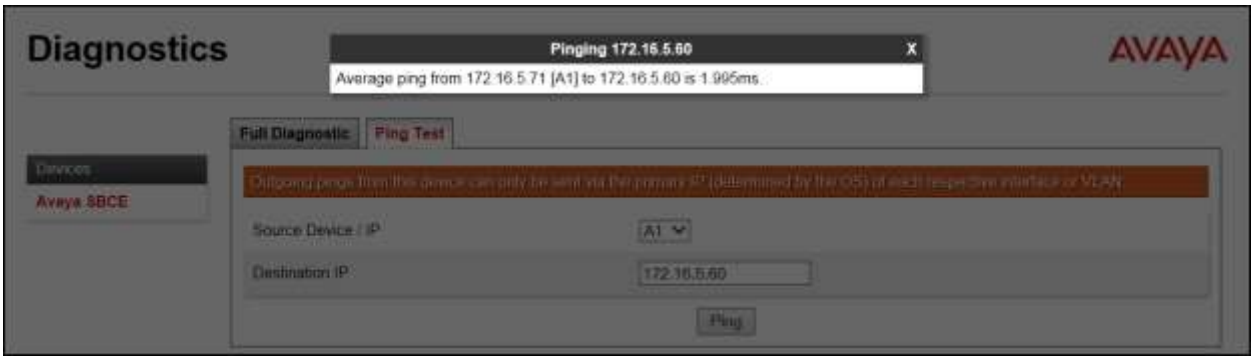


©2016 Avaya Inc. All Rights Reserved.

Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



The following screen shows the Diagnostics page with the results of a ping test.

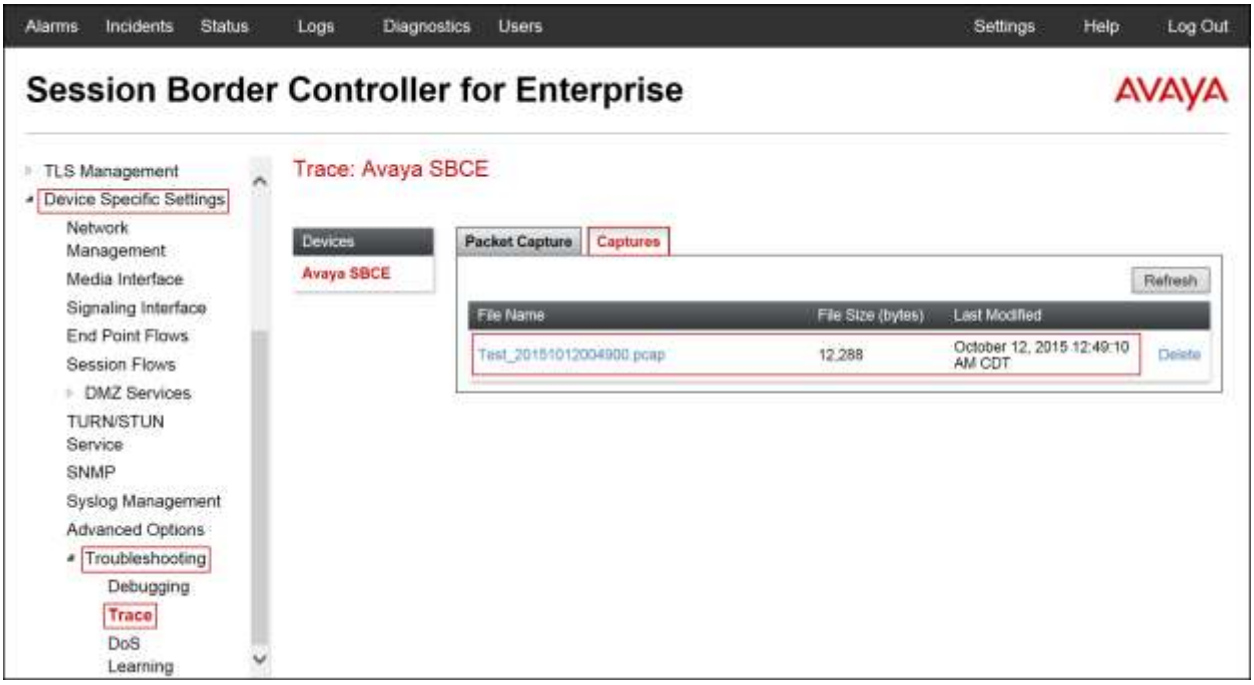


©2016 Avaya Inc. All Rights Reserved.

Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as pcap files. Navigate to **Device Specific Settings → Troubleshooting → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

©2016 Avaya Inc. All Rights Reserved.

Once the capture is stopped, click on the **Captures** tab and select the proper pcap file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.



9.6 TraceSBC Tool

traceSBC is a perl script that parses Avaya SBCE log files and displays SIP and PPM messages in a ladder diagram. Because the logs contain the decrypted messages, you can use the tool easily even in case of TLS and HTTPS. traceSBC can parse the log files downloaded from Avaya SBCE. traceSBC can also process log files in real time on Avaya SBCE, so that you can check SIP and PPM traffic during live calls. Refer to items [10] in **Section 11**

Operation modes:

- **Non real-time mode**:
  The tool starts with at least one file in the command line parameters. The tool automatically detects the type of files, processes the files, and finally displays messages from the different files in one diagram ordered by the timestamp. If filters are set, only the messages that match the filters are displayed in the diagram. In this mode, enabling live capture is not an option.
  Examples: # traceSBC tracesbc_sip_1408635251

- **Real-time mode**
  In this mode, traceSBC must be on active Avaya SBCE. traceSBC is started without specifying a file in the command line parameters. The tool automatically starts processing the log files. The live capture can be started and stopped anytime without affecting service.
  Example: # traceSBC

Log Files

©2016 Avaya Inc. All Rights Reserved.

Avaya SBCE can log SIP messages as processed by different subsystems and also log PPM messages. The traceSBC utility can process the log files real-time by opening the latest log files in the given directories. TraceSBC also checks regularly if a new file is generated, in which case the old one is closed and processing continues with the new one. A new log file is generated every time the relevant processes restart, or when the size reaches the limit of ~10 M.

Log Locations:
SIP messages are found at /archive/log/tracesbc/tracesbc_sip/ and PPM messages can be found at /archive/log/tracesbc/tracesbc_ppm/.

Active files are of the following format:
-rw-rw---- 1 root root 112445 Aug 21 10:12 tracesbc_sip_1408631651

Inactive or closed files are of the following format:
-rw-rw---- 1 root root 175236 Aug 21 06:33 tracesbc_sip_1408617250_1408620820_1

or

-rw-rw---- 1 root root 31706 Jul 10 13:34 tracesbc_sip_1436549674_1436553270_1.gz

©2016 Avaya Inc. All Rights Reserved.

10. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 9.1 and the Avaya Session Border Controller for Enterprise Release 7.0 to support Clearcom SIP Trunking Service using TLS, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

©2016 Avaya Inc. All Rights Reserved.

11. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya IP Office, including the following, is available at: http://support.avaya.com/

[1] *Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 30zc, March 21, 2016.
[2] *Using Avaya IP Office Platform System Status*, Document Number 15-601758, Issue 10f, August 2015.
[3] *Administering Avaya IP Office Platform Voicemail Pro*, Document Number 15-601063, Issue 10m, February 05, 2016.
[4] *Using IP Office System Monitor*, Document Number 15-601019, Issue 06g, February 08, 2016.
[5] *Avaya IP Office Platform Security Guidelines, Release 9.1.* Issue 01.05, October 2015.
[6] *Administering Avaya IP Office Platform with Manager, Release 9.1.2.* Issue 10.38, February 2016.
[7] *IP Office Technical Bulletin number 175 (*http://www.ipofficeinfo.com/TechBulletins/tb175.pdf)

Product documentation for the Avaya Session Border Controller for Enterprise, including the following, is available at: http://support.avaya.com/

[8] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
[9] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
[10] *Troubleshooting and Maintaining Avaya session Border Controller for Enterprise*, Release 7.0, Issue 1, December 2015.

Additional Avaya IP Office documentation can be found at: http://marketingtools.avaya.com/knowledgebase/

©2016 Avaya Inc. All Rights Reserved.

©2016 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.