Avaya Solution & Interoperability Test Lab

Application Notes for Telecommunications Services of Trinidad and Tobago SIP Trunking Service with Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Telecommunications Services of Trinidad and Tobago Session Initiation Protocol (SIP) Trunking Service with Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise Release 6.2.

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

Telecommunications Services of Trinidad and Tobago 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.

Table of Contents

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Telecommunications Services of Trinidad and Tobago and Avaya IP Office solution.

In the sample configuration, Avaya IP Office solution consists of Avaya IP Office (IP Office) Release 8.1 500v2, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2, Avaya IP Office soft clients and Avaya desk phones, including SIP, H.323, digital, and analog endpoints. The Avaya SBCE provides UC security for the Avaya IP Office solution, as well as interoperability features for the SIP trunk.

Telecommunications Services of Trinidad and Tobago SIP Trunking Service (TSTT) 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 and 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

Telecommunications Services of Trinidad and Tobago will be referred to as **TSTT** here after.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using IP Office to connect to TSTT via the Avaya SBCE. This configuration (shown in **Figure 1**) was used to exercise the feature and functionality tests listed in **Section 2.1**.

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

2.1 Interoperability Compliance Testing

To verify TSTT SIP Trunking interoperability, the following features and functionalities were exercised during the compliance testing:

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types including SIP, H.323, digital and analog telephones at the enterprise. All incoming calls from PSTN were routed to the enterprise across the SIP Trunk from the service provider networks.
- Outgoing PSTN calls from various phone types including SIP, H.323, digital and analog telephone at the enterprise. All outgoing calls to PSTN were routed from the enterprise across the SIP trunk to the service provider networks.
- Incoming and outgoing PSTN calls to/from Avaya IP Office Softphone using both SIP and H.323 protocols.

- Incoming and outgoing PSTN calls to/from Avaya IP Office Phone Manager using H.323 protocol.
- Dialing plans including long distance, international, outbound toll-free, etc.
- Caller ID presentation and Caller ID restriction.
- Codec's G.711MU and G.729A (For Codec G.729A Test Results refer to **Section 2.2**).
- Proper early media transmissions using G.711MU codec.
- DTMF tone transmissions per RFC 2833.
- Voicemail navigation for incoming and outgoing calls.
- Telephony features such as hold and resume, call transfer, call forward and conferencing.
- Off-net call forwards and transfers.
- Mobility Twinning of incoming calls to mobile phones.
- Response to incomplete call attempts and trunk errors.

2.2 Test Results

Interoperability testing with TSTT was successfully completed with the exception of observations/limitations described below:

- **SIP REFER** – On PSTN calls to or from IP Office that are transferred back to the PSTN on the SIP trunk, TSTT responds with a "202 Accepted" to the REFER message sent by IP Office, but the call between the two PSTN endpoints drops, the PSTN phone receives re-order tone. REFER needs to be disabled in IP Office for the Call Transfer to complete successfully, otherwise the call transfer will fail. The implication is that IP Office SIP trunk channels are not released after the call transfer is completed, two (2) trunk channels will remain connected/busy for the duration of the call..
- **T.38 or G.711 Pass-Through fax calls** – With IP Office **Fax Transport Support** set as **T.38** or **T.38 Fallback** on the **SIP Line/VoIP**, on outbound calls (IPO→PSTN) TSTT did not send a re-INVITE to switch from G.711 to T.38. TSTT's recommendation is **not** to use T.38 fax transport, only G.711 fax Pass-through. With IP Office **Fax Transport Support** set as **G.711** on the **SIP Line/VoIP**, fax calls were unsuccessful, thus **T.38 or G.711** fax transports **are not** recommended for this solution.
- **Codec G.729A** – TSTT supports codec's G.711MU and G.729A, but during the testing, TSTT was rejecting calls with G.729A codec offer with **488 Invalid Media Type**. This issue is under investigation by TSTT.

2.3 Support

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

For technical support on TSTT SIP Trunking Service visit http://tstt.co.tt/

3. Reference Configuration

Figure 1 below illustrates the test configuration. It shows an enterprise site connected to the TSTT network through the public internet.

For confidentiality and privacy purposes, actual public IP addresses and PSTN routable phone numbers (DIDs) used during the compliance testing have been replaced with fictitious IP addresses and PSTN routable phone numbers throughout the Application Notes.

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

- Avaya IP Office v500v2.
- Avaya Session Border Controller for Enterprise.
- Avaya Voicemail Pro for IP Office.
- Avaya 9600 Series H.323 IP Telephones.
- Avaya 11x0 Series SIP IP Telephones.
- Avaya IP Office Softphone (H.323 and SIP modes).
- Avaya IP Office Phone Manager (H.323).
- Avaya 1408 Digital Telephones.
- Avaya 9508 Digital Telephones.

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 has **LAN1** port connects to the inside interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE connects to TSTT networks via the public internet.

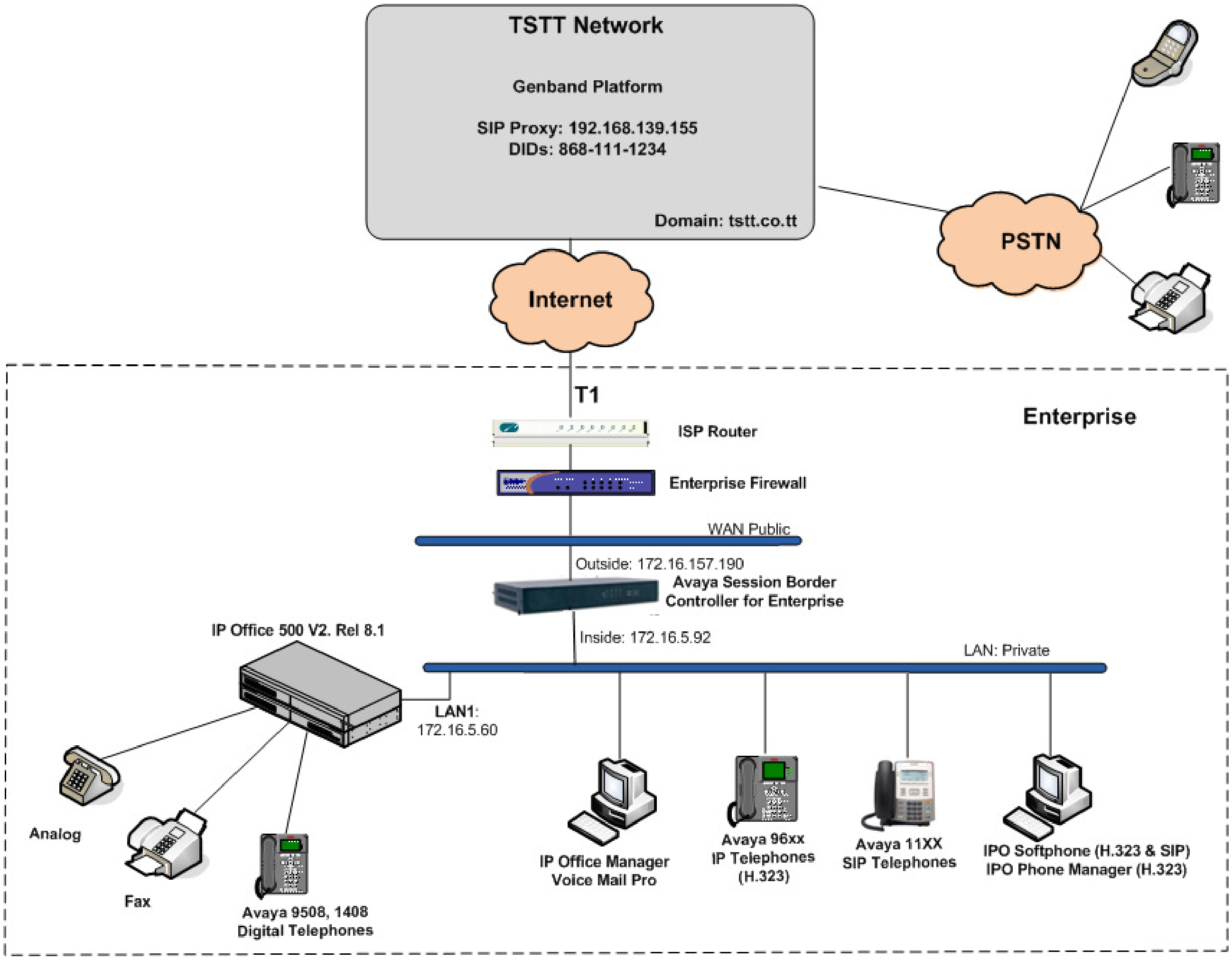

TSTT Network
Genband Platform
SIP Proxy: 192.168.139.155
DIDs: 868-111-1234
Domain: tstt.co.tt
PSTN
Internet
T1
ISP Router
Enterprise
Enterprise Firewall
WAN Public
Outside: 172.16.157.190
Avaya Session Border Controller for Enterprise
IP Office 500 V2. Rel 8.1
Inside: 172.16.5.92
LAN: Private
LAN1: 172.16.5.60
Analog
Fax
Avaya 9508, 1408 Digital Telephones
IP Office Manager Voice Mail Pro
Avaya 96xx IP Telephones (H.323)
Avaya 11XX SIP Telephones
IPO Softphone (H.323 & SIP)
IPO Phone Manager (H.323)

Figure 1: Avaya IP Telephony Network Connecting to TSTT SIP Trunking Service.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to TSTT. The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to the network. Since Trinidad and Tobago is a country member of the North American Numbering Plan (NANP), the users dialed 10 digits for local calls, including the area code, and 11 (1 + 10) digits for other calls between the NANP.

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

4. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration.

Avaya Telephony Components	
Equipment/Software	**Release/Version**
Avaya IP Office 500v2	8.1 (69)
Avaya IP Office DIG DCPx16 V2	10.1 (69)
Avaya IP Office Manager	10.1 (69)
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.2 (6.2.0.Q48)
Avaya Voicemail Pro for IP Office	8.1.9203.0
Avaya 9620 IP Telephone (H.323)	Avaya one-X® Deskphone Edition S3.2
Avaya 1140 IP Telephone (SIP)	04.03.12.00
Avaya IP Office Softphone (H.323 & SIP)	3.2.3.48 67009
Avaya IP Office Phone Manager (H.323)	4.2.42
Avaya Digital Telephones 1408	32
Avaya Digital Telephones 9508	0.45

Telecommunications Services of Trinidad and Tobago SIP Trunk Service	
Equipment/Software	**Release/Version**
Genband Softswitch	CVM13

Testing was performed with IP Office 500v2 R8.1, but it also applies to IP Office Server Edition R8.1. Note that IP Office Server Edition requires an Expansion IP Office 500 v2 R8.1 to support analog or digital endpoints or trunks.

5. Configure IP Office

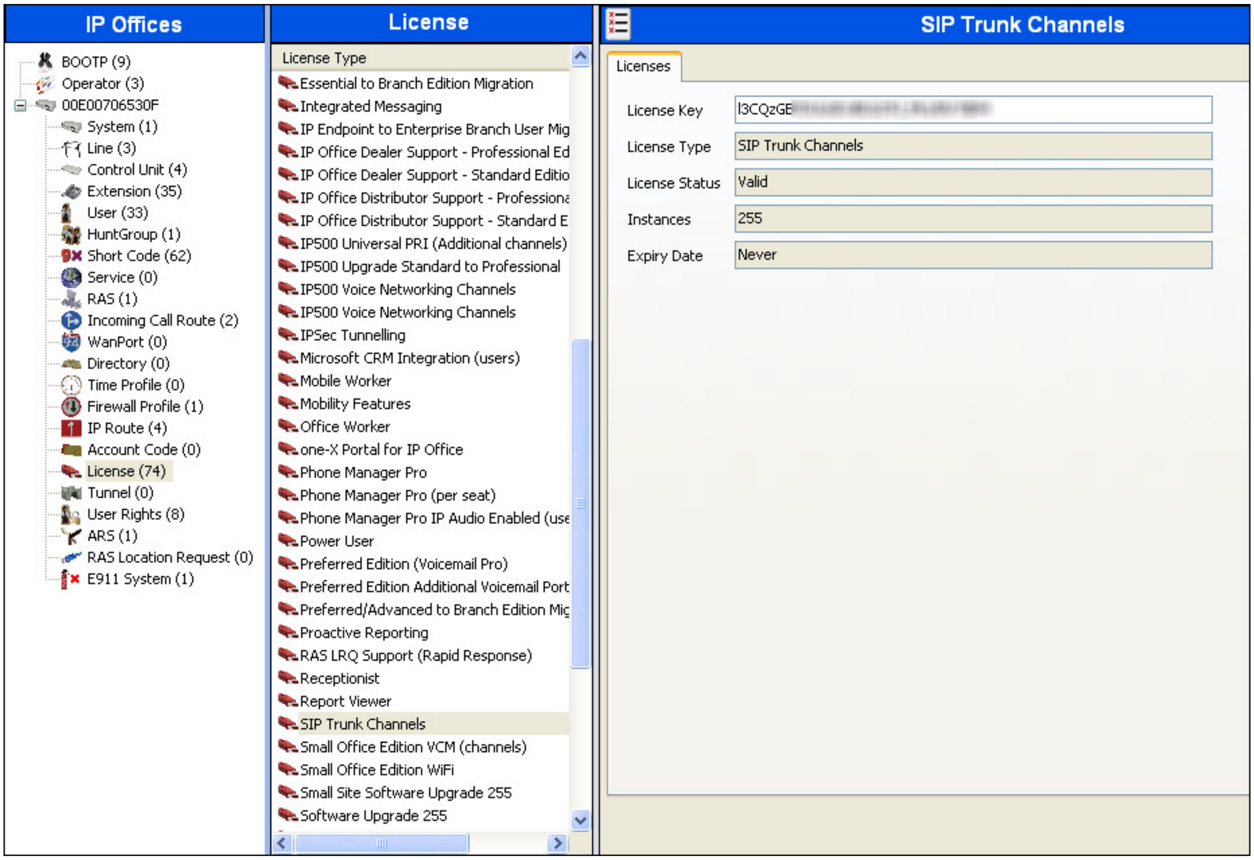
This section describes the IP Office configuration required to interwork with TSTT. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** (not shown) to launch IP Office Manager. Navigate to **File → Open Configuration** (not shown), 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 have already been completed and are not discussed here. For further information on IP Office, please consult References in **Section 10**.

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** in the Navigation pane and **SIP Trunk Channels** in the Group pane. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the Details pane. Note that the actual License Key in the screen below was edited for security purposes.



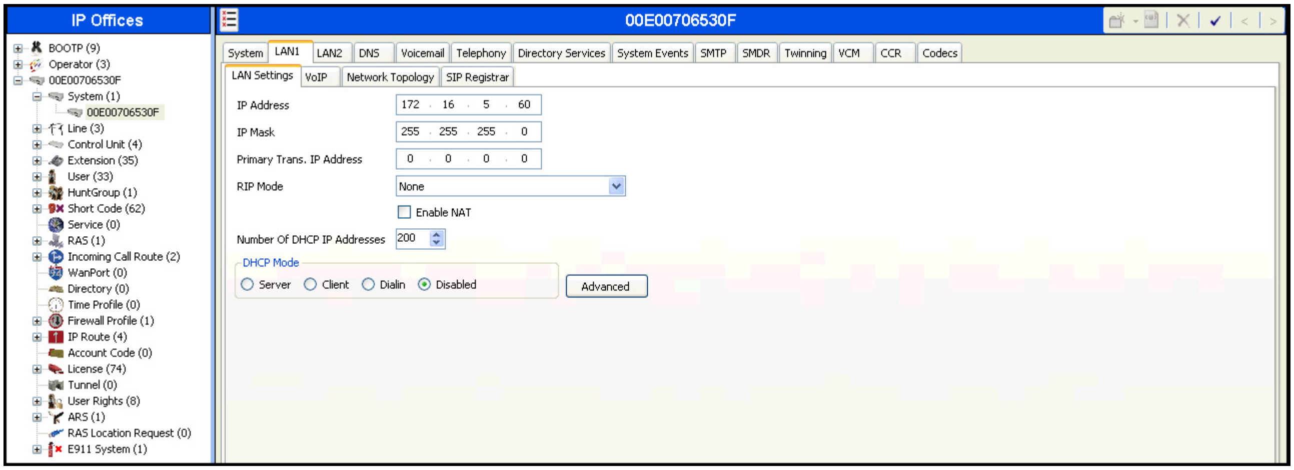
IP Offices
BOOTP (9)
Operator (3)
00E00706530F
System (1)
Line (3)
Control Unit (4)
Extension (35)
User (33)
HuntGroup (1)
Short Code (62)
Service (0)
RAS (1)
Incoming Call Route (2)
WanPort (0)
Directory (0)
Time Profile (0)
Firewall Profile (1)
IP Route (4)
Account Code (0)
License (74)
Tunnel (0)
User Rights (8)
ARS (1)
RAS Location Request (0)
E911 System (1)
License
License Type
Essential to Branch Edition Migration
Integrated Messaging
IP Endpoint to Enterprise Branch User Mig
IP Office Dealer Support - Professional Ed
IP Office Dealer Support - Standard Editio
IP Office Distributor Support - Professiona
IP Office Distributor Support - Standard E
IP500 Universal PRI (Additional channels)
IP500 Upgrade Standard to Professional
IP500 Voice Networking Channels
IP500 Voice Networking Channels
IPSec Tunnelling
Microsoft CRM Integration (users)
Mobile Worker
Mobility Features
Office Worker
one-X Portal for IP Office
Phone Manager Pro
Phone Manager Pro (per seat)
Phone Manager Pro IP Audio Enabled (use
Power User
Preferred Edition (Voicemail Pro)
Preferred Edition Additional Voicemail Port
Preferred/Advanced to Branch Edition Mig
Proactive Reporting
RAS LRQ Support (Rapid Response)
Receptionist
Report Viewer
SIP Trunk Channels
Small Office Edition VCM (channels)
Small Office Edition WiFi
Small Site Software Upgrade 255
Software Upgrade 255
SIP Trunk Channels
Licenses

License Key	I3CQzGE[redacted]
License Type	SIP Trunk Channels
License Status	Valid
Instances	255
Expiry Date	Never

5.2 LAN1 Settings

In the sample configuration, the MAC address **00E00706530F** was used as the system name and the **LAN** port connects to the inside interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE connects to TSTT networks via the public internet. 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 public network, e.g. **255.255.255.0**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown).



IP Address: 172 . 16 . 5 . 60

IP Mask: 255 . 255 . 255 . 0

Primary Trans. IP Address: 0 . 0 . 0 . 0

RIP Mode: None

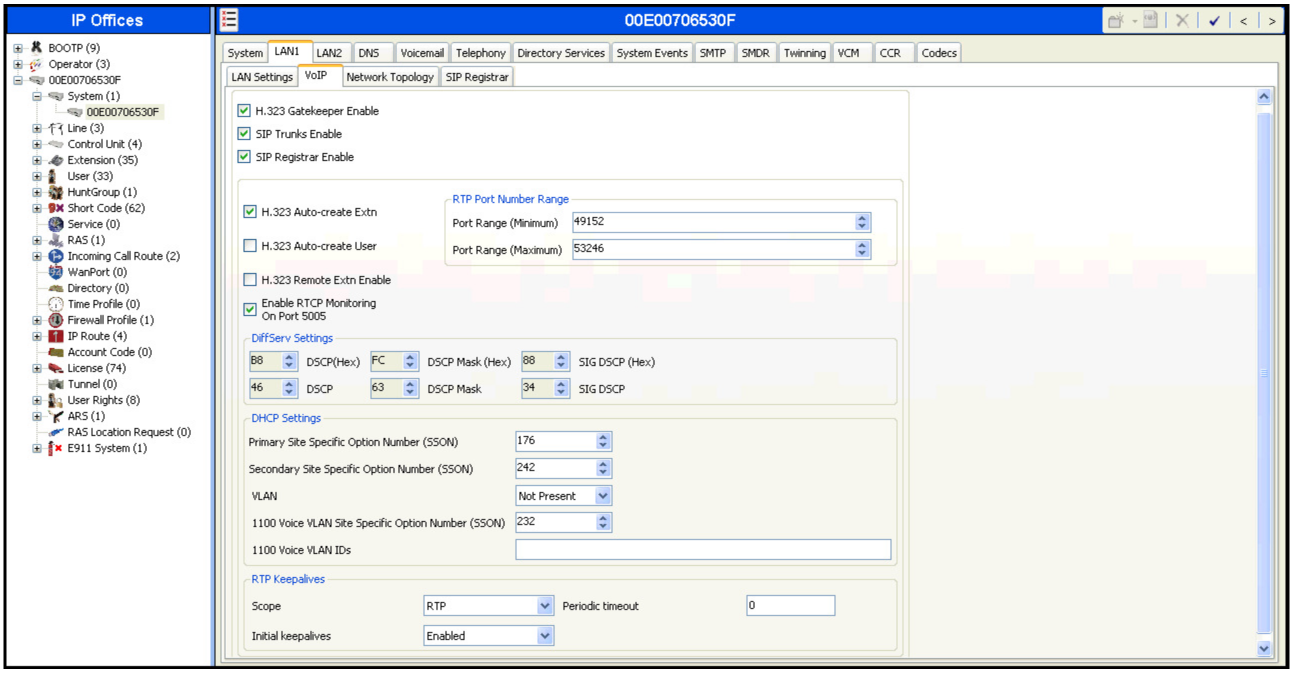
□ Enable NAT

Number Of DHCP IP Addresses: 200

DHCP Mode: ○ Server ○ Client ○ Dialin ● Disabled

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

- 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 TSTT.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- 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.
- Verify the **DiffServ Settings** were kept as default for the Differentiated Services Code Point (DSCP) parameters in the IP packet headers to support Quality of Services policies for both signaling and media, the **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling.
- In the **RTP Keepalives** section at the bottom of the page, set the **Scope** field to **RTP**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send RTP keepalive packets at the beginning of the calls, to avoid problems of media deadlock that can occur with certain types of forwarded calls that are routed from the IP Office back to the network, over the same SIP trunk.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown).



☑ H.323 Gatekeeper Enable

☑ SIP Trunks Enable

☑ SIP Registrar Enable

☑ H.323 Auto-create Extn

☐ H.323 Auto-create User

☐ H.323 Remote Extn Enable

☑ Enable RTCP Monitoring On Port 5005

RTP Port Number Range

Port Range (Minimum) 49152

Port Range (Maximum) 53246

DiffServ Settings

B8 DSCP(Hex) FC DSCP Mask (Hex) 88 SIG DSCP (Hex)

46 DSCP 63 DSCP Mask 34 SIG DSCP

DHCP Settings

Primary Site Specific Option Number (SSON) 176

Secondary Site Specific Option Number (SSON) 242

VLAN Not Present

1100 Voice VLAN Site Specific Option Number (SSON) 232

1100 Voice VLAN IDs

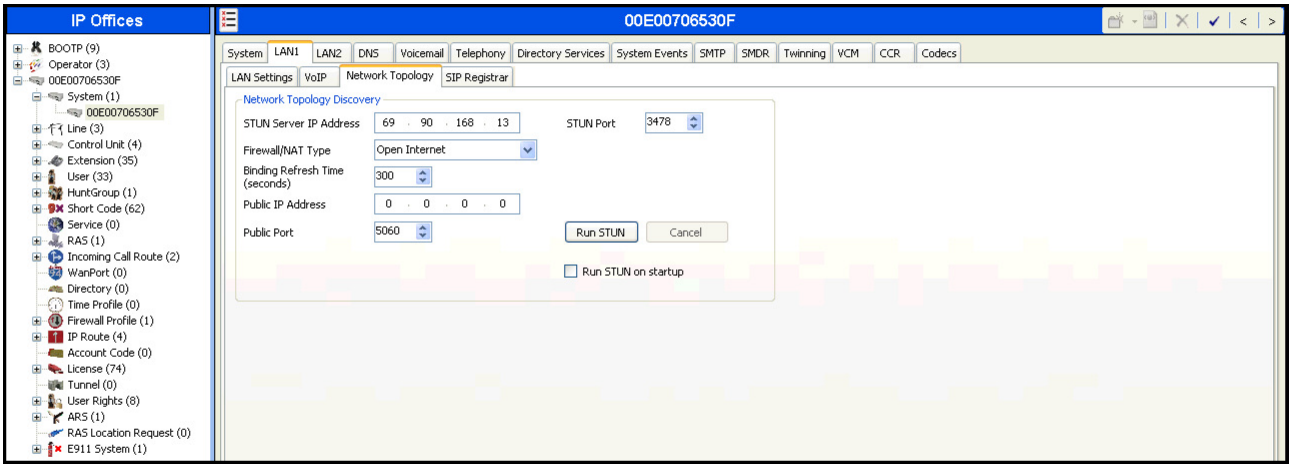
RTP Keepalives

Scope RTP Periodic timeout 0

Initial keepalives Enabled

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

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even the default STUN settings are populated but 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 heartbeat to the service provider.
- Leave the **Public IP Address** as **0.0.0.0**
- Set the **Public Port** to **5060**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown).



Network Topology Discovery

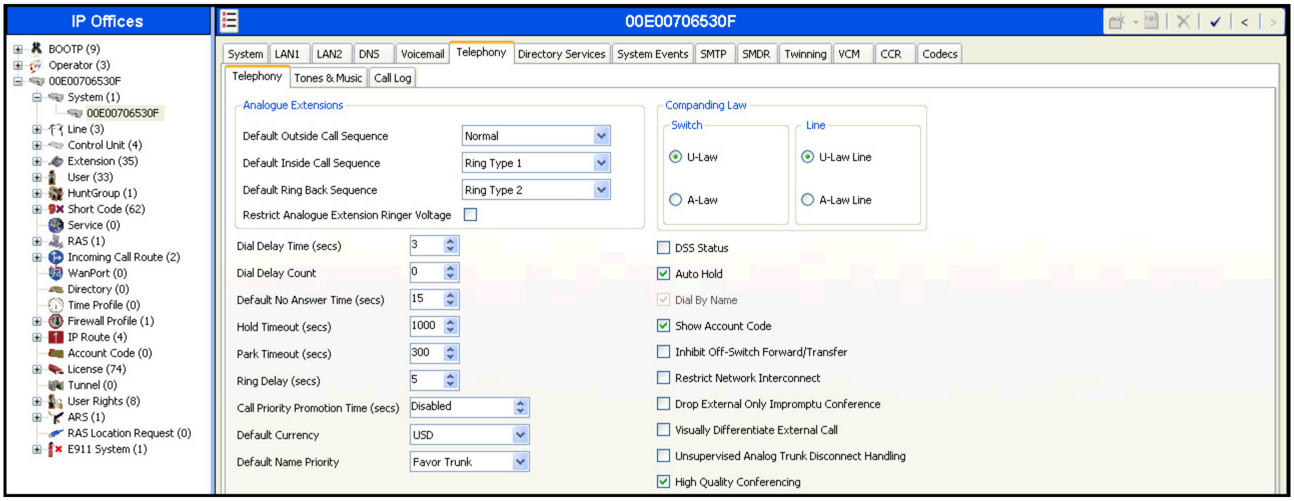
STUN Server IP Address: 69 . 90 . 168 . 13
STUN Port: 3478
Firewall/NAT Type: Open Internet
Binding Refresh Time (seconds): 300
Public IP Address: 0 . 0 . 0 . 0
Public Port: 5060
☐ Run STUN on startup

In the compliance test, the **LAN1** interface was used to connect Avaya IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.3 System Telephony Settings

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.
- Click OK to commit (not shown).



Analogue Extensions

Default Outside Call Sequence: Normal

Default Inside Call Sequence: Ring Type 1

Default Ring Back Sequence: Ring Type 2

Restrict Analogue Extension Ringer Voltage □

Companding Law

Switch: ● U-Law ○ A-Law

Line: ● U-Law Line ○ A-Law Line

Dial Delay Time (secs): 3

Dial Delay Count: 0

Default No Answer Time (secs): 15

Hold Timeout (secs): 1000

Park Timeout (secs): 300

Ring Delay (secs): 5

Call Priority Promotion Time (secs): Disabled

Default Currency: USD

Default Name Priority: Favor Trunk

□ DSS Status

☑ Auto Hold

☑ Dial By Name

☑ Show Account Code

□ Inhibit Off-Switch Forward/Transfer

□ Restrict Network Interconnect

□ Drop External Only Impromptu Conference

□ Visually Differentiate External Call

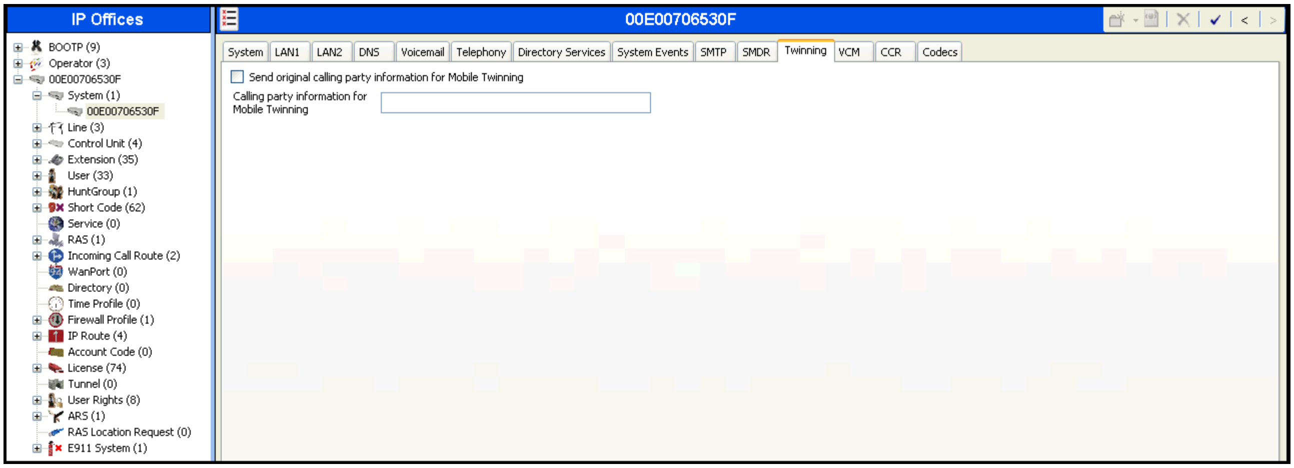
□ Unsupervised Analog Trunk Disconnect Handling

☑ High Quality Conferencing

5.4 Twinning Calling Party Settings

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 5.7**). This setting also impacts the Caller ID for call forwarding.
- Click OK to commit (not shown).



□ Send original calling party information for Mobile Twinning

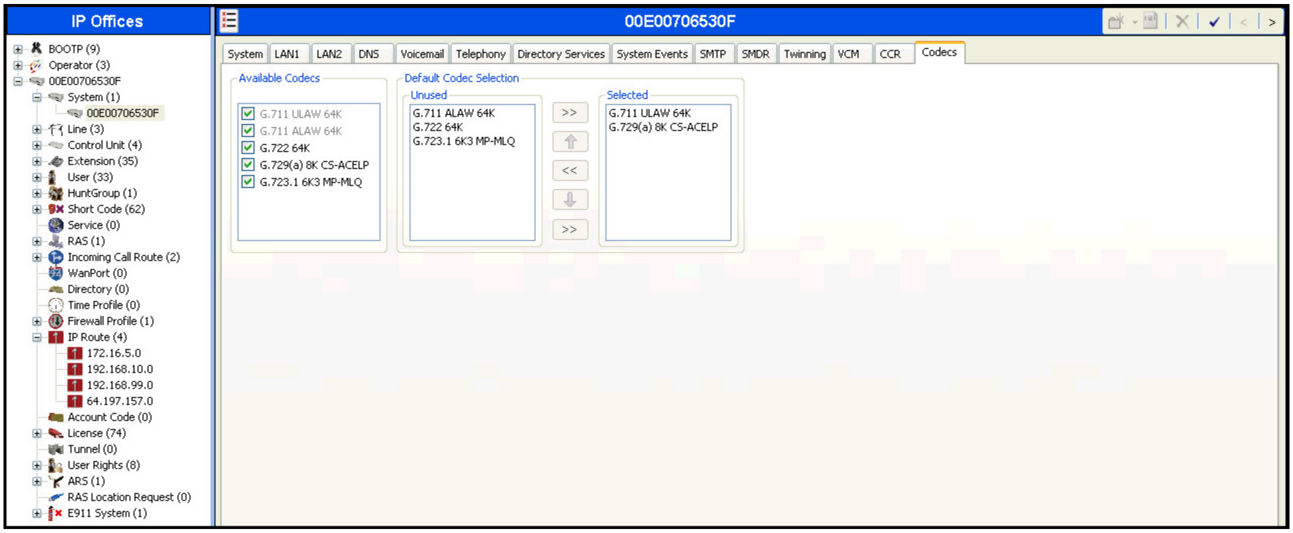
Calling party information for Mobile Twinning:

5.5 Codec’s settings

For **Codec’s** settings, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, configure the following parameters:

- Select the **Codecs**.
- Click OK to commit (not shown).

The **Codec’s** settings are shown in the screenshot below with G.711ULAW and G.729(a) were selected in prioritized order. During the compliance testing, only codec G.711ULAW was tested (For Codec G.729A Test Results refer to **Section 2.2**).



Available Codecs

☑ G.711 ULAW 64K
☑ G.711 ALAW 64K
☑ G.722 64K
☑ G.729(a) 8K CS-ACELP
☑ G.723.1 6K3 MP-MLQ

Default Codec Selection

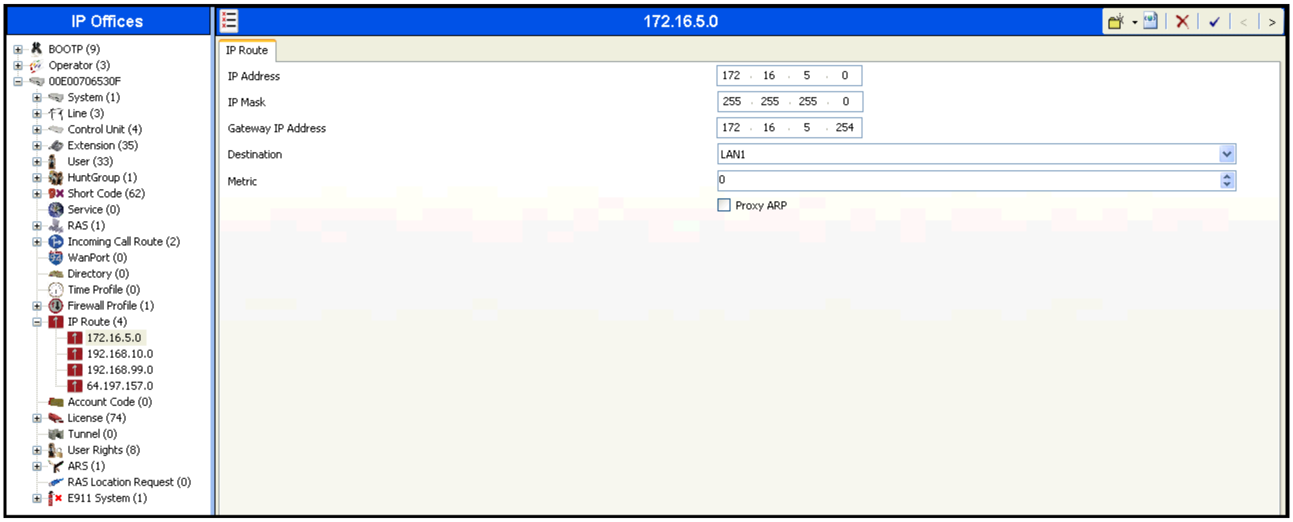
Unused:
G.711 ALAW 64K
G.722 64K
G.723.1 6K3 MP-MLQ

Selected:
G.711 ULAW 64K
G.729(a) 8K CS-ACELP

5.6 IP Route

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 subnet where the SIP proxy is located on the TSTT network. On the left navigation pane, right-click on **IP Route** and select **New**.

- Set the **IP Address** and **IP Mask** of LAN1 connecting to the Avaya SBCE for SIP and RTP traffics to TSTT.
- Set **Gateway IP Address** to the IP Address of the router used to reach the external network.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click OK to commit (not shown).



IP Address: 172 . 16 . 5 . 0
IP Mask: 255 . 255 . 255 . 0
Gateway IP Address: 172 . 16 . 5 . 254
Destination: LAN1
Metric: 0
□ Proxy ARP

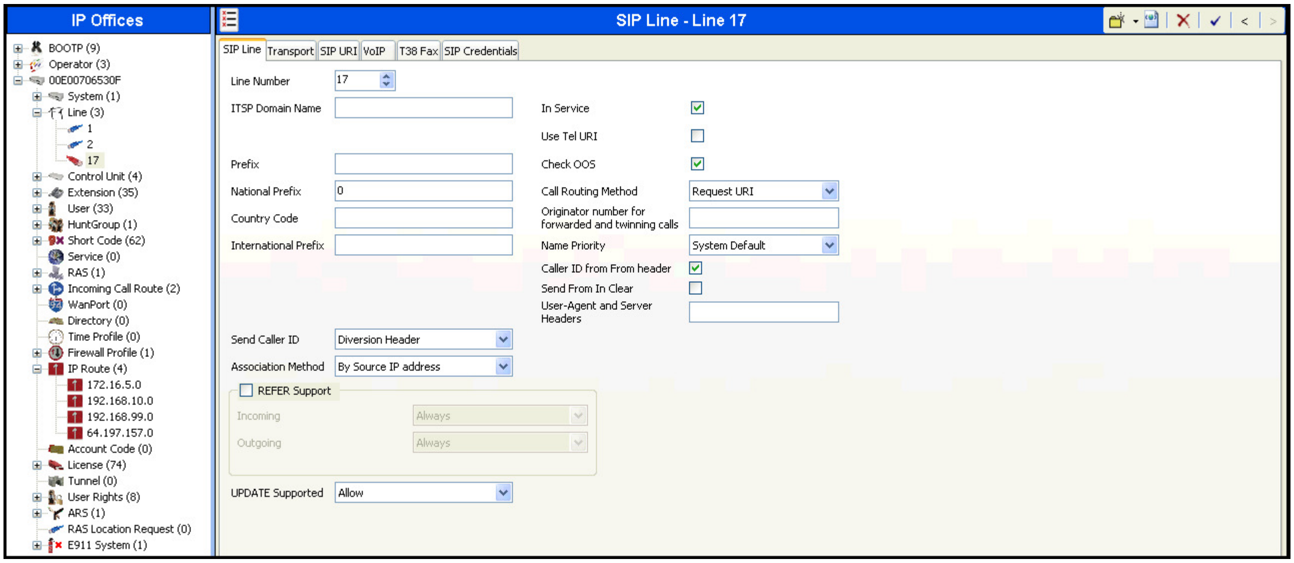
5.7 Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the TSTT SIP Trunk Service. To create a SIP line, begin by navigating to **Line** in the Navigation Pane. Right-click and select **New→ SIP Line** (not shown).

5.7.1 SIP Line Tab

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

- Leave the **ITSP Domain Name** blank.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Set **Call Routing Method** to **Request URI**.
- Check the **Caller ID from From header** box.
- Set **Send Caller ID** to **Diversion Header.**
- Uncheck the **REFER support** box. IP Office will not send REFER messages for calls that are transferred back to the PSTN. See **Section 2.2** for more information.
- Set **UPDATE Supported** to **Allow**.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

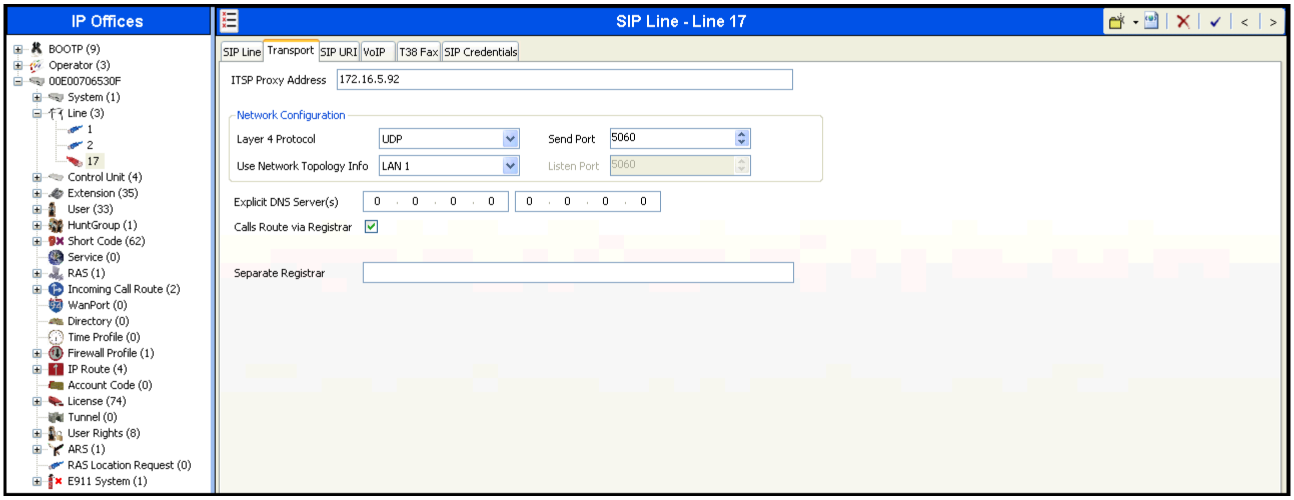


Line Number: 17
ITSP Domain Name:
In Service: ☑
Use Tel URI: ☐
Prefix:
Check OOS: ☑
National Prefix: 0
Call Routing Method: Request URI
Country Code:
Originator number for forwarded and twinning calls:
International Prefix:
Name Priority: System Default
Caller ID from From header: ☑
Send From In Clear: ☐
User-Agent and Server Headers:
Send Caller ID: Diversion Header
Association Method: By Source IP address
☐ REFER Support
Incoming: Always
Outgoing: Always
UPDATE Supported: Allow

5.7.2 Transport Tab

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

- Set the **ITSP Proxy Address** was set to the inside IP Address of the Avaya SBCE **172.16.5.92** as shown in **Figure 1**.
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).



ITSP Proxy Address 172.16.5.92

Network Configuration

Layer 4 Protocol UDP

Send Port 5060

Use Network Topology Info LAN 1

Listen Port 5060

Explicit DNS Server(s) 0 . 0 . 0 . 0 0 . 0 . 0 . 0

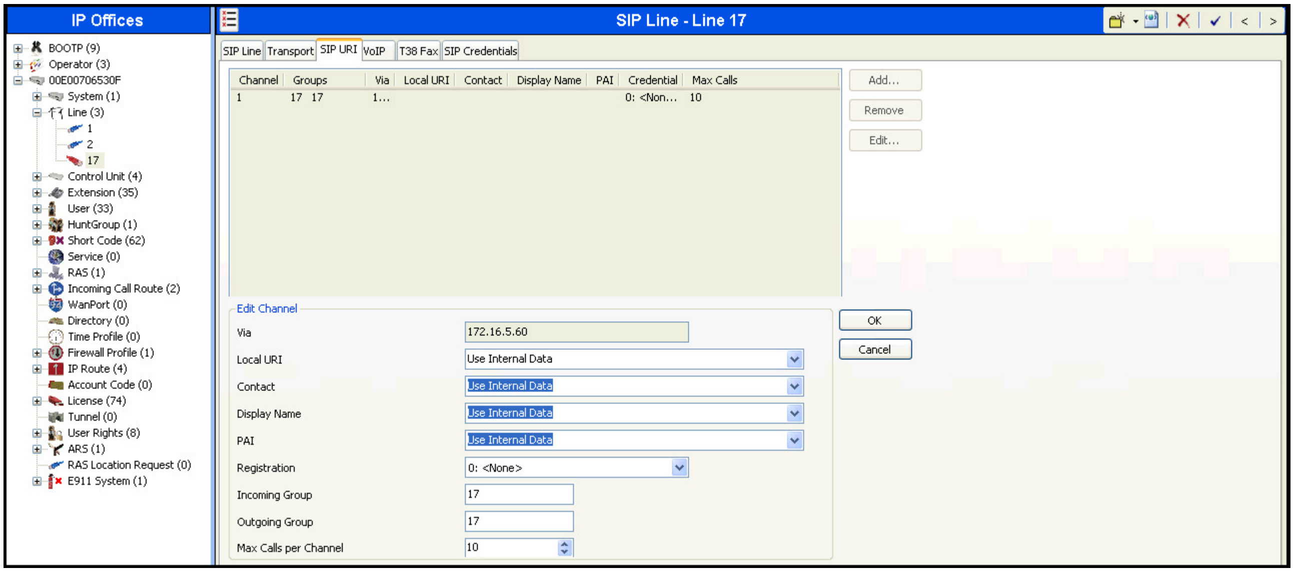
Calls Route via Registrar ☑

Separate Registrar

5.7.3 SIP URI Tab

A SIP URI entry needs to be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab, and then click the **Add** button (not shown) 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. In the example screen below, a previously configured entry was edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact, Display Name and PAI** to **Use Internal Data**. This setting allows calls on this line whose SIP URI match the number set in the **SIP** tab of any User as shown in **Section 5.9**.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click OK to commit (not shown).



Channel	Groups		Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	17	17	1...					0: <Non...	10

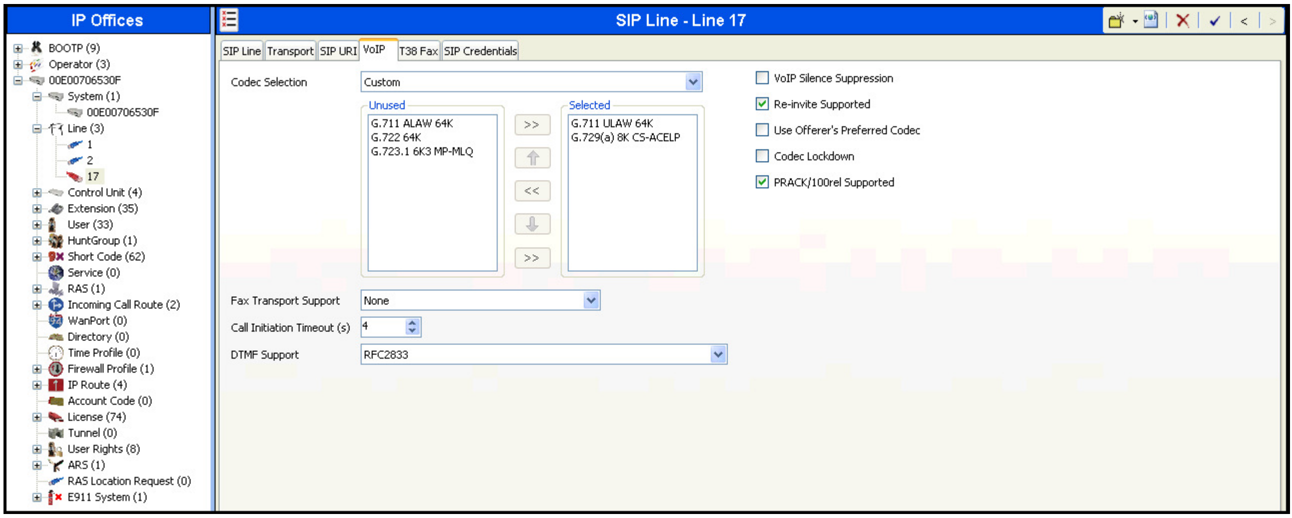
Edit Channel

Via	172.16.5.60
Local URI	Use Internal Data
Contact	Use Internal Data
Display Name	Use Internal Data
PAI	Use Internal Data
Registration	0: <None>
Incoming Group	17
Outgoing Group	17
Max Calls per Channel	10

5.7.4 VoIP Tab

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

- In the sample configuration, the **Codec Selection** was configured using the **Custom** option, allowing an explicit ordered list of codec's to be specified. The buttons allow setting the specific order of preference for the codec's to be used on the line, as shown. TSTT supports codec's G.711MU and G.729A, during the compliance testing, only codec G.711ULAW was tested (For Codec G.729A Test Results refer to **Section 2.2**).
- Set **Fax Transport Support** to **None**. **T.38 or G.711** fax transports **are not** recommended for this solution, as described in **Section 2.2**.
- Set the **DTMF Support** field to **RFC2833.** This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of 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 provisional responses and Early Media to TSTT.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).



Codec Selection: Custom

Unused	Selected
G.711 ALAW 64K	G.711 ULAW 64K
G.722 64K	G.729(a) 8K CS-ACELP
G.723.1 6K3 MP-MLQ	

Fax Transport Support: None

Call Initiation Timeout (s): 4

DTMF Support: RFC2833

□ VoIP Silence Suppression

☑ Re-invite Supported

□ Use Offerer's Preferred Codec

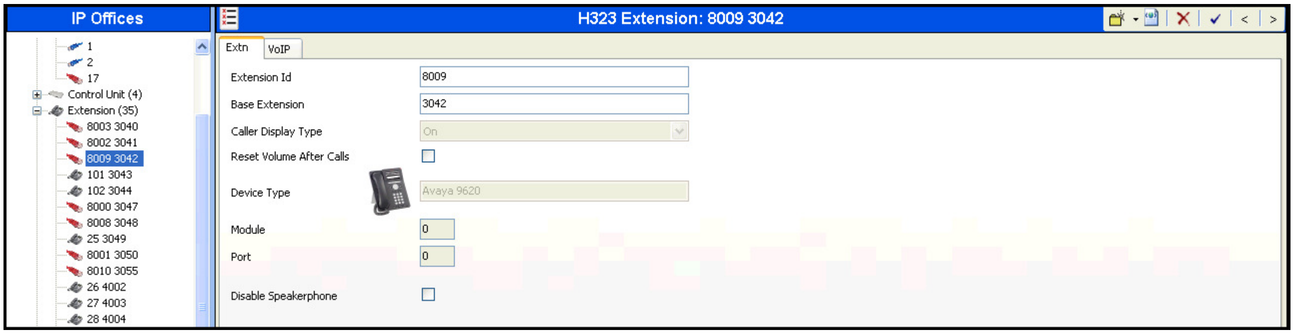
□ Codec Lockdown

☑ PRACK/100rel Supported

5.8 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** (not shown)**.**

Select the **Extn** tab. Following is an example of extension 3042; this extension corresponds to an H.323 extension.



IP Offices

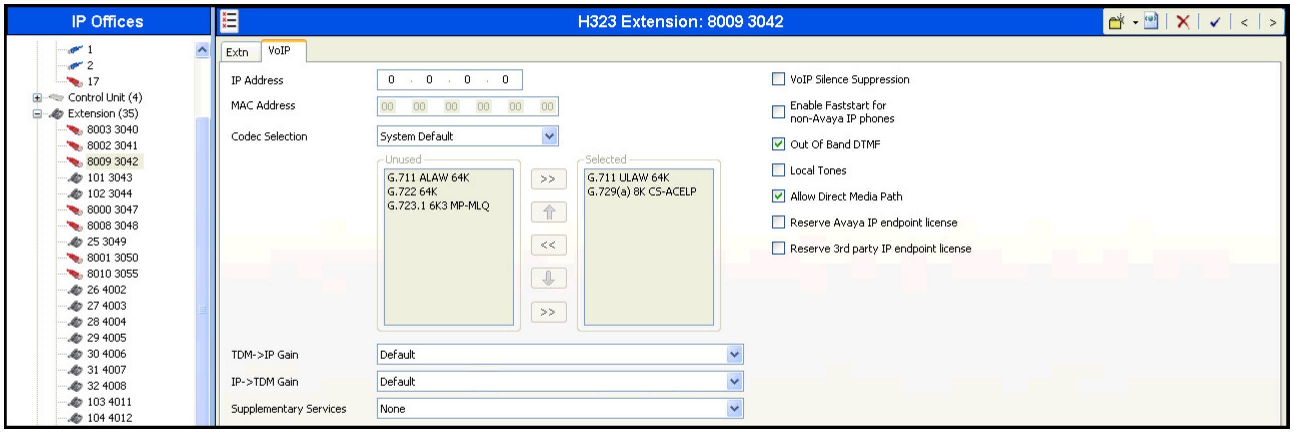
- 1
- 2
- 17
- Control Unit (4)
- Extension (35)
  - 8003 3040
  - 8002 3041
  - 8009 3042
  - 101 3043
  - 102 3044
  - 8000 3047
  - 8008 3048
  - 25 3049
  - 8001 3050
  - 8010 3055
  - 26 4002
  - 27 4003
  - 28 4004

H323 Extension: 8009 3042

Extn | VoIP

Extension Id	8009
Base Extension	3042
Caller Display Type	On
Reset Volume After Calls	□
Device Type	Avaya 9620
Module	0
Port	0
Disable Speakerphone	□

Select the **VOIP** tab. Use default values on VoIP tab. Following is an example for Extension 3042; this extension corresponds to an H.323 extension.



IP Offices

- 1
- 2
- 17
- Control Unit (4)
- Extension (35)
  - 8003 3040
  - 8002 3041
  - 8009 3042
  - 101 3043
  - 102 3044
  - 8000 3047
  - 8008 3048
  - 25 3049
  - 8001 3050
  - 8010 3055
  - 26 4002
  - 27 4003
  - 28 4004
  - 29 4005
  - 30 4006
  - 31 4007
  - 32 4008
  - 103 4011
  - 104 4012

H323 Extension: 8009 3042

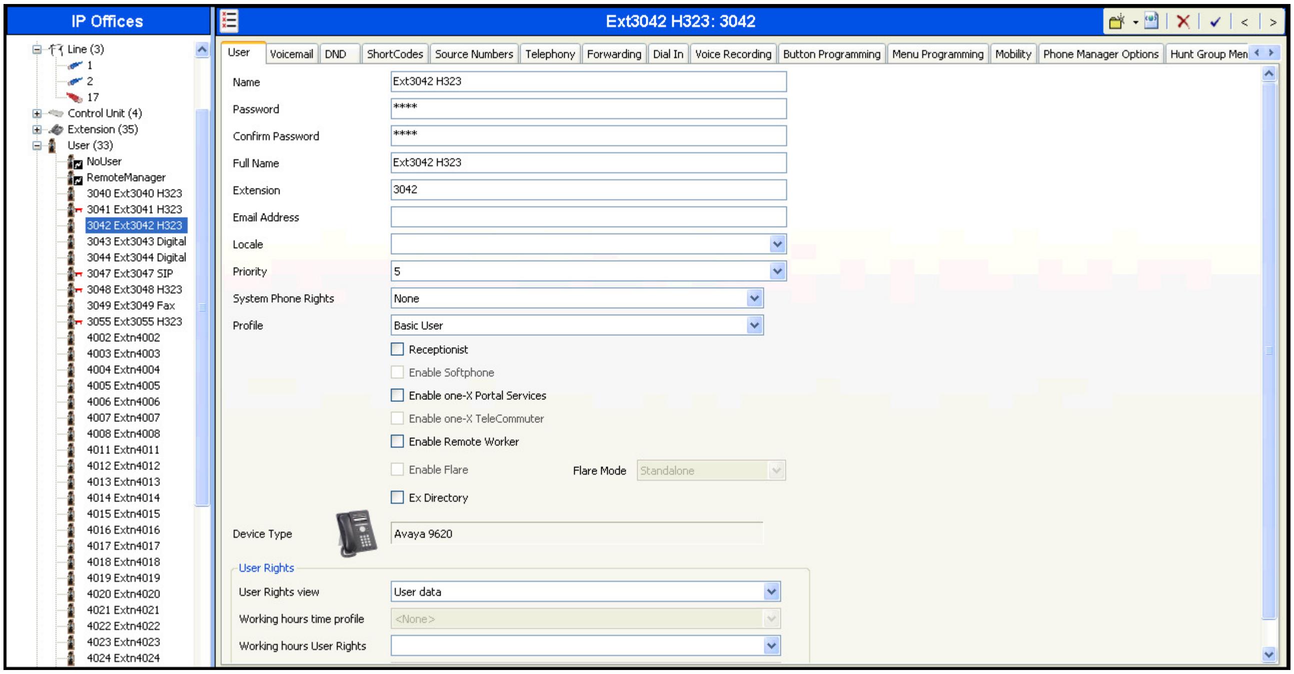
Extn | VoIP

IP Address	0 . 0 . 0 . 0
MAC Address	00 00 00 00 00 00
Codec Selection	System Default
Unused	G.711 ALAW 64K G.722 64K G.723.1 6K3 MP-MLQ
Selected	G.711 ULAW 64K G.729(a) 8K CS-ACELP
TDM->IP Gain	Default
IP->TDM Gain	Default
Supplementary Services	None

- □ VoIP Silence Suppression
- □ Enable Faststart for non-Avaya IP phones
- ☑ Out Of Band DTMF
- □ Local Tones
- ☑ Allow Direct Media Path
- □ Reserve Avaya IP endpoint license
- □ Reserve 3rd party IP endpoint license

5.9 Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.7**. 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 center Group Pane. In the example below, the name of the user is **Ext3042 H323**.



Ext3042 H323: 3042

Name	Ext3042 H323
Password	****
Confirm Password	****
Full Name	Ext3042 H323
Extension	3042
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Basic User

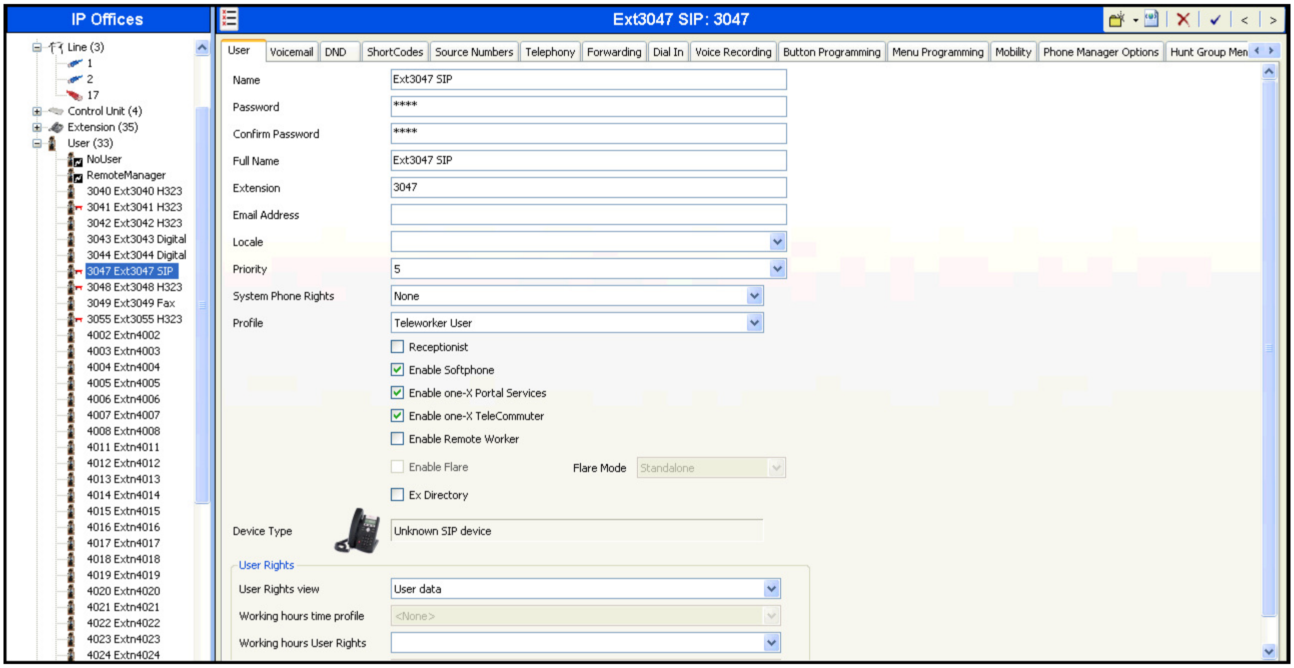
□ Receptionist
□ Enable Softphone
□ Enable one-X Portal Services
□ Enable one-X TeleCommuter
□ Enable Remote Worker
□ Enable Flare   Flare Mode Standalone
□ Ex Directory

Device Type: Avaya 9620

User Rights

User Rights view	User data
Working hours time profile	<None>
Working hours User Rights	

In the example below, the name of the user is “Ext3047 SIP”. This is an Avaya IP Office SIP Softphone user, set the Profile to **Teleworker User** and check **Enable Softphone**.



Ext3047 SIP: 3047

Name	Ext3047 SIP
Password	****
Confirm Password	****
Full Name	Ext3047 SIP
Extension	3047
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Teleworker User

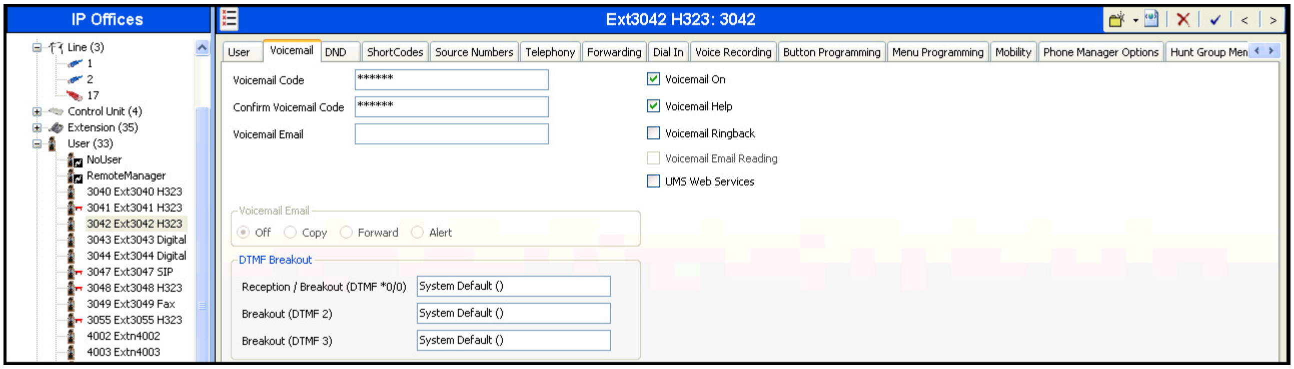
□ Receptionist
☑ Enable Softphone
☑ Enable one-X Portal Services
☑ Enable one-X TeleCommuter
□ Enable Remote Worker
□ Enable Flare   Flare Mode Standalone
□ Ex Directory

Device Type: Unknown SIP device

User Rights

User Rights view	User data
Working hours time profile	<None>
Working hours User Rights	

Select the **Voice Mail** tab. The following screen shows the **Voicemail** tab for the user with extension 3042. 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 TSTT SIP Trunk 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.



Ext3042 H323: 3042

Voicemail Code	******
Confirm Voicemail Code	******
Voicemail Email	

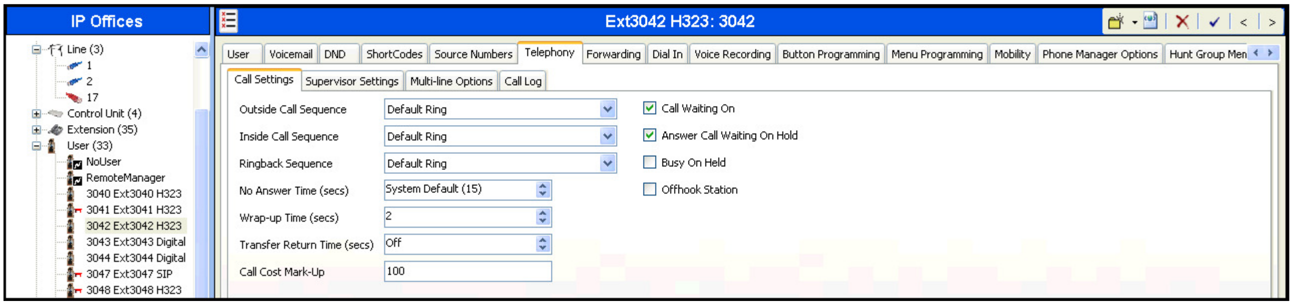
☑ Voicemail On
☑ Voicemail Help
☐ Voicemail Ringback
☐ Voicemail Email Reading
☐ UMS Web Services

Voicemail Email
● Off ○ Copy ○ Forward ○ Alert

DTMF Breakout

Reception / Breakout (DTMF *0/0)	System Default ()
Breakout (DTMF 2)	System Default ()
Breakout (DTMF 3)	System Default ()

Select the **Telephony** tab, then **Call Settings** tab as shown below. Check the **Call Waiting On** box to allow an Avaya IP Office phone logged in as this extension to have multiple call appearances. Note: **Call Waiting On** is necessary for call transfer.

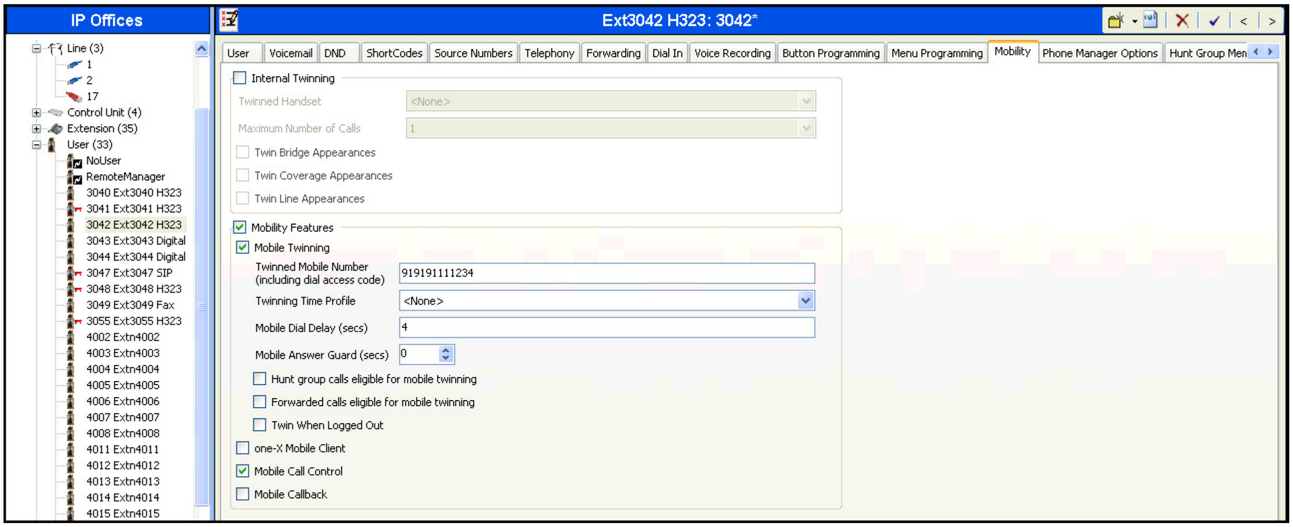

IP Offices
Line (3)
1
2
17
Control Unit (4)
Extension (35)
User (33)
NoUser
RemoteManager
3040 Ext3040 H323
3041 Ext3041 H323
3042 Ext3042 H323
3043 Ext3043 Digital
3044 Ext3044 Digital
3047 Ext3047 SIP
3048 Ext3048 H323
User | Voicemail | DND | ShortCodes | Source Numbers | Telephony | Forwarding | Dial In | Voice Recording | Button Programming | Menu Programming | Mobility | Phone Manager Options | Hunt Group Men
Call Settings | Supervisor Settings | Multi-line Options | Call Log

Ext3042 H323: 3042

Outside Call Sequence	Default Ring
Inside Call Sequence	Default Ring
Ringback Sequence	Default Ring
No Answer Time (secs)	System Default (15)
Wrap-up Time (secs)	2
Transfer Return Time (secs)	Off
Call Cost Mark-Up	100

☑ Call Waiting On
☑ Answer Call Waiting On Hold
☐ Busy On Held
☐ Offhook Station

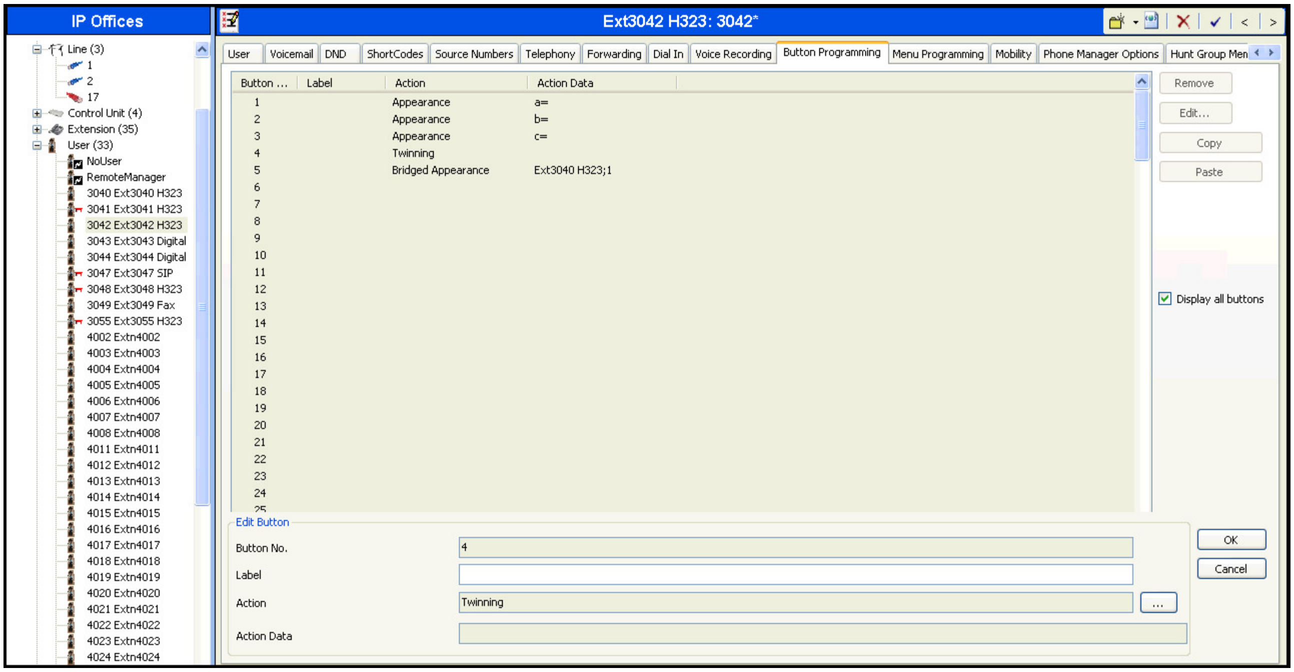
Select the **Mobility** tab. In the sample configuration user 3042 was one of the users configured to test the Mobile Twinning feature. The following screen shows the **Mobility** tab for User 3042. The **Mobility Features** and **Mobile Twinning** boxes are checked**.** The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned telephone, in this case **919191111234**. Other options can be set according to customer requirements.



Ext3042 H323: 3042*

- □ Internal Twinning
  - Twinned Handset: <None>
  - Maximum Number of Calls: 1
  - □ Twin Bridge Appearances
  - □ Twin Coverage Appearances
  - □ Twin Line Appearances
- ☑ Mobility Features
  - ☑ Mobile Twinning
  - Twinned Mobile Number (including dial access code): 919191111234
  - Twinning Time Profile: <None>
  - Mobile Dial Delay (secs): 4
  - Mobile Answer Guard (secs): 0
  - □ Hunt group calls eligible for mobile twinning
  - □ Forwarded calls eligible for mobile twinning
  - □ Twin When Logged Out
  - □ one-X Mobile Client
  - ☑ Mobile Call Control
  - □ Mobile Callback

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 → Emulation → Twinning** (not shown). In the sample below, button **4** was programmed to turn Mobile Twinning on and off on user 3042.



Button ...	Label	Action	Action Data
1		Appearance	a=
2		Appearance	b=
3		Appearance	c=
4		Twinning	
5		Bridged Appearance	Ext3040 H323;1
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

☑ Display all buttons

Edit Button

Button No. 4

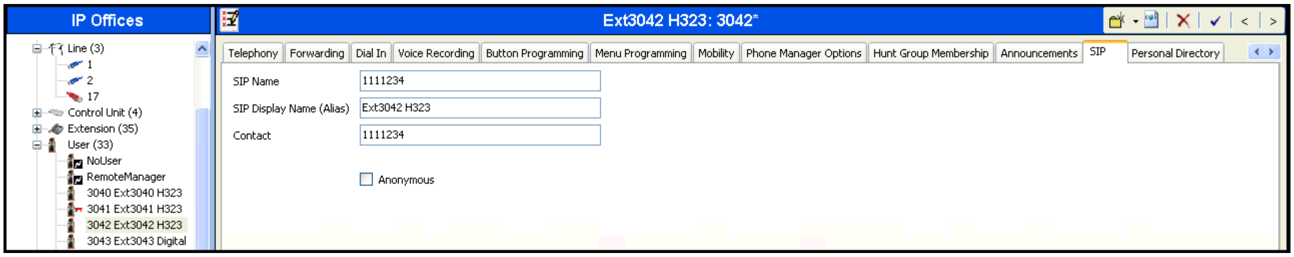
Label

Action Twinning

Action Data

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 5.7**). The example below shows the settings for user "Ext3042 H323". The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by TSTT. In the example, DID number **1111234** was used. Only the last seven digits of the DID were assigned since TSTT only sends seven digits without the area code (868). 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.



SIP Name 1111234

SIP Display Name (Alias) Ext3042 H323

Contact 1111234

☐ Anonymous

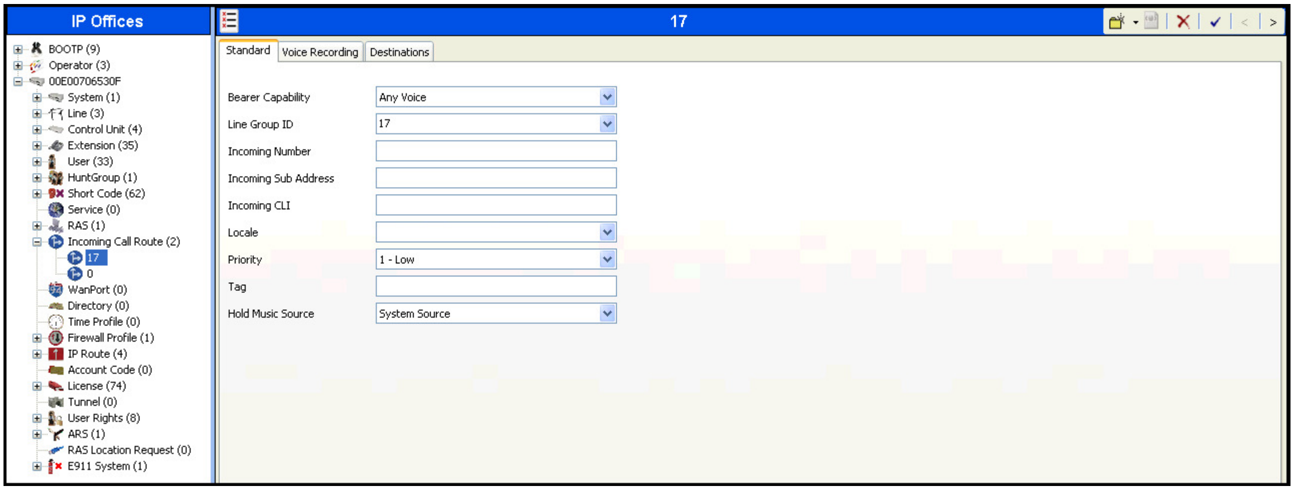
5.10 Incoming Call Route

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. Incoming call routes should be defined for each DID number assigned by the service provider.

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 5.7)** and the users **SIP Name** and **Contact**, already populated with the assigned TSTT DID numbers **(Section 5.9)**

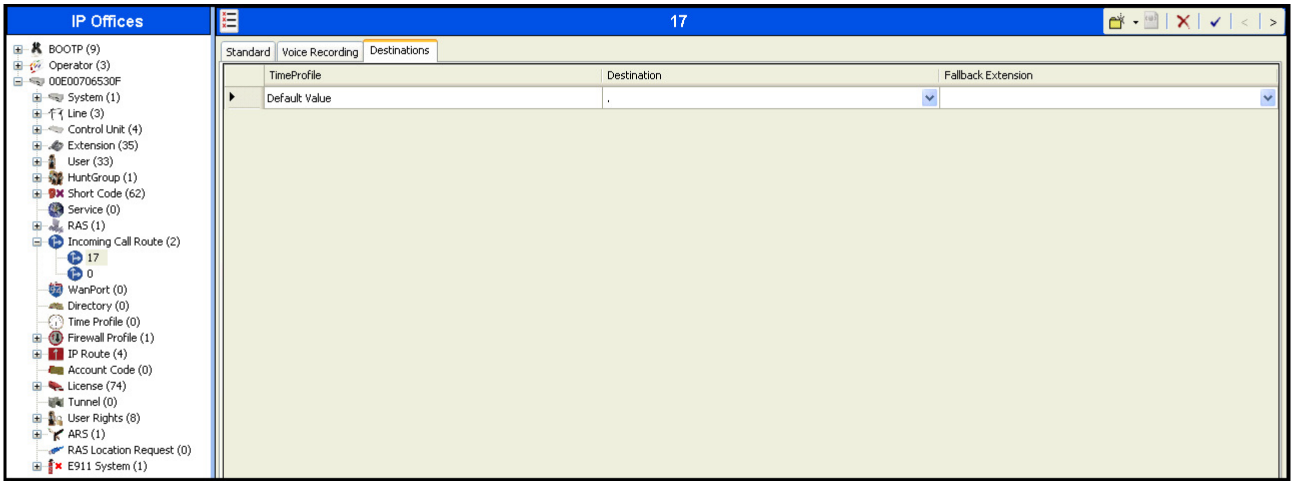
From the left Navigation Pane, right-click on **Incoming Call Route** and select **New** (not shown)**.** On the Details Pane, under the **Standard** tab, set the parameters as show bellow:

- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.7**.
- Default values may be used for all other parameters.



Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source

- Under the **Destinations** tab, enter "**.**" for the **Default Value**. 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.



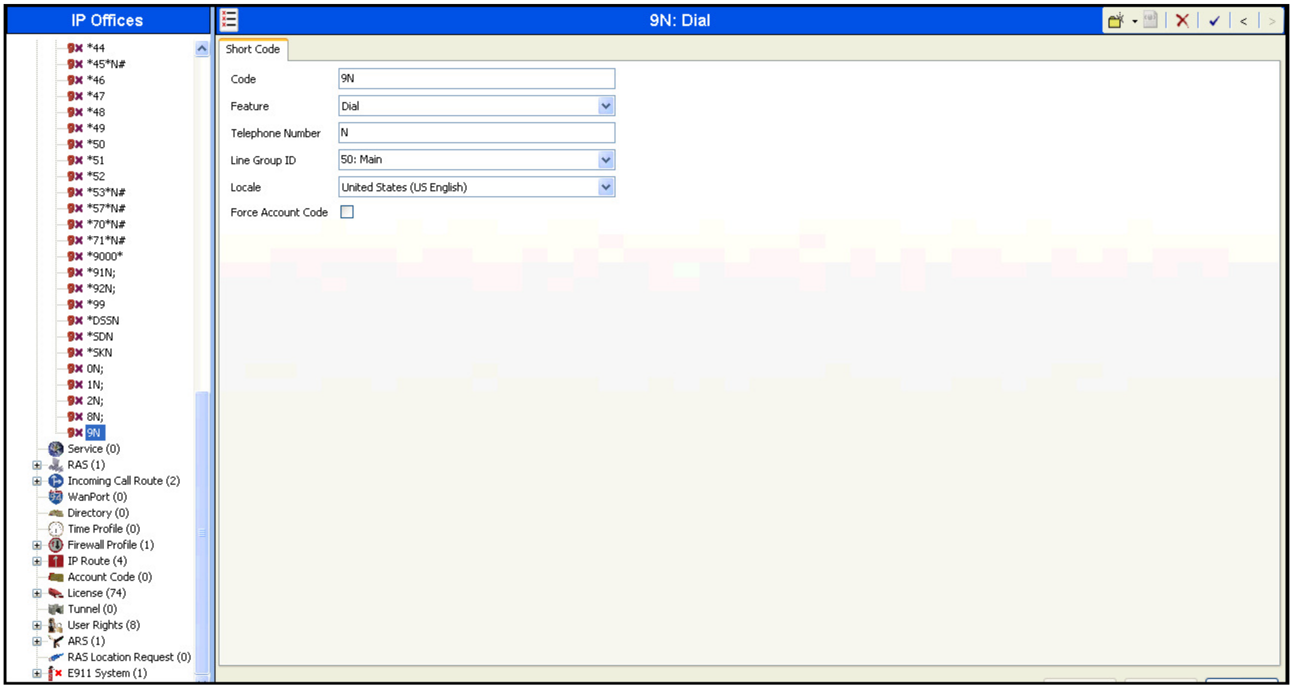
TimeProfile	Destination	Fallback Extension
Default Value	.	

5.11 Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. While detailed coverage of ARS is beyond the scope of these Application Notes and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance test

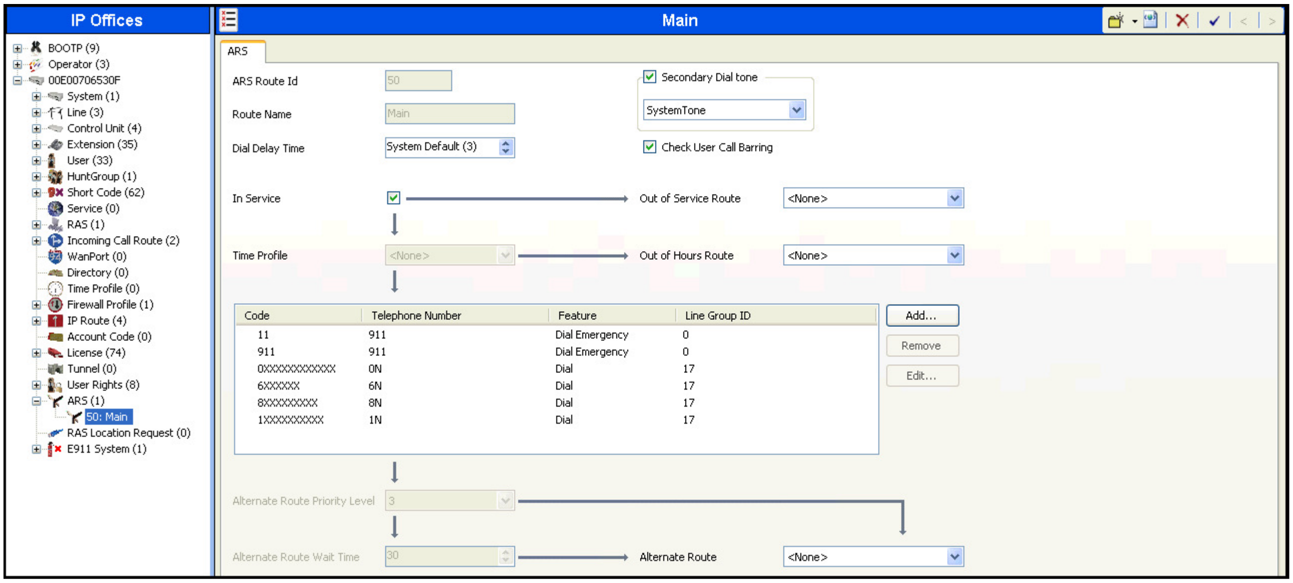
5.11.1 Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code** (not shown) in the Navigation Pane and select **New** (not shown). 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.



Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	50: Main
Locale	United States (US English)
Force Account Code	□

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 digit on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office. The example below shows that for local calls, the user dialed 9, then 10 digit numbers starting with an 8. For calls to other area codes in the North American Numbering Plan, the user dialed 9, followed by 11 digits, starting with a 1.



ARS Route Id: 50

Route Name: Main

Dial Delay Time: System Default (3)

☑ Secondary Dial tone: SystemTone

☑ Check User Call Barring

In Service: ☑

Out of Service Route: <None>

Time Profile: <None>

Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
0XXXXXXXXXXXX	0N	Dial	17
6XXXXXX	6N	Dial	17
8XXXXXXXXX	8N	Dial	17
1XXXXXXXXXX	1N	Dial	17

Alternate Route Priority Level: 3

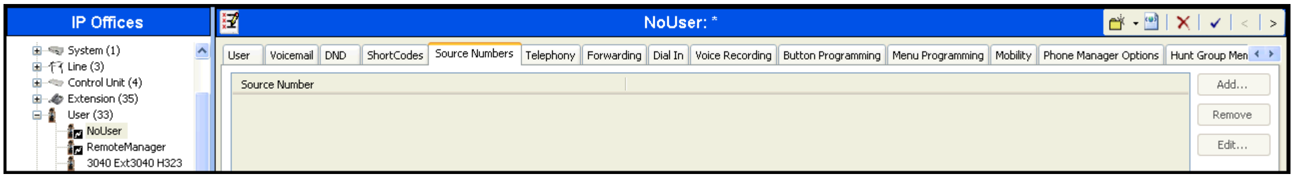
Alternate Route Wait Time: 30

Alternate Route: <None>

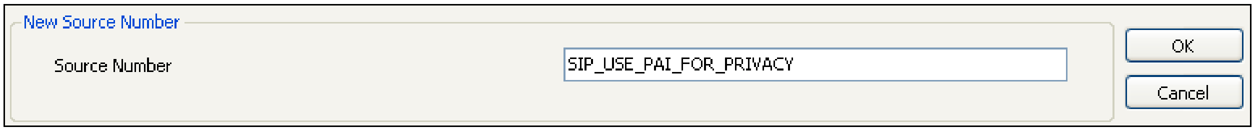
5.12 Privacy/Anonymous Calls

For outbound calls with privacy (anonymous) enabled, Avaya IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with “restricted” and “anonymous” respectively. Avaya 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. By default, Avaya IP Office will use PPI for privacy. For the compliance test, PAI was used for the purposes of privacy.

To configure Avaya IP Office to use PAI for privacy calls, navigate to **User → NoUser** in the Navigation Pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.

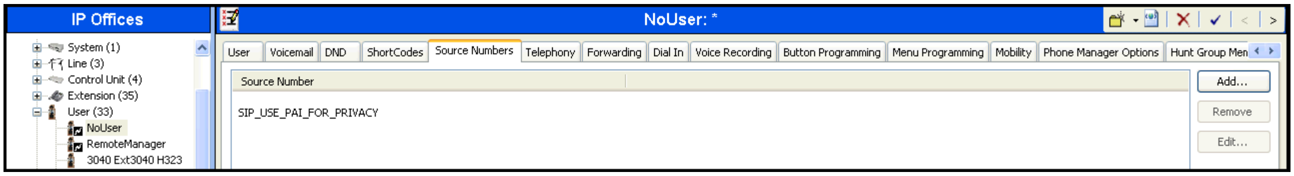


At the bottom of the Details Pane, the **Source Number** field will appear. Enter **SIP_USE_PAI_FOR_PRIVACY**. Click **OK**.



Source Number: SIP_USE_PAI_FOR_PRIVACY

The **SIP_USE_PAI_FOR_PRIVACY** parameter will appear in the list of Source Numbers as shown below.



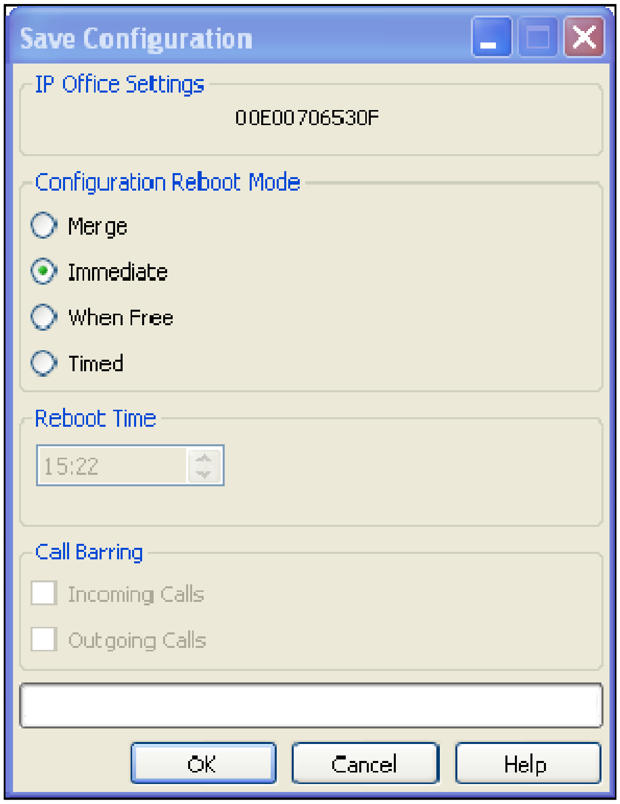
Source Number
SIP_USE_PAI_FOR_PRIVACY

5.13 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** (not shown) 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.



Save Configuration

IP Office Settings

00E00706530F

Configuration Reboot Mode

○ Merge
● Immediate
○ When Free
○ Timed

Reboot Time

15:22

Call Barring

□ Incoming Calls
□ Outgoing Calls

6. Configure the Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the software has already been installed. For additional information on these configuration tasks, see **References** [**4**], [**5**] and [**6**] in **Section 10**.

The configuration of the Avaya SBCE covers two major components, the Trunk Server for the service provider and Call Server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration was defined using the Avaya SBCE web user interface as described in the following sections.

Trunk Server configuration elements for the service provider - TSTT:

- Global Profiles:
    - URI Groups
    - Routing
    - Topology Hiding
    - Server Interworking
    - Signaling Manipulation
    - Server Configuration
- Domain Policies:
    - Application Rules
    - Media Rules
    - Signaling Rules
    - Endpoint Policy Group
    - Session Policy
- Device Specific Settings:
    - Network Management
    - Media Interface
    - Signaling Interface
    - End Point Flows → Server Flows
    - Session Flows

Call Server configuration elements for the enterprise - IP Office:

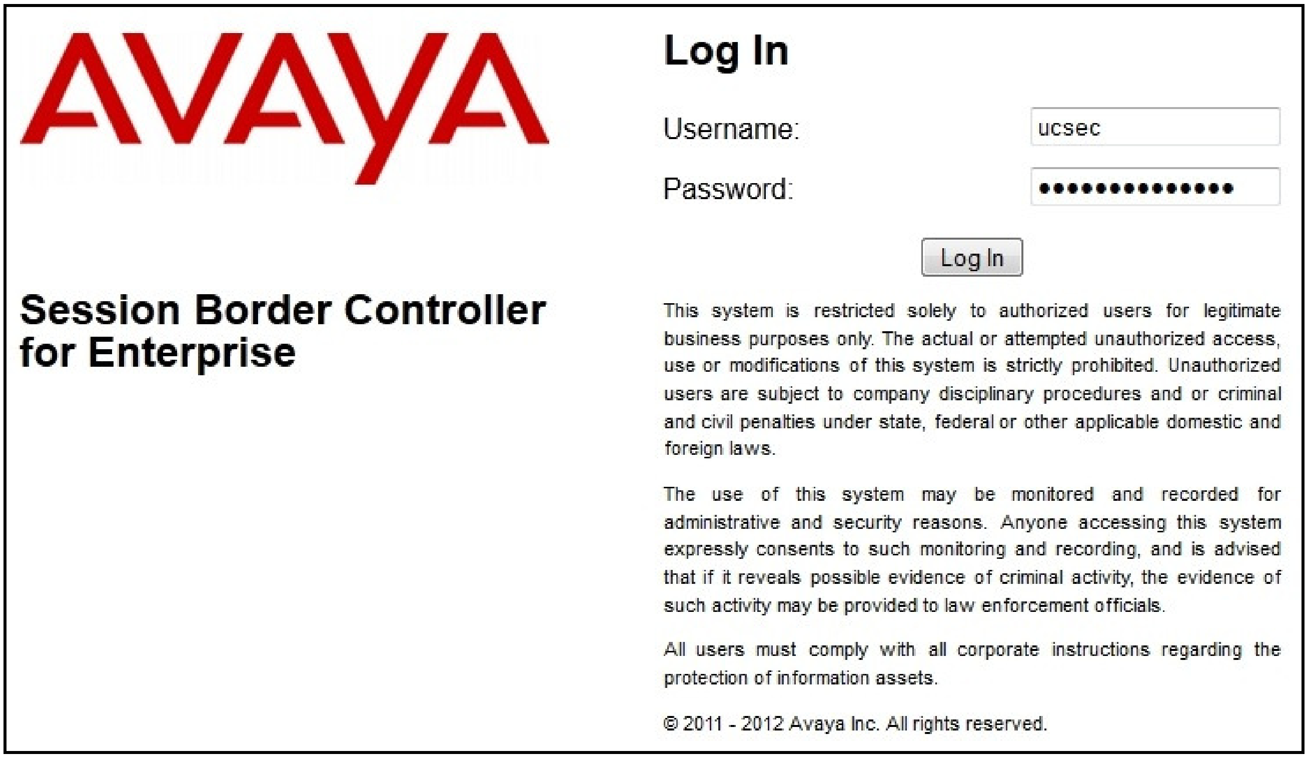
- Global Profiles:
    - URI Groups
    - Routing
    - Topology Hiding
    - Server Interworking
    - Server Configuration
- Domain Policies:
    - Application Rules
    - Media Rules
    - Signaling Rules
    - Endpoint Policy Group
    - Session Policy
- Device Specific Settings:

- Network Management
- Media Interface
- Signaling Interface
- End Point Flows → Server Flows
- Session Flows

6.1 Log into the Avaya Session Border Controller for Enterprise

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 management IP address.

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



Session Border Controller for Enterprise

Log In

Username: ucsec

Password: ••••••••••••••

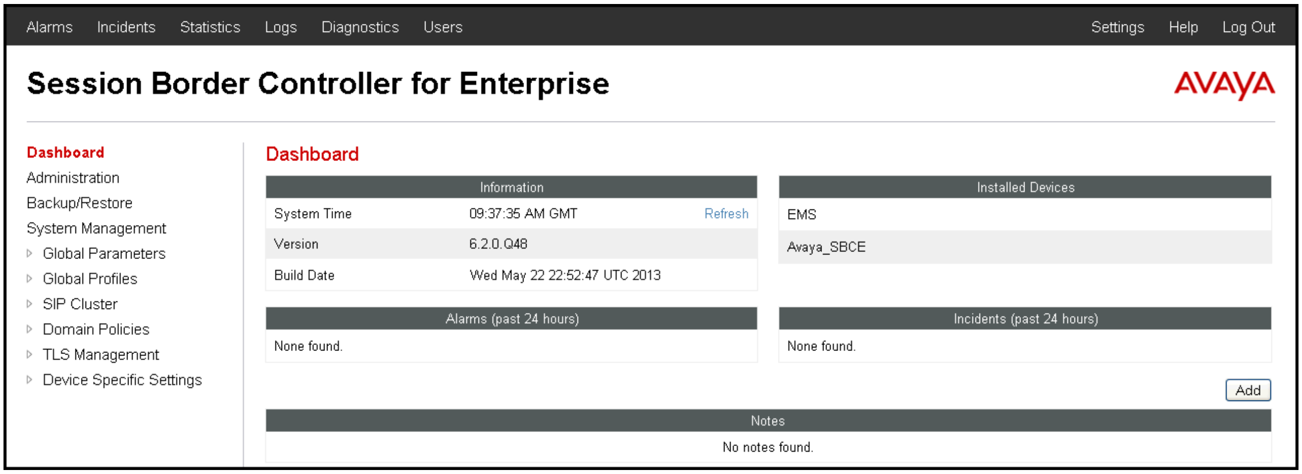
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2012 Avaya Inc. All rights reserved.

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



Dashboard

Information		
System Time	09:37:35 AM GMT	Refresh
Version	6.2.0.Q48	
Build Date	Wed May 22 22:52:47 UTC 2013	

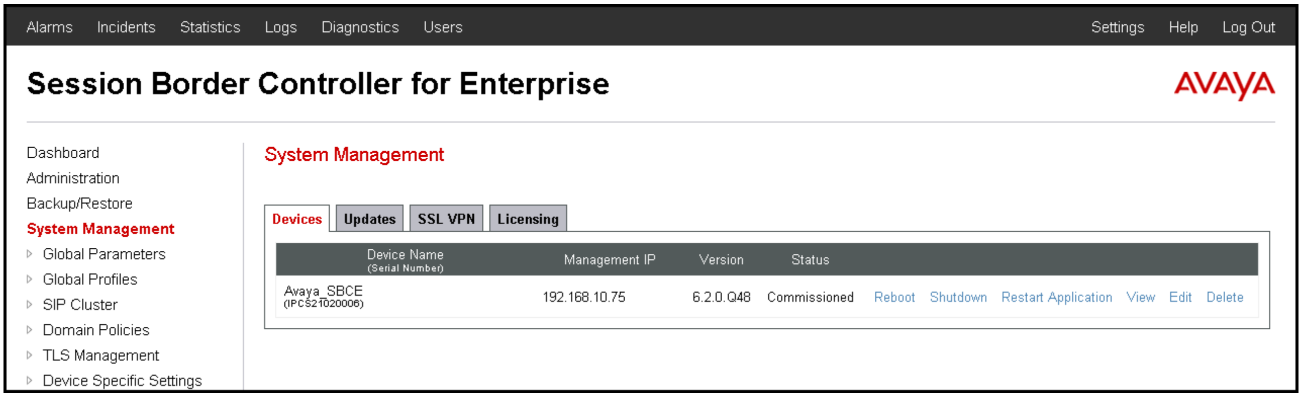
Installed Devices
EMS
Avaya_SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

Notes
No notes found.

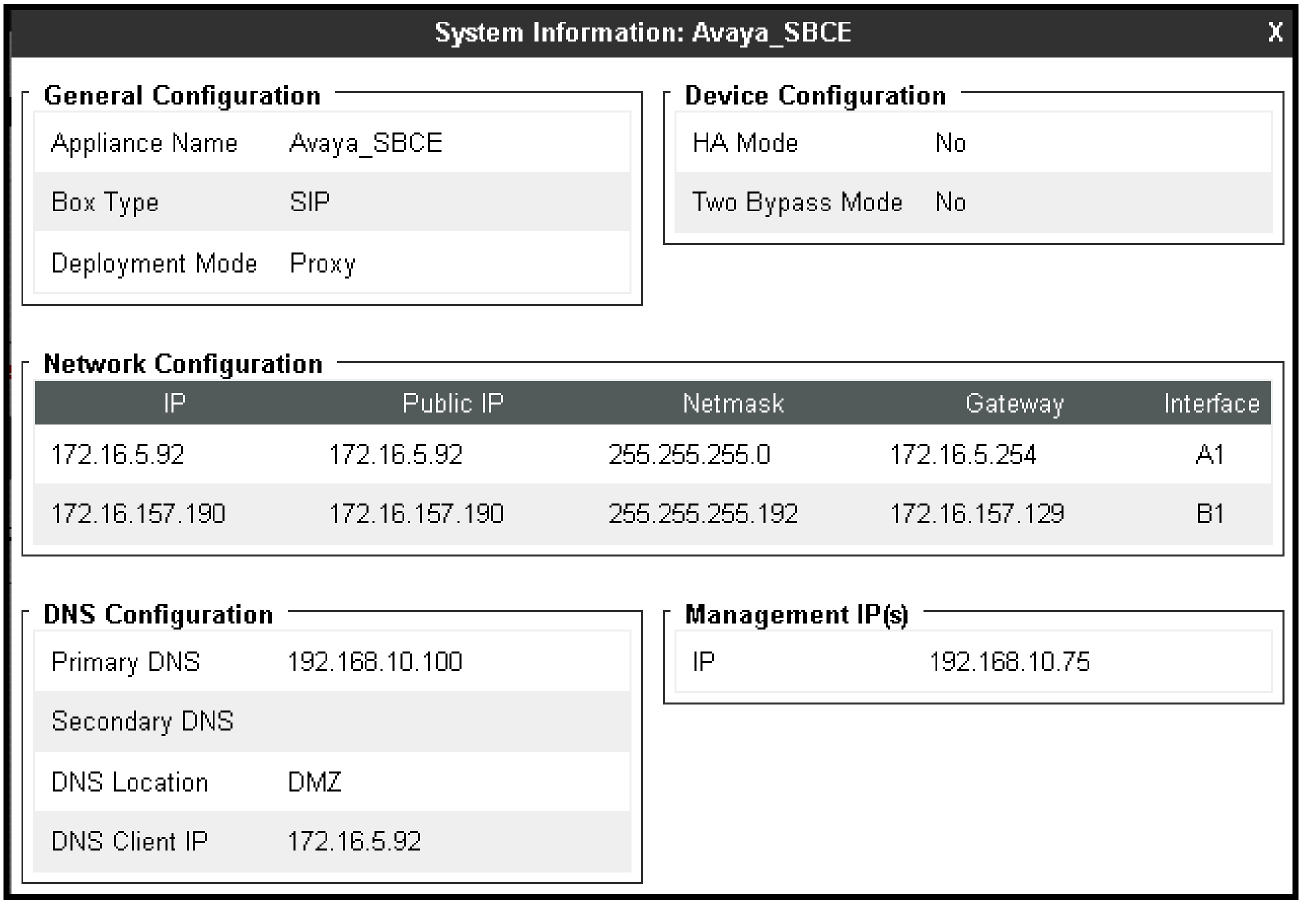
To view the system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Avaya SBCE** was already added. To view the configuration of this device, click the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



System Management

Device Name (Serial Number)	Management IP	Version	Status						
Avaya_SBCE (IPCS21020006)	192.168.10.75	6.2.0.Q48	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Delete

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



General Configuration

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
172.16.5.92	172.16.5.92	255.255.255.0	172.16.5.254	A1
172.16.157.190	172.16.157.190	255.255.255.192	172.16.157.129	B1

DNS Configuration

Primary DNS	192.168.10.100
Secondary DNS	
DNS Location	DMZ
DNS Client IP	172.16.5.92

Management IP(s)

IP	192.168.10.75

6.2 Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters that affect all the devices under the UC-Sec control Center.

6.2.1 Server Interworking Avaya

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 modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or "cloned", and then modified to meet specific requirements for the enterprise SIP-enabled solution.

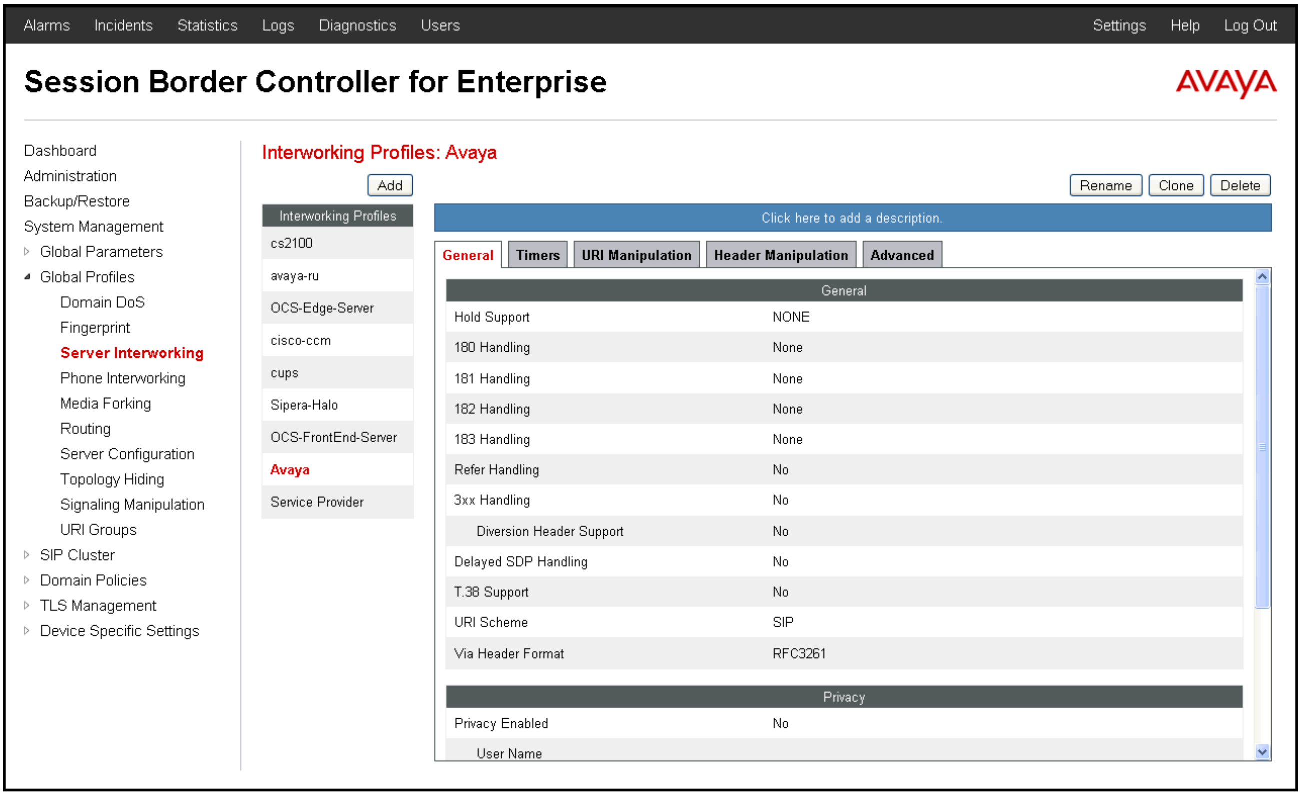
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone Profile** (not shown)**.**

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

For the newly created **Avaya** profile, click **Edit** (not shown) at the bottom of the General tab

- Click **Next** (not shown).
- Click **Finish** (not shown) on the **Privacy and DTMF** tab.
- Leave other fields with their default values.

The following screen capture shows the newly added **Avaya** Profile.



General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	

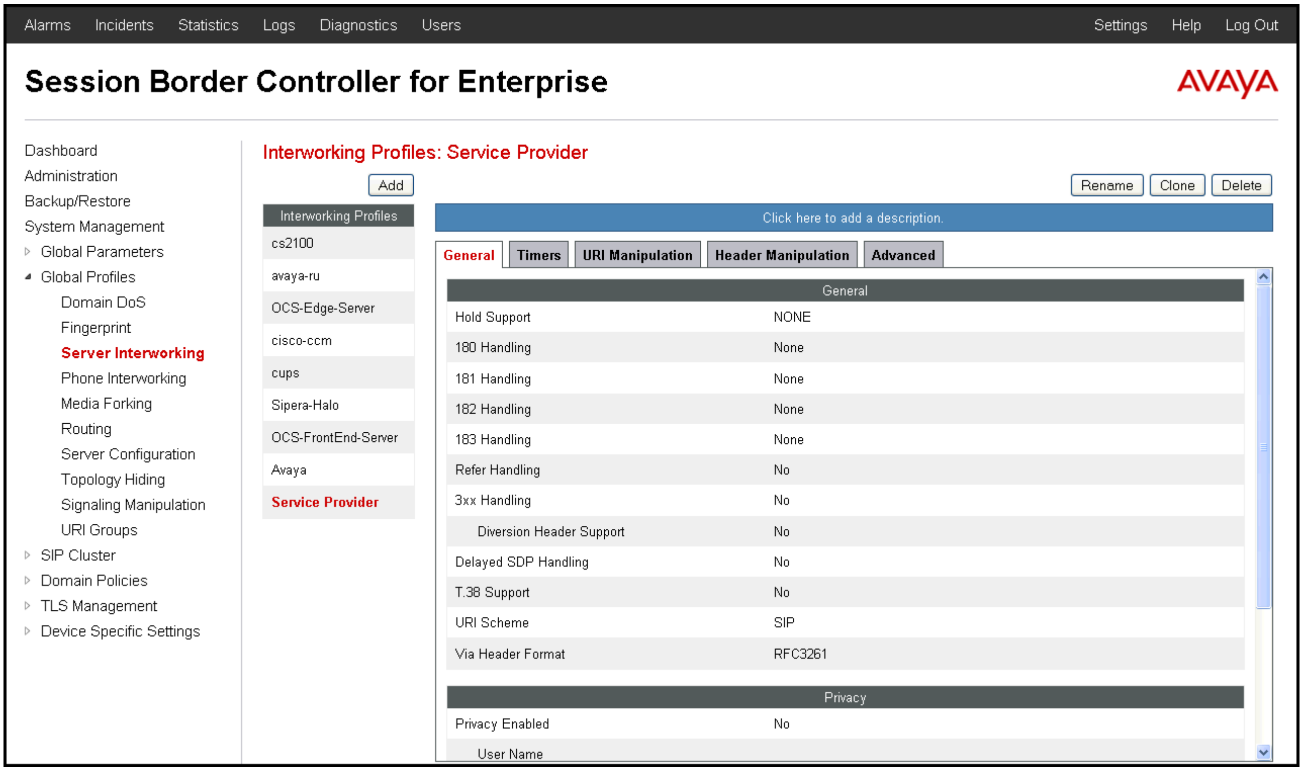
6.2.2 Server Interworking Service Provider

A second Server Interworking profile named **Service Provider** was created for the Service Provider.

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add.**

Enter the new profile name (not shown), the name of **Service Provider** was chosen in this example. Accept the default values for all fields by clicking **Next** (not shown) and then Click **Finish** (not shown)**.**

The following screen capture shows the newly added **Service Provider** Profile.



General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	

6.2.3 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 in the test configuration, one for inbound calls, with IP Office as the destination, and the second for outbound calls, which are sent to the Service Provider SIP trunk.

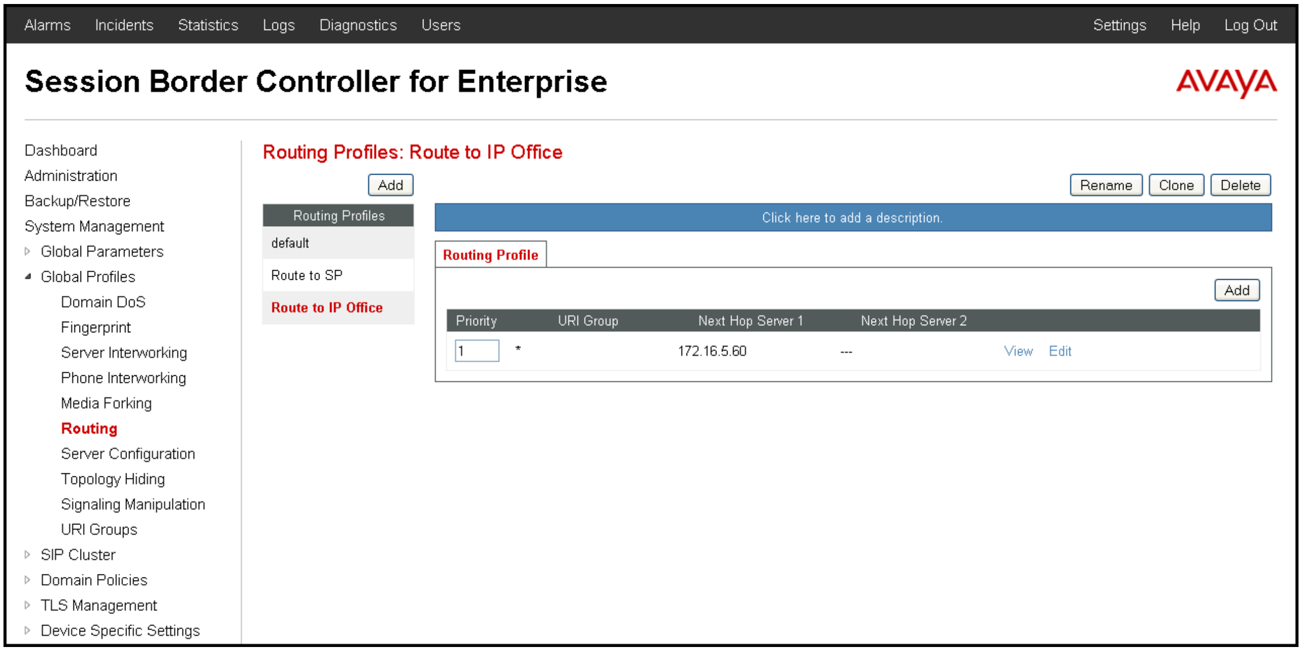
To create the inbound route, from the **Global Profiles** menu on the left-hand side:

- Select the **Routing** tab.
- Select **Add Profile.**
- Enter Profile Name: **Route to IP Office.**
- Click **Next** (not shown)**.**

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.5.60** (IP Office IP address).
- Check **Routing Priority Based on Next Hop Server** (not shown).
- Check **Outgoing Transport: UDP** (not shown).
- Click **Finish** (not shown)**.**

The following screen shows the newly added **Route to IP Office** Profile.



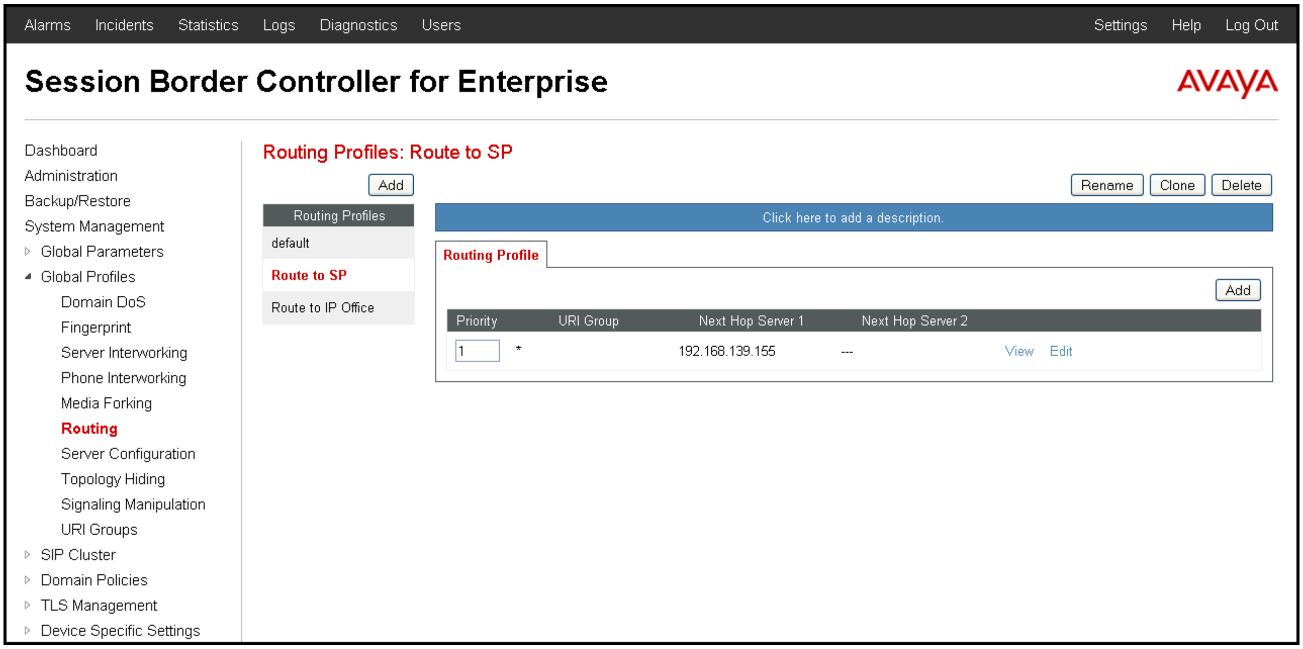
Routing Profiles: Route to IP Office

Priority	URI Group	Next Hop Server 1	Next Hop Server 2		
1	*	172.16.5.60	---	View	Edit

Similarly, for the outbound route:

- Select **Add Profile.**
- Enter Profile Name: **Route to SP**
- Click **Next** (not shown)**.**
- **Next Hop Server 1: 192.168.139.155** (IP address for Service Provider's proxy server)
- Check **Routing Priority Based on Next Hop Server** (not shown).
- Check **Outgoing Transport: UDP** (not shown).
- Click **Finish** (not shown)**.**

The following screen capture shows the newly added **Route_to_SP** Profile.



Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	192.168.139.155	---	View Edit

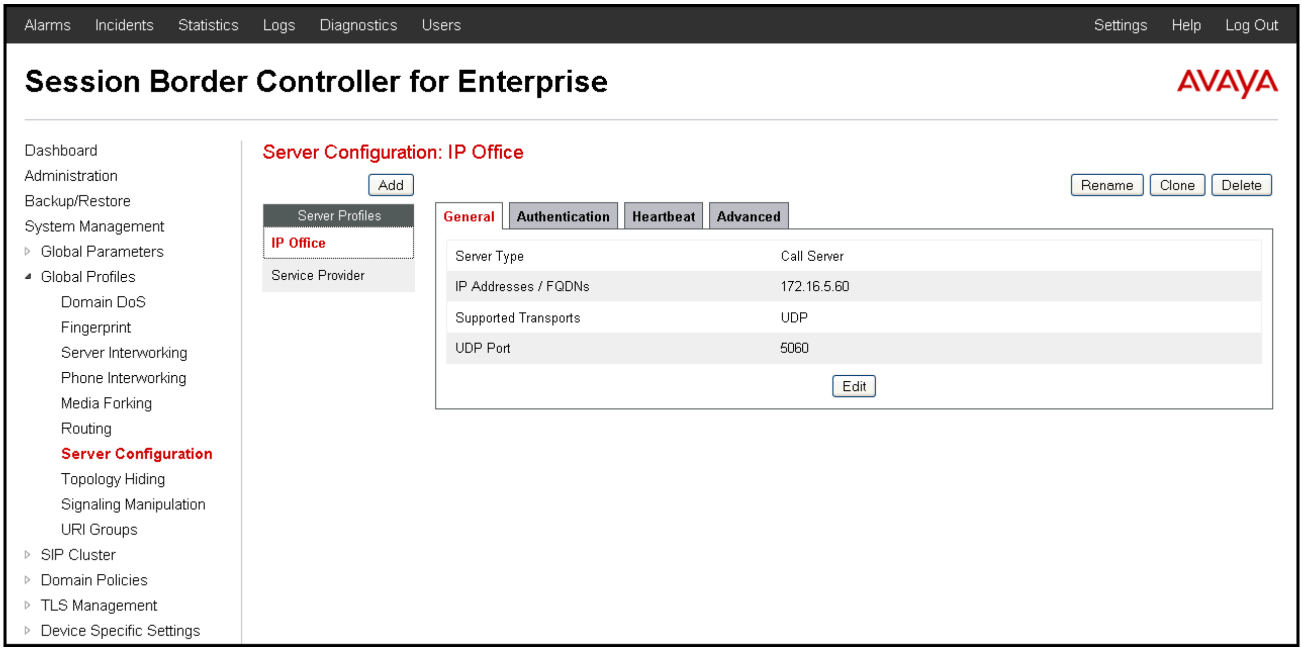
6.2.4 Server Configuration

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**. Click **Add Profile** and enter the profile name: **IP Office**.
On the **Add Server Configuration Profile** Tab:

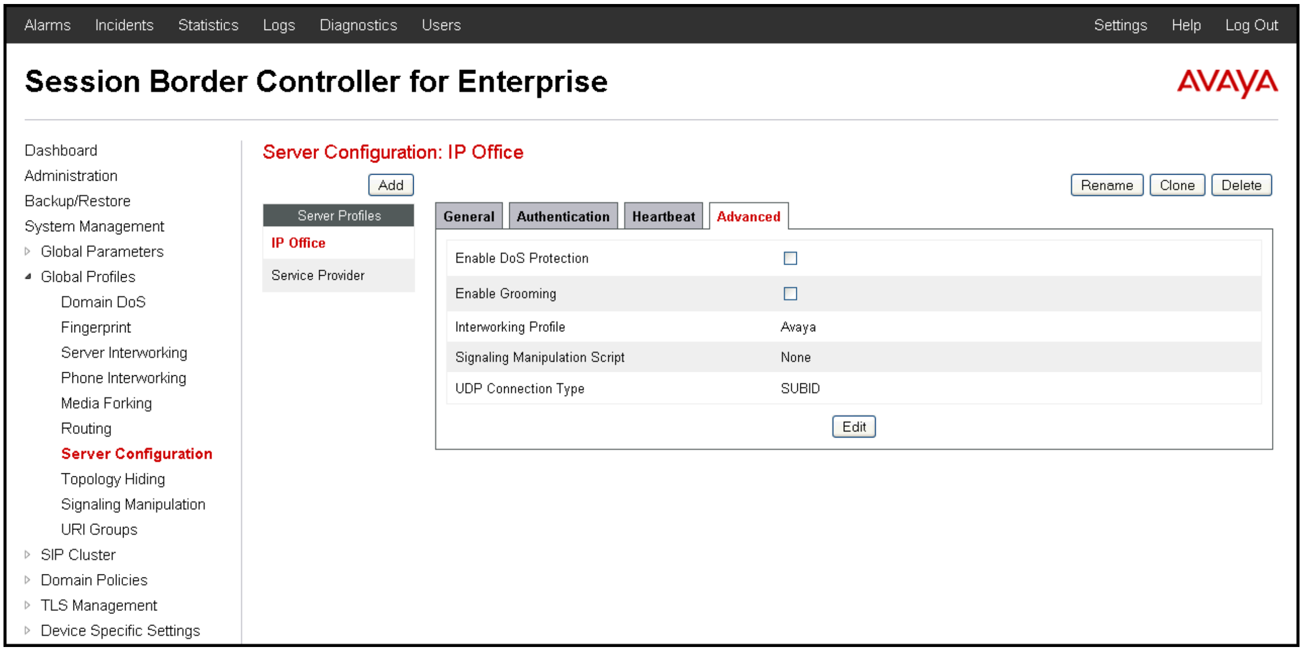
- Select Server Type**: Call Server.**
- **IP Address: 172.16.5.60** (IP Address of IP Office).
- **Supported Transports**: Check **UDP**.
- **TCP Port: 5060.**
- Click **Next** (not shown)**.**
- Click **Next** on the **Authentication** tab (not shown).
- Click **Next** on the **Heartbeat** tab (not shown).
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish** (not shown)**.**

The following screen capture shows the **General** tab of the newly added **IP Office** Profile.



Server Type	Call Server
IP Addresses / FQDNs	172.16.5.60
Supported Transports	UDP
UDP Port	5060

The following screen capture shows the **Advanced** tab of the added **IP Office** Profile.



Server Configuration: IP Office

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Avaya
Signaling Manipulation Script	None
UDP Connection Type	SUBID

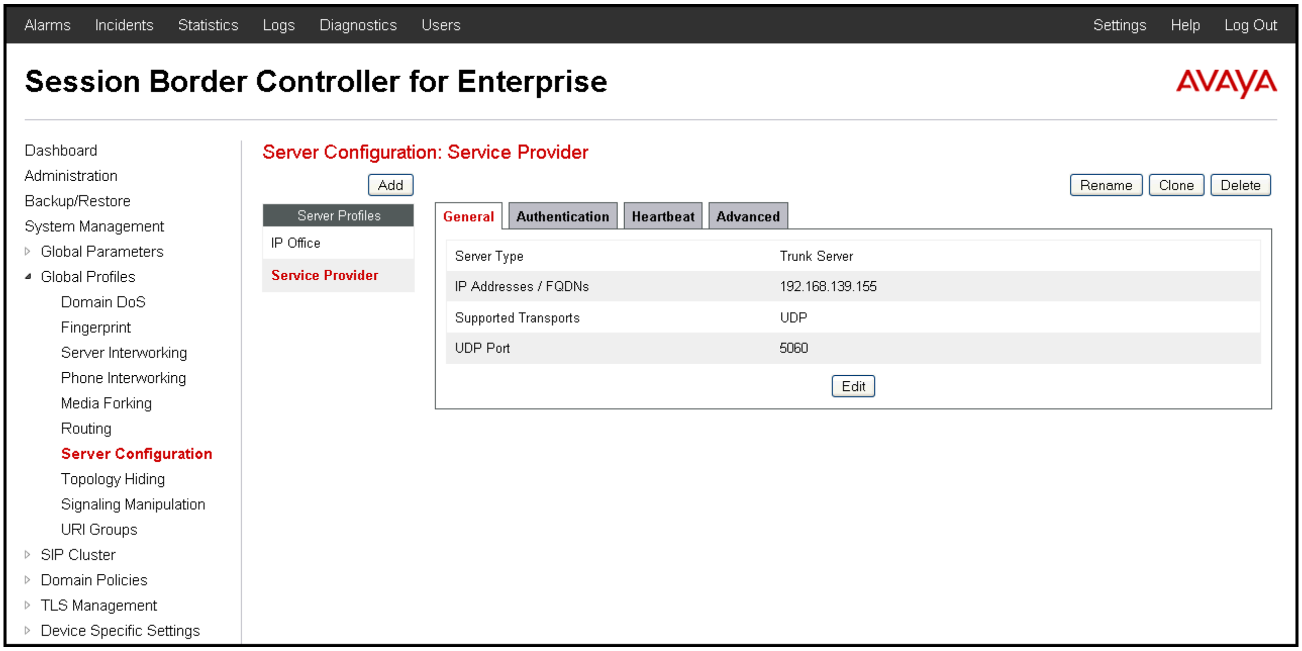
To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add Profile** and enter the profile name: **Service Provider.**

On the **Add Server Configuration Profile** Tab:

- Select Server Type**: Trunk Server.**
- **IP Address: 192.168.139.155** (service provider's SIP Proxy IP address).
- **Supported Transports**: Check **UDP**.
- **UDP Port: 5060.**
- Click **Next** (not shown)**.**
- Click **Next** on the **Authentication** tab (not shown).
- Click **Next** on the **Heartbeat** tab (not shown).
- On the **Advanced** tab, select **Service Provider** from the **Interworking Profile** drop down menu.

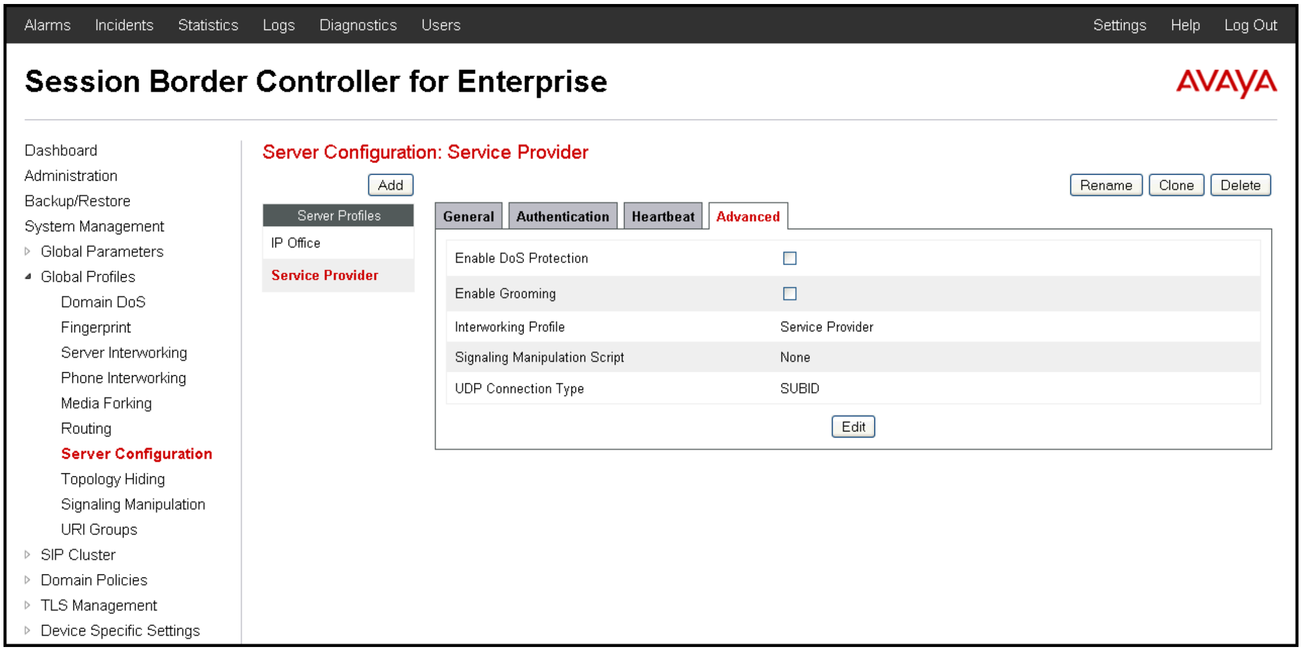
  Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish** (not shown)**.**

The following screen capture shows the **General** tab of the **Service Provider** Profile.



Server Type	Trunk Server
IP Addresses / FQDNs	192.168.139.155
Supported Transports	UDP
UDP Port	5060

The following screen capture shows the **Advanced** tab of the **Service Provider** Profile.



Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Service Provider
Signaling Manipulation Script	None
UDP Connection Type	SUBID

6.2.5 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.

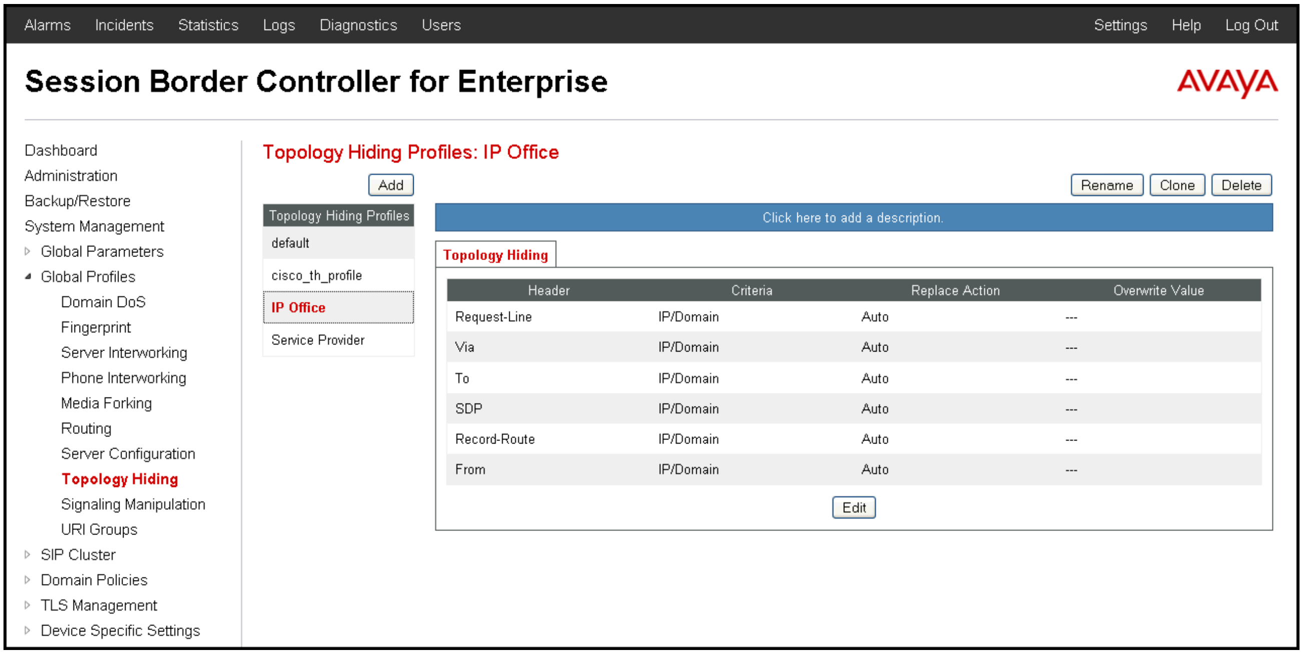
Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by IP Office and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

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

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

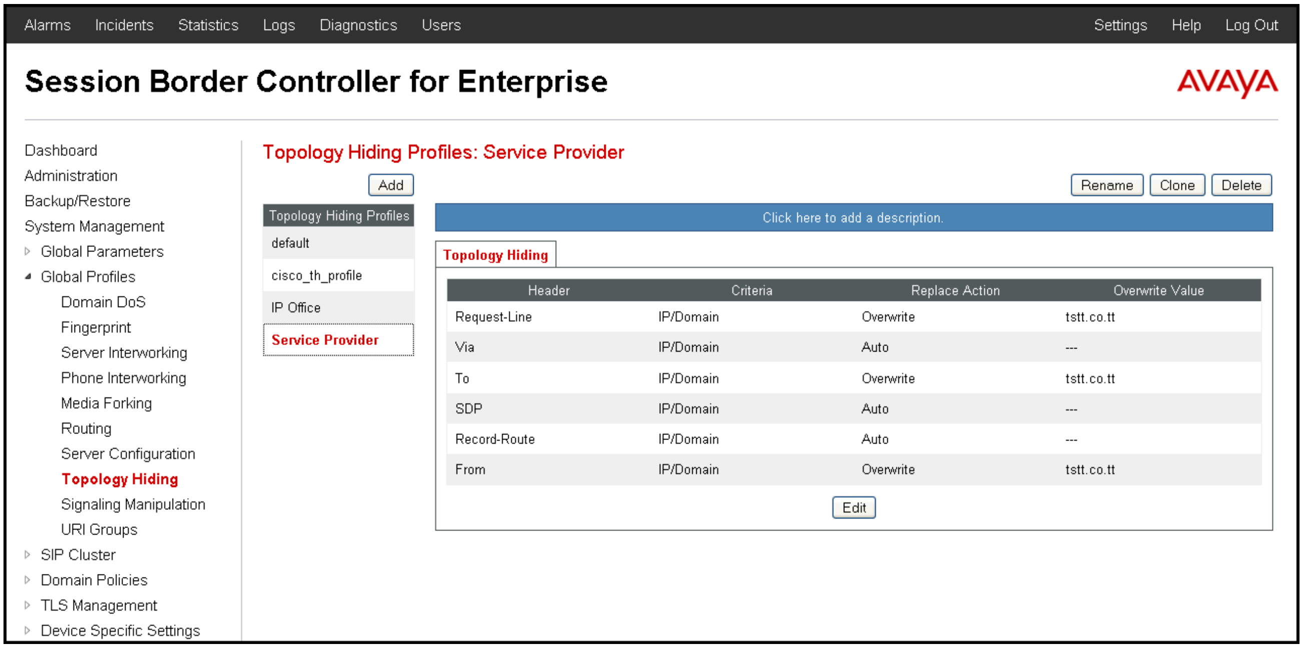


Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Auto	---

To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile**
- Enter the **Profile Name**: **Service Provider.**
- Click **Finish** (not shown).
- Click **Edit** (not shown) on the newly added **Service Provider** Topology Hiding profile.
- In the **From** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the enterprise **(tstt.co.tt)** under **Overwrite Value**.
- In the **To** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Enterprise **(tstt.co.tt)** under **Overwrite Value**.
- In the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Enterprise **(tstt.co.tt)** under **Overwrite Value**.

The following screen capture shows the newly added **Service Provider** Profile.



Topology Hiding Profiles: Service Provider

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	tstt.co.tt
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	tstt.co.tt
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	tstt.co.tt

6.2.6 Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows to perform a granular header manipulation on the headers in the SIP messages, which sometimes is not possible by direct configuration on the web interface. The ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

Signaling Manipulation was not necessary and was not used during the compliance testing.

6.3 Domain Policies

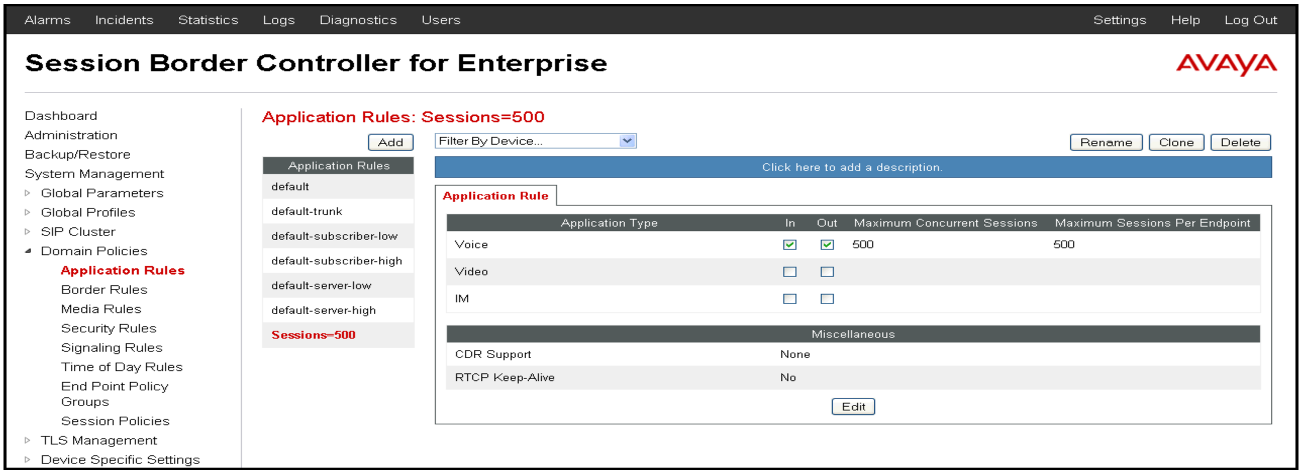
Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

In the reference configuration, only a new Application Rule was defined. All other rules under Domain Policies, linked together on End Point Policy Groups, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

6.3.1 Create Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define 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**
- Select **default trunk** Rule (not shown)
- Select **Clone Rule** button (not shown)
- Name**: Sessions=500**
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **500** was used in the sample configuration.
- Click Finish (not shown).



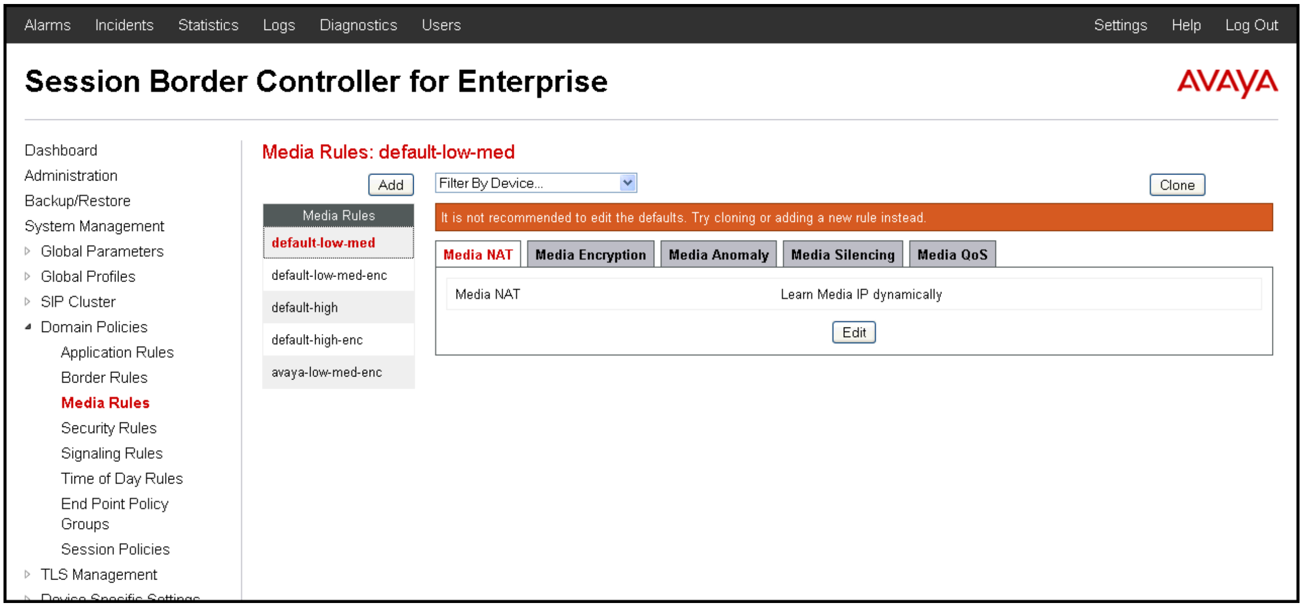
Application Rules: Sessions=500

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	☑	☑	500	500
Video	□	□		
IM	□	□		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

6.3.2 Media Rules

For the compliance test, the **default-low-med** Media Rule was used.



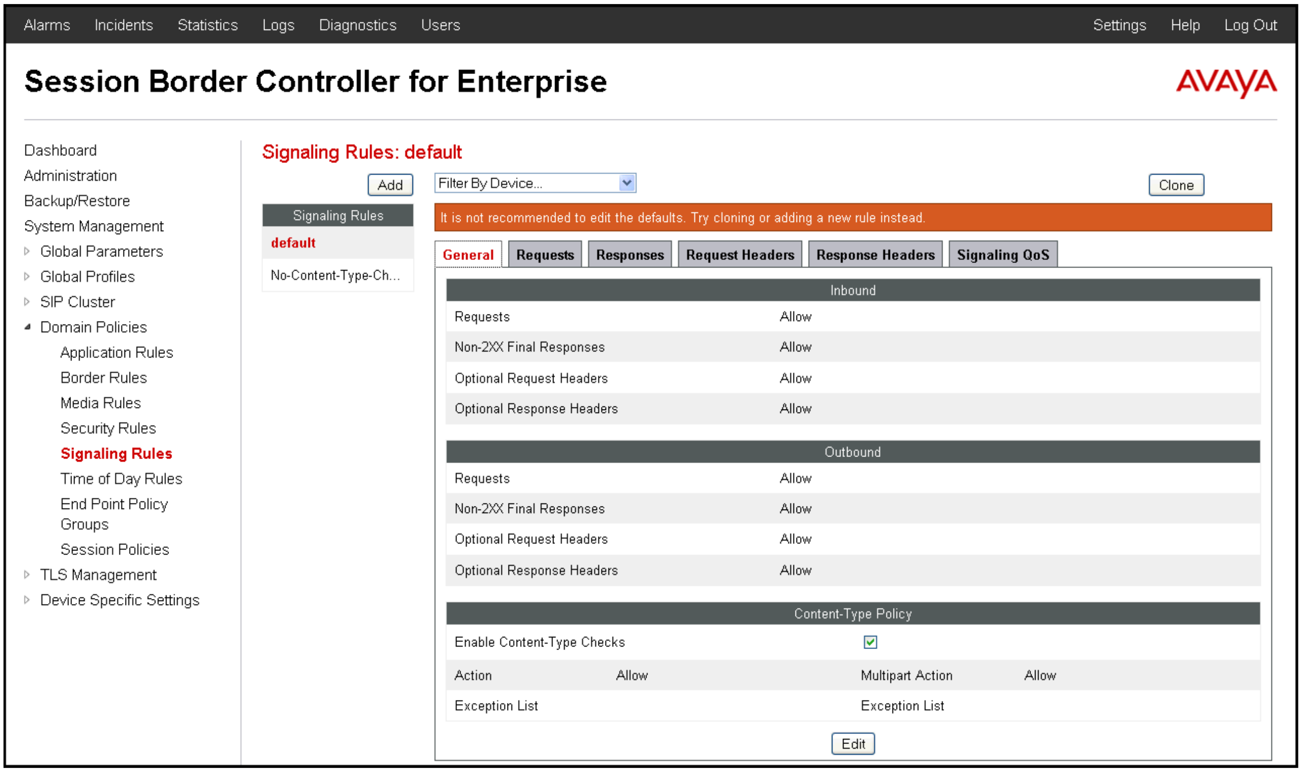
Media Rules: default-low-med

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Media NAT	Learn Media IP dynamically

6.3.3 Signaling Rules

For the compliance test, the **default** Signaling Rule was used.



Signaling Rules: default

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks		☑	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

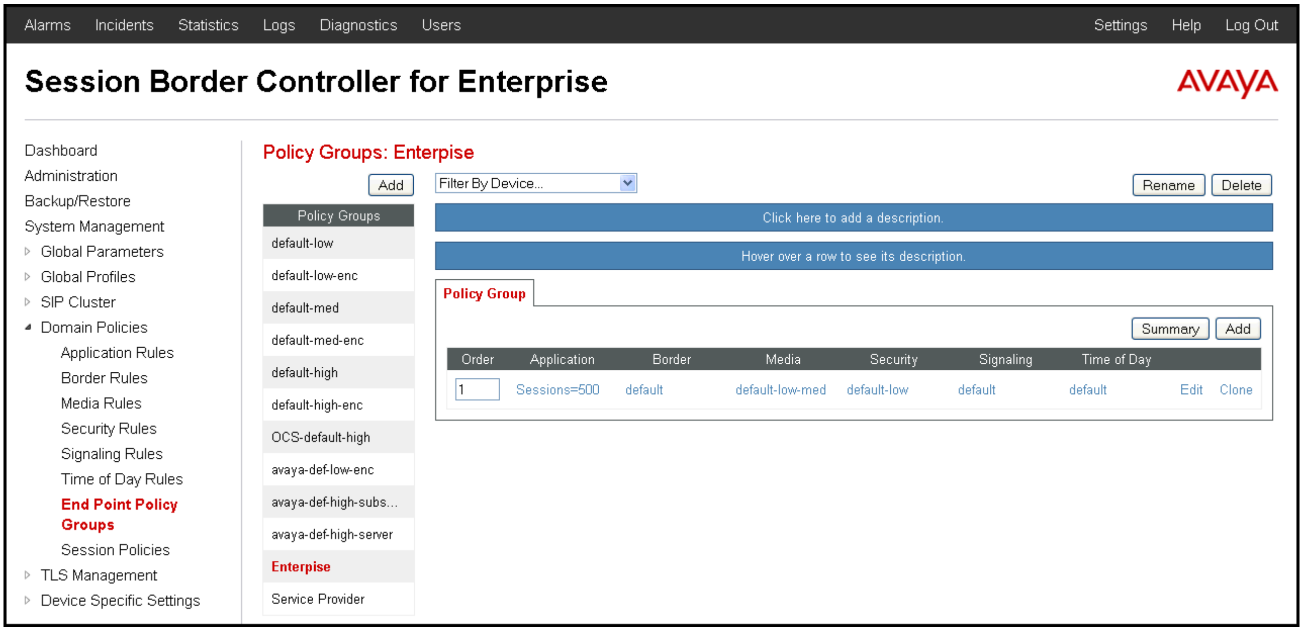
6.3.4 End Point Policy Groups

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**. Select **Add Group**.

- **Group Name: Enterprise**.
- **Application Rule: Sessions=500.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- **Time of Day: default.**
- Click **Finish** (not shown).

The following screen capture shows the newly added **Enterprise** End Point Policy Group.

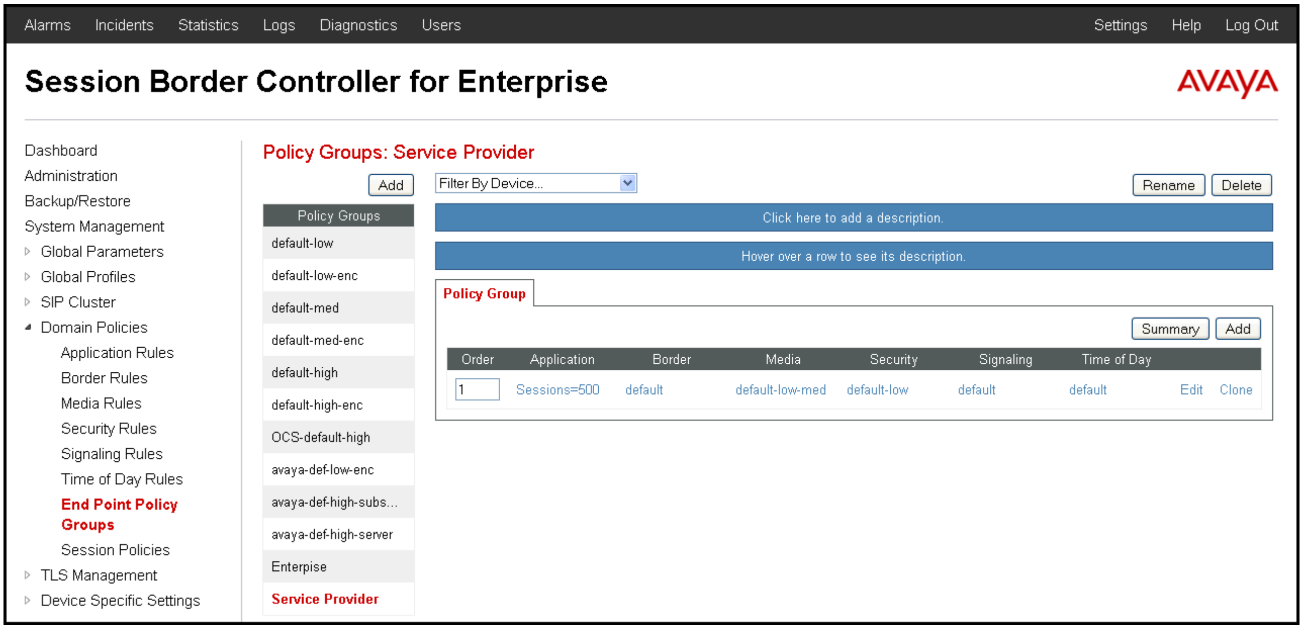


Order	Application	Border	Media	Security	Signaling	Time of Day		
1	Sessions=500	default	default-low-med	default-low	default	default	Edit	Clone

Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add Group**.

- **Group Name: Service Provider**.
- **Application Rule: Sessions=500.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- **Time of Day: default.**
- Click **Finish** (not shown).

The following screen capture shows the newly added **Service Provider** End Point Policy Group.



Policy Groups: Service Provider

Policy Groups
default-low
default-low-enc
default-med
default-med-enc
default-high
default-high-enc
OCS-default-high
avaya-def-low-enc
avaya-def-high-subs...
avaya-def-high-server
Enterpise
Service Provider

Click here to add a description.

Hover over a row to see its description.

Policy Group

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	Sessions=500	default	default-low-med	default-low	default	default	Edit	Clone

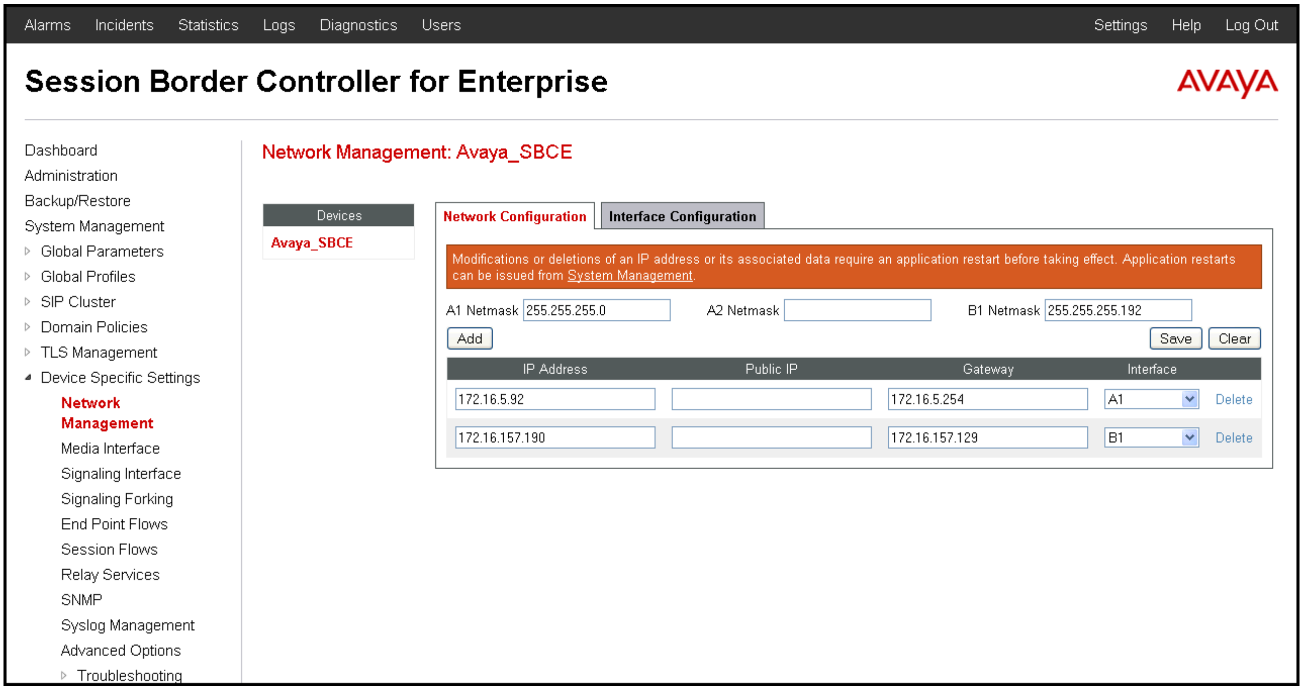
6.4 Device Specific Settings

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.

6.4.1 Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Menu** 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 could be entered here.



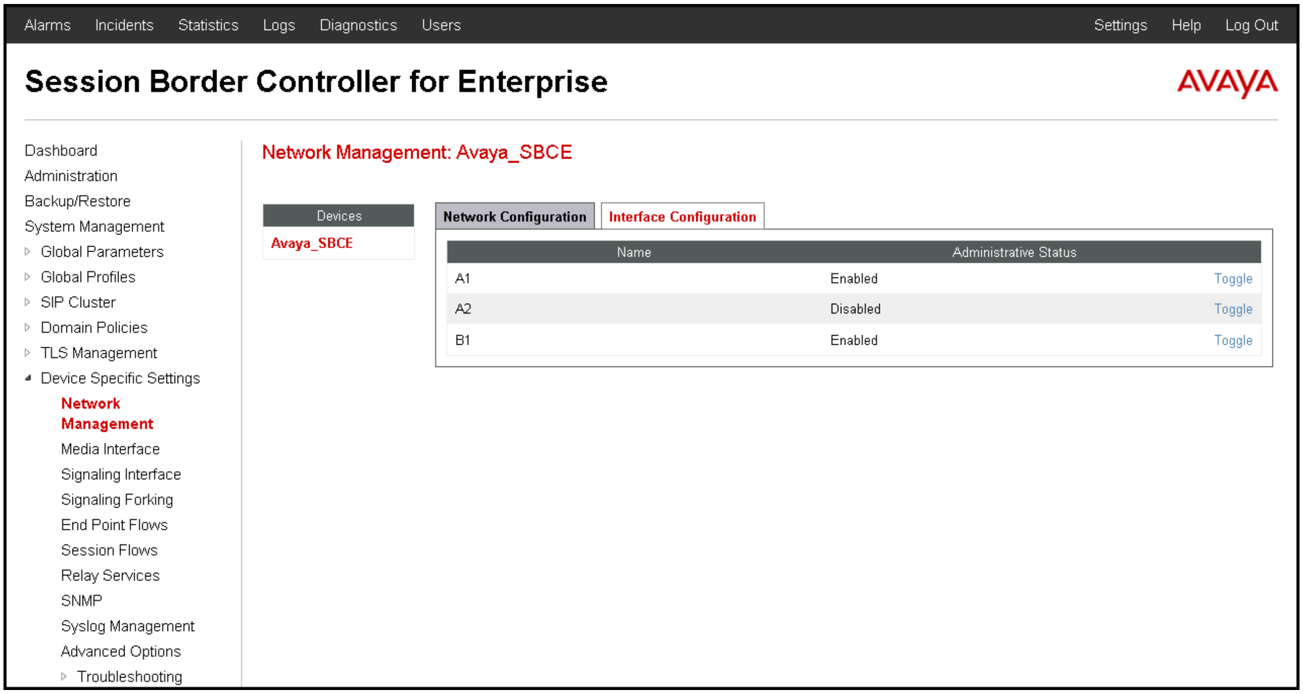
Network Management: Avaya_SBCE

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.192

IP Address	Public IP	Gateway	Interface	
172.16.5.92		172.16.5.254	A1	Delete
172.16.157.190		172.16.157.129	B1	Delete

On the Interface Configuration tab, click the **Toggle State** control 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.



Network Management: Avaya_SBCE

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle

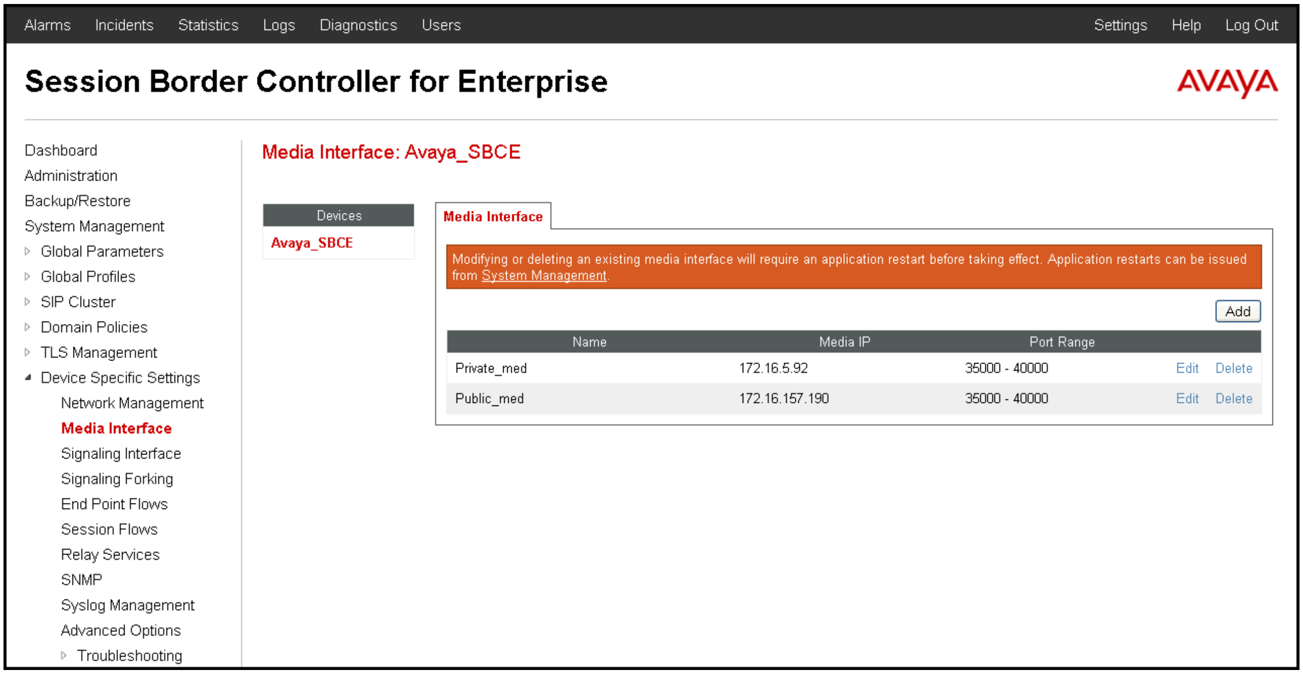
6.4.2 Media Interface

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 ports range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**

- Select **Add Media Interface.**
- **Name: Private_med.**
- Select **IP Address: 172.16.5.92** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **Port Range: 35000-40000.**
- Click **Finish** (not shown)**.**
- Select **Add Media Interface.**
- **Name: Public_med.**
- Select **IP Address: 172.16.157.190** (Outside IP Address of the Avaya SBCE, toward Service Provider).
- **Port Range: 35000-40000.**
- Click **Finish** (not shown)**.**

The following screen capture shows the added **Media Interfaces**.



Media Interface: Avaya_SBCE

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

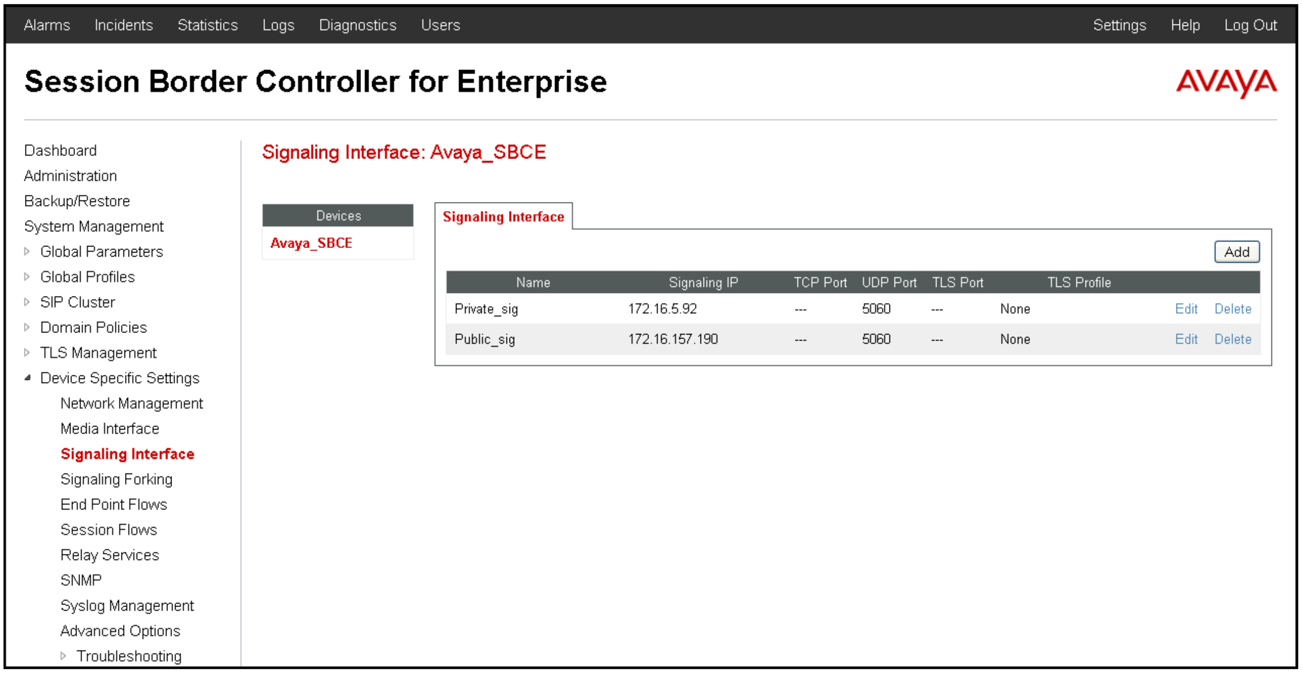
Name	Media IP	Port Range		
Private_med	172.16.5.92	35000 - 40000	Edit	Delete
Public_med	172.16.157.190	35000 - 40000	Edit	Delete

6.4.3 Signaling Interface

To create the Signaling Interface toward IP Office, from the **Device Specific** menu on the left hand side, select **Signaling Interface**

- Select **Add Signaling Interface**:
- **Name: Private_sig.**
- Select **IP Address: 172.16.5.92** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **UDP Port: 5060.**
- Click **Finish** (not shown)**.**
- Select **Add Signaling Interface**:
- **Name: Public_sig**
- Select **IP Address: 172.16.157.190** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port: 5060.**
- Click **Finish**(not shown)**.**

The following screen capture shows the newly added **Signaling Interfaces**.

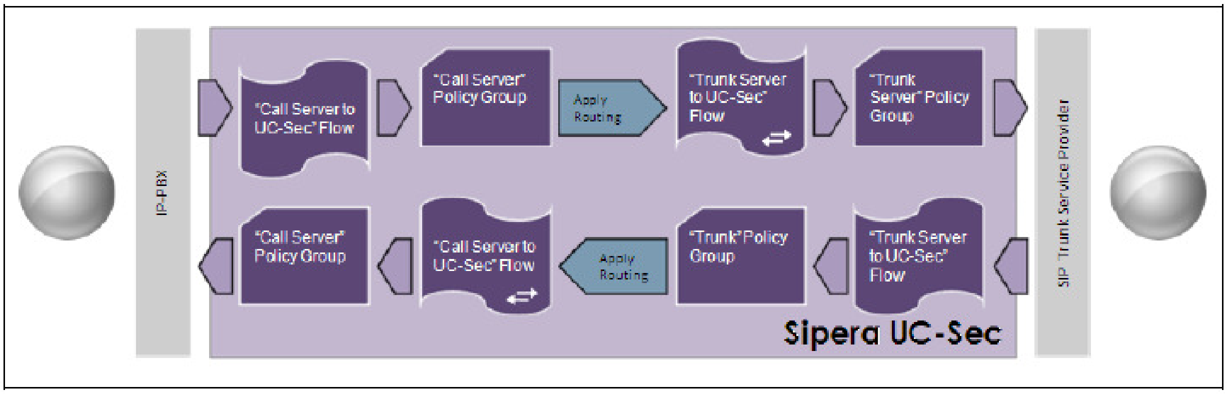


Signaling Interface: Avaya_SBCE

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Private_sig	172.16.5.92	---	5060	---	None	Edit	Delete
Public_sig	172.16.157.190	---	5060	---	None	Edit	Delete

6.4.4 End Point Flows

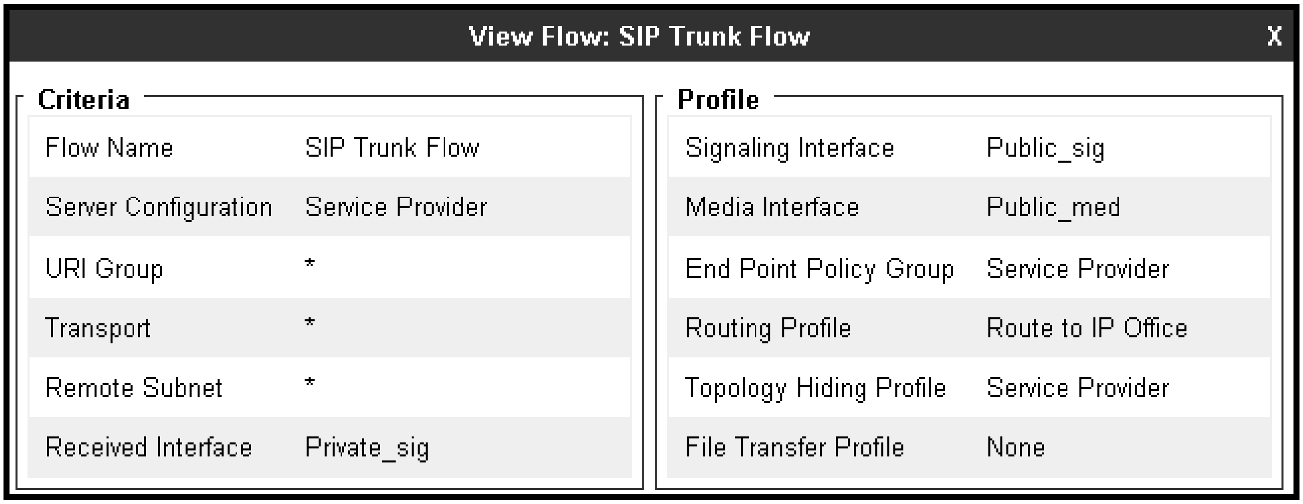
When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is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


IP-PBX
"Call Server to UC-Sec" Flow
"Call Server" Policy Group
Apply Routing
"Trunk Server to UC-Sec" Flow
"Trunk Server" Policy Group
"Call Server" Policy Group
"Call Server to UC-Sec" Flow
Apply Routing
"Trunk" Policy Group
"Trunk Server to UC-Sec" Flow
Sipera UC-Sec
SIP Trunk Service Provider

The **End-Point Flows** defines 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 the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, tab **Server Flows**. Click **Add Flow** (not shown).

- **Name: SIP Trunk Flow.**
- **Server Configuration**: **Service Provider.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Private_sig.**
- **Signaling Interface: Public_sig.**
- **Media Interface**: **Public_med.**
- **End Point Policy Group: Service Provider.**
- **Routing Profile: Route to IP Office** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service Provider.**
- **File Transfer Profile: None.**
- Click **Finish** (not shown)**.**



View Flow: SIP Trunk Flow

Criteria

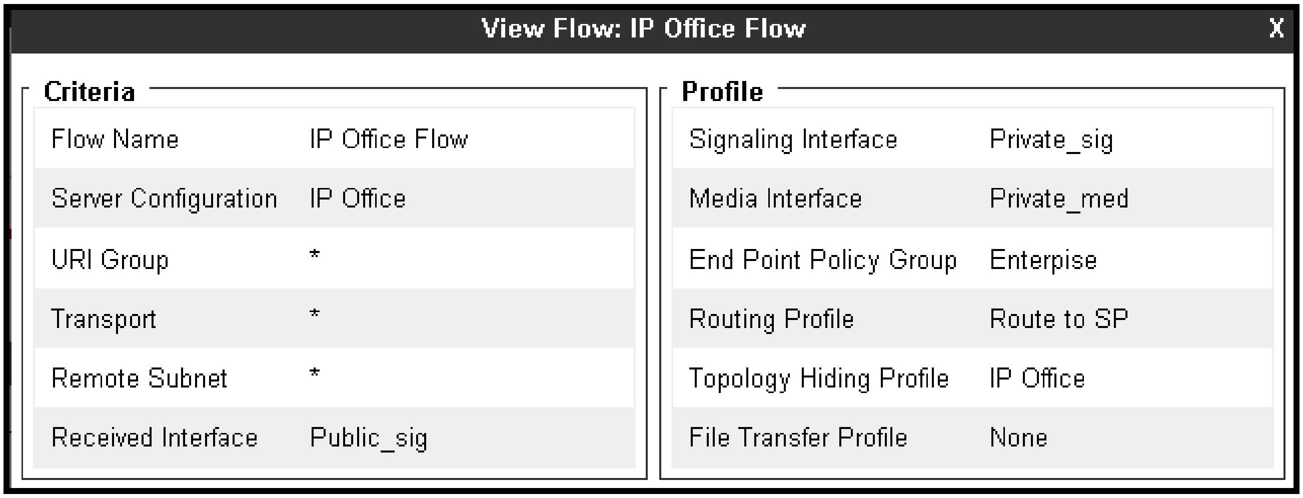
Flow Name	SIP Trunk Flow
Server Configuration	Service Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig

Profile

Signaling Interface	Public_sig
Media Interface	Public_med
End Point Policy Group	Service Provider
Routing Profile	Route to IP Office
Topology Hiding Profile	Service Provider
File Transfer Profile	None

To create the call flow toward the IP Office, click **Add Flow**.

- **Name: IP Office Flow** (not shown)**.**
- **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: Enterprise.**
- **Routing Profile: Route to SP** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: IP Office.**
- **File Transfer Profile: None.**
- Click **Finish** (not shown)**.**



View Flow: IP Office Flow

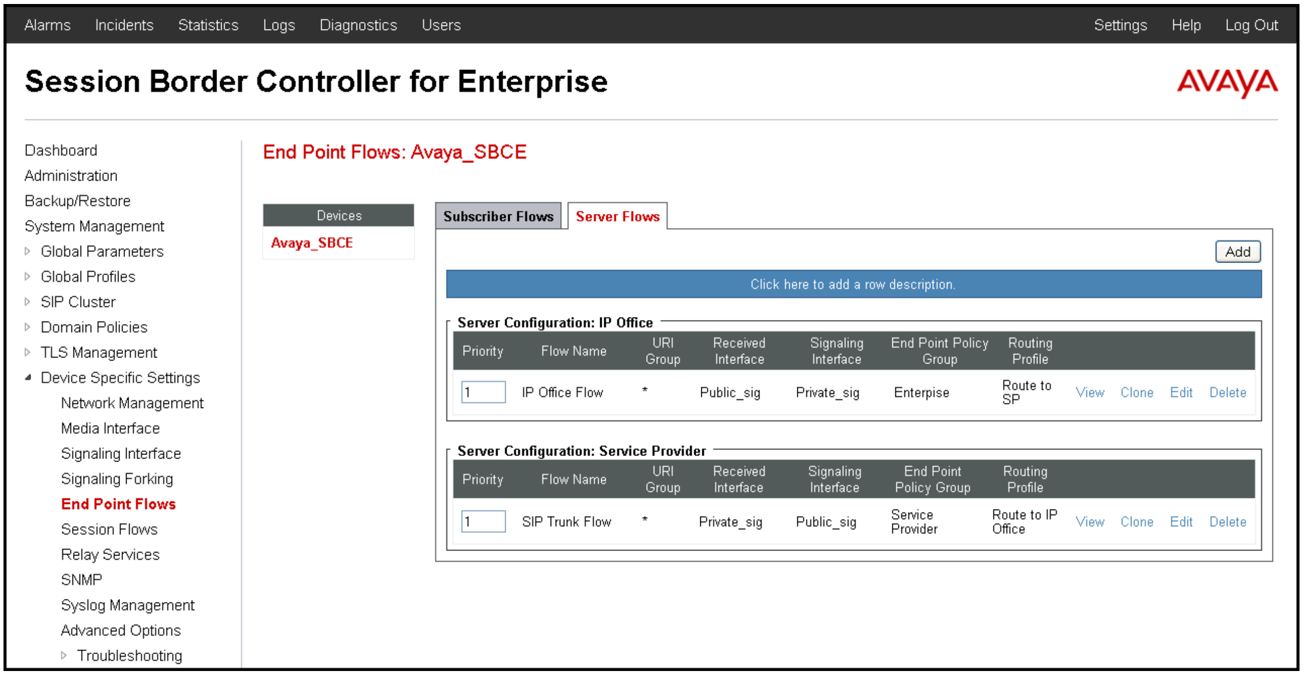
Criteria

Flow Name	IP Office Flow
Server Configuration	IP Office
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig

Profile

Signaling Interface	Private_sig
Media Interface	Private_med
End Point Policy Group	Enterpise
Routing Profile	Route to SP
Topology Hiding Profile	IP Office
File Transfer Profile	None

The following screen capture shows the added **End Point Flows.**



End Point Flows: Avaya_SBCE

Server Configuration: IP Office

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	IP Office Flow	*	Public_sig	Private_sig	Enterprise	Route to SP	View	Clone	Edit	Delete

Server Configuration: Service Provider

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	SIP Trunk Flow	*	Private_sig	Public_sig	Service Provider	Route to IP Office	View	Clone	Edit	Delete

7. Telecommunications Services of Trinidad and Tobago SIP Trunking Configuration

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

- IP address of the TSTT SIP Proxy server.
- Supported codec's and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

8. 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.

8.1 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 the call remains 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 the call can remain active for more than 35 seconds.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

8.2 Protocol Traces

The following SIP message headers are inspected using 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.

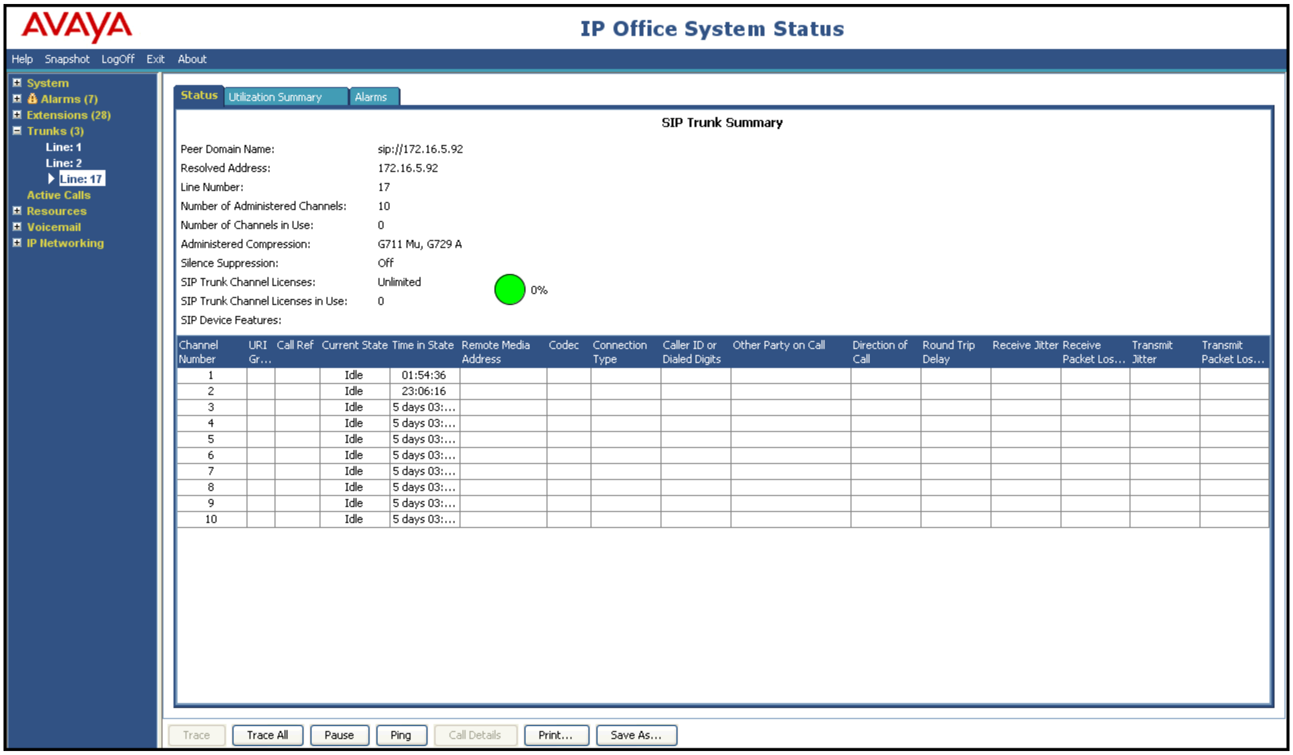
The following attributes in SIP message body are inspected using sniffer trace analysis tool:

- 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 event and fax attributes.

8.3 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 the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** (not shown) on the PC where IP Office Manager is installed. 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).

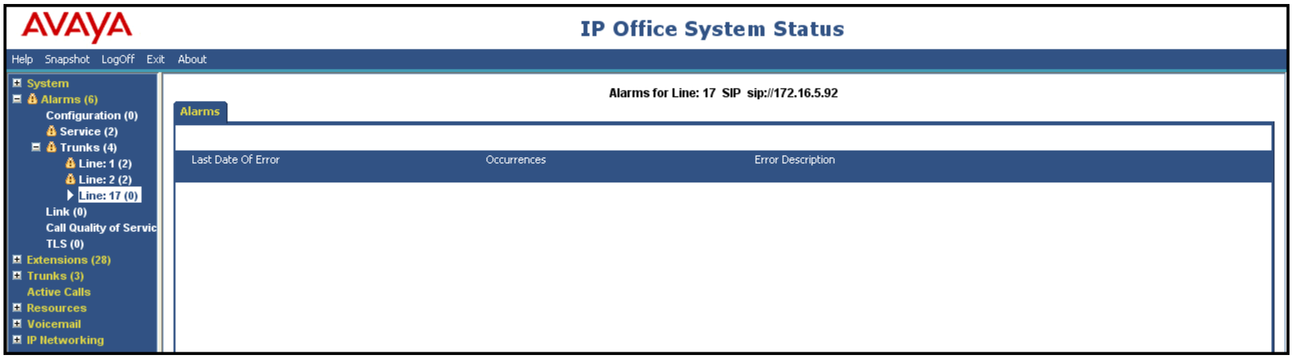


SIP Trunk Summary

Peer Domain Name:	sip://172.16.5.92
Resolved Address:	172.16.5.92
Line Number:	17
Number of Administered Channels:	10
Number of Channels in Use:	0
Administered Compression:	G711 Mu, G729 A
Silence Suppression:	Off
SIP Trunk Channel Licenses:	Unlimited ● 0%
SIP Trunk Channel Licenses in Use:	0
SIP Device Features:	

Channel Number	URI Gr...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Los...	Transmit Jitter	Transmit Packet Los...
1			Idle	01:54:36											
2			Idle	23:06:16											
3			Idle	5 days 03:...											
4			Idle	5 days 03:...											
5			Idle	5 days 03:...											
6			Idle	5 days 03:...											
7			Idle	5 days 03:...											
8			Idle	5 days 03:...											
9			Idle	5 days 03:...											
10			Idle	5 days 03:...											

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



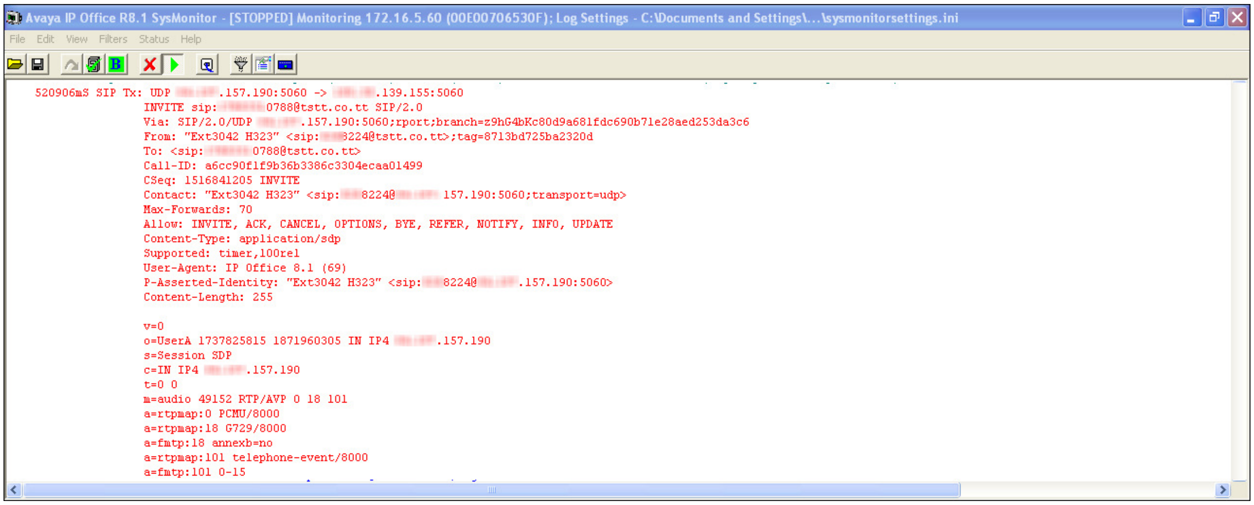
Alarms for Line: 17 SIP sip://172.16.5.92

Last Date Of Error	Occurrences	Error Description

8.4 IP Office Monitor

The Avaya IP Office Monitor application can also be used to monitor and troubleshoot SIP signaling messaging between TSTT and IP Office. Launch the application from **Start →Programs →IP Office →Monitor** (not shown) on the PC where Avaya IP Office Manager was installed.

The sample screen below shows part of the messages on an outbound call.



Avaya IP Office R8.1 SysMonitor - [STOPPED] Monitoring 172.16.5.60 (00E00706530F); Log Settings - C:\Documents and Settings\...\sysmonitorsettings.ini
File Edit View Filters Status Help

```
    520906mS SIP Tx: UDP [redacted].157.190:5060 -> [redacted].139.155:5060
                    INVITE sip:[redacted]0788@tstt.co.tt SIP/2.0
                    Via: SIP/2.0/UDP [redacted].157.190:5060;rport;branch=z9hG4bKc80d9a681fdc690b71e28aed253da3c6
                    From: "Ext3042 H323" <sip:[redacted]224@tstt.co.tt>;tag=8713bd725ba2320d
                    To: <sip:[redacted]0788@tstt.co.tt>
                    Call-ID: a6cc90f1f9b36b3386c3304ecaa01499
                    CSeq: 1516841205 INVITE
                    Contact: "Ext3042 H323" <sip:[redacted]8224@[redacted] 157.190:5060;transport=udp>
                    Max-Forwards: 70
                    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, UPDATE
                    Content-Type: application/sdp
                    Supported: timer,100rel
                    User-Agent: IP Office 8.1 (69)
                    P-Asserted-Identity: "Ext3042 H323" <sip:[redacted]8224@[redacted].157.190:5060>
                    Content-Length: 255

                    v=0
                    o=UserA 1737825815 1871960305 IN IP4 [redacted].157.190
                    s=Session SDP
                    c=IN IP4 [redacted].157.190
                    t=0 0
                    m=audio 49152 RTP/AVP 0 18 101
                    a=rtpmap:0 PCMU/8000
                    a=rtpmap:18 G729/8000
                    a=fmtp:18 annexb=no
                    a=rtpmap:101 telephone-event/8000
                    a=fmtp:101 0-15
```

9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 8.1, Avaya Session Border Controller for Enterprise R6.2 and Telecommunications Services of Trinidad and Tobago SIP Trunk Service, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations noted in **Section 2.2**

10. References

[1] *IP Office 8.1 IP500/IP500 V2 Installation*, Document Number 15-601042, Issue 27f, 04 March 2013.

[2] *IP Office 8.1 Manager FP1 10.1*, Document Number 15-601011, Issue 29t, 20 February 2013.

[3] *IP Office 8.1 Administering Voicemail Pro*, Document Number 15-601063, Issue 8b, 11 December 2012.

[4] *Administering Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, March 2013.

[5] *Installing Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, March 2013.

[6] *Upgrading Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, March 2013.

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

Product documentation for TSTT SIP Trunking Service is available from TSTT.

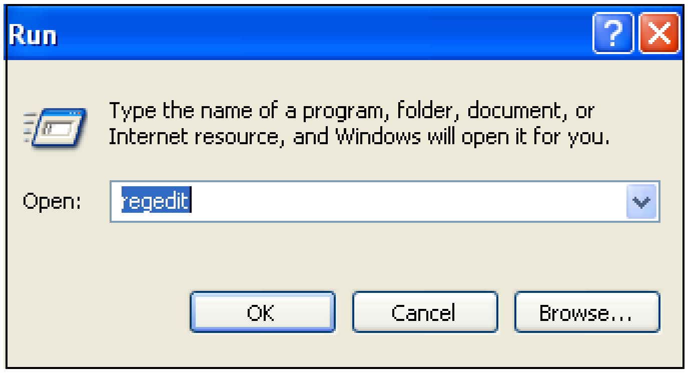
11. Appendix: SIP Line Template

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

Not all of the configuration information is included in the SIP Line Template, therefore, it is critical that the SIP Line configuration be verified/updated after a template has been imported, and additional configuration be supplemented using **Section 5.7** in these Application Notes as a reference.

To create a SIP Line Template from the configuration described in these Application Notes, configure the parameters as described below.

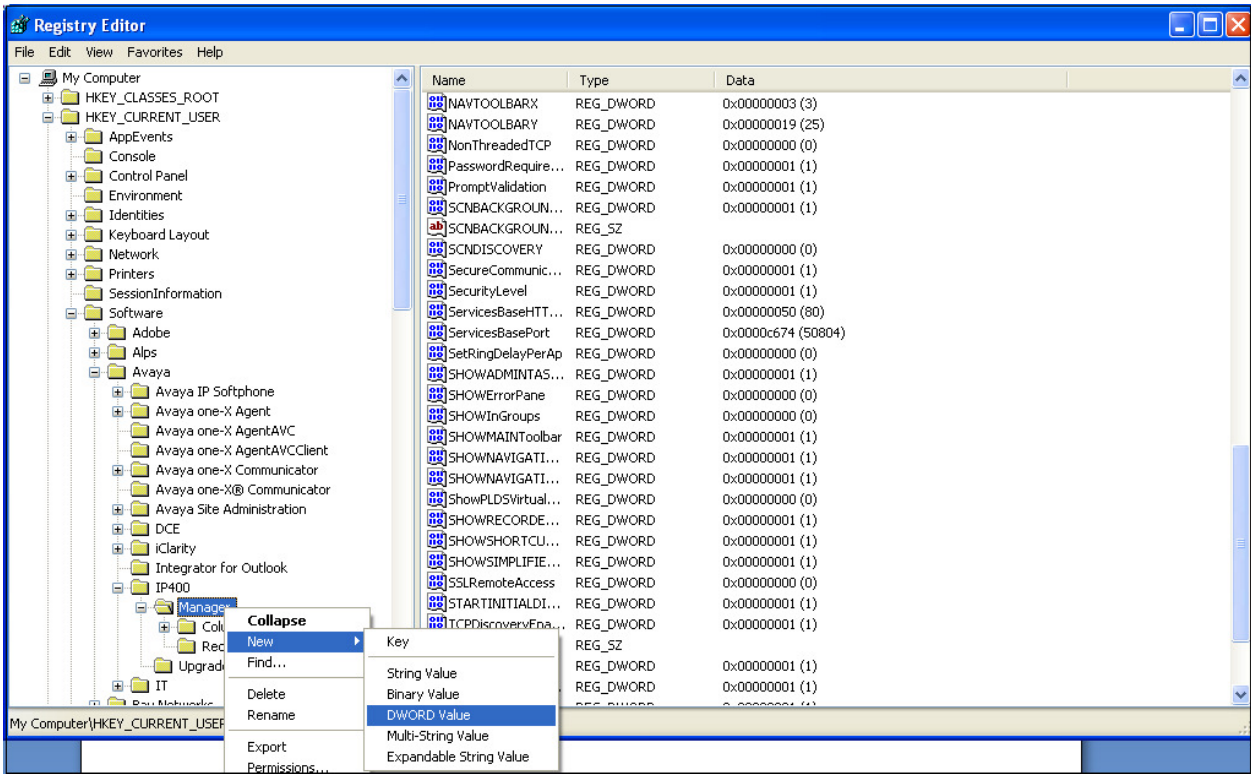
Use the Windows Registry Editor on the PC where Avaya IP Office Manager is installed to add a new **TemplateProvisioning** registry entry. Select **Start → Run**. Enter **regedit** in the **Open** box.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

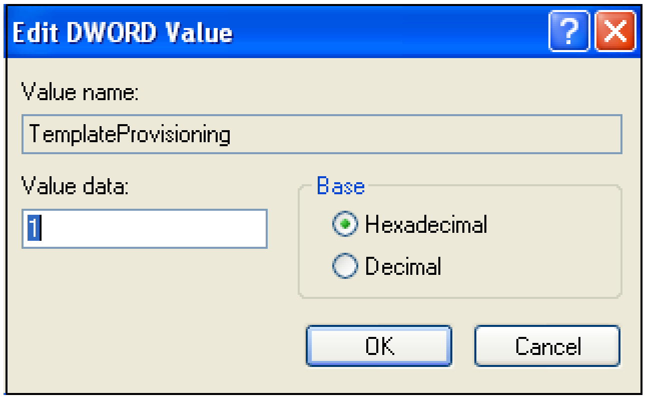
Open: regedit

On the Registry Editor, navigate to **HKEY_CURRENT_USER → Software → Avaya →IP400**. Right click on **Manager** and select **New → DWORD Value**.



Name	Type	Data
NAVTOOLBARX	REG_DWORD	0x00000003 (3)
NAVTOOLBARY	REG_DWORD	0x00000019 (25)
NonThreadedTCP	REG_DWORD	0x00000000 (0)
PasswordRequire...	REG_DWORD	0x00000001 (1)
PromptValidation	REG_DWORD	0x00000001 (1)
SCNBACKGROUN...	REG_DWORD	0x00000001 (1)
SCNBACKGROUN...	REG_SZ	
SCNDISCOVERY	REG_DWORD	0x00000000 (0)
SecureCommunic...	REG_DWORD	0x00000001 (1)
SecurityLevel	REG_DWORD	0x00000001 (1)
ServicesBaseHTT...	REG_DWORD	0x00000050 (80)
ServicesBasePort	REG_DWORD	0x0000c674 (50804)
SetRingDelayPerAp	REG_DWORD	0x00000000 (0)
SHOWADMINTAS...	REG_DWORD	0x00000001 (1)
SHOWErrorPane	REG_DWORD	0x00000000 (0)
SHOWInGroups	REG_DWORD	0x00000000 (0)
SHOWMAINToolbar	REG_DWORD	0x00000001 (1)
SHOWNAVIGATI...	REG_DWORD	0x00000001 (1)
SHOWNAVIGATI...	REG_DWORD	0x00000001 (1)
ShowPLDSVirtual...	REG_DWORD	0x00000000 (0)
SHOWRECORDE...	REG_DWORD	0x00000001 (1)
SHOWSHORTCU...	REG_DWORD	0x00000001 (1)
SHOWSIMPLIFIE...	REG_DWORD	0x00000001 (1)
SSLRemoteAccess	REG_DWORD	0x00000000 (0)
STARTINITIALDI...	REG_DWORD	0x00000001 (1)
TCPDiscoveryEna...	REG_DWORD	0x00000001 (1)
	REG_SZ	
	REG_DWORD	0x00000001 (1)
	REG_DWORD	0x00000001 (1)

Right click the newly created entry and rename it to **TemplateProvisioning**. Double click the entry and change the value under **Value Data** from “**0**” to “**1**”. Restart the PC.

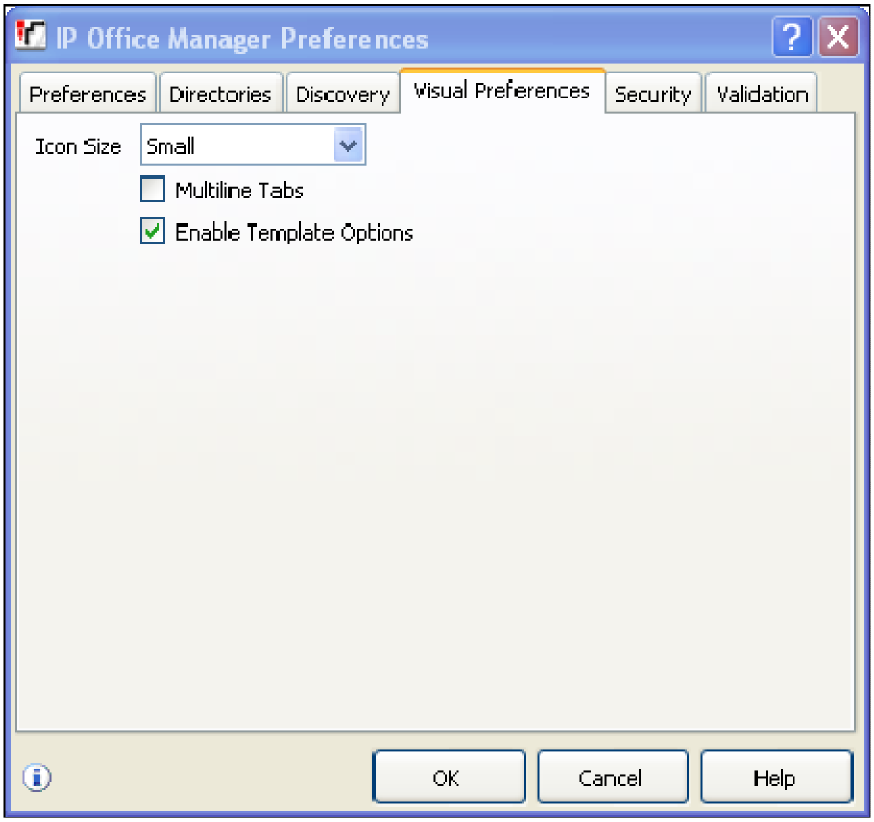


Value name: TemplateProvisioning

Value data: 1

Base
● Hexadecimal
○ Decimal

To enable template support in the IP Office Manager, select **File**, then **Preferences** (not shown). On the **Visual Preferences** tab, check the **Enable Template Options** box.

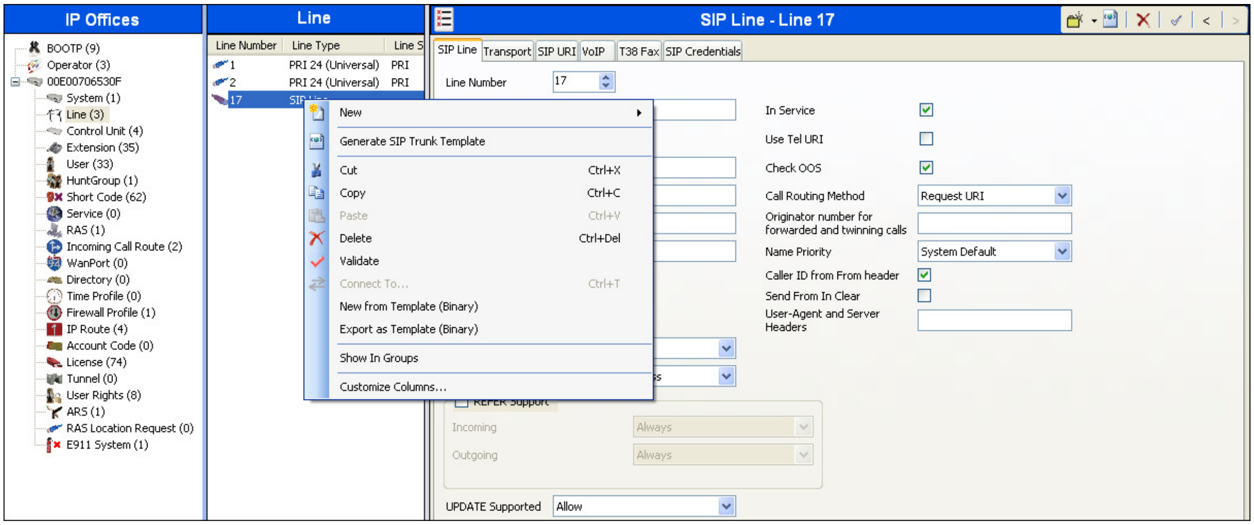


Icon Size: Small

☐ Multiline Tabs

☑ Enable Template Options

To create a SIP Line Template from the configuration, on the left Navigation Pane, right click the Sip Line (**17**), and select **Generate SIP Trunk Template**.



Line Number	Line Type	Line S
1	PRI 24 (Universal)	PRI
2	PRI 24 (Universal)	PRI
17	SIP Line	

Line Number: 17

In Service ☑

Use Tel URI ☐

Check OOS ☑

Call Routing Method: Request URI

Originator number for forwarded and twinning calls:

Name Priority: System Default

Caller ID from From header ☑

Send From In Clear ☐

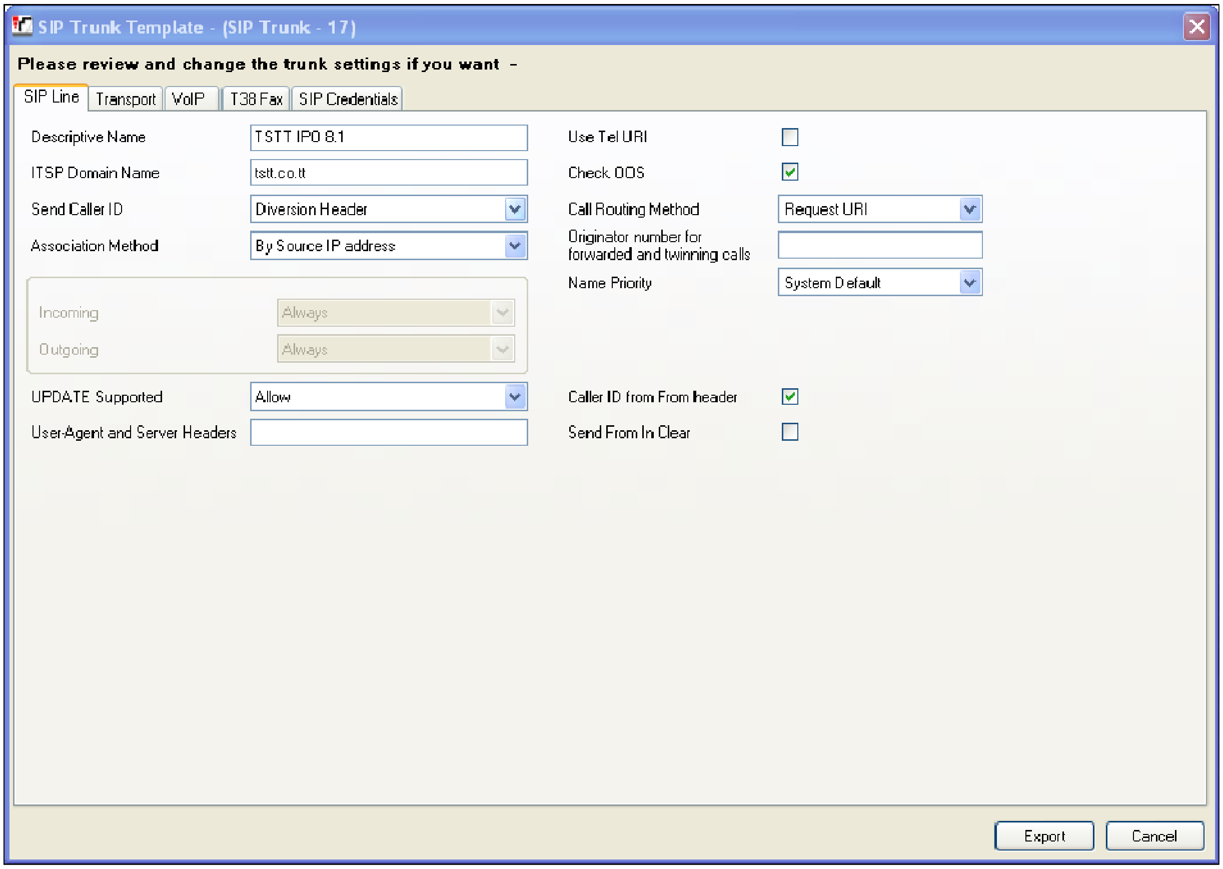
User-Agent and Server Headers:

Incoming: Always

Outgoing: Always

UPDATE Supported: Allow

The trunk's settings are displayed as configured in **Section 5.7.** Enter a descriptive name for the template, adjust the settings if required, and then click on **Export**.

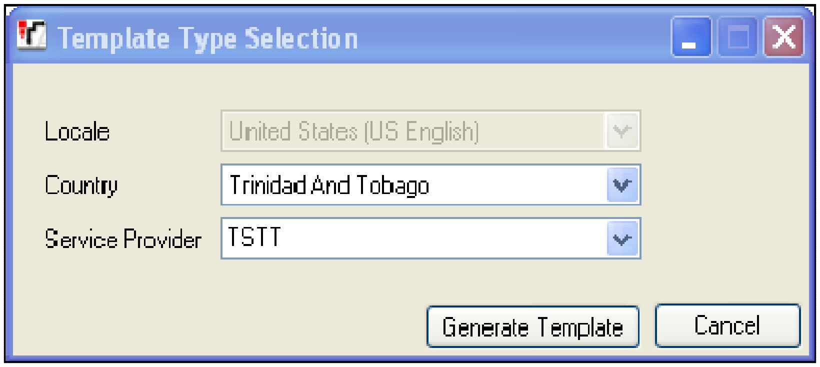


SIP Trunk Template - (SIP Trunk - 17)

Please review and change the trunk settings if you want -

Descriptive Name	TSTT IPO 8.1	Use Tel URI	□
ITSP Domain Name	tstt.co.tt	Check OOS	☑
Send Caller ID	Diversion Header	Call Routing Method	Request URI
Association Method	By Source IP address	Originator number for forwarded and twinning calls	
Incoming	Always	Name Priority	System Default
Outgoing	Always		
UPDATE Supported	Allow	Caller ID from From header	☑
User-Agent and Server Headers		Send From In Clear	□

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



Template Type Selection

Locale	United States (US English)
Country	Trinidad And Tobago
Service Provider	TSTT

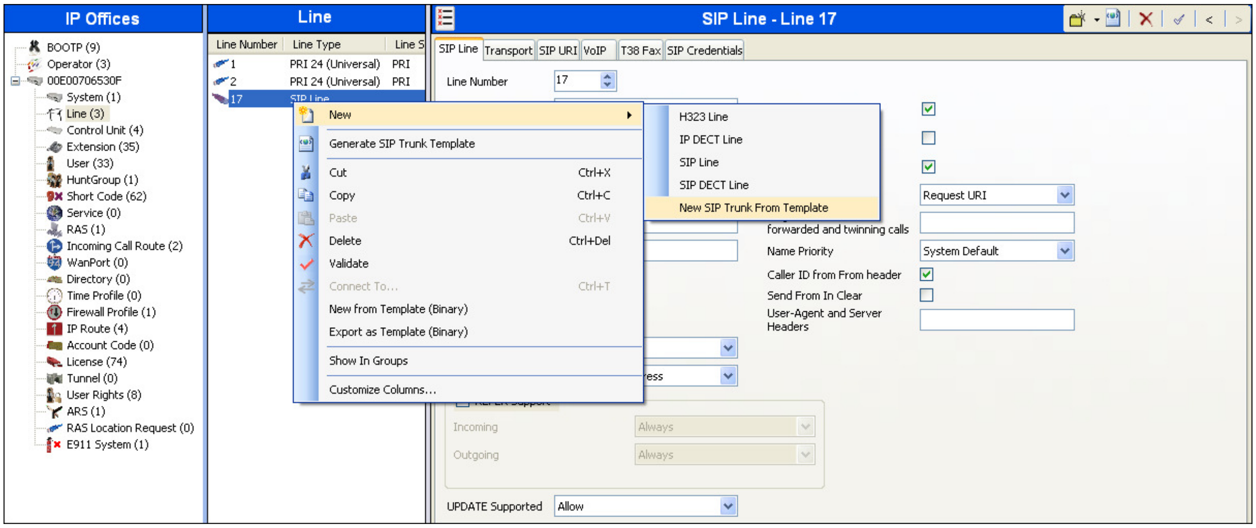
The following is the exported SIP Line Template file **TT_TSTT_SIPTrunk.xml**:

```
<?xml version="1.0" encoding="utf-8" ?>
<Template xmlns="urn:SIPTrunk-schema">
  <TemplateType>SIPTrunk</TemplateType>
  <Version>20130924</Version>
  <SystemLocale>enu</SystemLocale>
  <DescriptiveName>TSTT IPO 8.1</DescriptiveName>
  <ITSPDomainName>tstt.co.tt</ITSPDomainName>
  <SendCallerID>CallerIDDIV</SendCallerID>
  <ReferSupport>false</ReferSupport>
  <ReferSupportIncoming>1</ReferSupportIncoming>
  <ReferSupportOutgoing>1</ReferSupportOutgoing>
  <RegistrationRequired>false</RegistrationRequired>
  <UseTelURI>false</UseTelURI>
  <CheckOOS>true</CheckOOS>
  <CallRoutingMethod>1</CallRoutingMethod>
  <OriginatorNumber />
  <AssociationMethod>SourceIP</AssociationMethod>
  <LineNamePriority>SystemDefault</LineNamePriority>
  <UpdateSupport>UpdateAllow</UpdateSupport>
  <UserAgentServerHeader />
  <CallerIDfromFromheader>true</CallerIDfromFromheader>
  <PerformUserLevelPrivacy>false</PerformUserLevelPrivacy>
  <ITSPProxy>172.16.5.92</ITSPProxy>
  <LayerFourProtocol>SipUDP</LayerFourProtocol>
  <SendPort>5060</SendPort>
  <ListenPort>5060</ListenPort>
  <DNSServerOne>0.0.0.0</DNSServerOne>
  <DNSServerTwo>0.0.0.0</DNSServerTwo>
  <CallsRouteViaRegistrar>true</CallsRouteViaRegistrar>
  <SeparateRegistrar />
  <CompressionMode>AUTOSELECT</CompressionMode>
  <UseAdvVoiceCodecPrefs>true</UseAdvVoiceCodecPrefs>
  <AdvCodecPref>G.711 ULAW 64K,G.729(a) 8K CS-ACELP</AdvCodecPref>
  <CallInitiationTimeout>4</CallInitiationTimeout>
  <DTMFSupport>DTMF_SUPPORT_RFC2833</DTMFSupport>
  <VoipSilenceSupression>false</VoipSilenceSupression>
  <ReinviteSupported>true</ReinviteSupported>
  <FaxTransportSupport>FOIP_NONE</FaxTransportSupport>
  <UseOffererPrefferedCodec>false</UseOffererPrefferedCodec>
  <CodecLockdown>false</CodecLockdown>
  <Rel100Supported>true</Rel100Supported>
  <T38FaxVersion>3</T38FaxVersion>
  <Transport>UDPTL</Transport>
  <LowSpeed>0</LowSpeed>
  <HighSpeed>0</HighSpeed>
  <TCFMethod>Trans_TCF</TCFMethod>
  <MaxBitRate>FaxRate_14400</MaxBitRate>
  <EflagStartTimer>2600</EflagStartTimer>
```

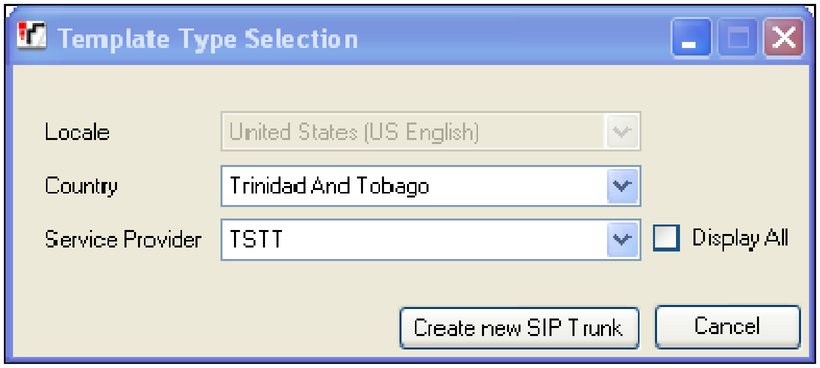
```
<EflagStopTimer>2300</EflagStopTimer>
<UseDefaultValues>true</UseDefaultValues>
<ScanLineFixup>true</ScanLineFixup>
<TFOPEnhancement>true</TFOPEnhancement>
<DisableT30ECM>false</DisableT30ECM>
<DisableEflagsForFirstDIS>false</DisableEflagsForFirstDIS>
<DisableT30MRCompression>false</DisableT30MRCompression>
<NSFOverride>false</NSFOverride>
</Template>
```

To import the template into a new IP Office system, copy and paste the exported xml template file into the Templates directory (C:\Program Files\Avaya\IP Office\Manager\Templates) on the PC where IP Office Manager for the new system is running.

Next, import the template into the new IP Office system by creating a new SIP Line as shown in the screenshot below. In the Navigation Pane on the left, right-click on **Line** then navigate to **New, New SIP Trunk From Template**:



On the next screen, **Template Type Selection**, verify that the information in the **Country** and **Service Provider** fields is correct. If more than one template is present, use the drop-down menus to select the required template. Click **Create new SIP Trunk** to finish the process.


Template Type Selection

Locale: United States (US English)

Country: Trinidad And Tobago

Service Provider: TSTT

□ Display All

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.