



## Avaya Solution & Interoperability Test Lab

# **Application Notes for Avaya IP Office Release 10.1, Avaya Session Border Controller for Enterprise Release 7.2 with the AT&T IP Toll Free Service – Issue 1.0**

### **Abstract**

These Application Notes describe the steps for configuring Avaya IP Office Release 10.1 and Avaya Session Border Controller for Enterprise Release 7.2, with the AT&T IP Toll Free service and AVPN or MIS/PNT transport connections.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution providing toll-free services over SIP trunks for business customers.

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

AT&T 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.

# 1. Introduction

These Application Notes describe a sample configuration using Session Initiation Protocol (SIP) trunking between an Avaya IP Office solution and the AT&T IP Toll Free service using **AVPN** or **MIS/PNT** transport connections. In the sample configuration, the Avaya IP Office solution consists of an Avaya IP Office IP500 V2, Avaya IP Office Platform Application Server, Avaya Communicator for Windows, Avaya SIP, H.323, digital, and analog endpoints.

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

The Avaya Session Border Controller for Enterprise is the point of connection between Avaya IP Office and the AT&T IP Toll Free service, and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling and media for interoperability.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution providing toll-free services over SIP trunks for business customers. The AT&T Toll Free service utilizes AVPN<sup>1</sup> or MIS/PNT<sup>2</sup> transport services.

**Note** – Avaya Session Border Controller for Enterprise will be referred to as *Avaya SBCE* in the remainder of this document. AT&T IP Toll Free service will be referred to as *IPTF* in the remainder of this document.

## 2. General Test Approach and Test Results

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.

The interoperability compliance testing focused on verifying inbound and outbound call flows between IPTF and the Customer Premises Equipment (CPE) containing Avaya IP Office Release 10.1 and Avaya SBCE Release 7.2 (see **Section 3.2** for call flow examples).

The test environment described in these Application Notes consisted of:

- A simulated enterprise with Avaya IP Office 10.1, Avaya SBCE 7.2, Avaya SIP, H.323 and Analog telephones, as well as a fax machine emulator (Ventafax).
- Laboratory versions of the IPTF service, to which the simulated enterprise was connected via AVPN/MIS transport.

---

<sup>1</sup> AVPN uses compressed RTP (cRTP).

<sup>2</sup> MIS/PNT does not support cRTP.

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

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

For the testing associated with this Application Note, the interface between Avaya systems and the AT&T Flexible Reach service did not include use of any specific encryption features as requested by AT&T.

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

## 2.1. Interoperability Compliance Testing

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the IPTF network. Calls were made from the PSTN across the IPTF test network, to the CPE.

The interoperability compliance testing focused on verifying inbound call flows (see **Section 3.2**) between Avaya IP Office, Avaya SBCE, and the IPTF service.

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the AT&T network.

The following SIP trunking VoIP features were tested with the IPTF service:

- Incoming calls from PSTN, routed by the IPTF service, to Avaya SBCE and Avaya IP Office. These calls are via the Avaya IP Office SIP Line and may be generated/answered by Avaya SIP telephones/softphones, H.323 telephones, Analog telephones, Analog fax machines or via Hunt Groups. Coverage to Voicemail Pro, and Voicemail Pro auto-attendant applications, were also used.
- Inbound fax using T.38 or G.711, and G3 or SG3 endpoints.
- Proper disconnect when the caller abandons a call before answer, and when the Avaya IP Office party or the PSTN party terminates an active call.
- Proper busy tone heard when an Avaya IP Office user calls a busy PSTN user, or a PSTN user calls a busy Avaya IP Office user (i.e., if no redirection was configured for user busy conditions).
- SIP OPTIONS monitoring the health of the SIP trunk. In the reference configuration Avaya IP Office sent OPTIONS to the IPTF service Border Element and AT&T

responded with *405 Method Not Allowed* (which is the expected response). That response is sufficient for Avaya IP Office to consider the connection up.

- Incoming calls using the G.729A and G.711 ULAW codecs.
- Long duration calls.
- DTMF transmission (RFC 2833) for successful voice mail navigation, including navigation of a simple auto-attendant application configured on Voicemail Pro, as well as IPTF DTMF generated features.
- Telephony features such as call waiting, hold, transfer, and conference.
- Avaya Remote Worker configuration (Avaya Communicator SIP softphone) via Avaya SBCE.
- Verify reception of IPTF SIP Multipart/NSS headers, including SDP and XML content.
- AT&T IP Toll Free features such as Legacy Transfer Connect and Alternate Destination Routing.

## 2.2. Test Results

The test objectives stated in **Section 2.1**, with limitations as noted below, were verified.

1. **Avaya IP Office only supports a packet size (ptime) of 20 msecs, and therefore does not specify a ptime value in the SIP SDP (in either requests or responses)** – Although no issues were found during testing, AT&T recommends that for maximum customer bandwidth utilization, a ptime value of 30 should be specified.
2. **IP Toll Free ADR Call Redirection feature based on SIP error code response** – Upon receiving an error response, IPTF service can be configured to invoke ADR Call Redirection. The following error codes were producible by the reference configuration and tested successfully; 408 Request Timeout, 480 Temporarily Unavailable, 486 Busy Here, and 500 Server Internal Error. The following error codes are also supported by IPTF service, but were not producible by the reference configuration, and thus not tested; 503 Service Unavailable, 504 Server Timeout, and 600 Busy Everywhere.
3. **Enhanced CID – NSS feature** – The inbound calls to Avaya IP Office are not exercising the Enhanced CID feature. Although Avaya IP Office is accepting SIP Multipart/NSS headers, it is neither passing nor acting upon it. It is simply being ignored.
4. **IP Office determines the codec priority** – IP Office will follow the codec priority based on the Codec Selection on the SIP Line VoIP tab, see **Section 5.4.6**. It will not follow the codec priority set by the IPTF service.
5. **Inbound User-to-User Information is not supported with IP Office** – User-to-User Information (UUI) is not supported on inbound SIP trunk calls. IP Office is able to successfully receive an inbound call from AT&T containing UUI, but the UUI data is simply ignored.
6. **Inbound Super Group 3 fax calls** – Avaya IP Office may not renegotiate to T.38 for inbound fax calls if both fax devices support Super Group 3 (SG3) speeds. If the SG3 connection is fully established at the beginning of the call, the CPE fax device may not negotiate down to G3 speeds and IP Office will not detect the G3 tones necessary for T.38. See **Section 5.5.6**. Since T.38 is the preferred method, if the CPE device supports SG3 speeds (33600 bps), the recommendation is to also disable SG3 on the CPE fax device if possible.

## 2.3. Support

AT&T customers may obtain support for the AT&T IP Toll Free service by calling (800) 325-5555.

Avaya customers may obtain documentation and support for Avaya products by visiting: <http://support.avaya.com>. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus. Customers may also use specific numbers (provided on <http://support.avaya.com>) to directly access specific support and consultation services based upon their Avaya support agreements.

## 3. Reference Configuration

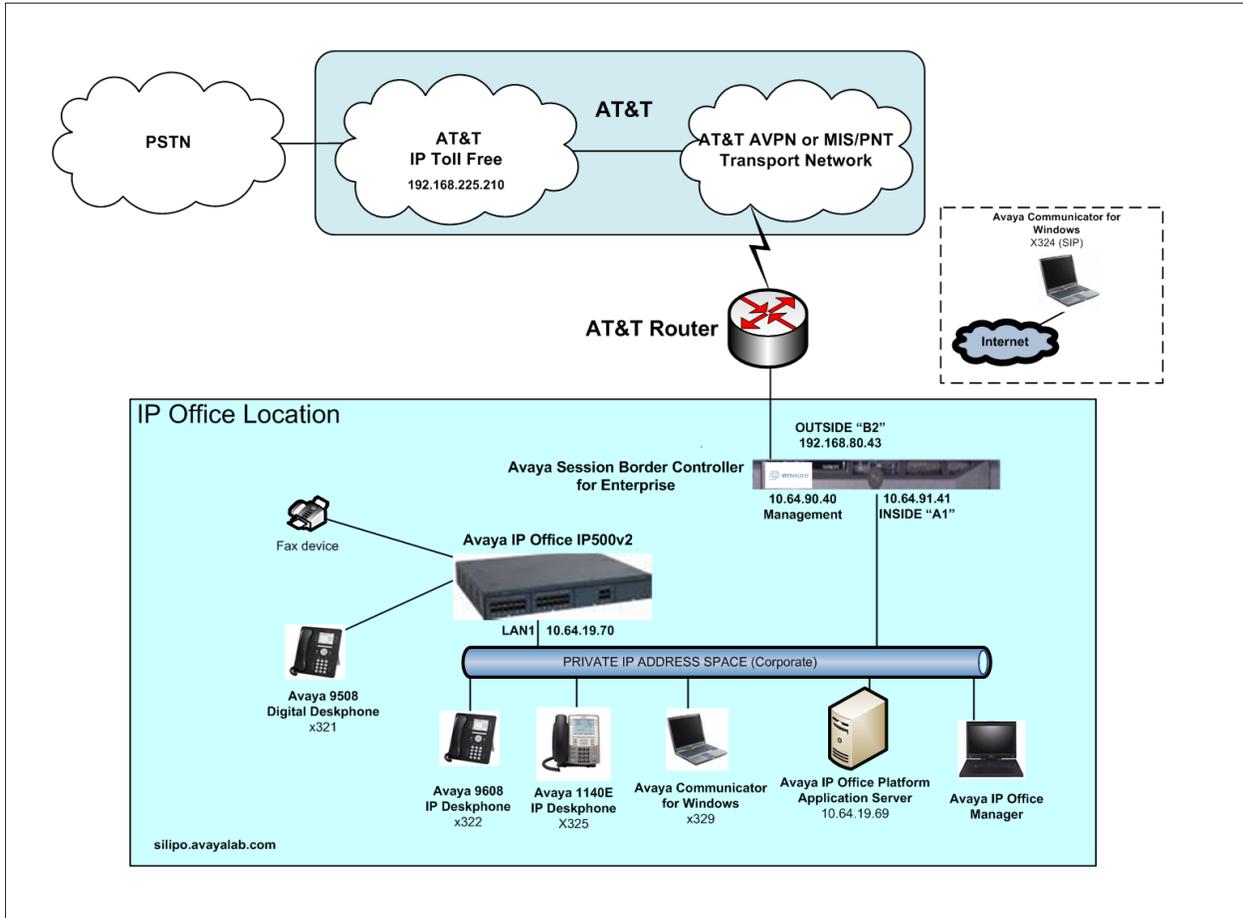
**Note** – Documents used to provision the test environment are listed in **Section 11**. References to these documents are indicated by the notation [x], where x is the document reference number.

The reference configuration used in these Application Notes is shown in **Figure 1** on the next page and consists of the following components:

- Avaya IP Office provides the voice communications services for a particular enterprise site. In the reference configuration, Avaya IP Office runs on the IP 500 V2 platform. This solution is extensible to the Avaya IP Office Server Edition platform as well.
- Voicemail Pro (running on the Application Server) provided the voice messaging capabilities in the reference configuration. This solution is extensible to the Avaya IP Office embedded voice mail as well.
- Avaya endpoints are represented with an Avaya 9608 H.323 Deskphone, an Avaya 9508 Digital Telephone, an Avaya 6211 Analog Telephone, an Avaya 1140E SIP Deskphone, and Avaya Communicator for Windows. Fax endpoints are represented by PCs running Ventafax emulation software connected by modem to an analog port.
- The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPTF service and the CPE. In the reference configuration, the Avaya SBCE runs on a VMWare platform.
- In the reference configuration, both the Avaya IP Office (interface “LAN1”), and the Avaya SBCE (interface “A1”) are connected to the private CPE network. The Avaya SBCE interface “B1” is connected to the AT&T network.
- TLS/5061 is the recommended transport protocol/port to use on the Avaya IP Office LAN1 connection to the Avaya SBCE A1 interface.
- UDP transport via port 5060 was used between the Avaya SBCE and AT&T.
- The AT&T IPTF service requires RTP port ranges 16384-32767.
- AT&T provided the inbound and outbound access numbers (DID and DNIS) used in the reference configuration. Note that the IPTF service may deliver various digit lengths in the SIP Invite Request-URI depending on the circuit order provisioning. In the reference configuration, the IPTF service delivered 15 digits.
- An Avaya Remote Worker endpoint (Avaya Communicator for Windows) was used in the reference configuration. The Remote Worker endpoint resides on the public side of an Avaya

SBCE (via a TLS connection), and registers/communicates with Avaya IP Office as though it was an endpoint residing in the private CPE space.

**Note** – The configuration of the Remote Worker environment is beyond the scope of this document. Refer to [7] for information on Remote Worker deployments.



**Figure 1: Reference Configuration**

### 3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes, and are for illustrative purposes only. Customers must obtain and use the values based on their own specific configurations.

**Note** – The Avaya SBCE “B1” interface communicates with AT&T Border Elements (BEs) located in the AT&T IPTF network. For security reasons, the IP addresses of the AT&T BEs are not included in this document. However as placeholders in the following configuration sections, the IP addresses **192.168.80.43** (Avaya SBCE “B1”), and **192.168.225.210** (AT&T BE address), are specified. In addition, AT&T DID/DNIS numbers shown in this document are examples as well. AT&T Customer Care will provide the actual Border Element IP addresses and DID/DNIS numbers as part of the IPTF provisioning process.

Component	Illustrative Value in these Application Notes
<b>Avaya IP Office</b>	
Private network LAN1 interface	10.64.19.70
<b>Avaya SBCE</b>	
Private network “A1” interface	10.64.91.41
Public network “B1” interface	192.168.80.43
<b>AT&amp;T IPTF Service</b>	
Border Element IP Address	192.168.225.210

**Table 1: Illustrative Values Used in these Application Notes**

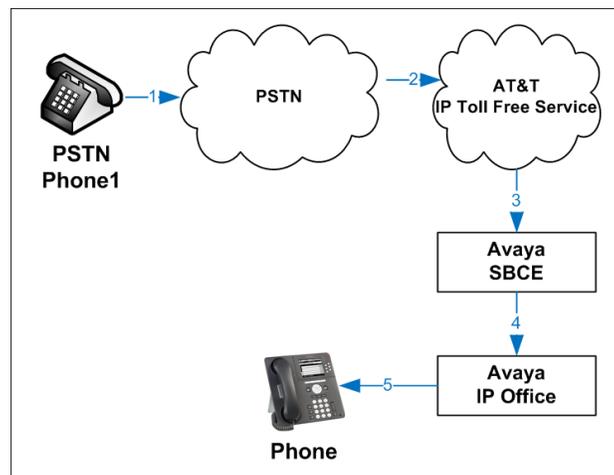
## 3.2. Call Flows

To understand how inbound AT&T IPTF service calls are handled by Avaya IP Office, two basic call flows are described in this section.

### 3.2.1. Basic Inbound

The first call scenario illustrated in the figure below is an inbound AT&T IPTF service call that arrives on Avaya IP Office, which in turn routes the call to a hunt group, phone or a fax endpoint.

1. A PSTN phone originates a call to an IPTF service number.
2. The PSTN routes the call to the AT&T IPTF service network.
3. The AT&T IPTF service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any specified SIP header modifications, and routes the call to Avaya IP Office.
5. Avaya IP Office applies any necessary digit manipulations based upon the DID and routes the call to a hunt group, phone or a fax endpoint.

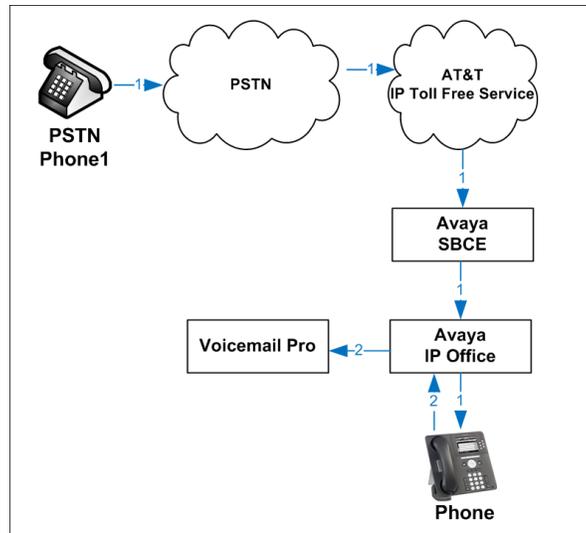


**Figure 2: Inbound AT&T IPTF Call**

### 3.2.2. Coverage to Voicemail

The call scenario illustrated in the figure below is an inbound call that is covered to Voicemail. In the reference configuration, the Voicemail system used is Voicemail Pro, running on the Application Server.

1. Same as the first call scenario in **Section 3.2.1**.
2. The Avaya IP Office phone does not answer the call, and the call covers to the external application Avaya IP Office Voicemail Pro.



**Figure 3: Coverage to Voicemail (Voicemail Pro)**

## 4. Equipment and Software Validated

The following equipment and software was used for the reference configuration described in these Application Notes.

Equipment/Software	Release/Version
Avaya Session Border Controller for Enterprise	Release 7.2.1.0-05-14222
Avaya IP Office IP500 V2 <ul style="list-style-type: none"><li>▪ IP Office</li><li>▪ Avaya IP Office TCM 8</li><li>▪ Avaya IP Office COMBO6210/ATM4</li></ul>	Release 10.1.0.1.0 build 3 Release 10.1.0.1.0 build 3 Release 10.1.0.1.0 build 3
Avaya IP Office Platform Application Server <ul style="list-style-type: none"><li>▪ Voicemail Pro</li><li>▪ Avaya WebRTC Gateway</li><li>▪ Avaya one-X® Portal for IP Office</li></ul>	Release 10.1.0.1.0 build 3 Release 10.1.0.1.0 build 3 Release 10.1.0.1.0 build 3
Avaya IP Office Manager	Release 10.1.0.1.0 build 3
Avaya 9611SW IP Deskphone (H.323)	Release 6.6506
Avaya 1140E IP Deskphone (SIP)	Release 04.04.23
Avaya 9508 Digital Telephone	Release 0.60
Avaya Communicator for Windows	Release 2.1.4.256
Analog Fax device	Ventafax 7.9

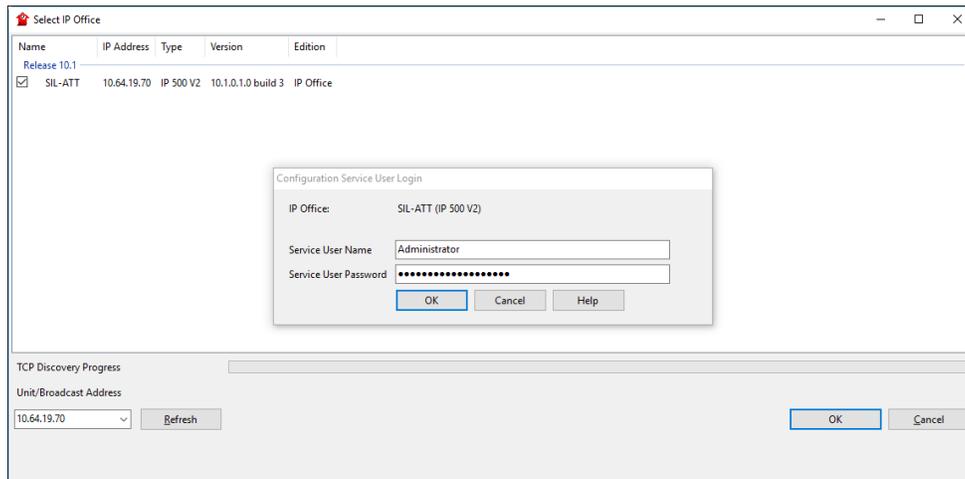
**Table 2: Equipment and Software Versions**

**Note** – Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2, and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks.

## 5. Avaya IP Office Configuration

**Note** – This section describes attributes of the reference configuration, but is not meant to be prescriptive. In the following sections, only the parameters that are highlighted in **bold** text are applicable to the reference configuration. Other parameter values may or may not match based on local configurations. Many forms contain multiple tabs. Only those tabs with provisioning related to the reference configuration are discussed. Any other tab/form should be considered default values. Additionally, the screen shots referenced in these sections may not be the complete form.

IP Office is configured via the IP Office Manager program. For more information on IP Office Manager, consult references [1], [2], and [3]. From the IP Office Manager PC, select **Start → All Apps → IP Office → Manager** to launch the Manager application. Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials.



The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this section, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center, and the Details pane on the right side.

## 5.1. Licensing and Physical Hardware

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. Confirm a valid **SIP Trunk Channels** license with sufficient **Instances** (trunk channels). If Avaya IP Telephones will be used as is the case in these Application Notes, verify the **Avaya IP endpoints** license.

Feature	Instances	Status	Expiration Date	Source
IPSec Tunnelling	1	Valid	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Customer Service Agent	100	Valid	Never	PLDS Nodal
Customer Service Supervisor	100	Valid	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Valid	Never	PLDS Nodal
SIP Trunk Channels	128	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Valid	Never	PLDS Nodal
CTI Link Pro	1	Valid	Never	PLDS Nodal
Wave User	16	Valid	Never	PLDS Nodal
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal
Essential Edition	1	Valid	Never	PLDS Nodal

In the sample configuration, looking at the IP500 V2 from left to right, the first module is a TCM 8 Digital Station Module. This module supports BCM / Norstar T-Series and M-Series telephones. The second module is a COMBO6210/ATM4 module. This module is used to add a combination of ports to an IP500 V2 control unit and is not supported by IP500 control units. The module supports 10 voice compression channels. Codec support is G.722, G.711, G729A and G.723 with 64ms echo cancellation. The “Combo” card will support 6 Digital Station ports for digital stations in slots 1-6 (except 3800, 4100, 4400, 7400, M and T-Series), 2 Analog Extension ports in slots 7-8, and 4 Analog Trunk ports in slots 9-12.

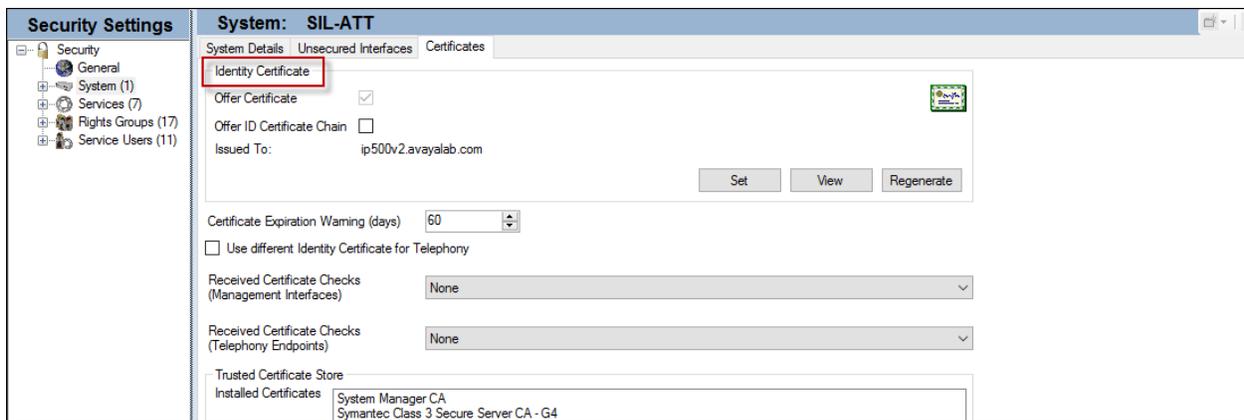
IP Offices	Control Unit	IP 500 V2																								
<ul style="list-style-type: none"> <li>BOOTP (22)</li> <li>Operator (3)</li> <li>SIL-ATT</li> <li>System (1)</li> <li>Line (8)</li> <li>Control Unit (3)</li> <li>Extension (23)</li> <li>User (25)</li> <li>Group (5)</li> <li>Short Code (79)</li> <li>Service (0)</li> <li>RAS (1)</li> <li>Incoming Call Rou</li> <li>WAN Port (0)</li> <li>Directory (0)</li> <li>Time Profile (0)</li> </ul>	<table border="1"> <thead> <tr> <th>Dev No.</th> <th>Dev Type</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>IP 500 V2</td> </tr> <tr> <td>2</td> <td>TCM8</td> </tr> <tr> <td>3</td> <td>COMBO6210/ATM4</td> </tr> </tbody> </table>	Dev No.	Dev Type	1	IP 500 V2	2	TCM8	3	COMBO6210/ATM4	<table border="1"> <thead> <tr> <th>Unit</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Device Number</td> <td>1</td> </tr> <tr> <td>Unit Type</td> <td>IP 500 V2</td> </tr> <tr> <td>Version</td> <td>10.1.0.1.0 build 3</td> </tr> <tr> <td>Serial Number</td> <td>00e007058e33</td> </tr> <tr> <td>Unit IP Address</td> <td>10.64.19.70</td> </tr> <tr> <td>Interconnect Number</td> <td>0</td> </tr> <tr> <td>Module Number</td> <td>Control Unit</td> </tr> </tbody> </table>	Unit	Value	Device Number	1	Unit Type	IP 500 V2	Version	10.1.0.1.0 build 3	Serial Number	00e007058e33	Unit IP Address	10.64.19.70	Interconnect Number	0	Module Number	Control Unit
Dev No.	Dev Type																									
1	IP 500 V2																									
2	TCM8																									
3	COMBO6210/ATM4																									
Unit	Value																									
Device Number	1																									
Unit Type	IP 500 V2																									
Version	10.1.0.1.0 build 3																									
Serial Number	00e007058e33																									
Unit IP Address	10.64.19.70																									
Interconnect Number	0																									
Module Number	Control Unit																									

## 5.2. TLS Management

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

To view the certificates currently installed on IP Office, navigate to **File → Advanced → Security Settings**. Log in with the appropriate security credentials (not shown). In the Security Settings window, navigate to **Security → System** and select the **Certificates** tab.

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

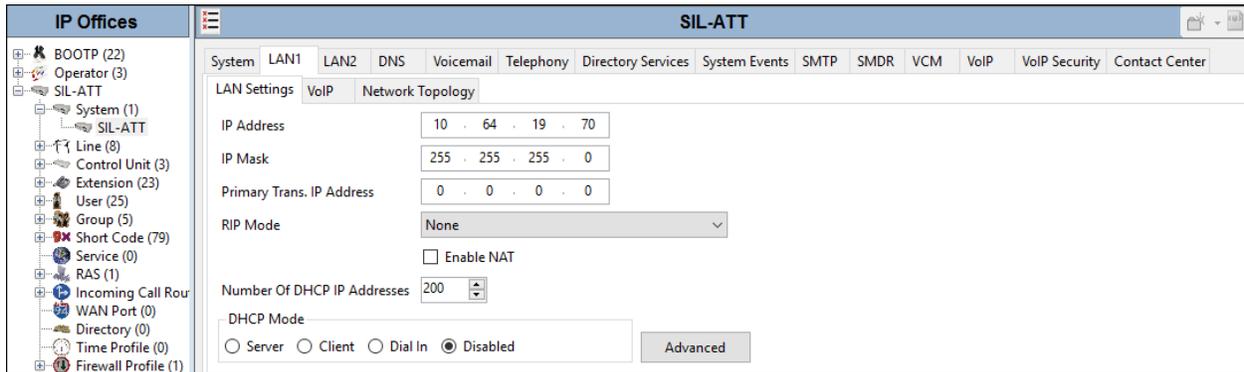


## 5.3. System Settings

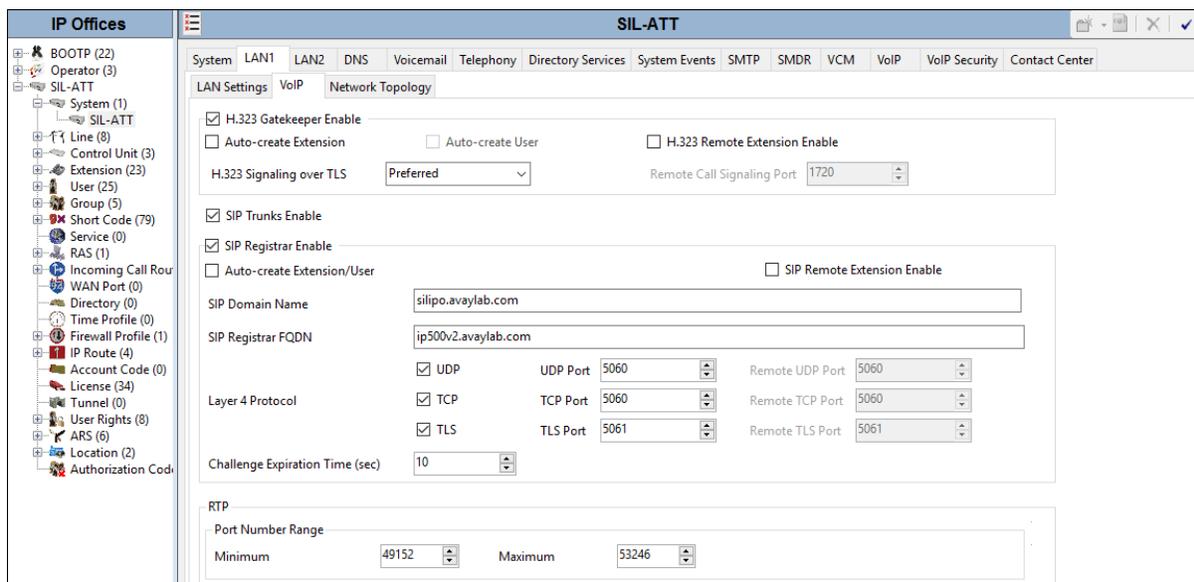
This section illustrates the configuration of system settings. Select **System** in the Navigation pane to configure these settings. The subsection order corresponds to a left to right navigation of the tabs in the Details pane for System settings. For all of the following configuration sections, the **OK** button (not shown) must be selected in order for any changes to be saved.

### 5.3.1. LAN Settings

In the sample configuration, LAN1 is used to connect IP Office to the enterprise network. To view or configure the **IP Address** of LAN1, select the **LAN1** tab followed by the **LAN Settings** tab. As shown in **Figure 1**, the IP Address of IP Office is **10.64.19.70**. Other parameters on this screen may be set according to customer requirements.



Select the **VoIP** tab as shown in the following screen. The **H323 Gatekeeper Enable** parameter is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the Avaya 9808 used in the sample configuration. The **SIP Registrar Enable** parameter is checked to allow Avaya 1140E and Avaya Communicator usage. The **SIP Trunks Enable** parameter must be checked to enable the configuration of SIP trunks to AT&T. The **SIP Domain Name** and **SIP Registrar FQDN** may be set according to customer requirements. If desired, the **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media paths from Avaya SBCE to IP Office. The defaults are used here.



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

IP Office can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Service policies. In the sample configuration shown below, IP Office will mark SIP signaling with a value associated with “Assured Forwarding” using DSCP decimal 28 (**SIG DSCP** parameter). IP Office will mark the RTP media with a value associated with “Expedited Forwarding” using DSCP decimal 46 (**DSCP** parameter). This screen enables flexibility in IP Office DiffServ markings (RFC 2474) to allow alignment with network routing policies, which are outside the scope of these Application Notes. Other parameters on this screen may be set according to customer requirements.

The screenshot shows the configuration interface for IP Office. The **Keepalives** section is expanded, showing the **Scope** set to **RTP-RTCP**, the **Periodic timeout** set to **30**, and **Initial keepalives** set to **Enabled**. Below this, the **DiffServ Settings** section is visible, containing several dropdown menus for DSCP values: **DSCP(Hex)** (B8), **DSCP (Hex)** (FC), **SIG DSCP (Hex)** (88), **DSCP** (46), **Video DSCP** (46), **DSCP Mask** (63), and **SIG DSCP** (34).

Select the **Network Topology** tab as shown in the following screen. The **Firewall/NAT Type** is set to **Unknown** in the sample configuration. The **Public IP Address** and **Public Port** sections are not used for the AT&T IPTF SIP trunk service connection.

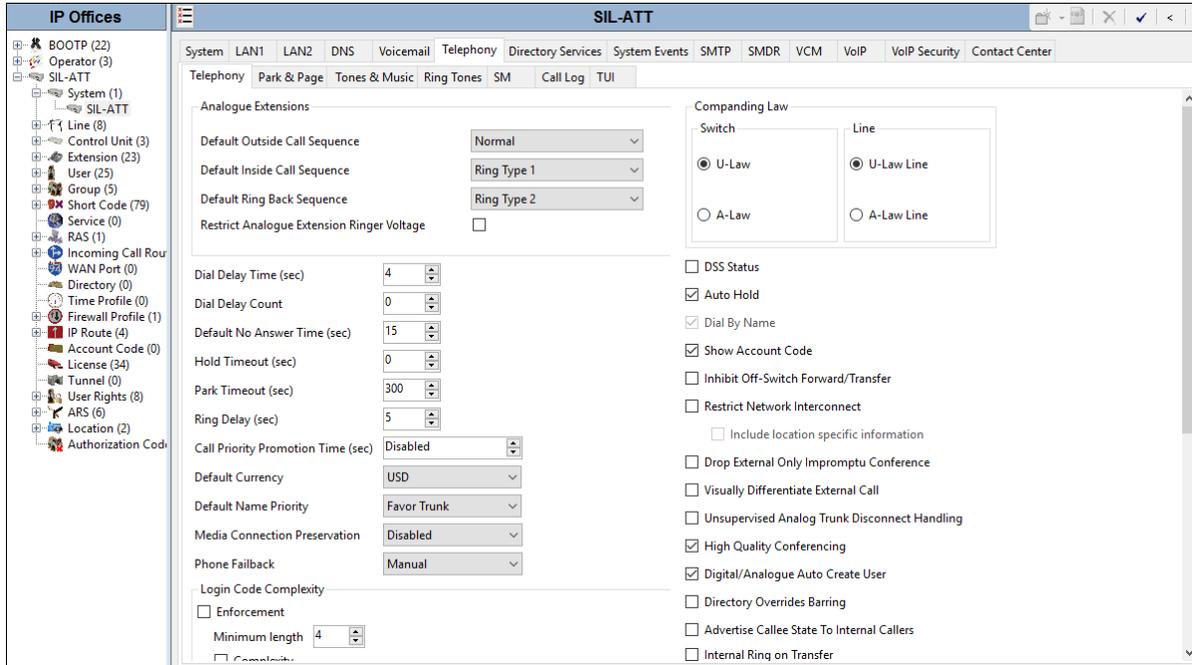
The screenshot shows the IP Office configuration interface with the **Network Topology** tab selected. The **STUN Server Address** is set to **0.0.0.0** and the **STUN Port** is set to **3478**. The **Firewall/NAT Type** is set to **Unknown**. The **Binding Refresh Time (sec)** is set to **60**. The **Public IP Address** is set to **0 . 0 . 0 . 0**. The **Public Port** section shows **UDP**, **TCP**, and **TLS** all set to **0**. There are **Run STUN** and **Cancel** buttons. A checkbox for **Run STUN on startup** is present and unchecked.

### 5.3.2. System Telephony Configuration

To view or change telephony settings, select the **Telephony** tab and **Telephony** sub-tab as shown below. The settings presented here simply illustrate the values used in the reference configuration and are not intended to be prescriptive.

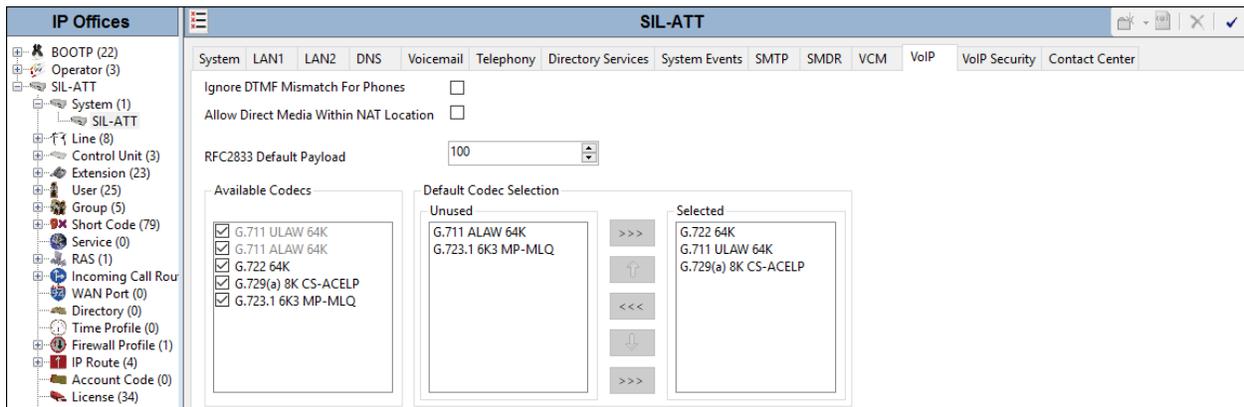
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box. This is so that call forwarding and call transfer to PSTN destinations via the AT&T IPTF service can be tested.
- Set the **Companding Law** parameters to **U-Law** as is typical in North America.

Default values are used in the other fields.



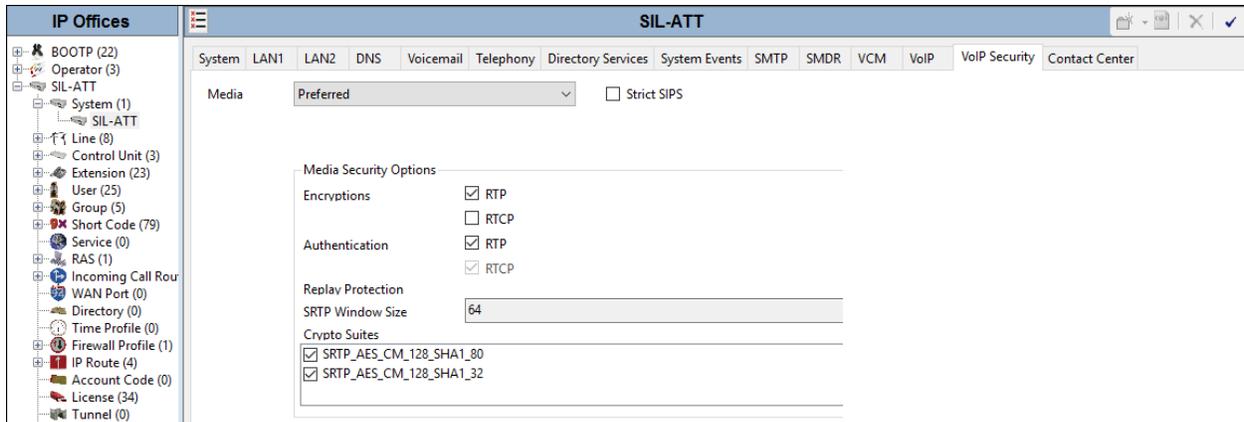
### 5.3.3. System Codecs Configuration

To view or change system codec settings, select the **VoIP** tab. On the left, observe the list of **Available Codecs**. In the example screen below, which is not intended to be prescriptive, the parameter next to each codec is checked, making all the codecs available in other screens where codec configuration may be performed (such as the SIP Line in **Section 5.5**). The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis, using the up, down, left, and right arrows. By default, all IP (SIP and H.323) lines and extensions will assume the system default codec selection, unless configured otherwise for the specific line or extension. The **RFC2833 Default Payload** parameter is set to **100**, the value preferred by AT&T.



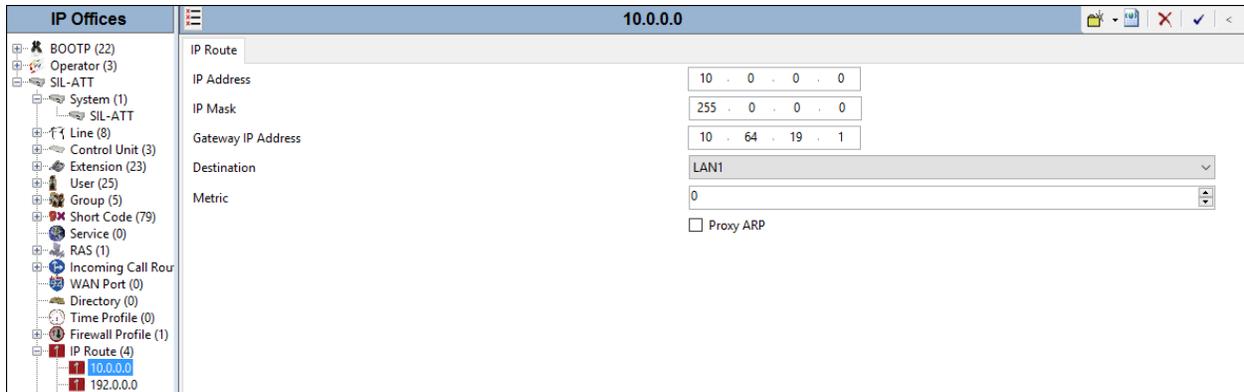
### 5.3.4. VoIP Security

For the compliance test, SRTP was used internal to the enterprise wherever possible. To view or configure the media encryption settings, select the **VoIP Security** tab. Set the **Media** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption. Under **Media Security Options**, select **RTP** for the **Encryptions** and **Authentication** fields. Under **Crypto Suites**, select **SRTP\_AES\_CM\_128\_SHA1\_80** and **SRTP\_AES\_CM\_128\_SHA1\_32**. Click **OK** to commit (not shown).



## 5.4. IP Route

In the sample configuration, IP Office LAN1 port is physically connected to the local area network switch at the IP Office customer site. The default gateway for this network is 10.64.19.1. The Avaya SBCE resides on a different subnet and requires an IP route to allow SIP traffic between the two devices. To add an IP route, right-click **IP Route** from the Navigation pane, and select **New** (not shown). To view or edit an existing route, select **IP Route** from the Navigation pane, and select the appropriate route from the Group pane. The following screen shows the Details pane with the relevant route using **Destination LAN1**.



## 5.5. SIP Line

The following sections describe the configuration of a SIP Line. The SIP Line terminates the CPE end of the SIP trunk to the AT&T IPTF service.

The recommended method for creating/configuring a SIP Line is to use the template associated with the provisioning described in these Application Notes. The template is an .xml file that can be used by Avaya IP Office Manager to create a new SIP Line for SIP trunking with the AT&T IPTF service. Follow the steps in **Section 5.5.2** to create a SIP Trunk from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary, after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration as shown in **Sections 5.5.3 – 5.5.7**.

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

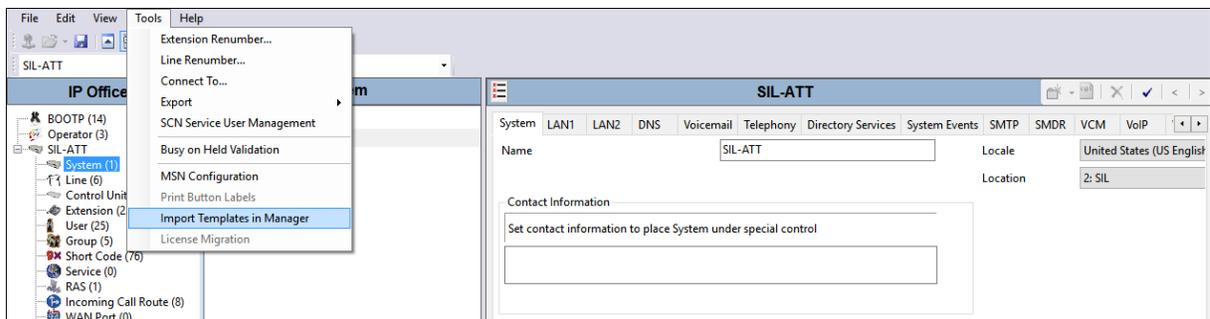
- SIL Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Requirements
- SIP Advanced Engineering

Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.5.3 – 5.5.8**.

### 5.5.1. Importing a SIP Line Template

**Note** – DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (IP500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer’s environment.

1. Copy a previously created template file to a location (e.g., *\temp*) on the same computer where IP Office Manager is installed.
2. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**.

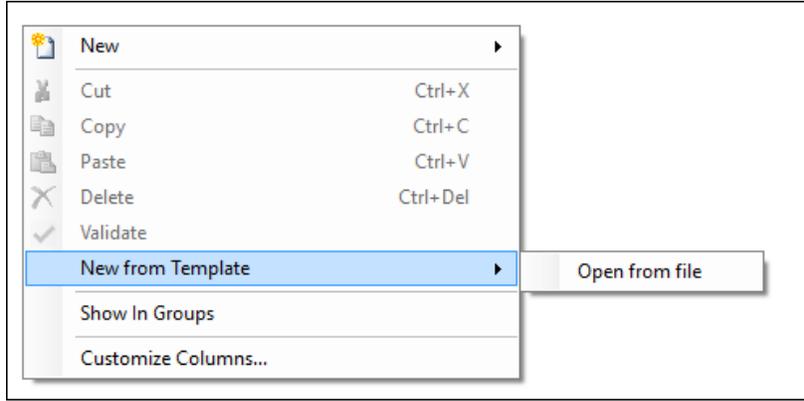


3. A folder browser will open (not shown). Select the directory used in **step 1** to store the template(s) (e.g., *\temp*). The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.
4. After the import is complete, a final import status pop-up window will open stating success or failure.

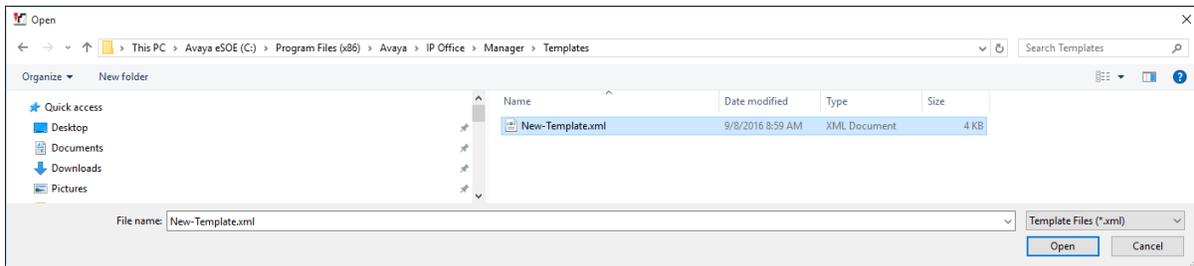


## 5.5.2. Creating a SIP Trunk from an XML Template

1. To create the SIP Trunk from a template, right-click on **Line** in the Navigation Pane, and hover over **New from Template**, and select either the imported template file listed (not shown) or **Open from file**.



If **Open from file** was selected, navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates**. Select **\*.xml** as the file type, find the template, and click **Open**.



The newly created SIP Line will appear in the Navigation pane (e.g., SIP Line 2).

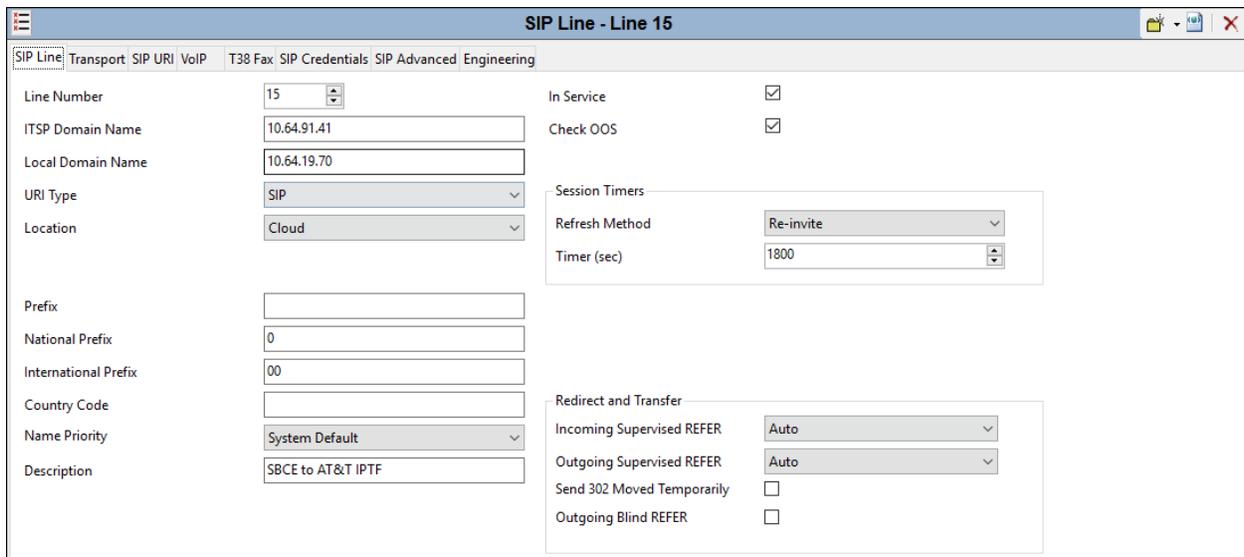
Line Number	Line Type	Line SubType
1	IP Office Line	WebSocket Server SCN
3	IP Office Line	WebSocket Server SCN
2	SIP Line	

Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.5.3 – 5.5.8**.

## 5.5.3. SIP Line - SIP Line tab

The **SIP Line** tab is shown below for **Line Number 15**, used for the SIP Trunk to AT&T. Note, if no SIP Line exists, right click on the **Line** item in the **Navigation** pane and select **New → SIP Line** (not shown). In the reference configuration, SIP Line 15 was created. The SIP Line form is completed as follows:

- **ITSP Domain Name:** Set to the IP address of the Avaya SBCE “A1” interface (e.g., **10.64.91.41**).
- **Local Domain Name:** Set to the IP address of the Avaya IP Office LAN1 interface (e.g., **10.64.19.70**).
- **In Service** and **Check OOS:** These boxes are checked (default).
- **Refresh Method:** Set to **Re-Invite**, as AT&T does not support UPDATE.
- **Incoming Supervised Refer:** Set this field to **Auto** (default).
- **Outgoing Supervised Refer:** Set this field to **Auto** (default).
- **Send 302 Moved Temporarily:** Verify this field is unchecked (default).
- **Outgoing Blind REFER:** Verify this field is unchecked (default).
- Use the default values for the other fields.
- Click **OK** (not shown).



**SIP Line - Line 15**

SIP Line | Transport: SIP | URI: VoIP | T38 Fax: SIP Credentials | SIP Advanced | Engineering

Line Number	15	In Service	<input checked="" type="checkbox"/>
ITSP Domain Name	10.64.91.41	Check OOS	<input checked="" type="checkbox"/>
Local Domain Name	10.64.19.70		
URI Type	SIP	Session Timers	
Location	Cloud	Refresh Method	Re-invite
		Timer (sec)	1800
Prefix			
National Prefix	0	Redirect and Transfer	
International Prefix	00	Incoming Supervised REFER	Auto
Country Code		Outgoing Supervised REFER	Auto
Name Priority	System Default	Send 302 Moved Temporarily	<input type="checkbox"/>
Description	SBCE to AT&T IPTF	Outgoing Blind REFER	<input type="checkbox"/>

### 5.5.4. SIP Line - Transport tab

Select the **SIP Line** → **Transport** tab and configure the following:

- **ITSP Proxy Address:** Set to the Avaya SBCE “A1” interface (e.g., **10.64.91.41**).
- **Network Configuration** → **Layer 4 Protocol:** Set to **TLS**.
- **Network Configuration** → **Send Port:** Set to **5061**.
- **Network Configuration** → **Use Network Topology Info:** Set to **None**.
- **Calls Route via Registrar:** Verify this field is checked (default).
- **Click OK** (not shown).

The screenshot shows the 'Transport' tab of a SIP Line configuration. The 'ITSP Proxy Address' is set to '10.64.91.41'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'TLS', 'Send Port' is '5061', and 'Use Network Topology Info' is set to 'None'. 'Listen Port' is also '5061'. 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0'. 'Calls Route via Registrar' is checked. 'Separate Registrar' is an empty field.

SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials	SIP Advanced	Engineering
ITSP Proxy Address: 10.64.91.41							
Network Configuration							
Layer 4 Protocol		TLS		Send Port		5061	
Use Network Topology Info		None		Listen Port		5061	
Explicit DNS Server(s)		0 . 0 . 0 . 0		0 . 0 . 0 . 0			
Calls Route via Registrar		<input checked="" type="checkbox"/>					
Separate Registrar							

### 5.5.5. SIP Line - SIP URI tab

Select the **SIP Line** → **SIP URI** tab. To add a new SIP URI, click the **Add...** button. At the bottom of the screen, a **New Channel** area will be opened. Configure the following:

- **Local URI, Contact, and Display Name** fields: Set these fields to **Auto**.
- Verify **Identity, Send Caller ID, and Diversion Header**: Set to the default **None**.
- Verify **Registration**: Set to the default **0: <None>**.
- **Incoming Group**: Set to an unused group number, e.g., **15**. This value references the table created with **Incoming Call Routes** in **Section 5.7**.
- **Outbound Group**: Set to an unused group number, e.g., **15**.
- **Max Sessions**: In the reference configuration, this was set to **10**. This sets the maximum number of simultaneous calls that can use the URI before Avaya IP Office returns busy to any further calls.
- Click **OK**.

URI	Groups	Local URI	Contact	Display Name	Identity	Header	Originator Number	Send Caller ID	Diversion Header	Credential	Max Calls
1	15 15	Auto	Auto	Auto	None	PAI		None	None	0: <Non...	10

**Edit URI**

Local URI: Auto

Contact: Auto

Display Name: Auto

Identity: None

Header: P Asserted ID

Forwarding And Twinning

Originator Number: [ ]

Send Caller ID: None

Diversion Header: None

Registration: 0: <None>

Incoming Group: 15

Outgoing Group: 15

Max Sessions: 10

Buttons: Add..., Remove, Edit..., OK, Cancel

- To edit an existing entry, click an entry in the list and click the **Edit** button.
- When all SIP URI entries have been added or edited, click **OK** at the bottom of the screen (not shown).

## 5.5.6. SIP Line - VoIP tab

Select the **SIP Line** → **VoIP** tab and enter the following:

- The **Codec Selection** drop-down box → **System Default** will list all available codecs. In the reference configuration, **Custom** was selected and **G729(a) 8K CS-ACELP**, and **G.711 ULAW 64K** were specified. This causes Avaya IP Office to include these codecs in the Session Description Protocol (SDP) offer, and in the order specified. Note that in the reference configuration G.729A is set as the preferred codec on the SIP trunk to the AT&T IPTF network.
- T.38 fax was used in the reference configuration. Set the **Fax Transport Support** drop-down menu to **T38**. G.711 fax also worked in the reference configuration (T.38 option disabled); however, T.38 is the preferred method.
- The **Re-invite Supported** parameter can be checked 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.
- The **DTMF Support** parameter can remain set to the default value **RFC2833/RFC4733**.
- Set the **Media Security** drop-down menu to **Same as System (Preferred)**. Verify that the **Same As System** parameter is checked. This setting will use the same media security level for the trunk as is defined for the system in **Section 5.3.5**. The system level media security is set to **Preferred** specifying that SRTP is preferred over RTP.
- Click **OK** (not shown).

The screenshot displays the configuration page for a SIP Line in the VoIP tab. The tabs at the top are: SIP Line, Transport, SIP URI, VoIP, T38 Fax, SIP Credentials, SIP Advanced, and Engineering. The main configuration area is divided into several sections:

- Codec Selection:** A dropdown menu is set to "Custom". Below it are two lists: "Unused" (G.711 ALAW 64K, G.722 64K, G.723.1 6K3 MP-MLQ) and "Selected" (G.729(a) 8K CS-ACELP, G.711 ULAW 64K). Navigation buttons (>>>, <<<, <-, >+) are between the lists.
- Fax Transport Support:** A dropdown menu set to "T38".
- DTMF Support:** A dropdown menu set to "RFC2833".
- Media Security:** A dropdown menu set to "Same as System (Preferred)". Below it is the "Advanced Media Security Options" section, which includes:
  - Same As System
  - Encryptions:**  RTP,  RTCP
  - Authentication:**  RTP,  RTCP
  - Replay Protection:** SRTP Window Size: 64
  - Crypto Suites:**  SRTP\_AES\_CM\_128\_SHA1\_80,  SRTP\_AES\_CM\_128\_SHA1\_32
- Other Options:** A list of checkboxes on the right side:
  - VoIP Silence Suppression
  - Local Hold Music
  - Re-invite Supported
  - Codec Lockdown
  - Allow Direct Media Path
    - Force direct media with phones
  - PRACK/100rel Supported
  - G.711 Fax ECAN

### 5.5.7. SIP Line – T38 Fax Tab

**Note** – The settings on this tab are only accessible if **Re-invite Supported** and a **Fax Transport Support** option (**T38**) are selected on the **VoIP** tab (**Section 5.6.6**).

Select the **T38 Fax** tab. The **Use Default Values** is unchecked and the **T38 Fax Version** is set to **0**. All other values are left at default.

The screenshot shows the 'T38 Fax' configuration tab. The interface includes several sections:

- General Settings:**
  - T38 Fax Version: 0
  - Transport: UDPTL
- Redundancy:**
  - Low Speed: 0
  - High Speed: 0
- TCF Method:** Trans TCF
- Max Bit Rate (bps):** 14400
- EFlag Start Timer (ms):** 2600
- EFlag Stop Timer (ms):** 2300
- Tx Network Timeout (sec):** 150

On the right side, there is a list of checkboxes:

- Scan Line Fix-up
- TFOP Enhancement
- Disable T30 ECM
- Disable EFlags For First DIS
- Disable T30 MR Compression
- NSF Override

Below these checkboxes are two input fields:

- Country Code: 0
- Vendor Code: 0

At the bottom left, there is a checkbox labeled 'Use Default Values' which is currently unchecked.

### 5.5.8. SIP Line - SIP Advanced Tab

IP Office can be configured to signal when a call is placed on hold by sending an INVITE with media attribute “sendonly”. AT&T in turn will respond with media attribute “recvonly”, and will stop sending RTP media for the duration the call is on hold. When the call is taken off of hold, IP Office will send another INVITE with media attribute “sendrecv” indicating to AT&T to start sending RTP again.

To have Avaya IP Office signal to AT&T when a call is placed on/off hold, select the **SIP Line** → **SIP Advanced** tab and enter the following:

- Select **Indicate HOLD**.

The screenshot shows the 'SIP Line - SIP Advanced' configuration tab. The 'Media' section contains the following settings:

Setting	Value
Allow Empty INVITE	<input type="checkbox"/>
Send Empty re-INVITE	<input type="checkbox"/>
Allow To Tag Change	<input type="checkbox"/>
P-Early-Media Support	None
Send SilenceSupp=Off	<input type="checkbox"/>
Force Early Direct Media	<input type="checkbox"/>
Media Connection Preservation	Disabled
Indicate HOLD	<input checked="" type="checkbox"/>

The 'Call Control' section contains the following settings:

Setting	Value
Call Initiation Timeout (s)	4
Call Queuing Timeout (mins)	5
Service Busy Response	486 - Busy Here
on No User Responding Send	408-Request Timeout
Action on CAC Location Limit	Allow Voicemail
Suppress Q.850 Reason Header	<input type="checkbox"/>
Emulate NOTIFY for REFER	<input type="checkbox"/>
No REFER if using Diversion	<input type="checkbox"/>

## 5.6. Users, Extensions, and Hunt Groups

In this section, examples of Avaya IP Office Users, Extensions, and Hunt Groups are illustrated. Note that the following examples do not discuss all available options, and the screen shots may not display all available parameters. Parameters/options not discussed, should assume to be default.

### 5.6.1. Analog User 320

The following screen shows the **User** tab for analog phone User **320**. This user corresponds to a fax machine.

- To add a User, right click on **User** in the Navigation pane, and select **New** (not shown). To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured.

User			Analog: 320										
Name	Extension	Profile	User	Voicemail	DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming	Mer
RemoteManager		Non-licensed User	Name	Analog									
NoUser		Non-licensed User	Password										
Extn202	202	Basic User	Confirm Password										
Extn203	203	Basic User	Unique Identity										
Extn204	204	Basic User	Conference PIN										
Extn205	205	Basic User	Confirm Audio Conference PIN										
Extn206	206	Basic User	Account Status	Enabled									
Extn207	207	Basic User	Full Name										
Extn208	208	Basic User	Extension	320									
Extn210	210	Basic User	Email Address										
Extn211	211	Basic User	Locale										
Extn212	212	Basic User	Priority	5									
Extn213	213	Basic User	System Phone Rights	None									
Extn214	214	Basic User	Profile	Basic User									
Extn216	216	Basic User	<input type="checkbox"/> Receptionist										
T7316E	231	Power User	<input type="checkbox"/> Enable Softphone										
Avaya9630	236	Power User	<input type="checkbox"/> Enable one-X Portal Services										
Analog	320	Basic User	<input type="checkbox"/> Enable one-X TeleCommuter										
Avaya9508	321	Power User	<input type="checkbox"/> Enable Remote Worker										
Avaya9611	322	Basic User											
Avaya1616	323	Power User											
Softphone	324	Power User											
Avaya1140E	325	Power User											
Avaya9621	328	Power User											
Mobile	329	Power User											
ATT User 873	873	Power User											
ATT User 874	874	Power User											
ATT User 875	875	Power User											
ATT User 876	876	Power User											

2. Analog (or digital) phone extension ports are either integral to the control unit or added by the installation of an analog or digital phone expansion module. Analog (or digital) extension records are automatically created for each physical extension port within the system. These ports cannot be added or deleted manually.
  - To edit an existing analog extension, select the appropriate extension to be configured (e.g., 320).

Extension				Analogue Extension: 31 320	
ID	Extension	Module	Port	Extension	Analogue
2	202	BD1	2	Extension ID	31
3	203	BD1	3	Base Extension	320
4	204	BD1	4	Caller Display Type	On
5	205	BD1	5	Device Type	Analogue Handset
6	206	BD1	6	Location	System (2: SIL)
7	207	BD1	7	Module	BP2
8	208	BD1	8	Port	7
26	210	BD2	2	Disable Speakerphone	<input type="checkbox"/>
27	211	BD2	3		
28	212	BD2	4		
29	213	BD2	5		
30	214	BD2	6		
32	216	BP2	8		
1	231	BD1	1		
8014	236	0	0		
31	320	BP2	7		
25	321	BD2	1		

- Select the Analogue tab and verify that **Standard Telephone** is selected. Note that even though a fax machine is connected, it needs to be classified as a standard telephone.
- Click the **OK** button (not shown).

Extension				Analogue Extension: 31 320	
ID	Extension	Module	Port	Extension	Analogue
2	202	BD1	2	Equipment Classification	Flash Hook Pulse Width
3	203	BD1	3	<input type="radio"/> Quiet Headset <input type="radio"/> Paging Speaker <input checked="" type="radio"/> Standard Telephone <input type="radio"/> Door Phone 1 <input type="radio"/> Door Phone 2 <input type="radio"/> IVR Port <input type="radio"/> FAX Machine <input type="radio"/> MOH Source	<input checked="" type="checkbox"/> Use System Defaults Minimum Width: 20 ms Maximum Width: 500 ms
4	204	BD1	4	Message Waiting Lamp Indication Type	None
5	205	BD1	5	Hook Persistency	100 ms
6	206	BD1	6		
7	207	BD1	7		
8	208	BD1	8		
26	210	BD2	2		
27	211	BD2	3		
28	212	BD2	4		
29	213	BD2	5		
30	214	BD2	6		
32	216	BP2	8		
1	231	BD1	1		
8014	236	0	0		
31	320	BP2	7		
25	321	BD2	1		

## 5.6.2. IP Phone User 322

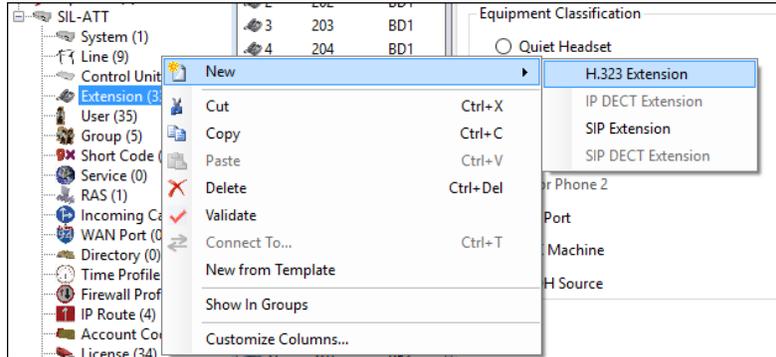
1. Following the steps shown in **Section 5.6.1**, create a 9611 H.323 IP phone user (e.g., **322**).
  - **Password:** This password is used by user applications such as SoftConsole, one-X® Portal and TAPI, or users with Dial In access. Note that this is *not* the user's phone login code (see the information on the **Extension** tab below), or their Voicemail mailbox password (see information on the **Voicemail** tab below).
  - **Conference PIN:** This is the pin number used to access the user's meet me conference.
  - The **Profile** parameter is set to **Power User**. This gives this user access to additional IP Office features. See [3] for more information.

User		Avaya9611: 322*										
Name	Extension	User	Voicemail	DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming	Menu Programming
RemoteManager		Name	Avaya9611									
NoUser		Password	.....									
Extn202	202	Confirm Password	.....									
Extn203	203	Unique Identity										
Extn204	204	Conference PIN	....									
Extn205	205	Confirm Audio Conference PIN	....									
Extn206	206	Account Status	Enabled									
Extn207	207	Full Name										
Extn208	208	Extension	322									
Extn210	210	Email Address										
Extn211	211	Locale										
Extn212	212	Priority	5									
Extn213	213	System Phone Rights	Level 2									
Extn214	214	Profile	Power User									
Extn216	216	<input type="checkbox"/> Receptionist										
T7316E	231	<input checked="" type="checkbox"/> Enable Softphone										
Avaya9630	236	<input checked="" type="checkbox"/> Enable one-X Portal Services										
Analog	320	<input checked="" type="checkbox"/> Enable one-X TeleCommuter										
Avaya9508	321	<input checked="" type="checkbox"/> Enable Remote Worker										
Avaya9611	322	<input checked="" type="checkbox"/> Enable Communicator										
Avaya1616	323	<input checked="" type="checkbox"/> Enable Mobile VoIP Client										
Softphone	324	<input type="checkbox"/> Send Mobility Email										
Avaya1140E	325	<input type="checkbox"/> Web Collaboration										
Avaya9621	328											
Mobile	329											
ATT User 873	873											
ATT User 874	874											
ATT User 875	875											
ATT User 876	876											
ATT User 877	877											
ATT User 878	878											
ATT User 879	879											
ATT User 880	880											
ATT User 881	881											
ATT User 882	882											

The following screen shows the **Voicemail** tab for user 322. The **Voicemail On** box is checked and a Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters.

User	Voicemail	DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming	Menu Programming	Mobility
	Voicemail Code	....		<input checked="" type="checkbox"/> Voicemail On							
	Confirm Voicemail Code	....		<input type="checkbox"/> Voicemail Help							
	Voicemail Email			<input type="checkbox"/> Voicemail Ringback							
				<input type="checkbox"/> Voicemail Email Reading							
				<input type="checkbox"/> UMS Web Services							

- To create an associated extension, right click on **Extension** in the Navigation Pane, and select **New → H323 Extension**.

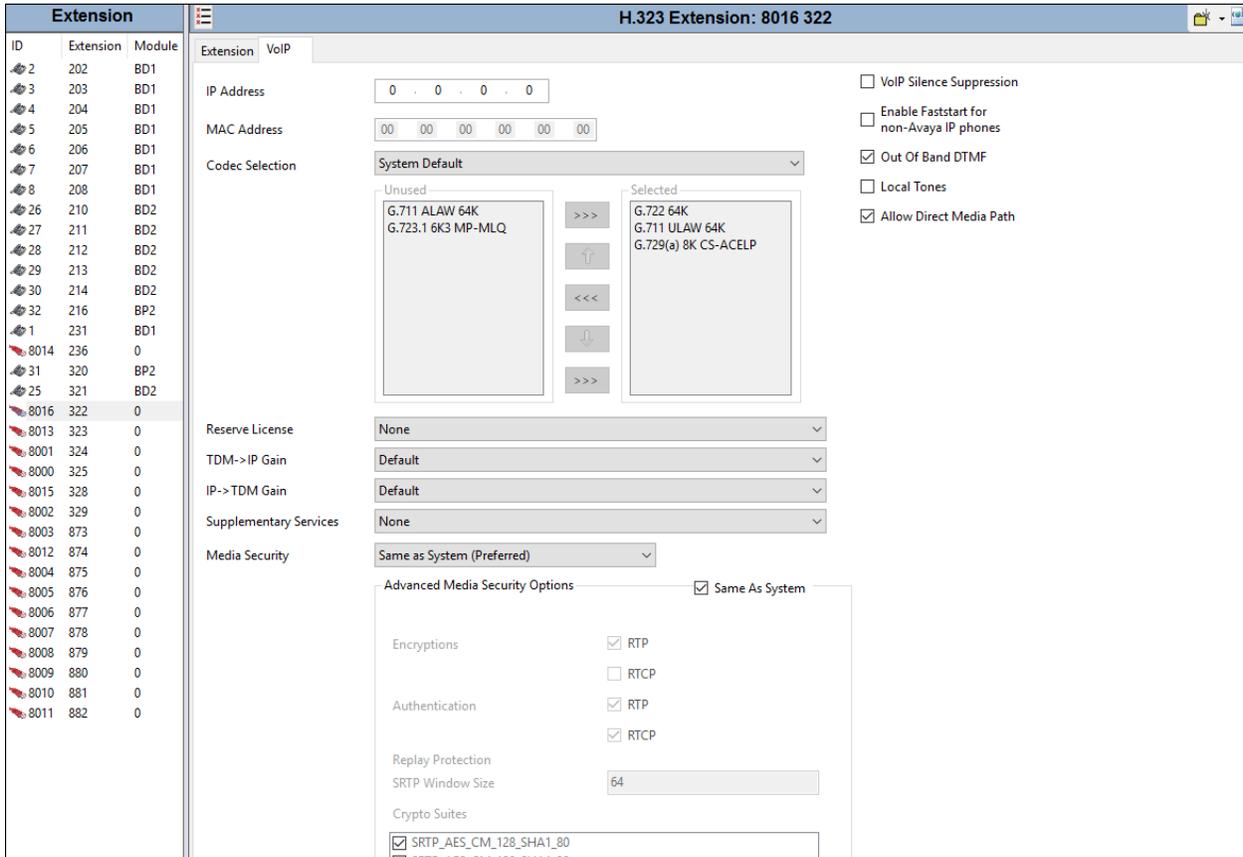


On the **Extension** tab, enter the **Base Extension** (e.g., **6237**). Note that the **Extension ID** field will auto populate. The **Phone Password** will be used by the telephone user as the phone login password.

Extension			H.323 Extension: 8016 322	
ID	Extension	Module	Extension	VoIP
2	202	BD1	Extension ID	8016
3	203	BD1	Base Extension	322
4	204	BD1	Phone Password	••••
5	205	BD1	Confirm Phone Password	••••
6	206	BD1	Caller Display Type	On
7	207	BD1	Reset Volume After Calls	<input type="checkbox"/>
8	208	BD1	Device Type	Avaya 9608
26	210	BD2	Location	Automatic
27	211	BD2	Fallback As Remote Worker	Auto
28	212	BD2	Module	0
29	213	BD2	Port	0
30	214	BD2	Disable Speakerphone	<input type="checkbox"/>
32	216	BP2		
1	231	BD1		
8014	236	0		
31	320	BP2		
25	321	BD2		
8016	322	0		
8013	323	0		
8001	324	0		
8000	325	0		

Select the **VoIP** tab and provision the following:

- **IP Address** field is set to the default value (**0.0.0.0**).
- **Codec Selection** is set to **System Default**, (see **Section 5.3.3**).
- **Media Security** is set to **Same as System (Preferred)**, (see **Section 5.3.4**).
- Click the **OK** button (not shown).



### 5.6.3. Hunt Groups

Users may also receive incoming calls as members of a hunt group. To configure a new hunt group, right-click **Group** from the Navigation pane and select **New**. To view or edit an existing hunt group, select **Group** from the Navigation pane, and the appropriate hunt group from the Group pane.

1. The following screen shows the **Group** tab for hunt group **Call Center**. This hunt group was configured to contain various IP Office extensions. In the reference configuration, these telephones extensions are rung based on idle time, due to the **Ring Mode** setting **Longest Waiting**. Click the **Edit** button to select/deselect from the **User List** included in the Hunt Group from the list of available users.

Group Queuing Overflow Fallback Voicemail Voice Recording Announcements SIP

Name: Call Center Profile: Standard Hunt Group

Extension: 401  Exclude From Directory

Ring Mode: Longest Waiting No Answer Time (sec): System Default (15)

Hold Music Source: No Change

Ring Tone Override: None

Agent's Status on No-Answer Applies To: None

Central System: IPOSE-Primary  Advertise Group

User List

Extension	Name	System
<input checked="" type="checkbox"/> 6242	Avaya 9508	IP500 Expansion
<input checked="" type="checkbox"/> 6237	Avaya 9641	IPOSE-Primary
<input checked="" type="checkbox"/> 6233	Avaya 1616	IPOSE-Primary
<input checked="" type="checkbox"/> 6235	Avaya 1140E	IPOSE-Primary
<input checked="" type="checkbox"/> 6239	Avaya Com	IPOSE-Primary

Edit... Remove

- Under the **Queuing** tab, check the **Queuing On** box and set the **Queue Length** field to any desirable value. Use the default values for all the other fields.

Group Queuing Overflow Fallback Voicemail Voice Recording Announcements SIP

Queuing On

Queue Length: 5  Normalize Queue Length

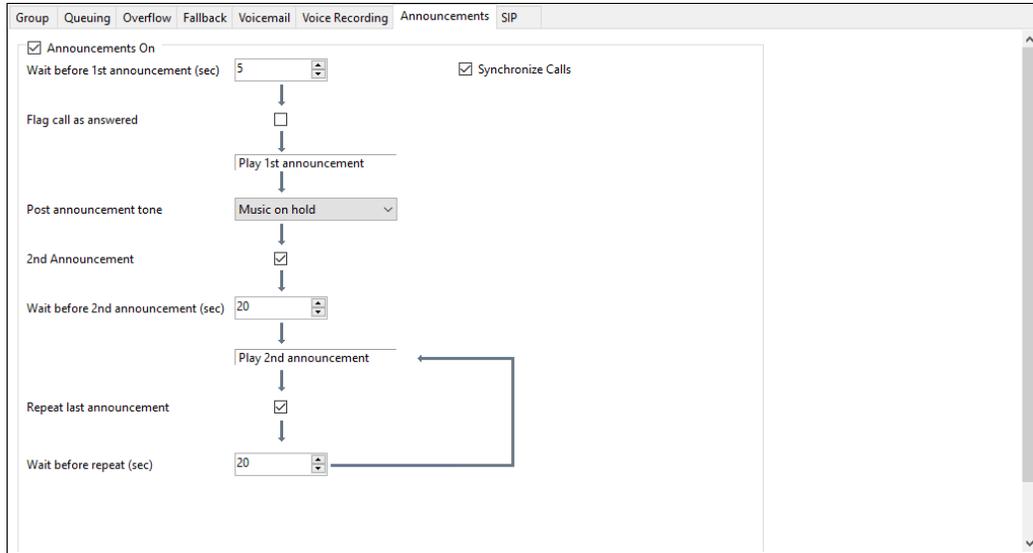
Queue Type: Assign Call On Agent Answer

Calls In Queue Alarm

Calls In Queue Threshold: 1

Analog Extension to Notify: <None>

- Under the **Announcements** tab, check the **Announcements On** box. The wait time can be set to any desirable value. The **Synchronize Calls** box is checked to greatly reduce the number voicemail channels needed to play announcements. These announcements are played if an agent for a particular skill is unavailable.



- Click on **OK** (not shown).

In the reference configuration, these steps were used to create additional Hunt Group “Support” (402).

## 5.7. Incoming Call Routes

**Note** – The digits defined and matched in the Incoming Call Route table, are the DNIS digits specified in the AT&T Request-URI, not the DID digits dialed by the caller.

The Incoming Call Route table will map specific AT&T DNIS numbers to an IP Office User, or Hunt Group, as well as to Voicemail Pro scripts.

To add an incoming call route, right click on **Incoming Call Route** in the Navigation pane, and select **New** (not shown). To edit an existing incoming call route, select an **Incoming Call Route** in the Navigation pane, and the associated call route information is displayed in the Group pane.

### 5.7.1. Calls to IP Office Stations and Hunt Groups

In the example below, the incoming number **000008885551025** is directed to H.323 phone 6237.

1. On the **Standard** tab enter the following:

- **Line Group ID:** Enter the SIP Line defined in **Section 5.4** (e.g., **15**).
- **Incoming Number:** Enter the associated DNIS digits sent by AT&T (e.g., **000008885551025**).
- Use default values for the remaining fields and click **OK** (not shown).

Configuration	15 000008885551025
	Standard   Voice Recording   Destinations
	Bearer Capability: Any Voice
	Line Group ID: 15
	Incoming Number: 000008885551025
	Incoming Sub Address:
	Incoming CLI:
	Locale:
	Priority: 1 - Low
	Tag:
	Hold Music Source: System Source
	Ring Tone Override: None

2. On the **Destinations** tab enter the following:
  - In the **Destinations** column, select extension **6237** from the drop down menu.
  - Use default values for the remaining fields and click **OK** (not shown).

TimeProfile	Destination	Fallback Extension
Default Value	6237 Avaya 9611	

Below is an example of a call for **000008885551026** being directed to Hunt Group **401** (Call Center).

Bearer Capability	Any Voice
Line Group ID	15
Incoming Number	000008885551026
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

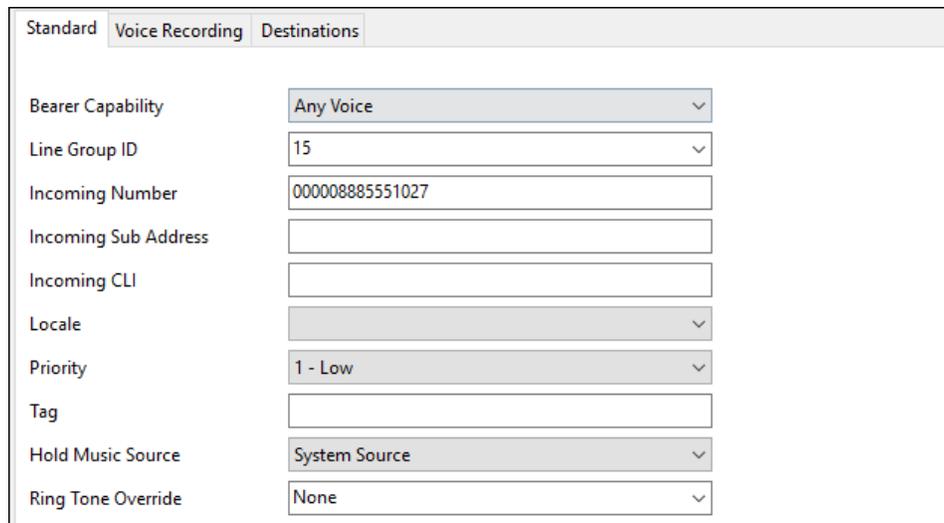
TimeProfile	Destination	Fallback Extension
Default Value	401 Call Center	

## 5.7.2. Calls to Voicemail Pro Scripts

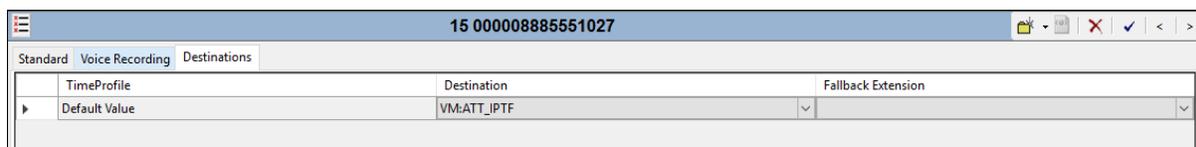
As described in **Section 5.8**, Voicemail Pro scripts are defined with specific names. These script names are specified as destinations in the Incoming Call Route table.

In the example below, incoming number **000008885551027** is directed to the Voicemail Pro Auto-Attendant script **ATT\_IPTF**.

1. On the **Standard** tab repeat the steps in **Section 5.7.1**, with the following changes:
  - **Incoming Number:** Enter the associated DNIS digits sent by AT&T (e.g., **000008885551027**).
2. On the **Destinations** tab enter the following:
  - In the **Destinations** column, enter the string **VM:ATT\_IPTF** from the drop down menu (note if the voicemail module does not appear in the list, enter the value manually).
  - Use default values for the remaining fields and click **OK** (not shown).



Bearer Capability	Any Voice
Line Group ID	15
Incoming Number	000008885551027
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None



TimeProfile	Destination	Fallback Extension
Default Value	VM:ATT_IPTF	

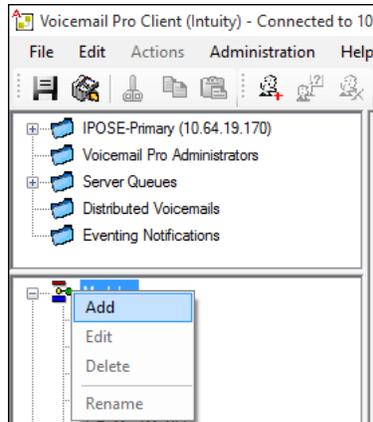
## 5.8. Call Center Provisioning in Voicemail Pro

**Note** – While Voicemail Pro provisioning and programming is beyond the scope of this document, a sample Auto-Attendant script is described below.

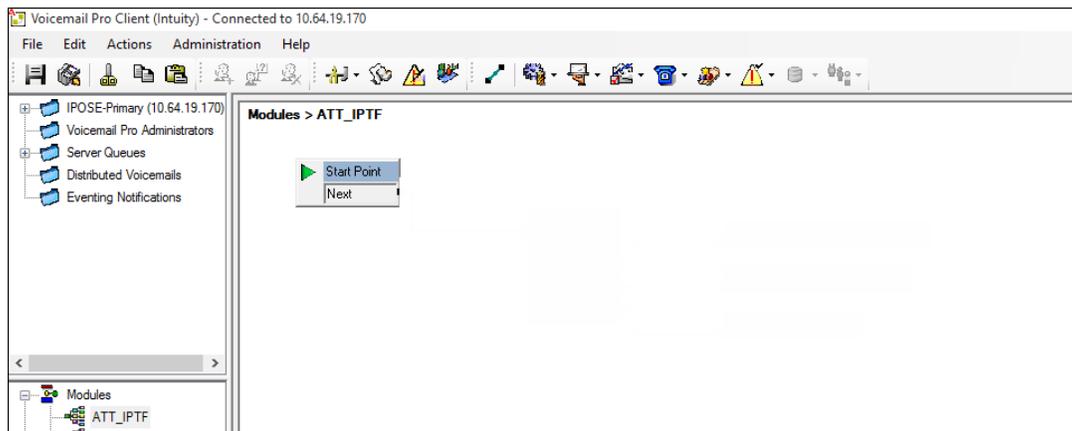
In the reference configuration, Voicemail Pro is used for Voicemail processing as well as for simulating basic Call Center functionality.

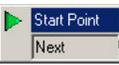
The Auto-Attendant function was provisioned to prompt callers to select a numeric option (1, 2, or 3), that would forward the call to an associated Avaya IP Office Hunt Group (Call Center, and Support), or user 6237. This is accomplished via the following steps:

1. Hunt Groups **Call Center** and **Support** are created in IP Office (**Section 5.6.3**).
2. User 6237 is created in IP Office (**Section 5.6.2**).
3. Incoming Call Route for DNIS digits **000008885551027** is defined for access to the Auto-Attendant script (**Section 5.7.2**).
4. Via the Voicemail Pro GUI interface:
  - Open the **Voicemail Pro Client** application and log in to the Voicemail Pro server (not shown).
  - Create a **Start Point** by right clicking on **Modules** and selecting **Add**.

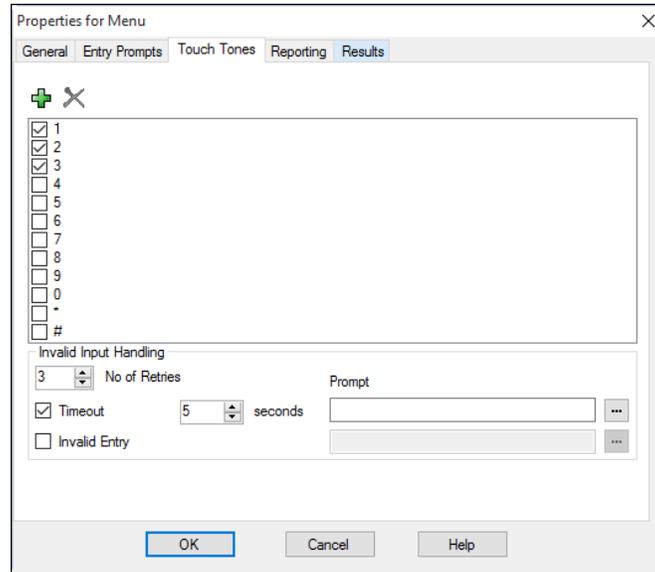


- Enter a name (e.g., **ATT\_IPTF**) and click on **OK** (not shown). The new script **ATT\_IPTF** will appear under **Modules** and a **Start Point** icon will appear in the work area.



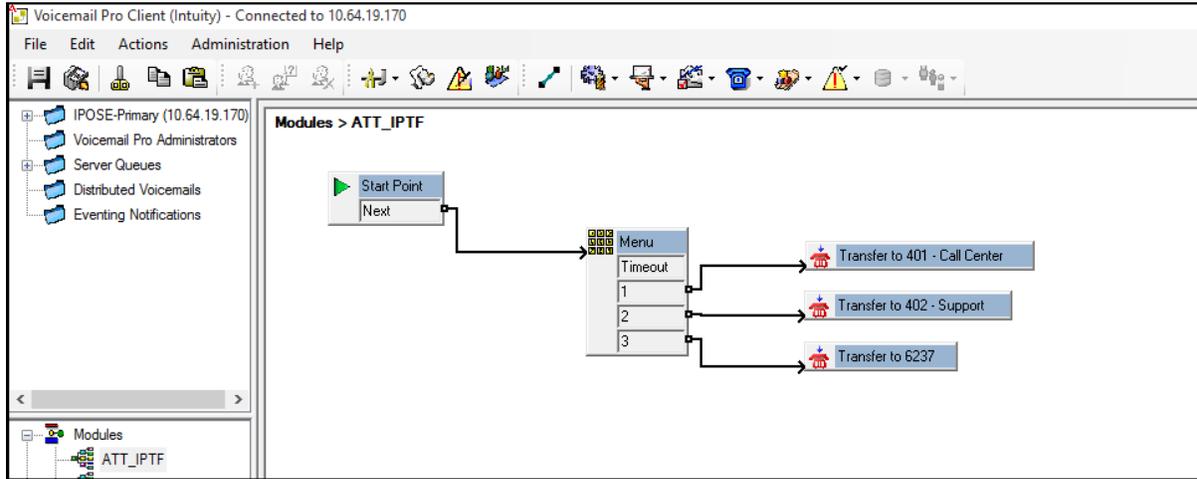
- Click on the **Start Point** icon  to activate the script options at the top of the screen. From the options, select the **Basic Actions** icon , select the **Menu** icon , and click on the work area to place the **Menu** icon.
  - i. Double click the **Menu** icon.
    1. On the **General** tab → **Token Name**, enter **Menu** (not shown).

2. On the **Entry Prompts** tab (not shown), select or create an **Entry Prompt** that will tell the caller what digits to press (e.g., **mainmenu.wav**). To modify an existing recording, double click on the .wav file and rerecord. If no .wav files exist, double click on the  icon to open the .wav editor.
3. On the **Touch Tone** tab:
  - a. Select **1, 2,** and **3** as the possible entry digits.
  - b. Select **3** for **No of Retries**.
4. Click on **OK**.



- Click on the Telephony Actions icon , select the Transfer icon , and click on the work area to place the **Transfer** icon in the work area. This will be used for “Call Center”. Select and place two more Transfer Icons (these will be used for “Service” and extension 6237).
  - i. Double click on the first **Transfer** icon (“**Call Center**”)
    1. On the **General** tab → **Token Name = Transfer to 401 - Call Center** (not shown).
    2. On the **Specific** tab → **Destination = 401** (not shown).
  - ii. Double click on the second **Transfer** icon (“**Support**”).
    1. On the **General** tab → **Token Name = Transfer to 402 - Support** (not shown).
    2. On the **Specific** tab → **Destination = 402** (not shown).
  - iii. Double Click on the third **Transfer** icon (“**Ext6237**”).
    1. On the **General** tab, **Token Name = Transfer to 6237** (not shown).
    2. On the **Specific** tab, **Destination = 6237** (not shown).
- From the options bar, select the Connector icon  and:
  - i. Drag a connecting flow line from the **Start Point** box to the **Menu** box (see screen shot below).

- ii. Drag connecting flow lines from each of the **Menu** options to their associated **Transfer** boxes (see screenshot below).



5. From the top menu select **File → Save & Make Live**, or select the  icon.

When the associated AT&T DNIS number is received (e.g., **000008885551027**), IP Office will send the call to Voicemail Pro. The caller will be prompted to enter 1, 2, or 3 to access Call Center, Support, or user 6237. The associated Avaya IP Office extension (e.g., 401, 402, or 6237) will then ring.

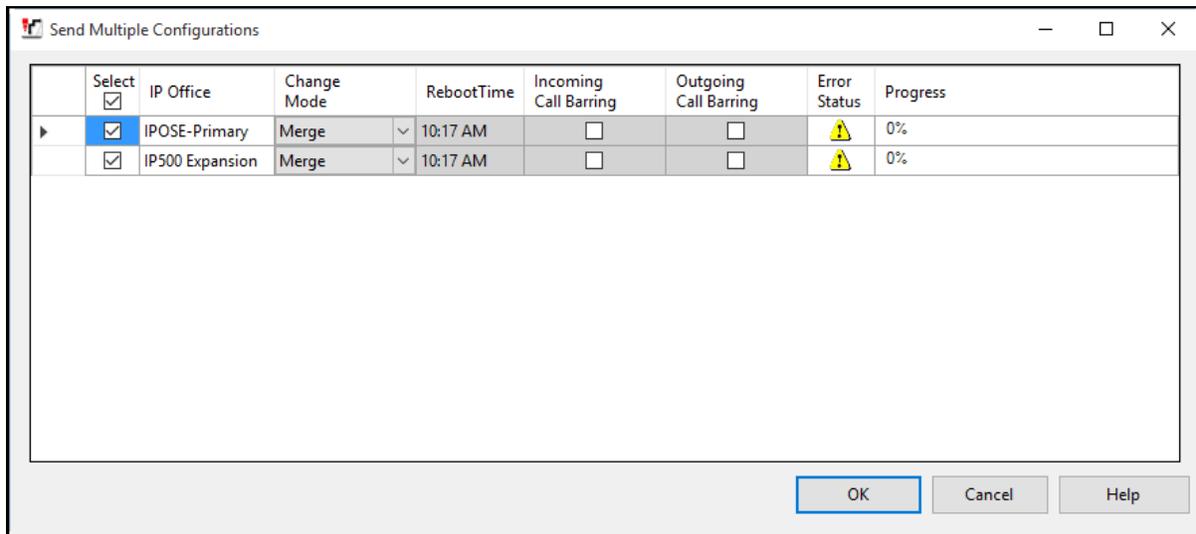
## 5.9. Saving Configuration Changes to Avaya IP Office

The provisioning changes made in Avaya IP Office Manager must be applied to the Avaya IP Office server in order for the changes to take effect. As noted in the previous sections, any changes made to an IP Office provisioning tab must be accepted by clicking **OK** on the associated screen. However these changes will not take effect until they are written to the IP Office configuration.

At the top of the Avaya IP Office Manager GUI, click **File → Save Configuration** (note that if that option is grayed out, no changes are pending).

A screen similar to the one below will appear, with either **Merge** or **Immediate** automatically selected, based on the nature of the configuration changes. The **Merge** option will save the configuration change with no impact to the current system operation. The **Immediate** option will save the configuration and cause the Avaya IP Office server to reboot.

Click **OK** to execute the save.



The active configuration may be saved to a file at any time by selecting **File → Save Configuration As**.

## 6. Configure Avaya Session Border Controller for Enterprise

In the reference configuration, Avaya SBCE is used as an edge device between the CPE and AT&T.

This section covers the configuration of the Avaya SBCE. It is assumed that the initial provisioning of the Avaya SBCE, including the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBCE consult references [5] and [6].

Use a web browser to access the Element Management Server (EMS) web interface, and enter `https://ipaddress/sbc` in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE.

Enter the **Username** and click on **Continue**.



**AVAYA**

**Session Border Controller  
for Enterprise**

**Log In**

Username:

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2017 Avaya Inc. All rights reserved.

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



**AVAYA**

**Session Border Controller  
for Enterprise**

**Log In**

Username:

Password:

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2017 Avaya Inc. All rights reserved.

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

The screenshot shows the Avaya SBCE Dashboard. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left sidebar lists navigation options under "Dashboard": Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings), and Device Specific Settings. The main content area is titled "Dashboard" and contains several panels:
 

- Information**: System Time (02:32:41 PM MDT), Version (7.2.1.0-05-14222), Build Date (Tue Oct 31 00:06:46 UTC 2017), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (04/03/2018 14:28:44 MDT), Failed Login Attempts (0).
- Installed Devices**: A table listing EMS and SBCE.
- Active Alarms (past 24 hours)**: None found.
- Incidents (past 24 hours)**: Two incidents listed as "SBCE : Phone Stealth DDOS Detected".
- Notes**: No notes found.

## 6.1. System Management – Status

Select **System Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative. To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the reference configuration, a single device named **SBCE** is shown. To view the configuration of this device, click **View** as highlighted below.

**Note** – Certain Avaya SBCE configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.

The screenshot shows the Avaya SBCE System Management page. The top navigation bar is the same as the dashboard. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left sidebar lists navigation options under "Dashboard": Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings), and Device Specific Settings. The main content area is titled "System Management" and contains a sub-navigation bar with tabs: Devices, Updates, SSL VPN, Licensing, and Key Bundles. Below this is a table of installed devices:
 

Device Name	Management IP	Version	Status	Actions
SBCE	10.64.90.40	7.2.1.0-05-14222	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

 The "Commissioned" status and the "Restart Application" and "View" buttons are highlighted with red boxes.

The **System Information** screen shows the **Device Configuration, License Allocation, Network Configuration, DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. In the shared test environment, the **A1** and **B1** IP addresses displayed below are the ones relevant to the configuration of the SIP trunk to AT&T.

**System Information: SBCE** X

<p><b>General Configuration</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Appliance Name</td><td>SBCE</td></tr> <tr><td>Box Type</td><td>SIP</td></tr> <tr><td>Deployment Mode</td><td>Proxy</td></tr> </table>	Appliance Name	SBCE	Box Type	SIP	Deployment Mode	Proxy	<p><b>Device Configuration</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>HA Mode</td><td>No</td></tr> <tr><td>Two Bypass Mode</td><td>No</td></tr> </table>	HA Mode	No	Two Bypass Mode	No	<p><b>License Allocation</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Standard Sessions <small>Requested: 50</small></td><td style="text-align: right;">50</td></tr> <tr><td>Advanced Sessions <small>Requested: 50</small></td><td style="text-align: right;">50</td></tr> <tr><td>Scopia Video Sessions <small>Requested: 5</small></td><td style="text-align: right;">5</td></tr> <tr><td>CES Sessions <small>Requested: 0</small></td><td style="text-align: right;">0</td></tr> <tr><td>Transcoding Sessions <small>Requested: 50</small></td><td style="text-align: right;">50</td></tr> <tr><td>Encryption</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> </table>	Standard Sessions <small>Requested: 50</small>	50	Advanced Sessions <small>Requested: 50</small>	50	Scopia Video Sessions <small>Requested: 5</small>	5	CES Sessions <small>Requested: 0</small>	0	Transcoding Sessions <small>Requested: 50</small>	50	Encryption	<input checked="" type="checkbox"/>													
Appliance Name	SBCE																																				
Box Type	SIP																																				
Deployment Mode	Proxy																																				
HA Mode	No																																				
Two Bypass Mode	No																																				
Standard Sessions <small>Requested: 50</small>	50																																				
Advanced Sessions <small>Requested: 50</small>	50																																				
Scopia Video Sessions <small>Requested: 5</small>	5																																				
CES Sessions <small>Requested: 0</small>	0																																				
Transcoding Sessions <small>Requested: 50</small>	50																																				
Encryption	<input checked="" type="checkbox"/>																																				
<p><b>Network Configuration</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 15%;">IP</th> <th style="width: 15%;">Public IP</th> <th style="width: 25%;">Network Prefix or Subnet Mask</th> <th style="width: 15%;">Gateway</th> <th style="width: 30%;">Interface</th> </tr> </thead> <tbody> <tr><td></td><td></td><td></td><td></td><td style="text-align: right;">A1</td></tr> <tr><td>10.64.91.41</td><td>10.64.91.41</td><td>255.255.255.0</td><td>10.64.91.1</td><td style="text-align: right;">A1</td></tr> <tr><td></td><td></td><td></td><td></td><td style="text-align: right;">B2</td></tr> <tr><td></td><td></td><td></td><td></td><td style="text-align: right;">B1</td></tr> <tr><td></td><td></td><td></td><td></td><td style="text-align: right;">B1</td></tr> <tr><td>192.168.80.43</td><td>192.168.80.43</td><td>255.255.255.128</td><td>192.168.80.1</td><td style="text-align: right;">B1</td></tr> </tbody> </table>			IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface					A1	10.64.91.41	10.64.91.41	255.255.255.0	10.64.91.1	A1					B2					B1					B1	192.168.80.43	192.168.80.43	255.255.255.128	192.168.80.1	B1
IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface																																	
				A1																																	
10.64.91.41	10.64.91.41	255.255.255.0	10.64.91.1	A1																																	
				B2																																	
				B1																																	
				B1																																	
192.168.80.43	192.168.80.43	255.255.255.128	192.168.80.1	B1																																	
<p><b>DNS Configuration</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Primary DNS</td><td>10.64.90.201</td></tr> <tr><td>Secondary DNS</td><td></td></tr> <tr><td>DNS Location</td><td>DMZ</td></tr> <tr><td>DNS Client IP</td><td>10.64.91.40</td></tr> </table>	Primary DNS	10.64.90.201	Secondary DNS		DNS Location	DMZ	DNS Client IP	10.64.91.40	<p><b>Management IP(s)</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>IP #1 (IPv4)</td><td>10.64.90.40</td></tr> </table>	IP #1 (IPv4)	10.64.90.40																										
Primary DNS	10.64.90.201																																				
Secondary DNS																																					
DNS Location	DMZ																																				
DNS Client IP	10.64.91.40																																				
IP #1 (IPv4)	10.64.90.40																																				

## 6.2. TLS Management

**Note** – Testing was done using identity certificates signed by a local certificate authority. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

In the reference configuration, TLS transport is used for the communication between IP Office and Avaya SBCE. The following procedures show how to view the certificates and configure the profiles to support the TLS connection.

## 6.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

**Step 1** - Select **TLS Management** → **Certificates** from the left-hand menu. Verify the following:

- The root CA certificate is present in the **Installed CA Certificates** area.
- The signed identity certificate is present in the **Installed Certificates** area.
- The private key associated with the identity certificate is present in the **Installed Keys** area.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The page title is "Session Border Controller for Enterprise" and the AVAYA logo is in the top right corner. The left-hand navigation menu includes: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management), Certificates (highlighted in red), Client Profiles, Server Profiles, and Device Specific Settings. The main content area is titled "Certificates" and contains two buttons: "Install" and "Generate CSR". Below these are three sections: "Installed Certificates" with a table listing "sbc40.crt" and "View Delete" links; "Installed CA Certificates" with a table listing "GSSCPSMGRCA.pem" and "SystemManagerCA.pem", each with "View Delete" links; and "Installed Certificate Revocation Lists" with the message "No certificate revocation lists have been installed." At the bottom is the "Installed Keys" section with a table listing "sbc40.key" and a "Delete" link.

Installed Certificates	
sbc40.crt	<a href="#">View</a> <a href="#">Delete</a>

Installed CA Certificates	
GSSCPSMGRCA.pem	<a href="#">View</a> <a href="#">Delete</a>
SystemManagerCA.pem	<a href="#">View</a> <a href="#">Delete</a>

No certificate revocation lists have been installed.

Installed Keys	
sbc40.key	<a href="#">Delete</a>

## 6.2.2. Server Profiles

**Step 1** - Select **TLS Management** → **Server Profiles**, and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbc40.crt**, from pull down menu.
- **Peer Verification = None.**
- Click **Next**.

**Step 2** - Accept default values for the next screen (not shown) and click **Finish**.

**Edit Profile**

**WARNING:** Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

**TLS Profile**

Profile Name: sbc40-server

Certificate: sbc40.crt

**Certificate Verification**

Peer Verification: None

Peer Certificate Authorities: GSSCPSMGRCA.pem, SystemManagerCA.pem

Peer Certificate Revocation Lists: (empty)

Verification Depth: 0

Next

The following screen shows the completed TLS server profile form:

**Session Border Controller for Enterprise** AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
‣ Global Parameters  
‣ Global Profiles  
‣ PPM Services  
‣ Domain Policies  
‣ TLS Management  
‣ Certificates  
‣ Client Profiles  
‣ **Server Profiles**  
‣ Device Specific Settings

**Server Profiles: sbc40-server** Add Delete

Server Profiles: sbc40-server

Click here to add a description.

**Server Profile**

**TLS Profile**

Profile Name: sbc40-server  
Certificate: sbc40.crt

**Certificate Verification**

Peer Verification: None  
Extended Hostname Verification:

**Renegotiation Parameters**

Renegotiation Time: 0  
Renegotiation Byte Count: 0

**Handshake Options**

Version:  TLS 1.2  TLS 1.1  TLS 1.0  
Ciphers:  Default  FIPS  Custom  
Value: HIGH:DH:ADH:IMD5:1aNULL:1eNULL:@STRENGTH

Edit

### 6.2.3. Client Profiles

**Step 1** - Select **TLS Management** → **Server Profiles**, and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbc40.crt**, from pull down menu.
- **Peer Verification = Required.**
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **SystemManagerCA.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

**Step 2** - Accept default values for the next screen (not shown) and click **Finish**.

The screenshot shows a dialog box titled "Edit Profile" with a close button (X) in the top right corner. At the top, there is a warning message in a red box: "WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems." Below the warning, the dialog is organized into sections: "TLS Profile" with fields for "Profile Name" (containing "sbc40-client") and "Certificate" (a dropdown menu showing "sbc40.crt"); "Certificate Verification" with "Peer Verification" set to "Required", a list of "Peer Certificate Authorities" (containing "GSSCPSMGRCA.pem" and "SystemManagerCA.pem"), and an empty "Peer Certificate Revocation Lists" field; "Verification Depth" set to "1"; "Extended Hostname Verification" with an unchecked checkbox; and "Custom Hostname Override" with an empty text field. A "Next" button is located at the bottom center of the dialog.

The following screen shows the completed TLS client profile form:

The screenshot shows the 'Client Profiles: sbc40-client' configuration page. The left sidebar contains a navigation menu with 'Client Profiles' selected. The main content area displays the configuration for the 'sbc40-client' profile, organized into several sections:

- TLS Profile:** Profile Name: sbc40-client; Certificate: sbc40.crt
- Certificate Verification:** Peer Verification: Required; Peer Certificate Authorities: SystemManagerCA.pem; Peer Certificate Revocation Lists: ---; Verification Depth: 1; Extended Hostname Verification:
- Renegotiation Parameters:** Renegotiation Time: 0; Renegotiation Byte Count: 0
- Handshake Options:** Version:  TLS 1.2,  TLS 1.1,  TLS 1.0; Ciphers:  Default,  FIPS,  Custom; Value: HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Buttons for 'Add', 'Delete', and 'Edit' are visible on the page.

### 6.3. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the enterprise interface is assigned to **A1** and the interface towards AT&T is assigned to **B1**.

The following Avaya SBCE IP addresses and associated interfaces were used in the reference configuration:

- **B1: 192.168.80.43** – IP address configured for the AT&T IPTF service. This address is known to AT&T. See **Section 3**.
- **A1: 10.64.91.41** – IPv4 address configured for AT&T IPTF service to IP Office.

**Session Border Controller for Enterprise** AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
  ▸ Global Parameters  
  ▸ Global Profiles  
  ▸ PPM Services  
  ▸ Domain Policies  
  ▸ TLS Management  
  ▸ Device Specific Settings  
    **Network Management**  
    Media Interface  
    Signaling Interface

Network Management: SBCE

Devices  
SBCE

Interfaces Networks Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Inside-A1	10.64.91.1	255.255.255.0	A1	10.64.91.41	<a href="#">Edit</a>	<a href="#">Delete</a>
Outside-B2					<a href="#">Edit</a>	<a href="#">Delete</a>
Outside-B1-IPv6					<a href="#">Edit</a>	<a href="#">Delete</a>
Outside-B1	192.168.80.1	255.255.255.128	B1	192.168.80.43	<a href="#">Edit</a>	<a href="#">Delete</a>

The following screen shows interface **A1**, and **B1** are **Enabled**. To enable an interface click the corresponding **Disabled** Status link to change it to **Enabled**.

**Session Border Controller for Enterprise** AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
  ▸ Global Parameters  
  ▸ Global Profiles  
  ▸ PPM Services  
  ▸ Domain Policies  
  ▸ TLS Management  
  ▸ Device Specific Settings  
    **Network Management**  
    Media Interface  
    Signaling Interface

Network Management: SBCE

Devices  
SBCE

Interfaces Networks Add VLAN

Interface Name	VLAN Tag	Status
A1		<a href="#">Enabled</a>
A2		<a href="#">Disabled</a>
B1		<a href="#">Enabled</a>
B2		<a href="#">Enabled</a>

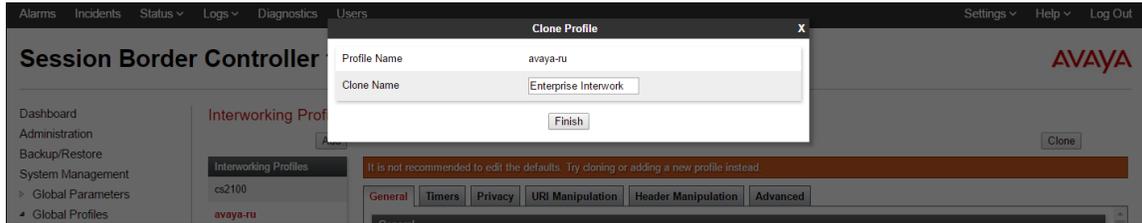
## 6.4. Server Interworking Profile

The Server Internetworking profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

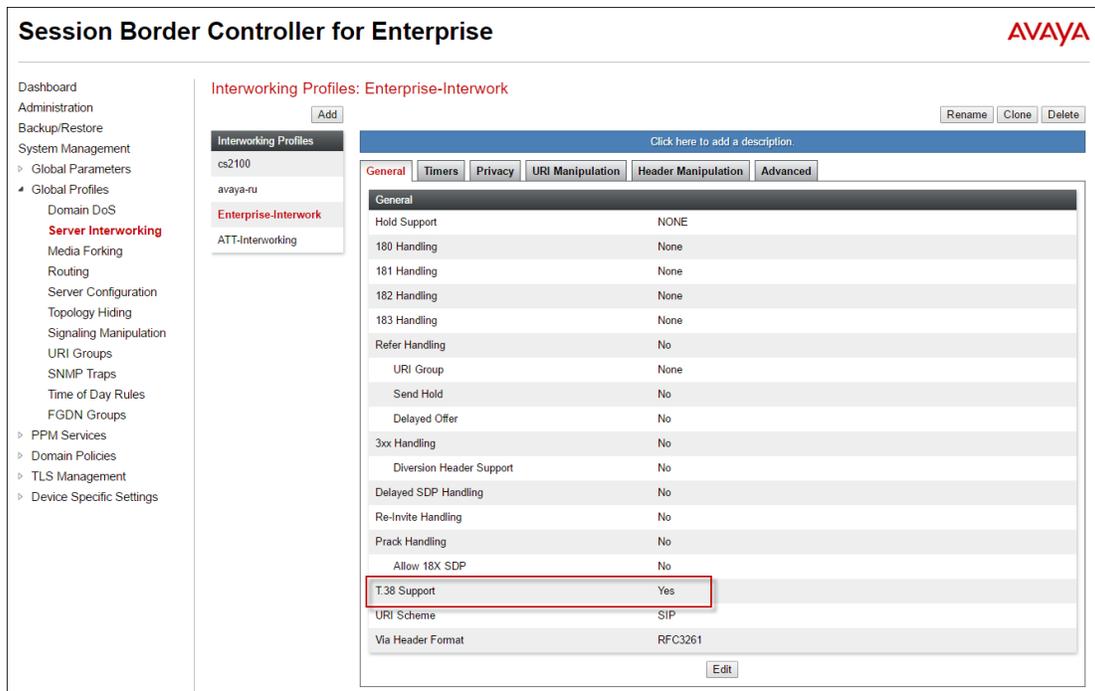
In the reference configuration, separate Server Interworking Profiles were created for IP Office and AT&T IPTF service.

## 6.4.1. Server Interworking Profile – IP Office

In the reference configuration, the IP Office Server Interworking profile was cloned from the default **avaya-ru** profile. To clone a Server Interworking Profile for IP Office, navigate to **Global Profiles → Server Interworking**, select the **avaya-ru** profile and click the **Clone** button. Enter a **Clone Name** and click **Finish** to continue.

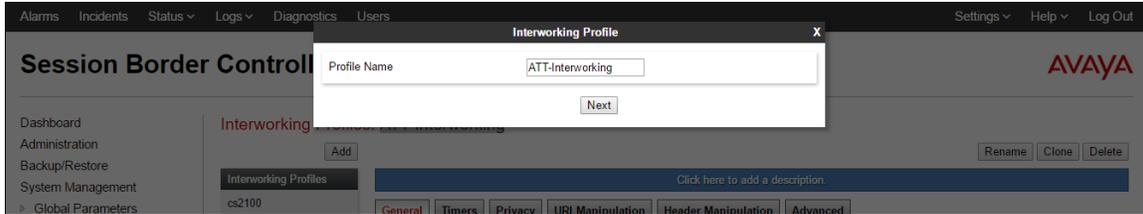


The following screen shows the **Enterprise-Interwork** profile used in the reference configuration, with **T.38 Support** set to **Yes**. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish** (not shown).

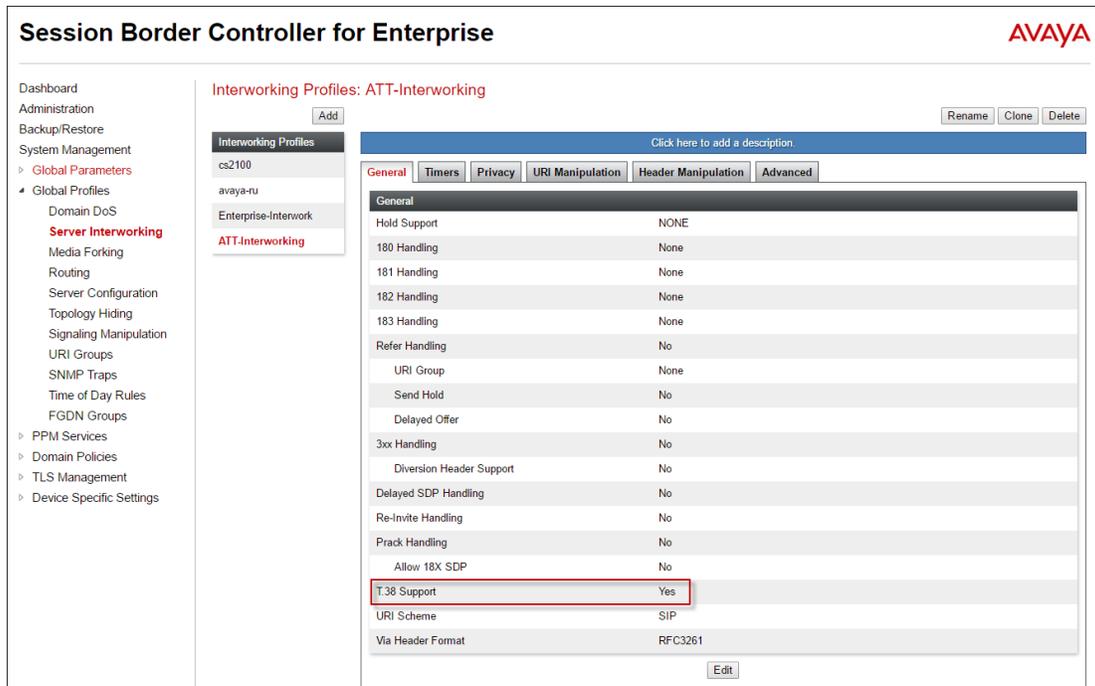


## 6.4.2. Server Interworking Profile – AT&T

To create a new Server Interworking Profile for AT&T, navigate to **Global Profiles** → **Server Interworking** and click **Add** as shown below. Enter a **Profile Name** and click **Next**.



The following screens show the **ATT-Interworking** profile used in the reference configuration. On the **General** tab, default values are used with the exception of **T.38 Support** set to **Yes**.



General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
<b>T.38 Support</b>	<b>Yes</b>
URI Scheme	SIP
Via Header Format	RFC3261

The **Timers** tab shows the values used for compliance testing for the **Trans Expire** field. The **Trans Expire** timer sets the allotted time the Avaya SBCE will try the first primary server before trying the secondary server, if one exists.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the Avaya logo in the top right. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking (highlighted), Media Forking, Routing, Server Configuration, Topology Hiding, Signaling Manipulation, URI Groups, and SNMP Traps. The main content area is titled "Interworking Profiles: ATT-Interworking" and includes an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a "Click here to add a description" link. The "Timers" tab is selected, showing a table of SIP Timers:

SIP Timers	
Min-SE	---
Init Timer	---
Max Timer	---
Trans Expire	4 seconds
Invite Expire	---

An "Edit" button is located at the bottom right of the table.

Click **Next** to accept default parameters for the **Privacy**, **URI Manipulation**, and **Header Manipulation** tabs (not shown) and advance to the **Advanced** area. **Record Routes** is set to **Both Sides**. Default values can be used for all other fields.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface, now displaying the "Advanced" tab for the "ATT-Interworking" profile. The navigation menu is similar to the previous screenshot, but "Server Interworking" is no longer highlighted. The main content area shows the "Advanced" configuration options:

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
DTMF	
DTMF Support	None

An "Edit" button is located at the bottom right of the configuration area.

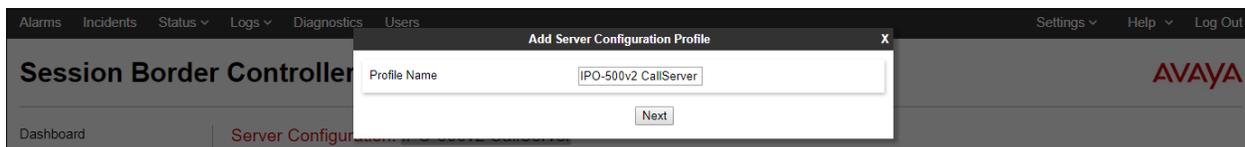
## 6.5. Server Configuration

The **Server Configuration** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

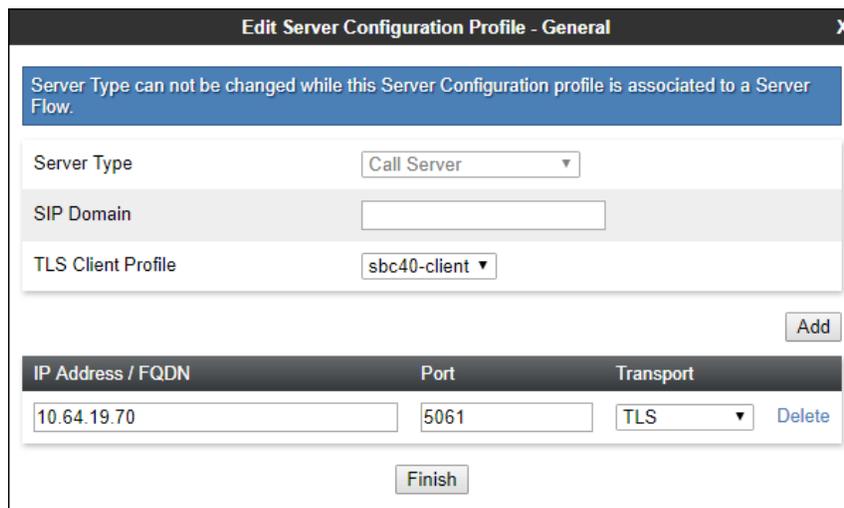
In the reference configuration, separate Server Configurations were created for IP Office and AT&T IPTF service.

### 6.5.1. Server Configuration – IP Office

To add a Server Configuration Profile for IP Office, navigate to **Global Profiles** → **Server Configuration** and click **Add**. Enter a descriptive name for the new profile and click **Next**.



The following screens illustrate the Server Configuration for the Profile name **IPO-500v2 CallServer**. In the **General** parameters, the **Server Type** is set to **Call Server**. In the **IP Address / FQDN** field, the IP Address of IP Office LAN 1 interface in the sample configuration is entered. This IP address is **10.64.19.70**. Under **Port**, **5061** is entered, and the **Transport** parameter is set to **TLS**. The TLS profile **sb40-client** created in **Section 6.2.3** is selected for **TLS Client Profile**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeat** tab. The Avaya SBCE can be configured to source “heartbeats” in the form of PINGs or SIP OPTIONS towards IP Office.

Select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS towards IP Office.

The screenshot shows the configuration page for 'IPO-500v2 CallServer'. The 'Heartbeat' tab is selected. The configuration is as follows:

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	SBCE@sillipo.avayalab.com
To URI	IP500v2@sillipo.avayalab.com

Buttons: Rename, Clone, Delete, Edit

On the **Advanced** tab, the **Interworking Profile** is set to **Enterprise-Interwork** created in **Section 6.4.1** for IP Office.

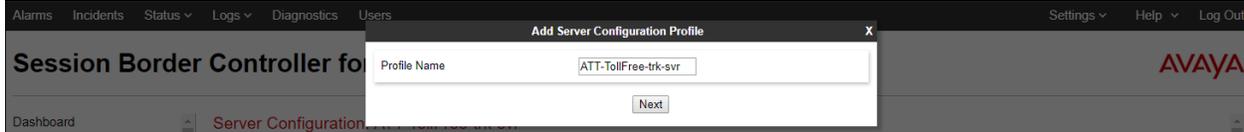
The screenshot shows the configuration page for 'IPO-500v2 CallServer'. The 'Advanced' tab is selected. The configuration is as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Enterprise Interwork
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
Tolerant	<input type="checkbox"/>
URI Group	None

Buttons: Rename, Clone, Delete, Edit

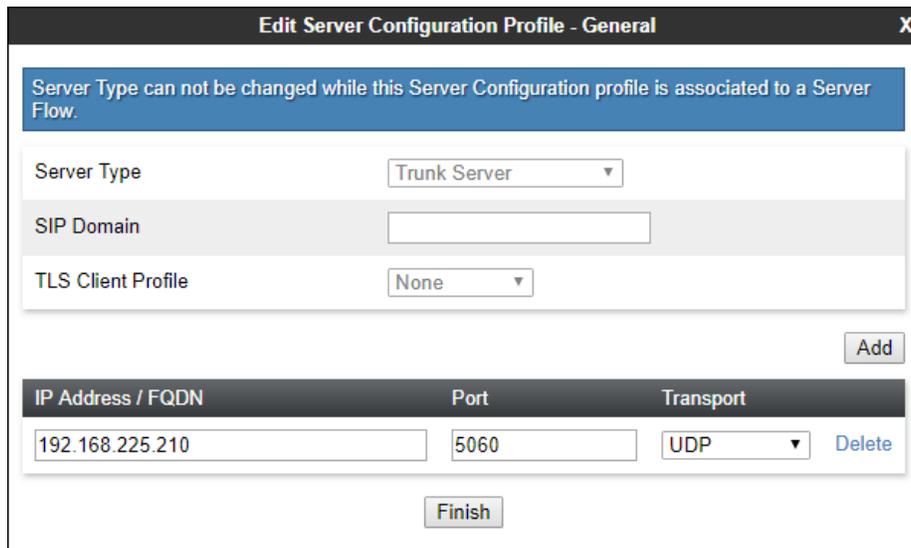
## 6.5.2. Server Configuration – AT&T

To add a Server Configuration Profile for AT&T, navigate to **Global Profiles** → **Server Configuration** and click **Add**. Enter a descriptive name for the new profile and click **Next**.



The screenshot shows a web interface for adding a server configuration profile. The main window is titled "Add Server Configuration Profile". Inside, there is a form with a "Profile Name" field containing the text "ATT-TollFree-trk-svr". Below the field is a "Next" button. The background shows a navigation menu with "Alarms", "Incidents", "Status", "Logs", "Diagnostics", and "Users". The "Server Configuration" menu item is highlighted. The Avaya logo is visible in the top right corner.

The following screens illustrate the Server Configuration for the Profile name **ATT-TollFree-trk-svr**. In the **General** parameters, the **Server Type** is set to **Trunk Server**. In the **IP Address / FQDN** field, the AT&T-provided IP address is entered. This is **192.168.225.210**. Under **Port**, **5060** is entered, and the **Transport** parameter is set to **UDP**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



The screenshot shows the "Edit Server Configuration Profile - General" dialog box. At the top, a blue warning message states: "Server Type can not be changed while this Server Configuration profile is associated to a Server Flow." Below this, the "Server Type" dropdown is set to "Trunk Server". The "SIP Domain" field is empty. The "TLS Client Profile" dropdown is set to "None". An "Add" button is located to the right of the TLS Client Profile field. Below these fields is a table with the following data:

IP Address / FQDN	Port	Transport	
192.168.225.210	5060	UDP	Delete

At the bottom of the dialog box is a "Finish" button.

Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeats** tab. The Avaya SBCE can be configured to source “heartbeats” in the form of SIP OPTIONS towards AT&T. This configuration is optional. Independent of whether the Avaya SBCE is configured to source SIP OPTIONS towards AT&T, AT&T will receive OPTIONS from the IP Office site as a result of the **Check OOS** parameter being enabled on IP Office (see **Section 5.5.3**). When IP Office sends SIP OPTIONS to the inside private IP Address of the Avaya SBCE, the Avaya SBCE will send SIP OPTIONS to AT&T. When AT&T responds, the Avaya SBCE will pass the response to IP Office.

Select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE. If adding a new profile, click **Next** to continuing to the **Advanced** settings.

The screenshot shows the configuration page for 'ATT-TollFree-trk-svr'. The 'Heartbeat' tab is selected. The configuration is as follows:

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	300 seconds
From URI	SBCE@avaya.com
To URI	ATTBE@att.com

Buttons: Rename, Clone, Delete, Edit

On the **Advanced** tab, **Enable Grooming** is not used for UDP connections and is left unchecked. The **Interworking Profile** is set to **ATT-Interworking** created in **Section 6.4.2** for AT&T.

The screenshot shows the configuration page for 'ATT-TollFree-trk-svr'. The 'Advanced' tab is selected. The configuration is as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT-Interworking
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
Tolerant	<input type="checkbox"/>
URI Group	None

Buttons: Rename, Clone, Delete, Edit

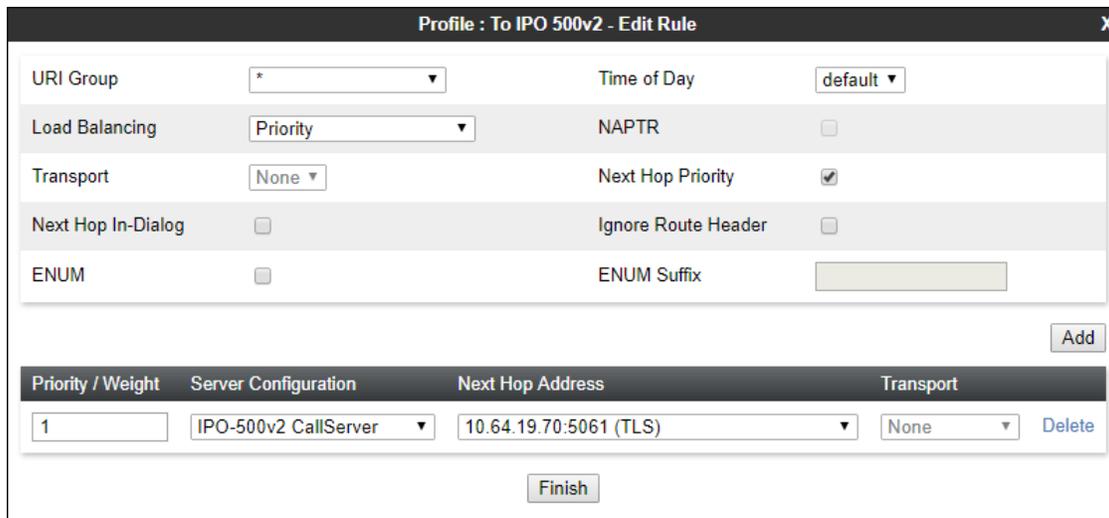
## 6.6. Routing Profile

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

Create a Routing Profile for IP Office and AT&T IPTF service. To add a routing profile, navigate to **Global Profiles** → **Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.



The following screen shows the Routing Profile **To IPO 500v2** created in the sample configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to **1**, and the IP Office **Server Configuration**, created in **Section 6.5.1**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with one of the values from the IP Office Server Configuration, and **Transport** becomes greyed out. Select the **TLS** entry from the drop-down menu for the **Next Hop Address**, and select **Finish**.



Similarly add a Routing Profile to AT&T. The following screen shows the Routing Profile **To ATT IPTF** created in the reference configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to **1**, and the **AT&T Server Configuration**, created in **Section 6.5.2**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the Server Configuration, and **Transport** becomes greyed out. Click **Finish**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	ATT-TollFree-trk-svr	192.168.225.210:5060 (UDP)	None

## 6.7. Topology Hiding Profile

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the reference configuration, the **default** profile was cloned for IP Office and AT&T.

In the **Replace Action** column an action of **Auto** will replace the header field with the IP address of the Avaya SBCE interface and the **Overwrite** will use the value in the **Overwrite Value**.

In the example shown, **SIP-Trunk-Topology** was cloned from the **default** profile and will later be applied to the Server Flows in **Section 6.15**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Topology Hiding Profiles: SIP-Trunk-Topology". On the left is a navigation menu with "Topology Hiding" selected. The main content area has an "Add" button and a list of profiles: "default", "cisco\_th\_profile", "Enterprise-Topology", and "SIP-Trunk-Topology". Below this is a table for "Topology Hiding" with columns: Header, Criteria, Replace Action, and Overwrite Value.

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

## 6.8. Application Rule

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

Select **Domain Policies** → **Application Rules** from the left-side menu as shown below. Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the reference configuration, the **sip-trunk** profile was created for IP Office and AT&T. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** and **Video** applications to a value slightly larger than the licensed sessions. For example, if licensed for 150 session set the values to **200**. The **Maximum Session Per Endpoint** should match the **Maximum Concurrent Sessions**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Application Rules: sip-trunk". On the left is a navigation menu with "Application Rules" selected. The main content area has an "Add" button, a "Filter By Device..." dropdown, and buttons for "Rename", "Clone", and "Delete". Below this is a table for "Application Rule" with columns: Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	200
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	200

Below the table is a "Miscellaneous" section with two rows:

CDR Support	Off
RTCP Keep-Alive	No

## 6.9. Media Rule

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

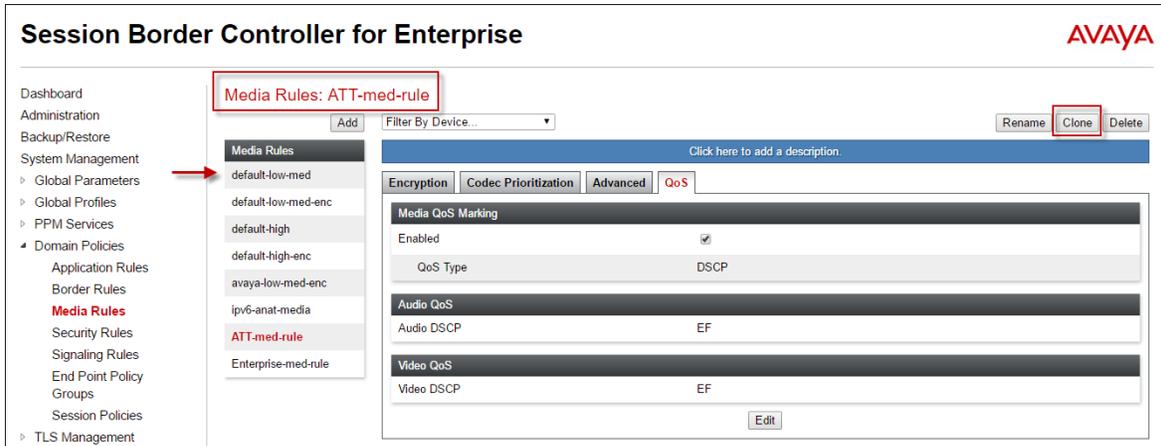
Select **Domain Policies** → **Media Rules** from the left-side menu as shown below. In the sample configuration, the default media rule **avaya-low-med-enc** was cloned for IP Office, **enterprise med rule**, and modified as shown below. With the **avaya-low-med-enc** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

Highlight the newly cloned media rule, select the **Encryption** tab and click **Edit**. The **Media Encryption** window will open (not shown). Select **RTP** from the drop-down for **Preferred Format #2** in the Audio and Video Encryption sections. In the **Miscellaneous** section, check **Capability Negotiation**. In the reference configuration, media rule **enterprise-med-rule** was used for IP Office as shown below.

The screenshot displays the Avaya SBCE configuration interface. On the left is a navigation menu with 'Domain Policies' expanded to 'Media Rules'. The main content area shows the configuration for the 'enterprise med rule'. The 'Encryption' tab is selected, and the 'Edit' button is visible at the bottom. The configuration is divided into three sections: Audio Encryption, Video Encryption, and Miscellaneous. In the Audio Encryption section, 'Preferred Formats' is set to 'SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80 RTP', 'Encrypted RTCP' is unchecked, 'MKI' is unchecked, 'Lifetime' is 'Any', and 'Interworking' is checked. The Video Encryption section has identical settings. In the Miscellaneous section, 'Capability Negotiation' is checked.

Section	Parameter	Value
Audio Encryption	Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
	Encrypted RTCP	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	Any
	Interworking	<input checked="" type="checkbox"/>
Video Encryption	Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
	Encrypted RTCP	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	Any
	Interworking	<input checked="" type="checkbox"/>
Miscellaneous	Capability Negotiation	<input checked="" type="checkbox"/>

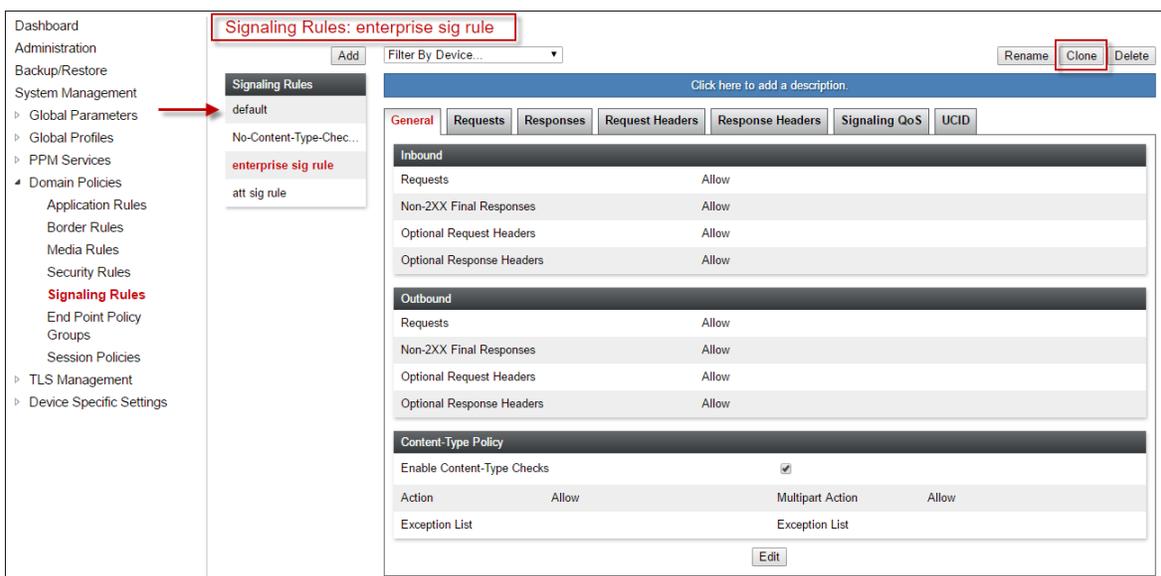
Similarly, the default media rule **default-low-med** was cloned for AT&T IPTF, “**ATT-med-rule**”. The AT&T Media Rule is shown below with the DSCP values **EF** for expedited forwarding (default value) for **Media QoS**.



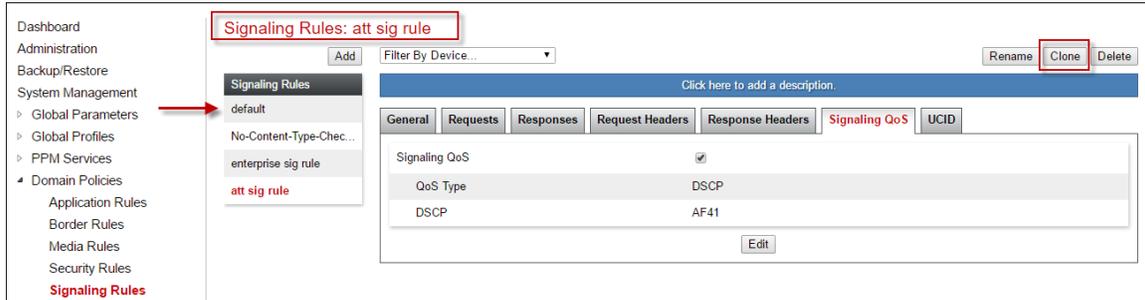
## 6.10. Signaling Rule

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and pattern-matched against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Clone and modify the **default** signaling rule to add the proper quality of service to the SIP signaling. To clone a signaling rule, navigate to **Domain Policies** → **Signaling Rules**. With the **default** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown). In the reference configuration, signaling rule **enterprise-sig-rule** is unchanged from the default rule.



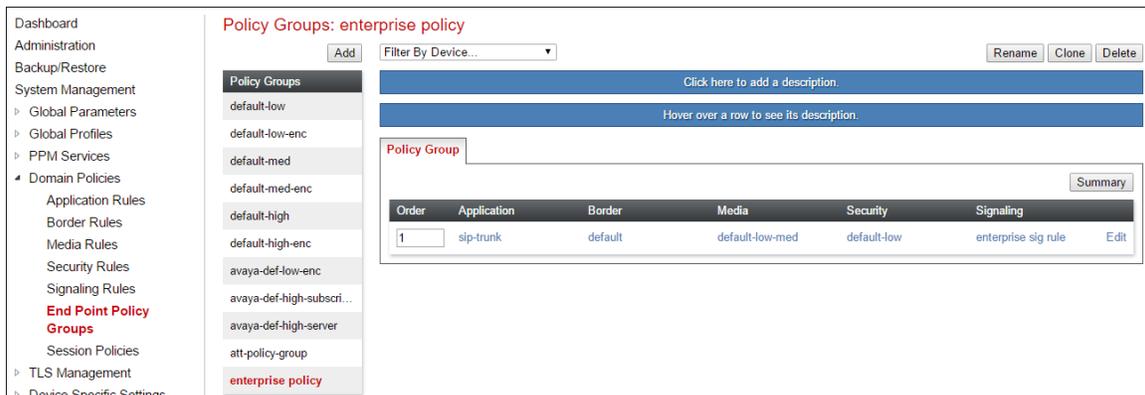
Signaling rule **att sig rule** was also cloned from the default rule and used for AT&T. The DSCP value **AF41** for assured forwarding (default value) for **Signaling QoS**.



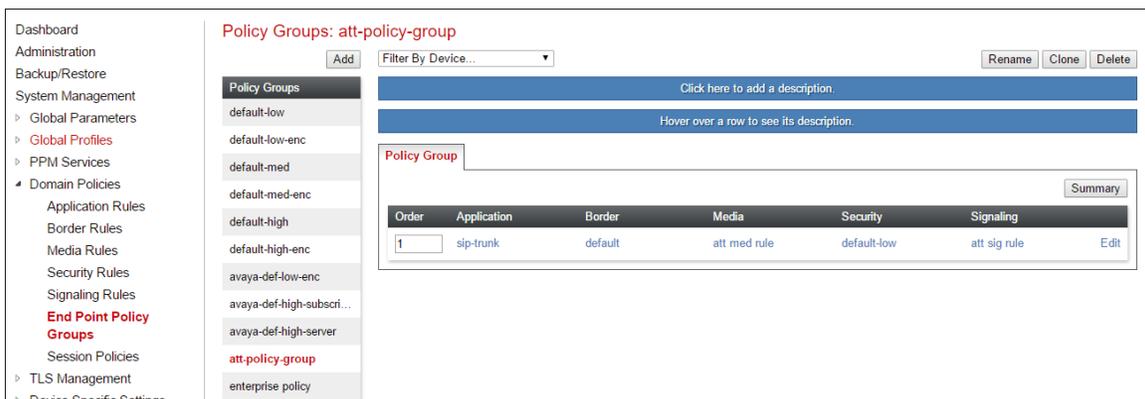
## 6.11. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 6.15**.

To create a new policy group, navigate to **Domain Policies** → **Endpoint Policy Groups** and click on **Add** as shown below. The following screen shows the **enterprise policy** created for IP Office. The details of the non-default rules chosen are shown in previous sections.



The following screen shows the **att-policy-group** created for AT&T. The details of the non-default rules chosen are shown in previous sections.



## 6.12. Advanced Options

In **Section 6.13**, the media UDP port ranges required by AT&T are configured (**16384 – 32767**). However, by default part of this range is already allocated by the Avaya SBCE for internal use (22000 - 31000). The following steps reallocate the port ranges used by the Avaya SBCE so the range required by AT&T can be defined in **Section 6.13**.

1. Select **Device Specific Settings** → **Advanced Options** from the menu on the left-hand side.
2. Select the **Port Ranges** tab.
3. In the **Signaling Port Range** row, change the range to **12000 – 16380**
4. In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.
5. In the **Listen Port Range** row, change the range to **6000 – 6999**.
6. In the **HTTP Port Range** row, change the range to **51001 – 62000**.
7. Select **Save**. Note that changes to these values require an application restart (see **Section 6.1**).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded to 'Device Specific Settings', with 'Advanced Options' highlighted. The main content area is titled 'Advanced Options: SBCE' and features several tabs: 'CDR Listing', 'Feature Control', 'SIP Options', 'Network Options', 'Port Ranges' (which is selected), 'RTCP Monitoring', and 'Load Monitoring'. A warning message states: 'Changes to the settings below require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, the 'Port Range Configuration' section contains four rows of input fields:

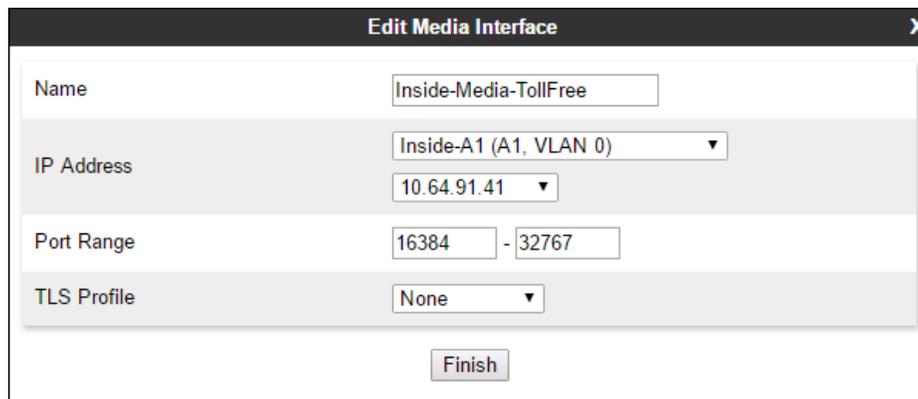
Port Range Configuration	
Signaling Port Range	12000 - 16380
Config Proxy Internal Signaling Port Range	42000 - 51000
Listen Port Range	6000 - 6999
HTTP Port Range	51001 - 62000

A 'Save' button is located at the bottom right of the configuration area.

## 6.13. Media Interface

The AT&T IPTF service specifies that customers use RTP ports in the range of **16384 – 32767**. Both inside and outside ports have been changed to this range, but only the outside is required by the AT&T IPTF service.

1. Select **Device Specific Settings → Media Interface** from the left-hand menu (not shown).
2. Select **Add** (not shown). The Add Media Interface window will open. Enter the following:
  - a) **Name: Inside-Media-TollFree**
  - b) **IP Address:** Select the internal network interface and IP address (Avaya SBCE A1 address toward Avaya IP Office)
  - c) **Port Range: 16384 - 32767**
3. Click **Finish**.

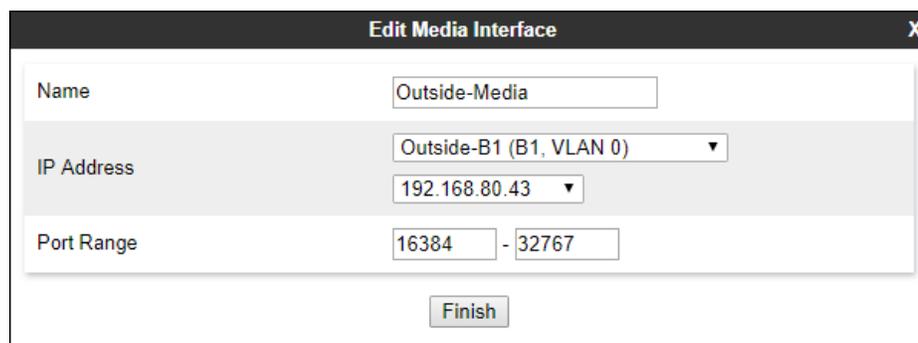


The screenshot shows a window titled "Edit Media Interface" with a close button (X) in the top right corner. The window contains the following fields:

Name	Inside-Media-TollFree
IP Address	Inside-A1 (A1, VLAN 0) 10.64.91.41
Port Range	16384 - 32767
TLS Profile	None

At the bottom center of the window is a "Finish" button.

4. Select **Add** (not shown). The Add Media Interface window will open. Enter the following:
  - a) **Name: Outside-Media**
  - b) **IP Address:** Select the external network interface and IP address (Avaya SBCE B1 address toward AT&T)
  - c) **Port Range: 16384 - 32767**
5. Click **Finish**.



The screenshot shows a window titled "Edit Media Interface" with a close button (X) in the top right corner. The window contains the following fields:

Name	Outside-Media
IP Address	Outside-B1 (B1, VLAN 0) 192.168.80.43
Port Range	16384 - 32767

At the bottom center of the window is a "Finish" button.

The completed **Media Interface** screen is shown below.

**Media Interface: 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 Network	Port Range	Edit	Delete
Outside-B2-Media	Outside-B2 (B2, VLAN 0)	16384 - 32767	Edit	Delete
Inside-Media-Interface	Inside-A1 (A1, VLAN 0)	16384 - 32767	Edit	Delete
Outside-Media-IPv6	Outside-B1-IPv6 (B1, VLAN 0)	16384 - 32767	Edit	Delete
Outside-Media	192.168.80.43 Outside-B1 (B1, VLAN 0)	16384 - 32767	Edit	Delete
Outside-Media-IPv6-TF	Outside-B1-IPv6 (B1, VLAN 0)	16384 - 32767	Edit	Delete
Inside-Media-TollFree	10.64.91.41 Inside-A1 (A1, VLAN 0)	16384 - 32767	Edit	Delete

## 6.14. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a signaling interface for the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** and click **Add**. The following screen shows the signaling interfaces defined for the reference configuration.

**Signaling Interface: SBCE**

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

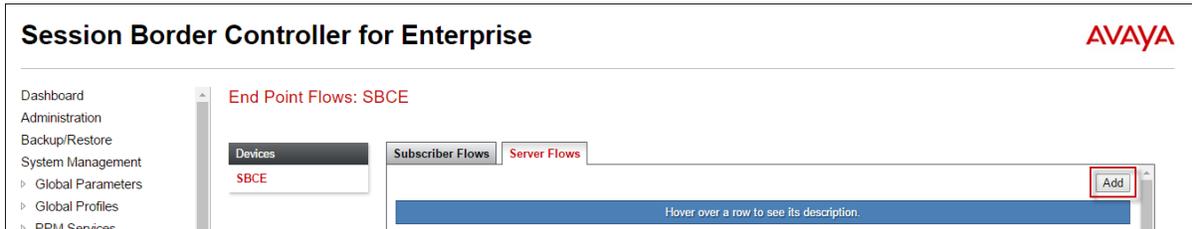
Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Outside-B2-Signaling	Outside-B2 (B2, VLAN 0)	---	5060	---	None	Edit	Delete
Inside-Sig-40	Inside-A1 (A1, VLAN 0)	---	---	5061	sbce40-server	Edit	Delete
Outside-Signaling	192.168.80.43 Outside-B1 (B1, VLAN 0)	---	5060	---	None	Edit	Delete
Outside-Signaling-IPv6-TF	Outside-B1-IPv6 (B1, VLAN 0)	---	5060	---	None	Edit	Delete
Inside-Sig-TollFree-41	10.64.91.41 Inside-A1 (A1, VLAN 0)	---	---	5061	sbce40-server	Edit	Delete
Outside-Signaling-IPv6	Outside-B1-IPv6 (B1, VLAN 0)	---	5060	---	None	Edit	Delete

## 6.15. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this

destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow.

Create a Server Flow for IP Office and AT&T IPTF service. To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add** as highlighted below.



The following screen shows the flow named **ATT IPTF** viewed from the reference configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.

Criteria		Profile	
Flow Name	ATT IPTF	Signaling Interface	Outside-Signaling
Server Configuration	ATT-TollFree-trk-svr	Media Interface	Outside-Media
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	att-policy-group
Remote Subnet	*	Routing Profile	To IPO 500v2
Received Interface	Inside-Sig-TollFree-41	Topology Hiding Profile	SIP-Trunk-Topology
		Signaling Manipulation Script	None
		Remote Branch Office	Any

Once again, select the **Server Flows** tab and click **Add**. The following screen shows the flow named **IP500v2 flow IPv4 Toll Free** viewed from the reference configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.

Criteria		Profile	
Flow Name	IP500v2 flow IPv4 Toll Free	Signaling Interface	Inside-Sig-TollFree-41
Server Configuration	IPO-500v2 CallServer	Media Interface	Inside-Media-TollFree
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	enterprise policy
Remote Subnet	*	Routing Profile	To ATT IPTF
Received Interface	Outside-Signaling	Topology Hiding Profile	SIP-Trunk-Topology
		Signaling Manipulation Script	None
		Remote Branch Office	Any

## 7. AT&T IP Toll Free Service Configuration

AT&T provides the IPTF service border element IP address, the access DID numbers, and the associated DNIS digits used in the reference configuration. In addition the AT&T IPTF features, and their associated access numbers, are also assigned by AT&T. AT&T requires that the Avaya SBCE public (B1) IP address be provided to the IPTF service, as part of the provisioning process. For more information, consult reference [8].

## 8. Verification Steps

The following procedures may be used to verify the Avaya IP Office Release 10.1 and Avaya SBCE Release 7.2 with the AT&T IPTF service configuration.

### 8.1. AT&T IP Toll Free Service

The following scenarios may be executed to verify Avaya IP Office R10.1 functionality with the AT&T IPTF service:

- Place inbound calls, answer the calls, and verify that two-way talk path exists. Verify that the calls remain stable for several minutes and disconnects properly.
- Incoming calls using the G.729A and G.711 ULAW codecs.
- Verify basic call functions such as hold, transfer, and conference.
- Place an inbound call to a telephone, but do not answer the call. Verify that the call covers to voicemail (e.g., Voicemail Pro). Retrieve the message either locally or from PSTN.
- Using the appropriate IPTF access numbers and codes, verify the “Legacy Transfer Connect” DTMF initiated features.
- Inbound fax using T.38 or G.711.
- SIP OPTIONS monitoring of the health of the SIP trunk.

### 8.2. Avaya SBCE

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

#### 8.2.1. Incidents

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



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

Type	ID	Date	Time	Category	Device	Cause
Server Heartbeat	761394944756355	4/3/18	3:11 PM	Policy	SBCE	Heartbeat Failed, Server is Down
Server Heartbeat	761394943796635	4/3/18	3:11 PM	Policy	SBCE	Heartbeat Successful, Server is UP
Server Heartbeat	761394943785180	4/3/18	3:11 PM	Policy	SBCE	Heartbeat Successful, Server is UP
Server Heartbeat	761394943777164	4/3/18	3:11 PM	Policy	SBCE	Heartbeat Successful, Server is UP
Server Heartbeat	761394943763490	4/3/18	3:11 PM	Policy	SBCE	Heartbeat Successful, Server is UP

### 8.2.2. Server Status

The **Server Status** can be access from the Avaya SBCE Dashboard by selecting the **Status** menu, and then **Server Status**.



A pop-up window will appear with the **Status** of **UP** for the AT&T IPTF service. The **Server Profile** will only list servers with Server Configuration settings that have Heartbeats enabled, see **Section 6.5.2**.

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Status	TimeStamp
ATT-IPv6-trk-svr			5060	UDP	DOWN	04/03/2018 15:16:44 MDT
IPO-500v2 CallServer	10.64.19.70	10.64.19.70	5061	TLS	UP	04/03/2018 15:16:27 MDT
			5061	TLS	UP	04/03/2018 15:16:27 MDT
			5061	TLS	UP	04/03/2018 15:16:27 MDT
			5060	UDP	UP	04/03/2018 15:16:27 MDT
			5060	UDP	UP	04/03/2018 15:16:27 MDT
ATT-TollFree-trk-svr			5060	UDP	UP	04/03/2018 15:16:27 MDT

### 8.2.3. Tracing

To take a call trace, navigate to **Device Specific Settings** → **Troubleshooting** → **Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with 'Trace' selected under 'Troubleshooting'. The main content area is titled 'Trace: SBCE' and has two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' section shows the following settings:

Field	Value
Status	Ready
Interface	B2
Local Address (IP[:Port])	All
Remote Address (IP[:Port], IP, IP:Port)	*
Protocol	UDP
Maximum Number of Packets to Capture	10000
Capture Filename (Using the name of an existing capture will overwrite it.)	protocol-trace-att.pcap

Buttons for 'Start Capture' and 'Clear' are visible at the bottom of the configuration area.

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the **Stop Capture** button at the bottom.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with 'Trace' selected under 'Troubleshooting'. The main content area is titled 'Trace: SBCE' and has two tabs: 'Packet Capture' (active) and 'Captures'. A blue notification banner at the top states: 'A packet capture is currently in progress. This page will automatically refresh until the capture completes.' The 'Packet Capture Configuration' section shows the following settings:

Field	Value
Status	In Progress
Interface	B2
Local Address (IP[:Port])	All
Remote Address (IP[:Port], IP, IP:Port)	*
Protocol	UDP
Maximum Number of Packets to Capture	10000
Capture Filename (Using the name of an existing capture will overwrite it.)	protocol-trace-att.pcap

A 'Stop Capture' button is visible at the bottom of the configuration area.

Select the **Captures** tab to view the files created during the packet capture.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The title bar reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand navigation menu includes categories like "Global Parameters", "Global Profiles", "PPM Services", "Domain Policies", "TLS Management", and "Device Specific Settings". Under "Device Specific Settings", the "Trace" option is highlighted. The main content area is titled "Trace: SBCE" and contains two tabs: "Packet Capture" and "Captures". The "Captures" tab is active, showing a table with the following data:

File Name	File Size (bytes)	Last Modified	
protocol-trace-att_20161202095602.pcap	45,056	December 2, 2016 9:56:36 AM MST	Delete

A "Refresh" button is located in the top right corner of the captures table.

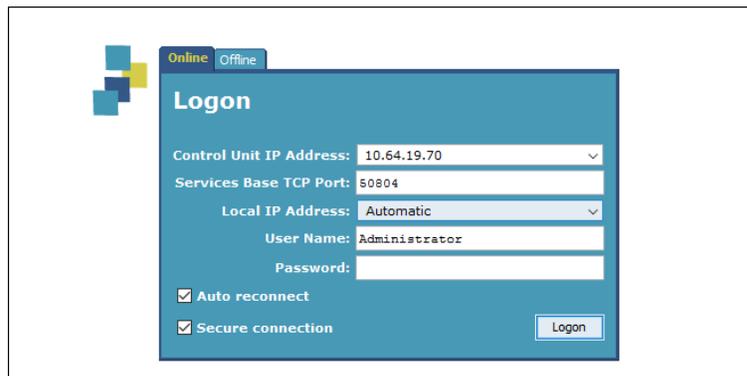
The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like WireShark.

## 8.3. Avaya IP Office

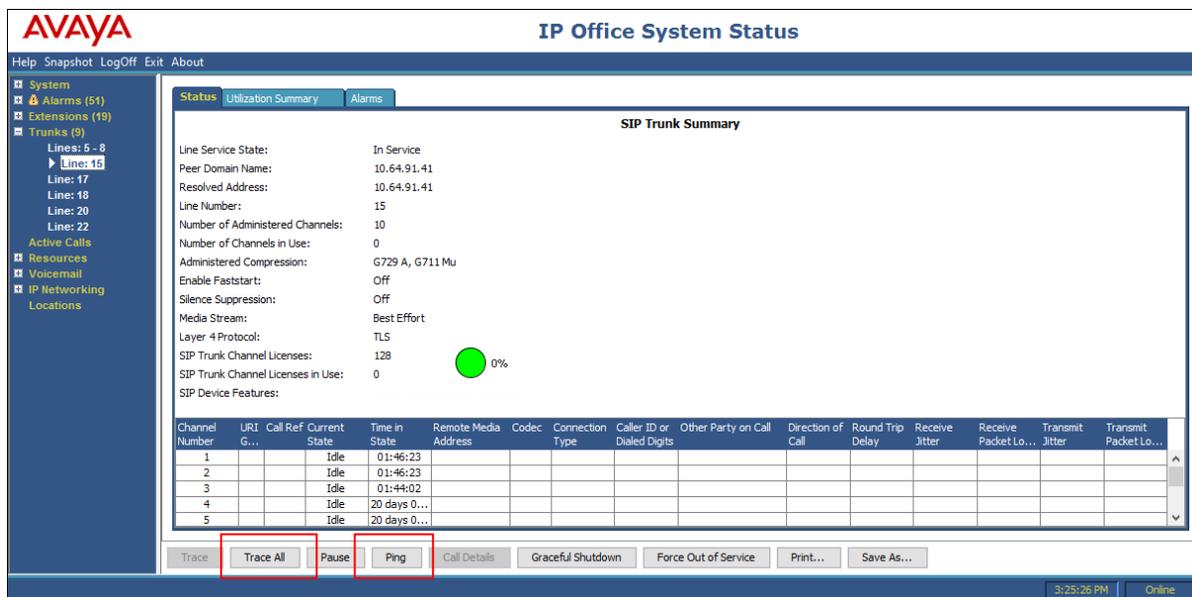
The following items may be used to analyze/troubleshoot Avaya IP Office operations.

### 8.3.1. System Status Application

The System Status application can be used to monitor or troubleshoot Avaya IP Office. The System Status application can typically be accessed from **Start → Programs → Avaya IP Office → System Status**. The following screen shows an example **Logon** screen. Enter the Avaya IP Office IP address in the **Control Unit IP Address** field, and enter an appropriate **User Name** and **Password**. Click **Logon**.

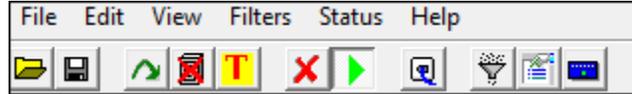


After logging in, select **Trunks → Line: 15** from the left navigation menu. (SIP Line 15 is configured in **Section 5.4**). A screen such as the one shown below is displayed. In the lower left, the **Trace All** button may be pressed to display tracing information as calls are made using this SIP Line. The **Ping** button can be used to ping the other end of the SIP trunk (e.g., the Avaya SBCE).



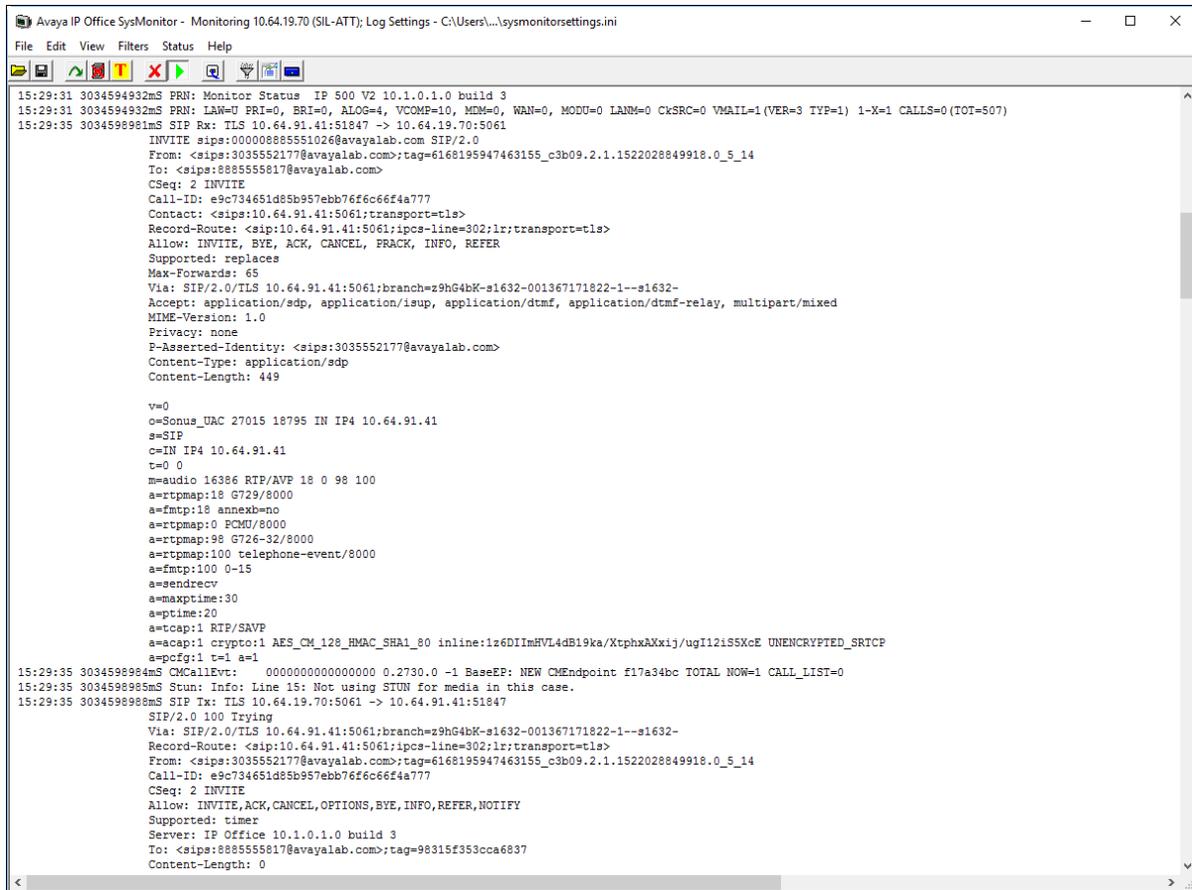
### 8.3.2. System Monitor Application

The System Monitor application can also be used to monitor or troubleshoot Avaya IP Office functionality (see reference [3]). The System Monitor application can typically be accessed from **Start → Programs → Avaya IP Office → Monitor**.

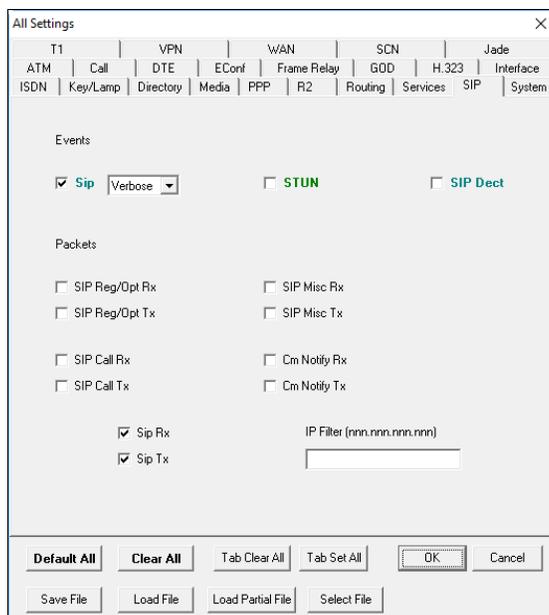


The Monitor will be active at startup. To pause the Monitor, press the Pause  button.

The pause button will be replaced with the Start  button. Press this button to resume the monitoring. To clear the Monitor display, press the Clear  button. Below is a sample of a monitored inbound call.



The displayed data may be customized. Select the **Options** button , or select **Filters** → **Trace Options**. The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, **Sip Verbose** is selected along with the **SIP Rx** and **SIP Tx** boxes.



## 9. Conclusion

As illustrated in these Application Notes, Avaya IP Office Release 10.1 and Avaya Session Border Controller for Enterprise Release 7.2 can be configured to interoperate successfully with the AT&T IP Toll Free service and AVPN or MIS/PNT transport connections, utilizing service features listed in **Section 2.1**, and within the limitations described in **Section 2.2**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

## 10. References

### Avaya:

Avaya product documentation is available at <http://support.avaya.com>. Additional Avaya IP Office information can be found at: <http://marketingtools.avaya.com/knowledgebase/>

- [1] *IP Office™ Platform 10.1, Deploying Avaya IP Office Servers as Virtual Machines*, Document Number 15-601011, Issue 05g, July 2017
- [2] *IP Office™ Platform 10.1, Deploying Avaya IP Office™ Platform IP500 V2*, Document Number 15-601042, Issue 32g, Aug 2017
- [3] *Administering Avaya IP Office™ Platform with Manager*, Release 10.1, June 2017
- [4] *IP Office™ Platform 10.1, IP Office SIP Phones with ASBCE*, Issue 02b, July 2017
- [5] *Deploying Avaya Session Border Controller in Virtualized Environment*, June 2017
- [6] *Administering Avaya Session Border Controller for Enterprise*, June 2017
- [7] *IP Office™ Platform 10.1, IP Office SIP Phones with ASBCE*, Issue 02b, July 2017

### AT&T IPTF Service:

- [8] AT&T IP Toll Free Service description - <http://www.business.att.com/enterprise/Service/voice-services/contact-center-solutions/ip-toll-free/>

---

©2018 Avaya Inc. All Rights Reserved.

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect program at [devconnect@avaya.com](mailto:devconnect@avaya.com).