



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Configuring Fusion Connect SIP Trunking Service with Avaya IP Office R9.1 and Avaya Session Border Controller for Enterprise R6.3 - Issue 0.1

### Abstract

These Application Notes describe the procedures for configuring Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 6.3 to inter-operate with the Fusion Connect SIP Trunking Service. Fusion Connect is a member of the Avaya DevConnect Service Provider program..

The Fusion Connect SIP Trunking Service provides PSTN access via a SIP trunk between an enterprise site and the Fusion Connect network as an alternative to legacy analog or digital trunks. This approach generally results in easier maintenance and lower cost for the business customer.

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

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

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results .....	5
2.3.	Support .....	6
3.	Reference Configuration.....	6
4.	Equipment and Software Validated .....	8
5.	Configure Avaya IP Office .....	9
5.1.	Licensing and Physical Hardware .....	10
5.2.	System .....	12
5.2.1.	System – LAN1 Tab .....	12
5.2.2.	System - Voicemail Tab.....	16
5.2.3.	System - Telephony Tab .....	17
5.2.4.	System - Twinning Tab.....	18
5.2.5.	System – Codecs Tab.....	18
5.3.	IP Route.....	19
5.4.	Administer SIP Line.....	20
5.4.1.	Create SIP Line From Template .....	21
5.4.2.	SIP Line – SIP Line Tab .....	25
5.4.3.	SIP Line – Transport Tab.....	26
5.4.4.	SIP Line – SIP URI Tab.....	26
5.4.5.	SIP Line – VoIP Tab.....	29
5.4.6.	SIP Line – T38 Fax .....	30
5.4.7.	SIP Line – SIP Credentials Tab .....	30
5.4.8.	SIP Line – SIP Advanced Tab .....	31
5.5.	Short Code.....	32
5.6.	User .....	34
5.7.	Incoming Call Route .....	35
5.8.	ARS and Alternate Routing.....	37
5.9.	Mobility.....	38
5.10.	SIP Options.....	39
5.11.	Save Configuration .....	40
6.	Configure Avaya Session Border Controller for Enterprise.....	41
6.1.	Access Management Interface .....	41
6.2.	Verify Network Configuration and Enable Interfaces .....	43
6.3.	Signaling Interface .....	45
6.4.	Media Interface .....	46
6.5.	Server Interworking.....	47
6.5.1.	Server Interworking – Avaya IP Office .....	48
6.5.2.	Server Interworking – Fusion Connect .....	50
6.6.	Server Configuration .....	52
6.6.1.	Server Configuration – Avaya IP Office .....	53
6.6.2.	Server Configuration – Fusion Connect .....	54
6.7.	Application Rules.....	55
6.8.	Media Rules.....	56

6.9.	Signaling Rules .....	58
6.10.	End Point Policy Groups .....	59
6.10.1.	End Point Policy Group – Avaya IP Office .....	60
6.10.2.	End Point Policy Group – Fusion Connect .....	61
6.11.	Routing .....	62
6.11.1.	Routing – Avaya IP Office.....	63
6.11.2.	Routing – Fusion Connect.....	64
6.12.	Topology Hiding.....	66
6.13.	End Point Flows.....	67
6.13.1.	End Point Flow – Avaya IP Office.....	68
6.13.2.	End Point Flow – Fusion Connect.....	70
7.	Fusion Connect SIP Trunking Configuration .....	71
8.	Verification Steps .....	72
8.1.	Avaya IP Office System Status .....	72
8.2.	Avaya IP Office Monitor.....	73
8.3.	Avaya SBCE Traces.....	74
9.	Conclusion .....	74
10.	Additional References.....	75

# 1. Introduction

These Application Notes describe the procedures for configuring an enterprise solution using Avaya IP Office Release R9.1 and Avaya Session Border Controller for Enterprise (Avaya SBCE) R6.3 to inter-operate with the Fusion Connect SIP Trunking Service.

In the sample configuration, the enterprise solution consists of an Avaya SBCE, an Avaya IP Office 500 V2 running Release 9.1 software, Avaya Preferred Edition (a.k.a Voicemail Pro) messaging application, Avaya H.323 and SIP deskphones, and the SIP-based Avaya Communicator softphone. Customers using this Avaya IP Office enterprise solution with the Fusion Connect SIP Trunking Service are able to place and receive PSTN calls via a broadband WAN connection using SIP. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

## 2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office to connect to Fusion Connect via Avaya SBCE and the public Internet. The configuration shown in **Figure 1** was used to exercise the features and functionality tests listed in **Section 2.1**.

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

### 2.1. Interoperability Compliance Testing

To verify SIP Trunking interoperability, the following features and functionality were covered during the compliance test.

- SIP OPTIONS queries and responses.
- Incoming calls from the PSTN to H.323 and SIP telephones at the enterprise. All inbound calls from the PSTN were routed from the service provider across the SIP trunk to the enterprise.
- Outgoing calls to the PSTN from H.323 and SIP telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound calls to the Avaya Communicator for Windows (SIP soft client).
- Various call types including: local, long distance, toll-free, international, Local Directory Assistance, and Emergency 911 calls.
- G.711u and G.729a codecs.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call transfer, conference, forwarding and mobility (mobile twinning).

- Use of the SIP REFER method for call transfers to the PSTN.
- Voicemail navigation for inbound and outbound calls, and voicemail Message Waiting Indicator (MWI).
- T.38 fax and G.711u pass-through fax.
- Inbound and outbound long-duration and long hold time call stability.
- Response to incomplete call attempts and trunk errors.
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise extensions.

## 2.2. Test Results

Interoperability compliance testing of the Fusion Connect SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Supported Codecs** – Fusion Connect supports both G.711u and G.729a codecs. However, the codecs cannot be changed dynamically from one to the other through Avaya IP Office just on the enterprise side. Fusion Connect must be notified about which one of the two codecs a customer prefers before configuring for and turning up the service. If a customer desires to change to a different codec (e.g., from G.711u to G.729a) afterwards, Fusion Connect must make the configuration change on the service side after receiving notification from the customer.
- **Inbound T.38 Fax** – After initial connect, Fusion Connect would reject the re-INVITE from Avaya IP Office for switching to T.38 with "488 Not Acceptable Here", and issue its own T.38 re-INVITE towards the enterprise. This extra round of T.38 signaling exchange had no negative impact: the T.38 fax job would run to completion successfully.
- **Outbound T.38 Fax** – No re-INVITE was issued by Fusion Connect for switching to T.38 after an outbound fax call was connected. The fax call would go through successfully using the G.711u pass-through mode (treating fax as regular voice call with best effort).
- **Direct Media** – The Direct Media capability on IP Office allows IP endpoints to send RTP media directly to each other rather than having all the media flow through the IP Office, using up VoIP and relay resources. This capability is not supported by Avaya IP Office on the SIP trunk connection which allows T.38 fax in addition to voice calls. Consequently, Direct Media was disabled for the test circuit configured for the compliance test.

Items not supported by the Fusion Connect SIP Trunking Service included the following:

- **Operator Calls** – Fusion Connect does not support Operator (0) and Operator-Assisted (0 + 10-digits) calls.
- **Session Timer** – Session timer based on RFC 4028 is not implemented by Fusion Connect. During compliance testing, the enterprise sent session refresh re-INVITE messages towards Fusion Connect with the configured session timer on Avaya IP Office.
- **UPDATE Message** – Fusion Connect does not support UPDATE (the Allowed header in SIP messages from Fusion Connect does not contain UPDATE). Consequently, Avaya IP Office used re-INVITE messages to refresh active call sessions during the compliance test.

## 2.3. Support

For support on the Fusion Connect SIP Trunking Service, please contact Fusion Connect via the following:

- Web: <https://www.fusionconnect.com/support>
- Phone: (888) 301-1721

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>.

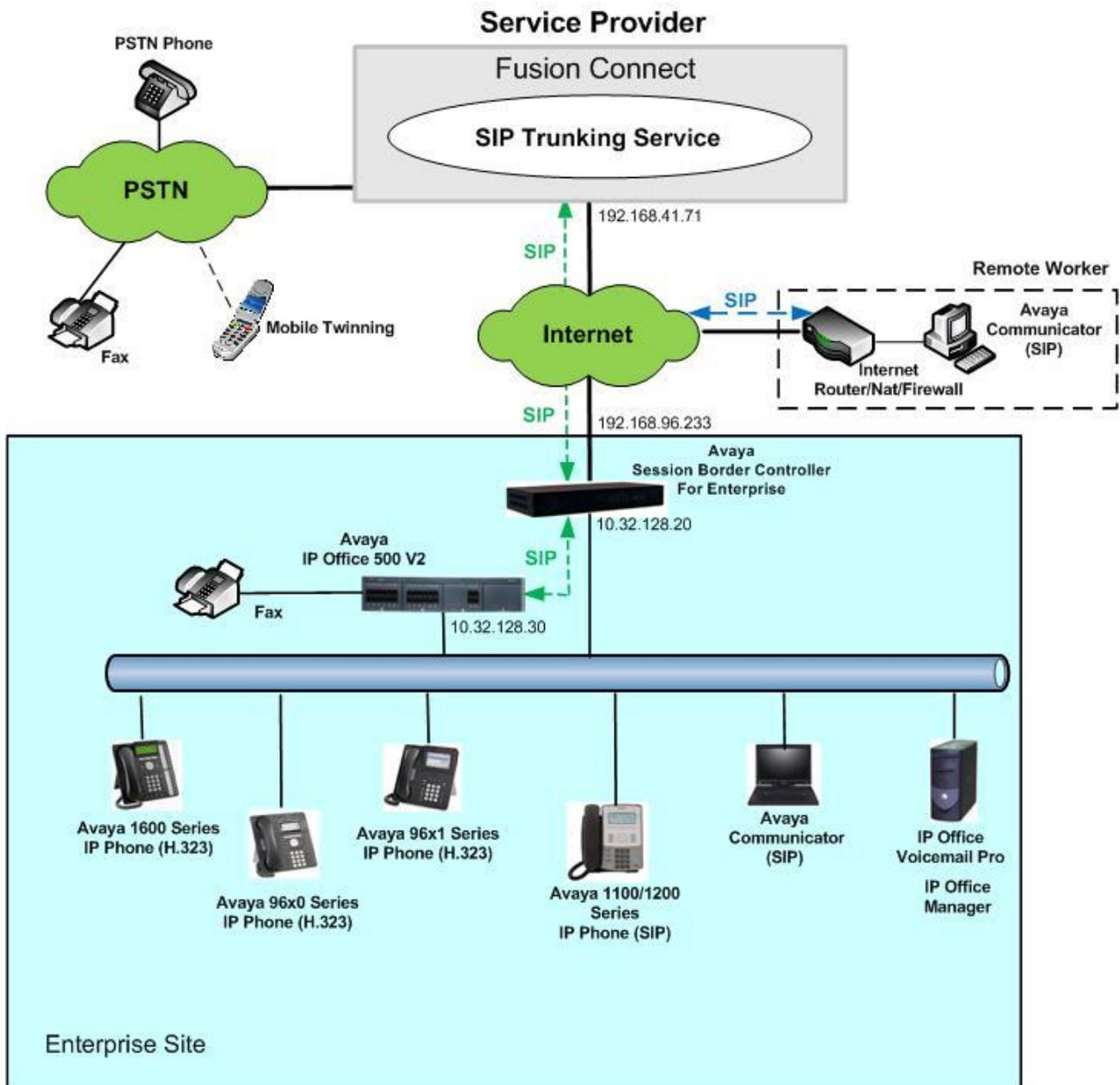
## 3. Reference Configuration

**Figure 1** illustrates the test configuration showing an enterprise site connected to the Fusion Connect SIP Trunking Service.

Located at the edge of the enterprise network is the Avaya SBCE. It has a public side that connects to the Fusion Connect network via the public Internet, and a private side that connects to the enterprise LAN network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers.

Within the enterprise site is an Avaya IP Office 500 V2 running the Release 9.1 software. Endpoints include various Avaya IP Telephones (with H.323 and SIP firmware) and the SIP-based Avaya Communicator softphone. The site also has a Windows PC running Avaya Preferred Edition (a.k.a. Voicemail Pro) for providing voice messaging service to the Avaya IP Office users, and Avaya IP Office Manager for administering the Avaya IP Office.

Mobility Twinning is configured for some of the Avaya IP Office users so that calls to these user phones will also ring and can be answered at the configured mobile phones.



**Figure 1: Avaya IP Office with Fusion Connect SIP Trunking Service**

For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses in these Application Notes.

During compliance testing, enterprise users dialed a prefix digit 8 or 9 plus N digits to send an outbound call to the number N across the SIP trunk to Fusion Connect. The short code of 8 or 9 was stripped off by Avaya IP Office but the remaining N digits were sent to the service provider network. For calls within the North American Numbering Plan (NANP), the user dialed 11 (1 + 10) digits for long distance and local calls. Thus, for these NANP calls, Avaya IP Office sent 11 digits in the

Request URI and the To header of an outbound SIP INVITE message. Fusion Connect sent 10 digits in the Request URI and the To header of inbound SIP INVITE messages.

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

The administration of the Avaya Preferred Edition (Voicemail Pro) messaging service and endpoints on Avaya IP Office is standard. Since these configuration tasks are not directly related to the inter-operation with the Fusion Connect SIP Trunking Service, they are not included in these Application Notes.

Remote Worker configuration is also not covered by these Application Notes. For configuration details on Avaya IP Office and Avaya SBCE to support Remote Worker, see [9] in **Section 10**.

## 4. Equipment and Software Validated

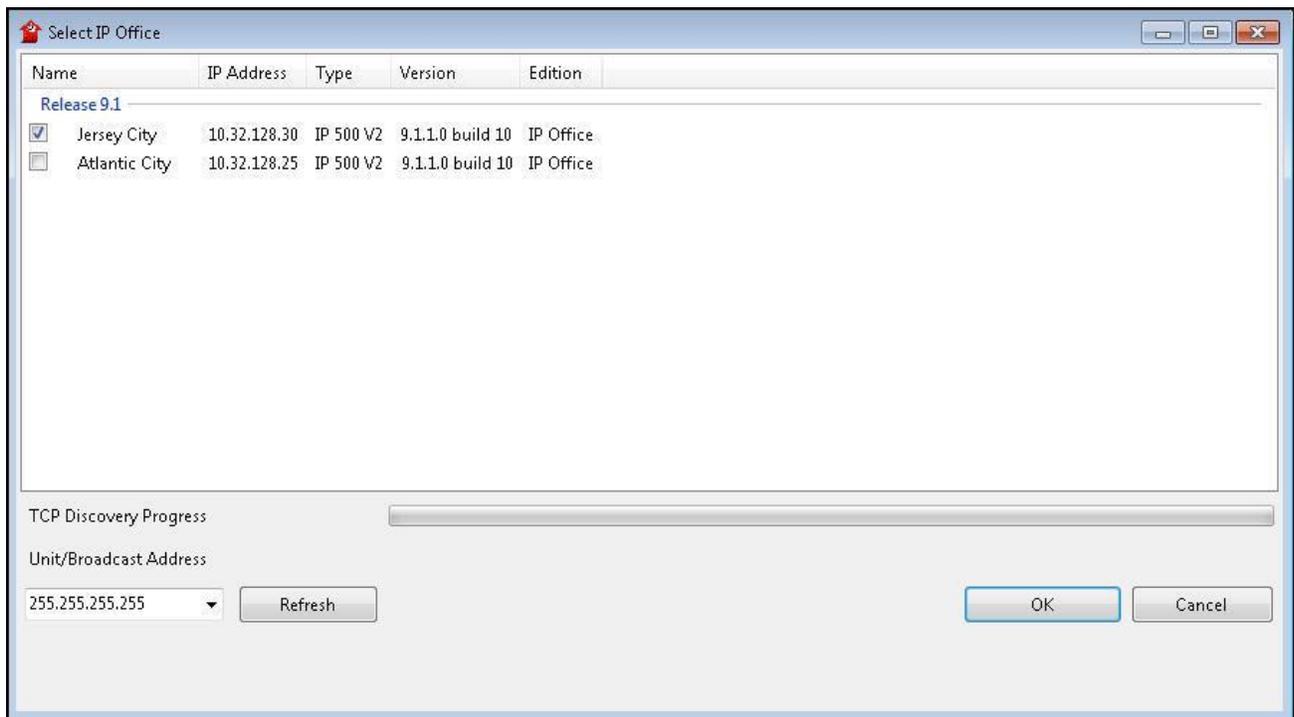
The following equipment and software/firmware were used for the sample configuration provided:

<b>Avaya Telephony Components</b>	
<b>Equipment / Software</b>	<b>Release / Version</b>
Avaya IP Office 500 V2	9.1.1.0 build 10
Avaya IP Office COMBO6210/ATM4 Module	9.1.1.0 build 10
Avaya IP Office Manager	9.1.1.0 build 10
Avaya Preferred Edition (a.k.a Voicemail Pro)	9.1.100.3
Avaya 1616 IP Telephones (H.323)	Avaya one-X® Deskphone 1.3 SP5
Avaya 9611G IP Telephones (H.323)	Avaya one-X® Deskphone 6.4.0.14_V452
Avaya 9630G IP Telephones (H.323)	Avaya one-X® Deskphone 3.2.2
Avaya 1120E IP Telephone (SIP)	4.04.18.00
Avaya Communicator for Windows	2.0.3.30
Avaya Session Border Controller for Enterprise running on Portwell CAD-0208 server	6.3.2-08-5478
<b>Fusion Connect Components</b>	
<b>Equipment / Software</b>	<b>Release / Version</b>
NBSVoice	3.0
ACME Net-Net 4500 Session Border Controller	SCX6.2

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 without T.38 Fax service (T.38 fax is not supported on IP Office Server Edition). Note that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog/digital endpoints or trunks.

## 5. Configure Avaya IP Office

Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the PC running Avaya IP Office Manager, select **Start → All Programs → IP Office → Manager** to launch the application. A **Select IP Office** pop-up window is displayed as shown below. Select the proper Avaya IP Office system from the pop-up window and click **OK** to log in with the appropriate credentials (not shown). The configuration may alternatively be opened by navigating to **File → Open Configuration** at the top of the Avaya IP Office Manager window.



The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation Pane on the left side, omit the Group Pane in the center, and show the Details Pane on the right side. Since the Group Pane has been omitted, its content is shown as submenus in the Navigation Pane. These panes (Navigation and Details) will be referenced throughout the Avaya IP Office configuration.

All licensing and feature configuration that is not directly related to the interface with the service provider (such as administering IP endpoints) is assumed to already be in place.

In the sample configuration, **Jersey City** was used as the system name. All navigation described in the following sections (e.g., **Control Unit → IP 500 V2**) appears as submenus underneath the system name **Jersey City** in the Navigation Pane. The configuration screens highlight values/settings configured for the compliance test. Defaults were used for other values and may be customized based upon requirements in the field.

## 5.1. Licensing and Physical Hardware

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

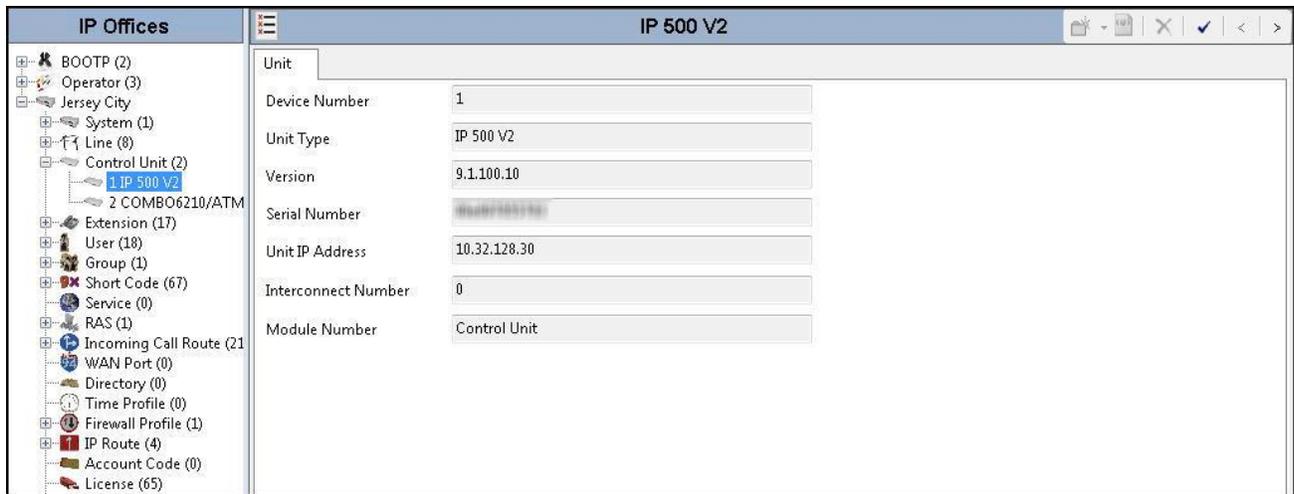
To verify that there is a **SIP Trunk Channels** License with sufficient capacity, click **License** in the Navigation Pane. Confirm a valid license with sufficient **Instances** (trunk channels) in the Details Pane. The screen below also shows the valid license for **Avaya IP endpoints**.

Feature	License Key	Instances	Status	Expiry Date
SIP Trunk Channels	...	255	Valid	Never
IP500 Universal PRI (Additional cha...	...	255	Valid	Never
RAS LRQ Support (Rapid Response)	...	255	Valid	Never
IP Office Dealer Support - Standar...	...	255	Valid	Never
IP Office Dealer Support - Professi...	...	255	Valid	Never
IP Office Distributor Support - Stan...	...	255	Valid	Never
IP Office Distributor Support - Prof...	...	255	Valid	Never
UMS Web Services	...	255	Valid	Never
CCR SUP	...	255	Obsolete	Never
Customer Service Agent	...	255	Obsolete	Never
CCR Designer	...	255	Obsolete	Never
CCR CCC UPG	...	255	Obsolete	Never
1600 Series Phones	...	255	Valid	Never
Third Party API	...	255	Valid	Never
one-X Portal for IP Office	...	255	Valid	Never
Avaya IP endpoints	...	255	Valid	Never

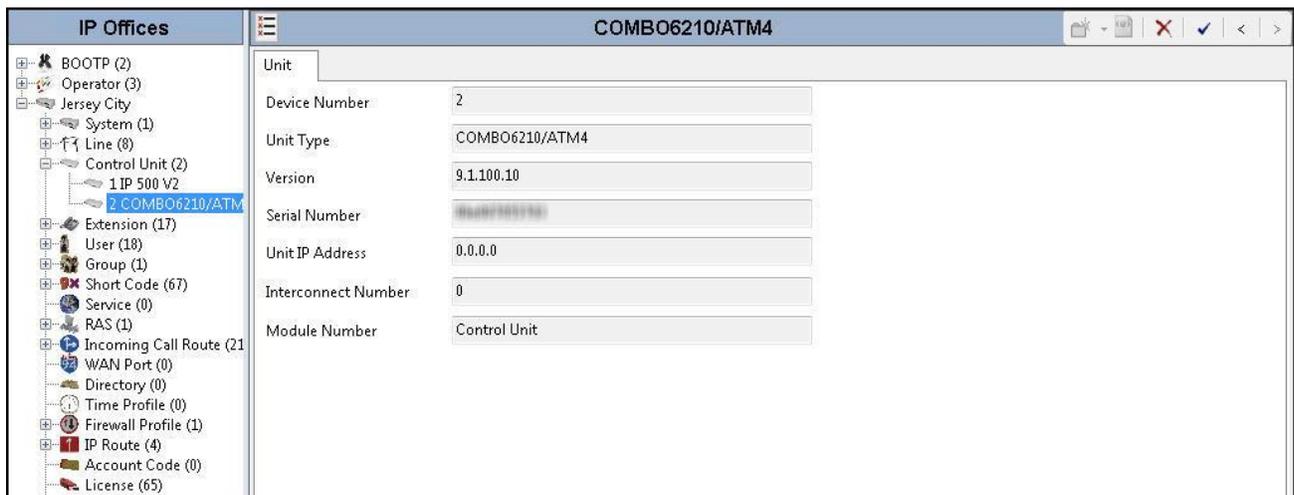
To view the physical hardware comprising the Avaya IP Office system, expand the components under **Control Unit** in the Navigation Pane. In the sample configuration, the second component listed is a Combination Card. This module has 6 digital station ports, two analog extension ports, 4 analog trunk ports and 10 VCM channels. The VCM is a Voice Compression Module supporting VoIP codecs. An Avaya IP Office hardware configuration with a VCM component is necessary to support SIP Trunking.

To view the details of the component, select the component in the Navigation Pane.

The screen below shows the details of the IP 500 V2.



The screen below shows the details of the Combination Card.

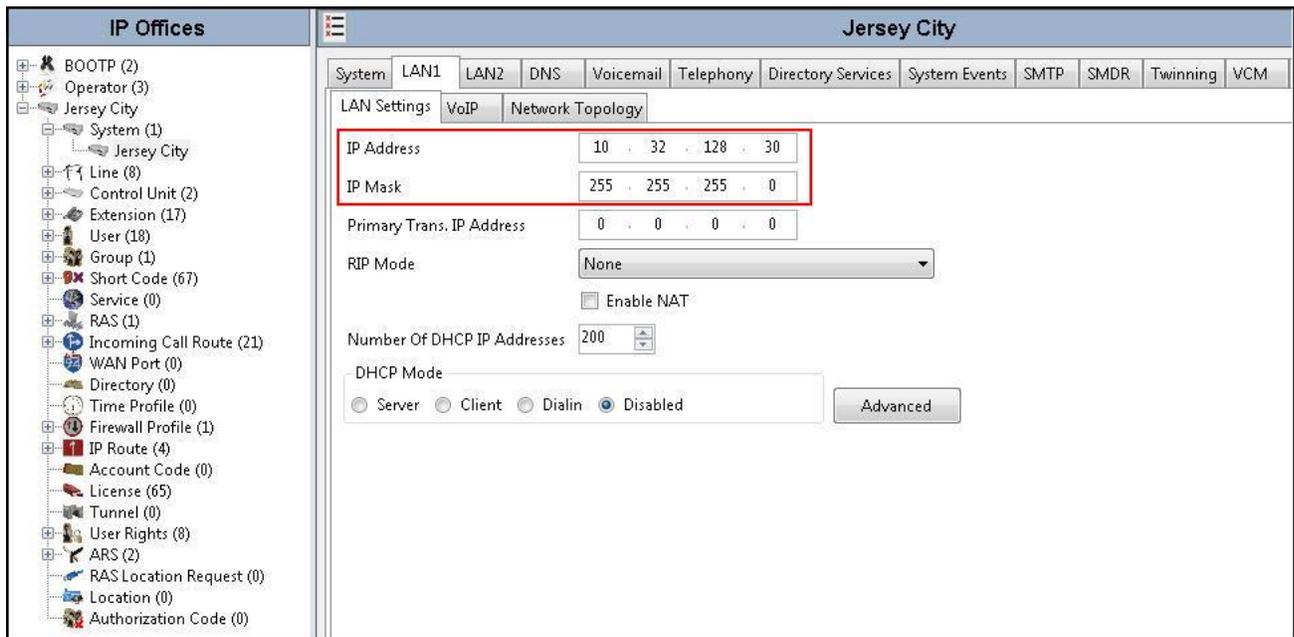


## 5.2. System

This section configures the necessary system settings.

### 5.2.1. System – LAN1 Tab

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



The screenshot displays the configuration interface for the 'Jersey City' system. The left sidebar shows a tree view of system components, including 'System (1)' and 'Jersey City'. The main pane is titled 'Jersey City' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', 'System Events', 'SMTP', 'SMDR', 'Twinning', and 'VCM'. The 'LAN1' tab is active, and the 'LAN Settings' sub-tab is selected. The 'IP Address' field is highlighted with a red box and contains the value '10 . 32 . 128 . 30'. The 'IP Mask' field also contains '255 . 255 . 255 . 0'. Other fields include 'Primary Trans. IP Address' (0 . 0 . 0 . 0), 'RIP Mode' (None), 'Enable NAT' (unchecked), 'Number Of DHCP IP Addresses' (200), and 'DHCP Mode' (Disabled). An 'Advanced' button is visible at the bottom right of the settings pane.

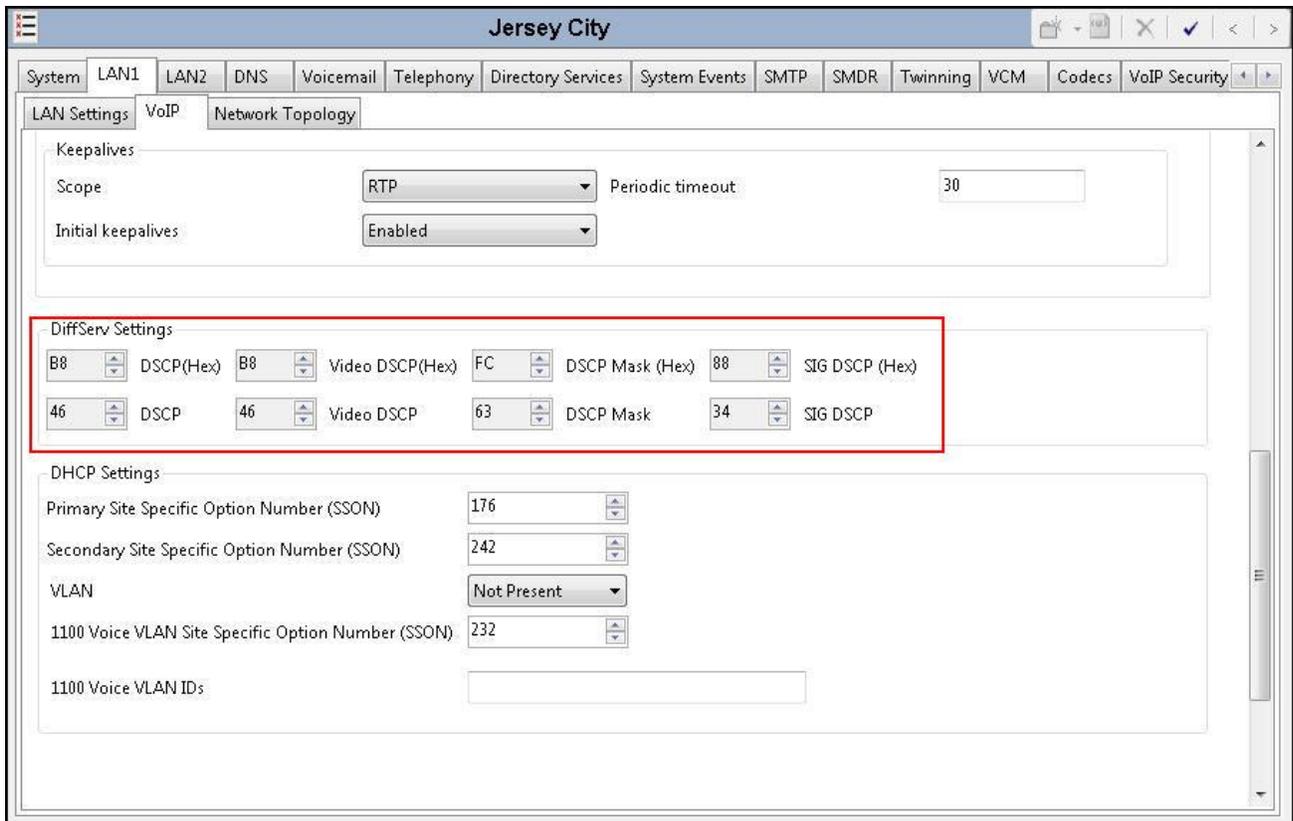
On the **VoIP** tab of LAN1 in the Details Pane, configure the following parameters:

- Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks.
- In the **RTP** section, the **RTP Port Number Range** can be customized to a specific range of receiving ports for the RTP media, as agreed with the service provider. Based on this setting, Avaya IP Office would request RTP media be sent to a port in the configurable range for calls using LAN1.
- In the **Keepalives** section, select **RTP** for **Scope**; select **Enabled** for **Initial keepalives**; enter **30** for **Periodic timeout**. These settings direct IP Office to send a RTP keepalive packet starting at the time of initial connection and every 30 seconds thereafter if no other RTP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting for media from the other, as well as helping to keep firewall (if used) ports open for the duration of the call.

The screenshot shows the configuration interface for LAN1 VoIP settings. The interface is titled "Jersey City" and has tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, VCM, Codecs, and VoIP Security. The VoIP tab is selected, and the "VoIP" sub-tab is active. The "SIP Trunks Enable" checkbox is checked and highlighted with a red box. Below it, the "SIP Registrar Enable" checkbox is also checked. The "Domain Name" is set to "avaya.com". The "Layer 4 Protocol" section has checkboxes for UDP, TCP, and TLS, all of which are checked. The "Challenge Expiry Time (secs)" is set to 10. The "RTP" section has a "Port Number Range" section with "Minimum" set to 49152 and "Maximum" set to 53246, both highlighted with a red box. Below this, the "Port Number Range (NAT)" section has the same values. The "Enable RTCP Monitoring on Port 5005" checkbox is checked. The "RTCP collector IP address for phones" is set to 0.0.0.0. The "Keepalives" section has "Scope" set to "RTP", "Initial keepalives" set to "Enabled", and "Periodic timeout" set to 30, all highlighted with a red box.

Though not highlighted in the above screen, note the settings for **SIP Registrar Enable**, **Domain Name**, and **Layer 4 Protocol**. These settings are necessary for the IP Office to serve as the SIP Registrar Server for the IP Office SIP endpoints.

Scroll down to the **DiffServ Settings** section. Avaya IP Office can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for both signaling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling. The specific values used for the compliance test are shown in the screen below and are also the default values. For a customer installation, if the default values are not sufficient, appropriate values should be provided by the customer.



On the **Network Topology** tab of LAN1 in the Details Pane, configure the following parameters:

- Select **Firewall/NAT Type** from the pull-down menu that matches the network configuration. No firewall or network address translation (NAT) device was used in the compliance test as shown in **Figure 1**, so the parameter was set to **Open Internet**. With the **Open Internet** setting, **STUN Server Address** is not used.
- Set **Binding Refresh Time (seconds)** to a desired value. This value is used as one input to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider. See **Section 5.10** for complete details.
- Set **Public Port** to **5060** for **UDP**.

The screenshot shows the configuration window for 'Jersey City' with the 'Network Topology' tab selected for 'LAN1'. The 'Network Topology Discovery' section contains the following settings:

- STUN Server Address: [Redacted]
- STUN Port: 3478
- Firewall/NAT Type: Open Internet (highlighted with a red box)
- Binding Refresh Time (seconds): 120
- Public IP Address: 0 . 0 . 0 . 0
- Public Port: UDP (5060) (highlighted with a red box), TCP (0), TLS (0)
- Run STUN on startup:

Buttons for 'Run STUN' and 'Cancel' are visible at the bottom right of the configuration area.

## 5.2.2. System - Voicemail Tab

In the **Voicemail** tab of the Details Pane, configure the **SIP Settings** section. The **SIP Name** and **Contact** are set to one of the DID numbers provided by Fusion Connect. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. Uncheck the **Anonymous** box to allow the Voicemail Caller ID information to be sent to the network.

Note the selection for **Voicemail Type** and the IP address setting for **Voicemail IP Address**. These are for configuring Voicemail Pro as the voice messaging service for Avaya IP Office users (part of the standard IP Office setup beyond the scope of these Application Notes).

The screenshot shows the configuration interface for the Voicemail tab in Jersey City. The interface includes several sections:

- Voicemail Type:** Set to "Voicemail Lite/Pro".
- Voicemail Destination:** (Empty dropdown)
- Voicemail IP Address:** 10 . 32 . 128 . 78
- Backup Voicemail IP Address:** 0 . 0 . 0 . 0
- Voicemail Channel Reservation:**
  - Unreserved Channels: 237
  - Auto-Attendant: 2
  - Voice Recording: 5
  - Mandatory Voice Recording: 5
  - Announcements: 5
  - Mailbox Access: 5
- DTMF Breakout:**
  - Reception / Breakout (DTMF 0): (Empty dropdown)
  - Breakout (DTMF 2): (Empty dropdown)
  - Breakout (DTMF 3): (Empty dropdown)
- Voicemail Code Complexity:**
  - Enforcement:
  - Minimum length: 4
  - Complexity:
- SIP Settings:**
  - SIP Name: 4405963561
  - SIP Display Name (Alias): Voicemail
  - Contact: 4405963561
  - Anonymous:
- Call Recording:**
  - Auto Restart Paused Recording (secs): 15
  - Hide Auto Recording:

Buttons at the bottom: OK, Cancel, Help.

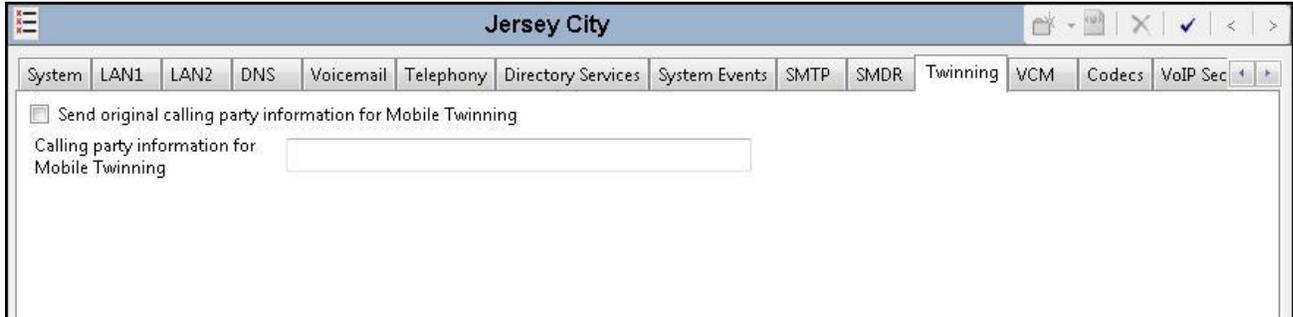
### 5.2.3. System - Telephony Tab

Navigate to the **Telephony** → **Telephony** tab in the Details Pane. Enter or select **0** for **Hold Timeout (secs)** so that calls on hold will not time out. Choose the **Companding Law** typical for the enterprise site. For the compliance test, **U-LAW** was used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the service provider per customer business policies. Note that this configuration might pose a security issue (Toll Fraud). Customers should exercise caution with this configuration.

The screenshot shows the 'Jersey City' configuration window for the 'Telephony' tab. The 'Hold Timeout (secs)' field is highlighted with a red box and set to 0. The 'Companding Law' section is also highlighted with a red box, showing 'U-Law' selected for both 'Switch' and 'Line'. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked and highlighted with a red box. Other settings include 'Default Outside Call Sequence' set to 'Normal', 'Default Inside Call Sequence' set to 'Ring Type 1', and 'Default Ring Back Sequence' set to 'Ring Type 2'. The 'Dial Delay Time (secs)' is 4, 'Dial Delay Count' is 0, and 'Default No Answer Time (secs)' is 15. The 'Park Timeout (secs)' is 300, 'Ring Delay (secs)' is 5, and 'Call Priority Promotion Time (secs)' is 'Disabled'. The 'Default Currency' is 'USD', 'Default Name Priority' is 'Favor Trunk', and 'Media Connection Preservation' is 'Enabled'. The 'Phone Failback' is 'Manual'. The 'Login Code Complexity' section has 'Enforcement' checked and 'Minimum length' set to 4. The 'DSS Status' is unchecked, 'Auto Hold' is checked, 'Dial By Name' is checked, and 'Show Account Code' is checked. Other options like 'Restrict Network Interconnect', 'Include location specific information', 'Drop External Only Impromptu Conference', 'Visually Differentiate External Call', 'Unsupervised Analog Trunk Disconnect Handling', 'High Quality Conferencing', 'Digital/Analogue Auto Create User', and 'Directory Overrides Barring' are unchecked.

## 5.2.4. System - Twinning Tab

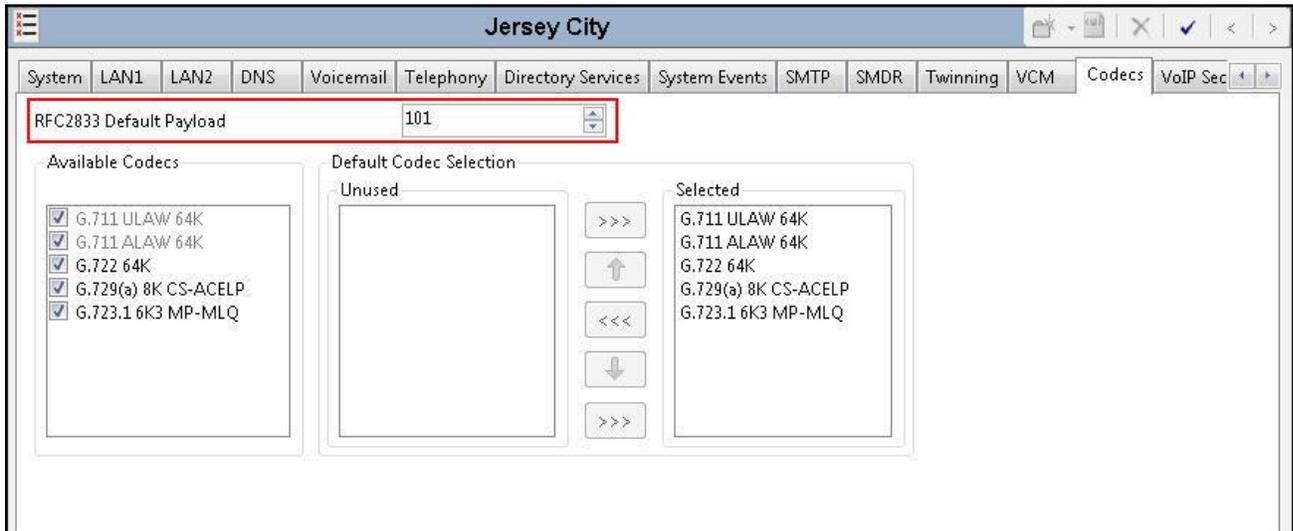
To view or change the System Twinning settings, navigate to the **Twinning** tab in the Details Pane as shown in the following screen. The **Send original calling party information for Mobile Twinning** box is not checked in the sample configuration, and the **Calling party information for Mobile Twinning** is left blank.



## 5.2.5. System – Codex Tab

In the **Codex** tab of the Details Pane, select or enter **101** for **RFC2833 Default Payload**. This setting was preferred by Fusion Connect for use with out-band DTMF tone transmissions.

On the left, observe the list of **Available Codex**. In the screen below, which is not intended to be prescriptive, the box next to each codec is checked, making all the codex available in other screens where codec configuration may be performed. The **Default Codex Selection** area enables the codec preference order to be configured on a system-wide basis. 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.



### 5.3. IP Route

Navigate to **IP Route** → **0.0.0.0** in the left Navigation Pane if a default route already exists.

Otherwise, to create the default route, right-click on **IP Route** and select **New** (not shown). Create and verify a default route with the following parameters:

- Set **IP Address** and **IP Mask** to **0.0.0.0**.
- Set **Gateway IP Address** to the IP address of the enterprise LAN gateway for the subnet where the Avaya IP Office is connected.
- Set **Destination** to **LAN1** from the drop-down list.



## 5.4. Administer SIP Line

A SIP Line is needed to establish the SIP connection between Avaya IP Office and the Fusion Connect network. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.4.1** to create the SIP Line from the 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 (500 V2) and IP Office Server Edition systems.

Some items relevant to a specific customer environment are not included in the template associated with these Application Notes, 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 SIP Line **Transport** tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2** through **5.4.8**.

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

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

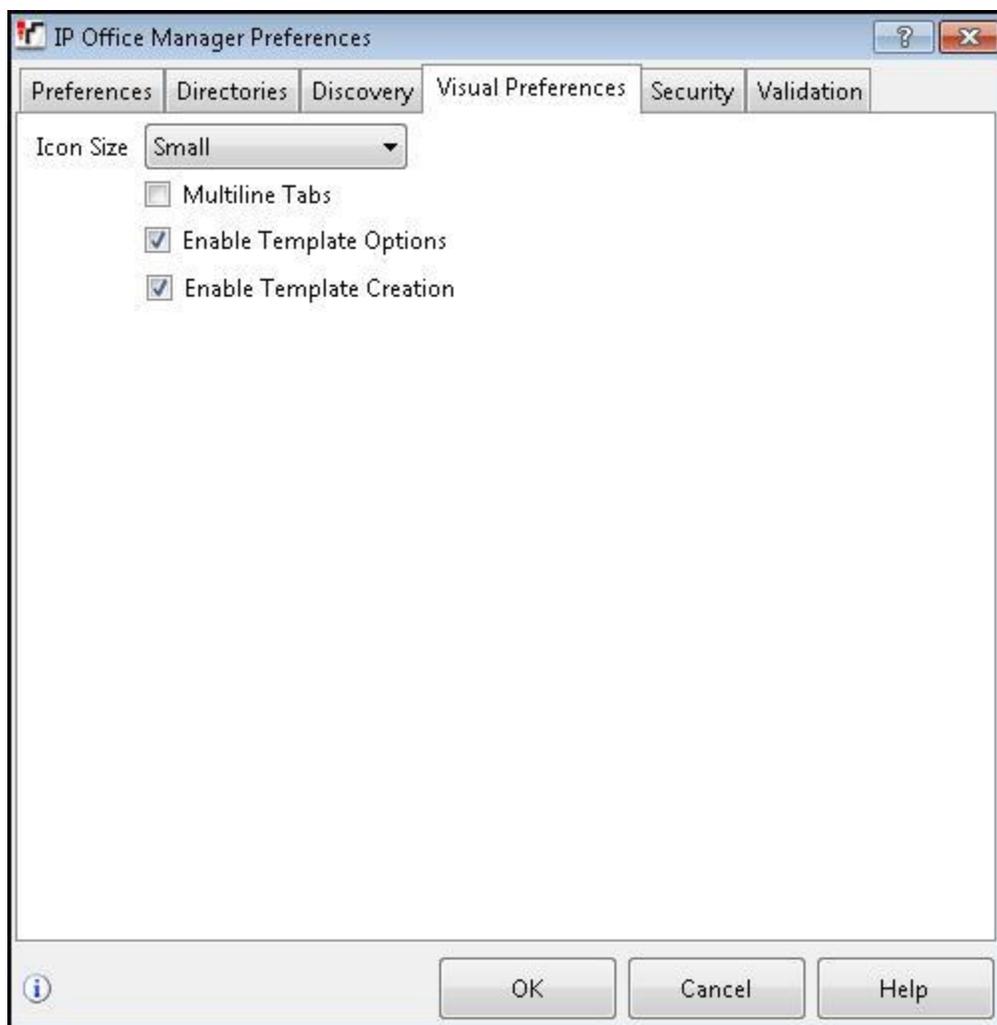
### 5.4.1. Create SIP Line From Template

1. Copy the template file to a location (e.g., C:\Temp) on the computer where IP Office Manager is installed. Verify that the template file name is

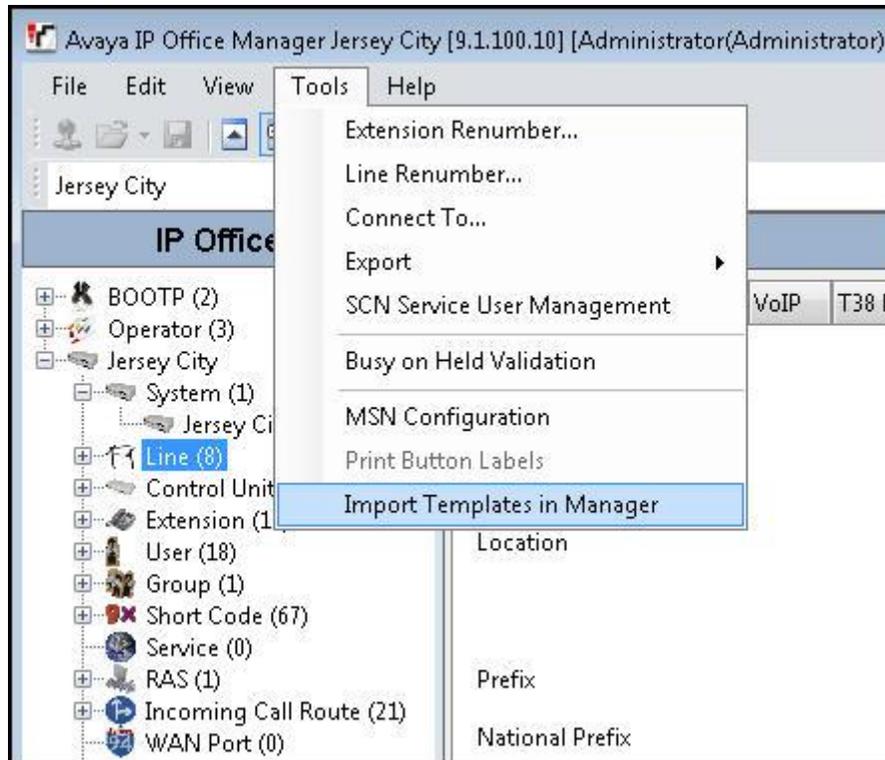
**AF\_Fusion Connect\_SIPTrunk.xml**

The file name is important in locating the proper template file in **Step 4**.

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



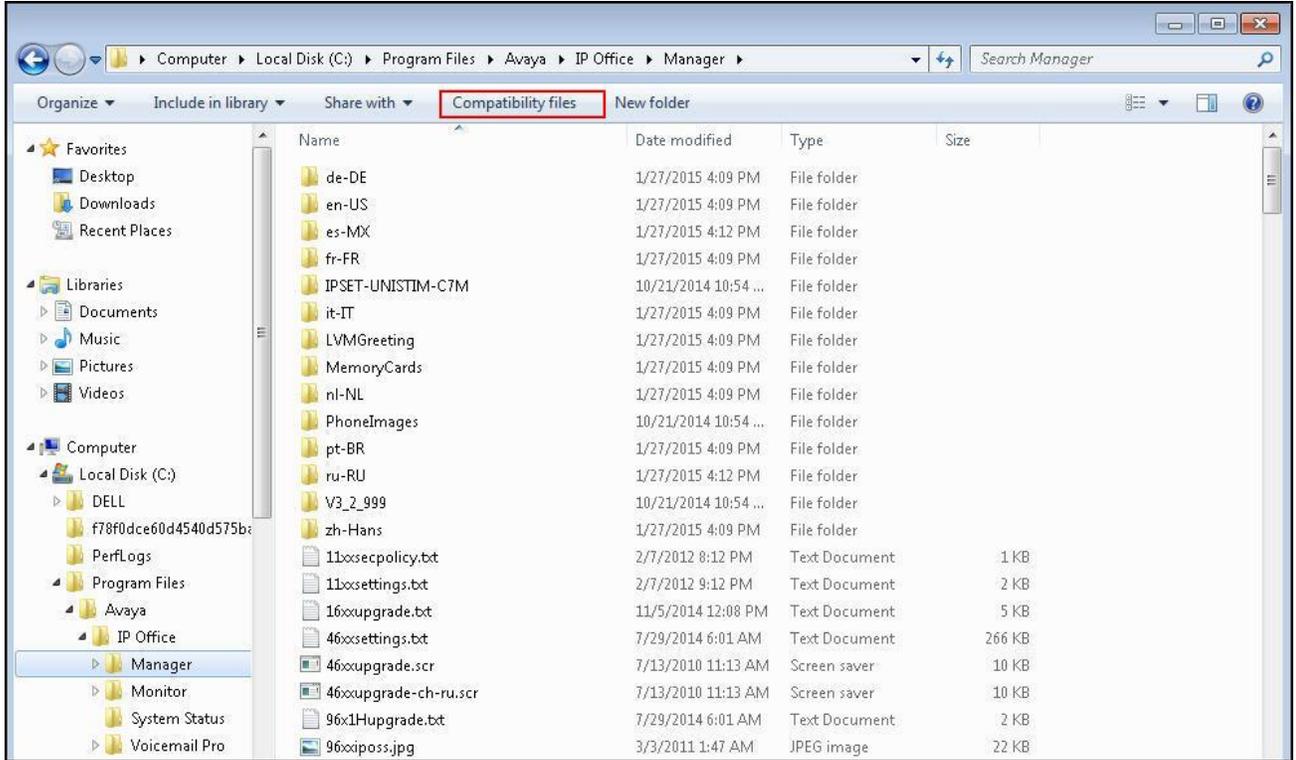
3. Import the template into IP Office Manager. From IP Office Manager, select **Tools** → **Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 4**. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.



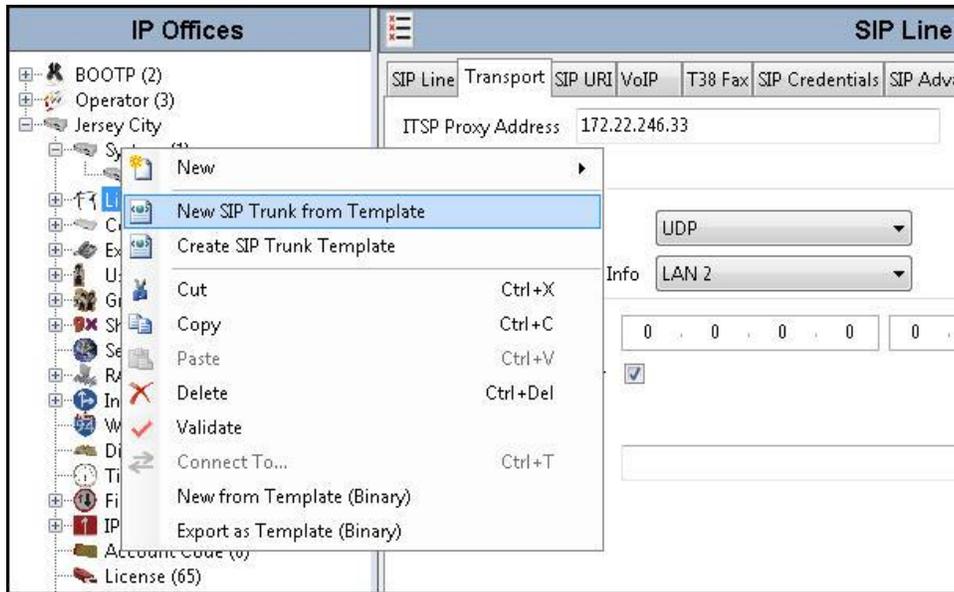
In the pop-up window that appears (not shown), select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue.

If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

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



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



In the subsequent **Template Type Selection** pop-up window, select *Fusion Connect* from the **Service Provider** drop-down list as shown below. This selection corresponds to parts of the template file name as specified in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.



Note that the newly created SIP Line may not immediately appear in the Navigation pane until the configuration was saved, closed and reopened in IP Office Manager.

5. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2** through **5.4.8**.

## 5.4.2. SIP Line – SIP Line Tab

In the **SIP Line** tab of the Details Pane, configure the parameters as shown below:

- Set **ITSP Domain Name** to the IP address of the internal signaling interface of the Avaya SBCE.
- Check the **In Service** box.
- Check **OOS** box. Avaya IP Office will check the SIP OPTIONS response from the far end to determine whether to take the SIP Line out of service.
- In the **Session Timers** section, set **Method for Session Refresh** to *Auto*. With this setting Avaya IP Office will send UPDATE messages for session refresh if the other party supports UPDATE. If UPDATE is not supported, re-INVITE messages are sent. Set **Timer (seconds)** to a desired value. Avaya IP Office will send out session refresh UPDATE or re-INVITE at the specified intervals (half of the specified value).
- Set **Send Caller ID** under **Forwarding and Twinning** to *Diversion Header*. With this setting and the related configuration in **Section 5.2.4**, Avaya IP Office will include the Diversion Header for calls that are redirected via Mobile Twinning out the SIP Line to the PSTN. It will also include the Diversion Header for calls that are forwarded out the SIP Line.
- Under Redirect and Transfer, select *Always* for **Incoming Supervised REFER** and **Outgoing Supervised REFER**. Fusion Connect supports use of the REFER method for off-net call transfer.

The screenshot displays the configuration window for 'SIP Line - Line 17'. The left sidebar shows a tree view of the system hierarchy, including IP Offices, BOOTP, Operator, Jersey City, System, Line, Control Unit, Extension, User, Group, Short Code, Service, RAS, Incoming Call Route, WAN Port, Directory, Time Profile, Firewall Profile, IP Route, and Account Code. The main configuration area is divided into several tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax, SIP Credentials, SIP Advanced, and Engineering. The 'SIP Line' tab is active, showing the following configuration details:

- Line Number: 17
- ITSP Domain Name: 10.32.128.20
- URI Type: SIP
- Location: Cloud
- Prefix: (empty)
- National Prefix: (empty)
- International Prefix: (empty)
- Country Code: (empty)
- Name Priority: System Default
- Description: (empty)
- In Service:
- Check OOS:
- Session Timers:
  - Refresh Method: Auto
  - Timer (seconds): 480
- Forwarding and Twinning:
  - Originator number: (empty)
  - Send Caller ID: Diversion Header
- Redirect and Transfer:
  - Incoming Supervised REFER: Always
  - Outgoing Supervised REFER: Always
  - Send 302 Moved Temporarily:
  - Outgoing Blind REFER:

### 5.4.3. SIP Line – Transport Tab

Navigate to the **Transport** tab and set the following:

- Set the **ITSP Proxy Address** to the IP address of the internal signaling interface of the Avaya SBCE.
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to the network port used by the SIP line to access the far-end as configured in **Section 5.2.1**.
- Set the **Send Port** to **5060**.

The screenshot shows the configuration interface for a SIP Line, specifically the Transport tab. The ITSP Proxy Address is set to 10.32.128.20. The Network Configuration section is highlighted with a red box and includes the following settings: Layer 4 Protocol is set to UDP, Send Port is 5060, Use Network Topology Info is set to LAN 1, and Listen Port is 5060. Below this, the Explicit DNS Server(s) field is empty. The Calls Route via Registrar checkbox is checked. The Separate Registrar field is empty.

### 5.4.4. SIP Line – SIP URI Tab

Select the **SIP URI** tab to create or edit a SIP URI entry. A SIP URI entry matches each incoming number that Avaya IP Office will accept on this line. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane. For the compliance test, a single SIP URI entry was created to match any DID number assigned to Avaya IP Office users. The following screen shows the edit window on this URI entry for the compliance test.

- Set **Local URI** to **Use Internal Data**. This setting allows calls on this line whose SIP URI matches the **SIP Name** set on the **SIP** tab of any **User** as shown in **Section 5.6**, or the **SIP Name** set in the **SIP Settings** area of the System **Voicemail** tab as shown in **Section 5.2.2**.
- Set **Contact** and **Display Name** to **Use Internal Data**. This setting will cause the Contact and Display Name data for outbound messages to be set from the corresponding fields on the **SIP** tab of the individual **User** as shown in **Section 5.66**.
- Set **PAI** to **Use Internal Data**. This setting directs Avaya IP Office to send the PAI (P-Asserted-Identity) header when appropriate. The PAI header will be populated from the data set in the **SIP** tab of the call initiating **User** as shown in **Section 5.66**.
- Select **0: <None>** for **Registration**.
- Associate this line with an incoming line group by entering line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes

for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. For the compliance test, the incoming and outgoing group **17** was specified. Note that this group number can be different than the SIP Line number.

- Set **Max Calls per Channel** to the number of simultaneous SIP calls allowed using this SIP URI pattern.

**SIP Line - Line 17**

Channel	Groups	Via	Local URI	Contact	Display...	PAI	Credential	Max Calls
1	17 17	10.32.128.30					0: <Non...	10
2	17 0	10.32.128.30	4405963560	4405963560	FNE31	N...	0: <Non...	10

**Edit Channel**

Via: 10.32.128.30

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

PAI: Use Internal Data

Registration: 0: <None>

Incoming Group: 17

Outgoing Group: 17

Max Calls per Channel: 10

The screen below shows the edit window for the pre-configured SIP URI entry for matching inbound calls to the Mobile Call Control application (see **Section 5.9**). This entry was necessary since the DID number assigned to the Mobile Call Control application was not configured elsewhere for matching the incoming call Request URI. Without this SIP URI entry, the Avaya IP Office would have responded to an incoming call to the DID meant for the Mobile Call Control application with a “404 Not Found” status message and the call would have failed.

The DID **4405963560** will be configured in the Incoming Call Route in **Section Error! Reference source not found.** to deliver the call to the Mobile Call Control application.

The screenshot shows the 'SIP Line - Line 17' configuration window. At the top, there are tabs for 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. Below the tabs is a table with the following columns: Channel, Groups, Via, Local URI, Contact, Display..., PAI, Credential, and Max Calls. Two rows are visible: Row 1 has Channel 1, Groups 17 17, Via 10.32.128.30, Local URI, Contact, Display..., PAI, Credential 0: <Non..., and Max Calls 10. Row 2 is highlighted and has Channel 2, Groups 17 0, Via 10.32.128.30, Local URI 4405963560, Contact 4405963560, Display... FNE31, PAI N..., Credential 0: <Non..., and Max Calls 10. To the right of the table are buttons for 'Add...', 'Remove', and 'Edit...'. Below the table is the 'Edit Channel' form with the following fields: Via (10.32.128.30), Local URI (4405963560), Contact (4405963560), Display Name (FNE31), PAI (None), Registration (0: <None>), Incoming Group (17), Outgoing Group (0), and Max Calls per Channel (10). At the bottom right of the form are 'OK' and 'Cancel' buttons.

Channel	Groups	Via	Local URI	Contact	Display...	PAI	Credential	Max Calls
1	17 17	10.32.128.30					0: <Non...	10
2	17 0	10.32.128.30	4405963560	4405963560	FNE31	N...	0: <Non...	10

Note that a **0** setting means no line group number was configured for **Outgoing Group** for this SIP URI entry. This is because this SIP URI entry is used only for inbound calls to the Mobile Call Control application.

### 5.4.5. SIP Line – VoIP Tab

Select the **VoIP** tab. Set the parameters as shown below.

- Select **Custom** for **Codec Selection**.
- Choose **G.711 ULAW 64K** or **G.729(a) 8K CS-ACELP** from the **Unused** box and move the selection to the **Selected** box. Fusion Connect supports both G.711u and G.729a codecs, but customer must inform Fusion Connect about the one preferred codec to use so that the codec configuration on the service side can match the enterprise. See the item **Supported Codecs** in the observation/limitation list in **Section 2.2** for more details. The screen below shows configuration of G.711u as the preferred codec.
- Select **T38 Fallback** for **Fax Transport Support** to direct Avaya IP Office to use T.38 for fax calls and use G.711u pass-through for fax if the remote end does not support T.38.
- Select **RFC2833** for **DTMF Support**. This directs Avaya IP Office to send DTMF tones as out-band RTP events as per RFC2833.
- Uncheck the **VoIP Silence Suppression** option box.
- Check the **Re-invite Supported** option box. When enabled, re-INVITE can be used during a call session to change the characteristics of the session including codec re-negotiation.
- Check the **PRACK/100rel Supported** option box. This setting enables support by Avaya IP Office for the PRACK (Provisional Reliable Acknowledgement) message on SIP trunks.
- Check **G.711 Fax ECAN**.

The screenshot shows the configuration window for a SIP Line (Line 17\*). The 'VoIP' tab is active. The 'Codec Selection' is set to 'Custom'. In the 'Unused' list, 'G.711 ALAW 64K', 'G.722 64K', 'G.729(a) 8K CS-ACELP', and 'G.723.1 6K3 MP-MLQ' are listed. 'G.711 ULAW 64K' has been moved to the 'Selected' list. The 'Fax Transport Support' is set to 'T38 Fallback' and 'DTMF Support' is set to 'RFC2833'. The 'Media Security' is set to 'Disabled'. On the right, the following options are checked: 'Re-invite Supported', 'PRACK/100rel Supported', and 'G.711 Fax ECAN'. The following options are unchecked: 'VoIP Silence Suppression', 'Codec Lockdown', 'Allow Direct Media Path', and 'Force direct media with phones'.

### 5.4.6. SIP Line – T38 Fax

The settings on this tab configures T.38 fax parameters and are only accessible if **Re-invite Supported** was checked and either **T38** or **T38 Fallback** was selected for **Fax Transport Support** in the **VoIP** tab in **Section 5.4.5**.

The screen below shows the settings used for the compliance test. The **T38 Fax Version** is set to **0**. In the **Redundancy** area, **Low Speed** and **High Speed** are set to **2**. The **Disable T30 ECM** must be checked or fax errors may be experienced when using T.38 Fax. When selected, it disables the T.30 Error Correction Mode used for fax transmission. All other values are left at default.

The screenshot shows the configuration window for 'SIP Line - Line 17'. The 'T38 Fax' tab is active. The 'T38 Fax Version' dropdown is set to '0'. The 'Transport' dropdown is set to 'UDPTL'. In the 'Redundancy' section, 'Low Speed' and 'High Speed' are both set to '2'. The 'Disable T30 ECM' checkbox is checked. Other settings include 'TCF Method' (Trans TCF), 'Max Bit Rate (bps)' (14400), 'Eflag Start Timer (msecs)' (2600), 'Eflag Stop Timer (msecs)' (2300), and 'Tx Network Timeout (secs)' (150). On the right, 'Scan Line Fix-up' and 'TFOP Enhancement' are checked, while 'Disable EFlags For First DIS' and 'Disable T30 MR Compression' are unchecked. 'NSF Override' is also unchecked, with 'Country Code' and 'Vendor Code' both set to '0'.

### 5.4.7. SIP Line – SIP Credentials Tab

SIP Credentials are used to register the SIP Trunk with a service provider that requires SIP Registration. SIP Credentials are also used to provide the required information for Digest Authentication of outbound calls. SIP Credentials are unique per customer and therefore customers must contact the service provider to obtain the proper registration and/or Digest Authentication credentials for their deployment.

For this compliance test, Fusion Connect configured the test circuit as a static trunk that did not require trunk registration or Digest Authentication for outbound calls. Therefore, this tab did not need to be visited.

## 5.4.8. SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab to configure advanced SIP Line parameters.

In the **Identity** area, the **Use PAI for Privacy** box is checked for Avaya IP Office to use the P-Asserted-Identity (PAI) SIP header for privacy-requested outbound calls. With this configuration, Avaya IP Office will populate the From and Contact headers of the anonymous outbound call INVITE with “anonymous” as the URI user part, but include the normal calling user information in the PAI header. The **Caller ID from From header** box is checked for Avaya IP Office to use the Caller ID information in the From SIP header rather than the PAI or Contact SIP header for inbound calls.

In the **Media** area, select **System** for **Media Connection Preservation** to allow established calls to continue despite brief network failures.

In the **Call Control** area, **No REFER if using Diversion** is checked to prevent Avaya IP Office from using the SIP REFER method on call scenarios that use the Diversion SIP header (e.g., off-net call forward or outbound call to mobile twinning number).

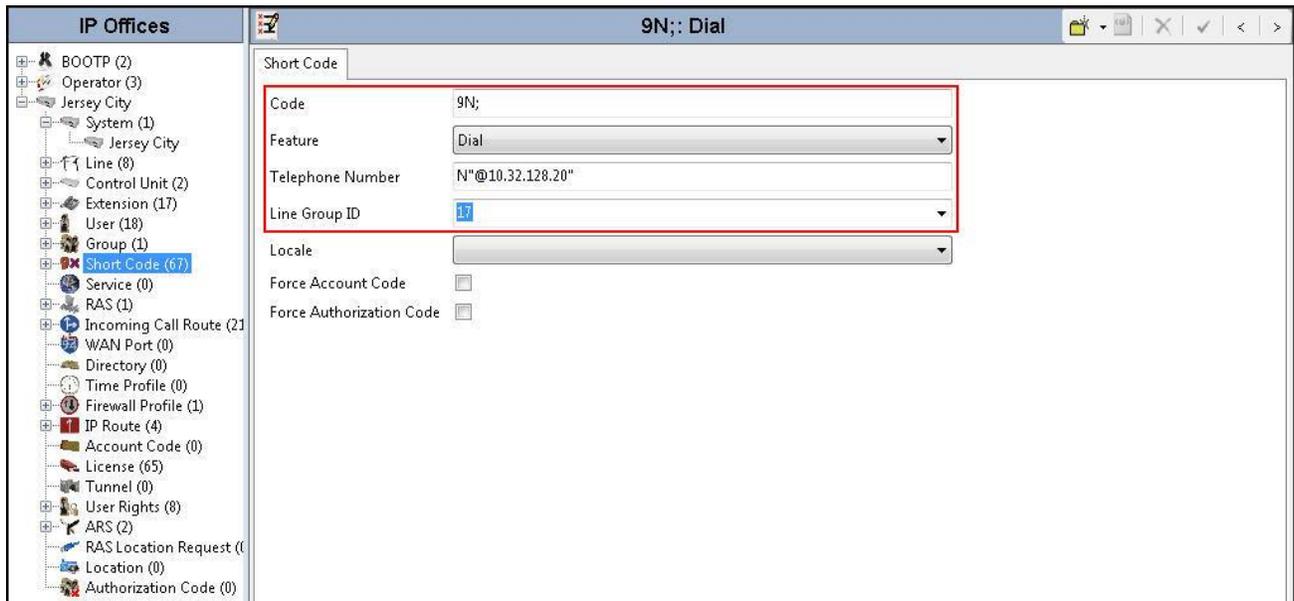
The screenshot displays the configuration interface for SIP Line - Line 17, specifically the SIP Advanced tab. The interface is organized into several sections:

- Addressing:** Association Method is set to "By Source IP address" and Call Routing Method is set to "Request URI".
- Identity:** A list of checkboxes includes "Use PAI for Privacy" (checked), "Caller ID from From header" (checked), "Use Phone Context", "Add user=phone", "Use + for International", "Use Domain for PAI", "Swap From and PAI", "Send From In Clear", "Cache Auth Credentials", and "User-Agent and Server Headers".
- Media:** A dropdown menu for "Media Connection Preservation" is set to "System".
- Call Control:** Includes fields for "Call Initiation Timeout (s)" (4), "Call Queuing Timeout (m)" (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", "Emulate NOTIFY for REFER", and "No REFER if using Diversion" (checked).

## 5.5. Short Code

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

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. The **9N;** short code, used for the compliance test, will be invoked when the user dials 9 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N"@10.32.128.20"**. This field is used to construct the Request URI and the To header in the outgoing SIP INVITE message. The value **N** represents the number dialed by the user. The IP address following the @ sign is the IP address of the private interface of the Avaya SBCE.
- Set the **Line Group Id** to the **Outgoing Group** number defined on the **SIP URI** tab of the SIP Line in **Section 5.4.4**. This short code will use this line group when placing outbound calls.



The simple **9N;** short code illustrated above does not provide a means of alternate routing if the configured SIP Line is out of service or temporarily not responding. When alternate routing options and/or more customized analysis of the dialed digits following the short code are desired, the Automatic Route Selection (ARS) feature may be used.

In the screen below, the short code **8N;** is illustrated for access to ARS. When the Avaya IP Office user dials 8 plus any number *N*, rather than being directed to a specific **Line Group ID**, the call is directed to **50: Main**, configurable via ARS. See **Section 5.8** for example ARS route configuration.

Short Code	
Code	8N;
Feature	Dial
Telephone Number	N
Line Group ID	50: Main
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

Optionally, add or edit a short code used to access the SIP Line anonymously. In the screen shown below, the short code **\*67N;** is illustrated. This short code is similar to the **9N;** short code except that the **Telephone Number** field begins with the letter **W**, which means “withhold the outgoing calling line identification”. In the case of the compliance test, when a user dialed \*67 plus the destination number, Avaya IP Office would include the user’s telephone number (DID number assigned to the user) in the **P-Asserted-Identity (PAI)** header, populate the URI user part with “anonymous” in the From and Contact headers, and include the **Privacy: id** header in the outbound INVITE message. Consequently Fusion Connect would prevent presentation of the caller id to the called PSTN destination.

Short Code	
Code	*67N;
Feature	Dial
Telephone Number	WN"@10.32.128.20"
Line Group ID	17
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

For completeness, the short code **FNE31** for the Mobile Call Control application is shown below. See **Section 5.7** for routing incoming call to this application to receive internal IP Office dial tones. See **Section 5.9** for configuration to enable this mobility feature.

## 5.6. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line. To configure these settings, first navigate to **User**→**Name** in the Navigation Pane, where **Name** is the name of the user to be modified. In the example below, the name of the user is “Tony 9611” at extension 256. Select the **SIP** tab in the Details Pane. The **SIP Name** and **Contact** are set to one of the DID numbers provided by Fusion Connect. The **SIP Display Name (Alias)** can optionally be configured with a descriptive text string. The value entered for the **Contact** field will be used in the Contact header for outgoing SIP INVITE to the service provider. The value entered for the **SIP Name** is used as the user part of the SIP URI in the From header for outgoing SIP INVITE.

If outbound calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user information from the network (or alternatively use the **\*67N**; short code as defined in **Section 5.5**).

## 5.7. Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal destination. This procedure should be repeated for each DID number provided by the service provider. To create an incoming call route, right-click **Incoming Call Route** in the Navigation Pane and select **New** (not shown). On the **Standard** tab in the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capacity** to *Any Voice*.
- Set the **Line Group Id** to the **Incoming Group** of the SIP Line defined in **Section 5.4.4**.
- Set the **Incoming Number** to the incoming number on which this route should match.

Field	Value
Bearer Capacity	Any Voice
Line Group ID	17
Incoming Number	4405963562
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

On the **Destinations** tab, select the destination from the pull-down list of the **Destination** field. In this example, incoming calls to 4405963562 on Incoming Group 17 are to be routed to the user “Tony 9611” at extension 256.

Field	Value
TimeProfile	Default Value
Destination	256 Tony 9611
Fallback Extension	

The screen below shows calls routed to the IP Office fax endpoint which is an analog extension (Extn 208).

TimeProfile	Destination	Fallback Extension
Default Value	208 Extn208	

The screen below shows calls routed to IP Office Voicemail Pro for message retrieval. Note that the DID 4405963561 was assigned to Voicemail in **Section 5.2.2**.

TimeProfile	Destination	Fallback Extension
Default Value	VoiceMail	

The following **Destinations** tab for an incoming call route contains the **Destination** “FNE31” entered manually. The name “FNE31” is the short code for accessing the Mobile Call Control application. An incoming call to 4405963560 from an IP Office user’s twinned mobile phone will be delivered directly to an internal dial tone from the Avaya IP Office, allowing the caller to dial call destinations, both internal and external. See **Section 5.9** on configuration to enable the Mobile Call Control application.

TimeProfile	Destination	Fallback Extension
Default Value	FNE31	

## 5.8. ARS and Alternate Routing

While detailed coverage of Automatic Route Selection (ARS) is beyond the scope of these Application Notes, this section includes basic ARS screen illustration and considerations. ARS is shown here mainly to illustrate alternate routing should the SIP Line be out of service or temporarily not responding.

Optionally, ARS can be used to supplement or replace the simple **9N**; short code approach documented in **Section 5.5**. With ARS, secondary dial tone can be provided after the access code, time-based routing criteria can be introduced, and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. ARS also facilitates more specific dialed telephone number matching, enabling immediate routing and alternate treatment for different types of numbers following the access code. For example, if all local and long distance calls should use the SIP Line, but service numbers should prefer a different outgoing line group, ARS can be used to distinguish between the two call patterns.

To add a new ARS route, right-click **ARS** in the Navigation Pane and select **New** (not shown). To view or edit an existing ARS route, expand ARS in the Navigation Pane and select a route name.

The following screen shows an example ARS configuration for the route named **50: Main**. The **In Service** parameter refers to the ARS form itself, not the Line Groups that may be referenced in the form. If the **In Service** box is un-checked, calls are routed to the ARS route name specified in the **Out of Service Route** parameter. IP Office short codes may also be defined to allow an ARS route to be disabled or enabled from a telephone. The configurable provisioning of an Out of Service Route and the means to manually activate the Out of Service Route can be helpful for scheduled maintenance or other known service-affecting events for the primary route.

The screenshot displays the configuration for an ARS route named 'Main' (ARS Route Id: 50). The interface includes a navigation pane on the left and a main configuration area on the right. The main area is divided into several sections:

- General Settings:** Includes fields for ARS Route Id (50), Route Name (Main), Dial Delay Time (System Default (4)), and Description. There are checkboxes for 'Secondary Dial tone' (checked) and 'Check User Call Barring' (checked). A 'SystemTone' dropdown is also present.
- Routing Logic:** A flow diagram shows the 'In Service' checkbox checked, leading to the 'Out of Service Route' dropdown set to '51: backup'. Below this, the 'Time Profile' is set to '<None>', leading to the 'Out of Hours Route' dropdown set to '<None>'.
- Code Table:** A table with columns for Code, Telephone Number, Feature, and Line Group ID. Two entries are shown:

Code	Telephone Number	Feature	Line Group ID
911	911	Dial Emergency	1
N;	N"@10.32.128.20"	Dial	17
- Alternate Routing:** A section at the bottom shows 'Alternate Route Priority Level' set to 3 and 'Alternate Route Wait Time' set to 30. The 'Alternate Route' dropdown is set to '51: backup'.

Assuming the primary route is in-service, the number passed from the short code used to access ARS (e.g., **8N**; in **Section 5.5**) can be further analyzed to direct the call to a specific Line Group ID. Per the example screen above, if the user dialed 8 plus any number, the processing for the short code **8N**; would direct the call via ARS to Line Group 17. A short code **911** can be configured to send the emergency call out using Line Group 1 when the user dials “911”. If the primary route cannot be used, the call can automatically route to the route name specified in the **Alternate Route** field in the lower right of the screen (**51: Backup**). Since alternate routing is considered a privilege not available to all callers, IP Office can control access to the alternate route by comparing the calling user’s priority, configured in the **User** tab of individual users, to the value in the **Alternate Route Priority Level** field.

## 5.9. Mobility

With Mobility configured for an Avaya IP Office user, an inbound call routed to this user automatically triggers an outbound call to the configured Mobile Twinning number for this user.

The following screen shows the **Mobility** tab for User “Tony 9611” at extension 256. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number for the twinned mobile telephone including the dial access code (short code), in this case **919088485526** (short code 9 plus the ensuing twinned mobile number). The **Mobile Call Control** option box is also checked so that an inbound call from the twinned mobile number (9088485526 in this example) to the Mobile Call Control application (see Incoming Call Route to “FNE31” in **Section 5.7**) will be delivered directly to an internal dial tone from the Avaya IP Office, allowing the caller to perform further dialing actions including making calls and activating Short Codes. Other options can be set according to customer requirements.

The screenshot displays the configuration page for user 'Tony 9611: 256\*'. The left sidebar shows a tree view of IP Offices, with 'User (18)' expanded to show '256 Tony 9611'. The main panel has tabs for Telephony, Forwarding, Dial In, Voice Recording, Button Programming, Menu Programming, Mobility, and Group Membership. The Mobility tab is selected, showing the following settings:

- Internal Twinning
  - Twinned Handset: <None>
  - Maximum Number of Calls: 1
  - Twin Bridge Appearances
  - Twin Coverage Appearances
  - Twin Line Appearances
- Mobility Features
- Mobile Twinning
  - Twinned Mobile Number (including dial access code): 919088485526
  - Twinning Time Profile: <None>
  - Mobile Dial Delay (secs): 2
  - Mobile Answer Guard (secs): 0
  - Hunt group calls eligible for mobile twinning
  - Forwarded calls eligible for mobile twinning
  - Twin When Logged Out
- one-X Mobile Client
- Mobile Call Control
- Mobile Callback

Note that when an inbound call is from the twinned mobile number to the Mobile Call Control application, the caller ID contained in the From header of the incoming INVITE must match the

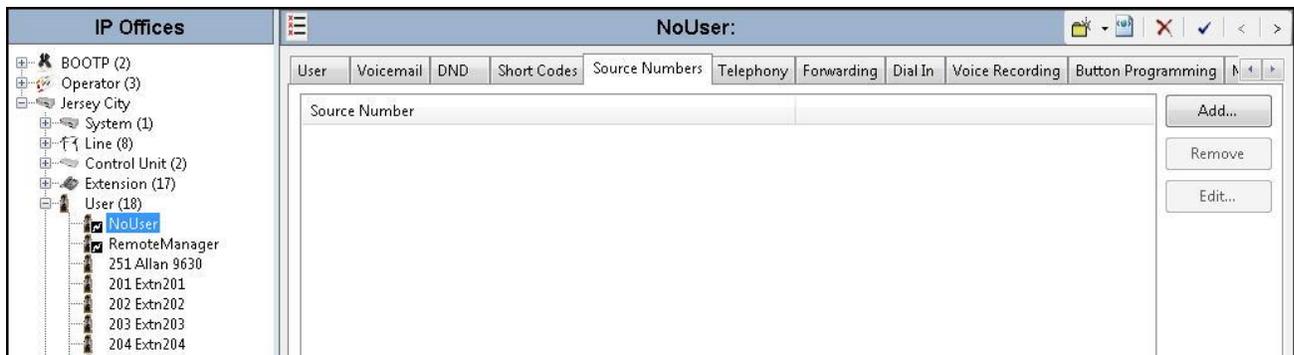
twinned mobile number (without the leading short code digit and the PSTN access code 1 for the North American Numbering Plan), otherwise the Avaya IP Office responds with a “486 Busy Here” message and the caller will hear busy tones.

## 5.10. SIP Options

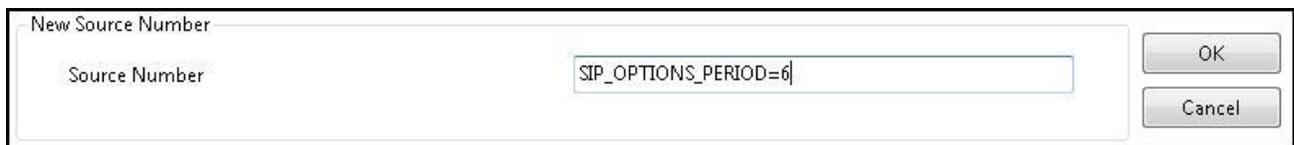
Avaya IP Office sends SIP OPTIONS messages periodically to determine if the SIP connection is active. By default, Avaya IP Office Release 9.1 sends out OPTIONS every 300 seconds. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time** (in seconds) set on the **Network Topology** tab in **Section 5.2.1** and the **SIP\_OPTIONS\_PERIOD** parameter (in minutes) that can be set on the **Source Number** tab of the **noUser** user. The OPTIONS period is determined in the following manner:

- To use the default value, set **Binding Refresh Time** to 300. OPTIONS will be sent at the 300 second frequency.
- To establish a period of less than 300 seconds, do not define the **SIP\_OPTIONS\_PERIOD** parameter and set the **Binding Refresh Time** to a value less than 300 seconds. The OPTIONS message period will be equal to the **Binding Refresh Time** setting.
- To establish a period greater than 300 seconds, a **SIP\_OPTIONS\_PERIOD** parameter must be defined. The **Binding Refresh Time** must be set to a value greater than 300 seconds. The OPTIONS message period will be the smaller of the **Binding Refresh Time** and the **SIP\_OPTIONS\_PERIOD** settings.

To configure the **SIP\_OPTIONS\_PERIOD** parameter, navigate to **User → NoUser** in the Navigation Pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.



At the bottom of the Details Pane, the **Source Number** field will appear. Enter **SIP\_OPTIONS\_PERIOD=X**, where **X** is the desired value in minutes. Click **OK**.



The **SIP\_OPTIONS\_PERIOD** parameter will appear in the list of Source Numbers as shown below. Click **OK** at the bottom of the screen (not shown).

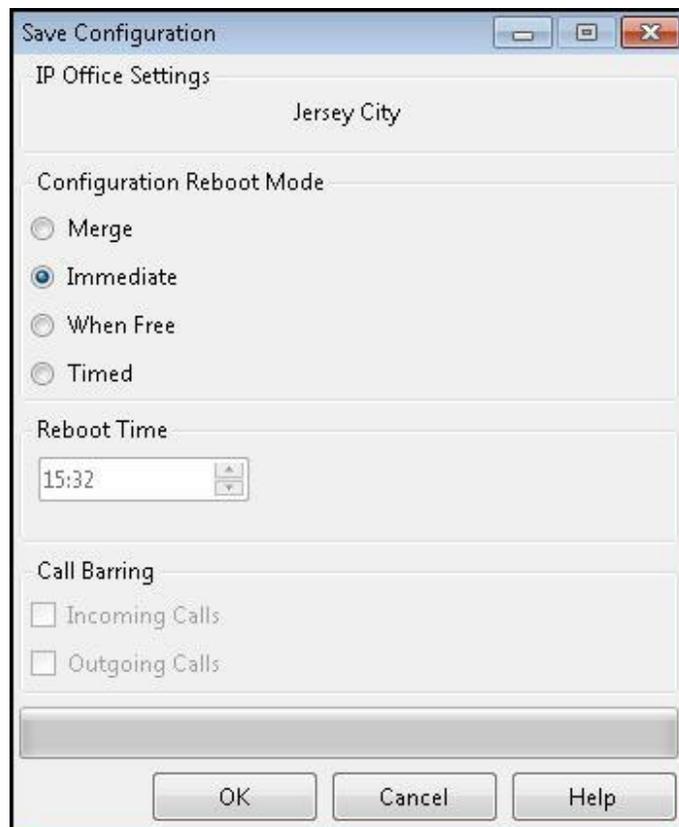


For the compliance test, an **OPTIONS** period of 2 minutes was desired. The **Binding Refresh Time** was set to **120** seconds in **Section 5.2.1**. Thus, there was no need to define **SIP\_OPTIONS\_PERIOD**.

## 5.11. Save Configuration

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

The following **Save Configuration** screen will appear, with either **Merge** or **Immediate** automatically selected, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a system reboot or a service disruption. Click **OK** to proceed.



## 6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed, including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (i.e., A1 and B1). If the management interface has not been configured on a separate subnet, then contact your Avaya representative for guidance in correcting the configuration.

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

### 6.1. Access Management Interface

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



The screenshot shows the login page for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, the "Log In" section contains a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there are three paragraphs of legal disclaimer text and a copyright notice at the bottom: "© 2011 - 2013 Avaya Inc. All rights reserved."

After logging in, the Dashboard screen will appear as shown below. Verify that **License State** is **OK** as highlighted. The Avaya SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license if necessary.

All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

The screenshot displays the Avaya Session Border Controller for Enterprise dashboard. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand menu tree lists various administration options. The main content area is titled 'Dashboard' and contains several panels: 'Information' (with 'License State' highlighted in red and showing 'OK'), 'Installed Devices' (listing 'EMS' and 'vnj-sbce2'), 'Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (None found), and 'Notes' (No notes found). An 'Add' button is visible in the bottom right of the dashboard area.

Information	
System Time	01:50:53 PM EDT <a href="#">Refresh</a>
Version	6.3.2-08-5478
Build Date	Thu Apr 2 06:51:39 EDT 2015
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0

Installed Devices
EMS
vnj-sbce2

Alarms (past 24 hours): None found.

Incidents (past 24 hours): None found.

Notes: No notes found.

## 6.2. Verify Network Configuration and Enable Interfaces

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

**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

**System Management**

Devices Updates SSL VPN Licensing

Device Name	Management IP	Version	Status				
vnj-sbce2	10.32.101.20	6.3.2-08-5478	Commissioned	Reboot	Shutdown	Restart Application	<b>View</b> Edit Uninstall

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

**System Information: vnj-sbce2**

**General Configuration**

Appliance Name **vnj-sbce2**  
Box Type SIP  
Deployment Mode Proxy

**Device Configuration**

HA Mode No  
Two Bypass Mode No

**License Allocation**

Standard Sessions 0  
Requested: 0  
Advanced Sessions 0  
Requested: 0  
Scopia Video Sessions 0  
Requested: 0  
Encryption

**Network Configuration**

IP	Public IP	Netmask	Gateway	Interface
192.168.96.233	192.168.96.233	255.255.255.224	192.168.96.254	B1
10.32.128.20	10.32.128.20	255.255.255.0	10.32.128.254	A1
192.168.96.234	192.168.96.234	255.255.255.224	192.168.96.254	B1
192.168.96.235	192.168.96.235	255.255.255.224	192.168.96.254	A1

**DNS Configuration**

Primary DNS 10.32.128.200  
Secondary DNS  
DNS Location DMZ  
DNS Client IP 10.32.128.20

**Management IP(s)**

IP 10.32.101.20

To enable the interfaces, first navigate to **Device Specific Settings** → **Network Management** in the left pane and select the device being managed in the center pane. In the right pane, in the **Interfaces** tab verify that **Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click on **Disabled** and confirm in the pop-up confirmation window to toggle to **Enabled**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the AVAYA logo. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. Under "Device Specific Settings", "Network Management" is highlighted with a red box. The main content area is titled "Network Management: vnj-sbce2" and features two tabs: "Devices" and "Interfaces". The "Interfaces" tab is active, showing a table with the following data:

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled

An "Add VLAN" button is located in the top right corner of the interface table.

### 6.3. Signaling Interface

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

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

For the compliance test, signaling interface **Int\_Sig\_Intf** was created for the Avaya SBCE internal interface and signaling interface **Ext\_Sig\_Intf** was created for the Avaya SBCE external interface. These two signaling interfaces are highlighted below.

When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Signaling IP** to the IP address associated with the private interface (A1) shown in **Section 6.2**. For the external interface, set the **Signaling IP** to the IP address associated with the public interface (B1) shown in **Section 6.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port the Avaya SBCE will listen on for each transport protocol. For the internal interface, the Avaya SBCE was configured to listen for UDP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port 5060. Since the Fusion Connect SIP Trunking Services uses UDP, it would have been sufficient to simply configure the Avaya SBCE for UDP.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main content area is titled "Signaling Interface: vnj-sbce2". Below this, there is a "Signaling Interface" section with a warning message: "Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#)." Below the warning is an "Add" button and a table of signaling interfaces.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Int_Sig_Intf	10.32.128.20	--	5060	--	None	Edit	Delete
Ext_Sig_Intf	192.168.96.233	5060	5060	--	None	Edit	Delete
Int_Sig_Intf_2	10.32.128.20	--	5060	--	None	Edit	Delete
Ext_Sig_Intf_2	192.168.96.233	--	5060	--	None	Edit	Delete

## 6.4. Media Interface

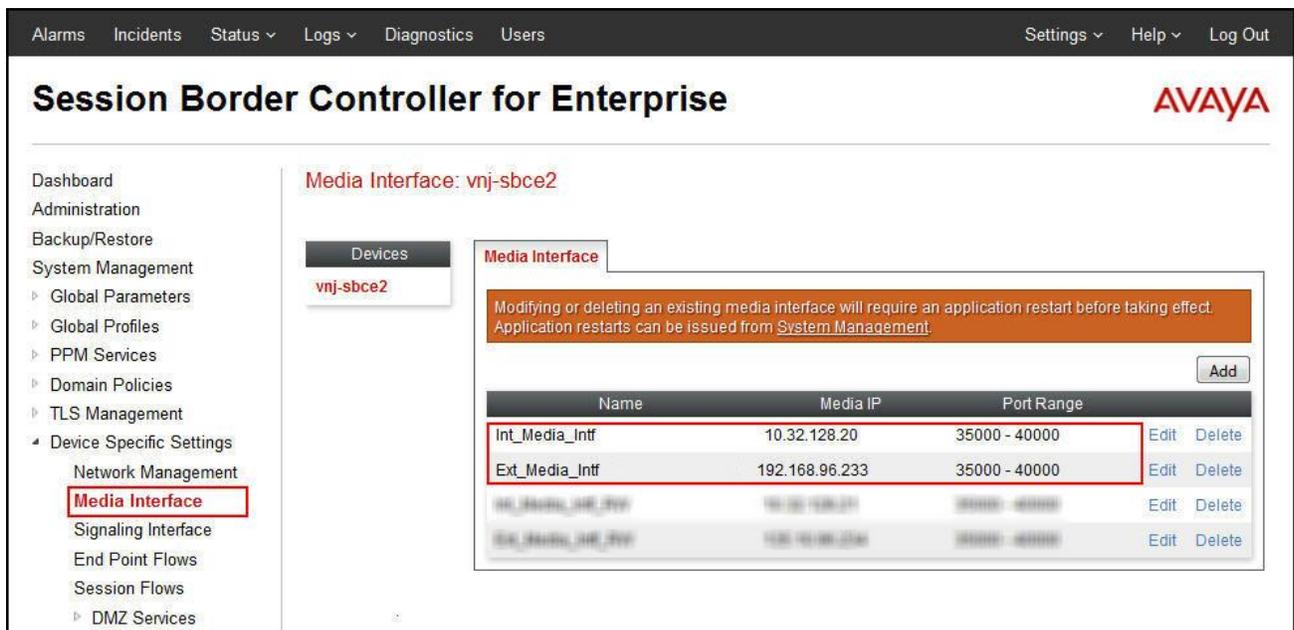
A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

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

For the compliance test, media interface **Int\_Media\_Intf** was created for the Avaya SBCE internal interface and media interface **Ext\_Media\_Intf** was created for the Avaya SBCE external interface. Both are highlighted below.

When configuring the interfaces, configure the parameters as follows:

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



The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the AVAYA logo. The left sidebar contains a navigation menu with categories like Dashboard, Administration, System Management, and Device Specific Settings. The "Media Interface" option under "Device Specific Settings" is highlighted with a red box. The main content area shows the configuration for device "vnj-sbce2". A warning message states: "Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below this is a table of media interfaces:

Name	Media IP	Port Range	Edit	Delete
Int_Media_Intf	10.32.128.20	35000 - 40000	Edit	Delete
Ext_Media_Intf	192.168.96.233	35000 - 40000	Edit	Delete
Int_Media_Intf	10.32.128.21	35000 - 40000	Edit	Delete
Ext_Media_Intf	192.168.96.234	35000 - 40000	Edit	Delete

## 6.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create one server interworking profile for Avaya IP Office and another for the service provider SIP server. These profiles will be applied to the appropriate servers in **Section 6.6.1** and **6.6.2**.

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and Server Interworking. The main content area is titled "Interworking Profiles: cs2100" and features an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead." Below this, there are tabs for "General", "Timers", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is active, showing a table of settings:

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No

### 6.5.1. Server Interworking – Avaya IP Office

For the compliance test, the server interworking profile *IPOffice-T.38* was created for Avaya IP Office. The **General** tab parameters are shown below. Note the setting for **T.38 Support**.

The screenshot shows the configuration page for the 'IPOffice-T38' interworking profile. The left sidebar lists various profiles, with 'IPOffice-T38' selected. The main area has tabs for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, displaying a table of parameters. The 'T.38 Support' parameter is highlighted with a red box and set to 'Yes'. Other parameters include 'Hold Support' (NONE), '180 Handling' (None), '181 Handling' (None), '182 Handling' (None), '183 Handling' (None), 'Refer Handling' (No), 'URI Group' (None), 'Send Hold' (No), '3xx Handling' (No), 'Diversion Header Support' (No), 'Delayed SDP Handling' (No), 'Re-Invite Handling' (No), 'URI Scheme' (SIP), and 'Via Header Format' (RFC3261). Below the 'General' tab are sections for 'Privacy' and 'DTMF', with 'DTMF Support' set to 'None'. Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

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
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
<b>T.38 Support</b>	<b>Yes</b>
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

The **Timers**, **URI Manipulation** and **Header Manipulation** tabs have no configured entries.

The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to **Yes**.

General	Timers	URI Manipulation	Header Manipulation	Advanced	
Record Routes			Both		
Topology Hiding: Change Call-ID			No		
Call-Info NAT			No		
Change Max Forwards			Yes		
Include End Point IP for Context Lookup			Yes		
OCS Extensions			No		
AVAYA Extensions			Yes		
NORTEL Extensions			No		
Diversion Manipulation			No		
Metaswitch Extensions			No		
Reset on Talk Spurt			No		
Reset SRTP Context on Session Refresh			No		
Has Remote SBC			Yes		
Route Response on Via Port			No		
Cisco Extensions			No		
Lync Extensions			No		

## 6.5.2. Server Interworking – Fusion Connect

For the compliance test, server interworking profile *SP-General-T38* was created for the Fusion Connect SIP server. The **General** tab parameters are shown below. Note the setting for **T.38 Support**.

Interworking Profiles: SP-General-T38

Buttons: Add, Rename, Clone, Delete

Interworking Profiles List:

- cs2100
- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- OCS-FrontEnd-S...
- IPOffice
- IPOffice-T38
- SP-General
- SP-General-T38**
- ...

Click here to add a description.

General | Timers | URI Manipulation | Header Manipulation | Advanced

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
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
<b>T.38 Support</b>	<b>Yes</b>
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

Edit

The **Timers**, **URI Manipulation**, **Header Manipulation** tabs have no entries.

The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to *No*.

General	Timers	URI Manipulation	Header Manipulation	Advanced	
Record Routes			Both		
Topology Hiding: Change Call-ID			No		
Call-Info NAT			No		
Change Max Forwards			Yes		
Include End Point IP for Context Lookup			No		
OCS Extensions			No		
AVAYA Extensions			No		
NORTEL Extensions			No		
Diversion Manipulation			No		
Metaswitch Extensions			No		
Reset on Talk Spurt			No		
Reset SRTP Context on Session Refresh			No		
Has Remote SBC			Yes		
Route Response on Via Port			No		
Cisco Extensions			No		
Lync Extensions			No		

## 6.6. Server Configuration

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

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

The screen below shows the GUI elements described above before the servers profiles were added for the compliance test.



### 6.6.1. Server Configuration – Avaya IP Office

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

- Set **Server Type** to *Call Server*.
- Set **IP Addresses / FQDNs** to the IP address of the Avaya IP Office LAN1 port.
- Set **Transport** to *UDP*, the transport protocol used for SIP signaling between Avaya IP Office and the Avaya SBCE.
- Set **Port** to the port Avaya IP Office will listen on for SIP requests from the Avaya SBCE.

Note that TCP was also set in the screen below, though UDP connectivity would have been sufficient.

Server Configuration: IPO-JCity

Buttons: Add, Rename, Clone, Delete

Server Profiles: IPO-JCity (selected)

General | Authentication | Heartbeat | Advanced

Server Type: Call Server

IP Address / FQDN	Port	Transport
10.32.128.30	5060	UDP
10.32.128.30	5060	TCP

Edit

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Avaya IP Office defined in **Section 6.5.1**.

General | Authentication | Heartbeat | **Advanced**

Enable DoS Protection

Enable Grooming

Interworking Profile: IPOffice-T38

Signaling Manipulation Script: None

Connection Type: SUBID

Edit

## 6.6.2. Server Configuration – Fusion Connect

For the compliance test, server configuration profile Fusion Connect was created for Fusion Connect. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to *Trunk Server*.
- Set **IP Addresses / FQDN** to the IP address of the Fusion Connect network access interface.
- Select the appropriate **Transport** protocol used for SIP signaling between Fusion Connect and the Avaya SBCE. In the compliance test, **UDP** was tested.
- Set **Port** to the standard SIP port of **5060**. This is the port the Fusion Connect SIP server will listen on for SIP messages from the Avaya SBCE.

The screenshot shows the 'Server Configuration: FusionConnect' interface. On the left is a sidebar with a list of server profiles: IPO-JCity, IPO-JCity, FusionConnect (highlighted), and others. The main area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active and contains the following configuration:

Server Type	Trunk Server	
IP Address / FQDN	Port	Transport
192.168.41.71	5060	UDP

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

On the **Advanced** tab, select the **Interworking Profile** for Fusion Connect defined in **Section 6.5.2**.

The screenshot shows the 'Advanced' tab configuration. The 'Interworking Profile' field is highlighted with a red box and set to 'SP-General-T38'. Other fields include 'Enable DoS Protection', 'Enable Grooming', 'Signaling Manipulation Script', and 'Connection Type'.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General-T38
Signaling Manipulation Script	None
Connection Type	SUBID

An 'Edit' button is located at the bottom.

## 6.7. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 6.10**. For the compliance test, the predefined **default-trunk** application rule (shown below) was used for both Avaya IP Office and the Fusion Connect SIP server.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation pane shows a tree structure with 'Domain Policies' expanded to 'Application Rules'. The main content area is titled 'Application Rules: default-trunk' and includes an 'Add' button, a 'Filter By Device...' dropdown, and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this is a table for the 'Application Rule' configuration.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Below the table is a 'Miscellaneous' section with the following settings:

Setting	Value
CDR Support	None
RTCP Keep-Alive	No

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

## 6.8. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger end point policy group defined in **Section 6.10**. For the compliance test, the predefined **default-low-med** media rule (shown below) was used for both Avaya IP Office and the Fusion Connect SIP server.

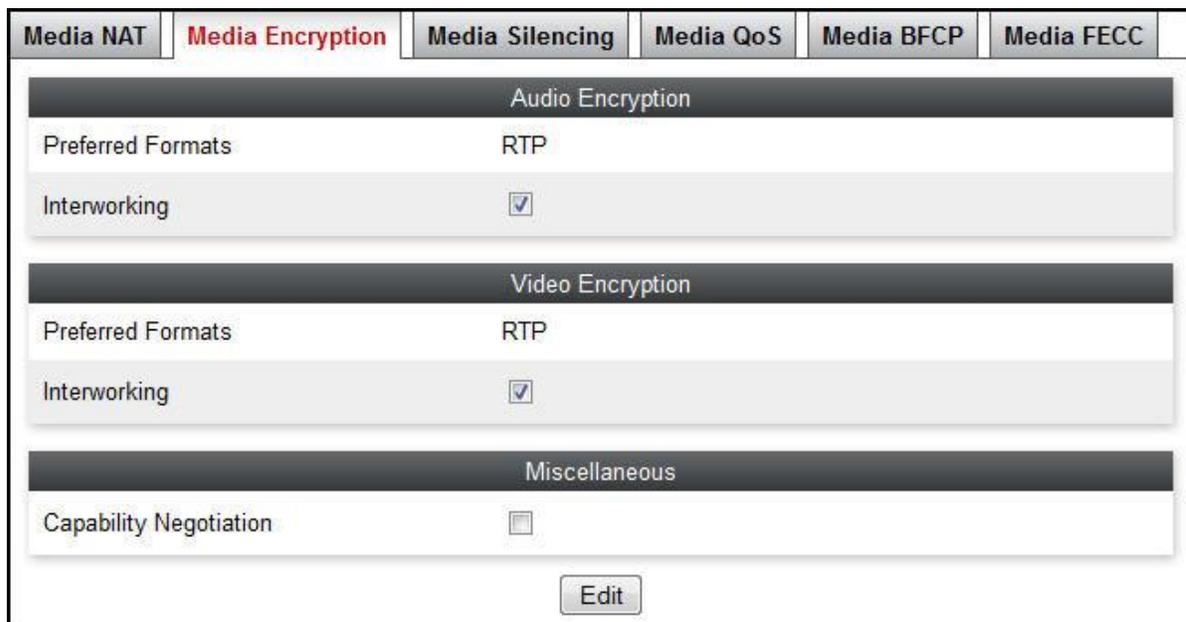
To view an existing rule, navigate to **Domain Policies** → **Media Rules** in the left pane. In the center pane, select the rule (e.g., **default-low-med**) to be viewed.



The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left navigation pane is expanded to 'Domain Policies' > 'Media Rules'. The main content area displays the configuration for the 'default-low-med' media rule. At the top, there are 'Add' and 'Clone' buttons, and a 'Filter By Device...' dropdown. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'Media NAT', 'Media Encryption', 'Media Silencing', 'Media QoS', 'Media BFCP', and 'Media FECC'. The 'Media NAT' tab is active, showing a 'Learn Media IP dynamically' checkbox and an 'Edit' button. The 'Media Rules' list on the left includes 'default-low-med...', 'default-high', 'default-high-enc', 'avaya-low-med-...', 'modified-dft-low...', and 'default\_sRTP...'.

Each of the tabs of the **default-low-med** media rule is shown below (the **Media NAT** tab is shown above).

The **Media Encryption** tab indicates that no encryption was used.



The screenshot shows the 'Media Encryption' configuration tab. It is divided into three sections: 'Audio Encryption', 'Video Encryption', and 'Miscellaneous'. Each section has 'Preferred Formats' and 'Interworking' options. The 'Interworking' checkboxes are checked. The 'Miscellaneous' section has a 'Capability Negotiation' checkbox which is unchecked. An 'Edit' button is located at the bottom of the configuration area.

Section	Option	Value
Audio Encryption	Preferred Formats	RTP
	Interworking	<input checked="" type="checkbox"/>
Video Encryption	Preferred Formats	RTP
	Interworking	<input checked="" type="checkbox"/>
Miscellaneous	Capability Negotiation	<input type="checkbox"/>

The **Media Silencing** tab shows **Media Silencing** was disabled.

Media NAT	Media Encryption	<b>Media Silencing</b>	Media QoS	Media BFCP	Media FECC
Media Silencing <input type="checkbox"/>					
<input type="button" value="Edit"/>					

The **Media QoS** settings are shown below.

Media NAT	Media Encryption	Media Silencing	<b>Media QoS</b>	Media BFCP	Media FECC
Media QoS Reporting					
RTCP Enabled <input type="checkbox"/>					
Media QoS Marking					
Enabled <input checked="" type="checkbox"/>					
QoS Type DSCP					
Audio QoS					
Audio DSCP EF					
Video QoS					
Video DSCP EF					
<input type="button" value="Edit"/>					

The **Media BFCP** tab is shown below.

Media NAT	Media Encryption	Media Silencing	Media QoS	<b>Media BFCP</b>	Media FECC
Binary Floor Control Protocol					
BFCP Enabled <input type="checkbox"/>					
<input type="button" value="Edit"/>					

The **Media FECC** tab is shown below.

Media NAT	<b>Media Encryption</b>	Media Silencing	Media QoS	Media BFCP	<b>Media FECC</b>
Far End Camera Control					
FECC Enabled <input type="checkbox"/>					
<input type="button" value="Edit"/>					

## 6.9. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger end point policy group defined in **Section 6.10**. For the compliance test, the predefined **default** signaling rule (shown below) was used for both Avaya IP Office and the Fusion Connect SIP server.

To view an existing rule, navigate to **Domain Policies** → **Signaling Rules** in the left pane. In the center pane, select the rule (e.g., **default**) to be viewed. The **General** tab settings of the default signaling rule are shown below.

**Session Border Controller for Enterprise** AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
‣ Global Parameters  
‣ Global Profiles  
‣ PPM Services  
‣ Domain Policies  
  Application Rules  
  Border Rules  
  Media Rules  
  Security Rules  
  **Signaling Rules**  
  Time of Day Rules  
  End Point Policy Groups  
  Session Policies  
‣ TLS Management  
‣ Device Specific Settings

**Signaling Rules: default**

Add Filter By Device... Clone

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

General Requests Responses Request Headers Response Headers Signaling QoS UCID

**Inbound**

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

**Outbound**

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

**Content-Type Policy**

Enable Content-Type Checks

Action	Allow	Multipart Action	Allow
Exception List	Exception List		

Edit

The **Requests**, **Responses**, **Request Headers**, **Response Headers** and **UCID** tabs have no entries. The **Signaling QoS** tab is shown below.

General Requests Responses Request Headers Response Headers **Signaling QoS** UCID

Signaling QoS

QoS Type DSCP

DSCP AF41

Edit

## 6.10. End Point Policy Groups

An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the service provider SIP server. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 6.13**.

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

The screen below shows the GUI elements described above before specific endpoint policy groups were added for the compliance test.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Domain Policies. Under Domain Policies, 'End Point Policy Groups' is highlighted. The main content area is titled 'Policy Groups: default-low' and includes an 'Add' button and a 'Filter By Device...' dropdown. A warning message states: 'It is not recommended to edit the defaults. Try adding a new group instead.' Below this is a table with columns for Order, Application, Border, Media, Security, Signaling, and Time of Day. A single row is visible with the following values: Order: 1, Application: default, Border: default, Media: default-low-med, Security: default-low, Signaling: default, Time of Day: default. Action buttons 'Edit' and 'Clone' are present for this row. A 'Policy Group' pop-up window is partially visible, showing 'Summary' and 'Add' buttons.

### 6.10.1. End Point Policy Group – Avaya IP Office

For the compliance test, the end point policy group *IPO-EP-Policy* was created for Avaya IP Office. Default values were used for each of the rules which comprise the group. The details of the default settings for **Application**, **Media** and **Signaling** are shown in **Section 6.7**, **Section 6.8** and **Section 6.9** respectively.

The screenshot shows the 'Policy Groups: IPO-EP-Policy' configuration interface. On the left is a sidebar with a list of policy groups, including 'IPO-EP-Policy' which is highlighted with a red box. The main area contains a table of policy rules. The table has columns for Order, Application, Border, Media, Security, and Signaling. One rule is visible with Order 1, Application 'default-trunk', Border 'default', Media 'default-low-med', Security 'default-low', and Signaling 'default'. There are also buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', 'Delete', and 'Summary'.

Order	Application	Border	Media	Security	Signaling
1	default-trunk	default	default-low-med	default-low	default

## 6.10.2. End Point Policy Group – Fusion Connect

For the compliance test, the end point policy group *SP-EP-Policy* was created for the Fusion Connect SIP server. Same default values were used for each of the rules which comprise the group. Thus, the *SP-EP-Policy* is identical to the *IPO-EP-Policy* created in **Section 6.10.1**.

The screenshot shows the configuration interface for the 'SP-EP-Policy' group. On the left is a sidebar with a list of policy groups, where 'SP-EP-Policy' is highlighted with a red border. The main area contains a 'Filter By Device...' dropdown, 'Add', 'Rename', 'Clone', and 'Delete' buttons, and two blue instruction bars. Below these is a 'Policy Group' section with a 'Summary' button and a table of rules.

Order	Application	Border	Media	Security	Signaling	
1	default-trunk	default	default-low-med	default-low	default	Edit

## 6.11. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 6.13**. Create one routing profile for Avaya IP Office and another for the service provider SIP server.

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

The screen below shows the GUI elements described above before specific routing profiles were added for the compliance test.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation pane includes the following menu items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, **Routing** (highlighted), and Server Configuration. The main content area is titled "Routing Profiles: default" and features an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead." Below this, a "Routing Profile" table is shown with an "Add" button. The table has the following structure:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	---	---	<a href="#">View</a> <a href="#">Edit</a>

### 6.11.1. Routing – Avaya IP Office

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

- Set **URI Group** to the wild card \* to match on any URI.
- Select **Priority** for **Load Balancing**.
- Enable **Next Hop Priority**.
- When adding an entry for routing destination (Next Hop Address)
  - Enter **1** for **Priority/Weight**.
  - For **Server Configuration**, select the Server for Avaya IP Office as configured in **Section 6.6.1**.
  - Set **Next Hop Address** to the IP address of Avaya IP Office LAN1 port.
  - Select **UDP** for **Transport** (the transport will be displayed in the Next Hop Address field once the entry is added).

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	IPO-JCity	10.32.128.30:5060 (UDP)	None

The following screen shows the routing profile for Avaya IP Office when configured.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	10.32.128.30	UDP

## 6.11.2. Routing – Fusion Connect

For the compliance test, routing profile *To-FusionConnect* was created for routing calls to Fusion Connect. When creating the profile, configure the parameters as follows:

- Set **URI Group** to the wild card \* to match on any URI.
- Select **Priority** for **Load Balancing**.
- Enable **Next Hop Priority**.
- When adding an entry for routing destination (Next Hop Address)
  - Enter a sequential number starting with **1** for **Priority/Weight**.
  - For **Server Configuration**, select the Server for Fusion Connect as configured in **Section 6.6.2**.
  - Set **Next Hop Address** to the IP address of the Fusion Connect SIP server as configured in **Section 6.6.2**.
  - Select **UDP** for **Transport** (the transport will be displayed in the Next Hop Address field once the entry is added).

Profile : To-FusionConnect - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	FusionConnect	192.168.41.71:5060 (UDP)	None	Delete

Finish

The following screen shows the routing profile for Fusion Connect when configured.

**Routing Profiles: To-FusionConnect**

Buttons: Add, Rename, Clone, Delete

Click here to add a description.

**Routing Profile**

Buttons: Update Priority, Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	192.168.41.71	UDP	Edit Delete

## 6.12. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the end point flow in **Section 6.13**. For the compliance test, the predefined **default** topology hiding profile (shown below) was used for both Avaya IP Office and the Fusion Connect SIP servers.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the 'Global Profiles' section expanded to 'Topology Hiding'. The main content area is titled 'Topology Hiding Profiles: default' and includes an 'Add' button and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this is a table for the 'default' profile:

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

An 'Edit' button is located at the bottom of the table.

## 6.13. End Point Flows

End point flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source end point flow and the destination end point flow. In the case of the compliance test, the signaling endpoints are Avaya IP Office and the Fusion Connect SIP server.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with 'End Point Flows' highlighted. The main content area is titled 'End Point Flows: vnj-sbce2' and features a 'Devices' dropdown menu with 'vnj-sbce2' selected. The 'Server Flows' tab is active, showing a table of server configurations. The table has columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. There are three rows of configuration, each with an 'Update' button and 'View', 'Clone', 'Edit', and 'Delete' actions.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1							View Clone Edit Delete
1							View Clone Edit Delete
1							View Cl

### 6.13.1. End Point Flow – Avaya IP Office

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

- For **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Avaya IP Office server created in **Section 6.6.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to \*.
- Set **Received Interface** to the external signaling interface.
- Set **Signaling Interface** to the internal signaling interface.
- Set **Media Interface** to the internal media interface.
- Set **End Point Policy Group** to the endpoint policy group defined for Avaya IP Office in **Section 6.10.1**.
- Set **Routing Profile** to the routing profile defined in **Section 6.11.2** used to direct traffic to the Fusion Connect SIP server.
- Set **Topology Hiding Profile** to the topology hiding profile specified for Avaya IP Office in **Section 6.12**.

Parameter	Value
Flow Name	IPO-JCity
Server Configuration	IPO-JCity
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig_Intf
Signaling Interface	Int_Sig_Intf
Media Interface	Int_Media_Intf
End Point Policy Group	IPO-EP-Policy
Routing Profile	To-FusionConnect
Topology Hiding Profile	default
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

The screen below shows the saved **IPO-JCity** configuration as a Server Flow. Note the server name by the **Server Configuration** heading.

End Point Flows: vnj-sbce2

Devices

vnj-sbce2

Subscriber Flows
Server Flows

**Server Configuration: IPO-JCity**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile						
1	IPO-JCity	*	Ext_Sig_Intf	Int_Sig_Intf	IPO-EP-Policy	To-FusionConnect	View	Clone	Edit	Delete		
2	IPO-JCity_200	*	Ext_Sig_Intf_200	Int_Sig_Intf_200	IPO-EP-Policy_200	Default_200	View	Clone	Edit	Delete		

**Server Configuration: IPO-EP**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile						
1	IPO-EP	*	Ext_Sig_Intf	Int_Sig_Intf	IPO-EP-Policy	Default	View	Clone	Edit	Delete		

### 6.13.2. End Point Flow – Fusion Connect

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

- For **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Fusion Connect SIP server created in **Section 6.6.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to \*.
- Set **Received Interface** to the internal signaling interface.
- Set **Signaling Interface** to the external signaling interface.
- Set **Media Interface** to the external media interface.
- Set **End Point Policy Group** to the endpoint policy group defined for Fusion Connect in **Section 6.10.2**.
- Set **Routing Profile** to the routing profile defined in **Section 6.11.1** used to direct traffic to Avaya IP Office.
- Set **Topology Hiding Profile** to the topology hiding profile specified for Fusion Connect in **Section 6.12**.

Field	Value
Flow Name	FusionConnect
Server Configuration	FusionConnect
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_Intf
Signaling Interface	Ext_Sig_Intf
Media Interface	Ext_Media_Intf
End Point Policy Group	SP-EP-Policy
Routing Profile	To-IPO-JCity
Topology Hiding Profile	default
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

The screen below shows the saved Fusion Connect configuration as a Server Flow. Note the server name by the **Server Configuration** heading.

End Point Flows: vnj-sbce2

Devices

Subscriber Flows

Server Flows

Server Configuration: **IP-Office**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Office	*	HL_Sig_Intf	HL_Sig_Intf	SP-EP-Policy	To-IP-Office	View Clone Edit Delete

Server Configuration: **FusionConnect**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	FusionConnect	*	Int_Sig_Intf	Ext_Sig_Intf	SP-EP-Policy	To-IPO-JCity	View Clone Edit Delete

Server Configuration: **IP-Office**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IP-Office	*	HL_Sig_Intf	HL_Sig_Intf	SP-EP-Policy	To-Office	View Clone Edit Delete
2	IP-Office-Ext	*	HL_Sig_Intf_Ext	HL_Sig_Intf_Ext	SP-EP-Policy_Ext	Office_Ext	View Clone Edit Delete

## 7. Fusion Connect SIP Trunking Configuration

Clearly is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise site (i.e., the IP address of the public interface on the Avaya SBCE) and the codec preferred (G.711u or G.729a). Fusion Connect will provide the customer the necessary information to configure the Avaya IP Office and Avaya SBCE including:

- Access interface IP address of the Fusion Connect SIP Trunking Service.
- Transport and port for the Fusion Connect SIP connection to the Avaya SBCE at the enterprise.
- DID numbers to assign to users at the enterprise.

## 8. Verification Steps

This section provides verification steps that may be performed to verify the solution configuration.

### 8.1. Avaya IP Office System Status

Use the Avaya IP Office System Status application to check the SIP Line channels state and alarms:

- Launch the application from **Start → Programs → IP Office → System Status** on the Avaya IP Office Manager PC. Select the SIP Line under **Trunks** from the left pane. In the **Status** tab in the right pane, verify the **Current State** is *Idle* for channels not taken by active calls; the state should be *Connected* for the channels engaged in active calls with the PSTN.

The screenshot shows the Avaya IP Office System Status application. The left pane shows a tree view with 'Trunks (8)' expanded to 'Line:17'. The main pane shows the 'Status' tab for 'SIP Trunk Summary'.

**SIP Trunk Summary**

- Line Service State: In Service
- Peer Domain Name: 10.32.128.20
- Resolved Address: 10.32.128.20
- Line Number: 17
- Number of Administered Channels: 20
- Number of Channels in Use: 2
- Administered Compression: G711 Mu
- Enable Faststart: Off
- Silence Suppression: Off
- Media Stream: RTP
- Layer 4 Protocol: UDP
- SIP Trunk Channel Licenses: Unlimited
- SIP Trunk Channel Licenses in Use: 0 (0%)
- SIP Device Features: REFER (Incoming and Outgoing), UPDATE (Incoming and Outgoing)

Below the summary is a table showing channel states:

Channel Number	URI G...	C...	Current State	Time in State	Remote Address	Media Address	Codec	Connection Type	C. Other Party on Call	Direction of Call	Rou...	Rec...	Rec...	Tra...	Tra...
1	1	...	Connected	00:04:12	10.32.128.20	10.32.128.20	G711 Mu	RTP Relay	...	Extn 256, Tony 9611	Incoming				
2	0	...	Connected	00:03:54	10.32.128.20	10.32.128.20	G711 Mu	RTP Relay	...	Extn 258, Jim 1120E	Outgoing				
3			Idle	3 days...											
4			Idle	3 days...											
5			Idle	3 days...											
6			Idle	3 days...											
7			Idle	3 days...											
8			Idle	3 days...											
9			Idle	3 days...											
10			Idle	3 days...											
11			Idle	3 days...											
12			Idle	3 days...											
13			Idle	3 days...											
14			Idle	3 days...											
15			Idle	3 days...											
16			Idle	3 days...											
17			Idle	3 days...											
18			Idle	3 days...											
19			Idle	3 days...											
20			Idle	3 days...											

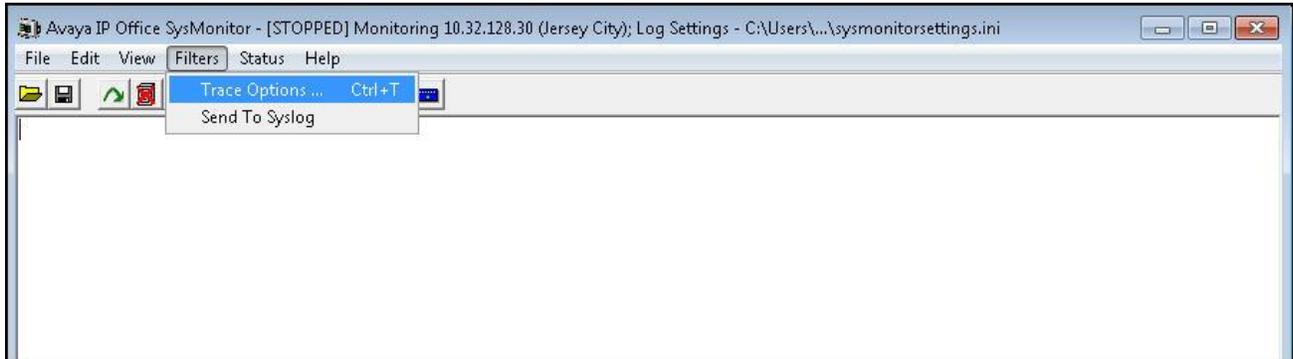
- Select the **Alarms** tab and verify that no alarms are active on the SIP Line.

The screenshot shows the 'Alarms' tab in the application. The title bar reads 'Alarms for Line: 17 SIP 10.32.128.20'. Below the title bar is a table with the following columns:

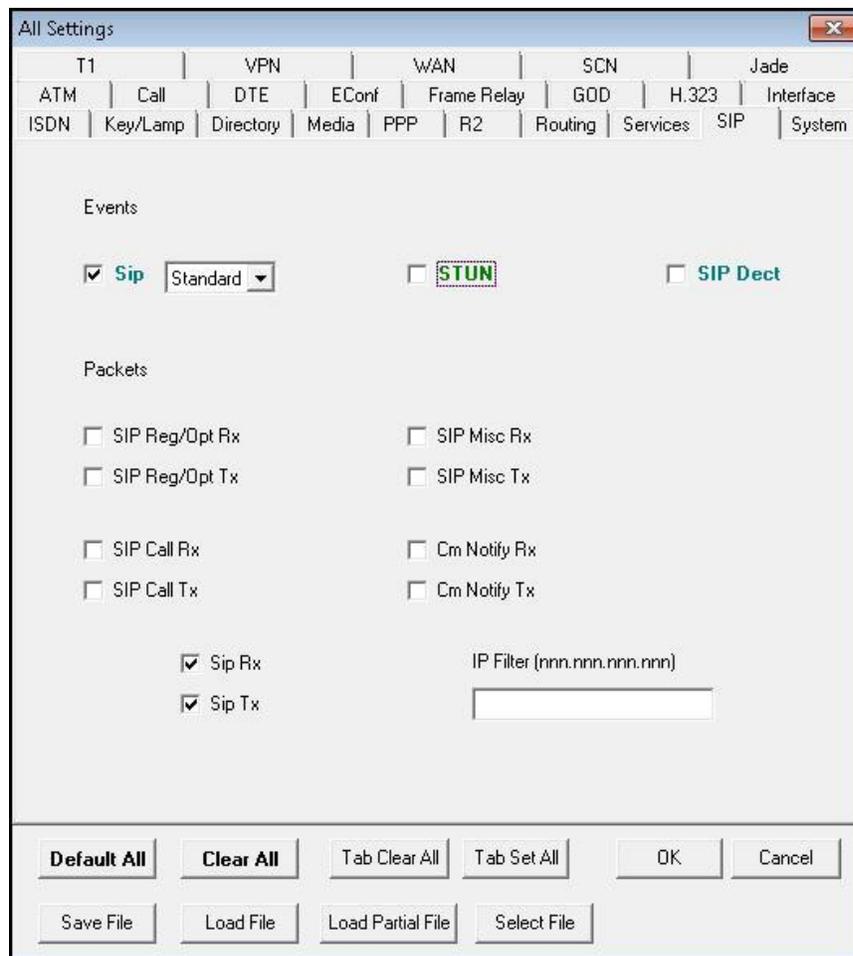
Last Date Of Error	Occurrences	Error Description

## 8.2. Avaya IP Office Monitor

The Monitor application can be used to monitor and troubleshoot Avaya IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor** on the Avaya IP Office Manager PC. The application allows monitored information to be customized. To customize, select **Filters → Trace Options...** as shown below:



The following screen shows the **SIP** tab of trace options. In this example, **Standard Sip Events** and the **Sip Rx** and **Sip Tx** boxes are checked.



### 8.3. Avaya SBCE Traces

The Avaya SBCE can take traces on specified interfaces. SIP signaling crossing both interfaces A1 and B1 can be captured for troubleshooting. In the Avaya SBCE web interface, navigate to **Device Specific Settings** → **Troubleshooting** → **Trace** to invoke this facility. In the **Packet Capture** tab, select or supply the relevant information (e.g., A1 or B1 or any interfaces, IP/port, protocol, number of packets to capture, capture file name, etc.), then press the **Start Capture** button to start the trace. After the trace capture has been stopped, the captured trace file can then be downloaded from the **Captures** tab for examination using a protocol sniffer application such as Wireshark.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top header shows the product name and the AVAYA logo. On the left is a navigation menu with categories like Dashboard, Administration, System Management, and Device Specific Settings. The 'Trace' option under Troubleshooting is highlighted with a red box. The main content area shows a 'Trace: vnj-sbce2' header and two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' form includes fields for Status (Ready), Interface (B1), Local Address (All : 5060), Remote Address (\*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (SBCEToFromFC.pcap). 'Start Capture' and 'Clear' buttons are at the bottom.

## 9. Conclusion

The Fusion Connect SIP Trunking Service passed compliance testing with Avaya IP Office R9.1 and Avaya Session Border Controller for Enterprise R6.3. These Application Notes describe the configuration necessary to connect Avaya IP Office R9.1 and Avaya SBCE R6.3 to Fusion Connect as shown in **Figure 1**. Test results and observations are noted in **Section 2.2**.

## 10. Additional References

- [1] *IP Office™ Platform 9.1, Deploying Avaya IP Office™ Platform IP500 V2*, Document Number 15-601042, Issue 30g, January 2015.
- [2] *Administering Avaya IP Office™ Platform with Manager*, Release 9.1, Issue 10.04, February 2015.
- [3] *IP Office™ Platform 9.1, Administering Avaya IP Office™ Platform Voicemail Pro*, Document Number 15-601063, Issue 10c, December 2014.
- [4] *IP Office™ Platform 9.1, Using IP Office System Monitor*, Document Number 15-601019, Issue 06b, November 2014.
- [5] *IP Office™ Platform 9.1, Using Avaya IP Office™ Platform System Status*, Document Number 15-601758, October 2014.
- [6] *Using Avaya Communicator on IP Office*, Release 9.1, December 2014.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.
- [9] *Application Notes for configuring Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.3 to support Remote Workers*, Issue 1.0, February 2015.
- [10] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>.
- [11] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>.

Product documentation for Avaya products may be found at <http://support.avaya.com> or [http://marketingtools.avaya.com/knowledgebase/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf\\_feed\\_template.html](http://marketingtools.avaya.com/knowledgebase/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf_feed_template.html).

Product documentation for Fusion Connect SIP Trunking Service is available from Fusion Connect.

---

**©2015 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).