



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring IntelPeer SIP Trunking Service with Avaya IP Office R9.0.1 and Avaya Session Border Controller for Enterprise 6.2.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between IntelPeer and an enterprise solution using Avaya IP Office Release 9.0.1 and Avaya Session Border Controller for Enterprise 6.2.1.

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

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

Table of Contents

1.	Introduction.....	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.....	7
4.	Equipment and Software Validated	9
5.	Configure Avaya IP Office	10
5.1.	Licensing and Physical Hardware	11
5.2.	System	13
5.2.1.	System - LAN1 Tab	13
5.2.2.	System - Voicemail Tab.....	17
5.2.3.	System - Telephony Tab	18
5.2.4.	System - Twinning Tab.....	19
5.2.5.	System – Codecs Tab.....	19
5.3.	IP Route.....	20
5.4.	Administer SIP Line.....	21
5.4.1.	Create SIP Line from Template	21
5.4.2.	SIP Line – SIP Line Tab	24
5.4.3.	SIP Line – Transport Tab.....	25
5.4.4.	SIP Line – SIP Credentials Tab	26
5.4.5.	SIP Line – SIP URI Tab.....	27
5.4.6.	SIP Line – VoIP Tab.....	28
5.4.7.	SIP Line – T.38 Fax Tab.....	29
5.5.	Short Code.....	30
5.6.	User	32
5.7.	Incoming Call Route	33
5.8.	ARS and Alternate Routing.....	34
5.9.	SIP Options	35
5.10.	Privacy/Anonymous Calls	37
5.11.	Save Configuration	38
6.	Configure Avaya Session Border Controller for Enterprise	39
6.1.	Access the Management Interface.....	39
6.2.	Verify Network Configuration and Enable Interfaces	41
6.3.	Signaling Interface	43
6.4.	Media Interface	44
6.5.	Server Interworking.....	45
6.5.1.	Server Interworking – Avaya IP Office	46
6.5.2.	Server Interworking – IntelePeer	47
6.6.	Signaling Manipulation	48
6.7.	Server Configuration	49
6.7.1.	Server Configuration – Avaya IP Office	50
6.7.2.	Server Configuration – IntelePeer	51

6.8.	Application Rules.....	52
6.9.	Media Rules.....	53
6.10.	Signaling Rules.....	55
6.11.	Endpoint Policy Groups.....	57
6.11.1.	Endpoint Policy Group – Avaya IP Office.....	57
6.11.2.	Endpoint Policy Group – IntelPeer.....	58
6.12.	Routing.....	58
6.12.1.	Routing – Avaya IP Office.....	59
6.12.2.	Routing – IntelPeer.....	60
6.13.	Topology Hiding.....	61
6.14.	End Point Flows.....	62
6.14.1.	End Point Flow – Avaya IP Office.....	63
6.14.2.	End Point Flow – IntelPeer.....	64
7.	IntelPeer SIP Trunking Configuration.....	65
8.	Verification Steps.....	66
8.1.	Avaya IP Office System Status.....	66
8.2.	Avaya IP Office Monitor.....	68
8.3.	Avaya SBCE Protocol Trace.....	69
9.	Conclusion.....	69
10.	Additional References.....	70
11.	Appendix - Remote Worker Configuration via Avaya SBCE.....	71
11.1.	Provisioning Avaya SBCE for Remote Worker.....	72
11.1.1.	Network Management.....	72
11.1.2.	Signaling Interfaces.....	73
11.1.3.	Media Interfaces.....	74
11.1.4.	Server Profile for Avaya IP Office.....	75
11.1.5.	Routing Profiles.....	76
11.1.6.	User Agent.....	77
11.1.7.	Application Rules.....	78
11.1.8.	Media Rules.....	79
11.1.9.	End Point Policy Groups.....	81
11.1.10.	End Point Flows.....	82
11.2.	Remote Worker Endpoint Configuration on Avaya IP Office.....	86
11.2.1.	Extension and User Configuration.....	86
11.2.2.	Incoming Call Route.....	87
11.3.	Remote Worker Avaya Flare® Experience for Windows Configuration.....	88
11.3.1.	Settings - Server Screen.....	88
11.3.2.	Settings - Video Screen.....	89

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between IntelPeer and an enterprise solution using Avaya IP Office Release 9.0.1 and Avaya Session Border Controller for Enterprise 6.2.1.

The IntelPeer SIP Trunking Service referenced within these Application Notes is positioned for customers who have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

The IntelPeer SIP Trunking Service will enable delivery of origination and termination of local, long-distance, Toll-free, international, and other types of calls across a single broadband IP connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE).

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the IntelPeer SIP Trunking Service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site comprised of an Avaya IP Office 500 V2 running Release 9.0.1 software, Avaya Voicemail Pro messaging application, Avaya H.323 and SIP hard phones, and SIP-based Avaya softphones. The enterprise solution connects to the IntelPeer network via the Avaya Session Border Controller for Enterprise (Avaya SBCE).

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 interoperability compliance test:

- Sending/receiving SIP OPTIONS queries to/from the service provider.
- Incoming calls from the PSTN to H.323 and SIP telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing calls to the PSTN from H.323 and SIP telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Various call types including: local, long distance, outbound toll-free and international.
- G.711MU and G.729A codecs.
- Caller ID presentation and Caller ID restriction.
- DTMF transmission using RFC 2833.
- Voicemail access and navigation for inbound and outbound calls.
- Telephony supplementary features such as hold and resume, transfer, and conference.

- Off-net call forwarding and call transfer/conference.
- Twinning on inbound calls to PSTN mobile phones.
- Use of SIP INVITE message for call redirection to the PSTN.
- Inbound and outbound long-duration calls stability.
- Inbound and outbound long hold time call stability.
- Response to incomplete call attempts and trunk busy or error conditions.
- T.38 fax.
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

Items not supported or not tested include the following:

- Inbound toll-free and emergency calls (911) were not tested as part of the compliance test.
- IntelPeer SIP Trunking does not support use of the SIP REFER method for network redirection (transferring calls with the PSTN back to the PSTN).
- IntelPeer SIP Trunking does not support Operator call (0), Operator-Assisted (0 + 10-digit), and Directory Assistance (411) calls.

2.2. Test Results

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

- **"200 OK" Contact Header** – For outbound calls, the Contact header in the "200 OK" message from IntelPeer to signal call connect contained the caller number instead of the number for the actual connected party (i.e., the callee number). As a consequence, if the call was terminated by the IP Office caller, the BYE message to IntelPeer would contain the caller DID number in its Request URI instead of the PSTN callee number. The call would terminate properly though the signaling was not clean as described. The same problem existed with the "200 OK" response from IntelPeer to the session-refresh re-INVITE messages from IP Office, with no negative impact observed. IntelPeer has been investigating this issue.
- **Codec Lockdown** – For outbound calls with multiple codes offered in the SDP of outbound INVITE, the call connect "200 OK" from IntelPeer contained the same set of codecs in the SDP instead of just the preferred coded (first in the list).
- **Session Refresh** – IntelPeer issued session refresh SIP re-INVITE messages towards the IP Office at 3-minute intervals for both inbound and outbound calls, but SIP messages from IntelPeer contained no information relating to session refresh handshake (e.g., Session-Expires, Min-SE headers).
- **RFC2833 Payload Type** – IntelPeer configured SIP Trunking to match to only one specific RFC2833 payload type. Payload type 101 was used for the compliance test. This static payload type configuration worked well for most of the Avaya IP Office endpoints. However, the Avaya Flare® Experience for Windows softphone used payload type 120 which IntelPeer was not able to match, resulting in failure of out-band DTMF tone transmission from this specific endpoint. IntelPeer was investigating a SIP Trunking

configuration capable of dynamically matching to different RFC2833 payload types from the enterprise site.

- **Outbound T.38 Fax Interworking with G.729A Codec** – IntelPeer did not initiate re-INVITE to switch to T.38. IP Office would time out eventually, failing the outbound fax when the voice codec was G.729A. Outbound T.38 fax interworking with the G.711MU codec worked successfully. Since IntelPeer recommends configuring G.711MU as the preferred codec, this would not be a problem in deployed customer environments.
- **Direct Media** – Starting with R9.0, Avaya IP Office offers a new Direct Media capability on IP Office 500 V2 that 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 resources. Though Direct Media was tested and verified for straight inbound / outbound calls during testing, the following issues were experienced when the Direct Media option was enabled:
 - When Direct Media was enabled, Avaya IP Office IP endpoints did not send RTP Events.
 - Only Direct Media *or* T.38 fax is supported on a SIP Line. The use of both features on the same SIP Line is not supported.
 - As a result of these issues, the recommended configuration is to have Direct Media disabled (see **Section 5.4.6**).

2.3. Support

Contact information for technical support on the IntelPeer SIP Trunking service:

- Email: support@intelepeer.com
- Telephone: (877) 780-8639

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

3. Reference Configuration

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

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

The enterprise endpoints include both local extensions and Remote Worker phones that connect directly to the public Internet. The same Avaya SBCE was configured to connect to both the service provider network and Remote Worker using separate sets of public/private interfaces (**Figure 1** only shows the public/private interfaces used for connecting to the service provider network).

The Avaya IP Office 500 V2 at the enterprise site runs IP Office Release 9.0.1 software. Endpoints include various Avaya IP Telephones (with H.323 and SIP firmware) and SIP-based Avaya softphones (Avaya IP Office Softphone and Avaya Flare® Experience for Windows). The site also has a Windows PC running Avaya 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.

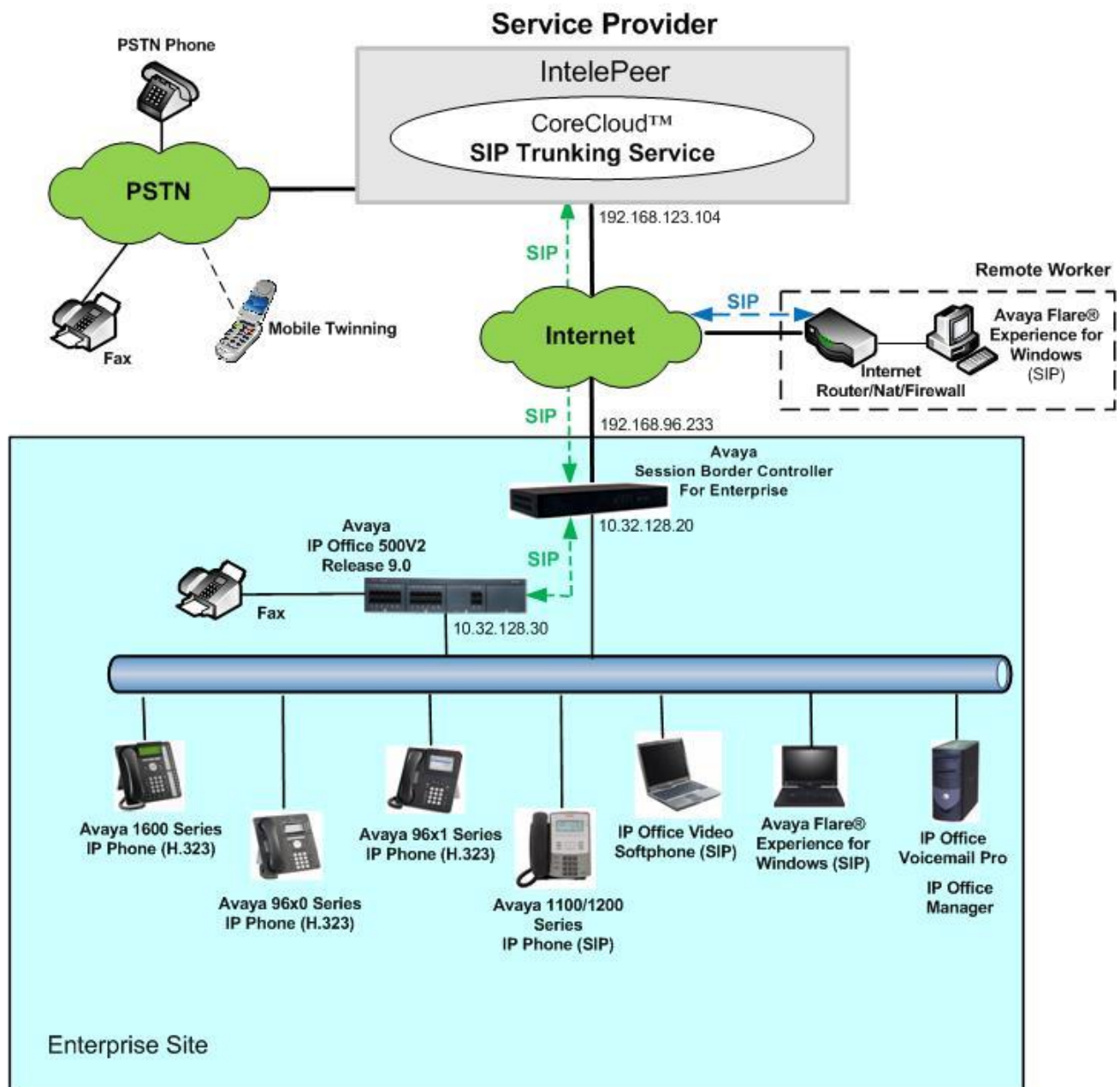


Figure 1: Test Configuration

For security purposes, any actual public IP addresses used in the compliance test were changed to 192.168.x.x throughout these Application Notes.

For the purposes of the compliance test, 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 IntelePeer. 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. IntelPeer also 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 Voicemail Pro messaging service and endpoints on Avaya IP Office are standard. Since these configuration tasks are not directly related to the inter-operation with the IntelPeer SIP Trunking Service, they are not included in these Application Notes. The configuration for Remote Worker via Avaya SBCE is contained in the Appendix to this document.

4. Equipment and Software Validated

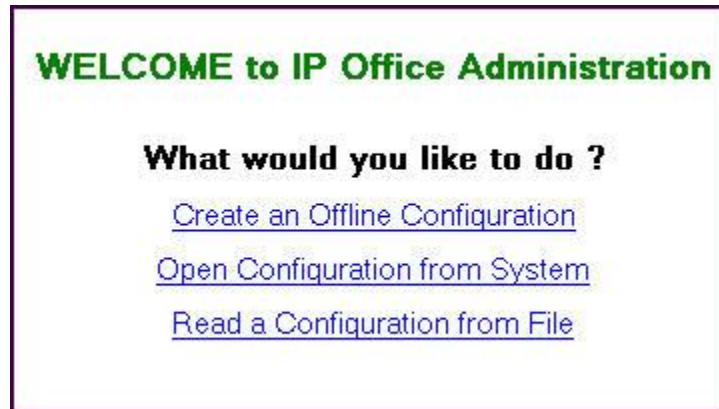
The following equipment and software/firmware were used for the sample configuration provided:

Avaya Telephony Components	
Equipment / Software	Release / Version
Avaya IP Office 500V2	9.0.100.845
Avaya IP Office COMBO6210/ATM4 Module	9.0.100.845
Avaya IP Office Manager	9.0.100.845
Avaya Preferred Edition (a.k.a Voicemail Pro)	9.0.1.0.53
Avaya Session Border Controller for Enterprise running on a Portwell CAD-0208 server	6.2.1.Q07
Avaya 1616 IP Telephones (H.323)	Avaya one-X Deskphone 1.3 SP4
Avaya 9611G IP Telephones (H.323)	Avaya one-X Deskphone 6.3.0.37_V452
Avaya 9630G IP Telephones (H.323)	Avaya one-X Deskphone 3.2.1.2A
Avaya 1120E IP Telephone (SIP)	4.03.18.00
Avaya 1140E IP Telephone (SIP)	4.03.18.00
Avaya IP Office Video Softphone (Windows)	3.2.3.49 68975
Avaya Flare® Experience for Windows	1.1.4.23
IntelPeer Components	
Equipment / Software	Release / Version
Taqua T7100 Multimedia Controller	3.0.0.29

Testing was performed with IP Office 500 V2 R9.0.1, but this testing also applies to IP Office Server Edition 9.0.1. Note that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or 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 → Programs → IP Office → Manager** to launch the application. A screen that includes the following in the center may be displayed:



Select **Open Configuration from System**. If the above screen does not appear, the configuration may be alternatively opened by navigating to **File → Open Configuration** at the top menu of the Avaya IP Office Manager window. Select the proper Avaya IP Office system from the pop-up window and log in with the appropriate credentials.

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 twinning and IP Office Softphone support) 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., **License → SIP Trunk Channels**) appears as submenus underneath the system name **Jersey City** in the Navigation Pane. The configuration screens only 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 to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

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

Avaya IP Office Manager Jersey City [9.0.100.845] [Administrator/Administrator]

File Edit View Tools Help

IP Offices

- BOOTP (2)
- Operator (3)
- Jersey City
 - System (1)
 - Line (6)
 - Control Unit (2)
 - Extension (17)
 - User (18)
 - Group (1)
 - Short Code (66)
 - Service (0)
 - RAS (1)
 - Incoming Call Route (21)
 - WanPort (0)
 - Directory (0)
 - Time Profile (0)
 - Firewall Profile (1)
 - IP Route (4)
 - Account Code (0)
 - License (64)**
 - Tunnel (0)
 - User Rights (8)
 - ARS (2)
 - RAS Location Request (0)
 - Location (0)

License Remote Server

License Mode: License Normal

PLDS Host ID: 111311587034

Feature	License Key	Instances	Status
Report Viewer		255	Valid
Mobility Features		255	Obsolete
IP500 Voice Networking Channels		255	Valid
IP500 Voice Networking Channels		4	Valid
VCM Channel Migration		255	Valid
SIP Trunk Channels		255	Valid
IP500 Universal PRI (Additional chan...		255	Valid
RAS LRQ Support (Rapid Response)		255	Valid
IP Office Dealer Support - Standard E...		255	Valid
IP Office Dealer Support - Profession...		255	Valid
IP Office Distributor Support - Standa...		255	Valid
IP Office Distributor Support - Profes...		255	Valid
UMS Web Services		255	Valid
CCR SUP		255	Valid
Customer Service Agent		255	Valid
CCR Designer		255	Valid
CCR CCC UPG		255	Valid
1600 Series Phones		255	Valid
Third Party API		255	Valid
one-X Portal for IP Office		255	Valid
Avaya IP endpoints		255	Valid
Customer Service Supervisor		255	Valid
Essential Edition Additional Voicemail ...		255	Valid
Teleworker		255	Valid
Mobile Worker		255	Valid
Power User		255	Valid
Advanced Edition		255	Valid

Add... Remove

OK Cancel Help

To view the physical hardware comprising the Avaya IP Office system, expand the components under the **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 screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, showing a tree structure with 'Jersey City' expanded, then 'System (1)', 'Line (6)', and 'Control Unit (2)'. Under 'Control Unit (2)', '1 IP 500 V2' is selected. The main pane on the right is titled 'IP 500 V2' and shows the following details:

Unit	
Device Number	1
Unit Type	IP 500 V2
Version	9.0.100.845
Serial Number	
Unit IP Address	10.32.128.30
Interconnect Number	0
Module Number	Control Unit

The screen below shows the details of the Combination Card:

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, showing a tree structure with 'Jersey City' expanded, then 'System (1)', 'Line (6)', and 'Control Unit (2)'. Under 'Control Unit (2)', '2 COMBO6210/ATM4' is selected. The main pane on the right is titled 'COMBO6210/ATM4' and shows the following details:

Unit	
Device Number	2
Unit Type	COMBO6210/ATM4
Version	9.0.100.845
Serial Number	
Unit IP Address	0.0.0.0
Interconnect Number	0
Module Number	Control Unit

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 Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows the hierarchy: BOOTP (2), Operator (3), Jersey City, System (1), and Jersey City. The 'Jersey City' system is selected. The main pane shows the 'LAN1' tab under 'LAN Settings'. The 'IP Address' field is set to 10.32.128.30 and the 'IP Mask' field is set to 255.255.255.0, both highlighted with a red box. Other fields include 'Primary Trans. IP Address' (0.0.0.0), 'RIP Mode' (None), 'Enable NAT' (unchecked), and 'Number Of DHCP IP Addresses' (200). The 'DHCP Mode' section shows 'Server', 'Client', 'Dialin', and 'Disabled' (selected) radio buttons. An 'Advanced' button is also present.

Field	Value
IP Address	10 . 32 . 128 . 30
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	0 . 0 . 0 . 0
RIP Mode	None
Enable NAT	<input type="checkbox"/>
Number Of DHCP IP Addresses	200
DHCP Mode	<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dialin <input checked="" type="radio"/> Disabled

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.
- The **RTP Port Number Range** can be customized to a specific range of receiving ports for the RTP media. 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 ports open for the duration of the call.

The screenshot shows the 'Jersey City' configuration window with the 'VoIP' tab selected for 'LAN1'. 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 shows 'UDP' and 'TCP' checked, with their respective ports (5060 and 5061) and remote ports (5060 and 5061) configured. The 'Challenge Expiry Time (secs)' is set to 10. The 'RTP' section is expanded, showing the 'Port Number Range' (Minimum: 49152, Maximum: 53246) and 'Port Number Range (NAT)' (Minimum: 49152, Maximum: 53246) both highlighted with red boxes. The 'Enable RTCP Monitoring on Port 5005' checkbox is checked. The 'Keepalives' section is expanded, showing 'Scope' set to 'RTP', 'Initial keepalives' set to 'Enabled', and 'Periodic timeout' set to 30, all highlighted with a red box.

Jersey City

System LAN1 LAN2 DNS Voicemail Telephony Directory Services System Events SMTP SMDR Twinning VCM CCR Codecs

LAN Settings VoIP Network Topology

☒ H323 Gatekeeper Enable
☐ Auto-create Extn ☐ Auto-create User ☐ H323 Remote Extn Enable

☒ SIP Trunks Enable

☒ SIP Registrar Enable
☐ Auto-create Extn/User ☐ SIP Remote Extn Enable

Domain Name avaya.com

Layer 4 Protocol
☒ UDP UDP Port 5060 Remote UDP Port 5060
☒ TCP TCP Port 5060 Remote TCP Port 5060
☐ TLS TLS Port 5061 Remote TLS Port 5061

Challenge Expiry Time (secs) 10

RTP

Port Number Range
Minimum 49152 Maximum 53246

Port Number Range (NAT)
Minimum 49152 Maximum 53246

☒ Enable RTCP Monitoring on Port 5005

Keepalives
Scope RTP Periodic timeout 30
Initial keepalives Enabled

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.

The screenshot displays the 'Jersey City' configuration window for an Avaya IP Office. The 'LAN1' tab is selected, and the 'VoIP' sub-tab is active. The 'DiffServ Settings' section is highlighted with a red rectangle. It contains the following fields:

Field	Value
DSCP (Hex)	B8
Video DSCP (Hex)	FC
DSCP Mask (Hex)	88
SIG DSCP (Hex)	88
DSCP	46
Video DSCP	46
DSCP Mask	63
SIG DSCP	34

Below the DiffServ Settings, the 'DHCP Settings' section is visible, containing fields for Primary Site Specific Option Number (SSON), Secondary Site Specific Option Number (SSON), VLAN, and 1100 Voice VLAN Site Specific Option Number (SSON).

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

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. The Avaya SBCE will perform network address translation of SIP traffic but it is not necessary for IP Office to have any knowledge of this translation. Thus, the parameter was set to **Open Internet**.
- 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 5.9** for complete details.
- Set **Public Port** to **5060** for **UDP**.

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

- STUN Server Address: [Empty text box]
- STUN Port: 3478 (spin box)
- Firewall/NAT Type: Open Internet (dropdown menu, highlighted with a red box)
- Binding Refresh Time (seconds): 60 (spin box)
- Public IP Address: 0 . 0 . 0 . 0 (text box)
- Run STUN button
- Cancel button

The 'Public Port' section contains the following fields:

- UDP: 5060 (spin box, highlighted with a red box)
- TCP: 0 (spin box)
- TLS: 0 (spin box)

At the bottom, there is a checkbox labeled 'Run STUN on startup' which is currently unchecked.

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 assigned to the enterprise from IntelPeer. 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.

Jersey City

System LAN1 LAN2 DNS **Voicemail** Telephony Directory Services System Events SMTP SMDR Twinning VCM CCR Codecs

Voicemail Type: Voicemail Lite/Pro ☐ Messages Button Goes To Visual Voice

Voicemail Destination: [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): [Dropdown]

Breakout (DTMF 2): [Dropdown]

Breakout (DTMF 3): [Dropdown]

SIP Settings

SIP Name: 7207291059

SIP Display Name (Alias): Voicemail

Contact: 7207291059

Anonymous: ☐

Call Recording

Auto Restart Paused Recording (secs): 15

Hide Auto Recording: ☐

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 across the SIP trunk 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 with the 'Telephony' tab selected. The 'Telephony' sub-tab is also selected. The 'Analogue Extensions' section includes fields for 'Default Outside Call Sequence' (Normal), 'Default Inside Call Sequence' (Ring Type 1), 'Default Ring Back Sequence' (Ring Type 2), and 'Restrict Analogue Extension Ringer Voltage' (unchecked). The 'Hold Timeout (secs)' is set to 0. The 'Companding Law' section shows 'U-Law' selected for both 'Switch' and 'Line'. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked. Other settings include 'Dial Delay Time (secs)' (4), 'Dial Delay Count' (0), 'Default No Answer Time (secs)' (15), 'Park Timeout (secs)' (300), 'Ring Delay (secs)' (5), 'Call Priority Promotion Time (secs)' (Disabled), 'Default Currency' (USD), 'Default Name Priority' (Favor Trunk), 'Media Connection Preservation' (Disabled), 'DSS Status' (unchecked), 'Auto Hold' (checked), 'Dial By Name' (checked), 'Show Account Code' (checked), 'Restrict Network Interconnect' (unchecked), 'Drop External Only Impromptu Conference' (unchecked), 'Visually Differentiate External Call' (unchecked), 'Unsupervised Analog Trunk Disconnect Handling' (unchecked), 'High Quality Conferencing' (checked), 'Strict SIPs' (unchecked), and 'Digital/Analogue Auto Create User' (checked).

5.2.4. System - Twinning Tab

To view or change the System Twinning settings, navigate to the **Twining** 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.

The screenshot shows the 'Jersey City' system configuration window with the 'Twining' tab selected. The 'Send original calling party information for Mobile Twinning' checkbox is unchecked. Below it, the 'Calling party information for Mobile Twinning' field is empty.

5.2.5. System – Codecs Tab

In the **Codecs** tab of the Details Pane, select or enter **101** for **RFC2833 Default Payload**. This setting matched the configuration by IntelPeer for use with out-band DTMF tone transmissions.

The screenshot shows the 'Jersey City' system configuration window with the 'Codecs' tab selected. The 'RFC2833 Default Payload' dropdown menu is set to '101'. Below this, there are three panels: 'Available Codecs' with a list of codecs (G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, G.729(a) 8K CS-ACELP, G.723.1 6K3 MP-MLQ) with checkboxes; 'Default Codec Selection' with an 'Unused' label and an empty box; and 'Selected' with a list of selected codecs (G.711 ULAW 64K, G.711 ALAW 64K, G.729(a) 8K CS-ACELP, G.723.1 6K3 MP-MLQ). Navigation buttons (>>, <<, <-, >+) are located between the panels.

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**. Create/verify a default route with the following parameters:

- Set **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.

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, showing a tree structure with 'Jersey City' expanded, and 'IP Route (4)' selected. The main pane shows the configuration for the '0.0.0.0' IP route. The fields are as follows:

Field	Value
IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	10 . 32 . 128 . 254
Destination	LAN1
Metric	0
Proxy ARP	<input type="checkbox"/>

5.4. Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the IntelPeer SIP Trunking service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.4.1** to create the SIP Line from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2 – 5.4.7**.

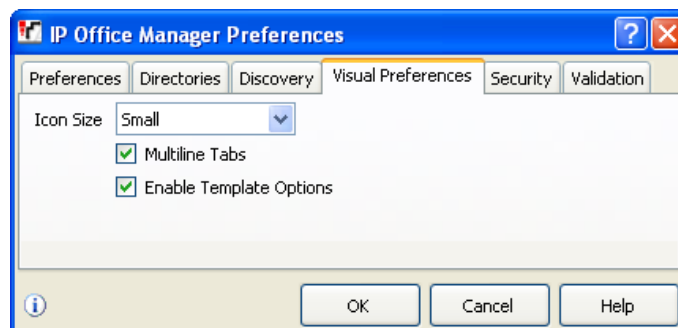
Also, the following SIP Line settings are not supported on Basic Edition:

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

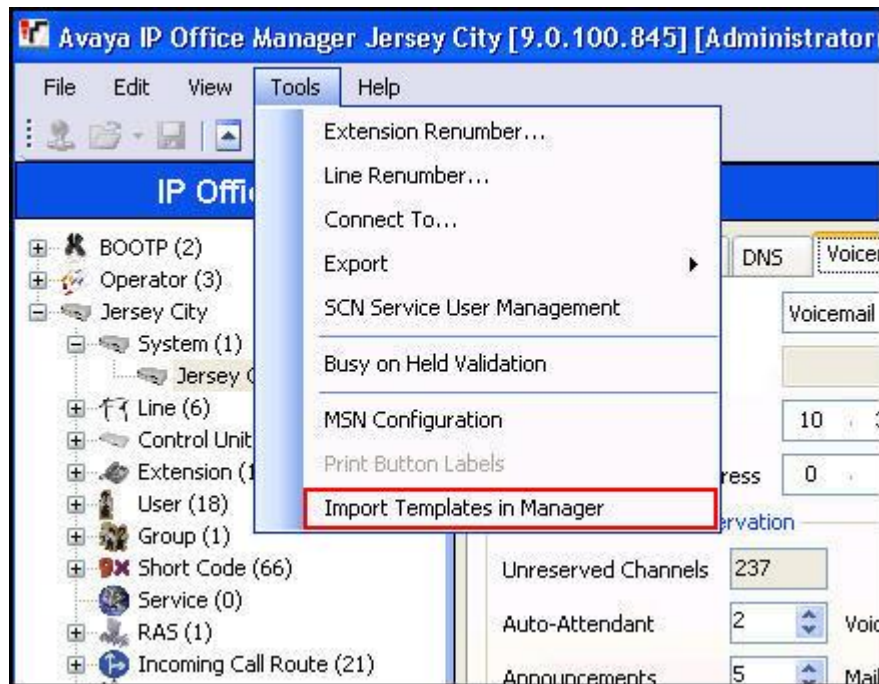
Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2 – 5.4.7**.

5.4.1. Create SIP Line from Template

1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **US_IntelePeer_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**.
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**.

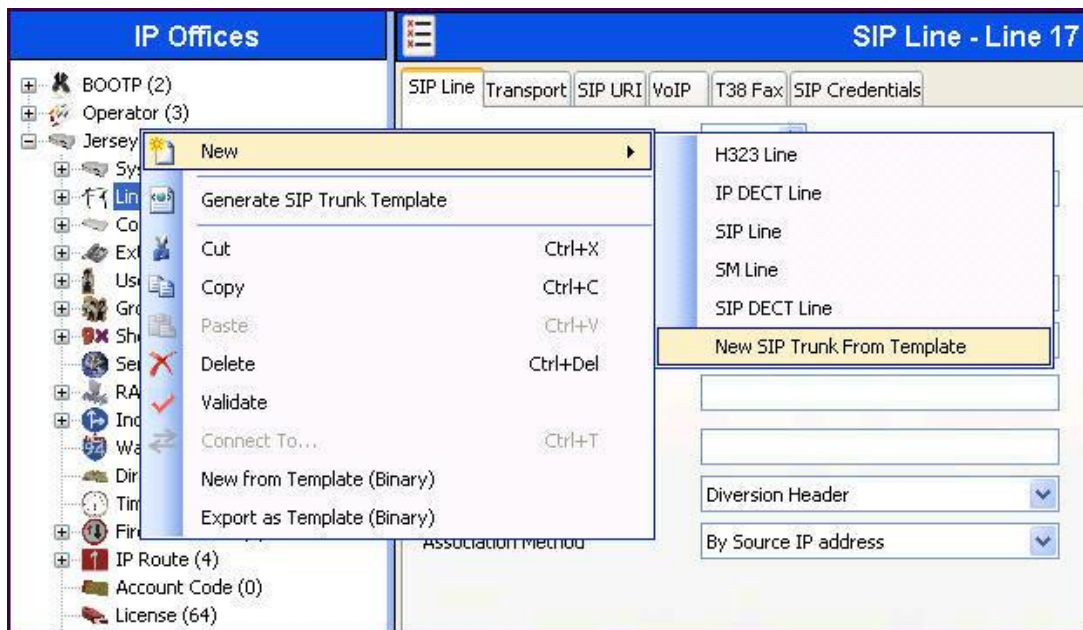


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools** → **Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.



In the pop-up window (not shown) that appears, 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.

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



- In the subsequent **Template Type Selection** pop-up window, select **United States** from the **Country** drop-down list and select **IntelePeer** from the **Service Provider** drop-down list as shown below. These values correspond to parts of the file name (**US_IntelePeer_SIPTrunk.xml**) created 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.

- Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2 – 5.4.7**.

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. This makes the trunk available to incoming and outgoing calls.
- Check **OOS** box. Avaya IP Office will use the SIP OPTIONS method to periodically check the SIP Line. See **Section 5.9** for details on time between SIP OPTIONS sent by IP Office.
- Set **Call Routing Method** to **Request URI**. Avaya IP Office will route inbound calls based on the number in the Request URI.
- Set **Send Caller ID** 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 forwarded or redirected via Mobile Twinning out the SIP Line to the service provider.
- Uncheck **REFER Support**. IntelPeer SIP Trunking does not support use of REFER for off-net call re-direction as in call transfers.
- 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 **Session Timer (seconds)** to a desired value. With the value as shown below, Avaya IP Office will send session refresh UPDATE or re-INVITE to the service provider every 5 minutes (half of the specified value).

IP Offices

- BOOTP (2)
- Operator (3)
- Jersey City
- System (1)
 - Line (6)
 - 1
 - 2
 - 3
 - 4
 - 17
 - 18
- Control Unit (2)
- Extension (17)
- User (18)
- Group (1)
- Short Code (66)
- Service (0)
- RAS (1)
- Incoming Call Route (21)
- WanPort (0)
- Directory (0)
- Time Profile (0)
- Firewall Profile (1)
- IP Route (4)
- Account Code (0)
- License (64)
- Tunnel (0)
- User Rights (8)
- ARS (2)
- RAS Location Request (0)
- Location (0)

SIP Line - Line 17

SIP Line | Transport | SIP URI | VoIP | T38 Fax | SIP Credentials

Line Number: 17

ITSP Domain Name: 10.32.128.20

In Service: ☒

URI Type: SIP

Check OOS: ☒

Call Routing Method: Request URI

Originator number for forwarded and twinning calls:

Name Priority: System Default

Caller ID from From header: ☐

Send From In Clear: ☐

User-Agent and Server Headers:

Service Busy Response: 486 - Busy Here

Action on CAC Location Limit: Allow Voicemail

☐ REFER Support

Incoming: Always

Outgoing: Always

Method for Session Refresh: Auto

Session Timer (seconds): 600

Media Connection Preservation: Disabled

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 'SIP Line - Line 17' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '10.32.128.20'. The 'Network Configuration' section is expanded, showing 'Layer 4 Protocol' set to 'UDP', 'Send Port' set to '5060', and 'Use Network Topology Info' set to 'LAN 1'. The 'Listen Port' is also set to '5060'. Below this, 'Explicit DNS Server(s)' are set to '0.0.0.0' and '0.0.0.0'. 'Calls Route via Registrar' is checked, and 'Separate Registrar' is empty.

SIP Line - Line 17					
SIP Line Transport SIP URI VoIP T38 Fax SIP Credentials					
ITSP Proxy Address: 10.32.128.20					
Network Configuration					
Layer 4 Protocol		UDP		Send Port: 5060	
Use Network Topology Info		LAN 1		Listen Port: 5060	
Explicit DNS Server(s)		0.0.0.0		0.0.0.0	
Calls Route via Registrar		<input checked="" type="checkbox"/>			
Separate Registrar					

5.4.4. 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 unique per customer and therefore customers must contact the service provider to obtain the proper registration credentials for their deployment. IntelPeer uses static IP authentication for the customer account, therefore the SIP Credentials configuration is not needed. This section is included in these application notes for reference and completeness.

Select the **SIP Credentials** tab, and then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button. The screen below shows a previously configured entry being edited. The entry was created with sample settings as shown below:

- Set the **User name**, **Authentication Name**, and **Contact** fields to the registration string provided by the service provider. This is generally a 10-digit telephone number like **7329624489** as shown below.
- In the **Password** field, enter the registration password provided by the service provider.
- In the **Expiry (mins)** field, enter the time in minutes until the registration expires.
- Check the **Registration required** field if Registration is required for the SIP Trunking customer account.

The screenshot shows the 'SIP Line - Line 17' configuration window. The 'SIP Credentials' tab is selected. The table below lists the credentials:

Index	UserName	Authentication Name	Contact	Expiry (mins)	Register
1	7329624489	7329624489	7329624489	60	True

Buttons: Add..., Remove, Edit...

Edit SIP Credentials

User name: 7329624489

Authentication Name: 7329624489

Contact: 7329624489

Password: *****

Expiry (mins): 60

Registration required: ☒

Buttons: OK, Cancel

5.4.5. SIP Line – SIP URI Tab

Select the **SIP URI** tab to create a SIP URI entry or edit an existing 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 a previously configured entry for the compliance test.

- Set **Local URI**, **Contact**, and **Display Name** to *Use Internal Data*. This setting allows calls on this line who's SIP URI matches the number set in the **SIP** tab of any User as shown in **Section 5.6**.
- Set **PAI** to *None*. This setting directs Avaya IP Office to send the PPI (P-Preferred-Identity) header when appropriate instead of the PAI header (P-Asserted-Identity). The PPI header will be populated from the data set in the **SIP** tab of the call initiating **User** as shown in **Section 5.66**.
- Select the **Registration** value that was configured in **Section 5.4.4**, or *0: <None>* if the service provider uses static IP authentication (as was the case with the compliance test and shown below).
- 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.
- Set **Max Calls per Channel** to the number of simultaneous SIP calls allowed using this SIP URI pattern.

The screenshot shows the 'SIP Line - Line 17' configuration window. The 'SIP URI' tab is selected. A table lists the SIP URI entries:

Channel	Groups	Via	Local URI	Contact	Display Name	PAI
1	17 17	1...				N...

Buttons: Add..., Remove, Edit...

Edit Channel

Via: 135.10.96.231

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

PAI: None

Registration: 0: <None>

Incoming Group: 17

Outgoing Group: 17

Max Calls per Channel: 10

Buttons: OK, Cancel

5.4.6. SIP Line – VoIP Tab

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

- Set the **Codec Selection** to *Custom*.
- Choose **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** from the **Unused** box and move these 2 selections to the **Selected** box. These 2 codecs are supported by the IntelPeer SIP Trunking Service. Use the down/up arrows to order the 2 selected codecs as shown. IntelPeer recommends G.711MU as the preferred codec.
- Select **T38** for **Fax Transport Support**.
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones as out-band RTP events as per RFC2833.
- Uncheck the **VoIP Silence Suppression** option box.
- Verify that **Allow Direct Media Path** is disabled (see observation/limitation list in **Section 2.2**).
- Check the **Re-invite Supported** option box.
- 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.

5.4.7. SIP Line – T.38 Fax Tab

Select the **T38 Fax** tab to set the Fax over Internet Protocol parameters of the SIP line. Set the parameters as shown below.

- Uncheck **Use Default Values** at the bottom of the screen.
- Set **T38 Fax Version** to **0**. IntelPeer SIP Trunking supports T.38 fax version 0.
- Set **Max Bit Rate (bps)** to 14400, the highest fax bit rate that Avaya IP Office supports for T.38 faxing.
- Check the **Disable T30 ECM** option.

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'T38 Fax' tab selected. The window has a blue title bar and a toolbar with icons for help, save, delete, confirm, and navigation. The configuration is organized into several sections:

- Top Tabs:** SIP Line, Transport, SIP URI, VoIP, T38 Fax (selected), SIP Credentials.
- T38 Fax Version:** A dropdown menu set to '0'.
- Transport:** A dropdown menu set to 'UDPTL'.
- Redundancy:** Two spinners for 'Low Speed' and 'High Speed', both set to '0'.
- TCF Method:** A dropdown menu set to 'Trans TCF'.
- Max Bit Rate (bps):** A dropdown menu set to '14400'.
- EFlag Start Timer (msecs):** A spinner set to '2600'.
- EFlag Stop Timer (msecs):** A spinner set to '2300'.
- Tx Network Timeout (secs):** A spinner set to '200'.
- Checkboxes (right side):**
 - ☒ Scan Line Fix-up
 - ☒ TFOP Enhancement
 - ☒ Disable T30 ECM (highlighted with a red box)
 - ☐ Disable EFlags For First DIS
 - ☐ Disable T30 MR Compression
- NSF Override:** A section with 'Country Code' and 'Vendor Code' spinners, both set to '0'.
- Bottom:** A checkbox for 'Use Default Values' which is unchecked (highlighted with a red box).

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). 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 To headers 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 on the **SIP Line** in **Section 5.4.5**. This short code will use this line group when placing the outbound calls.

The screenshot displays the Avaya Management System (AMS) interface. On the left is the 'IP Offices' navigation pane, which includes a tree view with categories like BOOTP, Operator, Jersey City, System, Line, Control Unit, Extension, User, Group, Short Code (66), Service, RAS, Incoming Call Route, WanPort, Directory, Time Profile, Firewall Profile, and IP Route. The 'Short Code (66)' item is selected. The main area on the right is titled '9N;; Dial' and contains a 'Short Code' configuration form. The form fields are as follows:

Code	9N;
Feature	Dial
Telephone Number	N"@10.32.128.20"
Line Group ID	17
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>

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.

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

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

Code	*67N;
Feature	Dial
Telephone Number	WN"@10.32.128.20"
Line Group ID	17
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>

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 **Jim 1120E**. Select the **SIP** tab in the Details Pane. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by IntelPeer. 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 trunk calls.

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's information from the network (or alternatively use the *67 short code as defined in **Section 5.5**).

The screenshot displays the Avaya User Configuration interface. On the left, the 'IP Offices' navigation pane shows a hierarchy: BOOTP (2), Operator (3), Jersey City, System (1), Line (6), Control Unit (2), Extension (17), and User (18). Under 'User (18)', several users are listed, including '258 Jim 1120E', which is highlighted. The main pane on the right is titled 'Jim 1120E: 258' and contains multiple tabs: User, Voicemail, DND, Short Codes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, Button Programming, Menu Programming, Mobility, Group Membership, Announcements, SIP, and Personal Directory. The 'SIP' tab is active, showing three input fields: 'SIP Name' with the value '17207291050', 'SIP Display Name (Alias)' with 'Jim 1120E', and 'Contact' with '17207291050'. Below these fields is an unchecked checkbox labeled 'Anonymous'. At the bottom right of the main pane are three buttons: 'OK', 'Cancel', and 'Help'.

The following screen shows the similar SIP settings for an analog extension user for fax:

This screenshot shows the Avaya User Configuration interface for an analog extension user. The left pane shows the 'User (18)' list with '208 Extn208' selected. The main pane is titled 'Extn208: 208' and has the same tabs as the previous screenshot. The 'SIP' tab is active, showing three input fields: 'SIP Name' with the value '17207291055', 'SIP Display Name (Alias)' with 'Extn208 FAX', and 'Contact' with '17207291055'. Below these fields is an unchecked checkbox labeled 'Anonymous'. At the bottom right of the main pane are three buttons: 'OK', 'Cancel', and 'Help'.

5.7. Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal extension. 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 5.4.5**.
- Set the **Incoming Number** to the incoming DID number on which this route should match. Matching is right to left.

The screenshot shows the 'Standard' tab of the configuration window for Incoming Call Route 17 17207291050. The left pane shows a tree view with 'Incoming Call Route (15)' expanded, listing several routes. The main pane shows the configuration fields for the selected route. A red box highlights the 'Bearer Capacity', 'Line Group ID', and 'Incoming Number' fields.

Field	Value
Bearer Capacity	Any Voice
Line Group ID	17
Incoming Number	17207291050
Incoming Sub Address	
Incoming CLI	
Locale	United States (US English)
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 the DID number 17207291050 on Incoming Group 17 are to be routed to the user "Jim 1120E" at extension 258.

The screenshot shows the 'Destinations' tab of the configuration window for Incoming Call Route 17 17207291050. The left pane shows the 'Standard' tab selected. The main pane shows a table with columns for TimeProfile, Destination, and Fallback Extension.

TimeProfile	Destination	Fallback Extension
Default Value	258 Jim 1120E	

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 shows the IP Office configuration interface. On the left is the 'IP Offices' navigation pane with a tree structure including BOOTP, Operator, Jersey City, System, Line, Control Unit, Extension, User, Group, Short Code, Service, RAS, Incoming Call Route, WanPort, Directory, Time Profile, Firewall Profile, IP Route, Account Code, License, Tunnel, User Rights, and ARS. The ARS section is expanded, showing '50: Main' and '51: backup'. The main window is titled 'Main*' and displays the configuration for the selected ARS route.

ARS Configuration for 50: Main

ARS Route Id: 50
Route Name: Main
Dial Delay Time: System Default (4)
Secondary Dial tone: ☒ SystemTone
Check User Call Barring: ☒

In Service: ☒ Out of Service Route: 51: backup
Time Profile: <None> Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
911	911	Dial Emergency	0
N;	N"@10.32.128.20"	Dial	17

Alternate Route Priority Level: 3
Alternate Route Wait Time: 30
Alternate Route: 51: backup

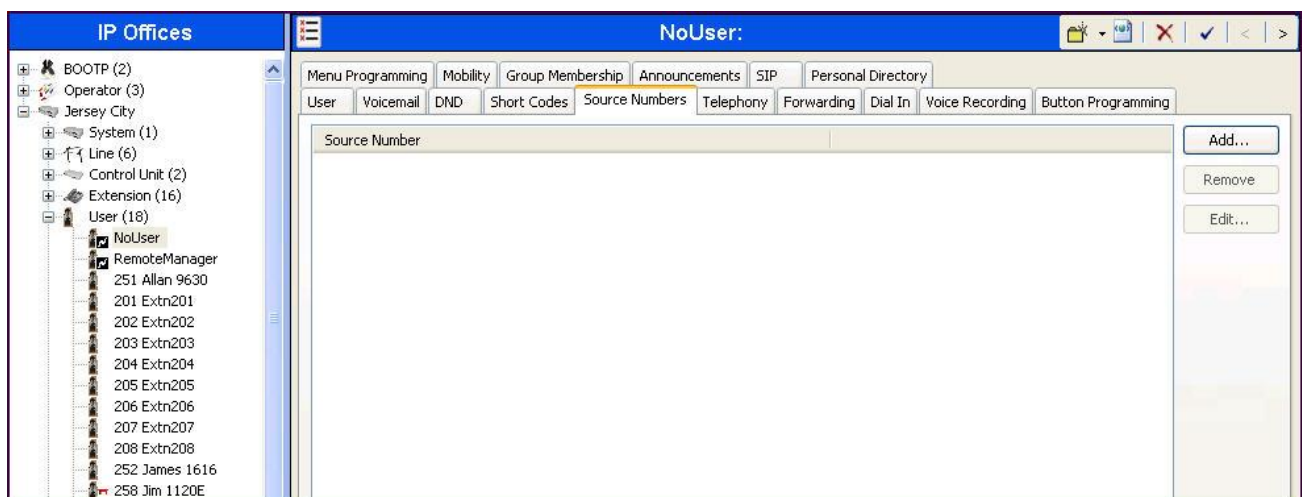
Assuming the primary route is in-service, the number passed from the short code used to access ARS (e.g., **8N**; in **Section 5.5**) can be further analyzed to direct the call to a specific Line Group ID. Per the example screen above, if the user dialed 8-911, the call would be directed to Line Group 0 to be sent out to the local area emergency response center (note that a short code 911 can also be configured to send the emergency call out when the user simply dials 911); if the user dialed 8 + any other number, the call would be directed to Line Group 17 as configured in **Section 5.4.5**. 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. SIP Options

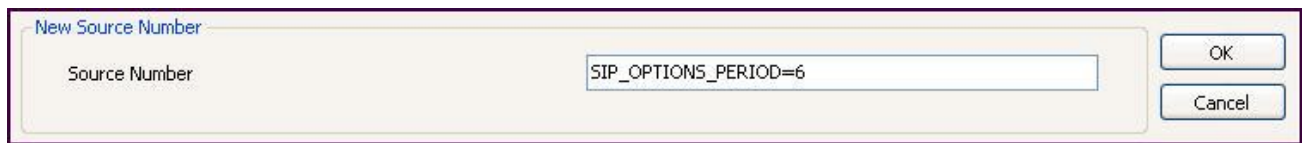
Avaya IP Office sends SIP OPTIONS messages periodically to determine if the SIP connection is active. By default, Avaya IP Office Release 9.0 sends out OPTIONS every 300 seconds. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time** (in seconds) set 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 0 or 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.

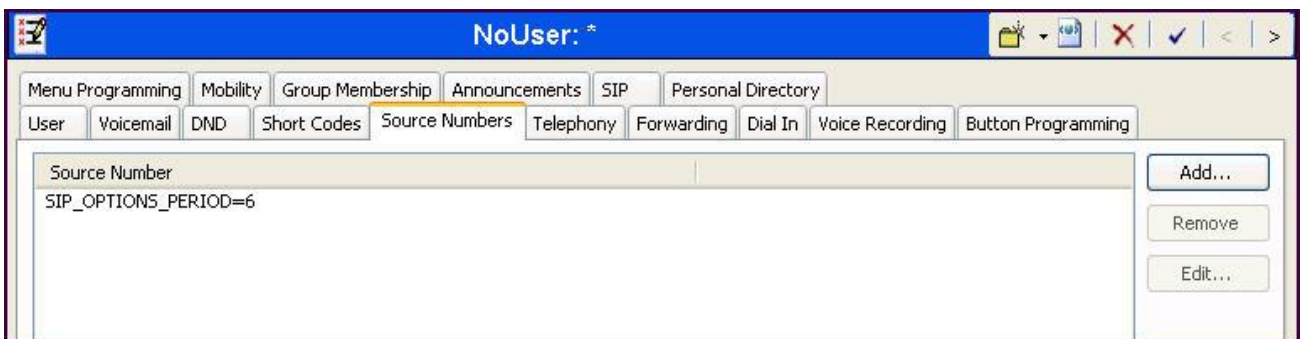


At the bottom of the Details Pane, the **Source Number** field will appear. Enter **SIP_OPTIONS_PERIOD=X**, where **X** is the desired value in minutes. Click **OK**.



A dialog box titled "New Source Number" with a light beige background. It contains a label "Source Number" on the left and a text input field on the right containing the text "SIP_OPTIONS_PERIOD=6". To the right of the input field are two buttons: "OK" and "Cancel".

The **SIP_OPTIONS_PERIOD** parameter will appear in the list of Source Numbers as shown below. For the compliance test, an OPTIONS period of 60 seconds was desired. The **Binding Refresh Time** was set to **60** seconds on the **Network Topology** tab in **Section 5.2.1**. There was no need to define **SIP_OPTIONS_PERIOD**.



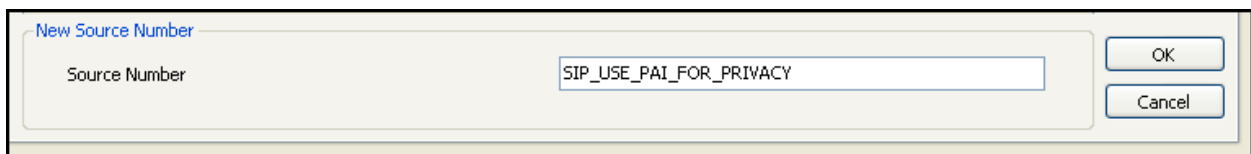
A screenshot of the "NoUser: *" application window. The "Source Numbers" tab is selected in the top menu bar. Below the menu bar is a list of source numbers. The first entry is "SIP_OPTIONS_PERIOD=6". To the right of the list are three buttons: "Add...", "Remove", and "Edit...".

5.10. Privacy/Anonymous Calls

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

To configure Avaya IP Office to use PAI for privacy calls, select **NoUser** under **User** in the Navigation Pane, then select the **Source Numbers** tab in the Details Pane as shown in the first screen in **Section 5.9**. Click the **Add** button.

At the bottom of the Details Pane, the **Source Number** field will appear. Enter **SIP_USE_PA1_FOR_PRIVACY**. Click **OK**.



New Source Number

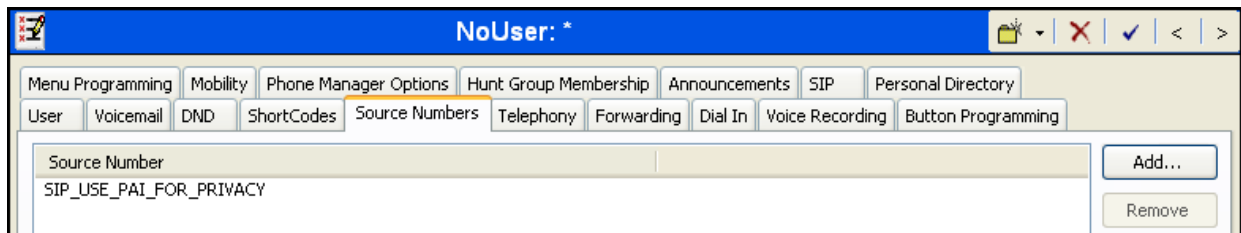
Source Number

SIP_USE_PA1_FOR_PRIVACY

OK

Cancel

The **SIP_USE_PA1_FOR_PRIVACY** parameter will appear in the list of Source Numbers as shown below. Click **OK** at the bottom of the screen (not shown).



NoUser: *

Menu Programming Mobility Phone Manager Options Hunt Group Membership Announcements SIP Personal Directory

User Voicemail DND ShortCodes Source Numbers Telephony Forwarding Dial In Voice Recording Button Programming

Source Number

SIP_USE_PA1_FOR_PRIVACY

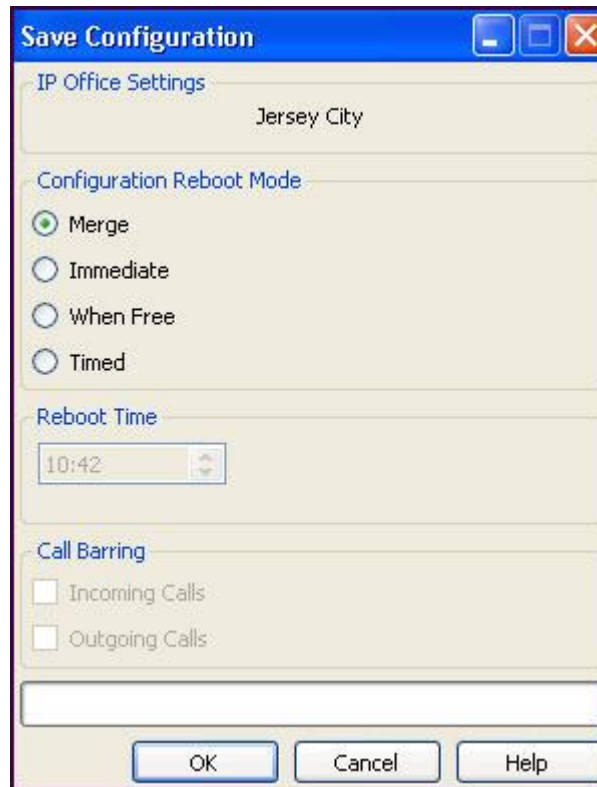
Add...

Remove

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



The image shows a 'Save Configuration' dialog box with a blue title bar and standard window controls. It contains several sections: 'IP Office Settings' with a text field showing 'Jersey City'; 'Configuration Reboot Mode' with four radio buttons ('Merge' is selected, followed by 'Immediate', 'When Free', and 'Timed'); 'Reboot Time' with a time picker set to '10:42'; and 'Call Barring' with two unchecked checkboxes ('Incoming Calls' and 'Outgoing Calls'). At the bottom is an empty text field and three buttons: 'OK', 'Cancel', and 'Help'.

Section	Field/Option	Value/State
IP Office Settings	Text Field	Jersey City
	Configuration Reboot Mode	<input checked="" type="radio"/> Merge <input type="radio"/> Immediate <input type="radio"/> When Free <input type="radio"/> Timed
Reboot Time	Time Picker	10:42
Call Barring	<input type="checkbox"/> Incoming Calls	Unchecked
	<input type="checkbox"/> Outgoing Calls	Unchecked
Buttons	OK, Cancel, Help	Standard buttons

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 (e.g., 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 the Management Interface

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




The image shows the login page for the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in bold black. On the right, under the heading 'Log In', there are two input fields for 'Username:' and 'Password:'. Below these fields is a blue 'Log In' button. To the right of the button, there is a block of text stating: 'This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.' Below this, another block of text states: 'The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.' A third block of text states: 'All users must comply with all corporate instructions regarding the protection of information assets.' At the bottom, there is a copyright notice: '© 2011 - 2013 Avaya Inc. All rights reserved.'

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

[Alarms](#) [Incidents](#) [Statistics](#) [Logs](#) [Diagnostics](#) [Users](#) [Settings](#) [Help](#) [Log Out](#)

Session Border Controller for Enterprise



Dashboard

- Administration
 - Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - SIP Cluster
 - Domain Policies
 - TLS Management
 - Device Specific Settings

Dashboard

Information		
System Time	12:50:26 PM EDT	Refresh
Version	6.2.1.Q07	
Build Date	Mon Dec 9 17:33:02 CST 2013	

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

[Add](#)

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
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings

System Management

Devices Updates SSL VPN Licensing

Device Name (Serial Number)	Management IP	Version	Status	
vnj-sbce2 (IFCS11010169)	10.32.101.20	6.2.1.Q07	Commissioned	Reboot Shutdown Restart Application View Edit Delete

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

System Information: vnj-sbce2 X

General Configuration

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

Device Configuration

HA Mode No
Two Bypass Mode No

Network Configuration

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

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, click on the **Interface Configuration** tab. Verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click **Toggle** to enable the interface.

Session Border Controller for Enterprise



Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▸ Global Profiles

▸ SIP Cluster

▸ Domain Policies

▸ TLS Management

▸ Device Specific Settings

Network Management

Media Interface

Network Management: vnj-sbce2

Devices

vnj-sbce2

Network Configuration

Interface Configuration

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

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 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 shown 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) defined in **Section 6.2**. For the external interface, set the **Signaling IP** to the IP address associated with the public interface (B1) defined 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 IntelPeer uses UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. Under Device Specific Settings, there are sub-options for Network Management, Media Interface, and Signaling Interface (which is highlighted in red). The main content area is titled 'Signaling Interface: vnj-sbce2'. It features a tab labeled 'Signaling Interface' and an 'Add' button. Below this is a table listing the configured signaling interfaces.

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

6.4. Media Interface

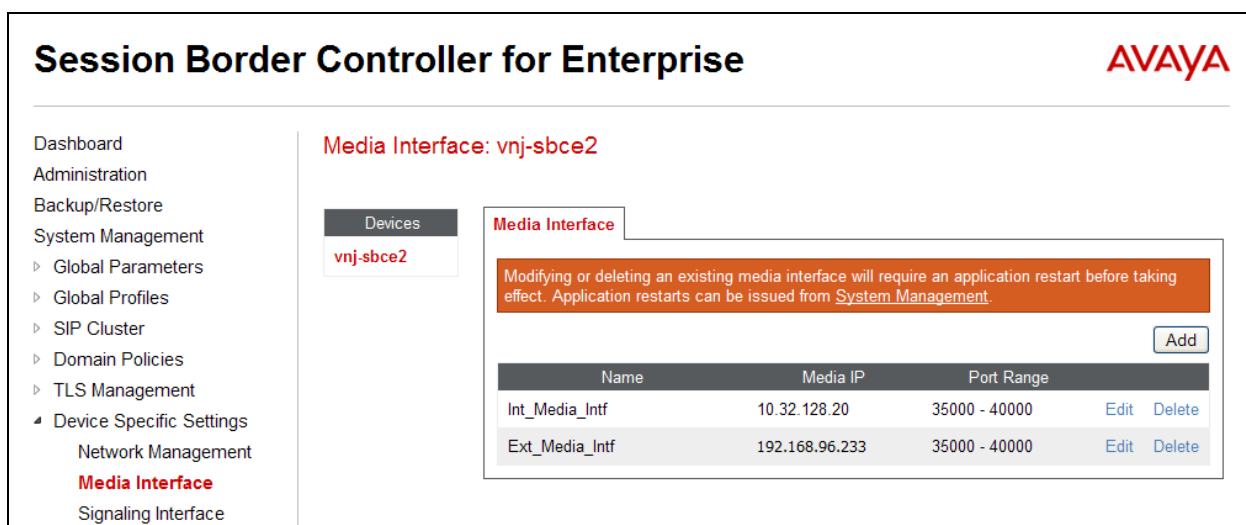
A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

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 series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, media interface **Int_Media_Intf** was created for the Avaya SBCE internal interface and media interface **Ext_Media_Intf** was created for the Avaya SBCE external interface. Each is shown 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) defined in **Section 6.2**. For the external interface, set the **Media IP** to the IP address associated with the public interface (B1) defined in **Section 6.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the far-end. For the compliance test, the default port range was used for both interfaces.



Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ **Device Specific Settings**
  Network Management
  Media Interface
  Signaling Interface

Media Interface: vnj-sbce2

Devices
vjn-sbce2

Media Interface

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

[Add](#)

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

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 6.7.1** and **6.7.2**.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the hierarchy: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Fingerprint, **Server Interworking** (highlighted), Phone Interworking, Media Forking, Routing, and Server Configuration. The main content area is titled "Interworking Profiles: cs2100" 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, there are tabs for "General", "Timers", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is active, showing a table of interworking parameters.

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, server interworking profile *IPOffice-T38* was created for Avaya IP Office by creating a new profile and accepting the default values for all settings with the exception of setting the **T.38 Support** to *Yes*. The **General** tab parameters are shown below.

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			
3xx Handling	No			
Diversion Header Support	No			
Delayed SDP Handling	No			
Re-Invite Handling	No			
T.38 Support	Yes			
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** and **Header Manipulation** tabs have no entries.

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

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

6.5.2. Server Interworking – IntelPeer

For the compliance test, server interworking profile **SP-General-T38** was created for the IntelPeer SIP server. When creating the profile, the default values were used for all parameters with the exception of **T.38 Support** set to **Yes**. Thus, the **SP-General-T38** profile is identical to the **IPOffice-T38** profile created in **Section 6.5.1**.

6.6. Signaling Manipulation

Signaling manipulation scripts provides for the manipulation of SIP messages which cannot be done by other configuration within the Avaya SBCE.

The compliance test used a signaling manipulation script to remove a Remote-Address header from messages (INVITE and 200 OK) originated from the Avaya IP Office. This header needed to be removed since it could contain an IP address on the private enterprise network.

To create a signaling manipulation script, navigate to **Global Profiles → Signaling Manipulation**. Click on **Add Script** (not shown), then type in a script title and enter the script statements/commands. Save the script by clicking on **Save** (not shown). For the compliance test, a script named “Remove_Remote-Address” was created. The script is shown below.

Signaling Manipulation

```
//Remove Remote Address header in outbound INVITE and 200 OK

within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Remote-Address"][1]);
  }
}
```

Edit

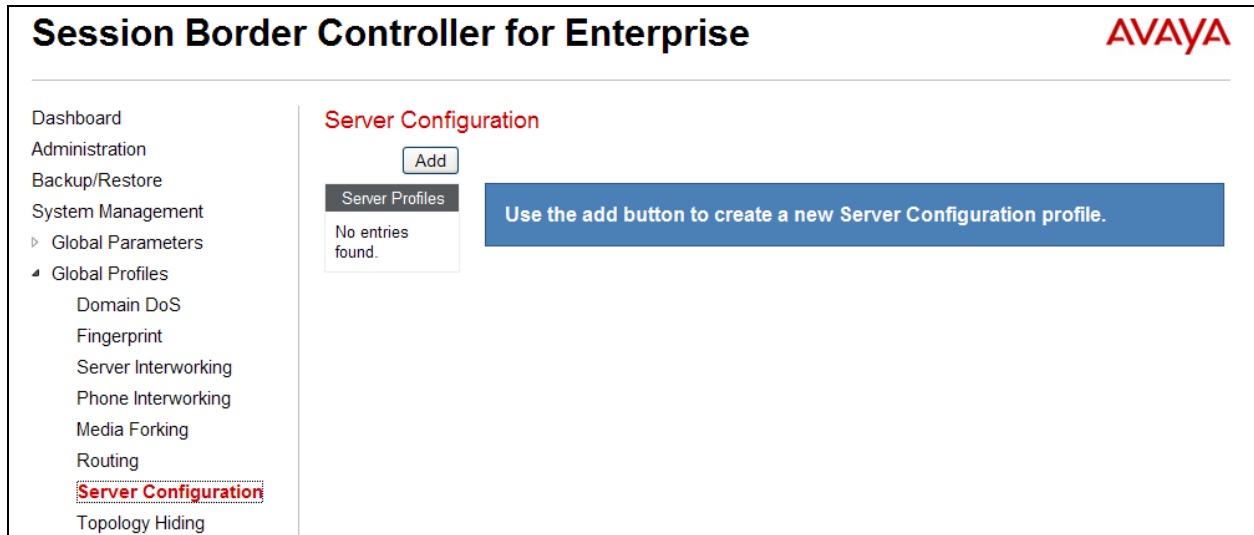
The above script is tied to the IntelPeer trunk server in Server Configuration (**Section 6.7.2**).

Note that use of the Signaling Manipulation scripts demands higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should be used with care and only in cases where the use of Signaling Rules (**Section 6.10**) does not meet the desired result. Refer to [11] for information on the Avaya SBCE scripting language

6.7. Server Configuration

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

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



6.7.1. Server Configuration – Avaya IP Office

For the compliance test, server configuration profile **IPO-JCcity** 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 **Supported Transports** to the transport protocol used for SIP signaling between Avaya IP Office and the Avaya SBCE.
- Set the **UDP Port** to the port Avaya IP Office will listen on for SIP requests from the Avaya SBCE.

The screenshot shows a configuration window with four tabs: General, Authentication, Heartbeat, and Advanced. The General tab is selected. It contains a table with the following data:

Server Type	Call Server
IP Addresses / FQDNs	10.32.128.30
Supported Transports	UDP
UDP Port	5060

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

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

The screenshot shows the same configuration window, but with the Advanced tab selected. It contains a table with the following data:

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

The 'Interworking Profile' field is highlighted with a red box. Buttons for 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

6.7.2. Server Configuration – IntelPeer

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

- Set **Server Type** to *Trunk Server*.
- Set **IP Addresses / FQDNs** to the IP address of the IntelPeer SIP server.
- Set **Supported Transports** to the transport protocol used for SIP signaling between IntelPeer and the Avaya SBCE. In the compliance test, UDP was used.
- Set the **UDP Port** to the standard SIP port of 5060. This is the port IntelPeer will listen on for SIP requests from the Avaya SBCE.

The screenshot shows the 'General' tab of a configuration window. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below the tabs are four configuration rows: 'Server Type' set to 'Trunk Server', 'IP Addresses / FQDNs' set to '192.168.123.104', 'Supported Transports' set to 'UDP', and 'UDP Port' set to '5060'. An 'Edit' button is located at the bottom center of the configuration area.

Field	Value
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.123.104
Supported Transports	UDP
UDP Port	5060

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for IntelPeer defined in **Section 6.5.2**. For **Signaling Manipulation Script**, select the script created in **Section 6.6**.

The screenshot shows the 'Advanced' tab of the same configuration window. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below the tabs are four configuration rows: 'Enable DoS Protection' with an unchecked checkbox, 'Enable Grooming' with an unchecked checkbox, 'Interworking Profile' set to 'SP-General-T38' (highlighted with a red box), and 'Signaling Manipulation Script' set to 'Remove_Remote-Addr' (highlighted with a red box). The 'UDP Connection Type' is set to 'SUBID'. An 'Edit' button is located at the bottom center of the configuration area.

Field	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General-T38
Signaling Manipulation Script	Remove_Remote-Addr
UDP Connection Type	SUBID

6.8. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 6.11**. For the compliance test, the predefined **default-trunk** application rule (shown below) was used for both Avaya IP Office and the IntelPeer 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.

Session Border Controller for Enterprise

Dashboard

Administration

Backup/Restore

System Management

- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
 - Application Rules**
 - Border Rules
 - Media Rules
 - Security Rules
 - Signaling Rules
 - Time of Day Rules
 - End Point Policy Groups
 - Session Policies
- TLS Management

Application Rules: default-trunk

Add

Filter By Device...

Clone

Application Rules

- default
- default-trunk**

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

Application Rule

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

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

Edit

AMC; Reviewed:
SPOC mm/dd/yyyy

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

52 of 90
IntP-IPO9-ASBCE

6.9. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 6.11**. For the compliance test, the predefined **default-low-med** media rule (shown below) was used for both Avaya IP Office and the IntelPeer 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.

Each of the tabs of the **default-low-med** media rule containing data is shown below.

The **Media NAT** tab has no entries.

The screenshot shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation menu with 'Media Rules' selected. The main area is titled 'Media Rules: default-low-med' 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 are tabs for 'Media NAT', 'Media Encryption', 'Media Anomaly', 'Media Silencing', and 'Media QoS'. The 'Media NAT' tab is active, showing a 'Media NAT' section with the text 'Learn Media IP dynamically' and an 'Edit' button.

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

The screenshot shows the 'Media Encryption' tab selected. It contains three sections: 'Audio Encryption', 'Video Encryption', and 'Miscellaneous'. Under 'Audio Encryption', 'Preferred Formats' is set to 'RTP' and 'Interworking' is checked. Under 'Video Encryption', 'Preferred Formats' is set to 'RTP' and 'Interworking' is checked. Under 'Miscellaneous', 'Capability Negotiation' is unchecked. An 'Edit' button is at the bottom.

The **Media Anomaly** tab shows **Media Anomaly Detection** was disenabled.

Media NAT	Media Encryption	Media Anomaly	Media Silencing	Media QoS
Media Anomaly Detection <input type="checkbox"/>				
<div>Edit</div>				

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

Media NAT	Media Encryption	Media Anomaly	Media Silencing	Media QoS
Media Silencing <input type="checkbox"/>				
<div>Edit</div>				

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

Media NAT	Media Encryption	Media Anomaly	Media Silencing	Media QoS
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				
<div>Edit</div>				

6.10. Signaling Rules

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the hierarchy: Dashboard, Administration, Backup/Restore, System Management, and Domain Policies. Under Domain Policies, the 'Signaling Rules' link is selected. The main content area shows the 'Signaling Rules: default' configuration. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' The 'General' tab is active, showing settings for Inbound and Outbound traffic. The 'Content-Type Policy' section is also visible, with 'Enable Content-Type Checks' checked. The 'Action' is set to 'Allow' and the 'Multipart Action' is set to 'Allow'. The 'Exception List' is empty. An 'Edit' button is located at the bottom right of the configuration area.

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 <input checked="" type="checkbox"/>			
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

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

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS				
<div>Signaling QoS <input checked="" type="checkbox"/></div> <table><tr><td>QoS Type</td><td>DSCP</td></tr><tr><td>DSCP</td><td>AF41</td></tr></table> <div>Edit</div>						QoS Type	DSCP	DSCP	AF41
QoS Type	DSCP								
DSCP	AF41								

6.11. Endpoint Policy Groups

An endpoint 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 endpoint policy group must be created for Avaya IP Office and another for the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 6.14**.

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

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left navigation pane includes 'Domain Policies' and 'End Point Policy Groups'. The main area displays 'Policy Groups: default-low' with a list of groups: default-low, default-low-enc, default-med, default-med-enc, default-high, default-high-enc, OCS-default-high, and avaya-def-low-e... The 'default-low' group is selected. A table below shows the configuration for this group, with columns for Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row with the following values: Order 1, Application default, Border default, Media default-low-med, Security default-low, Signaling default, and Time of Day default. There are 'Edit' and 'Clone' buttons for each row.

Order	Application	Border	Media	Security	Signaling	Time of Day
1	default	default	default-low-med	default-low	default	default

6.11.1. Endpoint Policy Group – Avaya IP Office

For the compliance test, endpoint policy group **IPO-EP-Policy** was created for Avaya IP Office. Default values were used for each of the rules which comprise the group with the exception of **Application**. For **Application**, enter the application rule specified in **Section 6.8**. The details of the default settings for **Media** and **Signaling** are shown in **Section 6.9** and **Section 6.10** respectively.

The screenshot shows a 'Policy Group' configuration window. It features a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row with the following values: Order 1, Application default-trunk, Border default, Media default-low-med, Security default-low, Signaling default, and Time of Day default. There are 'Edit' and 'Clone' buttons for each row. The window also has 'Summary' and 'Add' buttons.

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

6.11.2. Endpoint Policy Group – IntelPeer

For the compliance test, endpoint policy group *SP-EP-Policy* was created for the IntelPeer SIP server. Default values were used for each of the rules which comprise the group with the exception of **Application**. For **Application**, enter the application rule specified in **Section 6.8**. Thus, the **SP-EP-Policy** is identical to the **IPO-EP-Policy** created in **Section 6.11.1**.

6.12. Routing

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

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with the following 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 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, there is a 'Routing Profile' section with a table. The table has four columns: Priority, URI Group, Next Hop Server 1, and Next Hop Server 2. The first row shows '1' in the Priority column, '*' in the URI Group column, and dashes in the Next Hop Server columns. There are 'View' and 'Edit' links for this row. An 'Add' button is located to the right of the table.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	---	---

6.12.1. Routing – Avaya IP Office

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

- Set the **URI Group** to the wild card * to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of Avaya IP Office LAN1 port.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP**.

View Routing Rule		X
Priority	1	
URI Group	*	
Next Hop Server 1	10.32.128.30	
Next Hop Server 2	---	
Next Hop Priority	<input checked="" type="checkbox"/>	
NAPTR	<input type="checkbox"/>	
SRV	<input type="checkbox"/>	
Next Hop in Dialog	<input type="checkbox"/>	
Ignore Route Header	<input type="checkbox"/>	
Outgoing Transport	UDP	

6.12.2. Routing – IntelPeer

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

- Set the **URI Group** to the wild card * to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of the IntelPeer SIP server.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP** as defined by IntelPeer.

View Routing Rule		X
Priority	1	
URI Group	*	
Next Hop Server 1	192.168.123.104	
Next Hop Server 2	---	
Next Hop Priority	<input checked="" type="checkbox"/>	
NAPTR	<input type="checkbox"/>	
SRV	<input type="checkbox"/>	
Next Hop in Dialog	<input type="checkbox"/>	
Ignore Route Header	<input type="checkbox"/>	
Outgoing Transport	UDP	

6.13. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 6.14**. For the compliance test, the predefined **default** topology hiding profile (shown below) was used for both Avaya IP Office and the IntelPeer SIP server.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the hierarchy: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), and SIP Cluster. Under Global Profiles, the following options are listed: Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, **Topology Hiding** (highlighted), Signaling Manipulation, URI Groups, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings.

The main content area is titled "Topology Hiding Profiles: default". It 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, the "Topology Hiding" tab is active, showing a table with the following data:

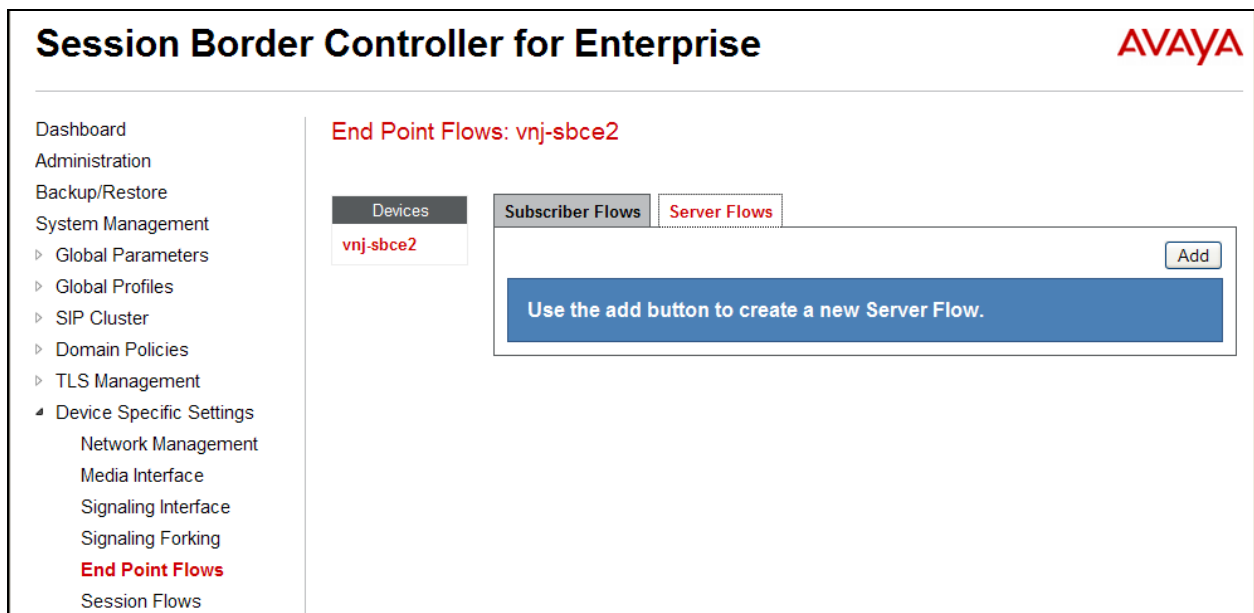
Header	Criteria	Replace Action	Overwrite Value
Referred-By	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
To	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---

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

6.14. End Point Flows

Endpoint 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 endpoint flow and the destination endpoint flow. In the case of the compliance test, the signaling endpoints are Avaya IP Office and the service provider SIP server.

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



6.14.1. End Point Flow – Avaya IP Office

For the compliance test, endpoint 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-IntelePeer** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Avaya IP Office server created in **Section 6.7.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *.
- Set the **Received Interface** to the external signaling interface.
- Set the **Signaling Interface** to the internal signaling interface.
- Set the **Media Interface** to the internal media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Avaya IP Office in **Section 6.11.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.12.2** used to direct traffic to the IntelePeer SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Avaya IP Office in **Section 6.13**.

View Flow: IPO-JCity

Criteria

Flow Name	IPO-JCity
Server Configuration	IPO-JCity
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig_Intf

Profile

Signaling Interface	Int_Sig_Intf
Media Interface	Int_Media_Intf
End Point Policy Group	IPO-EP-Policy
Routing Profile	To-IntelePeer
Topology Hiding Profile	default
File Transfer Profile	None

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

Server Configuration: IPO-JCity

Update

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-IntelePeer	View Clone Edit Delete

6.14.2. End Point Flow – IntelPeer

For the compliance test, endpoint flow **IntelPeer** was created for the IntelPeer SIP server. All traffic from IntelPeer 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** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the IntelPeer SIP server created in **Section 6.7.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *.
- Set the **Received Interface** to the internal signaling interface.
- Set the **Signaling Interface** to the external signaling interface.
- Set the **Media Interface** to the external media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for IntelPeer in **Section 6.11.2**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.12.1** used to direct traffic to Avaya IP Office.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for IntelPeer in **Section 6.13**.

View Flow: IntelPeer		X	
Criteria		Profile	
Flow Name	IntelPeer	Signaling Interface	Ext_Sig_Intf
Server Configuration	IntelPeer	Media Interface	Ext_Media_Intf
URI Group	*	End Point Policy Group	SP-EP-Policy
Transport	*	Routing Profile	To-IPO-JCity
Remote Subnet	*	Topology Hiding Profile	default
Received Interface	Int_Sig_Intf	File Transfer Profile	None

The screen below shows the saved **IntelPeer** configuration as a Server Flow. Note that the server name is in the **Server Configuration** heading.

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

7. IntelPeer SIP Trunking Configuration

IntelPeer 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). IntelPeer will provide the customer the necessary information to configure the Avaya IP Office and Avaya SBCE including:

- Network edge IP addresses of the IntelPeer SIP Trunking Service.
- Transport and port for the IntelPeer SIP Trunking connection to the Avaya SBCE at the enterprise.
- DID numbers to assign to users at the enterprise.
- Supported codecs and their preference order.

8. Verification Steps

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

8.1. Avaya IP Office System Status

Use the Avaya IP Office System Status application to verify the SIP Line channels state and to check 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. On the **Status** tab in the right pane, verify the **Current State** is **Idle** for channels where no active calls are currently in session; the state should be **Connected** for channels engaged in active calls.

Avaya IP Office System Status - Jersey City (10.32.128.30) - IP500 V2 9.0.1.0 build 845

IP Office System Status

Help Snapshot LogOff Exit About

- System
- Alarms (1)
- Extensions (12)
- Trunks (6)
 - Lines: 1 - 4
 - Line: 17
 - Line: 18
- Active Calls
- Resources
- Voicemail
- IP Networking
- Locations

SIP Trunk Summary

Peer Domain Name: 10.32.128.20
Resolved Address: 10.32.128.20
Line Number: 17
Number of Administered Channels: 10
Number of Channels in Use: 2
Administered Compression: G711 Mu, G729 A
Silence Suppression: Off
Layer 4 Protocol: UDP
SIP Trunk Channel Licenses: Unlimited
SIP Trunk Channel Licenses in Use: 2
SIP Device Features:

1%

Channel Number	URI G...	Call Ref	Current State	Time in State	R...	Codec	Connection Type	C. Other Party on Call	Direction of Call	R. Receive Jitter	Receive Packe...	Transmit Jitter	Transmit Packet...
1	1	14	Connected	00:02:09	...	G711 Mu	RTP Relay	Extn 256, Tony 9611	Incoming				
2	0	15	Connected	00:01:51	...	G711 Mu	RTP Relay	Extn 258, Jim 1120E	Outgoing				
3			Idle	1 day 20...									
4			Idle	1 day 20...									
5			Idle	1 day 20...									
6			Idle	1 day 20...									
7			Idle	1 day 20...									
8			Idle	1 day 20...									
9			Idle	1 day 20...									
10			Idle	1 day 20...									

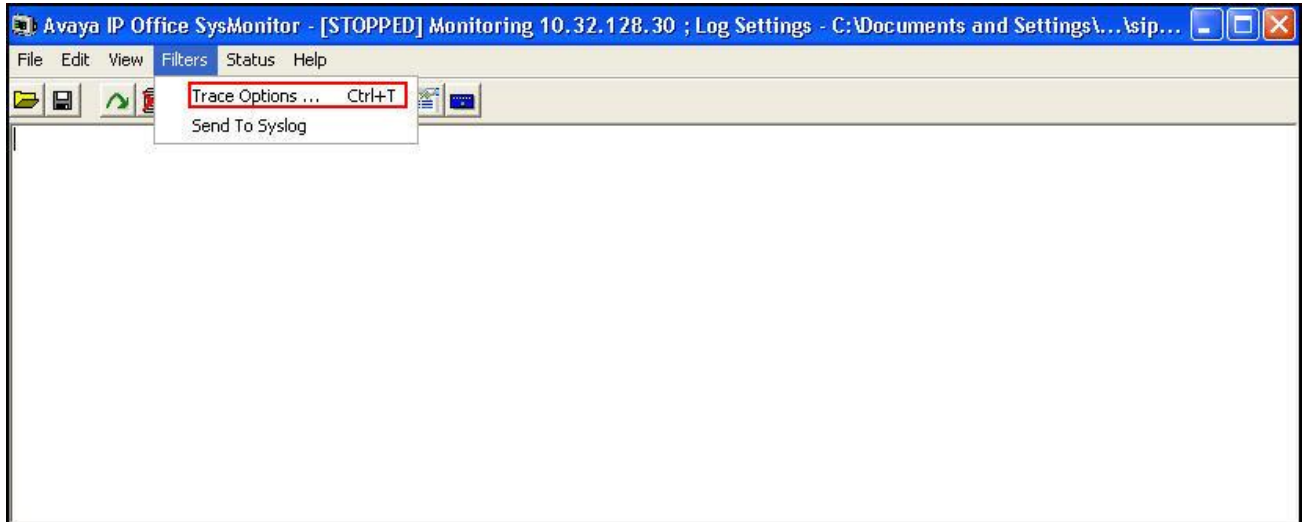
Trace Trace All Pause Ping Call Details Print... Save As...

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

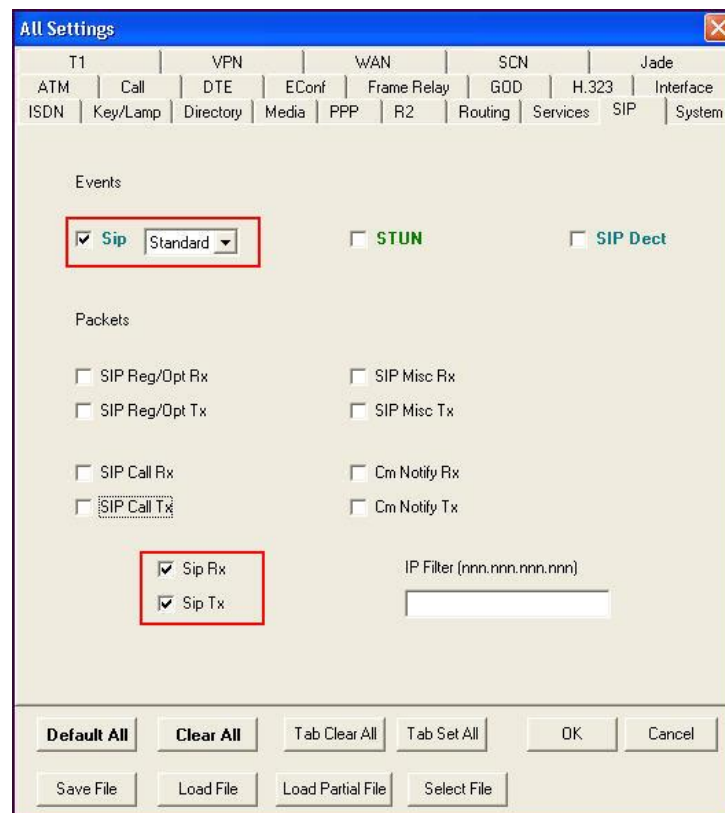
Status	Utilization Summary	Alarms	Registration
Alarms for Line: 17 SIP 10.32.128.20			
Last Date Of Error	Occurrences	Error Description	

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 the monitored information to be customized. To customize, select **Filters → Trace Options ...** as shown below:



The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, **Standard** SIP Events and the **SIP Rx** and **SIP Tx** boxes are checked.



8.3. Avaya SBCE Protocol Trace

The Avaya SBCE can take internal traces on specified interfaces. Both SIP signaling crossing 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, 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 start the trace. The captured trace can then be downloaded for examination using a protocol sniffer application such as Wireshark.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office R9.0.1 and the Avaya Session Border Controller for Enterprise R6.2.1 to the IntelPeer SIP Trunking Service. The IntelPeer SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks. The IntelPeer SIP Trunking Service passed compliance testing. Please refer to **Section 2.2** for any exceptions.

10. Additional References

Avaya IP Office R9.0

- [1] *IP Office Documentation Library*, Release 9.0, Documentation number 15-604278 Issue 1, September 2013
- [2] *IP Office 9.0 Product Description*, Documentation number 15-601041 Issue 27.02.0, January 2014
- [3] *Avaya IP Office 9.0 Installing IP500/IP500 V2*, Document number 15-601042 Issue 28j, January 2014
- [4] *Avaya IP Office 9.0 Administering Voicemail Pro*, Document number 15-601063 Issue 9.01.0, September 2013
- [5] *Avaya IP Office Manager Release 9.0*, Document number 15-601011 Issue 9.02.0, January 2014
- [6] *Avaya IP Office 9.0 Using System Status*, Document number 15-601758 Issue 09c, August 2013
- [7] *Avaya IP Office 9.0 Using IP Office System Monitor*, Document Number 15-601019, Issue 05c, August 2013
- [8] *Avaya IP Office 9.0 H.323 Telephone Installation*, Document Number 15-601046, Issue 18b, August 2013
- [9] *Avaya IP Office 9.0 SIP Extension Installation*, Issue 3c, August 2013

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

Avaya Session Border Controller for Enterprise

- [10] *Avaya Session Border Controller for Enterprise Overview and Specification*, Issue 2, December 2013
- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, January 2014
- [12] *Configuring the Avaya Session Border Controller for IP Office Remote Workers*, September 2013

Product documentation for the IntelPeer SIP Trunking is available from IntelPeer. See **Section 2.3** on how to contact IntelPeer.

11. Appendix - Remote Worker Configuration via Avaya SBCE

This section describes the process for connecting select remote Avaya SIP endpoints on the public Internet to Avaya IP Office on the private enterprise network via the Avaya SBCE. The provisioning builds on the reference configuration described in previous sections of this document.

Note – This Remote Worker configuration is based on provisioning the Avaya SBCE. It is not to be confused with “native” Avaya IP Office Remote Worker configurations.

Supported Remote Worker endpoints for Avaya IP Office are:

- Flare® Experience for iPad
- Flare® Experience for Windows
- one-X® Mobile Preferred VoIP client for iOS
- one-X® Mobile Preferred VoIP client for Android

For Avaya IP Office R9.0, the following table summarizes encryption support for these remote worker endpoints (see **Section 11.1.8**):

Client type	Uses to the external interface of the SBCE		
	TLS	SRTP Audio	SRTP Video
Flare Experience for iPad	Y*	Y*	N
Flare Experience for Windows	Y*	Y*	N
one-X Mobile Preferred VoIP client for iOS	Y	N	N
one-X Mobile Preferred VoIP client for Android	N	N	N
* If the client is used inside and outside of the IP Office core, the signalling type must be changed. IP Office 9.0 does not support TLS or SRTP connections to these clients on the inside of the SBCE.			

In the configuration for the compliance test, Avaya Flare® Experience for Windows was used as the Remote Worker SIP endpoint.

The reference configuration for the compliance test, including the Remote Worker endpoint, is shown in **Figure 1** in **Section 3**. Internet access by the Remote Worker endpoint is through a Router/NAT/Firewall/Default Gateway provided by the Verizon FiOS Internet Service located between the Remote Worker private LAN and the public Internet. The Verizon FiOS router also provides DHCP functionality in the private space. Note that the use of the Verizon FiOS router is for functionality testing only and is not prescriptive.

Provisioning of the Verizon FiOS router is beyond the scope of this document.

11.1. Provisioning Avaya SBCE for Remote Worker

Provisioning of the Avaya SBCE to support Avaya IP Office SIP connection to the service provider is described in **Section 6**. The following sections build on that provisioning.

11.1.1. Network Management

This section shows the **Network Management** configuration of the Avaya SBCE to support Remote Worker. For this purpose, the Avaya SBCE is configured with a second outside IP address assigned to physical interface B1, and a second inside address assigned to physical interface A1.

The following IP addresses were used on the Avaya SBCE in the configuration used for the compliance test:

- **192.168.128.20** is the inside address previously provisioned for SIP Trunking with the service provider (see **Section 6.2**).
- **192.168.128.21** is the new inside address for Remote Worker.
- **192.168.96.233** is the outside address previously provisioned for SIP Trunking with the service provider (see **Section 6.2**).
- **192.168.96.234** is the new outside address for Remote Worker.

1. On the **Network Configuration** tab, select **Add** to create an entry for **192.168.128.21** on interface **A1**, then select **Save**.
2. Repeat step 1 for adding an entry for **192.168.96.234** on interface **B1**.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings

Network Management

Media Interface
Signaling Interface
Signaling Forking
End Point Flows
Session Flows

Network Management: vnj-sbce2

Devices
vnj-sbce2

Network Configuration **Interface Configuration**

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

A1 Netmask: 255.255.255.0 A2 Netmask: B1 Netmask: 255.255.255.224

Add **Save** **Clear**

IP Address	Public IP	Gateway	Interface	
10.32.128.20		10.32.128.254	A1	Delete
192.168.96.233		192.168.96.254	B1	Delete
10.32.128.21		10.32.128.254	A1	Delete
192.168.96.234		192.168.96.254	B1	Delete

11.1.2. Signaling Interfaces

Two new Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic. Interface **Ext_Sig_Intf_RW** supports TLS, while interface **Int_Sig_Intf_RW** supports TCP.

1. From **Device Specific Settings** on the left-hand menu, select **Signaling Interface**. Click on the **Add** button to create Signaling Interface **Ext_Sig_Intf_RW**
 - Signaling IP = **192.168.96.234**
 - TLS Port = **5061**
 - Select TLS Profile **AvayaSBCServer** from the drop down menu
2. Repeat step 1 to create Signaling Interface **Int_Sig_Intf_RW**
 - Signaling IP = **192.168.128.21**
 - TCP Port = **5060**

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand menu is expanded to 'Device Specific Settings', and 'Signaling Interface' is selected. The main content area shows the 'Signaling Interface' configuration page for device 'vnj-sbce2'. A table lists the configured signaling interfaces, with 'Int_Sig_Intf_RW' and 'Ext_Sig_Intf_RW' highlighted by a red box.

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_RW	10.32.128.21	5060	---	---	None	Edit	Delete
Ext_Sig_Intf_RW	192.168.96.234	---	---	5061	AvayaSBCServer	Edit	Delete

Signaling Interface **Int_Sig_Intf_RW** is used in the Remote Worker Server Flow (**Section 11.1.10.2**). Signaling Interface **Ext_Sig_Intf_RW** is used in the Remote Worker Subscriber Flow (**Section 11.1.10.1**), and in the Remote Worker Server Flow (**Section 11.1.10.2**).

11.1.3. Media Interfaces

Two new Media interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic

1. From **Device Specific Settings** on the left-hand menu, select **Media Interface**. Click on the **Add** button to create Media Interface **Int_Media_Intf_RW** using the parameters shown below.
2. Repeat step **1** to create Media Interface **Ext_Media_Intf_RW**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. Under Device Specific Settings, 'Media Interface' is selected. The main content area is titled 'Media Interface: vnj-sbce2'. It features a 'Media Interface' tab and a table listing configured interfaces. A red box highlights the newly added 'Int_Media_Intf_RW' and 'Ext_Media_Intf_RW' entries. A warning message at the top states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' An 'Add' button is visible in the top right of the table area.

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_RW	10.32.128.21	35000 - 40000	Edit	Delete
Ext_Media_Intf_RW	192.168.96.234	35000 - 40000	Edit	Delete

Media Interface **Int_Media_Intf_RW** is used in the Remote Worker Server Flow (**Section 11.1.10.2**). Media Interface **Ext_Media_Intf_RW** is used in the Remote Worker Subscriber Flow (**Section 11.1.10.1**).

11.1.4. Server Profile for Avaya IP Office

TCP transport protocol (which is required for the Remote Worker connection between the Avaya SBCE and Avaya IP Office) needs to be added to the existing **IPO-JCity** Server Profile (see **Section 6.7.1**).

1. From **Global Profiles** on the left-hand menu, select **Server Configuration**
2. Select the existing **IPO-JCity** profile and click on **Edit**.
3. In the **Edit Server Configuration Profile - General** window, perform the following additional configurations:
 - **Supported Transports:** Check **TCP**
 - **TCP Port:** **5060**

Server Type: Call Server

IP Addresses / Supported FQDNs: 10.32.128.30

Supported Transports: ☒ TCP, ☒ UDP, ☐ TLS

TCP Port: 5060

UDP Port: 5060

TLS Port:

Finish

The **General** tab of the completed server profile is shown below.

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration
Topology Hiding

Server Configuration: IPO-JCity

Add

Server Profiles

IPO-JCity

General Authentication Heartbeat Advanced

Server Type: Call Server

IP Addresses / FQDNs: 10.32.128.30

Supported Transports: TCP, UDP

TCP Port: 5060

UDP Port: 5060

Edit

Rename Clone Delete

11.1.5. Routing Profiles

Two new Routing Profiles are required to support Remote Worker.

1. From **Global Profiles** on the left-hand menu, select **Routing**.
2. Select the **Add** button to create Routing Profile **To-IPO-JCity_RW**, select **Next** (not shown).
3. Enter the following:
 - a. **URI Group** = * (default)
 - b. **Next Hop Server 1** = **10.32.128.30** (IP Office LAN1 interface defined in **Section 5.2.1**)
 - c. Verify **Routing Priority based on Next Hop Server** is checked.
 - d. Select **TCP**.

Next Hop Routing	
URI Group	*
Next Hop Server 1 <small>IP, IP:Port, Domain, or Domain:Port</small>	10.32.128.30
Next Hop Server 2 <small>IP, IP:Port, Domain, or Domain:Port</small>	
Routing Priority based on Next Hop Server	<input checked="" type="checkbox"/>
Use Next Hop for In Dialog Messages	<input type="checkbox"/>
Ignore Route Header for Messages Outside Dialog	<input type="checkbox"/>
NAPTR	<input type="checkbox"/>
SRV	<input type="checkbox"/>
Outgoing Transport	<input type="radio"/> TLS <input checked="" type="radio"/> TCP <input type="radio"/> UDP

4. Select the existing **default** Routing Profile and click on the **Clone** button, and name it **default_RW**, then select **Next** (not shown). Keep all the default values.

View Routing Rule	
Priority	1
URI Group	*
Next Hop Server 1	---
Next Hop Server 2	---
Next Hop Priority	<input type="checkbox"/>
NAPTR	<input checked="" type="checkbox"/>
SRV	<input checked="" type="checkbox"/>
Next Hop in Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>
Outgoing Transport	None

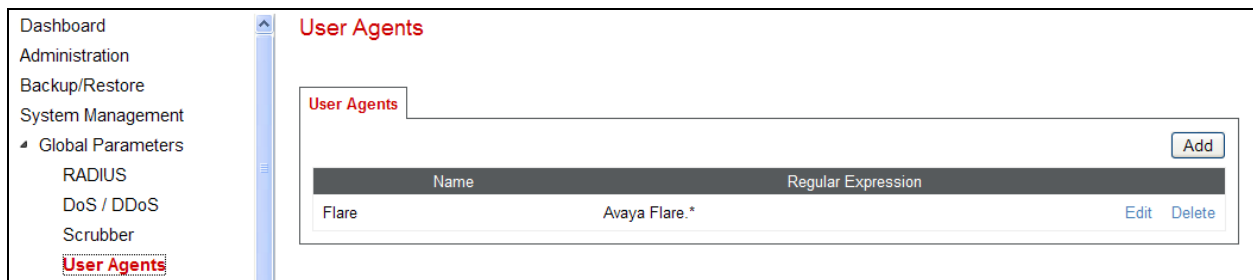
The Routing Profile **To-IPO-JCity_RW** is used in the Remote Worker Subscriber Flow (**Section 11.1.10.1**). The Routing Profile **default_RW** is used in the Remote Worker Server Flow (**Section 11.1.10.2**).

11.1.6. User Agent

User Agents are created for each type of Remote Worker endpoint used. In the configuration for the compliance test, the Avaya Flare® Experience for Windows SIP softphone was used, and its configuration is shown below.

1. From **Global Parameters** on the left-hand menu, select **User Agents**.
2. Select the **Add** button to create a new User Agent.
3. Enter the following:
 - **User Agent = Flare**
 - **Regular expression = Avaya Flare.***

In this expression, “Avaya Flare.*” will match any software version listed after the user agent name.



The **Flare** User Agent is defined in the Remote Worker Subscriber Flow (**Section 11.1.10.1**).

11.1.7. Application Rules

Application Rule **AppRule_RW** is created for Remote Worker.

1. From **Domain Policies** on the left-hand menu, select **Application Rules**.
2. Select **Add** button to create a new Application Rule.
3. Enter a name (e.g., **AppRule_RW**), and click on **Next** (not shown).
4. In the **Voice** field:
 - Check **In** and **Out**.
 - Enter an appropriate value in the **Maximum Concurrent Sessions** field, (e.g., **2000**).
 - Enter **10** in the **Maximum Session per Endpoint** field.
 - Leave the **CDR** field at **None** and the **RTCP Keep-Alive** field unchecked (**No**).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu includes Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, Application Rules (highlighted), Border Rules, Media Rules, Security Rules, Signaling Rules, Time of Day Rules, End Point Policy Groups, Session Policies, and TLS Management. The main content area is titled 'Application Rules: AppRule_RW' and features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. A blue bar with the text 'Click here to add a description.' is visible. Below this, the 'Application Rule' configuration is shown in a table format. The table has columns for Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The rows are Voice, Video, and IM. The Voice row has checkboxes for In and Out checked, and values of 2000 for Maximum Concurrent Sessions and 10 for Maximum Sessions Per Endpoint. The Video and IM rows have unchecked checkboxes. Below the table, there is a 'Miscellaneous' section with fields for CDR Support (set to None) and RTCP Keep-Alive (set to No). An 'Edit' button is located at the bottom right of the configuration area.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	10
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

The rule **AppRule_RW** is assigned to the End Point Policy Groups (Section 11.1.9).

11.1.8. Media Rules

Two Media Rules are defined. Rule **SRTP_RW** is defined to enable the use of SRTP between the Avaya Flare® Experience for Windows Remote Worker (which also uses TLS for transport; see **Section 11.3.1**) and the Avaya SBCE. Rule **RTP_RW** is created for the Remote Worker connection from the Avaya SBCE to Avaya IP Office.

1. From **Domain Policies** on the left-hand menu, select **Media Rules**
2. To create the **SRTP_RW** rule, select the **default-low-med** and click on the **Clone** button.
3. Enter a name (e.g., **SRTP_RW**) and click **Finish** (not shown).
4. Edit the created Media Rule to populate the fields in the **Media Encryption** tab as shown below.

The screenshot shows a 'Media Encryption' configuration window with three tabs: Audio Encryption, Video Encryption, and Miscellaneous. The Audio Encryption tab is active, showing settings for Preferred Format #1 (SRTP_AES_CM_128_HMAC_SHA1_80), Preferred Format #2 (NONE), Preferred Format #3 (NONE), Encrypted RTCP (unchecked), MKI (unchecked), Lifetime (2^), and Interworking (checked). The Video Encryption tab shows Preferred Format #1 (RTP), Preferred Format #2 (NONE), Preferred Format #3 (NONE), Encrypted RTCP (checked), MKI (unchecked), Lifetime (2^), and Interworking (checked). The Miscellaneous tab shows Capability Negotiation (unchecked). A 'Finish' button is at the bottom.

Audio Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input type="checkbox"/>

Finish

Create the Media Rule **RTP_RW** from cloning the **default-low-med** again. The screen below shows the rule's Media encryption tab.

Media Encryption

Audio Encryption

Preferred Format #1

RTP

Preferred Format #2

NONE

Preferred Format #3

NONE

Encrypted RTCP

☒

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Video Encryption

Preferred Format #1

RTP

Preferred Format #2

NONE

Preferred Format #3

NONE

Encrypted RTCP

☒

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Miscellaneous

Capability Negotiation

☐

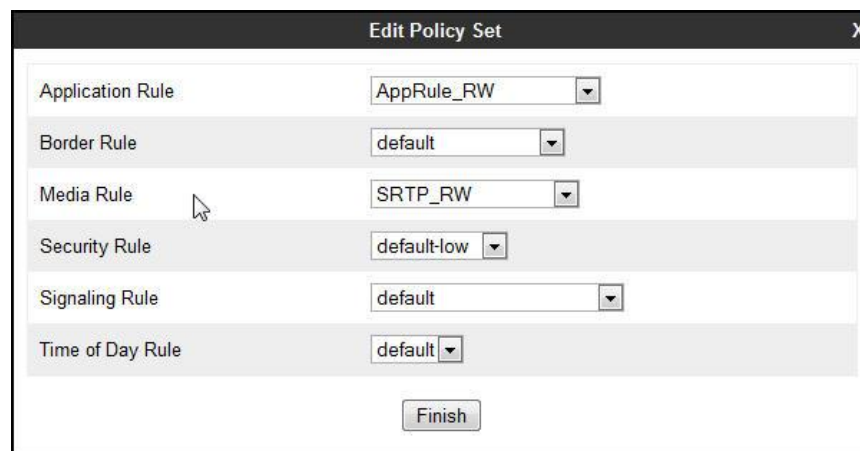
Finish

Media Rule **SRTP_RW** is assigned to the End Point Policy Group **SRTP-Policy_RW** (Section 11.1.9). Media Rule **RTP_RW** is assigned to the End Point Policy Group **RTP-Policy_RW** (Section 11.1.9).

11.1.9. End Point Policy Groups

Two new End Point Policy Groups are defined for Remote Worker. Group **SRTP-Policy_RW** is defined for the SRTP connection and **RTP-Policy_RW** is defined for the RTP connection.

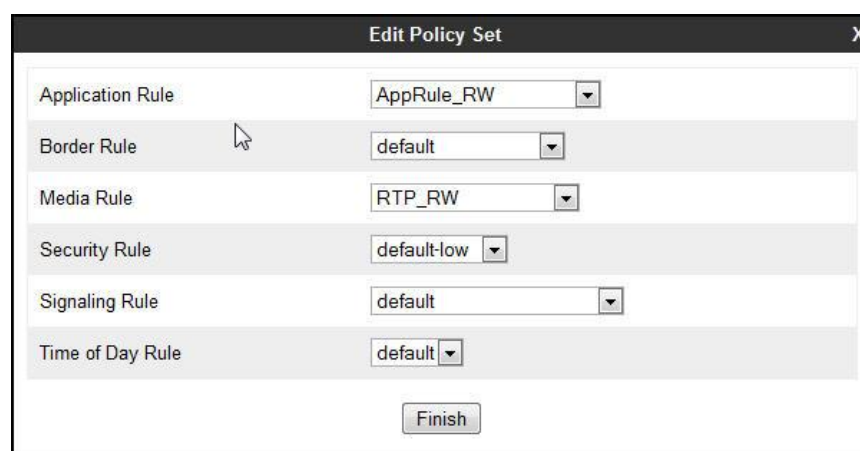
1. From **Domain Policies** on the left-hand menu, select **End Point Policy**.
2. Select **Add** button to create a new End Point Policy Group.
3. Enter a name (e.g., **SRTP-Policy_RW**), and click on **Next** (not shown).
4. The **Policy Group** window will open. Enter the following:
 - **Application Rule** = AppRule_RW (Section 11.1.7)
 - **Border Rule** = default
 - **Media Rule** = SRTP_RW (Section 11.1.8)
 - **Security Rule** = default-low
 - **Signaling Rule** = default
 - **Time of Day Rule** = default



Rule Type	Value
Application Rule	AppRule_RW
Border Rule	default
Media Rule	SRTP_RW
Security Rule	default-low
Signaling Rule	default
Time of Day Rule	default

Finish

5. End Point Policy Group **RTP-Policy_RW** is similarly created with Media Rule **RTP_RW** (Section 11.1.8):



Rule Type	Value
Application Rule	AppRule_RW
Border Rule	default
Media Rule	RTP_RW
Security Rule	default-low
Signaling Rule	default
Time of Day Rule	default

Finish

End Point Policy Group **SRTP-Policy_RW** is used in the Subscriber Flow (Section 11.1.10.1). End Point Policy Group **RTP-Policy_RW** is used in the Server Flow (Section 11.1.10.2).

11.1.10. End Point Flows

A Subscriber Flow and a Server Flow are created for Remote Worker.

11.1.10.1 Subscriber Flow

A **Subscriber Flow** is defined as follows:

1. From **Device Specific Settings** on the left-hand menu, select **End Point Flows**. Click on **Add** and the **Criteria** window will open (not shown).
 - Enter a name (e.g., **Flare_RW**)
 - **URI Group** = * (default)
 - **User Agent** = **Flare**
 - **Source Subnet** = * (default)
 - **Via Host** = * (default)
 - **Contact Host** = * (default)
 - **Signaling Interface** = **Ext_Sig_Intf_RW** (Section 11.1.2)
2. Click on **Next** (not shown) and the **Profile** window will open (not shown).
 - **Source** = **Subscriber**
 - **Methods Allowed Before REGISTER**: Leave as default
 - **Media Interface** = **Ext_Media_Intf_RW** (Section 11.1.3)
 - **End Point Policy Group** = **SRTP-Policy_RW** (Section 11.1.9).
 - **SIP Cluster Flow**: unchecked
 - **Routing Profile** = **To-IPO-JCity_RW** (Section 11.1.5)
 - **Topology Hiding Profile** = **None**
 - **Phone Interworking Profile** = **Avaya-Ru**
 - **TLS Client Profile** = **AvayaSBCCClient**
 - **Radius Profile** = **None**
 - **File Transfer Profile** = **None**
 - **Signaling Manipulation Script** = **None**

The **Subscriber Flows** tab shown below displays the finished Subscribe Flow **Flare_RW**:

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

SIP Cluster

Domain Policies

TLS Management

Device Specific Settings

Network Management

Media Interface

Signaling Interface

Signaling Forking

End Point Flows

Session Flows

End Point Flows: vnj-sbce2

Devices

vnj-sbce2

Subscriber Flows

Server Flows

Add

Hover over a row to see its description.

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group	
1	Flare_RW	*	*	Flare	SRTP-Policy_RW	<div>ViewCloneEditDelete</div>

Clicking on the highlighted View link brings up the following **View Flow** window:

View Flow: Flare_RW

X

Criteria

Flow Name	Flare_RW
URI Group	*
User Agent	Flare
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	Ext_Sig_Intf_RW

Optional Settings

Topology Hiding Profile	None
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	AvayaSBCCClient
RADIUS Profile	None
File Transfer Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	Flare
Media Interface	Ext_Media_Intf_RW
End Point Policy Group	SRTP-Policy_RW
Routing Profile	To-IPO-JCity_RW

11.1.10.2 Server Flow

The following section shows the new **Server Flow** settings for Remote Worker.

1. From **Device Specific Settings** on the left-hand menu, select **End Point Flows**, then the **Server Flows** tab
2. Select **Add** (not shown), and enter the following:
 - **Name** = **IPO-JCity_RW**
 - **Server Configuration** = **IPO-JCity** (Section 6.7.1)
 - **URI Group** = * (default)
 - **Transport** = * (default)
 - **Remote Subnet** = * (default)
 - **Received Interface** = **Ext_Sig_Intf_RW** (Section 11.1.2)
 - **Signaling Interface** = **Int_Sig_Intf_RW** (Section 11.1.2)
 - **Media Interface** = **Int_Media_Intf_RW** (Section 11.1.3)
 - **End Point Policy Group** = **RTP-Policy_RW** (Section 11.1.9)
 - **Routing Profile** = **default_RW** (Section 11.1.5)
 - **Topology Hiding Profile** = **default**
 - **File Transfer Profile** = **None** (default)

View Flow: IPO-JCity_RW

Criteria

Flow Name	IPO-JCity_RW
Server Configuration	IPO-JCity
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig_Intf_RW

Profile

Signaling Interface	Int_Sig_Intf_RW
Media Interface	Int_Media_Intf_RW
End Point Policy Group	RTP-Policy_RW
Routing Profile	default_RW
Topology Hiding Profile	default
File Transfer Profile	None

If this Remote Worker server flow is listed ahead of the flow for SIP Trunking (**IPO-JCity** as created in **Section 6.14.1**), enter **2** in the **Priority** box at the start of the Remote Worker flow entry and click the **Update** button under the server name. The completed flow should show up in the **Server Flows** tab as below.

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
End Point Flows
Session Flows
Relay Services

End Point Flows: vnj-sbce2

Devices

vnj-sbce2

Subscriber Flows

Server Flows

Server Configuration: IPO-JCity

Update

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-Broadvox	View Clone Edit Delete
2	IPO-JCity_RW	*	Ext_Sig_Intf_RW	Int_Sig_Intf_RW	RTP-Policy_RW	default_RW	View Clone Edit Delete

Server Configuration: Remote Worker

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Remote Worker	*	Ext_Sig_Intf	Ext_Sig_Intf	RTP-Policy	To-Broadvox	View Clone Edit Delete

11.2. Remote Worker Endpoint Configuration on Avaya IP Office

The Remote Worker Avaya Flare® Experience for Windows endpoint is added to the Avaya IP Office **User** and **Extension** configuration.

11.2.1. Extension and User Configuration

No special configurations are required to create the Remote Worker extension and user in Avaya IP Office. Follow the same standard procedures for creating a local extension and user for Avaya Flare® Experience for Windows.

The Remote Worker user provisioned is shown below. Note that since the Remote Worker endpoint used in the reference configuration is Avaya Flare® Experience for Windows, the **Enable Softphone** and **Enable Flare** options are selected.

Note – Do not check the **Enable Remote Worker** option. This is only enabled for Avaya IP Office “native” Remote Worker configurations, not for Remote Worker configurations utilizing the Avaya SBCE.

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view shows the hierarchy: IP Offices > Jersey City > System (1) > Line (6) > Control Unit (2) > Extension (17) > User (18). The user 'RW FlareWin' is selected. The main pane shows the configuration for 'RW FlareWin: 255'. The 'User' tab is active, showing fields for Name, Password, Confirm Password, Account Status (Enabled), Full Name, Extension (255), Email Address, Locale (United States (US English)), Priority (5), System Phone Rights (None), and Profile (Power User). Below these fields, several checkboxes are visible: 'Enable Softphone' (checked), 'Enable one-X Portal Services' (unchecked), 'Enable one-X TeleCommuter' (unchecked), 'Enable Remote Worker' (unchecked), 'Enable Flare' (checked), 'Enable Mobile VoIP Client' (unchecked), 'Send Mobility Email' (unchecked), and 'Ex Directory' (unchecked). Red boxes highlight the 'Enable Softphone' and 'Enable Flare' checkboxes.

The **SIP** tab for the Remote User is configured the same way as with local IP Office user (see **Section 5.6**).

The screenshot shows the 'RW FlareWin: 255*' configuration window with the 'SIP' tab selected. The window has a blue title bar and a toolbar with icons for save, delete, check, and navigation. Below the title bar is a tabbed interface with the following tabs: User, Voicemail, DND, Short Codes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, Button Programming, Menu Programming, Mobility, Group Membership, Announcements, SIP (selected), and Personal Directory. The SIP tab contains three text input fields: 'SIP Name' with the value '17207291051', 'SIP Display Name (Alias)' with the value 'RW FlareWin', and 'Contact' with the value '17207291051'. At the bottom, there is an unchecked checkbox labeled 'Anonymous'.

11.2.2. Incoming Call Route


Follow the same procedures described in **Section 5.7** for defining an Incoming Call Route to the Remote Worker.

The screenshot shows the '17 17207291051*' configuration window with the 'Destinations' tab selected. The window has a blue title bar and a toolbar with icons for save, delete, check, and navigation. Below the title bar is a tabbed interface with the following tabs: Standard, Voice Recording, and Destinations (selected). The Destinations tab contains a table with three columns: 'TimeProfile', 'Destination', and 'Fallback Extension'. The table has one row with the following values: 'Default Value' in the 'TimeProfile' column, '255 RW FlareWin' in the 'Destination' column, and a dropdown menu in the 'Fallback Extension' column.

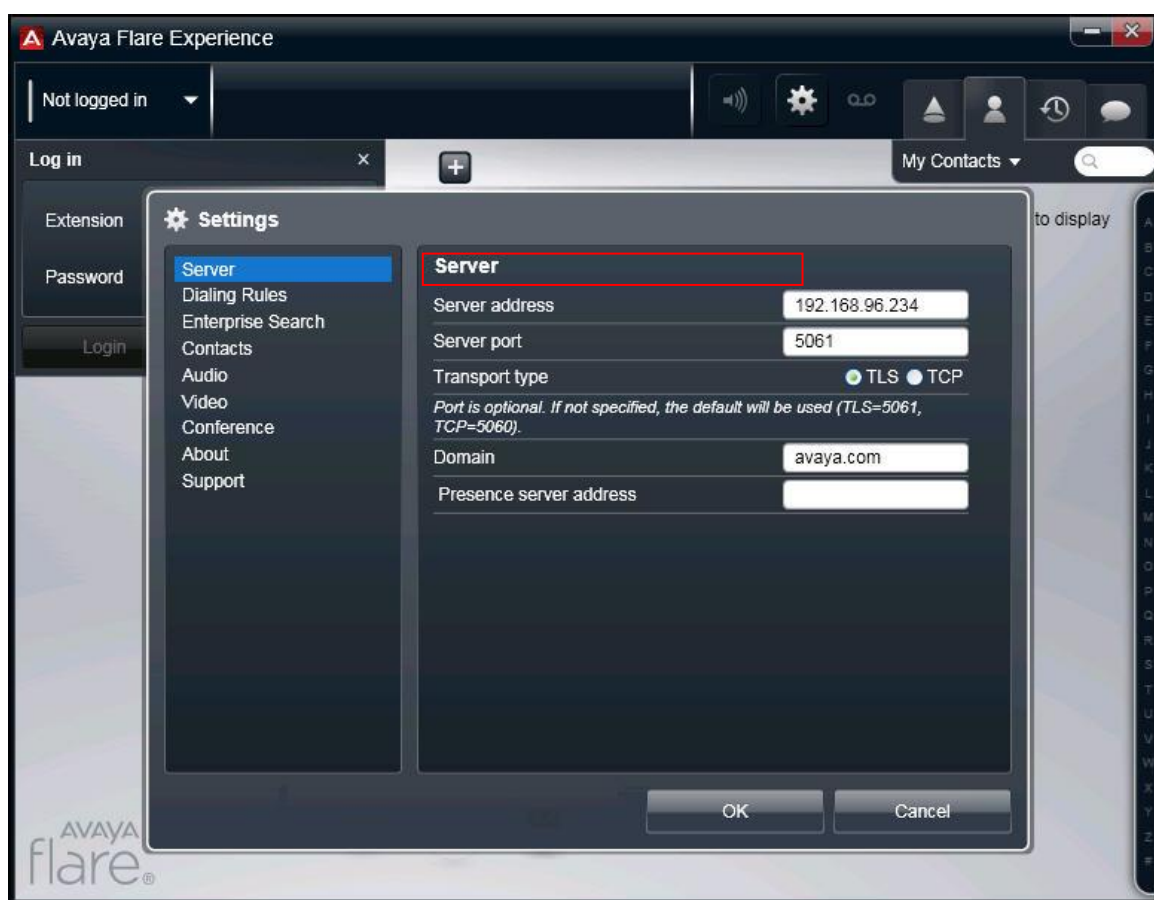
11.3. Remote Worker Avaya Flare® Experience for Windows Configuration

The following screens illustrate Avaya Flare® Experience for Windows administration settings for Remote Worker as used in the reference configuration.

11.3.1. Settings - Server Screen

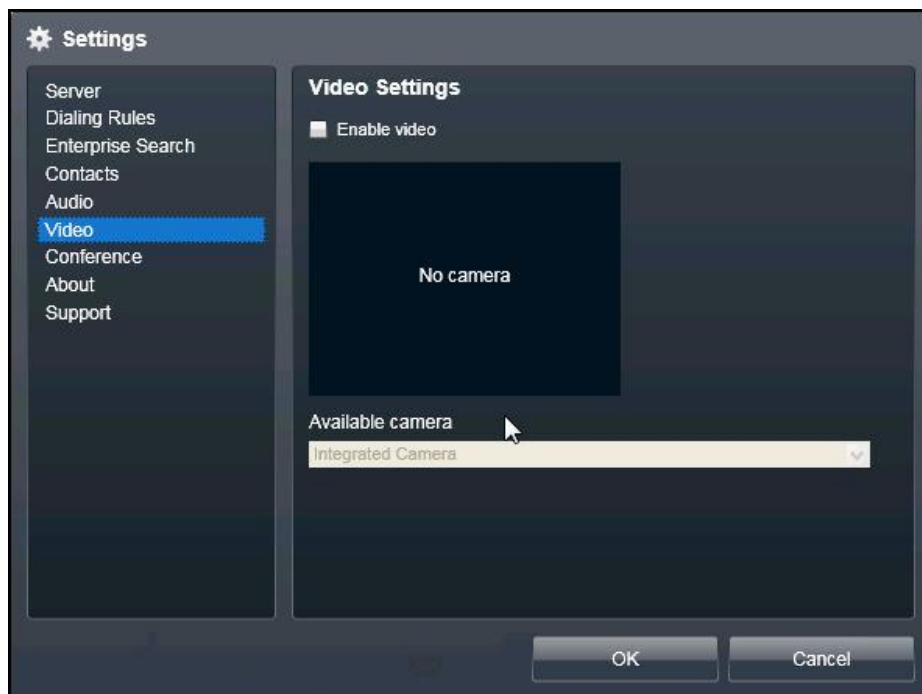
After opening the Avaya Flare® Experience for Windows application, select the Settings icon , select **Server** from the Settings menu, and enter the following:

- **Server address** = **192.168.96.234** (the IP address of Remote Worker outside interface B1 on Avaya SBCE (see **Section 11.1.1**)).
- **Server port** = **5061** (note that the **Transport type** will automatically change to TLS).
- **Domain** = IP Office SIP Registrar domain name (**avaya.com** was used for the compliance test, see the VoIP tab screenshot in **Section 5.2.1**).



11.3.2. Settings - Video Screen

Select **Video** from the Settings menu, *unselect* the **Enable Video** option. In Release 1.1 of Avaya Flare® Experience for Windows, only audio calls are supported with SRTP media encryption (see **Section 11.1.8**).



©2014 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.