



Application Notes for Configuring the Vodafone DE (Germany) SIP Trunk Service with Avaya IP Office 10.0 and Avaya Session Border Controller for Enterprise 7.1 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking for an enterprise solution using Avaya IP Office 10.0 and Avaya Session Border Controller for Enterprise 7.1 to interoperate with the Vodafone DE SIP Trunk Service.

The Vodafone DE SIP Trunk Service provides PSTN access via a SIP trunk connected to the Vodafone DE Voice Over Internet Protocol (VoIP) network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise. Vodafone DE is a member of the Avaya DevConnect Service Provider program.

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

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking for an enterprise solution using Avaya IP Office 10.0 and the Avaya Session Border Controller for Enterprise 7.1 (Avaya SBCE) to interoperate with the Vodafone DE SIP Trunk Service.

The Vodafone DE SIP Trunk Service referenced within these Application Notes is designed for business customers. Customers using this service with the IP Office solution are able to place and receive PSTN calls via a broadband WAN connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Avaya IP Office, Avaya SBCE and various Avaya endpoints listed in **Section 4**.

The Vodafone DE SIP Trunk Service passed compliance testing with observations/ limitations described in **Section 2.2**.

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.

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

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

For the testing associated with this Application Note, the interface between Avaya systems and the Vodafone DE SIP Trunk Service did not include use of any specific encryption features as requested by Vodafone DE.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products wherever possible (see **Section 2.2**).

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Establishment of the SIP trunk
- SIP OPTIONS queries and responses
- Incoming PSTN calls (via the SIP trunk) to SIP and H.323 telephones at the enterprise
- Outgoing PSTN calls (via the SIP trunk) from SIP and H.323 telephones at the enterprise
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows and Avaya Communicator for Web
- Various call types including: local, long distance, international, outbound toll-free, operator, and local directory assistance
- Codec G.711A and G.729
- Caller ID presentation and Caller ID restriction
- DTMF transmission using RFC 2833
- Response to incomplete call attempts and trunk errors
- Voicemail navigation using DTMF input for inbound and outbound calls
- Voicemail message waiting indicator (MWI)
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and twinning (mobility)
- G.711 fax
- Long duration calls and simultaneous active calls
- Remote worker

The following items are not supported or were not tested:

- The REFER method and T.38 Fax are not supported by the Vodafone DE SIP Trunk Service.
- Inbound toll-free calls and emergency calls were not tested.

2.2. Test Results

Interoperability testing of the Vodafone DE SIP Trunk Service was successful with the following observations.

- **Outbound Caller ID:** On outbound calls, the calling party number is shown as the pilot/base number of the account and not the actual DDI sent by Avaya IP Office. The trunk was configured by Vodafone DE with a length that was longer than the set of numbers provided for testing. In this case, it is expected behavior that the pilot/base number is used as the calling party.
- **Call Forward and Caller ID:** For inbound PSTN calls that are call forwarded to another PSTN endpoint, the forwarding party number is shown as the calling party instead of the original PSTN caller (forwarded party). This also impacts enterprise users with Twinning (mobility) enabled. These users have their inbound calls also ring a mobile

phone. On the mobile phone, the enterprise host number is shown as the calling party instead of the original PSTN caller.

- **Call Forward and SRTP:** For inbound PSTN calls that are call forwarded to another PSTN endpoint, the call results in no audio if SRTP is used on the connection between Avaya IP Office and the Avaya SBCE. This is believed to be an Avaya issue and is under investigation. As a workaround, this connection can be set to use TCP and RTP (Sections 5.5.3 and 5.5.6).
- **G.711 fax:** Some G.711 fax calls failed due to excessive jitter on the trunks used in the test environment.
- **G.729 and SRTP:** Inbound or outbound calls from an Avaya 96x1 H.323 phone to the PSTN using G.729 and encrypted media inside the enterprise results in one-way audio in the outbound direction from the enterprise. On an outbound call with G.729 selected, Vodafone requests a ptime of 30 and cannot be changed on a per customer basis. Inbound calls requests a ptime of 20 but the failure is the same. This issue is believed to be an issue with the Avaya 96x1 H323 phone. The issue has been raised to the Avaya development team and is under investigation. Other phone types tested (Avaya 16xx H.323 and Avaya 11xx SIP phones) did not have this issue. Workarounds include **one** of the following:
 - Do not use G.729 on the trunk to Vodafone DE (Section 5.5.6).
 - Do not use encryption TLS/SRTP internal to the enterprise (Sections 5.3.1 for signaling and Section 5.3.4 for media).
- **Intermittent loss of audio in one direction after session refresh in some call scenarios:** An outbound call from an Avaya 1100 Series SIP phone or Avaya Communicator for Web to the PSTN which is blind transferred to a local extension, would intermittently lose audio in one direction when a session refresh reINVITE was sent by Avaya IP Office. Audio may not be impacted on the first session refresh but may be impacted on subsequent session refreshes. A failure occurred approximately one in twelve calls. The issue has been raised to the Avaya development team and is under investigation. As a workaround, session refresh should be disabled (Section 5.5.2).

2.3. Support

For technical support on Vodafone DE products please visit the website at www.vodafone.de or contact an authorized Vodafone DE representative.

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

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 Vodafone DE SIP Trunk Service.

Located at the enterprise is the Avaya SBCE. It has a public side that connects to the Vodafone DE SIP Trunk Service. The private side of the Avaya SBCE 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 site contains an Avaya IP Office 500 V2 with various endpoints and a Windows PC running both Avaya IP Office Manager to configure Avaya IP Office and Avaya VoiceMail Pro for voicemail. In addition, the Avaya IP Office Application Server is present to support use of Avaya Communicator for Web (WebRTC client).

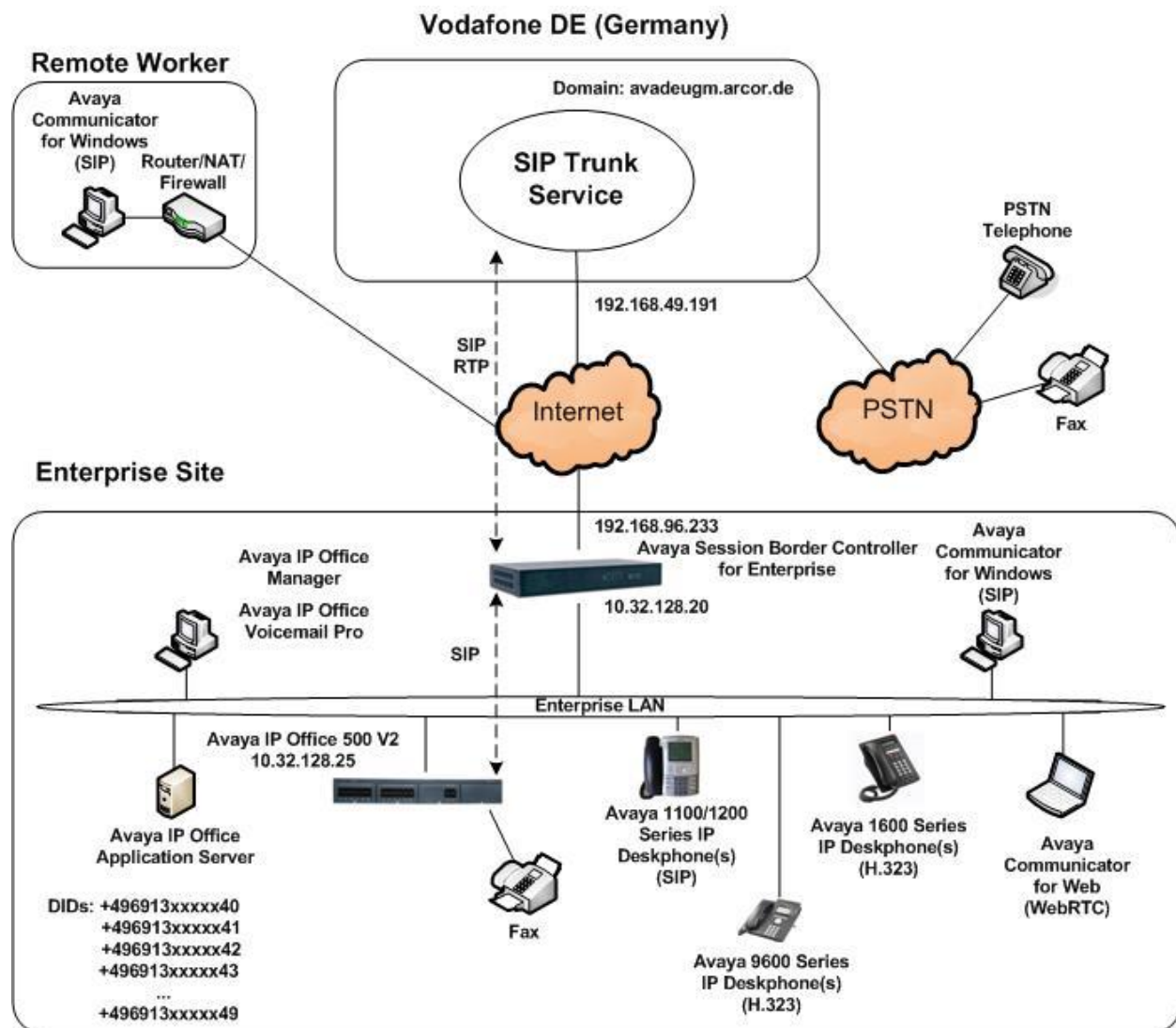


Figure 1: Avaya Interoperability Test Lab Configuration

For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes. Instead, public IP addresses have been replaced with private addresses and all phone numbers have been partially masked or replaced with numbers that cannot be routed over the PSTN.

For the purposes of the compliance test, users dialed a prefix digit 9 plus N digits to send an outbound call to the number N across the SIP trunk to the service provider. The short code of 9 was stripped off by Avaya IP Office and the remaining N digits were sent to the service provider network. For international calls, Avaya IP Office was configured to replace the dialed international access code (00) with a + sign in the SIP headers (**Section 5.5.8**). In the source headers (e.g., From, PAI, and Contact), Avaya IP Office was configured to send the DDI number assigned by Vodafone DE in international format (e.g., +496913xxxxxxx) (**Section 5.7**).

The Vodafone DE SIP Trunk Service sends the destination number in international format (e.g., +496913xxxxxxx) in the Request-Line and the To header in an inbound SIP INVITE message.

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 interoperability with the Vodafone DE SIP Trunk Service, they are not included in these Application Notes.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment	Software
Avaya IP Office 500 v2	10.0 SP3 (10.0.0.3.0 Build 5)
Avaya IP Office Manager	10.0 SP3 (10.0.0.3.0 Build 5)
Avaya IP Office VoiceMail Pro	10.0 SP3 (10.0.0.3.0 Build 5)
Avaya IP Office Application Server <ul style="list-style-type: none">• one-X® Portal• WebRTC Gateway	10.0 SP3 (10.0.0.3.0 Build 5) (10.0.0.3.0 Build 5) (10.0.0.3.0 Build 10)
Avaya Session Border Controller for Enterprise running on a Portwell CAD-0208 server	7.1 SP2 (7.1.0.2-01-13249)
Avaya 1140E IP Deskphone (SIP)	4.4 SP4 (4.04.23)
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3.5 (1.3.50B)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.6.4 (6.6401)
Avaya Communicator for Windows	2.1.3 (2.1.3.237)
Avaya Communicator for Web	1.0.16.1718

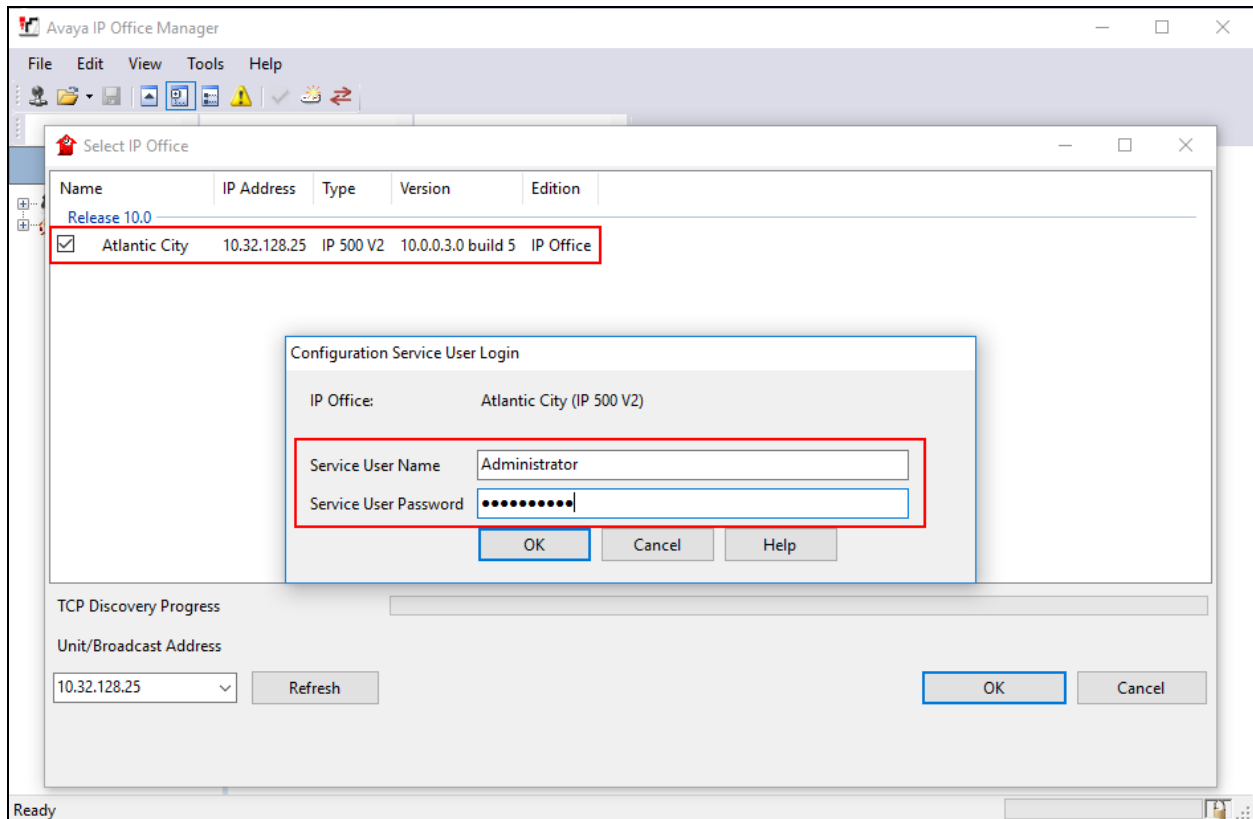
Vodafone DE Components	
Equipment	Software
Oracle Session Border Controller	7.2
Italtel Softswitch	20.50.52

Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with IP Office Server Edition in all configurations.

Avaya IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog/digital endpoints or analog/digital trunks.

5. Configure Avaya IP Office

Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the PC running Avaya IP Office Manager, select **Start → All Programs → IP Office → Manager** to launch the application. Select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials.



If the above screen does not appear, the configuration may be alternatively opened by navigating to **File → Open Configuration** at the top of the Avaya IP Office Manager window.

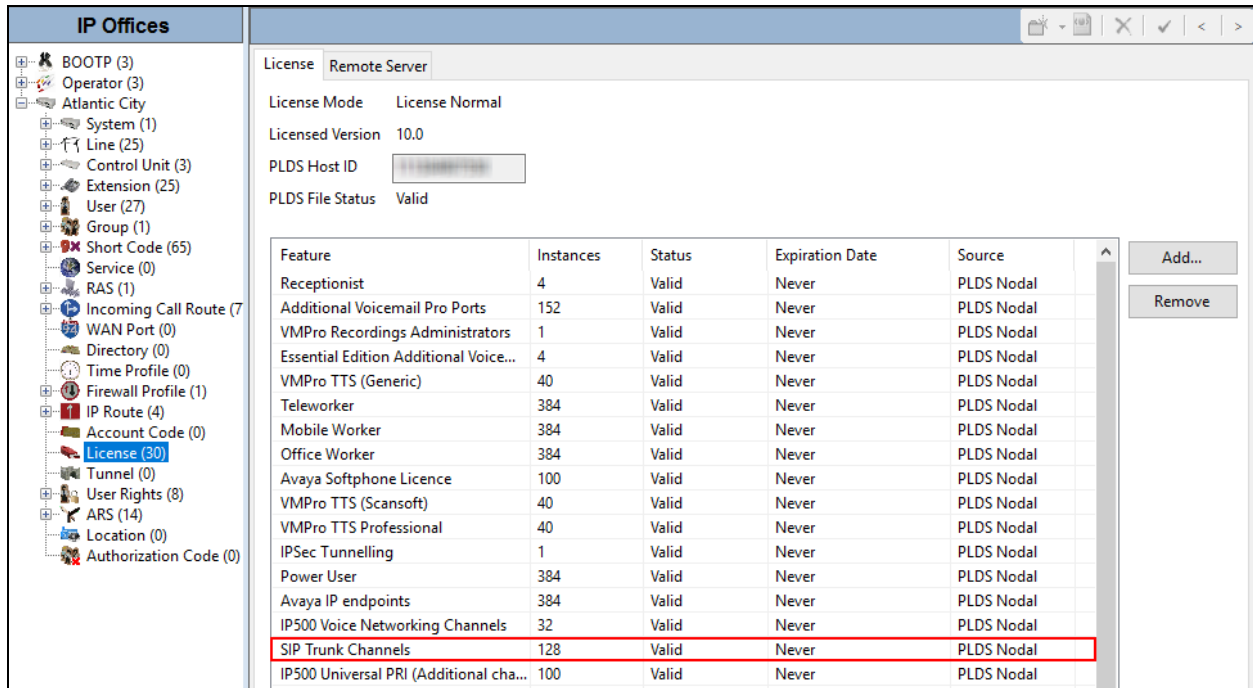
The appearance of the Avaya IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation pane on the left side, omit the Group pane in the center, and show the Details pane on the right side. Since the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

In the sample configuration, **Atlantic 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 **Atlantic City** in the Navigation Pane.

5.1. Licensing

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) appears in the Details pane.



The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'License (30)' selected. The main pane is titled 'License' and 'Remote Server'. It shows the following details:

- License Mode: License Normal
- Licensed Version: 10.0
- PLDS Host ID: [Redacted]
- PLDS File Status: Valid

Below these details is a table listing various features and their instances:

Feature	Instances	Status	Expiration Date	Source
Receptionist	4	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	1	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	4	Valid	Never	PLDS Nodal
VMPro TTS (Generic)	40	Valid	Never	PLDS Nodal
Teleworker	384	Valid	Never	PLDS Nodal
Mobile Worker	384	Valid	Never	PLDS Nodal
Office Worker	384	Valid	Never	PLDS Nodal
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	40	Valid	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	1	Valid	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Valid	Never	PLDS Nodal
SIP Trunk Channels	128	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Valid	Never	PLDS Nodal

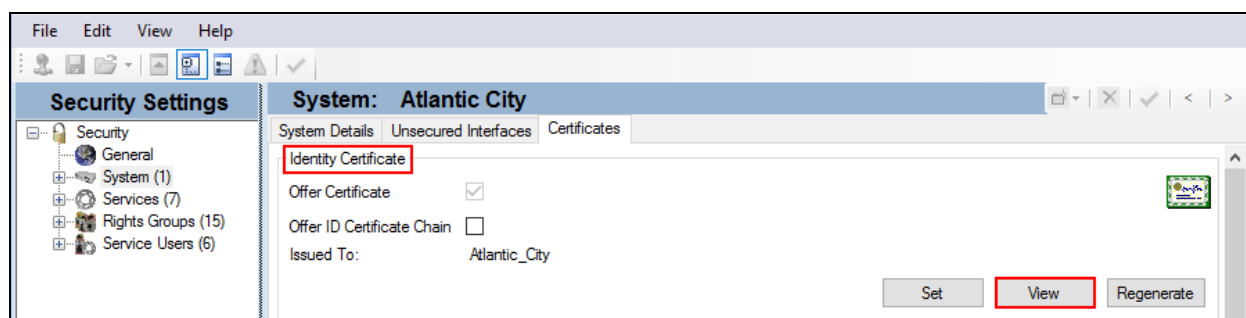
On the right side of the table, there are 'Add...' and 'Remove' buttons.

5.2. TLS Management

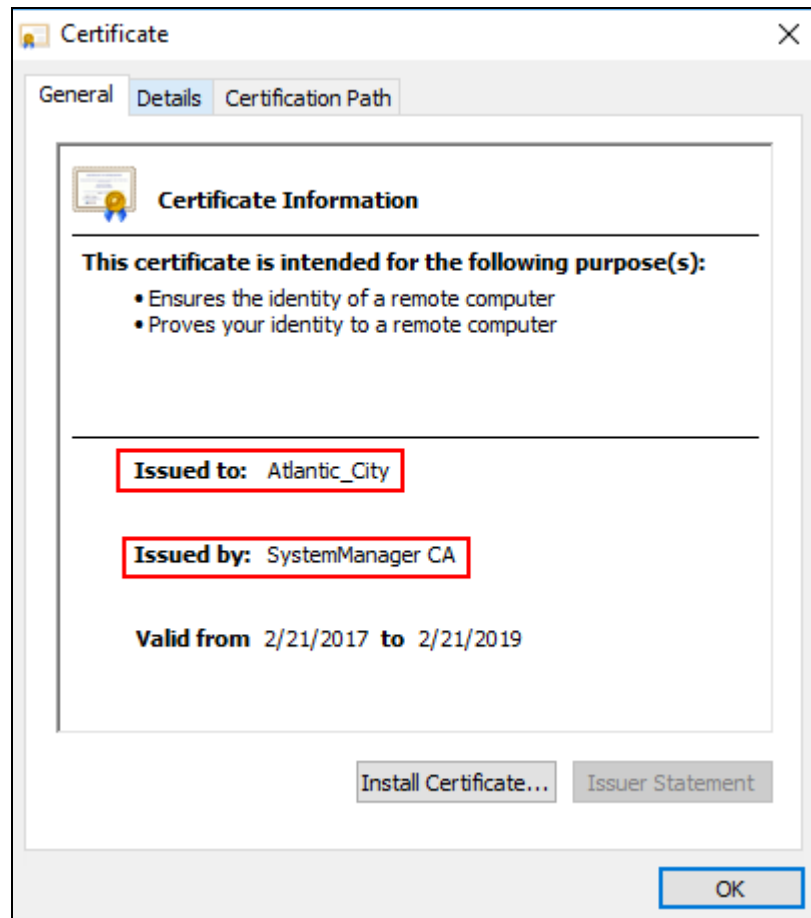
For the compliance test, the signaling on the SIP trunk between Avaya IP Office and the Avaya SBCE was secured using TLS. Testing was done using identity certificates signed by a local certificate authority **SystemManager CA**. The generation and installation of these certificates are beyond the scope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

To view the certificates currently installed on Avaya IP Office, navigate to **File → Advanced → Security Settings**. In the Security Settings window, navigate to **Security → System** and select the **Certificates** tab.

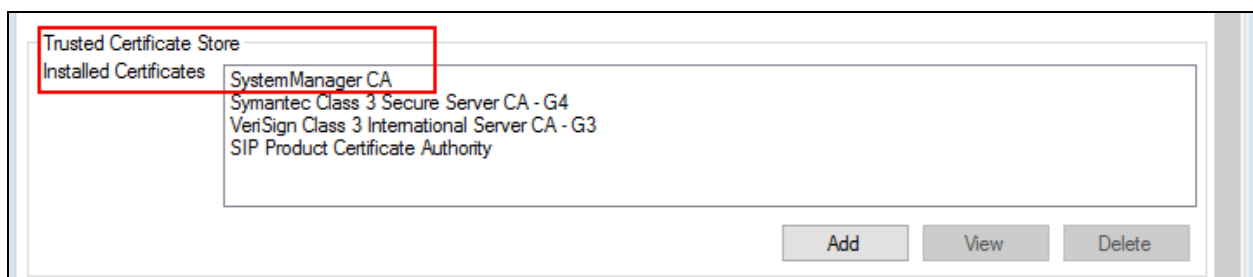
To verify the identity certificate, locate the **Identity Certificate** section and click **View** to see the details of the certificate.



A pop-up window will appear showing that the certificate is issued to the Avaya IP Office (**Atlantic_City**) and signed/issued by **SystemManager CA**. Click **OK** to close the pop-up window.



To verify the trusted certificates, return to the **Security → System → Certificates** tab and scroll down to the **Trusted Certificate Store** section. Verify that **SystemManager CA** is listed as an **Installed Certificate**.



5.3. System

Configure the necessary system settings.

5.3.1. 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 Avaya IP Office. In the case of the compliance test, the system name is **Atlantic 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. All other parameters should be set according to customer requirements.

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows the hierarchy: BOOTP (4), Operator (3), Atlantic City, System (1), Atlantic City, Line (27), Control Unit (4), Extension (25), User (27), Group (1), Short Code (65), Service (0), RAS (1), Incoming Call Route (0), WAN Port (0), Directory (0), Time Profile (0), Firewall Profile (1), IP Route (4), and Account Code (0). The 'Atlantic City' system is selected. The main pane shows the 'Atlantic City' configuration tabs: SMDR, VCM, VoIP, VoIP Security, Contact Center, System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, and SMTP. The 'LAN1' tab is active, and the 'LAN Settings' sub-tab is selected. The 'IP Address' field is set to 10 . 32 . 128 . 25, and the 'IP Mask' field is set to 255 . 255 . 255 . 0. Other fields include 'Primary Trans. IP Address' (0 . 0 . 0 . 0), 'RIP Mode' (None), 'Enable NAT' (unchecked), 'Number Of DHCP IP Addresses' (200), and 'DHCP Mode' (Disabled). An 'Advanced' button is visible at the bottom right.

Field	Value
IP Address	10 . 32 . 128 . 25
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"/> Dial In <input checked="" type="radio"/> Disabled

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

- In the test environment, Avaya IP Office endpoints used TLS for signaling. As a result, the **H.323 Signaling over TLS** was set to **Preferred**. To disable TLS on H.323 phones, then set **H.323 Signaling over TLS** to **Disabled**.
- Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks.
- To enable TLS for SIP endpoints, in the **Layer 4 Protocol** section, the **TLS** box was checked and the **TLS Port** was set to **5061**. To disable TLS on SIP phones, then uncheck the **TLS** box.

The screenshot displays the Avaya IP Office configuration interface for a system named 'Atlantic City'. The 'VoIP' tab is selected, and the 'Network Topology' section is active. The following parameters are configured and highlighted with red boxes:

- H.323 Signaling over TLS** is set to **Preferred**.
- SIP Trunks Enable** is checked.
- SIP Registrar Enable** is checked.
- Auto-create Extension/User** is unchecked.
- SIP Remote Extension Enable** is checked.
- SIP Domain Name** and **SIP Registrar FQDN** are empty text fields.
- Layer 4 Protocol** section:
 - UDP** is checked, **UDP Port** is 5060, **Remote UDP Port** is 5060.
 - TCP** is checked, **TCP Port** is 5060, **Remote TCP Port** is 5060.
 - TLS** is checked, **TLS Port** is 5061, **Remote TLS Port** is 5061.
- Challenge Expiration Time (sec)** is 10.

The **RTP** section is also visible, showing port ranges for Minimum and Maximum values, both set to 49152 and 53246.

Scroll down the page.

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

The screenshot shows the Avaya IP Office configuration interface for 'Atlantic City'. The 'Network Topology' tab is selected under the 'VoIP' section. The 'Keepalives' section is highlighted with a red box. It contains the following settings:

- ☒ Enable RTCP Monitoring on Port 5005
- RTCP collector IP address for phones: 0 . 0 . 0 . 0
- Scope: RTP-RTCP (dropdown)
- Periodic timeout: 30 (text input)
- Initial keepalives: Enabled (dropdown)

Below the 'Keepalives' section, there are 'DiffServ Settings' and 'DHCP Settings' sections. The 'DiffServ Settings' section includes fields for B8, DSCP(Hex), B8, Video DSCP (Hex), FC, DSCP Mask (Hex), 88, and SIG DSCP (Hex). The 'DHCP Settings' section includes fields for Primary Site Specific Option Number (4600/5600), Secondary Site Specific Option Number (1600/9600), VLAN, 1100 Voice VLAN Site Specific Option Number (SSON), and 1100 Voice VLAN IDs.

No configuration was necessary on the **LAN2 → Network Topology** tab for SIP Trunking since the **SIP Line → Transport** tab has the **Use Network Topology Info** field set to **None** (Section 5.5.3).

5.3.2. System - Telephony Tab

To access the System Telephony settings, navigate to the **Telephony** → **Telephony** tab in the Details Pane.

- Choose the **Companding Law** typical for the enterprise location. For the compliance test, **A-Law** was used for both **Switch** and **Line**.
- Enter or select **0** for **Hold Timeout (sec)** so that calls on hold will not time out.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN. If for security reasons incoming calls should not be allowed to transfer back to the PSTN then leave this setting checked.
- All other parameters should be set according to customer requirements.

The screenshot displays the 'Atlantic City' system configuration interface, specifically the 'Telephony' tab. The 'Telephony' sub-tab is active, showing settings for analogue extensions, dial delay, hold timeout, and companding law. The 'Hold Timeout (sec)' field is set to 0. The 'Companding Law' section shows 'A-Law' selected for the Switch and 'A-Law Line' selected for the Line. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked.

Setting	Value
Default Outside Call Sequence	Normal
Default Inside Call Sequence	Ring Type 1
Default Ring Back Sequence	Ring Type 2
Restrict Analogue Extension Ringer Voltage	<input type="checkbox"/>
Dial Delay Time (sec)	4
Dial Delay Count	0
Default No Answer Time (sec)	25
Hold Timeout (sec)	0
Park Timeout (sec)	300
Ring Delay (sec)	5
Call Priority Promotion Time (sec)	Disabled
Default Currency	USD
Default Name Priority	Favor Trunk
Media Connection Preservation	Disabled
Phone Failback	Manual
Login Code Complexity	<input type="checkbox"/> Enforcement Minimum length: 4 <input type="checkbox"/> Complexity
Companding Law	Switch: <input checked="" type="radio"/> A-Law Line: <input checked="" type="radio"/> A-Law Line
DSS Status	<input type="checkbox"/>
Auto Hold	<input checked="" type="checkbox"/>
Dial By Name	<input checked="" type="checkbox"/>
Show Account Code	<input checked="" type="checkbox"/>
Inhibit Off-Switch Forward/Transfer	<input type="checkbox"/>
Restrict Network Interconnect	<input type="checkbox"/>
Include location specific information	<input type="checkbox"/>
Drop External Only Impromptu Conference	<input type="checkbox"/>
Visually Differentiate External Call	<input type="checkbox"/>
Unsupervised Analog Trunk Disconnect Handling	<input type="checkbox"/>
High Quality Conferencing	<input checked="" type="checkbox"/>
Digital/Analogue Auto Create User	<input checked="" type="checkbox"/>
Directory Overrides Barring	<input type="checkbox"/>
Advertise Callee State To Internal Callers	<input type="checkbox"/>

5.3.3. System – VoIP

For the compliance test, all codecs were checked under **Available Codecs** and all were moved to the **Selected** group using the arrow buttons. The group of **Selected** codecs are the codecs which are available to the system for use. The list can be further restricted for the SIP trunk on the **SIP Line → VoIP** tab (Section 5.5.6). The **RFC2833 Default Payload** was left at the system default of **101**. Vodafone sends 106 as the payload value. For each call, the payload value was negotiated to 101 or 106; both values were used successfully.

The screenshot displays the 'Atlantic City' configuration window, specifically the 'VoIP' tab. The interface includes a top navigation bar with tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, and SMDR. Below this, there are sub-tabs for VCM, VoIP, VoIP Security, and Contact Center. The 'VoIP' sub-tab is active, showing several configuration options: 'Ignore DTMF Mismatch For Phones' (unchecked), 'Allow Direct Media Within NAT Location' (unchecked), and 'RFC2833 Default Payload' (set to 101). The 'RFC2833 Default Payload' field is highlighted with a red rectangle. Below these options, there are three main sections: 'Available Codecs', 'Default Codec Selection', and 'Selected'. The 'Available Codecs' section lists five codecs with checkboxes: G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, G.729(a) 8K CS-ACELP, and G.723.1 6K3 MP-MLQ. The 'Default Codec Selection' section is currently empty. The 'Selected' section, highlighted with a red rectangle, lists the same five codecs. Arrows between the sections indicate the ability to move codecs between the available, unused, and selected groups.

5.3.4. System – VoIP Security

For the compliance test, SRTP was used internal to the enterprise wherever possible. Thus, the **Media** parameter was set to **Preferred**, specifying that SRTP is preferred before RTP. One way to avoid the issue with Avaya 96x1 H.323 phones using SRTP and G.729 documented in **Section 2.2** is to set the **Media** parameter to **Disabled**. This will disable the use of SRTP to the enterprise phones. If SRTP is disabled for media, then TLS should be disabled for signaling (**Section 5.3.1**).

For the compliance test, **Media** was set to **Preferred** and the Media Security Options were set as follows:

- Under **Encryptions**, check **RTP**.
- Under **Authentications**, check **RTP**.
- Under **Crypto Suites**, both **SRTP_AES_CM_128_SHA1_80** and **SRTP_AES_CM_128_SHA1_32** were selected.
- Click **OK** to commit (not shown).

The screenshot shows the 'Atlantic City' configuration window with the 'VoIP Security' tab selected. The 'Media' dropdown is set to 'Preferred'. The 'Media Security Options' section is expanded, showing the following settings:

Category	Option	Status
Encryptions	RTP	Checked
	RTCP	Unchecked
Authentication	RTP	Checked
	RTCP	Checked
Replay Protection	SRTP Window Size	64
Crypto Suites	SRTP_AES_CM_128_SHA1_80	Checked
	SRTP_AES_CM_128_SHA1_32	Checked

5.4. IP Route

A default route is needed so IP Office can reach other network subnets other than the one where it resides. Since IP Office and the private side of the Avaya SBCE reside on the same subnet, the default route is not specifically used for SIP Trunking. 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 Address** and **IP Mask** to **0.0.0.0**.
- Set **Gateway IP Address** to the IP address of the default router on the network where Avaya IP Office is connected.
- For the **Destination**, select from the drop-down list the Avaya IP Office LAN interface that is used for this route (**LAN1**).

Click the **OK** button at the bottom of the page (not shown).

The screenshot displays the Avaya IP Office configuration window for an IP Route. The left-hand 'IP Offices' navigation pane shows a tree structure with 'IP Route (4)' selected, leading to the '0.0.0.0' configuration page. The main configuration area is titled 'IP Route' and '0.0.0.0'. A red rectangular box highlights the configuration fields: 'IP Address' (0 . 0 . 0 . 0), 'IP Mask' (0 . 0 . 0 . 0), 'Gateway IP Address' (10 . 32 . 128 . 254), and 'Destination' (LAN1). The 'Metric' is set to 0, and the 'Proxy ARP' checkbox is unchecked. The 'Destination' dropdown menu is open, showing 'LAN1' as the selected option.

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"/>

5.5. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Avaya SBCE. 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 5.5.1** 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 5.5.2 – 5.5.8**.

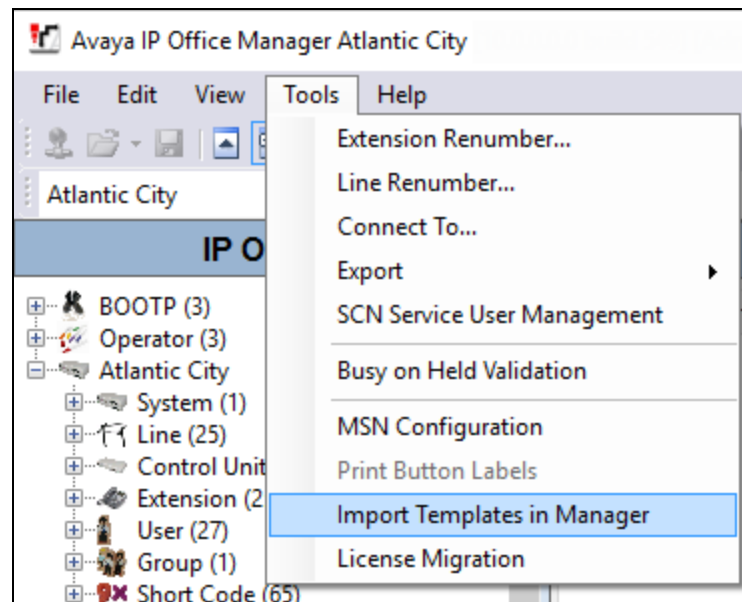
Also, the following SIP Line settings are not supported on Basic Edition:

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

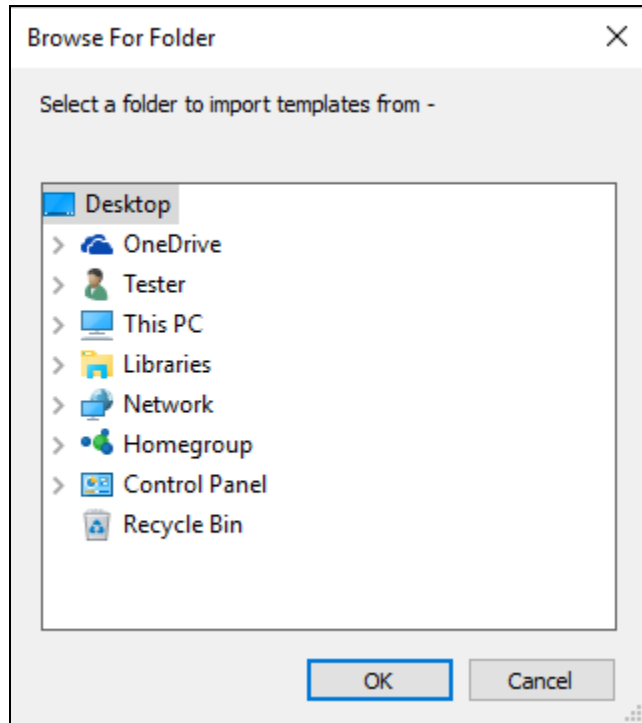
To create a SIP Line manually, right-click **Line** in the Navigation Pane and select **New → SIP Line**; then, follow the steps outlined in **Sections 5.5.2 – 5.5.8**.

5.5.1. SIP Line From Template

1. Copy the template file to the computer where IP Office Manager is installed. Place it in an empty directory. This is important because **Step 2** will import all templates located in this directory not just the template file associated with these Application Notes.
2. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy all the template files located in the selected directory into the IP Office template directory and make the templates available in the IP Office Manager pull-down menus in **Step 3**.



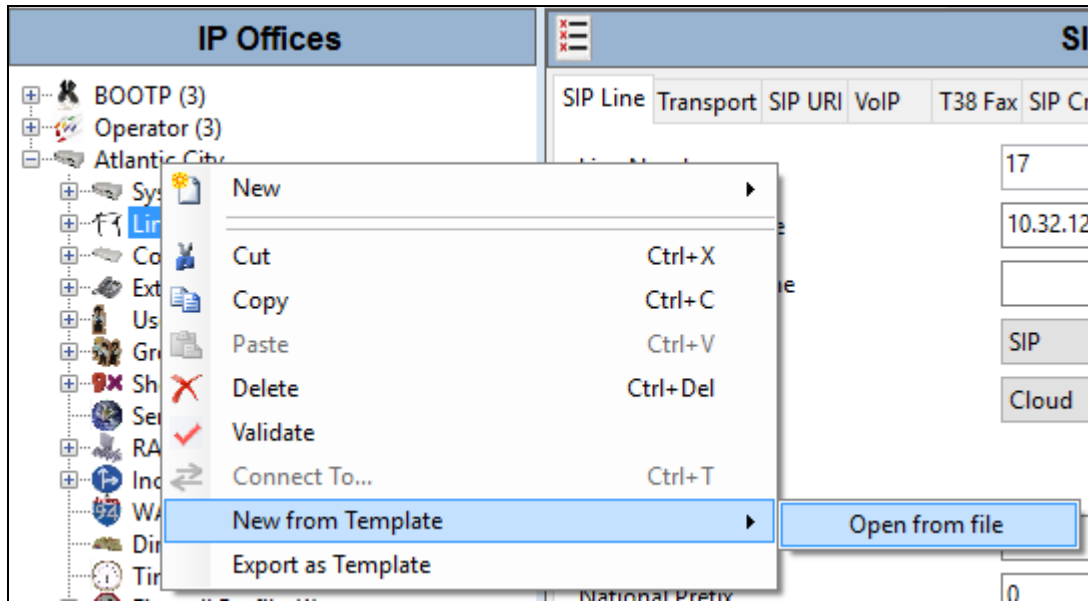
In the pop-up window that appears, select the directory where the template file was copied in **Step 1**, then click **OK**.



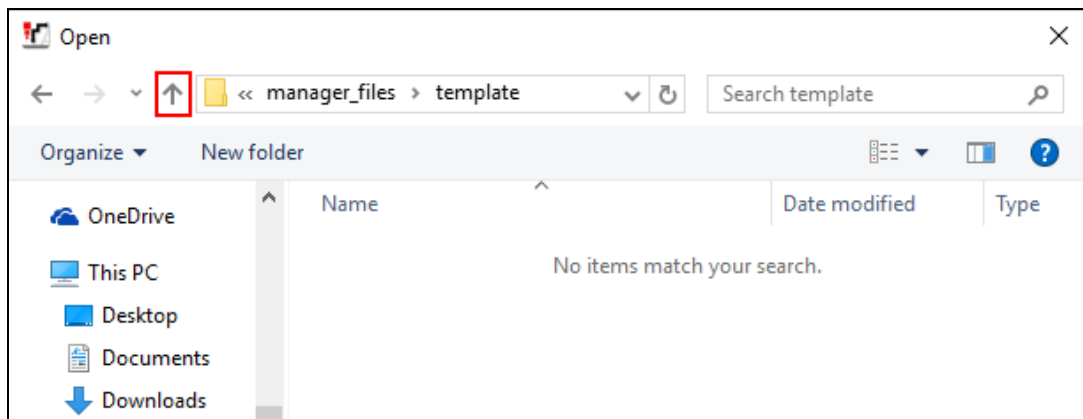
After the import is complete, a final import status pop-up window will appear stating success or failure (not shown). Click **OK** (not shown) to continue.

Note - Within Avaya IP Office Manager menus, the template directory may be accessed by navigating to **C:\Program Files\Avaya\IP Office\Manager\Templates**. However, the template directory is physically located in the User Access Control Virtual Store area of Windows. To view the directory from outside Avaya IP Office Manager (e.g., Windows Explorer), replace the **C:** portion of the template path above with **%UserProfile%\AppData\Local\VirtualStore**.

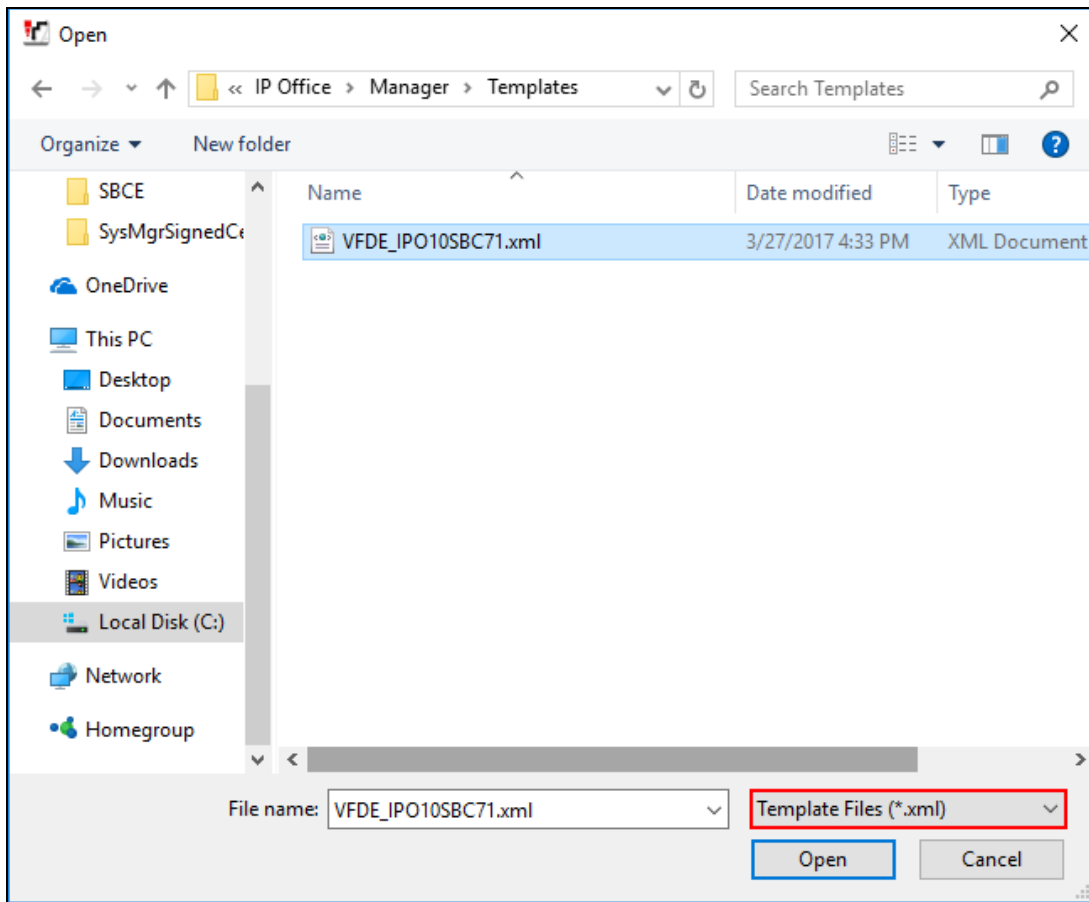
3. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, and select **New From Template** → **Open File**.



4. The subsequent pop-up window opens to **C:\Program Files\Avaya\IP Office\Manager\manager_files\template**. Navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates**. The up arrow icon can be used to move up through the directory tree.



- Once reaching the correct directory, select **Template Files (.xml)** in the lower right corner to ensure that .xml template files are displayed. From the list of template files, select the one to be used and click **Open**.



A final status pop-up window will appear stating whether the trunk creation was a success or failure (not shown). Click **OK** (not shown) to continue.

- Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.5.2 – 5.5.8**.

5.5.2. SIP Line – SIP Line Tab

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

- Set the **ITSP Domain Name** to the IP address of the internal signaling interface of the Avaya SBCE or this field may be left blank. If left blank, Avaya IP Office will automatically use the **ITSP Proxy Address (Section 5.5.3)** for this value which is also set 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 the **Check OOS** box. Avaya IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Set the **Refresh Method** to **Re-invite** and the **Timer (seconds)** to **On Demand**. This setting will disable session refresh messages from Avaya IP Office. This is recommended based on intermittent failures observed during testing (**Section 2.2**).
- Set the **National Prefix**, **International Prefix**, and **Country Code** to values appropriate for the location. In the case of the compliance test, the **National Prefix** was set to **0**, the **International Prefix** was set to **00** and the **Country Code** was set to **49** (Germany).
- Enter a **Description** for the trunk (optional).
- Set the **Incoming Supervised REFER** field and **Outgoing Supervised REFER** field to **Never** since Vodafone does not support the REFER method.
- Default values may be used for all other parameters.

The screenshot displays the 'SIP Line - Line 21' configuration window. The left sidebar shows a tree view of IP Office components. The main area has tabs for SIP Line, Transport, SIP URI, VoIP, T38 Fax, SIP Credentials, SIP Advanced, and Engineering. The 'SIP Line' tab is active, showing fields for Line Number (21), ITSP Domain Name, Local Domain Name, URI Type (SIP), Location (Cloud), Prefix, National Prefix (0), International Prefix (00), Country Code (49), Name Priority (System Default), and Description (Vodafone DE with SBCE). On the right, there are checkboxes for 'In Service' and 'Check OOS', both checked. Below these are 'Session Timers' with 'Refresh Method' set to 'Re-invite' and 'Timer (sec)' set to 'On Demand'. At the bottom right, 'Redirect and Transfer' settings show 'Incoming Supervised REFER' and 'Outgoing Supervised REFER' both set to 'Never'. Other options like 'Send 302 Moved Temporarily' and 'Outgoing Blind REFER' are unchecked.

5.5.3. SIP Line - Transport Tab

Select the **Transport** tab. Set or verify the parameters as shown below. TLS was used for the signaling connection between Avaya IP Office and the Avaya SBCE.

- Set the **ITSP Proxy Address** to the IP address of the internal signaling interface of the Avaya SBCE.
- Set **Layer 4 Protocol** to **TLS**. To avoid the issue of loss of audio on inbound calls from the PSTN that are call forwarded back to the PSTN (**Section 2.2**), the **Layer 4 Protocol** can be set to **TCP**, as well as setting the media to use RTP instead of SRTP (**Section 5.5.6**)
- Set **Use Network Topology Info** to **None**.
- If **Layer 4 Protocol** is set to **TLS**, then set the **Send Port** and **Listen Port** to **5061**. If **Layer 4 Protocol** is set to **TCP**, then the **Send Port** and **Listen Port** should be set to **5060**.
- Default values may be used for all other parameters.

The screenshot shows the 'SIP Line - Line 21' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' field is set to '10.32.128.20'. The 'Network Configuration' section is expanded, showing 'Layer 4 Protocol' set to 'TLS', 'Use Network Topology Info' set to 'None', 'Send Port' set to '5061', and 'Listen Port' set to '5061'. The 'Explicit DNS Server(s)' field is set to '0 . 0 . 0 . 0' and '0 . 0 . 0 . 0'. The 'Calls Route via Registrar' checkbox is checked. The 'Separate Registrar' field is empty.

SIP Line - Line 21	
SIP Line Transport SIP URI VoIP T38 Fax SIP Credentials SIP Advanced Engineering	
ITSP Proxy Address 10.32.128.20	
Network Configuration	
Layer 4 Protocol	TLS
Send Port	5061
Use Network Topology Info	None
Listen Port	5061
Explicit DNS Server(s) 0 . 0 . 0 . 0 0 . 0 . 0 . 0	
Calls Route via Registrar <input checked="" type="checkbox"/>	
Separate Registrar	

5.5.4. SIP Line – SIP Credentials

The Vodafone DE SIP Trunk Service does not require SIP credentials for registration or authentication so the **SIP Credentials** tab has no entry.

The screenshot shows a configuration window titled "SIP Line - Line 21". It features a tabbed interface with the following tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax, SIP Credentials (selected), SIP Advanced, and Engineering. The "SIP Credentials" tab is active, displaying a table with the following headers: Index, User Name, Authentication Name, Contact, Expiration (mins), and Register. The table is currently empty. To the right of the table are three buttons: "Add...", "Remove", and "Edit...". The window also includes a standard toolbar with icons for saving, deleting, and navigating.

Index	User Name	Authentication Name	Contact	Expiration (mins)	Register
-------	-----------	---------------------	---------	-------------------	----------

5.5.5. SIP Line - SIP URI Tab

The set of SIP URI entries define which incoming calls will be accepted on the line and provide configuration control of various SIP headers for outbound calls. A single SIP URI can be used for both incoming and outgoing calls but this requires that the **SIP Name** setting on the **User → SIP** tab (used in the From header for outbound calls) must match exactly with what the service provider sends in the Request-Line for inbound calls.

To create the entry for inbound and outbound calls, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**. For outbound calls, these settings will populate the user portion of the From and Contact headers as well as the display name with the contents of the **User → SIP** tab (Section 5.7). The From header is populated from the **SIP Name** field, while the Contact header and Display Name are populated from the **Contact** and **Display Name** fields respectively. The **User → SIP** tab is only present if a trunk in the system has a SIP URI using **Internal Data**. The **Local URI** setting also impacts inbound calls. In this case, an inbound call is only accepted if the user portion of the inbound INVITE Request-Line header matches a value configured on the system for a user (**User → SIP**), hunt group (**Hunt Group → SIP**) or voicemail (**System → Voicemail**).
- Under **Identity**, set **Identity** to **Use Internal Data** and **Header** to **P Asserted ID**. This enables the sending of the P-Asserted Identity (PAI) header in each outbound INVITE. The user portion of the PAI header will be populated from the **SIP Name** field on the **User → SIP** tab (Section 5.7).
- Under **Forwarding and Twinning**, set **Send Caller ID** to **Diversion Header**. With this setting, Avaya IP Office will include the Diversion header for calls that are forwarded or directed via Mobile Twinning out the SIP Line. The Diversion header will contain the redirecting party which is a DDI provided by the service provider.
- Set **Diversion Header** to **None**. This disables the sending of the Diversion header in each outbound INVITE. The Diversion header is only sent for **Forwarding and Twinning** as described above.
- For the **Registration** field, select **0: <None>** from the pull-down menu.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line in Section 5.8.1. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining Automatic Route Selection (ARS) or short code entries for routing outbound traffic to this line in Section 5.6. For the compliance test, a new incoming and outgoing group **21** was defined that only contained this line (line 21).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

Click **OK**.

SIP Line - Line 21

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

URI	Groups	Local URI	Contact	Display...	Identity	Header	Originator Number	Send Caller ID	Div

Add...
Remove
Edit...

New URI

Local URI Use Internal Data

Contact Use Internal Data

Display Name Use Internal Data

Identity

Identity Use Internal Data

Header P Asserted ID

Forwarding And Twinning

Originator Number

Send Caller ID Diversion Header

Diversion Header None

Registration 0: <None>

Incoming Group 21

Outgoing Group 21

Max Sessions 10

OK
Cancel

If **Use Internal Data** is selected, additional SIP URIs may be required to allow inbound calls to numbers not associated with a user, such as a short code. These URIs are created in the same manner as shown above with the exception that the incoming DDI number is entered directly in the **Local URI**, **Contact**, and **Display Name** fields.

5.5.6. SIP Line - VoIP Tab

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

- For **Codec Selection**, select **System Default** from the pull-down menu to use the default list of codecs. A list of the codecs in their current order of preference will be shown on the right in the **Selected** column. To use a custom list of codecs, select **Custom** for **Codec Selection**. Next, move unwanted codecs from the **Selected** column to the **Unused** column. Lastly, move the codecs up or down the list in the **Selected** column to achieve the desired order of preference. The example below shows the codecs used for the compliance test. One way to avoid the issue with Avaya 96x1 H.323 phones using SRTP and G.729 documented in **Section 2.2**, is to exclude G.729 in the **Selected** column.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box.
- Verify that **Allow Direct Media Path** is unchecked.
- 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.
- Set the **Fax Transport Support** to **G.711**. T.38 fax is not supported by the Vodafone DE SIP Trunk Service.
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- To use SRTP on the SIP Trunk, set **Media Security** to **Same as System (Preferred)** and verify that the **Same as System** box is checked. The system level media security is set to **Preferred** specifying that SRTP is preferred over RTP. To avoid the issue of loss of audio on inbound calls from the PSTN that are call forwarded back to the PSTN (**Section 2.2**), the SIP trunk can be configured to use RTP. To use RTP on the SIP Trunk, set **Media Security** to **Disabled**. If the trunk is set to use RTP for media, then signaling should be set to use TCP instead of TLS (**Section 5.5.3**).
- Default values may be used for all other parameters.

SIP Line - Line 21

SIP Line

Transport

SIP URI

VoIP

T38 Fax

SIP Credentials

SIP Advanced

Engineering

Codec Selection

Custom

Unused

G.711 ULAW 64K
G.722 64K
G.723.1 6K3 MP-MLQ

>>>

↑

<<<

↓

>>>

Selected

G.711 ALAW 64K
G.729(a) 8K CS-ACELP

☐ VoIP Silence Suppression

☐ Local Hold Music

☒ Re-invite Supported

☐ Codec Lockdown

☐ Allow Direct Media Path

☐ Force direct media with phones

☒ PRACK/100rel Supported

☐ G.711 Fax ECAN

Fax Transport Support

G.711

DTMF Support

RFC2833

Media Security

Same as System (Preferred)

Advanced Media Security Options

☒ Same As System

Encryptions

☒ RTP

☐ RTCP

Authentication

☒ RTP

☒ RTCP

Replay Protection

SRTP Window Size

64

Crypto Suites

☒ SRTP_AES_CM_128_SHA1_80
☒ SRTP_AES_CM_128_SHA1_32

5.5.7. SIP Line – T38 Fax Tab

Vodafone DE does not support T.38, so no changes are needed on the **T38 Fax** tab.

5.5.8. SIP Line – SIP Advanced

Select the **SIP Advanced** tab. Set the parameters as shown below.

- Set **Call Routing Method** to **Request URI**. Avaya IP Office will route calls based on the contents of the Request URI in the incoming INVITE.
- Check the **Use + for International** box. In outbound SIP headers, the user dialed international code (in this case 00) will be replaced with a + sign. For example, 0019085551234 will become +19085551234.
- Check the **Use PAI for Privacy** box. By default, Avaya IP Office uses the P-Preferred-ID header (PPI) for privacy calls. When this box is checked, the PAI header is used instead.

Click the **OK** button at the bottom of the page (not shown).

The screenshot displays the 'SIP Line - Line 21' configuration window with the 'SIP Advanced' tab selected. The 'Addressing' section shows 'Call Routing Method' set to 'Request URI'. The 'Identity' section has 'Use + for International' and 'Use PAI for Privacy' checked. The 'Media' section shows 'P-Early-Media Support' set to 'None' and 'Media Connection Preservation' set to 'Disabled'. The 'Call Control' section shows 'Call Initiation Timeout (s)' set to 4, 'Call Queuing Timeout (mins)' set to 5, 'Service Busy Response' set to '486 - Busy Here', 'on No User Responding Send' set to '408-Request Timeout', and 'Action on CAC Location Limit' set to 'Allow Voicemail'.

5.6. Short Codes

A short code is a dial pattern that triggers a specific function. A short code is used by the caller to route outbound traffic to a specific trunk or ARS route. To create a short code, right-click on **Short Code** in the Navigation Pane and select **New** (not shown). On the **Short Code** tab in the Details Pane, configure the parameters as shown below.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **9N;**. This short code 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**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value forms the user portion of the Request-Line and To headers of an outbound INVITE.
- Set the **Line Group Id** to the outgoing line group number defined on the SIP URI tab on the SIP Line in **Section 5.5.5**. Alternatively, the **Line Group ID** may point to an ARS route which allows for more comprehensive routing decisions based on the number dialed and available trunks. More information on using ARS may be found in [2].

Click the **OK** button (not shown).

The screenshot shows a software interface for configuring a short code. On the left is a tree view under 'IP Offices' with various categories like BOOTP, Operator, Atlantic City, System, Line, Control Unit, Extension, User, Group, Short Code (65), Service, RAS, Incoming Call Route, and WAN Port. The 'Short Code (65)' item is selected. The main area is titled '9N;; Dial' and contains a 'Short Code' tab. This tab has several input fields: 'Code' with the value '9N;;', 'Feature' with a dropdown set to 'Dial', 'Telephone Number' with the value 'N', 'Line Group ID' with a dropdown set to '21', 'Locale' with a dropdown, 'Force Account Code' with an unchecked checkbox, and 'Force Authorization Code' with an unchecked checkbox. A red rectangular box highlights the 'Code', 'Feature', 'Telephone Number', and 'Line Group ID' fields.

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** begins with the letter **W**, which means “withhold the outgoing calling line identification”.

In the case of the SIP Line documented in these Application Notes, when a user dials *67 plus the number, Avaya IP Office will include the calling number in the P-Asserted-Identity (PAI) header and will include the Privacy Id header.

Short Code	
Code	*67N;
Feature	Dial
Telephone Number	WN
Line Group ID	21
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

5.7. User

If the SIP Line is configured to use the **Use Internal Data** setting in **Section 5.5.5**, then 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 **Extn243**. Select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers for outgoing SIP trunk calls. The value entered in the **SIP Name** field is also used in the PAI and Diversion headers.

The example below shows the settings for user **Extn243**. The **SIP Name** and **Contact** are set to one of the DDI numbers assigned to the enterprise from Vodafone DE in international format.

The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all 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.

Click the **OK** button (not shown).

Extn243: 243	
Voice Recording Button Programming Menu Programming Mobility Group Membership	
User Voicemail DND Short Codes Source Numbers Telephony Forwarding Dial In	
Announcements SIP Personal Directory Web Self-Administration	
SIP Name	+496913...42
SIP Display Name (Alias)	Extn243
Contact	+496913...42

5.8. Incoming Call Route

An incoming call route maps an inbound DDI number on a specific line to an internal extension. This procedure should be repeated for each DDI number provided by the service provider. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**.

5.8.1. Incoming Call Route – Standard Tab

On the **Standard** tab of the Details Pane, enter the parameters as shown below.

- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.5.5**.
- Set the **Incoming Number** to the incoming number on which this route should match. The matching is performed from right to left. Thus, the local number was entered without the 0 prefix so it would match the number in local format (06913xxxxx42) or international format (+496913xxxxx42).
- Default values can be used for all other fields.

21 6913 42	
Standard Voice Recording Destinations	
Bearer Capability	Any Voice
Line Group ID	21
Incoming Number	6913 42
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

5.8.2. Incoming Call Route – Destinations Tab

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. Click the **OK** button (not shown). In this example, incoming calls to this number on line **21** are routed to extension **243**.

TimeProfile	Destination	Fallback Extension
Default Value	243 Extn243	

Incoming Call Routes for other direct mappings of DDI numbers to Avaya IP Office users listed in **Figure 1** are omitted here, but can be configured in the same fashion.

5.9. 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.

Save Configuration

IP Office Settings
Atlantic City

Configuration Reboot Mode

☒ Merge
☐ Immediate
☐ When Free
☐ Timed

Reboot Time
12:01

Call Barring

☐ Incoming Calls
☐ Outgoing Calls

OK Cancel Help

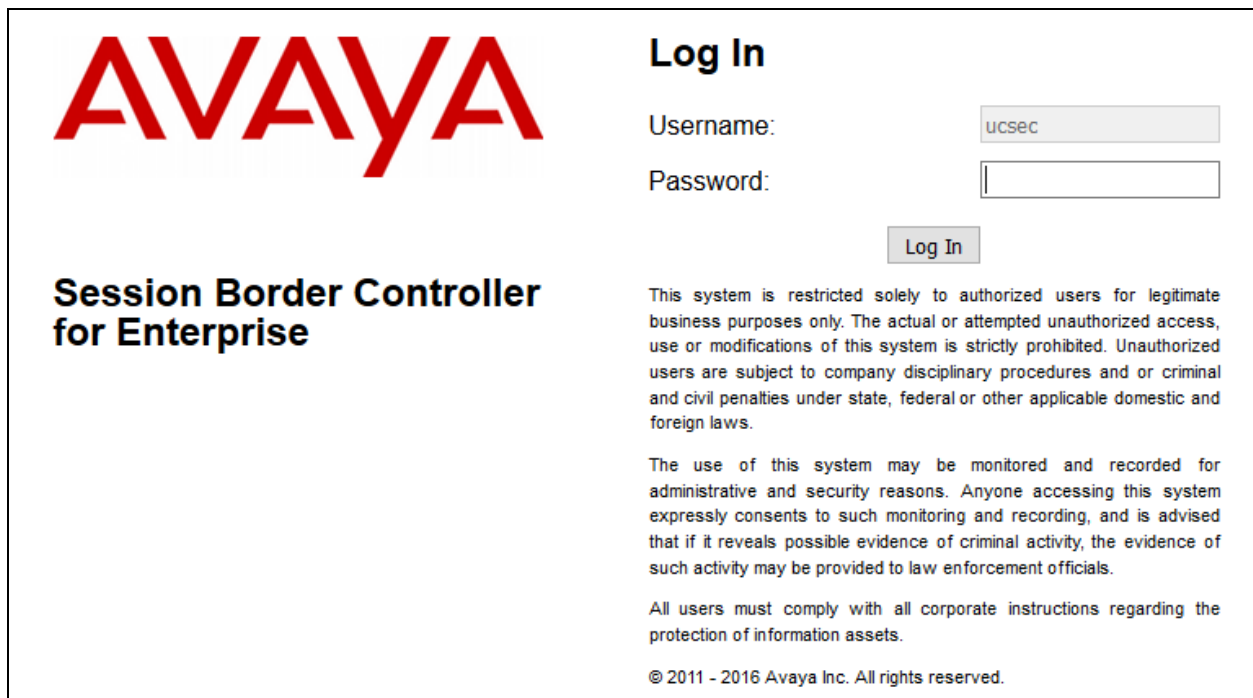
6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed, including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (i.e., A1 and B1).

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 the 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. On the right, under the heading 'Log In', there are input fields for 'Username:' (containing 'ucsec') and 'Password:'. Below these is a 'Log In' button. To the right of the button, there is a block of text: '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 is another block of text: '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.' At the bottom, it says 'All users must comply with all corporate instructions regarding the protection of information assets.' and '© 2011 - 2016 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.

Session Border Controller for Enterprise



Dashboard

Administration

Backup/Restore

System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- Device Specific Settings

Dashboard

Information

System Time	02:23:20 PM EDT	Refresh
Version	7.1.0.2-01-13249	
Build Date	Fri Mar 3 17:33:08 EST 2017	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	05/08/2017 17:11:38 EDT	
Failed Login Attempts	0	

Alarms (past 24 hours)

None found.

Installed Devices

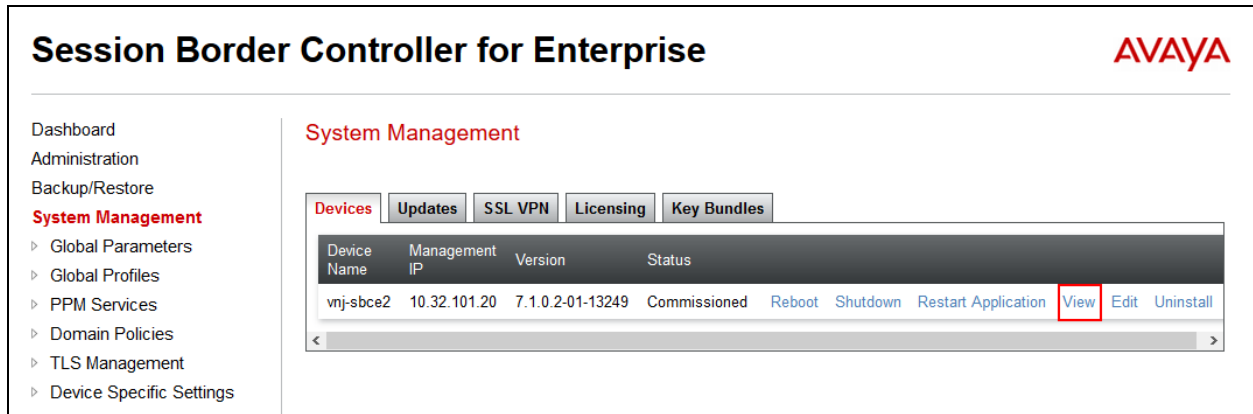
EMS
vnj-sbce2

Incidents (past 24 hours)

None found.

6.2. Verify Network Configuration and Enable Interfaces

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



Session Border Controller for Enterprise AVAYA

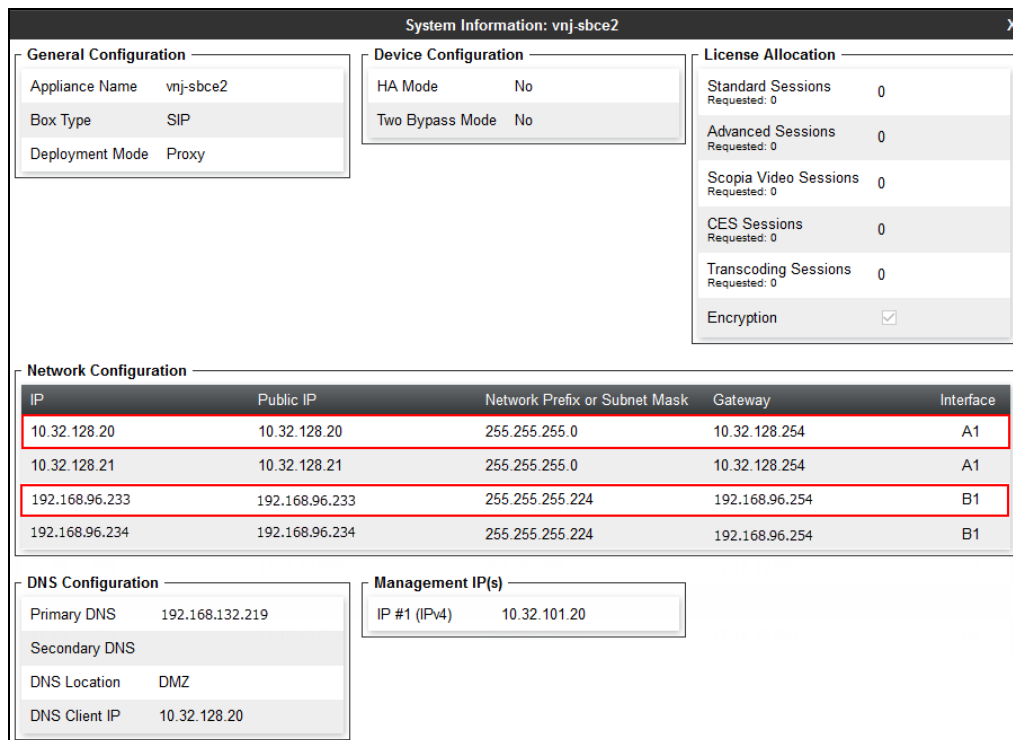
Dashboard
Administration
Backup/Restore
System Management
 ▸ Global Parameters
 ▸ Global Profiles
 ▸ PPM Services
 ▸ Domain Policies
 ▸ TLS Management
 ▸ Device Specific Settings

System Management

Devices Updates SSL VPN Licensing Key Bundles

Device Name	Management IP	Version	Status	
vnj-sbce2	10.32.101.20	7.1.0.2-01-13249	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

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



System Information: vnj-sbce2

General Configuration

Appliance Name	vnj-sbce2
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 0	0
Advanced Sessions Requested: 0	0
Scopia Video Sessions Requested: 0	0
CES Sessions Requested: 0	0
Transcoding Sessions Requested: 0	0
Encryption	<input checked="" type="checkbox"/>

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.32.128.20	10.32.128.20	255.255.255.0	10.32.128.254	A1
10.32.128.21	10.32.128.21	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
192.168.96.234	192.168.96.234	255.255.255.224	192.168.96.254	B1

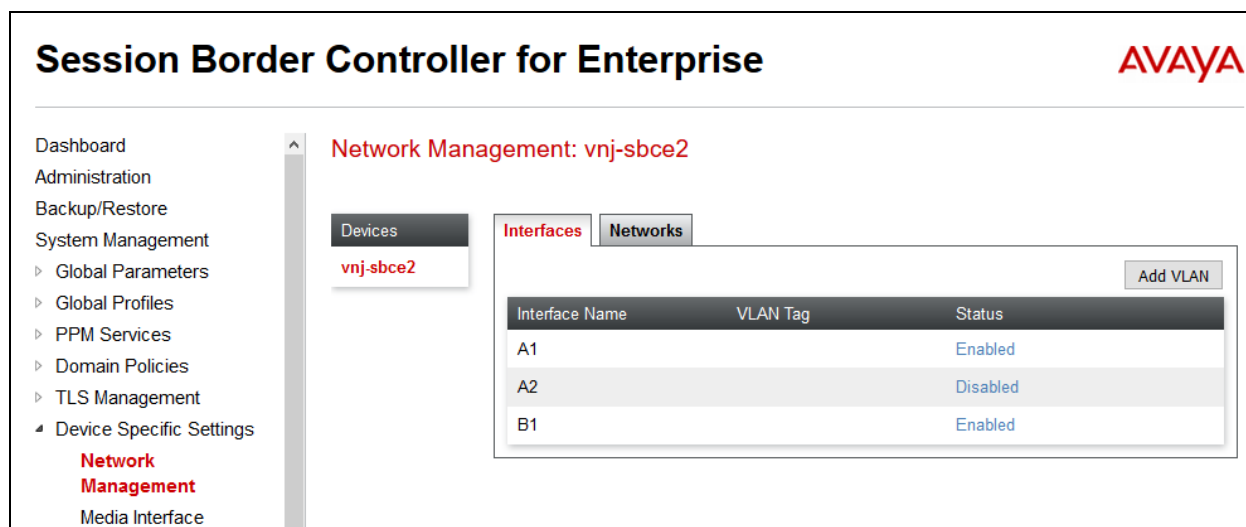
DNS Configuration

Primary DNS	192.168.132.219
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.32.128.20

Management IP(s)

IP #1 (IPv4)	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 **Interfaces** tab. Verify the **Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click the **Disabled** status to enable the interface.



6.3. TLS Management

For the compliance test, the signaling on the SIP trunk between Avaya IP Office and the Avaya SBCE was secured using TLS. Testing was done using identity certificates signed by a local certificate authority **SystemManager CA**. The generation and installation of these certificates are beyond the scope of these Application Notes. However, once the certificates are available, the following sections show how to view the certificates and configure the profiles to support the TLS connection.

6.3.1. Certificates

To view the certificates currently installed on the Avaya SBCE, navigate to **TLS Management** → **Certificates**. Perform the following:

- Verify that an Avaya SBCE identity certificate (**vnj_sbce2.crt**) is present under **Installed Certificates**.
- Verify that certificate authority root certificate (**System ManagerCA.crt**) is present under **Installed CA certificates**.
- Verify that private key associated with the identity certificate (**vnj_sbce2.key**) is present under **Installed Keys**.

Session Border Controller for Enterprise

AVAYA

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

Certificates

InstallGenerate CSR

Certificates

Installed Certificates

vnj_sbce2.crt	ViewDelete
AvayaSBC.crt	ViewDelete

Installed CA Certificates

Cisco_phone_CA.crt	ViewDelete
SystemManagerCA.crt	ViewDelete
AvayaSBCCA.crt	ViewDelete

Installed Certificate Revocation Lists

No certificate revocation lists have been installed.

Installed Keys

vnj_sbce2.vnjlabs.com.key	Delete
AvayaSBC.key	Delete
vnj_sbce2.key	Delete

Lastly, verify the Avaya SBCE identity certificate (**vnj_sbce2.crt**) was signed/issued by the certificate authority **System Manager CA**. Click **View** next to the identity certificate (**vnj_sbce2.crt**) to see the details of the certificate.

A pop-up window will appear showing that the **vnj_sbce2.crt** identity certificate was signed by **SystemManager CA**. Close the pop-up window.

View Certificate X

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 2862256211728751096 (0x27b8c6dc143f59f8)
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN=SystemManager CA, OU=MGMT, O=AVAYA
Validity
Not Before: Mar 1 16:34:33 2017 GMT
Not After : Mar 1 16:34:33 2019 GMT
Subject: CN=vnj-sbce2.vnjlabs.com, OU=SIL, O=AVAYA, L=Aberdeen, ST=NJ, C=US
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:

CTM; Reviewed:
SPOC 8/16/2017

Solution & Interoperability Test Lab Application Notes
©2017 Avaya Inc. All Rights Reserved.

41 of 74
VFDE_IPO10SBC71

6.3.2. Client Profile

To create a new profile, navigate to **TLS Management** → **Client Profile** in the left pane. In the right 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.

For the compliance test, client profile **sbce2Client** was created. This profile will be applied to the Avaya IP Office server configuration in **Section 6.7.1**. When configuring the profile, configure the parameters as follows:

- Set **Profile Name** to a descriptive name.
- Set **Certificate** to the identity certificate (**vnj_sbce2.crt**) to be sent by the Avaya SBCE.
- Set **Peer Verification** to **Required**.
- From the list of **Peer Certificate Authorities**, select the certificate authorities which will be accepted as signers of an incoming identity certificate from the far-end. For the test environment, the list must include **SystemManagerCA.crt** who is the signer of the Avaya IP Office identity certificate.
- Set **Verification Depth** to **1**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Client Profiles' selected under 'TLS Management'. The main content area is titled 'Client Profiles: sbce2Client' and includes an 'Add' button. Below this, a list of client profiles shows 'sbce2Client' selected. The configuration details for 'sbce2Client' are shown in a table-like format with sections: TLS Profile, Certificate Verification, Renegotiation Parameters, and Handshake Options. The 'sbce2Client' profile is highlighted with a red border. The 'Certificate Verification' section is also highlighted with a red border.

Client Profile	
Click here to add a description.	
TLS Profile	
Profile Name	sbce2Client
Certificate	vnj_sbce2.crt
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.crt AvayaSBCCA.crt
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:IDH:ADH:IMD5:1aNULL:1eNULL:@STRENGTH
Edit	

6.3.3. Server Profile

To create a new profile, navigate to **TLS Management** → **Server Profile** in the left pane. In the right 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.

For the compliance test, client profile **sbce2Srvr-Internal** was created. This profile will be applied to the Avaya SBCE internal signaling interface in **Section 6.4**. When configuring the profile, configure the parameters as follows:

- Set **Profile Name** to a descriptive name.
- Set **Certificate** to the identity certificate (**vnj_sbce2.crt**) to be sent by the Avaya SBCE.
- Set **Peer Verification** to **None**.
- Set **Verification Depth** to **1**.
- Under Handshake Options, for **Version** check the **TLS 1.0** box in addition to the **TLS 1.2** and **TLS 1.1** boxes to include TLS 1.0 as an acceptable TLS version for the connection. This is needed to support Avaya Communicator for Windows as a remote worker since it only supports TLS 1.0.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management (selected), Certificates, Client Profiles, **Server Profiles**, and Device Specific Settings. The main content area is titled 'Server Profiles: sbce2Srvr-Internal' and includes an 'Add' button and a 'Delete' button. Below this, there's a 'Click here to add a description.' link. The 'Server Profile' configuration form is shown with several sections: 'TLS Profile' (Profile Name: sbce2Srvr-Internal, Certificate: vnj_sbce2.crt), 'Certificate Verification' (Peer Verification: None, Extended Hostname Verification: unchecked), 'Renegotiation Parameters' (Renegotiation Time: 0, Renegotiation Byte Count: 0), and 'Handshake Options' (Version: TLS 1.2, TLS 1.1, and TLS 1.0 are all checked; Ciphers: Default, FIPS, and Custom are radio buttons; Value: HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH).

6.4. 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 (**vnj-sbce2**) 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 highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Signaling IP** to the IP address associated with the private interface (A1) specified in **Section 6.2**. For the external interface, set the **Signaling IP** to the IP address associated with the public interface (B1) specified 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. The internal interface was configured to listen for UDP or TCP on port **5060** and TLS on **5061**. Since TLS was selected, the **TLS profile** was set to **sbce2Svr-Internal** which point to the proper TLS certificate. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port **5060**. Since Vodafone DE uses UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE external interface for UDP only.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
 ▸ Global Parameters
 ▸ Global Profiles
 ▸ PPM Services
 ▸ Domain Policies
 ▸ TLS Management
 ▸ **Device Specific Settings**
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 ▸ DMZ Services
 TURN/STUN Service
 SNMP

Signaling Interface: vnj-sbce2

Devices
 vnj-sbce2

Signaling Interface

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

[Add](#)

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Ext_Sig_Intf	135.10.96.232 Network_B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete
Int_Sig_Intf	10.32.128.20 Network_A1 (A1, VLAN 0)	5060	5060	5061	sbce2Svr-Internal	Edit Delete
Int_Sig_Intf_RW	10.32.128.21 Network_A1 (A1, VLAN 0)	5060	---	5061	sbce2Svr-Internal	Edit Delete
Ext_Sig_Intf_RW	135.10.96.234 Network_B1 (B1, VLAN 0)	---	---	5061	sbce2Svr-Internal	Edit Delete

6.5. 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 (**vnj-sbce2**) 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 highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Media IP** to the IP address associated with the private interface (A1) specified in **Section 6.2**. For the external interface, set the **Media IP** to the IP address associated with the public interface (B1) specified 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



Dashboard

Administration

Backup/Restore

System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management

Device Specific Settings

- Network Management
- Media Interface**
- Signaling Interface
- End Point Flows
- Session Flows
- DMZ Services

Media Interface: vnj-sbce2

Devices

vnj-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 Network	Port Range	Edit	Delete
Int_Media_Intf	10.32.128.20 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Ext_Media_Intf	192.168.96.233 Network_B1-2 (B1, VLAN 0)	35000 - 40000	Edit	Delete
Int_Media_Intf_RW	10.32.128.21 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Ext_Media_Intf_RW	192.168.96.234 Network_B1-2 (B1, VLAN 0)	35000 - 40000	Edit	Delete

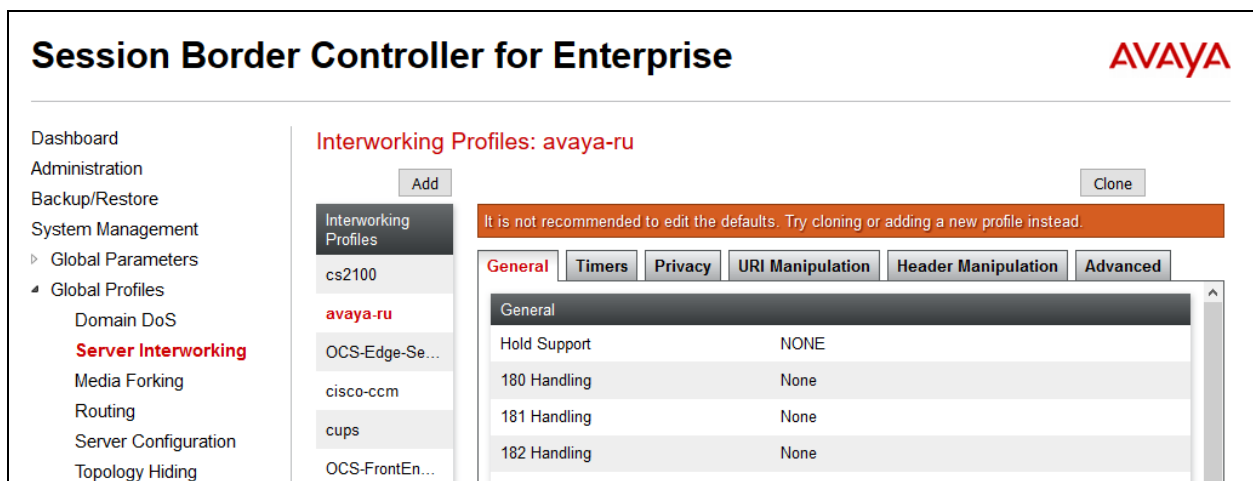
6.6. Server Interworking

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



6.6.1. Server Interworking – Avaya IP Office

The recommended method of creating a server interworking profile for Avaya IP Office is to first clone the predefined profile **avaya-ru** and then make any changes necessary to support a specific service provider. For the compliance test, server interworking profile **IPOffice** was created for Avaya IP Office using this approach and **T.38 Support** parameter was set to **No**. The **General** tab parameters are shown below.

The screenshot displays the configuration interface for a server interworking profile. At the top, there are six tabs: **General** (selected), **Timers**, **Privacy**, **URI Manipulation**, **Header Manipulation**, and **Advanced**. Below the tabs is a table of parameters. The **T.38 Support** parameter is highlighted with a red rectangular box. At the bottom of the table is an **Edit** button.

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

Edit

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs use default values.

The **Advanced** tab parameters are shown below. Highlighted values below indicate differences between the cloned profile and the default value.

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
<div>Record RoutesBoth Sides</div>					
<div>Include End Point IP for Context LookupYes</div>					
<div>ExtensionsAvaya</div>					
<div>Diversion ManipulationNo</div>					
<div>Has Remote SBCYes</div>					
<div>Route Response on Via PortNo</div>					
<div>Relay INVITE Replace for SIPRECNo</div>					
<div>DTMF</div>					
<div>DTMF SupportNone</div>					
<div>Edit</div>					

6.6.2. Server Interworking – Vodafone DE

For the compliance test, server interworking profile **VF-DE-Intwk** was created for the Vodafone DE SIP server. To create the profile, click **Add** (not shown). When creating the profile, the default values were used for all parameters including that the **T.38 Support** parameter was set to **No**. The **General** tab parameters are shown below.

The screenshot shows a configuration window with six tabs: General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The General tab is active and displays a list of parameters. The 'T.38 Support' parameter is highlighted with a red rectangular box. Below the list of parameters is an 'Edit' button.

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

Edit

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs use default values.

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

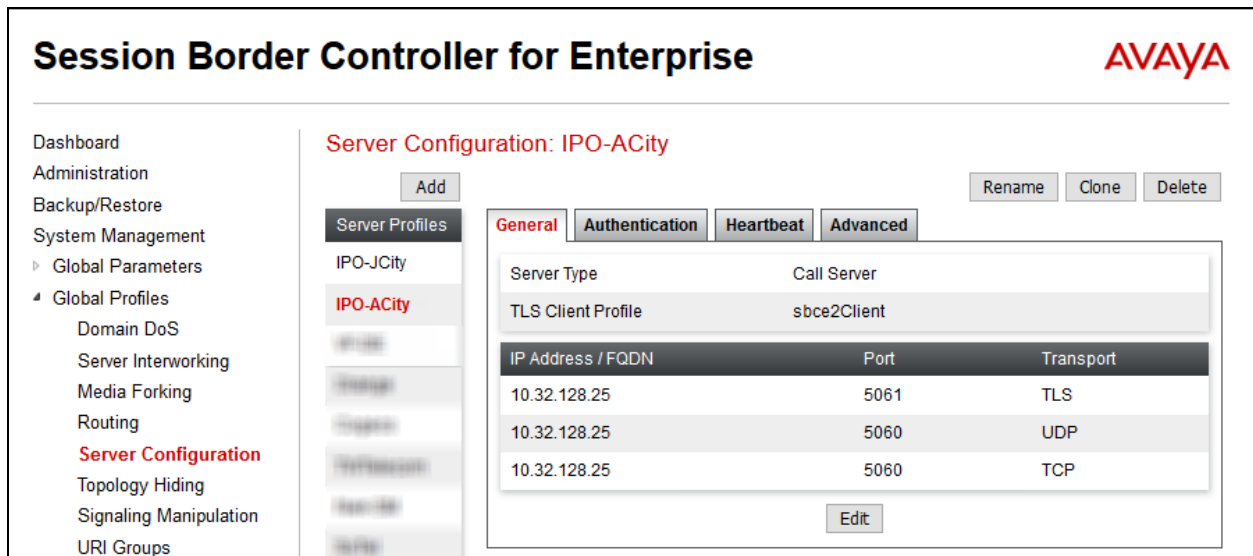
General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Record Routes		Both Sides			
Include End Point IP for Context Lookup		No			
Extensions		None			
Diversion Manipulation		No			
Has Remote SBC		Yes			
Route Response on Via Port		No			
Relay INVITE Replace for SIPREC		No			
DTMF					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

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 profile name will appear under **Server Profiles** in the center pane and 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 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 (expanded), and Server Configuration (selected). The main content area is titled "Server Configuration: IPO-ACity" and features an "Add" button. Below this is a list of server profiles: IPO-JCity, IPO-ACity (selected), and IPO-BCity. The right pane shows the configuration for the selected profile, IPO-ACity, with tabs for General, Authentication, Heartbeat, and Advanced. The General tab is active, showing the following configuration:

Server Type	Call Server	
TLS Client Profile	sbce2Client	
IP Address / FQDN	Port	Transport
10.32.128.25	5061	TLS
10.32.128.25	5060	UDP
10.32.128.25	5060	TCP

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

6.7.1. Server Configuration – Avaya IP Office

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

- Set **Server Type** to **Call Server**.
- Set **TLS Client Profile** to **sbce2Client** (Section 6.3.2).
- Set **IP Address / FQDN** to the Avaya IP Office LAN1 address (Section 5.3.1).
- Enter a valid combination of **Port** and **Transport** that Avaya IP Office may use to listen for SIP requests. For the compliance test, Avaya IP Office was configured to use port **5060** for **UDP/TCP** or port **5061** for **TLS**.

The screenshot shows the 'General' tab of a configuration interface. It contains the following fields and values:

Server Type	Call Server	
TLS Client Profile	sbce2Client	
IP Address / FQDN	Port	Transport
10.32.128.25	5061	TLS
10.32.128.25	5060	UDP
10.32.128.25	5060	TCP

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

The **Authentication** and **Heartbeat** tabs use the default values.

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Avaya IP Office defined in Section 6.6.1. Leave the other fields at the default values.

The screenshot shows the 'Advanced' tab of the configuration interface. It contains the following fields and values:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	IPOffice
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>

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

6.7.2. Server Configuration – Vodafone DE

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

- Set **Server Type** to **Trunk Server**.
- Set **IP Address / FQDN** to the Vodafone DE SIP proxy IP address provided by Vodafone DE.
- Enter a valid combination of **Port** and **Transport** that the Vodafone DE SIP proxy may use to listen for SIP requests. Additional combinations can be entered by clicking the **Add** button (not shown).

The screenshot shows the 'General' tab of a configuration window. At the top, there are four tabs: 'General' (selected), 'Authentication', 'Heartbeat', and 'Advanced'. Below the tabs, the 'Server Type' is set to 'Trunk Server'. A table lists the server details:

IP Address / FQDN	Port	Transport
192.168.49.191	5060	UDP

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

The **Authentication** and **Heartbeat** tabs use the default values.

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Vodafone DE defined in **Section 6.6.2**. Leave the other fields at the default values.

The screenshot shows the 'Advanced' tab of the same configuration window. The 'Interworking Profile' field is highlighted with a red rectangle and is set to 'VF-DE-Intwk'. Other fields include 'Enable DoS Protection', 'Enable Grooming', 'Signaling Manipulation Script' (set to 'None'), 'Securable', and 'Enable FGDN', all with checkboxes that are currently unchecked. An 'Edit' button is at the bottom right.

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**.

To create a new profile, navigate to **Domain Policies → Application Rules** 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.

For the compliance test, the application rules profile named **low-AudioSessions** was cloned from the **default-trunk** profile in which the settings for both **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** were adjusted down to **500** (from 2000) for **Audio**. This change was to accommodate the maximum capacity on the Avaya SBCE running on the Portwell CAD-0208 server. The **low-AudioSessions** application rules profile was used for both Avaya IP Office and the Vodafone DE SIP server.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, and System Management. Under 'Domain Policies', 'Application Rules' is selected. The main area is titled 'Application Rules: low-AudioSessions' and includes an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. A list of application rules is shown, with 'Audio' selected and highlighted by a red box. The 'Audio' rule has 'In' and 'Out' checkboxes checked, and 'Maximum Concurrent Sessions' and 'Maximum Sessions Per Endpoint' both set to 500. Below this is a 'Miscellaneous' section with 'CDR Support' set to 'None' and 'RTCP Keep-Alive' set to 'No'. An 'Edit' button is at the bottom right of the configuration area.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	500	500
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

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 end point policy group defined in **Section 6.11**. For the compliance test, a media rule was created for Avaya IP Office to use SRTP, while the predefined **default-low-med** media rule was used for the Vodafone DE SIP server.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation pane lists various system management options, with 'Domain Policies' expanded to show 'Media Rules' as the selected category. The main content area is titled 'Media Rules: default-low-med' and includes an 'Add' button and a 'Filter By Device...' dropdown. A warning banner states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing settings for 'Audio Encryption' and 'Video Encryption'. Both sections have 'Preferred Formats' set to 'RTP' and 'Interworking' checked. A 'Miscellaneous' section at the bottom shows 'Capability Negotiation' as unchecked. An 'Edit' button is located at the bottom right of the configuration area.

6.9.1. Media Rules – Avaya IP Office

For the compliance test, the media rule **IPO-SRTP-Pref** was created for Avaya IP Office. When creating the rule, configure the **Encryption** tab parameters as follows:

Under Audio Encryption and Video Encryption:

- Set **Preferred Formats** to **SRTP_AES_CM_128_HMAC_SHA1_80** followed by **RTP**.
The use of SRTP or RTP will be determined by the **Media Security** setting on the Avaya IP Office SIP Line described in **Section 5.5.6**.
- Check the **Interworking** box.

Under Miscellaneous:

- Check the **Capability Negotiation** box.

Default values were used for all other fields on this tab and the other **Media Rule** tabs.

The screenshot shows the 'Encryption' tab of a Media Rule configuration window. At the top, there are four tabs: 'Encryption' (selected), 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is divided into three sections: 'Audio Encryption', 'Video Encryption', and 'Miscellaneous'. Each section contains a table of settings. In the 'Audio Encryption' and 'Video Encryption' sections, 'Preferred Formats' is set to 'SRTP_AES_CM_128_HMAC_SHA1_80' followed by 'RTP'. 'Encrypted RTCP', 'MKI', and 'Lifetime' are all set to their default values, and 'Interworking' is checked. In the 'Miscellaneous' section, 'Capability Negotiation' is checked. An 'Edit' button is located at the bottom right of the configuration area.

Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

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

Edit

6.9.2. Media Rules – Vodafone DE

For the compliance test, the default media rule **default-low-med** was used for Vodafone DE SIP server. The **Encryption** tab parameters are as follows:

Under Audio Encryption and Video Encryption:

- The **Preferred Formats** is set to **RTP**.
- The **Interworking** box is checked.

Under Miscellaneous:

- The **Capability Negotiation** box is unchecked.

Default values were used for all other fields on this tab and the other **Media Rule** tabs.

The screenshot shows a configuration window with four tabs: **Encryption** (selected), **Codec Prioritization**, **Advanced**, and **QoS**. The **Encryption** tab is divided into three sections: **Audio Encryption**, **Video Encryption**, and **Miscellaneous**. In the **Audio Encryption** section, **Preferred Formats** is set to **RTP** and **Interworking** is checked. In the **Video Encryption** section, **Preferred Formats** is set to **RTP** and **Interworking** is checked. In the **Miscellaneous** section, **Capability Negotiation** is unchecked. An **Edit** button is located at the bottom right of the configuration area.

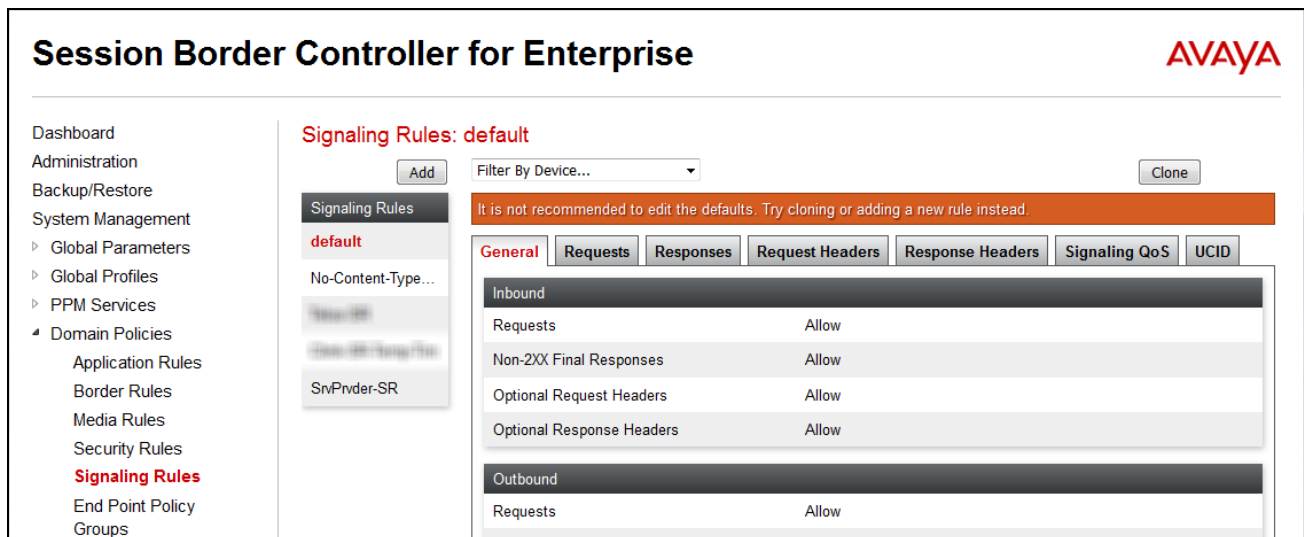
Section	Field	Value
Audio Encryption	Preferred Formats	RTP
	Interworking	<input checked="" type="checkbox"/>
Video Encryption	Preferred Formats	RTP
	Interworking	<input checked="" type="checkbox"/>
Miscellaneous	Capability Negotiation	<input type="checkbox"/>

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 end point policy group defined in **Section 6.11**. For the compliance test, the predefined **default** media rule (shown below) was used for both Avaya IP Office and the Vodafone DE SIP server.

To create a new profile, navigate to **Domain Policies → Signaling Rules** 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 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.



6.11. End Point Policy Groups

An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the service provider SIP server. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 6.14**.

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.

Session Border Controller for Enterprise

AVAYA

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

Policy Groups: default-low

Add
Filter By Device...

Policy Groups

default-low
default-low-enc
default-med
default-med-enc
default-high
default-high-enc
OCS-default-high
avaya-def-low-e...

It is not recommended to edit the defaults. Try adding a new group instead.

Hover over a row to see its description.

Policy Group

Summary
Add

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

6.11.1. End Point Policy Group – Avaya IP Office

For the compliance test, the end point policy group **IPO-EP-Policy** was created for Avaya IP Office. Default values were used for each of the rules which comprise the group with the exception of **Application** and **Media**. For **Application**, enter the application rule specified in **Section 6.8**. For **Media**, enter the media rule defined in **Section 6.9.1**.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling
1	low-AudioSessions	default	IPO-SRTP-Pref	default-low	default

6.11.2. End Point Policy Group – Vodafone DE

For the compliance test, the end point policy group **VF-DE-EP-Policy** was created for the Vodafone DE 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**.

Policy Group

Summary

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

CTM; Reviewed:
SPOC 8/16/2017

Solution & Interoperability Test Lab Application Notes
©2017 Avaya Inc. All Rights Reserved.

59 of 74
VFDE_IPO10SBC71

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 options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Server Interworking, Media Forking, Routing (highlighted), Server Configuration, and Topology Hiding. The main content area is titled 'Routing Profiles: To-IPO-ACity' and includes an 'Add' button. Below this is a list of routing profiles: 'default', 'To-IPO-ACity' (selected), 'To-IPO-JCity', 'To-Trunks', 'To-Accelerated', and 'To-SP'. The 'To-IPO-ACity' profile is expanded, showing a table with the following data:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.32.128.25	TLS	Edit Delete

Additional buttons visible include 'Update Priority', 'Add', 'Rename', 'Clone', and 'Delete'.

6.12.1. Routing - Avaya IP Office

For the compliance test, the routing profile **To-IPO-ACity** 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 **Load Balancing** to **Priority** from the pull-down menu.
- Enable **Next Hop Priority**.
- Click **Add** to enter the following for the Next Hop Address:
 - Set **Priority/Weight** to **1**.
 - For **Server Configuration**, select **IPO-ACity** (Section 6.7.1) from the pull-down menu. The **Next Hop Address** pull-down menu will show each entry of Address/Port/Transport defined in the **Server Configuration** selected. For the **Next Hop Address**, select the entry that represents the connection between Avaya IP Office and the Avaya SBCE. In this case, the connection used **TLS** on port **5061**.

Click **Finish**.

Profile : To-IPO-ACity - Edit Rule

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

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	IPO-ACity	10.32.128.25:5061 (TLS)	None	Delete

Finish

6.12.2. Routing – Vodafone DE

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

- Set the **URI Group** to the wild card * to match on any URI.
- Set **Load Balancing** to **Priority** from the pull-down menu.
- Enable **Next Hop Priority**.
- Click **Add** to enter the following for the Next Hop Address:
 - Set **Priority/Weight** to **1**.
 - For **Server Configuration**, select **VF-DE** (Section 6.7.2) from the pull-down menu. The **Next Hop Address** pull-down menu will show each entry of Address/Port/Transport defined in the **Server Configuration** selected. For the **Next Hop Address**, select the entry that represents the connection between Vodafone DE and the Avaya SBCE. This connection used **UDP** on port **5060**.

Click **Finish**.

Profile : To-Trunks - Edit Rule

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

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	VF-DE	192.168.49.191:5060 (UDP)	None	Delete

Finish

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 end point flow in **Section 6.14**.

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.

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▾ Global Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Server Configuration

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

▸ PPM Services

▸ Domain Policies

Topology Hiding Profiles: default

Add

Clone

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

Topology Hiding

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

Edit

6.13.1. Topology Hiding – Avaya IP Office

Avaya IP Office used the predefined **default** topology hiding profile shown below.

Topology Hiding			
Header	Criteria	Replace Action	Overwrite Value
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
<input type="button" value="Edit"/>			

6.13.2. Topology Hiding – Vodafone DE

The topology hiding profile for Vodafone DE (**VF-DE-TH**) was created by cloning the predefined **default** profile and changing the value of the **Request-Line**, **To** and **From** headers. The profile is configured to overwrite the host part of these headers with the Vodafone DE domain.

Topology Hiding			
Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	avadeugm.arcor.de
Refer-To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	avadeugm.arcor.de
To	IP/Domain	Overwrite	avadeugm.arcor.de
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
<input type="button" value="Edit"/>			

6.14. End Point Flows

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane includes sections for Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. Under Device Specific Settings, the 'End Point Flows' option is highlighted. The main content area is titled 'End Point Flows: vnj-sbce2'. It features a 'Devices' sidebar with 'vnj-sbce2' selected, and a 'Server Flows' tab. Below the tab is a table of server configurations for 'IPO-ACity'.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IPO-ACity	*	Ext_Sig_Intf	Int_Sig_Intf	IPO-EP-Policy	To-Trunks	View
2	IPO-ACity-RW	*	Ext_Sig_Intf_RW	Int_Sig_Intf_RW	RTP-EP-RW	default_RW	View

6.14.1. End Point Flow – Avaya IP Office

For the compliance test, the end point flow **IPO-ACity** 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-Trunks** 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 Vodafone DE SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Avaya IP Office in **Section 6.13.1**.

View Flow: IPO-ACity		X	
Criteria		Profile	
Flow Name	IPO-ACity	Signaling Interface	Int_Sig_Intf
Server Configuration	IPO-ACity	Media Interface	Int_Media_Intf
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	IPO-EP-Policy
Remote Subnet	*	Routing Profile	To-Trunks
Received Interface	Ext_Sig_Intf	Topology Hiding Profile	default
		Signaling Manipulation Script	None
		Remote Branch Office	Any

6.14.2. End Point Flow – Vodafone DE

For the compliance test, the end point flow **VF-DE-Flow** was created for the Vodafone DE SIP server. All traffic from Vodafone DE will match this flow as the source flow and use the specified routing profile **To-IPO-ACity** 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 Vodafone DE 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 Vodafone DE 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 Vodafone DE in **Section 6.13.2**.

View Flow: VF-DE-Flow

X

Criteria

Flow Name	VF-DE-Flow
Server Configuration	VF-DE
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_Intf

Profile

Signaling Interface	Ext_Sig_Intf
Media Interface	Ext_Media_Intf
Secondary Media Interface	None
End Point Policy Group	VF-DE-EP-Policy
Routing Profile	To-IPO-ACity
Topology Hiding Profile	VF-DE-TH
Signaling Manipulation Script	None
Remote Branch Office	Any

7. Vodafone DE SIP Trunk Service Configuration

Vodafone DE is responsible for the configuration of the Vodafone DE SIP Trunk Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise. In the case of the compliance test, this is the public IP address of the Avaya SBCE. Vodafone DE will provide the customer the necessary information to configure Avaya IP Office and the Avaya SBCE including:

- Vodafone DE SIP proxy IP address
- Transport protocol and port
- SIP Domain
- Supported codecs and order of preference
- DDI numbers

In addition, to configure any possible firewall/security devices at the enterprise, Vodafone DE will provide the IP address and port of any media sources that will need access to the enterprise.

8. Verification Steps

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

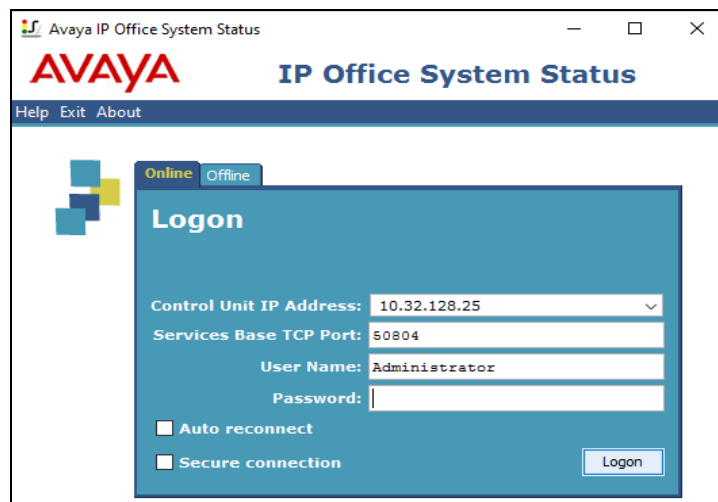
8.1. Avaya IP Office

Avaya IP Office has several tools that can be used to verify and troubleshoot the system operation. Two of these tools are described in the following subsections.

8.1.1. System Status

The System Status application is used to monitor and troubleshoot Avaya IP Office. Use the System Status application to verify the state of the SIP trunk. System Status can be accessed from **Start → All Programs → IP Office → System Status**.

The following screen shows an example **Logon** screen. Enter the Avaya IP Office IP address in the **Control Unit IP Address** field, and enter an appropriate **User Name** and **Password**. Click **Logon**.



The screenshot shows the 'Avaya IP Office System Status' application window. The title bar includes the Avaya logo and the text 'IP Office System Status'. Below the title bar is a menu bar with 'Help', 'Exit', and 'About'. The main content area has a 'Logon' dialog box. The dialog box has a 'Logon' title and a blue background. It contains the following fields and controls:

- Control Unit IP Address:** A dropdown menu with '10.32.128.25' selected.
- Services Base TCP Port:** A text field with '50804' entered.
- User Name:** A text field with 'Administrator' entered.
- Password:** A text field with a password mask (dots) entered.
- Auto reconnect:** A checkbox that is currently unchecked.
- Secure connection:** A checkbox that is currently unchecked.
- Logon:** A button to submit the login information.

At the top left of the dialog box, there are 'Online' and 'Offline' status indicators, with 'Online' being the active one.

Select the SIP line under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current State** does not indicate an error. The state of **Idle** indicates the channel does not have an active call.

Help Snapshot LogOff Exit About

System
Alarms (10)
Extensions (19)
Trunks (25)
Lines: 1 - 4
Lines: 5 - 8
Line: 17
Line: 18
Line: 19
Line: 20
Line: 21
Line: 22
Line: 23
Line: 24
Line: 25
Line: 26
Line: 27
Line: 28
Line: 29
Line: 30
Line: 31
Line: 32
Line: 33
Active Calls
Resources
Voicemail
IP Networking
Locations

Status Utilization Summary Alarms

SIP Trunk Summary

Line Service State: In Service
 Peer Domain Name: sip://10.32.128.20
 Resolved Address: 10.32.128.20
 Line Number: 21
 Number of Administered Channels: 10
 Number of Channels in Use: 0
 Administered Compression: G711 A, G729 A
 Enable Faststart: Off
 Silence Suppression: Off
 Media Stream: Best Effort
 Layer 4 Protocol: TLS
 SIP Trunk Channel Licenses: 128
 SIP Trunk Channel Licenses in Use: 0
 SIP Device Features:

Channel Number	U...	Call Ref	Current State	Time in State	Remote Media A...	Co...	Connection Type	Caller ID or ...	Other Party on Call	Direct...	Round Trip D...	Receive Jitter	Receive Pack...	Trans...	Trans...
1			Idle	00:00...											
2			Idle	00:13...											
3			Idle	00:13...											
4			Idle	00:13...											
5			Idle	00:13...											
6			Idle	00:13...											
7			Idle	00:13...											
8			Idle	00:13...											
9			Idle	00:13...											
10			Idle	00:13...											

Trace Trace All Pause Ping Call Details Graceful Shutdown Force Out of Service Print... Save As...

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

Status Utilization Summary Alarms

Alarms for Line: 21 SIP sip://10.32.128.20

Last Date Of Error	Occurrences	Error Description
--------------------	-------------	-------------------

8.1.2. Monitor

The Monitor application can also be used to monitor and troubleshoot Avaya IP Office. The Monitor application can be accessed from **Start → All Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select **Filters → Trace Options**.

The following screen shows the **SIP** tab, allowing configuration of SIP monitoring.

The screenshot shows the 'All Settings' dialog box with the 'SIP' tab selected. The dialog has a tabbed interface at the top with categories: T1, VPN, WAN, SCN, and Jade. Under 'T1' are ATM, ISDN, and Key/Lamp. Under 'VPN' are Call, DTE, Directory, and Media. Under 'WAN' are EConf, PPP, R2, and Frame Relay. Under 'SCN' are GOD, Routing, and Services. Under 'Jade' are H.323, SIP, Interface, and System. The 'SIP' tab is active, showing 'Events' and 'Packets' sections. In the 'Events' section, 'Sip' is checked with a dropdown set to 'Standard', 'STUN' is checked, and 'SIP Dect' is unchecked. In the 'Packets' section, 'SIP Reg/Opt Rx', 'SIP Reg/Opt Tx', 'SIP Call Rx', and 'SIP Call Tx' are unchecked. 'SIP Misc Rx' and 'SIP Misc Tx' are unchecked. 'Cm Notify Rx' and 'Cm Notify Tx' are unchecked. At the bottom of the 'Events' section, 'Sip Rx' and 'Sip Tx' are checked. To the right of these is an 'IP Filter (nnn.nnn.nnn.nnn)' field which is empty. At the bottom of the dialog are buttons: 'Default All', 'Clear All', 'Tab Clear All', 'Tab Set All', 'OK', 'Cancel', 'Save File', 'Load File', 'Load Partial File', and 'Select File'.

T1	VPN	WAN	SCN	Jade
ATM	Call	EConf	GOD	H.323
ISDN	Key/Lamp	PPP	Routing	Interface
	Directory	R2	Services	SIP
	Media	Frame Relay		System

Events

☒ **Sip** Standard ▼ ☒ **STUN** ☐ **SIP Dect**

Packets

☐ SIP Reg/Opt Rx ☐ SIP Misc Rx

☐ SIP Reg/Opt Tx ☐ SIP Misc Tx

☐ SIP Call Rx ☐ Cm Notify Rx

☐ SIP Call Tx ☐ Cm Notify Tx

☒ Sip Rx ☒ Sip Tx

IP Filter (nnn.nnn.nnn.nnn)

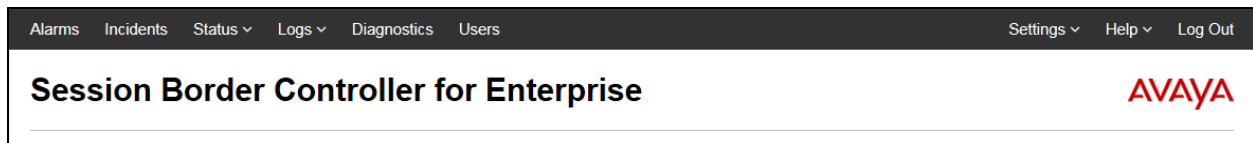
Default All Clear All Tab Clear All Tab Set All OK Cancel

Save File Load File Load Partial File Select File

8.2. Avaya Session Border Controller for Enterprise

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

- **Alarms:** This option provides information about active alarms.
- **Incidents:** This option provides detailed reports of anomalies, errors, policies violations, etc.
- **Status:** This option provides statistical and current status information.
- **Diagnostics:** This option provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office 10.0 and Avaya Session Border Controller for Enterprise 7.1 to the Vodafone DE SIP Trunk Service. The Vodafone DE SIP Trunk 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 Vodafone DE SIP Trunk Service passed compliance testing. Please refer to **Section 2.2** for any observations/exceptions.

10. Additional References

This section references documentation relevant to these Application Notes. In general, Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 31q, February 6, 2017.
- [2] *Administering Avaya IP Office Platform with Manager*, Release 10, September 2016.
- [3] *Using System Status*, Document Number 15-601758, Issue 11f, February 6, 2017.
- [4] *Administering Avaya IP Office Platform Voicemail Pro*, Document Number 15-601063, Issue 11f, November 22, 2016.
- [5] *Using IP Office System Monitor*, Document Number 15-601019, Issue 08b, November 25, 2016.
- [6] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.1, Issue 2, January 2017.
- [7] *Administering Avaya Session Border Controller for Enterprise*, Release 7.1, Issue 3, May 2017.

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

©2017 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.